

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

最終更新：2026 年 10 月 30 日

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

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

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

© 2026 Cisco Systems, Inc. All rights reserved.



目 次

第 1 章 新機能および変更された機能 Catalyst Center 1

第 I 部： はじめに 17

第 2 章 概要 Catalyst Center 19

Catalyst Center の概要 19

ログイン 19

初回セットアップ 20

Catalyst Center への初回ログイン 21

クイック スタート ワークフローの完了 23

デバイスログイン情報 26

Catalyst Center 設定方法 29

Express セットアップを完了します 30

標準セットアップの完了 31

エキスパートセットアップの完了 34

ユーザープロファイルのロールおよび権限 35

デフォルトホームページ 36

メイン メニュー 37

ツールバーアイコンとヘルプオプション 38

ホームページのデフォルトセクション 40

ネットワークとアクティビティのステータスアイコン 47

インタラクティブヘルプ 48

ホームページのカスタマイズ 49

Cisco.com とスマートアカウントのログイン情報の再認証 49

Catalyst Center ジャーニーマップ 50
リモートサポート許可ダッシュボードの表示 51
グローバル検索の使用 52
クロック形式を 12 時間または 24 時間に設定 54
Catalyst Center における明暗の外観の適用 55
ローカリゼーションの有効化 55
ウィンドウをお気に入りに追加 56
お気に入りの管理 57
Catalyst Center Insights への登録 58

第 3 章 テレメトリの設定 59
テレメトリの設定について 59
テレメトリを使用した syslog、SNMP トラップ、NetFlow コレクタサーバー、および有線クライアントデータ収集の設定 59
デバイスでのアプリケーションテレメトリ有効化の基準 61
アプリケーションテレメトリ設定のプロビジョニング 64
ワイヤレスコントローラ のアプリケーションテレメトリの有効化 65
新しいクラスタ仮想 IP アドレスを使用するためのアプリケーションテレメトリの更新 67
テレメトリを使用したデバイス設定の更新 69

第 II 部 : ネットワークインベントリとトポロジの検出および管理 71

第 4 章 ネットワークの検出 73
検出の概要 73
検出ダッシュボード 74
ディスカバリの前提条件 75
ディスカバリクレデンシャル 76
検出ログイン情報と Cisco ISE 82
検出ログイン情報のガイドラインと制限事項 82
検出ログイン情報の例 83
優先管理 IP アドレス 84

検出設定のガイドラインと制限事項 84
ディスカバリの実行 86
CDP を使用したネットワークの検出 86
IP アドレス範囲または CIDR を使用したネットワークの検出 90
LLDP を使用したネットワークの検出 92
ディスカバリジョブの管理 96
ディスカバリ ジョブの停止および開始 96
検出ジョブでのログイン情報の変更 96
ディスカバリジョブの複製 97
ディスカバリ ジョブの削除 97

第 5 章 インベントリの管理 99
インベントリについて 100
インベントリと Cisco ISE の認証 101
インベントリに関する情報の表示 102
デバイスに関する情報の表示 111
デバイスのインターフェイスに関する情報の表示 117
イーサネットポートに関する情報の表示 119
ポート詳細の管理 121
Cisco Catalyst スイッチのデバイスごとの設定を管理する 123
デバイスのレイヤ 2 設定の表示と編集 125
デバイスのレイヤ 3 設定の表示と編集 130
デバイスのセキュリティ設定の表示および編集 136
デバイスのネットワーク設定の表示と編集 139
デバイスの産業用設定の表示および編集 145
デバイスのポート設定の表示と編集 149
インベントリ ユーザー インターフェイスの機能強化 151
ユーザー定義フィールドの管理 153
ユーザー定義フィールドの作成 153
デバイスへのユーザー定義フィールドの追加 154
インベントリからのトポロジマップの起動 154

Catalyst Center インベントリ内のデバイスのタイプ 155
Catalyst Center インベントリへのデバイスの追加 155
ネットワークデバイスの管理 157
ネットワークデバイスの追加 157
ネットワーク デバイス クレデンシャルの更新 164
ネットワークデバイスのセキュリティフォーカス 169
デバイスの完全性検証ステータスの表示 170
デバイス証明書ステータスの表示 170
計算デバイスの管理 171
コンピューティングデバイスの追加 171
計算デバイスのログイン情報の更新 176
Cisco Meraki ダッシュボードの管理 180
Cisco Meraki ダッシュボードの統合 180
Cisco Meraki ダッシュボードのログイン情報の更新 181
Firepower Management Center の管理 181
Firepower Management Center の統合 181
Firepower Management Center のログイン情報の更新 182
サードパーティ製デバイスの追加 184
デバイスのフィルタリング 187
[Inventory] ウィンドウでのデバイスの管理 189
プロビジョニングされていないデバイスのサイトへの割り当て 189
プロビジョニングされたデバイスを別のサイトに割り当てる 191
デバイスのタグ付け 191
ネットワーク デバイス グループ タグの作成 192
ルールを使用したデバイスのタグ付け 193
デバイスタグの編集 194
タグの削除 195
SSH キー検証エラーへの対処 195
SSH キー変更の自動承認の設定 196
デバイスの REP リングの構成 196
非ファブリック展開用 REP リングへのノードの追加 198

非ファブリック展開用 REP リングからのノードの削除 200
非ファブリック展開用の MRP リング 201
非ファブリック展開用の MRP リングステータスの表示 201
Parallel Redundancy Protocol 203
PRP トポロジステータスの表示 204
ポートグループの作成 206
ポートへのタグの割り当て 207
ポート使用情報 208
デバイスのメンテナンスモード 208
デバイスのメンテナンスのスケジュール 208
デバイスのメンテナンススケジュールの管理 210
メンテナンス状態のデバイスの削除 211
インベントリインサイト 211
速度とデュプレックス設定の不一致 212
VLAN の不一致 212
システムビーコンの管理 213
デバイスのロール 214
デバイスロールを手動で変更する 215
デバイス管理 IP アドレスの更新 216
デバイスポーリング間隔の更新 216
デバイス情報の再同期 217
ネットワークデバイスの削除 218
コマンド ランナーを起動（インベントリ） 219
Run コマンドを使用したデバイスの到達可能性に関する問題のトラブルシューティング 220
CSV ファイルを使用したデバイス設定のインポート/エクスポート 221
CSV ファイルからのデバイス設定のインポート 222
デバイスデータのエクスポート 223
デバイスのログイン情報のエクスポート 224
デバイスの構成ドリフト 225
デバイスの構成ドリフトの表示 226
構成ドリフトのラベル付け 228

デバイス構成の可視性と制御 229
デバイス構成を今すぐまたは後で展開する 238
デバイス設定のプレビューと展開 238
ネットワーク プロビジョニングの事前チェック 240
故障したデバイスの交換 244
障害のあるアクセスポイントの交換 251
アウトオブバンド RMA デバイスの交換の管理 255
Catalyst Center の RMA ワークフローの制限事項 255
アクセスポイントの再起動 258

第 6 章 ネットワーク トポロジを表示 259
トポロジについて 259
エリア、サイト、ビルディング、フロアのトポロジの表示 260
トポロジマップでのデバイスのフィルタリング 261
デバイス情報の表示 262
リンク情報の表示 263
トポロジマップへのデバイスのピン留め 264
トポロジマップレイアウトの保存 265
トポロジマップレイアウトを開く 265
トポロジマップレイアウトの共有 266
トポロジのレイアウトをエクスポート 266

第 III 部 : ネットワークの設計 269

第 7 章 ネットワーク階層の設計 271
ネットワーク階層 271
新しいネットワーク階層の設計 273
既存の Cisco ネットワーク階層 274
Cisco Prime Infrastructure からのサイト階層のエクスポート 275
Cisco Prime Infrastructure からのマップアーカイブのエクスポート 276
Catalyst Center へのサイト階層のインポート 277

Catalyst Center へのマップアーカイブのインポート 277
既存の Ekahau ネットワーク階層の使用 278
Catalyst Center からの Ekahau プロジェクトのエクスポート 278
Ekahau プロジェクトを Catalyst Center にインポートします。 279
Ekahau サイト調査の Catalyst Center へのインポート 280
Catalyst Center からのネットワーク階層のエクスポート 282
Catalyst Center からのサイト階層のエクスポート 283
Catalyst Center からのマップアーカイブのエクスポート 283
ネットワーク階層の検索 284
ネットワーク階層の作成 285
サイトの作成、編集、削除 285
ビルディングの追加、編集、および削除 286
フロアの追加、編集、および削除 287
屋外エリアの追加、編集、削除 289

第 8 章 ワイヤレス 2D および 3D マップの操作 293
フロアマップの概要 293
ヒートマップの概要 294
マップファイルを使用したフロアの追加 295
フロアマップの作成方法 295
マップ内で使用するイメージファイルに関するガイドライン 296
CAD マップファイルを使用したフロアの追加 296
CAD 以外のマップファイルを使用したフロアの追加 299
2D マップの操作 302
2D フロアマップのデバイスとオーバーレイオブジェクトの 302
フロアマップでの AP の取り扱い 304
Cisco Prime Infrastructure からの AP のエクスポートと Catalyst Center へのインポート 304
マップへの AP の追加 306
マップへの計画済み AP の追加 307
マップへの計画済み AP の自動配置 309
マップ上の AP の自動検出 310

計画済み AP への実際の AP の割り当て 314
AP をマップ上に配置する 314
マップへの AP の再配置 318
AP の編集 318
複数の AP の編集 321
AP をマップから削除する 324
フロアマップでのセンサーの操作 324
マップへのセンサーの追加 325
センサーをマップ上に配置する 325
マップへのセンサーの再配置 326
マップでのセンサーの削除 326
カバレッジエリアの追加、編集、削除 327
吹き抜けの追加、編集、コピー、および削除 328
ロケーションリージョンの追加、編集、および削除 329
包含リージョンの追加、編集、および削除 329
除外リージョンの追加、編集、および削除 330
壁の追加、編集、および削除 331
シェルフユニットの追加、コピー、編集、および削除 332
マーカーの追加、編集、および削除 333
GPS マーカーの追加、編集、および削除 333
位置合わせポイントの追加、編集、および削除 334
2D ワイヤレスヒートマップの表示 335
2D マップツールバー 337
2D マップビューオプション 340
2D マップ ナビゲーション コントロール 344
AP アイコンと計画済み AP アイコンについて 345
管理対象 AP に接続されたアンマネージドスイッチの表示 347
フロアのデバイスデータのフィルタ処理 349
フロアマップでのワイヤレス干渉源の特定 350
3D マップの操作 351
3D マップにおけるフロアマップ要素とオーバーレイの設定 352

AP のクローンの作成 352
3D ワイヤレスヒートマップの表示 353
3D ワイヤレスマップツールバー 355
3D マップビューオプション 356
3D マップ ナビゲーション コントロール 360
3D ワイヤレスマップの一人称ビューと三人称ビューの使用 364
AP およびクライアントに関する詳細の表示 366
3D ワイヤレスマップからのインサイトの取得 367
ワイヤレス カバレッジ オプティマイザの実行 369
3D ワイヤレスマップのシミュレーションの作成 370

第 9 章 ネットワークの設定 373
ネットワーク設定の概要 373
サイトのタイムゾーンの設定 374
今日のメッセージの設定 375
Cisco ISE またはその他の AAA サーバーの追加 375
グローバル ネットワーク サーバーの設定 377
グローバル デバイス クレデンシャルの設定 379
グローバルデバイスログイン情報ワークフローの設定 379
グローバル CLI クレデンシャルの追加 379
グローバル SNMPv2c ログイン情報の追加 380
グローバル SNMPv3 ログイン情報の追加 382
グローバル HTTPS ログイン情報の追加 385
デバイスログイン情報のサイトへの割り当て 387
グローバルデバイスログイン情報の管理 389
サイトのデバイスへのデバイスログイン情報の適用 389
デバイスログイン情報のステータスの表示 392
グローバルデバイスログイン情報の編集のガイドライン 393
グローバル デバイス クレデンシャルの編集 394
デバイスログイン情報の削除 395
デバイス上のデバイスログイン情報の更新 396

IP アドレスプールを設定する 397
IP アドレスマネージャからの IP アドレスプールのインポート 398
CSV ファイルからの IP アドレスプールのインポート 398
IP アドレスプールの予約 399
IP アドレスプールをオーバーラップ 401
外部 IPAM 統合 402
重複する IP アドレスプールに関する注意事項と要件 403
重複する IP アドレスプールの障害対応 404
IP アドレスプールの編集 405
IP アドレスプールの削除 406
IP アドレスプールの複製 406
IP アドレスプールのリリース 407
IP アドレスプールの表示 407
サービス プロバイダ プロファイルの設定 413
グローバルワイヤレス設定の構成 414
ワイヤレスネットワーク設定ダッシュボードのカスタマイズ 415
エンタープライズ ワイヤレス ネットワーク用 SSID の作成 415
エンタープライズ ネットワークの SSID のサイトレベルのオーバーライドの設定 426
認証前アクセス制御リストの作成 427
エンタープライズ ワイヤレス ネットワーク用の AAA サーバーの設定 430
ゲスト ワイヤレス ネットワークの SSID の作成 432
ゲストネットワークの SSID に対するサイトレベルのオーバーライドの設定 444
ゲスト ワイヤレス ネットワーク用の AAA サーバーの設定 446
SSID スケジューラの作成 448
ワイヤレスインターフェイスの作成 449
非ファブリック展開用の VLAN グループの設計とプロビジョニング 450
ワイヤレス無線周波数プロファイルの作成 451
基本無線周波数プロファイルの編集または削除 466
基本無線周波数プロファイルの複製 467
AI 無線周波数プロファイルを設定するための前提条件 467
AI 無線周波数プロファイルの作成 468

AI 無線周波数プロファイルの編集 480
AI 無線周波数プロファイルの削除 481
AI 無線周波数プロファイルの複製 482
AI 拡張 RRM の設定 482
既存の AI RF プロファイルへの場所の割り当て 486
既存の AI RF プロファイルから場所の割り当てを解除 488
基本無線周波数プロファイルを AI 無線周波数プロファイルにアップグレードする 491
AP 認証リストの作成 492
AP 承認リストの編集または削除 495
AP LSC 更新プロファイルの作成 495
AP LSC 更新プロファイルの編集 497
AP LSC 更新プロファイルの削除 498
アンカーグループの作成 499
アンカーグループを編集または削除 501
AP プロファイル 501
Cisco IOS XE デバイスの AP プロファイルの作成 502
Cisco AireOS デバイスの AP プロファイルの作成 510
AP プロファイルの編集または削除 514
AP 電力プロファイルの作成 514
AP 電力プロファイルの編集または削除 516
非ファブリック展開用の Cisco センサー SSID のプロビジョニング 516
バックホール設定の管理 518
アンテナ無線プロファイルの作成 520
アンテナ無線プロファイルの編集または削除 521
Cisco Connected Mobile Experiences の統合について 521
Cisco CMX 設定の作成 521
Cisco Spaces 統合について 524
Cisco Spaces のサイトへの割り当て 524
Cisco Spaces を使用したサイトのモニタリング 525
FlexConnect VLAN の設定 526
802.11be プロファイルの作成 527

802.11be プロファイルの編集または複製 529
802.11be プロファイルの削除 530
ワイヤレス メッシュ ネットワークについて 531
証明書失効確認の設定 533

第 10 章 ネットワークプロファイルの設定 535
ネットワークプロファイルの概要 535
アシュアランス用のネットワークプロファイルの作成 535
ファイアウォール用のネットワークプロファイルの作成 537
ルーティング用のネットワークプロファイルの作成 539
スイッチ用のネットワークプロファイルの作成 541
ワイヤレス用のネットワークプロファイルの作成 543
ネットワークプロファイルへの SSID の追加 544
ネットワークプロファイルへの AP ゾーンの追加 547
ネットワークプロファイルへの機能テンプレートの追加 549
ネットワークプロファイルへのテンプレートの追加 549
AP グループ、Flex グループ、サイトタグ、およびポリシータグの概要 550
カスタム AP グループと Flex グループの再利用の例 556
カスタムポリシータグの再利用の使用例 559
ネットワークプロファイルへの AP グループ、Flex グループ、サイトタグ、およびポリシータグの追加 563
ネットワークプロファイルの追加インターフェイスの構成 566

第 IV 部 : ネットワークデバイスの設定と保守 569

第 11 章 デバイス設定の変更を自動化するテンプレートの作成 571
CLI テンプレートについて 571
オンボーディング テンプレートまたは Day-0 テンプレート 573
Day-n テンプレートを使用したネットワークデバイスへの設定の展開 574
プロジェクトの作成 575
テンプレートの作成 575

標準テンプレートの作成 576
ブロックリストコマンド 578
サンプルテンプレート 578
コンポジットテンプレートの作成 579
テンプレートの編集 581
テンプレートのシミュレーション 582
テンプレートのエクスポート 582
テンプレートのインポート 583
テンプレートの複製 584
ネットワークプロファイルへの CLI テンプレートの関連付け 585
CLI テンプレートのプロビジョニング 586
プロジェクトのエクスポート 587
プロジェクトのインポート 587
テンプレート変数 588
変数バインド 589
特別なキーワード 593
テンプレートのネットワークプロファイルへの関連付け 596
CLI テンプレートの競合の検出 598
CLI テンプレートとサービス プロビジョニング インテント間の潜在的な設計競合の検出 598
CLI テンプレートのランタイム競合の検出 599

第 12 章 機能テンプレートの設計 603
機能テンプレートの概要 603
サポートされている機能テンプレート 604
レガシーデバイスからの設計の検出と作成 604
AAA RADIUS 属性の機能テンプレートの作成 605
高度な SSID の機能テンプレートの作成 606
Cisco CleanAir の機能テンプレートの作成 613
Dot11ax 設定用の機能テンプレートの作成 615
Dot 11be ステータス設定用の機能テンプレートの作成 618

イベント駆動型 RRM 設定の機能テンプレートの作成 619
Flex 設定の機能テンプレートの作成 620
グローバル IPv6 設定の機能テンプレートの作成 622
マルチキャストの機能テンプレートの作成 623
RRM FRA パラメータの機能テンプレートの作成 624
RRM 一般パラメータの機能テンプレートの作成 626
不正な一般パラメータ用の機能テンプレートの作成 628

第 13 章 ソフトウェア イメージの管理 631
ソフトウェアイメージ管理について 631
ソフトウェアイメージの完全性検証 632
ソフトウェア イメージの表示 632
推奨されるソフトウェアイメージの使用 637
ソフトウェアイメージのインポート 638
デバイスファミリに対するソフトウェアイメージの割り当ての管理 640
イメージ更新のスケジュール 642
デバイスのソフトウェアイメージをインストールモードでアップロードする 644
標準ソフトウェアイメージについて 646
ソフトウェアイメージをスタンダードとしてマークする 646
標準ソフトウェアイメージの管理 649
イメージ配信サーバーの設定 651
イメージ配信サーバーのプロトコル順序の変更 652
サイトへのイメージ配信サーバーの追加 653
ソフトウェアイメージのプロビジョニング 653
ISSU 互換性マトリックスのインポート 656
ISSU または xFSU を使用したソフトウェアイメージのアップグレード 657
デバイスのアップグレードの準備の事前チェックリスト 660
イメージ更新ステータスの表示 661
イメージ更新ワークフローの表示 662
自動フラッシュクリーンアップ 664

第 14 章 ネットワークデバイスのコンプライアンス監査 665
コンプライアンスの概要 665
コンプライアンスカテゴリ 666
ネットワークのコンプライアンスの監視 675
設定コンプライアンスの管理 676
コンプライアンス設定の構成 678
コンプライアンスサマリーの表示 680
手動コンプライアンスの実行 682
ネットワークデバイスのコンプライアンス監査レポートの生成 683
コンプライアンス違反の確認 683
デバイスのスタートアップ設定と実行中の設定の同期 685
コンプライアンス違反の修正 686
デバイスのアップグレード後のコンプライアンス動作 687
CLI テンプレートコンプライアンスの制限事項 688

第 15 章 デバイスの診断コマンドを実行 691
コマンドランナーの概要 691
デバイスの診断コマンドの実行 691

第 V 部 : ネットワークのプロビジョニング 693

第 16 章 プラグアンドプレイを使用したデバイスのオンボーディングとプロビジョニング 695
プラグアンドプレイ プロビジョニングの概要 695
プラグ アンド プレイ プロビジョニングの前提条件 698
プラグアンドプレイのシステム証明書の要件 701
DHCP コントローラディスカバリ 702
DNS コントローラディスカバリ 704
Plug and Play Connect コントローラディスカバリ 704
プラグアンドプレイ展開のガイドライン 705
デバイスの表示 706

デバイスの追加または編集 710
デバイスの一括追加 711
バーチャル アカウント プロファイルの登録または編集 712
スマートアカウントからのデバイスの追加 714
プラグアンドプレイ対応デバイスのプロビジョニング 716
スイッチまたはルータデバイスのプロビジョニング 717
ワイヤレスコントローラ のプロビジョニング 722
AP またはセンサーデバイスのプロビジョニング 726
StackWise Virtual Link スイッチのプロビジョニング 729
プロビジョニングプロセスの完了 730
デバイスの削除 732
デバイスのリセット 733

第 17 章 ワイヤレスデバイスのプロビジョニング 735
ワイヤレスデバイスのプロビジョニングの概要 735
ワイヤレスデバイスと国コードについて 735
ロールベース アクセス コントロール 736
Cisco AireOS コントローラのプロビジョニングの前提条件 736
Cisco AireOS コントローラのプロビジョニング 738
シスコ ワイヤレス コントローラ高可用性（HA）の設定 741
シスコ ワイヤレス コントローラ 高可用性（HA）を設定するための前提条件 741
シスコ ワイヤレス コントローラ HA の設定 742
高可用性（HA）プロセス中および完了後に起こること 743
高可用性を設定および確認するためのコマンド 744
既存の展開での高可用性が設定されたデバイスの無効化 744
Day 1 の Cisco AP プロビジョニング 745
ワイヤレスコントローラ から別の ワイヤレスコントローラ に AP を移行する 749
AP のリセット 750
FlexConnect モードの AP における ICMP ping の有効化 751
Cisco AireOS Mobility Express AP の Day-0 ワークフロー 752
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの設定とプロビジョニング 754

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの概要 754
Catalyst Center での Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の構成 757
Cisco Catalyst 9800 シリーズ ワイヤレスコントローラでのソフトウェアイメージのアップグレードのサポート 762
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の高可用性の設定 763
高可用性（HA）に関する情報 766
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラで高可用性を設定するためのコマンド 767
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの高可用性を確認するためのコマンド 768
N+1 高可用性（HA） 768
N+1 高可用性（HA）の概要 768
Catalyst Center から N+1 高可用性を設定するための前提条件 769
Catalyst Center からの N+1 高可用性の設定 770
モビリティ設定の概要 772
モビリティ設定ワークフロー 773
モビリティ設定のユースケース 773
モビリティグループの設定 774
AP 偽装の設定 776
DTLS 暗号スイートについて 777
複数の DTLS 暗号スイートの設定 777
N+1 ローリング AP アップグレードについて 779
ローリング AP アップグレードを設定するワークフロー 780
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のプロビジョニング 782
Catalyst アクセスポイント上の Cisco Embedded Wireless Controller の Day-0 ワークフロー 788
Catalyst 9000 シリーズ スイッチ用 Cisco Catalyst 9800 組み込みワイヤレスコントローラの設定とプロビジョニング 790
サポートされているハードウェア プラットフォーム 790
事前設定 792
Catalyst 9000 スイッチ用 Cisco Catalyst 9800 組み込みワイヤレスコントローラの設定 792
Cisco Catalyst 9000 シリーズ スイッチでの組み込みワイヤレスのプロビジョニング 795

ワイヤレスデバイスの AP LSC の更新 799
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の デバイスごとの設定 801
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のための デバイスごとの設定 の前提条件 801
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の デバイスごとの設定 を有効にします。 802
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のデバイスごとの機能を設定する 803
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ に関連付けられた AP の管理 805
デバイスごとの設定のテーブル設定のカスタマイズ 807
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ 用の デバイスごとの設定 の編集 808
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の デバイスごとの設定 の複製 809
別の Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ から デバイスごとの設定 を複製 810
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の デバイスごとの設定 を削除 812
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の SSID の設定 813
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の WLAN プロファイルの作成 813
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のポリシープロファイルの作成 830
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のリモート LAN プロファイルの作成 840
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のリモート LAN ポリシーの作成 843
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のポリシータグの作成 847
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の 802.11be プロファイルの設定 849
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の RF 設定 852
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の RF プロファイルの作成 852
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの無線アンテナプロファイルの作成 860
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の RF タグの作成 862

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のマルチ BSSID プロファイルの作成 **864**

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のデフォルト RF 設定の編集 **865**

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の AP 設定 **867**

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの AP 参加プロファイルの作成 **867**

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のグローバル メッシュ パラメータの設定 **888**

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のメッシュ PSK の作成 **890**

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのメッシュプロファイルの作成 **892**

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の電力プロファイルの作成 **896**

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の Flex プロファイルの作成 **899**

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のサイトタグの作成 **906**

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のカレンダープロファイルの作成 **908**

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のタグマッピング設定 **909**

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の AP プライミングプロファイルの作成 **909**

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のタグ優先順位の設定 **911**

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの静的タグマッピングの作成 **912**

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のロケーションベースのタグマッピングルールの作成 **914**

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のルールベース タグマッピング プロファイルの作成 **916**

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のセキュリティ設定 **918**

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の RADIUS サーバーの作成 **918**

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の RADIUS サーバーグループの作成 **921**

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の TACACS+ サーバーの作成 **922**

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の TACACS+ サーバーグループの作成 **924**

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の LDAP サーバーの作成 **925**

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の LDAP サーバーグループの作成 927

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の認証方式リストの作成 928

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の認証方式リストの作成 929

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のアカウンティング方式リストの作成 931

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のグローバル AAA パラメータの設定 932

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のパスワードポリシーの作成 934

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の RADIUS フォールバックの設定 936

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の属性リストの作成 937

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の AAA ポリシーの作成 939

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の IPv4 ACL の作成 940

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の IPv4 ロールベース ACL の作成 942

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの IPv4 拡張 ACL の作成 945

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の IPv6 ACL の作成 949

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の IPv6 ロールベース ACL の作成 953

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の MAC ベースの ACL の作成 956

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のローカル EAP プロファイルの作成 958

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の EAP-FAST プロファイルの作成 959

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の高度な EAP の設定 961

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の基本的な URL フィルタの作成 962

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の拡張 URL フィルタの作成 964

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のゲストユーザーの作成 966

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の Web 認証パラメータの設定 967

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの Web 認証プロファイルの作成 970

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の CTS の設定 975
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の SXP の設定 979
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の CTS リンク設定の作成 980
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの SXP AP プロファイルの作成 981
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の不正ポリシーの設定 984
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの不正 AP ルールの作成 987
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のクライアント除外ポリシーの設定 991
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の LSC プロビジョニングパラメータの設定 992
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの LSC プロビジョニングエントリの作成 994
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のキーチェーンの作成 996
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の AP 証明書ポリシーを設定します。 998
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の MAC アドレスを使用した AP 証明書ポリシーの作成 999
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のシリアル番号を使用した AP 証明書ポリシーの作成 1001
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のグローバルワイヤレス設定 1002
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の CleanAir の設定 1003
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の高スループットパラメータの設定 1006
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のメディアパラメータの設定 1009
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の Air Time Fairness の設定 1013
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の Air Time Fairness ポリシーの作成 1015
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のネットワークパラメータの設定 1016
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のグローバル無線パラメータの設定 1023
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの 6 GHz 帯域における RRM の設定 1027

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の 5 GHz 帯域での RRM の設定 1033

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の 2.4 GHz 帯域での RRM の設定 1041

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の RRM FRA パラメータの設定 1048

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のグローバル ワイヤレス パラメータの設定 1051

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のロードバランシングの設定 1055

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の帯域選択の設定 1056

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の最適化されたローミングの設定 1058

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の高密度パラメータの設定 1060

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の優先コールの追加 1061

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の RFID の設定 1063

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のセルラーステアリングの設定 1064

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの 6 GHz クライアントステアリングの設定 1065

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の mDNS の設定 1067

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の mDNS サービス定義の作成 1068

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の mDNS サービスリストの作成 1070

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の mDNS サービスポリシーの作成 1072

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の mDNS 有線フィルタの作成 1074

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの mDNS Flex プロファイルの作成 1075

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のマルチキャストの設定 1077

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の IGMP スヌーピングの設定 1078

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の MLD スヌーピングの設定 1079

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の PIM とマルチキャストルーティングの設定 1080

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの VRF - RP アドレスマップの作成 1081

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのためのワイヤレスブロードキャストおよび非 IP マルチキャストの作成 1083

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のロケーションの設定 1084

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの国コードの設定 1086

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の Cisco DNA 統合設定 1087

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の AP ポリシーの設定 1088

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のデバイス認証シリアル番号の作成 1090

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のデバイス認証 MAC アドレスの作成 1091

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のワイヤレス地理位置情報設定の構成 1092

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのサービス設定 1093

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のサービステンプレートの作成 1093

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のポリシーマップの作成 1094

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の QoS ポリシーの作成 1097

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのカスタムアプリケーションの作成 1101

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のエクスポータの作成 1104

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのフローモニターの作成 1105

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の EoGRE グローバルパラメータの設定 1106

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の EoGRE ゲートウェイの作成 1108

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの EoGRE ドメインの作成 1109

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の EoGRE トンネルプロファイルの作成 1110

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのメディアストリームの設定 1113

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のメディア ストリーム プロファイルの作成 1114

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のゲスト LAN プロファイルの作成 1116

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのゲスト LAN マップの作成 1118

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の 除外クライアントを追加 1120

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のレイヤ 2 設定 1122

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の SVI プロファイルの作成 1122

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の VLAN プロファイルの作成 1126

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の VLAN グループプロファイルの作成 1127

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのポート チャネル インターフェイスの作成 1128

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのループバック インターフェイスの作成 1131

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのイーサネットポートの設定 1133

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の VRF インターフェイスの作成 1134

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのワイヤレス管理インターフェイスの設定 1135

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の検出プロトコルの設定 1137

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のネットワーク設定 1139

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの DNS ループバックの設定 1139

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の IPv4 DHCP プールの作成 1142

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の IPv6 DHCP プールの作成 1144

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの DHCP パーシステンスの設定 1146

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の HTTP および HTTPS の設定 1148

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の一般的な SNMP パラメータの設定 1151

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の SNMP ワイヤレストラップの設定 1152

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の SNMP コミュニティ文字列の追加 1153

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの SNMPv3 ユーザーグループの作成 1154
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの SNMPv3 ユーザーの作成 1156
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の SNMP ホストの作成 1158
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の NTP サーバープロファイルの作成 1160
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の認証キープロファイルの作成 1161
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のレイヤ 3 の設定 1162
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のスタティックルートの作成 1162
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の管理設定 1166
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のデバイス管理設定の構成 1166
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のデバイス FTP/SFTP/TFTP 設定 1167
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のユーザー管理設定を設定します。 1168
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の AP アップグレード設定をします。 1170
リリース間コントローラモビリティの概要 1171
ゲストアンカーの設定とプロビジョニングプロセス 1172
シスコのコントローラデバイスで IRCM を設定するための前提条件 1173
Cisco AireOS コントローラおよび Cisco Catalyst 9800 シリーズ ワイヤレス コントローラでの IRCM の設定 1174
Meraki デバイスをプロビジョニングするための前提条件 1175
Meraki デバイスのプロビジョニング 1177
リモート テレワーカー デバイスのプロビジョニング 1178
リモートテレワーカーの導入の概要 1179
リモートテレワーカーサイトの作成 1180

第 18 章 ルーティングプロファイルのプロビジョニング 1185
ルータのプロビジョニング 1185
VPC インベントリ収集 1187

第 19 章 ファイアウォール プロファイルのプロビジョニング 1189

Firewall Threat Defense デバイスのプロビジョニング 1189

ファイアウォール適応型セキュリティ アプライアンス デバイスのプロビジョニング 1191

第 20 章 LAN アンダーレイのプロビジョニング 1193

LAN の自動化 1193

LAN 自動化によるネットワークのプロビジョニングの前提条件 1195

LAN 自動化によるネットワークのプロビジョニング 1196

LAN 自動化のピアデバイスのユースケース 1204

LAN 自動化のステータスの確認 1206

インターフェイス間のリンクを作成 1206

インターフェイス間のリンクの削除 1207

LAN 自動化デバイスのホスト名とループバック IP アドレスの編集 1208

Strict 検出モードのデバイスの管理 1209

第 21 章 SD-Access LISP ファブリックネットワークのプロビジョニング 1213

Cisco SD-Access ゼロトラスト セキュリティソリューション 1214

[Zero Trustの概要（Zero-Trust Overview）] ダッシュボード 1215

[Zero Trustの概要（Zero-Trust Overview）] ダッシュボードの Day-0 ビュー 1215

SD-Access Zero Trust ワークプレイスへの移行の開始 1217

[Zero Trustの概要（Zero Trust Overview）] ダッシュボードの Day-n ビュー 1218

SD-Access Zero Trust ワークプレイスへの移行の変更 1221

ファブリックネットワークについて 1222

ファブリックサイト 1222

トランジット 1223

ファブリックの準備状況、イメージの互換性、およびコンプライアンスのチェック 1223

ファブリックの正常性チェック 1225

ファブリックのスケールチェック 1225

ファブリックサイトの更新 1226

Cisco SD-Access のロールベース アクセス コントロール 1228

ファブリックサイトの追加 1229
ファブリックサイトの移動 1232
ファブリックサイトの設定 1234
デバイスをファブリックに追加 1235
ファブリックからデバイスを削除 1239
ボーダーノードとしてのデバイスの追加 1240
LISP Pub/Sub の設定 1245
ファブリックの再設定 1246
IP トランジットの作成 1247
SD-Access トランジットの作成 1248
ファブリックサイトの認証テンプレートの設定 1250
ファブリックサイト内のポートの設定 1252
ファブリックネットワークのワイヤレス SSID の設定 1254
ファブリックでのワイヤレス メッシュ アクセス ポイントの設定 1255
ファブリックサイトでのセキュリティサービスの挿入の設定 1256
仮想ネットワーク 1256
レイヤ 3 仮想ネットワークの作成 1257
レイヤ 2 仮想ネットワークの作成 1258
ファブリックサイトへのレイヤ 3 仮想ネットワークの関連付け 1260
エニーキャストゲートウェイの作成 1262
エクストラネットポリシー 1267
エクストラネットポリシー管理 1267
エクストラネットポリシーの設定に関するガイドライン 1268
エクストラネットポリシーの作成 1269
エクストラネットポリシーの編集 1270
エクストラネットポリシーの削除 1270
ファブリックゾーンの設定 1270
ファブリックサイトとファブリックゾーンの作成 1271
ファブリックサイト内のファブリックゾーンの作成 1273
ファブリックゾーンへのレイヤ 3 仮想ネットワークの関連付け 1274
ファブリックゾーンへのレイヤ 2 仮想ネットワークの関連付け 1275

ファブリックゾーンへのエニーキャストゲートウェイの関連付け 1276
拡張ノードデバイスの設定 1278
拡張ノードの設定 1279
拡張ノードのポリシー拡張ノードへのアップグレード 1281
拡張ノードの削除 1283
拡張ノードおよびポリシー拡張ノードの REP リングトポロジの設定 1284
REP リングステータスの表示 1286
REP リングの削除 1287
REP リングへのノードの追加 1287
REP リングからのノードの削除 1289
サプリカントベースの拡張ノードの設定 1289
サプリカントベースの拡張ノードの設定手順 1290
障害のあるポートの交換 1292
サプリカントベースの拡張ノードをオンボードするための Cisco Identity Services Engine の設定 1293
ポートチャネルの設定 1296
ポートチャネルの作成 1296
ポートチャネルの更新 1298
ポートチャネルの削除 1299
マルチキャスト 1299
マルチキャストの設定 1300
ファブリックサイトの BGP AS 番号の編集 1302

第 22 章 キャンパスネットワークのプロビジョニング 1305
キャンパスネットワーク 1305
ネットワークの管理 1306
ネットワークの作成 1308
設定プロファイルの管理 1309
デバイスグループを切り替えるための設定プロファイルの作成 1310
ワイヤレスコントローラ から 設定プロファイル を学習する 1311
スイッチング デバイス グループの管理 1312

スイッチから設定プロファイルを学習 1315
デバイスの管理 1317
既存のネットワークに対する ワイヤレスコントローラ の割り当て 1319
設定プロファイル の ワイヤレスコントローラ への割り当て 1320
設定プロファイル の ワイヤレスコントローラ 割り当ての編集 1321
ワイヤレスコントローラからの 設定プロファイル の削除 1323
デバイス設定の比較 1323

第 23 章 サービスのプロビジョニング 1327
アプリケーション 1327
アプリケーションの可視性について 1327
アプリケーション可視性ビュー 1328
CBAR クラウドの設定 1332
CBAR クラウドの有効化または無効化 1333
ネットワークデバイスでの CBAR の有効化 1334
ネットワークデバイスでの CBAR の無効化 1335
アプリケーションテレメトリの有効化 1336
アプリケーションテレメトリの無効化 1337
CBAR 対応デバイスでのプロトコルパックの更新 1337
ネットワークデバイスでの CBAR の再設定 1339
アプリケーションおよびアプリケーションセット 1340
単方向と双方向のアプリケーション トラフィック 1340
カスタムアプリケーション 1341
検出されたアプリケーション 1341
お気に入りのアプリケーション 1342
アプリケーションおよびアプリケーションセットの設定 1343
アプリケーション設定の変更 1343
サーバー名に基づくカスタムアプリケーションの作成 1344
IP アドレスおよびポートに基づくカスタムアプリケーションの作成 1345
URL に基づくカスタム アプリケーションの作成 1346
カスタムアプリケーションの編集または削除 1346

アプリケーションをお気に入りにする 1348
カスタム アプリケーション セットの作成 1348
カスタム アプリケーション セットの編集または削除 1349
未分類アプリケーションの検出 1349
Catalyst Center トラフィック テレメトリ アプライアンス のアプリケーション可視性サービスのサポート 1350
Infoblox アプリケーションの検出 1350
検出されたアプリケーションの編集と削除 1352
アプリケーション ホスティング 1352
アプリケーション ホスティングについて 1353
アプリケーション ホスティング サービス パッケージのインストールと更新 1354
アプリケーションホスティングの前提条件 1354
アプリケーションをホストするデバイスの準備状況の表示 1355
アプリケーション ホスティングの準備状況チェック 1356
選択したアプリケーションのデバイスとステータスの表示 1357
アプリケーションの追加 1358
ThousandEyes Enterprise Agent アプリケーションの自動ダウンロード 1359
アプリケーションの更新 1360
アプリケーションの起動 1360
アプリケーションの停止 1361
デバイスでホストされているアプリケーションの表示 1361
アプリケーション ホスティングを使用したアプリケーションのインストール 1362
CSV ファイルを使用したアプリケーションの一括インストール 1364
Cisco Catalyst 9300 デバイスからのアプリケーションのアンインストール 1365
Cisco Catalyst 9300 デバイスでのアプリケーション設定の編集 1366
アプリケーションの削除 1366
アプリケーションログのダウンロード 1367
デバイスのテクニカルサポートログのダウンロード 1367
Cisco Catalyst 9100 シリーズ アクセスポイントでのアプリケーション ホスティング 1368
Cisco Catalyst 9100 シリーズ アクセス ポイントでのアプリケーション ホスティングについて 1368

Cisco Catalyst 9100 シリーズ アクセス ポイントでの USB アプリケーションのインストールと管理のアプリケーション ホスティング ワークフロー 1369
Cisco Catalyst 9100 シリーズ アクセスポイントにインストールされているホスティングアプリケーションの表示 1370
Cisco Catalyst 9100 デバイスからのアプリケーションのアンインストール 1371
Cisco Catalyst 9100 デバイスからのアプリケーションの削除 1371
サイト間 VPN の設定 1372
サイト間 VPN の作成 1372
サイト間 VPN の編集 1374
サイト間 VPN の削除 1374
Cisco Umbrella の設定 1374
Cisco Umbrella について 1374
Cisco Umbrella のロールベース アクセス コントロールの設定 1375
Catalyst Center での Cisco Umbrella の設定 1375
Cisco Umbrella ダッシュレットの追加 1377
Cisco Umbrella サービス統計ダッシュボードの表示 1377
ネットワークデバイスでの Cisco Umbrella のプロビジョニングの前提条件 1378
ネットワークデバイスでの Cisco Umbrella のプロビジョニング 1378
ネットワークデバイスでの Cisco Umbrella の無効化 1381
ネットワークデバイスでの Cisco Umbrella 設定の更新 1382
セキュアトンネルの作成 1383
セキュアトンネルの設定 1384
SD-Access へのセキュリティサービスの挿入 1386
サービス挿入サイト 1387
デイゼロでサービス挿入サイトを有効にするための事前チェック 1388
サービス挿入サイトの有効化 1389
サービス挿入サイトの編集 1391
サービス挿入サイトの削除 1396
トラフィック ステアリング コントラクトの設定 1397
Secure Equipment Access 1397
Cisco IoT ダッシュボードのセットアップ 1398
Cisco IoT ダッシュボードへのログイン 1399

Secure Equipment Access の設定 1400
API キーの生成 1403
Cisco Cyber Vision Center と Catalyst Center の統合 1403
Cyber Vision Center の管理 1404
Cyber Vision Center のセンサーの展開 1405

第 VI 部： ポリシーの設定 1407

第 24 章 グループベースのアクセス コントロール ポリシーおよび分析の設定 1409
グループベースのアクセスコントロール 1409
グループベースのアクセス コントロール ポリシー ダッシュボード 1410
グループベースのアクセス コントロール ポリシー 1411
ポリシー作成の概要 1415
セキュリティグループの作成 1416
セキュリティグループの編集 1417
セキュリティグループの削除 1418
Catalyst Center と Cisco ISE 間のセキュリティグループの同期 1418
アクセス契約の作成 1419
アクセス契約の編集 1421
アクセス契約の削除 1422
Catalyst Center と Cisco ISE 間のアクセス契約の同期 1422
グループベースのアクセス コントロール ポリシーの作成 1423
トラフィックフローに基づくグループベースのアクセス コントロール ポリシーの更新 1425
Catalyst Center と Cisco ISE の間のポリシーの同期 1426
シスコのグループベースポリシー分析 1427
シスコのグループベースポリシー分析について 1427
グループベースポリシー分析のインストール 1427
ハードウェアとソフトウェアの互換性 1428
コネクタについて 1431
シスコのグループベースポリシー分析の初期設定 1432
グループとエンドポイントの確認 1433

複数のグループから複数のグループ 1433
単一のグループから複数のグループ 1434
単一のグループから単一のグループ 1435
アクセス契約数 1438
日時セレクタ 1440
検索の使用 1440
ロールベース アクセス コントロール 1441

第 25 章 IP ベースおよび URL ベースのアクセス コントロール ポリシーの設定 1443
IP ベースのアクセス コントロール ポリシー 1443
IP ベースのアクセス コントロール ポリシー設定のワークフロー 1444
グローバル ネットワーク サーバーの設定 1445
IP ネットワーク グループの作成 1446
IP ネットワーク グループの編集または削除 1447
IP ベースのアクセスコントロール契約の作成 1447
IP ベースのアクセス コントロール コントラクトの編集または削除 1448
IP ベースおよび URL ベースのアクセス コントロール ポリシーの作成 1449
IP ベースおよび URL ベースのアクセス コントロール ポリシーの編集または削除 1451

第 26 章 アプリケーションポリシーの設定 1453
アプリケーションポリシーの概要 1453
アプリケーションポリシーでの CVD ベースの設定 1454
サイトの範囲 1454
ビジネス関連グループ 1455
コンシューマとプロデューサ 1456
マーキング、キューイング、ドロッピングの処理 1456
サービスプロバイダーのプロファイル 1458
キューイングプロファイル 1460
リソースが制限されているデバイスの処理順 1462
ポリシーのドラフト 1464
ポリシーのスケジューリング 1465

ポリシーのバージョン管理 1466
オリジナルポリシーの復元 1466
陳腐化したアプリケーションポリシー 1467
アプリケーションポリシーのガイドラインと制限事項 1468
アプリケーションポリシーの管理 1469
前提条件 1469
アプリケーションポリシーの作成 1470
アプリケーションポリシー情報の表示 1473
アプリケーションポリシーの編集 1475
アプリケーションポリシーのドラフトの保存 1476
アプリケーションポリシーの展開 1476
ポリシー展開のキャンセル 1477
アプリケーション ポリシーの削除 1478
アプリケーションポリシーの複製 1478
アプリケーションポリシーの復元 1479
デフォルトの CVD アプリケーションポリシーのリセット 1480
アプリケーション ポリシー履歴の表示 1481
以前のポリシーバージョンへのロールバック 1481
キューイングプロファイルの管理 1482
キューイングプロファイルの作成 1482
キューイングプロファイルの編集または削除 1483
WAN インターフェイスのアプリケーションポリシーの管理 1483
サービス プロバイダー プロファイルの SLA 属性のカスタマイズ 1483
サービス プロバイダー プロファイルの WAN インターフェイスへの割り当て 1485

第 27 章 トラフィックコピーポリシーの設定 1487
トラフィックコピーポリシー 1487
送信元、宛先、トラフィックのコピー先 1488
トラフィックコピーポリシーのガイドラインと制限事項 1489
トラフィックコピーポリシーの設定のワークフロー 1489
トラフィックのコピー先の作成 1490

トラフィックのコピー先の編集または削除 1490
トラフィックコピー契約の作成 1491
トラフィックコピー契約の編集または削除 1491
トラフィックコピーポリシーの作成 1492
トラフィックコピーポリシーの編集または削除 1492

第 28 章 ルールベースのコンプライアンスポリシーの設定 1493
ルールベースのコンプライアンスポリシー 1493
ルールベースのコンプライアンスポリシーの作成 1494
ルールベースのコンプライアンス ポリシー ルールの作成 1494
コンプライアンス ポリシー ルールへの条件の追加 1495
例：ブロック オプション 1501
条件およびアクションの例：NTP サーバーの冗長性 1503
ポリシールールへの変数の追加 1503
サイトへのポリシーの割り当て 1505
Cisco Prime Infrastructure からコンプライアンスポリシーを XML としてエクスポートして Catalyst Center にインポートする 1506
Catalyst Centerからルールベースのコンプライアンスポリシーをエクスポートし、別の Catalyst Center にインポートします。 1507

第 29 章 トラフィック ステアリング ポリシーの設定 1509
トラフィックス テアリング ポリシーの概要 1509
トラフィック ステアリング ポリシー 1510
Day 0 におけるトラフィック ステアリング ポリシーの作成 1511
Day N におけるトラフィック ステアリング ポリシーの作成 1511
トラフィック ステアリング ポリシーの編集 1513
トラフィック ステアリング ポリシーの削除 1514
トラフィック ステアリング ポリシーの展開 1515
トラフィック ステアリング コントラクト 1515
トラフィック ステアリング コントラクトの作成 1515
トラフィック ステアリング コントラクトの編集または複製 1517

トラフィック ステアリング コントラクトの削除 1518

第 VII 部 : ネットワークのモニタリングとトラブルシューティング 1519

第 30 章 高度な機能のトライアルの有効化 1521

高度な機能のトライアルの概要 1521

ネットワークバグ ID トライアルの有効化 1521

セキュリティ アドバイザリ トライアルの有効化 1522

Field Notice トライアルの有効化 1523

第 31 章 Cisco AI Endpoint Analytics 1525

Cisco AI エンドポイント分析 の概要 1525

Cisco AI エンドポイント分析の主な機能 1526

FIPS の準拠性 1527

Catalyst Center での Cisco AI エンドポイント分析のセットアップ 1528

ソフトウェアアップデートのインストール 1528

データソースの接続と有効化 1529

エンドポイント テレメトリ ソース 1532

Cisco AI エンドポイント分析の概要ウィンドウ 1533

Cisco Talos インテリジェンス 1534

アプリケーションの有効化による Cisco AI エンドポイント分析 と Cisco Talos インテリジェンスの統合 1535

クラウド認証を使用した Cisco AI エンドポイント分析 と Cisco Talos インテリジェンスの統合 1536

Cisco ISE への承認属性の公開 1538

Trust Analytics 1539

影響度のカスタマイズ 1540

アラートのリセットの設定 1542

エンドポイント パージ ポリシー 1543

パージポリシーの作成 1544

エンドポイントサブネット検査の設定 1544

エンドポイント インベントリ 1545

Cisco AI エンドポイント分析データのエクスポート 1547
エンドポイントのフィルタ処理 1548
属性用語集 1549
エンドポイントの登録 1550
登録済みエンドポイントの編集 1550
登録済みエンドポイントの削除 1551
信頼得点 1551
エンドポイントの信頼スコア 1552
エンドポイント属性の競合 1556
NAT モード検出 1558
Cisco Catalyst 9000 シリーズ デバイスに接続された同時 MAC アドレスを持つエンドポイント 1558
Cisco ISE からのポスチャおよび認証値を使用した初期信頼スコアアセスメント 1559
ランダムおよび変更 MAC アドレスを持つエンドポイントの信頼スコア 1560
オープンポートとログイン情報の脆弱性を確認するためのセンサースキャン 1560
エンドポイントの信頼スコアの表示と管理 1563
エンドポイント スプーフィングの制御 1568
プロファイリングルール 1570
ルールの優先順位付け 1570
プロファイリングルールのフィルタ処理 1571
更新されたプロファイリングルールの表示 1571
システムルール 1572
エンドポイント プロファイリング用の自動システムルール更新 1572
カスタムルール 1574
プロファイリングルールの論理と条件 1574
カスタムルールの作成 1575
カスタムルールの編集 1576
カスタムルールの削除 1576
展開間での API を使用したカスタム プロファイリング ルールのエクスポートとインポート 1576
スマートグループ化のための Cisco AI ルール 1577

ネットワーク内の類似のエンドポイントに対する新しいプロファイリングの提案 1578
プロファイリングルールのインポート 1580
プロファイリングルールのエクスポート 1580
階層 1581
カテゴリとサブカテゴリの作成 1581
カテゴリまたはサブカテゴリの編集 1582
カテゴリからのエンドポイントタイプの削除 1582
カテゴリからのエンドポイントタイプの再割り当て 1583
カテゴリの削除 1583

第 32 章 ネットワーク推論機能を使用したネットワークデバイスのトラブルシューティング 1585
ネットワーク推論機能の概要 1585
MRE ワークフローを使用した Cisco SD-Access への移行の検証 1586
CPU 使用率が高い場合のトラブルシューティング 1588
電源障害のトラブルシューティング 1590
インターフェイスが停止した場合のトラブルシューティング 1591
ネットワーク接続のトラブルシューティング 1593
デバイスの IP 接続のトラブルシューティング 1594
MRE ワークフローを使用したワイヤレスクライアントの障害対応 1594
MRE ワークフローを使用したワイヤレス AP のトラブルシューティング 1596
MRE ワークフローを使用した監視対象外のデバイスのトラブルシューティング 1597
MRE ワークフローを使用した シスコ ワイヤレス コントローラの HA のトラブルシューティング 1598

第 33 章 ネットワークバグの特定 1601
ネットワークバグ識別ツールの概要 1601
ネットワークのバグのスキャン 1602
Catalyst Center のバグのスキャン 1604

第 34 章 ネットワーク セキュリティ アドバイザリの識別 1605
セキュリティアドバイザリの概要 1605

前提条件 1606
セキュリティアドバイザリの表示 1606
セキュリティ アドバイザリ スキャンのスケジュール設定 1608
セキュリティアドバイザリのために呼び出される CLI コマンド 1610
ネットワークを再スキャンしてセキュリティアドバイザリを特定 1611
アドバイザリからのデバイスの表示/非表示 1611
デバイスからのアドバイザリの表示/非表示 1612
セキュリティ アドバイザリ ナレッジ バンドルの通知の追加 1613
インベントリでのセキュリティアドバイザリの表示 1614
一致パターンの追加 1615
一致パターンの AND/OR の定義 1616
一致パターンの編集 1616
一致パターンの削除 1617

第 35 章 ネットワークの Field Notice の特定 1619
Field Notice ID ツールの概要 1619
Field Notice の表示 1619

第 36 章 Catalyst Center からの根本原因分析ファイルの生成 1623
サポートバンドルの概要 1623
プロビジョニング失敗の根本原因分析データの収集とアップロード 1623

第 VIII 部： Catalyst Center の管理 1625

第 37 章 構築と展開のワークフロー 1627
Catalyst Center ワークフローナビゲーション 1627
デバイスの検出 1628
AP 更新ワークフロー 1630
スイッチでのアプリケーション ホスティングの有効化 1634
IoT サービスの有効化 1637
Cisco Catalyst 9100 シリーズ アクセス ポイントでの IoT サービスの有効化 1637

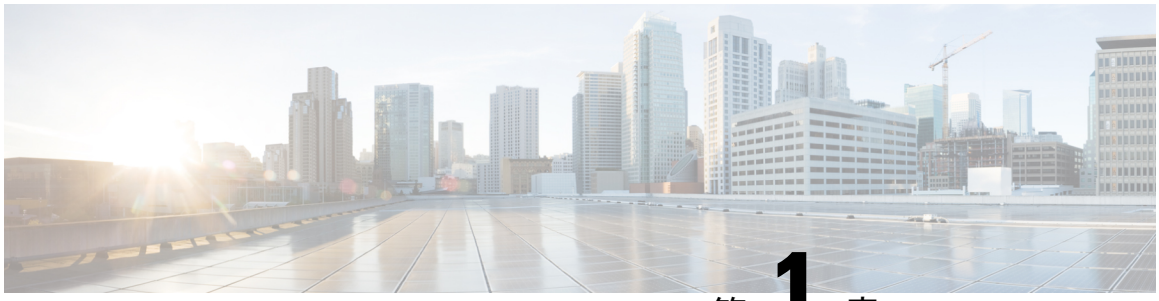
IoT アプリケーションの管理 1638
Catalyst Center での AP 設定 1638
AP の設定 1639
AP の定期的なイベントのスケジュール 1657
既存のテンプレートを使用した AP の設定 1660
デバイスの交換 1664
スイッチの更新 1670
リモートサポート許可の作成 1673
イベント通知の作成 1674
リモート LAN の設定 1679
ファブリックサイトでの Parallel Redundancy Protocol の設定 1684
PRP 設定の削除 1686
PRP チャネルの編集 1686

第 38 章 ワイヤレスネットワークの設定の使用例 1689
ワイヤレスネットワーク設定のユースケース 1689
ワイヤレスコントローラ 管理ユースケース 1689
WLAN プロファイルおよびポリシープロファイルの設定 1689
Wi-Fi 7 設定のユースケース 1693
Wi-Fi 7 設定の有効化 1693
高可用性のユースケース 1696
シスコ ワイヤレス コントローラ HA の設定 1696
シスコ ワイヤレス コントローラ N+1 HA の設定 1698
ワイヤレスモビリティのユースケース 1699
ワイヤレスモビリティの設定 1699
アンカーおよび外部ワイヤレスモビリティの設定 1702
AP 管理のユースケース 1707
AP の設定 1707
AP 更新 1707
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのプロビジョニング中に AP プロビジョニングをスキップする 1707

フラッピング AP の自動タグ付け 1710
ROW AP の設定 1711
ワイヤレス メッシュ ネットワークの設定 1712
ワイヤレスコントローラから別のワイヤレスコントローラへの AP の移行 1714
RMA ワークフローを使用した AP の交換 1714
非インテントベースの展開に PnP を使用する AP のオンボーディング 1714
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのキャンパスネットワーク設定のユースケース 1716
Day-0 における ワイヤレスコントローラ のすべての設定の標準化 1717
Day-0 における ワイヤレスコントローラ の部分的な設定の標準化 1718
Day-n のワイヤレスコントローラ設定の管理 1719

第 39 章 ネットワークのエネルギーの管理 1721
概要 1721
ネットワークデバイスのエネルギーの管理 1722
エネルギー管理ダッシュボードの使用 1723
ネットワークデバイスのエネルギー管理に関するレポートの生成 1725
ネットワークデバイスのエネルギー消費量の表示 1725
ネットワークデバイスの炭素排出量 1727
省エネルギーの表示 1728
サイト間のエネルギー比較 1729

第 40 章 データ プラットフォームを使用した Catalyst Center のトラブルシューティング 1733
データ プラットフォームについて 1733
コレクタの設定情報の表示または更新 1734
データ保持設定の表示 1735
パイプラインステータスの表示 1735



第 1 章

新機能および変更された機能 Catalyst Center

次の表に、Catalyst Center 3.2.3 の新機能および変更された機能の要約と参照先を示します。

表 *1 : Catalyst Center 3.2.3* の新機能と変更された機能

機能	説明
Cisco SD-Access ファブリックでのサイレントホスト検出のサポート	Catalyst Center は、エニーキャストゲートウェイでのサイレントホスト検出の設定をサポートしています。サイレントホスト検出によってサイレントホストの検出が可能になり、端末の到達可能性が向上します。 エニーキャストゲートウェイの作成 （1262 ページ） を参照してください。
LAN 自動化ワークフローでの OSPF ルーティングプロトコルのサポート	Catalyst Center は、LAN アンダーレイのプロビジョニングで OSPF ルーティングをサポートします。 LAN 自動化によるネットワークのプロビジョニング （1196 ページ） を参照してください。

次の表に、Catalyst Center 3.2.2 の新機能および変更された機能の要約と参照先を示します。

表 *2 : Catalyst Center 3.2.2* の新機能および変更された機能

機能	説明
AP 加速計のサポート	AP 加速計を有効にして、サポートされている AP のティルト情報を表示し、AP の方向を監視できるようになりました。 デフォルトでは、AP 加速計は無効になっています。Cisco Catalyst 9166D1、9176I、9176D1、9178I シリーズ AP でのみ使用できます。 AP の設定 （1639 ページ） を参照してください。

機能	説明
2D ワイヤレスマップの AP ラベル拡張機能	2D ワイヤレスマップで、AP ごとに最大 4 種のラベルタイプと、計画している AP ごとに最大 2 種のラベルタイプを表示できるようになりました。 「2D マップビューオプション （340 ページ）」と「AP アイコンと計画済み AP アイコンについて （345 ページ）」を参照してください。
AP ゾーンの最適化	Catalyst Center は AP ゾーンの最適化をサポートしており、大規模なワイヤレス展開での効率を向上させます。 以前のリリースからリリース 3.2.2 にアップグレードした後、すべての Cisco Catalyst 9800 シリーズ ワイヤレス コントローラを再プロビジョニングしてこの最適化を有効にします。他のインテント変更がない場合は、ワイヤレスコントローラ を再プロビジョニングしても、新しい設定がデバイスにプッシュされることはありません。 ネットワークプロファイルへの AP ゾーンの追加 （547 ページ） を参照してください。
プラグアンドプレイでの AP ゾーンのサポート	プラグアンドプレイプロセスから要求された AP に AP ゾーン設定を適用できます。 ワイヤレスコントローラ のプロビジョニング （722 ページ） を参照してください。

機能	説明
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのプロビジョニングの最適化	Catalyst Center には、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのプロビジョニングに関する次のパフォーマンスの最適化が含まれています。 • 直感的なスキップAPプロビジョニング：ワイヤレスコントローラを再プロビジョニングする場合、Catalyst Center は AP 関連の設定に変更がないかどうかを検出します。APインテント設定に変更がない場合、AP 関連コマンドの設定をスキップします。 • 選択的な AP グループ RFS 変換：この機能は、AP 関連の設定（APタグマッピング、RFタグ、フレックスプロファイルやRFプロファイルなど）の再プロビジョニングを最適化します。AP関連設定へのアウトオブバンド変更は、規則遵守レポートで明示的にフラグが付けられていない限り、再プロビジョニング中に自動的に修正されません。ネットワークインテントに一致するように AP 関連のアウトオブバンド設定を修正するには、ワイヤレスコントローラ再同期およびコンプライアンス実行を行います。この機能を無効にするには、Cisco Technical Assistance Center（TAC）にお問い合わせください。 「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のプロビジョニング （782 ページ）」と「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのプロビジョニング中にAPプロビジョニングをスキップする （1707 ページ）」を参照してください。
Catalyst Center からの Cyber Vision Center の展開	Catalyst Center は、ネットワーク セキュリティ ソリューションである Cisco Cyber Vision との統合をサポートしています。ブラウザベースのマネージャは、Cisco Cyber Vision Center と呼ばれます。Cyber Vision Centerは、ネットワークデバイスの監視と管理に役立ちます。 Cisco Cyber Vision Center と Catalyst Center の統合 （1403 ページ） を参照してください。
ダイナミック AP エレベーションのレポート	2D および 3D ワイヤレスマップの場合、**[エレベーション（Elevation）]** フィールドには、有効化しているサポート対象の加速計ハードウェアが搭載されている AP のティルト角が自動的に表示されます。 AP の編集 （318 ページ） を参照してください。
PRP チャネルの編集	PRP 設定で 許可された VLAN の詳細を変更できます。 PRP チャネルの編集 （1686 ページ） を参照してください。

機能	説明
強化された Catalyst Center ホームページ	このリリースでは、ネットワークの詳細な概要ビューを提供する強化版ホームページを導入しています。このデータで全体的なパフォーマンス、ステータス、正常性をすばやく評価できます。 メインメニュー、ウィンドウの右上部分にあるアイコン、**インタラクティブヘルプ**は、以前のホームページと同様に機能します。 デフォルトホームページ （36 ページ） を参照してください。
強化された Catalyst Center 初回セットアップ	Catalyst Center アプライアンスをインストールして設定した後、次のいずれかの強化版セットアップ方法を使用して Catalyst Center の初回セットアップを完了できます。 • エクスプレスセットアップ • 標準セットアップ • エキスパートによるセットアップ このセットアップ方法には柔軟性があり、システムや導入準備中のデバイスのセットアップ方法を選択できます。 初回セットアップ （20 ページ） を参照してください。
AP 設定ワークフローの拡張機能	**[アクセスポイント設定（Configure Access Points）]** ワークフローは、**[RAP ダウンリンクバックホール（RAP Downlink Backhaul）]** チェックボックスをサポートするように拡張されました。このオプションを有効にすると、ルートアクセスポイント（RAP）のダウンリンクバックホール無線帯域を選択できます。 「AP の設定 （1639 ページ）」、「AP の定期的なイベントのスケジュール（1657 ページ）」、および「既存のテンプレートを使用した AP の設定 （1660 ページ）」を参照してください。

機能	説明
AP 設定中の AP 選択の拡張機能	**[アクセスポイント設定（Configure Access Points）]** ワークフローでの AP の選択では、大規模な展開をサポートするため次の機能を拡張しています。 • [**Select All**] オプションが追加され、最大 4000 台の AP を同時に選択できるようになりました。 • [**Access Points**] テーブルに、ページあたり 200 または 300 行を表示できるようになりました。 • [**Access Points**] テーブルで列レベルのフィルタリングが使用可能になり、特定の AP をすばやく検索して選択できるようになりました。 • テーブル設定のスライドインペインが再構成され、カスタマイズしやすくなりました。 AP の設定 （1639 ページ） を参照してください。

機能	説明
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の デバイスごとの設定 の機能拡張	

機能	説明
	Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのデバイスごとの設定には次の機能拡張があります。 • [デバイス詳細（Device Details）] ウィンドウの **[設定（Configuration）]** タブのメニューグループ名を更新し、設定を再編成しました。更新したグループ名は、**SSID**、**RF**、**AP**、**タグマッピング**、**セキュリティ**、**グローバルワイヤレス**、**サービス**、**レイヤ 2**、**ネットワーク設定**、**レイヤ 3**、**管理**です。 Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のデバイスごとの機能を設定する （803 ページ） を参照してください。 • CTS over HTTPS と HTTPS ポリシーサーバー設定のサポート。 「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の CTS の設定 （975 ページ）」と「CTS 設定用のポリシーサーバーの作成 （977 ページ）」を参照してください。 • SXP と SXP ピア作成での IPv6 設定のサポート。 「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の SXP の設定 （979 ページ）」と「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの AP 参加プロファイルの作成 （867 ページ）」を参照してください。 • MACsec 設定のサポート。 Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のキーチェーンの作成 （996 ページ） を参照してください。 • Cisco IOS XE リリース 17.18.2 と Cisco IOS XE リリース 26.1.1 の新規設定と更新済み設定のサポート。 Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの SNMPv3 ユーザーの作成 （1156 ページ）、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのポート チャネル インターフェイスの作成 （1128 ページ）、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の AP 証明書ポリシーを設定します。 （998 ページ）、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の MAC アドレスを使用した AP 証明書ポリシーの作成 （999 ページ）、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のシリアル番号を使用した AP 証明書ポリシーの作成 （1001 ページ）、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の CTS リンク設定の作成 （980 ページ）、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の Cisco DNA 統合設定 （1087 ページ）、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のワイヤレス地理位置情報設定の構成 （1092 ページ）、CTS 設定用のポリシーサーバーの作成 （977 ページ）、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のデフォルト RF 設定

機能	説明
	の編集（865 ページ）、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の AP アップグレード設定をします。（1170 ページ）、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの AP 参加プロファイルの作成（867 ページ）、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの 6 GHz 帯域における RRM の設定（1027 ページ）、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのワイヤレス管理インターフェイスの設定（1135 ページ）、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の RF タグの作成（862 ページ）、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの無線アンテナプロファイルの作成（860 ページ）、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの SXP AP プロファイルの作成（981 ページ）、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のグローバル ワイヤレスパラメータの設定（1051 ページ）、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の Flex プロファイルの作成（899 ページ）、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の WLAN プロファイルの作成（813 ページ）、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のポリシープロファイルの作成（830 ページ）、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの CleanAir の設定（1003 ページ）、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の高スループット パラメータの設定（1006 ページ）、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのメディアパラメータの設定（1009 ページ）、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のネットワークパラメータの設定（1016 ページ）、および Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の EoGRE トンネルプロファイルの作成（1110 ページ）を参照してください。
Cisco IOS XE リリース 17.18.2 を実行しているワイヤレスコントローラ用のデバイスごとの設定の機能拡張	デバイスごとの設定の場合、Catalyst Center には、現在のセキュリティ基準を満たしておらず、Lightweight Extensible Authentication Protocol（LEAP）などの Cisco IOS XE リリース 17.18.2 で廃止される予定の安全でない設定オプションに対する警告メッセージが表示されます。 Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の デバイスごとの設定 （801 ページ） を参照してください。
ファブリックネットワークでの Cisco C9350 シリーズ スマートスイッチを拡張サポート	Cisco C9350 シリーズ スマートスイッチは、エッジ、ボーダー、コントロールプレーンノードなどのすべてのファブリック ネットワーク ロールでサポートしています。

機能	説明
Catalyst Center コンプライアンスの機能拡張	コンプライアンス ダッシュボードを表示して管理し、企業全体のネットワーク コンプライアンスの正常性を一元的に監視できます。ダッシュボードでは、コンプライアンスを **Configuration**、**Hardware/Software**、および **Vulnerability** バケットに分類し、複数のデバイス全体の違反を同時に確認して管理するための一括運用機能が導入されています。 「コンプライアンスの概要 （665 ページ）」、「コンプライアンス カテゴリ」、および「ネットワークのコンプライアンスの監視 （675 ページ）」を参照してください。
Catalyst Center インベントリにおける Cisco Catalyst スイッチのデバイスごとの設定の機能拡張	単一デバイスのレイヤ 3 設定、ネットワーク設定、ポート設定を表示し、編集できます。加えてレイヤ 2、セキュリティ、産業用プロファイルが更新され、新しい設定が含まれます。 Cisco Catalyst スイッチのデバイスごとの設定を管理する （123 ページ） を参照してください。
負荷分散のためのカスタムサイトタグへの機能拡張	Catalyst Center では、カスタムサイトタグの負荷値を設定できます。負荷の有効な範囲は 0～1000 で、サイトの AP 密度に応じて設定できます。 ネットワークプロファイルへの AP グループ、Flex グループ、サイトタグ、およびポリシータグの追加 （563 ページ） を参照してください。
AP リフレッシュと AP 設定ワークフローの機能拡張	Catalyst Center は、AP ワークフローにおける次の機能拡張をサポートしています。 • アシュアランスユースケースにおけるプラグアンドプレイによる AP のオンボーディング。 AP 更新ワークフロー （1630 ページ） を参照してください。 • AP 設定ワークフローによるメッシュロールの設定。 AP の設定 （1639 ページ） を参照してください。
Cisco Catalyst スイッチのキャンパス ネットワーク プロビジョニングの機能拡張	キャンパス ネットワーク ワークフローでは、レイヤ 2、レイヤ 3、セキュリティ、ネットワーク設定、産業、およびポートの各プロファイルのグループプロファイルを使用した、スイッチング デバイス グループのプロビジョニングをサポートするようになりました。 キャンパスネットワークのプロビジョニング （1305 ページ） を参照してください。

機能	説明
サプリカントベースの拡張ノードの導入準備のために MACsec 暗号化をサポート	MACsec が有効な状態で新しいサプリカントベースの拡張ノードの導入準備や、すでに導入準備した拡張ノードに MACsec 暗号化のサポートの提供ができます。 「エニーキャストゲートウェイの作成（1262 ページ）」と「サプリカントベースの拡張ノードをオンボードするための Cisco Identity Services Engine の設定 （1293 ページ）」を参照してください。
Catalyst Center におけるアウトオブバンド RMA デバイス交換の管理	ワークフローはシリアル番号の競合を検出し、アウトオブバンド RMA デバイスの交換の確認をユーザーに求めます。 アウトオブバンド RMA デバイスの交換の管理 （255 ページ） を参照してください。
プラグアンドプレイ（PnP）要求フローと StackWise 仮想スイッチ（SVL）の機能拡張	PnP 要求フローを強化し、PnP とインベントリでデバイスを管理する際の混乱を減らしています。 プラグアンドプレイ プロビジョニングの概要（695 ページ） を参照してください。 プラグアンドプレイ オンボーディング中の SVL サポートにより、ユーザーは接続された Catalyst 9500 スイッチのペアを単一の論理デバイスとしてオンボードできます。 StackWise Virtual Link スイッチのプロビジョニング （729 ページ） を参照してください。
ワイヤレスコントローラの RMA のサポート	Catalyst Center はワイヤレスコントローラの RMA をサポートしています。[**Replace Device**] ワークフローを使用して、スタンドアロンのワイヤレスコントローラや、高可用性（HA）ペアの両方のワイヤレスコントローラを交換できます。 このワークフローは、次のデバイスではサポートされていません。 • ワイヤレスコントローラが組み込まれているデバイス • ワイヤレスコントローラについて • Mobility Express デバイス 「故障したデバイスの交換 （244 ページ）」、「Catalyst Center の RMA ワークフローの制限事項（255 ページ）」、および「デバイスの交換 （1664 ページ）」を参照してください。

機能	説明
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラキャンパス ネットワーク プロビジョニングのサポート	キャンパスネットワークは、既存の Cisco Catalyst 9800 シリーズ ワイヤレス コントローラから設定を学習することにより、複数の Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのプロビジョニングをサポートします。Catalyst Center は、デバイスごとの設定を通じてプロビジョニングされたワイヤレスコントローラ、インテントベースのネットワーク設定を通じてプロビジョニングされたワイヤレスコントローラ、またはプロビジョニングされずにインベントリで利用可能なワイヤレスコントローラから設定を学習できます。 これらの設定は設定プロファイルとして保存されます。設定プロファイルを複数のワイヤレスコントローラに適用することで、一貫した設定と標準化された展開を実現できます。 （注） この機能はベータ版であり、機能を有効にする必要があります。有効にするには、Cisco TAC にお問い合わせください。この機能が有効になっていない場合、ワイヤレスコントローラ関連の設定のオプションは使用できないか、グレー表示されます。 「キャンパスネットワークのプロビジョニング（1305ページ）」と「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのキャンパスネットワーク設定のユースケース（1716ページ）」を参照してください。
Cisco C9610 シリーズ スマートスイッチをサポート	Catalyst Center は、ファブリックネットワーク内の Cisco C9610 シリーズ スマートスイッチをサポートしています。 （注） Cisco C9610 シリーズ スマートスイッチは、エッジおよび拡張ノードの機能をサポートしていません。
ファブリック展開 REP リングへのノードの動的な追加をサポート	REP リングを削除せずに、ファブリック展開のために既存の REP リングにノードを動的に追加できるようになりました。ノードは一度に 1 つだけ追加する必要があります。これには、Cisco IOS XE リリース 17.18.3 以降が必要です。 REP リングへのノードの追加（1287ページ） を参照してください。

機能	説明
BGP 自律システム（AS）番号の編集をサポート	Catalyst Center でファブリックサイトの BGP AS 番号を編集できるようになりました。 （注） BGP AS 番号を編集すると、BGP ピアリングが一時的に中断され、ボーダーノードとコントロールプレーンノードのカスタム BGP 設定が削除されるため、テンプレートの更新とカスタム設定の再構成が必要となります。BGP AS 番号を編集すると、すべての仮想ネットワークで外部接続が失われ、管理アクセスが一時的に中断される可能性があります。 ファブリックサイトの BGP AS 番号の編集（1302 ページ）を参照してください。
Cisco SD-Access ファブリックでの、ポリシーベースのルーティング設定を含まないエクストラネットポリシーのサポート	Catalyst Center では、Cisco SD-Access ファブリック内のエクストラネットポリシー操作用の新しい CLI 設定が導入されています。Cisco IOS XE 17.18.1 以降を実行しているボーダーデバイスで、この機能をサポートしています。さらに Catalyst Center では、ポリシーベースルーティング（PBR）から新しい CLI アプローチへの移行サポートを提供しています。 エクストラネットポリシー管理（1267 ページ）を参照してください。

機能	説明
ワイヤレスネットワークでの IPv6 のサポート	

機能	説明
	Catalyst Center は、ワイヤレスネットワークのシングルスタックおよびデュアルスタック展開で IPv6 をサポートしています。以下の設定では IPv6 アドレスをサポートします。 • デバイス一覧 • アンカーグループ • リモートテレワーカー用の NAT IP アドレス設定 • 事前認証 ACL • SSID を ACL に関連付け • IP ベースのアクセス コントロール ポリシー • モビリティ グループ • アプリケーション可視性とアプリケーションポリシー • AI-Enhanced RRM • Cisco Catalyst 9800 シリーズ ワイヤレス コントローラと AP のプロビジョニング • AP とワイヤレスコントローラのプラグアンドプレイ（PnP）オンボーディング • AP 設定ワークフローでの高可用性（HA） • デバイスごとの設定について • AP 更新 • ワイヤレスコントローラの RMA • AAA サポート 「アンカーグループの作成 （499 ページ）」、「リモートテレワーカーサイトの作成（1180ページ）」、「認証前アクセス制御リストの作成 （427 ページ）」、「エンタープライズ ワイヤレス ネットワーク用 SSID の作成 （415 ページ）」、「ゲスト ワイヤレス ネットワークの SSID の作成 （432 ページ）」、「IP ベースおよび URL ベースのアクセス コントロール ポリシーの作成（1449ページ）」、「IP ベースのアクセスコントロール契約の作成（1447ページ）」、「モビリティグループの設定（774ページ）」、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のプロビジョニング （782 ページ）」、「ワイヤレスコントローラ のプロビジョニング （722 ページ）」、「バーチャル アカウント プロファイルの登録または編集（712ページ）」、「デバイスの一括追加（711ページ）」、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のデバイスごとの機

機能	説明
	能を設定する （803 ページ）」、「故障したデバイスの交換 （244 ページ）」、および「デバイスの交換 （1664 ページ）」を参照してください。
ファブリック SSID の認証後の ACL 設定をサポート	Catalyst Center は [**Create IP & URL-Based Access Control Policy**] ワークフローで、ファブリック SSID の認証後アクセス制御リスト（ACL）設定をサポートしています。 IP ベースおよび URL ベースのアクセス コントロール ポリシーの作成 （1449 ページ） を参照してください。
エニーキャストゲートウェイでのセカンダリ IP アドレスプールをサポート	エニーキャストゲートウェイの追加 IP アドレスプールを最大 4 つ設定できます。 エニーキャストゲートウェイの作成 （1262 ページ） を参照してください。
ポリシー拡張ノードのアップグレードに対する構成の可視性と制御をサポート	ポリシー拡張ノードのアップグレード時に、構成の可視性と制御機能をサポートするようになりました。 可視化の強化により、デバイス構成を展開する前にプレビューできます。強化された制御により、IT サービス管理（ITSM）チェックを通じて、信頼できる承認された構成のみをネットワークデバイスにプロビジョニングできます。 拡張ノードのポリシー拡張ノードへのアップグレード （1281 ページ） を参照してください。
Cisco SD-Access ファブリックでの IPv6 アンダーレイのサポート	Cisco SD-Access ファブリックは、シングルスタックおよびデュアルスタック Catalyst Center 展開の IPv6 アンダーレイをサポートします。 「ファブリックサイトの追加 （1229 ページ）」、「ボーダーノードとしてのデバイスの追加 （1240 ページ）」、「エニーキャストゲートウェイの作成 （1262 ページ）」、および「IP アドレスプールの予約 （399 ページ）」を参照してください。
LAN 自動化ワークフローでの IPv6 をサポート	LAN 自動化ワークフローは、シングルスタック（IPv6 のみ）Catalyst Center 展開で IPv6 をサポートするように拡張されています。 「LAN 自動化によるネットワークのプロビジョニング （1196 ページ）」と「インターフェイス間のリンクを作成 （1206 ページ）」を参照してください。

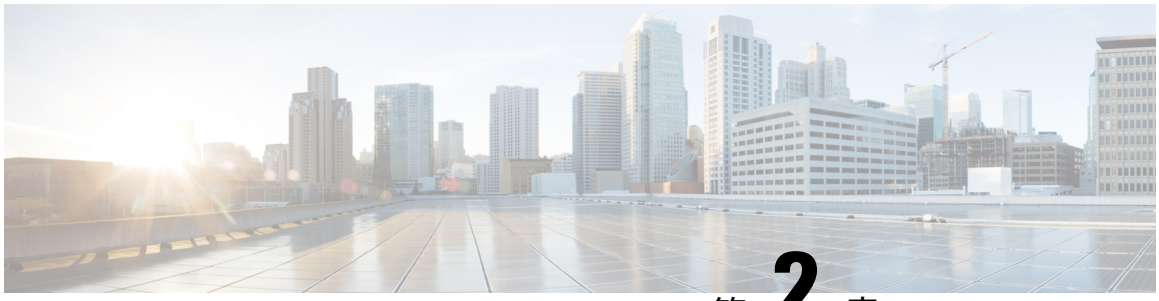
機能	説明
Catalyst Center ネットワーク階層での屋外エリアのサポート	Catalyst Center は、ネットワーク階層で [**Outdoor Areas**] のサイトエレメントをサポートしています。屋外エリアは住所または緯度経度座標を使用して追加でき、[**Global**] の下か、エリアやビルディングの下に配置できます。 （注） 屋外エリア機能はベータ版です。 屋外エリアに割り当てることができるのは、ワイヤレスアクセスポイントのみです。 屋外エリアは、ワイヤレスコントローラの物理サイトとして割り当てることはできませんが、ワイヤレスコントローラのプロビジョニング時に管理対象 AP の場所として選択できます。 「ネットワーク階層 （271 ページ）」と「屋外エリアの追加、編集、削除 （289 ページ）」を参照してください。
Catalyst 9300 シリーズ デバイス向けの拡張高速ソフトウェアアップグレード（xFSU）のサポート	xFSUを使用したデバイスのアップグレードを選択すれば、アップグレード中のダウンタイムを最小限に抑えられます。 「ISSU または xFSU を使用したソフトウェアイメージのアップグレード （657 ページ）」を参照してください。



第 I 部

はじめに

- 概要 Catalyst Center （19 ページ）
- テレメトリの設定 （59 ページ）



第 2 章

概要 Catalyst Center

- Catalyst Center の概要 （19 ページ）
- ログイン （19 ページ）
- 初回セットアップ （20 ページ）
- ユーザープロファイルのロールおよび権限 （35 ページ）
- デフォルトホームページ （36 ページ）
- Cisco.com とスマートアカウントのログイン情報の再認証 （49 ページ）
- Catalyst Center ジャーニーマップ （50 ページ）
- リモートサポート許可ダッシュボードの表示 （51 ページ）
- グローバル検索の使用 （52 ページ）
- クロック形式を 12 時間または 24 時間に設定 （54 ページ）
- Catalyst Center における明暗の外観の適用 （55 ページ）
- ローカリゼーションの有効化 （55 ページ）
- ウィンドウをお気に入りに追加 （56 ページ）
- お気に入りの管理 （57 ページ）
- Catalyst Center Insights への登録 （58 ページ）

Catalyst Center の概要

Catalyst Center を使用すると、ネットワークを一元管理できます。ポリシーの設計、プロビジョニング、適用を簡単かつ迅速に行えます。Catalyst Center GUI を使用することで、環境全体にわたるネットワークの可視性が得られます。ネットワークの洞察を活用してパフォーマンスを向上させることができます。

ログイン

ブラウザで Catalyst Center のネットワーク IP アドレスを入力してアクセスします。*Cisco Catalyst Center Release Notes* で互換性のあるブラウザのリストを確認します。この IP アドレスで外部ネットワークに接続します。これは、Catalyst Center のインストール時に設定されます。Catalyst

Center のインストールと設定の詳細については、*Cisco Catalyst Center Installation Guide*を参照してください。

アイドル セッション タイムアウトは、管理者オプションとして設定できます。アイドル セッション タイムアウトの設定方法については、*Cisco Catalyst Center Administrator Guide*の「アカウントロックアウト」を参照してください。

手順

ステップ 1 *server-ip* 形式で、Web ブラウザのアドレスバーにアドレスを入力します。*server-ip* は Catalyst Center をインストールしたサーバーの IP アドレスまたはホスト名を表します。

https://*server-ip*

例：https://192.0.2.1

ネットワーク設定によっては、ブラウザを更新して Catalyst Center サーバーのセキュリティ証明書を信頼する必要があります。これを行うと、クライアントと Catalyst Center 間のセキュアな接続が確保されます。

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

使用しているユーザー ID に SUPER-ADMIN-ROLE が割り当てられていて、このロールで最初にログインする場合、ホームページではなく初回セットアップウィザードが表示されます。

ステップ 3 右上隅に表示されたユーザー名をクリックし、[ログアウト（Log Out）] を選択すると、ログアウトできます。

初回セットアップ

このセクションでは、Catalyst Center アプライアンスのインストールと設定が完了した後に、初めて実稼働環境で使用するために Catalyst Center をセットアップする手順について説明します。初期 GUI アクセス、管理者ユーザーのセットアップ、Catalyst Center のセットアップオプションを取り上げます。

初めて実稼働環境で使用するために Catalyst Center をセットアップするには、次の手順を実行する必要があります。

1. 初めて Catalyst Center にログインし、新しい管理者ユーザーを作成します。手順については、「Catalyst Center への初回ログイン （21 ページ）.
2. クイック スタート ワークフローかいずれかの拡張セットアップ方式を使用して、Catalyst Center のセットアップを完了します。手順については、「クイック スタート ワークフローの完了 （23 ページ）」と「Catalyst Center 設定方法 （29 ページ）」を参照してください。

Catalyst Center への初回ログイン

Catalyst Center アプライアンスをインストールして設定した後、次の手順に従って初めてその GUI にログインします。初回は管理者スーパーユーザーとしてログインします（ユーザー名は「admin」で PER-ADMIN-ROLE が割り当てられます）。

（注） Catalyst Center にアクセスする際には、互換性のある HTTPS 対応ブラウザを使用してください。詳細については、『*Cisco Catalyst Center Installation Guide*』の「Complete First-Time Setup」の章にある「Compatible browsers」を参照してください。

Before you begin

Catalyst Center にログインできるように、次の情報を用意してください。

- *admin* スーパーユーザーのユーザー名とパスワードを、Catalyst Center アプライアンスの設定時に指定しました。
- 『*Cisco Catalyst Center Installation Guide*』の「Plan the Deployment」の章にある、「Required first-time setup information」に記載されている情報を参照してください。

手順

ステップ 1 Catalyst Center GUI にアクセスします。

a) Catalyst Center アプライアンスの再起動が完了したら、次のいずれかのタスクを実行します。

- ブラウザベースの構成ウィザードを使用した場合：ウィザードの最後のページで [**Open Catalyst Center Virtual Appliance**] をクリックします。
- Maglev 構成ウィザードを使用した場合：互換性のある HTTPS 対応のブラウザを起動します。**HTTPS://** と設定プロセスの最後に表示された Catalyst Center GUI の IP アドレスを使用して、Catalyst Center GUI にアクセスするホスト IP アドレスを入力します。

次のいずれかのメッセージが表示されます（使用しているブラウザによって異なります）。

- Google Chrome：接続のプライバシーは保護されません
- Mozilla Firefox：警告：今後セキュリティリスクが見つかる潜在的可能性があります

b) [**Advanced**] をクリックして続行します。

次のいずれかのメッセージが表示されます。

- Google Chrome：

```
This server could not prove that it is GUI-IP-address; its security certificate is not
trusted by your computer's
 operating system. This may be caused by a misconfiguration or an attacker intercepting your
 connection.
```

- Mozilla Firefox：

```
Someone could be trying to impersonate the site and you should not continue.
Websites prove their identity via certificates.
Firefox does not trust GUI-IP-address because its certificate issuer is unknown,
the certificate is self-signed, or the server is not sending the correct intermediate
certificates.
```

こうしたメッセージが表示されるのは、コントローラが自己署名証明書を使用しているためです。Catalyst Center での証明書の使用方法については、『*Cisco Catalyst Center Administrator Guide*』の「Certificate and private key support」を参照してください。

c) 続行するには、次のいずれかのタスクを実行します。

- Google Chrome：*GUI-IP-address*（**安全でない**）リンクをクリックして**開きます**。
- Mozilla Firefox：**[リスクを理解して続行する（Accept the Risk and Continue）]**をクリックします。

ステップ 2 Catalyst Center にログインします。

a) Catalyst Center ログインウィンドウが開いたら、次のいずれかの構成ウィザード完了タスクを実行します。

- Maglev 構成ウィザードを完了し、[**Start using DNAC pre manufactured cluster**] オプションを選択した場合は、管理者のユーザー名（**admin**）とパスワード（**P@ssword9**）を入力します。
- Maglev 構成ウィザードを完了し、[**Start configuration of DNAC in advanced mode**] オプションを選択した場合は、Catalyst Center アプライアンスの構成時に設定した管理者のユーザー名（**admin**）とパスワードを入力します。
- インストール構成ウィザードを完了したら、管理者のユーザー名（**admin**）を入力し、ウィザードの最後のウィンドウからコピーしたパスワード（**P@ssword9**）を貼り付けます。
- 高度なインストール構成ウィザードを完了した場合は、Catalyst Center アプライアンスの構成時に設定した管理者のユーザー名（**admin**）とパスワードを入力します。

b) [Log In] をクリックします。

ステップ 3 セキュリティ対策として新しい管理ユーザーを設定します。

a) 次の情報を入力します。

- [**Roles**]：`SUPER-ADMIN` ロールがすでに設定されていることを確認します。
- [**New Username**]：管理者ユーザーのユーザー名を入力します。
- [**Email**]：管理者ユーザーの電子メールアドレスを入力します。
- [**New Password**] および [**Confirm Password**]：管理者ユーザーのパスワードを入力します。このパスワードが のパスワードの要件に準拠していることを確認します。『*Cisco Catalyst Center Installation Guide*』の「Plan the Deployment」の章にある「Password requirements」を参照してください。

（注） デフォルトパスワードの変更は、特に仮想アプライアンスをセットアップするユーザーがその管理者となるユーザーと異なる場合に、ネットワークセキュリティにとって重要です。

b) [Submit] をクリックします。

Catalyst Center ログアウトされます。

ステップ 4 Catalyst Center に再度ログインします：

a) [Log In] をクリックします。
b) 新しい管理者ユーザーに関して設定したユーザー名とパスワードを入力します。
c) [Log In] をクリックします。

cisco.com のログイン情報を使用して認証するように求められます。これらのログイン情報は、ソフトウェアダウンロードの登録と、システム通信の受信に使用されます。

ステップ 5 [Authenticate] をクリックします。

（注） 今すぐ認証を行わない場合は、[**Skip**] をクリックします。

ステップ 6 [**Activate your device**] ポップアップウィンドウで、アクティベーションコードが表示されていることを確認し、[**Next**] をクリックします。

[Terms & Conditions] 画面が開き、ソフトウェアのシスコ エンドユーザー ライセンス契約（EULA）および現在利用可能な補足条件へのリンクが表示されます。

ステップ 7 各ドキュメントを確認したら、[**Next**] をクリックして EULA に同意します。

[Quick Start Overview] スライダが開きます。[>] をクリックすると、Catalyst Center の使用を開始するために、クイック スタート ワークフローで完了までサポートされるタスクの説明が表示されます。

次のタスク

クイック スタート ワークフローまたはいずれかの高度なセットアップ方式を完了することで、初回セットアップを続行できます。詳細については、「クイック スタート ワークフローの完了 （23 ページ）」および「Catalyst Center 設定方法 （29 ページ）」を参照してください。

クイック スタート ワークフローの完了

このワークフローを完了して、Catalyst Center がデバイスからのテレメトリの収集を管理および有効化するデバイスを検出します。

（注） または、強化されたセットアップ方式のいずれかを使用して Catalyst Center を設定することもできます。詳細については、Catalyst Center 設定方法 （29 ページ） を参照してください。

管理者スーパーユーザーとして初めてログインすると（ユーザー名 `admin` と SUPER-ADMIN-ROLE が割り当てられた）、クイック スタート ワークフローが自動的に開始されます。

Before you begin

以下の前提条件を満たしていることを確認します。

- 初期セットアップ：初めて Catalyst Center にログインし、新しい管理者ユーザーを作成した。詳細については、Catalyst Center への初回ログイン （21 ページ） を参照してください。
- 必要な情報：『*Cisco Catalyst Center Installation Guide*』の「Plan the Deployment」の章にある「Required first-time setup information」に記載されている情報を手元に用意してください。

  次の機能が含まれています。

  - ユーザーアクセス計画：ロール、一意のパスワード、権限設定を含む、システムにアクセスする必要があるユーザーのリスト。
  - サービス統合（オプション）：IPAM サーバーまたは Cisco Identity Services Engine （ISE）を使用する予定の場合は、関連する URL とログイン情報を用意しておきます。

手順

ステップ 1 **[クイックスタートの概要（Quick Start Overview）]** スライダで、[実行する（Let's Do it）] をクリックします。

ステップ 2 [デバイスの検出：IP範囲の指定（Discover Devices: Provide IP Ranges）] 画面で、次の情報を入力し、[次へ（Next）] を選択します。

- デバイス検出ジョブの名前。
- 検出するデバイスの IP アドレスの範囲。追加の範囲を入力するには、[+] をクリックします。
- アプライアンスのループバックアドレスを優先管理 IP アドレスとして指定するかどうかを指定します。詳細については、『*Cisco Catalyst Center User Guide*「Preferred management IP address」のトピックを参照してください。

ステップ 3 [デバイスの検出：ログイン情報の指定（Discover Devices: Provide Credentials）] 画面で、設定するログイン情報のタイプに関する情報（「デバイスログイン情報 （26 ページ）」を参照）を入力し、[次へ（Next）] を選択します。

ステップ 4 [サイトの作成（Create Site）] 画面で、テレメトリを容易にするために検出するデバイスを 1 つのサイトにグループ化し、[次へ（Next）] を選択します。

サイトの情報を手動で入力するか、提供されたマップで使用する場所をクリックします。

ステップ 5 [テレメトリの有効化（Enable Telemetry）] 画面で、Catalyst Center にテレメトリを収集させるネットワークコンポーネントを選択し、[次へ（Next）] をクリックします。



（注） [Enable Telemetry] オプションと [Disable Telemetry] オプションの両方がグレー表示されている場合、これは、デバイスがテレメトリをサポートできないか、デバイスがテレメトリの有効化をサポートしていない OS バージョンを実行していることを示しています。

ステップ 6 [**Summary**] 画面で、入力した設定を確認し、次のいずれかを実行します。

- 変更を加える場合は、該当する [編集（Edit）] リンクをクリックして、関連画面を開きます。
- 設定に問題がなければ、[検出とテレメトリの開始（Start Discovery and Telemetry）] をクリックします。Catalyst Center によって設定が検証され、問題が発生しないことが確認されます。検証が完了すると、画面が更新されます。

  Catalyst Center により、ネットワークのデバイスを検出し、選択したネットワークコンポーネントのテレメトリを有効にするプロセスが開始されます。このプロセスには 30 分以上かかります（大規模なネットワークの場合はさらに長くなります）。

ホームページの上部に、クイック スタート ワークフローが完了したことを示すメッセージが表示されます。

次のタスク

- [検出の表示（View Discovery）] を選択して [検出（Discovery）] ページを開き、ネットワーク内のデバイスが検出されたことを確認します。
- [ネットワーク設定に移動（Go to Network Settings）] リンクを選択し、[デバイスログイン情報（Device Credentials）] ページを開きます。ここから、以前に入力したログイン情報がサイトに設定されていることを確認できます。
- [アクティビティページの表示（View Activity Page）] リンクを選択して [タスク（Tasks）] ページを開き、Catalyst Center ですでに実行がスケジュールされているタスク（セキュリティアドバイザリの毎週のネットワークスキャンなど）を表示します。
- [ワークフローホーム（Workflow Home）] リンクを選択し、ネットワークのセットアップと維持に役立つガイド付きワークフローにアクセスします。

デバイスログイン情報

次の表に、クイックスタートワークフローを完了するときに [デバイスの検出：ログイン情報の入力（Discover Devices: Provide Credentials）] 画面に入力する必要がある情報を示します。

表 *3:* デバイスログイン情報フィールドの説明

フィールド	説明
[CLI (SSH) Credentials]	
Username	ネットワーク内のデバイスの CLI にログインするために使用するユーザー名。
パスワード	ネットワーク内のデバイスの CLI にログインするために使用するパスワード。入力するパスワードは、8 文字以上にする必要があります。
Name/Description	CLI ログイン情報の名前または説明。
パスワードの有効化	CLI でより高い権限レベルを有効にするために使用するパスワード。ネットワークデバイスで必要な場合にのみ、このパスワードを設定します。
[SNMP Credentials: SNMPv2c Read] タブ （注） Catalyst Center は、FIPS モードが有効になっている場合、SNMPv2c ログイン情報をサポートしません。代わりに、SNMPv3 ログイン情報を入力する必要があります。FIPS モードの詳細については、『*Cisco Catalyst Center Installation Guide*』の「Maglev ウィザードを使用したアプライアンスの設定」の章の「Maglev ウィザードを使用したプライマリノードの設定」を参照してください。	
Name/Description	SNMPv2c 読み取りコミュニティストリングの名前または説明。
Community String	デバイス上の SNMP 情報を表示するためにのみ使用される読み取り専用コミュニティ ストリング パスワード。
[SNMP Credentials: SNMPv2c Write] タブ	
Name/Description	SNMPv2c 書き込みコミュニティストリングの名前または説明。
Community String	デバイス上の SNMP 情報を変更するために使用される書き込みコミュニティストリング。
[SNMP Credentials: SNMPv3]	
Name/Description	SNMPv3 ログイン情報の名前または説明。
Username	SNMPv3 ログイン情報に関連付けられているユーザー名。

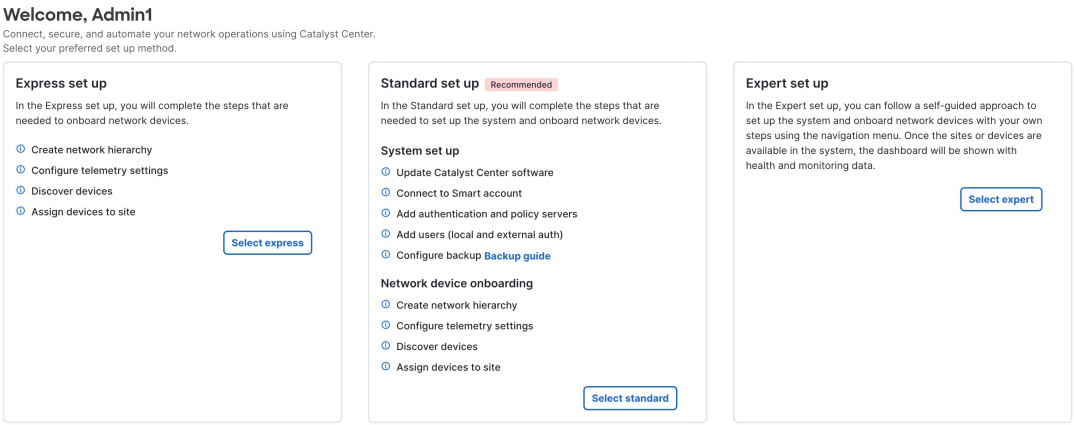
フィールド	説明
Mode	SNMP メッセージを必要とするセキュリティレベル。 • [No Authentication, No Privacy]（noAuthnoPriv）：認証も暗号化も行いません。 • [Authentication, No Privacy]（authNoPriv）：認証は行いますが、暗号化は行いません。 • [Authentication and Privacy]（authPriv）：認証と暗号化の両方を行います。 （注） FIPS モードが有効な場合、Catalyst Center では [Authentication and Privacy] モードのみがサポートされます。
Authentication Password	SNMPv3 を使用するデバイスから情報にアクセスするために必要なパスワード。パスワードの長さは、最低 8 文字である必要があります。次の点に注意してください。 • 一部のワイヤレスコントローラでは、パスワードは少なくとも 12 文字以上にする必要があります。ワイヤレス コントローラのパスワードの最小要件を必ず確認してください。パスワードに必要な最低限の文字数が守られないと、デバイスではCatalyst Centerによる検出、監視、管理が行われなくなります。 • パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。
Authentication Type	[Authentication and Privacy] または [Authentication、No Privacy] が認証モードとして設定されている場合に使用されるハッシュベースのメッセージ認証コード（HMAC）タイプ。 • [SHA]：HMAC-SHA 認証。 • [MD5]：HMAC-MD5 認証。 （注） Catalyst Center は、FIPS モードが有効になっている場合、この認証タイプをサポートしません。

フィールド	説明
Privacy Type	プライバシー タイプ。（[Mode] として [Authentication and Privacy] を選択した場合に有効になります）。次のいずれかのプライバシー タイプを選択します。 • [AES128]：暗号化の 128 ビット CBC モード AES。 • **CISCOAES192**：シスコのデバイス上での暗号化の 192 ビット CBC モード AES。 • **CISCOAES256**：シスコのデバイス上での暗号化の 256 ビット CBC モード AES。 （注） Catalyst Center 第 3 世代アプライアンスの場合は次のとおりです。 • 検出機能とインベントリ機能の使用は、プライバシータイプ CISCOAES192 およびCISCOAES256のみでサポートされています。Assurance機能はサポートされていません。 • プライバシータイプAES128は、検出、インベントリ、およびAssuranceでサポートされています。 Catalyst Center on ESXi の場合： • プライバシータイプ AES192 および AES256 は、検出機能とインベントリ機能での使用でのみサポートされています。アシュアランス機能はサポートされていません。 • プライバシータイプAES128は、検出、インベントリ、およびアシュアランスでサポートされています。
Privacy Password	AES128、AES192、およびAES256暗号化標準規格でサポートされているデバイスで交換されるメッセージを暗号化するための秘密鍵を生成するために使用されるSNMPv3 プライバシーパスワード。パスワード（またはパスフレーズ）は、8 文字以上にする必要があります。 （注） • 一部のワイヤレスコントローラでは、パスワードは少なくとも 12 文字以上にする必要があります。ワイヤレス コントローラのパスワードの最小要件を必ず確認してください。パスワードに必要な最低限の文字数が守られないと、デバイスではCatalyst Centerによる検出、監視、管理が行われなくなります。 • パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。
NETCONF	

フィールド	説明
Port	Cisco IOS-XE を実行するワイヤレスコントローラを検出するために Catalyst Center が使用する必要がある NETCONF ポート。

Catalyst Center 設定方法

初めてログインすると、クイックスタートワークフローが自動的に開始します。詳細な設定方法を表示するには、クイック スタート ワークフローを終了し、デフォルトのホームページに移動します。デフォルトのホームページには、利用可能な設定方法が表示されます。



SUPER-ADMIN-ROLE または NETWORK-ADMIN-ROLE 権限がある場合は、次のいずれかの方法を使用して Catalyst Center を設定できます。

- エクスプレスセットアップ：このセットアップは、ネットワークデバイスの導入準備に役立ちます。手順については、[Complete the express setup method] を参照してください。
- 標準セットアップ：この推奨セットアップは、システムの設定およびネットワークデバイスの導入準備に役立ちます。手順については、「Complete the standard setup method」を参照してください。
- エキスパートセットアップ：この自己主導型セットアップでは、システムとオンボーディングのネットワークデバイスを個別に設定できます。このオプションは、エキスパートユーザーにのみ推奨します。この説明については、エキスパートセットアップの完了 （34 ページ） を参照してください。

（注） あるセットアップ方法を開始した後で、別のセットアップ方法を使用する場合は、選択した方法を変更できます。デフォルトのホームページに戻り、[<設定方法名> の選択（Select <setup method name>）] をクリックして別の設定方法を開始してください。

Express セットアップを完了します

高速セットアップメソッドを使用して Catalyst Center を設定するには、次の手順に従います。

Before you begin

Catalyst Center への初回ログイン （21 ページ） が正常に完了したことを確認してください。

手順

ステップ 1 ホームページから、[エキスプレスを選択（Select express）] をクリックします。

Expressセットアップメソッドが起動し、[**Design** > **Network Hierarchy**] ページが開きます。[**Express set up**] スライドインペイン では、このセットアップメソッドを完了するための手順が表示されます。

ヒント

- 提示されている順序で手順を完了することを推奨します。
- [**Go to this step**] をクリックすると、任意の手順の関連ページを表示できます。
- [**Expressセットアップ**] スライドインペインをいつでも閉じるには、[**Exit**] をクリックします。ダイアログボックスで、[**Exit**] をもう一度クリックします。
- リストされている手順のいずれかを完了した後、Catalyst Center の右上にある [**Express set up**] をクリックすることで、この スライドインペイン を再度開くことができます。
- この スライドインペイン の最下部までスクロールし、[**<Number of> steps completed**] セクションを開きます。完了した手順を未完了としてマークするには、その手順の [**Mark as complete**] チェックボックスをオンにします。手順が不完全になり、進行状況バーがこの変更を反映して更新されます。

ステップ 2 ネットワーク階層の作成手順を完了します。

a) [**Design** > **Network Hierarchy**] ページで、エリア、建物、フロアを含むネットワーク階層を作成します。

手順については、「ネットワーク階層の設計 （271 ページ）.

b) [**Create network hierarchy**] で、この手順では [**Mark as complete**] チェックボックスをオンにします。

進行状況バーが更新され、4 つの手順のうちいずれかが完了したことが示されます。

ステップ 3 テレメトリ設定の手順を完了します。

a) [**Configure telemetry settings**] で、[**Go to this step**] をクリックします。

b) [**Telemetry**] の [**Design** > **Network Settings** ページのテレメトリデータ収集に必要な設定を行います。

手順については、「テレメトリを使用した syslog、SNMP トラップ、NetFlow コレクタサーバー、および有線クライアントデータ収集の設定 （59 ページ）.

c) [**Configure telemetry settings**] で、この手順の [**Mark as complete**] チェックボックスをオンにします。

進行状況バーが更新され、4 つの手順のうち 2 つの手順が完了したことが示されます。

ステップ 4 デバイスの検出手順を完了します。

a) [**Discover devices**] で、[**Go to this step**] をクリックします。

デバイスのオンボーディングワークフローが開始されます。

b) オンボーディングデバイスワークフローを完了して、デバイスを検出します。

手順については、「ディスカバリの実行 （86 ページ）.

c) [**Discover devices**] で、[**Mark as complete**] チェックボックスをオンにします。

進行状況バーが更新され、4 つの手順のうち 3 つの手順が完了したことが示されます。

ステップ 5 サイトへのデバイスの割り当て手順を完了します。

a) [**Assign devices to site**] で、[**Go to this step**] をクリックします。

b) [**Provision** > **Inventory**] ページで、関連するサイトにデバイスを割り当てます。

手順については、「プロビジョニングされていないデバイスのサイトへの割り当て（189ページ）」および「プロビジョニングされたデバイスを別のサイトに割り当てる （191ページ）」を参照してください。

c) [**Assign devices to site**] で、[**Mark as complete**] チェックボックスをオンにします。

進行状況バーが更新され、4つの手順のうち4つの手順が完了したことが示されます。完了メッセージには、作成されたサイト数と検出されたデバイス数が要約されます。

ステップ 6 [**Launch home page**] をクリックして、Catalyst Center のエクスプレスセットアップを完了します。

Catalyst Center の Express セットアップが完了すると、ホームページが表示されます。

（注） 検出されたデバイスがホームページに表示されるまでに時間がかかる場合があります。

標準セットアップの完了

標準のセットアップ方法を使用して Catalyst Center を設定するには、次の手順に従います。

Before you begin

Catalyst Center への初回ログイン （21 ページ） が正常に完了したことを確認してください。

手順

ステップ 1 ホームページから、[標準を選択（Select standard）] をクリックします。

標準のセットアップ方法では、起動して [**System** > **Software Management**] ページを開きます。**標準セットアップ** スライドインペイン では、このセットアップ方法を完了するための手順が表示されます。

ヒント

- 提示されている順序で手順を完了することを推奨します。
- [**Go to this step**] をクリックすると、任意の手順の関連ページを表示できます。
- **標準セットアップ**スライドインペインは、[**Exit**] をクリックすることでいつでも閉じることができます。ダイアログボックスで、[**Exit**] をもう一度クリックします。
- リストされている手順のいずれかを完了した後、Catalyst Center の右上にある [**Standard set up**] をクリックすると、このスライドインペイン を再度開くことができます。
- このスライドインペインの最下部までスクロールし、[**<Number of> steps completed**] セクションを開きます。完了した手順を未完了としてマークするには、その手順の [**Mark as complete**] チェックボックスをオンにします。手順が不完全になり、進行状況バーがこの変更を反映して更新されます。

ステップ 2 Catalyst Center ソフトウェアの更新の手順を完了します。

a) [**System** > **Software Management**] ページで、Catalyst Center ソフトウェアを最新の推奨バージョンに更新します。

手順については、「*Cisco Catalyst Center Upgrade Guide*」を参照してください。

b) [**Update Catalyst Center software**] で、この手順の [**Mark as complete**] チェックボックスをオンにします。

進行状況バーが更新され、9 つの手順のうちいずれかが完了したことが示されます。

ステップ 3 スマートアカウントへの接続の手順を完了します。

a) [**Connect to Smart account**] で、[**Go to this step**] をクリックします。

b) [**Smart Account**] ページで、シスコスマートアカウントをスマートライセンス アカウントに接続します。

手順については、『*Cisco Catalyst Center Administrator Guide*』の「スマートアカウントの設定」を参照してください。

c) [**Connect to Smart account**] で、この手順は [**Mark as complete**] チェックボックスをオンにします。

進行状況バーが更新され、9 つの手順のうち 2 つが完了したことが示されます。

ステップ 4 認証サーバーおよびポリシーサーバーの追加手順を完了します。

a) [**Add authentication and policy servers**] で、[**Go to this step**] をクリックします。

b) [**Authentication and Policy Servers**] ページで、Cisco Identity Services Engine（Cisco ISE）または AAA サーバーを追加します。

Catalyst Center は AAA サーバーをユーザー認証に使用し、Cisco ISE をユーザー認証とアクセス制御の両方に使用します。手順については、『*Cisco Catalyst Center Administrator Guide*』の「認証サーバーおよびポリシーサーバーの設定」を参照してください。

c) [**Add authentication and policy servers**] で、[この手順では [**Mark as complete**] チェックボックスをオンにします。

進行状況バーが更新され、9 つの手順のうち 3 つが完了したことが示されます。

ステップ 5 ユーザーの追加手順を完了します。

a) [**Add users (local and external auth)**] で、[**Go to this step**] をクリックします。

b) [**User Management**] ページで、必要なユーザーを追加して、ユーザーが Catalyst Center にアクセスできるようにします。

手順については、『*Cisco Catalyst Center Administrator Guide*』の「内部ユーザーの作成」を参照してください。

c) 外部ユーザーの認証と許可に外部サーバーを使用している場合、外部認証を有効にする必要があります。

手順については、『*Cisco Catalyst Center Administrator Guide*』の「外部認証の設定」を参照してください。

d) [**Add users (local and external auth)**] で、この手順の [**Mark as complete**] チェックボックスをオンにします。

進行状況バーが更新され、9 つの手順のうち 4 つが完了したことが示されます。

ステップ 6 バックアップの設定手順を完了します。

a) [**Configure backup**] で、[**Go to this step**] をクリックします。

b) [**System** > **Backup & Restore**] ページで、Catalyst Center の自動化および Assurance データをバックアップするようにリモートサーバーを設定し、Catalyst Center の自動化および Assurance データを復元するようにリモートサーバーを接続します。

手順については、『*Cisco Catalyst Center Administrator Guide*』の「バックアップファイルを保存する場所の設定」および「バックアップからのデータの復元」を参照してください。

c) [**Configure backup**] で、この手順の [**Mark as complete**] チェックボックスをオンにします。

進行状況バーが更新され、9 つの手順のうち 5 つが完了したことが示されます。

ステップ 7 ネットワーク階層の作成手順を完了します。

a) [**Create network hierarchy**] で、[**Go to this step**] をクリックします。

b) [**Design** > **Network Hierarchy**] ページで、エリア、建物、フロアを含むネットワーク階層を作成します。

手順については、「ネットワーク階層の設計 （271 ページ）.

c) [**Create network hierarchy**] で、この手順では [**Mark as complete**] チェックボックスをオンにします。

進行状況バーが更新され、9 つ中 6 つの手順が完了したことが示されます。

ステップ 8 テレメトリ設定の手順を完了します。

a) [**Configure telemetry settings**] で、[**Go to this step**] をクリックします。

b) [**Telemetry**] の [**Design** > **Network Settings** ページのテレメトリデータ収集に必要な設定を行います。

手順については、「テレメトリを使用した syslog、SNMP トラップ、NetFlow コレクタサーバー、および有線クライアントデータ収集の設定 （59 ページ）.

c) [**Configure telemetry settings**] で、この手順の [**Mark as complete**] チェックボックスをオンにします。

進行状況バーが更新され、9 つの手順のうち 7 つが完了したことが示されます。

ステップ 9 デバイスの検出手順を完了します。

a) [**Discover devices**] で、[**Go to this step**] をクリックします。

デバイスのオンボーディングワークフローが開始されます。

b) オンボーディングデバイスワークフローを完了して、デバイスを検出します。

手順については、「ディスカバリの実行 （86 ページ）.

c) [**Discover devices**] で、[**Mark as complete**] チェックボックスをオンにします。

進行状況バーが更新され、9 つのうち 8 つの手順が完了したことが示されます。

ステップ 10 サイトへのデバイスの割り当て手順を完了します。

a) [**Assign devices to site**] で、[**Go to this step**] をクリックします。

b) [**Provision** > **Inventory**] ページで、関連するサイトにデバイスを割り当てます。

手順については、「プロビジョニングされていないデバイスのサイトへの割り当て （189 ページ）」および「プロビジョニングされたデバイスを別のサイトに割り当てる （191 ページ）」を参照してください。

c) [**Assign devices to site**] で、[**Mark as complete**] チェックボックスをオンにします。

進行状況バーが更新され、9 つ中 9 つの手順が完了したことが示されます。完了メッセージには、作成されたサイト数と検出されたデバイス数が要約されます。

ステップ 11 [**Launch home page**] をクリックして、Catalyst Center の標準セットアップを完了します。

Catalyst Center の標準セットアップが完了すると、ホームページが表示されます。

（注） 検出されたデバイスがホームページに表示されるまでに時間がかかる場合があります。

エキスパートセットアップの完了

エキスパートセットアップメソッドを使用して Catalyst Center を設定するには、次の手順に従います。

Before you begin

（注） 専門ネットワーク管理者のみがこのセットアップ方法を使用することを推奨します。このメソッドでは、詳細なセットアップ手順は提供されません。Express および標準のセットアップ方法では、アップグレード方法が順に説明されています。詳細については、Catalyst Center 設定方法 （29 ページ）を参照してください。

Before you begin

Catalyst Center への初回ログイン （21 ページ） が正常に完了したことを確認してください。

手順

ステップ 1 ホームページから、[エキスパートの選択（Select expert）] をクリックします。

ステップ 2 **[エキスパートセットアップ（Expert set up）]** ダイアログボックスで、[OK] をクリックして続行します。

ステップ 3 ネットワークの必要に応じて Catalyst Center を設定してください。

ネットワーク設定に関する一般的な手順については、以下の情報を参考にしてください。

- ネットワーク階層の設計 （271 ページ）
- ネットワークの検出 （73 ページ）
- インベントリの管理 （99 ページ）

デバイス検出が完了すると、デフォルトのホームページが表示され、Catalyst Center のエキスパートセットアップが完了したことが示されます。

ユーザープロファイルのロールおよび権限

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

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

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

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

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

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

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

デフォルトホームページ

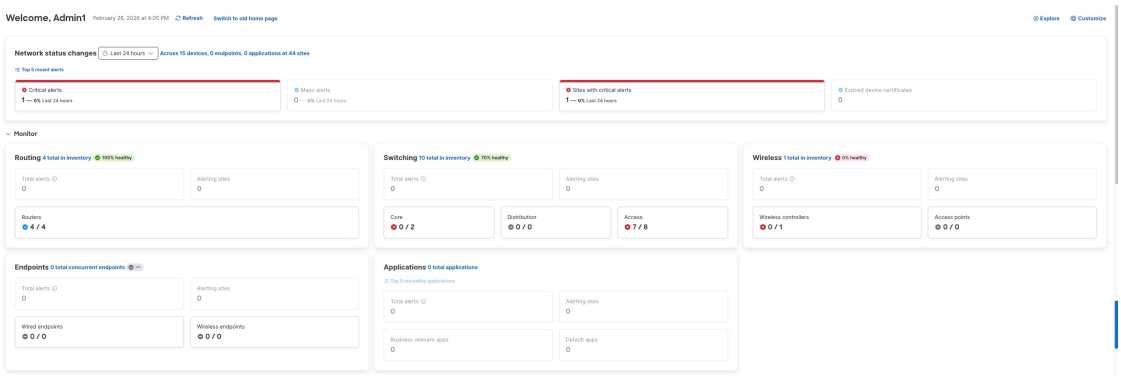
ログインすると、Catalyst Center ホームページが表示されます。このページでは、ネットワークのより詳細な概要ビューが提供され、全体的なパフォーマンス、ステータス、正常性をすばやく評価できます。メインメニュー、ウィンドウの右上部分にあるアイコン、および [インタラクティブヘルプ（Interactive Help）] は、以前のホームページと同様に機能します。

ホームページのさまざまなビュー

ホームページは、Catalyst Center のさまざまなステージやログインに使用されるロールなどの要因によって異なります。

たとえば、インベントリにデバイスがある場合、 Catalyst Center ホームページの Day-*N* ビューが表示されます。

図 *1 : Catalyst Center* ホームページの *Day-N* ビュー



クイックアクション

次の操作を実行できます。

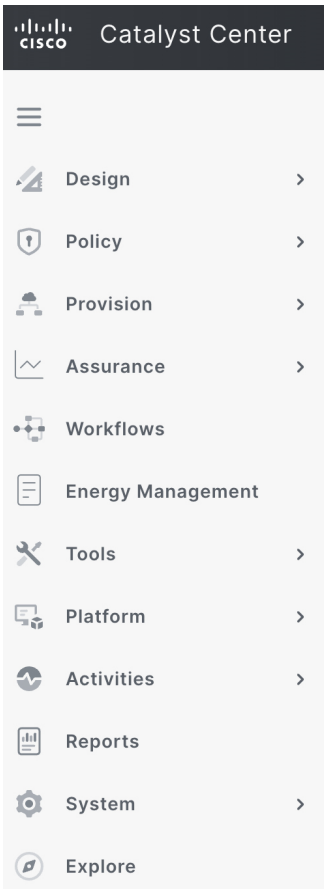
- ホームページデータを手動で更新するには、ページの上部にある [更新（Refresh）] をクリックします。
- 以前のホームページを表示するには、ページの上部にある [古いホームページに切り替える（Switch to old home page）] をクリック

  デフォルトのホームページに戻るには、古いホームページの上部にある [新しいホームページに切り替える（Switch to new home page）] をクリックします。
- [詳細（Explore）] ページに Catalyst Center ジャーニーマップを表示するには、ページの右上隅にある [詳細（Explore）] をクリックします。詳細については、Catalyst Center ジャーニーマップ （50 ページ）を参照してください。

メイン メニュー

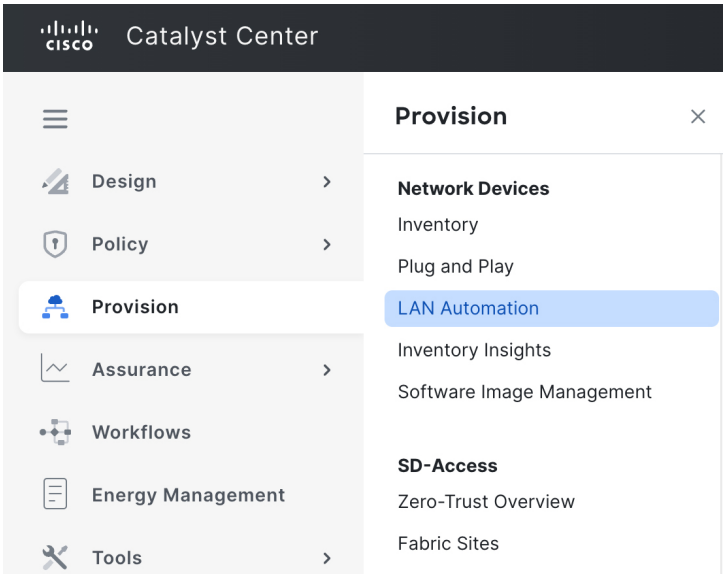
Catalyst Center のメインメニューから、Catalyst Center が提供する多くのネットワーク管理機能にアクセスできます。

図 *2 : Catalyst Center* メインメニュー



特定の Catalyst Center ページを開くには、該当するメニューオプションをクリックするか、該当するオプションにカーソルを合わせてそのサブメニューを表示します。次に、開くページ（[LAN自動化（LAN Automation）] ページなど）のリンクをクリックします。

図 *3 : Catalyst Center* サブメニュー



一部のオプション（[ワークフロー（Workflows）]など）にはサブメニューがありません。メインメニューから直接開くことができます。

デフォルトでは、Catalyst Center にはメインメニューラベルが表示されます。これらのラベルを表示するか非表示にするには、[展開（Expand）/折りたたみ（Collapse）] アイコン（≡）をクリックします。

ツールバーアイコンとヘルプオプション

[Catalyst Center] ウィンドウの右上部分はツールバーです。このツールバーのアイコンをクリックすると、一般的なタスクを実行できます。この表では、各アイコンについて説明します。

アイコン	説明
	[Search]：Catalyst Center データベース内の任意の場所に保存されているデバイス、ユーザー、ホスト、メニュー、およびその他の項目を検索します。
	[お気に入り（Favorite）]：Catalyst Center の任意のウィンドウをお気に入りに追加して、より簡単かつ迅速に移動できます。詳細については、ウィンドウをお気に入りに追加（56ページ）を参照してください。
	[ヘルプ（Help）]：ヘルプオプションのリストを表示します。詳細については、「ヘルプメニューオプション」を参照してください。
	[Software Updates]：利用可能なソフトウェアアップデートのリストが表示されます。[Go to Software Updates] リンクをクリックすると、システムとアプリケーションのアップデートを表示できます。

アイコン	説明
	[Notifications]：イベント通知を表示し、通知設定を指定します。通知アイコンの横にある赤色の丸は、新しい通知があることを示します。

ヘルプオプション

ツールバーのヘルプアイコンをクリックして、ヘルプオプションを表示します。この表は、これらのオプションを説明します。

オプション	説明
API リファレンス	Cisco DevNet に Catalyst Center プラットフォーム API ドキュメントが開きます。
バージョン情報	現在の Catalyst Center のソフトウェアバージョンが表示されます。 • [Release Notes] をクリックすると、別のブラウザタブでリリースノートが起動します。 • [Packages] をクリックすると、システムおよびアプリケーションパッケージのバージョンが表示されます。 • [Serial number] をクリックすると、Catalyst Center のアプライアンスのシリアル番号が表示されます。 • [Member ID] をクリックすると、メンバー ID が表示されます。
開発者リソース	開発者ツールにアクセスできる Cisco DevNet が開きます。
サポートに連絡	Cisco Technical Assistance Center（TAC）でサポートケースが開きます。
Help	状況に応じたオンラインヘルプが、ブラウザの別のタブで開きます。
リモートサポート許可	ネットワークのトラブルシューティングを行うために、シスコの専門家に Catalyst Center へのリモートアクセスを許可します。詳細については、リモートサポート許可ダッシュボードの表示（51 ページ）を参照してください。
Cisco CX Cloud Success Tracks	新しいウィンドウで Cisco CX Cloud Success Tracks の Web サイトにアクセスします。
キーボードショートカット	ショートカットグループのキーボードショートカット名、ショートカットキー、およびショートカットキーの組み合わせを表示します。

オプション	説明
Make a Wish	コメントや提案事項が Catalyst Center 製品チームに送信されます。

ホームページのデフォルトセクション

ホームページは、次のデフォルトセクションで構成されています。

- ネットワークステータスの変更
- モニター
- 規則遵守およびその他の通知
- デバイスの詳細機能

各セクションには、インタラクティブな要素と非インタラクティブな要素があります。ハイパーリンクが設定されたテキストやカードなど、セクション内のインタラクティブな要素をクリックすると、関連する Catalyst Center ページに移動して詳細情報や管理タスクを表示できます。

ネットワークステータスの変更

このセクションには、アラートおよび期限切れのデバイス証明書の最近のデータが表示されます。

次の表では、[ネットワークステータスの変更（Network status changes）] セクションで、最近のネットワーク ステータス データをフィルタ処理して表示する方法について説明します。

実行する操作	結果
このセクションのデータを特定の時間範囲でフィルタ処理する	**[最新（Last）] <*time range*>** ドロップダウンリストから、時間範囲オプションを選択して、その時間範囲のネットワークステータスの変更を表示します。 このセクションのデータは、選択した時間範囲に基づいて更新されます。
時間範囲の選択に基づいて、最近ネットワークステータスが変更されたデバイスを表示する	[N個のサイトでのN個のデバイス、N個のエンドポイント、N個のアプリケーション全体（Across <*number of*> devices, <*number of*> endpoints, <*number of*> applications at <*number of*> sites）] をクリックします。 **[プロビジョニング（Provision）] > [インベントリ（Inventory）]** ページが表示されます。

実行する操作	結果
最近の上位 5 つのアラートを表示する	[上位5つの最近のアラート（Top 5 recent alerts）] をクリックします。 スライドインペイン が開き、最近の重大なアラートおよび重要なアラートの上位 5 件が、優先順位、名前、サイト、およびシビラティ（重大度）とともに一覧表示されます。

次の表では、[ネットワークステータスの変更（Network status changes）] セクションのカードについて説明します。

（注） 次の重大な問題および重要な問題の定義を理解しておいてください。

- [P1]：ネットワーク運用に幅広い影響を与える前に早急な対応を必要とする重大な問題。
- [P2]：複数のデバイスまたはクライアントに影響を与える可能性がある主要な問題。

カード名	説明
重大アラート	重大なアラートの数を表示します。 このカードをクリックすると、**[アシュアランス（Assurance）]**>**[問題およびイベント（Issues and Events）]**ダッシュボードのすべての未解決の重大（P1）な問題が表示されます。『*Cisco Catalyst Assurance User Guide*』の「View and Manage Issues」を参照してください。
重要なアラート	重要なアラートの数を表示します。 このカードをクリックすると、**[アシュアランス（Assurance）]**>**[問題およびイベント（Issues and Events）]**ダッシュボードのすべての未解決の重要（P2）な問題が表示されます。『*Cisco Catalyst Assurance User Guide*』の「View and Manage Issues」を参照してください。
重大なアラートがあるサイト	重大なアラートがあるサイトの数を表示します。 このカードをクリックすると、**[アシュアランス（Assurance）]**>**[問題およびイベント（Issues and Events）]**ダッシュボードの重大（P1）な問題によって影響を受けるサイトが表示されます。『*Cisco Catalyst Assurance User Guide*』の「View and Manage Issues」を参照してください。
期限切れのデバイス証明書	期限切れのデバイス証明書の数を表示します。

監視

この折りたたみ可能なセクションには、ルーティング、スイッチング、ワイヤレス、エンドポイント、アプリケーション、および Software-Defined Access（Cisco SD-Access）のネットワーク モニタリング データが表示されます。

次の表では、[モニター（Monitor）] セクションのダッシュレットについて説明します。

（注） インベントリにルーティング、スイッチング、またはワイヤレスデバイスがない場合、関連するダッシュレットに [インベントリの合計数（<*Number of*> total in inventory）] ではなく [デバイスの追加（Add devices）] と表示されます。

ダッシュレットの名前	説明
ルーティング	アラート、アラートサイト、およびルータの総数を表示します。 [インベントリの合計数（<*Number of*> total in inventory ）] をクリックすると、**[プロビジョニング（Provision）]**>**[インベントリ（Inventory）]**ページでインベントリ内のすべてのルータを表示できます。インベントリの管理 （99 ページ） を参照してください。
スイッチング	アラート、アラートサイト、およびスイッチ（コア、ディストリビューション、およびアクセス）の合計数を表示します。 [インベントリの合計数（<*Number of*> total in inventory ）] をクリックすると、**[プロビジョニング（Provision）]**>**[インベントリ（Inventory）]**ページでインベントリ内のすべてのスイッチを表示できます。インベントリの管理 （99 ページ） を参照してください。
ワイヤレス	アラート、アラートサイト、ワイヤレスコントローラ、およびアクセスポイント（AP）の総数を表示します。 [インベントリの合計数（<*Number of*> total in inventory ）] をクリックすると、**[プロビジョニング（Provision）]**>**[インベントリ（Inventory）]**ページでインベントリ内のすべての AP と ワイヤレスコントローラ を表示できます。インベントリの管理 （99 ページ） を参照してください。
エンドポイント	アラート、アラートサイト、および有線およびワイヤレスエンドポイントの総数を表示します。 [同時エンドポイントの合計数（<*Number of*> total concurrent endpoints）] をクリックすると、**[アシュアランス（Assurance）]**>**[正常性（Health）]**ダッシュボードに移動してクライアントの正常性を表示できます。『*Cisco Catalyst Assurance User Guide*』の「Monitor and Troubleshoot Client Health」を参照してください。

ダッシュレットの名前	説明
アプリケーション	アラート、アラートサイト、およびビジネス関連のアプリケーションとデフォルトのアプリケーションの総数を表示します。 • [アプリケーションの合計数（<*Number of*> total applications）] をクリックすると、**[アシュアランス（Assurance）] > [正常性（Health ）]**ダッシュボードに移動してアプリケーションの正常性を表示できます。 • [上位5つの異常なアプリケーション（Top 5 unhealthy applications）] をクリックすると、スライドインペインに重大および重要なアラートの影響を受ける上位5つの異常なアプリケーションが一覧表示されます。 『*Cisco Catalyst Assurance User Guide*』の「Monitor Application Health」を参照してください。
ソフトウェア定義型アクセス	（注） このダッシュレットは、Cisco SD-Access パッケージがインストールされている場合にのみ表示されます。 アラート、ファブリックサイト、レイヤ3仮想ネットワーク、および Cisco SD-Access トランジットの総数を表示します。 [ファブリックサイトの合計数（<*Number of*> total fabric sites）] をクリックすると、**[アシュアランス（Assurance）] > [正常性（Health ）]**ダッシュボードに移動して Cisco SD-Access の正常性を表示できます。『*Cisco Catalyst Assurance User Guide*』の「Monitor and Troubleshoot SD-Access Health」を参照してください。

規則遵守およびその他の通知

この折りたたみ可能なセクションには、ソフトウェアイメージ管理（SWIM）、コンプライアンス、セキュリティ、ライセンス、システム、および最近のアクティビティに関する通知データが表示されます。

この表では、[規則遵守およびその他の通知（Compliance and other notices）] セクションのダッシュレットについて説明します。

ダッシュレットの名前	説明
ソフトウェアイメージ	高アドバイザリおよび重大なアドバイザリがあるデバイス、標準イメージのないデバイス、およびイメージの更新に失敗したデバイスの数を表示します。 [ソフトウェアイメージの合計数（<*Number of*> total software images）] をクリックして、**[プロビジョニング（Provision）]** > **[ソフトウェアイメージ管理（Software Image Management）]**ページに移動します。ソフトウェア イメージの管理 （631 ページ）を参照してください。
セキュリティ	（注） このダッシュレットは、不正および aWIPS パッケージがインストールされている場合にのみ表示されます。 不正な脅威、aWIPS の脅威、一意の不正クライアントの総数、重大なアドバイザリ、および高レベルのアドバイザリの数を表示します。 • [アドバイザリの合計数（<*Number of*> total advisories）] をクリックして、**[ツール（Tools）]** > **[セキュリティアドバイザリ（Security Advisories）]**ページに移動します。ネットワーク セキュリティ アドバイザリの識別（1605 ページ） を参照してください。 • 不正な脅威、aWIPS の脅威、または一意の不正クライアントの総数の数字をクリックして、**[アシュアランス（Assurance）]** > **[不正およびaWIPS（Rogue and aWIPs）]** ダッシュボードに移動します。『*Cisco Catalyst Center Rogue Management and aWIPS Application Quick Start Guide*』の「Monitor the Rogue and aWIPS Dashboard」を参照してください。
Config コンプライアンス	ネットワーク設定がないデバイスと、設定が競合しているデバイスの数を表示します。 [非準拠デバイスの合計数（<*Number of*> total of non compliant devices）] をクリックして、**[プロビジョニング（Provision）]** > **[インベントリ（Inventory）]**ページに移動します。このページでは、すべての非準拠デバイスが自動的にフィルタ処理されます。ネットワークデバイスのコンプライアンス監査（665 ページ） を参照してください。

ダッシュレットの名前	説明
最近のアクティビティ	次の項目の数を表示します。 • 成功したアクティビティ、進行中のアクティビティ、および失敗したアクティビティ • 過去 7 日間のプロビジョニングタスク • 過去 7 日間のイメージのアップグレード • 過去 7 日間の設定のコンプライアンスの修復 [過去7日間のアクティビティの総数（<*Number of*> total activities in last 7 days）] をクリックするか、または成功した、進行中の、または失敗したアクティビティの数をクリックして、**[アクティビティ（Activities）] > [タスク（Tasks）]**ページに移動します。このページでは、過去 7 日間の関連するすべてのアクティビティが自動的にフィルタ処理されます。『*Cisco Catalyst Center Administrator Guide*』の「View, edit, stop, and delete tasks」と「View and discard work items」を参照してください。
ライセンス	次の項目の数を表示します。 • 登録が必要なデバイス • 非準拠のデバイス • 1 ヵ月後に期限が切れるライセンス [ライセンスのあるデバイスの総数（<*Number of*> total devices with licenses）] または登録が必要なデバイスの数をクリックして、**[ツール（Tools）] > [License Manager]**ページに移動します。『*Cisco Catalyst Center Administrator Guide*』の「Manage Licenses」を参照してください。

ダッシュレットの名前	説明
システム	このダッシュレットには、次の2つのタイプのデータが表示されます。 • System： • サービスの合計数と、ダウンしているサービスの合計数を表示します。これらの数字のいずれかをクリックして、**[システム（System）]**>**[システム360（System 360）]**ページに移動します。『*Cisco Catalyst Center Administrator Guide*』の「Use System 360」を参照してください。 • クラウド接続ステータスを表示します。これは、システムがシスコソフトウェアカタログに接続されているかどうかを示します。『*Cisco Catalyst Center Administrator Guide*』の「Manage Applications」を参照してください。 • 期限切れとなる証明書：信頼できる証明書、デバイス証明書、およびシステム証明書の数を表示します。『*Cisco Catalyst Center Administrator Guide*』の「Security recommendations」を参照してください。

デバイスの詳細機能

この折りたたみ可能なセクションには、ネットワークバグ、Field Notice、およびサポート終了（EoX）アラートに関するデバイスデータが表示されます。

この表では、[デバイスの詳細機能（Device advanced features）]セクションのダッシュレットについて説明します。

ダッシュレットの名前	説明
ネットワークバグ	重大または高いシビラティ（重大度）のネットワークバグの数を表示します。 [ネットワークバグの総数（<*Number of*> total network bugs）]をクリックして、**[ツール（Tools）]**>**[ネットワークバグ識別子（Network Bug Identifier）]**ページに移動します。ネットワークバグの特定 （1601 ページ） を参照してください。
フィールド 通知	ネットワーク内のデバイスに影響を与える、ハードウェアおよびソフトウェアに関する Field Notice の数を示します。 [Field Noticeの総数（<*Number of*> total field notices）]をクリックし、**[ツール（Tools）]**>**[Field Notices]**ページに移動します。ネットワークの Field Notice の特定 （1619 ページ） を参照してください。

ダッシュレットの名前	説明
EoX マイルストーン	EoX アラートの数と、インベントリ内のデバイスのハードウェア、ソフトウェア、およびモジュールコンポーネントに関する EoX アラートの数を表示します。 [EoXアラートの合計数（<*Number of*> total EoX alerts）] をクリックして、**[プロビジョニング（Provision）] > [インベントリ（Inventory）]**ページに移動します。「インベントリに関する情報の表示 （102 ページ）」を参照してください。

ネットワークとアクティビティのステータスアイコン

ホームページでは、セクション内のステータスアイコンを表示して、さまざまなネットワークメトリックのステータスをすばやく評価できます。次の表で各ステータスアイコンについて説明します。

アイコン	説明	例
	正常、成功、または接続済み	たとえば、[ルーティング（Routing）] ダッシュレットにこのステータスがパーセンテージで表示された場合は、インベントリ内のルータが正常であることを示します。[最近のアクティビティ（Recent Activities）] ダッシュレットにこのステータスが表示された場合は、特定の数のアクティビティが正常に完了したことを示します。
	接続されている状態	たとえば、[重大アラート（Critical Alerts）] ダッシュレットにこのステータスが表示された場合は、最近の重大アラートがないことを示します。
	進行中	たとえば、[最近のアクティビティ（Recent Activities）] ダッシュレットにこのステータスが表示された場合は、特定の数のタスクが進行中であることを示します。
	異常、機能不全、または非準拠	たとえば、[ワイヤレス（Wireless）] ダッシュレットにこのアイコンがパーセンテージで表示された場合は、ワイヤレスデバイスが正常でないことを示します。[ソフトウェアイメージ（Software Images）] ダッシュレットにこのアイコンが表示された場合は、特定の数のデバイスファミリに標準イメージが適用されていないことを示します。

アイコン	説明	例
⊖	ステータス参照不可	たとえば、[エンドポイント（Endpoints）]ダッシュレットにこのステータスが表示された場合は、インベントリ内のエンドポイントのステータスが使用できないことを示します。

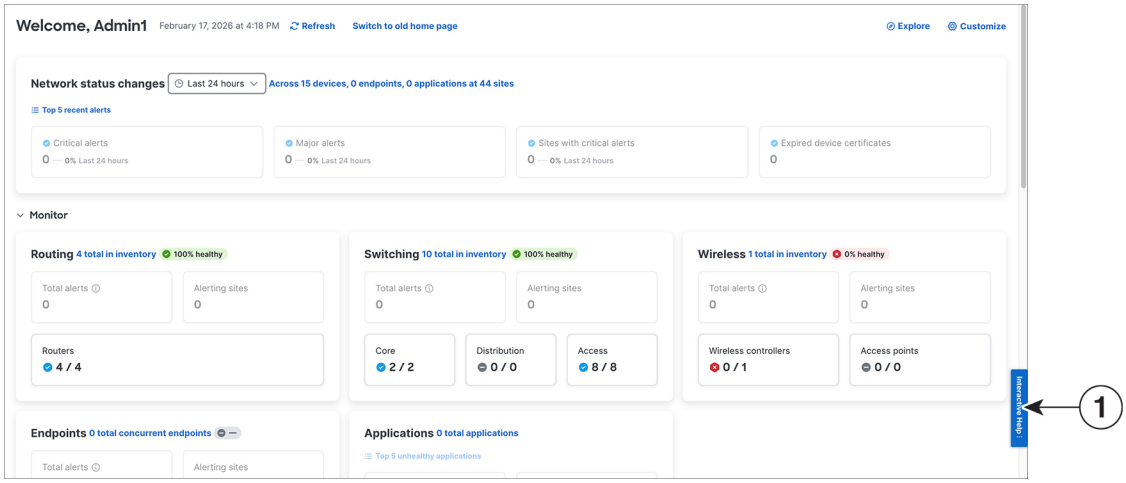
インタラクティブヘルプ

インタラクティブヘルスには、Catalyst Center の特定のタスクに関するウォークスルーが含まれています。このウォークスルーでは、タスクを完了するために役立つ画面上のガイダンスが示されます。

[インタラクティブヘルプ（Interactive Help）]は、次のいずれかの方法で開くことができます。

- ヘルプアイコンをクリックして[インタラクティブヘルプ（Interactive Help）]を選択する。
- デフォルトで Catalyst Center ウィンドウの右下隅に表示される [インタラクティブヘルプ（Interactive Help）] ウィジェットをクリックする。

図 *4:* インタラクティブ ヘルプ ウィジェット



この表は、[インタラクティブヘルプ（Interactive Help）] ウィジェットの図のコールアウトを示したものです。

1	**インタラクティブ ヘルプ** ウィジェット

[インタラクティブヘルプ（Interactive Help）]ウィジェット（引き出し線 1）は、デフォルトの場所から GUI ウィンドウの他の場所に移動することができます。ウィジェットを、緑色の点線の長方形で示されている移動可能な場所にドラッグアンドドロップします。

[インタラクティブヘルプ（Interactive Help）]ポップアップは、上部の境界をドラッグして GUI ウィンドウの新しい場所にドロップすることで移動できます。ただし、[インタラクティブヘ

ルプ（Interactive Help）] ポップアップが特定のメニューオプションに関連付けられている場合は、移動できません。

ホームページのカスタマイズ

Catalyst Center ホームページをカスタマイズするには、次の手順を実行します。

手順

ステップ 1 ホームページで、右上隅にある [カスタマイズ（Customize）] をクリックします。

ステップ 2 **[カスタマイズ（Customize）]** スライドインペインで、次の手順を実行します。

a) 次のいずれかのアクションを使用して、ホームページをカスタマイズします。

- セクション名の横にある [名前の変更（Rename）] をクリックして名前を変更します。
- セクションを削除するには、削除アイコン（）をクリックします。
- ダッシュレット名の横にあるトグルボタンをクリックして、ホームページ上でそのダッシュレットを表示または非表示にします。
- ホームページを再編成するには、セクションまたはダッシュレット名の横にあるドラッグアンドドロップアイコン（）をドラッグアンドドロップします。
- [+セクションの追加（+ Add Section）] ドロップダウンリストから、[新しいセクション（New Section）] を選択して、ホームページに新しいセクションを追加します。次に、[+ダッシュレットの追加（+ Add Dashlet）] ドロップダウンリストを使用して、この新しいセクションにダッシュレットを追加します。

b) 変更後、[適用（Apply）] をクリックして、ホームページのレイアウトを更新します。

Cisco.com とスマートアカウントのログイン情報の再認証

シスコは新しい認証インフラストラクチャを導入しました。そのため、Catalyst Center リリース 2.3.7.9 以降にアップグレードした場合、ホームページの上部に、以前に設定した cisco.com とスマートアカウントのログイン情報の有効期限が切れていることを示すメッセージが表示されます。[Cisco.comログイン情報（Cisco.com Credentials）] リンクと [スマートアカウント（Smart Account）] リンクをクリックして関連する [Catalyst Center] ウィンドウを開き、これらのログイン情報を再認証します。

関連情報

『*Cisco Catalyst Center Administrator Guide*』の「Configure Cisco credentials」と「Configure Smart Account」を参照してください。

Catalyst Center ジャーニーマップ

Catalyst Center ジャーニーマップには、Catalyst Center で提供されるさまざまな機能とその使用法が表示されます。

手順

ステップ 1 Catalyst Center ジャーニーマップを起動するには、次のいずれのタスクを実行します。

- メインメニューから次を選択します。[Explore] を選択します。
- Catalyst Center のホームページで、[Explore] をクリックします。

Catalyst Center ジャーニーマップでは、Catalyst Center で提供されるさまざまな機能が、[AIOps]、[NetOps]、[DevOps]、[SecOps] タブなどにグループ化されます。各タブの詳細を表示するには、ⓘ アイコンにカーソルを合わせます。

ステップ 2 ジャーニーマップを円グラフで表示するには、◷ アイコンをクリックします。

円グラフには、選択したタブの詳細が表示されます。ステップの横にある数字（例：①）は、ジャーニーマップのセグメント内における推奨ステップの順番を提案しています。円グラフでは、次のアクションを実行できます。

- 円グラフに表示されている機能にカーソルを合わせると、機能とそのステータスに関する簡単な説明が表示されます。
- 機能がインストールされているか使用中の場合は、ジャーニーマップで機能名をクリックすると、その構成または設定ページが表示されます。
- セグメントの詳細を表示するには、円グラフのセグメント名をクリックします。すべてのセグメントが含まれる前のビューに戻るには、セグメント名を再度クリックします。

ステップ 3 ジャーニーマップを表形式で表示するには、☰ アイコンをクリックします。

表には、選択したタブの詳細が表示されます。機能名にカーソルを合わせると、機能とそのステータスに関する簡単な説明が表示されます。

ステップ 4 [Completed]チェックボックスをオンすると、ジャーニーマップで完了したステップと未完了のステップに関する情報が表示されます。

- [Completed] をクリックすると、完了したステップが緑色の枠で強調表示されます。
- [Incomplete] をクリックすると、未完了のステップがオレンジ色の枠で強調表示されます。

リモートサポート許可ダッシュボードの表示

リモートサポートの許可を行うと、シスコの専門家にCatalyst Centerへのリモートアクセスが許可され、ネットワークのトラブルシューティングが行えます。

（注） Catalyst Center のリモートサポート承認は、RADKit バージョン 1.2.1 以降でのみサポートされます。

手順

ステップ 1 右上隅にあるヘルプアイコン（?）をクリックし、**[Remote Support Authorization]** を選択します。

[Remote Support Authorization] ダッシュボードの **[SUMMARY]** エリアには、リモートサポート承認の合計と、現在および過去のリモートサポート承認が表示されます。Remote Support Cloud サービスの接続ステータスは、次のように右上隅に表示されます。

- 緑色のチェックマークは、リモートサポート許可が Remote Support Cloud サービスに接続されていることを示します。
- 感嘆符は、リモートサポート許可が Remote Support Cloud サービスに接続されていないことを示します。

ステップ 2 **[Create New Authorization]** タブで **[Create a Remote Support Authorization]** をクリックし、新しい承認を作成します。詳細については、リモートサポート許可の作成 （1673 ページ）を参照してください。

ステップ 3 [現在の承認（Current Authorizations）] タブをクリックして、現在のリモートサポート承認タイルを表示します。これには、次のステータスがあります。

- [All]：スケジュール済みリモートサポート許可とアクティブなリモートサポート許可をすべて表示します。
- [Scheduled]：スケジュール済みリモートサポート許可を表示します。
- [Active]：アクティブなリモートサポート許可を表示します。

トラブルシューティングを目的として、サポート承認タイルにはシスコの専門家が Catalyst Center にアクセスするスケジュールと期間が表示されます。

ステップ 4 承認を取り消すには、それぞれのサポート承認タイルの **[Revoke Authorization]** をクリックします。

ステップ 5 [Past Authorizations] タブをクリックして、過去の許可を表示します。

[過去の承認（Past Authorizations）] テーブルには、[ケース番号（Case Number）]、[日付（Date）]、[セッションステータス（Session Status）]、[シスコ専門家（Cisco Specialist）] および [ログ（Log）] に基づいてサポート承認が示され、過去の承認について次のステータスが一覧表示されます。

- **All**：期限切れおよび失効したすべてのリモートサポート承認が一覧表示されます。
- [Expired]：期限切れのすべてのリモートサポート許可を一覧表示します。
- **Revoked**：失効したすべてのリモートサポート承認が一覧表示されます。

検索バーを使用して、ケース番号で過去の承認を検索できます。

ステップ 6 リモートサポート承認ログを表示するには、目的の承認の **[View Logs]** をクリックします。

[Audit Log] ウィンドウが表示されます。詳細については、*Cisco Catalyst Center Administrator Guide* の「View Audit Logs」を参照してください。

グローバル検索の使用

グローバル検索機能を使用して、Catalyst Center の任意の場所で次のカテゴリの項目を検索します。

- **アクティビティ**：Catalyst Center のメニュー項目、ワークフロー、および機能を名前で検索します。
- **アプリケーション**：名前で検索します。
- **アプリケーション グループ**：名前で検索します。
- **認証テンプレート**：名前またはタイプで検索します。
- **デバイス**：収集ステータス、到達可能性ステータス、ロケーション、またはタグで検索します。
- **ファブリック**：ファブリック名で検索します。
- 機能テンプレート：機能テンプレート名またはパラメータ名で検索します。
- **ヘルプ**：検索文字列を含むトピックを検索します。
- **ホストおよびエンドポイント**：名前、IP アドレスまたは MAC アドレスで検索します。
- **IP プール**：名前または IP アドレスでそれらを検索します。
- **ネットワーク デバイス**：名前、IP アドレス、シリアル番号、ソフトウェア バージョン、プラットフォーム、製品ファミリ、または MAC アドレスで検索します。
- **ネットワークプロファイル** ：プロファイル名で検索します。
- **ネットワーク設定**
  - **デバイスログイン情報**：名前で検索します。
  - **IP アドレスプール**：グループ名またはプールの CIDR で検索します。

- **サービス プロバイダ プロファイル**：プロファイル名、WANプロバイダ、またはモデルで検索します。
- ワイヤレスネットワーク設定：ワイヤレスネットワーク設定名またはパラメータ名で検索します。

- **ポリシー**：名前または説明で検索します。
- **サイト**：名前で検索します。
- **トラフィックのコピー** ：名前と説明で検索します。
- **移行**：移行名で検索します。
- **ユーザー**：システム設定およびユーザーをユーザー名で検索します。大文字と小文字は区別されません。ユーザー名のサブストリング検索はサポートされていません。
- ワークフロー：タスク名またはパラメータ名で検索します。
- 新しいバージョンの Catalyst Center として別のアイテムがリリースされます。

グローバル検索を開始するには、任意の Catalyst Center ウィンドウの右上隅にある [検索（Search）] アイコン（）をクリックします。Catalyst Center にグローバル検索ウィンドウが表示され、[検索（Search）] フィールドに検索項目に関する識別情報を入力できます。

項目の名前、アドレス、シリアル番号、またはその他の識別情報の全体または一部を入力できます。[検索（Search）] フィールドで大文字と小文字は区別されません。任意の文字または文字の組み合わせを入力できます。

検索文字列の入力を開始すると、入力に一致する可能性がある検索ターゲットのリストが Catalyst Center に表示されます。複数のカテゴリの項目が検索文字列と一致する場合は、Catalyst Center によってカテゴリ別にソートされます。各カテゴリには最大 5 つの項目が含まれます。最初のカテゴリの最初の項目が自動的に選択され、その項目の概要情報が右側の [概要（summary）] パネルに表示されます。

必要に応じてリストをスクロールできます。提案された検索ターゲットのいずれかをクリックすると、概要パネルにその項目の情報が表示されます。カテゴリに項目が 5 つ以上ある場合は、カテゴリ名の横にある [View All] をクリックします。検索ターゲットの完全なリストからカテゴリ化されたリストに戻るには、[Go Back] をクリックします。

検索文字列にさらに多くの文字を追加すると、グローバル検索で表示されるリストが自動的に絞り込まれます。

Catalyst Center では、IPv6 アドレス全体または IPv6 アドレスの省略形を使用してデバイスを検索できます。

例えば、「*2001:0db8:85a3:0000:0000:8a2e:0370:7334*」を検索する場合、次の検索エントリを使用できます。

- 2001:0db8:85a3:0000:0000:8a2e:0370:7334（完全な IPv6 アドレスを使用）
- 2001:db8:85a3:0:0:8a2e:0:7334（先行ゼロは切り捨て）

- 2001:db8:85a3::8a2e:0:7334（連続するゼロは二重コロンで圧縮）
- 2001:db8:85a3（IPv6 アドレスの一部を使用）

Catalyst Center を使用すると、IPv6 アドレスとプレフィックス、ポストフィックス、または任意の組み合わせで二重コロンを使用して IPv6 アドレスを検索できます。

たとえば、「*2001:db8:85a3::8a2e:0:7334*」を検索する場合、次の検索エントリを使用できます。

- ::（二重コロンのみを使用）
- 85a3::8a2e（二重コロン付きのプレフィックスとポストフィックスを使用）
- 85a3::（二重コロン付きのプレフィックスを使用）
- ::8a2e（二重コロン付きのポストフィックスを使用）

任意の形式（ハイフンまたはコロン付き）で MAC アドレスを入力することにより、Catalyst Center のデバイスを検索できます。

範囲ベースのアクセス権限を持つユーザーがデバイス名、クライアント ID、または IP アドレスでネットワークデバイスを検索すると、デバイスの詳細が表示されません。しかし、MAC アドレスで検索すると、デバイスまたはクライアント 360 相互起動リンクに限定されたデバイスデータが表示されます。

グローバル検索では、カテゴリごとに一度に 5 つの結果を表示できます。

検索は、10 分ごとに同期されたデータに対して行われます。したがって、変更が発生すると、最大 10 分後に検索結果に変更が反映されます。

クロック形式を 12 時間または 24 時間に設定

GUI を使用して、12 時間または 24 時間表示形式を設定できます。

手順

ステップ 1 右上隅で、表示されたユーザー名をクリックし、**[My Profile and Settings]** > **[Display Settings]**の順に選択します。

ステップ 2 [Set Clock Format] エリアで [12 hours] または [24 hours] をクリックします。

ステップ 3 [Save] をクリックします。

Catalyst Center における明暗の外観の適用

Catalyst Center は、明るい外観（デフォルト）または暗い外観で表示できます。

手順

ステップ 1 右上隅で、表示されたユーザー名をクリックし、**[My Profile and Settings]** > **[Display Settings]**の順に選択します。

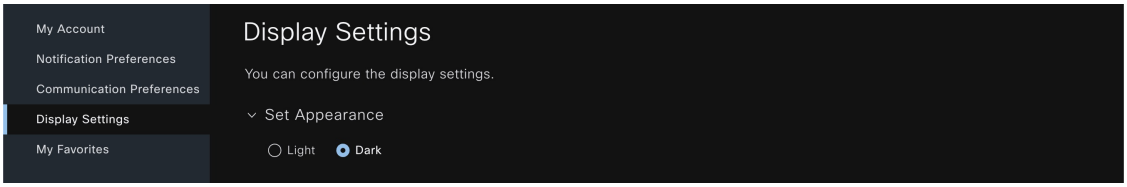
ステップ 2 [Set Appearance] 領域で、[Light] または [Dark] をクリックして、Catalyst Center を明るい外観または暗い外観で表示します。

ステップ 3 [Save] をクリックします。

Catalyst Centerでは、選択した外観をブラウザストレージにキャッシュされるため、外観を保存するブラウザキャッシュが使用できない次のシナリオでは、Catalyst Center GUI が数秒間明るい外観で表示されます。

- 別のブラウザから Catalyst Center にログインします。
- 3 ノードクラスタでは、プライマリノードで暗い外観が適用された後の初回は 2 番目または 3 番目の Catalyst Center ノードにログインします。

暗い外観が有効になっている場合、Catalyst Center GUI は次の例のように表示されます。



ローカリゼーションの有効化

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

デフォルトの言語は変更するには、次の手順を実行します。

手順

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

- Google Chrome の場合：

1. 右上隅にある アイコンをクリックし、[**Settings**] を選択します。
2. **[Languages]** をクリックします。
3. [Add Languages] をクリックします。
4. [**Add languages**] ダイアログボックスで、[**Chinese**]、[**Japanese**]、[**Korean**] のいずれかを選択して、[**Add**] をクリックします。

• Mozilla Firefox の場合：

1. 右上隅にある アイコンをクリックし、[**Settings**] を選択します。
2. **[Language and Appearance]** > **[Language]** エリアで、**[Choose]** をクリックします。
3. [**Select a language to add**] ドロップダウンリストで、[**Chinese**]、[**Japanese**]、[**Korean**] のいずれかを選択します。
4. [OK] をクリックします。

ステップ 2 Catalyst Center にログインします。

選択した言語で GUI が表示されます。

ウィンドウをお気に入りに追加

Catalyst Center の任意のウィンドウをお気に入り（お気に入りウィンドウのリスト）に追加できます。お気に入り機能を使用すると、お気に入りのウィンドウに簡単かつ迅速に移動できます。

ビューに一意の URL がある場合は、同じウィンドウのさまざまなビューをお気に入りに追加することもできます。たとえば [タスク（Tasks）] ウィンドウでは、ステータスが [成功（Success）] のタスクまたは作業項目をフィルタ処理している場合や、最終更新のステータスが [24時間（24 hours）] のタスクまたは作業項目をフィルタ処理している場合に、それぞれのウィンドウをお気に入りに追加できます。

手順

ステップ 1 お気に入りに追加するウィンドウに移動します。

ステップ 2 ウィンドウの右上隅にあるスターアイコン（☆）をクリックして、ウィンドウをお気に入りに追加します。

ステップ 3 **[このウィンドウはお気に入りに登録されました（This window is favorited）]** ダイアログボックスの [名前（Name）] フィールドで、次のいずれかを実行できます。

a) 自動入力された名前をお気に入りのウィンドウのタイトルとして保持します。
b) 自動入力された名前を削除し、新しい名前を入力します。

ステップ 4 （任意） お気に入りに追加したウィンドウのリストを表示するには、**[お気に入りの表示（View My Favorites）]** をクリックします。

[My Favorites] スライドインペインには、お気に入りに追加したウィンドウがすべて表示されます。

ヒント Catalyst Center で任意のウィンドウから [My Favorites] スライドインペインをすばやく表示するには、キーボードショートカットの q + f を使用します。

ステップ 5 [Done] をクリックして、お気に入りのウィンドウ名の編集内容を保存し、ダイアログボックスを閉じます。

ステップ 6 （任意）お気に入りからウィンドウを削除するには、**[このウィンドウはお気に入りに登録されました（This window is favorited）]** ダイアログボックスまたは **[お気に入り設定（Favorites Preferences）]** ウィンドウからお気に入りを削除します。

a) 削除するお気に入りウィンドウに移動し、スターアイコン（★）をクリックします。**[このウィンドウはお気に入りに登録されました（This window is favorited）]** ダイアログボックスで、[削除（Remove）] をクリックします。
b) お気に入りからウィンドウを削除する方法については、「お気に入りの管理 （57 ページ）」を参照してください。

お気に入りの管理

[お気に入り設定（Favorites Preferences）] ウィンドウでお気に入りのウィンドウを管理できます。ウィンドウをお気に入りに追加する方法については、ウィンドウをお気に入りに追加 （56 ページ）を参照してください。

手順

ステップ 1 右上隅で表示されたユーザー名をクリックし、**[マイプロファイルと設定（My Profile and Settings）]** > **[お気に入り設定（Favorites Preferences）]** を選択します。

[お気に入り設定（Favorites Preferences）] ウィンドウには、お気に入りに追加したウィンドウのリストが表示されます。

ステップ 2 （任意） お気に入りウィンドウを削除するには、次の手順を実行します。

a) リストから削除するお気に入りのウィンドウを見つけます。
b) お気に入りのウィンドウの横にあるスターアイコン（★）をクリックすると、リストから削除されます。

ステップ 3 （任意） お気に入りウィンドウに移動するには、次の手順を実行します。

a) 移動したいお気に入りのウィンドウを見つけます。

b) お気に入りウィンドウのハイパーリンクパスをクリックします。

Catalyst Center Insights への登録

製品の発表、ネットワークのハイライト、ネットワークパフォーマンスに関する情報などを含む *Catalyst CenterInsights* を購読できます。Catalyst Center Insights パブリケーションは、指定した電子メールアドレスに PDF 形式で送信されます。

（注） Catalyst Center アプライアンスが安全なエアギャップネットワークに展開されている場合、特定のメトリックは Catalyst Center Insights から除外されます。完全な Catalyst Center Insights を表示するには、エアギャップ環境では利用できないインターネットとテレメトリ接続が必要です。

始める前に

- **[System]** > **[Settings]** > **[Integration Settings]**で、コールバック URL のホスト名または IP アドレスを入力します。詳細については、*Cisco Catalyst Center Administrator Guide*の「Configure Integration Settings」を参照してください。
- **[System]** > **[Settings]** > **[External Services]** > **[Destinations]** > **[Email]**で、パブリケーションの受信に使用する SMTP サーバーを構成します。

手順

ステップ 1 右上隅で、表示されたユーザー名をクリックし、**[My Profile and Settings]** > **[Communication Preferences]**の順に選択します。

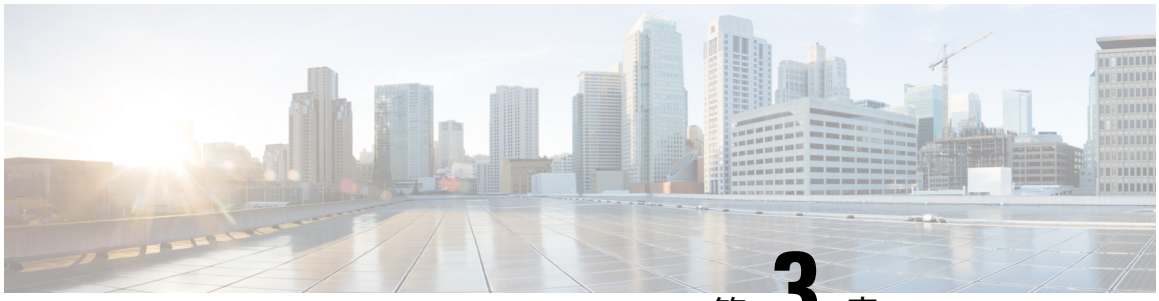
ステップ 2 [Subscription Off] トグルボタンをクリックして [Subscription On] に切り替えます。

ステップ 3 Catalyst Center Insights を受信するメールアドレスを入力し、[Save] をクリックします。

Insights は最大 1 年間アーカイブされます。目的の日付範囲の**[Actions]** > **[Download PDF]**を選択すると、過去のパブリケーションを読むことができます。

ステップ 4 （オプション）メールアドレスを変更するには、鉛筆アイコンをクリックします。

ステップ 5 （オプション）Catalyst Center Insights の登録を解除するには、[Subscription On] トグルボタンをクリックして [Subscription Off] に切り替えます。



第 3 章

テレメトリの設定

- テレメトリの設定について （59 ページ）
- テレメトリを使用した syslog、SNMP トラップ、NetFlow コレクタサーバー、および有線クライアントデータ収集の設定 （59 ページ）
- デバイスでのアプリケーションテレメトリ有効化の基準 （61 ページ）
- アプリケーションテレメトリ設定のプロビジョニング （64 ページ）
- ワイヤレスコントローラ のアプリケーションテレメトリの有効化 （65 ページ）
- 新しいクラスタ仮想IPアドレスを使用するためのアプリケーションテレメトリの更新（67 ページ）
- テレメトリを使用したデバイス設定の更新 （69 ページ）

テレメトリの設定について

Catalyst Center では、syslog、SNMP トラップ、有線クライアントデータ収集など、デバイスのグローバル テレメトリ パラメータの設定と更新を行えます。アプリケーションテレメトリは有効または無効にできます。アプリケーションテレメトリを有効にすると、デバイスの正常性を監視して評価するようにデバイスの NetFlow コレクタを設定できます。

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

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

始める前に

サイトを作成し、サイトにデバイスを割り当てます。『サイトの作成、編集、削除（285 ページ）』を参照してください。

手順

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

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

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

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

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

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

次のいずれか 1 つのタスクを実行します。

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

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

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

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

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

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

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

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

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

ステップ 7 [Save] をクリックします。

デバイスでのアプリケーションテレメトリ有効化の基準

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

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

サポートされているすべてのプラットフォームに対して、従来のタグ付けベースのアルゴリズム（キーワード **lan** を使用）と新しい自動選択アルゴリズムの両方を使用した、インターフェイスと WLAN の選択基準を次の表に示します。

プラットフォーム	従来のタギングベースのアルゴリズム	自動選択アルゴリズム
ルータ	• インターフェイスの説明に **lan** キーワードが含まれている。[1]、[2] • インターフェイスに管理 IP アドレス以外の IP アドレスがある。	• インターフェイスに管理 IP アドレス以外の IP アドレスがある。 • インターフェイスが次のいずれのタイプでもない。 • WAN （注） インターフェイスにパブリック IP アドレスがあり、パブリック IP アドレスがインターフェイスを経由するルートルールがある場合、そのインターフェイスは WAN 側インターフェイスとして扱われます。 このコンテキストでは、パブリック IP アドレスはプライベート範囲にない（たとえば、192.168.x.x、172.16.y.y、10.z.z.z にない）か、システムの IP プールにない IP アドレスです。 ルートルールは動的に学習できます。このコンテキストでは、**show ip route** コマンドでこのインターフェイスを通過するパブリック IP アドレスへのルートは表示されません。 • ループバック • 管理インターフェイス：GIGABITETHERNET0、GIGABITETHERNET0/0、MGMT0、FASTETHERNET0、FASTETHERNET1

プラットフォーム	従来のタギングベースのアルゴリズム	自動選択アルゴリズム

スイッチ	• インターフェイスの説明に **lan** キーワードが含まれている。[1、2]
	• スイッチポートがアクセスポートとして設定されている。
	• スイッチポートに **switch-mode access** コマンドが設定されている。
		• インターフェイスが物理インターフェイスである。
		• アクセスポートにネイバーがない。
		• インターフェイスが次のいずれのタイプでもない。
		  • 管理インターフェイス：FASTETHERNET0、FASTETHERNET1、GIGABITETHERNET0/0、MGMT0
		  • LOOPBACK0、Bluetooth、App Gigabit、WPAN、Cellular、Async
		  • VSL インターフェイス

Cisco AireOS コントローラ	WLAN プロファイル名が **lan** キーワードでタグ付けされている。[1、2]	SSID が混在している場合、つまりローカルモード、フレックスモード、およびファブリックモードの場合、Wireless Service Assurance（WSA）の処理が有効になります。すべての SSID がローカルモードの場合、NetFlow が有効になります。
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラと最適化アプリケーション パフォーマンス モニタリング（APM）プロファイルおよび IOS 16.12.1 以降	WLAN プロファイル名が **lan** キーワードでタグ付けされている。[1、2]	SSIDが混在している場合、つまり中央スイッチング、フレックスモード、およびファブリックモードの場合は、Cisco Application Visibility and Control（AVC）の基本レコードが設定されます。すべてのSSIDで中央スイッチングを使用している場合、最適化APMレコードが設定されます。 IOS 17.10 以降を備える Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの場合、Catalyst Center は、フレックスおよびファブリック SSID に対して、AVC 基本プロファイルではなく、APMプロファイルをプッシュします。
	（注） NetFlow 設定は、WLAN プロファイルに直接プッシュされるのではなく、「lan」キーワードを使用してポリシープロファイルにプッシュされます。ブラウンフィールド展開では、回避策は、「lan」キーワードを使用して新しいポリシープロファイルを作成し、既存のポリシープロファイルを削除して、新しいポリシープロファイルを既存の WLAN プロファイルと関連付けることです。ポリシープロファイルの名前を直接変更することはできません。	

プラットフォーム	従来のタギングベースのアルゴリズム	自動選択アルゴリズム
Catalyst Center トラフィックテレメトリアプライアンスと最適化 APM プロファイルおよび IOS 17.3 以降	• インターフェイスの説明に **lan** キーワードが含まれている。[1、2] • インターフェイスが物理インターフェイスである。	• インターフェイスが物理インターフェイスである。 • インターフェイスが管理インターフェイス（GIGABITETHERNET0、GIGABITETHERNET0/0、MGMT0、FASTETHERNET0、および FASTETHERNET1）ではない。

[1] **lan** キーワードは、大文字と小文字の区別はなく、スペース、ハイフン、または下線で区切ることができます。
[2] ネットワークデバイスを再同期して、**lan** キーワードを読み取ります。

たとえば、従来のタグベースのアルゴリズムを使用してアプリケーションテレメトリを有効にする場合は、次の条件を満たす必要があります。

- この Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の WLAN プロファイル名 *test-lan* に **lan** キーワードが含まれている。

```
WLAN Profile Name              SSID                    VLAN Status
-------------------------------------------------------------------------------
1    test-lan                  test1-ssid              137   UP
```

- このスイッチのインターフェイスの説明の *wired-lan* に **lan** キーワードが含まれている。

```
interface GigabitEthernet1/0/1
description wired-lan
```

アプリケーションテレメトリ設定のプロビジョニング

デバイスで NetFlow アプリケーションテレメトリ設定を行えます。

手順

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

[Inventory] ウィンドウには、検出プロセス中に収集されたデバイス情報が表示されます。特定のサイトで使用可能なデバイスを表示するには、左側のペインで [Global] サイトを展開し、サイト、ビルディング、またはフロアを選択します。

ステップ 2 プロビジョニングするデバイスを選択します。

ステップ 3 [Actions] ドロップダウンリストから、[Telemetry] を選択し、次の手順のいずれかを実行します。

（注） [Enable Application Telemetry] および [Disable Application Telemetry] オプションは、デバイスで Catalyst Center からのアプリケーションテレメトリがサポートされている場合のみ有効です。

a) [アプリケーションテレメトリの有効化（Enable Application Telemetry）]：選択したデバイスで NetFlow アプリケーションテレメトリを設定します。
b) [アプリケーションテレメトリの無効化（Disable Application Telemetry）]：選択したデバイスから NetFlow アプリケーションテレメトリ設定を削除します。

ステップ 4 [Apply] をクリックします。

[Application Telemetry] 列には、テレメトリの設定ステータスが表示されます。デフォルトの列設定で

[Application Telemetry] 列が表示されない場合は、列見出しの右端にある省略記号アイコン（⋮）をクリックし、[Application Telemetry] チェックボックスをオンにします。

ワイヤレスコントローラのアプリケーションテレメトリの有効化

新規および既存のデバイスのアプリケーションテレメトリを有効にすることができます。

（注） **[Application Visibility]** ウィンドウからアプリケーションテレメトリを有効にすることもできます。詳細については、アプリケーションテレメトリの有効化（1336ページ）を参照してください。

始める前に

アプリケーションテレメトリを有効にするには、デバイスに Advantage ライセンスが必要です。

（注） Catalyst Center でアプリケーションテレメトリを有効にする前に、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ インターフェースの**[設定（Configuration）]**>**[サービス（Services）]**>**[アプリケーション可視性（Application Visibility）]** > **[フローモニター（Flow Monitors）]**セクションから既存のフローモニターを手動で削除してください。

手順

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

ステップ 2 特定のサイトで使用可能なデバイスを表示するには、左側のペインで [Global] サイトを展開し、サイト、ビルディング、またはフロアを選択します。

ステップ 3 [インベントリ（Inventory）] ウィンドウで、デバイスを選択します。同時に複数のデバイスを選択できます。

ステップ 4 **[Actions]** ドロップダウンリストから、**[Telemetry]** > **[Enable Application Telemetry]** の順に選択します。

ステップ 5 [テレメトリの有効化（Enable Telemetry）] スライドインペインで、次の設定を完了します。

a) [AP mode] : [Flex/Fabric] または [Local] チェックボックスをオンにします。両方のオプションを選択することもできます。

b) ゲスト SSID のテレメトリを有効にするには、**[Include Guest SSID]** チェックボックスをオンにします。

（注） SSID 名に **guest** というキーワードが含まれている場合、テレメトリを有効にするには、SSID が企業のワイヤレスネットワークに属している場合であっても、[ゲストSSIDを含める（Include Guest SSID）] チェックボックスをオンにする必要があります。

c) [Telemetry Source] :

- 組み込みワイヤレスコントローラ - NetFlow
- AireOSワイヤレスコントローラ（ローカルモード）- NetFlow
- AireOSワイヤレスコントローラ（Flex/Fabricモード）- ワイヤレス サービス アシュアランス（WSA）

d) すべてのワイヤレスコントローラに同じ設定を適用するには、[Apply this selection to all wireless controllers] をオンにします。

e) [Next] をクリックします。

f) [設定プレビューの生成（Generate Configure Preview）] オプションボタンをクリックし、[プレビュー（Preview）] をクリックします。

[Enable Application Telemetry Task] ウィンドウで、Catalyst Center は、最初にリストされたデバイスの実行中の設定と計画された設定の並列比較を表示します。

[アプリケーションテレメトリの有効化タスク（Enable Application Telemetry Task）] ウィンドウで、次の手順を実行します。

- デバイス設定を確認し、準備ができたら **[Deploy]** をクリックします。
- [今すぐ（Now）] または [後で（Later）] のスケジューリングオプションを選択し、[展開（Deploy）] をクリックします。

（注） **[Application Telemetry]** 列には、アプリケーションテレメトリの展開ステータスが表示されます。

デバイスのアプリケーションテレメトリの展開が失敗した場合は、**[Application Telemetry Deployment Status]** 列のリンクをクリックして失敗の理由を確認します。

新しいクラスタ仮想IPアドレスを使用するためのアプリケーションテレメトリの更新

Catalyst Center アプリケーションテレメトリを使用してデバイスデータを監視し、Catalyst Center エンタープライズ仮想 IP アドレス（VIP）を変更する必要がある場合は、次の手順を実行して VIP を変更し、ノードテレメトリデータが新しい VIP に送信されることを確認します。

始める前に

- 使用している Catalyst Center のバージョンを確認します。バージョンを確認するには、Catalyst Center GUI にログインし、[バージョン情報（About）] オプションを選択して Catalyst Center のバージョン番号を表示します。
- SSH クライアントソフトウェアを入手します。
- Catalyst Center プライマリノード上のエンタープライズ ネットワーク側の 10 GB インターフェイスに設定された VIP アドレスを特定します。ポート 2222 上のこのアドレスを使用してアプライアンスにログインします。このポートを特定するには、『*Cisco Catalyst Center Installation Guide*』の「Front and Rear Panels」セクションにある背面パネルの図を参照してください。
- プライマリノードに設定されている Linux ユーザー名（**maglev**）とパスワードを取得します。
- 割り当てるクラスタ VIP を特定します。クラスタ VIP は、『*Cisco Catalyst Center Installation Guide*』の「Required IP Addresses and Subnets」セクションで説明されている要件に準拠している必要があります。

手順

ステップ 1 アプライアンス構成ウィザードを使用してクラスタ VIP を変更するには、次の手順を行います。

a) SSH クライアントを使用して、Catalyst Center プライマリノード上のエンタープライズ ネットワーク側の 10 GB インターフェイスに設定された VIP アドレスにログインします。ポート 2222 にログインしていることを確認します。
b) プロンプトが表示されたら、Linux のユーザー名とパスワードを入力します。
c) 次のコマンドを入力すると、プライマリノード上で構成ウィザードにアクセスできます。

```
$ sudo maglev-config update
```

Linux パスワードを入力するようプロンプトが表示されたら、再度入力します。

d) クラスタ仮想 IP の入力を求める画面が表示されるまで [Next] を繰り返しクリックします。新しいクラスタ VIP を入力し、以降のすべての画面で [Next] をクリックしてウィザードを終了します。

設定したインターフェイスごとに 1 つの仮想 IP を設定する必要があります。**sudo maglev-config update** コマンドを入力して、設定したインターフェイスごとに 1 つの VIP を入力するよう指示されるようにウィザードを設定することを推奨します。

最後の画面に到達すると、変更を適用する準備ができたことを示すメッセージが表示されます。

e) [proceed] をクリックして、クラスタ VIP の変更を適用します。

設定プロセスの最後に成功メッセージが表示され、SSH プロンプトに復帰します。

ステップ 2 SSH プロンプトで次の一連のコマンドを入力して、必要な Catalyst Center サービスを再起動します。

```
magctl service restart -d collector-netflow
magctl service restart -d collector-syslog
magctl service restart -d collector-trap
magctl service restart -d wirelesscollector
```

ステップ 3 すべてのサービスが再起動するまでお待ちください。次のコマンドを入力して、再起動の進行状況をモニターリングできます。必要に応じて、使用している Catalyst Center のバージョンが属するリリーストレインに適したサービス名に置き換えてください。

```
magctl appstack status | grep -i -e collector-netflow -e collector-syslog -e collector-trap -e
wirelesscollector
```

必要なすべてのサービスが実行されている場合は、この出力のようなコマンド出力が表示され、正常に再起動した各サービスの実行ステータスが表示されます。

```
assurance-backend  wirelesscollector-123-bc99s  1/1   Running   0   25d   <IP>   <IP>
ndp   collector-netflow-456-lxvlx   1/1   Running   0   1d   <IP>   <IP>
ndp   collector-syslog-789-r0rr1    1/1   Running   0   25d   <IP>   <IP>
ndp   collector-trap-101112-3ppllm  1/1   Running   0   25d   <IP>   <IP>
```

ステップ 4 Catalyst Center GUI にアクセスし、次の手順に従ってすべてのノードでアプリケーションテレメトリを有効にします。

a) メインメニューから次を選択します。**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。
b) 監視するすべてのサイトとデバイスを選択します。
c) [Actions] ドロップダウンリストから、[Telemetry] > [Enable Application Telemetry] の順に選択します。
d) サイトとデバイスでテレメトリが有効になったことが示されるまで待ちます。

テレメトリを使用したデバイス設定の更新

この手順を使用して、syslog、SNMP トラップ、NetFlow コレクタ、および有線クライアントのデータ収集の変更を含む設定の変更をデバイスにプッシュします。これは、デバイスの制御性が有効か無効かに関係なく適用されます。

手順

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

[Inventory] ウィンドウには、検出プロセス中に収集されたデバイス情報が表示されます。特定のサイトで使用可能なデバイスを表示するには、左側のペインで [グローバル（Global）] サイトを展開し、サイト、建物、またはフロアを選択します。

ステップ 2 設定の変更を反映するデバイスを選択します。

ステップ 3 [Actions] ドロップダウンリストから、**[Telemetry]** > **[Update Telemetry Settings]** の順に選択します。

[Update Telemetry Settings] スライドインペインが開きます。

ステップ 4 （オプション）設定の変更をデバイスにプッシュするには、[設定のプッシュを強制（Force Configuration Push）] チェックボックスをオンにします。

構成に変更がない場合は、既存の構成がデバイスに再度プッシュされます。設定の再プッシュは、すべての設定で一貫して発生するわけではありません。このオプションにより、デバイスの可制御性ワークフローがトリガーされます。この動作は、デバイスの可制御性の各設定によって異なります。

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

ステップ 5 [Next] をクリックします。

ステップ 6 展開のためのタスクのスケジュールを設定します。

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

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

（注） 設定のプレビュー中、PKCS12 証明書は、15 分以内に使用する必要があるため生成されません。[設定のプレビュー（Preview Configuration）] ウィンドウには、関連する設定コマンドのみが表示されます。設定をプレビューした後に展開すると、PKCS12 証明書が生成され、デバイスにプッシュされます。

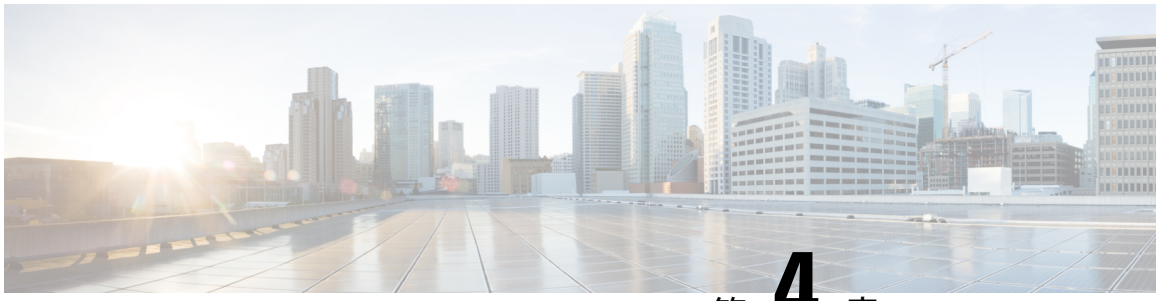
ステップ 7 [Tasks] ウィンドウで、タスクの展開を監視します。



第 II 部

ネットワークインベントリとトポロジの検出および管理

- ネットワークの検出 （73 ページ）
- インベントリの管理 （99 ページ）
- ネットワーク トポロジを表示 （259 ページ）



第 4 章

ネットワークの検出

- 検出の概要 （73 ページ）
- 検出ダッシュボード （74 ページ）
- ディスカバリの前提条件 （75 ページ）
- ディスカバリクレデンシャル （76 ページ）
- 優先管理 IP アドレス （84 ページ）
- 検出設定のガイドラインと制限事項 （84 ページ）
- ディスカバリの実行 （86 ページ）
- ディスカバリジョブの管理 （96 ページ）

検出の概要

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

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

デバイスは次の 4 つの方法で検出できます。

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

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

- [CDP Level] と [LLDP Level]：CDP または LLDP をディスカバリ方式として使用する場合は、CDP レベルまたはLLDP レベルを設定して、スキャンするシードデバイスからのホップ数を指定できます。デフォルトのレベル 16 では、大規模なネットワークの場合に時間がかかる可能性があります。検出する必要があるデバイスが少ない場合は、このレベルをより低い値に設定します。

- [**Prefix Length**]：検出方法として [**CIDR**] を使用する場合は、20 ～ 30 の範囲でプレフィックス長の値を設定できます。デフォルト値は 30 です。
- [Subnet Filters]： IP アドレスの範囲を使用する場合は、特定の IP サブネット内のデバイスをディスカバリで無視するように指定できます。
- [Preferred Management IP]：CDP、LLDP、CIDR、または IP アドレスの範囲のいずれを使用する場合でも、Catalyst Center がデバイスの任意の IP アドレスを追加するか、デバイスのループバックアドレスのみを追加するかを指定できます。

（注） Cisco SD-Access ファブリックおよび Cisco Catalyst Assurance については、デバイスのループバックアドレスを指定します。

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

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

検出ダッシュボード

メインメニューから次を選択します。 **[ツール（Tools）]** > **[検出（Discovery）]** の順に選択して、[検出ダッシュボード（Discovery Dashboard）] を表示します。検出ダッシュボードには、インベントリの概要、最新のディスカバリ、ディスカバリタイプ、ディスカバリステータス、最近のディスカバリが表示されます。

[検索（Search）] フィールドからデバイスを検索できます。[ステータス（Status）] と [タイプ（Type）] のドロップダウンリストを使用して、デバイスの詳細をフィルタリングして表示することもできます。[すべてをリセット（Reset all）] をクリックしてフィルタをクリアします。

[エクスポート（Export）] をクリックして、検出の詳細を CSV ファイルとしてエクスポートします。

[スケジュールされた検出を表示（View scheduled discoveries）] をクリックして、すべてのスケジュールされたネットワーク操作をモニターおよび管理します。

[検出を追加（Add discovery）] をクリックして、さまざまなパラメータを使用してデバイスを検出します。詳細については、ディスカバリクレデンシャル （76 ページ）を参照してください。

ディスカバリの前提条件

ディスカバリを実行する前に、次の最小要件を満たしてください。

- *Cisco Catalyst Center Compatibility Matrix* を表示して、Catalyst Center によって検出されるデバイスを把握してください。
- Catalyst Center とデバイス間の望ましいネットワーク遅延は 100 ミリ秒のラウンドトリップ時間（RTT）であることに注意してください（最大遅延は 200 ミリ秒 RTT です）。
- Catalyst Center が使用できるように 1 つ以上の SNMP クレデンシャルがデバイス上で設定されていることを確認してください。少なくとも、この設定は SNMPv2C 読み取りクレデンシャルにできます。詳細については、ディスカバリクレデンシャル （76 ページ）を参照してください。
- Catalyst Center がデバイスを検出して管理できるようにするには、デバイスで SSH ログイン情報を設定します。以下の基準のうち、少なくとも 1 つが満たされる場合、Catalyst Center はデバイスを検出し、そのインベントリに追加します。
  - デバイスへの SSH アクセスのために Catalyst Center が使用するアカウントが、特権 EXEC モード（レベル 15）である。
  - ディスカバリ ジョブで設定される CLI クレデンシャルの一部としてデバイスのイネーブルパスワードを設定している。詳細については、検出設定のガイドラインと制限事項 （84 ページ）を参照してください。
- デュアルスタック IPv4/IPv6 環境では、次の点に注意してください。
  - 単一の検出セッション中、デバイスが IPv4 と IPv6 の両方を介して到達可能である場合、Catalyst Center は検出された最初のアドレスファミリのみを保持します。デバイスエントリの重複を防ぐため、Catalyst Center はセカンダリアドレスファミリを無視します。
  - サイトベースのロールベースのアクセス制御（SRBAC）の場合、検出はサイトアクセスグループによって制限されます。あるサイトアクセスグループですでに検出されたデバイスは、別のサイトアクセスグループで再検出または管理できません。
  - ループバックオプションを有効にすると、システムのデフォルト設定は IPv6 になります。IPv6 ループバックを使用できない場合、システムは自動的に IPv4 にフォールバックします。
  - Catalyst Center は、クロスファミリネイバー探索をサポートしています。IPv4 でシードされた検出セッションは IPv6 のネイバーを特定でき、IPv6 でシードされたセッションは、CDP または LLDP を介して IPv4の ネイバーを特定できます。

ディスカバリクレデンシャル

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

- ネットワークデバイス：CLI と SNMP のクレデンシャル。

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

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

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

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

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

- CDP を使用したネットワークの検出 （86 ページ）
- IP アドレス範囲または CIDR を使用したネットワークの検出 （90 ページ）
- LLDP を使用したネットワークの検出 （92 ページ）

表 *4 : CLI* クレデンシャル

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

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

表 *5 : SNMPv2c* クレデンシャル

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

表 *6 : SNMPv3* クレデンシャル

フィールド	説明
Name/Description	追加した SNMPv3 設定の名前または説明。

フィールド	説明
Username	SNMPv3 設定に関連付けられている名前。
Mode	SNMP メッセージを必要とするセキュリティ レベル。次のいずれかのモードを選択します。 • [Authentication and Privacy]：認証と暗号化の両方を行います。 • [Authentication, No Privacy]：認証は行いますが、暗号化は行いません。 • [No Authentication, No Privacy]：認証も暗号化も行いません。
Auth. Type	使用する認証タイプ（[Mode] として [Authentication and Privacy] または [Authentication, No Privacy] を選択した場合に有効になります）。次のいずれかの認証タイプを選択します。 • [SHA]：HMAC-SHA に基づく認証。 • [SHA256]：HMAC-SHA256 に基づく認証。 • [MD5 (not recommended)]：HMAC-MD5 に基づく認証。
Auth. Password	SNMPv3 を使用するデバイスから情報にアクセスする際に使用する SNMPv3 パスワード。これらのパスワード（またはパスフレーズ）は、8 文字以上にする必要があります。 （注） • 一部のシスコ ワイヤレス コントローラでは、パスワード（あるいはパスフレーズ）は少なくとも 12 文字以上である必要があります。ワイヤレス コントローラのパスワードの最小要件を必ず確認してください。パスワードに必要な最低限の文字数が守られないと、デバイスではCatalyst Centerによる検出、監視、管理が行われなくなります。 • パスワードはセキュリティ上の理由から暗号化されており、この設定では非表示になります。
Privacy Type	プライバシー タイプ。（[Mode] として [Authentication and Privacy] を選択した場合に有効になります）。次のプライバシータイプのいずれかを選択します。 • [AES128]：暗号化の 128 ビット CBC モード AES。 • **CISCOAES192**：シスコのデバイス上での暗号化の 192 ビット CBC モード AES。 • **CISCOAES256**：シスコのデバイス上での暗号化の 256 ビット CBC モード AES。

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

表 *7 : SNMP* のプロパティ

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

表 *8 : HTTP* および *HTTPS* クレデンシャル

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

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

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

表 *9* : *NETCONF* 設定

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

検出ログイン情報と Cisco ISE

Cisco ISE を認証サーバーとして使用する場合、ディスカバリ機能では、Cisco ISE をディスカバリ プロセスの一部として使用してデバイスが認証されます。デバイスが正しく検出されるように、次のガイドラインに従ってください。

- 英数字 4 文字未満のディスカバリ クレデンシャルを使用しないでください。Cisco ISE では、ユーザー名とパスワードの両方に少なくとも 4 文字の英数字が必要です。デバイスのログイン情報が 4 文字未満の場合、Catalyst Center はデバイスのインベントリデータを収集できず、デバイスは部分的な収集状態になります。
- 同じユーザー名でパスワードが異なるログイン情報（ユーザー名「cisco」に対してパスワードが「cisco123」と「pw123」など）は使用しないでください。Catalyst Center では、ユーザー名が同じでパスワードが異なるデバイスを検出できますが、Cisco ISE では、ユーザー名が重複していると検出できません。重複したユーザー名が使用されている場合、Catalyst Center はデバイスを認証してインベントリ データを収集することができず、デバイスは不完全な収集状態になります。

Cisco ISE を AAA サーバーとして定義する方法については、Cisco ISE またはその他の AAA サーバーの追加 （375 ページ）を参照してください。

検出ログイン情報のガイドラインと制限事項

Catalyst Center の検出ログイン情報に関するガイドラインと制限事項は、次のとおりです。

- 検出ジョブで使用されるデバイスのログイン情報を変更するには、ジョブを編集し、使用しなくなったログイン情報の選択を解除します。次に、新しいログイン情報を追加して検出を開始します。詳細については、検出ジョブでのログイン情報の変更 （96 ページ）を参照してください。
- デバイスが正常に検出された後にデバイスのログイン情報を変更すると、そのデバイスのその後のポーリングサイクルは失敗します。この状況を修正するには、次のいずれかのオプションを使用します。
  - ディスカバリ ツールを使用します：
    - デバイスの新しいクレデンシャルと一致する、ジョブ固有のクレデンシャルを使用して、新しいディスカバリ ジョブを実行します。
    - 既存のディスカバリ ジョブを編集し、ディスカバリを再実行します。
  - 設計ツールを使用します：
    - 新しいグローバル クレデンシャルを作成し、適切なグローバル クレデンシャルを使用して新しいディスカバリ ジョブを実行します。
    - 既存のグローバルログイン情報を編集し、[コピーと編集（Copy and Edit）] を使用して検出ジョブを再作成します。または、新しいディスカバリジョブを作成します。

- デバイス認証に失敗するために進行中の検出ポーリングサイクルが失敗する場合は、次のいずれかのオプションを使用して状況を修正できます。
  - ディスカバリ ツールを使用します：
    - 現在の検出ジョブを停止または削除します。デバイスのログイン情報と一致するジョブ固有のログインを使用して、新しい検出ジョブを実行します。
    - 現在の検出ジョブを停止または削除します。既存のジョブを編集します。検出ジョブを再実行します。
  - 設計ツールを使用します：
    - 新しいグローバル クレデンシャルを作成し、適切なグローバル クレデンシャルを使用して新しいディスカバリ ジョブを実行します。
    - 既存のグローバルログイン情報を編集し、[コピーと編集（Copy and Edit）] を使用して検出ジョブを再作成します。または、新しいディスカバリジョブを作成します。
- グローバル クレデンシャルを削除しても、以前に検出されたデバイスは影響を受けません。これらのデバイスには認証エラーは表示されません。ただし、削除されたクレデンシャルの使用を試みる次回のディスカバリは失敗します。ディスカバリは、いずれかのデバイスへの接続を試みる前に失敗します。

検出ログイン情報の例

一般的なネットワークを構成するデバイスのディスカバリ要件は、非常に多岐にわたる場合があります。Catalyst Center では、これらの多様な要件をサポートするために、複数の検出ジョブを作成できます。たとえば、200 台のデバイスで構成されるネットワークが Cisco Discovery Protocol（CDP）ネイバーを形成しているとします。このネットワークでは、190 台のデバイスはグローバル クレデンシャル（クレデンシャル 0）を共有しており、残りのデバイスは独自のクレデンシャル（クレデンシャル 1 ～ クレデンシャル 10）を持っています。

FIPS モードの展開の場合、ディスカバリパスワードは必ず 8 文字以上とします。

Catalyst Center を使用してこのネットワーク内のすべてのデバイスを検出するには、次の手順を実行します。

手順

ステップ 1 クレデンシャル 0 として CLI グローバル クレデンシャルを設定します。

ステップ 2 SNMP（v2c または v3）グローバルクレデンシャルを設定します。

ステップ 3 190 台のデバイスの IP アドレス（グローバル クレデンシャルを共有する 190 台のデバイス）の 1 つとグローバル クレデンシャル 0 を使用してディスカバリ ジョブを実行します。

ステップ 4 該当するジョブ固有のログイン情報（ログイン情報 1、ログイン情報 2、ログイン情報 3 など）を使用して、残りの 10 台のデバイスごとに 10 個の別個のディスカバリジョブを実行します。

ステップ 5 [Inventory] ウィンドウで結果を確認します。

優先管理 IP アドレス

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

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

表 *10* : 優先管理 *IP* アドレスの決定基準

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

デバイスが検出された後に、**[Inventory]** ウィンドウから管理 IP アドレスを更新できます。詳細については、デバイス管理 IP アドレスの更新 （216 ページ）を参照してください。

検出設定のガイドラインと制限事項

ここでは、デバイス検出の制限事項とガイドラインについて説明します。

- Catalyst Center による Cisco Catalyst 3000 シリーズ スイッチおよび Catalyst 6000 シリーズ スイッチの検出に関する注意事項と制約事項は、次のとおりです。
  - CLI ユーザ名およびパスワードは特権 EXEC モード（レベル 15）で設定してください。これらのログイン情報は、ディスカバリ機能に関して Catalyst Center で設定する CLI ユーザー名およびパスワードと同じです。Catalyst Center にはデバイスへの最高レベルのアクセス権が必要です。
  - 着信接続と発信接続の両方に関して、個々のインターフェイスで許可されるトランスポート プロトコルを明示的に指定してください。この設定には、**transport input** と **transport output** コマンドを使用してください。これらのコマンドについては、各デバイス タイプ用のコマンド リファレンス ドキュメントを参照してください。
  - デバイスのコンソールポートと VTY 回線のデフォルトのログイン方式を変更しないでください。デバイスがすでに AAA（TACACS）ログインで設定されている場合は、Catalyst Center で定義されている CLI ログイン情報が、TACACS サーバで定義されている TACACS ログイン情報と同じであることを確認してください。

- Catalyst Center が ワイヤレスコントローラ と AP を検出する際のガイドラインと制限事項は次のとおりです。
  - シスコ ワイヤレス コントローラ は、サービスポート IP アドレスではなく、管理 IP アドレスを使用して検出する必要があります。それ以外の場合は、関連するワイヤレスコントローラ 360 および AP 360 のウィンドウでは、データが表示されません。
  - ワイヤレスコントローラ が検出されると、Catalyst Center にインベントリ内の関連付けられた AP のリストが表示されます。リストされた AP は、検出中またはインベントリ同期を通じて ワイヤレスコントローラ に接続されます。



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

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

- サードパーティ製デバイスは、Catalyst Center 検出機能では検出できません。サードパーティ製デバイスはネットワークに手動で追加する必要があります。詳細については、*Cisco Catalyst Center User Guide*のサードパーティ製デバイスの追加（184 ページ）を参照してください。

ディスカバリの実行

Link Layer Discovery Protocol（LLDP）、CDP、CIDR、または IP アドレス範囲を使用してデバイスを検出できます。

ディスカバリの前提条件（75 ページ）で説明されているように、デバイスには必須のデバイス設定が存在する必要があります。

- IP アドレス範囲のディスカバリの場合、検出されたデバイスの一覧には、ping で到達可能なデバイスのみが含まれます。ping で到達できないデバイスは含まれません。
- CDP、CIDR、および LLDP ベースのディスカバリの場合、CDP、CIDR、および LLDP プロトコルでは ping で到達できない IP にも応答するため、検出されたデバイスの一覧には、ping で到達できないデバイスも含まれます。
- CDP、CIDR、および LLDP ベースの検出の場合、クライアント IP アドレスとしてネットワークデバイスのホスト IP アドレスを設定します。（ホストは、ラップトップコンピュータまたはモバイルデバイスなどのエンドユーザデバイスです。）
- ディスカバリ機能では、正しい SNMP 読み取り専用コミュニティストリングが必要です。SNMP 読み取り専用コミュニティストリングが指定されていない場合、ディスカバリ機能では、デフォルトの SNMP 読み取り専用コミュニティストリング「public」が使用されます。
- ディスカバリ中に、すでに検出されてサイトと関連付けられているデバイスはスキップされます。それらのデバイスはサイトに再度割り当てられません。
- ホストの検出には CLI クレデンシャルは必要ありません。ホストは、接続されているネットワークデバイスを通じて検出されます。
- SNMPv3 ログイン情報を使用した検出の間、Catalyst Center は、デフォルトの SNMP ユーザーグループを使用して SNMPv3 ログイン情報をデバイスにプッシュし、デバイス上の既存のユーザーグループは無視します。
- [Discover new devices only] を選択すると、検出によって新しいデバイスのみがインベントリに追加されます。ディスカバリでは、インベントリ内の既存のデバイスに対しては何も更新されません。

CDP を使用したネットワークの検出

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

ディスカバリ メソッドの詳細については、IPアドレス範囲またはCIDR を使用したネットワークの検出 （90 ページ）およびLLDP を使用したネットワークの検出 （92 ページ）を参照してください。

（注）

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

始める前に

- ネットワークデバイスで CDP を有効にします。
- ディスカバリの前提条件 （75 ページ）で説明されているように、ネットワークデバイスを設定します。
- クライアント IP アドレスとしてネットワークデバイスのホストの IP アドレスを設定します。（ホストは、ラップトップコンピュータまたはモバイルデバイスなどのエンドユーザデバイスです。）

手順

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

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

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

a) 検出ジョブの名前を入力します。

b) [Discovery Type] で、[CDP] を選択します。

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

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

個別の IP アドレス（*x.x.x.x*）または Classless Inter-Domain Routing（CIDR）アドレス（*x.x.x.x/y*）としてアドレスを入力できます。ここで*x.x.x.x* は IP アドレスを示し、*y* はサブネット マスクを示します。サブネットマスクは、20 ～ 32 の値です。

e) ＋ をクリックします。

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

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

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

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

オプション	説明
なし（None）	デバイスはすべての IP アドレスを使用できます。
Use Loopback IP	デバイスのループバック インターフェイスの IP アドレスを指定します。 （注） [Use Loopback IP] を選択し、デバイスにループバック インターフェイスがない場合、Catalyst Center は「優先管理 IP アドレス （84 ページ）」で説明されているロジックを使用して、管理 IP アドレスを選択します。 （注） ループバック インターフェイスの IP アドレスを優先管理 IP アドレスとして使用するには、CDP ネイバーの IP アドレスがCatalyst Centerから到達可能であることを確認します。

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

少なくとも 1 つの CLI ログイン情報と 1 つの SNMP ログイン情報を入力します。このログイン情報は、Catalyst Center によって検出されたデバイスに対して構成されます。最大 5 つのグローバルログイン情報、およびタイプごとに 1 つのタスク固有のログイン情報を使用できます。詳細については、ディスカバリ クレデンシャル （76 ページ）を参照してください。

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

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

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

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

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

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

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

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

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

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

ダイアログボックスで、次のオプションのいずれかを選択します。

オプション	タスク
Assign to site without Configuration Preview	[Search Hierarchy] 検索フィールドまたはフィルタアイコンを使用して、サイト、ビルディング、またはエリアを見つけます。詳細については、ネットワーク階層の検索 （284 ページ）を参照してください。
Skip site assignment for now	後でデバイスをインベントリからサイトに割り当てる場合は、このオプションを使用します。

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

ステップ 7 [Start Discovery] をクリックします。

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

次のタスク

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

IP アドレス範囲または CIDR を使用したネットワークの検出

IP アドレス範囲、CIDR、CDP、または LLDP を使用してデバイスとホストを検出できます。この手順では、IP アドレス範囲または CIDR を使用して検出を実行する方法について説明します。その他の検出方法の詳細については、「CDP を使用したネットワークの検出 （86 ページ）」および「LLDP を使用したネットワークの検出 （92 ページ）」を参照してください。

始める前に

ディスカバリの前提条件 （75 ページ）で説明されているように、デバイスには必須のデバイス設定が存在する必要があります。

手順

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

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

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

a) 検出ジョブの名前を入力します。

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

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

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

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

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

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

d) [CIDR] 検出タイプを選択した場合は、次の手順を実行します。

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

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

   個別の IP アドレス（*x.x.x.x*）または Classless Inter-Domain Routing（CIDR）アドレス（*x.x.x.x/y*）としてアドレスを入力できます。ここで*x.x.x.x* は IP アドレスを示し、*y* はサブネット マスクを示します。サブネットマスクは、20 ～ 32 の値です。

3. をクリックします。

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

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

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

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

（注） [Use Loopback IP] の使用を選択し、デバイスにループバック インターフェイスがない場合、Catalyst Centerは優先管理 IP アドレス （84 ページ）で説明されているロジックを使用して、管理 IP アドレスを選択します。

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

少なくとも 1 つの CLI ログイン情報と 1 つの SNMP ログイン情報を入力します。このログイン情報は、Catalyst Center によって検出されたデバイスに対して構成されます。最大 5 つのグローバルログイン情報、およびタイプごとに 1 つのタスク固有のログイン情報を使用できます。詳細については、ディスカバリ クレデンシャル （76 ページ）を参照してください。

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

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

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

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

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

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

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

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

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

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

ダイアログボックスで、次のオプションのいずれかを選択します。

オプション	タスク
Assign to site without Configuration Preview	[Search Hierarchy] 検索フィールドまたはフィルタアイコンを使用して、サイト、ビルディング、またはエリアを見つけます。詳細については、ネットワーク階層の検索 （284 ページ）を参照してください。
Skip site assignment for now	後でデバイスをインベントリからサイトに割り当てる場合は、このオプションを使用します。

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

ステップ 7 [Start Discovery] をクリックします。

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

次のタスク

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

LLDP を使用したネットワークの検出

Link Layer Discovery Protocol（LLDP）、CDP、CIDR、または IP アドレス範囲を使用してデバイスを検出できます。この手順では、LLDP を使用してデバイスとホストを検出する方法を説明します。ディスカバリ メソッドの詳細については、CDP を使用したネットワークの検出

（86 ページ）およびIP アドレス範囲または CIDR を使用したネットワークの検出 （90 ページ）を参照してください。

（注）

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

始める前に

- ネットワークデバイスで LLDP プロトコルを有効にします。
- ディスカバリの前提条件 （75 ページ） に従ってネットワークデバイスを設定します。
- クライアント IP アドレスとしてネットワークデバイスのホスト IP アドレスを設定します。ホストは、ラップトップコンピュータまたはモバイルデバイスなどのエンドユーザーデバイスです。

手順

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

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

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

a) 検出ジョブの名前を入力します。

b) [Discovery Type] で、[LLDP] を選択します。

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

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

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

e) をクリックします。

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

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

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

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

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

（注） このオプションを選択し、デバイスにループバック インターフェイスがない場合、Catalyst Center は「優先管理 IP アドレス （84 ページ）」で説明されているロジックを使用して、管理 IP アドレスを選択します。

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

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

少なくとも 1 つの CLI ログイン情報と 1 つの SNMP ログイン情報を入力します。このログイン情報は、Catalyst Center によって検出されたデバイスに対して構成されます。最大 5 つのグローバルログイン情報、およびタイプごとに 1 つのタスク固有のログイン情報を使用できます。詳細については、ディスカバリ クレデンシャル （76 ページ）を参照してください。

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

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

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

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

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

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

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

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

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

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

ダイアログボックスで、次のオプションのいずれかを選択します。

オプション	タスク
Assign to site without Configuration Preview	[Search Hierarchy] 検索フィールドまたはフィルタアイコンを使用して、サイト、ビルディング、またはエリアを見つけます。詳細については、ネットワーク階層の検索 （284 ページ）を参照してください。
Skip site assignment for now	後でデバイスをインベントリからサイトに割り当てる場合は、このオプションを使用します。

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

ステップ 7 [Start Discovery] をクリックします。

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

次のタスク

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

ディスカバリジョブの管理

ここでは、ディスカバリジョブの管理方法について説明します。

ディスカバリ ジョブの停止および開始

手順

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

ステップ 2 アクティブなディスカバリジョブを停止するには、[**Actions**] 列の省略記号アイコン（ ••• ）にカーソルを合わせ、[**Stop Discovery**] を選択します。

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

検出ジョブでのログイン情報の変更

ディスカバリジョブで使用されるログイン情報を変更し、そのジョブを再実行します。

始める前に

開始する前に少なくとも 1 つのディスカバリジョブを作成します。

手順

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

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

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

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

ステップ 4 [New Discovery] ウィンドウで、[Credentials] エリアを展開し、すでに作成されているグローバルログイン情報のいずれかを選択するか独自に構成します。

既存のログイン情報を使用する場合は、それらを選択します。ログイン情報を除外するには、選択を解除します。

ステップ 5 独自のクレデンシャルを構成するには、[Add Credentials] をクリックします。

CLIおよびSNMPv2cログイン情報を設定する必要があります。その他のログイン情報はオプションです。各フィールドの詳細については、「ディスカバリクレデンシャル （76 ページ）」を参照してください。

現在のジョブのクレデンシャルのみを保存するには、[Save]をクリックします。現在のジョブと将来のジョブのクレデンシャルを保存するには、[Save as global settings] チェックボックスをオンにして、[Save] をクリックします。

ステップ 6 [Discover] をクリックします。

ディスカバリジョブの複製

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

始める前に

少なくとも 1 つのディスカバリジョブを実行します。

手順

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

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

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

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

ステップ 4 新しいディスカバリ ジョブのパラメータを定義または更新します。

ディスカバリ ジョブの削除

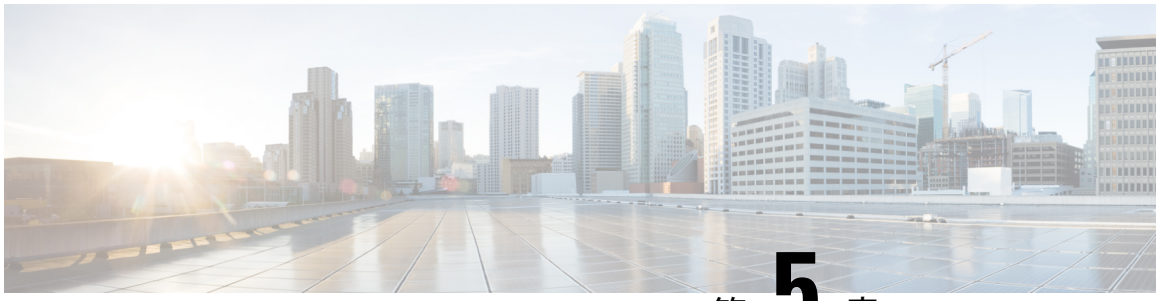
アクティブまたは非アクティブに関係なく、検出ジョブを削除できます。

手順

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

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

ステップ 3 [OK] をクリックして確定します。



第 5 章

インベントリの管理

- インベントリについて （100 ページ）
- インベントリと Cisco ISE の認証 （101 ページ）
- インベントリに関する情報の表示 （102 ページ）
- ユーザー定義フィールドの管理 （153 ページ）
- インベントリからのトポロジマップの起動 （154 ページ）
- Catalyst Center インベントリ内のデバイスのタイプ （155 ページ）
- デバイスのフィルタリング （187 ページ）
- [Inventory] ウィンドウでのデバイスの管理 （189 ページ）
- デバイスの REP リングの構成 （196 ページ）
- 非ファブリック展開用 REP リングへのノードの追加 （198 ページ）
- 非ファブリック展開用 REP リングからのノードの削除 （200 ページ）
- 非ファブリック展開用の MRP リング （201 ページ）
- 非ファブリック展開用の MRP リングステータスの表示 （201 ページ）
- Parallel Redundancy Protocol （203 ページ）
- PRP トポロジステータスの表示 （204 ページ）
- ポートグループの作成 （206 ページ）
- ポートへのタグの割り当て （207 ページ）
- ポート使用情報 （208 ページ）
- デバイスのメンテナンスモード （208 ページ）
- インベントリインサイト （211 ページ）
- システムビーコンの管理 （213 ページ）
- デバイスのロール （214 ページ）
- デバイスロールを手動で変更する （215 ページ）
- デバイス管理 IP アドレスの更新 （216 ページ）
- デバイスポーリング間隔の更新 （216 ページ）
- デバイス情報の再同期 （217 ページ）
- ネットワークデバイスの削除 （218 ページ）
- コマンド ランナーを起動（インベントリ） （219 ページ）

• Run コマンドを使用したデバイスの到達可能性に関する問題のトラブルシューティング（220 ページ）
• CSV ファイルを使用したデバイス設定のインポート/エクスポート （221 ページ）
• デバイスの構成ドリフト （225 ページ）
• デバイスの構成ドリフトの表示 （226 ページ）
• 構成ドリフトのラベル付け （228 ページ）
• デバイス構成の可視性と制御 （229 ページ）
• デバイス構成を今すぐまたは後で展開する （238 ページ）
• デバイス設定のプレビューと展開 （238 ページ）
• ネットワーク プロビジョニングの事前チェック （240 ページ）
• 故障したデバイスの交換 （244 ページ）
• 障害のあるアクセスポイントの交換 （251 ページ）
• アウトオブバンド RMA デバイスの交換の管理 （255 ページ）
• Catalyst Center の RMA ワークフローの制限事項 （255 ページ）
• アクセスポイントの再起動 （258 ページ）

インベントリについて

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

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

インベントリは、必要に応じて次のプロトコルを使用します。

- リンク層検出プロトコル（LLDP）
- IP デバイス トラッキング（IPDT）またはスイッチ統合セキュリティ機能（SISF）（IPDT または SISF をデバイス上で有効にする必要があります）。
- LLDP Media Endpoint Discovery （このプロトコルは IP フォンや一部のサーバーの検出に使用されます）。
- ネットワーク設定プロトコル（NETCONF）デバイスのリストについては、ディスカバリの前提条件 （75 ページ） を参照してください。

初期検出後、Catalyst Center は定期的にデバイスをポーリングすることでインベントリを維持します。デフォルトの間隔は 24 時間ごとです。ただし、この間隔は、ネットワーク環境の必要性に応じて変更できます。詳細については、デバイスポーリング間隔の更新 （216 ページ）を参照してください。ポーリングはデバイス、リンク、ホスト、およびインターフェイスごとに実行されます。アクティブ状態が 1 日未満のデバイスのみが表示されます。これによって、古いデバイス データが表示されないようにします。500 個のデバイスのポーリングに約 20 分かかります。デバイスの設定変更によって SNMP トラップがトリガーされ、次にデバイスの再同期がトリガーされます。以下の状況下では、インベントリサービスの再起動後にもデバイスの再同期がトリガーされます。

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

（注） デバイスの再同期に関するポイントは次のとおりです。

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

インベントリと Cisco ISE の認証

Cisco ISE における Catalyst Center のユースケースには、次の 2 つがあります。

- ネットワークでデバイス認証に Cisco ISE を使用する場合、Cisco ISE の設定を Catalyst Center で構成する必要があります。これにより、Catalyst Center でデバイスをプロビジョニングする際に、ユーザーが定義した Cisco ISE サーバーの情報を使用してデバイスが設定されます。また、Catalyst Center は Cisco ISE サーバーでデバイスを設定し、後に続くデバイスの更新プログラムについても伝えます。Catalyst Center における Cisco ISE の設定の構成については、「グローバル ネットワーク サーバーの設定（377 ページ）」を参照してください。

（注） Cisco ISE を使用して Cisco Catalyst 9800 シリーズ デバイスを認証する場合は、NETCONF ユーザーに権限が付与されるように Cisco ISE を設定する必要があります。

ネットワーク障害や Cisco ISE サーバーのダウンによって予定どおりにデバイスが Cisco ISE サーバーで設定または更新されていない場合、Catalyst Center は一定の待機期間が経過した後に自動的に操作を再試行します。ただし、入力の検証エラーとして Cisco ISE から拒否されていることが障害の原因である場合、Catalyst Center は操作を再試行しません。

Catalyst Center が Cisco ISE サーバーでデバイスを設定および更新する場合、トランザクションは Catalyst Center の監査ログでキャプチャされます。Catalyst Center や Cisco ISE インベントリに関する問題のトラブルシューティングに監査ログを役立てることができます。また、（[詳細の表示] リンクをクリックして）デバイスのプロビジョニングの概要や Catalyst Center インベントリの [プロビジョニングステータス（Provisioning Status）] 列で ISE 統合ステータスの情報を確認することもできます。

デバイスのプロビジョニング後、Catalyst Center は Cisco ISE でデバイスを認証します。Cisco ISE に到達できない（RADIUS 応答がない）場合、デバイスはローカルのログイン情報を使用します。Cisco ISE に到達できるものの Cisco ISE にデバイスが存在しない場合、またはそのログイン情報が Catalyst Center で設定されたログイン情報と一致しない場合、デバイスはローカルのログイン情報を使用するためにフォールバックしません。代わりに、部分的な収集状態になります。

この状態を回避するには、Catalyst Center を使用してデバイスをプロビジョニングする前に、必ず Catalyst Center で使用しているのと同じデバイスのログイン情報で Cisco ISE のデバイスを設定します。また、有効なディスカバリクレデンシャルを設定したことも確認してください。詳細については、ディスカバリクレデンシャル （76 ページ）を参照してください。デバイスにおける Cisco TrustSec（CTS）のログイン情報の逸脱は、コンプライアンスチェック中に特定され、コンプライアンスの概要の [ネットワーク設定（Network Settings）] タイルに表示されます。

- 必要に応じて、Cisco ISE を使用してデバイスのグループにアクセス制御を適用できます。

インベントリに関する情報の表示

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

始める前に

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

手順

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

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

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

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

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

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

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

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

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

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

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

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

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

詳細については、デバイスのフィルタリング （187 ページ）を参照してください。

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

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

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

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

（注） 列の選択はセッション間では保持されません。

このテーブルには、特定のテーブル列に関する重要な情報が表示されます。

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

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

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

カラム	説明
Manageability	デバイスのステータスが示されます。 • [Managed] と緑色のチェックアイコン：デバイスに到達可能で、完全に管理されています。 • [Managed] とオレンジ色のエラーアイコン：デバイスは管理されていますが、到達不能、認証失敗、NETCONF ポートがない、内部エラーなど、何らかのエラーがあります。エラーメッセージにカーソルを合わせると、エラーおよび影響を受けるアプリケーションに関する詳細が表示されます。 （注） デバイスの SSH キーの検証に失敗した場合の対処方法については、SSH キー検証エラーへの対処 （195 ページ） を参照してください。 • [Unmanaged]：デバイスの接続の問題が原因でデバイスに到達できず、インベントリ情報が収集されていません。 （注） デバイスの再同期が進行中の場合は、[Syncing] ステータスが表示されます。ステータスをクリックすると、次が表示されます。 • 進行中の同期の詳細 • 以前の同期の詳細 • 同期の理由 • 同期を要求したアプリケーション。 キューにある保留中の再同期要求については、メッセージが表示されます。複数の要求が保留中の場合は、同期する機能と優先順位に基づいてマージされます。同期の詳細には、同期イベントの理由が複数表示される場合があります。
Platform	シスコ製品の部品番号
Device Role	スキャン プロセス中に、検出された各デバイスに割り当てられているロール。デバイス ロールは、ネットワーク内での役目と配置に従って、デバイスを識別およびグループ分けするために使用されます。Catalyst Center でデバイス ロールを特定できない場合、デバイス ロールは不明に設定されます。 （注） デバイスロールを手動で変更すると、割り当ては静的のままになります。Catalyst Center は、後続のデバイスの再同期中に変更が検知されたとしても、デバイスロールを更新しません。 必要に応じて、このカラムのドロップダウン リストを使用して、割り当てられたデバイス ロールを変更することができます。

カラム	説明
Site	デバイスに割り当てられているサイト。 デバイスがどのサイトにも割り当てられていない場合は、次の手順を実行します。 **1.** [**Assign**] をクリックします。 **2.** [Choose a Site] をクリックします。 **3.** 階層からサイトを選択します。 **4.** [Save] をクリックします。 詳細については、ネットワーク階層 （271 ページ）を参照してください。
Last Updated	Catalyst Center がデバイスをスキャンし、デバイスに関する新しい情報でデータベースを更新した最新の日付と時刻。 （注） [Sync Details] をクリックして、**最後の同期の開始時刻**と**最後の同期の理由**を表示します。 デバイスの再同期が進行中の場合は、[Sync Details] に次が表示されます。 • 進行中の同期の詳細 • 以前の同期の詳細 • 同期の理由 • 同期を要求したアプリケーション。 キューにある保留中の再同期要求については、メッセージが表示されます。複数の要求が保留中の場合は、同期する機能と優先順位に基づいてマージされます。同期の詳細には、同期イベントの理由が複数表示される場合があります。
Resync Interval	デバイスのポーリング間隔。 再同期間隔は、[Inventory] ウィンドウから **[Actions]** > **[Edit Device]** > **[Resync Interval]** の順に選択して設定します。 再同期タイプを [Global] として設定するには、メインメニューから **[System]** > **[Settings]** の順に選択します。詳細については、*Cisco Catalyst Center Administrator Guide*を参照してください。

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

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

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

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

名前	説明
タグ	[タグ（Tag）] をクリックして、デバイスにタグを付けたり、タグを編集および削除したり、ポートグループを作成したりします。 詳細については、[Inventory] ウィンドウでのデバイスの管理 （189 ページ）を参照してください。
Add Device	[デバイスの追加（Add Device）] をクリックして、ネットワークデバイスを追加するか、コンピューティングデバイスを追加するか、Cisco Meraki ダッシュボードまたは Firepower Management Center（FMC）を Catalyst Center と統合します。 詳細については、Catalyst Center インベントリ内のデバイスのタイプ （155 ページ）を参照してください。
[Actions] ドロップダウン リスト	[Actions] ドロップダウンリストを使用して、デバイス、ソフトウェアイメージ、テレメトリなどを管理します。 各アクションオプションの詳細を表示するには、右隣の情報アイコン（ⓘ）をクリックします。

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

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

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

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

デバイスに関する情報の表示

検出されたデバイス、そのデバイスのセキュリティ、およびコンプライアンスに関する情報を表示、フィルタ処理、検索できます。

始める前に

インベントリにデバイスがあることを確認します。デバイスがない場合は検出機能を使用します。

手順

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

[インベントリ（Inventory）] ウィンドウに、検出されたデバイスに関する情報が表示されます。

ステップ 2 [デバイス（Devices）] テーブルでデバイスの名前をクリックすると、そのデバイスの詳細情報が表示されます。

ステップ 3 [View Device Details] をクリックします。

デバイスの詳細がウィンドウに表示されます。

ステップ 4 このウィンドウで利用可能な情報を示す次の表を使用して、デバイスの詳細を表示、フィルタ処理、検索します。

名前	説明
run コマンド	このリンクは、ルータ、ワイヤレスコントローラ、スイッチ、ハブに対してのみ表示されます。 デバイスでコマンド ランナー アプリケーションを起動して診断 CLI コマンドを実行し、結果のコマンド出力を表示します。

名前	説明
[APの管理（Manage APs）	このリンクは、デバイスごとの設定機能が有効になっている Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ でのみ使用できます。 デバイスごとの設定 を使用してプロビジョニングされた ワイヤレスコントローラについては、このリンクをクリックして関連する AP を管理します。 （注） ワイヤレスコントローラ がサイトベースのネットワークプロファイルでインテントベースのワイヤレスネットワーク設定を使用してプロビジョニングされている場合は、このリンクを使用して関連付けられた AP のリストのみを表示できます。 詳細については、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ に関連付けられた AP の管理 （805 ページ） を参照してください。
View 360	このリンクは、すべてのデバイスに対して表示されます。 そのデバイスの [Device 360] ウィンドウが表示されます。 このウィンドウを開くには、Assurance アプリケーションをインストールしておく必要があります。
インターフェイス	この機能は、AP を除くすべてのデバイスで使用できます。 イーサネットポートなど、デバイスのポートに関する情報がトポロジまたはテーブルビューで表示されます。 [詳細（Details）] タブで設定を表示できます。 デバイスインターフェイスの詳細については、「デバイスのインターフェイスに関する情報の表示 （117 ページ）」を参照してください。
Hardware & Software	この機能はすべてのデバイスで使用できます。 稼働時間やプロビジョニングステータス、Cisco ISE 統合ステータスなど、デバイスのハードウェアとソフトウェアの詳細が操作の概要とともに表示されます。

名前	説明
Configuration（実行コンフィギュレーション）	この機能は、AP、ルータ、スイッチに対してのみ使用できます。 設定を表示するには、**[詳細（Details）]** > **[設定を参照（Browse configurations）]**に移動してください。 ルータ、スイッチ、ハブに関しては、このオプションに**show running-config**コマンドの出力で表示される内容に似た詳細な設定情報が表示されます。行番号を非表示にしたり、コマンドラインやテキストを検索したり、CLI出力をエクスポートしたりできます。 AP の場合、このタブに AP 設定および無線設定に関する情報が表示されます。 この機能はワイヤレスコントローラではサポートされていないため、このデバイスタイプの設定データは返されません。
Power	この機能は、ルータとスイッチでのみ使用できます。 デバイスの電力使用量と電源の詳細が表示されます。 設定を表示するには、**[詳細（Details）]** > **[システム（System）]** に移動してください。 [名前（Name）]、[動作ステータス（Operational Status）] などのフィールドに値を入力して、[電源（Power Supplies）] テーブル内のデータを検索およびフィルタ処理します。絞り込まれた検索結果は、テーブル全体で一致する値が強調表示された状態で表示されます。
Fans	この機能は、ルータとスイッチでのみ使用できます。 ファンの詳細が表示されます。 設定を表示するには、**[詳細（Details）]** > **[システム（System）]** に移動してください。 [名前（Name）]、[動作ステータス（Operational Status）] などのフィールドに値を入力して、[ファン（Fans）] テーブル内のデータを検索およびフィルタ処理します。絞り込まれた検索結果は、テーブル全体で一致する値が強調表示された状態で表示されます。

名前	説明
SFP Modules	この機能は、ルータとスイッチでのみ使用できます。 製造元や Small Form-Factor Pluggable（SFP）モジュールが接続されているポートなどの詳細が表示されます。 設定を表示するには、**[詳細（Details）]** > **[システム（System）]** に移動してください。 [名前（Name）]、[プラットフォーム（Platform）] などのフィールドに値を入力して、[SFP モジュール（SFP Modules）] テーブル内のデータを検索およびフィルタ処理します。絞り込まれた検索結果は、テーブル全体で一致する値が強調表示された状態で表示されます。
User Defined Fields	この機能はすべてのデバイスで使用できます。 デバイスに関連付けられているユーザー定義フィールドが表示されます。 [詳細（Details）] タブで設定を表示できます。 [Manage User Defined Fields] をクリックし、[Manage User Defined Fields] スライドインペインを表示します。 次のタスクを実行できます。 • [Create New Fields] をクリックし、新しいフィールドを作成します。 • [Search Table] をクリックし、手動で値を入力して Enter キーを押します。絞り込まれた検索結果は、テーブル全体で値が強調表示された状態で表示されます。 ユーザー定義フィールドをデバイスに追加するには、最初に [ユーザー定義フィールドの管理（Manage User Defined Fields）] スライドインペインでユーザー定義フィールドを作成する必要があります。 詳細については、ユーザー定義フィールドの作成 （153 ページ） を参照してください。 ユーザー定義フィールドをデバイスに割り当て、値を追加すると、そのフィールドが表示されます。詳細については、デバイスへのユーザー定義フィールドの追加 （154 ページ） を参照してください。
Config Drift	この機能はすべてのデバイスで使用できます。 変更履歴を含むデバイスの構成の変更が表示され、2 つの構成が比較されます。次のタスクを実行できます。 設定を表示するには、**[詳細（Details）]** > **[設定を参照（Browse configurations）]**に移動してください。 • 将来の参照のために、時系列で構成ドリフトにラベルを付けます。詳細については、構成ドリフトのラベル付け （228 ページ） を参照してください。 • 同じデバイスの任意のバージョンを 2 つ選択し、それらの実行コンフィギュレーション データを比較します。

名前	説明
REP Rings	このタブは、Cisco Catalyst Industrial Ethernet 3100、3200、3300、3400、4000、5000、および 9300 シリーズ スイッチで使用できます。 Cisco エンベデッドサービス 3300 シリーズ スイッチ（ESS3300）、S5200、および S5800。 名前、リングサイズ、最初の隣接デバイスなど、Resilient Ethernet Protocol（REP）リングの詳細が表示されます。 [冗長性（Redundancy）] タブで設定を表示できます。 [Create REP Ring] をクリックし、ワークフローに従って REP リングを作成します。 詳細については、「REP リングからのノードの削除（1289ページ）」または「REP リングの削除（1287 ページ）」を参照してください。
[MRP Rings]	このタブは、Cisco Industrial Ethernet（IE）3000、4000、5000 シリーズ スイッチでのみ使用できます。 リング ID、リングサイズ、VLAN ID、ネットワーク トポロジ ステータス、プロファイル値、リングの詳細など、Media Redundancy Protocol（MRP）リングの詳細が表示されます。 [冗長性（Redundancy）] タブで設定を表示できます。 MRP リングの詳細を表示するには、**[プロビジョニング（Provision）]** > **[インベントリ（Inventory）]** > **[トポロジ（Topology）]** ビューで、リングの任意の場所をクリックします。 詳細については、非ファブリック展開用の MRP リング（201 ページ）および非ファブリック展開用の MRP リングステータスの表示（201 ページ）を参照してください。
Wireless Info	このタブは ワイヤレスコントローラ でのみ使用できます。 管理対象サイト、ワイヤレス設定、冗長性、正常性パラメータなどの詳細が表示されます。 [Wireless Summary] タブの [SSIDs] テーブルで、[Search Table] をクリックし、手動で値を入力して Enter キーを押すことにより、特定の値を検索できます。絞り込まれた検索結果は、テーブル全体で値が強調表示された状態で表示されます。

名前	説明
Configuration（デバイスごとの設定）	このエリアは、ワイヤレスコントローラ およびスイッチでのみ使用できます。 **ワイヤレスコントローラ** • [モビリティ（Mobility）]：このタブには、モビリティの詳細（例：モビリティグループ名、RF グループ名）が表示されます。 [モビリティピア（Mobility Peers）] テーブルは、デバイスでモビリティピアが設定されている場合に表示されます。モビリティピアが設定されていない場合は、「モビリティグループの設定 （774ページ）」を参照してください。 [MAC address]、[Device Name]、および [IP Address] フィールドの値など、任意の値を組み合わせてテーブルをフィルタ処理し、特定のモビリティピアを表示できます。 • デバイスごとの設定：この機能が有効になっている Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ でのみ使用できます。 ワイヤレスコントローラ の場合、デバイスごとの設定 を使用して、WLAN 設定、RF 設定などの個々の機能を管理できます。 （注） ワイヤレスコントローラ がサイトベースのネットワークプロファイルでインテントベースの設定を使用してプロビジョニングされている場合、このエリアではデバイス設定のみを表示できます。 詳細については、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の デバイスごとの設定 （801 ページ） を参照してください。 **スイッチ**：Cisco Catalyst スイッチのデバイスごとの設定を表示します。この機能は、Cisco IOS XE リリース 17.12.x 以降を実行している Cisco Catalyst 9000 シリーズ スイッチおよび Cisco Catalyst 産業用イーサネット（IE）スイッチで使用できます。詳細については、Cisco Catalyst スイッチのデバイスごとの設定を管理する （123 ページ） を参照してください。

名前	説明
セキュリティ	このタブは、すべてのデバイスに対して表示されます。 [アドバイザリ（Advisories）] テーブルにデバイスのアドバイザリの詳細が表示されます。次のタスクを実行できます。 • [Manage All] をクリックして [Security Advisories] ウィンドウを表示し、デバイスとアドバイザリを管理します。 • [Filter] をクリックし、[Advisory ID] および [Advisory Title] フィールドの値など、任意の値を組み合わせてアドバイザリを表示します。次に、[Apply] をクリックします。 • アドバイザリ ID をクリックし、そのアドバイザリの詳細情報を表示します。 • [Custom Match Pattern] 列で [Add match pattern] をクリックし、条件を追加または更新して [CONDITIONS] テキストボックスのデバイスと一致させます。その後一致パターンを保存し、スキャンを実行して一致パターンに一致するデバイスの数を確認できます。
フィールド 通知	デバイスの Field Notice に関する情報が表示されます。「Field Notice の表示」を参照してください。
潜在的な Field Notice	デバイスの潜在的な Field Notice に関する情報が表示されます。
コンプライアンス	このタブは、すべてのデバイスに対して表示されます。 スタートアップ コンフィギュレーションと実行コンフィギュレーションのコンプライアンスが最後に実行されたタイミングなど、デバイスのコンプライアンスの概要が表示されます。次のタスクを実行できます。 • [Run Compliance Check] をクリックし、デバイスのコンプライアンスをチェックします。 • [View Preference for Acknowledged Violations] をクリックし、認識されている違反属性のリストを表示します。違反をリストから除外して開くことができます。

デバイスのインターフェイスに関する情報の表示

ルータ、ワイヤレスコントローラ、スイッチ、またはハブに関しては、デバイスのインターフェイスに関する情報を表示、検索、フィルタ処理できます。デバイスによっては、特定の情報を表示できます。

手順

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

[Inventory] ウィンドウには、検出プロセス中に収集されたデバイス情報が表示されます。

ステップ 2 [Devices] テーブルでデバイスの名前をクリックしてから、[View Device Details] をクリックします。

ステップ 3 **[詳細（Details）]** > **[インターフェイス（Interfaces）]** をクリックします。

ステップ 4 [インターフェイス（Interfaces）] ドロップダウンリストのオプションが記載された次の表を使用して、インターフェイスの詳細を表示します。

名前	説明

イーサネット ポート	• このタブは、AP 以外のすべてのデバイスに対して表示されます。
	ルータおよびスイッチの場合、ポート情報は[概要（Summary）]タブに表示されます。
	• イーサネットポートの詳細は、トポロジとテーブルの 2 つのビューで表示されます。
	  • トポロジビューには、色分けされた各ポートの接続ステータスとともにデバイスのイーサネットポートトポロジが表示されます。
	  • テーブルビューには、動作ステータスや管理ステータスなど、イーサネットポートの詳細が表示されます。
	• 2 つのビューの詳細については、「イーサネットポートに関する情報の表示 （119 ページ）」を参照してください。

名前	説明

VLAN	• このタブは、スイッチとハブに対してのみ表示されます。
	• 動作ステータスや管理ステータスなど、VLANの詳細がテーブル形式で表示されます。
	• [VLANs] テーブルには、次のタイプの VLAN の ID が表示されます。
	  • 製造時提供のデフォルト VLAN の VLAN ID
	  • 設定されたデフォルト VLAN の VLAN ID
	  • 設定された VLAN の VLAN ID
	
	[**Name**]、[**Operational Status**]、およびその他のフィールドに値を入力して、[**VLANs**] テーブル内のデータの検索とフィルタ処理を行います。絞り込まれた検索結果は、テーブル全体で一致する値が強調表示された状態で表示されます。

Virtual Ports	• このタブは、ワイヤレスコントローラとルータに対してのみ表示されます。 • 動作ステータスや管理ステータスなど、ポートの詳細が表示されます。 • [**Name**]、[**Operational Status**]、およびその他のフィールドに値を入力して、[**Virtual Ports**] テーブル内のデータの検索とフィルタ処理を行います。絞り込まれた検索結果は、テーブル全体で一致する値が強調表示された状態で表示されます。

イーサネットポートに関する情報の表示

この手順を使用して、トポロジビューまたはテーブルビューのいずれかでポートに関する特定の情報を表示、検索、フィルタ処理できます。

手順

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

ステップ 2 [Devices] テーブルからデバイス名をクリックし、[View Device Details] をクリックします。

ステップ 3 **[詳細（Details）]** > **[インターフェイス（Interfaces）]** > **[イーサネットポート（Ethernet Ports）]** をクリックします。

ルータおよびスイッチの場合、ポート情報は [概要（Summary）] タブに表示されます。

ステップ 4 右上隅の [Topology View]（ ）をクリックし、イーサネットポートトポロジを表示します（まだ表示されていない場合）。

このビューには、色分けされた各ポートの接続ステータスとともにデバイスのイーサネットポートトポロジが表示されます。詳細を確認する場合は、ポートにカーソルを合わせてください。

（注） Cisco Catalyst 4000 シリーズ、6000 シリーズ、および 9000 シリーズ スイッチと Cisco ASR 1000 シリーズ アグリゲーション サービス ルータの場合、このビューには、部品番号やシリアル番号などのラインカードとスーパーバイザカードの詳細が表示されます（カードが使用可能な場合）。

ステップ 5 トポロジビューでは、次のタスクを実行できます。

- error-disabled ポートのエラーの理由を表示するには、ポートをクリックします。
- 特定のイーサネットポートをフィルタ処理するには、[Color Code] ドロップダウンリストを使用します。次の表では、利用可能なドロップダウン リスト オプションについて説明します。

表 *11* : カラー コード ドロップダウン リスト オプション

名前	説明
Status	トポロジビューのデフォルトビューが表示されます。
Access VLANs	特定のポートに割り当てられているアクセス VLAN が表示されます。[Access VLANs] ビューでは、最大 5 つのアクセス VLAN を選択でき、ポートに関連付けられているアクセス VLAN のみが一覧表示されます。 このオプションでは、アクセス VLAN が [選択済み（Selected）]、[未設定（Not Configured）]、[デフォルト（Default）]、[VLAN] に色分けされて表示されます。
Port Channels	デバイスで設定されている上位 5 つのポートチャネルが表示されます。 このオプションでは、デバイスで設定されたポートチャネルのみが、[選択済み（Selected）] と [ポートチャネル（Port-channel）] で色分けされて対応する番号とともに表示されます。

ステップ 6 右上隅の [Table View]（ ）をクリックし、[Ports] テーブルを表示します。

[Ports] テーブルには、ポートの動作ステータスや管理ステータスなど、イーサネットポートの詳細が表示されます。

ステップ 7 （任意） [ポート名（Port name）]、[操作ステータス（Operational status）]、[タグ（Tags）] などのフィールドに値を入力して、[ポート（Ports）] テーブル内のデータを検索およびフィルタ処理します。絞り込まれた検索結果は、テーブル全体で一致する値が強調表示された状態で表示されます。

ステップ 8 （任意） テーブルビューでは、次のタスクを実行できます。

- [Tag] をクリックして、ポートにタグを付けたり、タグを検索したり、タグを管理したりします。

  詳細については、ポートへのタグの割り当て （207 ページ）を参照してください。
- [Export] をクリックし、[Ports] テーブルのデータをエクスポートします。

ポート詳細の管理

この手順を使用して、デバイスのポートの詳細を管理および編集します。

手順

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

ステップ 2 [Devices] テーブルからデバイス名をクリックし、[View Device Details] をクリックします。

ステップ 3 [詳細（Details）] をクリックします。

ステップ 4 左側のペインで [Interfaces] を展開し、[Ethernet Ports] を選択します。

ステップ 5 トポロジビュー（ ）で、ポートをクリックします。テーブルビュー（ ）で、ポート名をクリックします。

（注）
- Catalyst 2000、3000、および 9000 シリーズ スイッチの場合、ポート詳細にはポートの最大割り当て電力と消費電力が含まれます。
- このウィンドウには、CDP ネイバーの詳細が表示されます。CDP がない場合は、LLDP ネイバーの詳細が表示されます。CDP ネイバーと LLDP ネイバーの両方が存在しない場合、[ネイバーの詳細（Neighbor Details）] エリアは非表示になります。
- Cisco IOS XE リリース 17.12.x 以降を実行している Cisco Catalyst 9000 シリーズ スイッチおよび Cisco Catalyst IE スイッチの場合、ポートのデバイスごとの設定が表示されます。

ステップ 6 （任意） [タグ（Tag）] をクリックして、ポートにタグを付けたり、タグを検索したり、タグを管理したり、新しいタグを作成したりします。

詳細については、ポートへのタグの割り当て （207 ページ）を参照してください。

ステップ 7 （任意） ポートを管理するには、[ポート動作（Port Actions）] ドロップダウンリストをクリックし、次のオプションから選択します。

- ポートをシャットダウンしてポートの管理ステータスを [Down] に変更するには、[ポート閉塞（Port Shut）] を選択します。次に、[OK] をクリックして確定します。

  このオプションは、ポートが開いており、管理ステータスが [Up] の場合にのみ使用できます。

- ポートを開いてポートの管理ステータスを [Up] に変更するには、[ポート開通（Port No Shut）] を選択します。次に、[OK] をクリックして確定します。

  このオプションは、ポートが閉じており、管理ステータスが [Down] の場合にのみ使用できます。

- ポートの MAC アドレスをクリアするには、[MACアドレスをクリア（Clear Mac Address）] を選択します。

- エラー ディセーブルポートをアクティブにするには、MAC アドレスをクリアして、ポートをシャットダウンします。

（注）

- MAC アドレスをクリアしたり、ポートをシャットダウンしたりするには、デバイスソフトウェアタイプが Cisco IOS か Cisco IOS XE である必要があります。
- ワイヤレスコントローラ の場合、MAC アドレスのクリアとポートのシャットダウンはサポートされていません。
- MAC アドレスのクリアとポートのシャットダウンは、アクセスポートでのみサポートされています。
- ポートをシャットダウンすると、ポートのトラフィックが中断されます。

ステップ 8 [ポートの説明（Port Description）]エリアなどの特定のポート詳細を編集するには、次の表を使用します。

名前	説明
Access VLAN	[Edit]アイコンをクリックします。[Edit Access VLAN] ダイアログボックスで、ドロップダウンリストからアクセス VLAN を選択し、[Save] をクリックしてアクセス VLAN をポートに割り当てます。ポートで 2 つのアクセス VLAN が事前設定されている場合、そのアクセス VLAN を更新することはできません。
Voice VLAN	[Voice VLAN] の横にある [Edit] アイコンをクリックします。[Edit Voice VLAN] ダイアログボックスで、[Select Value] ドロップダウンリストから音声 VLAN を選択し、[Save] をクリックして音声 VLAN をポートに割り当てます。

名前	説明
Port Description	[ポートの説明（PORT DESCRIPTION）] の横にある [編集（Edit）] アイコンをクリックします。説明を入力します。[保存（Save）] をクリックします。[Okay] をクリックして、ポートに説明を追加します。 説明を削除するには、削除アイコンをクリックします。**[警告（Warning）]** ダイアログボックスにプロンプトが表示されたら、[Okay] をクリックします。

（注）
- VLAN の詳細とポートの説明を編集するには、デバイスソフトウェアタイプが Cisco IOS か Cisco IOS XE である必要があります。
- VLAN の詳細の編集は、アクセスポートでのみサポートされています。
- ワイヤレスコントローラの場合、VLAN の詳細の編集はサポートされていません。

ステップ 9 （任意）[設定（Configurations）] エリアで、[編集（Edit）] をクリックして、ポートのデバイスごとの設定を変更します。（Cisco Catalyst 9000 シリーズ スイッチおよび Cisco Catalyst IE スイッチの場合）

Cisco Catalyst スイッチのデバイスごとの設定を管理する

このセクションでは、Cisco Catalyst スイッチのデバイスごとの設定を表示および編集する方法について説明します。ここに示されている設定は、Cisco IOS XE リリース 17.12.x 以降が実行されている Cisco Catalyst 9000 シリーズ スイッチと Cisco Catalyst 産業用イーサネット（IE）スイッチでサポートされています。

（注）
- サポートされる設定は、デバイスモデルによって異なる場合があります。
- ネットワーク、ネットワークグループ、または Cisco SD-Access ファブリックネットワークの一部であるデバイスの設定は編集できません。
- サポートされる Cisco Catalyst IE スイッチ：
  - Cisco Catalyst IE3100 高耐久性シリーズ
  - Cisco Catalyst IE3100 Heavy Duty シリーズ
  - Cisco Catalyst IE3200 高耐久性シリーズ
  - Cisco Catalyst IE3300 高耐久性シリーズ
  - Cisco Catalyst IE3400 高耐久性シリーズ
  - Cisco Catalyst IE3400 Heavy Duty シリーズ
  - Cisco IE3500 高耐久性シリーズ
  - Cisco IE3500 Heavy Duty シリーズ
  - Cisco エンベデッド サービス 3300 シリーズ スイッチ
  - Cisco Catalyst IE9300 高耐久性シリーズ
  - Cisco Catalyst ESS9300 エンベデッド シリーズ スイッチ

Before you begin

インベントリにデバイスがあることを確認します。デバイスがない場合は検出機能を使用します。

デバイスが到達可能であることを確認します。

スイッチの設定を表示および管理するには、次の手順を実行します。

手順

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

[インベントリ（Inventory）] ウィンドウには、検出プロセス中に収集されたデバイス情報が表示されます。

ステップ 2 [Devices] テーブルからデバイス名をクリックし、[View Device Details] をクリックします。

ステップ 3 デバイスごとの設定を有効にします（まだ有効になっていない場合）。

[設定（Configuration）] ウィンドウで、[詳細（Learn more）] をクリックし、指示に従って、デバイスでデバイスごとの設定を有効にします。

ステップ 4 [**Configuration**] ウィンドウで、必要に応じてデバイス設定を表示および管理します。

次のオプションを使用して、設定の詳細ウィンドウに表示されるテーブルデータをソート、フィルタ処理、およびエクスポートします。

- 昇順または降順で列をソートするには、列ヘッダーをクリックします。
- 項目を検索するには、**[Search Table]** オプションを使用します。
- 値の任意の組み合わせでテーブル項目を表示するには、フィルタアイコンをクリックします。
- テーブルデータをエクスポートするには、**[Export]** をクリックします。
- テーブルをカスタマイズするには、設定アイコンをクリックします。

設定を編集または追加するには、設定の詳細ウィンドウで [**Edit**] アイコンをクリックします。

編集ウィンドウでは、次のオプションを使用できます。

- **[Reset]** および **[Set to Default]** オプションは、設定をリセットするか、デフォルト設定を復元します。
- [削除（Remove）] アイコンはフィールドから値を削除し、[削除（Delete）] アイコンは設定を削除します。
- [**Add Configurations**] をクリックして、追加の設定を行います。

デバイスのレイヤ 2 設定の表示と編集

スイッチのレイヤ 2 設定を表示および編集するには、次の手順を実行します。

手順

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

ステップ 2 [Devices] テーブルからデバイス名をクリックし、[View Device Details] をクリックします。

ステップ 3 レイヤ 2 設定の詳細を表示するには、次のいずれかのオプションを選択します。

- [レイヤ2（Layer 2）] エリアで、[レイヤ2の詳細の表示（View Layer 2 Details）] をクリックします。
- [設定（Configuration）] タブをクリックし、[レイヤ2設定（Layer 2 Configuration）] を展開します。

ステップ 4 レイヤ 2 設定の表示および編集の詳細については、表を参照してください。

- すべてのデフォルト設定を表示するには、[デフォルト設定をすべて表示（Show all default configurations）] トグルボタンをクリックします。
- 必要に応じて設定を編集または追加するには、設定の詳細ウィンドウで [編集（Edit）] アイコンをクリックします。

  編集ウィンドウでは、次のオプションを使用できます。

- **[Reset]** および **[Set to Default]** オプションは、設定をリセットするか、デフォルト設定を復元します。
- [削除（Remove）] アイコンはフィールドから値を削除し、[消去（Delete）] アイコンは設定を削除します。
- [**Add Configurations**] をクリックして、追加の設定を行います。

表 *12 :* レイヤ *2* の設定詳細

名前	説明
VLAN	サポートされている VLAN のリストを表示します。 詳細を表示するには、VLAN ID をクリックします。 VLAN を追加または編集するには、次のオプションを使用します。 • 新しい VLAN を追加するには、**[Add VLAN]** をクリックします。VLAN ID、VLAN 名を入力し、必要に応じて他の設定を追加します。 • VLAN を編集するには、VLAN ID の横にあるチェックボックスをオンにして、[編集（Edit）] をクリックします。必要に応じて設定の編集や他の設定の追加を行います。
検出プロトコル	検出プロトコル（CDP および LLDP）の詳細を表示します。 • [管理ステータス（Admin Status）]：検出プロトコルを有効または無効にします。 • [ホールド時間（Hold Time）]：ネイバーが CDP/LLDP 情報を保持する期間を決定します。 [CDP]：範囲は 10 ～ 255、デフォルト値は 180 です。 [LLDP]：範囲は 0 ～ 65535、デフォルト値は 120 です。 • [タイマー（Timer）]：CDP/LLDP パケットを送信する間隔。 [CDP]：範囲は 5 ～ 254、デフォルト値は 60 です。 [LLDP]：範囲は 5 ～ 65534、デフォルト値は 30 です。 • [アドバタイズメントバージョン（Advertisement version）]：CDP のバージョン（V1、V2）。デフォルト値は V2 です。 • [再初期化遅延（Reinitialization Delay）]：設定の変更またはリセット後に LLDP が再起動されるまでの時間の遅延。

名前	説明
STP	STP 設定の詳細を表示します。 • [モード（Mode）]：STP モード（Rapid-pvst、mst、pvst）。デフォルト値は Rapid-pvst です。 • [PortFastモード（Portfast Mode）]：デバイスの PortFast モードを有効化または無効化します。 • [BPDUフィルタ（BPDU Filter）]：PortFast ポートの BPDU フィルタリングを有効または無効にします。デフォルト値は[無効（Disabled）]です。 • [BPDUガード（BPDU Guard）]：PortFast ポートの BPDU ガードを有効または無効にします。デフォルト値は [無効（Disabled）] です。 • [バックボーンファスト（Backbonefast）]：間接的なリンク障害からの検出と回復を可能にするバックボーンファスト機能を有効または無効にします。デフォルト値は [無効（Disabled）] です。 • [ロギング（Logging）]：STP イベントのロギングを有効または無効にします。デフォルト値は [無効（Disabled）] です。 • [アップリンクファスト（Uplinkfast）]：リンク障害後の接続の回復を高速化する Uplinkfast 機能を有効または無効にします。デフォルト値は [無効（Disabled）] です。 • [ループガード（Loopguard）]：STP の Loopguard を有効または無効にします。ループガードは、BPDU の予期しない損失から保護します。デフォルト値は [無効（Disabled）] です。 • [送信保留カウント（Transmit Hold Count）]：秒あたりに送信された BPDU の数。有効な範囲は、1 ～ 20 秒です。デフォルト値は、6 です。 • [アップリンクファストの最大更新レート（Uplinkfast Max Update Rate）]：アップリンクファストの最大更新レート（パケット数/秒）。有効な範囲は 0 ～ 32000 です。デフォルトは 150 です。
VTP	VTP の詳細を表示します。 • [バージョン（Version）]：VTP バージョン（V1、V2、V3）。デフォルト値は V1 です。 • [VTPモード（VTP Mode）]：デバイスの VTPモード（クライアント、サーバー、トランスペアレント、オフ）。デフォルト値は「サーバー」です。 • [ドメイン名（Domain Name）]：VTP ドメイン名。最大長は 32 文字です。

名前	説明
IGMP スヌーピング	IGMP スヌーピングの詳細を表示します。 • [管理ステータス（Admin Status）]：IGMP スヌーピングを有効または無効にします。 • [クエリア（Querier）]：クエリア機能の IGMP スヌーピングを有効または無効にします。 • [クエリアアドレス（Querier Address）]：IGMP クエリアの IP アドレス。 • [クエリアクエリ間隔（Querier Query Interval）]：IGMP クエリの間隔。有効な範囲は 1 ～ 18000 です。デフォルト値は 60 です。 • [クエリアバージョン（Querier Version）]：クエリアによって使用される IGMP バージョン。有効な範囲は V1、V2、V3 です。デフォルト値は V2 です。 • [最後のメンバークエリ間隔（ミリ秒）（Last Member Query Interval (msec)）]：IGMP 最後のメンバークエリの間隔。この値はミリ秒単位です。有効な範囲は 100 ～ 32767 です。デフォルト値は 1000 です。
MLD スヌーピング	MLD スヌーピングの詳細を表示します。 • [管理ステータス（Admin Status）]：MLD スヌーピングを有効または無効にします。 • [MLDクエリ間隔（ミリ秒）（MLD Query Interval (msec)）]：MLD の最後のリスナーの間隔。この値はミリ秒単位です。有効な範囲は100 ～ 32768 です。デフォルト値は 1000 です。
UDLD	UDLD の詳細を表示します。 • [管理ステータス（Admin Status）]：UDLD を有効または無効にします。 • [アグレッシブ（Aggressive）]：UDLD のアグレッシブモードを有効または無効にします。 • [メッセージ間隔（Message Interval）]： UDLD メッセージの間隔。値は秒単位です。有効な範囲は 1 ～ 90 です。デフォルト値は 15 です。 • [リカバリ（Recovery）]：UDLD のリカバリを有効または無効にします。 • [リカバリ間隔（Recovery Interval）]：UDLD リカバリの間隔。値は秒単位です。有効な範囲は 30 ～ 86400 です。デフォルト値は 3000 です。

名前	説明
MAC アドレステーブル	MAC アドレスエージングや通知設定などの MAC アドレステーブル設定を表示します。 • [エージング時間（Aging Time）]：テーブルから削除する前に、MAC アドレスを保持する時間を指定します。 • [変更通知（Change Notification）]：MAC アドレステーブルの変更の通知を有効または無効にします。 • [通知しきい値（Notification Threshold）]：MAC アドレステーブルのしきい値に基づく通知を有効または無効にします。 • [MAC移動通知（MAC Move Notification）]：インターフェイス間の MAC アドレス移動の通知を有効または無効にします。 • [通知しきい値間隔（Notification Threshold Interval）]：MAC アドレステーブルのしきい値ベースの通知の間隔。値は秒単位です。有効な範囲は 120 ～ 1000000 です。デフォルト値は 120 です。 • [通知制限パーセンテージ（Notification Limit Percentage）]：MAC アドレステーブル通知のパーセンテージしきい値。有効な範囲は 0 ～ 100 です。デフォルト値は 50 です。
EtherChannel	ポートチャネル設定を表示します。 • [システム優先順位（System Priority）]：LACP（Link Aggregation Control Protocol）のシステム優先順位。有効な範囲は 0 ～ 65535 です。デフォルト値は 32768 です。 • [ロードバランシング方式（Load Balance Method）]：ポートチャネルのロードバランシング方式。

次のオプションを使用して、設定の詳細ウィンドウに表示されるテーブルデータをソート、フィルタ処理、およびエクスポートします。

- 昇順または降順で列をソートするには、列ヘッダーをクリックします。
- 項目を検索するには、**[Search Table]** オプションを使用します。
- 値の任意の組み合わせでテーブル項目を表示するには、フィルタアイコンをクリックします。
- テーブルデータをエクスポートするには、**[Export]** をクリックします。
- テーブルをカスタマイズするには、設定アイコンをクリックします。

ステップ 5 必要な設定を編集したら、[次へ（Next）] をクリックします。

ステップ 6 展開のためのタスクのスケジュールを設定します。

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

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

ステップ 7 [Tasks] ウィンドウで、タスクの展開を監視します。

デバイスのレイヤ 3 設定の表示と編集

レイヤ 3 設定を表示および管理するには、次の手順を実行します。

手順

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

ステップ 2 デバイス名をクリックして、[デバイスの詳細の表示（View Device Details）] を選択します。

ステップ 3 レイヤ 3 設定の詳細を表示するオプションを選択します。

- [概要（Summary）] の [レイヤ3（Layer 3）] エリアで、[レイヤ3の詳細の表示（View Layer 3 Details）] をクリックします。
- [設定（Configuration）] をクリックし、[レイヤ3（Layer 3）] を展開します。

ステップ 4 設定の詳細を表示および変更するには、テーブルを参照してください。

表 *13 :* レイヤ *3* 設定の詳細

名前	説明
VRF	デバイスに設定されている IPv4 および IPv6 VRF を表示します。 **IPv4 VRF** • [VRF名（VRF Name）]：VRF インスタンスの名前。 • [**Route Distinguisher**]：異なる VRF 内のルートを区別するための一意の識別子。 • [Route-Target]：設定された VRF ルートターゲットの数。 [IPv4/IPv6 VRF] • [VRF名（VRF Name）]：VRF インスタンスの名前。 • [**Route Distinguisher**]：異なる VRF 内のルートを区別するための一意の識別子。 • [IPv4]：ルーティングおよびアドレス割り当て用の IPv4 を有効または無効にします。 • [IPv6]：ルーティングおよびアドレス割り当て用の IPv6 を有効または無効にします。

名前	説明
ループバック	デバイスに設定されているループバックインターフェイスを表示します。インターフェイスの詳細を表示するには、ループバック番号を選択します。 • [ループバック番号（Loopback Number）]：ループバック インターフェイスの識別子。 • [説明（Description）]：インターフェイスのテキストの説明。 • [IPv4アドレス（IPv4 Address）]：インターフェイスに割り当てられている IPv4 アドレス。 • [IPv4サブネットマスク（IPv4 Subnet Mask）]：IPv4 アドレスのサブネットマスク。 • [IPv6]：インターフェイスで IPv6 を有効または無効にします。 • [IPv4/IPv6 VRF名（IPv4/IPv6 VRF Name）]：インターフェイスの IPv4/IPv6 VRF 名。 • [IPv4 VRF名（IPv4 VRF Name）]：インターフェイスの IPv4 VRF 名。 • [BFD]：インターフェイスで Bidirectional Forwarding Detection（BFD）を有効または無効にします。 • [BFDテンプレート（BFD Template）]：インターフェイスに適用される BFD テンプレートの名前。 • [BFD間隔ステータス（BFD Interval Status）]：BFD 間隔設定を有効または無効にします。

名前	説明
SVI	デバイスに設定されているスイッチ仮想インターフェイス（SVI）の詳細を表示します。インターフェイスの詳細を表示するには、VLAN 番号を選択します。 • [VLAN番号（VLAN Number）]：インターフェイスの識別子。有効な範囲は 1 ～ 4094 です。 • [説明（Description）]：インターフェイスのテキストの説明。 • [IPアドレスタイプ（IP Address Type）]：インターフェイスに割り当てられている IPv4 アドレス。 • [IPv6]：インターフェイスで IPv6 を有効または無効にします。 • [IPv4/IPv6 VRF名（IPv4/IPv6 VRF Name）]：インターフェイスの IPv4/IPv6 VRF 名。 • [IPv4 VRF名（IPv4 VRF Name）]：インターフェイスの IPv4 VRF 名。 • [管理ステータス（Admin Status）]：インターフェイスを有効または無効にします。 • [BFD]：インターフェイスで Bidirectional Forwarding Detection（BFD）を有効または無効にします。 • [BFDテンプレート（BFD Template）]：インターフェイスに適用される BFD テンプレートの名前。 • [BFD間隔ステータス（BFD Interval Status）]：BFD 間隔設定を有効または無効にします。
ルーティング	デバイスのユニキャストルーティング設定を表示します。 • [**IPv4 Unicast Routing**]：IP ルーティングをグローバルに有効化または無効化します。有効にすると、デバイスはルーティングテーブルに基づいてネットワーク間でパケットを転送できるため、ネットワーク間通信がサポートされます。 • [**IPv6 Unicast Routing**]：IPv6 ユニキャストルーティングをグローバルに有効にします。有効にすると、デバイスはルーティングテーブルに基づいてネットワーク間でIPv6パケットを転送できるため、ネットワーク間 IPv6 通信がサポートされます。

名前	説明
スタティック ルート	デバイスに設定されているスタティックルートを表示します。 • [IPv4] スタティックルート。 • [プレフィックス（Prefix）]：スタティックルートのIPプレフィックス。 • [プレフィックスマスク（Prefix Mask）]：スタティックルートのサブネットマスク。 • [転送リスト（Forwarding list）]：スタティックルートの転送リストの数。 • [IPv4 Per-VRF名（IPv4 Per-VRF Name）] スタティックルート： • [VRF名（VRF Name）]：スタティックルートの VRF 名。 • [転送リスト（Forward list）]：スタティックルートの転送リストの数。 • [IPv6]： • [VRF名（VRF Name）]：スタティックルートの VRF 名。 • [転送リスト（Forward list）]：スタティックルートの転送リストの数。 • [IPv6 Per-VRF名（IPv6 Per-VRF Name）] スタティックルート • [プレフィックス（Prefix）]：スタティックルートのIPプレフィックス。 • [転送リスト（Forwarding list）]：スタティックルートの転送リストの数。

名前	説明

BFD	デバイスに設定されている BFD プロトコルの詳細を表示します。
	• [IPv6 L3 CoS]：BFD パケットの IPv6 レイヤ 3 サービスクラス（CoS）値。
	• [その他のSNMPトラップ（More SNMP Traps）]：BFD イベントのその他の SNMP トラップを有効または無効にします。
	• [**BFD Template Single Hop**]
	  • [名前（Name）]：テンプレートの名前。
	  • [エコー（Echo）]：BFDエコー機能を有効または無効にします。
	  • [最小送信間隔（Minimum Transmit Interval）]：送信される BFD パケット間の最小間隔。
	  • [最小受信間隔（Minimum Receive Interval）]：受信される BFD パケット間の最小間隔。
	  • [間隔乗数（Interval Multiplier）]：障害がトリガーされる前に受信できなかった BFD パケットの数。
	  • [認証キーチェーン（Authentication Keychain）]：BFD シングルホップテンプレートで認証に使用されるキーチェーン名。

DHCP リレー	DHCPリレー情報オプションを表示します。 • [すべての情報を信頼（Trust All Information）]：すべてのリレー情報の受け入れを有効または無効にするオプション。 • [情報オプションの挿入（Insert Information Option）]：デフォルトのリレー情報オプションを有効または無効にします。 • [VPNサブオプションの挿入（Insert VPN suboption）]：DHCP リレーメッセージに VPN 関連情報を含めるオプションを有効または無効にします。

ステップ 5 [編集（Edit）] アイコンをクリックして設定を更新します。

ステップ 6 必要な設定を編集したら、[次へ（Next）] をクリックします。

ステップ 7 展開のためのタスクのスケジュールを設定します。

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

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

ステップ 8 [Tasks] ウィンドウで、タスクの展開を監視します。

デバイスのセキュリティ設定の表示および編集

スイッチのセキュリティ設定を表示および管理するには、次の手順を実行します。

始める前に

インベントリにデバイスがあることを確認します。デバイスがない場合は検出機能を使用します。

デバイスが到達可能であることを確認します。

スイッチ設定を管理するには、デバイスごとの設定を有効にする必要があります。[設定（Configuration）] ウィンドウで、[詳細（Learn more）] をクリックし、手順に従って、デバイスでデバイスごとの設定を有効にします。

手順

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

ステップ 2 デバイス名をクリックして、[デバイスの詳細の表示（View Device Details）] を選択します。

ステップ 3 セキュリティ設定の詳細を表示するオプションを選択します。

- [セキュリティ（Security）]エリアの [概要（Summary）] で、[セキュリティの詳細の表示（View Security Details）] をクリックします。
- [設定（Configuration）] タブをクリックし、[セキュリティ（Security）] を展開します。

ステップ 4 設定の詳細を表示および変更するには、テーブルを参照してください。

名前	説明
ACL	IPv4 ACL、MAC ACL、IPv6 ACL などの ACL のリストを表示します。 • **IPv4 拡張アクセスリスト** • **IPv4 標準アクセスリスト** • **IPv4 ロールベースアクセスリスト** • **MAC アクセスリスト** • **IPv6 アクセスリスト** • **IPv6 ロールベースアクセスリスト**

名前	説明
認証	認証設定を表示します。 • [管理ステータス（Admin Status）]：802.1x 認証モードを有効または無効にします。 • [詳細なロギング（Verbose Logging）]：802.1x 認証イベントの詳細なロギングを有効または無効にします。 • [802.1xログイン情報（802.1x Credentials）]：802.1x 認証情報。
DHCP スヌーピング	ステータス、DHCP スヌーピング VLAN、その他のデフォルト設定など、DHCP スヌーピングの詳細を表示します。 • [スヌーピング（Snooping）]：DHCP スヌーピングを有効または無効にします。 • [グリーニング（Glean）]：DHCP スヌーピング情報のグリーニングを有効または無効にします。 • [情報オプション（Information Option）]：DHCP スヌーピング情報のオプション。 • [DHCPスヌーピングVLAN（DHCP Snooping VLANs）]：DHCP スヌーピング VLAN の数。

名前	説明
CTS	Cisco TrustSec の詳細を表示します。 • [デバイスSGT（Device SGT）]：着信トラフィックの SGT 番号。有効な範囲： • 2 ～ 65519（IOS XE 17.6 以降の場合）。 • 2 ～ 65521（IOS XE 17.6 以前の場合）。 • [認可リスト名（Authorization List Name）]：Cisco TrustSec グローバル承認。 • [適用（Enforcement）]：ロールベース アクセス コントロールを有効または無効にします。デフォルトでは、無効に設定されています。 • [SGT VLANマップ（SGT VLAN Map）]：SGTからVLANへのマッピングの数を表示します。数字をクリックすると、SGTとマッピングされた VLAN が表示されます。 • [適用VLAN（Enforcement VLANs）]：SGACL ポリシーが有効になっているVLANのリストを表示します。
ARP インスペクション	ARP インスペクション VLAN を表示します。 VLAN の有効な範囲は 1 ～ 4094 です。
デバイス トラッキング	トラッキングが有効か無効かを表示し、トラッキングポリシーを一覧表示します。デフォルトでは、デバイストラッキングは無効になっています。

ステップ 5 [編集（Edit）] アイコンをクリックして設定を更新します。

（注） ネットワーク、ネットワークグループ、または Cisco SD-Access ファブリックネットワークの一部であるデバイスの設定は編集できません。

ステップ 6 必要な設定を編集したら、 [次へ（Next）] をクリックします。

ステップ 7 展開のためのタスクのスケジュールを設定します。

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

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。

- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238ページ）を参照してください。

ステップ 8 [Tasks] ウィンドウで、タスクの展開を監視します。

デバイスのネットワーク設定の表示と編集

スイッチで構成されているネットワーク設定を表示および管理するには、次の手順を実行します。

Before you begin

インベントリにデバイスがあることを確認します。デバイスがない場合は検出機能を使用します。

デバイスが到達可能であることを確認します。

スイッチ設定を管理するには、デバイスごとの設定を有効にする必要があります。[設定（Configuration）] ウィンドウで、[詳細（Learn more）] をクリックし、手順に従って、デバイスでデバイスごとの設定を有効にします。

手順

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

ステップ 2 デバイス名をクリックして、[デバイスの詳細の表示（View Device Details）] を選択します。

ステップ 3 デバイスで構成されているネットワーク設定を表示するオプションを選択します。

- [ネットワーク設定（Network Settings）] エリアの [概要（Summary）] で、[ネットワーク設定の表示（View Network Settings）] をクリックします。
- [設定（Configuration）] をクリックし、[ネットワーク設定（Network Settings）] を展開します。

ステップ 4 設定の詳細を表示および変更するには、テーブルを参照してください。

表 *14 :* ネットワーク設定（***Network settings***）

名前	説明
NTP	

名前	説明

	デバイスに設定されているNTP設定を表示します。
	• [認証（Authenticate）]：NTP 認証を有効または無効にします。デフォルトでは、無効になっています。
	• [ロギング（Logging）]：NTP イベントのロギングを有効または無効にします。デフォルトでは、無効になっています。
	• [ストラタム番号（Stratum Number）]：NTP マスター設定のストラタム番号。有効な範囲は 1 ～ 15 です。デフォルト値は 8 です。
	• [**Source Loopback Interface**]：NTP パケットのループバック インターフェイス。有効な範囲は 0 ～ 2147483647 です。
	• [NTPサーバー（NTP Servers）]：NTP サーバーのリスト。
	  • [NTPサーバーアドレス（NTP Server Address）]：NTP サーバーの IPv4 または IPv6 アドレス。
	  • [ピア認証キー（Peer Authentication Key）]：NTP サーバーの認証キー番号。
	  • [優先（Preferred）]：NTP サーバーを優先サーバーとして有効または無効にするオプション。
	• [VRFサーバーごとのNTP（NTP Per VRF Server）]：VRF サーバーごとの NTP のリスト。
	  • [VRF]：NTP サーバーの VRF 名。最大長は 32 文字です。
	  • [NTPサーバー（NTP Servers）]：VRF に関連付けられている NTP サーバーの数。
	• [NTP信頼キー（NTP Trusted Key）]：NTP 認証用の信頼できるキー番号。有効範囲は1～65535です。
	• [NTP認証 キー（NTP Authentication Key）]：
	  • 認証キー番号：NTP 認証のキー番号。有効な範囲は 1 ～ 4294967295 です。

名前	説明
	• 認証キー：NTP 認証キーの MD5 設定文字列。最大長は 32 文字です。
DNS	DNS ルックアップステータス、デフォルトドメイン名、DNS サーバーのリストなどの DNS 設定を表示します。 • [DNSルックアップ（DNS Lookup）]：DNS ドメインルックアップを有効または無効にします。 • [DNSクエリタイムアウト（DNS Query Timeout）]：DNS の試行が失敗とみなされるまでの DNS 応答の待機時間を指定します。 • [デフォルトドメイン名（Default Domain Name）]：ドメインコンテナ名。 • [VRFごとのデフォルトドメイン名（Per VRF Default Domain Name）]：IP ドメインの数（VRF）。 • [デフォルトドメイン名リスト（Default Domain Name List）]：DNS 解決用のドメイン名。 • [送信元ループバックインターフェイス（Source Loopback Interface）]：DNS ルックアップの送信元として使用されるループバックインターフェイス。 • [DNSサーバー（DNS Servers）]：DNS サーバーの IP アドレスのリスト。 • [VRFごとのDNSサーバー（Per VRF DNS Servers）]：VRF ごとの DNS サーバーの数。

名前	説明
DHCP	

名前	説明
	Ignore BOOTP、IPv4 および IPv6 DHCP プール、DHCP の除外アドレスなど、DHCP 設定を表示します。 • [**Ignore BOOTP**]：DHCP 処理で BOOTP パケットを無視する場合は有効にします。 • [IPv4 DHCPプール（IPv4 DHCP Pools）]：IPv4 DHCP プールのリスト。 • [**DHCP Pool Name**]：DHCP プールの一意の識別子。 • [**Network**]：プライマリ DHCP プールのネットワーク番号。 • [**Subnet Mask**]：プライマリ DHCP プールネットワークのサブネットマスク。 • [**VRF Name**]：DHCP プールの VRF 名。論理的なネットワークのセグメンテーションを有効にします。 • [**DNS Server**]：DHCP クライアントの DNS サーバー IP アドレスのリスト。 • [IPv6 DHCPプール（IPv6 DHCP Pools）]：IPv6 DHCP プールのリスト。 • [**DHCP Pool Name**]：DHCPv6 プールの名前。 • [**DNS Server**]：DHCPv6 クライアントの DNS サーバー IPv6 アドレスのリスト。IPv6 名前解決のためにクライアントに提供する、1 つまたは複数の DNS サーバーを指定します。 • [**DNS Default Domain Name**]：DHCPv6 クライアントに割り当てられるドメイン名のリスト。 • [除外アドレス（Excluded Addresses）]：DHCP の除外アドレスのリスト。 • [**Excluded Address Low**]：DHCP 割り当ての除外範囲における最小の IP アドレス。これは、DHCP によって割り当てられないアドレスブロックの起点を示します。

名前	説明
	• [**Excluded Address High**]：DHCP 割り当てから除外する最大の IP アドレス。予約済みアドレスの除外範囲の上限を定義するにはこれを使用します。 • [**Excluded Low Addresses**]：このタブで、[**Excluded Address Low**] は、DHCP 割り当てから除外する最小の IP アドレスを示します。クライアントに割り当ててはならないアドレスを予約するには、これを使用します。 （注） DHCP プールオプションを追加するときは、サポートされているオプションコードのみを含めることができます。

ステップ 5 [編集（Edit）] アイコンをクリックして設定を更新します。

（注） ネットワーク、ネットワークグループ、または Cisco SD-Access ファブリックネットワークの一部であるデバイスの設定は編集できません。

ステップ 6 必要な設定を編集したら、[次へ（Next）] をクリックします。

ステップ 7 展開のためのタスクのスケジュールを設定します。

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

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

ステップ 8 [Tasks] ウィンドウで、タスクの展開を監視します。

デバイスの産業用設定の表示および編集

Cisco IOS XE リリース 26.1 移行を実行している、Cisco Catalyst 産業用イーサネット（IE）スイッチの産業用設定を表示および編集するには、次の手順を実行します。

始める前に

スイッチ設定を管理するには、デバイスごとの設定を有効にする必要があります。[設定（Configuration）] ウィンドウで、[詳細（Learn more）] をクリックし、手順に従って、デバイスでデバイスごとの設定を有効にします。

手順

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

ステップ 2 [Devices] テーブルからデバイス名をクリックし、[View Device Details] をクリックします。

デバイスの詳細が表示されます。[産業用（Industrial）] エリアには、デバイスの産業設定の概要が表示されます。

ステップ 3 産業用設定の詳細を表示するには、次のいずれかのオプションを使用します。

- [産業用（Industrial）] 設定エリアで、[産業用設定の詳細を表示（View Industrial Configuration Details）] をクリックします。
- [設定（Configuration）] タブをクリックし、[産業用（Industrial）] を展開します。

ステップ 4 設定の詳細を表示および変更するには、テーブルを参照してください。

名前	説明
CIP	Common Industrial Protocol（CIP）の詳細を表示します。 • [セキュリティパスワード（Security Password）]：CIP セキュリティパスワード。パスワードの長さは 1 ～ 32 文字にしてください。 • [ウィンドウタイムアウト（Window Timeout）]：タイムアウト時間が経過すると、CIP セッションがシャットダウンします。有効な範囲は 1 ～ 3600 秒で、デフォルト値は 600 秒です。 • [カプセル化非アクティブタイムアウト（Encap Inactivity Timeout）]：CIP 下のスイッチでセッションタイムアウトを共有します。有効な値の範囲は 0 ～ 3600 秒です。デフォルト値は 120 秒です。

名前	説明
PROFINET	次の Profinet の詳細を表示します。 • [Profinetを有効化（Enable Profinet）]：Profinet のステータス（有効または無効）を表示します。デフォルトでは有効になっています。 • [**Profinet** VLAN ID]：Profinet の VLAN。デフォルトの VLAN ID は 1 です。 • [MRPを有効化（Enable MRP）]：MRP のステータス（有効または無効）を表示します。デフォルトでは有効になっています。
Modbus	Modbus 設定の詳細を表示します。 • [TCP接続の数（Number of TCP connections）]：サポートされている並列TCP接続の数を表示します。有効な範囲は 1 ～ 5 です。デフォルト値は 1 です。 • [ポート番号（Port Number）]：TCP ポート番号。有効な範囲は 1 ～ 65535 です。デフォルト値は 502 です。 • [Modbusステータス（Modbus Status）]：デバイスの Modbus ステータス（有効または無効）を表示します。デフォルトでは、無効です。

名前	説明

Alarm	デバイスのアラーム設定を表示します。
	• [アラーム機能（Alarm Facility）]：デバイスでサポートされているアラーム機能を表示します。デバイスモデルによって、サポートされるアラーム機能が決まります。
	  • [編集（Edit ）] を使用してアラーム機能の設定を変更します。
	• [アラームコンタクト（Alarm Contact）]：デバイスでサポートされているアラームコンタクトを表示します。
	  • 数字をクリックすると、コンタクトの詳細が表示されます
	  • [編集（Edit ）] を使用して設定を変更します。
	• [アラームプロファイル（Alarm Profile）]：デバイスでサポートされているアラームプロファイルを表示します。
	  • [プロファイル名（profile name）] をクリックすると、プロファイルの詳細が表示されます。
	  • [編集（Edit ）] を使用して設定を変更します。

L2 NAT	レイヤ2ネットワークアドレス変換（L2 NAT）インスタンスを、各 L2 NAT インスタンスのフィックスアップと許可タイプを含めて表示します。インスタンス名をクリックすると、変換設定が表示されます。

ステップ 5 [編集（Edit）] をクリックして、設定を追加または更新します。

ステップ 6 必要な設定を編集したら、[次へ（Next）] をクリックします。

ステップ 7 展開のためのタスクのスケジュールを設定します。

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

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。

- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238ページ）を参照してください。

ステップ 8 [Tasks] ウィンドウで、タスクの展開を監視します。

デバイスのポート設定の表示と編集

ポート設定を表示および管理するには、次の手順を使用します。

手順

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

ステップ 2 デバイス名をクリックして、[デバイスの詳細の表示（View Device Details）] を選択します。

ステップ 3 [設定（Configuration）] をクリックし、[ポート（Port）] を展開します。

[概要（Summary）] タブでも、ポートの詳細を表示および管理できます。ポート詳細の管理（121ページ）を参照してください。

ステップ 4 設定の詳細を表示および変更するには、テーブルを参照してください。

表 *15 :* ポート設定の詳細

名前	説明
ポートチャネル	次の詳細を含むサポートされているポートチャネルのリストを表示します。 • [ポートチャネル番号（Portchannel Number）]：ポート チャネル インターフェイスの識別子。 • [説明（Description）]：インターフェイスを説明するテキスト。 • [管理ステータス（Admin Status）]：ポート チャネル インターフェイスを有効または無効にするオプション。 • [レイヤ3（Layer 3）]：インターフェイスでスイッチポートモードを有効または無効にするオプション。 [トランクで許可されるVLAN（Trunk Allowed VLANs）]：ポート チャネル インターフェイスのトランクで許可される VLAN のリスト。 ポートチャネル名をクリックすると、詳細が表示されます。 ポートチャネルを追加するには、次の手順に従います。 **1.** [編集（Edit）] をクリックします。 **2.** [Add] をクリックします。 **3.** [ポートチャネルの追加（Add Port Channel）] ウィンドウで、[ポートチャネル番号（Portchannel Number）] を入力し、必要に応じてその他のフィールドを設定します。 **4.** [Save] をクリックします。

名前	説明
イーサネット ポート	次の詳細を含むデバイスに設定されているイーサネットポートのリストを表示します。 • [ポート名（Port Name）]：イーサネットポート名。 • [レイヤ3（Layer 3）]：インターフェイスでスイッチポートモードを有効または無効にするオプション。 • [説明（Description）]：ポートを説明するテキスト。 • [管理ステータス（Admin Status）]：インターフェイスを有効または無効にするオプション。 • [トランクで許可されるVLAN（Trunk Allowed VLANs）]：インターフェイスのトランクで許可される VLAN のリスト。

ステップ 5 [編集（Edit）] アイコンをクリックして設定を更新します。

ステップ 6 必要な設定を編集したら、[次へ（Next）] をクリックします。

ステップ 7 展開のためのタスクのスケジュールを設定します。

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

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

ステップ 8 [Tasks] ウィンドウで、タスクの展開を監視します。

インベントリ ユーザー インターフェイスの機能強化

機能拡張された Catalyst Center のインベントリ ユーザー インターフェイスは、既存のインベントリ機能を備えています。また、ユーザー体験を向上させる改善されたフィルタと更新されたレイアウトも含まれています。

始める前に

インベントリにデバイスがあることを確認します。デバイスがない場合は検出機能を使用します。

手順

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

機能拡張された [インベントリ（Inventory）] ウィンドウがデフォルトで表示され、検出プロセス中に収集されたデバイス情報が表示されます。

ステップ 2 上部メニューバーの場所オプションをクリックします。次に、ネットワーク階層から、デバイスを管理するサイト、ビルディング、またはフロアを選択します。

ステップ 3 [インベントリ（Inventory）] ウィンドウの上部に表示されるデバイスファミリエリアを使用して、1 つ以上のデバイスファミリを選択します。

選択できるデバイスファミリは、[ルータ（Routers）]、[スイッチ（Switches）]、[ワイヤレスコントローラ（Wireless Controllers）]、[アクセスポイント（Access Points）]、[センサー（Sensors）] です。

ステップ 4 [Focus] ドロップダウンリストを使用すると、[Inventory] 、[Default] 、[Software Image] 、[Provision] 、[Security] 、または [Device Replacement] に基づいてデバイスをフィルタ処理できます。

ステップ 5 [Device] テーブルの左隅にある分割バーを使用すると、テーブルの表示を調整できます。

ステップ 6 デバイスを絞り込むには、[DEVICE WORK ITEMS] 領域で、フィルタする条件を1 つ以上指定します。

ステップ 7 [デバイスの追加（Add Device）] をクリックし、新しいデバイスをインベントリに追加します。詳細については、「Catalyst Center インベントリへのデバイスの追加 （155 ページ）」を参照してください。

ステップ 8 デバイスにタグを付けるには、[Tag] を使用します。詳細については、[Inventory] ウィンドウでのデバイスの管理 （189 ページ）を参照してください。

ステップ 9 [アクション（Action）] ドロップダウンリストを使用して、1 つ以上のデバイスでアクションを実行します。

ステップ 10 動作のリストとそれぞれの内容は、[i] アイコンをクリックしてください。

ステップ 11 インベントリテーブルを編集またはカスタマイズするには、テーブルの右上隅にある歯車アイコンをクリックして次の手順を実行します。

1. [Table Appearance] で、[Table Density] と [Table Striping] を設定します。
2. [Edit Table Columns] で、検出プロセスでインベントリテーブルに含めたいデバイス情報を選択します。
3. [Edit Custom Views] でビューの設定をカスタマイズできます。
4. [Apply] をクリックして変更を保存するか、[Reset All Settings] をクリックしてインベントリテーブルをデフォルト設定に戻します。

ステップ 12 デバイステーブルに更に詳細なフィルタ設定を行うには[Filter Devices] オプションを使います。詳細については、「デバイスのフィルタ」デバイスのフィルタリング （187 ページ）を参照してください。

ステップ 13 右上隅にあるトグルボタンをクリックすると、[Dashboard] 、[Table] 、[Topology] 、[Map] の各ビュー間で切り替えることができます。

ステップ 14 過去のインベントリウィンドウを見るには [Go to old page] をクリックします。

ステップ 15 デバイステーブルの全てのデータをエクスポートするには、[Export] をクリックします。

ユーザー定義フィールドの管理

ユーザー定義フィールドはカスタムラベルです。これらのラベルを作成し、Catalyst Center の任意のデバイスに割り当てることができます。これらのラベルを使用すると、デバイスに関するより多くの詳細情報を表示できます。ユーザー定義フィールドをデバイスに割り当てて値を追加すると、詳細が表示されます。

ユーザー定義フィールドの作成

Catalyst Center では、ユーザー定義フィールドを作成し、任意のデバイスに割り当てることができます。

手順

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

[Inventory] ウィンドウには、検出プロセス中に収集されたデバイス情報が表示されます。

ステップ 2 [Devices] テーブルでデバイスの名前をクリックしてから、[View Device Details] をクリックします。

ステップ 3 [詳細（Details）] をクリックしてから [ユーザー定義フィールド（User Defined Fields）] をクリックします。

ステップ 4 [ユーザー定義フィールドの管理（Manage user defined fields）] をクリックします。

ステップ 5 [新しいフィールドの作成（Create new field）] をクリックします。

ステップ 6 [新しいフィールドの作成（Create new field）] ダイアログボックスで、フィールドの名前と説明を入力します。

（注） お客様の IP アドレスやお客様のデバイス名など、[デバイスの詳細（Device Details）] ウィンドウにまだ表示されていないデバイスの詳細を追加できます。

ステップ 7 [Save] をクリックします。

さらにユーザー定義フィールドを作成するには、[新しいフィールドの作成（Create new field）] を再度クリックします。

ステップ 8 （任意） ユーザー定義フィールドを編集するには、[編集（Edit）] をクリックして必要な変更を行い、[保存（Save）] をクリックします。

ステップ 9 （任意） ユーザー定義フィールドを削除するには、[削除（Delete）] をクリックして確定します。

デバイスへのユーザー定義フィールドの追加

始める前に

[Manage User Defined Fields] ウィンドウで少なくとも 1 つのユーザー定義フィールドを作成しておく必要があります。詳細については、ユーザー定義フィールドの作成（153ページ）を参照してください。

手順

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

ステップ 2 ユーザー定義フィールドを追加するデバイスの名前をクリックし、**[View Device Details]** をクリックします。

ステップ 3 左側のペインで、[User Defined Fields] をクリックします。

ステップ 4 **[Add User Defined field]** をクリックします。

ステップ 5 [Field Name] ドロップダウンリストでユーザー定義フィールドを選択し、[Value] フィールドにその値を入力します。

たとえば、お客様の IP アドレスのユーザー定義フィールドを作成した場合、[Field Name] ドロップダウンリストからそのフィールドを選択し、[Value] フィールドにお客様の IP アドレスを入力します。

ステップ 6 （任意） デバイスからユーザー定義フィールドを削除するには、対応する削除アイコンをクリックします。

ステップ 7 [Save] をクリックします。

インベントリからのトポロジマップの起動

[Inventory] ウィンドウから、検出されたデバイスのトポロジマップを起動できます。

手順

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

ステップ 2 トグルボタン（）を使用して、トポロジマップビューとインベントリビューを切り替えます。トポロジマップビューには、デバイスのトポロジとプロビジョニングステータスが表示されます。各ノードをクリックすると、デバイスの詳細が表示されます。トポロジマップの詳細については、「トポロジについて （259 ページ）」を参照してください。

（注） トポロジマップビューを折りたたむには [Collapse all] を、展開するには [expand all] をクリックします。

Catalyst Center インベントリ内のデバイスのタイプ

デバイスは、検出または手動追加のいずれかの方法でインベントリに表示されます。Catalyst Center インベントリは、次のようなさまざまなタイプのデバイスをサポートしています。

- **ネットワークデバイス**：サポート対象のネットワークデバイスには、シスコルータ、スイッチ、およびワイヤレスコントローラやアクセスポイント（AP）などのワイヤレスデバイスが含まれます。
- **計算デバイス**：サポート対象の計算デバイスには、Cisco Unified Computing System（UCS）、シスコ エンタープライズ ネットワーク機能仮想化インフラストラクチャ ソフトウェア（NFVIS）を実行しているデバイス、その他のデータセンターデバイスが含まれます。
- **Meraki ダッシュボード**：Cisco Meraki 製品を管理するためのシスコクラウド管理プラットフォームのダッシュボード。
- Firepower Management Center（FMC）：シスコのネットワーク セキュリティ ソリューションを管理するための Firepower Threat Defense（FTD）デバイスを介した完全かつ統合された管理を提供します。
- **サードパーティデバイス**：サードパーティデバイスは、SNMP MIB 2 の値を入力することができます。Catalyst Center は、インベントリやトポロジの限られた基本的な自動化機能をサポートします。さらに、アシュアランス機能は、サードパーティ製デバイス 360、到達可能性ステータスに基づくデバイスの正常性計算、およびデバイスインターフェイスと到達可能性の問題を対象とします。

サポート対象デバイスの完全なリストについては、*Cisco Catalyst Center Compatibility Matrix*を参照してください。

Catalyst Center インベントリへのデバイスの追加

Catalyst Center インベントリに新しいデバイスと既存のデバイスの両方を追加できます。

デバイスを追加または管理する際は、デュアルスタック IP アドレスファミリ（IPv4 および IPv6）に関する次の制約事項に注意してください。

- 競合防止：IPv4 と IPv6 の両方を使用して同じデバイスを追加することはできません。
- FQDN の処理：

- FQDN は、デュアルスタック環境で解決可能である必要があります。FQDN を解決できない場合、または有効な DNS レコードがない場合、デバイスの追加は失敗します。
- FQDN を介して追加されたデバイスには、成功した DNS 解決結果に基づいて、自動的にアドレスファミリ（IPv4 または IPv6）が割り当てられます。

- デバイスが追加された後は、そのアドレスファミリを変更できません。デバイスを IPv4 から IPv6 （またはその逆）に切り替えるには、インベントリからデバイスを削除し、目的の IP タイプを使用して再度追加する必要があります。
- インベントリ収集中に IP タイプの競合が検出されると、システムはそのデバイスの更新を停止し、そのデバイスを「エラー」としてマークして、データの不整合を防ぎます。

手順

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

[Inventory] ウィンドウには、検出プロセス中に収集されたデバイス情報が表示されます。

ステップ 2 [Add Device] をクリックします。

[デバイスの追加（Add Device）] スライドインペインが表示され、プラグアンドプレイを使用した新しいデバイスの追加や既存のデバイスの追加のオプションが示されます。

ステップ 3 既存のデバイスをインベントリに追加するオプションを選択します。

- 検出プロセスを使用してデバイスを追加するには、**[Discovery]** をクリックし、ワークフローに従います。詳細については、デバイスの検出 （1628 ページ）を参照してください。
- 単一のデバイスを追加するには、**[Single Device]** をクリックします。追加するデバイスのタイプを選択します。
  - ネットワークデバイスを追加するには、ネットワークデバイスの追加 （157 ページ） を参照してください。
  - コンピューティングデバイスを追加するには、コンピューティングデバイスの追加 （171 ページ）を参照してください。
  - Cisco Meraki ダッシュボードを統合するには、Cisco Meraki ダッシュボードの統合 （180 ページ）を参照してください。
  - Firepower Management Center を統合するには、Firepower Management Center の統合 （181 ページ）を参照してください。
  - サードパーティ製デバイスを追加するには、サードパーティ製デバイスの追加 （184 ページ） を参照してください。
- CSV ファイルからデバイス設定をインポートするには、**[Import Inventory]** をクリックします。詳細については、CSV ファイルからのデバイス設定のインポート （222 ページ）を参照してください。

ステップ 4 既存のデバイスをインベントリに追加するオプションを選択します。

新しいデバイスは、プラグアンドプレイプロセスを使用して追加します。単一のデバイス、複数のデバイス、またはスマートアカウントからのデバイスを追加できます。任意のタイルを選択すると、**[プラグアンドプレイ（Plug and Play）]** ウィンドウ内のオプションが開きます。

- 単一のデバイスを追加するには、**[Single Device]** をクリックします。詳細については、デバイスの追加または編集 （710 ページ）を参照してください。
- CSV ファイルからデバイスを一括で追加するには、**[Bulk Devices]** をクリックします。詳細については、デバイスの一括追加 （711 ページ）を参照してください。
- スマートアカウントからデバイスを追加するには、**[Smart Account]** をクリックします。詳細については、スマートアカウントからのデバイスの追加 （714 ページ）を参照してください。

次のタスク

インベントリ内のデバイスを表示および管理できます。詳細については、[Inventory] ウィンドウでのデバイスの管理 （189 ページ）を参照してください。**[Plug and Play]** ウィンドウから新しく追加されたデバイスを管理するには、デバイスの表示 （706 ページ） を参照してください。

ネットワークデバイスの管理

ネットワークデバイスの追加

ネットワーク デバイスは、インベントリに手動で追加できます。

始める前に

ネットワークデバイスを設定していることを確認します。詳細については、「ディスカバリの前提条件 （75 ページ）」を参照してください。

手順

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

検出プロセスでは、[インベントリ] ウィンドウに表示されるデバイス情報が収集されます。

ステップ 2 [Add Device] をクリックします。

[Add Device] スライドインペインが表示され、デバイスを追加するためのオプションが示されます。

ステップ 3 **[既存のデバイス（Existing devices）]** エリアで、[単一デバイス（Single Device）] タイルをクリックします。

ステップ 4 **[デバイスタイプ（Device type）]** ドロップダウンリストから、[ネットワークデバイス（Network Device）] を選択します。

ステップ 5 **[IPアドレス（IP address）]** フィールドで、デバイスの IP アドレスまたは名前を入力します。

（注） デバイスで HSRP プロトコルを使用している場合は、プライマリ IP アドレスを入力する必要があります。

ステップ 6 [CLI] ログイン情報を設定します。

a) グローバルログイン情報を使用するには、グローバルログイン情報オプションボタンをクリックします。

（注） 使用可能なグローバル CLI クレデンシャルがない場合は、**[Network Settings]** > **[Device Credentials]** ウィンドウでグローバル CLI クレデンシャルを作成します。グローバル CLI クレデンシャルの追加 （379 ページ）を参照してください。

b) 特定のデバイスのログイン情報を設定するには、**[追加（Add）]** をクリックし、次のフィールドを設定します。

表 *16 : CLI* クレデンシャル

フィールド	説明
Name/Description	CLIクレデンシャルを説明する名前または語句。 CLI の認証が失敗した場合、Catalyst Center は、認証プロセスを 300 秒（5 分）間再試行します。
Username	ネットワーク内のデバイスの CLI にログインするために使用する名前。
Password	ネットワーク内のデバイスの CLI にログインするために使用されるパスワード。 セキュリティ上の理由から、確認のためにパスワードを再入力します。 （注） パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。
Enable Password	CLI で高い権限レベルに移るために使用するパスワード。ネットワークデバイスで必要な場合にのみ、このパスワードを設定します。 セキュリティ上の理由から、有効なパスワードを再入力します。 （注） パスワードはセキュリティ上の理由から暗号化されており、この設定では非表示になります。

ステップ 7 [SNMP] ログイン情報を設定します。

a) グローバルログイン情報を使用するには、グローバルログイン情報オプションボタンをクリックします。

（注） 使用可能なグローバル SNMP クレデンシャルがない場合は、**[Network Settings]** > **[Device Credentials]**ウィンドウでグローバル SNMP クレデンシャルを作成します。グローバル SNMPv2c ログイン情報の追加 （380 ページ）およびグローバル SNMPv3 ログイン情報の追加 （382 ページ）を参照してください。

b) 特定のデバイスのログイン情報を設定するには、**[追加（Add）]**をクリックしてから、次の手順を続行します。

ステップ 8 ドロップダウンリストから、[SNMPv2C] または [SNMPv3] を選択します。

SNMPv2c を選択した場合は、次のフィールドを設定します。

表 *17 : SNMPv2c* クレデンシャル

フィールド	説明
Name/Description	追加する SNMPv2c 設定の名前または説明。
Read Community	デバイス上の SNMP 情報を表示するためにのみ使用される読み取り専用コミュニティ ストリング パスワード。 （注） パスワードはセキュリティ上の理由から暗号化されており、この設定では非表示になります。
Write Community	デバイス上の SNMP 情報を変更するために使用される書き込みコミュニティストリング。 （注） パスワードはセキュリティ上の理由から暗号化されており、この設定では非表示になります。

SNMPv3 を選択した場合は、次のフィールドを設定します。

表 *18 : SNMPv3* クレデンシャル

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

フィールド	説明
Mode	SNMP メッセージを必要とするセキュリティ レベル。次のいずれかのモードを選択します。 • [Authentication and Privacy]：認証と暗号化の両方を行います。 • [Authentication, No Privacy]：認証は行いますが、暗号化は行いません。 • [No Authentication, No Privacy]：認証も暗号化も行いません。
Auth. Type	使用する認証タイプ（[Mode] として [Authentication and Privacy] または [Authentication, No Privacy] を選択した場合に有効になります）。次のいずれかの認証タイプを選択します。 • [SHA]：HMAC-SHA に基づく認証。 • [SHA256]：HMAC-SHA256 に基づく認証。 • [MD5 (not recommended)]：HMAC-MD5 に基づく認証。
Auth. Password	SNMPv3 を使用するデバイスから情報にアクセスする際に使用する SNMPv3 パスワード。これらのパスワード（またはパスフレーズ）は、8 文字以上にする必要があります。 （注） • 一部のシスコ ワイヤレス コントローラでは、パスワード（あるいはパスフレーズ）は少なくとも 12 文字以上である必要があります。ワイヤレス コントローラのパスワードの最小要件を必ず確認してください。パスワードに必要な最低限の文字数が守られないと、デバイスではCatalyst Centerによる検出、監視、管理が行われなくなります。 • パスワードはセキュリティ上の理由から暗号化されており、この設定では非表示になります。
Privacy Type	プライバシー タイプ。（[Mode] として [Authentication and Privacy] を選択した場合に有効になります）。次のプライバシータイプのいずれかを選択します。 • [AES128]：暗号化の 128 ビット CBC モード AES。 • **CISCOAES192**：シスコのデバイス上での暗号化の 192 ビット CBC モード AES。 • **CISCOAES256**：シスコのデバイス上での暗号化の 256 ビット CBC モード AES。

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

ステップ 9　[NETCONF] 設定を構成します。

（注）　NETCONF では、CLI プロトコルとして SSH を設定し、SSH クレデンシャルを定義することが必要です。

表 *19 : NETCONF* 設定

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

ステップ 10　[詳細設定の表示（Show advanced settings）] をクリックし、次の手順で説明するように必要な設定を構成します。

ステップ 11　SNMP の [再試行（Retries）] と [タイムアウト（Timeout）] の値を設定します。

表 *20* : *SNMP* のプロパティ

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

ステップ 12 [HTTP(S)] ログイン情報を設定します。

a) すでに作成されているグローバル HTTP(S) ログイン情報を使用するには、グローバルログイン情報オプションボタンをクリックします。

（注） 使用可能なグローバル HTTP または HTTPS ログイン情報がない場合は、**[ネットワーク設定（Network Settings）] > [デバイスクレデンシャル（Device Credentials）]**ウィンドウでグローバル HTTP または HTTPS ログイン情報を作成します。「HTTPS グローバルログイン情報の設定」を参照してください。

b) 特定のデバイスのログイン情報を設定するには、**[追加（Add）]**をクリックし、次のフィールドを設定します。

表 *21* : *HTTP* および *HTTPS* クレデンシャル

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

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

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

ステップ 13 Catalyst Center とリモートデバイスとの通信を可能にするいずれかのネットワークの [プロトコル（Protocol）] を選択します。有効な値は [SSH2] または [Telnet] です。

ステップ 14 （任意）[ログイン情報（Credentials）] の横にある [検証（Validate）] をクリックすると、Catalyst Center によってデバイスのログイン情報が検証されます。緑色のチェックマークは、有効なログイン情報を示します。赤色の X マークは、無効なログイン情報を示します。

SNMP 書き込みログイン情報を除くすべてのログイン情報が検証されます。

ステップ 15 設定の内容を確認します。（変更を加えるには [Edit] をクリックします）

ステップ 16 **[デバイスの追加（Add Device）]** をクリックします。

ネットワーク デバイス クレデンシャルの更新

選択したネットワーク デバイスのディスカバリ クレデンシャルを更新することができます。選択したデバイスに対しては、この更新された設定が、グローバル設定やジョブ固有の設定よりも優先されます。

（注） インベントリに追加されたサードパーティ製デバイスのログイン情報は更新できません。

始める前に

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

この手順を実行するには、管理者（ROLE_ADMIN）またはポリシー管理者（ROLE_POLICY_ADMIN）権限、および適切な RBAC スコープが必要です。

手順

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

[Inventory] ウィンドウには、検出プロセス中に収集されたデバイス情報が表示されます。

ステップ 2 更新するネットワーク デバイスを選択します。

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

ステップ 4 [CLI] 領域がまだ展開されていない場合は展開し、次のいずれかの手順を実行します。

a) すでに作成されているグローバル CLI クレデンシャルを使用する場合は、[Select global credential] オプションボタンをクリックします。

（注） 使用可能な CLI グローバルログイン情報がない場合は、**[Network Settings]** > **[Device Credentials]** ウィンドウで作成します。「グローバル CLI クレデンシャルの設定」を参照してください。

b) **[デバイス固有のログイン情報の追加（Add device specific credential）]** オプションボタンをクリックし、次のフィールドを設定します。

表 *22 : CLI* クレデンシャル

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

フィールド	説明
Enable Password	CLI で高い権限レベルに移るために使用するパスワード。 セキュリティ上の理由から、確認のためにパスワードを再入力します。 パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。

ステップ 5 [SNMP] 領域がまだ展開されていない場合は展開し、次のいずれかの手順を実行します。

a) すでに作成されている SNMP グローバルログイン情報を使用する場合は、[Select global credential] オプションボタンをクリックします。

（注） 使用可能な SNMP グローバルログイン情報がない場合は、**[Network Settings]** > **[Device Credentials]** ウィンドウで作成します。「グローバル SNMPv2c ログイン情報の設定」および「グローバル SNMPv3 ログイン情報の設定」を参照してください。

b) **[デバイス固有のログイン情報の追加（Add device specific credential）]** オプションボタンをクリックして、この手順を続行します。

ステップ 6 [Version] ドロップダウンリストから、[V2C]（SNMP バージョン 2c）または [V3]（SNMP バージョン 3）を選択します。

V2C を選択した場合、次のフィールドを設定します。

表 23 : SNMPv2c クレデンシャル

フィールド	説明
Read Community	デバイス上の SNMP 情報を表示するためにのみ使用される読み取り専用コミュニティ ストリング パスワード。 （注） パスワードはセキュリティ上の理由から暗号化されており、この設定では非表示になります。
Write Community	デバイス上の SNMP 情報を変更するために使用される書き込みコミュニティストリング。 （注） パスワードはセキュリティ上の理由から暗号化されており、この設定では非表示になります。

[V3] を選択した場合、次のフィールドを設定します。

表 *24 : SNMPv3* クレデンシャル

フィールド	説明
Name/Description	追加した SNMPv3 設定の名前または説明。
Username	SNMPv3 設定に関連付けられている名前。
Mode	SNMP メッセージを必要とするセキュリティ レベル。次のいずれかのモードを選択します。 • [Authentication and Privacy]：認証と暗号化の両方を行います。 • [Authentication, No Privacy]：認証は行いますが、暗号化は行いません。 • [No Authentication, No Privacy]：認証も暗号化も行いません。
Auth. Type	使用する認証タイプ（[Mode] として [Authentication and Privacy] または [Authentication, No Privacy] を選択した場合に有効になります）。次のいずれかの認証タイプを選択します。 • [SHA]：HMAC-SHA に基づく認証。 • [SHA256]：HMAC-SHA256 に基づく認証。 • [MD5 (not recommended)]：HMAC-MD5 に基づく認証。
Auth. Password	SNMPv3 を使用するデバイスから情報にアクセスする際に使用する SNMPv3 パスワード。これらのパスワード（またはパスフレーズ）は、8 文字以上にする必要があります。 （注） • 一部のシスコ ワイヤレス コントローラでは、パスワード（あるいはパスフレーズ）は少なくとも 12 文字以上である必要があります。ワイヤレス コントローラのパスワードの最小要件を必ず確認してください。パスワードに必要な最低限の文字数が守られないと、デバイスではCatalyst Centerによる検出、監視、管理が行われなくなります。 • パスワードはセキュリティ上の理由から暗号化されており、この設定では非表示になります。
Privacy Type	プライバシー タイプ。（[Mode] として [Authentication and Privacy] を選択した場合に有効になります）。次のプライバシータイプのいずれかを選択します。 • [AES128]：暗号化の 128 ビット CBC モード AES。 • **CISCOAES192**：シスコのデバイス上での暗号化の 192 ビット CBC モード AES。 • **CISCOAES256**：シスコのデバイス上での暗号化の 256 ビット CBC モード AES。

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

ステップ 7 まだ展開されていない場合は [SNMP RETRIES AND TIMEOUT] エリアを展開し、次のフィールドを設定します。

表 25 : SNMP のプロパティ

フィールド	説明
Retries	デバイスへ接続可能な試行回数。有効な値は 1 ～ 3 です。デフォルトは 3 です。
Timeout	タイムアウトになるまでにデバイスとの接続の確立を試みる際に、Catalyst Center が待機する秒数。有効な値は、5 秒間隔で 1 ～ 300 秒です。デフォルトは 5 秒です。

ステップ 8 [HTTP(S)] エリアがまだ展開されていない場合は展開し、次のいずれかの手順を実行します。

a) すでに作成されている HTTP（HTTPS）グローバルログインを使用する場合は、[Select global credential] オプションボタンをクリックします。

（注） 使用可能な HTTP または HTTPS グローバルクレデンシャルがない場合は、[Network Settings][Device Credentials]ウィンドウで作成します。「HTTPS グローバルログイン情報の設定」を参照してください。

b) **[デバイス固有のログイン情報の追加（Add device specific credential）]** オプションボタンをクリックし、次のフィールドを設定します。

表 *26 : HTTP* と *HTTPS*

フィールド	説明
Username	ネットワーク内のデバイスの HTTP（HTTPS）にログインするために使用する名前。
Password	ネットワーク内のデバイスの HTTP（HTTPS）にログインするために使用するパスワード。 セキュリティ上の理由から、確認のためにパスワードを再入力します。 パスワードはセキュリティ上の理由から暗号化されており、この設定では非表示になります。
Port	必要な HTTP（HTTPS）ポート番号を指定します。

ステップ 9 まだ展開されていない場合は **NETCONF** 領域を展開し、**ポート** フィールドを設定します。

NETCONF では、CLI プロトコルとして SSH を設定し、SSH クレデンシャルを定義することが必要です。

ステップ 10 Catalyst Center とリモートデバイスとの通信を可能にするいずれかのネットワークプロトコルの [Protocol] オプションボタンを選択します。有効な値は **SSH2** または **Telnet** です。

ステップ 11 （任意） [Credentials] の横にある [Validate] をクリックします。Catalyst Center により、デバイスログイン情報が検証され、有効なログイン情報には緑色のチェックマーク、無効なログイン情報には赤色の X マークが表示されます。

ログイン情報を更新する対象として複数のデバイスを選択した場合、[Validation] ボタンは無効になります。

ステップ 12 [Update] をクリックします。

ネットワークデバイスのセキュリティフォーカス

Catalyst Center のセキュリティフォーカスにより、デバイスでの信頼できるチェックの結果を表示できます。

ただし、シスコ製デバイスの真正性を保証し、物理的な改ざんや不正アクセスがないことを確認するためのセキュリティチェックがほとんど行われていません。

実際には、デバイスアイデンティティ検証の一環として、次のチェックが実行されています。

- セキュアな固有デバイス識別子（SUDI）証明書チェーンの検証。
- デバイスの SUDI 証明書応答の署名検証。
- SUDI 証明書による製品 ID 検証。
- SUDI 証明書によるシリアル番号検証。

これらのチェックは、次の状況でトリガーされます。

- Catalyst Center でインベントリが収集されるたび。
- デバイスの設定を変更するとき。
- デバイスでイメージをアップグレードするとき。

次の CLI コマンドを使用して、デバイスアイデンティティ検証チェックを実行します。

```
show platform sudi certificate sign nonce ${randomNonceValue}
```

デバイスの完全性検証ステータスの表示

この手順では、整合性検証チェックのステータスを表示する方法について説明します。

手順

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

[Inventory] ウィンドウには、検出プロセス中に収集されたデバイス情報が表示されます。

ステップ 2 [Focus] ドロップダウンメニューから [Security] を選択します。

ステップ 3 [Devices] テーブルで、デバイスの [Integrity Verification] 列にステータスとして [Failed] と表示されている場合は、情報アイコン（ⓘ）をクリックして理由を表示します。

（注） [Integrity Verification] 列が表示されない場合は、「インベントリに関する情報の表示（102 ページ）」を参照してください。

デバイス証明書ステータスの表示

デバイス証明書は、Catalyst Center が管理するデバイスを認証するために発行する証明書です。

デバイス証明書のステータスを表示するには、次の手順を実行します。

（注） 期限切れ間近または期限切れのデバイス証明書の数は、Catalyst Center ホームウィンドウの **[Device Certificate Issues]** タイルで確認できます。

手順

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

[Inventory] ウィンドウには、検出プロセス中に収集されたデバイス情報が表示されます。

ステップ 2 **[Focus]** ドロップダウンリストから **[Security]** を選択します。

ステップ 3 デバイス証明書のステータスは、**[Certificate Status]** 列で確認できます。

次のいずれかのステータスが表示されます。

アイテム	説明
Active	証明書は有効です。
Expiring	デバイスが証明書を更新するために必要な SCEP 接続または設定を確認します。
Expired	これが想定外である場合は、このテレメトリを使用したデバイス設定の更新（69 ページ） の手順に従って、デバイスの新しい証明書を生成できます
Not Provisioned	証明書がプロビジョニングされていません。
該当なし	デバイス証明書のステータスはまだ使用できません。後でもう一度確認してください。

ステップ 4 デバイス証明書の詳細を確認するには、デバイス証明書ステータスのハイパーリンクをクリックします。

計算デバイスの管理

コンピューティングデバイスの追加

計算デバイスは、インベントリに手動で追加できます。計算デバイスには、Cisco Unified Computing System（UCS）などのデバイス、Cisco Enterprise ネットワーク機能の仮想化インフラストラクチャ ソフトウェア（NFVIS）を実行しているデバイス、およびその他のデータセンター デバイスが含まれます。

手順

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

[Inventory] ウィンドウには、検出プロセス中に収集されたデバイス情報が表示されます。

ステップ 2 [Add Device] をクリックします。

[Add Device] スライドインペインが表示され、デバイスを追加するためのオプションが示されます。

ステップ 3 **[既存のデバイス（Existing devices）]** エリアで、[単一デバイス（Single Device）] タイルをクリックします。

ステップ 4 **[デバイスタイプ（Device type）]** ドロップダウンリストから、[計算デバイス（Compute Device）] を選択します。

ステップ 5 **[IPアドレス（IP address）]** フィールドで、デバイスの IP アドレスまたは名前を入力します。

ステップ 6 [HTTP(S)] ログイン情報を設定します。

a) すでに作成されているグローバル HTTP（HTTPS）ログイン情報を使用する場合は、グローバルログイン情報オプションボタンをクリックします。

（注） 使用可能な HTTP または HTTPS グローバルクレデンシャルがない場合は、[Network Settings][Device Credentials]ウィンドウで作成します。グローバル HTTPS ログイン情報の追加（385 ページ）を参照してください。

b) 特定のデバイスのログイン情報を設定するには、**[追加（Add）]** をクリックし、次のフィールドを設定します。

表 27 : HTTP と HTTPS

フィールド	説明
[名前または説明（Name or description）]	ログイン情報の名前または説明。
Username	HTTPS 接続の認証に使用される名前。
Password	HTTPS 接続の認証に使用されるパスワード。
Port	HTTPS トラフィックに使用される TCP/UDP ポートの番号。デフォルトはポート番号 443（HTTPS の既知のポート）です。

ステップ 7 [詳細設定の表示（Show advanced settings）] をクリックし、次の手順で説明するように必要な設定を構成します。

ステップ 8 [CLI] ログイン情報を設定します。

a) すでに作成されているグローバル CLI ログイン情報を使用する場合は、グローバルログイン情報オプションボタンをクリックします。

（注） 使用可能な CLI グローバルログイン情報がない場合は、**[Network Settings]** > **[Device Credentials]** ウィンドウで作成します。グローバル CLI クレデンシャルの追加 （379 ページ）を参照してください。

b) 特定のデバイスのログイン情報を設定するには、**[追加（Add）]** をクリックし、次のフィールドを設定します。

表 *28 : CLI* クレデンシャル

フィールド	説明
[名前または説明（Name or description）]	ログイン情報の名前または説明。
Username	ネットワーク内のデバイスの CLI にログインするために使用する名前。
Password	ネットワーク内のデバイスの CLI にログインするために使用されるパスワード。 セキュリティ上の理由から、確認のためにパスワードを再入力します。 パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。
Enable Password	CLI で高い権限レベルに移るために使用するパスワード。 セキュリティ上の理由から、有効なパスワードを再入力します。 パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。

ステップ 9 [SNMP] ログイン情報を設定します。

a) すでに作成されているグローバル SNMP ログイン情報を使用する場合は、グローバルログイン情報オプションボタンをクリックします。

（注） 使用可能な SNMP グローバルログイン情報がない場合は、**[Network Settings]** > **[Device Credentials]** ページで作成します。グローバル SNMPv2c ログイン情報の追加 （380 ページ）およびグローバル SNMPv3 ログイン情報の追加 （382 ページ）を参照してください。

b) 特定のデバイスのログイン情報を設定するには、**[追加（Add）]** をクリックし、次のフィールドを設定します。

ステップ 10 ドロップダウンリストから、[SNMPv2C] または [SNMPv3] を選択します。

SNMPv2c を選択した場合は、次のフィールドを設定します。

表 *29 : SNMPv2c* クレデンシャル

フィールド	説明
Name/Description	追加する SNMPv2c 設定の名前または説明。

フィールド	説明
Read Community	デバイス上の SNMP 情報を表示するためにのみ使用される読み取り専用コミュニティ ストリング パスワード。 （注） パスワードはセキュリティ上の理由から暗号化されており、この設定では非表示になります。
Write Community	デバイス上の SNMP 情報を変更するために使用される書き込みコミュニティストリング。 （注） パスワードはセキュリティ上の理由から暗号化されており、この設定では非表示になります。

SNMPv3 を選択した場合は、次のフィールドを設定します。

表 *30 : SNMPv3* クレデンシャル

フィールド	説明
Name/Description	追加した SNMPv3 設定の名前または説明。
Username	SNMPv3 設定に関連付けられている名前。
Mode	SNMP メッセージを必要とするセキュリティ レベル。次のいずれかのモードを選択します。 • [Authentication and Privacy]：認証と暗号化の両方を行います。 • [Authentication, No Privacy]：認証は行いますが、暗号化は行いません。 • [No Authentication, No Privacy]：認証も暗号化も行いません。
Auth. Type	使用する認証タイプ（[Mode] として [Authentication and Privacy] または [Authentication, No Privacy] を選択した場合に有効になります）。次のいずれかの認証タイプを選択します。 • [SHA]：HMAC-SHA に基づく認証。 • [SHA256]：HMAC-SHA256 に基づく認証。 • [MD5 (not recommended)]：HMAC-MD5 に基づく認証。

フィールド	説明
Auth. Password	SNMPv3 を使用するデバイスから情報にアクセスする際に使用する SNMPv3 パスワード。これらのパスワード（またはパスフレーズ）は、8 文字以上にする必要があります。 （注） • 一部のシスコ ワイヤレス コントローラでは、パスワード（あるいはパスフレーズ）は少なくとも 12 文字以上である必要があります。ワイヤレス コントローラのパスワードの最小要件を必ず確認してください。パスワードに必要な最低限の文字数が守られないと、デバイスではCatalyst Centerによる検出、監視、管理が行われなくなります。 • パスワードはセキュリティ上の理由から暗号化されており、この設定では非表示になります。
Privacy Type	プライバシー タイプ。（[Mode] として [Authentication and Privacy] を選択した場合に有効になります）。次のプライバシータイプのいずれかを選択します。 • [AES128]：暗号化の 128 ビット CBC モード AES。 • **CISCOAES192**：シスコのデバイス上での暗号化の 192 ビット CBC モード AES。 • **CISCOAES256**：シスコのデバイス上での暗号化の 256 ビット CBC モード AES。
Privacy Password	暗号化の標準規格をサポートしているデバイスで交換されるメッセージを暗号化するための秘密鍵を生成するために使用される SNMPv3 プライバシーパスワード。パスワード（またはパスフレーズ）は、8 文字以上にする必要があります。 （注） • 一部のシスコ ワイヤレス コントローラでは、パスワード（あるいはパスフレーズ）は少なくとも 12 文字以上である必要があります。ワイヤレス コントローラのパスワードの最小要件を必ず確認してください。パスワードに必要な最低限の文字数が守られないと、デバイスではCatalyst Centerによる検出、監視、管理が行われなくなります。 • パスワードはセキュリティ上の理由から暗号化されており、この設定では非表示になります。

ステップ 11 （任意） [Credentials] の横にある [Validate] をクリックします。Catalyst Center により、デバイスログイン情報が検証され、有効なログイン情報には緑色のチェックマーク、無効なログイン情報には赤色のXマークが表示されます。

SNMP 書き込みログイン情報を除くすべてのログイン情報が検証されます。

ステップ 12 設定の内容を確認します。（変更を加えるには [Edit] をクリックします）

ステップ 13 **[デバイスの追加（Add Device）]** をクリックします。

計算デバイスのログイン情報の更新

選択した計算デバイスのディスカバリクレデンシャルを更新することができます。選択したデバイスに対しては、この更新された設定が、グローバル設定やジョブ固有の設定よりも優先されます。

始める前に

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

手順

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

[Inventory] ウィンドウには、検出プロセス中に収集されたデバイス情報が表示されます。

ステップ 2 更新するデバイスを選択します。

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

ステップ 4 [HTTP(S)] エリアがまだ展開されていない場合は展開し、次のいずれかの手順を実行します。

a) すでに作成されている HTTP（HTTPS）グローバルログインを使用する場合は、[Select global credential] オプションボタンをクリックします。

（注） 使用可能な HTTP または HTTPS グローバルクレデンシャルがない場合は、[Network Settings][Device Credentials]ウィンドウで作成します。グローバル HTTPS ログイン情報の追加（385 ページ）を参照してください。

b) **[デバイス固有のログイン情報の追加（Add device specific credential）]** オプションボタンをクリックし、次のフィールドを設定します。

表 31 : HTTP と HTTPS

フィールド	説明
Username	ネットワーク内のデバイスの HTTP（HTTPS）にログインするために使用する名前。

フィールド	説明
Password	ネットワーク内のデバイスの HTTP（HTTPS）にログインするために使用するパスワード。 セキュリティ上の理由から、確認のためにパスワードを再入力します。 パスワードはセキュリティ上の理由から暗号化されており、この設定では非表示になります。
Port	必要な HTTP（HTTPS）ポート番号を指定します。

ステップ 5 [CLI] 領域がまだ展開されていない場合は展開し、次のいずれかの手順を実行します。

a) すでに作成されているグローバル CLI クレデンシャルを使用する場合は、[Select global credential] オプションボタンをクリックします。

（注） 使用可能な CLI グローバルログイン情報がない場合は、**[Network Settings]** > **[Device Credentials]** ウィンドウで作成します。グローバル CLI クレデンシャルの追加 （379 ページ）を参照してください。

b) **[デバイス固有のログイン情報の追加（Add device specific credential）]** オプションボタンをクリックし、次のフィールドを設定します。

表 *32 : CLI* クレデンシャル

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

ステップ 6 [SNMP] 領域がまだ展開されていない場合は展開し、次のいずれかの手順を実行します。

a) すでに作成されている SNMP グローバルログイン情報を使用する場合は、[Select global credential] オプションボタンをクリックします。

（注） 使用可能な SNMP グローバルログイン情報がない場合は、**[Network Settings]** > **[Device Credentials]** ウィンドウで作成します。グローバル SNMPv2c ログイン情報の追加 （380 ページ）およびグローバル SNMPv3 ログイン情報の追加 （382 ページ）を参照してください。

b) **[デバイス固有のログイン情報の追加（Add device specific credential）]** オプションボタンをクリックして、この手順を続行します。

ステップ 7 [Version] ドロップダウンリストから、[V2C]（SNMP バージョン 2c）または [V3]（SNMP バージョン 3）を選択します。

V2C を選択した場合、次のフィールドを設定します。

表 *33 : SNMPv2c* クレデンシャル

フィールド	説明
Read Community	デバイス上の SNMP 情報を表示するためにのみ使用される読み取り専用コミュニティ ストリング パスワード。 （注） パスワードはセキュリティ上の理由から暗号化されており、この設定では非表示になります。
Write Community	デバイス上の SNMP 情報を変更するために使用される書き込みコミュニティストリング。 （注） パスワードはセキュリティ上の理由から暗号化されており、この設定では非表示になります。

[V3] を選択した場合、次のフィールドを設定します。

表 *34 : SNMPv3* クレデンシャル

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

フィールド	説明
Auth. Type	使用する認証タイプ（[Mode] として [Authentication and Privacy] または [Authentication, No Privacy] を選択した場合に有効になります）。次のいずれかの認証タイプを選択します。 • [SHA]：HMAC-SHA に基づく認証。 • [SHA256]：HMAC-SHA256 に基づく認証。 • [MD5 (not recommended)]：HMAC-MD5 に基づく認証。
Auth. Password	SNMPv3 を使用するデバイスから情報にアクセスする際に使用する SNMPv3 パスワード。これらのパスワード（またはパスフレーズ）は、8 文字以上にする必要があります。 （注） • 一部のシスコ ワイヤレス コントローラでは、パスワード（あるいはパスフレーズ）は少なくとも 12 文字以上である必要があります。ワイヤレス コントローラのパスワードの最小要件を必ず確認してください。パスワードに必要な最低限の文字数が守られないと、デバイスではCatalyst Centerによる検出、監視、管理が行われなくなります。 • パスワードはセキュリティ上の理由から暗号化されており、この設定では非表示になります。
Privacy Type	プライバシー タイプ。（[Mode] として [Authentication and Privacy] を選択した場合に有効になります）。次のプライバシータイプのいずれかを選択します。 • [AES128]：暗号化の 128 ビット CBC モード AES。 • **CISCOAES192**：シスコのデバイス上での暗号化の 192 ビット CBC モード AES。 • **CISCOAES256**：シスコのデバイス上での暗号化の 256 ビット CBC モード AES。
Privacy Password	暗号化の標準規格をサポートしているデバイスで交換されるメッセージを暗号化するための秘密鍵を生成するために使用される SNMPv3 プライバシーパスワード。パスワード（またはパスフレーズ）は、8 文字以上にする必要があります。 （注） • 一部のシスコ ワイヤレス コントローラでは、パスワード（あるいはパスフレーズ）は少なくとも 12 文字以上である必要があります。ワイヤレス コントローラのパスワードの最小要件を必ず確認してください。パスワードに必要な最低限の文字数が守られないと、デバイスではCatalyst Centerによる検出、監視、管理が行われなくなります。 • パスワードはセキュリティ上の理由から暗号化されており、この設定では非表示になります。

ステップ 8 （オプション）[Credentials] の横にある [Validate] をクリックします。Catalyst Center により、デバイスログイン情報が検証され、有効なログイン情報には緑色のチェックマーク、無効なログイン情報には赤色の X マークが表示されます。

ログイン情報を更新する対象として複数のデバイスを選択した場合、[Validation] ボタンは無効になります。

ステップ 9 [Update] をクリックします。

Cisco Meraki ダッシュボードの管理

Cisco Meraki ダッシュボードの統合

Meraki ダッシュボードと Catalyst Center を統合できます。

手順

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

[Inventory] ウィンドウには、検出プロセス中に収集されたデバイス情報が表示されます。

ステップ 2 [Add Device] をクリックします。

[Add Device] スライドインペインが表示され、デバイスを追加するためのオプションが示されます。

ステップ 3 **[既存のデバイス（Existing devices）]** エリアで、[単一デバイス（Single Device）] タイルをクリックします。

ステップ 4 **[デバイスタイプ（Device type）]** ドロップダウンリストから [Merakiダッシュボード（Meraki Dashboard）] を選択します。

ステップ 5 [HTTP(S)] ログイン情報を設定します。

a) [APIキー/パスワード（API Key/Password）] フィールドで、Cisco Meraki ダッシュボードへのアクセスに使用する API キーを入力します。次に、[組織の詳細を取得（Get Organization details）] リンクをクリックします。

b) **[Merakiの詳細の選択（Select Meraki Details）]** ドロップダウンリストから組織のオプションを選択するか、組織名を検索します。

ステップ 6 （オプション）[ログイン情報（Credentials）] の横にある [検証（Validate）] をクリックします。Catalyst Center により、デバイスログイン情報が検証され、有効なログイン情報には緑色のチェックマーク、無効なログイン情報には赤色の X マークが表示されます。

ステップ 7 設定の内容を確認します。（変更を加えるには [Edit] をクリックします）

ステップ 8 **[デバイスの追加（Add Device）]** をクリックします。

選択した組織のみで Cisco Meraki ダッシュボードとデバイスの収集が開始されます。

Cisco Meraki ダッシュボードのログイン情報の更新

選択したデバイスの Meraki ダッシュボードログイン情報を更新することができます。選択したデバイスに対しては、この更新された設定が、グローバル設定やジョブ固有の設定よりも優先されます。

始める前に

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

手順

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

[Inventory] ウィンドウには、検出プロセス中に収集されたデバイス情報が表示されます。

ステップ 2 更新するデバイスを選択します。

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

ステップ 4 まだ展開されていない場合は、[HTTP（S）] エリアを展開します。

ステップ 5 [APIキー/パスワード（API Key/Password）] フィールドで、Cisco Meraki ダッシュボードへのアクセスに使用する API キーを入力します。

ステップ 6 [組織詳細の取得（Get Organization details）] をクリックします。

ステップ 7 [Cisco Merakiの詳細の選択（select meraki details）] ドロップダウンリストから組織のオプションを選択するか、組織名を検索します。

ステップ 8 （任意）[ログイン情報（Credentials）] の横にある [検証（Validate）] をクリックします。Catalyst Center により、デバイスログイン情報が検証され、有効なログイン情報には緑色のチェックマーク、無効なログイン情報には赤色の X マークが表示されます。

ログイン情報を更新する対象として複数のデバイスを選択した場合、[Validation] ボタンは無効になります。

ステップ 9 [Update] をクリックします。

Firepower Management Center の管理

Firepower Management Center の統合

Firepower Management Center（FMC）を Catalyst Center と統合できます。

手順

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

[Inventory] ウィンドウには、検出プロセス中に収集されたデバイス情報が表示されます。

ステップ 2 [Add Device] をクリックします。

[Add Device] スライドインペインが表示され、デバイスを追加するためのオプションが示されます。

ステップ 3 **[既存のデバイス（Existing devices）]** エリアで、[単一デバイス（Single Device）] タイルをクリックします。

ステップ 4 **[デバイスタイプ（Device type）]** ドロップダウンリストから、[Firepower Management Center] を選択します。

ステップ 5 **[IPアドレス（IP address）]** フィールドで、デバイスの IP アドレスまたは名前を入力します。

ステップ 6 [HTTP(S)] ログイン情報を設定します。

a) [Username]：HTTPS 接続の認証に使用される名前です。

b) [Password]：HTTPS 接続の認証に使用されるパスワードです。パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。

c) [Port]：HTTPS トラフィックで使用される TCP/UDP ポートの番号です。デフォルトのポート番号は 443 です。

ステップ 7 設定の内容を確認します。（変更を加えるには [Edit] をクリックします）

ステップ 8 **[デバイスの追加（Add Device）]** をクリックします。

（注） インベントリに FMC を追加すると、FMC によって管理される Firepower Threat Defense（FTD）デバイスもインベントリに自動的に追加されます。[インベントリ（Inventory）] ウィンドウに、アクティブ FTD とスタンバイ FTD の詳細を含む、使用可能な高可用性（HA）ペアが表示されます。

ステップ 9 ペアリングされた FTD の HA の詳細を表示するには、次の手順を実行します。

a) FTD のデバイス名をクリックします。

b) [View Device Details] をクリックします。

ペアリングされた FTD の名前が [デバイスの詳細Device Details] ウィンドウに表示されます。ペアリングされた FTD の名前をクリックすると、ペアリングされた FTD の詳細が表示されます。

c) [デバイスの詳細（Device Details）] ウィンドウで、[高可用性の詳細（High Availability Details）] をクリックします。

HA ペア情報、**高可用性リンク**、および**状態リンク** の詳細を表示できます。

Firepower Management Center のログイン情報の更新

Catalyst Center では Firepower Management Center（FMC）のログイン情報を更新できます。選択したデバイスに対しては、この更新された設定が、グローバル設定やジョブ固有の設定よりも優先されます。

始める前に

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

手順

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

[Inventory] ウィンドウには、検出プロセス中に収集されたデバイス情報が表示されます。

ステップ 2 更新する FMC デバイスを選択します。

（注） FMC によって管理されている Firepower Threat Defense（FTD）デバイスを更新、編集、または削除することはできません。インベントリ内の FMC を通じて FTD デバイスを管理する必要があります。

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

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

ステップ 5 [HTTP(S)] エリアを展開します（まだ展開していない場合）。

[Add device specific credential] オプションボタンは、デフォルトで選択されています。

ステップ 6 次の情報を入力します。

a) [Username]：HTTPS 接続の認証に使用される名前です。
b) [Password]：HTTPS 接続の認証に使用されるパスワードです。パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。
c) [Port]：HTTPS トラフィックで使用される TCP/UDP ポートの番号です。デフォルトのポート番号は 443 です。

ステップ 7 [Management IP] をクリックし、[Device IP/DNS Name] フィールドにデバイスの IP アドレスまたは名前を入力します。

ステップ 8 [Resync Interval] をクリックし、再同期間隔タイプを選択します。

- [Custom]：再同期間隔を分単位で入力できます。有効な範囲は 360 ～ 1,440 分（24 時間）です。
- [Global]：デフォルトでは、再同期間隔は 1,440 分（24 時間）に設定されます。
- [Disable]：再同期間隔が無効になるかゼロに設定されます。

ステップ 9 [Role] をクリックし、[Device Role] ドロップダウンリストからロールを選択します。

ステップ 10 [Update] をクリックします。

サードパーティ製デバイスの追加

サードパーティ製デバイスをインベントリに手動で追加できます。

Catalyst Center は、限定的な基本自動化（インベントリとトポロジ）と、サードパーティデバイス 360、到達可能性ステータスに基づくデバイス正常性の計算、デバイスインターフェイスと到達可能性の問題などのアシュアランス機能をサポートします。

サードパーティ製デバイスの場合、到達可能性とインターフェイス関連のメトリックは、Assurance 機能の一部としてキャプチャされます。詳細については、『*Cisco Catalyst Assurance User Guide*』を参照してください。

一部のサードパーティ製デバイスでは、SNMP MIB-II 値を入力できます。詳細については、*Cisco Catalyst Center Compatibility Matrix*を参照してください。

始める前に

ネットワークデバイスを設定していることを確認します。

手順

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

[Inventory] ウィンドウにデバイス情報が表示されます。

ステップ 2 [Add Device] をクリックします。

[Add Device] スライドインペインが表示されます。

ステップ 3 ネットワークにデバイスを追加するには、**[既存のデバイス（Existing devices）]** エリアの **[単一デバイス（Single Device）]** タイルをクリックし、次の手順を実行します。

a) **[デバイスタイプ（Device type）]** ドロップダウンリストから [サードパーティ製デバイス（Third Party Device）] を選択します。

b) **[IPアドレス（IP address）]** フィールドで、デバイスの IP アドレスまたは固有名を入力します。

c) （任意）[ログイン情報（Credentials）] エリアの [検証（Validate）] ハイパーリンクをクリックして、デバイスのログイン情報を検証します。有効なログイン情報には、緑色のチェックマークが表示されます。無効なログイン情報には赤いクロスマークが表示されます。

（注） SNMP 書き込みログイン情報を除くすべてのログイン情報が検証されます。

d) [SNMP] ログイン情報を設定します。

1. グローバル SNMP ログイン情報を使用するには、グローバルログイン情報オプションボタンを選択し、**[ネットワーク設定（Network Settings）]** > **[デバイスログイン情報（Device Credentials）]** ハイパーリンクをクリックしてログイン情報を追加します。詳細については、グローバル SNMPv2c

ログイン情報の追加（380ページ）およびグローバルSNMPv3ログイン情報の追加（382ページ）を参照してください。

2. 特定のデバイスのログイン情報を設定するには、**[追加（Add）]**をクリックし、次のフィールドを設定します。
   1. ドロップダウンリストから、[SNMPv2C] または [SNMPv3] を選択します。
   2. SNMPv2c を選択した場合は、次のフィールドを設定します。

      表 *35 : SNMPv2c* クレデンシャル

フィールド	説明
Name/Description	追加する SNMPv2c 設定の名前または説明。
Read Community	デバイス上の SNMP 情報を表示するためにのみ使用される読み取り専用コミュニティ ストリング パスワード。 （注） パスワードはセキュリティ上の理由から暗号化されており、この設定では非表示になります。
Write Community	デバイス上の SNMP 情報を変更するために使用される書き込みコミュニティストリング。 （注） パスワードはセキュリティ上の理由から暗号化されており、この設定では非表示になります。

   3. SNMPv3 を選択した場合は、次のフィールドを設定します。

      表 *36 : SNMPv3* クレデンシャル

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

フィールド	説明
Authentication Type	使用する認証タイプ（[Mode] として [Authentication and Privacy] または [Authentication, No Privacy] を選択した場合に有効になります）。次のいずれかの認証タイプを選択します。 • [SHA]：HMAC-SHA に基づく認証。 • [SHA256]：HMAC-SHA256 に基づく認証。 • [MD5 (not recommended)]：HMAC-MD5 に基づく認証。 （注） ソフトウェアイメージバージョン 17.14.1 以降のデバイスで MD5 認証タイプのみが設定されている場合、Catalyst Center はデバイスの検出をサポートしません。 MD5 認証を使用する場合は、SHA 認証も設定します。この設定により Catalyst Center はソフトウェアイメージ 17.14.1 以降で実行されているデバイスを検出して管理できます。
Authentication Password	SNMPv3 を使用するデバイスから情報にアクセスする際に使用する SNMPv3 パスワード。これらのパスワード（またはパスフレーズ）は、8 文字以上にする必要があります。 （注） • 一部のシスコ ワイヤレス コントローラでは、パスワード（あるいはパスフレーズ）は少なくとも 12 文字以上である必要があります。ワイヤレス コントローラのパスワードの最小要件を必ず確認してください。パスワードに必要な最低限の文字数が守られないと、デバイスではCatalyst Center による検出、監視、管理が行われなくなります。 • パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。
Privacy Type	プライバシータイプ（[モード（Mode）] として [認証およびプライバシー（Authentication and Privacy）] を選択した場合に有効になります）。プライバシータイプを選択します。 [AES128]：暗号化の 128 ビット CBC モード AES。 （注） プライバシー タイプ AES128 は、検出、インベントリ、および Assuranceでサポートされています。

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

e) [詳細設定の表示（Show advanced settings）] をクリックし、次の手順で説明するように必要な設定を構成します。

f) SNMP の [再試行（Retries）] と [タイムアウト（Timeout）] の値を設定します。

表 *37 : SNMP* のプロパティ

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

ステップ 4 設定の内容を確認します。（変更を加えるには [Edit] をクリックします）

ステップ 5 **[デバイスの追加（Add Device）]** をクリックします。

デバイスのフィルタリング

[**Inventory**] ウィンドウでは、[**Devices**] テーブル内のデバイスの詳細をフィルタ処理するための、基本的または高度なオプションを選択できます。

手順

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

[Inventory] ウィンドウには、検出プロセス中に収集されたデバイス情報が表示されます。

ステップ 2 **[Filter devices]** をクリックします。

使用可能なフィルタリングオプションは次のとおりです。

名前	説明
クイック フィルタ	基本的なフィルタリングオプションから、デバイスの詳細を絞り込むことができます。 たとえば、[Manageability] フィルタ処理オプションを [Managed] に切り替えて、すべての管理対象デバイスを表示できます。
詳細フィルタ	[Contains]、[Regex]（正規表現）などの演算子を使用してフィルタリング基準を設定し、デバイスの詳細を絞り込むことができます。 たとえば、[Tags] ドロップダウンリストで、演算子の [Contains] を選択し、[Tags] フィールドに「**ipsec**」と入力できます。次に、オートコンプリート ドロップダウン リストから、[branch-router-ipsec] などの 1 つのオプションを選択できます。これは、IP セキュリティでタグ付けされたブランチルータをフィルタ処理します。 さらに、使用可能なデータに基づいてフィルタ処理基準の値を入力する必要があります。
最近のフィルタ	[RECENT] エリアでは、再適用する最近のフィルターを選択できます。 最近のフィルタ処理を保存するには、最近のフィルタ処理を [SAVED] エリアにドラッグアンドドロップします。

ステップ 3 フィルタリングオプションを選択して、選択したフィルタ処理フィールドに適切な値を入力します。

Catalyst Centerその他のフィールドに値を入力すると、オートコンプリート値が提示されます。提示された値のいずれかを選択するか、目的の値を最後まで入力します。

複雑なワイルドカードを用いたフィルタリングシナリオでは、[Advanced Filtering] で正規表現オプションを使用します。次に、ワイルドカードを使用した正規表現フィルタリングの使用例を示します。

ワイルドカードを使用した正規表現	結果
^AP00.*9.*	デバイス名が AP00 で始まり、残りの任意の部分に 9 を含むデバイス名をフィルタリングします。
^AP84.*24.*	デバイス名が AP84 で始まり、残りの任意の部分に 24 を含むデバイス名をフィルタリングします。
^.*47B3.*24.*	デバイス名に 47B3 を含み、さらに残りの任意の部分に 24 を含むデバイス名をフィルタ処理します。

正規表現の値を入力したら、**Enter** を押します。

ステップ 4 [Apply] をクリックして情報をフィルタします。

[Devices] テーブルに表示されるデータは、フィルタ選択に従って自動的に更新されます。

（注） フィルタごとに複数のフィルタ タイプと複数の値を使用できます。

ステップ 5 （任意） 必要に応じて、さらにフィルタを追加します。

ステップ 6 （任意） すべてのフィルタ処理を削除するには、[Filter devices] フィールドで [x] をクリックし、[Apply] をクリックします。

ステップ 7 （任意） 特定のフィルター値を削除するには、[Filter devices] フィールドでカーソルを削除したい値の上にドラッグし、[Delete] を押して [Apply] をクリックします。

[Inventory] ウィンドウでのデバイスの管理

ここでは、[Inventory] ウィンドウで、サイトにデバイスを割り当て、デバイスタグを管理する方法について説明します。

プロビジョニングされていないデバイスのサイトへの割り当て

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

（注）
- まだプロビジョニングされていないワイヤレス AP は、フロアにのみ割り当てることができます。その後、まだプロビジョニングされていない場合は、割り当てられたフロアマップから削除することで、フロアからワイヤレス AP の割り当てを解除できます。手順の詳細については、AP をマップから削除する （324 ページ）を参照してください。
- サードパーティ製デバイスはサイトに割り当てられますが、そのデバイスは Catalyst Center によって管理されません。可視性だけが提供されます。

手順

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

ステップ 2 サイトに割り当てるデバイスのチェックボックスをオンにします。

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

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

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

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

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

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

（注） アプリケーションテレメトリとコントローラベースのアプリケーション認識（CBAR）は、[Design] > [Network Settings] > [Telemetry] ウィンドウで [Application Telemetry] と [CBAR] を有効にすると、該当するネットワーク デバイスでデフォルトで有効になります。詳細については、テレメトリを使用した syslog、SNMP トラップ、NetFlow コレクタサーバー、および有線クライアントデータ収集の設定 （59 ページ）を参照してください。

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

ステップ 8 展開のためのタスクのスケジュールを設定します。

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

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

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

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

ステップ 9 [Tasks] ウィンドウで、タスクの展開を監視します。

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

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

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

プロビジョニングされたデバイスを別のサイトに割り当てる

プロビジョニング済みのデバイス（ワイヤレス APを除く）を別のサイトに割り当てるには、次の大まかな手順を実行してください。

プロビジョニング済みのワイヤレス AP を別のフロアに割り当てる場合は、APの再プロビジョニング時に AP 用の別のサイトを選択する必要があります。再プロビジョニングの詳細については、「Day 1 の Cisco AP プロビジョニング （745 ページ）」を参照してください。

手順

ステップ 1 別のサイトに再割り当てするプロビジョニング済みデバイスを、インベントリから削除します。

手順の詳細については、ネットワークデバイスの削除 （218 ページ）を参照してください。

ステップ 2 削除したデバイスをインベントリに再度追加します。

手順の詳細については、ネットワークデバイスの追加 （157 ページ）を参照してください。

ステップ 3 新しく追加したデバイスを必要なサイトに割り当てます。

手順の詳細については、プロビジョニングされていないデバイスのサイトへの割り当て （189 ページ）を参照してください。

デバイスのタグ付け

デバイスタグは属性またはルールに基づいてデバイスをグループ化することができます。各デバイスには複数のタグを付けることができ、各タグは複数のデバイスに適用できます。

デバイスまたはポートがタグ付けされると、そのデバイスまたはポートはそのタグのメンバーになります。タグには次の 2 つのタイプがあります。

- 静的：これらのタグを手動でメンバーに割り当てることができます。

- 動的：Catalyst Center は、定義されたルールに基づいて、これらのタグをメンバーに自動的に割り当てます。

デバイスが削除されて再度追加されると、次の手順が実行されます。

- 静的タグは、メンバーに再割り当てされません。
- 動的タグは、タグ用に定義されたルールを満たすメンバーに再割り当てされます。

[インベントリ（Inventory）] ウィンドウで、デバイス対してタグを追加したり、削除したりできます。

手順

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

ステップ 2 タグを適用するデバイスの横にあるチェックボックスをオンにして、[タグ（Tag）] をクリックします。

ステップ 3 [タグ名（Tag Name）] フィールドにタグ名を入力します。

- 新しいタグを作成するには、[新しいタグの作成（Create New Tag）] をクリックします。ルールを使用して新規タグを作成することもできます。ルールを使用したデバイスのタグ付け （193 ページ） を参照してください。
- 既存のタグを使用する場合は、一覧からタグを選択して、[適用（Apply）] をクリックします。

タグを適用したデバイス名の下に、タグアイコンとタグ名が表示されます。

ステップ 4 デバイスからタグを削除するには、次のいずれか 1 つを行います。

- デバイスを選択し、[Tag] をクリックします。すべてのタグの選択を解除し、[Apply] をクリックします。
- 黄色のタグアイコンまたはタグ名をクリックし、削除アイコンをクリックしてデバイスからタグを削除します。

ネットワーク デバイス グループ タグの作成

ネットワーク デバイス グループ（NDG）タグを作成するには、次の手順を実行します。

手順

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

ステップ 2 タグを適用するデバイスの横にあるチェックボックスをオンにして、[Tag] をクリックします。

ステップ 3 [Create New Tag] をクリックします。

命名パターンには、プレフィックス **NDG:** を使用します。親子階層にタグを設定します。すべての NDG タイプにルートを使用します。たとえば、Location#All Locations、Device Type#All Device Types、または IPSEC#Is IPSEC を使用します。NDG タグの作成時には、ルート全体を使用します。

（注）
- NDG タグの作成中は、カスタムルートを使用できません。Cisco ISE 内のデフォルトの NDG ルート（Location#All Locations、Device Type#All Device Types、および IPSEC#Is IPSEC）のみが許可されます。

  Cisco ISE には、Catalyst Center NDGタグによって上書きされない限り、常にデバイスのデフォルトの NDG ルートがあります。
- デバイスの NDG タイプごとに追加できる NDG タグは 1 つだけです。
- 階層は、親やルートを含む最大 7 レベルです。タグを作成するときに、少なくとも 1 つの子レベルを含めます。
- 各レベル名の最大長は 32 文字です。タグの長さは 100 文字を超えてはなりません。
- NDG タグは、標準 ASCII 文字セットをサポートしています。
- Catalyst Center は、Cisco ISE で設定された NDG 値を反映しません。Catalyst Center での NDG タグの更新により、Cisco ISE で設定された値が上書きされます。

タグを適用したデバイス名の下に、タグアイコンと名前が表示されます。

（注） プレフィックス **NDG:** が付いたタグは、Cisco ISE に反映されます。

ルールを使用したデバイスのタグ付け

タグを定義するルールを作成することによって、デバイスをグループ化できます。ルールを定義するとき、Catalyst Center はルールと一致するすべてのデバイスにタグを適用します。ルールはデバイス名、デバイスファミリ、デバイスシリーズ、IPアドレス、ロケーション、またはバージョンを基準に設定できます。

手順

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

[Inventory] ウィンドウには、検出プロセス中に収集されたデバイス情報が表示されます。

ステップ 2 タグを適用する各デバイスの横にあるチェックボックスをオンにして、[タグ（Tag）]をクリックします。

ステップ 3 [タグ名（Tag Name）] フィールドにタグ名を入力し、 [ルールによる新規タグの作成（Create New Tag with Rule）] をクリックします。

[タグ付きデバイスの合計数（Total Devices Tagged Count）] の下にある [手動で追加（Manually Added）] フィールドは、選択されたデバイスの数を示します。

ステップ 4 [条件の追加（Add Condition）] をクリックして、ルールに必要なフィールドに記入します。

[一致するデバイス（Matching Devices）] の数は、この条件に一致するデバイスの数に応じて、自動的に変更されます。

追加条件を作成するためには、次の 2 つのオプションがあります。

- *And* 条件：[Add Condition] リンクをクリックします。**And** が条件の上に表示されます。
- *Or* 条件：既存の条件の横にある追加アイコン（プラス記号）をクリックします。**Or** は条件の隣に表示されます。

必要に応じていくつでも条件を追加できます。ルールを変更すると、[一致デバイス（Matching Devices）] の数が更新され、ルールに一致するデバイスの数が表示されます。デバイス番号をクリックすると、一致するデバイスが表示されます。

ステップ 5 [保存（Save）] をクリックして、定義されたルールと共にタグを保存します。

タグ付けした各デバイスのデバイス名の下に、タグアイコンとタグ名が表示されます。

デバイスがインベントリに追加されると、定義したruleと一致する場合、タグは自動的にデバイスに適用されます。

デバイスタグの編集

以前に作成したデバイスタグを編集できます。

手順

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

[インベントリ（Inventory）] ウィンドウには、検出プロセス中に収集されたデバイス情報が表示されます。

[デバイス名（Device Name）] 列のデバイス名の下に以前に作成したデバイスタグがありある場合はそれがリスト表示されます。

ステップ 2 デバイスを選択しないで、**[Tag]** をクリックします。

以前に作成されたタグがリストされます。

ステップ 3 [Manage Tags] をクリックします。

[すべてのタグ（All Tags）] スライドイン ペインが表示されます。

ステップ 4 編集するタグの横にある鉛筆アイコンをクリックします。

ステップ 5 タグを編集し、[保存（Save）] をクリックします。

タグの削除

デバイスタグまたはテンプレートタグは、デバイスまたはテンプレートに関連付けられていない場合にのみ削除できます。

始める前に

ルールを使用して、デバイスに静的または動的に関連付けられているタグを削除します。

テンプレートに関連付けられているタグを削除します。

手順

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

ステップ 2 デバイスを選択しないで、**[Tag]** > **[Manage Tags]** の順に選択します。

ステップ 3 削除するタグにマウスカーソルを合わせてから、タグ名の横にある削除アイコンをクリックします。

ステップ 4 プロンプトで [Yes] をクリックします。

タグがデバイスまたはテンプレートに関連付けられている場合は、エラーメッセージが表示されます。デバイスまたはテンプレートに関連付けられているタグを削除してから、タグを削除します。

SSH キー検証エラーへの対処

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

手順

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

ステップ 2 [管理性（Manageability）] 列で、デバイスの [SSHキー認証に失敗（SSH key verification failed）] のリンクをクリックします。

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

問題	結果
SSH キー変更のグローバルな自動受け入れを有効または無効にするには、	[**SSH key configuration**] をクリックします。 詳細については、SSH キー変更の自動承認の設定（196 ページ） を参照してください。
SSH キー検証エラーがあるすべてのデバイスの一覧が表示されるスライドインペインを開くには、	1. [**All errors**] をクリックします。 2. SSH キーの変更を承認するデバイスのチェックボックスをオンにします。 3. [確認（Confirm）] をクリックします。 これにより、選択したデバイスの再同期がトリガーされます。
デバイスの SSH キーが意図的に変更されたことを知っている場合、	[**Confirm**] をクリックします。 これにより、デバイスの再同期がトリガーされます。

SSH キー変更の自動承認の設定

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



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

手順

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

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

デバイスの REP リングの構成

Resilient Ethernet Protocol（REP）はネットワークループの制御、リンク障害の処理、コンバージェンス時間の改善を実現します。

（注）
- REP リングの制限：リングのインターフェイスを介してしか接続できないルートノードは選択しないでください。
- REP リング（非ファブリック）のデバイスサポート：Cisco Catalyst 産業用イーサネット（IE）シリーズ スイッチ 3100、3200、3300、3400、4000、5000、および 9300、ならびに Cisco エンベデッドサービス 3300 シリーズ スイッチ（ESS3300）、S5200、S5800。
- MACsec 暗号化を使用した REP リングを設定できます。

  Cisco Catalyst IE 3100 シリーズ スイッチおよび Cisco Catalyst 9000 シリーズ スイッチは、REP リングを使用した MACsec 暗号化をサポートしていません。

始める前に

- デバイスがオンボーディングされており、到達可能な状態であることを確認します。
- REP リングの終端となっているデバイスとそのインターフェイスを特定します。
- リング内のすべてのインターフェイスが「switchport mode trunk」を使用して設定されていることを確認します。

手順

ステップ 1 メインメニューから次を選択します。**[Workflows]**。次に、[REPリングの設定（非ファブリック）（Configure REP ring (Non-Fabric)）] カードを見つけて、[開始（Start）] をクリックします。

または、次の手順を使用することもできます。

1. [インベントリ（Inventory）] サイトトポロジビューに移動します。
2. REP リングを作成するデバイスノードをクリックして、詳細を表示します。
3. [REPリング（REP Rings）] をクリックし、次に [REPリングを作成（Create REP Ring）] をクリックします。

ステップ 2 タスクの概要ウィンドウが表示されたら、[Let's Do It] をクリックして、ワークフローを開始します。

ステップ 3 **[ルートデバイスを選択（Select a root device）]** ウィンドウで、ルートデバイスを選択し、[次へ（Next）] をクリックします。

（注） デバイスは到達可能で、アップストリーム接続が確立されている必要があります。

ステップ 4 **[ルートデバイスに接続されている隣接デバイスを選択（Select adjacent devices connected to root device）]** ウィンドウで、同じリングに属し、ルートデバイスに直接接続されている 2 つの隣接デバイスを選択します。

a) 1 つ目のデバイスを選択して [次へ（Next）] をクリックします。
b) 2 つ目のデバイスを選択して [次へ（Next）] をクリックします。

ステップ 5 [REPリング検出選択の確認（Review your REP Ring discovery selections）] ウィンドウで、次のタスクを完了します。

a) 設定する REP リングの名前を入力します。
b) 選択したルートおよび隣接デバイスが表示されていることを確認します。
c) 必要に応じて、適切な [編集（Edit）] リンクをクリックして変更を加えます。

ステップ 6 REP リングの設定を開始するには、[プロビジョニング（Provision）] をクリックします。

[REP Ring Configuration Status] ウィンドウで、設定の進捗状況の詳細なステータスを確認できます。

ステップ 7 [REP Ring Summary] ウィンドウに、作成された REP リングの詳細情報が、検出されたデバイスとともに表示されます。
REP リングの作成後、成功メッセージが表示されます。

ステップ 8 REP リングの作成を確認するには、[Inventory] ウィンドウのトポロジビューに移動し、リングの一部であるデバイスをクリックします。 スライドインペインの [REP Rings] タブで、そのデバイスに存在するすべての REP リングのリストを確認できます。

リスト内の REP リング名をクリックすると、リングに存在するデバイス、リングに接続する各デバイスのポートなど、その REP リングの詳細情報が表示されます。

非ファブリック展開用 REP リングへのノードの追加

既存の REP リングに単一のノードを追加するには、次の手順を実行します。ノードは 1 つずつ追加する必要があります。

（注） この機能は、Cisco IE 2000 シリーズ スイッチ、Cisco Catalyst IE 3200 高耐久性シリーズ スイッチ、Cisco Catalyst IE 3300 高耐久性シリーズ スイッチ、Cisco Catalyst IE 3400 高耐久性シリーズ スイッチ、Cisco Catalyst IE 3400 Heavy Duty シリーズ スイッチ、Cisco IE 4000 シリーズ スイッチ、Cisco IE 4010 シリーズ スイッチ、Cisco IE 5000 シリーズ スイッチ、Cisco IE 9300 シリーズ スイッチ、Cisco Catalyst ESS3300 エンベデッド シリーズ スイッチで使用できます。

始める前に

デバイスをCatalyst Centerに追加してください。デバイスを追加する方法については、「デバイスの追加または編集 （710 ページ）」を参照してください。

手順

ステップ 1 [プラグアンドプレイ（Plug and Play）] ワークフローを使用してデバイスの導入準備をして、要求します。

a) メインメニューから次を選択します。[プロビジョニング（Provision）] > [プラグアンドプレイ（Plug and Play）] の順に選択します。

オンボーディングされたデバイスは、[プラグアンドプレイ（Plug and Play）] ウィンドウに表示されます。

b) [Actions] ドロップダウンリストから、[Claim] をクリックします。

c) [サイトの割り当て（Assign Site）] ウィンドウで、[割り当て（Assign）] をクリックしてノードを追加するサイトにデバイスを割り当て、[次へ（Next）] をクリックします。

d) [割り当て（Assign）]、[次へ（Next）] の順にクリックして設定をデバイスに展開します。

（注） プラグアンドプレイ プロビジョニングにより、デバイス オンボーディング テンプレートが自動的に展開されます。詳細については、プラグアンドプレイ プロビジョニングの概要 （695 ページ） を参照してください。

e) [Provision Templates] ウィンドウで、[Preview Configuration] をクリックして設定を確認し、[Claim] をクリックします。

f) [OK] をクリックし、[Yes] をクリックします。

デバイスを要求すると、成功メッセージが表示されます。

g) [Refresh] をクリックします。デバイスのオンボーディングプロセスが完了するまで待ちます。このプロセスには数分かかることがあります。

デフォルトでは、デバイステーブルは 30 秒ごとに更新されます。[Auto-Refresh] ドロップダウンリストをクリックして、更新間隔を選択します。

プロセスが完了すると、デバイスは [プロビジョニング済み（Provisioned）] タブに移動します。

ステップ 2 メインメニューから次を選択します。[Provision] > [Inventory] の順に選択します。

ステップ 3 [Refresh] をクリックし、デバイスが管理対象状態になるまで待ちます。

ステップ 4 デバイスを REP リングに追加します。

a) トポロジマップビューに切り替えるには、トグルボタン（ ）を使用します。

b) REP をクリックし、スライドインペイン で [REP Rings] タブをクリックします。

c) [アクション（Actions）] 列で、省略記号をクリックして [再検出（Rediscover）] を選択します。
デバイスが REP に正常に追加されると、ノード挿入ステータスが [Success] になります。

d) （任意） [REPリング（REP Rings）] タブで、[REP] リンクをクリックして実行された手順を表示します。失敗した場合は、リストを参照して、手順のどの部分でデバイスの挿入に失敗したのかを特定します。

ノードの挿入に失敗した場合は、ノードを再検出します。

非ファブリック展開用 REP リングからのノードの削除

非ファブリック展開の既存の REP リングからノードを削除できます。

REP リングからは次のデバイスを設定できます。

- Cisco Industrial Ethernet（IE）2000、3100、4000、4010、および 5000 シリーズ スイッチ
- Cisco Catalyst IE 3200、3300、3400、3400H、9300、9310、および 9320 高耐久性シリーズ スイッチ
- Cisco エンベデッドサービス 3300（ESS3300）および 9300（ESS9300）シリーズ スイッチ
- Stratix 5400、5410、および 5800 スイッチ

この機能には、次のような制限事項があります。

- 到達不能なデバイスを削除し、REPが設定されたポートではなく、到達可能なデバイスの他のポートを接続すると、REP の検出が失敗します。
- ルートデバイスは削除できません。
- REP リングに物理チャネルとポートチャネルの両方が含まれている場合、ノードを削除すると REP リングが破損する可能性があります。

始める前に

ノードが属する REP リングが完全であることを確認してください。

手順

ステップ 1 デバイスをネットワークから手動で削除します。

ステップ 2 メインメニューから次を選択します。[Provision] > [Inventory] の順に選択します。

ステップ 3 トポロジマップビューに切り替えるには、トグルボタン（ ）を使用します。

REP リングに到達不能なデバイス（手動で削除されたデバイスまたはダウンしたデバイス）がある場合、警告アラートが表示されます。

ステップ 4 警告アラートで、REP リングのリンクをクリックします。
対応する REP リングの スライドインペイン が開きます。

ステップ 5 [REP Rings] タブの [Actions] 列で、省略記号アイコン（ ••• ）にカーソルを合わせ、[Rediscover] をクリックします。

ステップ 6 ダイアログボックスで、**Yes** をクリックします。
システムは REP リングからデバイスを削除し、REP リングの詳細を更新します。

非ファブリック展開用の MRP リング

中断のないネットワーク接続を確保するために、Media Redundancy Protocol（MRP）は、リングネットワークトポロジ内のネットワークリンクのステータスを継続的にモニタリングすることで、産業用ネットワークに耐障害性を提供します。

MRP Media Redundancy Manager（MRM）は、リングの最大リカバリ時間を 10 ミリ秒、30 ミリ秒、200 ミリ秒、500 ミリ秒の範囲で定義します。

MRP は、Cisco Industrial Ethernet（IE）3000、4000、5000 シリーズ スイッチをサポートしています。

（注） 現在、MRP リングのサポートは、Cisco エンベデッドサービス 9300 スイッチ（ESS9300）では利用できません。

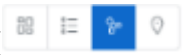
（注）
- システムは、MRP リング内の複数のリングをサポートします。1 つの MRM は最大 3 つのリングで構成できます。
- デフォルトでは、1 つの MRP リングに最大 50 台のデバイスをオンボードできます。
- MRP では、トランクポートとアクセスポートの両方の設定がサポートされています。

非ファブリック展開用の MRP リングステータスの表示

次の手順を使用して、Media Redundancy Protocol（MRP）リングステータスを表示します。

手順

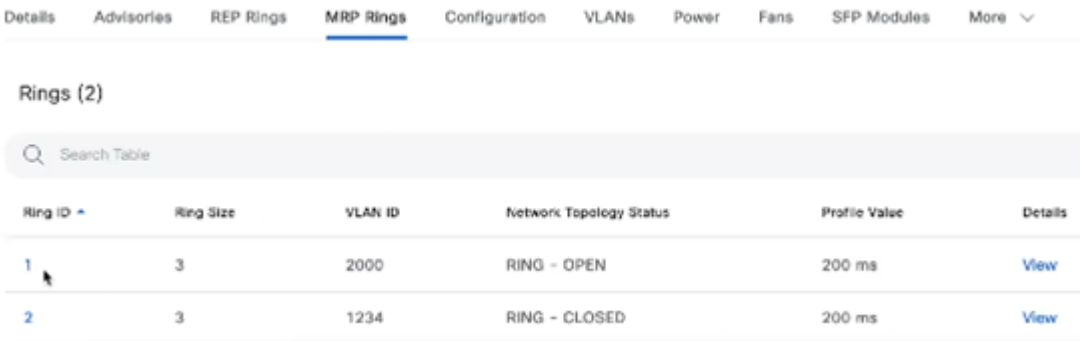
ステップ 1 メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。

ステップ 2 トグルボタン（）を使用して、トポロジマップに切り替えます。

ステップ 3 MRP リングの詳細を表示するには、リングの任意の場所をクリックして、[MRP リング（MRP Rings）] タブをクリックします。

次のテーブルに記載されている詳細を表示できます。

フィールド	説明
Ring ID	デフォルトで割り当てられる番号
Ring Size	リング内のデバイスの数
VLAN ID	デフォルトで割り当てられる番号
Network Topology Status	このフィールドには、次のいずれかのステータスが表示されます。 • [リングオープン（Ring Open）] は、ネットワーク接続の障害を示します。 • [リングクローズ（Ring Closed）]は、ネットワークの正常な動作を示します。
Profile Value	リングの最大回復時間を定義します。



ステップ 4 [リングID（Ring ID）] をクリックすると、次の詳細が表示されます。

フィールド	説明
Hostname	デバイスのホスト名
コンフィギュレーション モード	デバイスのコンフィギュレーション モード

フィールド	説明
Operational Mode	このフィールドには、次のいずれかの動作モードが表示されます。 • [マネージャ（Manager）] は、デバイスがリングの MRM として機能することを示します。 MRM は、ネットワーク障害に対応するためにリングトポロジを開始および制御します。一方のリングポートからリングを介して制御フレームを送信し、もう一方のリングポートからリングを介して受信します。このプロセスは逆方向にも発生します。 • [クライアント（Client）] は、デバイスがメディア冗長性クライアント（MRC）として機能することを示します。 MRC は MRM から受信した再構成フレームに応答し、そのリングポート上のリンクの変化を検出して通知できます。
Port-1/Port-2	インターフェイス名。
Port-1/Port-2 Status	このフィールドには、次のいずれかのステータスが表示されます。 • [無効（Disabled）] は、リングポートが受信したすべてのフレームを破棄することを意味します。 • [ブロック（Blocked）] は、リングポートが、MRP 制御フレームと、LLDP などの一部の標準フレームを除くすべての受信フレームを破棄することを意味します。 • [フォワーディング（Forwarding）]は、リングポートがすべての受信フレームを転送することを意味します。 • [未接続（Not Connected）]は、リンクが物理的にダウンしているか切断されていることを意味します。（この状態は、MRP ポートがソフトウェアによって手動で無効にされている [無効（Disabled）] の状態とは異なります。）

ステップ 5 [リング（Rings）] テーブルの [詳細（Details）] 列にある [表示（View）] ハイパーリンクをクリックして、MRP リングの [概要（Overview）] を表示します。

ドメイン ID、ドメイン名、優先順位、管理対象の Profinet および CLI、ポート MAC アドレスなどの詳細を確認できます。

Parallel Redundancy Protocol

Parallel Redundancy Protocol（PRP）は、イーサネットネットワークでヒットレス冗長性（障害後の回復時間ゼロ）を提供するように設計されています。

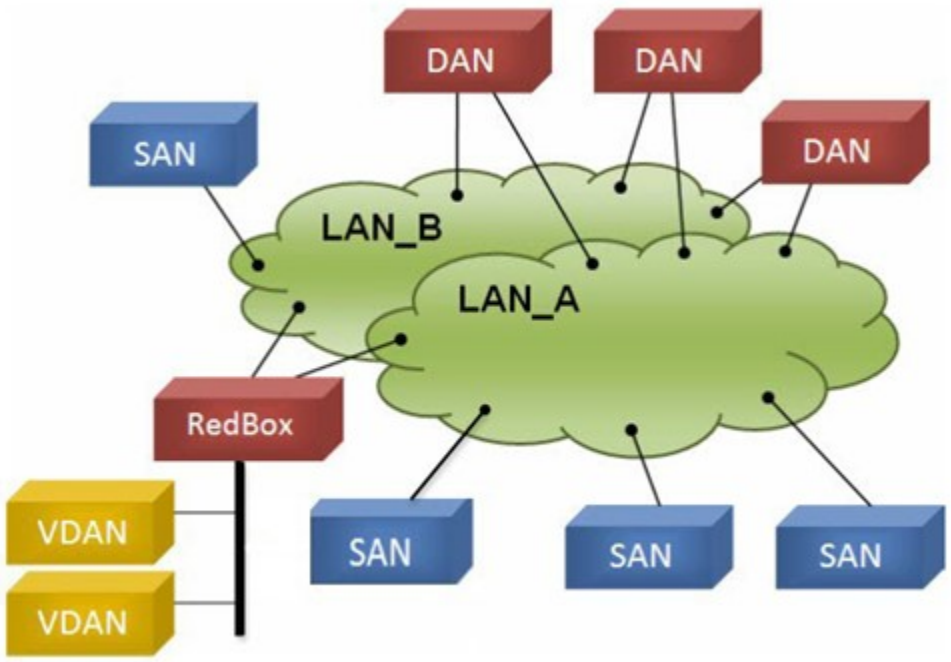
REP や MRP などのプロトコルを使用して、メッシュトポロジまたはリングトポロジでネットワーク要素を設定することで、ネットワーク障害から回復できます。これらの冗長性スキームを使用すると、通常、ネットワークは数ミリ秒から数秒以内にトラフィックフローを回復して再開します。

PRP トポロジのコンポーネント

PRP は、エンドノードを独立した分離した 2 つの並列ネットワーク（LAN-A および LAN-B）に接続することにより、冗長性を提供します。各デュアル通信ノード（DAN）には、ネットワーク内にある他のすべての DAN への冗長パスがあります。

シングル接続ノード（SAN）は、LAN-A または LAN-B のいずれかにのみ接続するネットワーク内の非冗長エンドポイントです。

冗長性ボックス（RedBox）は、エンドノード（デバイス）に 2 つのネットワークポートがなく、PRP 自体を実装しないが、ネットワークの冗長性が必要な場合に、並列冗長プロトコル（PRP）ネットワークで使用されます。このようなエンドノードは、デバイスに 2 つの異なるネットワークへの接続を提供する RedBox に接続できます。RedBox の背後にあるノードは、他のノードに DAN として表示され、仮想 DAN（VDAN）と呼ばれます。RedBox 自体は DAN であり、VDAN に代わってプロキシとして機能します。



PRP トポロジステータスの表示

次の手順を実行して、Parallel Redundancy Protocol（PRP）のステータスを表示します。

PRP トポロジの特性は、次のとおりです。

- Cisco SD-Access 展開にのみ適用
- 設定が正しいことを確認して、適切な LAN A と LAN B を表示します。

PRP は、Cisco Catalyst 産業用イーサネット 3400、4000、4010、および 9320 シリーズ スイッチで動作します。

手順

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

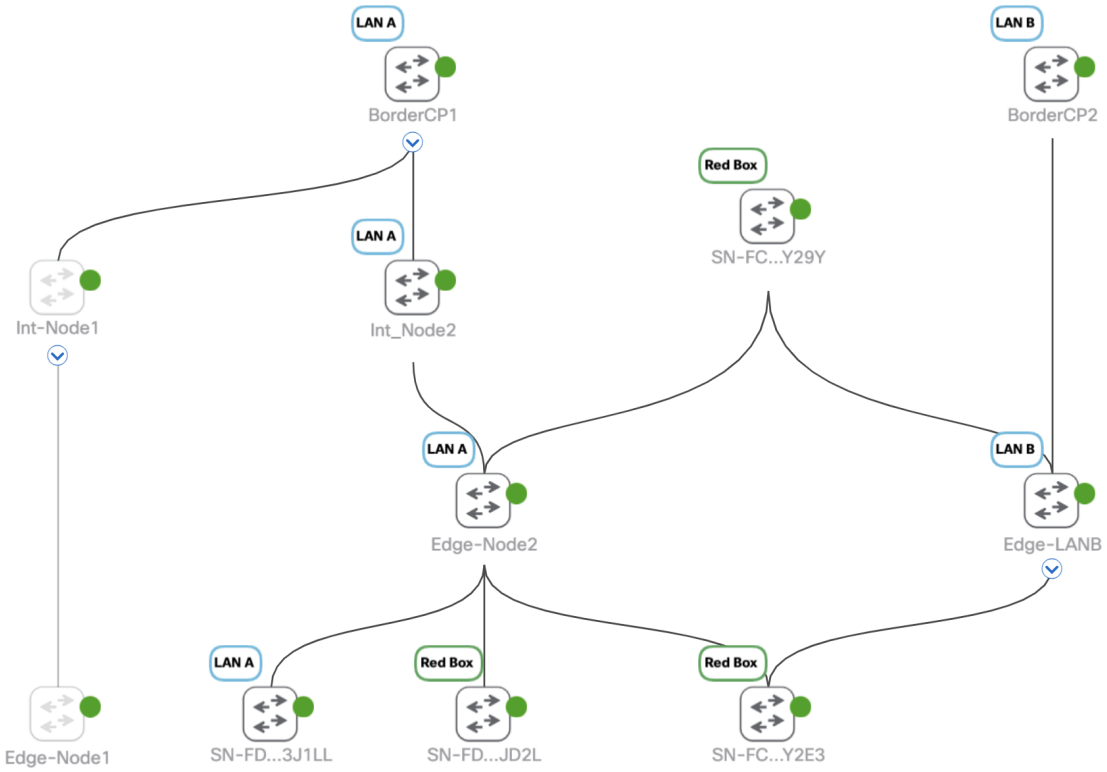
ステップ 2 トポロジマップビューに切り替えるには、トグルボタン（）を使用します。

また、**[ツール（Tools）]** > **[トポロジ（Topology）]**ウィンドウから PRP トポロジを表示することもできます。階層ツリーで、エリア、サイト、建物、またはフロアを選択します。ウィンドウの右上隅にある [トポロジビューのトグル（Toggle Topology View）] ボタンをクリックします。

ステップ 3 RedBox、LAN A、および LAN B のラベルが付けられたデバイスでトポロジをフィルタ処理します。

a) （**フィルタ処理**）アイコンをクリックします。
b) [冗長性（Redundancy）] > [PRP] オプションボタンをクリックします。
c) ドロップダウンリストから、[Redbox、LAN A、LAN Bを表示（Show Redbox, LAN A, LAN B）] を選択します。

トポロジビューに、RedBox、LAN A、LAN B のラベルが付けられたデバイスが表示されます。



（注）
- PRP に参加していないノードとリンクは薄く表示されます。
- ダウンしているリンクは赤い点線で表示されます。

ポートグループの作成

属性またはルールに基づいてポートをグループ化できます。

手順

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

[Inventory] ウィンドウには、ディスカバリプロセス中に収集されたデバイス情報が表示されます。

ステップ 2 新しいポートタグを作成するには、[Tag] をクリックし、[Create New Tag] を選択します。

[Create New Tag] スライドインペインが表示されます。

ステップ 3 [Tag Name] フィールドに、タグ名を入力します。[Description] フィールドに、タグの説明を追加します。

（注） [WAN] タグは予約済みのタグ名です。WAN タグは自動生成されるため、*WAN* という名前の新しいポートタグは作成できません。

ステップ 4 [Tag Rule] 領域で、[Port] タブをクリックします。

ステップ 5 [Device Scope] 領域で、ドロップダウンリストをクリックし、デバイスの [Location] または [Tag Name] を選択して、フィルタを定義します。

ステップ 6 ポートにタグを付けるためのルールを追加するには、アイコンをクリックします。ポートステータス、速度、タグ名、動作ステータス、および説明に基づいてポートにタグを付けることができます。ブール演算子（AND、OR）を使用して条件を追加できます。

条件を削除するには、削除アイコンをクリックします。

ステップ 7 条件が設定されると、ペインの左下隅に条件に一致するポートのリンクが表示されます。

リンクをクリックしてポートを表示します。[Matching Ports] スライドインペインで、ポートが属するデバイスとポート名を表示できます。

ステップ 8 [Save] をクリックします。

ポートへのタグの割り当て

ポートにタグを手動で割り当てることができます。たとえば、システムで生成された **WAN** タグをポートに手動で割り当てることができます。

手順

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

ステップ 2 [Inventory] ウィンドウで、デバイス名をクリックし、[View Device Details] を選択します。

ステップ 3 左ペインで [Interfaces] を展開し、[Ethernet Ports] をクリックします。

ステップ 4 ウィンドウの右上隅で、テーブルビューに切り替えます。

ステップ 5 タグ付けするポート（1 つまたは複数）を選択し、[Tag] をクリックします。

ステップ 6 適切なタグを選択します。

ステップ 7 [Apply] をクリックします。

ポート使用情報

ポートが最後に受信した入力と最後に送信した出力を確認できます。

手順

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

ステップ 2 [Devices] テーブルからデバイス名をクリックし、[View Device Details] をクリックします。

デバイスの詳細がウィンドウに表示されます。

ステップ 3 左ペインで**[Interfaces]** > **[Ethernet Ports]** を選択します。

（注） このタブは、AP 以外のすべてのデバイスに対して表示されます。

ステップ 4 ポートの詳細を表示するには、ポートをクリックします。

このウィンドウでは、ポートが受信した [Last Input] と、ポートが送信した [Last Output] のタイムスタンプを表示できます。

デバイスのメンテナンスモード

デバイスのメンテナンスのスケジュール

Catalyst Center で 1 つ以上のデバイスをメンテナンスモードにすることができます。デバイスがメンテナンスモードになっている場合、Catalyst Center ではデバイスに関連付けられているテレメトリデータは処理されません。障害のあるデバイスをメンテナンスモードにすることで、不要なアラートを防ぐことができます。

（注） デバイスがメンテナンスモードの場合、情報を収集できません。また、ポーリング操作はできません。

（注） シスコ ワイヤレス コントローラおよび AP のメンテナンスモードをスケジュールする際について。

- シスコ ワイヤレス コントローラのメンテナンスをスケジュールすると、ワイヤレスコントローラに関連付けられているすべての AP が同じスケジュールでメンテナンスモードに移行します。
- ワイヤレスコントローラがメンテナンスモードの場合、ワイヤレスコントローラに関連付けられている単一の AP のメンテナンススケジュールを変更することはできません。システムは、デバイスのメンテナンスがすでにスケジュールされていることを示す警告メッセージを表示します。ワイヤレスコントローラのスケジュールを変更すると、そのワイヤレスコントローラの下にあるすべての AP が影響を受けます。
- ワイヤレスコントローラがメンテナンスモードでない場合は、AP を個別に選択し、それのメンテナンスのスケジュールを設定することができます。
- AP をワイヤレスコントローラ間で移動させると、メンテナンスモードは次のような影響を受けます。
  - AP がメンテナンスモードのワイヤレスコントローラからメンテナンスモードではないワイヤレスコントローラに移動する場合、その AP は、移動後にメンテナンスモードになりません。
  - AP がメンテナンスモードではないワイヤレスコントローラからメンテナンスモードのワイヤレスコントローラに移動する場合、その AP は、移動後にメンテナンスモードになります。
  - メンテナンスモードの AP が、メンテナンスモードではないワイヤレスコントローラから、やはりメンテナンスモードではないワイヤレスコントローラに移動する場合、その AP のメンテナンスモードは移動後も維持されます。

手順

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

[Inventory] ウィンドウには、検出プロセス中に収集されたデバイス情報が表示されます。

ステップ 2 メンテナンスをスケジュールするデバイスを選択します。

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

[Schedule Maintenance] スライドインペインが表示されます。

ステップ 4 [Reason For Maintenance] フィールドに、デバイスをメンテナンスモードにする理由を入力します。

デフォルトでは、Catalyst Center が理由を追加し、ユーザーがそれを変更できます。

ステップ 5 [メンテナンスウィンドウの定義（Define Maintenance Window）] エリアで、次の手順を実行します。

a) メンテナンスの開始日時を選択します。
b) メンテナンスの終了日時を選択します。
c) または、[Days/Hours] をクリックして、メンテナンスの日数と時間を入力します。



（注） メンテナンスの繰り返しを選択するには、[日数/時間（Days/Hours）] オプションを選択します。

ステップ 6 [Maintenance Recurrence] 領域で、[None]、[Daily]、または [Weekly] をクリックします。

- [None]：メンテナンスは繰り返されません。
- [Daily]：[Run at Interval（Days）] フィールドに間隔を日単位で入力します。
- [Weekly]:[Run at Interval（Weeks）] フィールドに間隔を週単位で入力します。

ステップ 7 繰り返しに [Daily] または [Weekly] を選択した場合は、[Set Schedule End]チェックボックスをオンにします。

ステップ 8 [End Date] または [End After (Occurrences)] をクリックします。

- [End Date]：メンテナンスを終了する月、日付、年を入力します。
- [End After (Occurrences)]：メンテナンスを終了するまでの回数を入力します。

ステップ 9 [メンテナンスのタイムゾーン（Maintenance Time Zone）] エリアで、メンテナンスのタイムゾーンを選択します。

ステップ 10 [Submit] をクリックします。

デバイスのメンテナンススケジュールの管理

手順

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

ステップ 2 [Actions] ドロップダウンリストから、**[Inventory]** > **[Manage Maintenance]** の順に選択します。

[メンテナンスの管理（Manage Maintenance）] スライドインペイン が表示されます。[Status] 列には、メンテナンススケジュールの現在のステータスが表示されます。

ステップ 3 [検索（Search）] アイコンをクリックしてメンテナンススケジュールを検索するか、[フィルタ（Filter）] アイコンをクリックしてメンテナンススケジュールをフィルタ処理します。

ステップ 4 [Actions] 列で、[Edit] アイコンをクリックして、メンテナンススケジュールを編集します。

（注） 進行中のメンテナンススケジュールの場合、メンテナンスの終了時間のみを延長できます。

ステップ 5 [アクション（Actions）] 列の [削除（Delete）] アイコンをクリックし、メンテナンススケジュールを削除します。

（注） 進行中のメンテナンススケジュールは削除できません。

メンテナンス状態のデバイスの削除

スケジュールされたメンテナンスの完了後に、メンテナンス状態のデバイスを削除できます。

手順

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

ステップ 2 [Actions] ドロップダウンリストから **[Inventory]** > **[Exit Maintenance]** の順に選択します。

ステップ 3 [Exit Maintenance] ウィンドウで、[Confirm] をクリックします。

（注） メンテナンス期間は、個々のデバイス割り当てとは独立して稼働します。メンテナンス期間が開始されると、デバイスがメンテナンス期間から削除されても、メンテナンス期間中は継続します。そのデバイスの新しいメンテナンス期間をスケジュールするには、次のいずれかを実行する必要があります。

- 現在のメンテナンス期間が完了するまで待つ。
- 既存のメンテナンス期間を編集して、より早い時間に終了するように変更する。

インベントリインサイト

[Inventory Insights] ウィンドウには、他の直接接続されたデバイスと設定が一致しないデバイスが表示されます。また、Catalyst Center のベストプラクティスの推奨事項と比較して、誤って設定されたデバイスも表示されます。さらに、デバイス間のリンクが稼働している（アクティ

ブ）かダウンしている（非アクティブ）かを確認できます。デバイス間の接続が存在しない場合、リンクはダウンしています。履歴データが、後で参照できるように保持されます。

たとえば、「デバイス A」と「デバイス B」の間にネットワークリンクがあるとします。「デバイス B」からリンクを削除し、新しい「デバイス C」に接続すると、次のようになります。

- 「デバイス A」と「デバイス B」の間の古いリンクは引き続き存在し、ユーザーが [Tools] > [Topology] ウィンドウから手動で削除できます。[Inventory Insights] ウィンドウでユーザーがアクションを実行する必要はありません。後で参照できるように履歴データが保持されることが示されます。
- 「デバイス A」と「デバイス C」の間の新しいリンクは、稼働状態として表示されます。

Catalyst Center は、推奨されるアクションとともにインサイトを提供します。

速度とデュプレックス設定の不一致

Catalyst Center には、接続されているが、デバイスリンクの両端で異なる速度とデュプレックス値が設定されているデバイスが表示されます。

手順

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

[Inventory Insights] ウィンドウが表示されます。

ステップ 2 [速度/デュプレックス設定の不一致（Speed/Duplex settings mismatch）] をクリックして、デバイスで実行できる推奨アクションを表示します。

推奨アクションが右側のペインに表示されます。

ステップ 3 インスタンスの番号をクリックして、不一致を確認します。

[Speed/Duplex settings mismatch] ウィンドウでは、速度とデュプレックスの不一致が強調表示されます。

ステップ 4 推奨アクションを行って、デバイス設定に必要な変更を加えます。

VLAN の不一致

Catalyst Center は、相互に接続されているが、デバイスリンクの両端で異なる VLAN に設定されているデバイスを示しています。

手順

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

[インベントリ（Inventory）] ウィンドウが表示されます。

ステップ 2 [VLANの不一致（VLAN Mismatch）] をクリックして、デバイスで実行できる推奨アクションを確認します。

推奨アクションが右側のペインに表示されます。

ステップ 3 インスタンスの番号をクリックして、不一致を確認します。

ステップ 4 推奨されるアクションに従ってデバイス設定を更新します。

システムビーコンの管理

システムビーコンを使用して、Catalyst Centerインベントリ内のスイッチを強調表示できます。

システムビーコンは、次のデバイスで有効にできます。

- Cisco Catalyst 9200 シリーズ スイッチ
- Cisco Catalyst 9300 シリーズ スイッチ
- Cisco Catalyst 3850 シリーズ イーサネット スタッカブル スイッチ

手順

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

[Inventory] ウィンドウには、ディスカバリプロセス中に収集されたデバイス情報が表示されます。

ステップ 2 ビーコンを有効または無効にするデバイスを選択します。

（注）
- 一度に最大 5 台のスタンドアロンデバイスでビーコンを有効にできます。
- スタックされたデバイスでビーコンを有効にするには、一度に1つのデバイスのみを選択する必要があります。スタックされたデバイスでは、1 つ以上のスタックメンバーでビーコンを有効にできます。

ステップ 3 [Actions] ドロップダウンリストから、**[Inventory]** > **[Manage System Beacon]**を選択します。

ステップ 4 [Manage System Beacon] スライドインペインで、[System Beacon State] の下の [Enabled] オプションボタンをクリックしてから [Apply] をクリックし、選択したデバイスでビーコンを有効にします。

システムビーコンが有効になると、インベントリのデバイス名の横に青いビーコンアイコン（ ）が表示されます。

ステップ 5 （任意） スタックされたデバイスを選択した場合は、[システムビーコンの管理（Manage System Beacon）] スライドインペインで次の手順を実行します。

a) ビーコンを有効にするスタックメンバーに対応する [システムビーコンステータスを更新しますか？（Update System Beacon Status?）] チェックボックスをオンにします。
b) [System Beacon State] で、[Enabled] オプションボタンをクリックします。
c) [Apply] をクリックします。

ステップ 6 （任意） 選択したデバイスでビーコンを無効にするには、[システムビーコンの管理（Manage System Beacon）] スライドインペインで次の手順を実行します。

a) [System Beacon State] で、[Disabled] オプションボタンをクリックします。
b) [Apply] をクリックします。

または、[インベントリ（Inventory）] ウィンドウで、デバイス名の横にある青いビーコンアイコン（ ）にカーソルを合わせ、[無効化（Disable）] をクリックします。

デバイスのロール

Catalyst Center によるデバイスロールの割り当て

- デバイスを識別してグループ化する
- 特定の設定がデバイスにプッシュされているかどうかを判断する
- ネットワークトポロジマップでのデバイス配置を決定する。

自動ロールは静的または動的に割り当てられます。

- 静的割り当て：プラットフォーム ID またはデバイスファミリに基づいて、特定のデバイスが固定ロールを受信します。これらのロールは変更されません。
- 動的割り当て：他のデバイスは、ネットワークの変更および隣接デバイスとの関係に基づいてロールを受信します。

手動ロールは、Catalyst Center GUI でユーザーによって割り当てられます。手動ロール割り当ては、自動ロール割り当てよりも優先されます。自動ロール割り当ては、トポロジ変更プロセスの一環として定期的に実行されます。

次の表に、各デバイスロールとネットワークトポロジにおける位置を示します。

表 *38* : デバイスのロールとトポロジにおける位置

トポロジにおける位置	デバイス ロール
階層 1	インターネット（設定不可）
階層 2	境界ルータ
階層 3	コア
階層 4	ディストリビューション
階層 5	アクセス
階層 6	不明（Unknown）

デバイスロールを手動で変更する

次の手順を使用して、[Inventory] ウィンドウでデバイスロールを手動で変更します。

デバイスロールの詳細については、「デバイスのロール（214ページ）」を参照してください。

（注）

- デバイスロールを手動で変更すると、割り当ては静的なままになります。変更が検知されたとしても、後続のデバイスの再同期中にデバイス ロールは更新されません。手動で変更した後は、デバイスロールも手動で管理する必要があります。
- Access ロールが自動または手動でデバイスに割り当てられると、サイトの IP デバイストラッキング（IPDT）設定に基づいて IPDT が設定されるか、デバイスから削除されます。

始める前に

インベントリにデバイスがあることを確認します。インベントリにデバイスが存在しない場合は、検出機能を使用して追加します。

手順

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

ステップ 2 [Inventory] テーブルで、ロールを変更するデバイスの横にあるチェックボックスをオンにします。

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

ステップ 4 [Edit Device] スライドインペインで、デバイスロールを更新します。

a) [Device Role] タブをクリックします。

b) [Device Role] ドロップダウンリストから適切なロールを選択します。

c) [Update] をクリックします。

デバイス管理 IP アドレスの更新

デバイスの管理 IP アドレスを更新することができます。

（注） 一度に 1 台のデバイスを更新します。Meraki デバイスの管理 IP アドレスは更新できません。

手順

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

[Inventory] ウィンドウには、検出プロセス中に収集されたデバイス情報が表示されます。

ステップ 2 更新するデバイスを選択します。

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

[デバイスの編集（Edit Device）] スライドインペインが表示されます。

ステップ 4 **[Management IP]** タブをクリックし、**[Device IP/DNS Name]** フィールドに新しい管理 IP アドレスを入力します。

（注） 新しい管理 IP アドレスが Catalyst Center から到達可能であることを確認します。また、デバイスのログイン情報が正しいことを確認します。これらの条件が満たされていない場合、デバイスは管理対象外になる可能性があります。

次のタスク

デバイスを再プロビジョニングして、送信元インターフェイスの設定を更新します。

デバイスポーリング間隔の更新

[システム（System）] > **[設定（Settings）]** > **[ネットワーク再同期間隔（Network Resync Interval）]** の順に選択すると、すべてのデバイスのポーリング間隔をグローバルに更新できます。特定のデバイスのポーリング間隔を更新するには、[デバイスインベントリ（Device Inventory）] を選択します。[ネットワーク再同期間隔（Network Resync Interval）] を使用して

設定した値により、[デバイスインベントリ（Device Inventory）] で設定した値が置き換えられます。

デバイスにポーリングさせない場合は、ポーリングを無効にできます。

始める前に

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

手順

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

ステップ 2 更新するデバイスを選択します。

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

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

ステップ 5 再同期タイプを選択します。

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

ステップ 6 [Resync Interval (in Mins)] フィールドで、連続するポーリングサイクル間の時間間隔（分単位）を入力します。

ステップ 7 [Update] をクリックします。

デバイス情報の再同期

選択したデバイスのデバイス情報は、デバイス再同期の間隔の設定にかかわらず、ただちに再同期できます。

（注） 同時に再同期できるデバイスの数は、デバイスの設定サイズや、関連付けられている AP の数によって異なります。何千もの AP がある環境では、リソースの競合により、同期リクエストはキューに入り、優先順位に基づいて処理される場合があります。

手順

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

[Inventory] ウィンドウには、検出プロセス中に収集されたデバイス情報が表示されます。

ステップ 2 情報を収集するデバイスを選択します。

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

（注） 特定のデバイスに対して再同期が行われると、そのデバイスのデバッグログが自動的に有効になり、XDE およびデバイスパックのログが **[System]** > **[System 360]** > **[Cluster Tools]** > **[Monitoring]** または > **[Log Explorer]**で収集されます。

ステップ 4 [OK] をクリックします。

ネットワークデバイスの削除

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

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

（注）
- デバイスがファブリックネットワークの一部である場合は削除できません。ファブリックネットワークからデバイスを削除し、その後インベントリから削除します。手順の詳細については、ファブリックからデバイスを削除 （1239 ページ）を参照してください。
- ワイヤレスセンサーをインベントリから削除すると、センサーは工場出荷時のデフォルト状態にリセットされます。センサーが再参加すると、現在の設定が取得されます。

始める前に

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

手順

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

[Inventory] ウィンドウには、検出プロセス中に収集されたデバイス情報が表示されます。

ステップ 2 削除するデバイスの横にあるチェックボックスをオンにします。

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

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

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

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

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

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

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

ステップ 5 **[OK]** をクリックして、アクションを確認します。

コマンド ランナーを起動（インベントリ）

[インベントリ（Inventory）] ウィンドウで、選択したデバイスのコマンドランナーアプリケーションを起動できます。

始める前に

コマンド ランナー アプリケーションをインストールします。詳細については、*Cisco Catalyst Center Administrator Guide*を参照してください。

手順

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

[Inventory] ウィンドウには、検出プロセス中に収集されたデバイス情報が表示されます。

ステップ 2 コマンドを実行するデバイスを選択します。

ステップ 3 [Actions] ドロップダウンリストから、**[More]** > **[Command Runner]** の順に選択します。

実行可能なコマンドの詳細とその実行方法については、「デバイスの診断コマンドの実行（691 ページ）」を参照してください。

Run コマンドを使用したデバイスの到達可能性に関する問題のトラブルシューティング

[インベントリ（Inventory）] ウィンドウから [コマンドの実行（Run Commands）] ウィンドウを起動し、ping、traceroute、snmpget などのプラットフォームコマンドを実行して、デバイスの到達可能性の問題をトラブルシュートできます。

（注） Catalyst Center クラスタでプラットフォームコマンドを直接実行する場合は、[Run Commands] を起動する前にデバイスを選択しないでください。デバイスを選択すると、プラットフォームではなく、そのデバイスに対してコマンドが実行されます。

始める前に

コマンド ランナー アプリケーションをインストールします。詳細については、*Cisco Catalyst Center Administrator Guide*を参照してください。

手順

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

ステップ 2 [Actions] ドロップダウンリストから、**[More]** > **[Run Commands]** の順に選択します。

man を入力すると、現在サポートされているコマンドおよびショートカットのリストをいつでも取得できます。

CSVファイルを使用したデバイス設定のインポート/エクスポート

CSV ファイルのインポート

CSV ファイルを使用して、別のソースから Catalyst Center にデバイスの設定やサイトをインポートできます。サンプルテンプレートをダウンロードするには、次の手順を完了します。

1. **[Inventory]** ウィンドウに移動し、**[Add Device]** をクリックします。
2. **[Add Device]** スライドインペインで、**[Import Inventory]** をクリックします。
3. [Download Template] をクリックして、サンプル CSV ファイルテンプレートをダウンロードします。

CSV ファイルを使用してデバイスまたはサイト設定をインポートする場合、Catalyst Center がデバイスをどれだけ管理できるのかは CSV ファイルに指定する情報に依存します。CLI ユーザー名、パスワード、およびイネーブルパスワードの値を指定しない場合、Catalyst Center の機能が制限され、デバイス設定の変更、デバイス ソフトウェア イメージの更新、および他の重要な機能を実行できません。

CSV ファイルでクレデンシャル プロファイルを指定し、対応するクレデンシャルをデバイスのセットに適用できます。ログイン情報プロファイルを指定して、CSV ファイルに手動で値も入力する場合、手動入力されたログイン情報が優先されます。管理では、手動入力されたログイン情報とログイン情報プロファイルの組み合わせが使用されます。たとえば、手動で入力した SNMP ログイン情報に加えて、SNMP および SSH または Telnet のログイン情報を含むログイン情報プロファイルが CSV ファイルに含まれている場合、デバイスは手動で入力された SNMP ログイン情報とログイン情報プロファイル内の SSH または Telnet ログイン情報に基づいて管理されます。セキュリティを確保するため、Telnet ではなく SSH を使用してください。

（注） また、指定したプロトコルに対応するフィールドにも値を入力する必要があります。たとえば、SNMPv3 を指定した場合、SNMPv3 のユーザー名や認証パスワードなど、サンプルの CSV ファイルの SNMPV3 フィールドに値を指定する必要があります。

Catalyst Center の部分的なインベントリ収集の場合は、CSV ファイルに次の値を指定する必要があります。

- デバイスの IP アドレス
- SNMP バージョン
- SNMP 読み取り専用コミュニティ ストリング
- SNMP 書き込みコミュニティ ストリング

- SNMP 再試行値
- SNMP タイムアウト値

Catalyst Center の完全なインベントリ収集では、CSV ファイルに次の値を指定する必要があります。

- デバイスの IP アドレス
- SNMP バージョン
- SNMP 読み取り専用コミュニティ ストリング
- SNMP 書き込みコミュニティ ストリング
- SNMP 再試行値
- SNMP タイムアウト値
- プロトコル
- CLI ユーザー名
- CLI パスワード
- CLI イネーブル パスワード
- CLI タイムアウト値

CSV ファイル エクスポート

Catalyst Center では、すべてまたは選択したデバイスを含む CSV ファイルをインベントリに作成できます。このファイルを作成するには、ファイルに含まれる設定データを保護するパスワードを入力する必要があります。

CSV ファイルからのデバイス設定のインポート

CSV ファイルからデバイス設定をインポートできます。

手順

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

[Inventory] ウィンドウには、検出プロセス中に収集されたデバイス情報が表示されます。

ステップ 2 [Add Device] をクリックします。

ステップ 3 [デバイスの追加（Add Device）] スライドインペインで、[インベントリのインポート（Import Inventory）] をクリックしてデバイスのログイン情報をインポートします。

ステップ 4 [インベントリのインポート（Import Inventory）] スライドインペインで、CSV ファイルをボックスエリアにドラッグアンドドロップします。または、[ファイルの選択（Choose a file）] をクリックし、CSV ファイルを参照します。

ステップ 5 [Import] をクリックします。

デバイスデータのエクスポート

選択したデバイスに関する特定のデータを CSV ファイルにエクスポートできます。CSV ファイルは圧縮されます。[Export] をクリックして、フィルタ処理されたデバイスまたはすべてのデバイスのデータをエクスポートします。



注意 CSV ファイルにはエクスポートされたデバイスに関する機密情報が含まれているため、取り扱いには注意してください。特別な権限を持つユーザーのみがデバイスのエクスポートを行うことを確認します。

手順

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

[Inventory] ウィンドウには、検出プロセス中に収集されたデバイス情報が表示されます。

ステップ 2 特定のデバイスのみの構成情報をエクスポートするには、含めるデバイスの横にあるチェックボックスをオンにします。すべてのデバイスを含めるには、デバイスリストの最上部にあるチェックボックスをオンにします。

ステップ 3 [Actions] ドロップダウンリストから、[Inventory] > [Export Inventory] > を選択してデバイス設定をエクスポートします。

[Export Inventory] ダイアログボックスが表示されます。

ステップ 4 **[パスワード（Password）]** フィールドに、エクスポートされた CSV ファイルを暗号化するために使用するパスワードを入力します。



（注） エクスポートしたファイルを開くには、パスワードが必要です。

ステップ 5 確認のために暗号化パスワードをもう一度入力します。

ステップ 6 [Include SSH key information] チェックボックスをオンにして、最初の SSH 鍵、最初の SSH 鍵アルゴリズム、現在の SSH 鍵、現在の SSH 鍵アルゴリズムなどの情報をエクスポートした CSV ファイルに追加します。

ステップ 7 [Export] をクリックします。

（注） ブラウザの設定によっては、圧縮したファイルを保存したり、開くことができます。

デバイスのログイン情報のエクスポート

デバイスのクレデンシャル CSV ファイルにエクスポートできます。不要なアクセスからファイルを保護するために、パスワードを設定する必要があります。ファイルを開くことができるように、受信者にパスワードを提供する必要があります。

注意 CSV ファイルにはエクスポートされたデバイスのすべてのクレデンシャルがリストされているため、取り扱いには注意してください。特別な権限を持つユーザーのみがデバイスのエクスポートを行うようにしてください。

手順

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

[Inventory] ウィンドウには、検出プロセス中に収集されたデバイス情報が表示されます。

ステップ 2 CSV ファイルに含めるデバイスの横にあるチェックボックスをオンにします。すべてのデバイスを含めるには、リストの最上部にあるチェックボックスをオンにします。

ステップ 3 [Actions] ドロップダウンリストから **[Inventory]** > **[Export Inventory]** を選択します。

[Export] ダイアログボックスが表示されます。

ステップ 4 [Select Export Type] で、[Credentials] オプションボタンをクリックします。

ステップ 5 [Include SSH key information] チェックボックスをオンにして、最初の SSH 鍵、最初の SSH 鍵アルゴリズム、現在の SSH 鍵、現在の SSH 鍵アルゴリズムなどの情報をエクスポートした CSV ファイルに追加します。

ステップ 6 **[パスワード（Password）]** フィールドに、エクスポートされた CSV ファイルを暗号化するために使用するパスワードを入力します。

（注） エクスポートしたファイルを開くには、パスワードが必要です。

ステップ 7 暗号化パスワードを確認し、[エクスポート（Export）] をクリックします。

（注） ブラウザの設定によっては、圧縮したファイルを保存したり、開くことができます。

デバイスの構成ドリフト

デバイスで行った構成の変更は、内部 Catalyst Center サーバーに保存されます。構成ドリフトの表示方法については、「デバイスの構成ドリフトの表示（226ページ）」を参照してください。

次のイベントが発生すると、構成ドリフトがキャプチャされます。

- 初回収集：Catalyst Center にデバイスを追加すると、デバイス構成が収集されます。
- syslog ベース収集：Catalyst Center は、デバイスによって送信された syslog イベントを監視し、構成の変更を特定します。構成アーカイブは、最新のイベントが発生してから 2 分後にトリガーされます。syslog イベントのログイン IP アドレスに基づいて、構成ドリフトは（Catalyst Center によって構成が変更される）インバンドか（Catalyst Center 外で構成が変更される）アウトオブバンドとしてマークされます。

（注）

- Syslog ベースの収集を機能させるには、[Design] > [Network Settings] > [Telemetry] > [Syslogs] で Catalyst Center を Syslog サーバーとして設定する必要があります。詳細については、テレメトリを使用した syslog、SNMP トラップ、NetFlow コレクタサーバー、および有線クライアントデータ収集の設定（59 ページ）を参照してください。
- 2 分以内の新しいトラップはタイマーを再起動し、部分的な変更を伴う複数のアーカイブを回避します。正確な結果を得るには、少なくとも 2 分間待つことをお勧めします。

- [Daily Backup Collection]：Catalyst Center は、毎日午後 11:00（UTC タイムゾーン）に実行するようにスケジュールされたデバイス構成の自動バックアップを実行します。このプロセス中、Catalyst Center は、最後にデバイス構成の収集が行われた時点のタイムスタンプと、デバイス構成がアーカイブされた時点のタイムスタンプを比較します。この差が 30 分を超える場合は、デバイス構成のアーカイブが実行されます。
- [Weekly Backup Collection]：Catalyst Center は、毎週日曜日の午後 11:30（UTC タイムゾーン）に実行するようにスケジュールされたデバイス構成の定期的な週次バックアップを実行します。デバイスに関して上記のどのイベントも受信されない場合、Catalyst Center の外部または Catalyst Center 内で行われた設定変更は、週次バックアップアーカイブによっ

てキャプチャされます。詳細については、『Cisco Catalyst Center Administrator Guide』の「Configure Device Configuration Backup Settings」を参照してください。

（注） 週次バックアップアーカイブによって検出された構成ドリフトは、Catalyst Center 外で構成が変更された可能性がある場合でも、（Catalyst Center によって構成が変更される）インバンドとして分類されます。

（注）
- デバイスに関して保存された構成ドリフトの数が、[System] > [Settings] > [Device Settings] > [Configuration Archive] > [Internal] ウィンドウで設定された値を超えると、最も古い構成が自動的に削除され、新しい構成をアーカイブするためのスペースが作成されます。デバイスごとに保存できる構成ドリフトのデフォルト値は 15 で、最大値は 50 です。
- 変更がない場合、収集されたアーカイブを無視することでディスク使用率が最適化されます。ディスク容量の最適化は、初回収集には適用されません。

デバイスの構成ドリフトの表示

手順

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

ステップ 2 [Devices] テーブルで、デバイス名をクリックします。そのデバイスに関する情報が表示されます。

ステップ 3 [View Device Details] ハイパーリンクをクリックします。

デバイスの詳細がウィンドウに表示されます。

ステップ 4 左ペインで、[Config Drift] をクリックします。

[設定の変更（Configuration Changes）] ウィンドウが表示され、次の情報を確認できます。

- [Total config drifts being saved]：ラベル付きの設定を含む、デバイスごとに保存された設定のばらつきの数が表示されます。

  デバイスごとに保存された設定のばらつきの数は、**[System]** > **[Settings]** > **[Device Settings]** > **[Configuration Archive]** ウィンドウから変更できます。

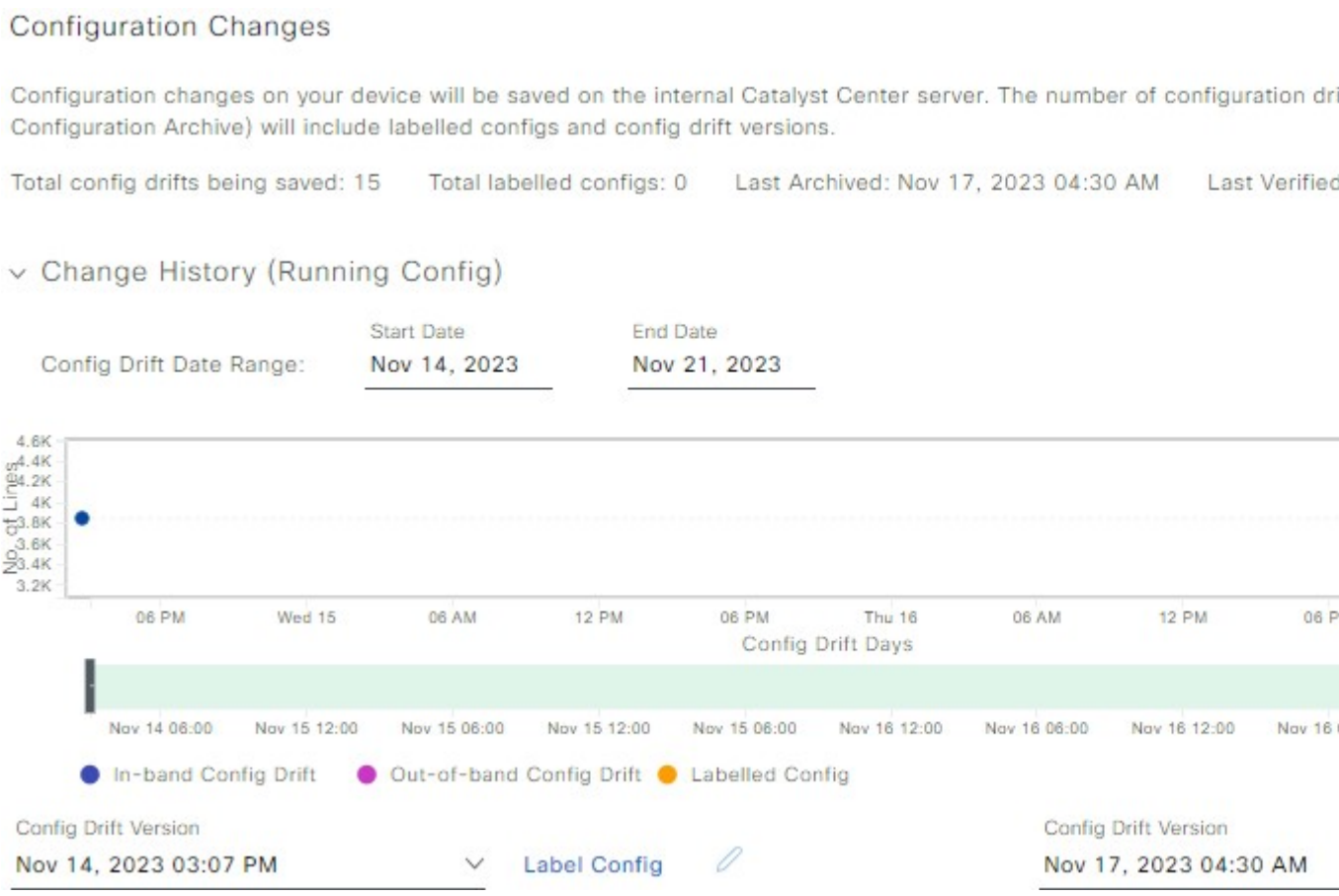
- [Total Labeled configs]：デバイスのラベル付き設定の数が表示されます。

- [Last Archived]：最後にアーカイブされた設定のタイムスタンプが表示されます。このタイムスタンプを確認することで、ユーザーは最新の設定データにアクセスできます。また、最後にアーカイブされた設定の特定の時刻を知ることで、変更を追跡し、潜在的な問題や不一致を特定できます。

  ネットワークデバイスの構成をアーカイブする方法については、Cisco Catalyst Center 管理者ガイド [英語] の「Configure Device Configuration Backup Settings」の項を参照してください。

- [Last Verified]：システムがイベントを受信したときに実行された config-rift 検証のタイムスタンプが表示されます。イベントは、前の項で説明した初回収集、syslog ベースの収集、日次バックアップ収集、または週次バックアップ収集を指します。

  最後に検証されたタイムスタンプを使用すると、チェックが最後に実行された時刻をモニターでき、デバイスの設定の不整合が継続的にモニターされます。



ステップ 5 [変更履歴（Change History）] タブを展開して、次の詳細を表示します。

a) [Config drift date range]：[Start Date] と [End date] をクリックして、構成ドリフトを表示する日付範囲を選択します。デフォルトでは、開始日と終了日は、過去 15 日間の構成ドリフトを表示するように設定されています。

b) [Config drift timeline graph]：選択した日付範囲の構成ドリフトを表示します。デフォルトでは、過去 15 日間の構成ドリフトがタイムライングラフに表示されます。

タイムライングラフには、次の詳細が表示されます。

- [In-band Config Drift]：Catalyst Center によって行われた設定変更は、タイムライングラフに青いバブルとして表示されます。
- [Out-of-band Config Drift]：Catalyst Center の外で行われた設定変更は、タイムライングラフに紫色のバブルとして表示されます。
- [Labeled Config]：ラベル付きで Catalyst Center にアーカイブされた設定バージョンは、タイムライングラフにオレンジ色のバブルとして表示されます。詳細については、構成ドリフトのラベル付け （228 ページ）を参照してください。

c) [Config Drift Version]：下矢印をクリックして、使用可能なすべての構成ドリフトバージョンを表示します。

d) [Running Config]：タイムライングラフの構成ドリフトをクリックします。比較が [Running Config] タブに表示されます。設定バージョン間の違いは、見やすくするために異なる色でマークされています。

構成ドリフトのラベル付け

将来の参照のために、時系列グラフで構成ドリフトにラベルを付けることができます。ラベル付き構成ドリフトは、ラベルが外されないかぎり削除されません。

手順

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

ステップ 2 デバイス名をクリックすると、そのデバイスの詳細情報が表示されます。

ステップ 3 [View Device Details] をクリックします。

デバイスの詳細がウィンドウに表示されます。

ステップ 4 左ペインで、[Config Drift] をクリックします。

[設定変更（Configuration Changes）] ウィンドウが表示されます。

ステップ 5 ラベルを付ける時系列グラフの構成ドリフトを選択します。選択した構成ドリフトのタイムスタンプは、時系列グラフの下の [構成ドリフトバージョン（Config Drift Version）] に表示されます。

ステップ 6 選択した構成ドリフトバージョンに対応する [Label Config] をクリックします。

ステップ 7 [Label Configuration] ウィンドウで、設定バージョンの名前を入力します。ラベル設定のプレフィックスは CCA_ に固定されています。

（注） 設定バージョン名に特殊文字を使用しないでください。

ステップ 8 [Save] をクリックします。ラベル付きの構成ドリフトは、時系列グラフでオレンジ色で表示されます。

（注）
- ラベル付けされた設定バージョンの数が選択した範囲より大きい場合は、保存される構成ドリフトの合計数を変更します。保存する構成ドリフトの数を設定する方法の詳細については、*Cisco Catalyst Center Administrator Guide* の「Configure Device Configuration Backup Settings」のセクションを参照してください。
- Catalyst Center では、構成ドリフト全体の最大 80% までラベル付けできます。ラベル付き構成ドリフトがこの 80% のしきい値に達したユーザーには、[設定変更（Configuration Changes）] ウィンドウの上部に警告バナーが表示されます。

ステップ 9 ラベルを削除するには、ラベル付きの設定バージョンを選択し、[Remove label] をクリックします。

デバイス構成の可視性と制御

[Visibility and Control of Configurations] 機能は、計画したネットワークの構成をデバイスに展開する前にセキュリティを強化するソリューションを提供します。優れた可視化機能により、デバイス構成を展開する前にプレビューできます（CLI および NETCONF コマンドを使用）。強化された制御機能により、IT サービス管理（ITSM）チェックを通じて、承認された構成のみをネットワークデバイスにプロビジョニングできます。これら 2 つのオプションにより、自分のペースで構成をプレビューできる柔軟性も得られます。構成は、可視性と制御がサポートされているワークフローの処理中に、すぐに、または処理後に **[Activities]** > **[Tasks]** ウィンドウでレビューできます。

デフォルトでは、[Visibility and Control of Configurations] 設定には次の構成が含まれています。

- 設定の可視性（[Configuration Preview]）が有効になっています。
- 設定の制御（[ITSM Approval]）が無効になっています。

これらの設定を有効または無効にするには、*Cisco Catalyst Center Administrator Guide*の「Enable Visibility and Control of Configurations」を参照してください。

（注）
プロビジョニング ワークフローで [Visibility and Control of Configurations] がサポートされている場合は、タスク展開のスケジュール時に次のバナーメッセージが表示されます。

このワークフローでは、ネットワーク管理者などのユーザーがネットワークデバイスにワークフローを展開する前に、設定をプレビューできます。ワークフロー設定を構成するには、**[System]** > **[Settings]** > **[Visibility and Control of Configurations]**に移動します。

構成ワークフローの可視性と制御

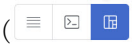
プロビジョニング ワークフロー中のタスクのスケジュール時に、[Visibility and Control of Configurations] の設定に基づいて、次のタスクを実行できます。

- [Configuration Preview] が有効になっている場合は、デフォルトで [Preview and Deploy (Recommended)] が選択されます。これは、デバイス構成を展開する前にプレビューする必要があるために、[Now] および [Later] のスケジュールオプションがグレー表示（使用不可）になることを意味します。
- [Configuration Preview] と [ITSM Approval] が有効になっている場合は、デフォルトで [Preview and Deploy (Recommended)] が選択されます。これは、デバイス構成を展開する前にプレビューし、IT 管理者に送信して承認を得る必要があるために、[Now] および [Later] のスケジュールオプションがグレー表示（使用不可）になることを意味します。
- [Configuration Preview] と [ITSM Approval] が無効になっている場合は、使用可能なオプション（[Now]、[Later]、または [Preview and Deploy (Recommended)]）を選択できます。

[Preview and Deploy (Recommended)] を選択した場合、Catalyst Center は次の基本的な手順を実行します。

	ステップ	説明
1	Catalyst Center は、一連のネットワーク プロビジョニングの事前チェックを実行して、シームレスなプロビジョニング操作を保証します。	[Performing Initial Checks] ウィンドウで、Catalyst Center により [Pending Operations] と [Device Compliance] の問題がチェックされて通知されます。 確認されたすべての問題に対処し、再チェックを実行して、すべての検証を成功させる必要があります。詳細については、ネットワーク プロビジョニングの事前チェック（240 ページ）を参照してください。
2	Catalyst Center により、構成を生成するために選択したデバイスが準備されます。	プロビジョニング ワークフローでワークフローの進行状況ビューがサポートされている場合、[Preparing Devices and Configuration Models] ウィンドウに、リストされたデバイスを準備するためにシステムで実行される手順が表示されます。それ以外の場合は、進行中のメッセージが表示されます。 この準備手順には時間がかかるため、ワークフローを終了して後で戻ることができます。その間、準備プロセスはバックグラウンドで続行されます。
3	Catalyst Center により、最初にリストされたデバイスのデバイス構成が表示されます。	Catalyst Center により、最初にリストされたデバイスの実行中の構成と計画された構成の対象比較が [Preview Configuration] ウィンドウに表示されます。 デバイス構成を確認し、準備ができたら展開するか、ITSM 承認のために送信できます。

[Preview Configuration] ウィンドウで構成を確認しながら、次のタスクを実行できます。

目的	手順
デバイスの構成をプレビューします。	左側のペインでデバイスを選択します。
[Configuration Preview] ペインでデータをフィルタ処理します。	[View by Configuration Source] ドロップダウンリストから、使用可能なオプションを選択します。
計画された構成と実行中の構成の対象比較を表示するか、計画された構成のみを表示します。	ビュースイッチャ（）をクリックします。 （注） 並列比較ビューは YANG 構成の表示には対応していません。
実行中の構成と計画された構成の間で対応するコマンドを強調表示します。	一方の構成で1つのコマンドをクリックすると、もう一方の構成で対応するコマンドが強調表示されます。 （注） 次の制限事項に注意してください。 • システムでは、サブレベルのコマンドではなく、第 1 レベルのコマンドに対する並列強調表示のみがサポートされています。 • 構成間で強調表示を並べて表示するには、すべてのコマンドが完全に一致している必要があります。 • 一方の構成で No で始まるコマンドをクリックすると、もう一方の構成で一致をチェックするときに No の部分が無視されます。
表示された構成内の値を検索します。	[Search configuration] フィールドを使用します。
Cisco Catalyst 9800 シリーズ ワイヤレスコントローラのツリービューで YANG 構成をプレビューします。	[Tree View]（）ボタンをクリックします。 （注） [View by Configuration Source] ドロップダウンリストは、ツリービューでは使用できません。

目的	手順
Cisco IOS XE リリース 17.15.1 以降を実行している Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの場合、YANG 構成から IOS CLI を生成します。	

目的	手順
	[Generate CLI from Yang Configuration]（）ボタンをクリックします。 （注） 次の制限事項に注意してください。 • IOS CLI の生成にかかる時間は、ネットワークの規模と現在の操作のタイプによって異なります。 • YANG 構成からの IOS CLI の生成は、Catalyst 9000 シリーズ スイッチの組み込み ワイヤレス コントローラ ではサポートされていません。 • ワイヤレスコントローラ で候補データストアを使用した候補設定機能が有効になっている場合、YANG 構成からの IOS CLI の生成はサポートされません。 • 設定を変更して IOS CLI を生成すると、YANG 構成を適用した後のデバイスでの CLI の変更が構成プレビューに表示されます。ワイヤレスコントローラ で生成された CLI を使用することはできません。 たとえば、現在のデバイス構成がすでに YANG 構成と一致している場合、構成プレビューで生成された IOS CLI にはコマンドは含まれません。 • 検証が失敗した場合、IOS CLI は構成プレビューの YANG 構成から生成されません。 • 一部のオブジェクトの管理状態は、変更された設定を適用する前に **shutdown** 状態に変更する必要があります。オブジェクトの管理状態は、このような変更に向けた CLI シーケンスの最後に **no shutdown** 状態に戻ります。これらの設定では、構成プレビューに **shutdown** コマンドの CLI がシーケンスに含まれていません。 たとえば、WLAN でメディアストリーム、ブロードキャスト SSID、および無線を設定する場合、YANG 構成はシャットダウンとアクティブ化を内部で処理します。次に、この設定に向けた理想的な CLI シーケンスの例を示します。

目的	手順
	wlan test4 shutdown broadcast-ssid dot11bg 11g media-stream multicast-direct no shutdown ただし、YANG 構成から生成された CLI には **shutdown** コマンドが含まれていない場合があります。次に、YANG構成から生成されたCLIの例を示します。 wlan test4 broadcast-ssid dot11bg 11g media-stream multicast-direct no shutdown したがって、構成プレビューで生成されたCLIは、Virtual TeleType（VTY）で使用すると、ワイヤレスコントローラ で機能しない場合があります。
ワークフローの進行状況ビューを表示します。	左側のペインでデバイスを選択し、右側のペインの右上隅にある [Back to workflow progress] をクリックします。[Configuration Preview] ペインに戻るには、[Go to generated config] をクリックします。 （注） [Back to workflow progress] および [Go to generate config] は、ワークフローでワークフローの進行状況ビューがサポートされている場合にのみ使用できます。
ワークフローを終了し、後でデバイス構成を確認します。	[Exit and Preview Later] をクリックします。 構成の確認を続ける準備ができたら、**[Activities]** > **[Tasks]**ウィンドウに移動し、関連する作業項目を開きます。

構成を確認したら、[Visibility and Control of Configuration] の設定に応じて、次のタスクを実行できます。

目的	手順
作業項目を完全に破棄します。	[**Discard**] をクリックし、[**Discard**] ダイアログボックスで [**Accept**] をクリックします。 （注） • 破棄した後、2 週間後に完全に破棄されます。 • 設定プレビューを破棄した後も、関連するデバイスの完了済み設定のプレビューを表示できます。この可視性により、ユーザーやIT管理者は、デバイス設定に関連する問題を調査できます。

目的	手順
構成を展開するか、ITSM承認のために送信します。	

目的	手順
	[Deploy] または [Submit for ITSM Approval] をクリックします。 （注） • [Deploy] ではなく [Save Intent] が表示される場合、ワークフロー中に選択したパラメータはすでにデバイスに存在します。これらのパラメータをデータベースに保存するには、[Save Intent] をクリックします。デバイスの構成要件はすでに満たされているため、構成はデバイスにプッシュされません。 • 複数のデバイスがある場合は、各デバイスをクリックして構成をプレビューする必要があります。ただし、[Deploy] をクリックすると、すべてのデバイスで構成がプレビューされていない場合でも、構成がすべてのデバイスにプッシュされます。 スライドインペインで、展開の日時をスケジュールし、ITSM承認のために構成を送信する場合は、IT管理者向けのメモを追加します。その後、[Submit] をクリックします。 （注） プロビジョニングタスクの場合、デバイスで構成を展開すると、**[Activities]** > **[Tasks]**で進行中のプロビジョニングタスクの進行状況が [Task Progress] バーに表示されます（タスク名をクリックすると表示されます）。 作業項目の承認ステータスまたはタスクの展開ステータスは、[Tasks] ウィンドウで確認できます。作業項目が承認されていない場合は、ITSM承認のために作業項目を再送信する必要があります。承認された作業項目は、スケジュールされた時刻に展開されます。 （注） 構成をプレビューすると、Catalyst Center によって構成プレビューのスナップショットが作成されます。展開の操作がスケジュールされた後にネットワーク設定またはネットワークプロファイルに変更があった場合、その変

目的	手順
	更はデバイスのプロビジョニング中に反映されません。

デバイス構成を今すぐまたは後で展開する

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

始める前に

設定で [Visibility and Control of Configurations] が無効になっていることを確認してください。詳細については、デバイス構成の可視性と制御 （229 ページ）を参照してください。

手順

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

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

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

a) すべての問題に対処し、デバイス設定を展開します。

[Recheck] をクリックし、すべての検証が成功したことを確認します。

b) [Submit] をクリックします。

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

デバイス設定のプレビューと展開

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

始める前に

設定で [Visibility and Control of Configurations] が有効になっていることを確認してください。詳細については、デバイス構成の可視性と制御 （229 ページ）を参照してください。

手順

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

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

ステップ 2 [**Performing Initial Checks**] ウィンドウで、すべての問題に対処した後、[**Next**] をクリックして現在の展開を続行します。

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

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

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

ステップ 4 [**Preview Configuration**] ウィンドウで、次の手順を実行します。

a) デバイス構成を確認します。

b) 展開オプションを選択します。

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

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

ステップ 5 展開のスケジュールを設定します。

a) 設定を展開するタイミングと場所（該当する場合）を指定します。

確認のために設定を送信する場合は、IT 管理者へのメモを追加します。

b) [Submit] をクリックします。

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

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

ネットワーク プロビジョニングの事前チェック

シームレスなプロビジョニング操作を保証するために、Catalyst Center は一連の事前チェックを実行して、現在のタスクと競合する可能性のある保留中の操作がないこと、およびデバイスが準拠していることを確認します。

（注） この機能は、プロビジョニング、SWIM、および RMA ワークフローにのみ適用されます。

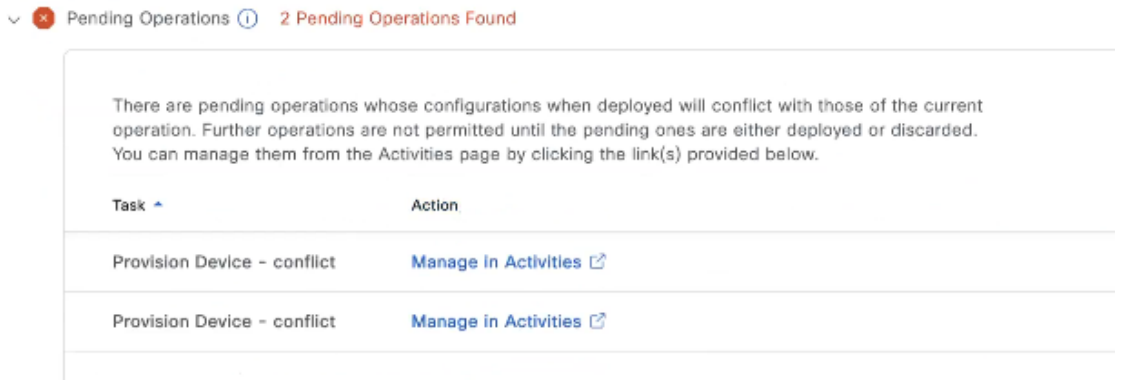
事前チェックは、任意のプロビジョニング ワークフロー中、[Now] または [Later] オプションを選択して設定の展開をスケジュールした後、あるいは該当する場合は [Preview and Deploy (Recommended)] オプションを選択した後に実行されます。

[Performing Initial Checks] ウィンドウで、Catalyst Center から次のような問題が通知されます。

アイテム	説明
アイコン	このアイコンはエラーがないことを示しており、[Next] または [Submit] をクリックしてプロビジョニングを続行できます。
アイコン	このアイコンは、プロビジョニングを続行するためにすべての問題に対処する必要があることを示しています。
アイコン	このアイコンは、注意が必要な問題であることを示します。 問題を無視することもできますが、問題に対処することをお勧めします。

問題が通知された場合は、次のタスクを実行します。

- 保留中の操作が特定された場合は、[Manage in Activities] リンクをクリックして、[Activities] >[Tasks] ウィンドウに移動します（図を参照）。保留中の操作を破棄することも、プロセスが完了するまで待機することもできます。保留中の操作を破棄する場合は、ウィンドウの右下隅にある [Recheck] をクリックして、検証ステータスを更新します。

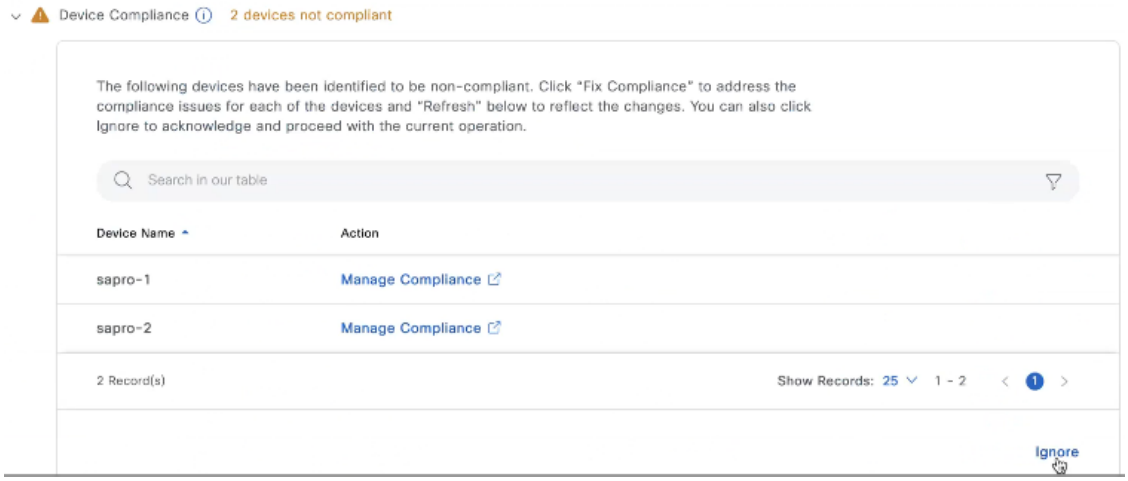


- （図に示すように）[Device Compliance] チェックで非準拠デバイスと各デバイスの [Compliance Summary] ウィンドウへのリンクが表示された場合、プロビジョニングを続行するには、コンプライアンスの問題を修正、確認、または無視する必要があります。
  - 問題を修正するには、[Manage Compliance] をクリックし、[Compliance Summary] ウィンドウで [Fix Compliance] をクリックします。詳細については、コンプライアンス違反の修正 （686 ページ）を参照してください。

（注） 事前チェックでは、[Network Settings]、[Network Profiles]、[Fabric]、[Application Visibility]、[Umbrella]、および [Workflows] のタイルについてのみ、コンプライアンス違反（未解決および確認済み）がチェックされます。[Compliance Summary] で使用可能な他のカテゴリには適用されません。それらのカテゴリはプロビジョニング ワークフローの影響を受けないためです。

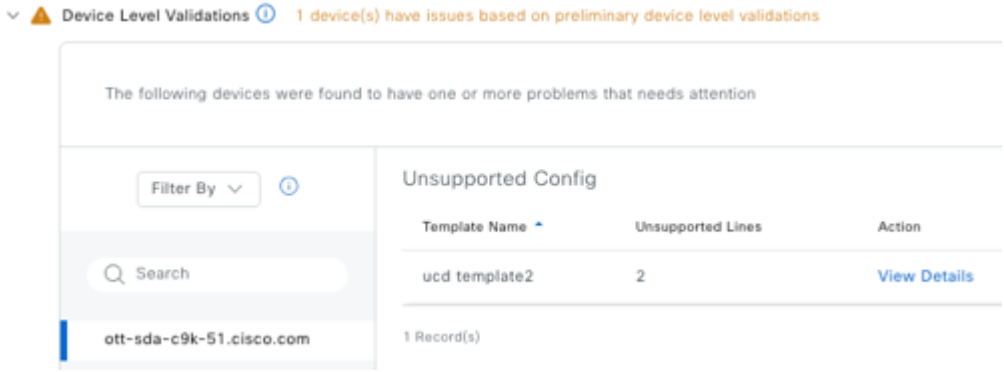
確認済みの違反には、事前チェック中にもフラグが付けられます。これは、デバイスをプロビジョニングする前にすべてのコンプライアンス違反がチェックされるようにするためです。

  - 問題を無視するには、この図に示すように、[Device Compliance] 領域にある [Ignore] をクリックします。



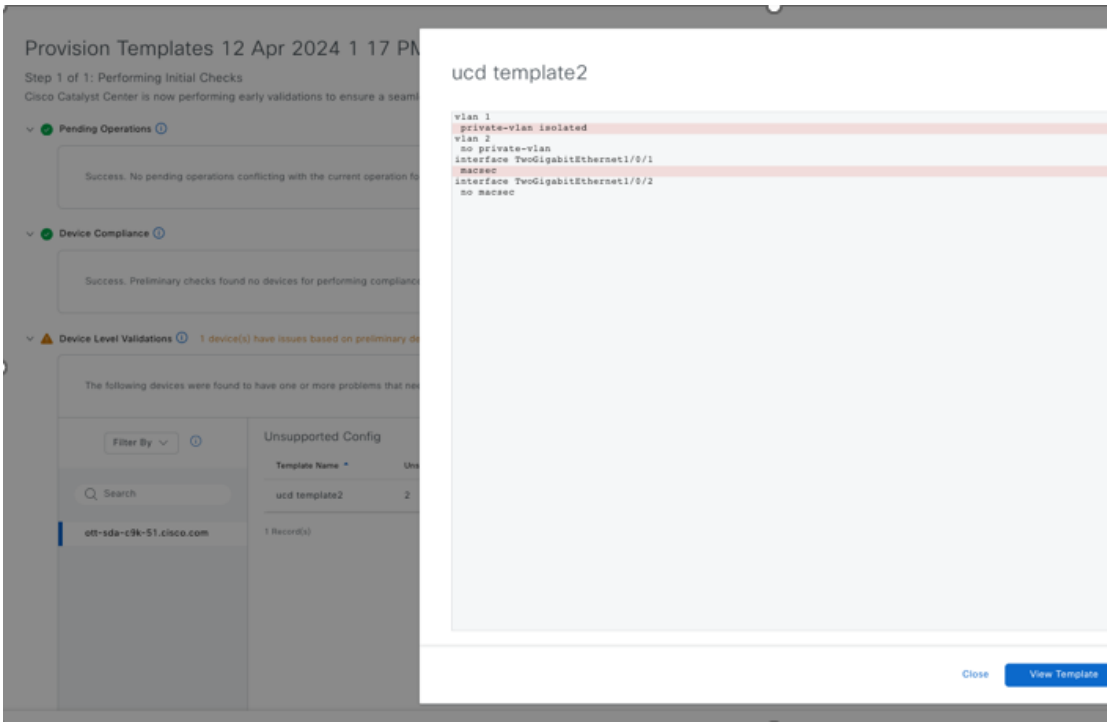
[Performing Validations] ウィンドウの右下にある [Recheck] をクリックし、事前チェックの横に アイコンが表示されていることを確認する必要があります。次に、[Next] をクリックして、プロビジョニング ワークフローの次の手順に進みます。

- [Device Level Validations] チェックでは、次のような問題が特定されます。
  - **CLI テンプレートで使用されているサポートされていない設定**：選択したデバイスの [Unsupported Lines] は、サポートされていない設定がある CLI テンプレートの行数を示します。



（注） このチェックは、ファブリックデバイスにのみ適用されます。現在、このチェックでは、非ファブリックデバイスの CLI テンプレートは検証されません。

[View Details] をクリックすると、この図に示されているように、サポートされていない設定を含む特定の行が強調表示されます。



強調表示されているCLIコマンドにカーソルを合わせると、その行が強調表示されている理由が表示されます。

サポートされていない設定を削除するには、[View Template] リンクをクリックします。[CLI Template] ウィンドウが表示され、テンプレートを編集できます。

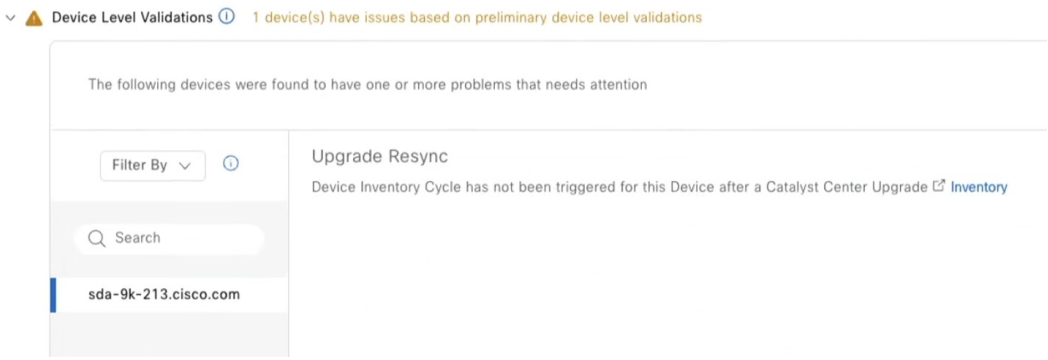
サポートされていない設定の例を次の表に示します。

アイテム	説明
Macsec	ファブリックエッジおよび拡張ノードでのみサポートされていません。
Private-vlan	すべてのファブリックロールでサポートされていません。
Flexlink＋CLI（Repセグメント）	ファブリックエッジデバイスでサポートされていません。

- 問題を修正したら、[Device Level Validations] ウィンドウの右下にある [Recheck] をクリックし、事前チェックの横に アイコンが表示されていることを確認します。次に、[Next] をクリックして、プロビジョニング ワークフローの次の手順に進みます。
- 問題を修正せずに続行する場合は、**[Ignore]** ボタンをクリックします。問題をスキップすることは推奨されません。

- **[Device is not resynchronized after an upgrade]**：アップグレード後に再同期されていない1つ以上のデバイスが一覧表示されます。プロビジョニングを続行するには、デバイスを再同期する必要があります。[Inventory] リンクをクリックして、インベントリ内のデバイスを表示し、[Resync] 操作を実行します。

（注）
- 現在のところ、このチェックはファブリックデバイスにのみ適用されます。
- アップグレード後に再同期されたものの、到達不能または管理状態にないデバイスについては、[Preview Configuration] ウィンドウにエラーメッセージが表示されます。再同期を再試行するか、生成された設定の展開を続行するかを選択できます。



問題を修正したら、[Device Level Validations] ウィンドウの右下にある [Recheck] をクリックし、事前チェックの横に アイコンが表示されていることを確認します。次に、[Next] をクリックして、プロビジョニング ワークフローの次の手順に進みます。

（注）展開を続行するには、事前チェック中に見つかった問題に対処する必要があります。

故障したデバイスの交換

返品許可（RMA）ワークフローにより、障害が発生したデバイスを迅速に交換できます。RMAでは、ルータ、スイッチ、ワイヤレスコントローラ、およびAPを交換するための共通のワークフローを提供します。

ルータおよびスイッチで RMA ワークフローを使用すると、ソフトウェアイメージ、構成、およびライセンスが、障害が発生したデバイスから交換用デバイスに復元されます。ワイヤレス AP の場合、交換用デバイスは同じサイトに割り当てられ、プライマリワイヤレスコントローラ、RF プロファイル、および AP グループ設定でプロビジョニングされ、障害が発生した AP と同じ Catalyst Center のフロアマップの場所に配置されます。

シスコスイッチスタック（ハードウェアスタッキング）内のメンバースイッチを交換する場合も、同じ手順で交換できます。アクティブスイッチは、交換用のソフトウェアイメージと設定を提供します。 Catalyst Center はスタック全体の交換を処理します。

（注）

- デバイス交換ワークフローを使用して、故障したデバイスを交換することもできます。詳細については、デバイスの交換 （1664 ページ） を参照してください。
- **[インベントリ（Inventory）]** ウィンドウから故障したデバイスを交換すると、ワークフローが合理化され、**[交換用デバイスの選択（Choose Replacement Device）]** ウィンドウから処理を開始できます。完全なデバイス交換ワークフローを使用して、故障したデバイスを交換するには、「デバイスの交換 （1664 ページ）」を参照してください
- デバイスを交換対象としてマーキングするのと、デバイスを交換するのは、異なるタイミングで実行できます。

始める前に

- 交換するデバイスにマークを付ける前に、故障したデバイスのソフトウェアイメージバージョンをイメージリポジトリにインポートしてください。
- 故障したデバイスが到達不能であることを確認します。
- プラグアンドプレイ（PnP）で交換用デバイスを Catalyst Center にオンボードしている場合は、故障したデバイスをユーザー定義サイトに割り当ててください。
- デバイスの交換ワークフローを開始するときに、交換用のデバイスがプロビジョニング状態ではないことを確認します。
- スイッチスタックを交換する場合、故障したデバイスと交換用デバイスのスタック数は同一である必要があります。
- 交換用の ワイヤレスコントローラ がサイトに割り当てられていないこと、またはプロビジョニングされていないことを確認してください。

手順

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

ステップ 2 **[インベントリ（Inventory）]** ウィンドウから、故障したデバイスを交換対象としてマーク付けします。

a) 交換する障害のあるデバイスのチェックボックスをオンにします。
b) [Actions] ドロップダウンリストから、**[Device Replacement]** > **[Mark Device for Replacement]** の順に選択します。
c) [交換用としてマーク（Mark for Replacement）] ダイアログボックスで、[マーク（Mark）] をクリックして確認します。



（注） ファブリックデバイスのシームレスな交換を実現するために、DHCP サーバーがネイバーデバイスで設定されます。これは、PnP でデバイスを Catalyst Center にオンボードするために、交換用デバイスに IP アドレスを割り当てるために必要です。この DHCP サーバーは、故障したデバイスが正常に交換されると削除されます。

障害のあるデバイスからの最新の構成変更は、RMA ワークフロー中に交換後のデバイスにプッシュされます。

d) [Inventory] ドロップダウンリストから、[Marked for Replacement] を選択します。

交換用としてマークされたデバイスのリストが表示されます。

e) （任意）このデバイスを交換しない場合は、デバイスのチェックボックスをオンにして、**[アクション（Actions）]** > **[交換用としてのマークを解除（Unmark for Replacement）]** の順に選択します。

ステップ 3 （任意）**[インベントリ（Inventory）]**ウィンドウから故障したデバイスを交換します。

a) 交換する障害のあるデバイスのチェックボックスをオンにします。
b) [アクション（Actions）] ドロップダウンリストから、**[デバイスの交換（Device Replacement）]** > **[デバイスを交換（Replace Device）]** の順に選択します。
c) **[交換用デバイスの選択（Choose Replacement Device）]** ウィンドウの [プラグアンドプレイ（Plug and Play）] タブまたは [インベントリ（Inventory）] タブから交換用デバイスを選択し、[次へ（Next）] をクリックします。

[プラグアンドプレイ（Plug and Play）] タブには、PnP によってオンボードされたデバイスが表示されます。[インベントリ（Inventory）] タブには、インベントリまたは検出プロセスによってオンボードされたデバイスが表示されます。

交換用のデバイスが PnP を介してオンボードされていない場合は、手動または自動で追加します。

- 手動：[プラグアンドプレイ（Plug and Play）] タブで、[デバイスの追加（Add Device）] をクリックします。**[新しいデバイスの追加（Add New Device）]** ウィンドウで、デバイスのシリアル番号を入力し、[新しいデバイスの追加（Add New Device）] をクリックします。
- 自動：[プラグアンドプレイ（Plug and Play）] タブで、[スマートアカウントとの同期（Sync with Smart Account）] をクリックします。**[スマートアカウントとの同期（Sync with Smart Account）]** ウィンドウで、[同期（Sync）] をクリックします。

d) ワイヤレスコントローラ の場合、**[交換デバイスの設定（Configure replacement device）]** ウィンドウで、交換に必要な設定の詳細を入力します。

- 故障した ワイヤレスコントローラ にマスター暗号化キーが設定されている場合は、ワイヤレスコントローラ 交換用の [マスター暗号化設定キー（Master Encryption Configuration Key）] フィールドにキーを入力します。

（注） 暗号化されたパスワードとキーは、正しいマスター暗号化キーがないと復元できません。このキーがないと、ワイヤレスコントローラにアクセスできなくなり、RMA プロセスが失敗します。

- [HAの設定（Configure HA）] で、次のいずれかのオプションを選択します。
  - [はい（Yes）]：故障した ワイヤレスコントローラ 高可用性（HA）ペアを新しいペアに置き換える場合。

    プライマリ交換とセカンダリ交換 ワイヤレスコントローラの両方に必要な設定を完了します。

（注） HAペアの ワイヤレスコントローラの場合、ペアの両方のデバイスがダウンしている場合にのみ、このワークフローを使用します。アクティブな HA ペア内の単一の故障したワイヤレスコントローラを置き換えるには、このワークフローを使用しないでください。

  - [いいえ（No）]：スタンドアロン ワイヤレスコントローラを交換する場合。

    交換用の ワイヤレスコントローラ に必要な設定を完了します。

交換用のデバイスを設定するには、IPv4 アドレスとその対応する設定、IPv6 アドレスとその対応する設定、またはその両方を使用できます。

（注） 障害のある ワイヤレスコントローラ の IP アドレスは、PnP を介して交換用 ワイヤレスコントローラ を要求するときに再利用できません。

オプション	説明
Wireless Management IPv4	ワイヤレス管理インターフェイスの有効な IPv4 アドレスを入力します。 （注） • 交換用 ワイヤレスコントローラ のワイヤレス管理 IP アドレスは、故障した ワイヤレスコントローラのワイヤレス管理 IP アドレスと異なる必要があります。 • 故障した ワイヤレスコントローラ HA ペアを新しいペアに置き換えるには、プライマリおよびセカンダリ ワイヤレスコントローラ のワイヤレス管理 IP アドレスが異なっている必要があります。
Subnet Mask	IPv4 サブネット マスクを選択します。
Wireless Management IPv6	該当する場合は、ワイヤレス管理インターフェイスの有効な IPv6 アドレスを入力します。 （注） • 交換用 ワイヤレスコントローラ のワイヤレス管理 IP アドレスは、故障した ワイヤレスコントローラのワイヤレス管理 IP アドレスと異なる必要があります。 • 故障した ワイヤレスコントローラ HA ペアを新しいペアに置き換えるには、プライマリおよびセカンダリ ワイヤレスコントローラ のワイヤレス管理 IP アドレスが異なっている必要があります。
Prefix Length	IPv6 プレフィックス長を選択します。
Gateway IPv4	デフォルトゲートウェイ IPv4 アドレスを入力します。
Gateway IPv6	デフォルト ゲートウェイ IPv6 アドレスを入力します。
VLAN ID	VLAN ID を入力します。 有効な範囲は 1 ～ 4094 です。 （注） 故障した ワイヤレスコントローラ と交換用の両方で VLAN ID が同じである必要があります。
Interface Name	ワイヤレス管理に使用する特定のインターフェイス名を入力します。

オプション	説明
ローカル冗長性管理 IP	該当する場合は、交換用 ワイヤレスコントローラ のローカル冗長管理 IP アドレスを入力します。 （注） • この IP アドレスとピア冗長性管理 IP アドレスが同じでないことを確認します。 • この IP アドレスが他のネットワークエンティティに割り当てられていないことを確認します。
セカンダリ WLC の選択	該当する場合は、HA のセカンダリ ワイヤレスコントローラを選択します。 （注） 障害のある ワイヤレスコントローラ HA ペアを新しいペアに置き換えるには、次のことを確認します。 • セカンダリ ワイヤレスコントローラ のワイヤレス管理 IP アドレスとサブネットマスクが、故障した ワイヤレスコントローラ のワイヤレス管理 IP アドレスと同じ IP サブネット内にあることを確認してください。 • セカンダリ ワイヤレスコントローラ のワイヤレス管理 VLAN がプライマリ ワイヤレスコントローラ の VLAN と一致していることを確認してください。 • 将来の ワイヤレスコントローラ をプライマリまたはセカンダリ ワイヤレスコントローラ として選択することはできません。要求元不明、オンボード済みの ワイヤレスコントローラ、およびプロビジョニングされていないインベントリベースの ワイヤレスコントローラ のみを選択できます。
ピア冗長性管理 IP	該当する場合は、セカンダリ ワイヤレスコントローラ のピア冗長管理 IP アドレスを入力します。 （注） • この IP アドレスとローカル冗長性管理 IP アドレスが同じでないことを確認します。 • この IP アドレスが他のネットワークエンティティに割り当てられていないことを確認します。

e) **[概要（Summary）]** ウィンドウで、要約された詳細を確認します。

必要に応じて、[編集（Edit）]をクリックして、デバイスタイプまたは故障したデバイスの詳細を更新します。

（注） 設定の可視性と制御が無効になっている場合は、[交換用デバイス（Replacement Device）] の [表示（View）] をクリックして、交換用デバイスの設定を確認します。

f) **[交換のスケジュール（Schedule Replacement）]** ウィンドウで、展開するタスクをスケジュールします。

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

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 4 **[インベントリ（Inventory）]** ウィンドウでは、デバイスが交換されるときに、デバイス交換タスクの進行状況を表示します。

または、**[タスク（Tasks）]** ウィンドウからタスクをモニターできます。

1. **[インベントリ（Inventory）]** ウィンドウで、[フォーカス（Focus）] ドロップダウンリストから [デバイスの交換（Device Replacement）] を選択します。
2. [交換ステータス（Replace Status）] 列で交換のステータスを確認します。

   デバイスが正常に交換されると、[交換済み（Replaced）] ステータスが表示されます。

   デバイスの交換に失敗し、エラーメッセージが表示された場合は、エラーリンクをクリックします。[再試行（Retry）] をクリックして、同じ障害のあるデバイスと交換デバイスのセットを使用してワークフローを再試行します。

   （注） [Main Inventory] ウィンドウには、故障したデバイスと交換した新しいデバイスの詳細情報が表示されます。

3. [交換ステータス（Replace Status）] 列で、デバイスのステータスをクリックすると、スライドインペインに詳細情報が表示されます。

   たとえば、スライドインペイン には、システムがタスクを完了するために次の手順が表示されます。

   1. デバイス交換の準備状況チェックを実行します。
   2. （PnP）交換用デバイスを請求します。
   3. 交換用デバイスにソフトウェアイメージを配信してアクティブ化します。
   4. ライセンスを展開する。

5. VLAN 構成をプロビジョニングします。
6. スタートアップ構成をプロビジョニングします。
7. 交換用デバイスをリロードします。
8. 交換用デバイスの到達可能性を確認します。
9. 交換用デバイスに SNMPv3 ログイン情報を展開します。
10. 交換用デバイスを同期します。
11. 故障したデバイスを CSSM から削除します。
12. 交換用デバイスを CSSM に追加します。
13. PKI 証明書を失効化して作成します。
14. Cisco ISE を更新します。
15. 障害のあるデバイスを削除します。

次のタスク

ワイヤレスコントローラの交換中には、次のファイルと設定は交換用のワイヤレスコントローラ に転送されません。

- カスタム Web 認証バンドルおよび NBAR プロトコルパック
- IP アドレス SSH RSA キーまたはキーペア名
- カスタムトラストポイント

交換後、交換用のワイヤレスコントローラでこれらの設定をコピーして手動で再設定します。

障害のあるアクセスポイントの交換

AP の RMA 機能を使用して、障害のある AP をデバイスインベントリに登録されている交換用 AP に交換できます。

始める前に

- アクセスポイント（AP）の返品許可（RMA）機能では、同等の交換のみをサポートしています。モデル番号と PID が障害のある AP と同じ交換用 AP を用意する必要があります。
- 交換用 AP を障害のある AP と同じ シスコ ワイヤレス コントローラに接続しておく必要があります。

- ワイヤレスコントローラとして機能する Cisco Mobility Express AP は、交換用 AP の候補ではありません。
- 障害のある AP のソフトウェア イメージ バージョンをイメージリポジトリにインポートしてから、交換用デバイスにマークを付ける必要があります。
- 障害のある AP はサイトに割り当てられ、Catalyst Center でプロビジョニング済みである必要があります。
- RMA ワークフローのトリガー中は、交換用 AP がプロビジョニング状態であってはなりません。
- 障害のある AP は到達不能な状態になっている必要があります。
- 交換を実行するサイトとデバイスにアクセスできる必要があります。

手順

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

ステップ 2 交換する故障した AP のチェックボックスをオンにします。

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

ステップ 4 [交換用としてマーク（Mark for Replacement）] ダイアログボックスで、[マーク（Mark）] をクリックして確認します。

今すぐこの AP を交換しない場合は、交換用マークを解除し、障害のある正しい AP を交換用としてマークできます。

1. 交換しない AP のチェックボックスをオンにします。
2. [アクション（Actions）] ドロップダウンリストから、**[アクション（Actions）]** > **[交換用マークの解除（Unmark for Replacement）]** の順に選択します。
3. 障害のある正しい AP に対して、「ステップ 2 （252 ページ）」、「ステップ 3 （252 ページ）」、「ステップ 4 （252 ページ）」を繰り返します。

ステップ 5 [Mark For Replacement] ウィンドウで、障害のあるデバイス名の横にあるオプションボタンをクリックします。

ステップ 6 [Actions] ドロップダウンリストから、**[Replace Device]** を選択します。

ステップ 7 [Replace Device] ウィンドウで、[Start] をクリックします。

ステップ 8 [Available Replacement Devices] テーブルで、交換用デバイスの名前の横にあるオプションボタンをクリックします。

ステップ 9 **[次へ (Next)]** をクリックします。

ステップ 10 [Replacement Summary] を確認し、[Next] をクリックします。

ステップ 11 [交換のスケジュール（Schedule Replacement）] ウィンドウで、スケジュールオプションを選択し、必要に応じてタスク名を更新してから [適用（Apply）] をクリックします。

- [Now]：設定をすぐに展開します。
- [Later]：日付、時刻、タイムゾーンを設定して、展開をスケジュールします。

ステップ 12 選択したオプションに基づいて展開を続行します。

- [今すぐ（Now）] を選択した場合は、[送信（Submit）] をクリックします。
- [後で（Later）] を選択した場合は、[スケジュール（Schedule）] をクリックします。

タスクは予定時刻に展開されます。[Tasks] ウィンドウでタスクを確認できます。

ステップ 13 [インベントリ（Inventory）] ウィンドウから、障害のある AP が交換されるときにタスクを監視します。次の表を使用して AP 交換タスクの詳細を表示し、失敗したタスクを再試行します。

実行する操作	結果
タスクの進行状況を表示する	**1.** [インベントリ（Inventory）] ウィンドウで、[フォーカス（Focus）] ドロップダウンリストから [デバイスの交換（Device Replacement）] を選択します。 **2.** [交換ステータス（Replace Status）] 列で、障害のある AP が交換されるときにそのステータスを表示します。 デバイスが正常に交換されると、[交換済み（Replaced）] ステータスが表示されます。 **3.** 障害のある AP のステータスをクリックすると、スライドインペインに詳細情報が表示されます。

実行する操作	結果
交換履歴を表示する	**1.** [インベントリ（Inventory）] ウィンドウで、[フォーカス（Focus）] ドロップダウンリストから [デバイスの交換（Device Replacement）] を選択します。 **2.** [アクション（Actions）] ドロップダウンリストから、**[デバイスの交換（Device Replacement）] > [交換履歴（Replacement History）]** の順に選択します。 [交換履歴（Replacement History）] スライドインペインに、交換されたデバイスが表形式で表示されます。 **3.** [交換ステータス（Replace Status）] 列で、デバイスが正常に交換されたことを示す [交換済み（Replaced）] などのステータスをクリックします。 [交換ステータス（Replace Status）] タブには、タスクを完了するためにシステムが実行した手順が一覧表示されます。
タスクが失敗した理由を表示する	**1.** [インベントリ（Inventory）] ウィンドウで、[フォーカス（Focus）] ドロップダウンリストから [デバイスの交換（Device Replacement）] を選択します。 **2.** [交換ステータス（Replace Status）] 列で、APの交換が失敗した理由とエラーメッセージを確認します。 故障したAPを別の新しいAPに交換するか、AP RMA再試行機能を使用して失敗した交換を再試行できます。
障害のあるAPの交換を再試行する	**1.** [インベントリ（Inventory）] ウィンドウで、[フォーカス（Focus）] ドロップダウンリストから [デバイスの交換（Device Replacement）] を選択します。 **2.** [交換ステータス（Replace Status）] 列で、障害のあるAPのエラーメッセージをクリックしてから、[再試行（Retry）] をクリックします。

アウトオブバンド RMA デバイスの交換の管理

アウトオブバンド交換という用語は、Catalyst Center でデバイス交換ワークフローをバイパスしながら、デバイスを手動で交換し、その設定、イメージ、およびライセンスを新しいデバイスに転送することを指します。

新しいデバイスが古いデバイスと同じ IP アドレスを使用している場合、アウトオブバンド交換プロセスではシリアル番号の競合が発生します。新しいデバイスが別の IP アドレスを受信した場合は、リストから正しい交換デバイスを選択する必要があります。

アウトオブバンド RMA デバイスを管理するには、次の手順を実行します。

手順

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

ステップ 2 Catalyst Center で管理するアウトオブバンド RMA デバイスのチェックボックスを選択します。

ステップ 3 [アクション（Actions）] ドロップダウンリストから、**[デバイスの交換（Device Replacement）]** > **[交換の確認（アウトオブバンド）（Confirm Replacement (Out-of-Band)）]** の順に選択します。

確認後、ワークフローは故障したデバイスを新しいデバイスにマッピングします。

1. ワークフローでは、登録、同期、および認定のタスクを実行します。
2. インベントリが更新され、新しいデバイスとそのシリアル番号が表示されます。
3. 交換履歴には、交換に関する詳細が表示されます。

Catalyst Center の RMA ワークフローの制限事項

- RMA は、以下を除くスイッチ、ルータ、ワイヤレスコントローラ、Cisco SD-Access デバイスの交換をサポートします。
  - Cisco AireOS ワイヤレスコントローラについて
  - Mobility Express デバイス
  - シャーシベース Nexus 7700 シリーズ スイッチ
  - スイッチスタック（SVL スタッキング）
- Cisco SD-Access ファブリックデバイスの場合、RMA ワークフローでは類似するデバイスの交換のみがサポートされます。障害が発生したデバイスと交換用デバイスは、同じモデル番号と PID である必要があります。異なるモデル番号または PID への交換はサポートされていません。

- RMA は、外部 SCEP ブローカ PKI 証明書を使用するデバイスをサポートします。RMA ワークフロー中に、交換デバイス用に PKI 証明書が作成および認証されます。交換した障害のあるデバイスの PKI 証明書は、証明書サーバーから手動で削除する必要があります。
- RMA ワークフローでは、次の場合にのみデバイスの交換が可能です。
  - 障害のあるデバイスと交換用デバイスの両方に同じ拡張カードが搭載されている。
  - 両方のデバイスのポート数が拡張カードによって変わらない。
  - 障害のあるデバイスは、Catalyst Center によって静的 IP で管理されます（RMA は、拡張ノードおよびファブリック内の AP を除く、Catalyst Center によって DHCP IP で管理されるデバイスではサポートされません）。
  - ソフトウェアイメージ管理（SWIM）はインストールモードでのみイメージの更新をサポートするため、交換用の ワイヤレスコントローラ はインストールモードです。交換用のデバイスがバンドルモードの場合、イメージの配布とアクティブ化に失敗します。
- 交換用デバイスが、障害のあるデバイスが接続されていたポートと同じポートに接続されていることを確認してください。
- RMA ワークフローは、同じインターフェイスで複数の CDP ネイバーが検出される共有 WAN リンク（Metro-Ethernet など）はサポートしていません。
- Catalyst Center 2.3.7.4 および 2.3.7.5 のみ、ネイバーデバイスがファブリックの一部でない場合、ファブリックエッジの交換ではネイバーデバイスの DHCP サーバー設定はサポートされていません。中間ノードは Cisco SD-Access ファブリックの一部ではないため、オプション 43 の DHCP サーバーはプッシュされません。

（注） この制限は、Catalyst Center 2.3.7.6 以降で削除されています。

- 障害が発生したデバイスがファブリックサイト内の唯一のデバイス（一体型ファブリック展開など）の場合、そのデバイスが Catalyst Center によって管理されている場合でも、Catalyst Center はネイバーデバイスでの DHCP サーバーの設定をサポートしません。
- Catalyst Center レガシーライセンスの導入はサポートされていません。

  RMA ワークフローにより、Cisco SSM から障害のあるデバイスの登録が解除され、交換用デバイスが Cisco SSM に登録されます。
  - 障害のあるデバイスにインストールされているソフトウェアイメージが Cisco IOS XE 16.8 よりも前のバージョンの場合、[License Details] ウィンドウにはネットワークと機能のライセンスの詳細が表示されず、警告メッセージも表示されません。そのため、障害のあるデバイスに設定されているレガシー ネットワーク ライセンスを確認し、交換用デバイスに同じレガシー ネットワーク ライセンスを手動で適用する必要があります。

- 故障したデバイスにインストールされているソフトウェアイメージが Cisco IOS XE 16.8 以降の場合は、[License Details] ウィンドウにネットワークライセンスの詳細（**レガシー**、**ネットワーク**など）と機能ライセンス（IP Base、IP Service、LAN Base など）が表示されます。障害のあるデバイスを交換対象としてマークしているときに、次の警告メッセージが表示されます。

  ```
  Some of the faulty devices don't have a license. Please ensure
  your replacement device has the same Legacy license of the faulty
  device enabled.
  ```

- 交換用デバイスと障害のあるデバイスのレガシー ネットワーク ライセンスが一致しない場合は、ライセンスの展開中に次のエラーメッセージが表示されます。

  ```
  Catalyst Center doesn't support legacy license deployment.
  ```
  そのため、交換用デバイスで障害のあるデバイスのライセンスを手動で更新し、再同期してから続行してください。

- Catalyst Center は、ファブリックネットワークでの交換デバイスの PnP オンボーディングをサポートします。ただし、次の場合を除きます。
  - 障害のあるデバイスが複数のインターフェイスを使用してアップリンクデバイスに接続されている。
  - LAN 自動化で重複するプールが使用されている。

- 交換用デバイスが PnP DHCP 機能によってオンボードされる場合は、リロードのたびにデバイスが同じ IP アドレスを取得し、DHCP のリースタイムアウトが 2 時間を超えていることを確認してください。

- Catalyst Center 9800 HA デバイスを使用したファブリックセットアップでは、HA デバイスの 1 つがダウンした場合、次の手順を完了して交換する必要があります。

  1. [Inventory] ウィンドウで、機能不全になった HA デバイスを再同期します。Catalyst Center はデバイスをスタンドアロン（スタンバイが失敗し、削除されている状態）として表示します。
  2. デバイスの優先順位を設定します。新しいデバイスで HA を形成した後に既存のデバイスをアクティブデバイスとして戻す場合は、既存のデバイスの HA 優先順位が 2（または使用可能な最高の優先順位値）に設定されていることを確認します。デバイスの優先順位は Web UI の**[Administration]** > **[Device]** > **[Redundancy]**で設定できます。

     または、次の CLI コマンドを入力して、デバイスの優先順位を設定することもできます。

     ```
     chassis <chassis_number> priority 2
     ```

     シャーシ番号と現在の優先順位値を表示するには、`show chassis` EXEC コマンドを入力します。

     両方のデバイスで優先順位がデフォルト値の 1 に設定されている場合、MAC アドレスが小さい方のデバイスがアクティブデバイスになります。

3. 機能不全のデバイスで使用されていたのと同じローカルおよびリモートIPアドレスを使用して、新しいデバイスでシャーシの冗長性コマンドを設定します。Web UIまたはCLIのいずれかでシャーシの冗長性を設定できます。
4. 両方のデバイスを再起動して、 HA ペアを形成します。
5. HA が起動したら、Catalyst Center でデバイスを再同期します。[Inventory] ウィンドウに新しい HA ペアが表示されます。[Serial Number] 列でシリアル番号を確認します。HA ペアの場合、アクティブとスタンバイの両方のシリアル番号が表示されます。

アクセスポイントの再起動

トラブルシューティングとメンテナンスのために 1 つ以上の AP を再起動できます。

始める前に

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

手順

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

ステップ 2 再起動する AP のチェックボックスをオンにします。

ステップ 3 [Actions] ドロップダウンリストから、**[Inventory]** > **[Reboot Device]** を選択します。

ステップ 4 [**Reboot Device**] スライドインペインで、次のいずれかのスケジュールオプションを選択します。

- [**Now**]：デバイスをすぐに再起動します。
- [**Later**]：将来の特定の時間に再起動するようにスケジュールします。
- [**Recurring**]：再起動を N 回実行するようにスケジュールします。

ステップ 5 [Selected Devices] を展開して、再起動 AP の AP 名とフロアの詳細を表示します。

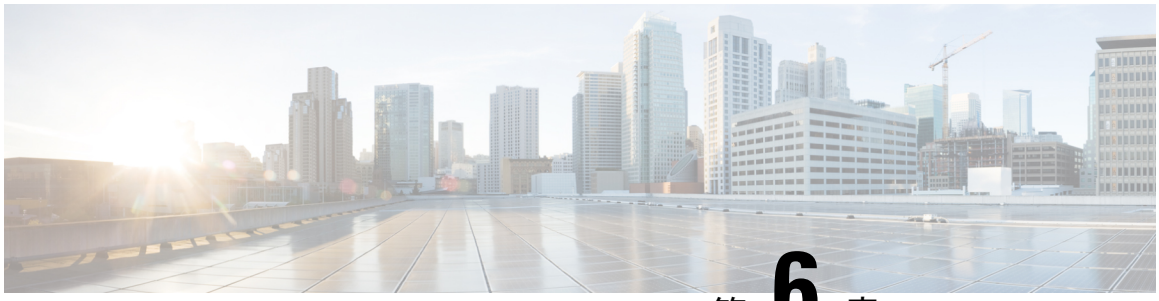
ステップ 6 [Reboot] をクリックします。

選択した AP を再起動するタスクが シスコ ワイヤレス コントローラで開始されると、「Reboot Initiated Successfully」というメッセージが表示されます。

ステップ 7 [Task Submitted] ダイアログボックスで、[Task] リンクをクリックします。

このダイアログボックスは表示されてから数秒で表示されなくなります。タスクに移動するには、メニューアイコンをクリックして次を選択します。 **[Activities]** > **[Tasks]**の順に選択します。

ステップ 8 タスク名をクリックして、再起動の開始ステータスを表示します。



第 6 章

ネットワーク トポロジを表示

- トポロジについて （259 ページ）
- エリア、サイト、ビルディング、フロアのトポロジの表示 （260 ページ）
- トポロジマップでのデバイスのフィルタリング （261 ページ）
- デバイス情報の表示 （262 ページ）
- リンク情報の表示 （263 ページ）
- トポロジマップへのデバイスのピン留め （264 ページ）
- トポロジマップレイアウトの保存 （265 ページ）
- トポロジマップレイアウトを開く （265 ページ）
- トポロジマップレイアウトの共有 （266 ページ）
- トポロジのレイアウトをエクスポート （266 ページ）

トポロジについて

[Topology] ウィンドウはネットワークのグラフィック ビューを表示します。Catalyst Center は、ユーザーが設定したディスカバリ設定を使用してネットワーク内のデバイスを検出して、デバイス ロールを割り当てます。検出中に割り当てられた（またはインベントリ内で手動で変更された）デバイス ロールに基づいて、Catalyst Center は詳細なデバイス レベルのデータを使用して物理トポロジ マップを作成します。

トポロジマップ

トポロジマップを使用して、次のようなさまざまなタスクを実行できます。

- 選択したエリア、サイト、ビルディング、またはフロアのトポロジを表示する。
- 詳細なデバイス情報を表示する。
- 詳細なリンク情報を表示する。
- 特定のレイヤ 2 VLAN に基づいてデバイスをフィルタ処理する。
- レイヤ 3 プロトコル（Intermediate System-to-Intermediate System（IS-IS）、Open Shortest Path First（OSPF）、Enhanced Interior Gateway Routing Protocol（EIGRP）、スタティック ルーティング）に基づいてデバイスをフィルタ処理する。

- Virtual Routing and Forwarding（VRF）機能を使用してデバイスをフィルタ処理する。
- トポロジ マップにデバイスをピン留めする
- トポロジ マップ レイアウトの保存
- トポロジ マップ レイアウトを開く
- トポロジレイアウト全体のスクリーンショットを SVG、PDF、PNG 形式でエクスポートする。

エリア、サイト、ビルディング、フロアのトポロジの表示

エリア、サイト、ビルディングまたはフロアのトポロジを表示できます。

始める前に

- インベントリにデバイスがあることを確認します。デバイスがない場合は、ディスカバリ機能を使用して検出します。
- ネットワーク階層を定義し、ビルディングまたはその内部のフロアにデバイスをプロビジョニングしている必要があります。

手順

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

ステップ 2 左側の階層ツリーから、興味のあるエリア、サイト、ビルディング、またはフロアを選択します。

ステップ 3 右上隅のトグルボタン（  ）を使用して、地理的マップビューとレイヤ 2 マップビューを切り替えます。

地理的マップビューにサイトが表示されます。近いサイトがグループ化され、グループ内のサイト数とともに示されます。デバイスの正常性は異なる色で示されます。サイトの上にカーソルを移動すると、デバイスの正常性の詳細が表示されます。

右上隅の [Search] フィールドを使用して、地理的マップビューのビルディング、およびレイヤ 2 マップビューのデバイスを検索できます。

（注）
- 右下隅の凡例アイコン（ⓘ）をクリックすると凡例が開き、トポロジマップで利用可能なショートカットキーが表示されます。
- [Toggle Annotate] アイコンをクリックして、レイヤ 2 マップに注釈を描画します。[export] アイコンをクリックして、トポロジマップを注釈とともにエクスポートできます。

ステップ 4 [Topology] ウィンドウのさまざまなオプションの詳細については、[Take a Tour] をクリックします。

トポロジマップでのデバイスのフィルタリング

次のいずれかの属性に基づいてデバイスをフィルタ処理できます。

- VRF
- VLAN
- ルーティング
- タギング
- 冗長性

始める前に

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

手順

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

ステップ 2 [Filter] をクリックします。

（注） [Filter] を表示できない場合は、左側のツリービューメニューでサイトをクリックします。

ステップ 3 次のいずれか 1 つのタスクを実行します。

- [VRF] ドロップダウン リストから表示する VRF を選択します。
- [VLAN] ドロップダウン リストから表示する VLAN を選択します。
- [ルーティング（Routing）] ドロップダウン リストから目的のプロトコルを選択します。

- [冗長性（Redundancy）] オプションボタンをクリックし、[PRP] ドロップダウンリストから [Redbox、LAN A、LAN Bを表示（Show Redbox, LAN A, LAN B）] を選択して、パラレル冗長プロトコル（PRP）のステータスを表示します。
- [View All Tags] をクリックして、表示するタグを選択します。選択したタグに関連付けられているデバイスが強調表示されます。新しいタグを作成する場合は、次の手順を実行します。

a) [Create New Tag] をクリックします。
b) [Tag Name] にタグ名を入力します。
c) **[Save]** をクリックします。

また、次の手順を実行して、デバイスをタグに関連付けることもできます。

a) デバイスをクリックします。
b) [Tag Device] をクリックします。
c) デバイスを関連付けるタグを選択します。
d) [Apply] をクリックします。

デバイス情報の表示

Catalyst Center では、デバイス名、IP アドレス、およびデバイスに関するその他の情報を表示できます。

（注） **[トポロジ（Topology）]** ウィンドウでアクセス可能なデバイス情報には、**[デバイス インベントリ（Device Inventory）]** ウィンドウでもアクセス可能です。

始める前に

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

手順

ステップ 1 メインメニューから次を選択します。[Tools] > [Topology] の順に選択します。
ステップ 2 [Tree View] メニューで、興味のあるエリア、サイト、ビルディング、またはフロアを選択します。
ステップ 3 トポロジ エリアで、興味のあるデバイスまたはデバイス グループにマウス オーバーします。

（注） デバイス グループには、含まれているデバイスの数と種類がラベル付けされています。スイッチの下にある青い矢印は、スイッチにホストがあることを示します。青い矢印をクリックすると、ホストが表示されます。

ステップ 4 [表示（Display）] をクリックして項目を有効にすると、追加のデバイス詳細が表示されます。詳細については、項目の横にある ⓘ アイコンにカーソルを合わせると確認できます。

- [Device Health]：デバイスの正常性が表示されます。
- [Link Health]：デバイス間のリンクの正常性が表示されます。
- [License status]：デバイスのライセンスステータスが表示されます。Catalyst Center では、ライセンスの有効期限が近づいているデバイスが強調表示され、デバイスの横に警告アイコンが表示されます。強調表示されたデバイスをクリックすると、そのライセンスの詳細が表示されます。
- [Device IP]：デバイスラベルの下にデバイスの IP アドレスが表示されます。
- [Device Suffixes]：デバイスのフルネームが、サフィックスと一緒に表示されます。

（注）
- ネットワークデバイスが Catalyst Center 内で Cisco Discovery Protocol（CDP）を使用して設定されていない場合、トポロジは Link Layer Discovery Protocol（LLDP）を使用してネイバーデバイスを決定します。
- サードパーティ製デバイスの場合、追加されたデバイスのアイコンのみが表示され、リンクは検出されません。

リンク情報の表示

Catalyst Center を使用すると、トポロジマップ内のリンクに関する情報を表示できます。単純なリンクの場合は、1 つのリンクの情報が表示されます。集約されたリンクの場合は、基本となるすべてのリンクのリストが表示されます。情報には、インターフェイス名、その速度、およびその IP アドレスが含まれます。

始める前に

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

手順

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

ステップ 2 [Tree View] メニューで、興味のあるエリア、サイト、ビルディング、またはフロアを選択します。

ステップ 3 興味のあるリンクにカーソルを合わせます。

ステップ 4 [Display] をクリックして、[Link Health] を有効にします。

ダウンリンクは赤色で表示されます。リンクを削除する場合は、削除するリンクを選択して [Delete] をクリックします。リンクを稼働状態にするには、次の手順を実行します。

a) デバイスにログインします。
b) インターフェイスをイネーブルにします。
c) [Inventory] ページでデバイスを再同期します。

（注） トポロジでは、Link Layer Discovery Protocol（LLDP）を使用して、Catalyst Center で LLDP を使用して検出されたデバイスのリンクが決定されます。

トポロジマップへのデバイスのピン留め

デバイスをグループ化または集約して、マップ上に表示するスペースを削減できます。ただし、グループからデバイスを区別する必要がある場合があります。これは、デバイスをマップにピン留めすることで可能になります。

始める前に

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

手順

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

ステップ 2 次のいずれか 1 つのタスクを実行します。

- デバイスをピン留めするには、デバイスグループを展開して展開されたグループをクリックし、ダイアログボックスでデバイス名の左側にあるピンのアイコンをクリックします。
- すべてのデバイスをピン留めするには、デバイスグループを展開して展開されたグループをクリックし、ダイアログボックスで [すべてピン留め（Pin All）] をクリックします。

（注） グループをダブルクリックすると、グループ内のデバイスのピン留めが解除されます。

トポロジマップレイアウトの保存

Catalyst Center にはシスコ推奨のトポロジレイアウトがあり、トポロジツールを開いたときにこれがデフォルトで表示されます。複数のレイアウトをカスタマイズし、後で確認するために保存できます。またレイアウトの1つを、トポロジマップを開いたときに表示されるデフォルトとして設定することもできます。

始める前に

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

手順

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

ステップ2 [Custom View] をクリックします。

ステップ3 [フォーカスタイトルの入力（Enter Focus Title）] フィールドに、カスタマイズしたマップの名前を入力します。

ステップ4 [Save] をクリックします。

ステップ5 （任意） カスタマイズしたマップをデフォルトに設定するには、[カスタムビュー（Custom View）] をクリックし、カスタムマップの名前にカーソルを合わせて、[*]（デフォルトフォーカス）をクリックします。

トポロジマップレイアウトを開く

以前に保存したトポロジ マップを開くことができます。

始める前に

トポロジ マップ レイアウトが保存済みである必要があります。

手順

ステップ 1 メインメニューから次を選択します。[Tools] > [Topology] の順に選択します。
ステップ 2 [Custom View] をクリックします。
ステップ 3 表示するマップの名前をクリックします。

トポロジマップレイアウトの共有

カスタマイズしたマップを他のユーザーと共有できます。

始める前に

- トポロジマップレイアウトが保存済みである必要があります。
- 少なくとも 1 つのトポロジビューが保存済みである必要があります。

手順

ステップ 1 メインメニューから次を選択します。[Tools] > [Topology] の順に選択します。
ステップ 2 [Custom View] をクリックします。
ステップ 3 カスタムマップの名前にマウスカーソルを合わせて、[Share Focus] アイコンをクリックします。
ステップ 4 確認ウィンドウで [Yes] をクリックします。

トポロジのレイアウトをエクスポート

最大 16,384 ピクセルまでの完全なトポロジレイアウトのスナップショットをエクスポートできます。スナップショットは、SVG、PDF、または PNG ファイルとしてローカル マシンにダウンロードされます。

始める前に

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

手順

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

ステップ 2 （このアイコンは [トポロジのエクスポート（Export Topology）]) をクリックします。

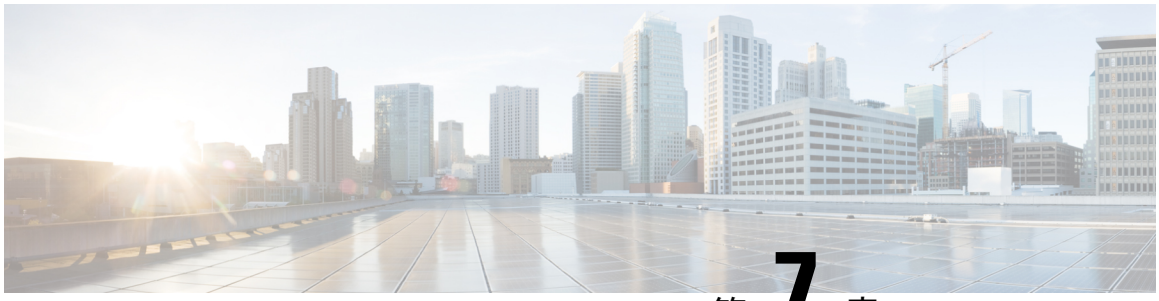
ステップ 3 ファイル形式を選択し、[エクスポート（Export）] をクリックします。



第 III 部

ネットワークの設計

- ネットワーク階層の設計 （271 ページ）
- ワイヤレス 2D および 3D マップの操作 （293 ページ）
- ネットワークの設定 （373 ページ）
- ネットワークプロファイルの設定 （535 ページ）



第 7 章

ネットワーク階層の設計

- ネットワーク階層 （271 ページ）
- 新しいネットワーク階層の設計 （273 ページ）
- 既存の Cisco ネットワーク階層 （274 ページ）
- 既存の Ekahau ネットワーク階層の使用 （278 ページ）
- Catalyst Center からのネットワーク階層のエクスポート （282 ページ）
- ネットワーク階層の検索 （284 ページ）
- ネットワーク階層の作成 （285 ページ）

ネットワーク階層

ネットワークの地理的な場所を表すネットワーク階層を作成できます。

ネットワーク階層の構造

ネットワーク階層は階層構造で編成されています。この階層はサイトで構成されています。サイトは、エリア、ビルディング、フロア、または屋外エリアを指している場合があります。階層構造内の各サイトの配置は、ネットワーク階層ルールによって異なります。ネットワーク階層内のさまざまなサイトをどのように構成できるかについては、次の図と表を参照してください。

図 *5 :* ネットワーク階層

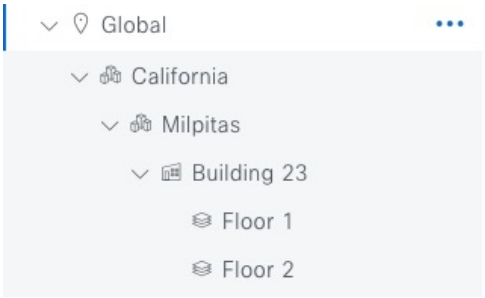


表 *39 :* ネットワーク階層の要素

サイトタイプ	説明（**Description**）	ルール（**Rule**）
Global（）	他のすべてのサイト要素が存在するデフォルトのサイト要素。	[Global] の下に直接配置できるのはエリアとビルディングのみです。
Areas（）	エリアは、地理的なリージョンを識別します。これらは、エリア、ビルディング、またはエリアとビルディングの両方をグループ化する方法を提供します。そのため、物理アドレスはありません。	エリアは、[Global] または他のエリアの下に直接配置できます。
Buildings（）	ビルディングでは物理アドレスまたは緯度と経度の座標を設定できます。	ビルディングは、[Global] またはエリアの下に直接配置できます。エリアを含めることはできませんが、フロアまたは屋外エリアを含めることはできます。
屋外エリア（）	屋外エリアは、住所または緯度経度座標を使用して、イメージマップありまたはなしで追加できます。	屋外エリアは、[グローバル（Global）] またはエリアやビルディングの下に配置できます。マップありまたはマップなしで追加できます。マップを使用する場合は、手動で作成するか、DXF、DWG、JPG、GIF、PNG、または PDF を含むファイルタイプのファイルからインポートできます。次に、ワイヤレスデバイスをマップに配置して、ワイヤレスネットワークのカバレッジを視覚化できます。 屋外エリアの下にサイト要素を追加したり、既存の屋外エリアをサイト間で移動したりすることはできません。

サイトタイプ	説明（Description）	ルール（Rule）
Floors（）	フロアは、壁や窓など、ビルディングのさまざまなコンポーネントを含む背景画像の有無にかかわらず、ビルディングに追加できます。 フロアマップでは、フロアに配置されたワイヤレスデバイスのワイヤレスネットワークのカバレッジを視覚化できます。フロアマップは手動で作成するか、DXF、DWG、JPG、GIF、PNG、PDF ファイルタイプなどの背景画像から追加できます。	ビルディングの下に配置されているフロアのみ。 （注） • 既存のフロアを別のビルディングに移動することはできません。 • プロビジョニングされていないデバイスのサイト階層は、フロアマップ上の AP の場所を維持したまま変更できます。

サイトにデザインの設定を適用する

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

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

ネットワーク階層の構築

開始するには、次のいずれかの方法を使用してネットワーク階層を構築します。

- ネットワーク階層を作成します。詳細については、「ネットワーク階層の作成 （285 ページ）」を参照してください。
- Cisco Prime Infrastructure または Ekahau Pro から既存のネットワーク階層をインポートする。詳細については、「既存の Cisco ネットワーク階層 （274 ページ）」または「既存の Ekahau ネットワーク階層の使用 （278 ページ）」を参照してください。

新しいネットワーク階層の設計

[設計（Design）] を使用して、ネットワーク全体のデバイスに適用可能なネットワーク構造、ネットワーク設定、デバイスタイププロファイルを作成します。既存のインフラストラクチャがない場合は、設計ワークフローを使用します。

既存のインフラストラクチャがある場合は、**ディスカバリ**機能を使用します。詳細については、検出の概要 （73 ページ） を参照してください。

新しいネットワーク階層を設計するには、次の手順を実行します。

手順

ステップ 1 ネットワーク階層を作成します。詳細については、「サイトの作成、編集、削除 （285 ページ）」を参照してください。

ステップ 2 グローバル ネットワーク設定を定義します。詳細については、「ネットワーク設定の概要 （373ページ）」を参照してください。

ステップ 3 ネットワーク プロファイルを定義します。詳細については、「ネットワークプロファイルの概要 （535ページ）」を参照してください。

既存の Cisco ネットワーク階層

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

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

次の情報を使用して、ネットワーク階層を再作成できます。

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

  マップアーカイブは、グローバル階層に基づくものにすることも、単一のサイト、ビルディング、またはフロアの階層に基づくものにすることもできます。

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

- [Floor]：選択したフロアがエクスポートされます。



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

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

FIPS モードが有効な場合：

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

FIPS モードが無効な場合：

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

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

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

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

手順

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

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

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

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

Cisco Prime Infrastructure からのマップアーカイブのエクスポート

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

手順

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

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

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

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

すべてのマップをエクスポートする場合は、[Select All] チェックボックスをオンにします。

ステップ 4 次のオプションのうち 1 つ以上を選択します。

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

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

  - [Calibration Information for selected maps]：選択したサイトマップのキャリブレーション情報がエクスポートされます。
  - [All Calibration Information]：選択したマップに加えて、システムで使用可能なその他のキャリブレーション情報もエクスポートされます。

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

次のメッセージは、操作の進行状況を示しています。

```
Exporting data is in progress
```

TAR ファイルが作成され、ローカルマシンに保存されます。

ステップ 6 [Done] をクリックします。

Catalyst Center へのサイト階層のインポート

Cisco Prime Infrastructure から CSV ファイルとしてエクスポートしたサイト階層をインポートするには、次の手順を実行します。サイト階層のエクスポートについては、「Cisco Prime Infrastructure からのサイト階層のエクスポート （275 ページ）」を『』で参照してください。

始める前に

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

手順

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

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

ステップ 3 ダイアログボックスで、次のいずれかのオプションを選択します。

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

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

代わりにファイルピッカーを使用するには、[ファイルの選択（Choose a file）] をクリックして CSV ファイルの場所に移動し、[インポート（Import）] をクリックします。

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

Catalyst Center へのマップアーカイブのインポート

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

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

サイト階層のエクスポートについては、「Cisco Prime Infrastructure からのマップアーカイブのエクスポート （276 ページ）」を参照してください。

手順

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

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

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

ステップ 4 [Import] をクリックします。

マップアーカイブファイルがインポートされます。

既存の Ekahau ネットワーク階層の使用

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

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

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

手順

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

世界地図が右側のペインに表示されます。

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

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

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

[Export Floor Maps] ダイアログボックスが表示されます。

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

ステップ 5 [エクスポート（Export）] をクリックします。

ESX ファイルが作成され、ローカルマシンに保存されます。

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

ステップ 7 Ekahau プロジェクトをサイトの下の Catalyst Center にインポートします。詳細については、Ekahau プロジェクトを Catalyst Center にインポートします。 （279 ページ）を参照してください。

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

始める前に

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

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

手順

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

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

（注） 詳細については、サイトの作成、編集、削除 （285 ページ）、ビルディングの追加、編集、および削除 （286 ページ）、およびフロアの追加、編集、および削除 （287 ページ）を参照してください。

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

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

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

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

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

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

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

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

- 新たに検出された AP が計画された AP と一致する場合、計画された AP は検出された実際の AP で置き換えられます。
- 計画された AP のマッピングが解除されたままの場合、計画された AP を実際の AP に手動で置き換えて、失敗の原因を示すことができます。

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

[Assign Planned APs] パネルが表示されます。

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

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

ステップ 9 [Save] をクリックします。

Ekahau サイト調査の Catalyst Center へのインポート

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

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

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

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

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

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

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

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

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

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

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

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

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

始める前に

- Ekahau でプロジェクトを開き、Ekahau で許可されているモデル名（たとえば、Catalyst Center 9130 AP の場合は *Cisco C9130i*）を使用して AP モデルを設定します。

- AP マッピングファイル（CSV 形式）を作成して、使用されている各 AP モデルの無線に関する情報を Catalyst Center に提供します。

手順

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

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

または、左側のペインで親サイトの横にある省略記号 ••• にカーソルを合わせるか、[**Global**] を選択して、[**Add Area**] を選択することもできます。詳細については、サイトの作成、編集、削除 （285 ページ）を参照してください。

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

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

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

（注） CSV ファイルがない場合は、[Download AP Mapping Template] をクリックして、編集可能な CSV ファイルをダウンロードして、アップロードすることができます。

ステップ 6 [Import] をクリックします。

ファイルが正常にダウンロードされると、成功メッセージが表示されます。

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

詳細を表示するには、デバイスにカーソルを合わせます。

Catalyst Center からのネットワーク階層のエクスポート

サイト階層を CSV 形式のファイルにエクスポートできます。完全なネットワークマップ（グローバル階層）、またはサイト、建物、フロアの階層をエクスポートすることもできます。Cisco Prime Infrastructure または Ekahau Pro 形式のいずれかを選択できます。ネットワーク階層をこれらの形式にエクスポートすると、これらのツールでネットワーク階層を引き続き操作できます。

Catalyst Center からのサイト階層のエクスポート

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

手順

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

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

ステップ 3 [Export Sites] ダイアログボックスで [OK] をクリックします。

Catalyst Center からのマップアーカイブのエクスポート

完全なネットワークマップ（グローバル階層）、またはサイト、建物、フロアの階層を Cisco Prime Infrastructure または Ekahau Pro 形式のいずれかにエクスポートすることができます。最大 500 のフロアをエクスポートできます。

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

FIPSモードは、マップアーカイブのエクスポートとインポートに次のような影響を与えます。

FIPS モードが有効な場合：

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

FIPS モードが無効な場合：

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

手順

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

ステップ 2 完全なネットワークマップをエクスポートするには、マップツールバーの [Export] をクリックし、[Export Floor Maps] を選択します。

サイト、建物、またはフロアマップの階層をエクスポートするには、左側のペインで、サイト、建物、またはフロアの横にある省略記号（...）にカーソルを合わせ、[Export Floor Maps] を選択します。

エクスポートされる情報は、選択内容によって異なります。

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

ステップ 3 [Export Floor Maps] ダイアログボックスで、[Ekahau Project] または [Prime] オプションボタンのいずれかをクリックします。

ステップ 4 [Export] をクリックします。

ネットワーク階層の検索

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

手順

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

階層は、検索フィールドに入力したテキストに基づきフィルタリングされます。

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

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

   フィルタ基準に基づいて、階層がフィルタリングされます。
5. 左側のペインの検索条件を除外するには、それぞれの条件の横にある X マークをクリックします。

ネットワーク階層の作成

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

サイトの作成、編集、削除

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

手順

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

世界地図が右側のペインに表示されます。

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

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

アクション	手順
サイトを編集します。	1. 左側のペインで、サイトの横にある省略記号 ••• にカーソルを合わせて、[Edit Area] を選択します。 2. [Edit Area] ダイアログボックスで、必要な編集を行います。 3. [更新（Update）] をクリックします。
サイトを削除する。	1. 左側のペインで、サイトの横にある省略記号 ••• にカーソルを合わせて、[Delete Area] を選択します。 2. [OK] をクリックします。

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

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

ビルディングの追加、編集、および削除

手順

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

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

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

フロアの追加、編集、および削除

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

建物に基本フロアを追加するには、次の手順を使用します。

フロアとフロアマップを同時に追加するには、次のいずれかのトピックを参照してください。

• CAD マップファイルを使用したフロアの追加 （296 ページ）

- CAD 以外のマップファイルを使用したフロアの追加 （299 ページ）
- Ekahau プロジェクトを Catalyst Center にインポートします。 （279 ページ）

手順

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

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

アクション	手順
基本フロアの追加	**1.** 左側のペインで、建物の横にある省略記号 ••• にカーソルを合わせ、[**Add Floor**] を選択します。 **2.** [Floor Name] フィールドにフロアの名前を入力します。 [**Floor Name**] フィールドには次のような制限があります。 • フロア名は 40 文字までです。 • 特殊文字（& > < ? ' " / [ ]）は使用できません。 **3.** [Global Unit System] エリアで、[Feet] または [Meters] を選択します。 フロアが追加されると、すべてのサイトの全フロアが同期され、選択した単位系ですべての測定値が表示されます。グローバル単位系を更新するには、2D マップビューオプション （340 ページ）を参照してください。 **4.** ワイヤレスデバイスがある場合は、[**Type (RF Model)**] ドロップダウンリストで、フロアに適用する RF モデルを選択します。 RF モデルにより、カバレッジエリア内の RF 信号の相対強度を示す 2D および 3D ヒートマップを計算するときの RF の計算方法が決まります。 **5.** [Floor Number]、[Floor Type]、および [Thickness] フィールドを設定します。 フロアのタイプと厚さは、ワイヤレスデバイスのヒートマップを計算するときに使用されます。 **6.** [Floor Image] エリアでのフロアマップイメージのアップロードをスキップします。 **7.** [Width]、[Length]、および [Height] フィールドでマップの寸法を設定します。 **8.** [Add] をクリックします。

アクション	手順
フロアの編集	1. 左側のペインで、そのフロアの横にある省略記号 ••• にカーソルを合わせ、[**Edit Floor**] を選択します。 2. [Edit Floor] ダイアログボックスで、必要な変更を行います。 3. [更新（Update）] をクリックして変更を保存します。
フロアの削除	1. 左側のペインで、そのフロアの横にある省略記号 ••• にカーソルを合わせ、[**Delete Floor**] を選択します。 2. [OK] をクリックします。

屋外エリアの追加、編集、削除

グローバルサイト、エリア、または建物の下に屋外エリアを追加できます。次の手順を使用して、屋外エリアを追加、更新、または削除します。

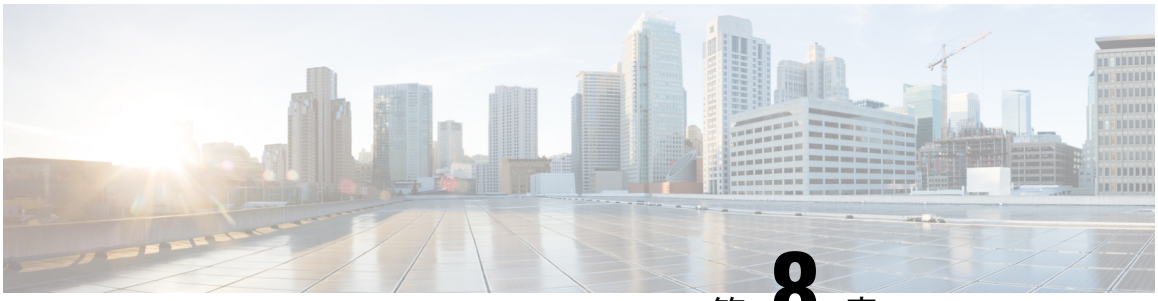
手順

ステップ 1 メインメニューから次を選択します。**[デザイン（Design）]** > **[ネットワーク階層（Network Hierarchy）]** の順に選択します。

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

アクション	手順
屋外エリアの追加	**1.** [ネットワーク階層（Network Hierarchy）] ウィンドウで、**[+サイトの追加（+ Add Site）]** > **[エリアの追加（Add Area）]** をクリックします。 または、左側のペインで親サイトの横にある省略記号アイコン（•••）にカーソルを合わせ、[屋外エリアの追加（Add Outdoor Area）] を選択することもできます。 **2.** [屋外エリア名（Outdoor Area Name）] フィールドに、屋外エリアの名前を追加します。 [屋外エリア名（Outdoor Area Name）] フィールドには、次のような制限があります。 • 名前は 40 文字までです。 • 特殊文字（& > < ? ' " / [ ]）は使用できません。 **3.** [住所（Address）] フィールドに、住所を入力するか、マップ内の任意の場所をクリックします。 住所を追加すると、[経度（Longitude）] および [緯度（Latitude）] の座標フィールドが自動的に設定されます。 **4.** [Global Unit System] エリアで、[Feet] または [Meters] を選択します。 **5.** [タイプ（RFモデル）（Type (RF Model)）] ドロップダウンリストから、屋外エリアに適用する RF モデルを選択します。 **6.** [屋外エリア画像（Outdoor Area Image）] エリアで、屋外エリアのマップ画像をアップロードします。 **7.** [幅（Width）]、[長さ（Length）]、および [高さ（Height）] フィールドでマップの寸法を設定します。 **8.** [Add] をクリックします。
屋外エリアの編集	**1.** 左側のペインで、屋外エリアの横にある省略記号（•••）にカーソルを合わせて、[屋外エリアの編集（Edit Outdoor Area）] を選択します。 **2.** [屋外エリアの編集（Edit Outdoor Area）] ダイアログボックスで、必要な編集を行います。 **3.** [更新（Update）] をクリックします。

アクション	手順
屋外エリアの削除	**1.** 左側のペインで、屋外エリアの横にある省略記号（•••）にカーソルを合わせて、[屋外エリアの削除（Delete Outdoor Area）] を選択します。 **2.** [OK] をクリックします。



第 8 章

ワイヤレス 2D および 3D マップの操作

- フロアマップの概要 （293 ページ）
- ヒートマップの概要 （294 ページ）
- マップファイルを使用したフロアの追加 （295 ページ）
- 2D マップの操作 （302 ページ）
- 3D マップの操作 （351 ページ）

フロアマップの概要

フロアマップ付きのフロアを追加する理由はいくつかあります。理由の 1 つは、ワイヤレスネットワークを現在の状態で表示することです。もう 1 つの理由は、将来の変更の計画と視覚化を支援するためです。

壁や窓などのさまざまな建物コンポーネントを含むフロアマップを作成またはインポートし、その上にワイヤレスデバイスを配置することで、ワイヤレスネットワークを視覚化できます。

インタラクティブ プランニングでは、ラスターイメージまたは CAD フロアプランを背景として計画された AP や仮想 AP および障害物を描くことで、フロアレイアウトを計画できます。フロアマップを PDF としてエクスポートして、AP を設置している技術者と共有できます。フロアの描画は、技術者がフロアのレイアウトと正確な AP の設置場所を可視化するのに役に立ちます。

インタラクティブ フロア プランニングにより、次のことが可能になります。

- キャンバスとしてラスターまたは CAD フロアプランを使用してフロアレイアウトを作成する。
- 信号カバレッジ要件に基づいて、計画された AP または仮想 AP をフロアマップに配置する。これらの仮想 AP または計画された AP は、Catalyst Center によってまだインストールまたは検出されていません。
- アンテナのタイプと方向を割り当てる。
- 信号の減衰に影響を与える壁や棚などの障害物をフロアに描画する。
- すべての AP を順番に計画する。

- フロアマップを PDF としてエクスポートする。

ヒートマップの概要

ヒートマップは、特定のエリア内のワイヤレス ネットワーク デバイスの無線周波数（RF）信号カバレッジを視覚的に表現したものです。Catalyst Center では、壁や窓など、建物のさまざまなコンポーネントを含むフロアマップを作成またはインポートし、その上にワイヤレスデバイスを配置することで、フロアごとにヒートマップを生成できます。

Catalyst Center ではフロアプランを使用して、カバレッジエリア内の RF 信号の相対強度を示す 2D および 3D ヒートマップが計算されます。2D ワイヤレスマップの場合、ヒートマップはフロアから約 91 cm（3 フィート）の高さで計算されますが、3D ワイヤレスマップの場合、ヒートマップはフロア全体のボリューム（床から天井まで）を使用して計算されます。そのため、3D ワイヤレスマップを使用すると、保管倉庫などの天井の高い環境でワイヤレスカバレッジを計算する場合に特に役立ちます。

さらに、3D ワイヤレスヒートマップでは、フロアの信号カバレッジが隣接フロアに与える影響を計算できます。隣接フロアとは、選択したフロアの真上と真下にある 2 つのフロアです。隣接フロアは設定可能なので、ヒートマップの計算で使用する隣接フロアを選択できます（3D マップビューオプション （356 ページ）の「**Contributing Floors**」を参照してください）。このようにして、あるフロアの信号カバレッジが他のフロアに与える影響を検出、可視化、および分析できます。たとえば、2 階の AP に接続しているクライアントが 1 階にある場合や、クライアントが同じチャネル上の信号を奪い合っていることがあります（同一チャネル干渉と呼ばれます）。場合によっては、意図的にこのように設計されることがありますが、意図的な設計でない場合は、変更手順を実行できます。

レガシー ヒートマップ ジェネレータは引き続き使用できます。ただし、ヒートマップをはるかに高速に生成できるため、2D と 3D の両方のヒートマップに拡張 3D 計算ヒートマップジェネレータを使用することを推奨します。

3D 計算ヒートマップジェネレータ

デフォルトで有効になっている 3D 計算ヒートマップジェネレータには、レガシー ヒートマップジェネレータに比べていくつかの利点があります。特殊なグラフィック処理ユニット（GPU）を使用して、グラフィックレンダリングが高速化されるため、レガシー ヒートマップ ジェネレータよりも大幅に高速にヒートマップを生成できます。さらに、ヒートマップの計算に含まれる壁の数に制限を設定できるため、処理速度の向上にも役立ちます。

3D 計算ヒートマップジェネレータでは、小さな障害物（約 23 cm（0.75 フィート未満））と壁の 2 番目の側面が自動的に取り除かれ、壁ごとに 1 つの側面だけが残ります。（Catalyst Center は、壁の各側面ではなく、壁ごとに減衰値を適用します。）

レガシー ヒートマップ ジェネレータ

レガシー（サーバーベース）のヒートマップジェネレータは引き続き使用できます。ただし、パフォーマンスと精度がはるかに優れているため、2D ヒートマップには拡張 3D 計算ヒートマップを使用することを推奨します。

レガシーサーバーベースのヒートマップジェネレータには、2Dおよび3Dヒートマップの計算に使用できる壁の数に制限があります。最適化後の 2D ヒートマップの最大壁数は 300 です。CAD ファイルにそれ以上が含まれている場合は、Catalyst Center で警告が表示され、（壁の長さにその減衰を掛けたものに基づいて）最適な 300 の壁が保持されます。最適化後の 3D ヒートマップの最大壁数は 3000 です。CAD ファイルにそれ以上が含まれている場合は、Catalyst Center で警告が表示され、（壁の長さにその減衰を掛けたものに基づいて）最適な 3000 の壁が保持されます。

3D 計算ヒートマップジェネレータはデフォルトで有効になっていますが、無効にして代わりにレガシー ヒートマップ ジェネレータを使用できます。

マップファイルを使用したフロアの追加

フロアを作成するときに、同時にフロアマップを含めることができます。次のトピックは、使用するフロアマップファイルタイプに応じたさまざまなフロア作成方法を理解するのに役立ちます。各方法の手順も記載されています。

フロアマップの作成方法

ワイヤレスマップを表示するには、まずフロアプランを作成するかインポートする必要があります。

- **フロアマップの作成**：フロアマップを最初から作成するには、フロア要素を手動で追加する必要があります。壁、窓、棚などのフロア要素はワイヤレスマップに表示され、ヒートマップの計算に使用されます。詳細については、2D フロアマップのデバイスとオーバーレイオブジェクトの （302 ページ）を参照してください。
- **CAD ファイルのインポート**：CAD ファイル（DXF または DWG ファイルタイプ）を使用してフロアマップをインポートすると、Catalyst Centerによって指定するフロア要素（壁、窓、棚など）にCADレイヤが変換されます。フロア要素はワイヤレスマップに表示され、ヒートマップの計算に使用されます。

  以前は、 Catalyst Center で CAD ファイルからインポートできる壁の数は制限されていませんでしたが、Catalyst Center で制限を設定できるようになりました。インポートする壁が少ないほど、ヒートマップの計算にかかる時間が短くなります。ヒートマップ生成の詳細については、ヒートマップの概要 （294 ページ）を参照してください。

  インポートするレイヤと要素を決定するときは、最も信号の減衰が大きい障害物に注目してください。原則として、壁が長く厚く高密度になればなるほど、減衰は大きくなります。キュービクルのような低い壁や柱のような狭い壁では、減衰が少なく、ヒートマップへの影響はほとんどありません。ただし、障害物の物質が高密度であっても、信号がその周囲に放射される場合、減衰は重要ではない可能性があります。建物の外側のカバレッジに関心がない場合は、外壁や窓を含めないでください。そうすることで、建物の内部をより適切に 3D で可視化できます。

CAD ファイルの特定のレイヤには壁がなく、他の要素と混在している壁がある場合は、それらの壁をインポート対象として選択しないでください。壁は後で手動で追加できます。詳細については、壁の追加、編集、および削除（331 ページ）を参照してください。

ブロック挿入とプロキシエンティティはインポートできません。インポートしたレイヤには、ライン、ポリライン、アークなどのネイティブ要素のみが含まれるようにしてください。

手順については、CAD マップファイルを使用したフロアの追加（296 ページ）を参照してください。

- **CAD 以外の画像ファイルをインポートする**：JPG、GIF、PNG、または PDF ファイルを使用してフロアプランをインポートできます。通常、このタイプのファイルは 2D フロアマップの作成に使用されます。ただし、壁や棚などのフロア要素をワイヤレスマップに表示するには、それらを手動で作成する必要があります。手順については、CAD 以外のマップファイルを使用したフロアの追加（299 ページ）を参照してください。
- **Ekahau Pro プロジェクトプランをインポートする**：障害物、AP などの Ekahau プロジェクトデータをインポートして、ワイヤレスマップを作成できます。手順については、Ekahau プロジェクトを Catalyst Center にインポートします。（279 ページ）を参照してください。

マップ内で使用するイメージファイルに関するガイドライン

マップイメージファイルを使用するには、次のガイドラインに従ってください。

- マップイメージファイルを JPG、GIF、PNG、PDF、DXF、DWG などの形式で保存できるグラフィカル アプリケーションを使用します。
- マップのイメージファイルのサイズはさまざまです。Catalyst Center は元のイメージをフル解像度でデータベースにインポートしますが、表示中は、ワークスペースに合わせてサイズが自動的に変更されます。
- インポートする前に、サイトの縦と横の寸法をフィートまたはメートル単位で取得してください。これにより、マップ インポート時にこれらの寸法を指定できます。
- 回転メタデータを持つフロアマップイメージは、CMX や Cisco Spaces に同期したときに正しく表示されないことがあるため、使用しないようにします。フロアマップイメージは Catalyst Center でサポートされているフォーマットだとしても、特定のツールがメタデータを追加する方法によって、異なる方法でレンダリングされる可能性があります。たとえば、回転メタデータを含むイメージファイルを 3 つの異なるアプリケーションで開くと、2 つのアプリケーションでは水平にレンダリングされ、もう一方のアプリケーションでは垂直にレンダリングされる場合があります。

CAD マップファイルを使用したフロアの追加

CAD ファイル（DXF または DWG ファイルタイプ）を使用して、フロアマップを作成できます。

2D フロアマップの場合、2D ビューに使用する CAD レイヤを選択する必要があります。3D フロアマップの場合、Catalyst Center によって、選択した CAD レイヤが定義したフロア要素に変換されます。フロア要素は、壁、棚、窓、障害物などと定義できます。

手順

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

ステップ 2 ビルディングを左側の階層ツリーから、横にある省略記号 ••• にカーソルを合わせて、、[Add Floor] を選択します。

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

ステップ 4 [Type（RF Model）] ドロップダウンリストから、フロアに適用する RF モデルを選択します。RF モデルは、フロアの特性に基づいて RF を計算する方法を決定します。

ステップ 5 CAD ファイル（DXF または DWG ファイルタイプ）を [Floor Image] エリアにドラッグアンドドロップします。

CAD ファイルをインポートする場合、Catalyst Center は次のタイプのエンティティのみをインポートします。

- ライン、開いたポリライン、閉じたポリゴン：LINE、LWPOLYLINE、POLYLINE、SOLID
- 半径ベース：ARC、CIRCLE、ELLIPSE（楕円の弧を含む）
- その他の形状要素：SPLINE
- テキスト：ATTRIB、MTEXT、TEXT
- ブロック挿入（通常は家具に使用）：INSERT

（注） デフォルトでは、マップをインポートした後にオーバーレイは表示されません。そのため、フロアプランをインポートしたら、必ずオーバーレイ表示を有効にしてください。マップツールバーから、[View Options] をクリックします。右側のペインで [Overlay Objects] を展開し、表示する各オブジェクトのトグルボタンをクリックします。

ステップ 6 [Floormap] ウィンドウで、フロアマップに含める CAD レイヤを選択します。

a) [2D] 列で、2D フロアマップに表示する CAD レイヤに対応するチェックボックスをオンにします。

ヒント　一部の要素がマップに表示されない場合（対応する CAD レイヤの [2D] チェックボックスがオンになっている場合でも）、AutoCAD に移動して必要な CAD ファイルを開き、必要なレイヤのすべての要素を選択し、**Explode** コマンドを実行して新しい DWG ファイルとして保存します。これで、グループエンティティやプロキシエンティティなど、サポートされていないラッパーエンティティが Catalyst Center で読み取り可能なエンティティに変換されます。次に、[Floormap] ウィンドウを閉じ、更新された CAD ファイルをアップロードします（ステップ 5（297 ページ）を参照）。

b) [Wall/Shelving Type] 列でドロップダウンをクリックし、変換する CAD レイヤごとに、変換先の壁または棚のタイプを選択します。

壁面または壁のタイプごとに、デシベル（dB）値が関連付けられています。この dB 値は、ヒートマップの信号の減衰を計算するために使用されます。詳細については、フロアマップの作成方法（295 ページ）を参照してください。

壁またはシェルフのタイプを選択すると、CAD ファイルで検出されたユニット数で [**Counter**] 列が更新され、[**Total Selected Walls Counter**] が増加します。選択した壁の総数が壁のインポート数の制限を超えた場合は、次の 3 つのオプションがあります。

- 現在の壁の数でフロアマップを追加します。この場合、Catalyst Center は最も関連性の高い壁（壁のインポート数の制限に相当）のみをインポートします。
- 壁のインポート数の制限を増やします。インポートする壁が多いほど、ヒートマップの計算に時間がかかることに注意してください。
- 1 つ以上の壁や棚のタイプの選択を解除して、選択した壁の総数を壁のインポート数の制限未満の数まで減らします。

c) [Use Selected Layers] をクリックします。

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

ステップ 8　[Add] をクリックします。

デフォルトでは、マップはグリッド付きで表示されます。グリッドのオンとオフを切り替えるには、マップの左下にある [Show Grid] トグルボタンを使用します。

（注）　フロアプランをインポートしたら、必ずオーバーレイ表示を有効にしてください。（フロアから、[View Options] をクリックし、[Overlay Objects] でオーバーレイの切り替えを有効にします）。デフォルトでは、マップをインポートした後にオーバーレイは表示されません。

CAD 以外のマップファイルを使用したフロアの追加

CAD 以外のファイル（JPG、GIF、PNG、または PDF ファイルタイプ）を使用して、フロアマップを作成できます。ただし、CAD 以外のファイルを使用する場合、壁や棚などの 3D フロア要素はインポートできず、後で手動で追加する必要があります。詳細については、2D フロアマップのデバイスとオーバーレイオブジェクトの （302 ページ）を参照してください。

手順

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

ステップ 2 ビルディングを左側の階層ツリーから、横にある省略記号 ••• にカーソルを合わせて、、[Add Floor] を選択します。

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

ステップ 4 [Global Unit System] エリアで、[Feet] または [Meters] を選択します。

フロアが追加されると、すべてのサイトの全フロアが同期され、選択した単位系ですべての測定値が表示されます。グローバル単位系を更新するには、2D マップビューオプション （340 ページ）を参照してください。

ステップ 5 [Type（RF Model）] ドロップダウンリストから、フロアに適用する RF モデルを選択します。RF モデルは、フロアの特性に基づいて RF を計算する方法を決定します。

ステップ 6 CAD 以外のファイル（JPG、GIF、PNG、または PDF ファイルタイプ）を [Floor Image] 領域にドラッグアンドドロップします。

（注） フロアから画像の幅と高さの比率を抽出できないため、フロアの正確な寸法を PDF 形式で指定してください。

ステップ 7 [Add] をクリックします。

フロアマップが作成されます。

（注） フロアプランをインポートしたら、必ずオーバーレイ表示を有効にしてください（フロアから、[View Options] をクリックし、[Overlay Objects] で、オーバーレイオブジェクトの対応するトグルボタンをクリックしてオーバーレイ表示を有効にします）。デフォルトでは、マップをインポートした後にオーバーレイは表示されません。

ステップ 8 壁を 3D フロア要素として追加するには、次の手順を実行します。

a) マップツールバーから、**[2D]** > **[Add/Edit]** > **[Overlays]** > **[Walls]** をクリックします。

b) マップの左ペインで、追加する壁のタイプをクリックします。

壁タイプがリストにない場合は、[Add Wall Type] をクリックして新しい壁タイプを作成します。

c) 描画ツールを使用してマップ上に壁を作成します。

- マップ上の壁を開始する場所をクリックします。次に、カーソルを次のポイントに移動して、もう一度クリックします。必要な形状の壁を作成するまで、このプロセスを続けます。
- 壁を完成させるには、壁を終了する場所をダブルクリックします。描画をキャンセルするには、マップを右クリックします。
- 既存の壁のタイプを変更するには、形状を右クリックして [Change Type] を選択します。
- 既存の壁を移動するには、形状を新しい場所にドラッグアンドドロップします。
- 既存の壁を削除するには、形状を右クリックして [Delete] を選択します。

図 7: 描画ツールで壁を追加する



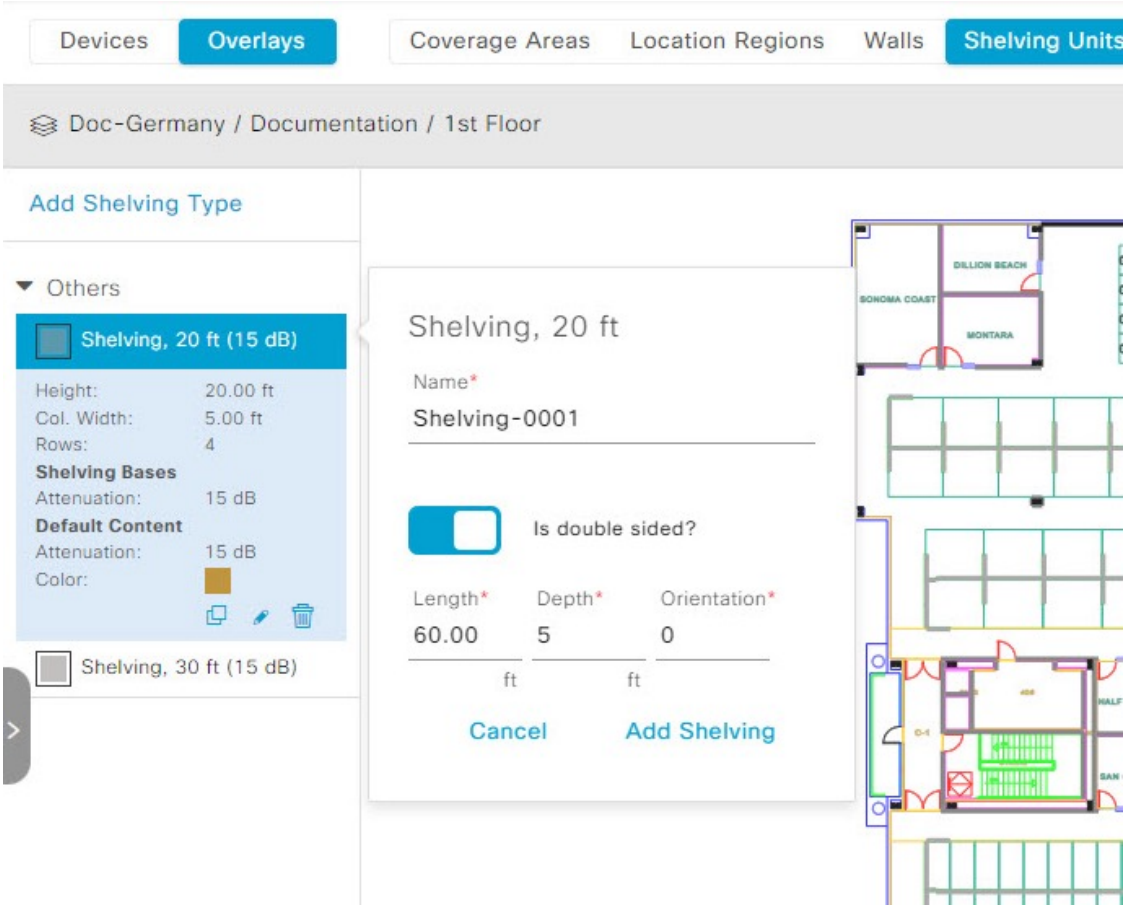
ステップ 9 シェルフユニットを 3D フロア要素として追加するには、次の手順を実行します。

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

b) マップの左ペインで、追加するシェルフタイプをクリックします。

- [Shelving] ダイアログボックスでは、シェルフタイプの名前、寸法、および向きを編集できます。向きはシェルフの角度を表します。たとえば、0 はシェルフが垂直で y 軸に平行であることを意味します。
- シェルフタイプがリストにない場合は、[Add Shelving Type] をクリックして新しいシェルフタイプを作成します。

図 *8* : 追加するシェルフタイプの選択



c) [Shelving] ダイアログボックスで、[Add Shelving] をクリックしてシェルフをフロアマップに追加します。

d) シェルフをドラッグアンドドロップして、フロアマップ上の場所に移動します。

e) シェルフを右クリックし、次のいずれかのアクションを選択します。

- [Edit]：シェルフの名前、寸法、および向きを編集します。
- [Clone]：シェルフのコピーを作成します。
- [Array]：シェルフの数とシェルフ間の距離を指定して、シェルフの配列を作成します。
- [Remove]：フロアマップからシェルフを削除します。

ステップ 10 完了したら、マップツールバーの [Save] をクリックします。

2D マップの操作

2D マップは、主にフロアマップ上の要素を構成し、ヒートマップを表示するために使用されます。

2Dマップを使用して、フロアマップの要素とオーバーレイを追加できます。2Dマップを表示しているときに、さまざまな要素とオーバーレイの表示を操作できます。デバイスデータをフィルタリングし、ワイヤレス干渉を特定することもできます。

Catalyst Center はワイヤレス信号の強度と品質を計算します。この RF 予測は、2D ワイヤレスカバレッジ領域マップ上で RF 信号の相対強度を示しているため、一般的にはヒートマップとして知られています。

前提条件

2Dワイヤレスヒートマップの計算と表示を最適に行うには、グラフィック処理ユニット（GPU）が取り付けられて有効になっているシステムを使用することを推奨します。

システムに GPU が搭載されていない場合、またはブラウザで GPU が無効になっている場合は、[3D計算ヒートマップの無効化（Disable 3D-Computed Heatmap）] オプションを必ずオンにしてください（詳細については、「2D マップビューオプション」を参照してください）。オンにしなければ、CPU使用率が高くなるなど、パフォーマンスが低下する可能性があります。このオプションを有効にすると、GPU がない場合でも 2D ビューを引き続き使用できます。

デフォルトでは、Catalyst Center 2.3.7.x で 2D マップを表示するときに 3D 計算ヒートマップエンジンが使用されます。[3D計算ヒートマップの無効化（Disable 3D-Computed Heatmap）] オプションを有効にすると、以前の Catalyst Center リリースと同様に、サーバー側のヒートマップに切り替わります。

2D フロアマップのデバイスとオーバーレイオブジェクトの

2D マップで、デバイスを設定し、フロアマップ上にオブジェクトをオーバーレイできます。

デバイス

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

してから、Assurance サーバーと直接通信します。センサーテストに関する情報を含む詳細については、「」『*Cisco Catalyst Assurance User Guide*』[英語] を参照してください。

オーバーレイオブジェクト

- [Coverage Areas]：デフォルトでは、フロアマップの一部として定義されたエリアは、無線カバレッジエリアと見なされます。ただし、長方形以外のビルディングがある場合、またはフロア内で長方形以外または多角形のエリアをマークする場合には、[Coverage Areas] 描画ツールを使用してカバレッジエリアを作成できます。
- [Openings]：吹き抜けはアトリウムとも呼ばれ、ビルディング内のオープンエアーまたは天窓で覆われたエリアです。吹き抜けは複数のフロアに伸びる可能性があり、ワイヤレス信号のカバレッジエリアに影響を与える可能性があります。
- [Location Regions]：ロケーションリージョンは、ロケーションサービス（Cisco CMX または Cisco Spaces）で使用されます。ロケーションリージョンでは、クライアントの配置時に包含エリアまたは除外エリアを定義します。包含エリアは計算に含まれ、除外エリアは計算に含まれません。デフォルトでは、フロアを作成すると、フロア上のリージョン全体が包含リージョンとして定義されます。デフォルトの包含リージョンを手動で編集し、フロアに除外リージョンを設定できます。たとえば、実際のクライアントを配置できない建物内の開口部やアトリウム、大型ラックなどのエリアを除外できます。
- [Walls]：壁は、窓、小部屋、ドアなど、建物の外部または内部の垂直構造を定義します。それぞれ異なる材料で構成され、密度が異なる可能性があるため、RF 信号の減衰とヒートマップの計算に大きな影響を与える可能性があります。たとえば、フロアマップに含める壁の数が多いほど、ヒートマップの計算にかかる時間が長くなります。ただし、フロアマップに多数の壁がある場合でも、ヒートマップの計算に使用される壁の数を調整できます。詳細については、「2D マップビューオプション （340 ページ）」および「3D マップビューオプション （356 ページ）」を参照してください。
- [Shelving Units]：シェルフユニットは、RF 信号の減衰とヒートマップの計算に大きな影響を与える可能性のある障害物です。シェルフユニットがある場所の例としては、天井が高い倉庫などがあります。
- [Markers]：マーカーは、マップ上の場所を示します。マーカーを作成するときは、後で識別しやすいように、マーカーに名前を付けて配置することができます。
- [GPS Markers] ：Catalyst Centerと統合すると、Cisco Spacesや Cisco Connected Mobile Experiences（CMX）などのロケーションサービスは、GPS マーカーを使用してクライアントのおおよその地理的位置を計算します。
- [Align Points]：位置合わせポイントは、物理的な形状が異なる複数のフロアを配置するために使用されるマーカーです。3D マップでは、フロアはマップの左上隅（ポイント 0,0）に配置されます。各フロアを独立して管理する場合、配置のずれは問題になりません。ただし、一部の 3D マップの機能を使用するには、実際のフロアをそのまま配置する必要があります。このずれを補正するために、2 つ以上のフロアに 1 つ以上の位置合わせポイントを挿入して、3D マップ内でフロアを上下に適切に配置できます。

フロアマップでの AP の取り扱い

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

フロア マップに AP を配置する際は、次の注意事項を考慮してください。

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

Cisco Prime Infrastructure からの AP のエクスポートと Catalyst Center へのインポート

Catalyst Center では、AP のコレクションをフロアマップにインポート、割り当て、および配置できます。Cisco Prime Infrastructure に AP の既存のコレクションがある場合は、それを Catalyst Center にインポートすると、フロアマップへの AP のインポート、割り当て、および配置に費やす時間と労力を節約できます。

この手順では、Cisco Prime Infrastructure から AP の既存のコレクションをエクスポートして Catalyst Center にインポートする方法について説明します。

始める前に

- このタスクを実行するには、**スーパー管理者**または**ネットワーク管理者**である必要があります。
- インベントリに AP があることを確認します。ない場合は、[Discovery] 機能を使用して検出します。
- フロアマップ上に AP を追加して配置します。

• エリア、ビルディング、およびフロアは、サイト階層に存在する必要があります。

手順

ステップ 1 AP 位置を CSV ファイルとして Cisco Prime Infrastructure からワークステーションにエクスポートします。

ステップ 2 メインメニューから次を選択します。**[Design]** > **[Network Hierarchy]**。

ステップ 3 サイト左側の階層ツリーから、横にある省略記号 ••• にカーソルを合わせて、、[Import Access Points] を選択します。

または、マップツールバーから、[Import] をクリックし、[Import Access Points] を選択します。

ステップ 4 [Import Access Points] ダイアログボックスで、AP ファイルをドラッグアンドドロップするか、[Choose a file] をクリックしてワークステーションからファイルを選択します。

（注）
- Prime テンプレートを使用して [AP Positions] CSV ファイルを手動で作成するには、[Download Prime Template] をクリックして、Prime テンプレートをワークステーションにエクスポートします。Prime テンプレートは、ネストされたファイルをサポートしていません。
- Catalyst Center テンプレートを使用して [APの配置（AP Positions）] CSV ファイルを手動で作成するには、[Cisco DNA Centerテンプレートのダウンロード（Download Cisco DNA Center Template）] をクリックして、Catalyst Center テンプレートをワークステーションにエクスポートします。Catalyst Center テンプレートは、ネストされたファイルをサポートしています。

CSV ファイルがダウンロードされるまで待ちます。CSV ファイルには、ネットワーク内のさまざまなサイトの AP 位置に関する情報が含まれています。

ステップ 5 [Import] をクリックします。

[概要のインポート（Import Summary）] ウィンドウが表示されます。

- [Information] タブに、正常にインポートされた AP のリストが表示されます。
- [Warning] タブをクリックすると、警告のリストが表示されます。
- [Error] タブをクリックすると、エラーのリストが表示されます。

ステップ 6 [Import Summary] ウィンドウの右上隅にある [Done] をクリックして、[Network Hierarchy] ウィンドウに戻ります。

マップへの AP の追加

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

始める前に

インベントリにシスコの AP があることを確認してください。ない場合は、[Discovery] 機能を使用して検出します。『検出の概要 （73 ページ）』を参照してください。

手順

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

ステップ 2 フロアを 左側の階層ツリーから、以下を選択します します。

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

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

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

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

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

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

編集モードでは、新しく追加されたAPは、マップの左ペインの **[Unpositioned]** カテゴリに表示されます。詳細については、AP をマップ上に配置する （314 ページ）を参照してください。

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

次のタスク

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

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

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

ワイヤレスコントローラとそのすべての管理対象 AP をインベントリから削除すると、Catalyst Center はマップ上に対応する AP の計画済み AP アイコンを表示します。詳細については、AP アイコンと計画済み AP アイコンについて （345 ページ）を参照してください。

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

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

- インベントリから ワイヤレスコントローラ を削除する前に、対応する AP を **[Global]** サイトに割り当てます。詳細については、プロビジョニングされていないデバイスのサイトへの割り当て （189 ページ）を参照してください。
- インベントリから ワイヤレスコントローラ を削除した後、対応する計画済み AP をマップから削除します。詳細については、AP をマップから削除する （324 ページ）を参照してください。

マップへの計画済み AP の追加

この手順では、AP モデルカタログ機能を使用して、計画済み AP をフロアに追加し、そのモデル、アンテナタイプ、方位角、および仰角を設定する方法を示します。作成して配置した計画済み AP を使用して、プロパティが同じ計画済み AP をさらに追加できます。

手順

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

ステップ 2 フロアを 左側の階層ツリーから、以下を選択します します。

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

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

ステップ 4 マップの左側のペインにある [Planned AP Models] エリアで、追加する計画済み AP の AP モデルをクリックします。

（注） AP モデルがリストにない場合は、[Add Model] をクリックして、リストに追加する AP モデルを選択します。

ステップ 5 フロアマップで、計画済み AP を配置する場所をクリックします。

選択したモデルの計画済み AP がフロアマップに追加され、[Edit Planned AP] スライドインペインが表示されます。このペインには、デフォルトで AP 名が追加されます。

ステップ 6 [Edit Planned AP] スライドインペインで、[AP Name] フィールドの横にある歯車のアイコンをクリックします。

[Name pattern] ダイアログボックスが表示されます。

ステップ 7 最初の AP をフロアに追加するときは、SJC-BLD21-FL2-AP#### などの有効な名前パターンを入力してから、[Set name pattern] をクリックするようにしてください。

（注） 計画済み AP は、Catalyst Center 内で一意である必要があります。そのため、名前パターンでフロアを識別できるようにします。

名前パターンの #### は、[AP Name] の番号に置き換えられます（SJC-BLD21-FL2-AP0001 や SJC-BLD21-FL2-AP0002 など）。

ステップ 8 [Antenna] ドロップダウンリストから、デュアルアンテナを含む、この AP の適切なアンテナタイプを選択します。

（注） アンテナイメージは、選択されたアンテナを反映しています。

ステップ 9 アンテナタイプに応じて、[Azimuth] と [Elevation] の方向を度数で入力します。

ステップ 10 （任意）必要に応じて、その他の設定を構成します。これらの設定の詳細については、AP の編集 （318 ページ）を参照してください。

ステップ 11 必要に応じて、次のタスクを実行します。

- 追加した計画済み AP と同じプロパティを持つ別の計画済み AP を追加するには、フロアマップ上で、新しい AP を配置する場所をクリックします。

  新しい AP アイコンがマップに表示されます。すべてのプロパティが継承され、AP 名が付加されています（例：BLD1-AP0002-TX）。

- 同じプロパティを持ち、AP 名が付加された計画済み AP をさらに追加するには、フロアマップをクリックします。
- フロアマップへの計画済み AP の追加を止めるには、**Esc** を押すか、フロアマップを右クリックします。
- 計画済み AP を再配置するには、AP をフロアマップ内の適切な場所にドラッグアンドドロップします。
- 計画済み AP を削除するには、AP のアイコンを右クリックし、[Remove] をクリックします。
- 計画済み AP を編集するには、AP のアイコンを右クリックし、[Edit] をクリックします。
- 計画済み AP を自動配置するには、マップへの計画済み AP の自動配置 （309 ページ）を参照してください。

ステップ 12 マップツールバーで [Save] をクリックします。

マップへの計画済み AP の自動配置

フロアマップで計画済み AP を自動配置すると、マップの寸法内に配置できる計画済み AP の数を確認できます。計画済み AP のモデル、計画済み AP 間の希望する最大距離、およびカバレッジエリアの寸法を使用して、システムは、計画済み AP の配置の最大数を計算し、それらをフロアマップに追加します。

手順

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

ステップ 2 フロアを 左側の階層ツリーから、以下を選択します します。

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

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

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

ステップ 5 [Autoplace Planned APs] ダイアログボックスで、AP のモデルを選択し、計画済み AP 間の希望する最大距離を入力し、有効な名前パターンを入力します。

名前パターンの #### は、計画済み AP の名前の番号に置き換えられます（AP-0001、AP-0002 など）。

ステップ 6 [作成（Create）] をクリックします。

システムは、計画済み AP の配置の最大数を計算し、それらをフロアマップに追加します。新たに配置されたすべての計画済み AP が自動的に選択され、[APの編集（Edit APs）] スライドインペインが表示されます。ここで、すべての新しい計画済み AP をまとめて編集できます。

ステップ 7 [Antenna] ドロップダウンリストから、アンテナタイプを選択します。

ステップ 8 （任意） 計画済みの AP をまとめて更新するには、使用可能なフィールドを編集します。

ステップ 9 [Apply] をクリックして、自動配置されたすべての計画済み AP に更新を適用します。

ステップ 10 （任意） 必要に応じて、次のタスクを実行します。

- 計画済み AP を編集するには、計画済み AP のアイコンをクリックするか、計画済み AP のアイコンを右クリックして [Edit] を選択します。
- 計画済み AP の編集を停止するには、**Esc** キーを押すか、フロアマップを右クリックするか、[Edit Planned AP] スライドインペインを閉じます。
- 計画済み AP を再配置するには、AP をフロアマップ内の適切な場所にドラッグアンドドロップします。
- 計画済み AP を削除するには、計画済み AP のアイコンを右クリックし、[Remove] を選択します。

ステップ 11 準備ができたら、[Save] をクリックしてマップの変更を保存します。

マップ上の AP の自動検出

アクセスポイントの自動検出機能により、マップ上の AP を自動的に位置付けして検出できます。この機能を使用すると、手動による介入なしでマップ上に AP をシームレスかつ正確に配置し、詳細なマップを介して AP の正確な場所を特定できます。AP の自動かつ正確な配置は、新しいサイトの追加またはサイトの拡張シナリオでの展開時間とコストの削減に役立ち、AP の遠隔管理アクティビティを容易にします。この機能の使用に関する詳細については、AP 自動検出のガイドラインと制約事項 （311 ページ）を参照してください。

始める前に

AP 測定データを生成します。詳細については、AP 間測定データの生成 （313 ページ）を参照してください。

手順

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

ステップ 2 左側の階層ツリーから、フロアを選択します。

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

ステップ 4 フロアマップに AP を 1 つも配置していない場合は、次の手順に従って AP を自動的に配置します。

a) 自動検出対応 AP をフロアマップに追加します。マップへの AP の追加 （306 ページ）を参照してください。

b) マップの左側のペインで、**[Auto Locate Access Points]** をクリックします。

自動検出対応 AP のリストが左側のペインに表示されます。AP 測定データに基づいて、AP はアンカー選択のために自動的にランク付けされます。

c) アンカー AP をマップ上に配置します。

マップの左側のペインから AP を選択し、マップ上の目的の場所にドラッグアンドドロップします。残りのアンカー AP も同様に配置します。残りの AP をフロアに配置する前に、少なくとも 4 つのアンカー AP を選択する必要があります。

d) [Run Auto Locate] をクリックして、マップ上に残りの AP を自動的に配置します。

AP はマップ上に自動的に配置され、ポップアップウィンドウに AP 自動検出の概要が表示されます。

e) **[AP Auto Locate Summary]** ポップアップウィンドウで、**[View Results]** をクリックします。

配置された AP の詳細なフロアマップが表示されます。結果は、アンカー AP と新しく配置された AP でフィルタ処理できます。

f) **[Save]** をクリックして、マップの変更を保存します。

ステップ 5 AP をフロアマップにすでに配置している場合は、次の手順に従って AP を検出し、AP の位置を確認します。

a) マップの左側のペインで、**[Auto Locate Access Points]** をクリックします。

b) マップ上のアンカー AP を選択します。自動検出を続行するには、少なくとも 4 つのアンカー AP を選択する必要があります。

c) AP フロアマップウィンドウで **[Run Auto Locate]** をクリックします。

ポップアップウィンドウに、アンカー AP の数、適切に配置された AP、移動またはスワップされた AP など、AP 自動検出の概要が表示されます。

d) **[AP Auto Locate Summary]** ポップアップウィンドウで、**[View Results]** をクリックします。

マップには、フロアマップ上のすべての AP の位置が、アンカー AP、適切に配置された AP、移動またはスワップされた AP などの詳細とともに表示されます。左側のペインでオプションを選択して、結果をフィルタ処理します。移動またはスワップされた AP がある場合、位置は自動的に修正されます。

e) **[Save]** をクリックして、マップの変更を保存します。

f) **[Run Auto Locate]** を再度クリックして、すべての AP が適切に配置されていることを確認します。

AP 自動検出のガイドラインと制約事項

AP 自動検出機能を使用する際のガイドラインと制限事項。

- 現在のリリースでは、自動検出機能はベータ版なので、機能を有効にする必要があります。ユーザーは、Catalyst Center ホームページで機能が使用可能なことを確認できます。

また、[Feature Enabling] ウィンドウにリダイレクトされます。機能を有効にすると、[Network Hierarchy] ウィンドウから自動検出機能を使用できます。機能の可用性とアクティベーションの詳細については、シスコのセールス担当者までお問い合わせください。

- この機能は、Cisco IOS XE リリース 17.12.x 以降を実行しているすべての Cisco Catalyst 9800 シリーズ ワイヤレス コントローラと、Fine Timing Measurement（FTM）、Wi-Fi 6E、Wi-Fi 7 機能を備えている AP でサポートされています。



（注）
- Cisco IOS XE リリース 17.12.x を実行しているワイヤレスコントローラでは、AP レンジングプロセスに最大 15 分かかる場合があります。
- FTM 信号を受信できない隔離された AP に関する AP レンジングデータは収集できません。
- 現在、この機能は GPS 対応 AP ではサポートされていません。

- 自動検出機能は、フロアごとに最大 50 の AP でサポートされます。
- この機能は、マルチフロア AP ではサポートされていません。一度に 1 つのフロアの AP に対して自動検出を実行できます。
- フロア境界の外側にある AP は、AP 測定データの生成対象とは見なされません。
- 十分なネイバー AP が存在しない AP は、自動検出に使用できません。
- AP 間のきめ細かいレンジングはサポートされていません。
- プロビジョニングとレンジングは、共有サイトタグ（複数のフロアで共有されるタグ）を使用する AP でサポートされます。
- デフォルトのタグを持つ AP は、測定データの生成ではサポートされていません。
- Catalyst Center が Cisco Spaces や Cisco Connected Mobile Experiences（CMX） などのロケーションサービスと統合されている場合、すべてのアンカー AP タグがエクスポートされるわけではありません。Catalyst Center と Cisco Spaces またはコネクテッド モバイル エクスペリエンス（CMX）間の相互運用性は、AP 自動検出機能ではサポートされていません。
- アンカータグを使用したマップアーカイブのエクスポートとインポートはサポートされていません。マップアーカイブをインポートした後、アンカー AP に手動でタグを付ける必要があります。
- AP 測定データを生成するための AP レンジングプロセスにより、接続されているクライアントのネットワークが中断されることがあるため、レンジングプロセスは、オフピーク時に実行することを推奨します。
- AP 自動検出のパフォーマンスは、フロア上の AP 数、AP の場所、フロアエリア、およびレンジングデータによって異なります。

- AP 測定データは Catalyst Center に 30 日間のみ保存され、その後は削除されます。AP 測定データを生成するには、レンジングプロセスを再トリガーする必要があります。
- AP レンジングプロセス中にワイヤレスコントローラの再プロビジョニングをトリガーしないことを推奨します。

AP 間測定データの生成

フロア上のすべての対象 AP の AP 測定データを生成するには、次の手順を使用します。このデータは、フロアマップ上の AP の自動配置や検出に使用されます。

始める前に

インベントリにシスコの AP があることを確認してください。ない場合は、[Discovery] 機能を使用して検出します。『検出の概要 （73 ページ）』を参照してください。

AP レンジングプロセスのガイドラインと制限事項については、AP 自動検出のガイドラインと制約事項 （311 ページ）を参照してください。

手順

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

ステップ 2 左側の階層ツリーから、フロアを選択します。

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

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

ステップ 5 アンカーリングのベストプラクティスを確認し、[閉じる（Close）] をクリックします。

ステップ 6 **[Generate AP to AP Measurement]** をクリックします。

[Generate AP to AP Measurement] ウィンドウには、測定対象となるフロア上のすべての AP が表示されます。

ステップ 7 測定する AP を選択します。

フロア上の対象となるすべての AP を選択するか、必要な AP を個別に選択するかを選べます。

ステップ 8 展開のためのタスクのスケジュールを設定します。

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

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

（注） 接続中のクライアントでネットワークの中断が発生する可能性があるため、測定プロセスは後でオフピーク時間帯に実行するようにスケジュールすることを推奨します。

ステップ 9 [Tasks] ウィンドウで、タスクの展開を監視します。

計画済み AP への実際の AP の割り当て

ワイヤレスネットワークに実際の AP をインストールした後、それらをマップ上の計画済み AP に割り当てることができます。この手順では、計画済み AP を実際の AP に割り当てる方法について説明します。

手順

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

ステップ 2 フロアを 左側の階層ツリーから、以下を選択します します。

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

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

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

ステップ 5 フロアマップで、計画済み AP をクリックします。

ステップ 6 [Assign Planned APs] スライドインペインで、割り当てる AP の横にあるチェックボックスをオンにします。

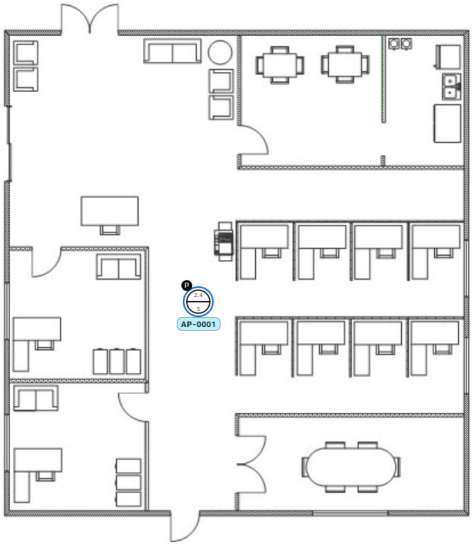
ステップ 7 [**Assign**] をクリックします。

ステップ 8 マップツールバーで [Save] をクリックします。

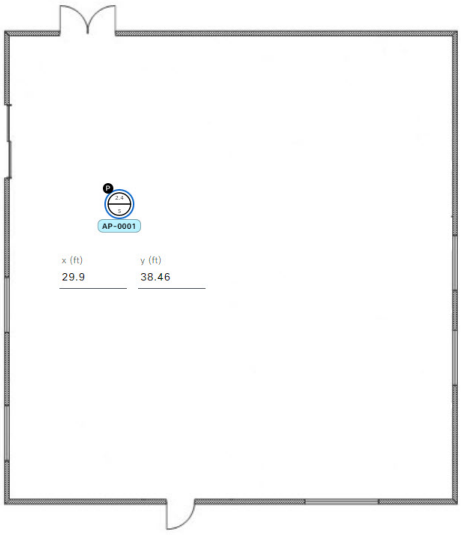
AP をマップ上に配置する

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

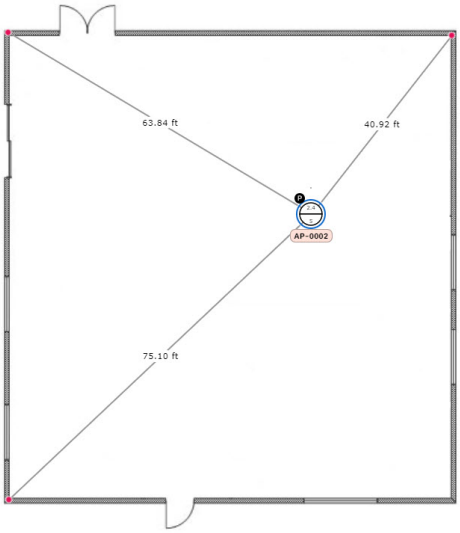
- マップ上に手動で配置します。フロアマップの詳細に関連付けることができる建物内の参照ポイントを使用して AP のおおよその位置を把握できる場合は、この方法を使用します。



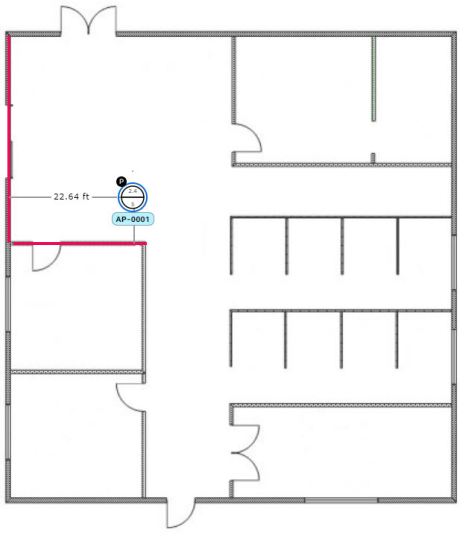
- **x** 座標と **y** 座標を定義します。AP の正確な座標が分かっており、マップ上の位置をできるだけ正確なものにしたい場合は、この方法を使用します。



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



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



最初の方法（手動配置）を除くすべての方法では、測定値を手元に用意し、[**Global Map Properties**] 設定で測定単位が正しく指定されていることを確認する必要があります。詳細については、2D マップビューオプション （340 ページ）を参照してください。

手順

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

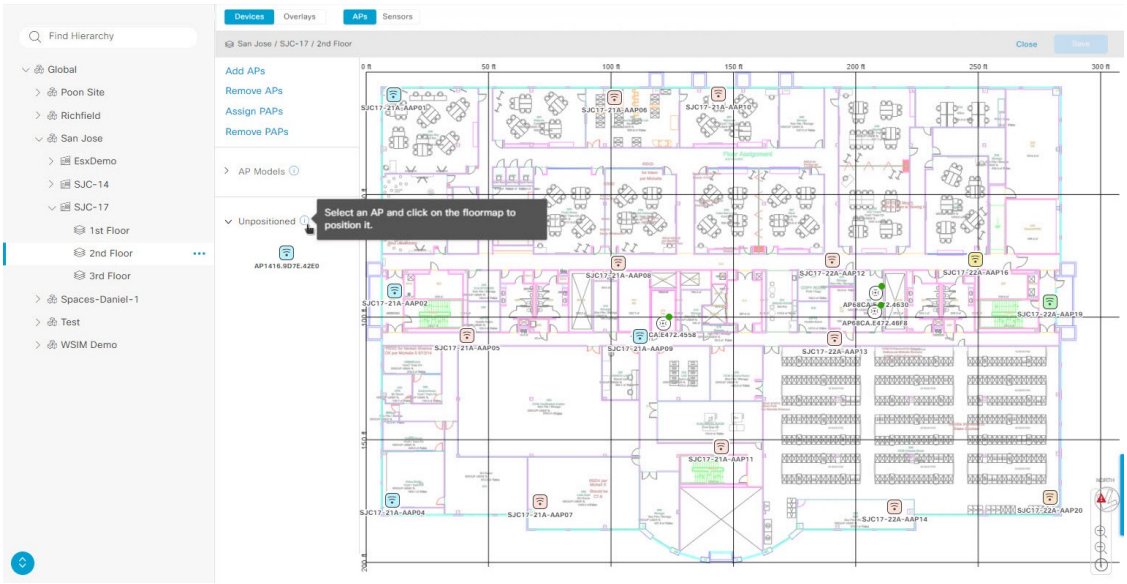
ステップ 2 フロアを 左側の階層ツリーから、以下を選択します します。

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

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

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

図 *9*：未配置の *AP*



ステップ 5 AP を配置するには、次のいずれの方法を使用します。

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

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

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

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

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

壁の間の定義された距離に基づいて AP が配置されます。

ステップ 6 マップツールバーで [Save] をクリックします。

（注） Cisco Connected Mobile experience（CMX）が Catalyst Center と同期されている場合は、ヒートマップ上のクライアントの場所を表示できます。Cisco CMX 設定の作成 （521 ページ）を参照してください。

マップへの AP の再配置

AP をマップ上に配置した後、それらを再配置できます。この手順では、AP をマップ上に再配置する方法を示します。

（注） このタスクは、2D または 3D マップで実行できます。

手順

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

ステップ 2 フロアを 左側の階層ツリーから、以下を選択します します。

ステップ 3 2D の場合：

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

b) マップで、AP を新しい位置にドラッグアンドドロップします。

ステップ 4 3D の場合：

a) マップツールバーで、**[3D]** > **[Edit/Clone]** をクリックします。

b) マップで AP を右クリックし、[Move] を選択します。

c) マップで、AP を新しい位置にドラッグアンドドロップします。

ステップ 5 マップツールバーで [Save] をクリックします。

AP の編集

この手順を使用して単一の AP または計画済み AP の構成を編集します。

一度に複数の AP の構成を変更するには、複数の AP の編集 （321 ページ）を参照してください。

（注） このタスクは、2D または 3D マップで実行できます。

手順

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

ステップ 2 フロアを 左側の階層ツリーから、以下を選択します します。

ステップ 3 ワイヤレスマップの種類に応じて、編集する AP をクリックします。

使用しているワイヤレスマップの種類	下記を実行
2D ワイヤレスマップ	**1.** マップツールバーで、**[2D]** > **[Add/Edit]** をクリックします。 **2.** マップで AP を右クリックし、[Edit] を選択します。
3D ワイヤレスマップ	**1.** マップツールバーで、**[3D]** > **[Edit/Clone]** をクリックします。 **2.** マップ上で、編集する AP をクリックします。

ステップ 4 スライドインペイン で、利用可能な AP と計画済み AP の設定を編集します。

- [AP Name] または [Planned AP Name]：AP の名前。
- [MAC Address]：選択した AP の MAC アドレス。
- [AP Model]：選択した AP のモデル。

（注） 3D マップの AP の場合、[AP Model] フィールドを変更してその影響を可視化できますが、変更は保存されず、フロア間で保持されません。代わりに、[Inventory] ウィンドウからこの AP フィールドを更新できます。

- [x (ft)]：AP の X 軸座標。
- [y (ft)]：AP の Y 軸座標。
- [AP Height (ft)]：AP の高さ。
- [Antenna]：この AP のアンテナタイプ。

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

• [Channel]：AP で使用されるチャネル。AP モデルでサポートされているチャネルのみが表示されます。

（注） 3D マップの AP の場合、[Channel] フィールドを変更してその影響を可視化できますが、変更は保存されず、フロア間で保持されません。代わりに、[Inventory] ウィンドウからこの AP フィールドを更新できます。

• [Tx Power (dBm)]：チャネルの送信電力。チャネルでサポートされている電力レベルのみが表示されます。

（注） 3D マップの AP の場合、[Tx Power (dBm)] フィールドを変更してその影響を可視化できますが、変更は保存されず、フロア間で保持されません。代わりに、[Inventory] ウィンドウからこの AP フィールドを更新できます。

• [Azimuth]：アンテナ方位角。x 軸に対して時計回りに測定されたアンテナの角度です。方位角の範囲は 0 ー 360 です。Catalyst Center では、右向きは 0 度または 360 度で、下向きは 90 度です。

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

（注） 無指向性アンテナの場合、仰角が 0 の場合、方位角は関係ありません。

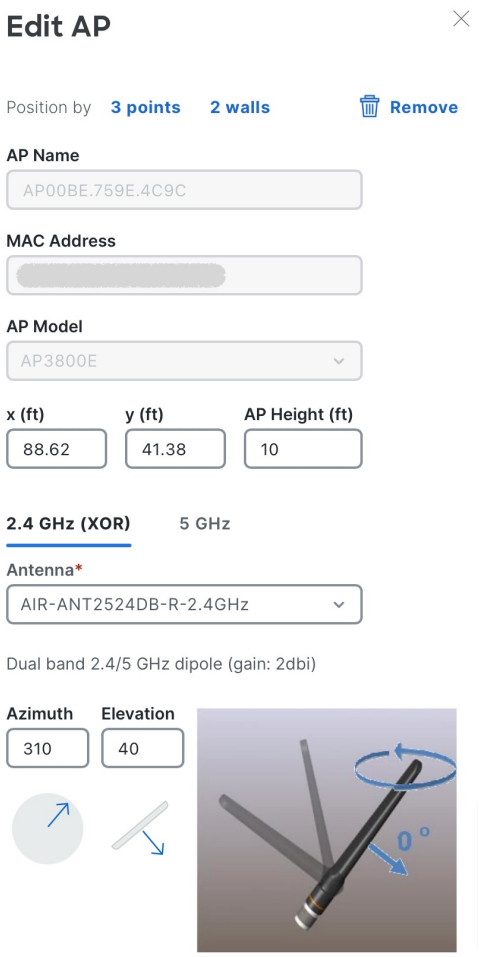
• [仰角（Elevation）]：度単位で測定されます。

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

（注） このフィールドが無効になっている場合は、グレー表示され、AP から報告されたチルト値が表示されます。この無効化は、AP 無線が加速度センサーハードウェアをサポートしており、AP で加速度センサー機能が有効になっていることを意味します。

（注） 天井に配置するように設計された AP およびアンテナモデルの場合、仰角が 0 の場合は下を向きます。壁に配置するように設計された AP およびアンテナモデルの場合、仰角を 0 にすると水平方向を向き、負の値の場合は下を向きます。

図 *10 : [Edit AP]* スライドインペイン



ステップ 5 編集を行った後、次の表を使用して続行します。

使用しているワイヤレスマップの種類	下記を実行
2D ワイヤレスマップ	スライドインペインを閉じます。
3D ワイヤレスマップ	[Apply] をクリックして、変更を適用します。

ステップ 6 マップツールバーで [Save] をクリックします。

複数の AP の編集

AP を 1 つだけ、または計画済み AP を選択すると、編集可能なすべての属性を変更できます。ただし、複数の AP または計画済み AP を選択すると、次のように一部の属性のみが編集可能になります。

- 選択したデバイスの属性値が同じ場合、その値が表示されます。それ以外の場合、値は空白です。いずれの場合も、値を変更すると、選択したすべてのデバイスに新しい値が適用されます。
- 選択した AP のモデル番号と無線（無線の数と動作帯域）が同じ場合、アンテナは編集可能です。それ以外の場合、アンテナは編集できません。
- 計画された AP のモデル番号は変更できますが、追加された AP のモデル番号は変更できません。そのため、AP を選択した場合、モデル番号は編集できません。
- 一括変更はより多くのデバイスに影響を与えるため、すぐには有効になりません。[Apply] をクリックして変更内容を適用する必要があります。

この手順では、一度に複数の AP の編集可能な属性を更新する方法について説明します。

（注） このタスクは、2D または 3D マップで実行できます。

手順

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

ステップ 2 フロアを 左側の階層ツリーから、以下を選択します します。

ステップ 3 次のいずれか 1 つのタスクを実行します。

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

ステップ 4 次のいずれかの方法を使用して、AP を選択します。

- 最初のデバイスをクリックし、Shift キーを押しながら残りのデバイスをクリックします。
- 2D マップ ナビゲーション コントロール ツールバーで、[Select by rectangle] アイコン（[ ]）をクリックします。次に、マップの領域をクリックし、強調表示された長方形をドラッグして、連続した領域内の AP を選択します。長方形内で強調表示されているすべての AP が選択されています。

AP の選択を解除するには、次のいずれかの方法を使用します。

- 1 つの AP の選択を解除するには、Shift キーを押しながら AP をクリックします。
- 1 つを除くすべての AP の選択を解除するには、選択したままにする AP をクリックします。その他はすべて選択解除されます。
- すべての AP の選択を解除するには、ESC キーを押すか、[Edit] ペインを閉じます。

ステップ 5 スライドインペイン で、必要に応じて次の AP の設定を行います。

- [AP Name] または [Planned AP Name]：AP の名前。
- [MAC Address]：選択した AP の MAC アドレス。
- [AP Model]：選択した AP のモデル。



（注） 3D マップの AP の場合、[AP Model] フィールドを変更してその影響を可視化できますが、変更は保存されず、フロア間で保持されません。代わりに、[Inventory] ウィンドウからこの AP フィールドを更新できます。

- [x]：AP の x 軸座標。値は手動で入力できます。
- [y]：AP の y 軸座標。値は手動で入力できます。
- [AP Height]：AP の高さ。値は手動で入力できます。
- [Antenna]：この AP のアンテナタイプ。



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

- [Channel]：AP で使用されるチャネル。AP モデルでサポートされているチャンネルのみが表示されます。



（注） 3D マップの AP の場合、[Channel] フィールドを変更してその影響を可視化できますが、変更は保存されず、フロア間で保持されません。代わりに、[Inventory] ウィンドウからこの AP フィールドを更新できます。

- [Tx Power (dBm)]：チャネルの送信電力。チャネルでサポートされている電力レベルのみが表示されます。



（注） 3D マップの AP の場合、[Tx Power (dBm)] フィールドを変更してその影響を可視化できますが、変更は保存されず、フロア間で保持されません。代わりに、[Inventory] ウィンドウからこの AP フィールドを更新できます。

- [Azimuth]：アンテナ方位角。x 軸に対して時計回りに測定されたアンテナの角度です。方位角の範囲は 0 ー 360 です。Catalyst Center では、右向きは 0 度または 360 度で、下向きは 90 度です。

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

（注） 無指向性アンテナの場合、仰角が 0 の場合、方位角は関係ありません。

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

（注） 天井に配置するように設計された AP およびアンテナモデルの場合、仰角が 0 の場合は下を向きます。壁に配置するように設計された AP およびアンテナモデルの場合、仰角を 0 にすると水平方向を向き、負の値の場合は下を向きます。

ステップ 6 スライドインペイン で [Apply] をクリックして、変更を適用します。

ステップ 7 マップツールバーで [Save] をクリックします。

AP をマップから削除する

この手順では、AP および計画済み AP（PAP）をマップから削除する方法について説明します。

手順

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

ステップ 2 フロアを 左側の階層ツリーから、以下を選択します します。

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

ステップ 4 AP（計画済み AP を含む）を削除するには、次の手順を実行します。

a) AP をクリックします。複数の AP を選択する場合は、最初の AP をクリックし、**Shift** キーを押しながら残りの AP をクリックします。

b) スライドインペインで、[Remove] をクリックします。

ステップ 5 マップツールバーで [Save] をクリックします。

フロアマップでのセンサーの操作

次のトピックでは、フロアマップにセンサーを追加し、必要に応じてセンサーを配置、再配置、および削除する方法を説明します。

センサーの詳細については、2D フロアマップのデバイスとオーバーレイオブジェクトの（302 ページ）を参照してください。

マップへのセンサーの追加

この手順では、センサーをマップに追加する方法を示します。

始める前に

インベントリに Cisco AP 1800S センサーがあることを確認します。Cisco Aironet 1800s アクティブセンサーをインベントリで表示するには、プラグアンドプレイを使用してプロビジョニングする必要があります。『*Cisco Catalyst Assurance User Guide*』の「Provision the Wireless Cisco Aironet 1800s Active Sensor」[英語] のトピックを参照してください。

手順

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

ステップ 2 フロアを 左側の階層ツリーから、以下を選択します します。

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

ステップ 4 [Add Sensors] スライドインペインで、追加するセンサーのチェックボックスをオンにします。またはセンサー行の横にある [Add] をクリックします。

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

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

ステップ 5 マップツールバーで [Save] をクリックします。

センサーをマップ上に配置する

新しく追加されたセンサーは、編集モードのマップの左ペインの [Unpositioned] カテゴリに表示されます。この手順では、センサーを最初に追加した後にセンサーを配置する方法を示します。

始める前に

センサーは、配置する前にマップに追加する必要があります。詳細については、マップへのセンサーの追加 （325 ページ）を参照してください。

手順

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

ステップ 2 フロアを 左側の階層ツリーから、以下を選択します します。

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

ステップ 4 マップの左側のペインで、[Unpositioned] カテゴリのセンサーをクリックして、センサーを配置します。

ステップ 5 フロアマップ上で、センサーを配置する場所をクリックします。

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

ステップ 6 マップツールバーで [Save] をクリックします。

マップへのセンサーの再配置

マップ上にセンサーを配置した後、それらを再配置できます。この手順では、センサーをマップ上に再配置する方法を示します。

（注） このタスクは、2D または 3D マップで実行できます。

手順

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

ステップ 2 フロアを 左側の階層ツリーから、以下を選択します します。

ステップ 3 マップツールバーで、次のいずれかのタスクを実行します。

- **[2D]** > **[Add/Edit]**の順にクリックします。
- **[3D]** > **[Edit/Clone]**の順にクリックします。

ステップ 4 マップで、センサーを新しい位置にドラッグアンドドロップします。

ステップ 5 マップツールバーで [Save] をクリックします。

マップでのセンサーの削除

この手順では、センサーをフロアマップから削除する方法を示します。

手順

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

ステップ 2 フロアを 左側の階層ツリーから、以下を選択します します。

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

ステップ 4 センサーを削除するには、次のタスクを実行します。

a) センサーをクリックします。複数のセンサーを選択する場合は、最初のセンサーをクリックし、Shift キーを押しながら残りのセンサーをクリックします。

b) [Edit] ペインで、[Remove] をクリックします。

ステップ 5 マップツールバーで [Save] をクリックします。

カバレッジエリアの追加、編集、削除

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

カバレッジエリアの詳細については、「2D フロアマップのデバイスとオーバーレイオブジェクトの （302 ページ）」[英語] を参照してください。

手順

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

ステップ 2 フロアを 左側の階層ツリーから、以下を選択します します。

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

ステップ 4 カバレッジエリアを追加するには、次の手順を実行します。

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

b) [Add Coverage] をクリックします。

c) マップをクリックしてポイントを作成し、描画ツールを開始します。

d) 引き続きポイントを作成して、カバレッジエリアの形状を定義します。

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

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

ステップ 5 カバレッジエリアを編集するには、次の手順を実行します。

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

b) カバレッジエリアの形状を定義し直すには、ポイントをクリックしてドラッグします。
c) カバレッジエリアの名前を編集するには、カバレッジエリアを右クリックして [**Edit**] を選択します。

ステップ 6 カバレッジエリアを削除するには、次の手順を実行します。

a) マップツールバーで、**[Add/Edit]** > **[Coverage Areas]** をクリックします。
b) カバレッジエリアを右クリックし、[**Remove**] を選択します。

ステップ 7 マップツールバーで [Save] をクリックします。

吹き抜けの追加、編集、コピー、および削除

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

吹き抜けの詳細については、「2D フロアマップのデバイスとオーバーレイオブジェクトの（302 ページ）」[英語] を参照してください。

手順

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

ステップ 2 フロアを 左側の階層ツリーから、以下を選択します します。

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

ステップ 4 吹き抜けを追加するには、次の手順を実行します。

a) マップの左ペインで、[Opening] をクリックします。
b) マップをクリックしてポイントを作成し、描画ツールを開始します。
c) 引き続きポイントを作成して、吹き抜けの形状を定義します。

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

d) ダブルクリックして描画ツールを終了し、形状を確定します。

ステップ 5 吹き抜けを編集するには、次の手順を実行します。

a) マップツールバーで、**[Add/Edit]** > **[Openings]** をクリックします。
b) 吹き抜けの形状を定義し直すには、ポイントをクリックしてドラッグします。
c) 吹き抜けを移動するには、網掛けされたエリア内をクリックします。次に、吹き抜けを配置する場所にドラッグアンドドロップします。

ステップ 6 吹き抜けを別のフロアにコピーするには、次の手順を実行します。

a) マップツールバーで、**[Add/Edit]** > **[Openings]** をクリックします。
b) 吹き抜けを右クリックし、[**Copy to other floors**] を選択します。
c) ダイアログボックスで、関連フロアの横にあるチェックボックスをオンにします。
d) [Copy] をクリックします。
e) [Close] をクリックします。

ステップ 7 吹き抜けを削除するには、次の手順を実行します。

a) マップツールバーで、**[Add/Edit]** > **[Openings]** をクリックします。
b) 吹き抜けを右クリックし、[**Remove**] を選択します。

ステップ 8 マップツールバーで [Save] をクリックします。

ロケーションリージョンの追加、編集、および削除

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

包含リージョンの追加、編集、および削除

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

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

包含リージョンの詳細については、2D フロアマップのデバイスとオーバーレイオブジェクトの （302 ページ）を参照してください。

手順

ステップ 1 メインメニューから次を選択します。**[Design]** > **[Network Hierarchy]**。
ステップ 2 フロアを 左側の階層ツリーから、以下を選択します します。
ステップ 3 マップツールバーで、**[2D]** > **[Add/Edit]** > **[Overlays]** > **[Location Regions]** をクリックします。
ステップ 4 マップの左側のペインで、[Inclusion] アイコンをクリックします。
ステップ 5 包含リージョンを作成するには、描画ツールを使用します。

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

d) 形状を完成させるには、マップをダブルクリックします。

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

e) 描画ツールを終了するには、マップをもう一度ダブルクリックします。

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

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

ステップ 8 マップツールバーで [Save] をクリックします。

除外リージョンの追加、編集、および削除

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

- 除外リージョンは多角形領域で表され、最低 3 点で構成される必要があります。
- 除外リージョンは包含リージョンの境界内で定義されます。
- フロアマップ上で除外リージョンを複数定義できます。

除外リージョンの詳細については、2D フロアマップのデバイスとオーバーレイオブジェクトの （302 ページ）を参照してください。

手順

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

ステップ 2 フロアを 左側の階層ツリーから、以下を選択します します。

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

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

ステップ 5 除外リージョンを作成するには、描画ツールを使用します。

a) マップをクリックして、除外リージョンを開始するポイントを作成します。

b) カーソルを次のポイントに移動して、もう一度クリックします。

c) 引き続きポイントを作成して、除外リージョンの形状を定義します。

d) 形状を完成させるには、マップをダブルクリックします。

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

e) 描画ツールを終了するには、マップをもう一度ダブルクリックします。

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

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

ステップ 8 マップツールバーで [Save] をクリックします。

壁の追加、編集、および削除

この手順では、フロアマップで壁を追加、編集、および削除する方法を示します。

壁がRF信号の減衰とヒートマップの計算に与える影響については、2Dフロアマップのデバイスとオーバーレイオブジェクトの （302 ページ）を参照してください。

手順

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

ステップ 2 フロアを 左側の階層ツリーから、以下を選択します します。

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

ステップ 4 壁を追加するには、次の手順を実行します。

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

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

b) マップをクリックして、壁の開始ポイントを作成します。

c) 壁を終了する次のポイント、またはコーナーを作成する次のポイントにカーソルを移動して、もう一度クリックします。

d) 引き続きポイントを作成して、壁の形状を定義します。

e) 壁を終了するには、マップをダブルクリックします。

または、左側のペインで壁のタイプをクリックします。

f) 描画ツールを終了するには、マップをもう一度ダブルクリックします。

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

a) 変更する壁をクリックします。

[Wall Type] ダイアログボックスが表示されます。

b) [**Wall Type**] ドロップダウンリストから、壁のタイプを選択します。

c) 新しい壁タイプに適したその他のパラメータを設定します。

d) [Update] をクリックします。

ステップ 6 壁を移動するには、次の手順を実行します。

a) 移動する壁にカーソルを合わせます。

壁が黒くなります。これは選択されたことを意味します。

b) 壁をクリックし、新しい場所にドラッグアンドドロップします。

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

ステップ 8 マップツールバーで [Save] をクリックします。

シェルフユニットの追加、コピー、編集、および削除

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

シェルフユニットの詳細については、「2D フロアマップのデバイスとオーバーレイオブジェクトの （302 ページ）」[英語] を参照してください。

手順

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

ステップ 2 フロアを 左側の階層ツリーから、以下を選択します します。

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

ステップ 4 シェルフユニットを追加するには、次の手順を実行します。

a) マップの左ペインで、追加するシェルフタイプをクリックします。

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

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

c) [Add Shellving] をクリックします。

シェルフユニットがマップに表示されます。

d) シェルフユニットをマップ上の場所にドラッグアンドドロップします。

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

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

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

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

ステップ 8 マップツールバーで [Save] をクリックします。

マーカーの追加、編集、および削除

この手順では、マーカーを追加、編集、および削除する方法を示します。

手順

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

ステップ 2 フロアを 左側の階層ツリーから、以下を選択します します。

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

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

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

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

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

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

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

ステップ 10 マップツールバーで [Save] をクリックします。

GPS マーカーの追加、編集、および削除

この手順では、GPS マーカーを追加、編集、および削除する方法を示します。GPS マーカーの詳細については、「2D フロアマップのデバイスとオーバーレイオブジェクトの（302 ページ）」[英語] を参照してください。

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

手順

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

ステップ 2 フロアを 左側の階層ツリーから、以下を選択します します。

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

ステップ 4 GPS マーカーを追加するには、次の手順を実行します。

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

b) マップ上で、GPS マーカーを配置する場所をクリックします。

GPS マーカーは、外壁の内側、通常は建物の角に配置する必要があります。

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

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

d) [Add] をクリックします。

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

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

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

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

ステップ 8 マップツールバーで [Save] をクリックします。

位置合わせポイントの追加、編集、および削除

この手順では、位置合わせポイントを追加、編集、および削除する方法を示します。位置合わせポイントの詳細については、「2D フロアマップのデバイスとオーバーレイオブジェクトの（302 ページ）」[英語] を参照してください。

手順

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

ステップ 2 フロアを 左側の階層ツリーから、以下を選択します します。

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

ステップ 4 位置合わせポイントを追加するには、次の手順を実行します。

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

b) マップ上で、位置合わせポイントを配置する場所をクリックします。

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

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

b) 名前を変更して、[Update] をクリックします。

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

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

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

ステップ 8 マップツールバーで [Save] をクリックします。

2D ワイヤレスヒートマップの表示

次の手順を使用して、2D ワイヤレスヒートマップ、およびワイヤレスネットワークに関する情報を表示します。

手順

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

ステップ 2 フロアを 左側の階層ツリーから、以下を選択します します。

ステップ 3 マップツールバーで、[2D] をクリックします。

ワイヤレス 2D マップが開きます。

ステップ 4 デバイスに関する具体的な詳細を表示するには、デバイスタイプに基づいて次のリストを使用します。

- [APs]：AP アイコンは、無線の数、その周波数と正常性、デバイスの全体的な正常性スコア、および AP の名前とモードを示します。AP アイコンの解釈については「AP アイコンと計画済み AP アイコンについて （345 ページ）」を参照してください。

  デバイスの詳細を表示するには、AP アイコンの上にカーソルを置きます。AP Rx ネイバー、クライアント、干渉源、正常性スコア、ライセンス非適合などの情報が表示されます。

  AP の詳細については、ダイアログボックスで [Device 360] リンクをクリックします。

  （注） [Device 360] を使用するには、「Assurance - Base」パッケージが必要です。

- [Mesh APs]：デバイスの詳細を表示するには、メッシュ AP アイコンの上にカーソルを置きます。メッシュ、バックホール、アクセスデータなどの情報が表示されます。
- [Clients]：関連付けられた AP へのリンクを含むクライアント情報を表示するには、カーソルをクライアントの上に置くか、クライアントをクリックします。クライアントの詳細については、ダイアログボックスで [Client 360] リンクをクリックします。
- [Sensors]：センサーのステータスとテスト結果を表示するには、センサーアイコンをクリックします。
- [Switches and Switch Stacks]：スイッチスタックのメンバースイッチを表示するには、スイッチスタックアイコンの横にある矢印をクリックします。スイッチとそれに関連付けられた AP 間の接続を表示するには、カーソルをスイッチまたはスイッチスタックアイコンの上に置きます。マップには、スイッチからそれに関連付けられた AP への接続を示す線が表示されます。スイッチと AP の関連付けを色で識別することもできます。1 つの特定のスイッチに接続されている AP には、スイッチアイコンのカラーコードと一致するラベルが付いています。

Catalyst Center では、Cisco Discovery Protocol（CDP）を使用して、管理対象 AP に接続されているアンマネージドスイッチを検出して表示できます。アンマネージドスイッチは、アンマネージド（）を表す「U」が付いた一般的なスイッチアイコンとして示されます。

デバイスの詳細を表示するには、スイッチまたはスイッチスタックのアイコンをクリックします。スライドインペインが開き、デバイスの詳細とヒートマップ表示のオプションが表示されます。[Select Heatmap] の下で、次のいずれかのオプションボタンをクリックできます。

- [All visible switches]：表示されているマップ領域内のすべてのスイッチのヒートマップを計算して表示します。
- [This switch]：選択したスイッチのみのヒートマップを計算して表示します。
- [Rest of visible switches]：選択したスイッチを除く、すべての可視スイッチのヒートマップを計算して表示します。
- [None]：ヒートマップ計算およびヒートマップ表示にスイッチを含めません。

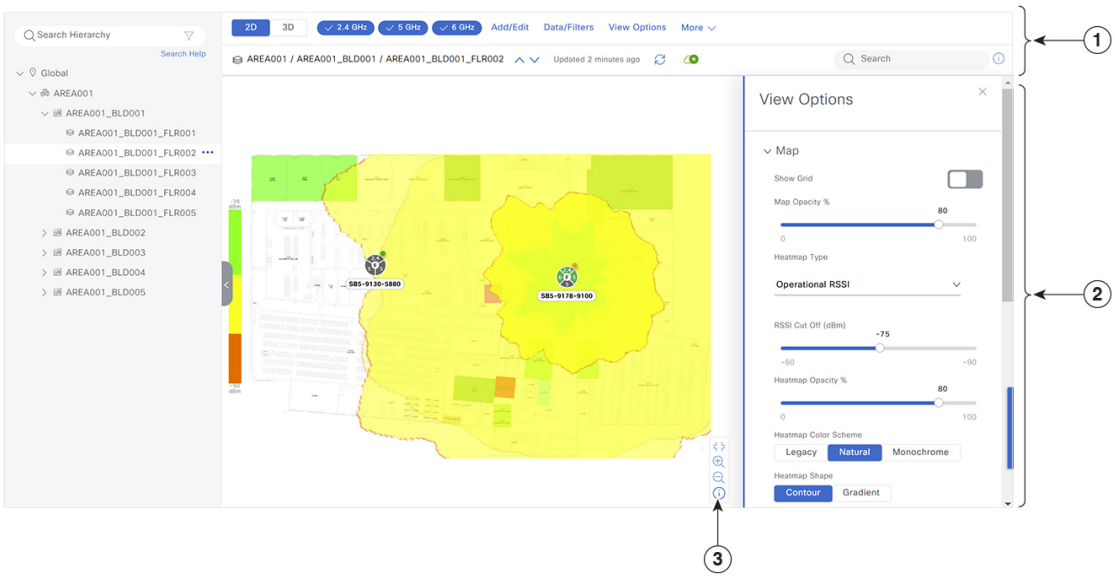
ステップ 5 リンクに関する情報を表示するには、リンクをクリックします。

リンクのタイプに応じて、リンクの状態やその他の統計などの情報が表示されます。

メッシュリンクの場合、2 つのメッシュ AP 間のリンクテストを実行できます。

ステップ 6 2D ワイアレスヒートマップに表示されるツールとオプションを使用して、ワイヤレスネットワークに関するインサイトを取得します。

図 *11* : ツールとオプションを示す *2D* ワイヤレスマップ

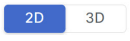


引き出し線	説明
1	**マップツールバー**：マップの上で、ツールバーオプションを使用して、ヒートマップに表示される内容を制御します。詳細については、2D マップツールバー （337 ページ）を参照してください。
2	[View Options] スライドインペイン：スライドインペインで、表示オプションを使用してヒートマップ表示をカスタマイズします。詳細については、2D マップビューオプション （340 ページ）を参照してください。
3	**ナビゲーションコントロール**：マップの右下隅から、マップナビゲーションコントロールを使用してヒートマップ表示を管理します。詳細については、「2D マップナビゲーション コントロール （344 ページ）」を参照してください。

2D マップツールバー

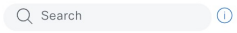
2Dマップにアクセスするには、左上隅で、メニューアイコンをクリックして次を選択します。**[Design]** > **[Network Hierarchy]**の順に選択します。フロアを 左側の階層ツリーから、以下を選択します し、マップツールバーで**[2D]**をクリックします。

マップツールバーは2つのバーで構成され、マップの上にあります。マップツールバーを使用して、ヒートマップの表示を制御し、デバイスやオーバーレイオブジェクトの追加や編集などのアクションを実行します。

アイテム	説明
	[2D] をクリックしてワイヤレスマップを 2D で表示するか、[3D] をクリックして 3D で表示します。
	Wi-Fi バンドボタンをクリックして、対応する Wi-Fi 帯域フィルタを選択します。複数の Wi-Fi 帯域を選択できます。

アイテム	説明
Add/Edit	このボタンをクリックして、次のデバイスおよびオーバーレイオブジェクトを追加、編集、および削除します。 • **[デバイス （Devices）]** • [Access points]：詳細については、フロアマップでの AP の取り扱い （304 ページ）を参照してください。 • [Sensor]：詳細については、マップへのセンサーの追加 （325 ページ）を参照してください。 • **オーバーレイオブジェクト** • [Coverage areas]：詳細については、カバレッジエリアの追加、編集、削除 （327 ページ）を参照してください。 • [Openings]：詳細については、吹き抜けの追加、編集、コピー、および削除 （328 ページ）を参照してください。 • [Location regions]：詳細については、ロケーションリージョンの追加、編集、および削除 （329 ページ）を参照してください。 • [Walls]：詳細については、壁の追加、編集、および削除 （331 ページ）を参照してください。 • [Shelving Units]：詳細については、シェルフユニットの追加、コピー、編集、および削除 （332 ページ）を参照してください。 • [Markers]：詳細については、マーカーの追加、編集、および削除 （333 ページ）を参照してください。 • [GPS Markers]：詳細については、GPS マーカーの追加、編集、および削除 （333 ページ）を参照してください。 • [Align points]：詳細については、位置合わせポイントの追加、編集、および削除 （334 ページ）を参照してください。
[Data/Filters]	[Data/Filters] をクリックして、デバイスタイプリストを表示する [Data/Filters] スライドインペイン を開きます。ワイヤレスマップに表示されるデバイスデータを表示およびフィルタ処理するには、デバイスタイプを選択します。詳細については、フロアのデバイスデータのフィルタ処理 （349 ページ）を参照してください。
View Options	[View Options] をクリックして、マップ、デバイス、およびオーバーレイオブジェクトを制御するためのオプションを含む [View Options] スライドインペインを開きます。詳細については、2D マップビューオプション （340 ページ）を参照してください。

アイテム	説明
More	[More] にカーソルを合わせ、ドロップダウンリストから使用可能なオプションを選択します。 • [Recompute]：ヒートマップを再計算します。 • [Export]：フロアマップを PDF または CSV ファイル形式でエクスポートします。 • [Edit Floor]：名前などのフロアの詳細情報を変更します。 • [Set Scale]：地図上に既知の測定値を表示して、地図の縮尺を変更します。 1. マップをクリックして、測定の開始点を指定します。 2. 地図をもう一度クリックして、測定の終点を指定します。 3. [New line length (ft)] フィールドに、測定位置の長さを入力します。 4. [OK] をクリックします。 フロアマップの寸法は、新しい測定値に基づいて再計算されます。 • [Measure Distance]：フロアマップ上の距離を測定します。マップをクリックして開始点を指定します。マップをもう一度クリックして、終点を指定します。測定距離が表示されます。 • [CMX/Cisco Spaces Sync History]：Cisco Connected Mobile Experiences（CMX）と Cisco Spaces がデータを同期した時刻を示すログが表示されます。ログエントリには、要求の受信時刻、開始時刻と終了時刻、ステータス、および失敗メッセージ（操作が失敗した場合）が含まれます。 • [Floor Import History]：マップアーカイブファイルのインポートに関するフロアインポート履歴ログが表示されます。ログには、正常にインポートされた AP、インポートに失敗した AP、計画済み AP、およびオーバーレイオブジェクトの詳細が表示されます。
Area or Site / Building / Floor	[Full Hierarchy Path]：フロアの完全なナビゲーションパスを表示します。関連する建物、エリアまたはサイトも含まれます。下矢印をクリックすると、別のフロアに移動します。
	[Refresh]：このアイコンをクリックすると、デバイスおよびマップデータが更新されます。アイコンの左側には、最後の更新のタイムスタンプが表示されます。
	[Cisco Spaces Connector]：このアイコンをクリックして、Cisco Spaces コネクタに関する IP アドレス、ステータス、バージョンなどの情報を表示します。
	[Map Notification]：このアイコンにカーソルを合わせて、未配置の AP または計画済みの AP の数などのマップ情報とマップに適用されるフィルタを表示します。フィルタを削除するには、[Click to clear] をクリックします。

アイテム	説明
	[Error]：エラー通知（AP ライセンスの非適合など）を表示します。対応するハイパーリンクをクリックすると、詳細が表示されます。
	[Search]：AP、センサー、クライアントなどの特定のフロアマップ要素を検索するには、[Search] フィールドを使用します。検索結果は、[Search] フィールドの下にある スライドインペイン に一覧表示されます。 リスト内の要素にカーソルを合わせると、インジケータがマップ上の要素を指します。要素が視野角の外にある場合、インジケータは赤い破線で表示されます。マップの向きを変えて要素を確認します。

2D マップビューオプション

2D マップにアクセスするには、左上隅で メニューアイコンをクリックして次を選択します。**[Design]** > **[Network Hierarchy]** の順に選択します。フロアを 左側の階層ツリーから、以下を選択します し、マップツールバーで **[2D]** > **[View Options]** をクリックします。

[View Options] スライドインペインが開きます。カテゴリを展開して設定を表示します。

- [Map]：さまざまなフロアマップおよびヒートマップ設定が含まれています。

アイテム	説明
Show Grid	フロアマップのグリッドを有効または無効にするには、このトグルボタンをクリックします。このグリッドにより、フロアマップの寸法を把握できます。
Map Opacity %	フロアマップの不透明度または透明度をカスタマイズするには、このスライダを使用します。

アイテム	説明
ヒートマップ タイプ	ヒートマップは、変数から取得した値をマップに色として表した、無線周波数（RF）ワイヤレスデータのグラフィック表示を提供します。RSSI ヒートマップは、フロアの RSSI 予測モデル、アンテナタイプ、およびその向きに基づいて計算されます。 2D ヒートマップは、2.4 GHz では 18 dB、5 GHz では 15 dB、6 GHz では 5dB の固定送信電力を使用します。 3D ヒートマップは、稼働中の AP のリアルタイム送信電力と、計画 AP の 11 dB を使用します。 ドロップダウンリストを使用してヒートマップタイプを選択します。 • [Operational RSSI]：稼働中 AP のワイヤレス信号の強度を特定するカバレッジヒートマップ。 • [Planned RSSI]：計画済み AP についてフロア上で設定される可能性があるカバレッジを示す架空のヒートマップ。 • [Operational + Planned (3D-only)]：（レガシー ヒートマップ ジェネレータが有効になっている場合にのみ表示されます）。2D マップでは、稼働中の AP のみがヒートマップの計算に使用されます。ヒートマップの計算で稼働中の AP と計画済みの AP を使用するには、3D 計算ヒートマップジェネレータを有効にするか、3D マップに移動します。詳細については、このトピックの [Disable 3D-Computed Heatmap] フィールドを参照してください。 • [Operational + Planned]：（3D 計算ヒートマップジェネレータが有効になっている場合にのみ表示されます）。稼働中の AP と計画済み AP の両方を使用して作成されたカバレッジヒートマップ。 • [Client Density]：関連付けられたクライアントの密度。 • [IDS]：ワイヤレスクライアントに提供されるモニターモード AP カバレッジをフロアマップ上に示すヒートマップ。
RSSI Cut off (dBm)	ヒートマップに表示される RSSI 値のしきい値を設定するには、このスライダを使用します。しきい値を満たさない RSSI 値は表示されません。
Heatmap Opacity %	ヒートマップの不透明度または透明度をカスタマイズするには、このスライダを使用します。
Heatmap Color Scheme	ヒートマップの電力レベルの配色をカスタマイズできます。オプションは、[Legacy]、[Natural]、および [Monochrome] です。[Monochrome] は、[Heatmap Shape] の [Contour] オプションのみをサポートしていることに注意してください。
[Heatmap Shape]	ヒートマップの電力レベルの色の進行をカスタマイズします。オプションは、[Contour] と [Gradient] です。

• [Access Points]：フロアマップ上の AP のアイコンを有効または無効にするには、このトグルボタンをクリックします。

このカテゴリを展開して、各 AP に表示するラベルのタイプを設定します。[**Display Label**] ドロップダウンリストから最大 4 つのラベルタイプを選択します。

AP に関するその他の詳細を表示するには、2D ワイヤレスヒートマップの表示 （335 ページ）を参照してください。

- [Planned Access Points]：フロアマップ上の計画 AP のアイコンの表示を有効または無効にするには、このトグルボタンをクリックします。

  このカテゴリを展開して、各計画 AP に表示するラベルのタイプを設定します。[**Display Label**] ドロップダウンリストから最大 2 つのラベルタイプを選択します。

- [Switches]：フロアマップ上のスイッチまたはスイッチスタックのアイコンの表示を有効または無効にするには、このトグルボタンをクリックします。Catalyst Center では、Cisco Discovery Protocol（CDP）を使用して、管理対象 AP に接続されているアンマネージドスイッチを検出して表示できます。アンマネージドスイッチは、アンマネージドを表す「U」が付いた一般的なスイッチアイコンとして示されます。

  このカテゴリを展開して、スイッチ名、MAC アドレス、または AP カウントのラベルを表示します。（アンマネージドスイッチの場合、スイッチ名と AP カウントのみ表示されます）。[Display Label] ドロップダウンリストからラベルタイプを選択します。

  スイッチに関するその他の詳細を表示するには、2D ワイヤレスヒートマップの表示 （335 ページ）を参照してください。

- [Sensors]：フロアマップ上のセンサーのアイコンの表示を有効または無効にするには、このトグルボタンをクリックします。

  このカテゴリを展開して、センサー名、MAC アドレス、または AP カウントのラベルを表示します。[Display Label] ドロップダウンリストからラベルタイプを選択します。

  センサーに関するその他の詳細を表示するには、2D ワイヤレスヒートマップの表示 （335 ページ）を参照してください。

- [Mesh]：フロアマップ上のメッシュ AP の表示を有効または無効にするには、このトグルボタンをクリックします。

  このカテゴリを展開して、メッシュ AP とルート AP のリンク関係の表示方法を制御するオプションを設定します。

  - [Link Label]：リンクラベルを無効にするには、[None] オプションボタンをクリックします。リンクの信号対雑音比のラベルを表示するには、[Link SNR] オプションボタンをクリックします。パケットエラーレートのラベルを表示するには、[Packet Error Rate] オプションボタンをクリックします。リンクのラベル設定は、ただちにマップ上に反映されます。

  - [Link Color]：リンクの色を無効にするには、[None] オプションボタンをクリックします。リンクの信号対雑音比を色で表示するには、[Link SNR] オプションボタンをクリックします。パケットエラーレートを色で表示するには、[Packet Error Rate] オプションボタンをクリックします。

リンクの色の設定は、ただちにマップ上に反映されます。色の定義については、次の表を参照してください。

リンクの色	リンク信号対雑音比（SNR）	パケットエラー率（PER）
●	SNR が 25 dB を超えている（高い値）ことを表します。	PER が 1% 以下であることを表します。
●	SNR が 20 ～ 25 dB（許容値）であることを表します。	PER が 1% より大きく 10% 未満であることを表します。
●	SNR が 20 dB を下回っている（低い値）ことを表します。	PER が 10% より大きいことを表します。

- [Mesh Parent-Child Hierarchical View]：表示するメッシュ AP を選択します。このドロップダウンリストから、[Select Only Root APs]、[Select up to 1st hops]、[Select up to 2nd hops]、[Select up to 3rd hops]、[Select up to 4th hops]、または [Select All] を選択します。

- [Overlay Objects]：このカテゴリを展開し、オーバーレイオブジェクトのいずれかをクリックしてフロアマップ上のオーバーレイオブジェクトを有効または無効にします。

- [Clients]：フロアマップ上のクライアントのアイコンの表示を有効または無効にするには、このトグルボタンをクリックします。

  このカテゴリを展開して、クライアント名、MAC アドレス、または AP カウントのラベルを表示します。[Display Label] ドロップダウンリストからラベルタイプを選択します。

  近接したクライアントのグループ化を有効または無効にするには、[Show Client Clusters] トグルボタンをクリックします。

- [Interferers]：フロアマップ上のクライアントのアイコンの表示を有効または無効にするには、このトグルボタンをクリックします。

  このカテゴリを展開して、干渉源からの影響ゾーンの表示を有効または無効にします。[Show Zone of Impact] トグルボタンをクリックします。

- [**Map Properties**]：このカテゴリを展開して、マップで次の設定を行います。

  - [Auto Refresh]：このドロップダウンリストから、マップ表示を更新する時間間隔を選択します。

  - [Heatmap Walls Limit]：（3D で計算されたヒートマップジェネレータでのみ使用可能）。ヒートマップの計算に使用する壁の数を入力します。計算に含まれる壁が多いほど、ヒートマップの計算に時間がかかります。デフォルトの推奨制限数は 3,000 です。

  - [Mesh SNR Colors] および [Mesh PER Colors]：（メッシュデバイスが存在する場合にのみ使用可能）。しきい値の範囲と対応する色を入力します。

- [**Global Map Properties**]：このカテゴリを展開して、すべてのワイヤレスマップに対して次の設定を行います。

- [Units of Measure]：ドロップダウンリストから、[Feet]（ヤードポンド法）または [Meters]（メートル法）を選択します。
- [Disable 3D-Computed Heatmap]：デフォルトの 3D 計算ヒートマップジェネレータを無効にして、レガシー ヒートマップ ジェネレータを有効にするには、このトグルボタンをクリックします。レガシー ヒートマップ ジェネレータを使用した計算とレンダリングは、3D 計算ヒートマップほど高速ではなく、ヒートマップの計算に含める壁の数に制限を設定できないことに注意してください。（[Heatmap Walls Limit] フィールドが表示から削除されます）。最適化後のレガシー ヒートマップ ジェネレータを使用した壁の最大数は 300 です。フロアマップに 300 以上の壁が含まれている場合は、Catalyst Center からアラートが表示され、（壁の長さにその減衰を掛けた数値に基づいて）最適な 300 の壁が保持されます。

  3D 計算ヒートマップジェネレータには、レガシー ヒートマップ ジェネレータに比べていくつかの利点があります。特殊なグラフィック処理ユニット（GPU）を使用するため、レガシー ヒートマップ ジェネレータよりも大幅に高速にヒートマップを生成できます。さらに、ヒートマップの計算に含まれる壁の数に制限を設定できるため、処理速度の向上にも役立ちます。

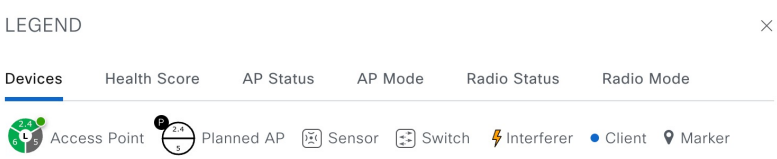
2D マップ ナビゲーション コントロール

2D マップにアクセスするには、左上隅で、メニューアイコンをクリックして次を選択します。**[Design]** > **[Network Hierarchy]** の順に選択します。フロアを 左側の階層ツリーから、以下を選択します し、マップツールバーで [2D] をクリックします。

2D マップ ナビゲーション コントロールは、マップの右下にあります。マップの詳細については、2D ワイヤレスヒートマップの表示 （335 ページ）を参照してください。

次の機能には、マップ ナビゲーション コントロールを使用します。

マップ ナビゲーション コントロール	説明
	[Select by rectangle]：編集モードでのみ表示されます。このアイコンを使用して、マップ上の連続したエリアにある複数の AP を選択します。最初にこのアイコンをクリックし、次にマップのエリアをクリックして、強調表示された長方形をドラッグします。長方形内で強調表示されているすべての AP が選択されています。
	[Alert]：このアイコンは、[Do not show this alert anymore] をクリックして、最初にエラーを解決せずにバナー通知を削除することを選択すると表示されます。エラーが解決されている場合、このアラートアイコンは表示されません。
	**デフォルトマップビュー**：クリックすると、マップビューがデフォルトにリセットされます。

マップ ナビゲーション コントロール	説明
	**ズームイン/ズームアウト**：ズームインおよびズームアウトのアイコンをクリックして、マップのサイズを拡大および縮小します。マウスホイールを使用して拡大/縮小することもできます。
	[Map Legend]：このアイコンをクリックすると、デバイスタイプ、平均正常性スコア、AP ステータスなど、マップのアイコンを説明するマップ凡例が表示されます。AP アイコンと計画済み AP アイコンの詳細については、「AP アイコンと計画済み AP アイコンについて（345 ページ）」を参照してください。 

AP アイコンと計画済み AP アイコンについて

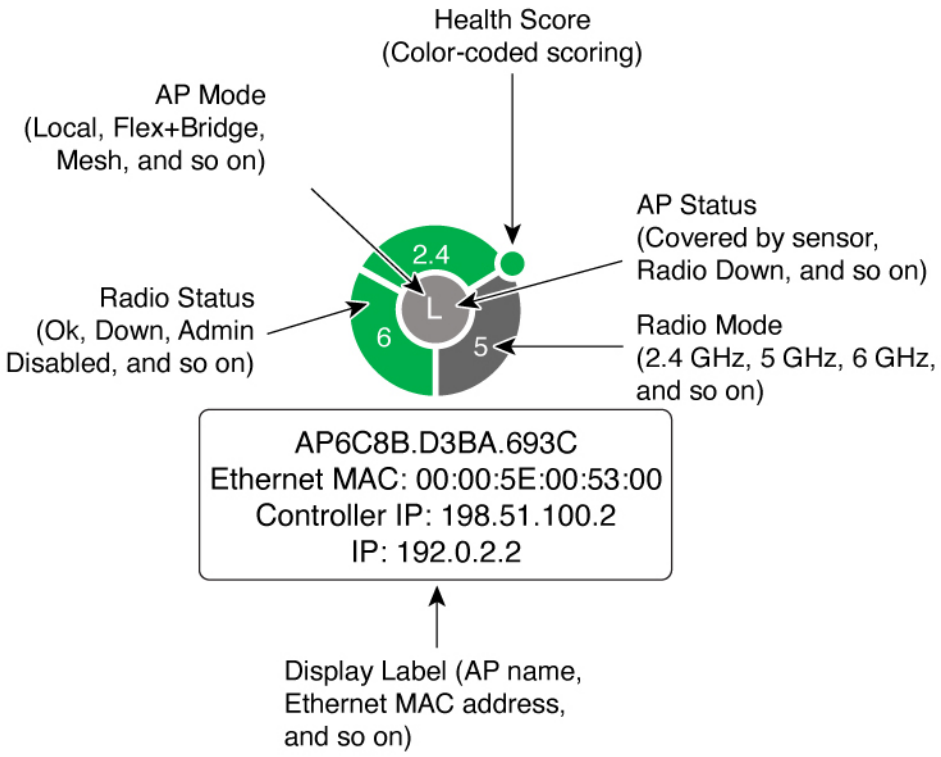
AP アイコン

AP アイコンは、ネットワーク内の AP の設定と正常性に関する情報を提供します。円形の AP アイコンは無線帯域に分割され、無線のステータスを示すために色分けされています。中央の円には、AP モードの文字が表示されます。中央の円の背景色または円上の「X」は、AP のステータスを示します。AP アイコンの右上隅にある色分けされた小さな円には、正常性スコアが表示されます。

次の詳細については、2D フロアマップのマップ凡例を参照してください。

- AP モードに使用される文字、
- 無線モード、および
- 無線ステータス、AP ステータス、および正常性スコアの色分け

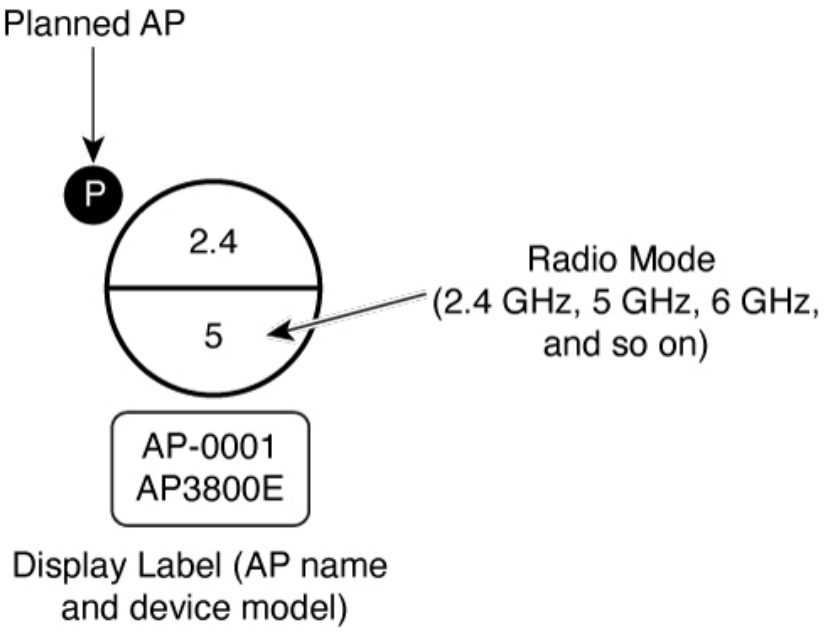
次の図に、AP アイコンのすべての要素を示します。



計画済み AP アイコン

計画済み AP アイコンには、ネットワーク内の計画済み AP の設定と正常性に関する情報が表示されます。円形の計画済み AP アイコンは無線帯域に分割され、左上隅に「P」が表示されます。無線モードの詳細については、2D フロアマップのマップ凡例を参照してください。

次の図に、計画済み AP アイコンのすべての要素を示します。



管理対象 AP に接続されたアンマネージドスイッチの表示

Catalyst Center は、ネットワーク内のアンマネージドスイッチと、それらが接続されている管理対象 AP を検出できます。アンマネージドスイッチとそれらの AP への接続は、2D フロアマップに表示できます。この機能は、Catalyst Center を使用して管理したくないものの管理対象 AP との関連で表示したいスイッチがある場合に役立ちます。

（注） この機能は、Cisco AireOS ワイヤレスコントローラではサポートされていません。

始める前に

- Catalyst Center プラットフォーム をインストールおよび設定していること。詳細については、*Cisco Catalyst Center Platform User Guide*を参照してください。
- Cisco Catalyst Assurance をイネーブルにします。詳細については、*Cisco Catalyst Assurance User Guide*を参照してください。
- ワイヤレスコントローラ を Catalyst Center インベントリに追加し、サイトに割り当てて、デバイスの可制御性設定が ワイヤレスコントローラ にプッシュされていることを確認します。詳細については、『*Cisco Catalyst Center Administrator Guide*』の「デバイスの可制御性」を参照してください。

手順

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

ステップ 2 フロアを 左側の階層ツリーから、以下を選択します します。

ステップ 3 マップツールバーで、[2D] をクリックします。

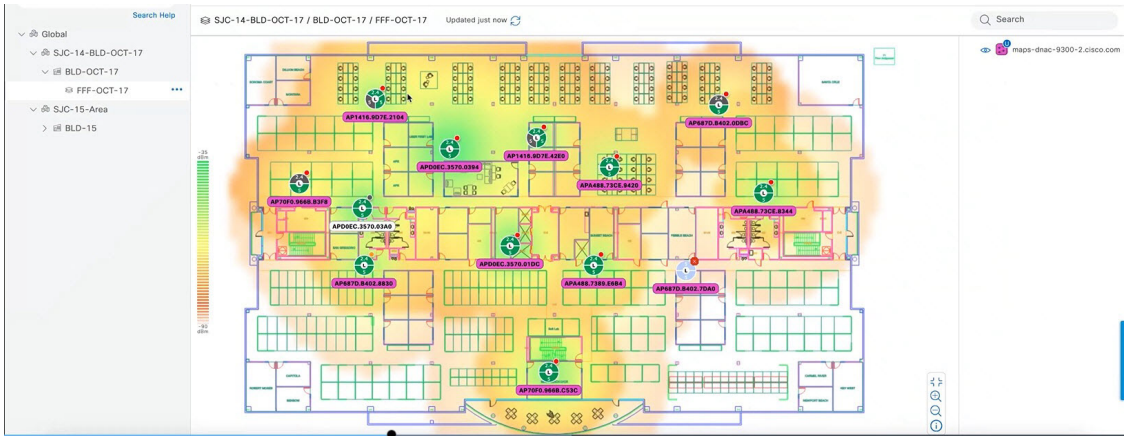
ワイヤレス 2D マップが開き、追加された AP が表示されます。

ステップ 4 AP をフロアマップに追加します。詳細については、マップへの AP の追加 （306 ページ）を参照してください。

（注） AP がローカル、ブリッジ、または FlexConnect モードの場合は、その AP をアンマネージドスイッチに接続し、ワイヤレスコントローラに参加させます。

Catalyst Center で表示が更新されると、アンマネージドスイッチが右側のペインに一覧表示されます。

アンマネージドスイッチは、アンマネージド（）を表す「U」が付いた一般的なスイッチアイコンとして示されます。



ステップ 5 （任意）アンマネージドスイッチにカーソルを合わせると、スイッチとそのスイッチが接続されている AP の間のリンクが表示されます。

ステップ 6 （任意）アンマネージドスイッチをクリックすると、スライドインペインにスイッチに関する追加の詳細が表示されます。マネージドスイッチで利用可能なすべての情報は、MAC アドレスとその到達可能性ステータスを除き、アンマネージドスイッチでも利用できます。

2D マップで使用可能な要素、ツール、およびオプションの詳細については、2D ワイヤレスヒートマップの表示 （335 ページ）を参照してください。

フロアのデバイスデータのフィルタ処理

2D ワイヤレスマップの場合、APやセンサーなどのネットワークデバイスにさまざまなフィルタを適用できます。フィルタ条件に基づいて、検索結果がテーブルに表示されます。デバイスデータのフィルタ処理は、多数のデバイスがあるフロアで特定のデバイスを見つけるのに役立ちます。

手順

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

ステップ 2 フロアを 左側の階層ツリーから、以下を選択します します。

ステップ 3 マップツールバーで、[2D] をクリックします。

ステップ 4 マップツールバーで、[Data/Filters] をクリックします。

ステップ 5 [Data/Filters] スライドインペインで、フィルタを適用するデバイスタイプをクリックします。

ステップ 6 ドロップダウンリストを使用してパラメータを選択することにより、フィルタルールを定義します。

ステップ 7 フィルタルールをさらに追加するには、スライドインペインの上部近くにある [+] アイコンをクリックします。

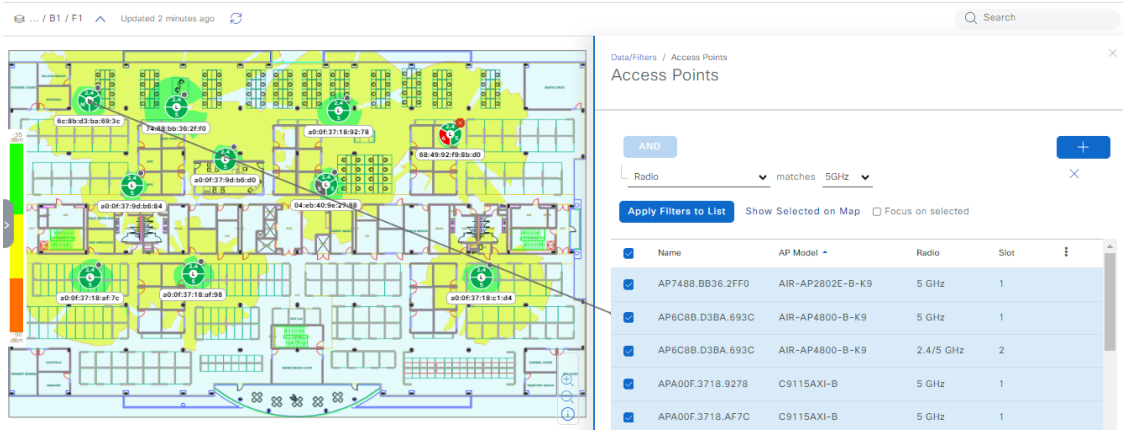
ステップ 8 テーブルに表示される列をカスタマイズするには、次の手順を実行します。

1. テーブルの右上隅にある縦に並んだ 3 つのドットをクリックします。
2. 列を表示するには、列名の横にあるチェックボックスをオンにします。
3. 列を非表示にするには、列名の横にあるチェックボックスをオフにします。
4. [Apply] をクリックします。

ステップ 9 完了したら、次のいずれかのタスクを実行できます。

- テーブルにフィルタの結果を表示するには、[Apply Filters to List] をクリックします。
- フィルタの結果をマップに表示するには、[Show Selected on Map] をクリックします。
- デバイスのマップ上の位置を確認するには、テーブル内のデバイスにカーソルを合わせます。デバイスからマップ上のその位置まで線が表示されます。

図 *12* : フィルタ結果によるデバイスの位置の特定



ステップ 10 適用されたフィルタを削除するには、下部にあるマップツールバーで、通知アイコンの上にカーソルを合わせて、[Click to clear] をクリックします。

ステップ 11 [Data/Filters] スライドインペインに戻るには、左上隅のナビゲーションパスから [Data/Filters] をクリックします。

ステップ 12 スライドインペインを閉じてフィルタを保存するには、[x] をクリックします。

フロアマップでのワイヤレス干渉源の特定

この機能は 2D マップ機能のものです。

Catalyst Center は、干渉を検出し、フロアマップ上の特定の帯域に対する干渉源を無効にすることができます。2.4 GHz 帯域に干渉があると、802.11 ワイヤレスネットワークのネットワークトラフィックが中断します。

Catalyst Center は、干渉源の場所、影響範囲、および強度を特定できます。

この手順では、フロアマップ上のネットワーク干渉源を特定する方法を示します。

始める前に

Cisco Connected Mobile Experiences（CMX） または Cisco Spaces が Catalyst Center と統合されていることを確認します。詳細については、Cisco Spaces 統合について （524 ページ）を参照してください。

手順

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

ステップ 2 フロアを 左側の階層ツリーから、以下を選択します します。

ステップ 3 マップツールバーで、[2D] をクリックします。

ステップ 4 [Network Hierarchy] ウィンドウで、[View Options] をクリックします。

ステップ 5 [View Options] ウィンドウで下にスクロールし、[Interferers] トグルボタンをクリックして、干渉源がフロアマップに表示されるようにします。

ステップ 6 [Interferers] カテゴリを展開し、[Show Zone of Impact] トグルボタンをクリックして、干渉源の影響ゾーンがフロアマップに表示されるようにします。

（注） デフォルトでは、[Zone of Impact] は無効になっています。

ステップ 7 フロアマップで、干渉源のアイコンにカーソルを合わせ、影響を受けるチャネルをクリックして干渉源デバイスの詳細情報を確認します。

3D マップの操作

3D マップは、主にフロア上のワイヤレスネットワークの計画と分析に使用されます。そのため、3D マップで実行できる最小限の構成および編集機能があります。

3D ワイヤレスマップを使用すると、ワイヤレスネットワークを 3D で表示できます。ほぼリアルタイムの予測モデルにより、3D マップが動的に更新され、RF カバレッジの変化が示されます。

前提条件

3D ワイヤレスヒートマップを計算して表示するために使用するシステムには、グラフィック処理ユニット（GPU）がインストールされ、有効になっている必要があります。たとえば、Windows 仮想マシン（VM）を使用している場合は、GPU が搭載されていることを確認する必要があります。

3D マップの特徴と機能

3D ワイヤレスマップが提供する独自の機能には、次のようなものがあります。

- 3D 環境で一人称ビューまたは三人称ビューを使用してワイヤレスネットワークを移動する。
- サービスレベル契約（SLA）が満たされていないワイヤレスネットワークのエリアに関するインサイトを得る。
- オプティマイザツールを実行して、SLA を満たす最適な AP レイアウトを計算します。
- さまざまな高度の RF カバレッジを表示し、**スキャナ**ツールを使用して特定の高度の RF カバレッジを表示する。
- クリッピングツールを使用して、重要業績評価指標（KPI）ヒートマップをクリッピングする。

- ピンツールを使用してフロアプラン上の特定ポイントの x、y、z 座標を予測し、AP またはセンサーの配置を適切に計画する。
- 壁などのフロアプラン要素を 3D で可視化して、RF カバレッジおよび減衰に与える影響を確認する。
- さまざまな構成でワイヤレスネットワークをシミュレートして、フロアのワイヤレスカバレッジがどのように影響を受けるかを確認する。これらのシミュレーションを保存し、後で開いてさらに変更を加えることができます。
- KPI、テレメトリ、および 3D マップ要素の設定を変更して、マップ表示をカスタマイズする。

3D マップにおけるフロアマップ要素とオーバーレイの設定

3D マップでは、次の設定および編集機能に制限されています。

- AP のクローンの作成 （352 ページ）
- AP の編集 （318 ページ）
- 複数の AP の編集 （321 ページ）
- マップへの AP の再配置 （318 ページ）
- マップへのセンサーの再配置 （326 ページ）

他のフロアマップ要素またはオーバーレイを設定するには、2D マップを使用する必要があります。詳細については、「2D フロアマップのデバイスとオーバーレイオブジェクトの （302 ページ）」を参照してください。

AP のクローンの作成

AP のクローンを作成することで、その構成を使用して AP を複製できます。

始める前に

クローンを作成する実際の AP が必要です。

手順

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

ステップ 2 フロアを 左側の階層ツリーから、以下を選択します します。

ステップ 3 マップツールバーから、[3D] をクリックします。

ステップ 4 マップツールバーで、[Simulation] トグルボタンをクリックして、シミュレーションモードでマップを表示します。

ステップ 5 マップツールバーで、[Edit/Clone] をクリックします。

ステップ 6 マップで、AP をクリックします。

ステップ 7 [AP Details] スライドインペインで、[Clone] をクリックします。

複製 AP が作成され、元の AP の下に表示されます。名前に **-1** が付きます。同じ AP のクローンを作成し続けると、名前は増分的に追加され続けます。たとえば、**a-floor1-ap01** の最初のクローンには **a-floor1-ap01-1** という名前が付けられ、同じ AP の 2 番目のクローンには **a-floor1-ap01-2** という名前が付けられます。

ステップ 8 マップで、クローンされた AP を右クリックし、[Move] を選択します。

ステップ 9 AP を新しい位置にドラッグアンドドロップします。

ステップ 10 [Save] をクリックします。

3D ワイヤレスヒートマップの表示

この手順を使用して、3D ワイヤレスマップを表示します。

手順

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

ステップ 2 フロアを 左側の階層ツリーから、以下を選択します します。

ステップ 3 マップツールバーから、[3D] をクリックします。

3D ワイヤレスマップが開きます。

（注） 3D ヒートマップは、デフォルトで、フロア全体の幅と長さであるカバレッジエリアによって区切られます。ヒートマップ境界のポリゴンを指定するには、**[2D]** > **[Add/Edit]** > **[Overlays]** をクリックし、マップの左側のペインで [Coverage Area] をクリックします。2D マップでカバレッジエリアを追加および編集できます。ただし、フロア全体の幅と長さが 2D マップビューで使用されるため、これらの境界は 2D マップビューには適用されません。

ステップ 4 デバイスに関する特定の詳細を表示するには、デバイスアイコンの上にカーソルを置きます。ダイアログボックスにデバイスに関する情報が表示されます。

（注） アシュアランス - 基本パッケージがインストールされている場合は、[Device 360] ウィンドウへのリンクもダイアログボックスに表示されます。

ステップ 5 1 つ以上の AP のヒートマップを表示するには、次のいずれかの方法を使用して AP を選択および選択解除します。

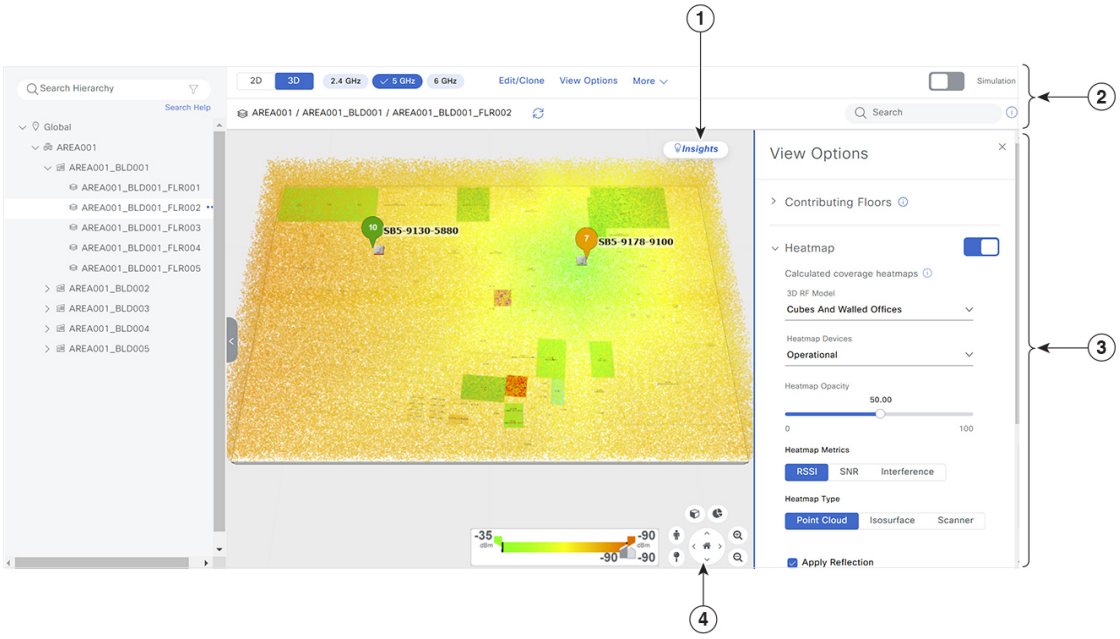
- 1 つの AP を選択するには、その AP をクリックします。
- 複数の AP を選択するには、**Shift** キーを押しながら各 AP をクリックし、**Shift** キーを放します。
- 1 つの AP の選択を解除するには、その AP をクリックします。

（注） AP が選択されていない場合、ヒートマップにはすべての AP が含まれます。

- すべての AP の選択を解除するには、**ESC** キーを押すか、AP がないマップの領域をダブルクリックします。

ステップ 6 次の図に示すツールとオプションを使用して、ワイヤレスネットワークに関する洞察を取得します。

図 *13* : ツールとオプションを示す *3D* ワイヤレスマップ



引き出し線	説明
1	インサイトオプション：マップの右上隅にある [Insights] をクリックして、ワイヤレスネットワークの潜在的な問題を表示して確認します。詳細については、3D ワイヤレスマップからのインサイトの取得 （367 ページ） を参照してください。
2	**マップツールバー**：マップの上で、ツールバーオプションを使用して、ヒートマップに表示される内容を制御します。詳細については、3D ワイヤレスマップツールバー （355 ページ） を参照してください。

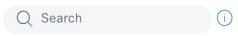
引き出し線	説明
3	[View Options] スライドインペイン：表示オプションを使用してヒートマップ表示を制御します。表示されるフロア、ヒートマップのカバレッジとメトリック、テレメトリのしきい値、デバイスとクライアント、オーバーレイオブジェクト、フロアと空の描写などの要素を操作できます。詳細については、3Dマップビューオプション（356 ページ） を参照してください。
4	**ナビゲーションコントロール**：マップの右下隅で、マップ ナビゲーション コントロールを使用して、さまざまな視点からヒートマップを表示します。詳細については、「3D マップ ナビゲーション コントロール （360 ページ）」を参照してください。

3D ワイヤレスマップツールバー

3Dマップにアクセスするには、左上隅で、メニューアイコンをクリックして次を選択します。**[Design]** > **[Network Hierarchy]**の順に選択します。フロアを 左側の階層ツリーから、以下を選択します し、マップツールバーで**[3D]**をクリックします。

マップツールバーは2つのバーで構成され、マップの上にあります。マップツールバーを使用して、ヒートマップの表示を制御し、ワイヤレスネットワークのシミュレーションの作成などのアクションを実行します。

アイテム	説明
2D 3D	[3D] をクリックしてワイヤレスマップを 3D で表示するか、[2D] をクリックして 2D で表示します。
2.4 GHz ✓ 5 GHz 6 GHz	Wi-Fi バンドボタンをクリックして、対応する Wi-Fi 帯域フィルタを選択します。
[Edit/Clone]	既存の AP または計画済みの AP を編集したり、それらのクローンを作成するには、[Edit/Clone] をクリックします。詳細については、AP のクローンの作成 （352 ページ） を参照してください。 （注） 3D マップでは、インベントリから使用可能な AP を追加することはできません。稼働中の AP を追加するには、2D マップツールバーで [Add/Edit] をクリックします。
View Options	関与しているフロア、マップ、テレメトリ、デバイス、オーバーレイオブジェクト、およびフロア形状の表示を制御するためのオプションを含む [View Options] スライドインペインを開くには、[View Options] をクリックします。詳細については、3D マップビューオプション（356 ページ） を参照してください。

アイテム	説明
More	インサイトの条件をカスタマイズするには、[More]にカーソルを合わせ、[Insights Configuration] をクリックします。詳細については、3D ワイヤレスマップからのインサイトの取得（367ページ）を参照してください。
Simulation	[Simulation] トグルボタンをクリックして、シミュレーションモードでマップを表示します。3D ワイヤレスマップがシミュレーションモードになると、下部のマップツールバーに「You are in Simulation Mode」というメッセージが表示されます。詳細については、3D ワイヤレスマップのシミュレーションの作成（370ページ）を参照してください。 （注） シミュレーションモードは 3D マップでのみ使用でき、2D マップでは使用できません。
	[Full Hierarchy Path]：フロアの完全なナビゲーションパスを表示します。関連する建物とサイトも含まれます。
	[Refresh]：デバイスおよびマップデータを更新するには、この更新アイコンをクリックします。
	[Search]：AP、センサー、クライアントなどの特定のフロアマップ要素を検索するには、[Search] フィールドを使用します。検索結果は、[Search] フィールドの下にある スライドインペインに一覧表示されます。 リスト内の要素にカーソルを合わせると、インジケータがマップ上の要素を指します。要素が視野角の外にある場合、インジケータは赤い破線で表示されます。マップの向きを変えて要素を確認します。

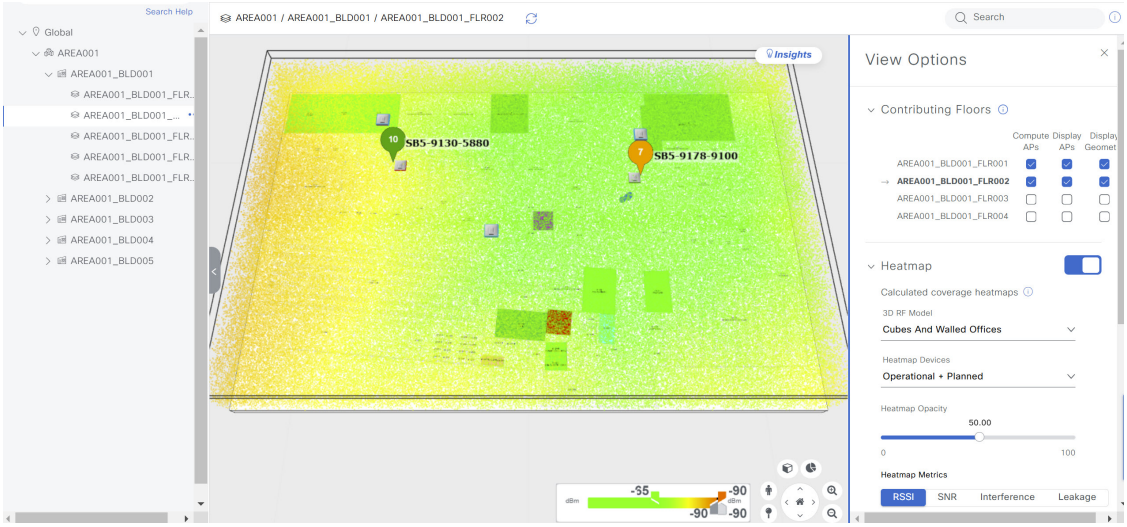
3D マップビューオプション

3Dマップにアクセスするには、左上隅で、メニューアイコンをクリックして次を選択します。**[Design]** > **[Network Hierarchy]** の順に選択します。フロアを左側の階層ツリーから、以下を選択します し、マップツールバーで **[3D]** > **[View Options]** をクリックします。

[View Options] スライドインペインが開きます。カテゴリを展開して設定を表示します。

- [Contributing Floors]：このオプションを展開して、ヒートマップの計算により多くのフロアを含めます。フロアを含める場合、その AP をヒートマップ計算に追加し、その AP とフロアの形状を表示することを選択できます。[Apply] をクリックして、設定を使用してヒートマップを生成します。

図 *14* : 複数のフロアの *3D* マップ



アイテム	説明
[Compute APs]	ヒートマップを計算するときにフロアの AP を含めるには、このチェックボックスをオンにします。
[Display APs]	このチェックボックスをオンにすると、ヒートマップにフロアの AP が表示されます。
[Display Geometry]	ヒートマップにフロアの物理属性を表示するには、このチェックボックスをオンにします。

- [**Heatmap**]：ヒートマップを表示するには、[**Heatmap**] トグルボタンをクリックします。次に、このオプションを展開し、次の表を使用して設定を行います。

アイテム	説明
3D RF Model	RF モデルを選択するには、このドロップダウンリストを使用します。 RF モデルは、フロアの形状に基づいて RF を計算する方法を決定します。使用可能なモデルには、乾式壁のオフィス、キューブおよび壁付きオフィス、フリースペース、屋外オープンスペース、天井の高い屋内があります。 （注） 壁を手動で配置した場合や、CAD ファイルまたは Ekahau プロジェクトからインポートした場合は、[Free Space] を選択することをお勧めします。壁を手動で配置しなかった場合は、[Free Space] 以外の RF モデルを使用します。

アイテム	説明
[Heatmap Devices]	このドロップダウンリストを使用して、稼働中のデバイス、稼働中および計画中のデバイス、または計画中のデバイスのみをヒートマップに表示するかどうかを選択します。
Heatmap Opacity	ヒートマップの不透明度または透明度をカスタマイズするには、このスライダを使用します。
Heatmap Metrics	ヒートマップに表示するメトリックのタイプを選択します。 • [RSSI]：受信信号強度インジケータ（RSSI）の値が表示されます。 • [SNR]：信号対雑音比（SNR）の値が表示されます。 • [Interference]：同一チャネル干渉（CCI）または隣接チャネル干渉によって発生した SNR が表示されます。 • [Leakage]：フロア間の信号漏えいを表示します。このオプションを使用できるようにするには、2 つ以上のフロアを関与させてヒートマップを計算する必要があります。
Heatmap Type	ヒートマップタイプを選択します。 • [Point Cloud]：空間内のデータポイントのコレクションを提供します。各データポイントには、x、y、および z 座標があります。 • [Isosurface]：等値線または連続値線による RSSI を提供します。 • [Scanner]：特定の高度の RSSI が表示されます。
[Apply Reflection]	このチェックボックスをオンにすると、信号の反射が表示されます。これは、信号がガラス、ホワイトボード、プラスチックなどの素材で跳ね返ったときに発生する可能性があります。

- [Telemetry]：テレメトリを有効または無効にするには、[Telemetry] トグルボタンをクリックします。テレメトリが有効になっている場合は、センサーまたは AP をクリックするとテレメトリが表示されます。
  - センサーのテレメトリには、センサー AP とその他の AP の間の予測される RSSI 値と測定された RSSI 値が表示されます。
  - AP のテレメトリには、近接 AP 間の予測される RSSI 値と測定された RSSI 値が表示されます。

このオプションを展開し、[Telemetry Threshold] スライダを使用して、ヒートマップに表示されるテレメトリソースのしきい値を設定します。予測値がしきい値を満たさないテレメトリソースは表示されません。

- [**Devices**]：このオプションを展開し、次の表を使用して設定を行います。

アイテム	説明
AP	このチェックボックスをオンにすると、マップ上に AP が表示されます。
[Planned APs]	このチェックボックスをオンにすると、マップ上に計画済み AP が表示されます。
Sensor	このチェックボックスをオンにすると、マップ上にセンサーが表示されます。
[Clients]	このチェックボックスをオンにすると、マップ上にクライアントが表示されます。さらに、次のタスクを実行できます。 • クライアントをデフォルトの青色（[None]）で、または [RSSI]、[SNR]、または [Health Score] で表示します。[RSSI]、[SNR]、および [Health Score] の場合、クライアントは、現在の状態に応じて、青、黄、または赤に色付けされます。 • [Ball Size] スライダを使用して、マップ上のクライアントを表すボールのサイズを変更します。

- [**Overlay Objects**]：このオプションを展開し、次の表を使用して設定を行います。

アイテム	説明
Geometry	このチェックボックスをオンにすると、フロアの形状が表示されます。
[Height]	このスライダを使用して、ヒートマップ上の壁の高さを設定します。

- [**Map**]：このオプションを展開し、次の表を使用して設定を行います。

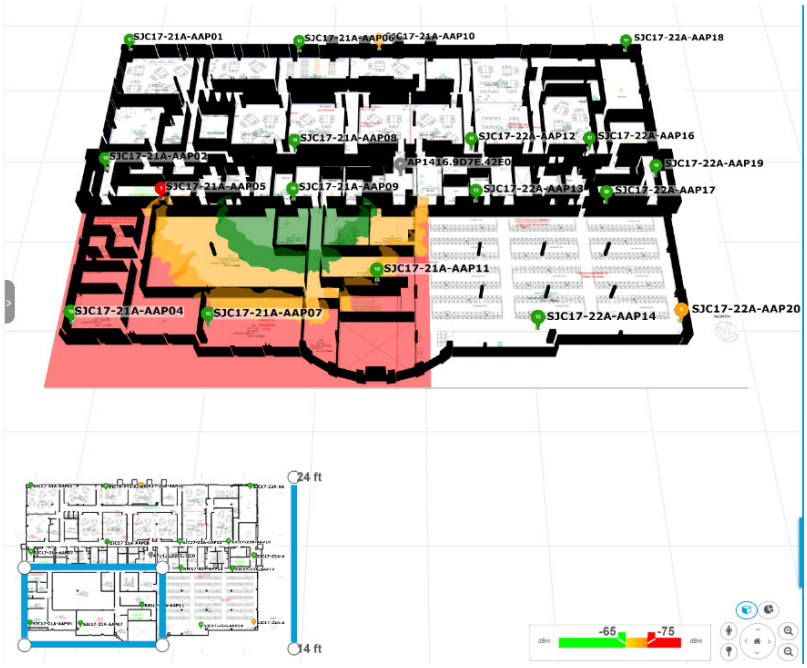
アイテム	説明
[Sky]	このチェックボックスをオンにすると、ヒートマップに空が表示されます。
Floor	このチェックボックスをオンにすると、ヒートマップにフロアが表示されます。

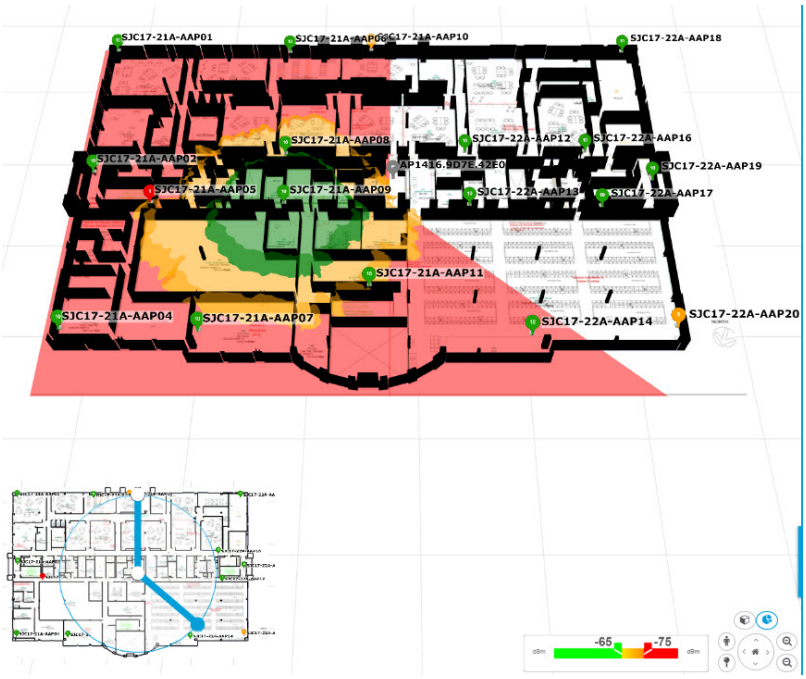
3D マップ ナビゲーション コントロール

3Dマップにアクセスするには、左上隅で、メニューアイコンをクリックして次を選択します。**[Design]** > **[Network Hierarchy]**の順に選択します。フロアを 左側の階層ツリーから、以下を選択します し、マップツールバーで [3D] をクリックします。

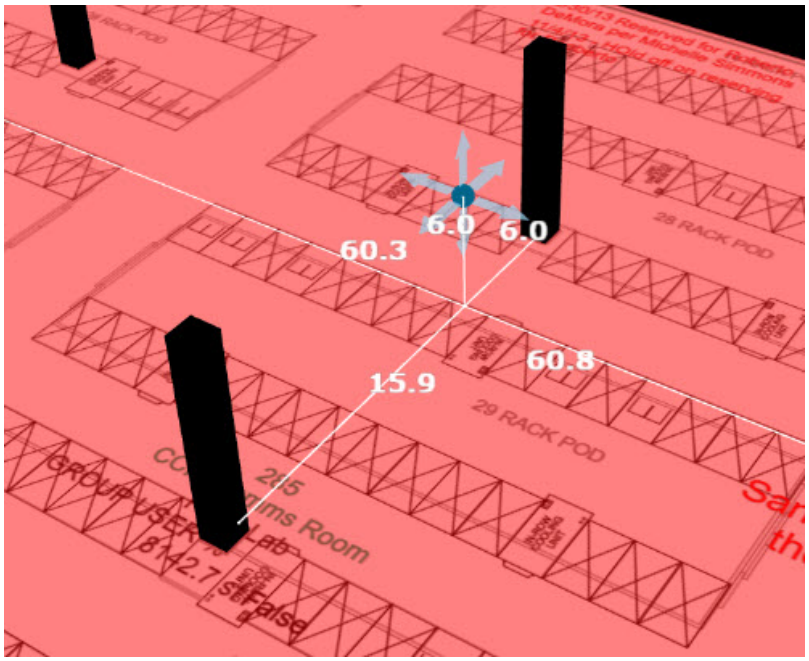
3D マップ ナビゲーション コントロールは、マップの右下隅にあります。マップの詳細については、3D ワイヤレスヒートマップの表示 （353 ページ）を参照してください。

マップビューを制御するには、マップの右下にあるマップ ナビゲーション コントロールを使用します。

マップ ナビゲーション コントロール	説明
	[Use clip box]：このアイコンをクリックし、ボックス形状を使用してヒートマップをトリミングします。マップの左下隅にあるクリッパーを使用して、トリミング位置を指定します。 • トリミングのサイズを変更するには、アンカーポイントの1つをクリックしてドラッグします。 • トリミングの上下の範囲を指定するには、右側にある垂直スライダのアンカーポイントの 1 つをクリックしてドラッグします。 **図 *15*：クリップボックス** 

マップ ナビゲーション コントロール	説明
	[Use clip planes]：このアイコンをクリックし、ドーナツ形状を使用してヒートマップをトリミングします。マップの左下隅にあるクリッパーを使用して、トリミング位置を指定します。 • ドーナツの位置を変更するには、ドーナツの中心にあるアンカーポイントをクリックしてドラッグします。 • トリミングの形状を変更するには、外周にある 2 つのアンカーポイントをクリックしてドラッグします。 **図 *16 :* 使用中のクリッププレーン** 
	[First Person View]：このアイコンをクリックして、一人称ビューと三人称ビューを切り替えます。 青い球は、マップ上の自分の位置を示しています。マップ全体にわたって移動すると、視野が変化します。左下隅にあるミニマップを使用して、視野と方向を把握できます。 （注） 表示用に複数のフロアを選択している場合、[First Person View] によって現在のフロアが自動的に自分の位置となります。 ビューのコントロールなどの詳細については、3D ワイヤレスマップの一人称ビューと三人称ビューの使用 （364 ページ）を参照してください。

マップ ナビゲーション コントロール	説明
	[Third Person View]：このアイコンをクリックして、一人称ビューと三人称ビューを切り替えます。マップ上の自分を配置したい場所にアイコンをドラッグアンドドロップすることもできます。 青い球は、マップ上の自分の位置を示しています。マップ全体にわたって移動すると、視野が変化します。左下隅にあるミニマップを使用して、視野と方向を把握できます。 ビューのコントロールなどの詳細については、3D ワイヤレスマップの一人称ビューと三人称ビューの使用 （364 ページ）を参照してください。

マップ ナビゲーション コントロール	説明
	[Place a pin]：このアイコンをクリックして、フロアマップ上の特定のポイントの予測測定値（x、y、z座標）を表示します。ピンを配置すると、ピンからヤードスティックの端までの距離の測定値を表示できます。ズームインまたはズームアウトすると、測定の位置が調整され、ビューに収まります。ピンをドラッグアンドドロップして位置を変更します。 • **ピンを水平に移動するには**：水平の矢印をクリックして、ピンを左、右、前、または後ろにドラッグします。選択した矢印とヤードスティックは、アクティブなときは強調表示されます。 • **ピンを垂直に移動するには**：垂直の矢印をクリックして、ピンを上下にドラッグします。選択した矢印とヤードスティックは、アクティブなときは強調表示されます。 ビデオデモンストレーションについては、ここをクリックしてください。 **図 *17*: ピンの調整** 
	[Zoom In]：このアイコンをクリックしてビューを拡大します。マウスホイールを使用して拡大することもできます。
	[Zoom Out]：このアイコンをクリックして、画像のサイズを縮小し、視野を広げます。マウスホイールを使用して縮小することもできます。

マップ ナビゲーション コントロール	説明
	[Map Rotation and Default Map View]：方向を示す矢印をクリックしてカメラの角度を変更します。 デフォルトのビューに戻るには、[Return Home] アイコンをクリックしてマップをリセットします。

3D ワイヤレスマップの一人称ビューと三人称ビューの使用

一人称ビューと三人称ビューを使用すると、ワイヤレスネットワークの異なる視点を得ることができます。

手順

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

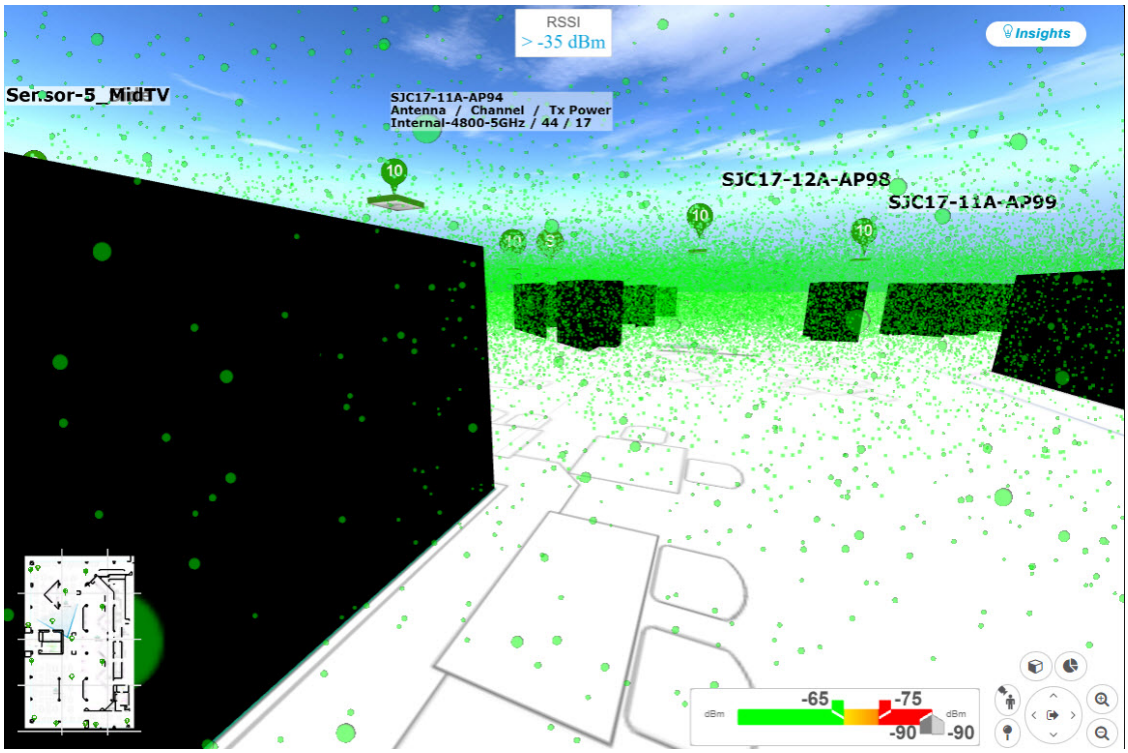
ステップ 2 フロアを 左側の階層ツリーから、以下を選択します します。

ステップ 3 マップツールバーから、[3D] をクリックします。

ステップ 4 一人称ビューを使用するには、マップ ナビゲーション コントロールの一人称ビューのアイコン  をクリックします。必要に応じて、人のアイコン  をマップ上の特定の場所にドラッグアンドドロップできます。

マップビューが一人称ビューに変わります。

図 *18* : 一人称ビュー



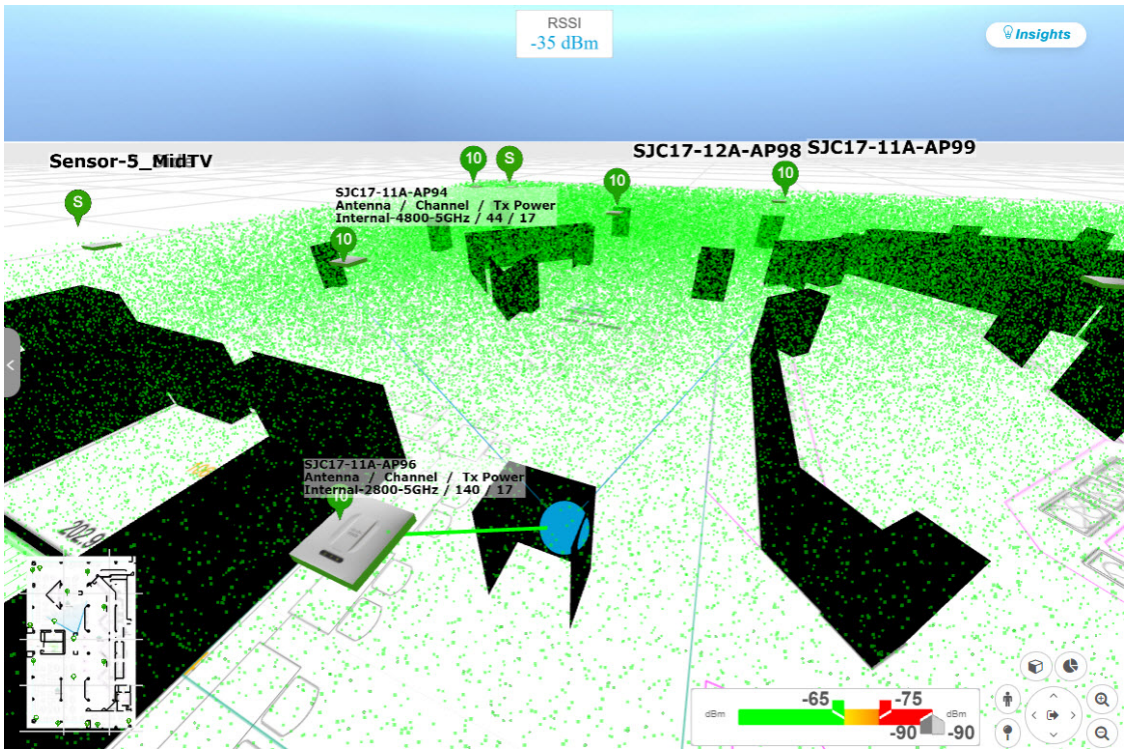
ステップ 5 一人称ビューを制御するには、次の操作を実行します。

アクション	コントロール
前後左右に移動します。	**W**、**A**、**S**、および **D** キーまたは矢印キーを使用します。
カメラアングルを変更します。	マップ上でマウスの左ボタンをクリックしたまま、マウスホイールを動かします。
カメラアングルの高度を上げます。	**スペースバー**を押しつづけます。
カメラアングルの高度を下げます。	**Shift** + **スペースバー**を押しつづけます。

ステップ 6 三人称ビューを使用するには、マップ ナビゲーション コントロールの三人称ビューのアイコン  をクリックします。

マップビューが三人称ビューに変わります。

図 *19* : 三人称ビュー



ステップ 7 三人称ビューを制御するには、次の操作を実行します。

アクション	コントロール
前後左右に移動します。	**W**、**A**、**S**、および **D** キーまたは矢印キーを使用します。
カメラアングルを変更します。	マップをクリックしてドラッグします。
カメラアングルの高度を上げます。	**スペースバー**を押しつづけます。
カメラアングルの高度を下げます。	**Shift** + **スペースバー**を押しつづけます。

ステップ 8 デフォルトのビューに戻るには、ホームに戻るアイコン をクリックします。

AP およびクライアントに関する詳細の表示

Cisco Spaces や Cisco Connected Mobile Experiences（CMX） などの位置情報サービスが Catalyst Center にインストールされている場合は、次の手順を実行してフロア上のクライアントの位置を表示できます。

クライアントは、マップ上で小さな青いボール（●）として識別されます。

手順

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

ステップ 2 フロアを 左側の階層ツリーから、以下を選択します します。

ステップ 3 マップツールバーから、[3D] をクリックします。

（注） 3D ヒートマップは、デフォルトで、フロア全体の幅と長さであるカバレッジエリアによって区切られます。ヒートマップ境界のポリゴンを指定するには、2D マップビューで [Coverage Area] フィールドの値を編集します。ただし、フロア全体の幅と長さが 2D マップビューで使用されるため、これらの境界は 2D マップビューには適用されません。

ステップ 4 AP に関する詳細を表示するには、その AP をクリックします。

スライドインペインには、AP タイプ、MAC アドレス、AP モデル、ソフトウェアバージョン、コントローラ IP アドレス、製品タイプ、AP モード（フレックス/ファブリック、ローカルなど）、センサーモード、正常性スコア、問題の数、無線インターフェイスの詳細（該当する Wi-Fi 帯域の動作モード（クライアントサービスまたはモニタリング）、チャンネル番号、スロット ID、チャンネル幅、送信電力、クライアント数、チャンネル使用率、アンテナ名、アンテナ角、および高度）が表示されます。

ステップ 5 クライアントに関する情報を表示するには、カーソルをボール（クライアント）の上に置きます。

クライアントとそれに関連付けられた AP の間に線が描画されます。クライアントの IPv4 アドレス、IPv6 IP アドレス、RSSI 値などの情報を含むダイアログボックスが表示されます。[Client 360] ウィンドウを開くには、ダイアログボックスの [Client 360] リンクをクリックします。

ステップ 6 RSSI、SNR、または正常性スコアに対応する色でクライアントを表示するには、次の手順を実行します。

a) **[View Options]** > **[Devices and Client]** をクリックします。
b) [Clients] チェックボックスをオンにします。
c) [Clients] チェックボックスで、[None]（デフォルトの青色）、[RSSI]、[SNR]、または [Health Score] をクリックします。

ステップ 7 ボールのサイズを変更するには、[View Options] ペインの [Ball Size] スライダを使用します。

この機能は、クライアントが多い場合や少ない場合にクライアントを表示するのに役立ちます。たとえば、クライアントが多い場合はボールを小さくし、クライアントが少ない場合はボールを大きくします。

3D ワイヤレスマップからのインサイトの取得

Catalyst Center は、3D ワイヤレスマップのネットワークパフォーマンスをアクティブにモニターし、サービスレベル契約（SLA）が満たされていないエリアへのインサイトを提供します。

手順

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

ステップ 2 フロアを 左側の階層ツリーから、以下を選択します します。

ステップ 3 マップツールバーから、[3D] をクリックします。

ステップ 4 マップの右上隅にある [Insights] をクリックします。

[Insights] エリアが開き、特定の KPI しきい値（たとえば、RSSI ≥ -70 dBm）を満たさないカバレッジエリアに関する情報が表示されます。

図 *20 : [Insights]* エリア



ステップ 5 [インサイト（Insights）] エリアでは、次のいずれの操作も実行できます。

項目	詳細
[View coverage gaps]	このリンクをクリックすると、ワイヤレスカバレッジエリアが表示されます。赤色の領域は、SLA が満たされていないエリアを示します。緑色の領域は、SLA が満たされているエリアを示します。
[Optimizer]	このリンクをクリックして、Catalyst Center でワイヤレスカバレッジエリアを分析します。移動および追加する AP の最大数を指定して、Catalyst Center でワイヤレスカバレッジが最大化される構成を計算します。 詳細については、ワイヤレスカバレッジオプティマイザの実行（369ページ）を参照してください。
[Mute This Insight]	このボタンをクリックして、インサイトを [インサイト] ダイアログボックスに表示しないようにします。 ミュートされたインサイトは、[All Insights] スライドインペインのリストの下部に表示されます。

項目	詳細
[View All Insights]	このボタンをクリックすると、アクティブなインサイトとミュートされたインサイトがすべて表示されます。 インサイトごとに、[Mute] または [Unmute] をクリックして、[Insights] ダイアログボックスに表示するかどうかを指定できます。 インサイトの KPI 設定をカスタマイズするには、[Edit Configuration] をクリックします。 インサイトのKPI設定は、マップツールバーでもカスタマイズできます。マップツールバーの歯車のアイコン にカーソルを合わせて、[Insights Configurations] を選択します。

ワイヤレス カバレッジ オプティマイザの実行

SLA を満たしていないワイヤレスエリアの場合、オプティマイザは、移動および追加の準備ができている AP の最大数の入力を取り、ワイヤレスカバレッジが最大化される構成を計算します。

この手順では、ワイヤレス カバレッジ オプティマイザを実行する方法を示します。

手順

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

ステップ 2 フロアを 左側の階層ツリーから、以下を選択します します。

ステップ 3 マップツールバーから、[3D] をクリックします。

ステップ 4 マップの右上隅にある [Insights] をクリックします。

[Insights] エリアが開き、特定の KPI しきい値（たとえば、RSSI ≥ -70 dBm）を満たさないカバレッジエリアに関する情報が表示されます。

ステップ 5 （任意） ワイヤレスカバレッジエリアを表示するには、[View] をクリックします。

赤色の領域は、SLA が満たされていないエリアを示します。緑色の領域は、SLA が満たされているエリアを示します。

ステップ 6 （任意） オプティマイザで特定の AP が移動されないようにする場合は、それらを右クリックし、[Lock] を選択してその位置をロックできます。ロックを解除するには、AP を右クリックし、[Unlock] を選択します。

ステップ 7 [Optimizer] をクリックします。

ステップ 8 [Coverage Optimizer] ダイアログボックスで、移動および追加の準備ができている AP の最大数を入力します。

AP を移動または追加しない場合は、対応するフィールドを空白のままにするか、「0」を入力します。

ステップ 9 [Run Optimizer] をクリックします。

必要に応じて、任意の AP を他の場所に手動で移動できます。

ステップ 10 分析が完了したら、[View Results] をクリックします。

Catalyst Center には、ワイヤレスカバレッジを拡大して SLA を最大化するレイアウト案が表示されます。オプティマイザが AP の移動を推奨する場合、新しいレイアウトでは推奨される新しい場所に青い線が表示されます。レイアウトに追加された新しい AP は、青いマーカー（）で表示されます。

ステップ 11 新しいレイアウトをシミュレーションとして保存するには、[Save as a plan] をクリックします。保存せずに終了するには、マップの右上隅にある [x] をクリックします。

後で、推奨の変更を物理ワイヤレスネットワークに実装すると、シミュレーションを運用マップとして保存できます。詳細については、3D ワイヤレスマップのシミュレーションの作成 （370 ページ）を参照してください。

3D ワイヤレスマップのシミュレーションの作成

3D ワイヤレスマップのシミュレーションを作成することができます。

（注） シミュレーションモードは 3D マップでのみ使用でき、2D マップでは使用できません。

シミュレーションを使用すると、実際に実装せずにデバイス構成を変更できます。複数のシミュレーションを作成し、いつでもロードすることができます。

手順

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

ステップ 2 フロアを 左側の階層ツリーから、以下を選択します します。

ステップ 3 マップツールバーから、[3D] をクリックします。

ステップ 4 マップツールバーで、[Simulation] トグルボタンをクリックして、シミュレーションモードでマップを表示します。

下部のマップツールバーに「You are in Simulation Mode」というメッセージが表示されます。

ステップ 5 マップツールバーで、[Edit/Clone] をクリックします。

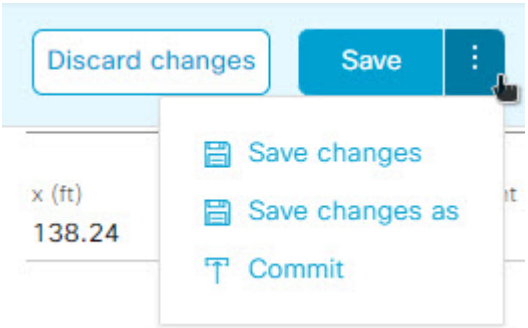
シミュレーションモードでは、特定の属性のみが編集可能であり、ヒートマップで変更の影響をプレビューするために使用できます。

ステップ 6 必要に応じて、シミュレーションのデバイスに変更を加え、[Apply] をクリックします。

- **AP**：モデル、チャネル、アンテナなどを変更できます。
- **PAP**：モデル、チャネル、アンテナなどを変更できます。

ステップ 7 マップツールバーで、垂直の省略記号にカーソルを合わせて、[Save changes as] を選択して設定を新しいシミュレーションとして保存します。

図 *21* : シミュレーションとして保存



（注） 既存のシミュレーションへの変更を保存する場合は、[Save changes] を選選択します。

シミュレーションを実稼働環境にコミットする場合は、[Commit] を選択します。コミットできるのは計画済み AP のみであることに注意してください。

ステップ 8 [Save Simulation] ダイアログボックスで、シミュレーションの名前を入力し、[Save] をクリックします。

マップに新しいシミュレーションが表示されます。

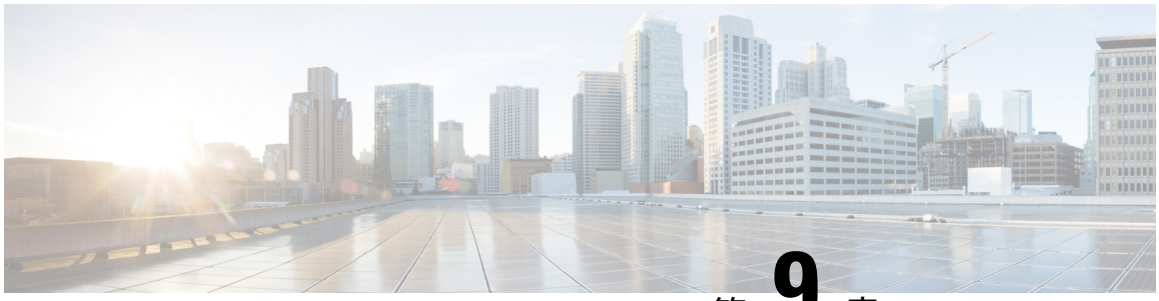
ステップ 9 （任意） 別のシミュレーションを表示するには、次の手順を実行します。

1. シミュレーションモードになっており、デバイスを編集していないことを確認します。
2. [Select Simulation] ドロップダウンリストから、シミュレーションを選択します。

   保存されたシミュレーションがない場合は、[Select Simulation] ドロップダウンリストの代わりに [None available] が表示されます。

ステップ 10 （任意） シミュレーションを削除するには、次の手順を実行します。

1. [Select Simulation] ドロップダウンリストから、シミュレーションを選択します。
2. [Select Simulation] ドロップダウンリストの横にある削除アイコンをクリックします。



第 9 章

ネットワークの設定

- ネットワーク設定の概要 （373 ページ）
- サイトのタイムゾーンの設定 （374 ページ）
- 今日のメッセージの設定 （375 ページ）
- Cisco ISE またはその他の AAA サーバーの追加 （375 ページ）
- グローバル ネットワーク サーバーの設定 （377 ページ）
- グローバル デバイス クレデンシャルの設定 （379 ページ）
- IP アドレスプールを設定する （397 ページ）
- サービス プロバイダ プロファイルの設定 （413 ページ）
- グローバルワイヤレス設定の構成 （414 ページ）
- 証明書失効確認の設定 （533 ページ）

ネットワーク設定の概要

ネットワーク全体のデフォルトになるネットワーク設定を作成できます。ネットワーク内の設定を定義可能な主なエリアは次の 2 つです。

- [Global settings]：ここで定義されている設定はネットワーク全体に適用されます。DHCP、DNS、AAA、NTP などのサーバー、IP アドレスプール、デバイス クレデンシャル プロファイル、Syslog、トラップ、Netflow などのテレメトリの設定が含まれます。
- [Site settings]：ここで定義されている設定はグローバル設定をオーバーライドします。また、サーバー、IPアドレスプール、デバイスのログイン情報プロファイルの設定を含めることができます。

（注） アクティブなファブリックで使用されているネットワーク設定の変更はサポートされていません。それらのネットワーク設定には、サイト階層、IPプールの名前変更など複数の機能が含まれます。

（注） 一部のネットワーク設定は、デバイスの可制御性機能を使用してデバイスに自動的に設定できます。Catalyst Centerによるデバイスの設定または更新時に、トランザクションがCatalyst Centerの監査ログにキャプチャされます。監査ログを使用すると、変更を追跡し、問題をトラブルシューティングするのに役立ちます。

[Design] > **[Network Settings]** の順に選択して該当するタブをクリックし、次のグローバルネットワーク設定を定義できます。

- AAA、DHCP、DNSサーバーなどのネットワークサーバー：詳細については、グローバルネットワーク サーバーの設定 （377 ページ）を参照してください。
- CLI、SNMP、HTTP、HTPSなどのデバイスのクレデンシャル：詳細については、「グローバル デバイス クレデンシャルの設定 （379 ページ）」を参照してください。
- IPアドレスプールの詳細については、IPアドレスプールを設定する （397ページ）を参照してください。
- SSID、ワイヤレス インターフェイス、および無線周波数プロファイルなどのワイヤレス設定：詳細については、グローバルワイヤレス設定の構成 （414ページ）を参照してください。
- テレメトリを使用して、syslog、SNMP、NetFlowコレクタサーバーなどのグローバルテレメトリ設定を構成します。

サイトのタイムゾーンの設定

サイトのタイムゾーンは、サイトへのデバイスの割り当て、プロビジョニング、テレメトリ設定の更新などのタスクのスケジュール設定に主に使用されます。

後でタスクをスケジュールする場合、サイトに割り当てられているタイムゾーンがデフォルトで使用されます。

サイトのタイムゾーンを設定するには、次の手順を実行します。

手順

ステップ 1 メインメニューから次を選択します。**[Design]** > **[Network settings]**。
ステップ 2 [Servers] タブをクリックします。
ステップ 3 左側の階層ツリーから、以下を選択します で、目的のサイトを選択します。
ステップ 4 [Time Zone] セクションのドロップダウンリストから目的のタイムゾーンを選択します。
ステップ 5 [Save] をクリックします。

今日のメッセージの設定

今日のメッセージは、デバイスの CLI にロギングしたときに表示されるグリーティングメッセージです。このメッセージは、ルータ、スイッチ、およびハブにのみ適用されます。

今日のメッセージの設定するには、次の手順を実行します。

手順

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

ステップ 2 [Servers] タブをクリックします。

ステップ 3 左側の階層ツリーから、以下を選択します で、目的のサイトを選択します。

ステップ 4 [今日のメッセージ（Message of the Day）] セクションで、次のいずれかのオプションを選択します。

- [Use device's existing message]

  これがデフォルトのオプションです。

- [Set custom message]

  独自のメッセージを入力できますが、次の制約に従う必要があります。

  - 「#」または「<」は使用できません
  - 「MLTCMD」または「mltcmd」は使用できません
  - 行の最大長：80 文字
  - 最大行数：40

ステップ 5 [Save] をクリックします。

Cisco ISE またはその他の AAA サーバーの追加

Cisco Identity Services Engine（ISE）サーバーまたはその他の同様の AAA サーバーを、ネットワーク、クライアント、およびエンドポイント認証のためにサイトまたはグローバル レベルで定義することができます。ネットワーク認証では、RADIUS および TACACS プロトコルがサポートされています。クライアントとエンドポイント認証では、RADIUS のみがサポートされます。Catalyst Center あたり、1 つの Cisco ISE のみサポートされます。

マルチ ISE 設定をサポートするために、RADIUS または TACACS サーバーグループの下に送信元インターフェイスを設定できます。各 Cisco ISE ISE クラスタには独自のサーバーグループがあります。Catalyst Center が管理 IP として使用するインターフェイスは、RADIUS および TACACS サーバーの送信元インターフェイスとして設定されます。

あるサイトに Cisco ISE サーバーを設定すると、割り当てられているデバイスは、対応する Cisco ISE サーバーで、自動的に /32 マスクに更新されます。 Cisco ISE でこれらのデバイスに加えた変更は、Catalyst Center にも自動的に送信されます。

FIPS モード展開の場合、共有秘密は、共有秘密、キーラップ、およびメッセージ認証コードキーを含みます。

始める前に

- [Advanced Network Settings] に対する読み取り権限が必要です。
- [システム（System）]>[設定（Settings）] ウィンドウで、Catalyst Center ユーザーを認証するサーバーを指定する必要があります。詳細については、『Cisco Catalyst Center Administrator Guide』の「Configure Authentication and Policy Servers」を参照してください。

手順

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

ステップ 2 [AAA] エリアを展開します。

ステップ 3 [Network] や [Client/Endpoint] タブの下にある [Add AAA servers] チェックボックスをオンにし、AAA サーバーのサーバーとプロトコルを設定します。

ステップ 4 認証と認可のための [Server Type]（[ISE] または [AAA]）を選択します。

a) [ISE] を選択した場合は、次の設定を行います。

- [Protocol] を選択します（[RADIUS] または [TACACS]）。
- [PAN] ドロップダウンリストから、Cisco ISE サーバーの IP アドレスを選択します。[PAN] ドロップダウンリストには、 [System] > [Settings] ウィンドウに登録されている Cisco ISE サーバーのすべての IP アドレスが含まれています。Cisco ISE の IP を選択すると、選択した Cisco ISE のポリシーサービスノード（PSN）の IP アドレスを持つプライマリおよびセカンダリ IP アドレスのドロップダウンリストが表示されます。AAA サーバーの IP アドレスを入力することも、[Primary Server] ドロップダウンリストと [Secondary Server] ドロップダウンリストから PSN IP アドレスを選択することもできます。
- [RADIUS] を選択すると、Catalyst Center は選択した Cisco ISE IP アドレスを認可変更（CoA）用にプロビジョニングします。Catalyst Center は CoA 操作の動的承認リストで pxGrid、PSN、および PAN IP アドレスを設定します。
- [TACACS] を選択する場合は、[Single Connection] チェックボックスをオンにして、重複トランザクションのために開かれる TCP 接続の数を最小限に抑えます。

（注） 特定のワイヤレスコントローラの物理サイトと管理サイトの AAA 設定が一致する必要があります。一致しない場合、プロビジョニングは失敗します。

b) [AAA] を選択した場合は、次の設定を行います。

- [Protocol] を選択します（[RADIUS] または [TACACS]）。
- [Primary Server] ドロップダウンリストから、AAA サーバーの IP アドレスを選択します。 アイコンをクリックし、[Secondary Server] ドロップダウンリストから IP アドレスを選択します。サーバーを削除するには、 アイコンをクリックします。

  これらのドロップダウンリストには、[System] > [Settings] ウィンドウに登録されている Cisco ISE 以外の AAA サーバーが含まれています。

  AAA サーバーの IP アドレスが既存の Cisco ISE クラスタに含まれていないことを確認します。
- [TACACS] を選択する場合は、[Single Connection] チェックボックスをオンにして、重複トランザクションのために開かれる TCP 接続の数を最小限に抑えます。

（注） [Server Type] を ISE（TACACS を使用）から TACACS を使用する AAA に切り替えると、TACACS は認証に使用されなくなるため、Cisco ISE サーバーで無効になります。

ステップ 5 [Save] をクリックします。

グローバル ネットワーク サーバーの設定

ネットワーク全体のデフォルトになるグローバル ネットワーク サーバーを定義することができます。

（注） サイト固有の設定を定義することで、サイトのグローバル ネットワーク設定をオーバーライドできます。

手順

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

ステップ 2 [Servers] タブをクリックします。

ステップ 3 [DHCP]エリアを展開します。クライアントデバイスのネットワーキング設定を管理するための 1 つまたは複数の専用 Dynamic Host Configuration Protocol（DHCP）サーバーを指定します。

ステップ 4 [Add DHCP servers] チェックボックスをオンにして、フィールドを表示します。

ステップ 5 [IP Address] フィールドに DHCP サーバーの IP アドレスを入力します。アイコンをクリックして、IP アドレスを追加します。

（注）
- アイコンをクリックすると、IPv4 アドレスと IPv6 アドレスの両方を入力できます。IP アドレスを削除するには、 アイコンをクリックします。

IP アドレス プールを作成するには、少なくとも 1 つの DHCP サーバーを定義する必要があります。

ステップ 6 [DNS]エリアを展開してネットワークのドメイン名を設定し、ホスト名解決用のDomain Name System（DNS）サーバーを指定します。

ステップ 7 [Set a domain name] チェックボックスをオンにして、DNS サーバーのドメイン名を入力します。

ステップ 8 [Add DNS servers] チェックボックスをオンにして、IP アドレスを入力します。

（注）
- アイコンをクリックすると、IPv4 アドレスと IPv6 アドレスの両方を入力できます。IP アドレスを削除するには、 アイコンをクリックします。

IP アドレス プールを作成するために、少なくとも 1 つの DNS サーバーを定義する必要があります。

ステップ 9 ネットワークのシステムクロックの同期を容易にするために、1 つ以上の Network Time Protocol（NTP）サーバーを指定するには、[NTP] エリアを展開します。

ステップ 10 [Add NTP servers] チェックボックスをオンにして、フィールドを表示します。

ステップ 11 [IP Address] フィールドに、NTP サーバーの IP アドレスを入力します。アイコンをクリックして、IP アドレスを追加します。

（注）
- アイコンをクリックすると、IPv4 アドレスと IPv6 アドレスの両方を入力できます。IP アドレスを削除するには、 アイコンをクリックします。

ステップ 12 [Save] をクリックします。

グローバル デバイス クレデンシャルの設定

「グローバル デバイス クレデンシャル」とは、ネットワーク内のデバイスに関する情報を検出して収集するために Catalyst Center で使用される共通の CLI、SNMP、および HTTPS クレデンシャルを指します。Catalyst Center は、グローバル クレデンシャルを使用して設定済みデバイス クレデンシャルを共有するネットワーク内のデバイスを認証し、アクセスします。

グローバルデバイスログイン情報ワークフローの設定

ネットワーク内のデバイスにグローバルデバイスログイン情報を設定するには、次の高度な手順を実行します。

1. グローバルデバイスログイン情報を作成します。グローバル CLI クレデンシャルの追加（379 ページ）、グローバル SNMPv2c ログイン情報の追加 （380 ページ）、グローバル SNMPv3 ログイン情報の追加 （382 ページ）、および グローバル HTTPS ログイン情報の追加 （385 ページ） を参照してください。
2. グローバルデバイスログイン情報をサイトに割り当てます。デバイスログイン情報のサイトへの割り当て （387 ページ）を参照してください。
3. 選択したサイト内のすべてのデバイスにグローバルデバイスログイン情報を適用します。サイトのデバイスへのデバイスログイン情報の適用 （389 ページ）を参照してください。
4. グローバルデバイスログイン情報を管理します。グローバルデバイスログイン情報の管理（389 ページ）を参照してください。

グローバル CLI クレデンシャルの追加

最大 10 のグローバル CLI ログイン情報を追加して保存できます。

手順

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

ステップ 2 [Device Credentials] タブをクリックします。

ステップ 3 左側の階層ツリーから、サイトを選択します。

ステップ 4 次のいずれか 1 つのタスクを実行します。

- ログイン情報をまだ作成していない場合は、[Create Credentials] をクリックします。
- ログイン情報を作成済みの場合は、[Manage Credentials] をクリックします。

ステップ 5 [Manage Credentials] スライドインペインで、[Add] ドロップダウンリストから [CLI] を選択します。

ステップ 6 次の表を使用して、表示されるフィールドに入力します。

表 *40 : CLI* クレデンシャル

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

ステップ 7 （任意） [Assign credential to site] チェックボックスをオンにして、選択したサイトに CLI ログイン情報を割り当てます。

ステップ 8 [Save] をクリックします。

成功メッセージが右下隅に表示されます。ログイン情報は、[Manage Credentials] スライドインペインで確認できます。ただし、サイトにログイン情報を割り当てなかった場合は、[System] フォーカスのみにログイン情報が表示されます。

グローバル SNMPv2c ログイン情報の追加

ネットワークデバイスをモニターおよび管理するために、グローバル SNMPv2c ログイン情報を追加できます。

（注） Catalyst Center は、FIPS モードが有効になっている場合、SNMPv2c デバイスクレデンシャルをサポートしません。代わりに、SNMPv3 クレデンシャルを指定する必要があります。

始める前に

ネットワークの SNMP 情報は必須です。

手順

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

ステップ 2 [Device Credentials] タブをクリックします。

ステップ 3 左側の階層ツリーから、サイトを選択します。

ステップ 4 次のいずれか 1 つのタスクを実行します。

- ログイン情報をまだ作成していない場合は、[Create Credentials] をクリックします。
- ログイン情報を作成済みの場合は、[Manage Credentials] をクリックします。

ステップ 5 [Manage Credentials] スライドインペインで、[Add] ドロップダウンリストから [SNMPv2c Read] または [SNMPv2c Write] を選択します。

ステップ 6 次の表を使用して、表示されるフィールドに入力します。

表 *41 : SNMPv2c* クレデンシャル

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

ステップ 7 （任意） [Assign credential to site] チェックボックスをオンにして、選択したサイトに SNMPv2c ログイン情報を割り当てます。

ステップ 8 [Save] をクリックします。

成功メッセージが右下隅に表示されます。ログイン情報は、[Manage Credentials] スライドインペインで確認できます。ただし、サイトにログイン情報を割り当てなかった場合は、[System] フォーカスのみにログイン情報が表示されます。

グローバル SNMPv3 ログイン情報の追加

ネットワークデバイスをモニターおよび管理するために、グローバル SNMPv3 ログイン情報を追加できます。

始める前に

ネットワークの SNMP 情報は必須です。

手順

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

ステップ 2 [Device Credentials] タブをクリックします。

ステップ 3 左側の階層ツリーから、サイトを選択します。

ステップ 4 次のいずれか 1 つのタスクを実行します。

- ログイン情報をまだ作成していない場合は、[Create Credentials] をクリックします。
- ログイン情報を作成済みの場合は、[Manage Credentials] をクリックします。

ステップ 5 [Manage Credentials] スライドインペインで、[Add] ドロップダウンリストから [SNMPv3] を選択します。

ステップ 6 次の表を使用して、表示されるフィールドに入力します。

表 *42 : SNMPv3* クレデンシャル

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

フィールド	説明
Auth Type	使用する認証タイプ（このフィールドは、認証モードとして [Authentication and Privacy] または [Authentication, No Privacy] を選択した場合に表示されます）。次のいずれかの認証タイプを選択します。 • [SHA]：HMAC-SHA に基づく認証 • [SHA256]：HMAC-SHA256 に基づく認証。 • [MD5]：HMAC-MD5 に基づく認証 （注） • MD5 認証タイプは推奨されません。 • ソフトウェア イメージ バージョン 17.14.1 以降のデバイスで MD5 認証タイプのみが設定されている場合、Catalyst Center はデバイスプロビジョニングをサポートしません。 MD5 認証を使用する場合は、Catalyst Center の SHA 認証も設定して、ソフトウェアイメージ 17.14.1 以降で実行されているデバイスを検出および管理することをお勧めします。
Privacy Type	使用するプライバシータイプ（このフィールドは、認証モードとして [Authentication and Privacy] を選択した場合に表示されます）。次のいずれかのプライバシータイプを選択します。 • [AES128]：暗号化の 128 ビット CBC モード AES。 • [AES192]：シスコのデバイス上での暗号化の 192 ビット CBC モード AES。 • [AES256]：シスコのデバイス上での暗号化の 256 ビット CBC モード AES。 • [DES]：CBC DES-56 規格に基づく認証に DES 56-bit 暗号化を追加。 （注） DES プライバシータイプは無効になっており、サポートされていません。

フィールド	説明
Auth Password	SNMPv3 を使用するデバイスから情報にアクセスする際に使用する SNMPv3 パスワード。（このフィールドは、認証モードとして [Authentication and Privacy] または [Authentication, No Privacy] を選択した場合に表示されます）。これらのパスワード（またはパスフレーズ）は、8 文字以上である必要があり、スペースや山カッコ（< >）は使用できません。 （注） • 一部のシスコ ワイヤレス コントローラでは、パスワード（あるいはパスフレーズ）は少なくとも 12 文字以上である必要があります。ワイヤレス コントローラのパスワードの最小要件を必ず確認してください。パスワードに必要な最低限の文字数が守られないと、デバイスではCatalyst Centerによる検出、監視、管理が行われなくなります。 • パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。
Privacy Password	DES または AES128 暗号化をサポートしているデバイスで交換されるメッセージを暗号化するための秘密鍵を生成するために使用される SNMPv3プライバシーパスワード。（このフィールドは、認証モードとして [Authentication and Privacy] を選択した場合に表示されます）。パスワード（またはパスフレーズ）は、8 文字以上である必要があり、スペースや山カッコ（< >）は使用できません。 （注） • 一部のシスコ ワイヤレス コントローラでは、パスワード（あるいはパスフレーズ）は少なくとも 12 文字以上である必要があります。ワイヤレス コントローラのパスワードの最小要件を必ず確認してください。パスワードに必要な最低限の文字数が守られないと、デバイスではCatalyst Centerによる検出、監視、管理が行われなくなります。 • パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。

ステップ 7 （任意） [Assign credential to site] チェックボックスをオンにして、選択したサイトに SNMPv3 ログイン情報を割り当てます。

ステップ 8 [Save] をクリックします。

成功メッセージが右下隅に表示されます。ログイン情報は、[Manage Credentials] スライドインペインで確認できます。ただし、サイトにログイン情報を割り当てなかった場合は、[System] フォーカスのみにログイン情報が表示されます。

グローバル HTTPS ログイン情報の追加

手順

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

ステップ 2 [Device Credentials] タブをクリックします。

ステップ 3 左側の階層ツリーから、サイトを選択します。

ステップ 4 次のいずれか 1 つのタスクを実行します。

- ログイン情報をまだ作成していない場合は、[Create Credentials] をクリックします。
- ログイン情報を作成済みの場合は、[Manage Credentials] をクリックします。

ステップ 5 [Manage Credentials] スライドインペインで、[Add] ドロップダウンリストから [HTTP(S) Read] または [HTTP(S) Write] を選択します。

ステップ 6 次の表を使用して、表示されるフィールドに入力します。

表 *43 : HTTP* および *HTTPS* クレデンシャル

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

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

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

ステップ 7 （任意） [Assign credential to site] チェックボックスをオンにして、選択したサイトに HTTPS ログイン情報を割り当てます。

ステップ 8 [Save] をクリックします。

成功メッセージが右下隅に表示されます。ログイン情報は、[Manage Credentials] スライドインペインで確認できます。ただし、サイトにログイン情報を割り当てなかった場合は、[System] フォーカスのみにログイン情報が表示されます。

デバイスログイン情報のサイトへの割り当て

グローバルデバイスログイン情報は、特定のサイトまたは階層内のすべてのサイトに割り当てることができます。[Global] を選択した場合、[Global] の下のすべてのサイトは、割り当てられたグローバルデバイスログイン情報を継承します。

手順

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

ステップ 2 [Device Credentials] タブをクリックします。

ステップ 3 左側の階層ツリーから目的のサイトを選択します。

ステップ 4 割り当てるグローバルデバイスログイン情報のタイプを見つけます。

ステップ 5 そのログイン情報に対応する [Assign] チェックボックスをオンにします。

ステップ 6 [Credential] ドロップダウンリストから、選択したサイトに割り当てるログイン情報を選択します。

ステップ 7 [Save] をクリックします。

確認ダイアログボックスが表示されます。次のいずれか 1 つのタスクを実行します。

- サイトのデバイスにデバイスログイン情報を適用する準備ができたら、[Yes] をクリックし、サイトのデバイスへのデバイスログイン情報の適用 （389 ページ） に進みます。
- サイトのデバイスにデバイスログイン情報を適用する準備ができていない場合は、[No] をクリックします。
- サイトにデバイスがない場合は、[OK] をクリックします。サイトにデバイスを追加した後で、サイトのデバイスにデバイスログイン情報を適用できます。

ステップ 8 サイトからデバイスログイン情報の割り当てを解除するには、次の手順を実行します。

1. 左側の階層ツリーから、必要なサイトを選択します。
2. 割り当てを解除するデバイスログイン情報の [Assign] チェックボックスをオフにします。
3. [Save] をクリックします。
4. 確認ダイアログボックスで、[Yes] をクリックして選択したサイトからのログイン情報の割り当て解除を続行するか、[No] をクリックして選択したサイトに割り当てられたログイン情報を保持します。

   [Yes] を選択すると、成功ダイアログボックスが表示され、更新されたサイトがサイトのデバイスに適用されているデバイスログイン情報と同期していない可能性があると表示されます。次のいずれか 1 つのタスクを実行します。

   - サイトのデバイスにデバイスログイン情報を適用する準備ができたら、[Yes] をクリックし、サイトのデバイスへのデバイスログイン情報の適用 （389 ページ） に進みます。
   - サイトのデバイスにデバイスログイン情報を適用する準備ができていない場合は、[No] をクリックします。
   - サイトにデバイスがない場合は、[OK] をクリックします。サイトにデバイスを追加した後で、サイトのデバイスにデバイスログイン情報を適用できます。

（注） サイトからデバイスログイン情報を割り当て解除しても、そのサイト内のすべてのデバイスに現在適用されているログイン情報は変更されません。サイト内のすべてのデバイスのデバイスログイン情報を更新するには、「デバイス上のデバイスログイン情報の更新（396ページ）」を参照してください。

グローバルデバイスログイン情報の管理

グローバルデバイスログイン情報は、[Manage Credentials] スライドインペインで管理できます。データのフォーカス（[Current site] または [System]）に応じて、特定のアクションを実行してグローバルデバイスログイン情報を管理できます。[Current site] フォーカスには、選択したサイトに割り当てられているグローバルデバイスログイン情報のみが表示されます。このフォーカスでは、現在選択されているサイトにのみグローバルデバイスログイン情報を追加して適用できます。[System] フォーカスには、システムのグローバルデバイスログイン情報のプールが表示されます。このフォーカスでは、グローバルデバイスログイン情報を追加、編集、および削除できます。また、このフォーカスから、階層内のすべてのサイトにデバイスログイン情報を適用できます。

サイトのデバイスへのデバイスログイン情報の適用

[Focus] ドロップダウンリストを使用すると、グローバルデバイスログイン情報をすべてのサイトまたは特定のサイトのデバイスに適用できます。[System] フォーカスを使用してデバイスログイン情報を適用する場合、Catalyst Center は、階層内のいずれかのサイトがこのデバイスログイン情報を使用するように割り当てられているかどうかを確認します。次に、それらのデバイスに変更をプッシュします。[Current site] フォーカスを使用してデバイスログイン情報を適用する場合、Catalyst Center は、現在選択されているサイトとその子サイトがこのデバイスログイン情報を使用するように割り当てられているかどうかを確認します。次に、それらのデバイスに変更をプッシュします。

デバイスクレデンシャルをすべてのサイトのデバイスまたは特定のサイトのデバイスに適用するには、次の手順を実行します。

（注） サイト内のデバイスに適用できるのは、CLI、SNMP v2c Read、SNMP v2c Write、および SNMPv3 クレデンシャルのみです。Catalyst Center は、サイト内のデバイスへの HTTPS 読み取りおよび HTTPS 書き込みログイン情報のアプリケーションをサポートしていません。

始める前に

（適用しようとしている）デバイスログイン情報が、必要なサイトに割り当てられていることを確認します。詳細については、デバイスログイン情報のサイトへの割り当て（387ページ）を参照してください。

手順

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

ステップ 2 [Device Credentials] タブをクリックします。

ステップ 3 左側の階層ツリーから、以下を選択します必要なサイトを選択します。

ステップ 4 [Manage Credentials] をクリックします。

ステップ 5 [Manage Credentials] スライドインペイン の [Focus] ドロップダウンリストから、フォーカス（[Current site] または [System]）を選択して、ログイン情報を適用する場所を定義します。

ステップ 6 ログイン情報に対応する [Actions] 列で、[...] にカーソルを合わせ、[Apply] を選択します。

ステップ 7 CLI クレデンシャルを適用する場合は、サイト内のデバイスにこのクレデンシャルを適用する方法を決定し、[Next] をクリックします。それ以外の場合はステップ 8 （391 ページ）に進みます。

次の場合は...	次の操作...
• [Push credential to devices] と [Verify authentication on devices] チェックボックスの両方をオンにするか、 • [Push credential to devices] チェックボックスをオンにし、[Verify authentication on devices] チェックボックスをオフにしている	Catalyst Center は、影響を受けるデバイスの CLI クレデンシャルをローカルで更新し（プロビジョニングと有効性検証の実行を含む）、影響を受けるデバイスのインベントリに保存されている CLI クレデンシャルを更新します。 （注） この設定の展開は、完了するまで時間がかかる場合があります。
[Push credential to devices] チェックボックスをオフにし、[Verify authentication on devices] チェックボックスをオンにしている	Catalyst Center は、影響を受けるデバイスでの認証のみを確認し、影響を受けるデバイスのインベントリに保存されている CLI クレデンシャルを更新します。 （注） この設定は、AAA または Cisco ISE 認証管理を使用しているデバイスに推奨されます。

次の場合は...	次の操作...
[Push credential to devices] と [Verify authentication on devices] チェックボックスの両方をオフにしている	Catalyst Center は、影響を受けるデバイスのインベントリに保存されている CLI クレデンシャルのみを更新します。 （注） • サイト内のデバイスが到達不能またはアクセス不能な場合にのみ、[Verify authentication on devices] チェックボックスをオフにします。 • [Verify authentication on devices] チェックボックスがオフで、影響を受けるデバイスに適用されたときに CLI クレデンシャルが正しくない場合、これらのデバイスは**[Provision]** > **[Inventory]** ウィンドウで [Unmanaged] 状態になることがあります。

ステップ 8 展開のためのタスクのスケジュールを設定します。

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

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

ステップ 9 [Tasks] ウィンドウで、タスクの展開を監視します。

デバイスログイン情報の適用の再スケジュール

（デバイスログイン情報をサイトのデバイスに適用する）デバイスログイン情報タスクを再スケジュールする場合は、次の手順を使用します。

手順

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

ステップ 2 [Device Credentials] タブをクリックします。

ステップ 3 次のいずれか 1 つのタスクを実行します。

- デバイスログイン情報を適用したときに [Current site] フォーカスを使用した場合は、デバイスログイン情報を適用したサイトと同じサイトを左側の階層ツリーから選択します。

- デバイスログイン情報を適用したときに[System]フォーカスを使用した場合は、ステップ4（392ページ）に進みます。

ステップ4 [Manage Credentials] をクリックします。

ステップ5 [Manage Credentials] スライドインペインの [Focus] ドロップダウンリストから、ログイン情報の適用に使用したのと同じフォーカスを選択します。

ステップ6 [Manage Credentials] テーブルで、再スケジュールするスケジュールされたアプリケーションがあるログイン情報を見つけます。

ステップ7 デバイスログイン情報の対応する [Actions] 列で、[...] にカーソルを合わせ [Reschedule] を選択します。

（注） [Reschedule] が表示されず、代わりに [Apply] が表示されている場合は、デバイスログイン情報のスケジュールされたアプリケーションで選択したのと同じフォーカスと同じサイトを選択していることを確認します。[Apply] をクリックすると、新しいタスクが作成されますが、既存のタスクは再スケジュールされません。

ステップ8 タスクの日時を再スケジュールし、[Apply] をクリックします。

（注） タイムゾーンは変更できません。

デバイスログイン情報が正常に再スケジュールされたことを示す成功メッセージが右下隅に表示されます。

デバイスログイン情報のステータスの表示

[Current site] で [Manage Credentials] スライドインペインにフォーカスすると、デバイスログイン情報のステータスを確認できます。

手順

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

ステップ2 [Device Credentials] タブをクリックします。

ステップ3 左側の階層ツリーから、以下を選択します必要なサイトを選択します。

ステップ4 [Manage Credentials] をクリックします。

ステップ5 [Manage Credentials] スライドインペインで、[Focus] ドロップダウンリストから [Current site] を選択します。

ステップ6 [Manage Credentials] テーブルで、関連するログイン情報を見つけます。

ステップ7 ログイン情報の対応する [Status] 列で、ログイン情報のステータスを表示します。

次のいずれかのステータスが表示されます。

- [Synced]：選択したサイトに割り当てられたデバイスログイン情報が、選択したサイトのデバイスに適用されているデバイスログイン情報と一致します。
- [Not Synced]：選択したサイトに割り当てられたデバイスログイン情報が、選択したサイトのデバイスに適用されているデバイスログイン情報と一致しません。
- [Date and time]：デバイスログイン情報の適用がスケジュールされた日時です。例：2024 年 2 月 1 日、午前 9 時。
- [Partial Success]：デバイスログイン情報の適用が部分的に成功しました。
- [Failed]：Catalyst Center は、選択したサイトに割り当てられている少なくとも 1 つのデバイスにデバイスログイン情報を適用できませんでした。
- [Not Applicable]：デバイスログイン情報は、いずれのサイトのデバイスでもサポートされていません。
- [--]：サイトにデバイスがないか、子サイトで同じログイン情報タイプの別のログイン情報が使用されているため、デバイスログイン情報を適用できません。

ログイン情報のステータスにカーソルを合わせると詳細が表示されます。

ヒント システムの最新ステータスを表示するには、テーブルの右上隅にある更新アイコンをクリックします。

ステップ 8 または、**[Provision]** > **[Inventory]** ウィンドウに移動します。

[ログイン情報ステータス（Credential Status）] 列に、次のいずれかのステータスが表示されます。

- [Success]：Catalyst Center がログイン情報の変更を正常に適用しました。
- [Failed]：Catalyst Center がログイン情報の変更を適用できませんでした。失敗したログイン情報の変更と失敗理由に関する詳細を表示するには、[See Details] をクリックします。
- [Not Applied]：選択したサイトのデバイスに適用されたデバイスログイン情報が、選択したサイトに割り当てられたデバイスログイン情報と一致しません。
- [Not Applicable]：デバイスログイン情報をデバイスタイプに適用できません。

複数のクレデンシャル（CLI、SNMP、HTTPS など）を編集して保存した場合、 Catalyst Center がいずれかのクレデンシャルを適用できなかったときには、[クレデンシャルステータス（Credential Status）] 列に [失敗（Failed）] と表示されます。失敗したログイン情報の変更に関する詳細を表示するには、[See Details] をクリックします。

グローバルデバイスログイン情報の編集のガイドライン

既存のグローバルデバイスログイン情報の編集に関するガイドラインと制約事項は、次のとおりです。

- Catalyst Center は、次のプロセスが使用してグローバルデバイス ログイン情報を編集、保存、および適用します。

  1. Catalyst Center からローカル認証を持つデバイスにログイン情報がプッシュされます。ローカル認証では、ログイン情報の変更が適用され、Catalyst Center はこれらのログイン情報を使用してデバイスを管理します。

     （AAA サーバーが継承または設定されたサイトにあるデバイスには、Catalyst Center から CLI ログイン情報の変更はプッシュされません。AAA 認証では、ログイン情報の変更は適用されません。Catalyst Center は、同じログイン情報が AAA サーバーに存在する場合にのみ、これらのログイン情報を使用してデバイスを管理します）

  2. クレデンシャルがデバイスに正常にプッシュされると、Catalyst Center は新しいクレデンシャルを使用してデバイスに到達できることを確認します。

（注） この手順に失敗すると、Catalyst Center が新しいクレデンシャルをデバイスにプッシュしていても、インベントリでは古いクレデンシャルを使用してデバイスが管理されます。この場合、既存のログイン情報を更新すると、**[Provision]** > **[Inventory]** ウィンドウでデバイスが管理対象外であると示される可能性があります。

  3. 新しいクレデンシャルを使用してデバイスに正常に到達すると、Catalyst Center のインベントリは、新しいクレデンシャルを使用してデバイスの管理を開始します。

- サイトには、SNMPv2c クレデンシャルと SNMPv3 クレデンシャルを使用するデバイスを含めることができます。SNMPv2c または SNMPv3 のグローバルクレデンシャルを編集、保存、および適用すると、Catalyst Center はその変更をデバイスにプッシュし、そのクレデンシャルを有効にします。たとえば、SNMPv2c を使用するデバイスがあるのに、SNMPv3 のグローバルクレデンシャルを編集、保存、および適用すると、Catalyst Center は関連付けられたサイトのすべてのデバイスに新しい SNMPv3 のクレデンシャルをプッシュして、そのクレデンシャルを有効にします。つまり、以前は SNMPv2c が有効になっていたデバイスを含め、すべてのデバイスが SNMPv3 を使用して管理されるようになります。
- 混乱が生じないようにするために、CLI ログイン情報を編集する際は [User Name] を変更してください。これにより、新しい CLI クレデンシャルが作成され、既存の CLI クレデンシャルは変更されません。

グローバル デバイス クレデンシャルの編集

準備が整うまで、Catalyst Center でクレデンシャルの変更を適用せずに、グローバル デバイス クレデンシャルを編集および保存できます。（デバイスログイン情報の適用に関する詳細は、「サイトのデバイスへのデバイスログイン情報の適用（389ページ）」を参照してください）。以前にサイトのデバイスに適用されたデバイスログイン情報を編集すると、このデバイスログイン情報を使用するすべてのサイトのデバイスログイン情報ステータスに、[Not Synced] と表示されます。このステータスが表示されるのは、サイトに割り当てられたデバイスログイン情

報が、そのサイトのデバイスに適用されているデバイスログイン情報と一致しなくなったためです。

手順

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

ステップ 2 [Device Credentials] タブをクリックします。

ステップ 3 [Manage Credentials] をクリックします。

ステップ 4 [Manage Credentials] スライドインペインで、[Focus] ドロップダウンリストから [System] を選択します。

ステップ 5 [Manage Credentials] テーブルで、編集するログイン情報を見つけます。

ステップ 6 ログイン情報に対応する [Actions] 列で、[...] にカーソルを合わせ、[Edit] を選択します。

ステップ 7 確認ダイアログボックスで、[OK] をクリックして、このログイン情報の編集を続行します。

（注） このログイン情報が他のサイトに割り当てられている場合、このログイン情報を変更すると、それらのサイトが影響を受けます。

ステップ 8 スライドインペイン で、必要な変更を行い、[Save] をクリックします。

デバイスのログイン情報が正常に更新されたことを示す成功メッセージが右下隅に表示されます。

（注） CLI パスワードログイン情報には、*ASCII* 印刷可能文字（文字コード 32 ー 127。https://en.wikipedia.org/wiki/ASCII#Printable_characters を参照）だけを使用できます。

デバイスログイン情報の削除

デバイスログイン情報を削除する場合は、まず、デバイスログイン情報がサイトに割り当てられていないか確認します。どのサイトにも割り当てられていない場合は、[System] フォーカスを使用して、システムのグローバルデバイスログイン情報のプールからデバイスログイン情報を削除できます。サイトに割り当てられている場合は、最初に、使用しているすべてのサイトからデバイスログイン情報の割り当てを解除するか、使用しているサイトを削除する必要があります。その後、システムのグローバルデバイスログイン情報のプールからデバイスログイン情報を削除できます。

（注） デバイスログイン情報を削除しても、システムのグローバルデバイスログイン情報のプールから削除されるだけです。Catalyst Center はデバイスからログイン情報を削除しません。

始める前に

削除するデバイスログイン情報がいずれかのサイトに割り当てられている場合は、まず、そのデバイスログイン情報を使用しているすべてのサイトから割り当てを解除するか、使用しているサイトを削除する必要があります。詳細については、デバイスログイン情報のサイトへの割り当て （387 ページ）のサイトの作成、編集、削除 （285 ページ）またはステップ 8 （388 ページ）を参照してください。

手順

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

ステップ 2 [Device Credentials] タブをクリックします。

ステップ 3 [Manage Credentials] をクリックします。

ステップ 4 [Manage Credentials] スライドインペインで、[Focus] ドロップダウンリストから [System] を選択します。

ステップ 5 [Manage Credentials] テーブルで、削除するログイン情報を見つけます。

ステップ 6 ログイン情報の対応する [Actions] 列で、[...] にカーソルを合わせ [Delete] を選択します。

ステップ 7 [Warning] ダイアログボックスで、[Yes] をクリックします。

デバイスログイン情報が正常に削除されたことを示す成功メッセージが右下隅に表示されます。

デバイス上のデバイスログイン情報の更新

デバイスログイン情報がサイトから割り当て解除されても、そのサイトのデバイスに現在適用されているログイン情報は自動的に更新されません。デバイスは、新しいログイン情報が適用されるまで既存のログイン情報を保持するため、デバイスは常にログイン情報が設定された状態となります。次の大まかな手順を使用することで、サイト内のすべてのデバイスのデバイスログイン情報を更新できます。

手順

ステップ 1 必要なサイトからデバイスログイン情報の割り当てを解除します。デバイスログイン情報のサイトへの割り当て （387 ページ）のステップ 8 （388 ページ）を参照してください。

ステップ 2 新しいデバイスログイン情報を同じサイトに割り当てます。デバイスログイン情報のサイトへの割り当て （387 ページ）を参照してください。

または、[Device Credentials] ウィンドウで [Save] をクリックして、割り当て解除と割り当てを一度に行うこともできます。

ステップ 3 そのサイトのデバイスに新しいデバイスログイン情報を適用します。サイトのデバイスへのデバイスログイン情報の適用 （389 ページ）を参照してください。

ステップ 4 または、デバイスにログインして、デバイスログイン情報を手動で更新することもできます。

IP アドレスプールを設定する

Catalyst Center IPv4 と IPv6 のデュアルスタック IP プールがサポートされています。

IPv4 および IPv6 アドレスプールは手動で設定できます。

グローバルレベルで IPv6 専用プールを作成し、サイトレベルで予約できます。

Catalyst Center を外部 IP アドレス マネージャと通信するように設定することもできます。詳細については、*Cisco Catalyst Center Administrator Guide*を参照してください。

手順

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

ステップ 2 [IPプールの追加（Add IP Pool）] をクリックし、[IPプールの追加（Add IP Pool）] スライドインペインの必須フィールドすべてに入力します。

- [IPプール名（IP Pool Name）]：IP アドレスプールの一意の名前。
- [Type]：IP アドレスプールのタイプ。
  - [LAN]：該当するアンダーレイの LAN インターフェイスに IP アドレスを割り当てる場合に使用します。LAN 自動化では、このオプションを選択します。
  - [管理（Management）]：管理インターフェイスに IP アドレスを割り当てる場合に使用します。
  - [サービス（Service）]：サービスインターフェイスに IP アドレスを割り当てる場合に使用します。
  - [WAN]：WAN インターフェイス IP アドレスを割り当てる場合に使用します。
  - [トンネル（Tunnel）]：IPsec トンネリングのためにサイト間 VPN に IP アドレスを割り当てる場合に使用します。
  - [Generic]：他のすべてのネットワークタイプで使用されます。
- [IPアドレス空間（IP Address Space）]：[IPv4] または [IPv6] を選択してアドレスプールを作成します。
- [IPサブネット（IP Subnet）]：プールが管理と割り当てを行う IP アドレスの範囲と構造を指定します。
- [プレフィックス長（Prefix length）]：グローバル IP アドレスプールまたは IP アドレスの数のすべてか一部を予約するために使用する IP サブネットとマスクアドレス。
- [Gateway]：ゲートウェイ IP アドレス。
- [DHCP Server(s)]：この IP プールに関連付けられている DHCP サーバーの IP アドレス。
- [DNS Server(s)]：このIPプールに関連付けられているDNSサーバーのIPアドレス。

Catalyst Center が外部の IP アドレスマネージャと通信するように設定した場合、外部 IP アドレスマネージャの既存の IP アドレスプールと重複する IP プールを作成することはできません。

ステップ 3 [Save] をクリックします。

新しく追加されたプールが [IP Address Pools] テーブルに表示されます。[Subnet Type] エリアで [IPv4] タブまたは [IPv6] タブをクリックすると、IPv4 または IPv6 のアドレスプールのみを表示できます。



（注） IP アドレスプールを編集して、DHCP を変更すると、その IP アドレスプールを使用してデバイスを再設定する必要はありません。ただし、ファブリックデバイスが更新された IP アドレスプールを使用する場合は、デバイスが関連付けられているファブリックを再設定する必要があります。 詳細については、ファブリックの再設定 （1246 ページ）を参照してください。

IP アドレスマネージャからの IP アドレスプールのインポート

Bluecat または Infoblox から IP アドレスプールをインポートできます。



（注） IP アドレスプールはサブプールまたは割り当てられた IP アドレスを持つことはできません。

外部 IP アドレスマネージャ（IPAM）と通信するには Catalyst Center を設定する必要があります。詳細については、*Cisco Catalyst Center Administrator Guide*を参照してください。

手順

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

ステップ 2 [Import] ドロップダウンリストから [Import from IPAM Server] を選択します。

ステップ 3 スライドインペイン で CIDR を入力し、[Retrieve] をクリックして、インポートできる IP プールのリストを取得します。

ステップ 4 [Select All] をクリックするか、インポートする IP アドレスプールを選択します。

ステップ 5 [Import] をクリックします。

プールはグローバルサイトにインポートされます。

CSV ファイルからの IP アドレスプールのインポート

CSV ファイルから IP アドレスプールをインポートできます。

手順

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

ステップ 2 [Import] ドロップダウンリストから [Import from CSV File] を選択します。

ステップ 3 [Download sample template] をクリックして最新のサンプルファイルをダウンロードします。

ステップ 4 ファイルに IP アドレスプールを追加して、ローカルマシンにファイルを保存します。

ステップ 5 次のアクションのいずれかを実行して、CSV ファイルをアップロードします。

a) ドラッグ アンド ドロップ エリアにファイルをドラッグアンドドロップします。

b) [Choose a file] をクリックし、ローカルマシンからファイルを選択します。

ステップ 6 [Import] をクリックします。

プールはグローバルサイトにインポートされます。

IP アドレスプールの予約

始める前に

グローバルサイトで 1 つまたは複数の IP アドレスプールが作成されていることを確認します。

手順

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

ステップ 2 左側の階層ツリーから、以下を選択します必要なサイトを選択します。

ステップ 3 [Reserve IP Pool] リンクをクリックします。

ステップ 4 [Reserve IP Pool] スライドインペインで以下のフィールドに入力し、使用可能なグローバル IP アドレスプールのすべてまたは一部を特定のサイト用に予約します。

- [IP プール名（IP Pool Name）]：予約済み IP アドレスのプールの一意の名前。
- [Type]：IP アドレスプールのタイプ。
  - [LAN]：該当するアンダーレイの LAN インターフェイスへの IP アドレスの割り当てを目的としています。LAN 自動化では、このオプションを選択します。
  - [Management]：IP アドレスを管理インターフェイスに割り当てます。
  - [Service]：IP アドレスをサービスインターフェイスに割り当てます。
  - [WAN]：IP アドレスを WAN インターフェイスに割り当てます。

- [Generic]：他のすべてのネットワークタイプで使用されます。 これがデフォルトのオプションです。

- [IP Address Space]：[IPv4] または [IPv6] チェックボックスをオンにしてアドレスプールを作成します。デュアルスタックプールを作成するには、[IPv4] と [IPv6] の両方のチェックボックスをオンにします。デフォルトでは、[IPv4] のチェックボックスはオンになっています。
- [Global Pool]：プールを予約するアドレスプールを選択します。検索フィールドにテキストを入力して、ドロップダウンリストに表示される結果を絞り込めます。
- [Prefix length / Number of IP Addresses]：予約するプールの選択方法を次から指定します。

実行する操作	結果...
特定の IP ルートプレフィックスでプールを予約し、	**1.** [Prefix length] ラジオボタンをクリックします。 **2.** ドロップダウンリストから適切なプレフィックス長の値を選択します。 **3.** [IPv4 Subnet] / [IPv6 Subnet] フィールドに、使用するサブネットアドレスを入力します。
特定の数を含むプールを予約し、	**1.** [Number of IP Addresses] ラジオボタンをクリックします。 **2.** [Total host] フィールドに、予約するプールのサイズを入力します。

IPv6 IP アドレスプールのプレフィックス長として [/64] を選択すると、[SLAAC Support] チェックボックスが表示され、デフォルトでオンになっています。このオプションが選択されている場合、デバイスは DHCP サーバーを必要とせずに、自動的に IP アドレスを獲得します。

- [Gateway]：ゲートウェイ IP アドレス。 このフィールドは、[Prefix length] ラジオボタンが選択されている場合にのみ表示されます。
- [Overlapping]：このプールの CIDR サブネットに対して重複を有効にするかどうかを指定します。

状況	結果...
このプールのサブネットと重複する IP プールの作成を許可しない場合は、	[Off] ラジオボタンがすでに選択されていることを確認してください。これはデフォルト設定です。

状況	結果...
このプールの CIDR サブネットの使用を許可する場合は、	**1.** [On] ラジオボタンをクリックします。 **2.** 使用するアドレス空間識別子を指定します。[Create new] ラジオボタンをクリックして識別子を入力するか、[Select existing] ラジオボタンをクリックしてドロップダウンリストから識別子を選択します。 **重要** 新しいアドレス空間識別子の名前を入力する場合は、注意してください。後で名前を変更することはできません。

- [DHCP Server(s)]：この IP プールに関連付けられている DHCP サーバーの IP アドレス。
- [DNS Server(s)]：このIPプールに関連付けられているDNSサーバーのIPアドレス。

ステップ 5 [予約（Reserve）] をクリックします。

重要 IPv4 と IPv6 の両方のアドレスプールを予約している場合（ファブリックがデュアルスタック IP プールでプロビジョニングされている場合）で、IPv6 プールがすでに VN に接続されているときは、シングルスタック IPv4 プールに戻すことはできません。

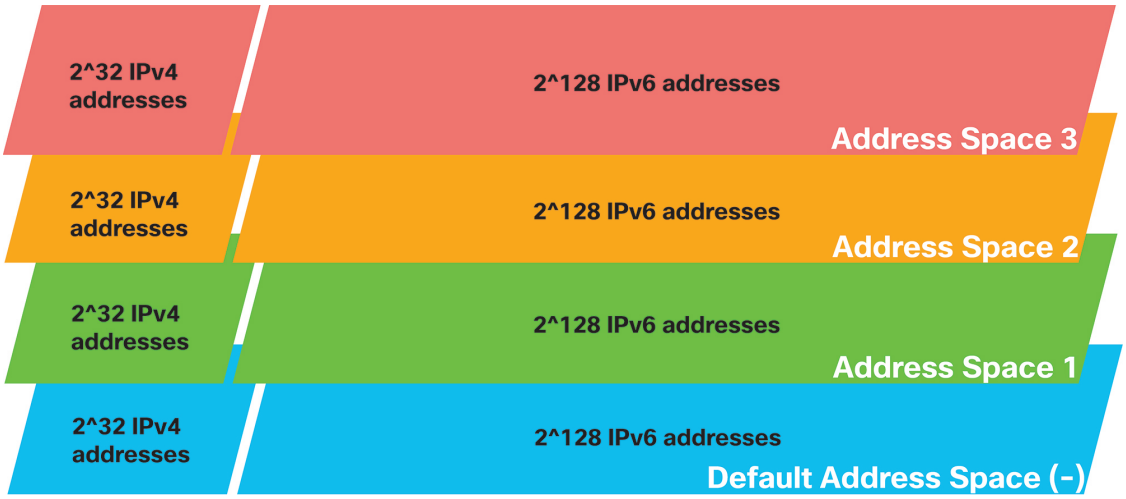
ただし、IPv6 プールが VN に接続されていない場合は、次の手順を完了することでシングルスタック IPv4 プールにダウングレードできます。

1. [IP Address Pools] ページの [Actions] 列で、省略記号アイコン（ ••• ）にカーソルを合わせ、[Edit] をクリックします。
2. **[Edit IP Pool]** スライドインペイン で、**[IPv6]** チェックボックスをオフにします。
3. [Save] をクリックします。

IP アドレスプールをオーバーラップ

Catalyst Center 3.1.5 では CIDR の重複がサポートされています。これにより、IP アドレスを動的に割り当てる場合の柔軟性が向上します。この機能を使用すると、重複する IP アドレスプールを設定して、図 22 : CIDR の重複 （402 ページ） に示されているように、異なるアドレス空間を作成できます。

図 *22 : CIDR* の重複



Catalyst Center 3.1.5 にアップグレードすると、すべての IP アドレスプールがデフォルトのアドレス空間に配置されます。デフォルトでは、新しく作成されたすべての IP プールはデフォルトアドレス空間に配置されます。各プールは単一のアドレス空間にマッピングされ、デフォルトで重複が無効になっています。アドレスプールが作成された後の任意の時点で、重複を有効または無効にできます。ただし、そのアドレスは展開のグローバルサイトより下のレベルに存在します。有効にすると、アドレスプールは、異なるアドレス空間間で（部分的または完全に）重複します。

Cisco SD-Access 環境での重複

Cisco SD-Access 環境では、IPAM サービスの IP プール コンテキスト テーブルにプッシュされる SDA_OVERLAP コンテキストキーを中心に重複が構築されます。Cisco SD-Access は、IPAM エンドポイントをクエリして、このキーに基づいて重複をフィルタ処理によって除外します。

IP プールには、主に次の 2 つのタイプのコンテキスト値がプッシュされます。

- SDA_VN_{VN_NAME}：この値により、異なる VN 間での IP プールの重複が可能になります。
- SDA_GLOBAL：この値は、関連付けられた IP プールの重複が許可されていないことを示します。

外部 IPAM 統合

重複する IP アドレスプールのサポートは、Infoblox と BlueCat という 2 つの外部 IP アドレス管理（IPAM）システムと統合されました。Catalyst Center のアドレススペースは、Infoblox Network Views と BlueCat Configurations にマッピングされます。外部 IPAM システムの Catalyst Center によって作成される Network Views または Configurations の名前は、*Cisco_Overlap_<address space identifier>* の形式に従います。*Cisco_Overlap_* は、Catalyst Center で使用されるアドレス空間識別子の前に付加されます。

Catalyst Center は、汎用 IPAM インターフェイスを介して Catalyst Center と統合された重複する IP アドレスプールの使用をサポートしていません。

以前の IPAM 統合では、プロビジョニングアプリケーション（LAN Automation および SD-Access）でプールから同じ IP アドレスを複数回割り当てることができました。この機能は、IPAM ユーザーインターフェイスには表示されません。サードパーティの IPAM が統合されている場合は、そのアプリケーションのユーザーインターフェイスから表示できます。

次に例を示します。

- Infoblox では、*CISCO_DNACenter-* で始まる名前の新しいネットワークビューが作成されます。
- BlueCat では、*CISCO-DNACenter-* で始まる名前の新しい設定が作成されます。

これらのネットワークビューと設定には、重複する IP プールと重複する IP アドレスが含まれています。

重複する IP アドレスプールに関する注意事項と要件

一般

- IP アドレスプールは、異なるアドレス空間で重複する場合があります。同じアドレス空間内で重複することはありません。
- 重複は、Catalyst Center の展開のグローバルサイトより下のレベルに存在する IP アドレスプールに対してのみ有効にできます。
- アドレス空間識別子の名前は、作成後に変更できません。
- 重複が有効になっていない IP アドレスプールは、任意のアドレス空間に存在できます。
- IP アドレスプールを作成または編集する際、デフォルト以外のアドレス空間を選択または作成できます。これらのアドレス空間の ID は一意である必要があります。アドレス空間の ID には、英数字のほか、ハイフン、下線を含めることができます。ただし、ID をハイフンまたは下線で開始することはできません。
- IP アドレスプールを作成すると、そのアドレス空間の割り当ては固定され、変更できません。

Cisco SD-Access

特定の機能の組み合わせで IP アドレスプールの重複がサポートされているかどうかを判断するには、この表を使用します。

機能	Segment	マルチキャスト	レイヤ 3 ハンドオフ	エクストラネット	LISP/BGP Cisco SD-Access トランジットを介して接続されているサイト
Segment	異なる VN 上	異なる VN 上	重複なし	重複なし	接続されたサイト間の重複なし
マルチキャスト	異なる VN 上	異なる VN 上	重複なし	重複なし	接続されたサイト間の重複なし
インフラストラクチャ VN	重複なし	重複なし	重複なし	重複なし	重複なし
レイヤ 3 ハンドオフ	重複なし	重複なし	重複なし	重複なし	重複なし
エクストラネット	重複なし	重複なし	重複なし	重複なし	重複なし
LISP/BGP Cisco SD-Access トランジットを介して接続されているサイト	接続されたサイト間の重複なし	接続されたサイト間の重複なし	重複なし	重複なし	接続されたサイト間の重複なし

重複する IP アドレスプールの障害対応

このトピックでは、Catalyst Center の展開内で重複する IP アドレスプールが設定されている場合に発生する可能性のある問題をトラブルシュートする方法について説明します。

一般

- IPAM サービスログは、重複する問題が発生した場合の主要な障害対応リソースです。
- 重複が無効になっているアドレスプールと競合する新しい重複 IP アドレスプールを作成すると、問題が発生する可能性があります。
- 既存の IP アドレスプールが UI に表示される場合、アプリケーションのプロビジョニングで許可されている場合は、その重複設定を変更できます。

- 重複が無効になっている一部の IP アドレスプールは、アプリケーションをプロビジョニングするための子プールであり、適切に動作するために重複しないようにする必要があるため、非表示になる場合があります。

Cisco Software-Defined Access

- Catalyst Center がまだ予約されていないサブネットと IP アドレスプールを検証する場合は、次の手順を実行します。
  - 次の SQL クエリを実行して、SDA_OVERLAP コンテキストがまだ含まれている未使用のプールを確認します（問題の原因となる可能性があるため）。

```
SELECT *
FROM   ippoolcontext
WHERE  contextkey='SDA_OVERLAP' <= This outer query is finding all SDA_OVERLAP
context pushed
AND    ipaddresspoolinfo_id IN
       (
              SELECT id
              FROM   ipaddresspoolinfo
              WHERE  usedpercentage = '0'); <= this inner query is finding all
pools who have 0% ussage
```

  - 次のテーブルから情報を収集します。ipaddresspoolinfo、ippoolcontext、および ippoolgroupinfo。

- SPF ログファイルで、トレーサビリティに関する次の項目を確認します。
  - すべての VN で重複する IP プールの検証
  - CIDR の重複
  - レポート対象の重複する CIDR がないこと
  - cfsPoolOverlapCheck

IP アドレスプールの編集

手順

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

ステップ 2 左側の階層ツリーから、以下を選択します必要なサイトを選択します。

ステップ 3 すべての IP アドレスプールを一括で編集するには、次の手順を実行します。

a) **[More Actions]** ドロップダウンリストから、**[Edit all]** を選択します。

b) [Warning] ダイアログボックスで、[Yes] をクリックします。

c) **[Edit IP Pool]** スライドインペイン で必要な変更を行い、**[Save]** をクリックします。

ステップ 4 特定の IP アドレスプールのみを編集するには、次の手順を実行します。

a) 目的の IP アドレス プールの横にあるチェックボックスをオンにします。
b) [その他のアクション（More Actions）] ドロップダウン リストから [編集（Edit）] を選択します。

または、**[Actions]** 列で省略記号アイコン（ ••• ）にカーソルを合わせ、選択した IP アドレスプールのいずれかの **[Edit]** をクリックします。

c) **[Edit IP Pool]** スライドインペイン で必要な変更を行い、**[Save]** をクリックします。

次のタスク

更新された IP アドレスプールがファブリックネットワークで使用されている場合は、**[Provision]** > **[Fabric Sites]** ウィンドウで対応するファブリックを再設定する必要があります。詳細については、ファブリックの再設定 （1246 ページ）を参照してください。

IP アドレスプールの削除

手順

ステップ 1 メインメニューから次を選択します。**[Design]** > **[Network Settings]** > **[IP Address Pools]** の順に選択します。
ステップ 2 左側の階層ツリーから目的のサイトを選択します。
ステップ 3 すべての IP アドレスプールを一括で削除するには、次の手順を実行します。
a) [More Actions] ドロップダウンリストから [Delete all] を選択します。
b) [Warning] ダイアログボックスで、[Yes] をクリックします。
ステップ 4 特定の IP アドレスプールのみを削除するには、次の手順を実行します。
a) 目的の IP アドレス プールの横にあるチェックボックスをオンにします。
b) [More Actions] ドロップダウンリストから [Delete] を選択します。

または、[Actions] 列で省略記号アイコン（ ••• ）にカーソルを合わせ、選択したいずれかの IP アドレスプールの [Delete] をクリックします。

c) [Warning] ダイアログボックスで、[Yes] をクリックします。

IP アドレスプールの複製

サイトレベルで既存の IP アドレスプールを複製できます。IP アドレスプールを複製すると、DHCP サーバーと DNS サーバーの IP アドレスが自動的に入力されます。

手順

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

ステップ 2 左側の階層ツリーから目的のサイトを選択します。

ステップ 3 目的の IP アドレスプールを見つけ、[Actions] エリアで [Clone] をクリックします。

ステップ 4 [IPプールの複製（Clone IP Pool）] ウィンドウで、次の手順を実行します。

a) 必要に応じて、プール名を編集します（タイプ、IP アドレス空間、またはグローバルプール値は、複製元のプールから継承されるため編集できません）。

b) 必要に応じて、CIDR プレフィックス値を編集します。

c) [Clone] をクリックします。

IP アドレスプールのリリース

サイトレベルで予約されているシングルスタックおよびデュアルスタックプールをリリースできます。

手順

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

ステップ 2 左側の階層ツリーから目的のサイトを選択します。

ステップ 3 すべての IP アドレスプールを一括でリリースするには、次の手順を実行します。

a) [その他のアクション（More Actions）] ドロップダウンリストから、[すべてをリリース（Release all）] を選択します。

b) [Warning] メッセージで [Yes] をクリックします。

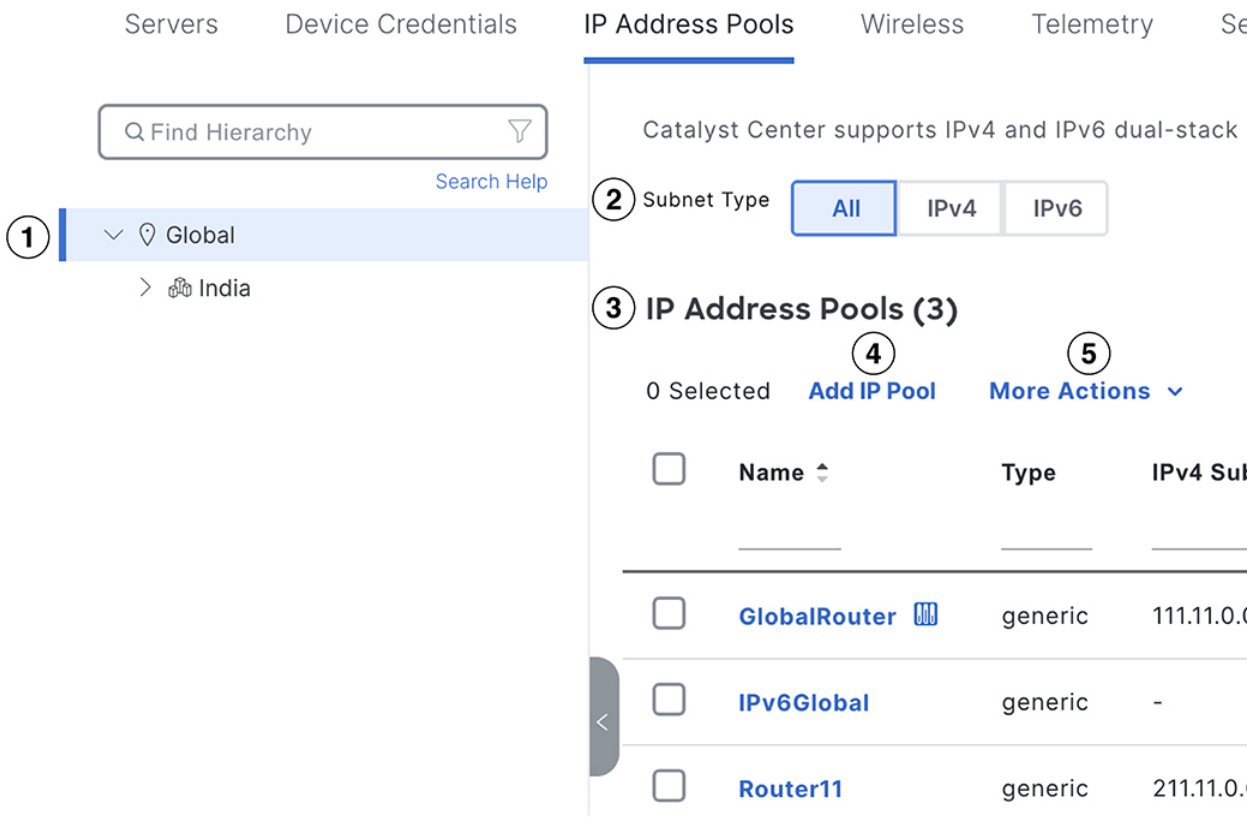
ステップ 4 目的の IP アドレスプールのみをリリースするには、次の手順を実行します。

a) 目的の IP アドレスプールを選択し、[その他のアクション（More Actions）] ドロップダウンリストから [リリース（Release）] をクリックします。

b) [Warning] メッセージで [Yes] をクリックします。

IP アドレスプールの表示

[IPアドレスプール（IP Address Pools）] ページでは、Catalyst Center の展開用に設定されている IP アドレスプールを表示できます。



このページに表示される項目は、（以下で説明されているように）左側の階層ツリーでネットワーク全体を選択するか、特定のサイトを選択するかによって異なります。

表 *44 : [IP*アドレスプール（*IP Address Pools***）*]* ページの要素**

引き出し線	説明
1	左側の階層ツリー：ここでは、ネットワーク全体の IP アドレスプール情報を表示するのか、特定のサイトの IP アドレスプール情報を表示するのかを選択できます。
2	[サブネットタイプ（Subnet Type）] エリア：ここでは、設定された IP バージョンで表示される IP アドレスプールをフィルタ処理できます。

引き出し線	説明
3	

引き出し線	説明
	[IPアドレスプール（IP Address Pools）] テーブル：このテーブルには、設定した IP アドレスプールの一覧と次の情報が表示されます。 • 名前：アドレスプールの名前をクリックすると、そのプールの詳細情報（マッピングされているグローバル/ネットワークレベルのアドレスプールやそのDHCP サーバーの IP アドレスなど）を示すスライドインペインが開きます。 • Type • IPv4 および IPv6 サブネット • 現在使用されている IPv4 および IPv6 アドレスの割合 （注） アドレスプールが使用可能な IP アドレスをどのように使用しているのかを示すポップアップウィンドウを開くには、情報（[i]）アイコンをクリックします。 アドレスプールの重複が有効になっている場合、ポップアップウィンドウには設定されている重複の数も示されます。[重複の詳細の表示（View Overlapping details）] リンクをクリックすると、各アドレス空間の割り当て済み IP アドレスと未割り当て IP アドレスの割合を一覧表示するスライドインペインが開きます。 • 重複が有効かどうかの表示（この列は、左側の階層ツリーでサイトが選択された場合にのみ表示されます） • アドレス空間識別子： • この列は、左側の階層ツリーでサイトが選択された場合にのみ表示されます。 • ハイフンは、アドレスプールがデフォルトアドレス空間内に存在することを示します。 • アドレスプールの継承元のサイト： • この列は、左側の階層ツリーでサイトが選択された場合にのみ表示されます。 • アドレスプールが選択したサイトによって予約済みの場合、値は表示されません。 [アクション（Actions）] 列の省略記号（[...]）にカーソルを合わせ、対応するアドレスプールに対する次のいずれかの操作を開始できます。 • [編集（Edit）]：詳細については、「IP アドレスプールの編集 （405 ページ）」を参照してください。

引き出し線	説明
	• [削除（Delete）]：このオプションは、左側の階層ツリーでネットワーク全体が選択されている場合にのみ表示されます。詳細については、「IP アドレスプールの削除 （406 ページ）」を参照してください。 • [複製（Clone）]：このオプションは、左側の階層ツリーでサイトが選択されている場合にのみ表示されます。詳細については、「IP アドレスプールの複製（406 ページ）」を参照してください。 • [解放（Release）]：このオプションは、左側の階層ツリーでサイトが選択されている場合にのみ表示されます。詳細については、IP アドレスプールのリリース （407 ページ） を参照してください。
4	• [IPプールの追加（Add IP Pool）] リンク：このリンクは、左側の階層ツリーでネットワーク全体が選択されている場合に表示されます。リンクをクリックして [IPプールの追加（Add IP Pool）] スライドインペインを開き、新しい IP アドレスプールの設定を構成します。 詳細については、「IP アドレスプールを設定する （397 ページ）」を参照してください。 • [IPプールの予約（Reserve IP Pool）]：このリンクは、左側の階層ツリーでサイトが選択されている場合に表示されます。リンクをクリックして [IPプールの予約（Reserve IP Pool）] スライドインペインを開き、予約する IP アドレスプールの設定を指定します。 詳細については、IP アドレスプールの予約 （399 ページ）を参照してください。

引き出し線	説明
5	[その他のアクション（More Actions）] ドロップダウンリスト：このドロップダウンリストをクリックして、次のいずれかのアクションを実行します。 • [編集（Edit）]：このオプションを選択して [IPプールの編集（Edit IP Pool）] スライドインペインを開き、選択した IP アドレスプールに変更を加えます。 詳細については、「IP アドレスプールの編集 （405 ページ）」を参照してください。 （注） 次の設定は固定されており、更新できません。 • Type • IP アドレス空間 • IP サブネット • プレフィックス長 • [削除（Delete）]：このオプションは、左側の階層ツリーでネットワーク全体が選択されている場合に表示されます。選択済みの IP アドレスプールを削除するには、このオプションを選択します。 詳細については、「IP アドレスプールの削除 （406 ページ）」を参照してください。 • [解放（Release）]：このオプションは、左側の階層ツリーでサイトが選択されている場合に表示されます。このサイトによって現在予約されている選択済みの IP アドレスプールを解放するには、このオプションを選択します。 詳細については、「IP アドレスプールのリリース （407 ページ）」を参照してください。 • [すべて編集（Edit all）]：設定済みのすべての IP アドレスプールを一括編集するには、このオプションを選択します。アドレスプールで使用される DHCP および DNS サーバーを更新できます。 • [すべて削除（Delete all）]：このオプションは、左側の階層ツリーでネットワーク全体が選択されている場合に表示されます。設定済みの IP アドレスプールのすべてを削除するには、このオプションを選択します。 • [すべて解放（Release all）]：このオプションは、左側の階層ツリーでサイトが選択されている場合に表示されます。このサイトによって現在予約されているすべての IP アドレスプールを解放するには、このオプションを選択します。
6	[ビューセレクタ（View selector）]：ここでは、このページをテーブルビューで表示するのかツリーマップビューで表示するのかを切り替えられます。

引き出し線	説明
7	[インポート（Import）] ドロップダウンリスト：IP アドレスプール情報を Catalyst Center にインポートする場合にクリックします。この情報は、Catalyst Center 展開が使用する IPAM サーバーか CSV ファイルのいずれかからインポートできます。 この項目は、左側の階層ツリーでネットワーク全体が選択されている場合にのみ表示されます。
8	[インポート（Import）] リンク：[IPアドレスプール（IP Address Pools）] テーブルを Microsoft Excel などのアプリケーションで表示できる CSV ファイルとしてエクスポートする場合にクリックします。 この項目は、左側の階層ツリーでネットワーク全体が選択されている場合にのみ表示されます。
9	[ツアーに参加（Take a Tour）] リンク：このページから完了できるアクションを強調表示するポップアップウィンドウを表示する場合にクリックします。
10	[テーブル設定（Table Settings）] アイコン：[テーブル設定（Table Settings）] スライドインペインを開く場合にクリックします。ここでは、[IPアドレスプール（IP Address Pools）] テーブルの表示方法と表示される情報を設定できます。

サービス プロバイダ プロファイルの設定

特定の WAN プロバイダーのサービスクラスを定義するサービス プロバイダー プロファイルを作成することができます。サービスモデルには、4 クラス、5 クラス、6 クラス、および 8 クラスを定義できます。サービス プロバイダー プロファイルの作成後、アプリケーションポリシーと、アプリケーションポリシーの範囲内の WAN インターフェイスにそれを割り当てることができます（必要に応じてインターフェイスのサブラインレート設定を含む）。

手順

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

ステップ 2 既存のサービス プロバイダー プロファイルがない場合は、[Create] をクリックします。

ステップ 3 プラスアイコンをクリックします。

ステップ 4 [Profile Name] フィールドに、サービス プロバイダー プロファイルの名前を入力します。

ステップ 5 [WAN Provider] フィールドに、WAN プロバイダーの名前を入力します。

ステップ 6 [Model] ドロップダウンリストから、クラスモデル（[4 class]、[5 class]、[6 class]、または [8 class]）のいずれかを選択します。

これらのクラスの詳細については、サービスプロバイダーのプロファイル（1458 ページ）を参照してください。

ステップ 7 [Save] をクリックします。

（注） 重複するサービス プロバイダー プロファイルは作成できません。

グローバルワイヤレス設定の構成

グローバル ワイヤレス ネットワーク設定には、次の設定が含まれます。

- Service Set Identifier（SSID）
- RF プロファイル
- ワイヤレスインターフェイスと VLAN グループ
- AP プロファイル
- FlexConnect
- アンカーグループ
- セキュリティ
- 電力プロファイル
- アンテナ無線プロファイル
- Cisco Spaces および Cisco Connected Mobile Experiences（CMX） サーバ
- リモートテレワーカー
- 802.11be プロファイル

（注） ワイヤレス センサー デバイス プロファイルを作成できるのは、Cisco Aironet 1800s アクティブ センサーデバイスに対してのみです。

ワイヤレスネットワーク設定ダッシュボードの [Search All Settings] フィールドを使用して、特定のワイヤレスネットワーク設定を見つけることができます。[Edit Dashboard] を使用して、ワイヤレスネットワーク設定ダッシュボードをカスタマイズできます。ワイヤレスネットワーク設定ダッシュボードのカスタマイズの詳細については、ワイヤレスネットワーク設定ダッシュボードのカスタマイズ （415 ページ）を参照してください。

ワイヤレスネットワーク設定ダッシュボードのカスタマイズ

[Edit Dashboard] オプションを使用して、ワイヤレスネットワーク設定ダッシュボードをカスタマイズし、ダッシュボードに表示されるネットワーク設定の優先順位を更新できます。Catalyst Center では、ワイヤレスネットワーク設定ダッシュボードのすべてのサイトにダッシュボードのカスタマイズが適用されます。

手順

ステップ 1 メインメニューから次を選択します。 **[Design]** > **[Network settings]** の順にクリックします。

ステップ 2 [Wireless] タブをクリックします。

ステップ 3 左側の階層ツリーから、[Global] を選択します。

ステップ 4 [Edit Dashboard] をクリックします。

ステップ 5 [Customize Wireless Settings Dashboard] スライドインペイン で、必要なネットワーク設定を新しい位置にドラッグアンドドロップして、ダッシュボードでの優先順位を変更します。

ステップ 6 [Save] をクリックします。

エンタープライズ ワイヤレス ネットワーク用 SSID の作成

次の手順では、エンタープライズ ワイヤレス ネットワークに SSID を設定する方法を説明しています。

（注） SSID は、グローバルレベルで作成されます。サイト、ビルディング、フロアは、グローバルレベルから設定が継承されます。

手順

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

ステップ 2 [Wireless] タブをクリックします。

ステップ 3 左側の階層ツリーから、[Global] を選択します。

ステップ 4 [SSIDs] をクリックします。

ステップ 5 [SSID] テーブルで、[Add] の上にカーソルを合わせて、[Enterprise] を選択します。

ステップ 6 [Wireless SSID] ワークフローで、[Basic Settings] のセットアップを完了します。

a) [Sensor] トグルボタンが使用可能な場合は、無効になっていることを確認します。

b) [Wireless Network Name (SSID)] フィールドに、ワイヤレスネットワークの一意の名前を入力します。

c) [WLAN Profile Name] フィールドに、WLAN プロファイルの名前を入力します。

d) （任意） [Policy Profile Name] フィールドで、ポリシープロファイル名を変更します。

デフォルトでは、Catalyst Centerにより WLANプロファイル名がポリシープロファイル名として自動的にコピーされます。

e) （任意） 次のいずれかのオプションで、[Copy to Policy Profile Name] チェックボックスを使用します。

- WLAN プロファイル名をポリシープロファイル名として自動的にコピーします。
- 別の名前をポリシープロファイルに入力します。

f) [Radio Policy] 領域で、次のタスクを実行します。

- 2.4 GHz の WLAN を作成するには、[2.4GHz] チェックボックスをオンにします。
- 5 GHz の WLAN を作成するには、[5GHz] チェックボックスをオンにします。
- 6 GHz の WLAN を作成するには、[6GHz] チェックボックスをオンにします。この帯域は、Cisco IOS XE リリース 17.7 以降を実行しているデバイスでサポートされます。
- [802.11b/g Policy] ドロップダウンリストから、 ポリシーを選択します。

（注） このドロップダウンリストは、[2.4GHz] チェックボックスをオンにした場合にのみ使用できます。

- [Band Select] チェックボックスをオンにして、必要な帯域を選択します。

（注） このチェックボックスは、[2.4GHz] と [5GHz] の両方のチェックボックスをオンにした場合にのみ使用できます。

- [6 GHz Client Steering] チェックボックスをオンにして、クライアントステアリングを有効にします。

（注） このチェックボックスは、[6GHz] チェックボックスをオンにした場合にのみ使用できます。

g) ネットワークで fastlane 機能を有効または無効にするには、[Fast Lane] トグルボタンを使用します。

fastlane を有効にすると、最適化されたレベルのワイヤレス接続と 拡張 QoS を受信するように IOS デバイスを設定できます。

fastlane 機能が有効になっている場合、選択した QoS は適用されません。

h) [Quality of Service(QoS)] 領域で、次のタスクを実行します。

- [Egress] ドロップダウンリストから、出力 QoS（[VoIP (Platinum)]、[Video (Gold)]、[Best Effort (Silver)]、または [Non-real Time (Bronze)]）を選択します。
- [Ingress] ドロップダウンリストから、入力 QoS（[VoIP (Platinum)]、[Video (Gold)]、[Best Effort (Silver)]、または [Non-real Time (Bronze)]）を選択します。

（注） 入力 QoS は、Cisco IOS XE ワイヤレスコントローラ にのみ適用されます。

ファストレーンが有効になっている場合、選択した QoS は適用されません。Cisco IOS XE ワイヤレスコントローラの場合、QoS（出力と入力の両方）は空に設定されます。Cisco AireOS ワイヤレスコントローラの場合、出力 QoS は [VoIP (Platinum)] に設定されます。

i) [SSID STATE] で、トグルボタンを使用して次の設定を有効または無効にします。

- [Admin Status]：このトグルボタンを使用して、AP の無線をオンまたはオフにします。[Admin Status] が無効になっている場合、AP は ワイヤレスコントローラ に関連付けられたままで、アクセス可能であり、AP には引き続きライセンスが必要です。
- [Broadcast SSID]：範囲内のすべてのワイヤレスクライアントに対して SSID の可視性を有効または無効にするには、このトグルボタンを使用します。

ステップ 7 [Security Settings] の設定を完了します。

a) [L2 Security] で、このネットワークの暗号化および認証タイプを選択します。サイト、ビルディング、およびフロアは、グローバル階層から設定を継承します。サイト、ビルディング、またはフロアレベルでセキュリティレベルをオーバーライドできます。

- [Enterprise]：それぞれのチェックボックスをオンにすることで、[WPA2] と [WPA3] の両方のセキュリティ認証を設定できます。デフォルトでは、[WPA3] チェックボックスがオンになっています。

  AP ビーコン保護を有効にするには、[AP Beacon Protection] チェックボックスをオンにします。

（注） Wi-Fi Protected Access（WPA2）では、Counter Mode with Cipher Block Chaining Message Authentication Code Protocol を使用した、より強力な Advanced Encryption Standard 暗号化アルゴリズム（AES-CCMP）が使用されます。

WPA3 は、WPA の最新バージョンです。これは、Wi-Fi ネットワークの認証と暗号化を提供するプロトコルとテクノロジーのスイートです。WPA3 エンタープライズは、センシティブ データ ネットワーク用に、より高いグレードのセキュリティプロトコルを提供します。WPA3 は、リリース 8.10 以降を実行している Cisco AireOS ワイヤレスコントローラ、および Cisco IOS XE リリース 16.12 以降を実行している Cisco Catalyst 9800 シリーズ ワイヤレス コントローラでサポートされています。

2.4 GHz および 5 GHz 帯域のみを使用するマルチバンド操作の場合、WPA2 を有効にする必要があります（WPA3 はオプションです）。

WPA2 は 6 GHz 帯域ではサポートされません。2.4 GHz、5 GHz、および 6 GHz 帯域を使用したマルチバンド動作の場合、Cisco IOS XE リリース 17.7 と Cisco IOS XE リリース 17.11 の間のバージョンを実行しているデバイスで 6 GHz 帯域を動作させるには、WPA3 を有効にし WPA2 を無効にする必要があります。Cisco IOS XE 17.12 以降を実行しているデバイスでは、WPA3 が有効になっている同じ SSID ですべての無線帯域を有効にできます。

- [Personal] ：それぞれのチェックボックスをオンにすることで、[WPA2] と [WPA3] の両方のセキュリティ認証を設定できます。デフォルトでは、[WPA3] チェックボックスがオンになっています。[Personal] を選択した場合は、[Pass Phrase] フィールドにパスフレーズキーを入力します。このキーは、クライアントと認証サーバーの間でペアワイズマスターキー（PMK）として使用されます。

  AP ビーコン保護を有効にするには、[AP Beacon Protection] チェックボックスをオンにします。

（注） WPA3-Personal は、パスワードベースの堅牢な認証を提供することによって個人ユーザーに対する保護を強化します。この認証により、ブルートフォース辞書攻撃が困難になり、時間がかかるようになります。

WPA2-Personal の場合は、サイト、ビルディング、またはフロアレベルで、事前共有キー（PSK）をオーバーライドできます。ビルディングレベルで PSK をオーバーライドすると、後続のフロアは新しい設定を継承します。詳細については、「エンタープライズネットワークの SSID のサイトレベルのオーバーライドの設定（426 ページ）」を参照してください。

2.4 GHz および 5 GHz 帯域のみを使用するマルチバンド操作の場合、WPA2 を有効にする必要があります（WPA3 はオプションです）。2.4 GHz、5 GHz、および 6 GHz 帯域を使用したマルチバンド動作の場合、Cisco IOS XE リリース 17.7 以降を搭載したデバイスで 6 GHz 帯域を動作させるには、WPA3 を有効にし WPA2 を無効にする必要があります。WPA2 は 6 GHz 帯域ではサポートされません。

（オプション）WPA2-Personal の場合、次の手順を実行してマルチ事前共有キー（MPSK）サポートを構成します。

1. [Configure MPSK] をクリックします。
2. [Configure MPSK] ダイアログボックスで、[Add] をクリックして MPSK を追加します。

   最大 5 つの MPSK を追加できます。
3. [Priority] ドロップダウンリストから優先順位を選択します。

（注） 優先順位 0 キーが中央 Web 認証（CWA）フレックスモードで設定されていない場合、WLAN へのクライアント接続が失敗する可能性があります。

4. [Passphrase Type] ドロップダウンリストから、パスフレーズタイプを選択します。
5. [Passphrase] フィールドに、パスフレーズを入力します。
6. [Save] をクリックします。

MPSK は Cisco AireOS ワイヤレスコントローラでサポートされていません。 MPSK は、WPA2-Personal のレイヤ 2 セキュリティ設定に適用されます。

- [Open Secured]：[Select existing Open SSID] ドロップダウンリストから、クライアントをオープンでセキュアな SSID にリダイレクトするためのオープン SSID を選択します。オープンでセキュアなポリシーは、セキュリティが最も低くなります。

（注） Fast Transition は、オープンでセキュアな SSID には適用できません。

オープンでセキュアな SSID はオープン SSID に依存しているため、オープンでセキュアな SSID でアンカーを有効にする前に、オープン SSID でアンカーを有効にしておく必要があります。

- [Open]：オープンなポリシーはセキュリティを備えていません。すべてのデバイスが認証なしでワイヤレスネットワークに接続できます。

（注） [Basic Settings] ウィンドウで [6GHz] 無線ポリシーのみを選択した場合、[Open] オプションはグレー表示されます。

b) [Fast Transition (802.11r)] で、次の手順を実行します。

- [Adaptive]、[Enable]、または [Disable] モードを選択します。

（注） 802.11r を使用すると、ワイヤレスクライアントは、ある AP から別の AP にすばやくローミングできます。Fast Transition によって、ワイヤレスクライアントが AP から別の AP にローミングするときの接続の中断が軽減されます。オープン認証を使用する WLAN の Fast Transition を無効にすることを推奨します。Cisco AireOS ワイヤレスコントローラでは、[Adaptive] モードの Fast Transition がサポートされていません。

- 分散システム経由の高速移行を有効にするには、[Over the DS] チェックボックスをオンにします。デフォルトで、分散システム上の高速移行は無効です。

c) [WPA2 Encryption]、[WPA3 Encryption]、または [WPA2/WPA3 Encryption] で、使用可能なオプションから必要なオプションを選択します。

このセクションで使用できるオプションは、[L2 Security] で選択した設定によって異なります。使用できるオプションは、[AES(CCMP128)]、[GCMP128]、[CCMP256]、および [GCMP256] です。

（注） このセクションは、[L2 Security] が [Open] のセキュリティでは使用できません。

d) [Auth Key Management] で、必要なオプションの横にあるチェックボックスをオンにします。

（注） このセクションは、[L2 Security] が [Open] のセキュリティでは使用できません。

このセクションで使用可能なオプションは、高速移行の設定によって異なります。次のオプションを使用できます。

- [AES(CCMP128)] の場合：OWE、802.1x (802.1X-SHA1)、FT + 802.1x、CCKM、802.1x-SHA256 (802.1X-SHA2)、PSK、FT + PSK、Easy-PSK、PSK-SHA256 (PSK-SHA2)、SAE、SAE-EXT-KEY、FT + SAE、FT + SAE-EXT-KEY
- [GCMP128] の場合：SUITEB-1X
- [CCMP256] の場合：SUITEB192-1X
- [GCMP256] の場合：SUITEB192-1X
- [Timestamp Tolerance (inms)]（CCKM の場合）：CCKM の許容レベルをミリ秒単位で入力します。有効な範囲は 1000 ～ 5000 です。デフォルト値は 1000 です。認証されたクライアントデバイスでは、再関連付け中に遅延を感じることなく、AP間でローミングできます。CCKM 許容レベルは、 Cisco AireOS ワイヤレスコントローラ には適用されません。

e) [Authentication, Authorization, and Accounting Configuration] で、[Configure AAA] をクリックして、エンタープライズ ワイヤレス ネットワーク SSID 用の AAA サーバーを追加および設定します。

詳細については、エンタープライズ ワイヤレス ネットワーク用の AAA サーバーの設定 （430 ページ）を参照してください。

表示されているチェックボックスを 1 つ以上オンにします。

- AAA オーバーライド機能を有効にするには、[AAA Override] チェックボックスをオンにします。

  デフォルトでは、このチェックボックスはグレー表示されています。このチェックボックスを使用するには、[Configure AAA] オプションを使用して AAA サーバを設定する必要があります。
- [Identity PSK]（パーソナルレイヤ 2 セキュリティ用）：SSID の個人またはユーザーグループのために一意の事前共有キーの作成を有効にするには、このチェックボックスをオンにします。このチェックボックスをオンにすると、[Enable Posture] チェックボックスが表示されます。
- [MAC Filtering]（エンタープライズレイヤ 2 セキュリティ用）：ワイヤレスネットワークでの MAC ベースのアクセス制御またはセキュリティを有効にするには、このチェックボックスをオンにします。

  （注） MAC フィルタリングを有効にすると、ワイヤレス LAN に追加した MAC アドレスにのみ WLAN への接続が許可されます。
- [Deny RCM Clients]：ランダム化された MAC アドレスを持つクライアントを拒否するには、このチェックボックスをオンにします。このオプションは、リリース 8.10 MR5 以降を搭載した

Cisco AireOS ワイヤレスコントローラ、および Cisco IOS XE 17.5 以降を搭載した Cisco Catalyst 9800 シリーズ ワイヤレス コントローラでサポートされています。

- [Enable Posture]：ポスチャ評価を有効にするには、このチェックボックスをオンにします。MAC フィルタリングを有効にすると、このチェックボックスはグレー表示になります。

  ポスチャは、Cisco Identity Services Engine（ISE）のサービスです。ポスチャを使用すると、ネットワークに接続されているすべてのエンドポイントの企業セキュリティ ポリシーとのコンプライアンスに関するステート（ポスチャとも呼ばれる）をチェックできます。これにより、ネットワークの防護領域にアクセスするクライアントを制御できます。

  [事前承認IPv4 ACLリスト名（Pre-Auth IPv4 ACL List Name）] および [事前承認IPv6 ACLリスト名（Pre-Auth IPv6 ACL List Name）] ドロップダウンリストから、必要な IP アドレスタイプの ACL リスト名を選択します。[URL ACL名（URL ACL Name）] ドロップダウンリストが表示されたら、必要に応じて URL ACL 名を選択します。

（注） ポスチャには AAA 設定が必須です。[Configure AAA] をクリックして、エンタープライズ ワイヤレス ネットワーク SSID 用の AAA サーバーを追加します。

f) [Next] をクリックします。

ステップ 8 [Advance Settings] の設定を完了します。

a) [MFP Client Protection] で、[Optional]、[Required]、または [Disabled] を選択します。

（注） 管理フレーム保護（MFP）により、管理フレームのセキュリティが強化されます。これによって、AP とクライアントとの間で送受信される、保護および暗号化されていない 802.11 管理メッセージのセキュリティが確保されます。MFP は、インフラストラクチャとクライアントサポートの両方を実現します。

デフォルトでは、[Optional] が選択されています。[Required] を選択すると、MFP がネゴシエートされている場合（つまり、WPA2 が ワイヤレスコントローラ 上で設定されており、クライアントも WPA2 用に設定されていて、CCXv5 MFP をサポートしている場合）にのみ、クライアントはアソシエーションを許可されます。

MFP クライアント保護は、Cisco AireOS ワイヤレスコントローラでのみサポートされます。MFP クライアント保護は、6 GHz 帯域ではサポートされていません。

b) [Protected Management Frame (802.11w)] で、必要なオプションを選択します。

（注） [Protected Management Frame (802.11w)] で使用できるオプションは、[L2 Security] で選択した設定によって異なります。[Optional]、[Required]、[Disabled] のいずれかのオプションが利用できます。

c) すべての 11k 対応クライアントが、ローミングの候補となる既知のネイバー AP に関するネイバーレポートを要求できるように設定するには、[11k - Neighbor List] トグルボタンを使用します。

ローミングを容易に行うため、AP にアソシエートした 11k 対応クライアントは、ネイバー AP のリストに対する要求を送信します。この要求は、アクションフレームと呼ばれる 802.11 管理フレームの形式で送信されます。AP は、同じ WLAN 上にあるネイバー AP の Wi-Fi チャネル番号が付いたリストを使用して応答します。この応答もアクションフレームです。クライアントは応答フレームに基づき、次のローミング先の AP 候補を識別します。

d) WLAN で RADIUS プロファイリングを有効または無効にするには、[Radius Client Profiling] トグルボタンを使用します。

（注） この機能を有効にするには、1 つ以上の AAA または PSN サーバーが必要です。

e) カバレッジホールの検出機能を有効または無効にするには、[Coverage Hole Detection] トグルボタンを使用します。

f) [WLAN Timeouts] で、次のタスクを実行します。

- [Session Timeout]：クライアントセッションがアクティブである最大時間を設定するには、このチェックボックスをオンにします。この時間が経過すると再認証を受ける必要があります。対応するフィールドに、セッションタイムアウトを秒単位で入力します。1 ～ 86400 の範囲の値を指定できます。

（注） デフォルトでは、[Session Timeout] が 1800 秒のタイムアウト付きで有効になります。

- [Client Exclusion]：クライアント除外タイマーを設定するには、このチェックボックスをオンにします。対応するフィールドに、クライアント除外時間を秒単位で入力します。0 ～ 2147483647 の範囲の値を指定できます。

（注） ユーザーが認証に失敗すると、ワイヤレスコントローラはクライアント接続を拒否します。除外タイマーが期限切れになるまで、クライアントはネットワークへの接続を許可されません。デフォルトでは、[Client Exclusion] が 180 秒のタイムアウト付きで有効になります。

- [Client User Idle Timeout]：WLAN のユーザー アイドル タイムアウトを設定するには、このチェックボックスをオンにします。対応するフィールドに、ユーザ アイドル タイムアウトを秒単位で入力します。15 ～ 100000 の範囲の値を指定できます。

  クライアントが送信するデータがユーザー アイドル タイムアウトとして指定されたしきい値を超える場合、クライアントはアクティブであると見なされ、ワイヤレスコントローラは別のタイムアウト期間を開始します。



（注） デフォルトでは、[Client User Idle Timeout] が 300 秒のユーザー アイドル タイムアウト付きで有効になっています。

g) [11v BSS Transition Support] で、次のタスクを実行します。

- [BSS Max Idle Service]：アイドル期間タイマー値を設定するには、このチェックボックスをオンにします。アイドル期間タイマー値は、AP からクライアントへのアソシエーションおよび再アソシエーション応答フレームを使用して送信されます。



（注） BSS最大アイドル期間は、接続先のクライアントからフレームが送信されないという理由で AP がこのクライアントをアソシエート解除しないタイムフレームのことです。

- [Directed Multicast Service]：Directed Multicast Service を有効にするには、このチェックボックスをオンにします。



（注） デフォルトでは、[Directed Multicast Service] が有効になっています。クライアントは Directed Multicast Service（DMS）を使用して、必要なマルチキャストパケットをユニキャストフレームとして送信するようにAPに要求します。これにより、クライアントは長時間スリープ状態になり、バッテリの電力が節約されます。

h) （任意） [NAS-ID] の場合：

1. [NAS-ID Opt] ドロップダウンリストから、必要なタイプのネットワーク アクセス サーバー識別子（NAS ID）を選択します。

   NAS ID のカスタムスクリプトを指定するには、[NAS-ID Opt] ドロップダウンリストから [Custom Option] を選択し、対応する [Custom Script for Opt] フィールドにカスタムスクリプトを入力します。カスタムスクリプトには、最大 31 文字の英数字、特殊文字、およびスペースを入力できます。Catalyst Center はカスタムスクリプトでの特殊文字 ? " < および末尾のスペースをサポートしていません。

（注） Catalyst Center は、Cisco IOS XE リリース 17.7 以降を実行する Cisco Catalyst 9800 シリーズ ワイヤレス コントローラに対してのみ、カスタムスクリプトで NAS ID をサポートします。

2. （オプション）[+] をクリックして、別の NAS ID を追加します。最大 3 つの NAS ID を追加できます。

（注） Catalyst Center は Cisco AireOS ワイヤレスコントローラ の 1 つの NAS ID のみ適用します。**[Design]** > **[Network Settings]** > **[Wireless]** ウィンドウからサイトレベルで NAS ID を上書きできます。

i) （任意）[Configure Client Rate Limit] で、クライアント レート制限の値をビット/秒で入力します。有効な範囲は 8000 ～ 100000000000 です。値は 500 の倍数である必要があります。

（注） この構成は Cisco AireOS ワイヤレスコントローラ に適用できます。Cisco AireOS ワイヤレスコントローラのクライアントレート制限を設定するには、メニューアイコンをクリックして次を選択します。 **[Design]** > **[Feature Templates]** > **[Wireless]** > **[Advanced SSID Configuration]** を選択します。詳細については、高度な SSID の機能テンプレートの作成 （606 ページ）を参照してください。

Cisco IOS XE デバイスには、次のようなクライアントレート制限の有効範囲があります。

- Cisco Catalyst 9800-L ワイヤレスコントローラ、Cisco Catalyst 9800-40 ワイヤレスコントローラ、および Cisco Catalyst 9800-80 ワイヤレスコントローラの有効範囲は、8000 ～ 67000000000 ビット/秒です。
- Cisco Catalyst 9800-CL ワイヤレスコントローラの有効範囲は、8000 ～ 10000000000 ビット/秒です。
- Catalyst アクセスポイント上の Cisco Embedded Wireless Controllerの有効範囲は、8000 ～ 2000000000 ビット/秒です。
- Catalyst 9000 シリーズスイッチ用 Cisco Catalyst 9800 組み込みワイヤレスコントローラの有効範囲は、8000 ～ 100000000000 ビット/秒です。

j) [Next] をクリックします。

ステップ 9 （任意） SSID への機能テンプレートの関連付けの設定を実行します。

a) 必要な機能テンプレートの横にあるチェックボックスをオンにします。

機能テンプレートを作成する場合は、[Add] をクリックして必要な設定を行います。詳細については、「高度な SSID の機能テンプレートの作成 （606 ページ）」を参照してください。

b) [Next] をクリックします。

ステップ 10 [Associate SSID to Profile] の手順を完了します。

a) 左側のペインからプロファイルを選択し、[Associate Profile] をクリックします。

プロファイルがない場合は、[Add Profile] をクリックして、プロファイル設定を指定します。詳細については、「ワイヤレス用のネットワークプロファイルの作成 （543 ページ）」を参照してください。

b) [Next] をクリックします。

ステップ 11 [Summary] ウィンドウで、設定を確認します。変更するには、[Edit] をクリックします。

ステップ 12 [Save] をクリックします。

SSID が作成されます。

エンタープライズ ネットワークの SSID のサイトレベルのオーバーライドの設定

SSID はグローバル階層で作成できます。エリア、ビルディング、およびフロアは、グローバル階層から設定を継承します。エリア、ビルディング、またはフロアのレベルで次の設定をオーバーライドできます。

- **WLAN プロファイル名**
- **Policy Profile Name**
- **L2 セキュリティ**
- **Fast Transition（802.11r）**
- **WPA2 暗号化、WPA3 暗号化、またはWPA2/WPA3 暗号化**
- **認証キー管理**
- **認証、認可、アカウンティング設定**
- **保護された管理フレーム（802.11w）**
- **RADIUS クライアント プロファイリング**
- **NAS-ID**
- **クライアントレート制限の設定**

ビルディングレベルの設定をオーバーライドすると、後続のフロアは新しい設定を継承します。次の手順では、エンタープライズ ネットワーク SSID のサイトレベルでのオーバーライドの設定方法を説明しています。

手順

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

ステップ 2 左側の階層ツリーから、オーバーライドを設定するサイト、ビルディング、またはフロアを選択します。

SSID の横にある検証アイコン にカーソルを合わせると、この設定の継承元が表示されます。

ステップ 3 SSID の横にあるチェックボックスをオンにし、[Edit] をクリックします。

ステップ 4 [Basic Settings] ウィンドウで、必要な設定を編集します。

（注）
- SSID のサイトレベルのオーバーライドを設定する場合は、同じ ワイヤレスコントローラによって管理されるサイト全体の WLAN プロファイルに一意の名前を入力することを推奨します。WLANプロファイル名またはポリシープロファイル名が同一である異なるサイトで、オーバーライドされた SSID を使用してワイヤレスコントローラをプロビジョニングするとプロビジョニングが失敗します。
- ネットワークプロファイルに関連付けられている SSID にサイトレベルのオーバーライドがある場合、Catalyst Center は対応するサイトの ワイヤレスコントローラ プロビジョニング中に、オーバーライドされた SSID の WLAN プロファイル名やポリシープロファイル名を使用します。このルールは、オーバーライドされたサイトが ワイヤレスコントローラのネットワークプロファイルに関連付けられ、同じ ワイヤレスコントローラ によって管理されている場合に適用されます。

ステップ 5 （任意） [Security Settings] ウィンドウで、必要な設定を編集します。

詳細については、エンタープライズ ワイヤレス ネットワーク用 SSID の作成 （415 ページ）を参照してください。

ステップ 6 （任意） [Advanced Settings] ウィンドウで、必要な設定を編集します。

詳細については、エンタープライズ ワイヤレス ネットワーク用 SSID の作成 （415 ページ）を参照してください。

ステップ 7 [Summary] ウィンドウで、設定を確認します。変更するには、[Edit] をクリックします。

ステップ 8 [Save] をクリックします。
サイトレベルのオーバーライドが、SSID に対して設定されます。

認証前アクセス制御リストの作成

認証前 ACL 機能を使用すると、Web 認証用の認証前 ACL を作成して、認証が完了する前に特定のタイプのトラフィックを許可できます。この ACL は、Cisco Identity Services Engine（ISE）の access-accept で参照され、ACL によって許可されるトラフィックと拒否されるトラフィックを定義します。シスコ ワイヤレス コントローラ でACL を設定すると、管理インターフェイス、AP マネージャインターフェイス、任意の動的インターフェイス、または WLAN に適用してワイヤレスクライアントとの双方向のデータトラフィックを制御できます。または、コントローラの中央処理装置（CPU）に適用して CPU 宛のすべてのトラフィックを制御できます。IPv4 と IPv6 の両方の ACL を設定できます。

手順

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

ステップ 2 [Wireless] タブをクリックします。

ステップ 3 左側の階層ツリーから、[Global] を選択します。

ステップ 4 [Security Settings] をクリックします。

ステップ 5 [Pre-Auth ACLs] タブをクリックします。

ステップ 6 [Pre-Auth Access Control Lists] エリアで、[Add] をクリックして認証前 ACL を作成します。

ステップ 7 [新しい事前認証ACL（New Pre-Auth ACL）] スライドインペインで、次の手順を実行します。

1. [Pre-Auth ACL List Name] フィールドに、Catalyst Center で使用する ACL リストの名前を入力します。
2. [Pre-Auth ACL List Name] フィールドに、ワイヤレスコントローラ で設定する ACL の名前を入力します。

ステップ 8 [IPアドレス（IP Addresses）] タブをクリックし、次の手順を実行します。

1. 作成する ACL タイプ（[IPV4] または [IPV6]）を選択します。
2. 該当する SSID への Catalyst Center で生成されたルールのプッシュを有効または無効にするには、[Include auto rules generated by Catalyst Center] トグルボタンを使用します。

   デフォルトでは、このトグルボタンは有効になっています。このトグルボタンを有効にすると、Catalyst Center は自動生成されたルールを該当する SSID にプッシュします。自動生成されたルールでは、DHCP、DNS、AAA、およびデフォルトの事前認証ルールの一部として作成されたその他の該当するポートと IP が許可されます。デフォルトルールは、ネットワーク設定で設定された IP アドレスに基づいて作成されます。

   ファブリック SSID の場合、IP アドレスマネージャの DHCP または DNS IP アドレスがネットワーク設定の IP アドレスと異なる場合、これらの IP アドレスを許可する追加のルールが作成されます。

   （注） このトグルボタンを無効にする場合は、WLANにマッピングされているすべてのDHCP、DNS、および AAA サーバーがカスタム事前認証 ACL ルールに含まれている必要があります。

3. [Protocol] ドロップダウン リストから、この ACL に使用する IP パケットのプロトコル ID を選択します。
4. [Source Port] フィールドに、送信元ポート番号を入力します。

   有効な範囲は 0 ～ 65535 です。単一のポート番号（120 など）またはポート番号の範囲（0 ～ 65535 など）を入力できます。

   ポート オプションは、ネットワーキング スタックとのデータ送受信をするアプリケーションによって使用されます。一部のポートは、Telnet、SSH、HTTP など特定のアプリケーション用に指定されています。

（注） 選択したプロトコルがポート設定（PIMなど）を必要としない場合、またはサポートしない場合、このフィールドはグレー表示されます。

5. [送信元IPアドレス（Source IP Address）] フィールドに、IP アドレスのタイプに基づいて IP アドレスを入力します。

IPアドレスのタイプが以下の場合：	結果
IPv4	[Source Subnet] ドロップダウンリストから、送信元サブネットの値を選択します。
IPv6	[プレフィックス長（Prefix Length）] ドロップダウンリストから、プレフィックス長を選択します。

6. [Destination Port] フィールドに宛先ポート番号を入力します。

有効な範囲は 0 ～ 65535 です。単一のポート番号（120 など）またはポート番号の範囲（0 ～ 65535 など）を入力できます。

（注） 選択したプロトコルがポート設定（PIMなど）を必要としない場合、またはサポートしない場合、このフィールドはグレー表示されます。

7. [宛先IPアドレス（Destination IP Address）] フィールドに、IP アドレスのタイプに基づいて IP アドレスを入力します。

IPアドレスのタイプが以下の場合：	結果
IPv4	[Destination Subnet] ドロップダウンリストから、宛先サブネットの値を選択します。
IPv6	[プレフィックス長（Prefix Length）] ドロップダウンリストから、プレフィックス長を選択します。

8. 複数のルールを追加するには、プラスアイコンをクリックします。最大 256 個のルールを追加できます。

（注） Cisco AireOS ワイヤレスコントローラ の場合、最大 64 のルールを設定できます。

ステップ 9 [Walled Garden URLs] タブをクリックして、キャプティブポータルとウォールドガーデンの Web 認証の許可リストに特定の URL を追加します。

URL の許可リストにアクセスする際に認証は必要ありません。許可リストに含まれていないサイトにアクセスしようとすると、ログインウィンドウにリダイレクトされます。

1. [URL] フィールドに URL を入力し、プラスアイコンをクリックして Web 認証の許可リストに URL を追加します。最大 16 個の URL エントリを追加できます。
   - Cisco AireOS ワイヤレスコントローラ の場合：有効な URL には少なくとも 1 つのピリオド（.）が必要です。その他の特殊文字はサポートされていません。例：cisco.com や www.cisco.com。
   - Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の場合：有効な URL には少なくとも 1 つのピリオド（.）が必要です。特殊文字.、*、-、_がサポートされています。例：www.cisco.com、*.cisco.com、www.cisco-.com。

ステップ 10 [Save] をクリックします。

次のタスク

SSID を作成するときに、ACL を SSID にマッピングします。詳細については、エンタープライズ ワイヤレス ネットワーク用 SSID の作成 （415 ページ）およびゲスト ワイヤレス ネットワークの SSID の作成 （432 ページ）を参照してください。

エンタープライズ ワイヤレス ネットワーク用の AAA サーバーの設定

始める前に

- **[System Settings]** > **[External Services]** > **[Authentication and Policy Servers]** で、AAA サーバーが定義されていることを確認してください。

（注） デュアルスタック展開では、SSID の AAA サーバーの IP アドレスタイプがワイヤレスコントローラの IP アドレスタイプと一致するようにしてください。ワイヤレスコントローラが検出されたか、IPv4 アドレスを使用してインベントリに追加された場合は、その SSID 用の IPv4 AAA サーバーを設定します。ワイヤレスコントローラ が検出されたか、IPv6 アドレスを使用してインベントリに追加された場合は、その SSID 用の IPv6 AAA サーバーを設定します。

- この手順を実行するには、管理者（ROLE_ADMIN）またはポリシー管理者（ROLE_POLICY_ADMIN）権限、および適切な RBAC スコープが必要です。

手順

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

ステップ 2 [Wireless] タブをクリックします。

ステップ 3 左側の階層ツリーから、[Global] を選択します。

ステップ 4 [SSIDs] をクリックします。

ステップ 5 [SSID] テーブルの [AAA Servers] 列で、AAA サーバーを設定する SSID の [Configure AAA] をクリックします。

ステップ 6 [Configure AAA Server] スライドインペイン の [Configure Authentication and Authorization Server] ドロップダウンリストから、[Search] フィールドに名前を入力してサーバーの IP アドレスを検索するか、AAA IP アドレスを選択します。

（注）
- [Configure AAA] オプションは、Mobility Express（ME）デバイスではサポートされていません。
- SSID の認証設定をプッシュするには、SSID の AAA サーバーを設定する必要があります。AAA サーバーが SSID に設定されていない場合、Catalyst Center は **aaa authentication dot1x default local** コマンドを ワイヤレスコントローラ にプッシュし、ローカル認証を指すデフォルトの方式リストが SSID にマッピングされます。

ステップ 7 [+] をクリックして、[Additional Server] を追加します。

（注） エンタープライズ ワイヤレス ネットワークの SSID には、最大 6 つの AAA サーバーを設定できます。

ステップ 8 [Additional Server] ドロップダウンリストから、サーバーの IP アドレスを選択します。

ステップ 9 アカウンティングに AAA サーバーを使用するには、[Copy Same Servers for Accounting] チェックボックスをオンにします。

（注） SSID のアカウンティング設定をプッシュするには、SSID にアカウンティングサーバーを設定する必要があります。

ステップ 10 SSID に別のアカウンティングサーバーを設定するには、次の手順を実行します。

a) [Configure Accounting Server] ドロップダウンリストから、[Search] フィールドに名前を入力してサーバーの IP アドレスを検索するか、アカウンティングサーバーの IP アドレスを選択します。

b) [+] をクリックして、[Additional Server] を追加します。

（注） エンタープライズ ワイヤレス ネットワークの SSID には、最大 6 つのアカウンティングサーバーを設定できます。

c) [Additional Server] ドロップダウンリストから、サーバーの IP アドレスを選択します。

ステップ 11 [Configure] をクリックします。

（注） Catalyst Center では、サイトレベルで SSID の一連の AAA サーバー設定をオーバーライドできます。SSID ごとにオーバーライドされた一連の AAA 設定ごとに、対応する AAA サーバーがマッピングされた新しい WLAN プロファイルが Catalyst Center によって作成されます。異なるフロアの SSID がオーバーライドされ、AAA サーバーで変更を行うと、フロア数に等しい数の新しい WLAN プロファイルが Catalyst Center によって作成されます。

サイトレベルで AAA サーバーをオーバーライドするためには、デバイスを再プロビジョニングする必要があります。ワイヤレスデバイスのプロビジョニングの概要 （735 ページ）を参照してください。

ゲスト ワイヤレス ネットワークの SSID の作成

この手順では、ゲスト ワイヤレス ネットワークの SSID を作成する方法について説明します。

[**Network Design** > **Profiles and Settings**] での書き込み権限を持つロールベース アクセス コントロール（RBAC）のユーザーは、ワイヤレス設計アーティファクトの作成と変更を行えます。これには、SSID、ゲストポータル、およびゲストポリシーが含まれます。詳細については、『Cisco Catalyst Center Administrator Guide』の「Catalyst Center user role and permissions」を参照してください。

手順

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

ステップ 2 [Wireless] タブをクリックします。

ステップ 3 左側の階層ツリーから、[Global] を選択します。

ステップ 4 [SSIDs] をクリックします。

ステップ 5 [SSID] テーブルで、[Add] の上にカーソルを合わせて、[Guest] を選択します。

ステップ 6 [Wireless SSID] ワークフローで、[Basic Settings] のセットアップを完了します。

a) [Wireless Network Name (SSID)] フィールドに、ワイヤレスネットワークの一意の名前を入力します。

b) [WLAN Profile Name] フィールドに、WLAN プロファイルの名前を入力します。

c) （任意） [Policy Profile Name] フィールドで、ポリシープロファイル名を変更します。

デフォルトでは、Catalyst Centerにより WLANプロファイル名がポリシープロファイル名として自動的にコピーされます。

d) （任意） 次のいずれかのオプションで、[Copy to Policy Profile Name] チェックボックスを使用します。

- WLAN プロファイル名をポリシープロファイル名として自動的にコピーします。
- 別の名前をポリシープロファイルに入力します。

e) [Radio Policy] 領域で、次のタスクを実行します。

- 2.4 GHz の WLAN を作成するには、[2.4GHz] チェックボックスをオンにします。
- 5 GHz の WLAN を作成するには、[5GHz] チェックボックスをオンにします。
- 6 GHz の WLAN を作成するには、[6GHz] チェックボックスをオンにします。この帯域は、Cisco IOS XE リリース 17.7 以降を実行しているデバイスでサポートされます。
- [802.11b/g Policy] ドロップダウンリストから、 ポリシーを選択します。

（注） このドロップダウンリストは、[2.4GHz] チェックボックスをオンにした場合にのみ使用できます。

- [Band Select] チェックボックスをオンにして、必要な帯域を選択します。

（注） このチェックボックスは、[2.4GHz] と [5GHz] の両方のチェックボックスをオンにした場合にのみ使用できます。

- [6 GHz Client Steering] チェックボックスをオンにして、クライアントステアリングを有効にします。

（注） このチェックボックスは、[6GHz] チェックボックスをオンにした場合にのみ使用できます。

f) ネットワークで fastlane 機能を有効または無効にするには、[Fast Lane] トグルボタンを使用します。

fastlane を有効にすると、最適化されたレベルのワイヤレス接続と 拡張 QoS を受信するように iOS デバイスを設定できます。

fastlane 機能が有効になっている場合、選択した QoS は適用されません。

g) [Quality of Service(QoS)] 領域で、次のタスクを実行します。

- [Egress] ドロップダウンリストから、出力 QoS（[VoIP (Platinum)]、[Video (Gold)]、[Best Effort (Silver)]、または [Non-real Time (Bronze)]）を選択します。
- [Ingress] ドロップダウンリストから、入力 QoS（[VoIP (Platinum)]、[Video (Gold)]、[Best Effort (Silver)]、または [Non-real Time (Bronze)]）を選択します。



（注） 入力 QoS は、Cisco IOS XE ワイヤレスコントローラ にのみ適用されます。

ファストレーンが有効になっている場合、選択した QoS は適用されません。Cisco IOS XE ワイヤレスコントローラの場合、QoS（出力と入力の両方）は空に設定されます。Cisco AireOS ワイヤレスコントローラの場合、出力 QoS は [VoIP (Platinum)] に設定されます。

h) [SSID STATE] で、トグルボタンを使用して次の設定を有効または無効にします。

- [Admin Status]：このトグルボタンを使用して、AP の無線をオンまたはオフにします。[Admin Status] が無効になっている場合、AP は ワイヤレスコントローラ に関連付けられたままで、アクセス可能であり、AP には引き続きライセンスが必要です。
- [Broadcast SSID]：範囲内のすべてのワイヤレスクライアントに対して SSID の可視性を有効または無効にするには、このトグルボタンを使用します。

ステップ 7 [Security Settings] の設定を完了します。

a) [L2 SECURITY] エリアで、L2 暗号化および認証タイプを選択します。

- [Enterprise]：[WPA2] または [WPA3] のいずれかのセキュリティ認証タイプを設定するには、それぞれのチェックボックスをオンにします。デフォルトでは、[WPA2] チェックボックスが有効になっています。

  AP ビーコン保護を有効にするには、[AP Beacon Protection] チェックボックスをオンにします。

（注） Wi-Fi Protected Access（WPA2）では、Counter Mode with Cipher Block Chaining Message Authentication Code Protocol を使用した、より強力な Advanced Encryption Standard 暗号化アルゴリズム（AES-CCMP）が使用されます。Fast transition は、エンタープライズ WPA2 SSID に適用できます。

WPA3 セキュリティ認証は、WPA の最新バージョンです。これは、Wi-Fi ネットワークの認証と暗号化を提供するプロトコルとテクノロジーのスイートです。WPA3 エンタープライズは、センシティブデータ ネットワーク用に、より高いグレードのセキュリティプロトコルを提供します。

2.4 GHz および 5 GHz 帯域のみを使用するマルチバンド操作の場合、WPA2 を有効にする必要があります（WPA3 はオプションです）。

WPA2 は 6 GHz 帯域ではサポートされません。2.4 GHz、5 GHz、および 6 GHz 帯域を使用したマルチバンド動作の場合、Cisco IOS XE リリース 17.7 と Cisco IOS XE リリース 17.11 の間のバージョンを実行しているデバイスで 6 GHz 帯域を動作させるには、WPA3 を有効にし WPA2 を無効にする必要があります。Cisco IOS XE 17.12 以降を実行しているデバイスでは、WPA3 が有効になっている同じ SSID ですべての無線帯域を有効にできます。

- [Personal]：**WPA2** と **WPA3** の両方を設定したり、**WPA2** と **WPA3** を個別に設定したりするには、それぞれのチェックボックスをオンにします。

  AP ビーコン保護を有効にするには、[AP Beacon Protection] チェックボックスをオンにします。

（注） WPA3-Personal セキュリティ認証は、パスワードベースの堅牢な認証を提供することによって個人ユーザーに対する保護を強化します。これにより、ブルートフォース辞書攻撃が困難になり、時間がかかるようになります。

[Pass Phrase] フィールドにパスフレーズキーを入力します。このキーは、クライアントと認証サーバーの間で Pairwise Master Key（PMK; ペアワイズ マスター キー）として使用されます。

2.4 GHz および 5 GHz 帯域のみを使用するマルチバンド操作の場合、WPA2 を有効にする必要があります（WPA3 はオプションです）。2.4 GHz、5 GHz、および 6 GHz 帯域を使用したマルチバンド動作の場合、Cisco IOS XE リリース 17.7 以降を搭載したデバイスで 6 GHz 帯域を動作させるには、WPA3 を有効にし WPA2 を無効にする必要があります。WPA2 は 6 GHz 帯域ではサポートされません。

（オプション）WPA2-Personalの場合、次の手順を実行してマルチ事前共有キー（MPSK）サポートを構成します。

1. [Configure MPSK] をクリックします。
2. [Configure MPSK] ダイアログボックスで、[Add] をクリックして MPSK を追加します。

   最大 5 つの MPSK を追加できます。
3. [Priority] ドロップダウンリストから優先順位を選択します。

（注） 優先順位 0 キーが中央 Web 認証（CWA）Flex モードで設定されていない場合、WLAN へのクライアント接続が失敗する可能性があります。

4. [Passphrase Type] ドロップダウンリストから、パスフレーズタイプを選択します。
5. [Passphrase] フィールドに、パスフレーズを入力します。
6. [Save] をクリックします。

MPSK は Cisco AireOS ワイヤレスコントローラでサポートされていません。 MPSK は、WPA2-Personal のレイヤ 2 セキュリティ設定に適用されます。

- [Open Secured]：[elect existing Open SSID] ドロップダウンリストから、オープン SSID に関連付けるためのオープンSSIDを選択します。関連付けにより、オープンSSIDが保護されます。オープンでセキュアな SSID に関連付ける前に、オープン SSID が作成されている必要があります。

（注） Fast Transitionは、オープンでセキュアなSSIDには適用できません。

オープンでセキュアな SSID はオープン SSID に依存しているため、オープンでセキュアなSSIDでアンカーを有効にする前に、オープン SSID でアンカーを有効にしておく必要があります。

- [Open]：オープンなポリシーはセキュリティを備えていません。すべてのデバイスが認証なしでワイヤレスネットワークに接続できます。

（注） [Basic Settings] ウィンドウで [6GHz] 無線ポリシーのみを選択した場合、[Open] オプションはグレー表示されます。

b) [Fast Transition (802.11r)] で、次の手順を実行します。

- [Adaptive]、[Enable]、または [Disable] モードを選択します。

（注） 802.11r を使用すると、ワイヤレスクライアントは、ある AP から別の AP にすばやくローミングできます。Fast Transition によって、ワイヤレスクライアントが AP から別の AP にローミングするときの接続の中断が軽減されます。オープン認証を使用する WLAN の Fast Transition を無効にすることを推奨します。Cisco AireOS ワイヤレスコントローラでは、[Adaptive] モードの Fast Transition がサポートされていません。

- 分散システム経由の高速移行を有効にするには、[Over the DS] チェックボックスをオンにします。デフォルトで、分散システム上の高速移行は無効です。

c) [WPA2 Encryption]、[WPA3 Encryption]、または [WPA2/WPA3 Encryption] で、使用可能なオプションから必要なオプションを選択します。

このセクションで使用できるオプションは、[L2 Security] で選択した設定によって異なります。使用できるオプションは、[AES(CCMP128)]、[GCMP128]、[CCMP256]、[GCMP256] です。

（注） このセクションは、[L2 Security] が [Open] のセキュリティでは使用できません。

d) [Auth Key Management] で、必要なオプションの横にあるチェックボックスをオンにします。

（注） このセクションは、[Level of Security] が [Open] のセキュリティでは使用できません。次のオプションを使用できます。

- [AES(CCMP128)] の場合：OWE、802.1x (802.1X-SHA1)、FT + 802.1x、CCKM、802.1x-SHA256 (802.1X-SHA2)、PSK、FT + PSK、Easy-PSK、PSK-SHA256 (PSK-SHA2)、SAE、SAE-EXT-KEY、FT + SAE、FT + SAE-EXT-KEY
- [GCMP128] の場合：SUITEB-1X
- [CCMP256] の場合：SUITEB192-1X
- [GCMP256] の場合：SUITEB192-1X

このセクションで使用可能なオプションは、高速移行の設定によって異なります。

- [Timestamp Tolerance (inms)]（CCKM の場合）：CCKM の許容レベルをミリ秒単位で入力します。有効な範囲は 1000 ～ 5000 です。デフォルト値は 1000 です。認証されたクライアントデバイスでは、再関連付け中に遅延を感じることなく、AP間でローミングできます。CCKM 許容レベルは、 Cisco AireOS ワイヤレスコントローラ には適用されません。

e) [L3 Security] 設定で、L3 暗号化および認証タイプを選択します。

• [Web Policy]：L3 セキュリティを強化します。

[Authentication Server] で、これらの認証サーバー設定を指定します。

認証サーバータイプ	説明
Central Web Authentication（中央 Web 認証）	中央 Web 認証（CWA）に AAA サーバーを使用します。 （オプション）CWA に Cisco ISE を選択した場合は、[What kind of portal are you creating today?] ドロップダウンリストで、作成するポータルのタイプを選択します。 • [Self Registered]：ゲストは自己登録ゲストポータルにリダイレクトされ、情報を提供して登録して、自動的にアカウントを作成します。 • [HotSpot]：ゲストはログイン情報なしでネットワークにアクセスできます。 （オプション）CWA に Cisco ISE を選択した場合は、[Where will your guests redirect after successful authentication?] ドロップダウンリストで、認証が成功した後にゲストをリダイレクトする場所を選択します。 • [Success page]：ゲストは [Authentication Success] ウィンドウにリダイレクトされます。 • [Original URL]：ゲストは最初にリクエストした URL にリダイレクトされます。 • [Custom URL]：ゲストはここで特定されたカスタム URL にリダイレクトされます。[Redirect URL] フィールドにリダイレクト URL を入力します。
• **Web 認証（内部）** • **Web 認証（外部）**	レイヤ 3 セキュリティ方式である Web 認証（Web Auth）を使用すると、クライアントは、何らかの認証方式に合格するまでの間、Dynamic Host Configuration Protocol（DHCP）およびドメインネームシステム（DNS）のトラフィックを通過させることができます。 Web認証（内部）の場合、クライアントはシスコワイヤレスコントローラによって作成されたウィンドウにリダイレクトされます。 Web 認証（外部）の場合は、クライアントが、指定された URL にリダイレクトされます。[Web Auth Url] フィールドにリダイレクト URL を入力します。

認証サーバータイプ	説明
• **Web パススルー（内部）** • **Web パススルー（外部）**	Web パススルーは、ゲストアクセスに使用され、認証ログイン情報を必要としません。Web パススルー認証では、ワイヤレスユーザーがインターネットを初めて使用するとき、[Usage Policy] ウィンドウにリダイレクトされます。ポリシーを承認すると、ユーザーはインターネットを使用できます。

- [Open]：レイヤ 3 レベルのセキュリティがなく、どのデバイスも SSID に接続できます。

f) [Web Authentication Internal]、[Web Authentication External]、[Web Passthrough Internal]、または [Web Passthrough External] を選択した場合、[Timeout Settings for sleeping clients] エリアで、スリープしているクライアントの認証設定を選択します。

- [Always authenticate]：スリープ状態のクライアントの認証が有効になります。
- [Authenticate after]：再認証が必要になるまでスリープ状態にあるクライアントが記憶される期間（分）を入力します。有効範囲は 10 ～ 43200 分、デフォルト期間は 720 分です。

（注） ゲストアクセスで Web 認証済みクライアントは、ログインウィンドウから再認証なしにスリープおよび復帰することを許可されています。WLAN にマッピングされるユーザーグループポリシーと WLAN に、クライアントが記憶される期間を設定できます。スリープ タイマーは、アイドル タイムアウト後に有効になります。クライアントタイムアウトが WLAN のスリープタイマーに設定された時間より短い場合は、クライアントのライフタイムがスリープ時間として使用されます。

g) [Authentication, Authorization, and Accounting Configuration] で、[Configure AAA] をクリックして、ゲスト ワイヤレス ネットワーク SSID 用の AAA サーバーを追加および設定します。

詳細については、ゲスト ワイヤレス ネットワーク用の AAA サーバーの設定（446 ページ）を参照してください。

（オプション）次の設定を完了します。

- AAA オーバーライド機能を有効にするには、[AAA Override] チェックボックスをオンにします。

  デフォルトでは、このチェックボックスはグレー表示されています。このチェックボックスを使用するには、[Configure AAA] オプションを使用して AAA サーバを設定する必要があります。

- [Identity PSK]（パーソナルレイヤ 2 セキュリティ用）：SSID の個人またはユーザーグループのために一意の事前共有キーの作成を有効にするには、このチェックボックスをオンにします。
- [MAC Filtering]（エンタープライズレイヤ 2 セキュリティ用）：ワイヤレスネットワークでの MAC ベースのアクセス制御またはセキュリティを有効にするには、このチェックボックスをオンにします。

（注） MAC フィルタリングを有効にすると、ワイヤレス LAN に追加した MAC アドレスにのみ WLAN への接続が許可されます。

- [Deny RCM Clients]：ランダム化された MAC アドレスを持つクライアントを拒否するには、このチェックボックスをオンにします。このオプションは、リリース 8.10 MR5 以降を搭載した Cisco AireOS ワイヤレスコントローラ、および Cisco IOS XE 17.5 以降を搭載した Cisco Catalyst 9800 シリーズ ワイヤレス コントローラでサポートされています。
- [事前認証IPv4 ACLリスト名（Pre-Auth IPv4 ACL List Name）] と [事前認証IPv6 ACLリスト名（Pre-Auth IPv6 ACL List Name）]：必要な IP アドレスタイプの ACL リスト名を選択します。

  [URL ACL名（URL ACL Name）] ドロップダウンリストが表示されたら、必要に応じて URL ACL 名を選択します。

  これらのドロップダウンリストは、[中央Web認証（Central Web Authentication）] および [外部Web認証（Web Authentication External）] を選択した場合にのみ使用できます。

（注） Cisco IOS XE デバイスの Cisco ISE で URL フィルタの認証プロファイルを手動で追加する必要があります。IPv4 と IPv6 の両方の事前認証 ACL を選択すると、Cisco ISE の認証プロファイルはデフォルトで IPv6 ACL を使用します。

h) [Next] をクリックします。

ステップ 8 [Advance Settings] の設定を完了します。

a) [MFP Client Protection] で、[Optional]、[Required]、または [Disabled] を選択します。

（注） 管理フレーム保護（MFP）により、管理フレームのセキュリティが強化されます。これによって、AP とクライアントとの間で送受信される、保護および暗号化されていない 802.11 管理メッセージのセキュリティが確保されます。MFP は、インフラストラクチャとクライアントサポートの両方を実現します。

デフォルトでは、[Optional] が選択されています。[Required] を選択すると、MFP がネゴシエートされている場合（つまり、WPA2 がワイヤレスコントローラ上で設定されており、クライアントも WPA2 用に設定されていて、CCXv5 MFP をサポートしている場合）にのみ、クライアントはアソシエーションを許可されます。

MFP クライアント保護は、Cisco AireOS ワイヤレスコントローラでのみサポートされます。MFP クライアント保護は、6 GHz 帯域ではサポートされていません。

b) [Protected Management Frame (802.11w)] で、必要なオプションを選択します。

（注） [Protected Management Frame (802.11w)] で使用できるオプションは、[Level of Security] で選択した設定によって異なります。[Optional]、[Required]、[Disabled] のいずれかのオプションが利用できます。

c) すべての 11k 対応クライアントが、ローミングの候補となる既知のネイバー AP に関するネイバーレポートを要求できるように設定するには、[11k - Neighbor List] トグルボタンを使用します。

（注） ローミングを容易に行うため、AP にアソシエートした 11k 対応クライアントは、ネイバー AP のリストに対する要求を送信します。この要求は、アクションフレームと呼ばれる 802.11 管理フレームの形式で送信されます。AP は、同じ WLAN 上にあるネイバー AP の Wi-Fi チャネル番号が付いたリストを使用して応答します。この応答もアクションフレームです。クライアントは応答フレームに基づき、次のローミング先の AP 候補を識別します。

d) WLAN で RADIUS プロファイリングを有効または無効にするには、[Radius Client Profiling] トグルボタンを使用します。

（注） この機能を有効にするには、1 つ以上の AAA または PSN サーバーが必要です。

e) カバレッジホールの検出機能を有効または無効にするには、[Coverage Hole Detection] トグルボタンを使用します。

f) [WLAN Timeouts] で、次のタスクを実行します。

- [Session Timeout]：クライアントセッションがアクティブである最大時間を設定するには、このチェックボックスをオンにします。この時間が経過すると再認証を受ける必要があります。対応するフィールドに、セッションタイムアウトを秒単位で入力します。1 ～ 86400 の範囲の値を指定できます。

（注） デフォルトでは、[Session Timeout] が 1800 秒のタイムアウト付きで有効になります。

- [Client Exclusion]：クライアント除外タイマーを設定するには、このチェックボックスをオンにします。対応するフィールドに、クライアント除外時間を秒単位で入力します。0 ～ 2147483647 の範囲の値を指定できます。

（注） ユーザーが認証に失敗すると、ワイヤレスコントローラはクライアント接続を拒否します。除外タイマーが期限切れになるまで、クライアントはネットワークへの接続を許可されません。デフォルトでは、[Client Exclusion] が 180 秒のタイムアウト付きで有効になります。

- [Client User Idle Timeout]：WLAN のユーザー アイドル タイムアウト期間を設定するには、このチェックボックスをオンにします。対応するフィールドに、ユーザ アイドル タイムアウトを秒単位で入力します。15 ～ 100000 の範囲の値を指定できます。

（注） クライアントが送信するデータがユーザー アイドル タイムアウト期間として指定されたしきい値のクォータを超える場合、クライアントはアクティブであると見なされ、ワイヤレスコントローラは別のタイムアウト期間を開始します。

デフォルトでは、[Client User Idle Timeout] が 300 秒のユーザー アイドル タイムアウト付きで有効になっています。

g) [11v BSS Transition Support] で、次の設定を指定します。

- [BSS Max Idle Service]：アイドル期間タイマー値を設定するには、このチェックボックスをオンにします。アイドル期間タイマー値は、AP からクライアントへのアソシエーションおよび再アソシエーション応答フレームを使用して送信されません。

（注） BSS最大アイドル期間は、接続先のクライアントからフレームが送信されないという理由で AP がこのクライアントをアソシエート解除しないタイムフレームのことです。

- [Directed Multicast Service]：Directed Multicast Service を有効にするには、このチェックボックスをオンにします。

（注） デフォルトでは、[Directed Multicast Service] が有効になっています。クライアントは Directed Multicast Service（DMS）を使用して、必要なマルチキャストパケットをユニキャストフレームとして送信するようにAPに要求します。これにより、クライアントは長時間スリープ状態になり、バッテリの電力が節約されます。

h) （オプション）[NAS-ID] で、次の設定を指定します。

1. [NAS-ID Opt] ドロップダウンリストから、必要なタイプのネットワーク アクセス サーバー識別子（NAS ID）を選択します。

   （オプション）NAS ID のカスタムスクリプトを指定するには、[NAS-ID Opt] ドロップダウンリストから [Custom Option] を選択し、対応する [Custom Script for Opt] フィールドにカスタムスクリプトを入力します。カスタムスクリプトには、最大 31 文字の英数字、特殊文字、およびスペースを入力できます。Catalyst Center はカスタムスクリプトでの特殊文字？" < および末尾のスペースをサポートしていません。



（注） Catalyst Center は、Cisco IOS XE リリース 17.7 以降を実行する Cisco Catalyst 9800 シリーズ ワイヤレス コントローラに対してのみ、カスタムスクリプトで NAS ID をサポートします。

2. （オプション）[+] をクリックして、別のネットワーク アクセス サーバー識別子を追加します。最大 3 つの NAS ID を追加できます。



（注） Catalyst Center は Cisco AireOS ワイヤレスコントローラ の 1 つの NAS ID のみ適用します。**[Design]** > **[Network Settings]** > **[Wireless]** ウィンドウからサイトレベルで NAS ID を上書きできます。

i) （任意）[Configure Client Rate Limit] で、クライアント レート制限の値をビット/秒で入力します。有効な範囲は 8000 ～ 100000000000 です。値は 500 の倍数である必要があります。



（注） この構成は Cisco AireOS ワイヤレスコントローラ に適用できます。Cisco AireOS ワイヤレスコントローラ のクライアントレート制限を設定するには、メニューアイコンをクリックして次を選択します。 **[Design]** > **[Feature Templates]** > **[Wireless]** > **[Advanced SSID Configuration]** を選択します。詳細については、高度な SSID の機能テンプレートの作成 （606 ページ）を参照してください。

Cisco IOS XE デバイスには、次のようなクライアントレート制限の有効範囲があります。

- Cisco Catalyst 9800-L ワイヤレスコントローラ、Cisco Catalyst 9800-40 ワイヤレスコントローラ、および Cisco Catalyst 9800-80 ワイヤレスコントローラの有効範囲は、8000 ～ 67000000000 ビット/秒です。
- Cisco Catalyst 9800-CL ワイヤレスコントローラの有効範囲は、8000 ～ 10000000000 ビット/秒です。
- Catalyst アクセスポイント上の Cisco Embedded Wireless Controllerの有効範囲は、8000 ～ 2000000000 ビット/秒です。
- Catalyst 9000 シリーズスイッチ用 Cisco Catalyst 9800 組み込みワイヤレスコントローラの有効範囲は、8000 ～ 100000000000 ビット/秒です。

j) [Next] をクリックします。

ステップ 9 （任意） SSID への機能テンプレートの関連付けの設定を実行します。

a) 必要な機能テンプレートの横にあるチェックボックスをオンにします。

機能テンプレートを作成する場合は、[Add] をクリックして必要な設定を行います。詳細については、「高度な SSID の機能テンプレートの作成 （606 ページ）」を参照してください。

b) [Next] をクリックします。

ステップ 10 [Associate SSID to Profile] の手順を完了します。

a) 左側のペインからプロファイルを選択し、[Associate Profile] をクリックします。

プロファイルがない場合は、[Add Profile] をクリックして、プロファイル設定を指定します。詳細については、「ワイヤレス用のネットワークプロファイルの作成 （543 ページ）」を参照してください。

b) [Next] をクリックします。

ステップ 11 [Summary] ウィンドウで、設定を確認します。変更するには、[Edit] をクリックします。

ステップ 12 [Save] をクリックします。

SSID が作成されます。

ゲストネットワークの SSID に対するサイトレベルのオーバーライドの設定

SSID はグローバル階層で作成できます。エリア、ビルディング、およびフロアは、グローバル階層から設定を継承します。エリア、ビルディング、またはフロアのレベルで次の設定をオーバーライドできます。

- **WLAN プロファイル名**
- **Policy Profile Name**
- **L2 セキュリティ**
- **Fast Transition（802.11r）**
- **WPA2 暗号化、WPA3 暗号化、またはWPA2/WPA3 暗号化**
- **認証キー管理**
- **認証、認可、アカウンティング設定**
- **NAS-ID**
- **クライアントレート制限の設定**

ビルディングレベルの設定をオーバーライドすると、後続のフロアは新しい設定を継承します。次の手順では、ゲストネットワークの SSID に対するサイトレベルのオーバーライドの設定方法について説明します。

手順

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

ステップ 2 左側の階層ツリーから、オーバーライドを設定するサイト、ビルディング、またはフロアを選択します。

SSID の横にある検証アイコン にカーソルを合わせると、この設定の継承元が表示されます。

ステップ 3 SSID の横にあるチェックボックスをオンにし、[Edit] をクリックします。

ステップ 4 [Basic Settings] ウィンドウで、必要な設定を編集します。

（注）
- SSID のサイトレベルのオーバーライドを設定する場合は、同じ ワイヤレスコントローラによって管理されるサイト全体の WLAN プロファイルに一意の名前を入力することを推奨します。WLANプロファイル名またはポリシープロファイル名が同一である異なるサイトで、オーバーライドされた SSID を使用してワイヤレスコントローラをプロビジョニングするとプロビジョニングが失敗します。
- ネットワークプロファイルに関連付けられている SSID にサイトレベルのオーバーライドがある場合、Catalyst Center は対応するサイトの ワイヤレスコントローラ プロビジョニング中に、オーバーライドされた SSID の WLANプロファイル名やポリシープロファイル名を使用します。このルールは、オーバーライドされたサイトが ワイヤレスコントローラのネットワークプロファイルに関連付けられ、同じ ワイヤレスコントローラ によって管理されている場合に適用されます。

ステップ 5 （任意） [Security Settings] ウィンドウで、必要な設定を編集します。

設定の編集の詳細については、「ゲスト ワイヤレス ネットワークの SSID の作成 （432 ページ）」を参照してください。

ステップ 6 （任意） [詳細設定（Advanced Settings）] ウィンドウで、次の手順を実行します。

設定の編集の詳細については、「ゲスト ワイヤレス ネットワークの SSID の作成 （432 ページ）」を参照してください。

ステップ 7 [Summary] ウィンドウで、設定を確認します。変更するには、[Edit] をクリックします。

ステップ 8 [Save] をクリックします。
サイトレベルのオーバーライドが、SSID に対して設定されます。

ゲスト ワイヤレス ネットワーク用の AAA サーバーの設定

始める前に

- **[System Settings]** > **[External Services]** > **[Authentication and Policy Servers]** ウィンドウで、AAA サーバーが定義されていることを確認してください。



（注） デュアルスタック展開では、SSID の AAA サーバーの IP アドレスタイプがワイヤレスコントローラの IP アドレスタイプと一致するようにしてください。ワイヤレスコントローラが検出されたか、IPv4 アドレスを使用してインベントリに追加された場合は、その SSID 用の IPv4 AAA サーバーを設定します。ワイヤレスコントローラが検出されたか、IPv6 アドレスを使用してインベントリに追加された場合は、その SSID 用の IPv6 AAA サーバーを設定します。

- この手順を実行するには、管理者（ROLE_ADMIN）またはポリシー管理者（ROLE_POLICY_ADMIN）権限、および適切な RBAC スコープが必要です。

手順

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

ステップ 2 [Wireless] タブをクリックします。

ステップ 3 左側の階層ツリーから、[Global] を選択します。

ステップ 4 [SSIDs] をクリックします。

ステップ 5 [SSID] テーブルの [AAA Servers] 列で、AAA サーバーを設定する SSID の [Configure AAA] をクリックします。

ステップ 6 [Configure AAA Server] スライドインペインの [Server] ドロップダウンリストから、[Search] フィールドに名前を入力して AAA IP アドレスを検索するか、AAA IP アドレスを選択します。

（注）
- ゲスト ワイヤレス ネットワークの中央 Web 認証（CWA）SSID 用に少なくとも 1 つの AAA またはポリシーサービスノード（PSN）サーバーを設定する必要があります。
- Catalyst Center で生成された事前認証 ACL は、ゲスト ワイヤレス ネットワークの CWA SSID に設定された AAA または PSN サーバーに対してのみ作成されます。以前のリリースからアップグレードする場合は、コンプライアンスの不一致がないことを確認するために、ワイヤレスコントローラ を再プロビジョニングする必要があります。
- Catalyst Center では、アイデンティティ サービス エンジンの PSN とサードパーティ AAA IP の任意の組み合わせで AAA サーバーをマッピングできます。
- [Server] ドロップダウンリストで、**AAA** IP アドレスと PSN IP アドレスが対応するセクションにおいてグループ化されています。
- [Configure AAA] オプションは、Mobility Express（ME）デバイスではサポートされていません。
- SSID の認証設定をプッシュするには、SSID の AAA サーバーを設定する必要があります。AAA サーバーが SSID に設定されていない場合、Catalyst Center は **aaa authentication dot1x default local** コマンドを ワイヤレスコントローラ にプッシュし、ローカル認証を指すデフォルトの方式リストが SSID にマッピングされます。

ステップ 7 [+] をクリックして、[Additional Server] を追加します。

（注） ゲスト ワイヤレス ネットワークの SSID には、最大 6 つの AAA サーバーを設定できます。

ステップ 8 [Additional Server] ドロップダウンリストから、サーバーの IP アドレスを選択します。

ステップ 9 （任意）サーバーまたは追加のサーバーを削除するには、各サーバーの横にある削除アイコンをクリックします。

ステップ 10 アカウンティングに AAA サーバーを使用するには、[Copy Same Servers for Accounting] チェックボックスをオンにします。

（注） SSID のアカウンティング設定をプッシュするには、SSID にアカウンティングサーバーを設定する必要があります。

ステップ 11 SSID に別のアカウンティングサーバーを設定するには、次の手順を実行します。

a) [Configure Accounting Server] ドロップダウンリストから、[Search] フィールドに名前を入力してサーバーの IP アドレスを検索するか、アカウンティングサーバーの IP アドレスを選択します。

b) [+] をクリックして、[Additional Server] を追加します。

（注） エンタープライズ ワイヤレス ネットワークの SSID には、最大 6 つのアカウンティングサーバーを設定できます。

c) [Additional Server] ドロップダウンリストから、サーバーの IP アドレスを選択します。

ステップ 12 [Configure] をクリックします。

（注） Catalyst Center では、サイトレベルで SSID の一連の AAA サーバー設定をオーバーライドできます。SSID ごとにオーバーライドされた一連の AAA 設定ごとに、対応する AAA サーバーがマッピングされた新しい WLAN プロファイルが Catalyst Center によって作成されます。異なるフロアの SSID がオーバーライドされ、AAA サーバーで変更を行うと、フロア数に等しい数の新しい WLAN プロファイルが Catalyst Center によって作成されます。

サイトレベルで AAA サーバーをオーバーライドするためには、デバイスを再プロビジョニングする必要があります。ワイヤレスデバイスのプロビジョニングの概要（735 ページ）を参照してください。

SSID スケジューラの作成

SSID スケジューラを作成して、タイムゾーンに基づき WLAN を有効化または無効化できます。

手順

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

ステップ 2 [Wireless] タブをクリックします。

ステップ 3 左側の階層ツリーから、[Global] を選択します。

ステップ 4 [SSIDs] をクリックします。

ステップ 5 [SSID] テーブルで、[SSID Scheduler] をクリックします。

ステップ 6 [SSID Scheduler] ウィンドウで、[Add] をクリックします。

ステップ 7 [スケジューラの作成（Create Scheduler）] スライドインペインで、次の手順を実行します。

a) 作成する SSID スケジューラの一意の名前を入力します。

b) クライアントが SSID に参加することを拒否するには、[Client Deny] オプションボタンをクリックします。

c) [Enable SSID] をクリックして、SSID ブロードキャストをスケジュールします。

d) [Scheduler Type] として [Daily] 、[Weekly] 、または [Monthly] を選択し、必要な設定を完了します。

e) [Time Zone] ドロップダウンリストから、タイムゾーンを選択します。
f) [Save] をクリックします。

作成された SSID スケジューラが、[SSID Scheduler] テーブルに表示されます。

ステップ 8 SSID スケジューラを編集するには、次の手順を実行します。
a) [SSID Scheduler] テーブルから、任意の SSID スケジューラを選択し、[Edit] をクリックします。
b) [Edit SSID Scheduler] スライドインペインで、必要な変更を行い、[Save] をクリックします。

ステップ 9 SSID スケジューラを削除するには、SSID スケジューラを選択して [Delete] をクリックします。

ステップ 10 SSID スケジューラの詳細を表示するには、SSID スケジューラを選択し、[Scheduler History] をクリックします。

（注） [Scheduler History] を表示するには、Assuranceパッケージをインストールする必要があります。

次のタスク

ワイヤレスコントローラの SSID スケジューラを有効にします。詳細については、ネットワークプロファイルへの SSID の追加 （544 ページ）を参照してください。

ワイヤレスインターフェイスの作成

非ファブリック展開でのみワイヤレスインターフェイスを作成できます。

手順

ステップ 1 メインメニューから次を選択します。**[Design]** > **[Network settings]**。
ステップ 2 [Wireless] タブをクリックします。
ステップ 3 左側の階層ツリーから、[Global] を選択します。
ステップ 4 [Interfaces & VLAN Groups] をクリックします。
ステップ 5 [インターフェイス（Interfaces）] タブをクリックします。
ステップ 6 [Wireless Interfaces] テーブルで、[Add] をクリックします。
ステップ 7 [Create a Wireless Interface] スライドペインでワイヤレスインターフェイスの設定を指定します。
a) [Interface Name] フィールドに、動的なインターフェイスの名前を入力します。
b) [VLAN ID] フィールドに、このインターフェイスの VLAN ID を入力します。

Cisco AireOS ワイヤレスコントローラ の場合、有効な範囲は 1 ～ 4094 です。Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の場合、有効な範囲は 2 ～ 4094 です。

ステップ 8 [Save] をクリックします。

ワイヤレスインターフェイスが作成され、[Wireless Interfaces] テーブルに表示されます。

非ファブリック展開用の VLAN グループの設計とプロビジョニング

Catalyst Center では、異なる VLAN を介して複数のブロードキャストドメインを持つネットワークを設定できます。同じ AP のセットが同じ WLAN をブロードキャストする場合、ブロードキャストドメインは、インターフェイスグループを介して同じ WLAN 上の複数の VLAN によって制御されます。

Catalyst Center インターフェイスグループは、ユーザー設定を容易にするインターフェイスの論理グループであり、同じインターフェイスグループを複数の WLAN で設定できます。その一方で、AP グループごとに WLAN インターフェイスをオーバーライドできます。1 つのインターフェイスを複数のインターフェイス グループに含めることができます。WLAN は、インターフェイスまたはインターフェイス グループに関連付けることができます。

（注） インターフェイスグループ名とインターフェイス名は同じ名前にできません。

Catalyst Center VLAN グループ機能は、VLAN グループを使用して WLAN を 1 つまたは複数の VLAN にマッピングします。VLAN グループは、ポリシープロファイルに関連付けることができます。

この手順では、非ファブリック展開のインターフェイスまたは VLAN グループを設計およびプロビジョニングする方法について説明します。

手順

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

ステップ 2 [Wireless] タブをクリックします。

ステップ 3 左側の階層ツリーから、[Global] を選択します。

ステップ 4 [Interfaces & VLAN Groups] をクリックします。

ステップ 5 [VLAN Groups] タブをクリックします。

ステップ 6 [VLAN Group] テーブルで、[Add] をクリックします。

ステップ 7 [VLANグループの追加（Add VLAN Group）] スライドインペインで、次の手順を実行します。

a) 有効な **VLAN グループ名**を入力してください。

b) リストから単一または複数のインターフェイスを選択します。

c) [Save] をクリックします。

（注） 15を超えるインターフェイスを選択すると、選択したインターフェイスが画面に正しく表示されない場合があります。

ステップ 8 [Edit Network Profile] ウィンドウで、VLAN グループが SSID に関連付けられます。

SSID の作成方法については、「エンタープライズ ワイヤレス ネットワーク用 SSID の作成」を参照してください。

ステップ 9 VLAN グループにさらに SSID を追加するには、[Add SSID] をクリックします。

ステップ 10 [Interface] または [VLAN] グループを選択します。

ステップ 11 [Add] アイコンをクリックして、新しいインターフェイスまたは VLAN グループを作成します。

（注） インターフェイスや VLAN グループは、FlexConnect ローカルスイッチングには適用できません。

ステップ 12 [Save] をクリックします。

ステップ 13 [Configure Interface and VLAN] では、インターフェイス名、インターフェイスグループ名、およびインターフェイスと VLAN の設定に必要なその他のパラメータのリストを確認できます。

（注） インターフェイスグループには、64 を超えるインターフェイスは含められません。

ステップ 14 メインメニューから次を選択します。**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。

ステップ 15 デバイスを選択します。

ステップ 16 [Actions] ドロップダウンメニューから、**[Provision]** > **[Provision Device]** の順に選択します。

ステップ 17 [Assign Site]、[Configuration]、[Feature Templates]、[Advanced Configuration]、および [Summary] ウィンドウで詳細を確認します。各ウィンドウで、[Next] をクリックして次のウィンドウに進みます。

ステップ 18 [展開（Deploy）] をクリックします。

[Provision Device] ダイアログボックスが開きます。

ステップ 19 [Now] を選択し、[Apply] をクリックします。

「Task Scheduled view status in Tasks」というメッセージが表示されます。

ワイヤレス無線周波数プロファイルの作成

デフォルトの無線周波数プロファイル（低、標準、高）を使用することも、カスタムの無線周波数プロファイルを作成することもできます。

手順

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

ステップ 2 [**Wireless**] エリアをクリックし、[**Add**] にカーソルを合わせて [**Basic RF Profile**] を選択します。

ステップ 3 [Create Wireless Radio Frequency Profile] ウィンドウの [Profile Name] フィールドに、RF プロファイル名を入力します。

ステップ 4 [2.4 GHz] タブで次の設定を行います。

a) [2.4 GHz] トグルボタンが有効になっていることを確認します。

（注）

- Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の場合、[2.4 GHz] トグルボタンを無効にすると、Catalyst Center は、[2.4 GHz] RF プロファイルの管理ステータスを無効にします。
- Cisco AireOS ワイヤレスコントローラ の場合、[2.4 GHz] トグルボタンを無効にして、ワイヤレスコントローラ または AP を再プロビジョニングすると、Catalyst Center は、対応する帯域の RF プロファイルを作成し、そのプロファイルを AP グループにマッピングして（プロファイルを [None] として設定するのではなく）、AP で対応する無線の管理ステータスを無効にします。
- Cisco AireOS ワイヤレスコントローラの場合、RF プロファイルで 2.4 GHz 帯域の管理ステータスを無効にすると、Catalyst Center ではその RF プロファイルを使用する AP の XOR 無線が手動 5 GHz モードに変更されます。後で管理ステータスを有効にして AP を再プロビジョニングすると、 Catalyst Center では無線が自動モードに変更され、2.4 GHz および 5 GHz 帯域とモニターモードを使用できるようになります。そのため、XOR 対応 AP で 2.4 GHz 帯域の管理ステータスを無効にする場合は、[Configure Access Points] ワークフローを使用して XOR 無線の管理ステータスを無効にすることを推奨します。[Configure Access Points] ワークフローを使用して設定された管理ステータスは、 ワイヤレスコントローラや AP が再プロビジョニングされても上書きされません。詳細については、AP の設定（1639 ページ）を参照してください。

b) [Parent Profile] で、[High]、[Medium (Typical)]、[Low]、[Custom] のいずれかを選択します。（使用可能なデータレートおよび電力設定値は、選択された親プロファイルに応じて変わります。たとえば、[High] を選択した場合、2.4 GHz のデバイスで使用可能なプロファイル設定が入力されます。入力されたデータレートおよび電力設定のいずれかの設定を変更すると、[Parent Profile] が自動的に [Custom] に変更されます）。選択したカスタムプロファイルに対してのみ、新しい RF プロファイルが作成されます。

（注） [Low]、[Medium (Typical)]、および [High] は、デフォルトの RF プロファイルです。デフォルトの RF プロファイルを選択すると、デバイスでそれぞれの RF プロファイルが使用され、ワイヤレスコントローラ では新しい RF プロファイルは作成されません。

c) [DCA Channel] は、RF グループへのチャネルの割り当てを動的に管理し、AP 無線ごとに割り当てを評価します。

- **[すべて選択（Select All）]** チェック ボックスをオンにして、DCA チャネル **[1]**、**[6]**、および **[11]** を選択します。または、チャネル番号の横にある個々のチェックボックスをオンにします。
- 個々のチャネル番号がまだ表示されていない場合は、[Show Advanced] をクリックして、[Advanced Options] でチャネル番号を選択します。
- [Select All] チェックボックスをオンにして、[Advanced Options] の下にある DCA チャネルを選択するか、個々のチャネル番号の横にあるチェックボックスをオンにします。使用可能なチャネル番号は、[2]、[3]、[4]、[5]、[7]、[8]、[9]、[10]、[12]、[13]、[14] です。

（注）
- Cisco AireOS ワイヤレスコントローラ の場合、Catalyst Center はグローバル RRM DCA チャネルリストで選択した DCA チャネルを自動的に設定します。
- デバイスの国コードに基づいて DCA チャネルを選択します。プロビジョニングでは、ワイヤレスコントローラ で設定した国に対して使用が許可されているチャネルのみが考慮され、サポートされていないチャネルは無視されます。コントローラに設定されている国コードでは、選択したすべてのチャネルがサポート対象外になる場合、プロビジョニングに失敗する可能性があります。

d) [Supported Data Rate]で、次の設定を行います。

- [Enable 802.11b data rates] チェックボックスをオンにして、802.11b データレートを有効にします。このアクションにより、[Mandatory Data Rates] エリアの [802.11b supported data rate] チェックボックスも有効になります。
- スライダを使用して、アクセスポイントとクライアント間でデータを送信できるレートを設定します。使用可能なデータ レートは、[1]、[2]、[5.5]、[6]、[9]、[11]、[12]、[18]、[24]、[36]、[48]、[54] です。

e) [Mandatory Data Rates] で、個々のデータレートの横にあるチェックボックスをオンにします。使用可能なデータ レートは、[6]、[9]、[12]、[18]、[24]、[36]、[48]、[54] です。

802.11b データレートを有効にした場合、データレート [1]、[2]、[5.5] も使用できます。

f) [Tx Power Configuration] で、AP の電力レベルと電力しきい値を設定できます。

- [Power Level]：AP の電力を削減する必要があるかどうかを判断します。AP の電力を削減すると、同一チャネルまたは近接するチャネル上の別の AP との同一チャネル干渉を軽減するのに役立ちます。[電力レベル（Power Level）] スライダを使用して、電力レベルの最小または最大値を設定します。範囲は、-10 dBm ～ 30 dBm です。

- [RX SOP Threshold (dBm)]：RX-SOP（Receiver Start of Packet Detection Threshold）は、AP 無線機がパケットを復調してデコードする dBm 単位の Wi-Fi 信号レベルを決定します。[RX SOP Threshold (dBm)] ドロップダウンリストで、しきい値を、[High]、[Medium]、[Low]、[Auto]、[Custom] から選択します。

  [Custom] RX SOP しきい値を選択すると、[RX-SOP Threshold (dBm) Custom Value] フィールドが表示されます。このフィールドには、RX SOP しきい値のカスタム値を dBm 単位で入力します。有効な範囲は -85 dBm ～ -60 dBm です。2.4 GHz 帯域の場合、高しきい値は -79 dBm、中しきい値は -82 dBm、低しきい値は -85 dBm です。

- [TPC Power Threshold]：無線リソース管理（RRM）を使用したカットオフ信号レベルで、AP の電力を削減するかどうかを判断します。[電力しきい値（Power Threshold）] スライダを使用して電力値を増減させ、APをより高い、またはより低い伝送電力レートで動作させるようにします。範囲は -80 dBm ～ -50 dBm です。

g) [Coverage Hole Detection] で、次の設定を行います。

（注） **[Design]** > **[Feature Templates]** > **[Wireless]** > **[RRM General Configuration]** で、対応する無線帯域のグローバルカバレッジホールの検出を有効にし、管理するワイヤレスコントローラでプロビジョニングする必要があります。RRM の一般パラメータの機能テンプレートについては、RRM 一般パラメータの機能テンプレートの作成 （626 ページ）を参照してください。プロビジョニングの詳細については、ワイヤレスデバイスのプロビジョニング （735 ページ）を参照してください。

- [Minimum Client Level（clients）] フィールドに、クライアントの最小数の値を入力します。有効な範囲は 1 ～ 200 です。デフォルト値は 3 です。
- [Data RSSI Threshold (dBm)] フィールドに、データの受信信号強度表示（RSSI）しきい値を dBm で入力します。有効な範囲は -90 dBm ～ -60 dBm です。デフォルト値は -80 dBm です。
- [Voice RSSI Threshold (dBm)] フィールドに、音声 RSSI しきい値を dBm で入力します。有効な範囲は -90 dBm ～ -60 dBm です。デフォルト値は -80 dBm です。
- [Exception Level（%）] フィールドに、例外レベルを入力します。有効な範囲は 0 ～ 100 %です。デフォルト値は 25% です。

h) [Client Limit] の下の [Max Client] フィールドに、クライアント数の上限値を入力します。有効な範囲は 0 ～ 500 です。

（注） Cisco AireOS ワイヤレスコントローラ では、クライアント数の上限は設定できません。

- Cisco IOS XE のバージョンが 17.7 以前の場合、ワイヤレスコントローラ のクライアント数の上限は 200 です。
- Cisco IOS XE のバージョンが 17.7 以降 17.9 以前の場合、ワイヤレスコントローラ のクライアント数の上限は 400 です。
- Cisco IOS XE のバージョンが 17.9 以降の場合、ワイヤレスコントローラ のクライアント数の上限は 500 です。

i) [802.11ax] で、802.11ax の次の空間再利用パラメータを構成します。

（注） 802.11ax は、Cisco IOS XE 17.6.1 以降を搭載した ワイヤレスコントローラでのみサポートされます。

- [OBSS PD] チェックボックスをオンにして、オーバーラップ BSS パケット検出（OBSS-PD）機能を有効にします。
- [Non-SRG OBSS PD Max Threshold (dBm)] フィールドに、非空間再利用グループ（SRG）OBSS-PD 最大しきい値の値を dBm で入力します。有効な範囲は -82 dBm ～ -62 dBm です。デフォルト値は -62 dBm です。
- [SRG OBSS-PD] チェックボックスをオンにして、SRG OBSS-PD 機能を有効にします。

  SRG OBSS-PD は、Cisco IOS XE 17.7.1 以降を搭載した ワイヤレスコントローラ でのみサポートされます。
- [SRG OBSS PD Min Threshold (dBm)] フィールドに、SRG OBSS-PD 最小しきい値の値を dBm で入力します。有効な範囲は -82 dBm ～ -62 dBm です。デフォルト値は -82 dBm です。
- [SRG OBSS PD Max Threshold (dBm)] フィールドに、SRG OBSS-PD 最大しきい値の値を dBm で入力します。有効な範囲は -82 dBm ～ -62 dBm です。デフォルト値は -62 dBm です。

ステップ 5 [5 GHz] タブで次の設定を行います。

a) [5 GHz] トグルボタンが有効になっていることを確認します。

（注）
- Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の場合、[5 GHz] トグルボタンを無効にすると、Catalyst Center は、[5 GHz] RF プロファイルの管理ステータスを無効にします。
- Cisco AireOS ワイヤレスコントローラ の場合、[2.4 GHz] トグルボタンを無効にして、ワイヤレスコントローラ または AP を再プロビジョニングすると、Catalyst Center は、対応する帯域の RF プロファイルを作成し、そのプロファイルを AP グループにマッピングして（プロファイルを [None] として設定するのではなく）、AP で対応する無線の管理ステータスを無効にします。
- Cisco AireOS ワイヤレスコントローラの場合、RF プロファイルで 5 GHz 帯域の管理ステータスを無効にすると、Catalyst Center ではその RF プロファイルを使用する AP の XOR 無線が手動 2.4 GHz モードに変更されます。後で管理ステータスを有効にして AP を再プロビジョニングすると、 Catalyst Center では無線が自動モードに変更され、2.4 GHz および 5 GHz 帯域とモニターモードを使用できるようになります。そのため、XOR 対応 AP で 5 GHz 帯域の管理ステータスを無効にする場合は、[Configure Access Points] ワークフローを使用して XOR 無線の管理ステータスを無効にすることを推奨します。[Configure Access Points] ワークフローを使用して設定された管理ステータスは、 ワイヤレスコントローラや AP が再プロビジョニングされても上書きされません。詳細については、AP の設定（1639 ページ）を参照してください。

b) [Parent Profile] で、[High]、[Medium (Typical)]、[Low]、[Custom] のいずれかを選択します。（使用可能なデータレートおよび電力設定値は、選択された親プロファイルに応じて変わります。たとえば、[High] を選択した場合、5 GHz のデバイスで使用可能な設定が入力されます。入力されたデータレートおよび電力設定のいずれかの設定を変更すると、[Parent Profile] が自動的に [Custom] に変更されます）。選択したカスタムプロファイルに対してのみ、新しい RF プロファイルが作成されます。

（注） [Low]、[Medium (Typical)]、および [High] は、デフォルトの RF プロファイルです。デフォルトの RF プロファイルを選択すると、デバイスに既に存在するそれぞれの RF プロファイルが使用され、ワイヤレスコントローラ では新しい RF プロファイルは作成されません。

c) [Channel Width] ドロップダウンリストから、チャネル帯域幅オプション（[20 MHz]、[40 MHz]、[80 MHz]、[160 MHz]、または [Best]）を選択します。

d) このバンドでプリアンブルパンチングを有効にするには、[Preamble Puncturing] トグルボタンをクリックします。

（注） プリアンブルパンチングは、Cisco IOS XE 17.15.2 以降を実行している シスコ ワイヤレス コントローラにのみ適用されます。

e) [Zero Wait DFS] チェックボックスをオンにして、5 GHz 無線帯域の AP が待機時間なしで新しいチャネルに切り替えることを許可します。

（注） Catalyst Center は、Cisco IOS XE リリース 17.9.1 以降を実行する シスコ ワイヤレス コントローラ のゼロウェイト DFS をサポートします。

f) [DCA Channels] で次の設定を行い、チャンネルの割り当てを管理します。

（注） Cisco AireOS ワイヤレスコントローラ の場合、Catalyst Center はグローバル RRM DCA チャネルリストで選択した DCA チャネルを自動的に設定します。

デバイスの国コードに基づいて DCA チャネルを選択します。プロビジョニングでは、ワイヤレスコントローラ で設定した国に対して使用が許可されているチャネルのみが考慮され、サポートされていないチャネルは無視されます。コントローラに設定されている国コードでは、選択したすべてのチャネルがサポート対象外になる場合、プロビジョニングに失敗する可能性があります。

- [Select All] チェックボックスをオンにして、DCA チャネル**UNII-1 36-48**、**UNII-2 52-144**、および**UNII-3 149-173**を選択します。または、チャネル番号の横にある個々のチェックボックスをオンにします。
- 個々のチャネル番号がまだ表示されていない場合は、[Show Advanced] をクリックして、各帯域のチャネル番号を選択します。
- [UNII-1 36-48]：UNII-1 バンドで使用可能なチャネルは、[36]、[40]、[44]、[48] です。[UNII-1 36-48]チェックボックスをオンにしてすべてのチャネルを含めるか、チャネルのチェックボックスをオンにして、個別に選択します。
- [UNII-2 52-144]：UNII-2 バンドで使用可能なチャネルは、[52]、[56]、[60]、[64]、[100]、[104]、[108]、[112]、[116]、[120]、[124]、[128]、[132]、[136]、[140]、[144] です。[UNII-2 52-144] チェックボックスをオンにしてすべてのチャネルを含めるか、チャネルのチェックボックスをオンにして、個別に選択します。
- [UNII-3 149-173]：UNII-3 バンドで使用可能なチャネルは、[149]、[153]、[157]、[161]、[165]、[169]、および [173] です。[UNII-3 149-173] チェックボックスをオンにしてすべてのチャネルを含めるか、チャネルのチェックボックスをオンにして、個別に選択します。

g) アクセスポイントとクライアント間でデータを転送できるレートを設定するには、[サポートされているデータレート（Supported Data Rate）] スライダを使用します。使用可能なデータ レートは、[6]、[9]、[12]、[18]、[24]、[36]、[48]、[54] です。

h) [Mandatory Data Rates] で、個々のデータレートの横にあるチェックボックスをオンにします。使用可能なデータ レートは、[6]、[9]、[12]、[18]、[24]、[36]、[48]、[54] です。

i) [Tx Power Configuration] で、AP の電力レベルと電力しきい値を設定できます。

- [Power Level]：AP の電力を削減する必要があるかどうかを判断します。AP の電力を削減すると、同一チャネルまたは近接するチャネル上の別の AP との同一チャネル干渉を軽減するのに役立ちます。[電力レベル（Power Level）] スライダを使用して、電力レベルの最小または最大値を設定します。指定できる範囲は -10 ～ 30 dBm で、デフォルトは -10 dBm です。
- [RX SOP Threshold (dBm)]：RX-SOP は、AP 無線機がパケットを復調してデコードする dBm 単位の Wi-Fi 信号レベルを決定します。[RX SOP Threshold (dBm)] ドロップダウンリストで、しきい値を、[High]、[Medium]、[Low]、[Auto]、[Custom] から選択します。

  [Custom] RX SOP しきい値を選択すると、[RX-SOP Threshold (dBm) Custom Value] フィールドが表示されます。このフィールドには、RX SOP しきい値のカスタム値を dBm 単位で入力します。有効な範囲は -85 dBm ～ -60 dBm です。5 GHz 帯域の場合、高しきい値は -76 dBm、中しきい値は -78 dBm、低しきい値は -80 dBm です。
- [TPC Power Threshold]：無線リソース管理（RRM）を使用したカットオフ信号レベルで、AP の電力を削減するかどうかを判断します。[電力しきい値（Power Threshold）] スライダを使用して電力値を増減させ、AP をより高い、またはより低い伝送電力レートで動作させるようにします。指定できる範囲は -50 ～ 80 dBm で、デフォルトのしきい値は -70 dBm です。

j) [Coverage Hole Detection] で、次の設定を行います。

（注） **[Design]** > **[Feature Templates]** > **[Wireless]** > **[RRM General Configuration]** で、対応する無線帯域のグローバルカバレッジホールの検出を有効にし、管理するワイヤレスコントローラでプロビジョニングする必要があります。RRM の一般パラメータの機能テンプレートについては、RRM 一般パラメータの機能テンプレートの作成 （626 ページ）を参照してください。プロビジョニングの詳細については、ワイヤレスデバイスのプロビジョニング （735 ページ）を参照してください。

- [Minimum Client Level（clients）] フィールドに、クライアントの最小数の値を入力します。有効な範囲は 1 ～ 200 です。デフォルト値は 3 です。
- [Data RSSI Threshold (dBm)] フィールドに、データの受信信号強度表示（RSSI）しきい値を dBm で入力します。有効な範囲は -90 dBm ～ -60 dBm です。デフォルト値は -80 dBm です。
- [Voice RSSI Threshold (dBm)] フィールドに、音声 RSSI しきい値を dBm で入力します。有効な範囲は -90 dBm ～ -60 dBm です。デフォルト値は -80 dBm です。
- [Exception Level（%）] フィールドに、例外レベルを入力します。有効な範囲は 0 ～ 100 %です。デフォルト値は 25% です。

k) [Client Limit] の下の [Max Client] フィールドに、クライアント数の上限値を入力します。有効な範囲は 0 ～ 500 です。

（注） Cisco AireOS ワイヤレスコントローラ では、クライアント数の上限は設定できません。

- Cisco IOS XE のバージョンが 17.7 以前の場合、ワイヤレスコントローラ のクライアント数の上限は 200 です。
- Cisco IOS XE のバージョンが 17.7 以降 17.9 以前の場合、ワイヤレスコントローラ のクライアント数の上限は 400 です。
- Cisco IOS XE のバージョンが 17.9 以降の場合、ワイヤレスコントローラ のクライアント数の上限は 500 です。

l) [Flexible Radio Assignment（FRA）] で、[Client Aware] チェックボックスをオンにして、クライアント認識機能を有効にします。

この機能は、5 GHz の専用無線をモニターします。クライアントの負荷がしきい値を超えると、FRA がモニターロールから 5 GHz のロールに自動的に変わり、オンデマンドでセルの容量が効率的に倍増されます。容量の心配がなくなり、Wi-Fi の負荷が正常に戻ると、無線で前のロールが再開されます。

（注） **[Design]** > **[Feature Templates]** > **[Wireless]** > **[RRM FRA Configuration]** で、対応する無線帯域の FRA を有効にし、管理する ワイヤレスコントローラでプロビジョニングする必要があります。RRM FRA パラメータの機能テンプレートについては、RRM FRA パラメータの機能テンプレートの作成（624ページ）を参照してください。プロビジョニングの詳細については、ワイヤレスデバイスのプロビジョニング （735 ページ）を参照してください。

クライアント対応機能を有効にする場合は、次の設定を行います。

- [Client Select (%)] フィールドに、クライアント選択の値を入力します。有効な範囲は 0 ～ 100% です。デフォルト値は 50% です。
- [Client Reset (%)] フィールドに、クライアントのリセット値を入力します。有効な範囲は 0 ～ 100 %です。デフォルト値は 5 パーセントです。

m) [802.11ax] で、802.11ax の次の空間再利用パラメータを構成します。

（注） 802.11ax は、Cisco IOS XE 17.6.1 以降を搭載した ワイヤレスコントローラでのみサポートされます。

- [OBSS PD] チェックボックスをオンにして、オーバーラップ BSS パケット検出（OBSS-PD）機能を有効にします。

- [Non-SRG OBSS PD Max Threshold (dBm)] フィールドに、非空間再利用グループ（SRG）OBSS-PD 最大しきい値の値を dBm で入力します。有効な範囲は -82 dBm ～ -62 dBm です。デフォルト値は -62 dBm です。
- [SRG OBSS-PD] チェックボックスをオンにして、SRG OBSS-PD 機能を有効にします。

  SRG OBSS-PD は、Cisco IOS XE 17.7.1 以降を搭載した ワイヤレスコントローラ でのみサポートされます。
- [SRG OBSS PD Min Threshold (dBm)] フィールドに、SRG OBSS-PD 最小しきい値の値を dBm で入力します。有効な範囲は -82 dBm ～ -62 dBm です。デフォルト値は -82 dBm です。
- [SRG OBSS PD Max Threshold (dBm)] フィールドに、SRG OBSS-PD 最大しきい値の値を dBm で入力します。有効な範囲は -82 dBm ～ -62 dBm です。デフォルト値は -62 dBm です。

ステップ 6 [6 GHz] タブで次を設定します。

a) [6 GHz] トグルボタンが有効になっていることを確認します。

（注）
- 6 GHz 無線は、Cisco IOS XE 17.7.1 以降を搭載した ワイヤレスコントローラでしかサポートされていません。
- Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の場合、[6 GHz] トグルボタンを無効にすると、Catalyst Center は、[6 GHz] RF プロファイルの管理ステータスを無効にします。

b) [DBS Channel Width] スライダを使用して、RF プロファイルの最小および最大のチャネル幅を設定します。

使用可能なチャネル幅オプションは、[20 MHz]、[40 MHz]、[80 MHz]、[160 MHz]、または [320 MHz] です。

（注） 320 MHz のチャネル幅は、Cisco IOS XE 17.15.2 以降を実行している シスコ ワイヤレス コントローラ にのみ適用されます。

c) このバンドでプリアンブルパンチングを有効にするには、[Preamble Puncturing] トグルボタンをクリックします。

（注） プリアンブルパンチングは、Cisco IOS XE 17.15.2 以降を実行している シスコ ワイヤレス コントローラにのみ適用されます。

d) [Enable PSC Enforcing] トグルボタンを有効にして、優先スキャンチャネル（PSC）の適用を許可します。

PSCの適用は、PSC対応チャネルに優先順位を付けることにより、6GHzデバイスの接続を改善します。

（注） PSC の適用を有効にすると、非 PSC チャネルの隣のチェックボックスがグレー表示になります。

e) [DCA Channels] で次の設定を行い、チャンネルの割り当てを管理します。

- [Select All] チェックボックスをオンにしてすべての DCA チャネルを含めるか、個々のチェックボックスをオンにして個々の DCA チャネルを選択します。
  - **UNII-5 1-93**
  - **UNII-6 97-113**
  - **UNII-7 117-185**
  - **UNII-8 189-233**
- チャネル番号がまだ表示されていない場合は、[Show Advanced] をクリックして、各バンドのチャネル番号を選択します。

（注） デバイスの国コードに基づいて DCA チャネルを選択します。プロビジョニングでは、ワイヤレスコントローラ で設定した国に対して使用が許可されているチャネルのみが考慮され、サポートされていないチャネルは無視されます。コントローラに設定されている国コードでは、選択したすべてのチャネルがサポート対象外になる場合、プロビジョニングに失敗する可能性があります。

f) アクセスポイントとクライアント間でデータを転送できるレートを設定するには、[サポートされているデータレート（Supported Data Rate）] スライダを使用します。使用可能なデータ レートは、[6]、[9]、[12]、[18]、[24]、[36]、[48]、[54] です。

g) [Mandatory Data Rates] で、個々のデータレートの横にあるチェックボックスをオンにします。使用可能なデータ レートは、[6]、[9]、[12]、[18]、[24]、[36]、[48]、[54] です。

h) [Tx Power Configuration] で、AP の電力レベルと電力しきい値を設定できます。

- [Standard Power Service]：標準電源機能を備えた AP の場合、FCC 規制に準拠するには、自動周波数調整（AFC）を有効にする必要があります。AFC は、AP の位置と高さのデータを使用して、最適なチャネルと送信電力を決定し、6GHz帯域のライセンスを持つ既存ユーザーと干渉しないことを確認します。Catalyst Center の [Standard Power Service] 機能を使用して AFC を有効にすることができます。デフォルトでは、この機能は無効になっています。この機能を有効にするには、[Standard Power Service] トグルボタンをクリックします。

  この機能は、Cisco IOS XE リリース 17.12.3 以降を実行している Cisco Catalyst 9800 シリーズ ワイヤレス コントローラにのみ適用されます。この機能を無効にすると、6GHzデュアル電力モー

ドの AP は低電力屋内モードでのみ動作するように制限され、標準電力モード専用の AP では無線が完全に無効になります。

（注） この機能を適切に機能させるには、対応する ワイヤレスコントローラで AP の高さ、AP の高さの不確実性、および外部アンテナケーブル長を設定する必要があります。標準電源対応 AP を標準電源で動作させるには、国固有の規制に基づいて、サポートされている DCA チャネルを少なくとも 1 つ選択する必要があります。

- [Power Level]：AP の電力を削減する必要があるかどうかを判断します。AP の電力を削減すると、同一チャネルまたは近接するチャネル上の別の AP との同一チャネル干渉を軽減するのに役立ちます。[電力レベル（Power Level）] スライダを使用して、電力レベルの最小または最大値を設定します。範囲は、-10 dBm ～ 30 dBm です。
- [RX SOP Threshold (dBm)]：RX-SOP は、AP 無線機がパケットを復調してデコードする dBm 単位の Wi-Fi 信号レベルを決定します。[RX SOP Threshold (dBm)] ドロップダウンリストで、しきい値を、[High]、[Medium]、[Low]、[Auto]、[Custom] から選択します。

  [Custom] RX SOP しきい値を選択すると、[RX-SOP Threshold (dBm) Custom Value] フィールドが表示されます。このフィールドには、RX SOP しきい値のカスタム値を dBm 単位で入力します。有効な範囲は -85 dBm ～ -60 dBm です。6 GHz 帯域の場合、高しきい値は -76 dBm、中しきい値は -78 dBm、低しきい値は -80 dBm です。
- [TPC Power Threshold]：無線リソース管理（RRM）を使用したカットオフ信号レベルで、AP の電力を削減するかどうかを判断します。[電力しきい値（Power Threshold）] スライダを使用して電力値を増減させ、AP をより高い、またはより低い伝送電力レートで動作させるようにします。範囲は -80 dBm ～ -50 dBm です。

i) [Coverage Hole Detection] で、次の設定を行います。

（注） **[Design]** > **[Feature Templates]** > **[Wireless]** > **[RRM General Configuration]** で、対応する無線帯域のグローバルカバレッジホールの検出を有効にし、管理する ワイヤレスコントローラでプロビジョニングする必要があります。RRM の一般パラメータの機能テンプレートについては、RRM 一般パラメータの機能テンプレートの作成 （626 ページ）を参照してください。プロビジョニングの詳細については、ワイヤレスデバイスのプロビジョニング （735 ページ）を参照してください。

- [Minimum Client Level（clients）] フィールドに、クライアントの最小数の値を入力します。有効な範囲は 1 ～ 200 です。デフォルト値は 3 です。
- [Data RSSI Threshold (dBm)] フィールドに、データの受信信号強度表示（RSSI）しきい値を dBm で入力します。有効な範囲は -90 dBm ～ -60 dBm です。デフォルト値は -80 dBm です。

- [Voice RSSI Threshold (dBm)] フィールドに、音声 RSSI しきい値を dBm で入力します。有効な範囲は -90 dBm ～ -60 dBm です。デフォルト値は -80 dBm です。
- [Exception Level（%）] フィールドに、例外レベルを入力します。有効な範囲は 0 ～ 100 %です。デフォルト値は 25% です。

j) [Client Limit] の下の [Max Client] フィールドに、クライアント数の上限値を入力します。有効な範囲は 0 ～ 500 です。

（注）
- Cisco IOS XE のバージョンが 17.7 以前の場合、ワイヤレスコントローラ のクライアント数の上限は 200 です。
- Cisco IOS XE のバージョンが 17.7 以降 17.9 以前の場合、ワイヤレスコントローラ のクライアント数の上限は 400 です。
- Cisco IOS XE のバージョンが 17.9 以降の場合、ワイヤレスコントローラ のクライアント数の上限は 500 です。

k) [Flexible Radio Assignment（FRA）] で、次のタスクを実行します。

（注）
- **[Design]** > **[Feature Templates]** > **[Wireless]** > **[RRM FRA Configuration]** で、対応する無線帯域の FRA を有効にし、管理する ワイヤレスコントローラでプロビジョニングする必要があります。RRM FRA パラメータの機能テンプレートについては、RRM FRA パラメータの機能テンプレートの作成（624 ページ）を参照してください。プロビジョニングの詳細については、ワイヤレスデバイスのプロビジョニング（735 ページ）を参照してください。
- FRA は、Cisco IOS XE 17.9.1 以降を搭載した ワイヤレスコントローラ でのみサポートされます。

- [Client Reset Count] フィールドに、クライアントのリセット回数の値を入力します。有効な範囲は 0 ～ 10 です。デフォルト値は 1 です。
- [Client Utilization Threshold（%）] フィールドに、クライアントの使用率のしきい値を入力します。有効な範囲は 0 ～ 100 %です。デフォルト値は 5 パーセントです。

l) [802.11ax] で、次の設定を行います。

- [6 GHz Discovery Frames] ドロップダウンリストから、必要なオプションを [None] 、[Broadcast Probe Response] 、および [FILS Discovery] から選択します。

  6 GHz バンドが唯一の動作可能なバンドの場合は、6 GHz 検出フレームが必要です。6 GHz 検出フレームの詳細については、[Learn More] をクリックしてください。

- [Broadcast Probe Response Interval（msec）] フィールドに、ブロードキャストプローブ応答間隔をミリ秒単位で入力します。有効な範囲は 5 ミリ秒から 25 ミリ秒です。デフォルト値は 20 ミリ秒です。

m) [MULTI BSSID] で、チェックボックスをオンにして、次の複数の基本サービスセット識別子（BSSID）パラメータを有効にします。

- ターゲット起動時間
- TWT ブロードキャストのサポート

（注） **[Design]** > **[Feature Templates]** > **[Wireless]** > **[Dot11ax Configuration]** で、対応する無線帯域の複数 BSSID を有効にし、管理する ワイヤレスコントローラでプロビジョニングする必要があります。Dot11ax の機能テンプレートの詳細については、Dot11ax 設定用の機能テンプレートの作成（615 ページ）を参照してください。プロビジョニングの詳細については、ワイヤレスデバイスのプロビジョニング （735 ページ）を参照してください。

n) [802.11AX PARAMETERS] で、対応するチェックボックスをオンにして、次のパラメータを有効にします。

- ダウンリンク OFDMA
- アップリンク OFDMA
- ダウンリンク MU-MIMO
- アップリンク MU-MIMO

（注） Cisco IOS XE リリース 17.18.2 以降、これらの設定は 6 GHz 無線帯域上の対応する 802.11be 設定にも使用されます。

o) [802.11BE PARAMETERS] で、対応するチェックボックスをオンにして、次のパラメータを有効にします。

- ダウンリンク OFDMA
- アップリンク OFDMA
- ダウンリンク MU-MIMO
- アップリンク MU-MIMO
- OFDMA Multi-RU

（注） 802.11be パラメータは、Cisco IOS XE 17.15.2 以降を実行している シスコ ワイヤレス コントローラ にのみ適用されます。

Cisco IOS XE リリース 17.18.2 以降、OFDMA Uplink、OFDMA Downlink、MU-MIMO Uplink、および MU-MIMO Downlink の設定は廃止され、このセクションでは無視されます。これらの設定を構成するには、[802.11AX PARAMETERS] セクションを使用します。

[Design] > **[Feature Templates]** > **[Wireless]** > **[Dot11be Status Configuration]** で、対応する無線帯域の複数 802.11be ステータスを有効にし、管理する ワイヤレスコントローラ でプロビジョニングする必要があります。802.11be の機能テンプレートの詳細については、Dot11be ステータス設定用の機能テンプレートの作成（618 ページ）を参照してください。プロビジョニングの詳細については、ワイヤレスデバイスのプロビジョニング （735 ページ）を参照してください。

p) [SPATIAL REUSE]で、次の設定を行います。

- [OBSS PD] チェックボックスをオンにして、オーバーラップ BSS パケット検出（OBSS-PD）機能を有効にします。
- [Non-SRG OBSS PD Max Threshold (dBm)] フィールドに、非空間再利用グループ（SRG）OBSS-PD 最大しきい値の値を dBm で入力します。有効な範囲は -82 dBm ～ -62 dBm です。デフォルト値は -62 dBm です。
- [SRG OBSS-PD] チェックボックスをオンにして、SRG OBSS-PD 機能を有効にします。

  SRG OBSS-PD は、Cisco IOS XE 17.7.1 以降を搭載した ワイヤレスコントローラ でのみサポートされます。
- [SRG OBSS PD Min Threshold (dBm)] フィールドに、SRG OBSS-PD 最小しきい値の値を dBm で入力します。有効な範囲は -82 dBm ～ -62 dBm です。デフォルト値は -82 dBm です。
- [SRG OBSS PD Max Threshold (dBm)] フィールドに、SRG OBSS-PD 最大しきい値の値を dBm で入力します。有効な範囲は -82 dBm ～ -62 dBm です。デフォルト値は -62 dBm です。

ステップ 7 [Save] をクリックします。

ステップ 8 （任意） プロファイルをデフォルトの RF プロファイルとしてマークするには、[Profile Name] チェックボックスをオンにし、[Mark Default] をクリックします。**[警告（Warning）]** ウィンドウで **[OK]** をクリックします。

次のタスク

デバイスに RF プロファイル設定を適用するには、AP をプロビジョニングする必要があります。詳細については、Day 1 の Cisco AP プロビジョニング （745 ページ）を参照してください。

基本無線周波数プロファイルの編集または削除

次の手順では、基本 RF プロファイルを編集または削除する方法について説明します。

手順

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

ステップ 2 [Wireless] タブをクリックします。

ステップ 3 左側の階層ツリーから、[Global] を選択します。

ステップ 4 [RF Profiles] をクリックします。

ステップ 5 [Wireless Radio Frequency Profile] 領域で、[Basic RF Profile] タブをクリックします。

（注） [Basic RF Profile] テーブルには、[Profile Name] 、[Type] 、[2.4 GHz Data Rates] 、[5 GHz Data Rates] 、[6 GHz Data Rates] 、[Channel Width] 、および [Profile Type] に基づいて作成された 基本 RF プロファイルの数がリストされます。

ステップ 6 編集する基本プロファイル名の横にあるチェックボックスをオンにします。

ステップ 7 [Actions] ドロップダウンリストから、[Edit/View] を選択します。

（注） 一度に 1 つの基本 RF プロファイルを編集できます。

ステップ 8 [Edit Wireless Radio Frequency Profile] ウィンドウで、基本 RF プロファイル設定を構成します。詳細については、ワイヤレス無線周波数プロファイルの作成 （451 ページ）を参照してください。

ステップ 9 [Save] をクリックします。

ステップ 10 基本 RF プロファイルを削除するには、基本 RF プロファイル名の横にあるチェックボックスをオンにします。

ステップ 11 [Actions] ドロップダウンリストから、[Delete] を選択してから [Yes] をクリックします。

ステップ 12 基本 RF プロファイルをデフォルトとしてマークするには、基本 RF プロファイル名の横にあるチェックボックスをオンにします。

ステップ 13 [Action] ドロップダウンリストから、[Mark Default] を選択してから [Yes] をクリックします。

次のタスク

Cisco AireOS ワイヤレスコントローラ の場合、ワイヤレスコントローラ ですでにプロビジョニングされている RF プロファイルの DCA チャネルまたはデータレートを変更すると、Catalyst Center によって対応する無線がリセットされます。

ワイヤレスコントローラ や AP ですでにプロビジョニング済みの RF プロファイルを更新する場合は、ワイヤレスコントローラ またはAP のいずれかを再プロビジョニングする必要があります。ワイヤレスコントローラ の再プロビジョニングでは、RF プロファイルの更新もデバイスにプッシュされるため、APの再プロビジョニングは必要ありません。ワイヤレスコントローラ のプロビジョニングの詳細については、Cisco AireOS コントローラのプロビジョニング （738 ページ）およびCisco Catalyst 9800 シリーズ ワイヤレス コントローラ のプロビジョニング （782 ページ）を参照してください。

基本無線周波数プロファイルの複製

基本RFプロファイルを複製してそのコピーを作成できます。複製することにより、既存のRF プロファイルの設定を新しい RF プロファイルに再利用できます。システムとカスタムの両方の RF プロファイルを複製できます。

手順

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

ステップ 2 [Wireless] タブをクリックします。

ステップ 3 左側の階層ツリーから、[Global] を選択します。

ステップ 4 [RF Profiles] をクリックします。

ステップ 5 [Basic RF Profile] タブで、複製するプロファイル名の横にあるチェックボックスをオンにします。

ステップ 6 [Actions] ドロップダウンリストから、[Create a Clone] を選択します。

ステップ 7 [Create Wireless Radio Frequency Profile] ウィンドウの [Profile Name] フィールドに、プロファイルの一意の名前を入力します。

ステップ 8 必要に応じて RF プロファイルの設定を編集します。詳細については、ワイヤレス無線周波数プロファイルの作成 （451 ページ）を参照してください。

ステップ 9 [Save] をクリックします。

AI 無線周波数プロファイルを設定するための前提条件

- システム設定でCisco AI Network Analyticsを有効にする必要があります。詳細については、*Cisco Catalyst Center Administrator Guide*の「**Cisco AI Network Analytics データ収集の設定**」を参照してください。
- AI 拡張 RRM を有効にする必要があります。メインメニューから次を選択します。**[System]** > **[Settings]** > **[External Services]** > **[Cisco AI Analytics]**の順に選択します。[Cisco AI Analytics] ウィンドウの [AI ENHANCED RRM] エリアで、トグルボタンをクリックして AI 拡張 RRM を有効にします。
- AI RF プロファイルは、Cisco IOS XE リリース 17.7.1 以降を搭載した Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ でのみサポートされています。

（注） 3 つの帯域すべて（2.4 GHz、5 GHz、および 6 GHz）の [Group Mode] オプションが、ワイヤレスコントローラで[Auto] または [Leader] として設定されていることを確認します。

- AI RF プロファイルは、Cisco IOS XE リリース 17.9.1 以降を搭載した ワイヤレスコントローラ でのみ、6-GHz 無線に対してサポートされています。
- デバイスプロビジョニングを使用しない展開の場合、AI RF プロファイルを有効にしてサイトにプッシュするには、AI 拡張 RRM を設定するサイトに AP を割り当てる必要があります。
- **スーパー管理者**または**ネットワーク管理者**である必要があります。

AI 無線周波数プロファイルの作成

この手順では、ビルディングまたはスタンドアロンの屋外エリアの AI 無線周波数プロファイルを作成する方法について説明します。

始める前に

前提条件を満たしていることを確認します。詳細については、AI 無線周波数プロファイルを設定するための前提条件 （467 ページ）を参照してください。

手順

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

ステップ 2 [Wireless] タブをクリックします。

ステップ 3 左側の階層ツリーから、[Global] を選択します。

ステップ 4 [RF Profiles] をクリックします。

ステップ 5 [Wireless Radio Frequency Profile] エリアで、[Add] にカーソルを合わせて [AI RF Profile] を選択します。

ステップ 6 **[Create AI Radio Frequency Profile]** ウィンドウの **[Profile Name]** フィールドに、RF プロファイル名を入力します。

ステップ 7 [Basic Settings] の[Radio Frequency Settings area] エリアで、[2.4 GHz] 、[5 GHz] 、[6 GHz] チェックボックスをオンにします。

RF バンドはデフォルトでチェックされます。バンドのチェックをオフにすると、Catalyst Center では対応する RF プロファイルの管理ステータスが無効になります。

（注） [6 GHz] バンドの AI RF プロファイルは、Cisco IOS XE 17.9.1 以降を実行している Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ でサポートされています。

ステップ 8 [Busy Hours] エリアで、サイトのタイムゾーンの開始時刻と終了時刻を定義します。

（注） ビジー時間は、サイトのタイムゾーンによって異なります。ネットワーク設定でそれぞれのサイトのタイムゾーンを設定する必要があります。

ステップ 9 [Busy Hour Sensitivity] エリアで、[Low]、[Medium]、または [High] オプションボタンをクリックして、ビジー時間間隔の無線リソース管理（RRM）の感度のしきい値を定義します。

ステップ 10 [Enable RF Settings] エリアで、[2.4 GHz]、[5 GHz]または [6 GHz] 列の下にあるトグルボタンをクリックして、バンドに対応する RF 設定を有効または無効にします。

サポートされている RF 設定は次のとおりです。

- [Flexible Radio Assignment (FRA)]：FRA は帯域ごとの無線カバレッジを最適化し、冗長無線の最適なロール割り当てを決定します。
- [Dynamic Channel Assignment (DCA)]：DCA は、RF グループへのチャネルの割り当てを動的に管理し、AP 無線ごとに割り当てを評価します。
- [Transmit Power Control (TPC)]：TPC は AP の電力を管理および送信します。また、干渉の低減中に SNR を最大化します。
- [Dynamic Bandwidth Selection (DBS)]：DBS は、チャネル幅を監視および調整して、パフォーマンスと干渉のバランスをとります。

（注）
- FRA の **2.4 GHz** バンドを無効にすると、FRA の **5 GHz** バンドが自動的に無効になります。逆の場合も同様です。
- DCA の **5 GHz** バンドを無効にすると、FRA の **2.4 GHz** バンド、および FRA と DBS の **5 GHz** バンドが無効になります。
- DCA と TPC の **2.4 GHz** バンド、および DCA、TPC、DBS の **5 GHz** バンドを個別に有効にすることができます。**5 GHz** バンドの場合、DCA と DBS が無効になっているときに DBS を有効にすると、DCA も有効になります。
- DCA および DBS RF 設定で、**6 GHz** バンドをまとめて有効または無効にすることができます。TPC の **6 GHz** バンドを個別に有効にできます。
- FRA は **6 GHz** バンドではサポートされていません。

ステップ 11 [Advanced] エリアで、[2.4 GHz] トグルボタンをクリックします。

a) [DCA Channel] エリアで、[Select All] チェックボックスをオンにして、DCA チャネル [1]、[6]、および [11] を選択します。または、チャネル番号の横にある個々のチェックボックスをオンにします。

b) [Advanced Options] エリアで、[Select All] チェックボックスをオンにして、すべての DCA チャネルを選択します。

c) 個々のチャネル番号がまだ表示されていない場合は、[Show Advanced] をクリックして残りのチャネル番号を選択します。

d) 個々のチャネル番号の横にあるチェックボックスをオンにします。プロファイルで使用可能なチャネル番号は、[2]、[3]、[4]、[5]、[7]、[8]、[9]、[10]、[12]、[13]、[14] です。



（注） デバイスの国コードに基づいて DCA チャネルを選択します。プロビジョニングでは、ワイヤレスコントローラ で設定した国に対して使用が許可されているチャネルのみが考慮され、サポートされていないチャネルは無視されます。コントローラに設定されている国コードでは、選択したすべてのチャネルがサポート対象外になる場合、プロビジョニングに失敗する可能性があります。

e) [Supported Data Rate] エリアで、次の設定を行います。

- [Enable 802.11b data rates] チェックボックスをオンにして、802.11b データレートを有効にします。このアクションにより、[Mandatory Data Rates] エリアの [802.11b supported data rate] チェックボックスも有効になります。
- スライダを使用して、AP とクライアント間でデータを送信できるレートを設定します。使用可能なデータ レートは、[1]、[2]、[5.5]、[6]、[9]、[11]、[12]、[18]、[24]、[36]、[48]、[54] です。

f) [Mandatory Data Rates] エリアで、個々のデータレートの横にあるチェックボックスをオンにします。使用可能なデータレートは、[6] 、[9] 、[11] 、[12] 、[18] 、[24] 、[36} 、[48} 、[54] です。

802.11b データレートを有効にした場合、データレート [1]、[2]、[5.5] も使用できます。

g) [Tx Power Configuration] エリアで、次の設定を行います。

- [Power Level]：AP の電力を削減する必要があるかどうかを判断します。AP の電力を削減すると、同一チャネル干渉を軽減できます。[電力レベル（Power Level）]スライダを使用して、電力レベルの最小または最大値を設定します。範囲は、-10 ～ 30 dBm です。最小のデフォルトは -10 dBm で、最大のデフォルトは 30 dBm です。
- [RX SOP Threshold (dBm)]：RX-SOP（Receiver Start of Packet Detection Threshold）は、AP 無線機がパケットを復調してデコードする dBm 単位の Wi-Fi 信号レベルを決定します。[RX SOP Threshold (dBm)] ドロップダウンリストで、しきい値を、[High]、[Medium]、[Low]、[Auto]、[Custom] から選択します。

  [Custom] RX SOP しきい値を選択すると、[RX-SOP Threshold (dBm) Custom Value] フィールドが表示されます。このフィールドには、RX SOP しきい値のカスタム値を dBm 単位で入力し

ます。有効な範囲は -85 dBm ～ -60 dBm です。2.4 GHz 帯域の場合、高しきい値は -79 dBm、中しきい値は -82 dBm、低しきい値は -85 dBm です。

- [TPC Power Threshold] ：RRM を使用したカットオフ信号レベルです。AP の電力レベルを削減するかどうかを判断します。[TPC Power Threshold] スライダを使用して電力値を増減させ、AP をより高い、またはより低い伝送電力レートで動作させるようにします。範囲は -80 dBm ～ -50 dBm です。

h) [Coverage Hole Detection] で、次の設定を行います。

（注） **[Design]** > **[Feature Templates]** > **[Wireless]** > **[RRM General Configuration]** で、対応する無線帯域のグローバルカバレッジホールの検出を有効にし、管理するワイヤレスコントローラでプロビジョニングする必要があります。RRM の一般パラメータの機能テンプレートについては、RRM 一般パラメータの機能テンプレートの作成 （626 ページ）を参照してください。プロビジョニングの詳細については、ワイヤレスデバイスのプロビジョニング （735 ページ）を参照してください。

- [Minimum Client Level（clients）] フィールドに、クライアントの最小数の値を入力します。有効な範囲は 1 ～ 200 です。デフォルト値は 3 です。
- [Data RSSI Threshold (dBm)] フィールドに、データの受信信号強度表示（RSSI）しきい値を dBm で入力します。有効な範囲は -90 dBm ～ -60 dBm です。デフォルト値は -80 dBm です。
- [Voice RSSI Threshold (dBm)] フィールドに、音声 RSSI しきい値を dBm で入力します。有効な範囲は -90 dBm ～ -60 dBm です。デフォルト値は -80 dBm です。
- [Exception Level（%）] フィールドに、例外レベルを入力します。有効な範囲は 0 ～ 100 %です。デフォルト値は 25% です。

i) [CLIENT LIMIT] の下の [Max Clients] フィールドに、クライアント数の上限値を入力します。有効な範囲は 0 ～ 500 です。

（注）
- Cisco IOS XE のバージョンが 17.7.1 以前の場合、ワイヤレスコントローラ のクライアント数の上限は 200 です。
- Cisco IOS XE のバージョンが 17.7.1 以降 17.9.1 以前の場合、ワイヤレスコントローラ のクライアント数の上限は 400 です。
- Cisco IOS XE のバージョンが 17.9.1 以降の場合、ワイヤレスコントローラ のクライアント数の上限は 500 です。

j) [802.11ax] では、次の空間再利用パラメータを構成します。

（注） 802.11ax は、Cisco IOS XE 17.6.1 以降を搭載した ワイヤレスコントローラでのみサポートされます。

- [OBSS PD] チェックボックスをオンにして、オーバーラップ BSS パケット検出（OBSS-PD）機能を有効にします。
- [Non-SRG OBSS PD Max Threshold (dBm)] フィールドに、非空間再利用グループ（SRG）OBSS-PD 最大しきい値の値を dBm 単位で入力します。有効な範囲は -82 dBm ～ -62 dBm です。デフォルト値は -62 dBm です。
- [SRG OBSS-PD] チェックボックスをオンにして、SRG OBSS-PD 機能を有効にします。

  SRG OBSS-PD は、Cisco IOS XE 17.7.1 以降を搭載した ワイヤレスコントローラ でのみサポートされます。
- [SRG OBSS PD Min Threshold (dBm)] フィールドに、SRG OBSS-PD 最小しきい値の値を dBm で入力します。有効な範囲は -82 dBm ～ -62 dBm です。デフォルト値は -82 dBm です。
- [SRG OBSS PD Max Threshold (dBm)] フィールドに、SRG OBSS-PD 最大しきい値の値を dBm で入力します。有効な範囲は -82 dBm ～ -62 dBm です。デフォルト値は -62 dBm です。

ステップ 12 [Advanced] エリアで、[5 GHz] トグルボタンをクリックします。

a) （任意） このバンドで DBS を無効化する場合は、[**Channel Width**] ドロップダウンリストから、チャネル帯域幅オプション（[**20 MHz**]、[**40 MHz**]、[**80 MHz**]、または [**160 MHz**]）を選択します。

b) このバンドでプリアンブルパンチングを有効にするには、[Preamble Puncturing] トグルボタンをクリックします。

（注） プリアンブルパンチングは、Cisco IOS XE 17.15.2 以降を実行している シスコ ワイヤレス コントローラにのみ適用されます。

c) [Zero Wait DFS] チェックボックスをオンにすると、5 GHz 無線の AP を待機時間なしで新しいチャネルに切り替えることができます。

（注） Catalyst Center は、Cisco IOS XE リリース 17.9.1 以降を実行する シスコ ワイヤレス コントローラ のゼロウェイト DFS をサポートします。

d) [DBS Max Width] スライダを使用して、AI RF プロファイルのチャネル幅を設定します。

使用可能なチャネル幅オプションは、[20 MHz]、[40 MHz]、[80 MHz]、または [160 MHz] です。

[Auto Channels Logic] エリアには、Unlicensed National Information Infrastructure（UNII）無線帯域で使用可能なチャネル幅のチャネルが色分けされて表示されます。

DBS が有効な場合にのみ、[DBS Max Width] を選択できます。

DBS を無効にすると、Catalyst Centerでは静的チャネル幅を選択できます。

e) [DCA Channel] を設定して、チャネルの割り当てを管理します。

- [UNII-1 36-48]：UNII-1 バンドで使用可能なチャネルは、[36]、[40]、[44]、[48] です。
- [UNII-2 52-144]：UNII-2 バンドで使用可能なチャネルは、[52]、[56]、[60]、[64]、[100]、[104]、[108]、[112]、[116]、[120]、[124]、[128]、[132]、[136]、[140]、[144] です。
- [UNII-3 149-165]：UNII-3 バンドで使用可能なチャネルは、[149]、[153]、[157]、[161]、[165] です。

f) [Select All] チェックボックスをオンにしてすべての DCA チャネルを含めるか、個々のチェックボックスをオンにして個々の DCA チャネルを選択します。

g) [Show Advanced] をクリックして、それぞれの DCA チャネル番号を確認、選択します。

- [UNII-1 36-48] チェックボックスをオンにしてすべてのチャネルを含めるか、チャネルのチェックボックスをオンにして、個別に選択します。
- [UNII-2 52-144] チェックボックスをオンにしてすべてのチャネルを含めるか、チャネルのチェックボックスをオンにして、個別に選択します。
- [UNII-3 149-165] チェックボックスをオンにしてすべてのチャネルを含めるか、チャネルのチェックボックスをオンにして、個別に選択します。

（注） デバイスの国コードに基づいて DCA チャネルを選択します。プロビジョニングでは、ワイヤレスコントローラ で設定した国に対して使用が許可されているチャネルのみが考慮され、サポートされていないチャネルは無視されます。コントローラに設定されている国コードでは、選択したすべてのチャネルがサポート対象外になる場合、プロビジョニングに失敗する可能性があります。

h) AP とクライアント間でデータを転送できるレートを設定するには、[Supported Data Rate] スライダを使用します。使用可能なデータレートは、[6]、[9]、[11]、[12]、[18]、[24]、[36}、[48}、[54] です。

i) [Mandatory Data Rates] エリアで、個々のデータレートの横にあるチェックボックスをオンにします。使用可能なデータレートは、[6] 、[9] 、[11] 、[12] 、[18] 、[24] 、[36} 、[48} 、[54] です。

j) [Tx Power Configuration] エリアで、次の設定を行います。

- [電力レベル（Power Level）] スライダを使用して、電力レベルの最小または最大値を設定します。範囲は、-10 ～ 30 dBm です。最小のデフォルトは -10 dBm で、最大のデフォルトは 30 dBm です。
- [RX SOP Threshold (dBm)]：RX-SOP は、AP 無線機がパケットを復調してデコードする dBm 単位の Wi-Fi 信号レベルを決定します。[RX SOP Threshold (dBm)] ドロップダウンリストで、しきい値を、[High]、[Medium]、[Low]、[Auto]、[Custom] から選択します。

[Custom] RX SOP しきい値を選択すると、[RX-SOP Threshold (dBm) Custom Value] フィールドが表示されます。このフィールドには、RX SOP しきい値のカスタム値を dBm 単位で入力します。有効な範囲は -85 dBm ～ -60 dBm です。5 GHz 帯域の場合、高しきい値は -76 dBm、中しきい値は -78 dBm、低しきい値は -80 dBm です。

- [TPC Power Threshold] スライダを使用して電力値を増減させ、AP をより高い、またはより低い送信電力レートで動作させるようにします。範囲は -80 dBm ～ -50 dBm です。

k) [Coverage Hole Detection] で、次の設定を行います。

（注） **[Design]** > **[Feature Templates]** > **[Wireless]** > **[RRM General Configuration]** で、対応する無線帯域のグローバルカバレッジホールの検出を有効にし、管理するワイヤレスコントローラでプロビジョニングする必要があります。RRM の一般パラメータの機能テンプレートについては、RRM 一般パラメータの機能テンプレートの作成 （626 ページ）を参照してください。プロビジョニングの詳細については、ワイヤレスデバイスのプロビジョニング （735 ページ）を参照してください。

- [Minimum Client Level（clients）] フィールドに、クライアントの最小数の値を入力します。有効な範囲は 1 ～ 200 です。デフォルト値は 3 です。
- [Data RSSI Threshold (dBm)] フィールドに、データの受信信号強度表示（RSSI）しきい値を dBm で入力します。有効な範囲は -90 dBm ～ -60 dBm です。デフォルト値は -80 dBm です。
- [Voice RSSI Threshold (dBm)] フィールドに、音声 RSSI しきい値を dBm で入力します。有効な範囲は -90 dBm ～ -60 dBm です。デフォルト値は -80 dBm です。
- [Exception Level（%）] フィールドに、例外レベルを入力します。有効な範囲は 0 ～ 100 %です。デフォルト値は 25% です。

l) [CLIENT LIMIT] の下の [Max Clients] フィールドに、クライアント数の上限値を入力します。有効な範囲は 0 ～ 500 です。

（注）
- Cisco IOS XE のバージョンが 17.7.1 以前の場合、ワイヤレスコントローラ のクライアント数の上限は 200 です。
- Cisco IOS XE のバージョンが 17.7.1 以降 17.9.1 以前の場合、ワイヤレスコントローラ のクライアント数の上限は 400 です。
- Cisco IOS XE のバージョンが 17.9.1 以降の場合、ワイヤレスコントローラ のクライアント数の上限は 500 です。

m) [802.11ax] では、次の空間再利用パラメータを構成します。

（注） 802.11ax は、Cisco IOS XE 17.6.1 以降を搭載した ワイヤレスコントローラでのみサポートされます。

- [OBSS PD] チェックボックスをオンにして、オーバーラップ BSS パケット検出（OBSS-PD）機能を有効にします。
- [Non-SRG OBSS PD Max Threshold (dBm)] フィールドに、非空間再利用グループ（SRG）OBSS-PD 最大しきい値の値を dBm 単位で入力します。有効な範囲は -82 dBm ～ -62 dBm です。デフォルト値は -62 dBm です。
- [SRG OBSS-PD] チェックボックスをオンにして、SRG OBSS-PD 機能を有効にします。

  SRG OBSS-PD は、Cisco IOS XE 17.7.1 以降を搭載した ワイヤレスコントローラ でのみサポートされます。
- [SRG OBSS PD Min Threshold (dBm)] フィールドに、SRG OBSS-PD 最小しきい値の値を dBm で入力します。有効な範囲は -82 dBm ～ -62 dBm です。デフォルト値は -82 dBm です。
- [SRG OBSS PD Max Threshold (dBm)] フィールドに、SRG OBSS-PD 最大しきい値の値を dBm で入力します。有効な範囲は -82 dBm ～ -62 dBm です。デフォルト値は -62 dBm です。

ステップ 13 [Advanced] エリアで、[6 GHz] トグルボタンをクリックします。

a) [**DBS Width**] スライダを使用して、AI RF プロファイルの最小および最大のチャネル幅を設定します。

使用可能なチャネル幅オプションは、[20 MHz]、[40 MHz]、[80 MHz]、[160 MHz]、または [320 MHz] です。

（注） 320 MHz のチャネル幅は、Cisco IOS XE 17.15.2 以降を実行している シスコ ワイヤレス コントローラ にのみ適用されます。

[Auto Channels Logic] エリアには、UNII 無線帯域で使用可能なチャネル幅のチャネルが色分けされて表示されます。

[**DBS Width**] は、DBS が有効になっている場合にのみ選択できます。

b) このバンドでプリアンブルパンチングを有効にするには、[Preamble Puncturing] トグルボタンをクリックします。

（注） プリアンブルパンチングは、Cisco IOS XE 17.15.2 以降を実行している シスコ ワイヤレス コントローラにのみ適用されます。

c) [Enable PSC Enforcing] トグルボタンを有効にして、優先スキャンチャネル（PSC）の適用を許可します。

PSC の適用は、PSC 対応チャネルに優先順位を付けることにより、6 GHz デバイスの接続を改善します。



（注） PSC の適用を有効にすると、非 PSC チャネルの隣のチェックボックスがグレー表示になり、PSC チャネルの隣のチェック ボックスがデフォルトでオンになります。必要に応じて、使用したい PSC チャネルのチェックボックスをオフにできます。

d) [DCA Channel] を設定して、チャネルの割り当てを管理します。

- UNII-5 1-93：UNII-5 帯域で使用できるチャネルは、1、5、9、13、17、21、25、29、33、37、41、45、49、53、57、61、65 、69、73、77、81、85、89、および 93。
- UNII-6 97-113：UNII-6 帯域で使用できるチャネルは、97、101、105、109、および 113です。
- UNII-7 117-185：UNII-7 帯域で使用可能なチャネルは 117、121、125、129、133、137、141、145、149、153、157、161、165、169、173、177、181、および 185。
- UNII-8 189-233：UNII-8 帯域で使用できるチャネルは、189、193、197、201、205、209、213、217、221、225、229、および 233です。

e) [Select All] チェックボックスをオンにしてすべての DCA チャネルを含めるか、個々のチェックボックスをオンにして個々の DCA チャネルを選択します。

f) [Show Advanced] をクリックして、残りの DCA チャネル番号を選択します。

- [UNII-5 1-93] チェックボックスをオンにしてすべてのチャネルを含めるか、チャネルのチェックボックスをオンにして、個別に選択します。
- [UNII-7 117-185] チェックボックスをオンにしてすべてのチャネルを含めるか、チャネルのチェックボックスをオンにして、個別に選択します。
- [UNII-8 189-233] チェックボックスをオンにしてすべてのチャネルを含めるか、チャネルのチェックボックスをオンにして、個別に選択します。



（注） デバイスの国コードに基づいて DCA チャネルを選択します。プロビジョニングでは、ワイヤレスコントローラ で設定した国に対して使用が許可されているチャネルのみが考慮され、サポートされていないチャネルは無視されます。コントローラに設定されている国コードでは、選択したすべてのチャネルがサポート対象外になる場合、プロビジョニングに失敗する可能性があります。

g) AP とクライアント間でデータを転送できるレートを設定するには、[Supported Data Rates] スライダを使用します。使用可能なデータ レートは、[6]、[9]、[12]、[18]、[24]、[36]、[48]、[54] です。

h) [Mandatory Data Rates] エリアで、個々のデータレートの横にあるチェックボックスをオンにします。使用可能なデータ レートは、[6]、[9]、[12]、[18]、[24]、[36]、[48]、[54] です。

i) [Tx Power Configuration] エリアで、次の設定を行います。

- [Standard Power Service]：標準電源機能を備えた AP の場合、FCC 規制に準拠するには、自動周波数調整（AFC）を有効にする必要があります。AFC は、AP の位置と高さのデータを使用して、最適なチャネルと送信電力を決定し、6 GHz 帯域のライセンスを持つ既存ユーザーと干渉しないことを確認します。Catalyst Center の [Standard Power Service] 機能を使用して AFC を有効にすることができます。デフォルトでは、この機能は無効になっています。この機能を有効にするには、[Standard Power Service] トグルボタンをクリックします。

  この機能は、Cisco IOS XE リリース 17.12.3 以降を実行している Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ にのみ適用されます。この機能を無効にすると、6 GHz デュアル電力モードの AP は低電力屋内モードでのみ動作するように制限され、標準電力モード専用の AP では無線が完全に無効になります。

（注） この機能を適切に機能させるには、対応するワイヤレスコントローラで AP の高さ、AP の高さの不確実性、および外部アンテナケーブル長を設定する必要があります。標準電源対応 AP を標準電源で動作させるには、国固有の規制に基づいて、サポートされている DCA チャネルを少なくとも 1 つ選択する必要があります。

- [電力レベル（Power Level）] スライダを使用して、電力レベルの最小または最大値を設定します。範囲は、-10 ～ 30 dBm です。
- [RX SOP Threshold (dBm)]：RX-SOP は、AP 無線機がパケットを復調してデコードする dBm 単位の Wi-Fi 信号レベルを決定します。[RX SOP Threshold (dBm)] ドロップダウンリストで、しきい値を、[High]、[Medium]、[Low]、[Auto]、[Custom] から選択します。

  [Custom] RX SOP しきい値を選択すると、[RX-SOP Threshold (dBm) Custom Value] フィールドが表示されます。このフィールドには、RX SOP しきい値のカスタム値を dBm 単位で入力します。有効な範囲は -85 dBm ～ -60 dBm です。6 GHz 帯域の場合、高しきい値は -76 dBm、中しきい値は -78 dBm、低しきい値は -80 dBm です。
- [TPC Power Threshold] スライダを使用して電力値を増減させ、AP をより高い、またはより低い送信電力レートで動作させるようにします。範囲は -80 dBm ～ -50 dBm です。

j) [Coverage Hole Detection] で、次の設定を行います。

（注） **[Design]** > **[Feature Templates]** > **[Wireless]** > **[RRM General Configuration]** で、対応する無線帯域のグローバルカバレッジホールの検出を有効にし、管理するワイヤレスコントローラでプロビジョニングする必要があります。RRM の一般パラメータの機能テンプレートについては、RRM 一般パラメータの機能テンプレートの作成 （626 ページ）を参照してください。プロビジョニングの詳細については、ワイヤレスデバイスのプロビジョニング （735 ページ）を参照してください。

- [Minimum Client Level（clients）] フィールドに、クライアントの最小数の値を入力します。有効な範囲は 1 ～ 200 です。デフォルト値は 3 です。
- [Data RSSI Threshold (dBm)] フィールドに、データの受信信号強度表示（RSSI）しきい値を dBm で入力します。有効な範囲は -90 dBm ～ -60 dBm です。デフォルト値は -80 dBm です。
- [Voice RSSI Threshold (dBm)] フィールドに、音声 RSSI しきい値を dBm で入力します。有効な範囲は -90 dBm ～ -60 dBm です。デフォルト値は -80 dBm です。
- [Exception Level（%）] フィールドに、例外レベルを入力します。有効な範囲は 0 ～ 100 %です。デフォルト値は 25% です。

k) [CLIENT LIMIT] の下の [Max Clients] フィールドに、クライアント数の上限値を入力します。有効な範囲は 0 ～ 500 です。

（注）
- Cisco IOS XE のバージョンが 17.7.1 以前の場合、ワイヤレスコントローラ のクライアント数の上限は 200 です。
- Cisco IOS XE のバージョンが 17.7.1 以降 17.9.1 以前の場合、ワイヤレスコントローラ のクライアント数の上限は 400 です。
- Cisco IOS XE のバージョンが 17.9.1 以降の場合、ワイヤレスコントローラ のクライアント数の上限は 500 です。

l) [802.11ax] で、次の設定を行います。

- [6 GHz Discovery Frames] ドロップダウンリストから、必要なオプションを [None] 、[Broadcast Probe Response] 、および [FILS Discovery] から選択します。

  6 GHz バンドが唯一の動作可能なバンドの場合は、6 GHz 検出フレームが必要です。6 GHz 検出フレームの詳細については、[Learn More] をクリックしてください。
- [Broadcast Probe Response Interval（msec）] フィールドに、ブロードキャストプローブ応答間隔をミリ秒単位で入力します。有効な範囲は 5 ミリ秒から 25 ミリ秒です。デフォルト値は 20 ミリ秒です。

m) [MULTI BSSID] で、チェックボックスをオンにして、次の複数の基本サービスセット識別子（BSSID）パラメータを有効にします。

- ターゲット起動時間
- TWT ブロードキャストのサポート

（注） **[Design]** > **[Feature Templates]** > **[Wireless]** > **[Dot11ax Configuration]** で、対応する無線帯域の複数 BSSID を有効にし、管理する ワイヤレスコントローラでプロビジョニングする必要があります。Dot11ax の機能テンプレートの詳細については、Dot11ax 設定用の機能テンプレートの作成 （615 ページ）を参照してください。プロビジョニングの詳細については、ワイヤレスデバイスのプロビジョニング （735 ページ）を参照してください。

n) [802.11AX PARAMETERS] で、対応するチェックボックスをオンにして、次のパラメータを有効にします。

- ダウンリンク OFDMA
- アップリンク OFDMA
- ダウンリンク MU-MIMO
- アップリンク MU-MIMO

（注） Cisco IOS XE リリース 17.18.2 以降、これらの設定は 6 GHz 無線帯域上の対応する 802.11be 設定にも使用されます。

o) [802.11BE PARAMETERS] で、対応するチェックボックスをオンにして、次のパラメータを有効にします。

- ダウンリンク OFDMA
- アップリンク OFDMA
- ダウンリンク MU-MIMO
- アップリンク MU-MIMO
- OFDMA Multi-RU

（注） 802.11be パラメータは、Cisco IOS XE 17.15.2 以降を実行している シスコ ワイヤレス コントローラ にのみ適用されます。

Cisco IOS XE リリース 17.18.2 以降、OFDMA Uplink、OFDMA Downlink、MU-MIMO Uplink、および MU-MIMO Downlink の設定は廃止され、このセクションでは無視されます。これらの設定を構成するには、[802.11AX PARAMETERS] セクションを使用します。

[Design] > **[Feature Templates]** > **[Wireless]** > **[Dot11be Status Configuration]** で、対応する無線帯域の複数 802.11be ステータスを有効にし、管理する ワイヤレスコントローラ でプロビジョニングする必要があります。802.11be の機能テンプレートの詳細については、Dot 11be ステータス設定用の機能テンプレートの作成 （618 ページ）を参照してください。プロビジョニングの詳細については、ワイヤレスデバイスのプロビジョニング （735 ページ）を参照してください。

ステップ 14 [Save] をクリックします。

次のタスク

デバイスに RF プロファイル設定を適用するには、AP をプロビジョニングする必要があります。詳細については、Day 1 の Cisco AP プロビジョニング （745 ページ）を参照してください。

AI 無線周波数プロファイルの編集

この手順では、AI RF プロファイルを編集する方法について説明します。

始める前に

前提条件を満たしていることを確認します。詳細については、AI 無線周波数プロファイルを設定するための前提条件 （467 ページ）を参照してください。

手順

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

ステップ 2 [Wireless] タブをクリックします。

ステップ 3 左側の階層ツリーから、[Global] を選択します。

ステップ 4 [RF Profiles] をクリックします。

ステップ 5 [Wireless Radio Frequency Profile] エリアで、[AI RF Profile] タブをクリックします。

[AI RF Profile] テーブルには、[Profile Name]、[Busy Hours]、[Busy Hour Sensitivity]、[FRA]、[DCA]、[DBS]、[TPC]、および [Mapped Buildings] に基づいて作成された AI RF プロファイルの数がリストされます。

ステップ 6 編集する AI RF プロファイル名の横にあるチェックボックスをオンにします。

一度に 1 つの AI RF プロファイルを編集できます。

ステップ 7 [Edit/View] をクリックします。

ステップ 8 [Edit AI RF Profile] ウィンドウで、AI RF プロファイル設定を構成します。詳細については、AI 無線周波数プロファイルの作成 （468 ページ）を参照してください。

ステップ 9 [Save] をクリックします。

次のタスク

ワイヤレスコントローラ や AP ですでにプロビジョニング済みの RF プロファイルを更新する場合は、ワイヤレスコントローラ またはAP のいずれかを再プロビジョニングする必要があります。ワイヤレスコントローラ の再プロビジョニングでは、RF プロファイルの更新もデバイスにプッシュされるため、AP の再プロビジョニングは必要ありません。ワイヤレスコントローラ のプロビジョニングの詳細については、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のプロビジョニング （782 ページ）およびを参照してください。

AI 無線周波数プロファイルの削除

この手順では、AI RF プロファイルを削除する方法について説明します。

始める前に

前提条件を満たしていることを確認します。詳細については、AI 無線周波数プロファイルを設定するための前提条件 （467 ページ）を参照してください。

手順

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

ステップ 2 [Wireless] タブをクリックします。

ステップ 3 左側の階層ツリーから、[Global] を選択します。

ステップ 4 [RF Profiles] をクリックします。

ステップ 5 [Wireless Radio Frequency Profile] エリアで、[AI RF Profile] タブをクリックします。

[AI RF Profile] テーブルには、[Profile Name]、[Busy Hours]、[Busy Hour Sensitivity]、[FRA]、[DCA]、[DBS]、[TPC]、および [Mapped Buildings] に基づいて作成された AI RF プロファイルの数がリストされます。

ステップ 6 AI RF プロファイルを削除するには、削除する AI RF プロファイルの横にあるチェックボックスをオンにします。

ステップ 7 [Delete] をクリックし、[Yes] をクリックします。

（注） Catalyst Center では、ビルディングにすでに割り当てられている AI RF プロファイルを削除することはできません。

次のタスク

ワイヤレスコントローラ や AP ですでにプロビジョニング済みの RF プロファイルを削除する場合は、ワイヤレスコントローラ を再プロビジョニングする必要があります。AP を再プロビジョニングする必要はありません。ワイヤレスコントローラ のプロビジョニングの詳細につい

ては、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のプロビジョニング （782 ページ）およびを参照してください。

AI 無線周波数プロファイルの複製

AI RF プロファイルを複製してそのコピーを作成できます。複製することにより、既存の AI RF プロファイルの設定を新しい AI RF プロファイルに再利用できます。

手順

ステップ 1 メインメニューから次を選択します。**[Design]** > **[Network Settings]** の順に選択します。
ステップ 2 [Wireless] タブをクリックします。
ステップ 3 左側の階層ツリーから、[Global] を選択します。
ステップ 4 [RF Profiles] をクリックします。
ステップ 5 [AI RF Profile] タブをクリックします。
ステップ 6 複製するプロファイル名の横にあるチェックボックスをオンにします。
ステップ 7 [Create a Clone] をクリックします。
ステップ 8 [Create AI Radio Frequency Profile] ウィンドウの [Profile Name] フィールドに、プロファイルの一意の名前を入力します。
ステップ 9 必要に応じて RF プロファイルの設定を編集します。詳細については、AI 無線周波数プロファイルの作成 （468 ページ）を参照してください。
ステップ 10 [Save] をクリックします。

AI 拡張 RRM の設定

AI RF プロファイルをビルディングに割り当てるには、次の手順を実行します。

始める前に

前提条件を満たしていることを確認します。詳細については、AI 無線周波数プロファイルを設定するための前提条件 （467 ページ）を参照してください。

手順

ステップ 1 メインメニューから次を選択します。**[Workflows]** > **[Configure AI-Enhanced RRM]**。
ステップ 2 **[Configure AI-Enhanced RRM]** ウィンドウで、**[Let's Do it]** をクリックしてワークフローに直接移動します。
ステップ 3 **[Get Started]** ウィンドウの **[Task Name]** フィールドにタスク名を入力します。

ステップ 4 [Select Deployment Type] ウィンドウで、利用可能なオプション（[Enable Without Device Provisioning] および [Enable with Device Provisioning]）から展開タイプを選択します。

ステップ 5 [AI拡張RRMの前提条件（AI-Enhanced RRM Prerequisites）] ウィンドウで、AI 拡張 RRM を設定するための前提条件を確認し、必要な設定が完了していることを確認します。

（オプション）カード内のリンクをクリックして、対応する設定を更新します。これらの設定を更新する場合は、カードを更新して更新されたステータスを表示します。

ステップ 6 **[AI-RFプロファイルを割り当てる場所の選択（Select Locations to Assign AI-RF Profiles）]** ウィンドウで、AI 対応 RF プロファイルを割り当てる場所を選択します。

[階層の検索（Search Hierarchy）]フィールドに名前を入力してサイトを検索するか、[グローバル（Global）] を展開してサイトを選択します。

[サイト選択の概要（Site selection summary）] テーブルに次の情報が表示されます。

- 選択済みのサイト
- 場所を管理するプライマリ ワイヤレスコントローラ
- 場所を冗長化するために割り当てられたセカンダリ ワイヤレスコントローラ
- 選択した ワイヤレスコントローラ によって管理される影響を受ける場所

ワイヤレスコントローラ で AI 拡張 RRM を有効にすると、ワイヤレスコントローラ によって管理されるすべてのサイトで AI 拡張 RRM が有効になります。

たとえば、ワイヤレスコントローラが 3 つのビルディングを管理しており、1 つのビルディングで AI RF プロファイルを有効にした場合、Catalyst Center は他の 2 つのビルディングで同じ AI RF プロファイルを自動的に有効にします。

[デバイスプロビジョニングなしで有効化（Enable Without Device Provisioning）] 展開タイプを選択した場合は、次の設定を完了します。

a) すべての場所にプライマリ ワイヤレスコントローラ を割り当てます。

1. 必要な場所のチェックボックスをオンにします。
2. [プライマリWLCの割り当て/更新（Assign/Update Primary WLC）] をクリックします。
3. [プライマリワイヤレスコントローラの割り当て（Assign Primary Wireless Controller）] ダイアログボックスで、展開タイプを選択します。

次を選択できます。	下記を実行
[すべてのフロアを同じワイヤレスコントローラで管理（All floors are managed by the same wireless controller）] オプション	必要な ワイヤレスコントローラ を選択します。

次を選択できます。	下記を実行
[一部のフロアを別のワイヤレスコントローラで管理（Some floors are managed by different wireless controller(s)）] オプション	1. 必要なフロアのチェックボックスをオンにします。 2. [プライマリWLCの割り当て（Assign Primary WLC）] をクリックします。 3. [フロアのプライマリワイヤレスコントローラの割り当て（Assign Primary Wireless Controller for floor(s)）] ダイアログボックスで、必要なワイヤレスコントローラを選択します。 4. [**Assign**] をクリックします。

4. [確認（Confirm）] をクリックします。

b) （任意） 場所にセカンダリ ワイヤレスコントローラ を割り当てます。

1. 必要な場所のチェックボックスをオンにします。
2. [セカンダリWLCの割り当て/更新（Assign/Update Secondary WLC）] をクリックします。
3. [セカンダリワイヤレスコントローラの割り当て（Assign Secondary Wireless Controller）] ダイアログボックスで、展開タイプを選択します。

次を選択できます。	下記を実行
[すべてのフロアを同じワイヤレスコントローラで管理（All floors are managed by the same wireless controller）] オプション	必要な ワイヤレスコントローラ を選択します。
[一部のフロアを別のワイヤレスコントローラで管理（Some floors are managed by different wireless controller(s)）] オプション	1. 必要なフロアのチェックボックスをオンにします。 2. [セカンダリWLCの割り当て（Assign Secondary WLC）] をクリックします。 3. [フロアのセカンダリワイヤレスコントローラの割り当て（Assign Secondary Wireless Controller for floor(s)）] ダイアログボックスで、必要なワイヤレスコントローラ を選択します。 4. [**Assign**] をクリックします。

4. [確認（Confirm）] をクリックします。

（注） プライマリとセカンダリのワイヤレスコントローラは異なる必要があります。

ステップ 7 場所に割り当てる AI RF プロファイルを選択します。

次を選択できます。	下記を実行
[デバイスプロビジョニングなしでの有効化（Enable Without Device Provisioning）] 展開タイプ	[AI RFプロファイルの割り当てとタグの確認（Assign AI RF Profile and Verify Tags）] ウィンドウ。 **1.** [サイト（Sites）] テーブルで、特定の場所の [AI RFフロアの選択（Select the AI RF profile）] にあるドロップダウンリストから AI RF プロファイルを選択します。 **2.** [アクション（Actions）] 列の下にある省略記号をクリックして AI RF プロファイルを作成するか、既存の RF プロファイルをコピーするか、RF プロファイルをすべての場所に適用します。 また、**[新しいAI RFプロファイルの作成（Create New AI RF Profile）]** オプションを使用して AI RF プロファイルを作成することもできます。詳細については、AI 無線周波数プロファイルの作成 （468 ページ）を参照してください。 **3.** 各場所に割り当てられた RF タグを確認します。 Catalyst Center は、選択された RF タグを設定された RF タグに関連付けます。異なる場所の AP 全体でワイヤレスコントローラに対して一意の RF タグを作成することを推奨します。一意の RF タグを使用すると、AI 拡張 RRM から生成された実用的な洞察を各場所に適用できます。
[デバイスプロビジョニングありでの有効化（Enable Without Device Provisioning）] 展開タイプ	[AI RFプロファイルの割り当て（Assign AI RF Profile）] ウィンドウ。 **1.** [サイト（Sites）] テーブルで、特定の場所の [AI RFフロアの選択（Select the AI RF profile）] にあるドロップダウンリストから AI RF プロファイルを選択します。 **2.** [アクション（Actions）] 列の下にある省略記号をクリックして AI RF プロファイルを作成するか、既存の RF プロファイルをコピーするか、RF プロファイルをすべての場所に適用します。 また、**[新しいAI RFプロファイルの作成（Create New AI RF Profile）]** オプションを使用して AI RF プロファイルを作成することもできます。詳細については、AI 無線周波数プロファイルの作成 （468 ページ）を参照してください。

ステップ 8 **[選択したAI RFプロファイルの詳細（Details of selected AI RF Profile）]** ウィンドウで、AI 対応 RF プロファイルの [AI設定（AI Settings）]、[共通設定（Common Settings）]、[割り当て（Assignment）] の詳細を確認します。

（注） AI 拡張 RRM の計算は 30 分ごとに発生します。RRM の決定は、計算後に更新され、デバイスにプッシュされます。

ステップ 9 [Summary] ウィンドウで、設定を確認します。変更するには、[Edit] をクリックします。

ステップ 10 展開のためのタスクのスケジュールを設定します。

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

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

（注） **[Download a backup of current RF settings]** ダイアログボックスで、選択したビルディングの現在の RF 設定の詳細を含むバックアップ CSV ファイルをダウンロードできます。準備ができたら、**[Confirm]** をクリックして続行します。

後で AI 拡張 RRM を無効にする場合は、このバックアップ CSV ファイルを使用して RF プロファイル設定を更新できます。詳細については、既存の AI RF プロファイルから場所の割り当てを解除 （488 ページ）を参照してください。

ステップ 11 [Tasks] ウィンドウで、タスクの展開を監視します。

既存の AI RF プロファイルへの場所の割り当て

次の手順では、既存の AI RF プロファイルに場所を割り当てる方法について説明します。

始める前に

前提条件を満たしていることを確認します。詳細については、AI 無線周波数プロファイルを設定するための前提条件 （467 ページ）を参照してください。

手順

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

ステップ 2 [Wireless] タブをクリックします。

ステップ 3 左側の階層ツリーから、[Global] を選択します。

ステップ 4 [RF Profiles] をクリックします。

ステップ 5 [Wireless Radio Frequency Profile] エリアで、[AI RF Profile] タブをクリックします。
[AI RF Profile] テーブルに、作成された AI RF プロファイルの数が一覧表示されます。

ステップ 6 AI RF プロファイルの [Action] 列の下にある 3 つのドットをクリックします。

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

[Manage Location Assignment] ウィンドウが開きます。

ステップ 8 [Search] フィールドに名前を入力してサイトを検索するか、[All Sites] を展開してサイトを選択します。

（注）
- サイト階層は、AI 対応の場所を示しています。
- AI プロファイルの対象とならないサイトまたは建物は無効になっています。
- 建物の下のフロアは選択できません。AI 対応 RF プロファイルに建物を選択すると、その下のフロアが自動的に割り当てられます。

同じワイヤレスコントローラが他の建物を管理している場合は、[Confirm Impacted Sites] ウィンドウが開きます。

ステップ 9 確認し、[Confirm] をクリックして、選択したサイトを AI 対応 RF プロファイルに割り当てます。

ステップ 10 展開のためのタスクのスケジュールを設定します。

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

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

（注） **[Download a backup of current RF settings]** ダイアログボックスで、選択したビルディングの現在の RF 設定の詳細を含むバックアップ CSV ファイルをダウンロードできます。準備ができたら、**[Confirm]** をクリックして続行します。

後で AI 拡張 RRM を無効にする場合は、このバックアップ CSV ファイルを使用して RF プロファイル設定を更新できます。詳細については、既存の AI RF プロファイルから場所の割り当てを解除 （488 ページ）を参照してください。

ステップ 11 [Tasks] ウィンドウで、タスクの展開を監視します。

次のタスク

AI RF プロファイル対応建物のデバイスのプロビジョニング

次の手順では、AI RF プロファイルを展開するためにロケーション全体のデバイスをプロビジョニングする方法について説明します。

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

   [Inventory] ウィンドウの [Device] テーブルには、検出された AI RF プロファイルに関連付けられたデバイスが一覧表示されます。

2. プロビジョニングする AI RF プロファイルに関連付けられたデバイス名の横にあるチェックボックスをオンにします。
3. [Actions] ドロップダウンリストから、**[Provision]** > **[Provision Device]** を選択します。
4. すべての手順を実行し、[Summary] ステップで [Deploy] をクリックします。
5. [Summary] ウィンドウで、デバイスにプッシュされる残りのネットワーク設定を確認します。詳細については、ワイヤレスデバイスのプロビジョニングの概要 （735 ページ）を参照してください。

既存の AI RF プロファイルから場所の割り当てを解除

次の手順では、既存の AI RF プロファイルから場所の割り当てを解除する方法について説明します。

始める前に

前提条件を満たしていることを確認します。詳細については、AI 無線周波数プロファイルを設定するための前提条件 （467 ページ）を参照してください。

手順

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

ステップ 2 [Wireless] タブをクリックします。

ステップ 3 左側の階層ツリーから、[Global] を選択します。

ステップ 4 [RF Profiles] をクリックします。

ステップ 5 [Wireless Radio Frequency Profile] エリアで、[AI RF Profile] タブをクリックします。
[AI RF Profile] テーブルに、作成された AI RF プロファイルの数が一覧表示されます。

ステップ 6 AI RF プロファイルの [アクション（Action）] 列の下にある省略記号アイコンをクリックし、[ロケーションの割り当て解除（Unassign Locations）] を選択します。

[Unassign AI RF Profile] ウィンドウが開きます。

ステップ 7 [タスク名（Task Name）] ウィンドウの **[タスク名（Task Name）]** フィールドにタスク名を入力します。

ステップ 8 **[AI拡張RRMを無効にするロケーションを選択（Select Locations to Disable AI-Enhanced RRM）]** ウィンドウで、AI RF プロファイルを割り当て解除する場所を選択します。

ステップ 9 **[プロビジョニングされた建物の交換RFプロファイルの選択（Select Replacement RF Profiles for Provisioned Buildings）]** ウィンドウで、プロビジョニングされた建物の交換用 RF プロファイルを選択します。

（注） 該当する建物がない場合は、次のステップにスキップします。

次のいずれかのオプションを使用して、RF プロファイルを選択します。

- [利用可能な基本RFプロファイルから選択（Select from Available Basic RF Profiles）]：ドロップダウンリストから、ワイヤレス RF プロファイルを選択します。

  （注） AP が AP ゾーンに関連付けられている場合、AP ゾーンで定義されたワイヤレス RF プロファイルが、選択された RF プロファイルよりも優先されます。

- [RFプロファイル設定を含むCSVのアップロード（Upload CSV with RF Profile configurations）]：カンマ区切り値（CSV）ファイルを使用して RF プロファイル設定をアップロードします。

  1. CSV ファイルをドラッグアンドドロップ領域にドラッグアンドドロップするか、[ファイルを選択（Choose a file）] をクリックして CSV ファイルの場所を参照し、[開く（Open）] をクリックします。

     （注） これらの建物に AI RF プロファイルを割り当てたときにダウンロードした CSV ファイルをアップロードして、建物を非 AI 設定に戻すか、選択した建物に基づいてメタデータを含むカスタム CSV ファイルをダウンロードし、ワイヤレス RF プロファイルの詳細を入力してからファイルをアップロードします。ファイルの最大サイズは 10 MB です。

  2. [Upload] をクリックします。

     Catalyst Center で検証チェックが実行されます。アップロードした CSV ファイルが要件を満たしていない場合は、エラーメッセージが表示されます。

アップロードされた CSV ファイルから、選択したロケーション名に基づく RF 設定が見つかった場合、[Confirm RF Settings for Selected Locations] ウィンドウに [Location] と [Matched RF Profiles] が表示されます。

ステップ 10 **[プロビジョニングされていない建物の交換RFプロファイルの選択（Select Replacement RF Profiles for Non-Provisioned Buildings）]** ウィンドウで、プロビジョニングされていない建物の交換用 RF プロファイルを選択します。Catalyst Center

（注） 該当する建物がない場合は、次のステップにスキップします。

次のいずれかのオプションを使用して、RF プロファイルを選択します。

- [利用可能な基本RFプロファイルから選択（Select from Available Basic RF Profiles）]：ドロップダウンリストから、ワイヤレス RF プロファイルを選択します。

  （注） AP が AP ゾーンに関連付けられている場合、AP ゾーンで定義されたワイヤレス RF プロファイルが、選択された RF プロファイルよりも優先されます。

- [RFプロファイル設定を含むCSVのアップロード（Upload CSV with RF Profile configurations）]：CSV ファイルを使用して RF プロファイル設定をアップロードします。

  1. CSV ファイルをドラッグアンドドロップ領域にドラッグアンドドロップするか、[ファイルを選択（Choose a file）] をクリックして CSV ファイルの場所を参照し、[開く（Open）] をクリックします。

     （注） これらの建物に AI RF プロファイルを割り当てたときにダウンロードした CSV ファイルをアップロードして、建物を非 AI 設定に戻すか、選択した建物に基づいてメタデータを含むカスタム CSV ファイルをダウンロードし、ワイヤレス RF プロファイルの詳細を入力してからファイルをアップロードします。ファイルの最大サイズは 10 MB です。

  2. [Upload] をクリックします。

     Catalyst Center で検証チェックが実行されます。アップロードした CSV ファイルが要件を満たしていない場合は、エラーメッセージが表示されます。

アップロードされた CSV ファイルから、選択したロケーション名に基づく RF 設定が見つかった場合、[Confirm RF Settings for Selected Locations] ウィンドウに [Location] と [Matched RF Profiles] が表示されます。

ステップ 11 [Summary] ウィンドウで、設定を確認します。変更するには、[Edit] をクリックします。

ステップ 12 展開のためのタスクのスケジュールを設定します。

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

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。

- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 13 [Tasks] ウィンドウで、タスクの展開を監視します。

次のタスク

AI RF プロファイルが割り当てられたロケーション全体にデバイスをプロビジョニングして、AI RF プロファイルを展開します。

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

   [Inventory] ウィンドウの [Device] テーブルには、検出された AI RF プロファイルに関連付けられたデバイスが一覧表示されます。

2. プロビジョニングする AI RF プロファイルに関連付けられたデバイス名の横にあるチェックボックスをオンにします。
3. [Actions] ドロップダウンリストから、**[Provision]** > **[Provision Device]** を選択します。
4. すべての手順を実行し、[Summary] ステップで [Deploy] をクリックします。
5. [概要] ウィンドウで、デバイスにプッシュされる残りのネットワーク設定を確認します。詳細については、ワイヤレスデバイスのプロビジョニングの概要 （735 ページ）を参照してください。

基本無線周波数プロファイルをAI無線周波数プロファイルにアップグレードする

始める前に

前提条件を満たしていることを確認します。詳細については、AI 無線周波数プロファイルを設定するための前提条件 （467 ページ）を参照してください。

AI 拡張 RRM サービスにサイトをオンボードするには、次のサービスの少なくとも 1 つを有効にする必要があります。

- フレキシブル ラジオ アサインメント（FRA）
- 動的チャネル割り当て（DCA）
- 伝送パワー コントロール（TPC）
- 動的帯域幅選択（DBS）

手順

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

ステップ 2 [Wireless] タブをクリックします。

ステップ 3 左側の階層ツリーから、[Global] を選択します。

ステップ 4 [RF Profiles] をクリックします。

ステップ 5 AI RF プロファイルにアップグレードする基本 RF プロファイル名の横にあるチェックボックスをオンにします。

ステップ 6 [Action] ドロップダウンリストから、[Upgrade to AI] を選択します。

ステップ 7 確認ウィンドウで [Yes] をクリックします。

ステップ 8 [Edit AI RF Profile] ウィンドウで、AI RF プロファイル設定を構成します。詳細については、AI 無線周波数プロファイルの作成 （468 ページ）を参照してください。

（注） 基本 RF プロファイルが 6 GHz 帯域に 320 MHz のチャネル幅を使用している場合、AI RF プロファイルでは 160 MHz に変更されます。

AP 認証リストの作成

許可された AP のリストを Catalyst Center で設定できます。Catalyst Center は、次のタイプの AP 認証をサポートします。

- ローカル認証では、ローカルデータベースに対する認証に、AP MAC アドレス、シリアル番号、または両方が使用されます。
- AAA 認証では、認証に AAA サーバーのリストが使用されます。

シスコ ワイヤレス コントローラ をプロビジョニングするときに、AP 認証リストを選択できます。シスコ ワイヤレス コントローラ は、AP 認証リストに存在する AP からの認証要求のみにしか応答しません。

（注）
- AP 認証に MAC アドレスとシリアル番号の両方が必要な場合は、両方が AP 認証リストに追加されていることを確認してください。ワイヤレスコントローラにプロビジョニングされたAP 認証リストに認証に必要なエントリが揃っていない場合、その AP はネットワークに入れません。
- メッシュ AP（MAP）の場合、AP 認証用の MAC アドレスを追加する必要があります。
- Cisco AireOS ワイヤレスコントローラ の場合、Catalyst Center は MAC アドレスの AP しか認証しません。MAC アドレスとシリアル番号の両方を設定した場合、Cisco AireOS ワイヤレスコントローラ には MAC アドレスのみ使用されます。
- Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の場合、Catalyst Center は Cisco IOS 17.5 以降を搭載した ワイヤレスコントローラ の AP 認証リストしかサポートしません。

手順

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

ステップ 2 [Wireless] タブをクリックします。

ステップ 3 左側の階層ツリーから、[Global] を選択します。

ステップ 4 [Security Settings] をクリックします。

ステップ 5 [AP Authorization List] タブをクリックします。

ステップ 6 [AP Authorization List] テーブルで [Add] をクリックします。

ステップ 7 [AP Authorization List] スライドインペインの [List Name] フィールドに、AP 承認リストの名前を入力します。

ステップ 8 ローカル認証を設定するには、次の手順を実行します。

a) [Local Auth] タブで、[Configure Local Authorization] チェックボックスをオンにします。

b) [Type] エリアで、認証タイプを選択します。
- AP MAC アドレスを設定するには、[Mac Address] をクリックします。
- AP シリアル番号を設定するには、[Serial Number] をクリックします。

c) AP の MAC アドレスまたはシリアル番号のデータを入力するには、次のいずれかのタスクを実行します。
- AP MAC アドレスまたはシリアル番号を個別に認証リストに追加するには、[Add] をクリックします。[AP Entry] フィールドにデータを入力します。
- データを含む CSV ファイルをアップロードするには、[Upload] をクリックします。ダイアログボックスで、次の手順を実行します。

1. ドラッグ アンド ドロップ エリアに CSV ファイルをドラッグアンドドロップします。または、[Choose a file] をクリックし、ローカルに保存されている CSV ファイルを参照して選択します。

（注） CSV ファイルがない場合は、[Download] をクリックして、編集およびアップロードできる CSV ファイルをダウンロードします。

2. [Save] をクリックします。

d) （任意） 認証に MAC アドレスとシリアル番号の両方を使用するには：

1. [Mac Address] をクリックし、AP MAC アドレスデータ（8.c （493 ページ））を入力します。
2. [Serial Number] をクリックし、AP シリアル番号データ（8.c （493 ページ））を入力します。

ステップ 9 AAA 認証を設定するには、次の手順を実行します。

a) [AAA Auth] タブで、[Configure AAA Authorization] チェックボックスをオンにします。

b) AAA サーバーの AP 認証要件に基づいて、次のいずれかのタスクを実行します。

- AAA サーバが AP 認証に MAC アドレスのみを使用する場合は、[Authorize AP against MAC Address] チェックボックスをオンにします。
- AAA サーバーが AP 承認にシリアル番号のみを使用する場合は、[Authorize AP against Serial Number] チェックボックスをオンにします。
- AAA サーバーが AP 承認に MAC アドレスとシリアル番号の両方を使用する場合は、[Authorize AP against MAC Address] チェックボックスと [Authorize AP against Serial Number] チェックボックスの両方をオンにします。

c) AP エントリを AP 認証リストに追加するには、次のいずれかのタスクを実行します。

- 必要な AP エントリの横にあるプラスアイコンをクリックします。
- AP エントリをクリックし、[Add Selected] をクリックします。

（注） 複数の AP エントリを選択するには、Shift キーを押しながら AP エントリをクリックし、[Add Selected] をクリックします。

- すべての AP エントリを AP 認証リストに追加するには、[Add All] をクリックします。

[Search] フィールドを使用して、AP エントリをフィルタ処理できます。

ステップ 10 [Save] をクリックします。

AP 承認リストの編集または削除

手順

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

ステップ 2 [Wireless] タブをクリックします。

ステップ 3 左側の階層ツリーから、[Global] を選択します。

ステップ 4 [Security Settings] をクリックします。

ステップ 5 [AP Authorization List] タブをクリックします。

ステップ 6 [AP Authorization List] テーブルで、編集または削除する認証リスト名の横にあるチェックボックスをオンにします。

- AP 認証リストを編集するには、[Edit] をクリックします。[AP Authorization List] スライドインペインで、必要に応じて設定を編集し、[Save] をクリックします。詳細については、AP 認証リストの作成（492 ページ）を参照してください。
- AP 認証リストを削除するには、[Delete] をクリックしてから [Yes] をクリックします。

AP LSC 更新プロファイルの作成

次の手順を使用して、AP ローカルで有効な証明書（LSC）更新プロファイルを作成します。

プラグアンドプレイ（PnP）AP 認証用の証明書は、限定された期間で発行されます。AP LSC 更新プロファイルを使用すると、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ は、期限切れになる前に証明書を自動的に更新できます。

Before you begin

ワイヤレスコントローラ は、Cisco IOS XE リリース 17.17.1 以降を実行している必要があります。

手順

ステップ 1 ワイヤレスセキュリティ設定に移動します。

a) メインメニューから次を選択します。**[Design]** > **[Network settings]**。
b) [Wireless] タブをクリックします。
c) 左側の階層ツリーから、以下を選択します [Global] を選択します。
d) [Security Settings] をクリックします。
e) [AP LSC Certificate Renewal] タブをクリックします。

ヒント　このタブの代わりに [More] ドロップダウンがウィンドウに表示される場合は、[More] にカーソルを合わせて、このタブを選択します。

ステップ 2　[Create Profile] をクリックして、AP LSC 更新プロファイルを作成します。

ステップ 3　[Create AP LSC Certificate Renewal Profile] スライドインペイン で、次の設定を実行します。

a) [Profile Name] フィールドに、AP LSC 更新プロファイルの名前を入力します。

b) [Due Time] フィールドに、証明書の自動更新の開始時刻（日数）を入力します。

デフォルト値は 30 日間です。有効範囲は 5 ～ 60 です。

c) [Execution] で、証明書の更新方法を選択します。

- [Staggered]（推奨）：クライアントの中断を最小限に抑えるために、対象 AP の証明書を一括更新します。ワイヤレスコントローラ プロビジョニング中に再起動する AP の割合を設定できます。
- [One Shot]：対象となるすべての AP の証明書を一度に更新するため、クライアントが中断する可能性があります。

  このオプションを選択する場合は、負荷の多くない時間に証明書の更新をスケジュールすることを推奨します。

d) （任意） [Scheduler] で、[Configure Scheduler] チェックボックスをオンにして、証明書の自動更新に必要なスケジュールを設定します。

デフォルトでは、ワイヤレスコントローラ は毎日午前 12:00 に証明書を自動的に更新します。スケジュールには、ワイヤレスコントローラ のローカルタイムゾーンが使用されます。

使用可能なオプションをクリックして、必要なスケジュールを選択します。

（注）　使用可能なオプションは、[Due Time] フィールドに入力した日数によって異なります。

表 *45 :* スケジュールオプション

証明書の更新をスケジュールする場合	結果
daily	[Daily] を選択して、以下の設定を実行します。 • 証明書更新の開始時刻を選択します。 • 時間差を設けて実行する場合は、証明書の更新の終了時刻を選択します。

証明書の更新をスケジュールする場合	結果
毎週、選択した曜日	[Weekly] を選択して、以下の設定を実行します。 • 証明書の更新をスケジュールする日の横にあるチェックボックスをオンにします。 • 証明書更新の開始時刻を選択します。 • 時間差を設けて実行する場合は、証明書の更新の終了時刻を選択します。
毎月、選択した日	[Monthly] を選択して、以下の設定を実行します。 • 証明書の更新をスケジュールする日付の横にあるチェックボックスをオンにします。 • 証明書更新の開始時刻を選択します。 • 時間差を設けて実行する場合は、証明書の更新の終了時刻を選択します。

ステップ 4 [Save] をクリックします。

次のタスク

プロビジョニング中に、AP LSC 更新プロファイルを必要な ワイヤレスコントローラ に割り当てます。詳細については、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のプロビジョニング （782 ページ）およびCisco Catalyst 9000 シリーズ スイッチでの組み込みワイヤレスのプロビジョニング （795 ページ）を参照してください。

AP LSC 更新プロファイルの編集

AP のローカルで有効な証明書（LSC）更新プロファイルを編集するには、次の手順を実行します。

手順

ステップ 1 ワイヤレスセキュリティ設定に移動します。

a) メインメニューから次を選択します。**[Design]** > **[Network settings]**。
b) [Wireless] タブをクリックします。
c) 左側の階層ツリーから、以下を選択します [Global] を選択します。
d) [Security Settings] をクリックします。
e) [AP LSC Certificate Renewal] タブをクリックします。

ヒント　このタブの代わりに [More] ドロップダウンがウィンドウに表示される場合は、[More] にカーソルを合わせて、このタブを選択します。

ステップ 2　AP LSC 更新プロファイルを編集します。

a) 編集する AP LSC 更新プロファイルを選択します。
b) [編集（Edit）] をクリックします。
c) [AP LSC証明書更新プロファイルの編集（Edit AP LSC Certificate Renewal Profile）] スライドインペインで、必要に応じて設定を編集します。

詳細については、AP LSC 更新プロファイルの作成 （495 ページ）を参照してください。

d) [Save] をクリックします。

AP LSC 更新プロファイルの削除

次の手順を使用して、1 つ以上の AP ローカル署名証明書（LSC）更新プロファイルを削除します。

手順

ステップ 1　ワイヤレスセキュリティ設定に移動します。

a) メインメニューから次を選択します。**[Design]** > **[Network settings]**。
b) [Wireless] タブをクリックします。
c) 左側の階層ツリーから、以下を選択します [Global] を選択します。
d) [Security Settings] をクリックします。
e) [AP LSC Certificate Renewal] タブをクリックします。

ヒント　このタブの代わりに [More] ドロップダウンがウィンドウに表示される場合は、[More] にカーソルを合わせて、このタブを選択します。

ステップ 2　1 つ以上の AP LSC 更新プロファイルを削除します。

a) 削除する AP LSC 更新プロファイルを選択します。
b) [Delete] をクリックします。
c) ダイアログボックスで、[Delete] をクリックします。

アンカーグループの作成

最大24シスコ ワイヤレス コントローラ でアンカーグループを作成し、アンカーの優先順位を設定できます。次のデバイスをアンカーとして追加できます。

- Catalyst Center によって管理されている シスコ ワイヤレス コントローラ。
- Catalyst Center（外部の ワイヤレスコントローラ）によって管理されていない シスコ ワイヤレス コントローラ

（注） アンカーグループには 1 つ以上のアンカーを追加する必要があります。

モビリティトンネルは、ペアリングされたデバイスに存在する使用可能なワイヤレス管理 IP アドレスに基づいて確立されます。たとえば、アクティブメインのワイヤレスコントローラに IPv6 アドレスがあり、アンカーのワイヤレスコントローラにデュアルスタック（IPv4 および IPv6 の両方）で設定されたワイヤレス管理インターフェイスがある場合、モビリティトンネルは IPv6 アドレスを使用して確立されます。

アンカーの優先順位によって、アンカー間のトラフィック共有が決まります。

- 均等共有：すべてのアンカーの優先順位が同じ場合（例：1、1、および 1）。
- 部分共有：複数のアンカーの優先順位が同じ場合（例：1、1、および 2）。
- 順次共有：アンカーの優先順位が順次である場合（例：1、2、および 3）。

アンカーグループをワイヤレスネットワークプロファイルと関連付けることができます。詳細については、ネットワークプロファイルへの SSID の追加 （544 ページ） を参照してください。

手順

ステップ 1 メインメニューから次を選択します。 **[Design]** > **[Network settings]** の順にクリックします。

ステップ 2 [Wireless] タブをクリックします。

ステップ 3 左側の階層ツリーから、[Global] を選択します。

ステップ 4 [Anchor Groups] をクリックします。

[Anchor Groups] ウィンドウが開きます。

ステップ 5 [Anchor Group] テーブルで、[Add] をクリックします。

ステップ 6 [Anchor Group] スライドインペインの [Anchor Group Name] フィールドに、アンカーグループ名を入力します。

ステップ 7 管理対象 ワイヤレスコントローラ をアンカーとして追加するには、[Add Managed WLC] をクリックし、[Add Managed WLC] ダイアログボックスで次の手順を実行します。

a) アンカーを追加するデバイス名のチェックボックスをオンにします。

デバイスを検索するには、[Search Table] の検索フィールドにデバイスの名前の一部または完全な名前を入力し、Enter キーを押します。

（注） ワイヤレスコントローラ のワイヤレス管理インターフェイスに静的 IP アドレスが割り当てられている必要があります。アクティブなメインロールでプロビジョニングすることはできません。

b) [Add] をクリックします。

ステップ 8 （任意） 外部の ワイヤレスコントローラ をアンカーとして追加するには、[Add External WLC] をクリックし、[Add External WLC] ダイアログボックスで次の手順を実行します。

a) [Device Name] フィールドに、デバイス名を入力します。
b) [Device Series] ドロップダウンリストからデバイスシリーズを選択します。
c) （任意） [**Peer IPv4 Address**] フィールドに、外部ワイヤレスコントローラのワイヤレス管理 IPv4 アドレスを入力します。
d) （任意） [NAT IPv4 Address] フィールドに、ネットワークアドレス変換（NAT）IPv4 アドレスを入力します。
e) （任意） [**Peer IPv6 Address**] フィールドに、外部ワイヤレスコントローラのワイヤレス管理 IPv6 アドレスを入力します。
f) （任意） [NAT IPv6 Address] フィールドに、NAT IPv6 アドレスを入力します。
g) [MAC Address] フィールドに、デバイスの MAC アドレスを入力します。
h) [Mobility Group Name] フィールドに、モビリティグループ名を入力します。
i) （任意） [Hash] フィールドに、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のハッシュを入力します。

（注） このフィールドは、Cisco Catalyst 9800-CL ワイヤレスコントローラでのみ使用できます。

j) [Add] をクリックします。

ステップ 9 （任意） 既存の外部の ワイヤレスコントローラ をアンカーとして追加するには、[Add Existing External WLC] をクリックし、[Add Existing External WLC] ダイアログボックスで次の手順を実行します。

a) アンカーを追加するデバイス名の横にあるチェックボックスをオンにします。

デバイスを検索するには、[Search Table] の検索フィールドにデバイスの名前の一部または完全な名前を入力し、Enter キーを押します。

b) [Add] をクリックします。

ステップ 10 （任意） アンカーの優先順位を設定するには、[Priority Order] ドロップダウンリストからアンカー ワイヤレスコントローラ の優先順位を選択します。

ステップ 11 [Save] をクリックします。

アンカーグループを編集または削除

手順

ステップ 1 メインメニューから次を選択します。 **[Design]** > **[Network settings]** の順にクリックします。

ステップ 2 [Wireless] タブをクリックします。

ステップ 3 左側の階層ツリーから、[Global] を選択します。

ステップ 4 [Anchor Groups] をクリックします。

ステップ 5 [Anchor Group] テーブルで、編集または削除するアンカーグループの横にあるチェックボックスをオンにします。

- アンカーグループを編集するには、[Edit] をクリックします。[Anchor Group] スライドインペインで、アンカーを構成し、[Save] をクリックします。詳細については、アンカーグループの作成 （499 ページ）を参照してください。
- アンカーグループを削除するには、[Delete] をクリックし、[Yes] をクリックします。

AP プロファイル

AP プロファイルは、プラグアンドプレイ（PnP）、Cisco Advanced Wireless Intrusion Prevention System（aWIPS）、不正管理、およびメッシュネットワークの AP 認証設定を統合します。AP プロファイルを使用すると、AP を管理およびプロビジョニングできます。

Catalyst Center は、Cisco IOS XE デバイスと Cisco AireOS デバイスのデフォルトの AP プロファイルを提供します。デフォルトの AP プロファイルは編集できますが、削除することはできません。Catalyst Center によって生成されたサイトタグと AP グループは、デフォルトの AP プロファイルを使用します。

認証方式が証明書ベースの認証を使用する EAP-Transport Level Security（EAP-TLS）の場合、下位 CA 証明書は使用できません。AP プロファイルの EAP-TLS 認証では、ルート CA 証明書のみを使用できます。

（注） 以前のバージョンからリリース 2.3.7.x にアップグレードする場合、デフォルトでは、Catalyst Center はデフォルトの AP プロファイルを ワイヤレスコントローラにプッシュしません。ワイヤレスコントローラ のデフォルトの AP プロファイルを更新するには、[AP Profiles] ウィンドウで明示的に保存する必要があります。詳細については、AP プロファイルの編集または削除（514 ページ）を参照してください。

デフォルトの AP プロファイルを保存するときに、現在の ワイヤレスコントローラ 設定と Catalyst Centerに保存された AP プロファイル設定との間に違いがある場合、Catalyst Center はその後の再プロビジョニング時にデフォルトの AP プロファイルを ワイヤレスコントローラにプッシュします。

デフォルトの AP プロファイルを保存した後、再プロビジョニング中に Catalyst Center がデフォルトの AP プロファイルを ワイヤレスコントローラ にプッシュしないようにするオプションはありません。

Cisco IOS XE および Cisco AireOS デバイスのカスタム AP プロファイルを作成することもできます。AP プロファイルをサイトに割り当てるには、それをワイヤレス ネットワーク プロファイルに関連付けます。

Cisco IOS XE デバイスの AP プロファイルの作成

手順

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

ステップ 2 [Wireless] タブをクリックします。

ステップ 3 左側の階層ツリーから、[Global] を選択します。

ステップ 4 [AP Profiles] をクリックします。

ステップ 5 [AP Profile] テーブルで、[Add] にカーソルを合わせて [AP Profile for IOS-XE] を選択します。

ステップ 6 [Create Access Point Profile] ウィンドウで、AP プロファイルの名前を入力します。

ステップ 7 （任意） AP プロファイルの説明を入力します。

ステップ 8 この AP プロファイルがリモートテレワーカー AP または Cisco OfficeExtend AP 用である場合は、[Remote Teleworker] チェックボックスをオンにします。

[Remote Teleworker] チェックボックスは、AP プロファイルの作成時にのみ有効または無効にできます。既存の AP プロファイルに対してこのオプションを更新することはできません。

（注） リモートテレワーカー対応の AP プロファイルは、次の設定をサポートしていません。

- aWIPS アプリケーション
- 不正の検出
- メッシュ
- 電源

ステップ 9 次のタブで必要な設定を構成します。

a) [Management]：詳細については、「Cisco IOS XE デバイスの AP プロファイルの管理設定を行う（503 ページ）」を参照してください。

b) [Security]：詳細については、「Cisco IOS XE デバイスの AP プロファイルのセキュリティ設定を行う（505 ページ）」を参照してください。

c) [Mesh]：詳細については、「Cisco IOS XE デバイスの AP プロファイルのメッシュ設定を行う（506 ページ）」を参照してください。

d) [Power]：詳細については、「Cisco IOS XE デバイスの AP プロファイルの電力設定を行う（508 ページ）」を参照してください。

e) [Additional]：詳細については、「Cisco IOS XE デバイスの AP プロファイルの追加設定を行う（509 ページ）」を参照してください。

ステップ 10 [Save] をクリックします。

Cisco IOS XE デバイスの AP プロファイルの管理設定を行う

この手順を使用して、Cisco IOS XE デバイスの AP プロファイルの次の設定を行います。

- PnP 要求プロセス中に AP を安全にオンボードするための認証設定。Catalyst Center のグローバルレベルまたはサイトレベルの階層で行われた認証設定に基づいて、AP を要求する際に PnP から 802.1x（Dot1x）サプリカントと証明書がプッシュされます。AP は、Cisco ISE での認証に 802.1x サプリカントを使用します。
- AP の n 日目の認証に関する認証設定。
- コンソールアクセス、SSH、および Telnet のログイン情報。
- Cisco Discovery Protocol（CDP）を有効にし、隣接デバイスから AP を検出できるようにする。

手順

ステップ 1 [Create Access Point Profile] ウィンドウ（**[Design]** > **[Network Settings]** > **[Wireless]** > **[AP Profiles]** > **[Add]** > **[AP Profile for IOS-XE]**）で、[Management] タブをクリックします。

ステップ 2 [Access Points Authentication] エリアで、認証方式を選択します。

（注） この認証方式は、AP PnP 要求時と n 日目の認証時に使用されます。認証方式を変更すると、PnP 要求プロセスでオンボードされた AP のサービスに影響します。認証方式を変更する場合は、PnP 要求プロセスでオンボードされた AP の工場出荷時設定へのリセットを実行します。AP が別の Extensible Authentication Protocol（EAP; 拡張可能認証プロトコル）方式で参加する場合、EAP 方式は選択した認証方式によって変わります。

次の認証方式を使用できます。

- [NO-AUTH]：デフォルトの認証方式。
- [EAP-TLS]：EAP-Transport Level Security（EAP-TLS）では、証明書ベースの認証を使用します。

（注） EAP-TLS では、相互認証にクライアント証明書とサーバー証明書が使用されます。AP でクライアント証明書をサポートするために、Day-0 オンボーディングまたは PnP 要求を介して、ローカルで有効な証明書（LSC）のプロビジョニングが AP でサポートされます。

LSC の有効期限が切れると、ライセンスの有効期限が切れたことを示すメッセージが 10 分ごとに AP コンソールに表示されますが、次の再起動時までは期限切れの証明書で AP を実行できます。後続の AP の再起動時に、LSC の有効期限が切れている場合、AP はその設定を削除して、Day-0 設定に戻ります。PnP 検出プロセスが再度開始され、Catalyst Center に再起動の理由として DOT1X_LSC_EXPIRY が表示されます。

期限切れの n 日前に LSC を更新するには、Cisco IOS XE Release 17.9.6 以降を実行している AP で **capwap ap erase lsc-cert** コマンドを使用します。

- [EAP-PEAP]：EAP-Protected Extensible Authentication Protocol（EAP-PEAP）では、相互認証が提供され、脆弱なユーザーログイン情報の機密性と整合性が保証されます。またこのプロトコルでは、自身をパッシブ（盗聴）およびアクティブ（中間者）攻撃から保護し、セキュアに暗号キー関連情報を生成します。EAP-PEAP は、IEEE 802.1X 標準および RADIUS プロトコルと互換性があります。

  [EAP-PEAP] を選択した場合は、ユーザー名とパスワードを入力します。Catalyst Center によって証明書が生成され、PnP 要求プロセス中にその証明書が適用されます。

- [EAP-FAST]：EAP-Flexible Authentication through Secure Tunneling（EAP-FAST）では、相互認証が提供され、共有秘密を使用してトンネルが確立されます。このトンネルは、パスワードに基づく弱い認証方式を保護するために使用されます。Protected Access Credentials（PAC）キーと呼ばれる共有秘密は、トンネルのセキュリティを確保するときにクライアントとサーバを相互認証するために使用されます。

  [EAP-FAST] を選択した場合は、ユーザー名とパスワードを入力します。Catalyst Center によって証明書が生成され、PnP 要求プロセス中にその証明書が適用されます。

ステップ 3 [SSH and Telnet] 領域で、次の設定を行います。

a) （任意） [SSH] トグルボタンをクリックし、SSH のログイン情報を設定します。

b) （任意） [Telnet] トグルボタンをクリックし、Telnet のログイン情報を設定します。

c) [Username] フィールドに、デバイスの認証に使用する名前を入力します。

ユーザー名にスペースや山カッコ（<>）は使用できません。

（注） SSH と Telnet を無効にした場合、[Username] フィールドの指定は任意となります。

d) [Password] フィールドに、デバイスの認証に使用するパスワードを入力します。

（注） SSH と Telnet を無効にした場合、[Password] フィールドの指定は任意となります。

e) [Enable Password] フィールドにパスワードを入力し、CLI でより高い権限レベルを有効にします。

（注） SSH と Telnet を無効にした場合、[Enable Password] フィールドの指定は任意となります。

ステップ 4 [Cisco Discovery Protocol (CDP) State] エリアで [CDP State] トグルボタンをクリックし、CDP を有効または無効にします。

次のタスク

AP プロファイルのその他の必要な設定を行います。詳細については、Cisco IOS XE デバイスの AP プロファイルの作成 （502 ページ）を参照してください。

Cisco IOS XE デバイスの AP プロファイルのセキュリティ設定を行う

この手順を使用して、Cisco IOS XE デバイスの AP プロファイルの次のセキュリティ設定を行います。

- Cisco Advanced Wireless Intrusion Prevention System（aWIPS）とフォレンジックキャプチャにより、侵入の脅威を検出して軽減します。Catalyst Center は、Cisco IOS XE リリース 17.3.1 以降を実行しているデバイスの aWIPS をサポートします。
- 不正検出により、システム管理者からの明示的な許可を得ずにネットワークにインストールされている AP を検出できます。Catalyst Center は、Cisco IOS XE リリース 17.4 以降を実行しているデバイスの不正検出をサポートします。

手順

ステップ 1 [Create Access Point Profile] ウィンドウ（**[Design]** > **[Network Settings]** > **[Wireless]** > **[AP Profiles]** > **[Add]** > **[AP Profile for IOS-XE]**）で、[Security] タブをクリックします。

ステップ 2 [aWIPS and Forensic Capture Enablement] 領域で、次の設定を行います。

a) [aWIPS] トグルボタンをクリックし、aWIPS を有効または無効にします。

b) [Forensic Capture Enablement] トグルボタンをクリックし、フォレンジックキャプチャを有効または無効にします。

（注） [Forensic Capture Enablement] トグルボタンを使用するには、[aWIPS] トグルボタンを有効にする必要があります。

ステップ 3 [Rogue Detection] 領域で、次の設定を行います。

a) [Rogue Detection] トグルボタンをクリックして不正検出を有効または無効にします。

b) [Minimum RSSI] フィールドに、有効な RSSI 値を入力します。有効な範囲は -128 ～ -70 dBm です。デフォルト値は -90 dBm です。

c) [Transient Interval] フィールドに、有効な過渡間隔を秒単位で入力します。有効な過渡間隔の範囲は 120 ～ 1800 秒です。デフォルト値は 0 です

d) [Report Interval] フィールドに、有効なレポート間隔を秒単位で入力します。有効なレポート間隔の範囲は 10 ～ 300 秒です。デフォルト値は 10 秒です。

ステップ 4 [Rogue Containment] 領域で、[PMF Denial] トグルボタンをクリックして、保護された管理フレーム（PMF）を実行している不正 AP の封じ込めを有効にします。

（注） [PMF Denial] はIOS-XEバージョン 17.12 以降でサポートされています。

次のタスク

AP プロファイルのその他の必要な設定を行います。詳細については、Cisco IOS XE デバイスの AP プロファイルの作成 （502 ページ）を参照してください。

Cisco IOS XE デバイスの AP プロファイルのメッシュ設定を行う

この手順を使用して、Cisco IOS XE デバイスの AP プロファイルのメッシュ設定を行います。

始める前に

メッシュアクセスポイント（MAP）の MAC アドレスを AP 承認リストに追加してください。詳細については、AP 認証リストの作成 （492 ページ）を参照してください。

手順

ステップ 1 [Create Access Point Profile] ウィンドウ（**[Design]** > **[Network Settings]** > **[Wireless]** > **[AP Profiles]** > **[Add]** > **[AP Profile for IOS-XE]**）で、[Mesh] タブをクリックします。

ステップ 2 [Mesh] トグルボタンをクリックします。

（注） [Mesh] トグルボタンを無効にすると、既存のカスタムメッシュ設定が削除され、AP プロファイルがデバイスのデフォルトのメッシュプロファイルに関連付けられます。

ステップ 3 （任意） [Range - Root AP to Mesh AP (in feet)] フィールドに、ルートアクセスポイント（RAP）からネットワーク内の MAP までの最大範囲（フィート）を入力します。有効な範囲は 150 フィートから 132,000 フィートです。

ステップ 4 （任意） バックホール無線を介したワイヤレスクライアント関連付けを許可するには、[Backhaul Client Access] チェックボックスをオンにします。

バックホール無線には、大部分の MAP で 5 GHz 帯が使用されます。バックホール無線は、バックホールトラフィックとクライアントトラフィックの両方を伝送できます。

[Backhaul Client Access] チェックボックスがオフになっている場合、Catalyst Center はバックホール無線を介してバックホールトラフィックのみを送信し、クライアント関連付けは 2 次的な無線のみを介して送信されます。

ステップ 5 （任意） [RAP Downlink Backhaul] エリアで、必要なオプションを選択します。

お住まいの国で [5 GHz] の使用が禁止されている場合は、[2.4 GHz] を選択してください。お住まいの国で [5 GHz] の使用が許可されている場合でも、[2.4 GHz] の使用を検討してください。2.4 GHz 無線は、より長いメッシュまたはブリッジ距離をカバーできるためです。

（注）
- メッシュ AP の場合、メッシュロールを RAP に変更して AP をプロビジョニングすると、AP が再起動します。RAP ダウンリンク バックホール メッシュ設定は、再起動後に有効になります。
- RAP 設定を [5 GHz] から [2.4 GHz] に変更すると、Catalyst Center は RAP からすべての MAP に更新を伝播します。この時点で、MAP は 5 GHz ネットワークから切断され、2.4 GHz ネットワークに接続します。

ステップ 6 （任意） [Backhaul Data Rates] エリアで、[5GHz Band Radio Type] および [2.4GHz Band Radio Type] ドロップダウンリストからインターフェイスレートを選択します。

有効なバックホール インターフェイス レートは、AP に応じて、[802.11abg]、[802.11n]、[802.11ac]（5GHz 帯域無線のみ）、[802.11ax]、および [Auto] となります。バックホールは、AP 間のワイヤレス接続を作成します。利用可能な RF スペクトラムを効果的に使用するにはレート選択が重要です。このレートは、クライアント デバイスのスループットにも影響を与える可能性があります

[Auto] データレートを使用すると、各リンクは、そのリンク品質に対して可能な限り最高のレートで到達できます。

メッシュバックホールのデータレートは [Auto] に設定することをお勧めします。

ステップ 7 （任意） [Bridge Group] エリアの [Bridge Group Name] フィールドに、ブリッジグループ名（最大 10 文字）を入力します。

ブリッジグループ名によって、MAP の関連付けが制御されます。無線をグループ化すると、同じチャネル上にあってもブリッジグループ名が異なる 2 つのネットワークは互いに通信できません。この設定はまた、同一セクター（エリア）のネットワーク内に複数の RAP がある場合にも便利です。

ブリッジグループ名を入力しない場合、Catalyst Center はメッシュプロファイルに**デフォルト**のブリッジグループ名を使用します。

次のタスク

AP プロファイルのその他の必要な設定を行います。詳細については、Cisco IOS XE デバイスの AP プロファイルの作成 （502 ページ）を参照してください。

Cisco IOS XE デバイスの AP プロファイルの電力設定を行う

この手順を使用して、Cisco IOS XE デバイスの AP プロファイルの次の電力設定を行います。

- AP 電力プロファイル：AP が必要な電力を受け取っていない場合、AP は AP 電力プロファイルの設定に基づいて、ディレーティング状態で機能します。詳細については、AP 電力プロファイルの作成 （514 ページ）を参照してください。



（注） 電力設定は、Cisco IOS XE リリース 17.10.1 以降を実行しているシスコ ワイヤレス コントローラにのみ適用されます。

- カレンダー電力プロファイル：省電力モードの AP のカレンダー電力プロファイルを作成できます。必要に応じて、複数の AP 電力プロファイルを別のカレンダースケジュールにマッピングできます。Catalyst Center は、設定されたスケジュールに基づいて、AP 電力プロファイルで定義されたすべてのルールを同時に実行します。

手順

ステップ 1 [Create Access Point Profile] ウィンドウ（**[Design]** > **[Network Settings]** > **[Wireless]** > **[AP Profiles]** > **[Add]** > **[AP Profile for IOS-XE]**）で、[Power] タブをクリックします。

ステップ 2 [AP Power Profile] エリアで、[Select Value] ドロップダウンリストから電力プロファイルを選択します。

（電力プロファイルを作成するには、[Create New] をクリックしてパラメータを設定します。詳細については、「AP 電力プロファイルの作成 （514 ページ）」を参照してください。）

ステップ 3 [Calendar Power Profile] 領域で、次の手順を実行します。

a) カレンダー電力プロファイルを追加するには、[Add] をクリックします。[Add Calendar Power Profile] スライドインペインで、次の手順を実行します。

1. [Select Power Profile] ドロップダウンリストから電力プロファイルを選択します。

   電力プロファイルを作成するには、[Create New] をクリックしてパラメータを設定します。詳細については、AP 電力プロファイルの作成 （514 ページ）を参照してください。

2. AP に電力プロファイルルールを適用するための繰り返し頻度を選択します。

   - [Daily]：AP に毎日電力プロファイルルールを適用します。
   - [Weekly]：毎週選択した曜日に AP に電力プロファイルルールを適用します。必要な曜日をクリックして選択します。
   - [Monthly]：毎月選択した日付に AP に電力プロファイルルールを適用します。必要な日付をクリックして選択します。

3. 電力プロファイルルールの開始時刻と終了時刻を指定します。
4. [Save] をクリックします。

b) （任意） 電力プロファイルルールを編集するには、対応する電力プロファイル名の横にあるチェックボックスをオンにし、[Edit] をクリックします。[Edit Power Profile] スライドインペインで、必要なパラメータを編集して [Save] をクリックします。

c) （任意） 電力プロファイルを削除するには、対応する電力プロファイル名の横にあるチェックボックスをオンにし、[Delete]、[Yes] の順にクリックします。

次のタスク

AP プロファイルのその他の必要な設定を行います。詳細については、Cisco IOS XE デバイスの AP プロファイルの作成 （502 ページ）を参照してください。

Cisco IOS XE デバイスの AP プロファイルの追加設定を行う

この手順を使用して、Cisco IOS XE デバイスの AP プロファイルの次の追加設定を行います。

- 国コード：国コードがまだ設定されていないその他の地域（ROW）ドメインAPの国コードを設定します。

（注） 国コードの設定は、すでに国コードが設定されている AP には影響しません。

- タイムゾーン：AP のタイムゾーンを選択します。
- クライアント制限：許可されるクライアントの最大数を指定します。

手順

ステップ 1 [Create Access Point Profile] ウィンドウ（**[Design]** > **[Network Settings]** > **[Wireless]** > **[AP Profiles]** > **[Add]** > **[AP Profile for IOS-XE]**）で、[Additional] タブをクリックします。

ステップ 2 [Country Code] エリアで、[Select Value] ドロップダウンリストから国コードが設定されていない ROW AP の国を選択します。

ステップ 3 [Time Zone] 領域で、次のいずれかのオプションを選択します。

- [Not Configured]：AP は UTC のタイムゾーンで動作します。
- [Controller]：AP は シスコ ワイヤレス コントローラのタイムゾーンで動作します。
- [Delta from Controller]：APはワイヤレスコントローラのタイムゾーンからのオフセットで動作します。次のオフセット値を設定します。
  - [HH]：時間の値を入力します。有効な範囲は 12 ～ 14 です。
  - [MM]：分の値を入力します。有効な範囲は 0 ～ 59 です。

ステップ 4 [Client Limit] エリアにクライアント数の上限値を入力します。有効な範囲は 0 ～ 1,200 です。

次のタスク

AP プロファイルに必要な設定をすべて指定したら、[Save] をクリックします。詳細については、Cisco IOS XE デバイスの AP プロファイルの作成 （502 ページ）を参照してください。

Cisco AireOS デバイスの AP プロファイルの作成

Cisco AireOS デバイスの場合、AP プロファイルは、AP レベルのパラメータと設定をグループ化します。AP プロファイルは、カスタム AP グループにマッピングできます。AP がプロビジョニングされると、対応する AP グループ内のすべての AP が、AP プロファイルで提供される設定を使用して設定されます。

手順

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

ステップ 2 [Wireless] タブをクリックします。

ステップ 3 左側の階層ツリーから、[Global] を選択します。

ステップ 4 [AP Profiles] をクリックします。

ステップ 5 [AP Profile] テーブルで、[Add] にカーソルを合わせて [AP Profile for AireOS] を選択します。

ステップ 6 [Create Access Point Profile] ウィンドウで、AP プロファイルの名前を入力します。

ステップ 7 （任意） AP プロファイルの説明を入力します。

ステップ 8 この AP プロファイルがリモートテレワーカー AP または Cisco OfficeExtend AP 用である場合は、[Remote Teleworker] チェックボックスをオンにします。

[Remote Teleworker] チェックボックスは、AP プロファイルの作成時にのみ有効または無効にできます。既存の AP プロファイルに対してこのオプションを更新することはできません。

（注） リモートテレワーカー対応の AP プロファイルは、次の設定をサポートしていません。

- 不正の検出
- メッシュ

ステップ 9 次のタブで必要な設定を構成します。

a) [Management]：詳細については、「Cisco AireOS デバイスの AP プロファイルの管理設定を行う （511 ページ）」を参照してください。

b) [Security]：詳細については、「Cisco AireOS デバイスの AP プロファイルのセキュリティ設定 （512 ページ）」を参照してください。

c) [Mesh]：詳細については、「Cisco AireOS デバイスの AP プロファイルのメッシュ設定 （513 ページ）」を参照してください。

ステップ 10 [Save] をクリックします。

Cisco AireOS デバイスの AP プロファイルの管理設定を行う

この手順を使用して、Cisco AireOS デバイスの AP プロファイルの以下の設定を行います。

- コンソールアクセス、SSH、および Telnet のログイン情報。
- Cisco Discovery Protocol（CDP）を有効にし、隣接デバイスから AP を検出できるようにします。

手順

ステップ 1 [Create Access Point Profile] ウィンドウ（**[Design]** > **[Network Settings]** > **[Wireless]** > **[AP Profiles]** > **[Add]** > **[AP Profile for AireOS]**）で、[Management] タブをクリックします。

ステップ 2 [SSH and Telnet] 領域で、次の設定を行います。

a) （任意） [SSH] トグルボタンをクリックし、SSH のログイン情報を設定します。

b) （任意） [Telnet] トグルボタンをクリックし、Telnet のログイン情報を設定します。

c) [Username] フィールドに、デバイスの認証に使用する名前を入力します。

ユーザー名にスペースや山カッコ（<>）は使用できません。

（注） SSH と Telnet を無効にした場合、[Username] フィールドの指定は任意となります。

d) [Password] フィールドに、デバイスの認証に使用するパスワードを入力します。

（注） SSH と Telnet を無効にした場合、[Password] フィールドの指定は任意となります。

e) [Enable Password] フィールドにパスワードを入力し、CLI でより高い権限レベルを有効にします。

（注） SSH と Telnet を無効にした場合、[Enable Password] フィールドの指定は任意となります。

ステップ 3 [Cisco Discovery Protocol (CDP) State] エリアで [CDP State] トグルボタンをクリックし、CDP を有効または無効にします。

次のタスク

AP プロファイルのその他の必要な設定を行います。詳細については、Cisco AireOS デバイスの AP プロファイルの作成 （510 ページ）を参照してください。

Cisco AireOS デバイスの AP プロファイルのセキュリティ設定

この手順を使用して、Cisco AireOS デバイスの AP プロファイルの不正検出を設定します。不正検出により、システム管理者からの明示的な許可を得ずにネットワークにインストールされている AP を検出できます。

手順

ステップ 1 [Create Access Point Profile] ウィンドウ（**[Design]** > **[Network Settings]** > **[Wireless]** > **[AP Profiles]** > **[Add]** > **[AP Profile for AireOS]**）で、[Security] タブをクリックします。

ステップ 2 [Rogue Detection] エリアで、[Rogue Detection] トグルボタンをクリックして不正検出を有効または無効にします。

次のタスク

AP プロファイルのその他の必要な設定を行います。詳細については、Cisco AireOS デバイスの AP プロファイルの作成 （510 ページ）を参照してください。

Cisco AireOS デバイスの AP プロファイルのメッシュ設定

この手順を使用して、Cisco AireOS デバイスの AP プロファイルのメッシュ設定を行います。

始める前に

MAP の MAC アドレスを AP 承認リストに追加してください。詳細については、AP 認証リストの作成 （492 ページ）を参照してください。

手順

ステップ 1 [Create Access Point Profile] ウィンドウ（**[Design]** > **[Network Settings]** > **[Wireless]** > **[AP Profiles]** > **[Add]** > **[AP Profile for AireOS]**）で、[Mesh] タブをクリックします。

ステップ 2 [Mesh] トグルボタンをクリックします。

ステップ 3 （任意） [RAP Downlink Backhaul] エリアで、必要なオプションの横にあるオプションボタンをクリックします。

お住まいの国で [5 GHz] の使用が禁止されている場合は、[2.4 GHz] を選択してください。お住まいの国で [5 GHz] の使用が許可されている場合でも、[2.4 GHz] の使用を検討してください。2.4 GHz 無線は、より長いメッシュまたはブリッジ距離をカバーできるためです。

（注）
- メッシュ AP の場合、メッシュロールを RAP に変更して AP をプロビジョニングすると、AP が再起動します。RAP ダウンリンク バックホール メッシュ設定は、再起動後に有効になります。
- RAP 設定を [5 GHz] から [2.4 GHz] に変更すると、Catalyst Center は RAP からすべての MAP に更新を伝播します。この時点で、MAP は 5 GHz ネットワークから切断され、2.4 GHz ネットワークに接続します。

ステップ 4 （任意）[Bridge Group] エリアの [Bridge Group Name] フィールドに、ブリッジグループ名（最大 10 文字）を入力します。

ブリッジグループ名によって、MAP の関連付けが制御されます。無線をグループ化すると、同じチャネル上にあってもブリッジグループ名が異なる 2 つのネットワークは互いに通信できません。この設定はまた、同一セクター（エリア）のネットワーク内に複数の RAP がある場合にも便利です。

ブリッジグループ名を入力しない場合、Catalyst Center はメッシュプロファイルに**デフォルト**のブリッジグループ名を使用します。

次のタスク

AP プロファイルに必要な設定をすべて指定したら、[Save] をクリックします。詳細については、Cisco AireOS デバイスの AP プロファイルの作成 （510 ページ）を参照してください。

AP プロファイルの編集または削除

手順

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

ステップ 2 [Wireless] タブをクリックします。

ステップ 3 左側の階層ツリーから、[Global] を選択します。

ステップ 4 [AP Profiles] をクリックします。

ステップ 5 [AP Profile] テーブルで、編集または削除する AP プロファイル名の横にあるチェックボックスをオンにします。

- AP プロファイルを編集するには、[Edit] をクリックします。[Edit Access Point Profile] スライドインペインで、必要に応じて設定を編集し、[Save] をクリックします。詳細については、Cisco AireOS デバイスの AP プロファイルの作成 （510 ページ）およびCisco IOS XE デバイスの AP プロファイルの作成 （502 ページ）を参照してください。
- AP プロファイルを削除するには、[Delete] をクリックしてから [Yes] をクリックします。

AP 電力プロファイルの作成

Cisco IOS XE リリース 17.10.1 以降を実行しているシスコ ワイヤレス コントローラの AP 電力プロファイルを作成できます。AP プロファイルに関連付けることにより、AP 電力プロファイルを AP に割り当てます。AP 電力プロファイルの複数のルールを定義し、ルールの順序を指定できます。

手順

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

ステップ 2 [Wireless] タブをクリックします。

ステップ 3 左側の階層ツリーから、[Global] を選択します。

ステップ 4 [Power Profile] をクリックします。

ステップ 5 [AP Power Profile] テーブルで、[Add] をクリックします。

ステップ 6 [Create Power Profile] スライドインペイン の [Power Profile Name] フィールドで、AP 電力プロファイルの名前を入力します。

ステップ 7 （任意） [Description] フィールドに、AP 電力プロファイルの説明を入力します。

ステップ 8 [Add] をクリックして、AP 電力プロファイルのルールを作成します。

ステップ 9 [Rule] ダイアログボックスで、次の設定を行います。

a) [Interface] ドロップダウンリストからインターフェイスのタイプを選択します。

b) [Interface ID] ドロップダウンリストからインターフェイス ID を選択します。

（注） 使用可能なインターフェイス ID が 1 つだけの場合、Catalyst Center で使用可能なインターフェイス ID が自動的に選択されます。

c) [Parameter] ドロップダウンリストからパラメータを選択します。

（注） 使用可能なパラメータが 1 つだけの場合、Catalyst Center で使用可能なパラメータが自動的に選択されます。

d) [Parameter Value] ドロップダウンリストからパラメータ値を選択します。

（注） 使用可能なパラメータ値が 1 つだけの場合、Catalyst Center で使用可能なパラメータ値が自動的に選択されます。

e) [Add] をクリックします。

ステップ 10 （任意） AP 電力プロファイルの別のルールを作成するには、「ステップ 8 （515 ページ）」と「ステップ 9 （515 ページ）」を繰り返します。

ステップ 11 （任意） [Rules] テーブルのルールの順序を更新するには、対応する アイコンをクリックし、ルールを必要な位置にドラッグアンドドロップします。

ステップ 12 [Save] をクリックします。

次のタスク

AP 電力プロファイルと AP プロファイルを関連付けます。詳細については、Cisco IOS XE デバイスの AP プロファイルの作成 （502 ページ）を参照してください。

AP 電力プロファイルの編集または削除

手順

ステップ 1 メインメニューから次を選択します。 **[Design]** > **[Network settings]** の順にクリックします。

ステップ 2 [Wireless] タブをクリックします。

ステップ 3 左側の階層ツリーから、[Global] を選択します。

ステップ 4 [Power Profile] をクリックします。

ステップ 5 [AP Power Profile] テーブルで、編集または削除する AP 電力プロファイル名の横にあるチェックボックスをオンにします。

- AP 電力プロファイルを編集するには、[Edit] をクリックします。[Edit Power Profile] スライドインペインで、必要に応じて説明、ルール、順序を編集し、[Save] をクリックします。詳細については、AP 電力プロファイルの作成 （514 ページ）を参照してください。
- AP 電力プロファイルを削除するには、[Delete] をクリックしてから [Yes] をクリックします。

非ファブリック展開用の Cisco センサー SSID のプロビジョニング

- Cisco センサー プロビジョニング サービス セット識別子（SSID）は、プラグアンドプレイ（PnP）サーバーと通信し、テストを実行するための Day-0 設定を取得します。

（注） Cisco センサープロビジョニング SSID は、センサーとして動作する AP には適用されません。

- ファブリック展開の場合、Cisco センサープロビジョニング SSID は、Catalyst Center と通信するためにインフラストラクチャ仮想ネットワーク アクセスポイント（INFRA VN-AP）プールにマッピングされます。
- 次のプラットフォームは Cisco センサープロビジョニング SSID をサポートしています。
  - Cisco AireOS ワイヤレスコントローラ

- Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ（ファブリック展開と非ファブリック展開の両方）

- Ciscoセンサープロビジョニング SSIDは次のネットワークコントローラをサポートしています。
  - Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ（クラウド用）
  - Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ
  - Cisco AireOS ワイヤレスコントローラ

次の手順で、非ファブリック展開の Cisco センサープロビジョニング SSID を設定できます。

手順

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

ステップ 2 [Wireless] タブをクリックします。

ステップ 3 [SSIDs] をクリックします。

ステップ 4 [SSID] テーブルから、Add にカーソルを合わせて、[Enterprise] を選択します。

ワイヤレス SSID ワークフローが開きます。

ステップ 5 [Basic Settings] ウィンドウで、[Sensor] フィールドをクリックし、[Next] をクリックします。

（注） SSID のパラメータは自動的に入力され、編集できません。

ステップ 6 [プロファイルへのSSIDの関連付け（Associate SSID to Profile）] ウィンドウの左側のペインで、プロファイルを選択し、次の手順を実行します。

a) [Fabric] で [Yes] を選択します。
b) [Associate Profile] をクリックします。
c) [Next] をクリックします。

（注） プロファイルがない場合は、[Add Profile] をクリックして、プロファイル設定を指定します。

ステップ 7 [Summary] ウィンドウで、設定を確認します。

ステップ 8 [**保存（Save**）] をクリックします。

ステップ 9 メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。

ステップ 10 デバイスの横にあるチェックボックスをオンにして、[Actions] ドロップダウンリストから、**[Provision]** > **[Provision Device]**を選択します。

ステップ 11 **[Assign Site]**、**[Configuration]**、**[Feature Templates]**、**[Advanced Configuration]**、および **[Summary]** で詳細を確認します。各画面で [Next] をクリックしてください。

ステップ 12 [Deploy] をクリックします。

[Provision Device] ダイアログボックスが表示されます。

ステップ 13 [Now] を選択し、[Apply] をクリックします。

結果：「Task Scheduled view status in Tasks」というメッセージが右下隅に表示されます。

ステップ 14 （任意） デバイスで構成を展開すると、[Task Progress] バーに、**[Activities]** > **[Tasks]**で進行中のプロビジョニングタスクの進行状況が表示されます（タスク名をクリックすると表示されます）。

バックホール設定の管理

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

手順

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

[Sensor List] ウィンドウが表示されます。

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

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

a) [Add Backhaul] をクリックします。

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

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

c) [Wired Backhaul] 領域で、次の設定を行います。

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

- [EAP-TLS]：[Enroll Using Certificate Bundle] または [Enroll Using SCEP] を選択します。

  [Enroll Using Certificate Bundle] を選択した場合は、[Certificate Bundle] の下にあるドロップダウン矢印をクリックし、[+ Add New Certificate Bundle] をクリックして、ユーザー名と証明書バンドルパスワードを入力します。

- [PEAP-TLS]：[Enroll Using Certificate Bundle] または [Enroll Using SCEP] を選択します。

  [Enroll Using Certificate Bundle] を選択した場合は、[Certificate Bundle] の下にあるドロップダウン矢印をクリックし、[+ Add New Certificate Bundle] をクリックして、ユーザー名と証明書バンドルパスワードを入力します。

d) [Wireless Network Name（SSID）] 領域で、ワイヤレスネットワーク（SSID）を選択して、次の設定を実行します。

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

    [WPA2 Personal] を選択した場合は、[Passphrase] テキストボックスにパスフレーズを入力します。

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

e) [Save] をクリックします。

ステップ 4 既存のバックホール設定を編集するには、次の手順を実行します。

a) バックホール設定のチェックボックスをオンにします。

b) [Actions] ドロップダウンリストにカーソルを合わせて、[Edit] を選択します。

ステップ 5 バックホール設定を削除するには、次の手順を実行します。

a) バックホール設定のチェックボックスをオンにします。

b) [Actions] ドロップダウンリストにカーソルを合わせて、[Delete] を選択します。

アンテナ無線プロファイルの作成

Catalyst Center は、C-ANT9104 アンテナをサポートします。これは、Cisco Catalyst 9130AXE ユニファイド アクセス ポイントと統合され、高ゲイン、操作可能、切り替え可能な機能を備えたデュアル 5 GHz 4x4 無線を提供します。Catalyst Center では、アンテナのビームステアリング（方向）を選択できます。使用可能なモードは次のとおりです。

- ワイドビーム
- ナロービーム
- 傾斜 10 度のナロービーム
- 傾斜 20 度のナロービーム

高いユーザー密度、正確なパターン制御、および5 GHz帯域での長距離パフォーマンスが必要な設置用に、ワイドおよびナロービーム幅状態を設定できます。

ビームステアリング構成は、アンテナの組み合わせ ABCD（左側のアンテナ）と EFGH（右側のアンテナ）で使用できます。アンテナパターン名は、選択したビームに基づいて設定されます。Catalyst Center フロアマップでヒートマップを可視化できます。

AP のプロビジョニング中にアンテナ無線プロファイルを使用できます。詳細については、Day 1 の Cisco AP プロビジョニング （745 ページ）を参照してください。

手順

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

ステップ 2 [Wireless] タブをクリックします。

ステップ 3 左側の階層ツリーから、[Global] を選択します。

ステップ 4 [Antenna Radio Profiles] をクリックします。

ステップ 5 [Antenna Radio Profile] テーブルで、[Add] をクリックします。

ステップ 6 [Antenna Radio Profile] スライドインペインで、アンテナのワイドおよびナロービームステアリングを設定します。

- [Radio Profile Name] フィールドに、無線プロファイルの一意の名前を入力します。
- [Beam Steer Mode] ドロップダウンリストから、ビームステアリングモードを選択します。

ステップ 7 [Save] をクリックします。

新しいアンテナ無線プロファイルが [**Antenna Radio Profile**] テーブルに表示されます。

アンテナ無線プロファイルの編集または削除

手順

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

ステップ 2 [Wireless] タブをクリックします。

ステップ 3 左側の階層ツリーから、[Global] を選択します。

ステップ 4 [Antenna Radio Profiles] をクリックします。

ステップ 5 [Antenna Radio Profile] テーブルで、編集または削除するアンテナ無線プロファイル名の横にあるチェックボックスをオンにします。

- アンテナ無線プロファイルを編集するには、[Edit] をクリックします。[Antenna Radio Profile] スライドインペインで、必要に応じて設定を編集し、[Save] をクリックします。詳細については、アンテナ無線プロファイルの作成 （520 ページ）を参照してください。
- アンテナ無線プロファイルを削除するには、[Delete] をクリックし、[Yes] をクリックします。

Cisco Connected Mobile Experiences の統合について

Catalyst Center は、ワイヤレスマップのためのオンプレミス Cisco Connected Mobile Experiences（CMX） の統合をサポートしています。CMX を統合すると、Catalyst Center ユーザーインターフェイス内で、フロアマップ上でのワイヤレスクライアント、不正アクセスポイントおよび干渉源の正確な場所を把握できます。

CMX の設定は、ユーザーの要件に応じて、グローバルレベルで、あるいはサイト、ビルディング、またはフロアレベルで作成できます。小企業の場合はグローバルレベル（親ノード）で CMX を割り当てることができます。すべての子ノードが親ノードから設定を継承します。中企業の場合はビルディングレベルで、大企業の場合はフロアレベルで CMX を割り当てることができます。

（注） セキュリティ上の理由から、CMX は匿名にする必要があります。

Cisco CMX 設定の作成

始める前に

CMX が有効な SSL/TLS 証明書で設定されていることを確認します。CMX 10.5 SSL 証明書のインストール手順 [英語] を参照してください。

手順

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

ステップ 2 [External Services] セクションで、[Cisco Spaces/CMX Servers] をクリックします。

[Cisco Spaces/CMX Servers] ウィンドウが開きます。

ステップ 3 [CMX Servers] テーブルから、[Add] をクリックします。

ステップ 4 [Add CMX Server] スライドインペインで、次のフィールドに入力します。

- [IP Address]：CMX Web GUI の有効な IP アドレスを入力します。
- [**Username**]：CMX Web GUI の管理者ユーザー名を入力します。

（注） CMX サーバーをサイト、ビルディング、またはフロアに割り当てるには、[Network Hierarchy] に対する書き込み権限が必要です。詳細については、『*Cisco Catalyst Center Administrator Guide*』の「Catalyst Center User Role and Permissions」を参照してください。

- [Password]：パスワードログイン情報を入力します。

（注） CMX が到達可能なことを確認します。

ステップ 5 [Add] をクリックします。

接続ステータスは、次の 3 段階で表示されます。

- [Initiating Connection]：サーバーへの接続を確認します。
- [Establishing Trust]：CMX サーバーへの信頼を確立します。CMX サーバーには、信頼を確立するために設定された有効な SSL/TLS 証明書が必要です。証明書が Catalyst Center の信頼できる証明書にまだ保存されていない場合、続行するには証明書を**受け入れる**ように求められます。
- [Connecting CMX Server]：指定されたユーザーログイン情報を検証します。

ステップ 6 CMX サーバーをサイト、建物、またはフロアに割り当てるには、メニューアイコンをクリックし、**[Design]** > **[Network Settings]**の順に選択します。

ステップ 7 [Wireless] タブをクリックします。

ステップ 8 [Global] または必要なエリア、建物、フロアを左側の階層ツリーから、以下を選択します。

ステップ 9 [Cisco Spaces/CMX Servers] をクリックします。

ステップ 10 [**Cisco Spaces/CMX Servers**] セクションで、[**Location Settings**] ドロップダウンリストから CMX サーバーを選択します。

ステップ 11 **[Save]** をクリックします。

[Create CMX Settings] ウィンドウが開きます。

CMX の追加後に [Network Hierarchy] ページのフロアに変更を加えた場合、その変更は自動的に CMX と同期されます。

CMX が同期されると、Catalyst Center はクライアントロケーションを CMX に照会し、その場所がフロアマップに表示されます。

ステップ 12 フロアマップでは、次のタスクを実行できます。

- クライアントの場所を表示します。これは青色のドットとして表示されます。
- AP 上にカーソルを移動します。[**Info**]、[**Rx Neighbor**]、[**Clients**] タブのあるダイアログボックスが表示されます。詳細については、各タブをクリックしてください。[Device 360] をクリックして、デバイス 360 ウィンドウを開き、問題を表示します。問題をクリックして、問題の場所とクライアント デバイスの場所を表示します。
- AP をクリックして、AP に関する詳細を含むサイド バーを開きます。
- Intelligent Capture と CMX を統合するときにリアルタイムでクライアントトラッキングを実行します。

ステップ 13 変更を加えたときに CMX がダウンした場合は、手動で同期する必要があります。同期するには、[**Network Hierarchy**] ウィンドウで、左側の階層ツリーで変更を加えた建物やフロアの横にある省略記号 ••• にカーソルを合わせ、[**Sync: Cisco Spaces/CMX Servers**] を選択して、変更を手動でプッシュします。

ステップ 14 CMX サーバーの詳細を編集する場合や CMX サーバーを削除する場合は、次の手順を実行します。

a) メインメニューから次を選択します。**[System]** > **[Settings]**の順に選択します。
b) [External Services] セクションで、[Cisco Spaces/CMX Servers] をクリックします。
c) 編集する CMX サーバーを選択して変更を加え、[Update] をクリックします。
d) 削除する CMX サーバーを選択し、[Delete] をクリックします。
e) [OK] をクリックして削除を実行します。

CMX 接続障害の場合

- CMX 証明書を **[System]** > **[Settings]** > **[Trusted Certificates]** にアップロードしているか確認します。
- Catalyst Center にアップグレード後、CMX SSL/TLS 証明書を確認して受け入れることで、CMX 接続の詳細を編集して接続を再確立します。

CMX 認証に失敗した場合

- Catalyst Center で CMX 設定の作成時に指定したログイン情報で、CMX Web GUI にログインできるか確認します。
- SSH を使用して CMX コンソールにログインできるかどうかを確認します。

- CMX GUI の API ドキュメンテーションリンクを使用して CMX REST API を使用できるかどうかを確認します。

クライアントが Catalyst Center フロアマップに表示されない場合

- 特定のフロアの シスコ ワイヤレス コントローラ が CMX で設定されており、アクティブになっているか確認します。
- CMX GUI でフロアマップにクライアントが表示されるか確認します。
- **[データ/フィルタ（Data/Filters）]** > **[クライアント（Clients）]** の順に選択し、[未配置（Unpositioned）] タブをクリックして、クライアントがフロアマップに表示されない理由を確認します。

Cisco Spaces 統合について

現実の世界で事業を行っている企業は、これまで、建物内の人々や接続されたアセットの動きを可視化できませんでした。Cisco Spaces は、基盤となるすべてのシスコ ワイヤレス ネットワークによって提供されるロケーション感知インテリジェンスを使用し、データをビジネス対応の洞察に変換することで、この物理的な死角の問題を解決します。

Catalyst Center を Cisco Spaces と統合すると、Catalyst Center フロアマップ上のワイヤレスクライアント、不正 AP、および干渉源の正確な場所が提供されます。Cisco Spaces の設定は、ユーザーの要件に応じて、グローバルレベルで、あるいはサイト、ビルディング、またはフロアレベルで作成できます。

Cisco Spaces/CMX 同期がトリガーされた後、フロアマップをクリックし、**[その他（More）]** > **[CMX/Cisco Spaces同期履歴（More CMX/Cisco Spaces Sync History）]**を選択すると、同期ステータスを表示できます。

Cisco Spaces と Catalyst Center を統合するには、『*Cisco Spaces Configuration Guide*』の「Catalyst Center Integration」を参照してください。

Cisco Spaces のサイトへの割り当て

Cisco Spaces を使用してサイトをモニターするには、モニターするサイトに Cisco Spaces を割り当てる必要があります。

始める前に

Cisco Spaces と Catalyst Center を連動させます。詳細については、『*Cisco Spaces Configuration Guide*』を参照してください。

手順

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

ステップ 2 [Wireless] タブをクリックします。

ステップ 3 左側の階層ツリーから、以下を選択します**[Global]** か、Cisco Spaces に割り当てるエリア、ビルディング、またはフロアを選択します。

ステップ 4 [Cisco Spaces/CMX Servers] をクリックします。

ステップ 5 [Cisco Spaces/CMX Servers] ウィンドウの [Location Services] ドロップダウンリストからサイトを選択します。

ステップ 6 [Save] をクリックします。

Catalyst Center により、サイト情報が Cisco Spaces に自動的に展開されます。

Cisco Spaces を使用したサイトのモニタリング

Cisco Spaces を使用してサイトをモニターできます。

始める前に

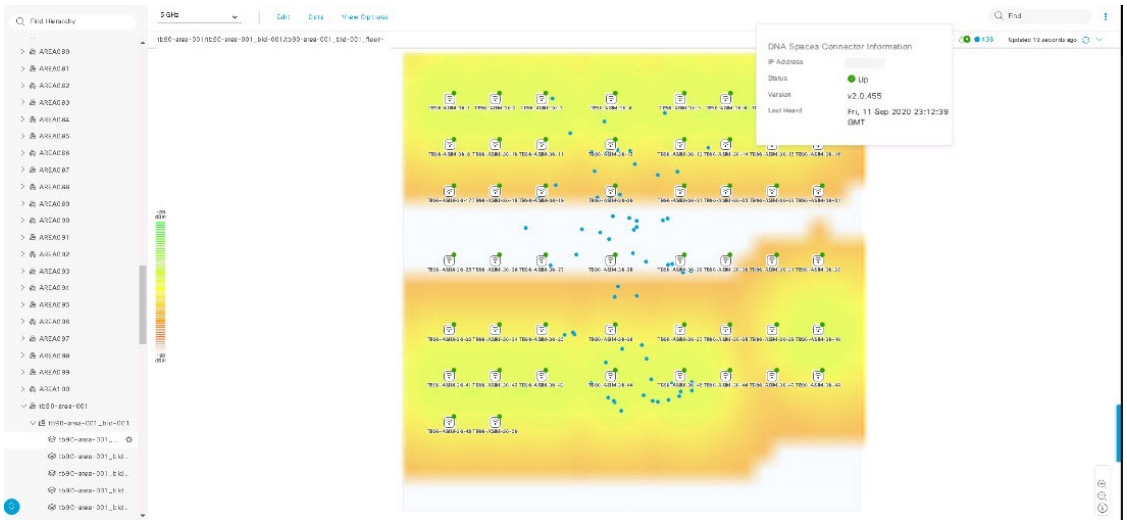
- Cisco Spaces と Catalyst Center を連動させます。詳細については、『*Cisco Spaces Configuration Guide*』を参照してください。
- モニターするサイトに Cisco Spaces を割り当てます。

手順

ステップ 1 Catalyst Center GUI でメニューアイコンをクリックして、**[Design]** > **[Network Hierarchy]**。

ステップ 2 左側の階層ツリーから、以下を選択します**[Global]** か、Cisco Spaces にモニターさせるエリア、ビルディング、またはフロアを選択します。

ステップ 3 Cisco Spaces が動作していることを確認するには、次の図に示すように、Cisco Spaces/CMX ステータスアイコンが監視するフロアに表示されていることを確認します。



FlexConnect VLAN の設定

次の FlexConnect VLAN 設定ができます。

- [Native VLAN]：FlexConnect グループが AP と シスコ ワイヤレス コントローラ の間で管理トラフィックを伝送できるようにします。
- [AAA Override VLAN]：ローカルでスイッチングされるクライアントの動的 VLAN 割り当てを提供します。

これらの設定をグローバルレベルで適用して、サイト、ビルディング、またはフロアレベルの設定をオーバーライドすることができます。

手順

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

ステップ 2 [Wireless] タブをクリックします。

ステップ 3 左側の階層ツリーから、以下を選択します必要なサイトを選択します。

- [Global]：すべてのサイトに対してグローバルレベルで VLAN を設定します。
- エリア、ビルディング、またはフロア：選択したレベルでのみ VLAN を設定します。

ステップ 4 [FlexConnect Settings] をクリックします。

子サイトは親サイトから FlexConnect 設定を継承します。継承された設定の横には継承アイコンが表示されます。継承アイコンにカーソルを合わせると、設定の継承元が表示されます。設定が継承されていない場

合は、[Delete] オプションを使用して設定を削除し、[Inherit] オプションを使用して親サイトから設定を継承できます。

ステップ 5 [Native VLAN ID] フィールドに、VLAN ID の値を入力します。有効な範囲は 1 ～ 4094 です。

ステップ 6 [AAA Override VLAN] 設定の場合は、VLAN ID と VLAN 名のマッピングを、対応する [VLAN ID] フィールドと [VLAN Name] フィールドに入力します。さらにマッピングを追加するには、[追加（Add）] アイコンをクリックします。

（注） FlexConnect 展開に対して定義できる VLAN マッピングの最大数は 16 です。ただし、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの場合、この数には、デフォルトの WLAN VLAN と、AAA によってプッシュされた VLAN が含まれます。

ステップ 7 [保存（**Save**）] をクリックします。

次のタスク

ワイヤレス ネットワーク プロファイルを作成するか、SSID を設定します。

- **ワイヤレス ネットワーク プロファイル**：ワイヤレス ネットワーク プロファイルを作成する場合は、[FlexConnect Local Switching] チェックボックスがオンになっていることを確認します。詳細については、ワイヤレス用のネットワークプロファイルの作成（543ページ）を参照してください。
- [SSID]：SSID を設定する場合は、エンタープライズ ワイヤレス ネットワーク用 SSID の作成 （415 ページ）およびゲスト ワイヤレス ネットワークの SSID の作成 （432 ページ）を参照してください。

保存済みの FlexConnect VLAN 設定をワイヤレスコントローラで設定するには、ワイヤレスコントローラをプロビジョニングする必要があります。詳細については、Cisco AireOS コントローラのプロビジョニング （738 ページ）またはCisco Catalyst 9800 シリーズ ワイヤレス コントローラの設定とプロビジョニング （754 ページ）を参照してください。

ワイヤレスコントローラ のプロビジョニング後に、コントローラに関連付けられている AP をプロビジョニングする必要があります。

802.11be プロファイルの作成

802.11be プロファイルは、Cisco IOS XE リリース 17.15.2 以降を実行している ワイヤレスコントローラ で Wi-Fi 7 を設定するために使用されます。

このプロファイルを使用すると、マルチリンク動作（MLO）グループを設定して複数の周波数帯域を同時に使用できます。この設定により、全体的なワイヤレスパフォーマンスが向上します。

（注）

- この 802.11be プロファイルは WLAN にマッピングされ、2.4 GHz および 5 GHz 帯域にのみ適用されます。6 GHz 帯域の 802.11be 設定では、RF プロファイルの対応する設定が使用されます。詳細については、ワイヤレス無線周波数プロファイルの作成（451 ページ）およびAI 無線周波数プロファイルの作成（468 ページ）を参照してください。
- Cisco IOS XE リリース 17.18.1 より前のバージョンを実行している ワイヤレスコントローラ は、1 つの dot11be-profile のみを使用します。これは、default-dot11be-profile です。各ワイヤレスコントローラ の SSID およびネットワークプロファイル全体で 1 つの 802.11be プロファイルのみを使用します。
- Cisco IOS XE リリース 17.18.1 以降を実行する ワイヤレスコントローラ では、カスタム 802.11be プロファイルがサポートされます。ワイヤレスコントローラ の単一ネットワークプロファイル内の SSID 全体では複数の 802.11be プロファイルが使用できます。

  802.11be プロファイルとワイヤレスネットワークプロファイルの関連付けについては、ネットワークプロファイルへの SSID の追加（544 ページ）を参照してください。
- MLO グループ設定は、Cisco IOS XE リリース 17.18.1 以降を実行している ワイヤレスコントローラ でサポートされています。

始める前に

[**Dot11be Status Configuration**] 機能テンプレートでグローバル 802.11be ステータスを有効にします。次に、管理 ワイヤレスコントローラ をプロビジョニングして、802.11be プロファイル設定を適用します。

機能テンプレートで 802.11be ステータスを有効にする方法の詳細については、Dot 11be ステータス設定用の機能テンプレートの作成（618 ページ）を参照してください。ワイヤレスコントローラ のプロビジョニングの詳細については、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のプロビジョニング（782 ページ）を参照してください。

手順

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

ステップ 2 [Wireless] タブをクリックします。

ステップ 3 左側の階層ツリーから、以下を選択します [Global] を選択します。

ステップ 4 [802.11be Profiles] をクリックします。

ステップ 5 [802.11be Profiles] テーブルで、[Add] をクリックします。

ステップ 6 [Add 802.11be Profile] スライドインペイン の [802.11be Profile Name] フィールドに、802.11be プロファイル名を入力します。

ステップ 7 [Mark as default] トグルボタンを有効にして、このプロファイルをデフォルトプロファイルとして設定します。

このプロファイルをデフォルトプロファイルとしてマークすると、この設定が ワイヤレスコントローラの default-dot11be-profile にプッシュされます。

（注） この設定は、Cisco IOS XE リリース 17.18.1 以降を実行している ワイヤレスコントローラ でのみサポートされています。

ステップ 8 [Description] フィールドに、説明を入力します

ステップ 9 （任意） トグルボタンを使用して次の設定を有効または無効にします。

- [**OFDMA Uplink**]：OFDMA を使用するためのアップリンク接続を有効にします。
- [**OFDMA Downlink**]：OFDMA を使用するためのダウンリンク接続を有効にします。
- [**MU-MIMO Uplink**]：MU-MIMO を使用するためのアップリンク接続を有効にします。
- [**MU-MIMO Downlink**]：MU-MIMO を使用するためのダウンリンク接続を有効にします。
- [**OFDMA Multi-RU**]：OFDMA を使用した単一ユーザーへの複数リソースユニット（RU）の同時割り当てを有効にします。

（注） Cisco IOS XE リリース 17.18.2 以降、OFDMA Uplink、OFDMA Downlink、MU-MIMO Uplink、および MU-MIMO Downlink の設定は廃止され、802.11be プロファイルでは無視されます。これらの設定を構成するには、[Advanced SSID Configuration] 機能テンプレートの **802.11ax Configuration** タブを使用します。詳細については、高度な SSID の機能テンプレートの作成（606 ページ）を参照してください。

ステップ 10 トグルボタンを使用して MLO グループ設定を有効または無効にします。

- [**Primary 2.4GHz**]：MLO グループで 2.4 GHz 帯域を設定します。
- [**Primary 5GHz**]：MLO グループで 5 GHz 帯域を設定します。
- [**Secondary 5GHz**]：MLO グループでセカンダリ 5 GHz 帯域を設定します。
- [**Primary 6GHz**]：MLO グループで 6 GHz 帯域を設定します。

ステップ 11 [Save] をクリックします。

802.11be プロファイルの編集または複製

次の手順を使用して、802.11be プロファイルを編集または複製します。

手順

ステップ 1 メインメニューから次を選択します。**[Design]** > **[Network settings]**。
ステップ 2 [Wireless] タブをクリックします。
ステップ 3 左側の階層ツリーから、以下を選択します [Global] を選択します。
ステップ 4 [802.11be Profiles] をクリックします。
ステップ 5 [802.11be Profiles] で、編集または複製する 802.11be プロファイルの横にあるチェックボックスをオンにします。
ステップ 6 プロファイルを編集するには、[Edit] をクリックします。
a) [Edit 802.11be Profile] スライドインペインで、必要に応じてパラメータを編集します。
詳細については、802.11be プロファイルの作成 （527 ページ）を参照してください。
b) [Save] をクリックします。
ステップ 7 プロファイルを複製するには、[Clone] をクリックします。
a) [Clone 802.11be Profile] スライドインペインの [802.11be Profile Name] フィールドで、802.11be プロファイル名を更新し、必要に応じて、他のパラメータを編集します。
詳細については、802.11be プロファイルの作成 （527 ページ）を参照してください。
b) [Save] をクリックします。

802.11be プロファイルの削除

次の手順を使用して、802.11be プロファイルを削除します。

手順

ステップ 1 メインメニューから次を選択します。**[Design]** > **[Network settings]**。
ステップ 2 [Wireless] タブをクリックします。
ステップ 3 左側の階層ツリーから、以下を選択します [Global] を選択します。
ステップ 4 [802.11be Profiles] をクリックします。
ステップ 5 [802.11be Profiles] で、削除する 802.11be プロファイルの横にあるチェックボックスをオンにします。
ステップ 6 [Delete] をクリックします。
ステップ 7 ダイアログボックスで、**Yes** をクリックします。

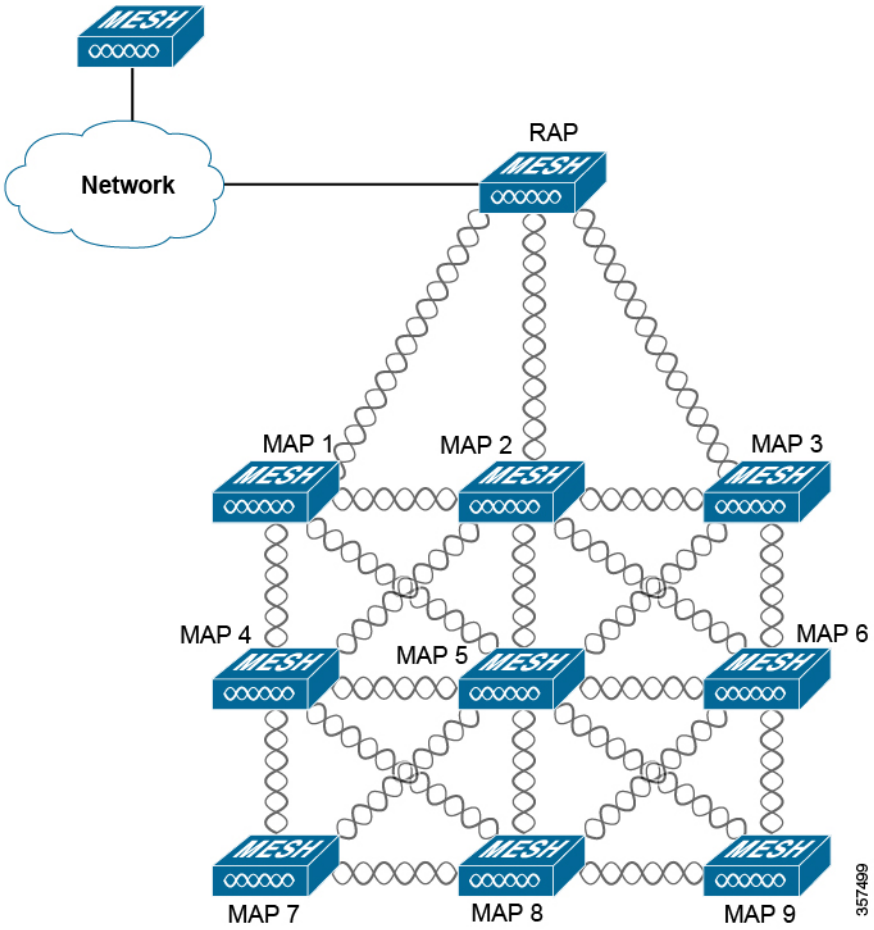
ワイヤレス メッシュ ネットワークについて

シスコ ワイヤレス メッシュ ネットワーク内のアクセスポイント（AP）は、次の 2 つの方法のいずれかで動作します。

- ルートアクセスポイント（RAP）：それぞれの場所で有線ネットワークに接続します。
- メッシュアクセスポイント（MAP）：ワイヤレスで通信し、安全でスケーラブルなワイヤレス LAN を提供します。

（注） すべての AP は MAP として設定され、出荷されています。AP を RAP として使用するには、RAP として再設定する必要があります。すべてのメッシュネットワークで、少なくとも 1 つの RAP があることを確認します。

RAP は、それぞれの場所で有線ネットワークに接続します。すべてのダウンストリーム AP は、MAP として動作し、ワイヤレスリンクを使用して通信します。



MAP と RAP はいずれも WLAN クライアントアクセスを提供します。ただし、一般に、RAP の場所は高い確率でクライアントアクセスの提供に向いていません。

MAP から Control and Provisioning of Wireless Access Point（CAPWAP）セッションを終端させるオンサイトコントローラがある建物もありますが、CAPWAP セッションは WAN を介して ワイヤレスコントローラ にバックホールできるため、それは必須要件ではありません。

Cisco ワイヤレス バックホール ネットワークでは、トラフィックを MAP と RAP の間でブリッジできます。このトラフィックは、ワイヤレスメッシュによってブリッジされている有線デバイスからのトラフィックか、MAP からの CAPWAP トラフィックになります。このトラフィックは、ワイヤレスバックホールなどのワイヤレスメッシュリンクを通過する際に必ず AES 暗号化されます。

メッシュネットワークの詳細については、最新の『Cisco Wireless Mesh Access Points, Design and Deployment Guide』を参照してください。

シスコ ワイヤレス コントローラ の設定

メッシュネットワークの場合は、ワイヤレスコントローラで許可 AP のリストを設定する必要があります。ワイヤレスコントローラは、許可リストに含まれている MAP からの要求にのみ応答します。

（注） Catalyst Center は、Cisco IOS リリース 17.5 以降を実行している Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ での承認リストの設定をサポートしています。

Cisco AireOS ワイヤレスコントローラと Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの両方で、Catalyst Center を使用してブリッジグループ名（BGN）と RAP ダウンリンク バックホール メッシュの設定を指定することができます。Cisco Catalyst 9800 シリーズ ワイヤレス コントローラでは、MAP の最大範囲、バックホール クライアント アクセス、およびバックホールデータレートを設定することもできます。

これらの設定は、[Create AP Profile] ウィンドウでグローバルサイトに対して指定されます。詳細については、Cisco IOS XE デバイスの AP プロファイルのメッシュ設定を行う （506 ページ）およびCisco AireOS デバイスの AP プロファイルのメッシュ設定 （513 ページ）を参照してください。

AP の設定

メッシュネットワークモードで使用する既存の AP がある場合は、最初に [Configure Access Point] ワークフローを使用して AP モードを [Bridge] または [Flex+Bridge] に変更する必要があります。詳細については、AP の設定 （1639 ページ）を参照してください。

AP を [Bridge] モードまたは [Flex+Bridge] モードに設定すると、[AP 360] ウィンドウにメッシュ設定が表示されます。この時点で、AP を新しい設定でプロビジョニングする必要があります。詳細については、Day 1 の Cisco AP プロビジョニング （745 ページ）を参照してください。

（注） Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの場合、複数のフロアにわたるメッシュ AP の一括プロビジョニング中に、すでにプロビジョニングされている AP で次の設定を同時に更新しないことをお勧めします。

- AP のメッシュロールと、AP プロファイルのメッシュ設定（**ブリッジグループ名**、**範囲 - ルート AP からメッシュ AP**（**フィート単位**）、**バックホール クライアント アクセス**）
- AP のメッシュロールと、AP プロファイルまたは Flex プロファイルとサイトタグのマッピング

メッシュ AP の一括プロビジョニング中にこれらの設定を同時に更新する場合は、次のいずれかを実行する必要があります。

- Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ を再プロビジョニングします。ワイヤレスコントローラを再プロビジョニングすると AP が再起動します。再起動が完了したら、必要なメッシュロールの変更を行って AP を再プロビジョニングできます。
- メッシュ設定が更新された AP の 1 つを再プロビジョニングします。メッシュ設定が更新された他の AP も再起動します。再起動が完了したら、必要なメッシュロールの変更を行って AP を再プロビジョニングできます。

証明書失効確認の設定

次の手順を使用して、コントローラ証明書の証明書失効確認を設定します。

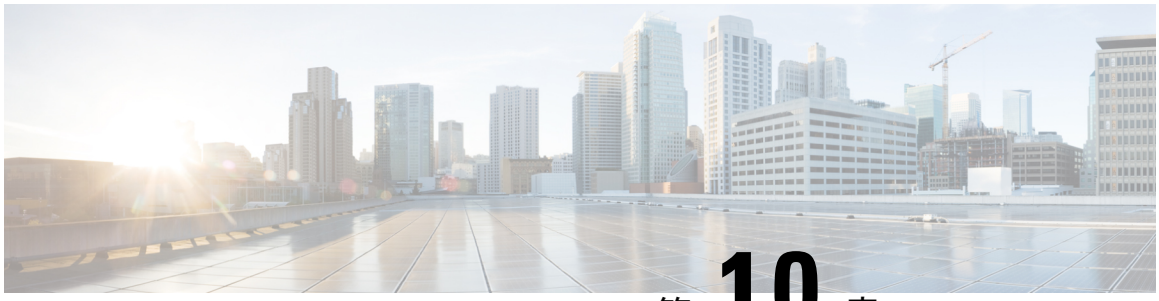
手順

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

ステップ 2 左側の階層ツリーから、以下を選択しますサイト、ビルディング、またはフロアを選択します。

ステップ 3 [Revocation Check] ドロップダウンリストでは、[Revocation - Check: CRL None] がデフォルトで選択されています。

ステップ 4 失効確認をスキップするには、[Revocation - Check: None] を選択し、[Save] をクリックします。



第 10 章

ネットワークプロファイルの設定

- ネットワークプロファイルの概要 （535 ページ）
- アシュアランス用のネットワークプロファイルの作成 （535 ページ）
- ファイアウォール用のネットワークプロファイルの作成 （537 ページ）
- ルーティング用のネットワークプロファイルの作成 （539 ページ）
- スイッチ用のネットワークプロファイルの作成 （541 ページ）
- ワイヤレス用のネットワークプロファイルの作成 （543 ページ）

ネットワークプロファイルの概要

ネットワークプロファイルを使用すると、設定を構成し、特定のサイトやサイトのグループに適用できます。 Catalyst Center のさまざまな要素のネットワークプロファイルを作成できます。

- アシュアランス用のネットワークプロファイルの作成 （535 ページ）
- ファイアウォール用のネットワークプロファイルの作成 （537 ページ）
- ルーティング用のネットワークプロファイルの作成 （539 ページ）
- スイッチ用のネットワークプロファイルの作成 （541 ページ）
- ワイヤレス用のネットワークプロファイルの作成 （543 ページ）

アシュアランス用のネットワークプロファイルの作成

Assurance のネットワークプロファイルを作成すると、問題を設定して、グローバルな問題の設定とは別にサイトまたはサイトのグループに適用できます。問題を有効または無効にしたり、優先順位を変更したりできます。

（注）
- Assurance では、ネットワークデバイスの正常性スコアへの同期は、グローバルな問題設定に対してのみ使用できます。カスタムの問題設定では使用できません。詳細については、*Cisco Catalyst Assurance User Guide*を参照してください。
- 一部のグローバルな問題はカスタマイズできません。これらの問題は、変更するカスタム問題のリストには表示されません。
- 変更された問題をリストの一番上に表示するには、[Last Modified] でソートします。
- カスタム設定を削除するには、最初にすべてのサイトの割り当てを解除する必要があります。

手順

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

ステップ 2 [+Add Profile] をクリックし、[Assurance] を選択します。

ステップ 3 [Profile Name] フィールドに有効なプロファイルの名前を入力し、[Next] をクリックします。

Catalyst Center によってプロファイルが追加され、[Edit Profile] ウィンドウが表示されます。

ステップ 4 設定する問題のタイプを表示するには、[DEVICE TYPE] と [CATEGORY] フィルタを設定します。

ステップ 5 [Issue Name] 列の問題をクリックすると、設定を含むスライドインペインが開きます。

（注） いくつかの問題については、設定に加えられた変更は複数のデバイスタイプで共有されます。スライドインペインに、影響を受けるデバイスタイプを示す注意が Catalyst Center によって表示されます。

ステップ 6 この問題の Catalyst Center によるモニタリングを有効または無効にするには、[Enabled] トグルボタンをクリックします。

ステップ 7 問題の優先順位を設定するには、[Priority] ドロップダウンリストをクリックし、優先順位を選択します。

- [P1]：ネットワーク運用に幅広い影響を与える可能性があり、早急な対応を必要とする重大な問題。
- [P2]：複数のデバイスまたはクライアントに影響を与える可能性がある重大な問題。
- [P3]：局所的または最小限の影響を与える軽微な問題。
- [P4]：ただちに問題になるものではないが、対処するとネットワークのパフォーマンスを最適化できる警告レベルの問題。

ステップ 8 （一部の問題のみ）[Trigger Condition] エリアで、問題が報告される条件のしきい値を変更できます。

トリガー条件の例：

```
No Activity on Radio(2.4 GHz) >= 60 minutes.
Memory Utilization of Access Points greater than 90%.
```

ステップ 9 （任意） 設定に変更がある場合は、[View Default Settings] の上にカーソルを置くと、デフォルトの設定が表示されます。問題の設定をすべてデフォルト値に復元するには、[Use Default] をクリックします。

ステップ 10 [Apply] をクリックします。

ステップ 11 （特定の問題について）[Manage Subscriptions] をクリックすると、サポートされている問題がトリガーされたときの外部通知に登録できます。

ステップ 12 このプロファイルをサイトに割り当てるには、[Assign Sites] をクリックします。このプロファイルを関連付けるサイトの横にあるチェックボックスをオンにし、[Save] をクリックします。

[Edit Profile] ウィンドウが表示されます。

（注） 親ノードまたは個々のサイトを選択できます。親ノードを選択すると、その親ノードに属する子もすべて選択されます。チェックボックスをオフにして、サイトの選択を解除できます。

ステップ 13 [Done] をクリックします。

新しく追加されたプロファイルが、[Network Profiles] ウィンドウに表示されます。

ファイアウォール用のネットワークプロファイルの作成

このワークフローでは、次を実行する方法を示します。

1. Cisco 適応型セキュリティアプライアンス（ASA）デバイスのプロファイルを作成し、プロファイルの概要を表示します。
2. Firepower Threat Defense（FTD）デバイスのプロファイルを作成し、プロファイルの概要を表示します。

手順

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

ステップ 2 [+Add Profile] をクリックし、[Firewall] を選択します。

[ファイアウォールプロファイルの追加（Add Firewall Profile）] ページが表示されます。

ステップ 3 Cisco ASA プロファイルを作成するには、次の手順を実行します。

a) [Name] フィールドに、プロファイルの名前を入力します。

b) [Devices] ドロップダウンリストからデバイスの番号を選択します。

（注） プロファイルごとに最大 10 のデバイスを選択できます。

c) [Device Type] ドロップダウンリストからデバイスのタイプを選択します。
d) （任意） [Device Tag] ドロップダウンリストからデバイスタグを選択します。
e) [Next] をクリックします。

[Custom Configuration] ページが表示されます。

f) [Day-Nテンプレート（Day-N Templates）] ドロップダウンリストから ASA テンプレートを選択します。

（注） テンプレートがない場合は、**[Design]** > **[CLI Templates]** で少なくとも 1 つのテンプレートを作成する必要があります。詳細については、「テンプレートの作成 （575 ページ）」を参照してください。

g) [Next] をクリックします。

[Summary] ページが表示されます。このページには、カスタム構成の概要が表示されます。選択されたデバイスタイプに基づいて、このページにハードウェアの推奨事項が提示されます。

h) [Save] をクリックします。

[Network Profiles] ページが表示されます。

i) ネットワークプロファイルにサイトを割り当てるには、[Assign Sites] をクリックします。詳細については、サイトの作成、編集、削除 （285 ページ） を参照してください。

ステップ 4 FTD プロファイルを作成するには、次の手順を実行します。

a) [Name] フィールドに、プロファイルの名前を入力します。
b) [Devices] ドロップダウンリストからデバイスの番号を選択します。

（注） プロファイルごとに最大 10 のデバイスを選択できます。

c) FTD ファイアウォールをプロビジョニングするには、[FTD] チェックボックスをオンにします。
d) [Device Type] ドロップダウンリストからデバイスのタイプを選択します。
e) （任意） [Device Tag] ドロップダウンリストからデバイスタグを選択します。
f) [Next] をクリックします。

[FTD Configuration] ページが表示されます。

g) [Routed Mode] または [Transparent Mode] オプションボタンをクリックします。
h) [Next] をクリックします。

[Summary] ページが表示されます。このページには、FTD 構成の概要が表示されます。選択されたデバイスタイプに基づいて、このページにハードウェアの推奨事項が提示されます。

i) [Save] をクリックします。

[Network Profiles] ページが表示されます。

j) ネットワークプロファイルにサイトを割り当てるには、[Assign Sites] をクリックします。詳細については、「サイトの作成、編集、削除 （285 ページ）」を参照してください。

ルーティング用のネットワークプロファイルの作成

このワークフローでは、次を実行する方法を示します。

1. ルータ WAN 設定の詳細を追加します。
2. ルータ LAN 設定の詳細を追加します。
3. 統合スイッチ設定の詳細を追加します。
4. カスタム設定を追加します。
5. プロファイルの概要を表示します。

手順

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

ステップ 2 [+ Add Profile] にカーソルを合わせ、[Routing] を選択します。

ステップ 3 [Router WAN Configuration] ページが表示されます。

- [Name] テキスト ボックスにプロファイル名を入力します。
- それぞれのドロップダウンリストから、[Service Providers] および [Devices] の数を選択します。プロファイルあたり最大 3 つのサービスプロバイダと 10 個のデバイスがサポートされます。
- ドロップダウンリストから [Service Provider Profile] を選択します。詳細については、サービス プロバイダ プロファイルの設定 （413 ページ） を参照してください。
- ドロップダウンリストから、[Device Type] を選択します。
- [Device Tag] に一意の文字列を入力して異なるデバイスを識別するか、ドロップダウンリストから既存のタグを選択します。2 つ以上のデバイスが同じタイプの場合は、デバイスタグを使用します。すべてのデバイスが異なるタイプの場合、デバイスタグはオプションです。適切なタグを確実に選択してください。ネットワークプロファイルに適用される Day-0 および Day-N テンプレートの一致基準の一部は、ここで選択した内容を使用します。

- デバイスごとに1つ以上の回線リンクを有効にして続行するには、接続アイコン（○）をクリックし、[接続（Connect）] の横にあるチェックボックスをオンにします。ドロップダウンリストから、[Line Type] を選択します。[OK] をクリックします。

  複数のサービスプロバイダーを選択する場合は、以下を選択できます。

  - プライマリインターフェイスに [ギガビットイーサネット（GigabitEthernet）]、セカンダリインターフェイスに [セルラー（Cellular）]
  - 両方のインターフェイスに [ギガビットイーサネット（GigabitEthernet）]
  - プライマリインターフェイスに[セルラー（Cellular）]、セカンダリインターフェイスに[ギガビットイーサネット（GigabitEthernet）]

  （注） セルラーインターフェイスは、次のサービス統合型ルータのみをサポートします。

  - Cisco 1100 シリーズ
  - Cisco 4200 シリーズ
  - Cisco 4300 シリーズ
  - Cisco 4400 シリーズ

- [Next] をクリックします。

ステップ 4 [Router LAN Configuration] ページが表示されます。

ルータの LAN 設定をスキップするには、[Skip] オプションボタンをクリックし、ステップ 5 に進みます。ルータ LAN を設定するには、次の手順を実行します。

- [Configure Connection] オプションボタンをクリックし、[L2] または [L3]、あるいはその両方を選択します。
- [L2] を選択した場合は、[+ Add Row] をクリックします。ドロップダウンリストから [Type] を選択し、[VLAN ID/Allowed VLAN] および [Description] を入力します。[+行を追加（+ Add Row）] をクリックすると複数の行を追加でき、[削除（Delete）] をクリックすると行を削除できます。
- [L3] を選択した場合は、ドロップダウンリストから [Protocol Routing] を選択し、[Protocol Qualifier] を入力します。
- **[Next]** をクリックします。

ステップ 5 ルータ設定に基づいて、[Integrated Switch Configuration] ページが表示されます。

[Integrated Switch Configuration] ページが表示されない場合は、ステップ 6 に進みます。

統合スイッチの設定では、新しい VLAN を追加したり、ルータの LAN 設定で以前に選択した設定を保持したりすることができます。

- 1 つ以上の新しい VLAN を追加するには、[+ Add Row] をクリックします。
- ドロップダウンリストから [Type] を選択し、[VLAN ID/Allowed VLAN] および [Description] を入力します。
- VLAN を削除するには、[Delete（削除）] をクリックします。
- [Next] をクリックします。



（注） Switchport インターフェイスのサポートは、Cisco 1100 シリーズおよび Cisco 4000 シリーズ サービス統合型ルータでのみ使用できます。

ステップ 6 [Custom Configuration] ページが表示されます。

カスタム構成はオプションです。この手順をスキップしても、[Network Profiles] ウィンドウでいつでも構成を適用できます。

カスタム構成の追加を選択した場合：

1. 必要に応じて、[Onboarding Template(s)] または [Day-N Template(s)] タブをクリックします。
2. ドロップダウンリストからテンプレートを選択します。テンプレートは、[Device Type] と [Tag Name] でフィルタリングされます。
3. [Next] をクリックします。

ステップ 7 [Summary] ページで、[Save] をクリックします。

このページには、ルータ設定の概要が表示されます。複数のデバイスがある場合は、各デバイスをクリックして設定データを表示できます。このページでは、デバイスと選択されたサービスに基づいてハードウェアの推奨事項が提示されます。

ステップ 8 [Network Profiles] ウィンドウが表示されます。このウィンドウでは、ネットワークプロファイルを編集および削除できます。

[Assign Site] をクリックして、ネットワーク プロファイルにサイトを割り当てます。詳細については、サイトの作成、編集、削除 （285 ページ）を参照してください。

スイッチ用のネットワークプロファイルの作成

スイッチングプロファイルには、次の 2 つのタイプの設定テンプレートを適用できます。

- オンボーディングテンプレート
- Day-*n* テンプレート

始める前に

デバイスに適用する [Onboarding Configuration] テンプレートを定義します。このようなテンプレートには、ネットワーク上で管理できるようにデバイスをオンボードするための基本的なネットワーク設定コマンドが含まれています。デバイス設定の変更を自動化するテンプレートの作成 （571 ページ）を参照してください。

手順

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

ステップ 2 [+Add Profile] をクリックし、[Switching] を選択します。

ステップ 3 [Add a Network Profile] ページで、[Profile Name] フィールドにプロファイルの名前を入力します。

ステップ 4 このプロファイルと関連付けるプロファイルタイプのタブをクリックします。

関連付けの対象	結果...
オンボーディング テンプレート	[OnBoarding Template(s)] タブをクリックします。
day-n テンプレート	[Day-N Template(s)] タブをクリックします。

ステップ 5 [Attach Template] をクリックします。

ステップ 6 [Add Template] スライドインペインで、次の手順を実行します。

a) [Template] で、テンプレート名をクリックします。

[Search] フィールドに名前を入力してテンプレートを検索するか、プロジェクトを展開してテンプレートを選択できます。

（注） 以前の Catalyst Center リリースでは、タグをテンプレートに関連付けることができました。この機能は削除されました。

b) [Add] をクリックします。

ステップ 7 [Save] をクリックします。

スイッチに設定されているプロファイルは、スイッチのプロビジョニング時に適用されます。サイトを有効にするには、サイトにネットワークプロファイルを追加する必要があります。

ワイヤレス用のネットワークプロファイルの作成

始める前に

- **[Design]** > **[Network Settings]** > **[Wireless]** タブでワイヤレス SSID、RF プロファイル、AP プロファイルを作成していることを確認します。
- 必要に応じて、**[Design]** > **[CLI Templates]** ウィンドウでテンプレートを作成したことを確認します。
- 必要に応じて、**[Design]** > **[Feature Templates]** ウィンドウで機能テンプレートを作成したことを確認します。

手順

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

ステップ 2 [Add Profile] をクリックし、[Wireless] を選択します。

ステップ 3 [Profile Name] フィールドに有効なプロファイル名を入力します。

ステップ 4 サイトをプロファイルに追加するには、[Assign] をクリックして、次の手順を実行します。

a) [Add Sites To Profile] スライドインペインで、このプロファイルを関連付けるサイトのチェックボックスをオンにします。

親ノードまたは個々のサイトを選択できます。親サイトを選択すると、その親ノードの下にある子もすべて選択されます。チェックボックスをオフにして、サイトの選択を解除できます。

b) [Save] をクリックします。

ステップ 5 次のタブで必要な設定を構成します。

- [SSIDs]：詳細については、ネットワークプロファイルへの SSID の追加 （544 ページ）を参照してください。
- （オプション）[AP Zones]：詳細については、ネットワークプロファイルへの AP ゾーンの追加 （547 ページ）を参照してください。
- **[Feature Templates]**：詳細については、ネットワークプロファイルへの機能テンプレートの追加 （549 ページ） を参照してください。
- [Templates]：詳細については、ネットワークプロファイルへのテンプレートの追加 （549 ページ）を参照してください。
- （オプション）[Advanced Settings]：詳細については、ネットワークプロファイルの追加インターフェイスの構成 （566 ページ）およびネットワークプロファイルへの AP グループ、Flex グループ、サイトタグ、およびポリシータグの追加 （563 ページ）を参照してください。

ステップ 6 [Save] をクリックして、ネットワークプロファイルを追加します。

Catalyst Center は、**[Design]** > **[Network Profiles]** ウィンドウに新しいネットワーク プロファイルを表示します。

ネットワークプロファイルへの SSID の追加

SSID をネットワークプロファイルに追加できます。

始める前に

[Design] > **[Network Settings]** > **[Wireless]** > **[SSIDs]** ウィンドウでワイヤレス SSID が作成済みであることを確認します。

手順

ステップ 1 [Add a Network Profile] ウィンドウ（**[Design]** > **[Network Profiles]** > **[Add Profile]** > **[Wireless]**）で、[SSID] タブをクリックします。

ステップ 2 [Add SSID] をクリックします。

ステップ 3 [SSID] ドロップダウンリストで、作成済みの SSID を選択します。

ステップ 4 （任意） [WLAN Profile Name] フィールドに、WLAN プロファイルの名前を入力します。

（注）

- ネットワークプロファイルに関連付けられている SSID に **[Design]** > **[Network Settings]** > **[Wireless]** ウィンドウでサイトレベルのオーバーライドがない場合、Catalyst Center はプロビジョニング中にネットワークプロファイルで使用可能な WLAN プロファイル名を使用します。
- **[Design]** > **[Network Settings]** > **[Wireless]** ウィンドウで（ファブリック、FlexConnect、ゲストアンカー、ユーザーインターフェイス、スケジューラなどの設定に対して）オーバーライドがある SSID を複数のネットワークプロファイルに関連付ける必要がある場合は、プロビジョニングの失敗を防ぐために、WLANプロファイル名がすべてのネットワークプロファイルで SSID に対して一意であることを確認してください。
- ネットワークプロファイルに関連付けられている SSID にサイトレベルのオーバーライドがある場合、Catalyst Center は対応するサイトの ワイヤレスコントローラ プロビジョニング中に、オーバーライドされた SSID の WLANプロファイル名やポリシープロファイル名を使用します。このルールは、オーバーライドされたサイトが ワイヤレスコントローラ のネットワークプロファイルに関連付けられ、同じ ワイヤレスコントローラ によって管理されている場合に適用されます。
- ワイヤレスコントローラ でプロビジョニングされている既存の SSID の WLAN プロファイル名を変更すると、ワイヤレスコントローラ の再プロビジョニング中に、その SSID が削除され、新しい WLAN プロファイル名で再作成されます。
- リリース 2.3.5 より前のリリースからこのリリースにアップグレードすると、Catalyst Center によって、プロビジョニングされた WLAN プロファイル名とポリシープロファイル名が対応する既存の SSID に入力されます。

ステップ 5 （任意） [Policy Profile Name] フィールドで、ポリシープロファイル名を変更します。

デフォルトでは、Catalyst Center により WLAN プロファイル名がポリシープロファイル名として自動的にコピーされます。

ステップ 6 （任意） 次のいずれかのオプションで、[Copy to Policy Profile Name] チェックボックスを使用します。

- WLAN プロファイル名をポリシープロファイル名として自動的にコピーします。
- 別の名前をポリシープロファイルに入力します。

ステップ 7 （任意） [802.11be Profile Name] ドロップダウン リストから、802.11be プロファイルを選択します。

デフォルトでは、default-dot11be-profile 802.11be プロファイルが使用されます。このプロファイルは、Cisco IOS XE リリース 17.15.2 以降を実行している ワイヤレスコントローラ にのみ適用されます。

Cisco IOS XE リリース 17.18.1 より前のバージョンを実行している ワイヤレスコントローラ は、1 つの dot11be-profile のみを使用します。これは、default-dot11be-profile です。802.11be プロファイルを選択すると、対応する属性は ワイヤレスコントローラ の default-dot11be-profile にマッピングされます。

Cisco IOS XE リリース 17.18.1 以降を実行する ワイヤレスコントローラ では、カスタム 802.11be プロファイルがサポートされます。ワイヤレスコントローラ の単一ネットワークプロファイル内の SSID 全体では複数の 802.11be プロファイルが使用できます。

802.11be プロファイルの詳細については、802.11be プロファイルの作成 （527 ページ）を参照してください。

ステップ 8 [Yes] または [No] オプションボタンを使用して、SSID がファブリックであるか、非ファブリックであるかを指定します。

非ファブリック SSID を作成する場合は、[No] をクリックして、次のパラメータを設定します。

- [Enable SSID Scheduler] トグルボタンをクリックし、ドロップダウンリストからスケジューラを選択します。
- トラフィックスイッチングにインターフェイスを使用するには、[Interface] オプションボタンをクリックします。[インターフェイス名（Interface Name）] ドロップダウンリストから、SSID のインターフェイス名を選択するか、プラスアイコンをクリックしてワイヤレスインターフェイスを作成します。
- トラフィックスイッチングに VLAN グループを使用するには、[VLAN Group] オプションボタンをクリックします。[VLANグループ名（VLAN Group Name）] ドロップダウンリストから、SSID の VLAN グループ名を選択するか、プラスアイコンをクリックして VLAN グループを作成します。
- SSID にアンカーを追加するには、[Do you need Anchor for this SSID?] エリアで、[Yes] をクリックします。デフォルトでは、 [No] が選択されています。
- [Yes] を選択した場合は、[Select Anchor Group] ドロップダウンリストから、SSID のアンカーグループを選択します。アンカーグループの詳細については、「アンカーグループの作成 （499 ページ）」を参照してください。
- [No] を選択した場合は、[Flex Connect Local Switching] をオンにしてWLAN のローカルスイッチングを有効化します。

  SSID にアンカーを追加する場合、[Flex Connect Local Switching] は有効にできません。

（注） ワイヤレスコントローラで Flex SSID に対してすでにプロビジョニングされている非 Flex SSID を変更する場合（またはその逆の場合）は、ワイヤレスコントローラを再プロビジョニングする必要があります。これを行わない場合、期待されるインテントは ワイヤレスコントローラ に設定されません。たとえば、非 Flex SSID を Flex SSID に変更し、ワイヤレスコントローラ を再プロビジョニングしない場合、SSID はワイヤレスコントローラ で非 Flex のままになり、Flex サイトタグは作成されません。

SSID に関して [Flex Connect Local Switching] を有効にしている場合、ネットワークプロファイルがマッピングされているフロア上のすべての AP が FlexConnect モードに切り替わります。

[Flex Group] オプションは、[Advanced Settings] タブで有効になります。詳細については、ネットワークプロファイルへの AP グループ、Flex グループ、サイトタグ、およびポリシータグの追加（563 ページ）を参照してください。

ローカルスイッチングを有効化すると、この WLAN をアドバタイズするすべての FlexConnect AP がデータパケットをローカルにスイッチングできるようになります。

- [Flex Connect Local Switching] チェックボックスをオンにしている場合は、[Local to VLAN] フィールドに VLAN ID の値を入力します。

（注） 既存の SSID のローカル VLAN ID を変更し、ワイヤレスコントローラを再プロビジョニングせずに AP を再プロビジョニングすると、AP で使用される Flex プロファイルでローカル VLAN ID の最新値が更新されます。同じ Flex プロファイルが他の AP で使用されている場合、それらの AP のローカル VLAN ID も更新されます。

ステップ 9 （任意） 別の SSID を追加するには、プラスアイコンをクリックしてそのパラメータを設定します。

次のタスク

ネットワークプロファイルのその他の必要な設定を構成します。詳細については、ワイヤレス用のネットワークプロファイルの作成 （543 ページ）を参照してください。

ネットワークプロファイルへの AP ゾーンの追加

AP ゾーンを使用すると、同じサイト上の一連の AP に異なる SSID と RF プロファイルを関連付けることができます。デバイスタグを使用して、AP ゾーンを適用する AP を識別できます。[AP Zones] タブから、デバイスタグのネットワークプロファイルで設定された SSID のサブセットを使用して個別の AP ゾーンを作成できます。

Catalyst Center は、AP プロビジョニング中に AP ゾーン設定を AP に適用します。

（注）

- AP ですでにプロビジョニング済みの AP ゾーンの設定を更新する場合は、ワイヤレスコントローラ を再プロビジョニングする必要があります。AP を再プロビジョニングする必要はありません。
- Catalyst Center は、AP ゾーンの最適化をサポートしています。以前のリリースからリリース 3.2.2 にアップグレードする場合は、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラを再プロビジョニングしてこの最適化を有効にします。他のインテント変更がない場合は、ワイヤレスコントローラ を再プロビジョニングしても、新しい設定がデバイスにプッシュされることはありません。

  ワイヤレスコントローラ の再プロビジョニングの詳細については、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のプロビジョニング （782 ページ）」を参照してください。

AP プロビジョニング時：

- AP のデバイスタグとサイトに基づいて、Catalyst Center は対応する AP ゾーンを選択し、RF プロファイルを自動的に割り当てます。
- AP に 2 つの AP ゾーンが設定されている場合、必要な AP ゾーンを選択できます。
- AP の AP ゾーンがない場合は、必要な RF プロファイルを選択できます。

始める前に

[Design] > **[Network Settings]** > **[Wireless]** > **[SSIDs]** ウィンドウでワイヤレス SSID が作成済みであることを確認します。

手順

ステップ 1 [Add a Network Profile] ウィンドウ（**[Design]** > **[Network Profiles]** > **[Add Profile]** > **[Wireless]**）で、[AP Zones] タブをクリックします。

ステップ 2 [Add AP Zone] をクリックします。

ステップ 3 [AP Zone Name] フィールドに、AP ゾーンの名前を入力します。

ステップ 4 [Device Tags] ドロップダウンリストから、選択するデバイスタグの横にあるチェックボックスをオンにします。

ステップ 5 [RF Profile] ドロップダウンリストから、RF プロファイルを選択します。

ステップ 6 [SSID] ドロップダウンリストから、SSID を選択します。

ステップ 7 （任意） 別の AP ゾーンを追加するには、プラスアイコンをクリックしてそのパラメータを設定します。

次のタスク

ネットワークプロファイルのその他の必要な設定を構成します。詳細については、ワイヤレス用のネットワークプロファイルの作成 （543 ページ） を参照してください。

AP ゾーン設定を AP に適用するには、次の手順を実行します。

1. ワイヤレスコントローラ を再プロビジョニングします。詳細については、Cisco AireOS コントローラのプロビジョニング （738 ページ）およびCisco Catalyst 9800 シリーズ ワイヤレス コントローラ のプロビジョニング （782 ページ）を参照してください。
2. AP をプロビジョニングします。詳細については、Day 1 の Cisco AP プロビジョニング （745 ページ）を参照してください。

ネットワークプロファイルへの機能テンプレートの追加

機能テンプレートをネットワークプロファイルにアタッチできます。

手順

ステップ 1 **[Add a Network Profile]** ウィンドウ（**[Design]** > **[Network Profiles]** > **[Add Profile]** > **[Wireless]**）で、**[Feature Templates]** タブをクリックします。

ステップ 2 **[Add Feature Template]** をクリックします。

ステップ 3 [Add Feature Template] スライドインペインで、次の手順を実行します。

1. **[Filter by Device Type(s)]** をクリックし、デバイスタイプを選択します。

   [Search] フィールドに名前を入力してデバイス名を検索するか、[Switches and Hubs] または [Wireless Controller] を展開してデバイスタイプを選択できます。

2. **[Wireless]** を展開し、このネットワークプロファイルにアタッチする機能テンプレートを選択します。

   [Search Feature Template Designs] フィールドを使用して、機能テンプレートをフィルタ処理できます。

3. [APPLICABILITY] の [Tags] ドロップダウンリストから、該当するタグを選択します。
4. [Add] をクリックします。

次のタスク

ネットワークプロファイルのその他の必要な設定を構成します。詳細については、ワイヤレス用のネットワークプロファイルの作成 （543 ページ）を参照してください。

ネットワークプロファイルへのテンプレートの追加

テンプレートをネットワークプロファイルに関連付けることができます。

始める前に

[Design] > **[CLI Templates]** ウィンドウで必要なテンプレートを作成する必要があります。詳細については、テンプレートの作成 （575 ページ）を参照してください。

手順

ステップ 1 [Add a Network Profile] ウィンドウ（**[Design]** > **[Network Profiles]** > **[Add Profile]** > **[Wireless]**） で、[Templates] タブをクリックします。

ステップ 2 次のタスクを実行します。

- 導入準備テンプレートを関連付けるには、[OnBoarding Template(s)] タブをクリックします。
- Day-*n* テンプレートを関連付けるには、[Day-N Template(s)] タブをクリックします。

ステップ 3 [Attach Template] をクリックします。

ステップ 4 [Add Template] スライドインペインで、次の手順を実行します。

a) [Template] で、テンプレート名をクリックします。

[Search] フィールドに名前を入力してテンプレートを検索するか、プロジェクトを展開してテンプレートを選択できます。

b) [Add] をクリックします。

次のタスク

ネットワークプロファイルのその他の必要な設定を構成します。詳細については、ワイヤレス用のネットワークプロファイルの作成 （543 ページ）を参照してください。

APグループ、Flexグループ、サイトタグ、およびポリシータグの概要

[**Design** > **Network Profiles** > **Wireless**] ウィンドウの [**Advanced Settings**] タブので、AP グループ、Flex グループ、サイトタグ、およびポリシータグのカスタム名を定義できます。詳細については、ネットワークプロファイルへの AP グループ、Flex グループ、サイトタグ、およびポリシータグの追加 （563 ページ）を参照してください。

AP のプロビジョニング時に Catalyst Center は [Advanced Settings] タブの [Provision Group] 設定で指定された、新しく追加されたカスタム名を設定し AP に適用します。

（注）

- AP グループと Flex グループの設定を Cisco AireOS ワイヤレスコントローラ に適用できます。
- サイトタグとポリシータグの設定を Cisco Catalyst 9800 シリーズ ワイヤレス コントローラに適用できます。

  新しく追加されたサイトとポリシータグの設定は、AP のプロビジョニング時に適用されます。ワイヤレスコントローラを単独でプロビジョニングしても、新しいカスタムタグは AP に設定されません。プロビジョニング後にタグを変更する場合は、ワイヤレスコントローラ または AP を再プロビジョニングする必要があります。

  ワイヤレスコントローラ および AP をプロビジョニングまたは再プロビジョニングするときは、次のシナリオについて考慮してください。

  - ネットワークプロファイルにカスタムサイトやポリシータグが設定されていない場合、Catalyst Center では自動生成されたタグが使用され、これが ワイヤレスコントローラ に設定され、この変更が AP のプロビジョニング時にのみ AP に適用されます。
  - ネットワークプロファイルにカスタムサイトやポリシータグが設定されている場合、Catalyst Center ではカスタムタグが ワイヤレスコントローラ に設定され、この変更が AP のプロビジョニング時にのみ AP に適用されます。
  - ワイヤレスコントローラ および AP が自動生成タグを使用してすでにプロビジョニングされている状況で、ネットワークプロファイルで新しいカスタムタグを作成する場合は、ワイヤレスコントローラ または AP を再プロビジョニングして変更を適用する必要があります。
  - ワイヤレスコントローラ および AP がすでにカスタムタグを使用してプロビジョニングされている状況で、ネットワークプロファイルからカスタムタグを削除する場合は、ワイヤレスコントローラ または AP を再プロビジョニングする必要があります。
    - ワイヤレスコントローラを再プロビジョニングすると、カスタムタグ設定が削除され、ワイヤレスコントローラおよび関連する AP に自動生成されたタグが設定されます。
    - ワイヤレスコントローラを再プロビジョニングせずに、AP を直接再プロビジョニングすると、自動生成されたタグが AP に設定されますが、カスタムタグ設定はワイヤレスコントローラから削除されません。タグは、次回の ワイヤレスコントローラ の再プロビジョニング時に削除されます。
  - FlexConnect ネイティブ VLAN のオーバーライドが設定されていて、サイトタグがサイト内のすべてのフロアに対して同じカスタム Flex プロファイルにマッピングされている状態で Catalyst Center にアップグレードした場合は、フロアごとに異なるサイトタグを使用してネットワークプロファイルを再設定する必要があります。再設定しないと、プロビジョニングが失敗する可能性があります。

複数のエリア内のサイト（建物またはフロア）全体で、同じ AP グループと Flex グループを使用できます。子サイトは、親サイトから AP グループと Flex グループを継承します。ただし、子サイトに AP グループまたは Flex グループを作成すると、親サイトから継承された設定は上書きされます。建物のさまざまなフロアで SSID が上書きされている場合、そのようなフロアでは AP グループまたはフレックス グループを再利用することはできません。AP グループと Flex グループの再利用の例については、カスタム AP グループと Flex グループの再利用の例（556 ページ）を参照してください。

複数のサイトで同じ AP グループと Flex グループを使用する場合は、次のシナリオを考慮してください。

- 共有 AP グループに同じ RF プロファイルを設定する必要があります。

  たとえば、カスタム AP グループ *AP-Group-1* は、*Network-Profile-1* と *Network-Profile-2* で共有されます。これは、同じ AP ゾーン名（デフォルトまたはカスタム AP ゾーン）を持つ同じ ワイヤレスコントローラ によって管理されます。*Network-Profile-1* で *RF-Profile-1* を使用し、*Network-Profile-2* で *RF-Profile-2* を使用する場合、プロビジョニング中に検証エラーが発生します。*AP-Group-1* に同じ RF プロファイルを設定する必要があります。

- 共有カスタム AP グループに同じ AP ゾーン名を設定する必要があります。

  たとえば、カスタム AP グループ *AP-Group-1* は、*Network-Profile-1* と *Network-Profile-2* で共有されます。両方のネットワークプロファイルで同じ RF プロファイル *RF-Profile-1* が使用されます。*Network-Profile-1* で AP ゾーンの *default-zone* を使用し、*Network-Profile-1* で *AP-Zone-1* を使用する場合、プロビジョニング中に検証エラーが発生します。*AP-Group-1* に同じ AP ゾーン名を設定する必要があります。

- 共有カスタム AP グループの場合、アクティブな AP があるサイトが削除され、同時に RF プロファイルも変更された場合は、AP を再プロビジョニングする前に次のタスクのいずれかを実行します。

  - 別のカスタム AP グループを作成し、カスタム AP グループから削除されたサイトの AP を再プロビジョニングします。
  - カスタム AP グループを作成せずに AP を再プロビジョニングし、Catalyst Centerで生成された AP グループがその AP で使用されるようにします。その後、更新された RF プロファイルと共有カスタム AP グループを使用して AP を再プロビジョニングします。

  たとえば、*RF-Profile-1* を使用するカスタム AP グループ *AP-Group-1* は、*Building-1*/*Floor-1* と *Building-2*/*Floor-2* で共有されます。*Building-1*/*Floor-1* および *Building-2*/*Floor-2* に AP をプロビジョニングすると、その AP は両方のフロアの *AP-Group-1* に参加します。RF プロファイルを *RF-Profile-2* に変更し、同時に *AP-Group-1* から *Building-2*/*Floor-2* を削除すると、プロビジョニング中に検証エラーが発生します。*Building-2*/*Floor-2* の AP を必要な AP グループに移動するには、それらの AP を再プロビジョニングする必要があります。その後、*Building-1*/*Floor-1* の AP を再プロビジョニングします。

- 共有カスタム AP グループの場合、AP ゾーン名が変更された場合は、古い AP ゾーンにある既存の AP を再プロビジョニングする必要があります。その後、新しい AP ゾーンとカスタム AP グループを使用して AP を再プロビジョニングします。

たとえば、*Network-Profile-1* は、*AP-Group-1*、*RF-Profile-1*、および *AP-Zone-1* を持つ *Building-1*/*Floor-1* に割り当てられます。*Network-Profile-2* は、*AP-Group-1*、*RF-Profile-1*、および *AP-Zone-1* を使用して *Building-2*/*Floor-2* に割り当てられます。*Wireless-Controller-1* の管理対象 AP の場所は、*Building-1* および *Building-2* として設定されます。*AP1* は *Building-1*/*Floor-1* でプロビジョニングされ、*AP2* は *Building-2*/*Floor-2* でプロビジョニングされます。*Network-Profile-1* と *Network-Profile-2* の両方で AP グループを *New-AP-Group* に、AP ゾーンを *AP-Zone-3* に変更し、対応するフロアで *AP1* または *AP2* を *AP-Zone-3* を使用して再プロビジョニングすると、検証エラーが発生します。*AP1* と *AP2* は *AP-Zone-1* を使用して再プロビジョニングする必要があります。その後、*AP1* と *AP2* を *AP-Zone-3* と *New-AP-Group* を使用して再プロビジョニングします。

- 共有カスタム AP グループの場合、親サイトの AP ゾーンを変更すると、変更内容は子サイトにも継承されます。子サイトに割り当てられるネットワークプロファイルに必要な AP ゾーンを作成する必要があります。

（注） 子サイトにオーバーライドされた設定がある場合、設定は上書きされません。

たとえば、*Building-1* に子サイト *Floor-1* と *Floor-2* が含まれている場合、*Network-Profile-1* は *Building-1* と *Floor-1* に割り当てられ、*AP-Group-1*、*AP-Zone-1*、および *RF-Profile-1* は *Building-1* に対して設定されます。*Network-Profile-2* は *Floor-2* に割り当てられ、*AP-Group-1*、*AP-Zone-1*、および *RF-Profile-1* は *Floor-2* に対して設定されます。*AP1* は *Floor-1* でプロビジョニングされ、*AP2* は *AP-Zone-1* を使用して *Floor-2* でプロビジョニングされます。*Building-1* の *AP-Group-1* の AP ゾーン設定は、*AP-Zone-2* と *RF-Profile-2* を使用するように更新されます。*Floor-2* は *Building-1* から値を継承するため、*Building-1* の AP グループ設定を更新すると、*Floor-2* に自動的に反映されるため、*APZone-2* は *Network-Profile-2* に存在しない場合でも、継承により *Floor-2* AP グループの設定で更新されます。*AP-Zone-2* を使用して *Floor-1* の *AP1* を再プロビジョニングすると、検証エラーが発生します。*Network-Profile-2* に *AP-Zone-1* を作成する必要があります。

- 共有カスタム AP グループが複数のサイトで使用されているが、それらのサイト間で SSID が異なる場合、AP のプロビジョニングは失敗します。SSID マッピングがサイト間で同一でない場合、Catalyst Center は AP グループの再利用をサポートしません。この問題を解決するには、異なる SSID が必要なサイトに一意のカスタム AP グループを作成してから、AP を再プロビジョニングします。

  たとえば、カスタム AP グループ APGroup1 は、AP-Zone-1、SSID WLAN-1、および RF プロファイル Typical を使用して Building-1/Floor-1 に設定されます。Building-1/Floor-2 には、AP-Group-1 が AP-Zone-1、SSID WLAN-2、および RF プロファイル Typical を持っています。*AP1* は *Floor-1* でプロビジョニングされ、*AP-Group-1* を使用します。APGroup1 を使用して Floor-2 で AP2 をプロビジョニングする場合、SSID マッピングがこれら 2 つのサイトで異なるため、検証エラーが発生します。AP2 を再プロビジョニングする前に、Floor-2 の一意のカスタム AP グループを作成する必要があります。

- 共有カスタム AP グループの場合、RF プロファイルを変更し、対応する AP を再プロビジョニングすると、カスタム AP グループを使用するすべての AP のサイト全体で新しい RF プロファイルを使用してカスタム AP グループが更新されます。

  たとえば、カスタム AP グループ *AP-Group-1* は、*Network-Profile-1* と *Network-Profile-2* で共有されます。Network-Profile-1 は Building-1/Floor-1 に割り当てられ、AP-Group-1 と RF-Profile-1 を使用します。Network-Profile-2 は Building-2/Floor-2 に割り当てられ、AP-Group-1 と RF-Profile-1 を使用します。ワイヤレスコントローラはプロビジョニングされ、AP1 は Building-1/Floor-1 でプロビジョニングされ、AP2 は Building-2/Floor-2 でプロビジョニングされます。ネットワークプロファイルの両方で AP-Group-1 の RF プロファイルを RF-Profile-2 に更新し、AP1 と AP2 を再プロビジョニングすると、AP-Group-1 は Floor-1 と Floor-2 の両方で RF-Profile-2 を使用するように更新されます。

- 異なるネイティブ VLAN または AAA オーバーライド VLAN を持つ複数のサイトで同じ Flex グループを使用することはできません。

カスタムポリシータグは、サイト（エリア、建物、フロア）全体で再利用できます。サイト（エリア、建物、または建物内の複数のフロア）にカスタムポリシータグを割り当てると、そのサイトと AP ゾーンに対してプロビジョニングされたすべての AP が同じカスタムポリシータグを使用できます。デフォルトでは、カスタムポリシータグはデフォルト AP ゾーンの AP に適用されます。カスタム AP ゾーンの場合は、ポリシータグを編集し、必要なゾーンにカスタムポリシータグを割り当てます。

（注） カスタムポリシータグを再利用する場合は、次の点に注意してください。

- 子サイトは、親サイトからカスタムポリシータグを継承します。ただし、子サイトに別のポリシータグを作成すると、親サイトから継承された設定はオーバーライドされます。
- 複数のサイトおよび複数の AP ゾーンにカスタムポリシータグを割り当てることができます。ポリシータグに関連付けられたすべての AP ゾーンは、同じ SSID のセットを共有する必要があり、SSID の設定は同じである必要があります。ポリシータグが、異なる SSID 設定を持つ複数の AP ゾーンに関連付けられている場合、ポリシータグまたはネットワークプロファイルの編集中にエラーが表示されます。
- カスタムポリシータグを共有し、同じ ワイヤレスコントローラ によって管理されているサイトのいずれかの SSID 設定が、サイトレベルの SSID オーバーライドが原因で異なっている場合、カスタムポリシータグは共有できません。このような場合、同じカスタムポリシータグで WLAN プロファイルとポリシー プロファイル マッピングが異なるため、プロビジョニング（AP プロビジョニングまたはワイヤレスコントローラ プロビジョニング（[Skip AP Provision] チェックボックスがオフの場合））中に検証エラーが発生します。失敗の理由を含むエラーメッセージが設定のプレビューに表示されます。このエラーメッセージには、カスタムポリシータグの不一致がある最大 5 つのサイトの詳細が示されます。カスタムポリシータグの使用方法の詳細については、「カスタムポリシータグの再利用の使用例 （559 ページ）」を参照してください。
- ポリシータグは、WLAN および RLAN プロファイルにマッピングされます。ポリシータグを変更すると、RLAN の設定に影響を与える可能性があります。
- ポリシータグの再利用は、Catalyst Center で自動生成されたタグではサポートされていません。

カスタム Flex プロファイルは、 ワイヤレスコントローラ プロビジョニング中または AP プロビジョニング中に、それぞれに応じて次のように設定されます。

- ワイヤレスコントローラのプロビジョニング中：ネットワークプロファイルにアタッチされている Flex 機能テンプレートがある場合、カスタム Flex プロファイルまたは Catalyst Center で自動生成された Flex プロファイル（カスタムサイトタグの設定時に選択したオプションに基づく）は ワイヤレスコントローラ のプロビジョニング中に作成されます。カスタム Flex プロファイルは、**[IP Overlap]** が有効になっている機能テンプレートで定義されている Catalyst Center インテント設定を除き、デフォルトの Flex プロファイルと同じ設定で構成されます。ワイヤレスコントローラ をプロビジョニングした後に AP をプロビジョニングすると、FlexConnect VLAN 設定（ネイティブ VLAN および AAA オーバーライド VLAN が設定されている場合）を除き、カスタム Flex プロファイルは上書きされません。
- AP プロビジョニング中：ネットワークプロファイルにアタッチされている機能テンプレートがない場合、AP プロビジョニング中にカスタム Flex プロファイルが作成されます。カスタム Flex プロファイルは、FlexConnect VLAN 設定（ネイティブ VLAN および AAA オーバーライド VLAN）を除き（設定されている場合）、デフォルトの Flex プロファイルと

同じ設定で構成されます。Catalyst Center では、AP のプロビジョニング中にカスタム Flex プロファイルでペアワイズマスターキー（PMK）の伝達が有効になります。

カスタム AP グループと Flex グループの再利用の例

シナリオ 1

カスタム AP グループと Flex グループは、サイトのオーバーライドがない複数のサイト間で共有され、すべてのサイトが同じ ワイヤレスコントローラ によって管理されます。

Site	サイトのオーバーライド	AP グループ、AP ゾーン、および RF プロファイル	ネイティブ VLAN ID のオーバーライド	プライマリ ワイヤレスコントローラ
Area-1/Building-1/Floor-1	なし	*Custom-AP-Group-1*、*default-zone*、*Typical*	なし	*Wireless-Controller-1*
Area-2/Building-1/Floor-1	なし	*Custom-AP-Group-1*、*default-zone*、*Typical*	なし	*Wireless-Controller-1*

このシナリオでは、カスタム AP グループと Flex グループをサイト間で共有でき、同じカスタム AP グループを使用して AP をそれらのサイトに正常にプロビジョニングできます。

シナリオ 2

カスタム AP グループは、一部のサイトに SSID のサイトのオーバーライドがある複数のサイト間で共有され、すべてのサイトが同じ ワイヤレスコントローラ によって管理されます。

Site	サイトのオーバーライド	AP グループ、AP ゾーン、および RF プロファイル	プライマリワイヤレスコントローラ
Area-1/Building-1/Floor-1	サイトのオーバーライド：PSK の変更	*Custom-AP-Group-1*、*AP-Zone-1*、*HIGH*	*Wireless-Controller-1*
Area-2/Building-1/Floor-1	なし	*Custom-AP-Group-1*、*AP-Zone-1*、*HIGH*	*Wireless-Controller-1*

このシナリオでは、同じSSIDに対して異なるWLANプロファイルマッピングがあるため、カスタム AP グループは再利用できません。同じカスタム AP グループを使用してこれらのサイトに AP をプロビジョニングすると、プロビジョニング中に検証エラーが発生します。

（注） このサイト階層の最初のサイト（*Area-1/Building-1/Floor-1*）の AP プロビジョニングは成功しますが、カスタム AP グループを再利用しようとしている *Area-2/Building-1/Floor-1* での 2 番目の AP プロビジョニング中に検証エラーが表示されます。

シナリオ 3

カスタム AP グループは、RF プロファイルが異なる複数のサイト間で共有され、すべてのサイトが同じ ワイヤレスコントローラ によって管理されます。

Site	サイトのオーバーライド	AP グループ、AP ゾーン、および RF プロファイル	プライマリ ワイヤレスコントローラ
Area-1/Building-1/Floor-1	なし	*Custom-AP-Group-1*、*AP-Zone-1*、*HIGH*	*Wireless-Controller-1*
Area-2/Building-1/Floor-1	なし	*Custom-AP-Group-1*、*AP-Zone-1*、*LOW*	*Wireless-Controller-1*

このシナリオでは、RF プロファイルが異なるため、カスタム AP グループは再利用できません。同じカスタム AP グループを使用してこれらのサイトに AP をプロビジョニングすると、プロビジョニング中に検証エラーが発生します。

（注） このサイト階層の最初のサイト（*Area-1/Building-1/Floor-1*）の AP プロビジョニングは成功しますが、カスタム AP グループを再利用しようとしている *Area-2/Building-1/Floor-1* での 2 番目の AP プロビジョニング中に検証エラーが表示されます。

シナリオ 4

カスタム AP グループは、一部のサイトにプライマリコントローラに対する SSID のサイトのオーバーライドがなく、セカンダリコントローラに対するオーバーライドがある複数のサイト間で共有されます。

Site	サイトのオーバーライド	AP グループ、AP ゾーン、および RF プロファイル	プライマリ ワイヤレスコントローラ	セカンダリ ワイヤレスコントローラ
Building-1	なし	*Custom-AP-Group-1*、*AP-Zone-1*、*HIGH*	*Wireless-Controller-1*	*Wireless-Controller-2*
Building-1/*Floor-1*	なし	*Custom-AP-Group-1*、*AP-Zone-1*、*HIGH*	*Wireless-Controller-1*	*Wireless-Controller-2*

Site	サイトのオーバーライド	AP グループ、AP ゾーン、および RF プロファイル	プライマリ ワイヤレスコントローラ	セカンダリ ワイヤレスコントローラ
Building-1/Floor-2	なし	*Custom-AP-Group-1*、*AP-Zone-1*、*HIGH*	*Wireless-Controller-1*	*Wireless-Controller-2*
Building-2/Floor-1	SSID オーバーライド	*Custom-AP-Group-1*、*AP-Zone-1*、*LOW*	*Wireless-Controller-2*	なし

このシナリオでは、*Wireless-Controller-2* に対して同じ SSID の異なる WLAN プロファイルマッピングがあるため、カスタム AP グループは再利用できません。同じカスタム AP グループを使用してこれらのサイトに AP をプロビジョニングすると、プロビジョニング中に検証エラーが発生します。

（注） このサイト階層の最初のサイト（*Building-1/Floor-1*）の AP プロビジョニングは成功しますが、カスタム AP グループを再利用しようとしている *Building-2/Floor-1* での 2 番目の AP プロビジョニング中に検証エラーが表示されます。

シナリオ 5

カスタム AP グループは、異なる一連の WLAN が複数のサイト間で共有され、すべてのサイトが同じ ワイヤレスコントローラ によって管理されます。

Site	サイトのオーバーライド	AP グループ、AP ゾーン、および RF プロファイル	プライマリ ワイヤレスコントローラ
Area-1/Building-1/Floor-1	なし	*Custom-AP-Group-1*、*AP-Zone-1*（*WLAN-1*、*WLAN-2*）、*HIGH*	*Wireless-Controller-1*
Area-2/Building-1/Floor-1	なし	*Custom-AP-Group-1*、*AP-Zone-1*（*WLAN-3*、*WLAN-4*）、*HIGH*	*Wireless-Controller-1*

このシナリオでは、同じ ワイヤレスコントローラ に対して異なる WLAN プロファイルマッピングがあるため、カスタム AP グループは再利用できません。同じカスタム AP グループを使用してこれらのサイトに AP をプロビジョニングすると、プロビジョニング中に検証エラーが発生します。

（注） このサイト階層の最初のサイト（*Area-1/Building-1/Floor-1*）の AP プロビジョニングは成功しますが、カスタム AP グループを再利用しようとしている *Area-2/Building-1/Floor-1* での 2 番目の AP プロビジョニング中に検証エラーが表示されます。

カスタムポリシータグの再利用の使用例

シナリオ 1

カスタムポリシータグは、サイトのオーバーライドがない複数のサイト間で共有され、すべてのサイトが同じ シスコ ワイヤレス コントローラ によって管理されます。

Site	サイトのオーバーライド	ポリシータグと AP ゾーン	プライマリワイヤレスコントローラ
建物 1/フロア 1	なし	カスタムポリシータグ 1、デフォルトゾーン	ワイヤレスコントローラ 1
建物 1/フロア 2	なし	カスタムポリシータグ 1、デフォルトゾーン	ワイヤレスコントローラ 1

このシナリオでは、カスタムポリシータグをサイト間で共有でき、同じカスタムポリシータグを使用して AP をこれらのサイトに正常にプロビジョニングできます。

シナリオ 2

カスタムポリシータグは、一部のサイトに SSID のサイトのオーバーライドがある複数のサイト間で共有され、すべてのサイトが同じ ワイヤレスコントローラ によって管理されます。

Site	サイトのオーバーライド	ポリシータグと AP ゾーン	プライマリワイヤレスコントローラ
建物 1/フロア 1	サイトのオーバーライド	カスタムポリシータグ 1、デフォルトゾーン	ワイヤレスコントローラ 1
建物 1/フロア 2	なし	カスタムポリシータグ 1、デフォルトゾーン	ワイヤレスコントローラ 1

このシナリオでは、同じタグに同じ SSID の 2 つの異なる WLAN プロファイルとポリシー プロファイルマッピングがあるため、カスタムポリシータグは再利用できません。同じカスタムポリシータグを使用してこれらのサイトに AP をプロビジョニングすると、プロビジョニング中に検証エラーが発生します。

（注） このサイト階層の最初のサイト（建物 1/フロア 1）の AP プロビジョニングは成功しますが、カスタムポリシータグを再利用しようとしている建物 1/フロア 2 での 2 番目の AP プロビジョニング中に検証エラーが表示されます。

シナリオ 3

カスタムポリシータグは、一部のサイトに SSID のサイトオーバーライドがある複数のサイト間で共有され、サイトが個々のプライマリ ワイヤレスコントローラ によって管理されます。

Site	サイトのオーバーライド	ポリシータグと AP ゾーン	プライマリワイヤレスコントローラ
建物 1/フロア 1	サイトのオーバーライド	カスタムポリシータグ 1、デフォルトゾーン	ワイヤレスコントローラ 2
建物 1/フロア 2	なし	カスタムポリシータグ 1、デフォルトゾーン	ワイヤレスコントローラ 1

このシナリオでは、カスタムポリシータグを再利用でき、同じカスタムポリシータグを使用して AP をこれらのサイトに正常にプロビジョニングできます。

シナリオ 4

カスタムポリシータグは、一部のサイトにプライマリ ワイヤレスコントローラ のサイトのオーバーライドがない場合と、セカンダリ ワイヤレスコントローラ のオーバーライドがある場合の複数のサイト間で共有されます。すべてのサイトが同じプライマリ ワイヤレスコントローラによって管理され、N+1 HA が設定されています。

Site	サイトのオーバーライド	ポリシータグと AP ゾーン	プライマリ ワイヤレスコントローラ	セカンダリ ワイヤレスコントローラ
建物 1/フロア 1	グローバルレベルからのオーバーライドなし	カスタムポリシータグ 1、デフォルトゾーン	ワイヤレスコントローラ 2	-
建物 *2*	サイトのオーバーライド	カスタムポリシータグ 1、デフォルトゾーン	ワイヤレスコントローラ 1	ワイヤレスコントローラ 2
建物 2/フロア 1	建物 2 からのオーバーライドなし	カスタムポリシータグ 1、デフォルトゾーン	ワイヤレスコントローラ 1	ワイヤレスコントローラ 2
建物 2/フロア 2	建物 2 からのオーバーライドなし	カスタムポリシータグ 1、デフォルトゾーン	ワイヤレスコントローラ 1	ワイヤレスコントローラ 2

このシナリオでは、すべてのサイトが同じ N+1 ワイヤレスコントローラ によって管理されているため、カスタムポリシータグをワイヤレスコントローラ 2 に再利用することはできません。同じタグの同じ ワイヤレスコントローラ（ワイヤレスコントローラ 2）の同じ SSID に、2 つの異なる WLAN プロファイルとポリシー プロファイル マッピングがあるからです。ワイ

ヤレスコントローラ2をプロビジョニングすると、検証エラーが発生します。ただし、ワイヤレスコントローラ 1 のプロビジョニング中にエラーは発生しません。

（注） 検証は、ワイヤレスコントローラ ごとに個別に実行されます。

シナリオ 5

カスタムポリシータグは、同じネットワークプロファイルを持つエリア間で共有されます。

Site	サイトのオーバーライド	ポリシータグと AP ゾーン	プライマリワイヤレスコントローラ
エリア 1/建物 1/フロア 1	なし	カスタムポリシータグ 1、デフォルトゾーン	ワイヤレスコントローラ 1
エリア 2/建物 2/フロア 1	なし	カスタムポリシータグ 1、デフォルトゾーン	ワイヤレスコントローラ 1 または 2

このシナリオでは、同じネットワークプロファイルの下で異なるエリアを管理するワイヤレスコントローラ 間でカスタムポリシータグを共有できます。

シナリオ 6

カスタムポリシータグは、複数のネットワークプロファイルを持つエリア間で共有されます。

例 *1*

この例では、カスタムポリシータグは、異なるネットワークプロファイルを持つエリア間で再利用できます。

Site	ネットワークプロファイル	サイトのオーバーライド	ポリシータグと AP ゾーン	プライマリ ワイヤレスコントローラ
エリア 1/建物 1/フロア 1	プロファイル *1*	なし	カスタムポリシータグ 1、デフォルトゾーン	ワイヤレスコントローラ 1
エリア 2/建物 2/フロア 1	プロファイル 2	なし	カスタムポリシータグ 1、デフォルトゾーン	ワイヤレスコントローラ 1 または 2

例 *2*

この例では、エリア2でのサイトのオーバーライドにより、カスタムポリシータグを再利用できません。

Site	ネットワークプロファイル	サイトのオーバーライド	ポリシータグと AP ゾーン	プライマリ ワイヤレスコントローラ
エリア 1/建物 1/フロア 1	プロファイル *1*	なし	カスタムポリシータグ 1、デフォルトゾーン	ワイヤレスコントローラ 1
エリア 2/建物 2/フロア 1	プロファイル 2	エリア 2 でのサイトのオーバーライド	カスタムポリシータグ 1、デフォルトゾーン	ワイヤレスコントローラ 1 または 2

シナリオ 7

カスタムポリシータグは、複数の AP ゾーン間で共有されます。

例 *1*

この例では、2 つの AP ゾーン（作業領域、廊下）に同じ SSID のセット（SSID 1）がある場合、これらの AP ゾーン間で同じカスタムポリシータグを再利用できます。

Site	サイトのオーバーライド	ポリシータグと AP ゾーン	プライマリワイヤレスコントローラ
エリア 1/建物 1/フロア 1	なし	カスタムポリシータグ 1、作業領域（SSID 1）	ワイヤレスコントローラ 1
エリア 2/建物 2/フロア 1	なし	カスタムポリシータグ 1、廊下（SSID 1）	ワイヤレスコントローラ 1

例 *2*

この例では、AP ゾーンに同じ SSID のセットがないため、カスタムポリシータグを再利用できません。

サイト	サイトのオーバーライド	ポリシータグと AP ゾーン	プライマリワイヤレスコントローラ
エリア 1/建物 1/フロア 1	なし	カスタムポリシータグ 1、作業領域（SSID 1、SSID 2）	ワイヤレスコントローラ 1
エリア 2/建物 2/フロア 1	なし	カスタムポリシータグ 1、廊下（SSID 1）	ワイヤレスコントローラ 1

（注） 共有カスタムポリシータグを再設定すると（たとえば、ポリシータグの AP ゾーンを別のタグと交換するなど）、まだ再プロビジョニングされていない他のフロアの既存の AP で設定の競合が発生します。まだプロビジョニングされていない AP は古い設定を使用しているため、これによりプロビジョニングが行われません。ただし、タグを共有するすべての AP が同じフロアにある場合は、共有カスタムポリシータグの再設定ができます。すべてのゾーンの AP を再プロビジョニングすると、AP は最新の設定で更新されます。

ネットワークプロファイルへの AP グループ、Flex グループ、サイトタグ、およびポリシータグの追加

Catalyst Center では、ネットワークプロファイルへの AP グループ、Flex グループ、サイトタグ、およびポリシータグの追加が可能です。AP グループと Flex グループを追加すると、反復的な構成変更の必要がなくなることで AP プロビジョニング時の時間を節約でき、デバイス間の一貫性を確保できます。カスタム名を設定しない場合、Catalyst Centerは自動生成された AP グループ名と AP のタグを使用します。

（注） Flex グループ設定は、ネットワークプロファイルに少なくとも 1 つのフレックスベースの SSID が関連付けられている場合にのみ使用できます。

始める前に

- ネットワークプロファイルにサイトが割り当てられていることを確認します。
- Flex グループ名を作成するには、[SSIDs] タブで、[Flex Connect Local Switching] チェックボックスをオンにし、[Local to VLAN] テキストボックスで VLAN ID を定義して、非ファブリック SSID を Flex ベースの SSID としてマークしていることを確認します。詳細については、ネットワークプロファイルへの SSID の追加（544 ページ）を参照してください。

  SSID に関して [Flex Connect Local Switching] を有効にしている場合、ネットワークプロファイルがマッピングされているフロア上のすべての AP が FlexConnect モードに切り替わります。
- ワイヤレスデバイスの再プロビジョニングと、グループおよびタグの使用については、AP グループ、Flex グループ、サイトタグ、およびポリシータグの概要（550 ページ）を参照してください。

手順

ステップ 1 [Add a Network Profile] ウィンドウ（**[Design]** > **[Network Profiles]** > **[Add Profile]** > **[Wireless]**）で、[Advanced Settings] にカーソルを合わせ [Provision Group] をクリックします。

ステップ 2 （任意）ネットワークプロファイルで AP グループを作成するには、[AP Groups and AP Profiles] を展開し、[Create Custom AP Group] をクリックします。

[Add AP Group] スライドインペインで、次の手順を実行します。

a) [AP Group Name] フィールドに、AP グループ名を入力します。

b) [AP Zone] ドロップダウンリストから、AP ゾーンを選択します。

ネットワークプロファイルに関連付けられたすべての SSID をブロードキャストするには、[Not Applicable] を選択します。

（注） このドロップダウンリストは、[AP Zones] タブでネットワークプロファイルに AP ゾーンを追加した場合に有効になります。詳細については、ネットワークプロファイルへの AP ゾーンの追加 （547 ページ）を参照してください。

AP ゾーンを選択した場合、RF プロファイルが AP ゾーン設定から継承されます。

c) [AP Profile] ドロップダウンリストから、AP プロファイルを選択します。

AP プロファイルを作成するには、[Create New] をクリックします。詳細については、AP プロファイル（501 ページ）を参照してください。

d) [RF Profile] ドロップダウンリストから、RF プロファイルを選択します。

（注） [AP Zone] ドロップダウンリストから AP ゾーンを選択した場合、このドロップダウンリストは無効になります。

e) [Select Sites] エリアで、名前を入力してサイトを検索するか、[Global] を展開してサイトを選択します。

f) [Save] をクリックします。

ステップ 3 （任意）ネットワークプロファイルで Flex グループを作成するには、[Flex Group] を展開し、[Create Flex Group] をクリックします。

[Create Flex Group] スライドインペインで、次の手順を実行します。

a) [Flex Group Name] フィールドに、Flex グループ名を入力します。

b) [Select Sites] エリアで、名前を入力してサイトを検索するか、[Global] を展開してサイトを選択します。

c) [Save] をクリックします。

ステップ 4 （任意） ネットワークプロファイルでサイトタグを作成するには、[Site Tags and AP Profiles] を展開し、[Create Custom Site Tag] をクリックします。

[Create Site Tag] スライドインペインで、次の手順を実行します。

a) [Site Tag Name] フィールドに、サイトタグ名を入力します。

最大 32 文字の英数字、特殊文字、およびスペースを入力できます。Catalyst Center はサイトタグ名で次の文字をサポートしています。

- ASCII 文字：32 ～ 126
- 特殊文字：! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~

Catalyst Center はサイトタグ名では <、/、'.*'、? および先頭または末尾のスペースをサポートしていません。

b) [AP Profile] ドロップダウンリストから、AP プロファイルを選択します。

AP プロファイルを作成するには、[Create New] をクリックします。詳細については、AP プロファイル（501 ページ）を参照してください。

c) [負荷（Load）] フィールドに、サイトタグの負荷値を入力します。有効な範囲は 0 ～ 1000 です。

負荷値は、アクセスポイント数に基づいて設定できます。値を設定すると、再プロビジョニング中に新しい負荷設定がワイヤレスコントローラにプッシュされます。これらの設定は、アクセスポイントが切断されて再接続された後、またはワイヤレスコントローラを再起動した後にのみ有効になります。負荷値を設定しない場合、ワイヤレスコントローラの既存の負荷設定は変更されません。

d) [Flex Profile Name] フィールドに、Flex プロファイル名を入力します。

（注） [Flex Profile Name] フィールドを有効にするには、[SSID] タブで、[Flex Connect Local Switching] チェックボックスをオンにします。詳細については、ネットワークプロファイルへの SSID の追加 （544 ページ）を参照してください。

Catalyst Center の自動生成された名前を使用するには、[Auto generate Flex Profile Name] チェックボックスをオンにします。

e) [Select Sites] エリアで、名前を入力してサイトを検索するか、[Global] を展開してサイトを選択します。

1 つのエリアの下で複数のエリアを選択できます。

f) [Save] をクリックします。

ステップ 5 （任意） ネットワークプロファイルでポリシータグを作成するには、[Policy Tag] を展開し、[Create Policy Tag] をクリックします。

[Create Policy Tag] スライドインペインで、次の手順を実行します。

a) [Policy Tag Name] フィールドに、ポリシータグ名を入力します。

最大 31 文字の英数字、特殊文字、およびスペースを入力できます。Catalyst Center はポリシータグ名で以下の文字をサポートしています。

- ASCII 文字：32 ～ 126
- 特殊文字：! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~

Catalyst Center はポリシータグ名では <、/、'.*'、? や、先頭または末尾のスペースをサポートしていません。

b) [AP Zone] ドロップダウンリストから、AP ゾーンを選択します。



（注） このドロップダウンリストは、[AP Zones] タブでネットワークプロファイルに AP ゾーンを追加した場合に有効になります。詳細については、ネットワークプロファイルへの AP ゾーンの追加 （547 ページ）を参照してください。

c) [Select Sites] エリアで、名前を入力してサイトを検索するか、[Global] を展開してサイトを選択します。
d) [Save] をクリックします。

次のタスク

ネットワークプロファイルのその他の必要な設定を構成します。詳細については、ワイヤレス用のネットワークプロファイルの作成 （543 ページ）を参照してください。

ネットワークプロファイルの追加インターフェイスの構成

シスコ ワイヤレス コントローラに加わったインターフェイスで WLAN を VLAN またはサブネットにマッピングできます。ワイヤレス用のネットワークプロファイルのインターフェイスの詳細を構成できます。

手順

ステップ 1 [Add a Network Profile] ウィンドウ（**[Design]** > **[Network Profiles]** > **[Add Profile]** > **[Wireless]**）で、カーソルを [Advanced Settings] の上に置き、[Additional Interface] をクリックします。

ステップ 2 追加のインターフェイスを作成するには、[Create New Interface] をクリックして、次の手順を実行します。

a) [Add Interface] スライドインペインの [Interface Name] フィールドに、インターフェイスの名前を入力します。
b) [VLAN ID] フィールドに、VLAN ID を入力します。

Cisco AireOS ワイヤレスコントローラ の場合、有効な範囲は 1 ～ 4094 です。Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の場合、有効な範囲は 2 ～ 4094 です。

c) [Save] をクリックします。

または、**[Design]** > **[Network Settings]** > **[Wireless]** > **[Interfaces & VLAN Groups]** > **[Interfaces]**ウィンドウで追加のインターフェイスを作成できます。詳細については、ワイヤレスインターフェイスの作成 （449 ページ）を参照してください。

ステップ 3 ネットワークプロファイルにインターフェイスを追加するには、次のいずれかのタスクを実行します。

- 必要な追加インターフェイスの横にあるプラスアイコンをクリックします。
- 追加のインターフェイス名をクリックし、[Add Selected] をクリックします。



（注） 追加のインターフェイスを複数選択するには、Shift キーを押して追加したいインターフェイス名をクリックし、[Add Selected] をクリックします。

- インターフェイスをすべて追加するには、[Add All] をクリックします。 追加したインターフェイスをフィルタリングするには[Search] フィールドを使用します。

次のタスク

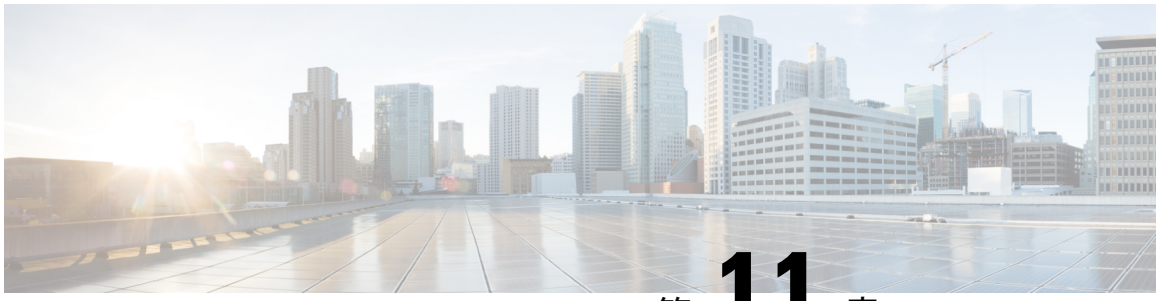
ネットワークプロファイルに必要な設定を入力後、[Save] をクリックします。詳細については、ワイヤレス用のネットワークプロファイルの作成 （543 ページ）を参照してください。



第 IV 部

ネットワークデバイスの設定と保守

- デバイス設定の変更を自動化するテンプレートの作成 （571 ページ）
- 機能テンプレートの設計 （603 ページ）
- ソフトウェア イメージの管理 （631 ページ）
- ネットワークデバイスのコンプライアンス監査 （665 ページ）
- デバイスの診断コマンドを実行 （691 ページ）



第 11 章

デバイス設定の変更を自動化するテンプレートの作成

- CLI テンプレートについて （571 ページ）
- オンボーディング テンプレートまたは Day-0 テンプレート （573 ページ）
- Day-n テンプレートを使用したネットワークデバイスへの設定の展開 （574 ページ）
- プロジェクトの作成 （575 ページ）
- テンプレートの作成 （575 ページ）
- テンプレートのエクスポート （582 ページ）
- テンプレートのインポート （583 ページ）
- テンプレートの複製 （584 ページ）
- ネットワークプロファイルへの CLI テンプレートの関連付け （585 ページ）
- CLI テンプレートのプロビジョニング （586 ページ）
- プロジェクトのエクスポート （587 ページ）
- プロジェクトのインポート （587 ページ）
- テンプレート変数 （588 ページ）
- テンプレートのネットワークプロファイルへの関連付け （596 ページ）
- CLI テンプレートの競合の検出 （598 ページ）

CLI テンプレートについて

Catalyst Center**CLI Templates** ウィンドウには、CLI テンプレートを作成するためのインタラクティブなウィンドウがあります。パラメータ化された要素または変数を使用して、事前に定義された設定で簡単にテンプレートを設計できます。テンプレートを作成したら、そのテンプレートを使用して、ネットワーク内の任意の場所に設定されている 1 つ以上のサイトにデバイスを展開できます。

CLI テンプレートを使用すると、次のことができます。

- 使用可能なテンプレートのリストを表示する。
- テンプレートを作成、編集、複製、インポート、エクスポート、削除する。

- [Project Name]、[Template Type]、[Template Language]、[Category]、[Device Family]、[Device Series]、[Commit State]、[Provision Status] に基づいてテンプレートをフィルタ処理する。
- [Design] > [CLI Templates] ウィンドウの [Template] テーブルで、次のテンプレート属性を確認する。
  - [Name]：CLI テンプレートの名前。
  - [Project]：CLI テンプレートが作成されるプロジェクト。
  - [Type]：CLI テンプレートのタイプ（通常または複合）。
  - [Version]：CLI テンプレートのバージョン数。
  - [Commit State]：コミットされたテンプレートの最新バージョン。[Commit State] 列には次の情報が表示されます。
    - 最後にコミットされた日付のタイムスタンプ。
    - 警告アイコンは、テンプレートが変更されたもののコミットされていないことを意味します。
    - チェックアイコンは、テンプレートの最新バージョンがコミットされていることを意味します。

（注） デバイスにテンプレートをプロビジョニングするには、最新バージョンをコミットする必要があります。

  - [Provision Status]：[Provision Status] 列には次の情報が表示されます。
    - テンプレートがプロビジョニングされているデバイスの数。
    - チェックアイコンには、CLI テンプレートが失敗せずにプロビジョニングされたデバイスの数が表示されます。
    - 警告アイコンには、CLI テンプレートの最新バージョンがまだプロビジョニングされていないデバイスの数が表示されます。
    - 十字アイコンには、CLI テンプレートの展開に失敗したデバイスの数が表示されます。
  - [Potential Design Conflicts]：CLI テンプレートの潜在的な競合が表示されます。
  - [Network Profiles]：CLI テンプレートが関連付けられているネットワークプロファイルの数が表示されます。[Network Profiles] 列の [Attach] をクリックして、ネットワークプロファイルに CLI テンプレートを関連付けます。
  - [Actions]：[Actions] 列の省略記号アイコン ⋮ にカーソルを合わせて、テンプレートを複製、コミット、削除、編集したり、プロジェクトを編集したり、ネットワークプロファイルにテンプレートを関連付けたりします。

- インタラクティブコマンドを追加する。
- CLI コマンドを自動保存する。
- 追跡のためにテンプレートのバージョンを管理する。

  [CLI Templates] ウィンドウで、テンプレート名、[Template History] タブの順にクリックしてテンプレートのバージョンを表示します。
- テンプレートのエラーを検出する。
- テンプレートのシミュレーションを行う。
- 変数を定義する。
- ランタイム競合を検出する。



（注）
- Catalyst Centerによってプッシュされるネットワークインテント設定がテンプレートによって上書きされないようにしてください。
- IP MACvバインディングなどの設定には機能テンプレート（インテントベース）を使用します。

オンボーディング テンプレートまたは Day-0 テンプレート

Catalyst Centerのオンボーディングテンプレートは、ネットワークデバイスでの初期プロビジョニングおよびオンボーディングプロセスを自動化するために使用されます。オンボーディングテンプレートでは、オンボーディングプロセス中にデバイスに適用する必要がある設定を定義します。

オンボーディングテンプレートは、主にプラグアンドプレイ（PnP）で使用され、ネットワーク内の新しいネットワークデバイスの展開を合理化します。

たとえば、ネットワークに展開する新しい一連のスイッチがあるとします。オンボーディングテンプレートを使用すると、オンボーディングプロセス中にそれらのスイッチに適用する必要があるインターフェイス設定、VLAN割り当て、基本的なセキュリティ設定などの初期設定を定義できます。新しいスイッチをネットワークに接続すると、Catalyst Center は PnP を使用してスイッチを自動的に検出し、オンボーディングテンプレートから定義済みの設定を適用するため、ネットワーク全体で一貫性のある標準化された設定が保証されます。

（注）

- Day-0 テンプレートは PnP の一部としてプッシュされます。
- Day-0 テンプレートでは、ソース変数やシステム変数をバインドできません。つまり、Day-0テンプレートには、編集中に、または入力フォーム機能拡張（DHCP サーバー、DNS サーバー、syslog サーバーなど）から、ソースオブジェクト値を使用して変数をバインドまたは使用するオプションがありません。
- Day-0 テンプレートでは、特別なキーワード （593 ページ）で説明されている特別なキーワードの使用がサポートされていません。
- Day-0テンプレートでは、誤った行を含む設定全体がそのままプッシュされるため、Day-0テンプレートで正しい設定を使用していることを確認することを推奨します。

Day-n テンプレートを使用したネットワークデバイスへの設定の展開

デバイスがインベントリに追加された後、Day-n テンプレートを使用して、ネットワークデバイスに設定を適用できます。Catalyst Center の Day-n テンプレートは、ネットワークデバイス全体の設定管理および一貫性を確保するために使用されます。

Day-n テンプレートは、設定変更、ファームウェア更新のプッシュ、またはネットワーク全体のポリシー変更を複数のデバイスに同時に展開するプロセスを簡素化するように設計されています。Day-n テンプレートは、1 つ以上のデバイスに適用する特定の設定状態や変更をキャプチャします。Catalyst Centerのインテント設定を使用しても完了できない設定については、day-n テンプレートを使用できます。

Day-nテンプレートは、ネットワークプロファイルへのCLIテンプレートの関連付け （585 ページ）で説明されているように、ネットワークプロファイルに関連付けられます。テンプレートは、デバイスのプロビジョニング中にデバイスに適用されます。デバイスは複数回プロビジョニングできます。デフォルトでは、新しい設定のみが再プロビジョニング中にプッシュされますが、設定はオーバーライドできます。

たとえば、ネットワーク内のスイッチグループに新しいアクセス制御リスト（ACL）を展開して、セキュリティポリシーを適用する場合、Day-nテンプレートを使用すると、ACL設定を定義して対象のスイッチに適用できます。Catalyst Center によって設定がデバイスにプッシュされ、ネットワーク全体で ACL の一貫した適用が保証されます。将来的に ACL を更新する必要がある場合は、Day-n テンプレートに変更を加えることができます。変更は Catalyst Center によって適宜デバイスにプッシュされます。

（注）

- Day-n テンプレートはコンパイルされて Catalyst Center に保存されますが、その設定は複数の同時 SSH セッションを介してインベントリ内のデバイスに配信されるため、コマンドは 1 行ずつデバイスに送信されます。
- Day-n テンプレートに誤った設定が含まれている場合、誤った行がデバイスにプッシュされて失敗すると、Catalyst Center によるテンプレートの残り部分の適用が停止します。

プロジェクトの作成

手順

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

ステップ 2 [Add] をクリックし、[New Project] を選択します。

[新規プロジェクトの追加（Add New Project）] スライドインペインが表示されます。

ステップ 3 [Project Name] フィールドに一意の名前を入力します。

ステップ 4 （任意） [Project Description] フィールドにプロジェクトの説明を入力します。

ステップ 5 [Continue] をクリックします。

プロジェクトが作成され、左側のペインに表示されます。

次のタスク

プロジェクトに新しいテンプレートを追加します。詳細については、標準テンプレートの作成（576 ページ）およびコンポジットテンプレートの作成 （579 ページ）を参照してください。

テンプレートの作成

テンプレートは、パラメータ要素と変数を使用して設定を簡単に事前定義する方法を提供します。テンプレートにより、管理者は複数のネットワークデバイスを一貫して設定するのに使用する CLI コマンドの設定を定義できるようになり、展開時間を短縮できます。テンプレートの変数を使用すると、デバイスごとに特定の設定をカスタマイズできます。

標準テンプレートの作成

手順

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

（注） デフォルトでは、[Onboarding Configuration] プロジェクトは、day-0 テンプレートの作成に使用できます。独自のカスタムプロジェクトを作成できます。カスタムプロジェクトで作成されたテンプレートは、day-*n* テンプレートとして分類されます。

ステップ 2 左側のペインで、[Project Name] をクリックし、テンプレートを作成するプロジェクトを選択します。

ステップ 3 [Add] をクリックし、ドロップダウンリストから [New Template] を選択します。

（注） day-0 用に作成したテンプレートは、day-*n* にも適用できます。

ステップ 4 [Add New Template] スライドインペインで、標準テンプレートの設定を指定します。

[Template Details] エリアで、次の手順を実行します。

1. [Template Name] フィールドに一意の名前を入力します。
2. ドロップダウンリストから [Project Name] を選択します。
3. [Template Type]：[Regular Template] をクリックします。
4. [Template Language]：テンプレートの内容に使用する言語（[Velocity] または [Jinja]）を選択します。
   - [Velocity]：Velocity Template Language（VTL）を使用します。詳細については、http://velocity.apache.org/engine/devel/vtl-reference.htmlを参照してください。

     Velocity テンプレートフレームワークでは、数字で始まる変数の使用が制限されます。変数名の先頭は数字ではなく文字にしてください。

     （注） Velocity テンプレートの使用中は、ドル記号（$）を使用しないでください。ドル記号（$）を使用すると、その後ろの値は変数として扱われます。たとえば、パスワードを「$a123$q1ups$va112」として設定すると、CLI テンプレートハブでは、変数「a123」、「q1ups」、および「va112」として処理されます。この問題を回避するために、Velocity テンプレートによるテキスト処理に合わせて Linux シェルスタイルを使用してください。

- [Jinja]：Jinja 言語を使用します。詳細については、https://palletsprojects.com/projects/jinja/ を参照してください。

5. ドロップダウンリストから [Software Type] を選択します。



（注） ソフトウェアタイプに固有のコマンドがある場合は、特定のソフトウェアタイプ（IOS XE や IOS XR など）を選択できます。ソフトウェアタイプに IOS を選択すると、IOS XE や IOS XR など、すべてのソフトウェアタイプにコマンドを適用できます。この値は、プロビジョニング時に、選択したデバイスがテンプレートの選択に準拠しているかどうかを確認するために使用されます。

[Device Type Details] エリアで、次の手順を実行します。

1. [Add Device Details] リンクをクリックします。
2. ドロップダウンリストから [Device Family] を選択します。
3. 次のいずれかを実行して、デバイスシリーズまたはデバイスモデルを選択します。
   - [Device Series] タブをクリックし、優先するデバイスシリーズの横にあるチェックボックスをオンにします。
   - [Device Models] タブをクリックし、優先するデバイスモデルの横にあるチェックボックスをオンにします。
4. [Add] をクリックします。

[Additional Details] エリアで、次の手順を実行します。

1. ドロップダウンリストから [Device Tags] を選択します。



（注） タグはキーワードのようなもので、テンプレートを見つけるのに役立ちます。

タグを使用してテンプレートをフィルタ処理する場合は、テンプレートを適用するデバイスに同じタグを適用する必要があります。そうしないと、プロビジョニング中に次のエラーが発生します。

```
Cannot select the device. Not compatible with template
```

2. [Software Version] フィールドに、ソフトウェアバージョンを入力します。



（注） プロビジョニングの間、Catalyst Center は、選択したデバイスにテンプレートに記載されているのと同じソフトウェアバージョンがあるか確認します。不一致がある場合、テンプレートはプロビジョニングされません。

3. [Template Description] にテンプレートの説明を入力します。

ステップ 5 [Continue] をクリックします。

CLI テンプレートが作成されます。



（注） コンプライアンスの問題を最小限に抑えるためにCLIテンプレートで使用する必要があるベストプラクティスの一部を表示するには、[Template] ウィンドウの右上隅にある [CLI Template Best Practices] リンクをクリックします。

ステップ 6 テンプレートの内容を編集するには、作成したテンプレートを選択し、[Actions] の省略記号をクリックして [Edit Template] を選択します。詳細については、テンプレートの編集 （581 ページ）を参照してください。

ブロックリストコマンド

ブロックリストコマンドは、テンプレートに追加できないコマンド、またはテンプレートを介してプロビジョニングできないコマンドです。テンプレートでブラックリストコマンドを使用すると、テンプレートに警告が表示されます。この場合、一部の Catalyst Center プロビジョニング アプリケーションと競合している可能性があります。

このリリースでは、次のコマンドがブロックされます。

- **router lisp**
- **hostname**：このコマンドは、ルータに対してのみブロックされます。

サンプルテンプレート

テンプレートの変数を作成する際は、次のスイッチのサンプルテンプレートを参照してください。

SNMP コミュニティの設定

```
snmp-server community $snmp_community_name RO
```

インターフェイスの設定

```
interface $interfaceName
description $description
```

シスコ ワイヤレス コントローラでの NTP の設定

```
config time ntp interval $interval
```

コンポジットテンプレートの作成

2つ以上の標準テンプレートは、連続した複合テンプレートにまとめられます。一連のテンプレートに対し、デバイスに集合的に適用される連続的な複合テンプレートを作成できます。たとえば、ブランチを展開するときに、ブランチルータの最小設定を指定する必要があります。作成したすべてのテンプレートは、単一の複合テンプレートに追加できます。これは、ブランチルータに必要なすべての個々のテンプレートを集約したものです。複合テンプレートに含まれるテンプレートが、デバイスに展開される順序を指定してください。

（注） 複合テンプレートには、コミットされたテンプレートのみを追加できます。

手順

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

ステップ 2 左側のペインで、[Project Name] をクリックし、テンプレートを作成するプロジェクトを選択します。

ステップ 3 ウィンドウの右上にある [Add] をクリックし、ドロップダウンリストから [New Template] を選択します。

[Add New Template] スライドインペインが表示されます。

ステップ 4 [Add New Template] スライドインペインで、複合テンプレートの設定を指定します。

[Template Details] エリアで、次の手順を実行します。

a) [Template Name] フィールドに一意の名前を入力します。
b) ドロップダウンリストから [Project Name] を選択します。
c) [Template Type]：[Composite Sequence] オプションボタンを選択します。
d) ドロップダウンリストから [Software Type] を選択します。

（注） ソフトウェアタイプに固有のコマンドがある場合は、特定のソフトウェアタイプ（IOS XE や IOS XR など）を選択できます。ソフトウェアタイプに IOS を選択すると、IOS XE や IOS XR など、すべてのソフトウェアタイプにコマンドを適用できます。この値は、プロビジョニング時に、選択したデバイスがテンプレートの選択に準拠しているかどうかを確認するために使用されます。

[Device Type Details] エリアで、次の手順を実行します。

1. [Add Device Details] リンクをクリックします。
2. ドロップダウンリストから [Device Family] を選択します。
3. 次のいずれかを実行して、デバイスシリーズまたはデバイスモデルを選択します。

- [Device Series] タブをクリックし、優先するデバイスシリーズの横にあるチェックボックスをオンにします。
- [Device Models] タブをクリックし、優先するデバイスモデルの横にあるチェックボックスをオンにします。

4. [Add] をクリックします。

[Additional Details] エリアで、次の手順を実行します。

1. ドロップダウンリストから [Device Tags] を選択します。



（注） タグはキーワードのようなもので、テンプレートを見つけるのに役立ちます。

タグを使用してテンプレートをフィルタ処理する場合は、テンプレートを適用するデバイスに同じタグを適用する必要があります。そうしないと、プロビジョニング中に次のエラーが発生します。

```
Cannot select the device. Not compatible with template
```

2. [Software Version] フィールドに、ソフトウェアバージョンを入力します。



（注） プロビジョニングの間、Catalyst Center は、選択したデバイスにテンプレートに記載されているのと同じソフトウェアバージョンがあるか確認します。不一致がある場合、テンプレートはプロビジョニングされません。

3. [Template Description] を入入力します。

ステップ 5 [Continue] をクリックします。
[Composite Template] ウィンドウが表示され、適用可能なテンプレートのリストが表示されます。

ステップ 6 [Add Templates] リンクをクリックしてから + をクリックしてテンプレートを追加し、[Done] をクリックします。
複合テンプレートが作成されます。



（注） コンプライアンスの問題を最小限に抑えるためにCLIテンプレートで使用する必要があるベストプラクティスの一部を表示するには、[Template] ウィンドウの右上隅にある [CLI Template Best Practices] リンクをクリックします。

ステップ 7 作成した複合テンプレートの横にあるチェックボックスをオンにして [Actions] 列の省略記号をクリックし、[Commit] を選択してテンプレートのコンテンツをコミットします。

テンプレートの編集

テンプレートを作成したら、テンプレートを編集して内容を記述できます。

手順

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

ステップ 2 左側のペインで、[Project Name] を選択してから編集するテンプレートを選択します。

選択したテンプレートが表示されます。

（注） コンプライアンスの問題を最小限に抑えるためにCLIテンプレートで使用する必要があるベストプラクティスの一部を表示するには、[Template] ウィンドウの右上隅にある [CLI Template Best Practices] リンクをクリックします。

ステップ 3 テンプレートの内容を入力します。単一行設定または複数選択設定を含むテンプレートを使用できます。

ステップ 4 ウィンドウ上部のテンプレート名の横にある [Properties] をクリックし、[Template Details]、[Device Details]、および [Additional Details] を編集します。それぞれのエリアの横にある [Edit] をクリックします。

ステップ 5 テンプレートは自動保存されます。[Auto Saved] の横にある時間の繰り返しをクリックすることにより、自動保存の時間間隔を変更することもできます。

ステップ 6 [Template History] をクリックし、テンプレートのバージョンを表示します。また、[Compare] をクリックし、テンプレートのバージョンの違いを表示することもできます。

ステップ 7 [Variables] タブをクリックし、CLI テンプレートの変数を表示します。

ステップ 8 [Show Design Conflicts] トグルボタンをクリックし、テンプレートの潜在的なエラーを表示します。

Catalyst Center では、潜在的なエラーとランタイムエラーを表示できます。詳細については、CLI テンプレートとサービス プロビジョニング インテント間の潜在的な設計競合の検出 （598 ページ）およびCLI テンプレートのランタイム競合の検出 （599 ページ）を参照してください。

ステップ 9 ウィンドウの下部にある [Save] をクリックします。

テンプレートを保存後、Catalyst Center がテンプレート内のすべてのエラーをチェックします。構文エラーがある場合、テンプレートの内容は保存されず、テンプレートで定義されているすべての入力変数が保存プロセス中に自動的に識別されます。ローカルの値（ループ用に使用され、セットを通じて割り当てられる変数など）は無視されます。

ステップ 10 [Commit] をクリックし、テンプレートをコミットします。

（注） ネットワーク プロファイルにコミットされたテンプレートのみを関連付けることができます。

ステップ 11 [Attach to Network Profile] リンクをクリックし、作成したテンプレートをネットワークプロファイルに関連付けます。

テンプレートのシミュレーション

インタラクティブ テンプレート シミュレーションを使用すると、変数にテストデータを指定することで、変数をデバイスに送信する前に、テンプレートのCLI生成をシミュレーションすることができます。テストシミュレーションの結果を保存し、必要に応じてそれらを後で使用することができます。

手順

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

ステップ 2 左側のペインで、プロジェクトを選択し、シミュレーションを実行するテンプレートをクリックします。

テンプレートが表示されます。

ステップ 3 [Simulation] タブをクリックします。

ステップ 4 [Create Simulation] をクリックします。

[シミュレーションの作成（Create Simulation）] スライドインペインが表示されます。

ステップ 5 [Simulation Name] フィールドに一意の名前を入力します。

（注） テンプレートに暗黙的な変数がある場合は、[Device] ドロップダウンリストからデバイスを選択し、バインディングに基づいて実際のデバイスに対してシミュレーションを実行します。

ステップ 6 [Import Template Parameters] をクリックしてテンプレートパラメータをインポートするか、[Export Template Parameters] をクリックしてテンプレートパラメータをエクスポートします。

ステップ 7 最後のデバイスプロビジョニングの変数を使用するには、[Use Variable Values from the Last Provisioning] リンクをクリックします。新しい変数は手動で追加する必要があります。

ステップ 8 リンクをクリックして変数の値を選択し、[Run] をクリックします。

テンプレートのエクスポート

テンプレートまたは複数のテンプレートを JSON フォーマットで 1 つのファイルにエクスポートできます。

手順

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

ステップ 2 テンプレート名の横にある 1 つか複数のチェックボックスをオンにして、エクスポートする 1 つか複数のテンプレートを選択します。

ステップ 3 [Export] ドロップダウンリストから、[Export Template] を選択します。

ステップ 4 （任意） 左側のペインのカテゴリに基づいてテンプレートをフィルタ処理できます。

ステップ 5 テンプレートの最新バージョンがエクスポートされます。

テンプレートの以前のバージョンをエクスポートするには、次の手順を実行します。

1. テンプレート名をクリックしてテンプレートを開きます。
2. [Template History] タブをクリックします。

   [テンプレート履歴（Template History）] スライドインペインが表示されます。
3. エクスポートしたいバージョンを選択します。
4. バージョンの下の [View] ボタンをクリックします。

   そのバージョンの CLI テンプレートが表示されます。
5. テンプレートの上部にある [Export] をクリックします。

JSON 形式のテンプレートがエクスポートされます。

テンプレートのインポート

プロジェクトの下に 1 つまたは複数のテンプレートをインポートできます。



（注） Catalyst Center の古いバージョンから新しいバージョンにのみテンプレートをインポートできます。その逆は、許可されません。

手順

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

ステップ 2 左側のペインの [Project Name] で、テンプレートをインポートするプロジェクトを選択してから、**[Import]** > **[Import Template]** の順に選択します。

ステップ 3 [テンプレートのインポート（Import Templates）] スライドインペインが表示されます。

1. ドロップダウンリストから [Project Name] を選択します。
2. 次のアクションのいずれかを実行して、JSON ファイルをアップロードします。
   1. ドラッグ アンド ドロップ エリアにファイルをドラッグ アンド ドロップします。
   2. [Choose a file] をクリックし、JSON ファイルの保存場所を参照して [Open] をクリックします。

   ファイルサイズは 10Mb を超えないようにしてください。
3. 階層内に同じ名前のテンプレートがすでに存在する場合は、チェックボックスをオンにして、インポートするテンプレートの新しいバージョンを作成します。
4. [Import] をクリックします。

これで選択したプロジェクトに CLI テンプレートが正常にインポートされます。

テンプレートの複製

テンプレートのコピーを作成して、その一部を再利用することができます。

手順

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

ステップ 2 [Action] 列の省略記号をクリックし、[Clone] を選択します。

ステップ 3 [テンプレートの複製（Clone Template）] スライドインペインが表示されます。

次の手順を実行します。

1. [Template Name] フィールドに一意の名前を入力します。
2. ドロップダウンリストから [Project Name] を選択します。

ステップ 4 [Clone] をクリックします。

テンプレートの最新バージョンが複製されます。

ステップ 5 （任意）または、テンプレート名をクリックしてテンプレートを複製することもできます。テンプレートが表示されます。テンプレートの上の [Clone] をクリックします。

ステップ 6 テンプレートの以前のバージョンを複製するには、次の手順を実行します。

1. テンプレート名をクリックしてテンプレートを選択します。
2. [Template History] タブをクリックします。

   [テンプレート履歴（Template History）] スライドインペインが表示されます。
3. 複製したいバージョンをクリックします。

選択した CLI テンプレートが表示されます。

4. テンプレートの上の [Clone] をクリックします。

ネットワークプロファイルへの CLI テンプレートの関連付け

CLIテンプレートをプロビジョニングするには、ネットワークプロファイルに関連付ける必要があります。この手順を使用して、CLI テンプレートを 1 つか複数のネットワークプロファイルに関連付けます。

手順

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

[CLI Templates] ウィンドウが表示されます。

ステップ 2 [Templates] テーブルで、[Network Profile] 列の [Attach] をクリックしてネットワークプロファイルにテンプレートを関連付けます。

（注） または、[Actions] 列の省略記号 ⋮ をクリックして [Attach to Profile] を選択するか、[Design] > [Network Profiles] ウィンドウからネットワークプロファイルにテンプレートを関連付けられます。詳細については、テンプレートのネットワークプロファイルへの関連付け （596 ページ）を参照してください。

[Attach to Network Profile] スライドインペインが表示されます。

ステップ 3 ネットワークプロファイル名の横のチェックボックスをオンにし、[Save] をクリックします。
選択したネットワークプロファイルに CLI テンプレートが関連付けられます。

ステップ 4 [Network Profile] 列に表示される数字は、CLI テンプレートが関連付けられているネットワークプロファイルの数を示します。この数字をクリックすると、ネットワークプロファイルの詳細が表示されます。

ステップ 5 CLI テンプレートに複数のネットワークプロファイルを関連付けるには、次の手順を実行します。

1. [Network Profile] 列の数字をクリックします。

   または、[Actions] 列の省略記号アイコン ⋮ をクリックし、[Attach to Profile] を選択します。

   [Network Profiles] スライドインペインが表示されます。

2. スライドインペインの右上にある [Attach to Network Profile] リンクをクリックし、ネットワークプロファイル名の横のチェックボックスをオンにして、[Attach] をクリックします。

CLI テンプレートのプロビジョニング

手順

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

ステップ 2 プロビジョニングするテンプレートの横にあるチェックボックスをオンにして、テーブルの上部にある [Provision Templates] をクリックします。

複数のテンプレートをプロビジョニングできます。

[Provision Template] のワークフローにリダイレクトされます。

ステップ 3 [Get Started] ウィンドウで、[Task Name] フィールドに一意の名前を入力します。

ステップ 4 [Select Devices] ウィンドウで、該当するデバイスリストから、テンプレートで定義されているデバイスの詳細に基づくデバイスを選択します。[Next] をクリックします。

ステップ 5 [Review Applicable Templates] ウィンドウで、デバイスと、関連付けられているテンプレートを確認します。必要に応じて、デバイスにプロビジョニングしないテンプレートを削除できます。

ステップ 6 [Configure Template Variables] ウィンドウで、各デバイスのテンプレートの変数を設定します。

ステップ 7 [Preview Configuration] ウィンドウで、デバイスでプロビジョニングされている設定をプレビューするデバイスを選択します。

ステップ 8 展開のためのタスクのスケジュールを設定します。

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

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

ステップ 9 [Tasks] ウィンドウで、タスクの展開を監視します。

テンプレートのプロビジョニングが失敗した場合、Catalyst Center ではテンプレートのプロビジョニングが失敗する前にプッシュされたコマンドのロールバックは試行されません。

プロジェクトのエクスポート

プロジェクトまたは複数のプロジェクト (テンプレートを含む) を JSON フォーマットの 1 つのファイルにエクスポートできます。

手順

ステップ 1 メインメニューから次を選択します。**[Design]** > **[CLI Templates]** の順に選択します。
ステップ 2 左側のペインの [Project Name] で、エクスポートする 1 つか複数のプロジェクトを選択します。
ステップ 3 [Export] ドロップダウンリストから、[Export Project] を選択します。
ステップ 4 プロンプトが表示されたら、[Save] をクリックします。

プロジェクトのインポート

テンプレートを使用して、1 つまたは複数のプロジェクトを Catalyst Center CLI テンプレートにインポートできます。

（注） Catalyst Center の古いバージョンから新しいバージョンにのみプロジェクトをインポートできます。その逆は、許可されません。

手順

ステップ 1 メインメニューから次を選択します。**[Design]** > **[CLI Templates]** の順に選択します。
ステップ 2 [Import] ドロップダウンリストから、[Import Project] を選択します。
ステップ 3 [プロジェクトのインポート（Import Projects）] スライドインペインが表示されます。

1. 次のアクションのいずれかを実行して、JSON ファイルをアップロードします。
   1. ドラッグ アンド ドロップ エリアにファイルをドラッグ アンド ドロップします。
   2. [Choose a file] をクリックし、JSON ファイルの保存場所を参照して [Open] をクリックします。

   ファイルサイズは 10Mb を超えないようにしてください。
2. 階層内に同じ名前のプロジェクトがすでに存在する場合は、チェックボックスをオンにして、既存のプロジェクトで新しいバージョンのテンプレートを作成します。
3. [Import] をクリックします。

これでプロジェクトが正常にインポートされます。

テンプレート変数

テンプレート変数は、追加のメタデータ情報をテンプレート内に追加するために使用します。また変数を使用して、最大長や範囲などの変数の検証を行うこともできます。

手順

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

ステップ 2 左側のペインからプロジェクトを選択し、テンプレートをクリックします。

テンプレートが表示されます。

ステップ 3 [Variables] タブをクリックします。

テンプレート変数にメタデータを追加できます。テンプレートで特定されたすべての変数が表示されます。以下のメタデータを設定できます。

- 文字列を変数と見なさない場合は、左側のペインから変数を選択し、[Variable] トグルボタンをクリックします。

  （注） デフォルトでは、文字列は変数と見なされます。文字列を変数と見なしたくない場合は、トグルボタンをクリックします。

- これがプロビジョニング中に必要な変数の場合は、[Required Variable] チェックボックスをオンにします。デフォルトでは、すべての変数に [必須（Required）] マークが付いています。これはつまり、プロビジョニング時にこの変数の値を入力する必要があることを意味します。パラメータに [Required Variable] マークがなく、このパラメータに何も値を渡さない場合は、実行時に空の文字列に置換されます。変数の不足は、コマンドの失敗につながります。また、構文上正しくない可能性があります。[Required Variable] マークが付いていない変数に基づいてコマンド全体をオプションにしたい場合は、テンプレートで **if-else** ブロックを使用します。

- [Field Name] にフィールド名を入力します。これは、プロビジョニング中に各変数の UI ウィジェットに使用されるラベルです。

- [Variable Data Value] エリアで、オプションボタンをクリックして [Variable Data Source] を選択します。[ユーザー定義（User Defined）] の値か [ソースにバインド（Bound to Source）] の値を選択して、特定の値を保持します。

  [ユーザー定義（User Defined）] の値を選択した場合は、次の手順を実行します。

1. ドロップダウンリストから、[Variable Type]（[String]、[Integer]、[IP Address]、または [Mac Address]）を選択します。
2. ドロップダウンリストから [Data Entry Type]（[Text Field]、[Single Select]、または [Multi Select]）を選択します。
3. [Default Variable Value] フィールドにデフォルト変数値を入力します。
4. 機密値の場合は、[Sensitive Value] チェックボックスをオンにします。
5. [Maximum Characters] フィールドに、入力できる最大文字数を入力します。これは文字列データタイプの場合にのみ適用可能です。
6. [Hint Text] フィールドにヒントテキストを入力します。
7. 詳細情報がある場合は [Additional Info] テキストボックスに入力ます。

[ソースにバインド（Bound to Source）] の値を選択した場合は、次の手順を実行します。

1. ドロップダウンリストから [Data Entry Type]（[Text Field]、[Single Select]、または [Multi Select]）を選択します。
2. [ネットワークプロファイル（Network Profile）]、[共通設定（Common Settings）]、[クラウド接続（Cloud Connect）]、および [インベントリ（Inventory）] ドロップダウンリストから [ソース（Source）] を選択します。
3. ドロップダウンリストから [Entity] を選択します。
4. ドロップダウンリストから [Attribute] を選択します。
5. [Maximum Characters] フィールドに、入力できる最大文字数を入力します。これは文字列データタイプの場合にのみ適用可能です。
6. [Hint Text] フィールドにヒントテキストを入力します。
7. 詳細情報がある場合は [Additional Info] テキストボックスに入力ます。

   [Bound to Source] の値の詳細については、「変数バインド （589 ページ）」を参照してください。

ステップ 4 メタデータ情報を設定したら、[Review Form] をクリックして変数情報を確認します。

ステップ 5 [Save] をクリックします。

ステップ 6 テンプレートをコミットするには、[Commit] を選択します。**[コミット（Commit）]** ウィンドウが表示されます。[コミットメモ（Commit Note）] テキストボックスに、コミットのメモを入力することができます。

変数バインド

テンプレートを作成する場合、コンテキストに合わせて置き換わる変数を指定できます。それらの変数の多くは、**[Design]** > **[CLI Templates]** で使用できます。

CLI テンプレートには、編集中に、または入力フォーム機能拡張（DHCP サーバー、DNS サーバー、syslog サーバーなど）から、ソースオブジェクト値を使用してテンプレートで変数をバインドまたは使用するオプションがあります。

一部の変数については、対応するソースに常にバインドされ、動作を変更することはできません。暗黙的な変数のリストを表示するには、テンプレートをクリックしてから、[Variables] タブをクリックします。



（注） 変数バインドは、Day-0 テンプレートではサポートされておらず、Day-n テンプレートでのみサポートされています。

事前定義済みのオブジェクト値は、次のいずれかにすることができます。

- ネットワークプロファイル：
  - SSID
  - ポリシープロファイル
  - AP グループ
  - Flex グループ
  - Flex プロファイル
  - サイト タグ
  - ポリシー タグ
- 共通設定：
  - DHCP サーバ
  - Syslog サーバー
  - SNMP トラップ 受信機
  - NTP サーバ
  - タイムゾーンサイト
  - デバイスバナー
  - DNS サーバ
  - NetFlow コレクタ
  - AAA ネットワークサーバー
  - AAA エンドポイントサーバー
  - AAA サーバー PAN ネットワーク

- AAA サーバー PAN エンドポイント
- WLAN 情報
- RF プロファイル情報

- クラウド接続：
  - クラウド router-1 トンネル IP
  - クラウド router-2 トンネル IP
  - クラウド router-1 ループバック IP
  - クラウド router-2 ループバック IP
  - ブランチ router-1 トンネル IP
  - ブランチ router-2 トンネル IP
  - クラウド router-1 パブリック IP
  - クラウド router-2 パブリック IP
  - ブランチ router-1 IP
  - ブランチ router-2 IP
  - プライベート subnet-1 IP
  - プライベート subnet-2 IP
  - プライベート subnet-1 IP マスク
  - プライベート subnet-2 IP マスク
- インベントリ：
  - デバイス
  - Interface
  - AP グループ
  - Flex グループ
  - WLAN
  - ポリシープロファイル
  - Flex プロファイル
  - Web 認証パラメータマップ
  - サイト タグ
  - ポリシー タグ

- RF プロファイル

- [Common Settings]：**[Design]** > **[Network Settings]** > **[Network]** で利用可能な設定。共通設定の変数バインドによって、デバイスが属するサイトに基づいた値が解決されます。

手順

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

ステップ 2 テンプレートを選択し、[Variables] タブをクリックして、テンプレート内の変数をネットワーク設定にバインドします。

ステップ 3 変数をネットワーク設定にバインドするには、左側のペインで変数を選択し、[Required Variable] チェックボックスをオンにします。

ステップ 4 変数をネットワーク設定にバインドするには、左側のペインから各変数を選択し、[Variable Data Source] で [Bound to Source] オプションボタンをクリックします。次の手順を実行します。

1. [Data Entry Type] ドロップダウンリストから、プロビジョニング時に作成する UI ウィジェットのタイプ（[Text Field]、[Single Select]、または [Multi Select]）を選択します。
2. それぞれのドロップダウンリストで、[Source]、[Entity]、および [Attributes] を選択します。
3. ソースタイプが [CommonSettings] の場合は、[dhcp.server]、[syslog.server]、[snmp.trap.receiver]、[ntp.server]、[timezone.site]、[device.banner]、[dns.server]、[netflow.collector]、[aaa.network.server]、[aaa.endpoint.server]、[aaa.server.pan.network]、[aaa.server.pan.endpoint]、[wlan.info]、[rfprofile.info] いずれかのエンティティを選択します。

   [dns.server] または [netflow.collector] 属性にフィルタ処理を適用して、デバイスのプロビジョニング時に、[bind] 変数の関連リストのみを表示することができます。属性にフィルタ処理を適用するには、[Filter by] ドロップダウンリストから属性を選択します。[Condition] ドロップダウンリストから、[Value] と一致させるための条件を選択します。
4. ソースタイプが [NetworkProfile] の場合、エンティティタイプとして [SSID] を選択します。入力される SSID エンティティは、**[Design]** > **[Network Profile]** で定義されます。バインドにより、SSID 名、サイト、および SSID カテゴリの組み合わせであるわかりやすい SSID 名が生成されます。[Attributes] ドロップダウンリストから、[wlanid] か [wlanProfileName] を選択します。この属性は、テンプレートのプロビジョニング時の高度な CLI 設定中に使用されます。
5. ソースタイプが [Inventory] の場合は、[Device]、[Interface]、[AP Group]、[Flex Group]、[Wlan]、[Policy Profile]、[Flex Profile]、[Webauth Parameter Map]、[Site Tag]、[Policy Tag]、[RF Profile] いずれかのエンティティを選択します。エンティティタイプ [Device] および [Interface] の場合、[Attribute] ドロップダウンリストにデバイスまたはインターフェイスの属性が表示されます。変数は、テンプレートを適用するデバイスで設定されている AP グループと Flex グループの名前を解決します。

   [Device]、[Interface]、または [Wlan] 属性にフィルタ処理を適用して、デバイスのプロビジョニング時に、[bind] 変数の関連リストのみを表示することができます。属性にフィルタ処理を適用するには、[Filter by] ドロップダウンリストから属性を選択します。[Condition] ドロップダウンリストから、[Value] と一致させるための条件を選択します。

変数を共通設定にバインドしたら、テンプレートをワイヤレスプロファイルに割り当て、テンプレートをプロビジョニングするときに、**[Network Settings]** > **[Network]** の下で定義したすべてのネットワーク設定がドロップダウンリストに表示されます。これらの属性は、ネットワークの設計時に **[Network Settings]** > **[Network]** の下で定義する必要があります。

ステップ 5 テンプレートに特定の属性にバインドする変数バインドが含まれており、テンプレートコードがそれらの属性に直接アクセスする場合は、次のいずれかのタスクを実行する必要があります。

- 属性へのバインディングではなくオブジェクトへのバインディングを変更します。
- テンプレートコードを更新して、属性に直接アクセスしないようにします。

たとえば、テンプレートコードが次のようになっており、**$interfaces** が特定の属性にバインドされている場合、次の例に示すようにコードを更新するか、属性へのバインディングではなくオブジェクトへのバインディングを変更する必要があります。

古いコードの例：

```
#foreach ( $interface in $interfaces )
 $interface.portName
      description "something"
#end
```

新しいコードの例：

```
#foreach ( $interface in $interfaces )
 interface $interface
           description "something"
#end
```

特別なキーワード

テンプレートを通じて実行されるすべてのコマンドは、常に **config t** モードになります。そのため、テンプレートで明示的に **enable or config t** コマンドを指定する必要はありません。

Day-0 テンプレートは特別なキーワードをサポートしていません。

イネーブルモードコマンド

config t コマンドの他に任意のコマンドを実行する場合は、**#MODE_ENABLE** コマンドを指定します。

次の構文を使用して、CLI テンプレートに **enable mode** コマンドを追加します。

```
#MODE_ENABLE
<<commands>>
#MODE_END_ENABLE
```

インタラクティブコマンド

ユーザー入力が必要なコマンドを実行する場合は、**#INTERACTIVE** を指定します。

インタラクティブコマンドには、コマンドを実行するために入力する必要がある入力が含まれています。[CLIコンテンツ（CLI Content）]領域にインタラクティブコマンドを入力するには、次の構文を使用します。

```
CLI Command<IQ>interactive question 1 <R> command response 1 <IQ>interactive question
2<R>command response 2
```

ここで、**<IQ>** および **<R>** タグは、デバイスに表示される内容に対して提供されるテキストを評価します。

インタラクティブな質問では、正規表現を使用して、デバイスから受け取ったテキストが入力されたテキストと類似しているかどうかを検証します。**<IQ><R>** タグに入力された正規表現が見つかった場合は、インタラクティブな質問が検証を通過し、出力テキストの一部が表示されます。つまり、質問の一部を入力する必要がありますが、質問全体を入力する必要はありません。**<IQ>**と **<R>** タグの間に「Yes」または「No」を入力するだけで十分ですが、デバイスからの質問の出力に「Yes」または「No」のテキストが表示されていることを確認する必要があります。これを行う最善の方法は、デバイスでコマンドを実行し、出力を確認することです。さらに、入力された正規表現のメタ文字または改行が適切に使用されるか、完全に回避されることを確認する必要があります。一般的な正規表現のメタ文字は **です。( ) [ ] { } |* + ? \ $ ^: &**。

たとえば、次のコマンドには、メタ文字と改行を含む出力があります。

```
Switch(config)# no crypto pki trustpoint server-CA
% Removing an enrolled trustpoint will destroy all certificates received from the related
 Certificate Authority
Are you sure you want to do this? [yes/no]:
```

テンプレートにこれを入力するには、メタ文字または改行がない部分を選択する必要があります。次に使用できる例をいくつか示します。

```
#INTERACTIVE
no crypto pki trustpoint server-CA<IQ>yes/no<R>yes
#ENDS_INTERACTIVE


#INTERACTIVE
no crypto pki trustpoint server-CA<IQ>Removing an enrolled<R>yes
#ENDS_INTERACTIVE


#INTERACTIVE
no crypto pki trustpoint server-CA<IQ>Are you sure you want to do this<R>yes
#ENDS_INTERACTIVE


#INTERACTIVE
crypto key generate rsa general-keys <IQ>yes/no<R> no
#ENDS_INTERACTIVE
```

ここで、**<IQ>** タグおよび **<R>** タグは大文字と小文字を区別し、大文字で入力する必要があります。

（注） 応答後にインタラクティブな質問に対応するとき、改行文字が必要ない場合は **<SF>** タグを入力する必要があります。**<SF>** タグの前にスペースを 1 つ含めます。**<SF>** タグを入力すると、**</SF>** タグが自動的にポップアップ表示されます。**</SF >** タグは不要なため削除できます。

次に例を示します。

```
#INTERACTIVE
config advanced timers ap-fast-heartbeat local enable 20 <SF><IQ>Apply(y/n)?<R>y
#ENDS_INTERACTIVE
```

インタラクティブ イネーブル モード コマンドの組み合わせ

次の構文を使用して、インタラクティブな **Enable Mode** コマンドを結合します。

```
#MODE_ENABLE
#INTERACTIVE
commands<IQ>interactive question<R> response
#ENDS_INTERACTIVE
#MODE_END_ENABLE


#MODE_ENABLE
#INTERACTIVE
mkdir <IQ>Create directory<R>xyz
#ENDS_INTERACTIVE
#MODE_END_ENABLE
```

複数行コマンド

CLI テンプレートで複数行をラップする場合は、**MLTCMD** タグを使用します。そうしなければ、コマンドは 1 行ずつデバイスに送信されます。[CLIコンテンツ（CLI Content）] 領域にマルチラインコマンドを入力するには、次の構文を使用します。

```
<MLTCMD>first line of multiline command
second line of multiline command
...
...
last line of multiline command</MLTCMD>
```

- ここで、**<MLTCMD>** および **</MLTCMD>** は大文字と小文字を区別し、大文字で入力する必要があります。
- 複数行のコマンドは、**<MLTCMD>** タグと **</MLTCMD>** タグの間に挿入する必要があります。
- タグをスペースで開始することはできません。
- 1 行に **<MLTCMD>** タグと **</MLTCMD>** タグを使用することはできません。

テンプレートのネットワークプロファイルへの関連付け

始める前に

テンプレートをプロビジョニングする前に、テンプレートがネットワークプロファイルに関連付けられており、そのプロファイルがサイトに割り当てられていることを確認してください。

プロビジョニング中にデバイスが特定のサイトに割り当てられると、ネットワークプロファイルを介してサイトに関連付けられたテンプレートが詳細設定に表示されます。

手順

ステップ 1 メインメニューから次を選択します。**[Design]** > **[Network Profiles]** の順に選択し、[Add Profile] をクリックします。

使用可能なプロファイルタイプは次のとおりです。

- [Assurance]：Assuranceプロファイルの作成時にこれをクリックします。
- [Firewall]：ファイアウォール プロファイルの作成時にこれをクリックします。
- [Routing]：ルーティングプロファイルの作成時にこれをクリックします。
- [Switching]：スイッチングプロファイルの作成時にこれをクリックします。
  - 必要に応じて、[Onboarding Templates] または [Day-N Templates] をクリックします。
  - [Profile Name] フィールドに、プロファイルの名前を入力します。
  - [+Add Template] をクリックして、[Device Type]、[Tag Name]、および [Template] ドロップダウンリストから、デバイスのタイプ、タグ、およびテンプレートを選択します。

    必要なテンプレートが表示されない場合は、**[Design]** > **[CLI Templates]** ウィンドウで新しいテンプレートを作成します。詳細については、標準テンプレートの作成 （576 ページ）を参照してください。
  - [Save] をクリックします。
- [Telemetry Appliance]：Catalyst Center トラフィック テレメトリ アプライアンス プロファイルの作成時にこれをクリックします。
- [Wireless]：ワイヤレスプロファイルの作成時にこれをクリックします。ワイヤレス ネットワーク プロファイルを割り当てる前に、ワイヤレス SSID が作成されていることを確認してください。
  - [Profile Name] フィールドに、プロファイルの名前を入力します。
  - [+ SSIDの追加（+ Add SSID）] をクリックします。**[Network Settings]** > **[Wireless]** で作成された SSID が表示されます。
  - [Attach Template(s)] で、[Template] ドロップダウンリストからプロビジョニングするテンプレートを選択します。

- **[Save]** をクリックします。



（注） スイッチングプロファイルとワイヤレスプロファイルは、[Cards] ビューおよび [Table] ビューで表示できます。

ステップ 2 [Network Profiles] ウィンドウには、次の値が表示されます。

- **Profile Name**
- **Type**
- **Version**
- **Created By**
- [Sites]：[Assign Site] をクリックして、選択したプロファイルにサイトを追加します。

ステップ 3 Day-*N* プロビジョニングの場合は、**[Provision] [Network Devices] [Inventory]** の順に選択して、次の操作を実行します。

a) プロビジョニングするデバイス名の横にあるチェックボックスをオンにします。

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

c) [サイトの割り当て（Assign Site）] ウィンドウで、プロファイルが添付されたサイトを割り当てます。

d) [Choose a Site] フィールドで、コントローラと関連付けるサイトの名前を入力するか、[Choose a Site] ドロップダウンリストから選択します。

e) **[次へ (Next)]** をクリックします。

f) **[** 設定（Configuration） **]** ウィンドウが表示されます。[管理対象 AP ロケーション（Managed AP Locations）] フィールドで、このコントローラによって管理される AP の場所を入力します。サイトの変更、削除、または再割り当てができます。これはワイヤレスプロファイルにのみ適用可能です。

g) [Next] をクリックします。

h) **[Advanced Configuration（詳細設定）]** ウィンドウが表示されます。ネットワークプロファイルを介してサイトに関連付けられたテンプレートが詳細設定に表示されます。

- テンプレート内のインテントからの構成を上書きして、変更を上書きする場合は、[Provision these templates even if they have been deployed before] チェックボックスをオンにします（このオプションは、デフォルトで無効です）。
- [Copy running config to startup config] オプションはデフォルトで有効になっています。つまり、テンプレート構成を展開した後、**write mem** が適用されます。実行コンフィギュレーションをスタートアップコンフィギュレーションに適用しない場合は、このチェック ボックスをオフにする必要があります。
- [Find] 機能を使用し、デバイス名を入力してすばやくデバイスを検索するか、左側のペインでテンプレートフォルダを展開してテンプレートを選択します。右側のペインで、送信元にバインドされている属性の値を選択します。
- テンプレートを導入する間にテンプレートの変数を CSV ファイルにエクスポートするには、右側のペインで [エクスポート（Export）] をクリックします。CSV ファイルを使用して変数設定

に必要な変更を加え、右側のペインで [Import] をクリックすると、後でそれを Catalyst Center にインポートできます。

i) [次へ（Next）] をクリックしてテンプレートを導入します。

j) テンプレートを今すぐ展開する場合は [Now] を選択します。または、後で展開するようにスケジュールすることを選択します。
展開が正常に完了すると、[Device Inventory] ウィンドウの [Status] 列に「SUCCESS」と表示されます。

ステップ 4 [Export Deployment CSV] をクリックして、1 つのファイルに含まれるすべてのテンプレートからテンプレート変数をエクスポートします。

ステップ 5 [Import Deployment CSV] をクリックして、1 つのファイルに含まれるすべてのテンプレートからテンプレート変数をインポートします。

ステップ 6 Day-0 プロビジョニングの場合は、**[Provision] [Plug and Play]** の順に選択して、次の操作を実行します。

a) [Actions] ドロップダウンリストからデバイスを選択し、[Claim] をクリックします。

b) [Next] をクリックし、[Site Assignment] ウィンドウで、[Site] ドロップダウンリストからサイトを選択します。

c) [Next] をクリックし、[Configuration] ウィンドウで、イメージと Day-0 テンプレートを選択します。

d) [Next] をクリックし、[Advanced Configuration] ウィンドウで場所を入力します。

e) [Next] をクリックして、[Device Details]、[Image Details]、[Day-0 Configuration Preview]、および [Template CLI Preview] を表示します。

CLI テンプレートの競合の検出

Catalyst Center では、CLI テンプレートの競合を検出できます。スイッチング、ワイヤレス、SD-Access、またはファブリックの潜在的な設計の競合とランタイムの競合を表示できます。

CLI テンプレートとサービス プロビジョニング インテント間の潜在的な設計競合の検出

同じコマンドがスイッチング、ワイヤレス、SD-Access、またはファブリックによってプッシュされた場合、潜在的な設計の競合により CLI テンプレート内のインテントコマンドが識別され、フラグが立てられます。Catalyst Center はデバイスのインテントプロビジョニングを通じてこの設定をサポートしているため、インテントコマンドの使用は推奨されません。

手順

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

[CLI Templates] ウィンドウが表示されます。

ステップ 2 （オプション）左側のペインで、[Project Name] ドロップダウンリストから、優先 CLI テンプレートを含むプロジェクトを選択します。

（注） 競合のあるテンプレートのみを表示するには、左側のペインの [Potential Design Conflicts] で [Conflicts] チェックボックスをオンにします。

ステップ 3 テンプレート名をクリックすると、競合の合計数が表示されます。

または、[Potential Design Conflicts] 列の下で警告アイコンをクリックして競合の合計数を確認できます。

CLI テンプレートが表示されます。

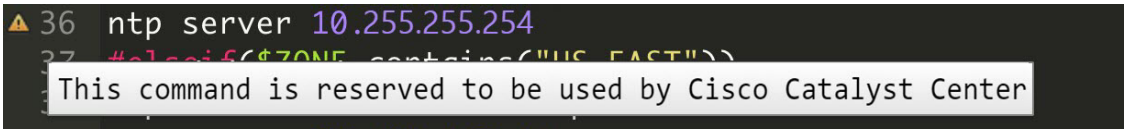
ステップ 4 競合を表示するには、[Show Design Conflicts] トグルボタンをクリックします。

ステップ 5 テンプレートで警告アイコンにカーソルを合わせると、競合の詳細が表示されます。

競合のある CLI コマンドには、警告アイコンのフラグが付けられます。新しいテンプレートの場合、テンプレートを保存した後に競合が検出されます。

例：

インテントコマンド **ntp server** が CLI テンプレートで使用されている場合、警告アイコンにカーソルを合わせると、Catalyst Center に次のメッセージが表示されます。



ステップ 6 （オプション）次の手順を実行して、新たに設定された CLI テンプレートの競合の数を表示することもできます。

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

[Inventory] ウィンドウに警告アイコン付きのメッセージが表示され、新たに設定された CLI テンプレートの競合の数が示されます。

b) [Update CLI Templates] リンクをクリックして競合を表示します。

CLI テンプレートのランタイム競合の検出

ランタイム競合検出では、CLI テンプレート内の CLI コマンドが、すでにプロビジョニングされているコマンドと正確に照合されます。コマンドの完全一致が検出された場合、Catalyst Center はコマンドにフラグを付けます。Catalyst Center を使用すると、スイッチング、ワイヤレス、SD-Access、またはファブリックのランタイム競合を検出できます。

（注） Catalyst Center は Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのランタイム競合検出はサポートしていません。

始める前に

ランタイム競合を検出するには、Catalyst Center で CLI テンプレートを設定する必要があります。

手順

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

[Inventory] ウィンドウが表示されます。

ステップ 2 [Template Provision Status] で、デバイスのテンプレート プロビジョニング ステータスを表示します。デバイスにプロビジョニングされたテンプレートの数が示されます。

正常にプロビジョニングされたテンプレートには、チェックアイコンが表示されます。競合のあるテンプレートには、警告アイコンが表示されます。

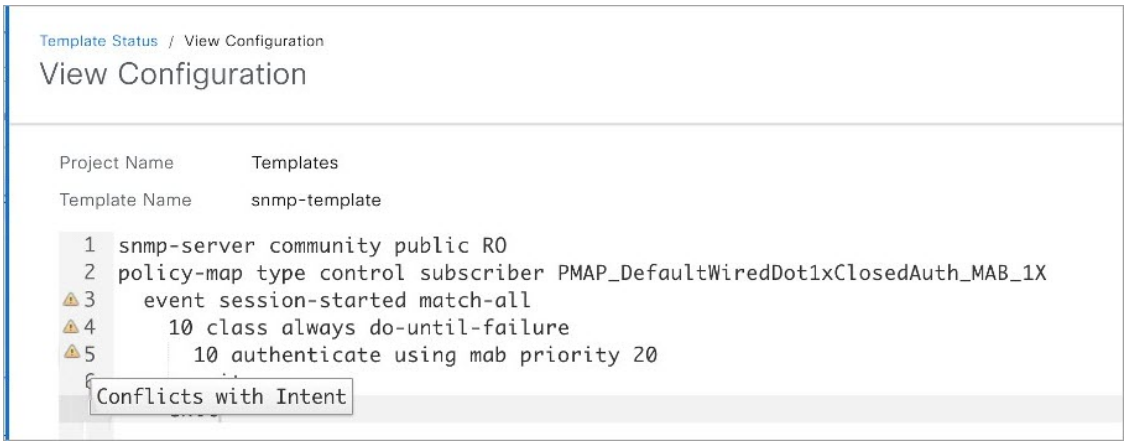
ステップ 3 [Template Provision Status] 列でリンクをクリックし、[Template Status] スライドインペインを開きます。

このテーブルで次の情報を確認できます。

- **テンプレート名**
- **プロジェクト名**
- プロビジョニングステータス：テンプレートが正常にプロビジョニングされた場合は [Template Provisioned]、テンプレートに競合がある場合は [Template Out of Sync] と表示されます。
- 競合ステータス：CLI テンプレートの競合数が表示されます。
- アクション：[View Configuration] をクリックすると CLI テンプレートが表示されます。競合のあるコマンドには、警告アイコンのフラグが付けられます。

例：

次の例は、ランタイム競合がある [View Configuration] スライドインペイン を示しています。



ステップ 4 （任意） [Inventory] ウィンドウの [Template Conflicts Status] 列で、CLI テンプレートの競合数を確認できます。

ステップ 5 設定プレビューを生成してランタイム競合を特定します。

a) デバイス名の横にあるチェックボックスをオンにします。

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

c) [Assign Site] ウィンドウで、[Next] をクリックします。[Advanced Configuration] ウィンドウで必要な変更を行い、[Next] をクリックします。[Summary] ウィンドウで、[Deploy] をクリックします。

d) [Provision Device] スライドインペインで、[Generate Configuration Preview] オプションボタンをクリックしてから、[Apply] をクリックします。

e) [Work Items] リンクをクリックし、生成された設定プレビューを表示します。

   または、メニューアイコンをクリックして次を選択します。 **[Activities]** > **[Tasks]** の順に選択し、作業項目を開いて生成された構成プレビューを表示します。

f) （オプション）アクティビティがまだロード中の場合は、[Refresh] をクリックします。

g) プレビューリンクをクリックし、[Configuration Preview] スライドインペインを開きます。 警告アイコンでフラグが付けられたランタイム競合のある CLI コマンドを確認できます。



第 12 章

機能テンプレートの設計

- 機能テンプレートの概要 （603 ページ）
- レガシーデバイスからの設計の検出と作成 （604 ページ）
- AAA RADIUS 属性の機能テンプレートの作成 （605 ページ）
- 高度な SSID の機能テンプレートの作成 （606 ページ）
- Cisco CleanAir の機能テンプレートの作成 （613 ページ）
- Dot11ax 設定用の機能テンプレートの作成 （615 ページ）
- Dot 11be ステータス設定用の機能テンプレートの作成 （618 ページ）
- イベント駆動型 RRM 設定の機能テンプレートの作成 （619 ページ）
- Flex 設定の機能テンプレートの作成 （620 ページ）
- グローバル IPv6 設定の機能テンプレートの作成 （622 ページ）
- マルチキャストの機能テンプレートの作成 （623 ページ）
- RRM FRA パラメータの機能テンプレートの作成 （624 ページ）
- RRM 一般パラメータの機能テンプレートの作成 （626 ページ）
- 不正な一般パラメータ用の機能テンプレートの作成 （628 ページ）

機能テンプレートの概要

機能テンプレート（旧モデル設定）では、プロビジョニングアプリケーション内にカプセル化される Cisco Validated Design（CVD）の高度なカスタマイズを定義できます。機能テンプレートは、高レベルのサービスインテントとデバイス固有の CLI テンプレートとともにネットワークデバイスに展開できる、モデルベースの検出可能でカスタマイズ可能な構成機能のセットです。

機能テンプレートは、複雑なデバイス設定を展開し、デバイス固有の CLI の代わりに直感的な GUI を使用してカスタマイズ可能なネットワーク構成を容易にすることで、ネットワークのプロビジョニングを簡素化します。共通の設計は、統一された方法で、さまざまなデバイス ハードウェア プラットフォームとソフトウェアタイプに展開されます。展開時に、Catalyst Center インフラストラクチャは、抽出された設計を自動的に検証してデバイス固有の CLI コマンドに変換します。

機能テンプレートをプロビジョニングするには、次の手順を実行します。

1. **[Design]** > **[Feature Templates]** ウィンドウで機能テンプレートを作成します。
2. さまざまなネットワークプロファイルに機能テンプレートを適用します。
3. プロビジョニング ワークフローを使用して、ネットワークプロファイルで指定された機能テンプレートをネットワークデバイスに適用します。



（注） CLIテンプレートを使用している場合、インベントリの同期が完了するのを待ってからプロビジョニングして機能テンプレートの設定を適用します。

サポートされている機能テンプレート

Catalyst Center は、次のワイヤレス機能テンプレートをサポートしています。

- AAA Radius 属性の設定
- 高度な SSID 構成
- CleanAir 構成
- Dot11ax の設定
- Dot11be ステータスの設定
- イベント駆動型 RRM の設定
- フレックスの設定
- グローバル IPv6 構成
- マルチキャストの設定
- RRM FRA の設定
- RRM の一般設定
- 不正な一般設定

レガシーデバイスからの設計の検出と作成

[機能テンプレート（Feature Templates）] を使用して手動で設計を作成する代わりに、[機能テンプレートの検出（Discover Feature Templates）] 機能を使用して、使用可能な既存の機能テンプレートをレガシーデバイスで検出し、新しい機能テンプレートを作成するためのテンプレートとして使用できます。

手順

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

ステップ 2 [Discovery] タブをクリックします。

検出された、**[インベントリ（Inventory）]** ウィンドウで使用可能なデバイスのリストが表示されます。

ステップ 3 デバイス名の横にあるオプションボタンをクリックし、[Discover Feature Templates] をクリックします。

ステップ 4 右側のペインで [Wireless] を展開し、機能テンプレートを選択します。

選択した機能テンプレートで使用可能な設定が表示されます。たとえば、[ワイヤレス（Wireless）] の [CleanAir設定（CleanAir Configuration）] を選択した場合、CleanAir の設定で使用可能な機能テンプレートが表示されます。

ステップ 5 新しい設計を作成するためのテンプレートとして使用する機能テンプレートの横にあるオプションボタンをクリックし、[Create Design] をクリックします。

ステップ 6 表示されるウィンドウで、必要な変更を行ってから [保存（Save）] をクリックします。

AAA RADIUS 属性の機能テンプレートの作成

[AAA Radius Attributes Configuration] 機能テンプレートを使用すると、Cisco AireOS ワイヤレス コントローラおよび Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの [Called-station-id] パラメータ値を定義できます。

[Default AAA Radius Attributes Configuration] では、**ap-macaddress-ssid** として called-station ID を定義します。このデフォルトの機能テンプレートは編集も削除もできません。ただし、特定のネットワーク設計用にカスタムの機能テンプレートを作成できます。

始める前に

検出されたデバイスが [Inventory] ウィンドウに一覧表示されるように、[Discovery] 機能を使用してネットワーク内のデバイスを検出しておきます。

手順

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

ステップ 2 左側のペインで、[Wireless] を展開して選択します。 [AAA Radius Attributes Configuration] を選択します。

または、[Search] フィールドに名前を入力して、機能テンプレートを検索することもできます。

ステップ 3 [Design Instances] ウィンドウで、[Add] をクリックします。

ステップ 4 [Add Called-station-id] スライドインペイン の [Design Name] フィールドに、機能テンプレートの名前を入力します。

ステップ 5 機能テンプレートのすべてのプロパティをロックするには、[Lock all] をクリックします。特定のプロパティをロックするには、そのプロパティの横にある対応するロックアイコンをクリックします。

設計でロックされているプロパティは、デバイスのプロビジョニング中に変更できません。

ステップ 6 [Called-station-id] ドロップダウンリストから、属性値を選択します。

ステップ 7 [保存（**Save**）] をクリックします。

[設計インスタンス（Design Instances）] ウィンドウに新しい設計インスタンスが表示されます。

ステップ 8 （オプション）設計を編集するには、編集する設計の名前の横にあるチェックボックスをオンにして [Edit] をクリックします。変更を加えたら、[Save] をクリックします。

次のタスク

1. 作成した機能テンプレートをネットワークプロファイルに関連付け、ワイヤレスコントローラに展開できるようにします。メインメニューから次を選択します。**[Design]** > **[Network Profiles]** の順に選択します。詳細については、ワイヤレス用のネットワークプロファイルの作成 （543 ページ）を参照してください。
2. ネットワークプロファイルで指定された機能テンプレートをネットワークデバイスにプロビジョニングします。メインメニューから次を選択します。**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。詳細については、Cisco AireOS コントローラのプロビジョニング （738 ページ）またはCisco Catalyst 9800 シリーズ ワイヤレス コントローラ のプロビジョニング （782 ページ）を参照してください。

高度な SSID の機能テンプレートの作成

WLANは、サービスセットID（SSID）をインターフェイスまたはインターフェイス グループにアソシエートします。WLAN で、セキュリティ、Quality of Service（QoS）、無線ポリシーなど、ワイヤレスネットワークのパラメータが設定されます。ワイヤレスコントローラごとに最大 512 個の WLAN を設定できます。

デバイスの高度な SSID パラメータの設定には、[Advanced SSID Configuration] 機能テンプレートを使用します。**[Default Advanced SSID Design]** は、デフォルトの高度な SSID 機能テンプレートです。デフォルト設計は編集や削除ができません。ただし、特定のネットワーク設計用にカスタムの機能テンプレートを作成できます。

始める前に

検出されたデバイスが [Inventory] ウィンドウに一覧表示されるように、[Discovery] 機能を使用してネットワーク内のデバイスを検出する必要があります。

手順

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

ステップ 2 左側のペインで、[Wireless] を展開して選択します。 [Advanced SSID Configuration] の順に選択します。

または、[Search] フィールドに名前を入力して、機能テンプレートを検索することもできます。

ステップ 3 [Design Instances] ウィンドウで、[Add] をクリックします。

ステップ 4 [Add Advanced SSID Configuration] スライドインペインの [Design Name] フィールドに、機能テンプレートの名前を入力します。

ステップ 5 機能テンプレートのすべてのプロパティをロックするには、[Lock all] をクリックします。特定のプロパティをロックするには、そのプロパティの横にある対応するロックアイコンをクリックします。

設計でロックされているプロパティは、デバイスのプロビジョニング中に変更できません。

ステップ 6 [General] タブで、次の手順を実行します。

a) [Peer-to-Peer Blocking] ドロップダウンリストから、ピアツーピアブロッキングのオプションを選択します。

ピアツーピアブロッキングは、個々の WLAN に適用されます。各クライアントは、アソシエート先のWLANのピアツーピアブロッキング設定を継承します。ピアツーピアブロッキングを使用すると、トラフィックの転送方法を細かく制御できます。

- [DISABLE]：ピアツーピアブロッキングを無効にし、可能な場合はワイヤレスコントローラ内においてローカルでトラフィックを転送し ます。
- [DROP]：ワイヤレスコントローラでクライアントパケットを破棄します。
- [FORWARD UP]：クライアントパケットをアップストリームの VLAN に転送します。パケットに対して行われる操作は、ワイヤレスコントローラよりも上流にあるデバイスにより決定されます。このデバイスは、ルータまたはレイヤ 3 スイッチのいずれかになります。
- [ALLOW PVT GROUP]：事前共有キー（PSK）クライアントにのみ適用されます。送信元と宛先のクライアントデバイスに関連付けられている Identity PSK（IPSK）タグに基づいてトラフィックが転送されます。

b) パッシブクライアント機能を有効にするには、[Passive Client Enable] トグルボタンをクリックします。

パッシブクライアントとは、固定 IP アドレスが設定されている、スケールやプリンタなどのワイヤレスデバイスです。パッシブクライアントは、AP との関連付けの際に IP 情報（IP アドレス、サブネットマスク、ゲートウェイ情報など）を送信しません。その結果、パッシブクライアントが使用された場合、それらのクライアントが DHCP を使用しない限り、ワイヤレスコントローラではその IP アドレスは認識されません。

c) WLAN の経由ローミング予測リストを設定するには、[Assisted Roaming Prediction Optimization] トグルボタンをクリックします。

d) デュアル無線バンドのネイバーリストを設定するには、[Neighbor List Dual Band] トグルボタンをクリックします。

e) WLAN で SNMP NAC サポートを有効にするには、[Network Admission Control (NAC-SNMP)] トグルボタンをクリックします。

f) WLAN で RADIUS NAC サポートを有効にするには、[Network Admission Control (NAC-Radius)] トグルボタンをクリックします。

g) [DHCP Required] ドロップダウンリストで、RUN 状態（クライアントからのトラフィックがワイヤレスコントローラを通過できる状態）になるために DHCP 要求が必要かどうかに応じて、[Yes] または [No] のいずれかを選択します。

h) [DHCP Server - IP Address] フィールドに、DHCP サーバーの IP アドレスを入力します。

i) FlexConnect ローカル認証を有効にするには、[FlexConnect Local Authentication] トグルボタンをクリックします。

j) [802.11ax Status] トグルボタンをクリックして、802.11ax 構成パラメータを有効にします。

k) [Aironet IE] トグルボタンをクリックして、この SSID で Aironet IE のサポートを有効にします。

l) [Load Balance Enable] トグルボタンをクリックして、負荷分散機能を有効にします。

m) [DTIM Period 5GHz Band (In Beacon Intervals) [1-255]] フィールドに、5 GHz 無線の値を入力します。

有効な範囲は 1 ～ 255 です。デフォルト値は 1（ブロードキャストフレームおよびマルチキャストフレームはビーコンのたびに送信）です。

802.11 ネットワークのビーコン間隔が 100 ミリ秒で DTIM 値が 1 に設定されている場合、AP は、バッファされたブロードキャストフレームおよびマルチキャストフレームを毎秒10回送信します。ビーコン間隔が 100 ミリ秒で DTIM 値が 2 に設定されている場合、AP は、バッファされたブロードキャストフレームおよびマルチキャストフレームを毎秒5回送信します。これらの設定はいずれも、ブロードキャスト フレームおよびマルチキャスト フレームの頻度を想定する、Voice over IP（VoIP）を含むアプリケーションに適しています。

ただし、DTIM 値は 255 まで設定できます（255 回のビーコンごとにブロードキャストフレームおよびマルチキャストフレームを送信します）。

n) [DTIM Period 2.4GHz Band (In Beacon Intervals) [1-255]] フィールドに、2.4 GHz 無線の値を入力します。有効な範囲は 1 ～ 255 です。デフォルト値は 1（ブロードキャストフレームおよびマルチキャストフレームはビーコンのたびに送信）です。

o) [Max Clients Per WLAN] フィールドに、WLAN への参加を許可されるクライアントの最大数を入力します。

有効な範囲は 0 ～ 10,000 です。

p) [Max Clients Per AP Radio Per WLAN [0-500]] フィールドに、WLAN への参加を許可される AP ごとのクライアントの最大数を入力します。

有効な範囲は 0 ～ 500 です。

q) [Max Clients Per AP Radio Per WLAN [0-1200]] フィールドに、AP ごとに許可されるクライアント接続の最大数を入力します。

有効な範囲は 0 ～ 1200 です。

r) [WMM Policy] ドロップダウンリストから、WMM ポリシーのオプション [Allowed]、[Disabled]、または [Required] を選択します。

WMM ポリシーのデフォルトは [Allowed] です。

s) [NAS ID] フィールドにネットワークアクセスサーバー識別子を入力します。

ステップ 7 [Client Data Rate] タブで、次の各フィールドに値を入力して、クライアントごとのこれらのクライアントデータレート制限を設定します。

- **Average Downstream Data Rate Per Client (kbps)**
- **Burst Downstream Data Rate Per Client (kbps)**
- **Average Downstream Real-Time Rate Per Client (kbps)**
- **Burst Downstream Real-Time Rate Per Client (kbps)**
- **Average Upstream Data Rate Per Client (kbps)**
- **Burst Upstream Data Rate Per Client (kbps)**
- **Average Upstream Real-Time Rate Per Client (kbps)**
- **Burst Upstream Real-Time Rate Per Client (kbps)**

ステップ 8 [SSID Data Rate] タブで、次の各フィールドに値を入力して、SSID ごとのこれらの SSID データレート制限を設定します。

- **Average Upstream Data Rate Per SSID (kbps)**
- **Burst Upstream Data Rate Per SSID (kbps)**
- **Average Upstream Real-Time Rate Per SSID (kbps)**
- **Burst Upstream Real-Time Rate Per SSID (kbps)**
- **Average Downstream Data Rate Per SSID (kbps)**
- **Burst Downstream Data Rate Per SSID (kbps)**
- **Average Downstream Real-Time Rate Per SSID (kbps)**
- **Burst Downstream Real-Time Rate Per SSID (kbps)**

ステップ 9 カーソルを [More] にホバーし、[802.11ax Configuration] をクリックして、802.11ax BSS 構成パラメータを設定します。次のパラメータを有効化または無効化するには、対応するトグルボタンを使用します。

- **BSS ターゲット起動時間**
- **ダウンリンク OFDMA**
- **アップリンク OFDMA**
- **ダウンリンク MU-MIMO**
- **アップリンク MU-MIMO**

（注） これらのパラメータは、2.4 GHz および 5 GHz の無線帯域にのみ適用されます。**[Design]** > **[Network Settings]** > **[Wireless]** > **[RF Profiles]** ウィンドウで、6 GHz 無線帯域の 802.11ax パラメータを設定できます。詳細については、ワイヤレス無線周波数プロファイルの作成（451 ページ）を参照してください。

Cisco IOS XE リリース 17.18.2 以降、**OFDMA Uplink**、**OFDMA Downlink**、**MU-MIMO Uplink**、および **MU-MIMO Downlink** の各パラメータは、2.4 GHz および 5 GHz 無線帯域上の対応する 802.11be 設定にも使用されます。

ステップ 10 [More] にカーソルを合わせて [Off Channel Scanning Defer] をクリックし、スキャンの保留時間と保留の優先順位を設定します。

a) [Scan Defer Time [0-60000msecs]] フィールドにミリ秒単位で時間を設定します。

有効な範囲は 0 ～ 60,000 ミリ秒、デフォルト値は 100 ミリ秒です。時間を 0 に設定すると、スキャンの保留は実行されません。スキャンの保留時間は同じ WLAN のすべてのプライオリティに共通です。また、スキャンは保留プライオリティのいずれかでパケットが送信または受信される場合に保留されます。

b) 対応するトグルボタンをクリックして、パケットに必要な優先順位マーキングを設定します。

- [Defer Priority0]
- [Defer Priority1]
- [Defer Priority2]
- [Defer Priority3]
- [Defer Priority4]
- [Defer Priority5]
- [Defer Priority6]
- [Defer Priority7]

（注） これらのパラメータは、Cisco AireOS ワイヤレスコントローラ ではサポートされません。

ステップ 11 [More] にカーソルを合わせて [Device Analytics] をクリックし、デバイス分析パラメータを設定します。

a) [Share Data with Client] トグルボタンをクリックして、Cisco デバイスデータをクライアントと共有できるようにします。
b) [Advertise Support] トグルボタンをクリックして、デバイス分析サポートを設定します。
c) [Advertise PC Analytics Support] トグルボタンをクリックして、PC 分析サポートを設定します。

（注） これらのパラメータは、Cisco AireOS ワイヤレスコントローラ ではサポートされません。

ステップ 12 [More] にカーソルを合わせて [802.11k Beacon Radio Measurement] をクリックし、802.11k ビーコン無線測定パラメータを設定します。

a) [Client Scan Report On Association] トグルボタンをクリックして、クライアントの関連付け時にビーコン測定要求（クライアント スキャン レポート）を送信します。

b) [Client Scan Report On Roam] トグルボタンをクリックして、クライアントローミング時にビーコン測定要求（クライアント スキャン レポート）を送信します。

（注） これらのパラメータは、Cisco AireOS ワイヤレスコントローラ ではサポートされません。

ステップ 13 [More] にカーソルを合わせて [Multicast Buffer] をクリックし、マルチキャスト バッファ パラメータを設定します。

a) [Multicast Buffer Enable] トグルボタンをクリックして、WLAN の 802.11a 無線のマルチキャストバッファ調整モードを設定します。

（注） このパラメータは、Cisco AireOS ワイヤレスコントローラ ではサポートされません。

ステップ 14 [More] にカーソルを合わせて [SIP-CAC] をクリックし、SIP コールアドミッション制御（CAC）パラメータを設定します。

a) [Call Snooping] トグルボタンをクリックして、ポリシープロファイルにマッピングされた WLAN のコールスヌーピングを設定します。

b) [Send Disassociate] トグルボタンをクリックして、SIP CAC の関連付け解除送信オプションを設定します。

c) [Send 486 Busy] トグルボタンをクリックして、SIP CAC の 486 busy 送信オプションを設定します。

（注） これらのパラメータは、Cisco AireOS ワイヤレスコントローラ ではサポートされません。

ステップ 15 [More] にカーソルを合わせて [Miscellaneous] をクリックし、次のパラメータを設定します。

a) [Media Stream Multicast-Direct] トグル ボタンをクリックして、WLAN のマルチキャストダイレクトを設定します。

b) [802.11ac MU-MIMO] トグルボタンをクリックして、WLAN で 802.11ac MU-MIMO を設定します。

c) [Wifi To Cellular Steering] トグルボタンをクリックして、WLAN で Wi-Fi をセルラーステアリングに設定します。

d) [Wi-Fi Alliance Agile Multiband] トグルボタンをクリックして、Wi-Fi Alliance Agile Multiband（MBO）サポートを設定します。

e) [Fastlane+ (ASR)] トグルボタンをクリックして、WLAN での高度なスケジューリング要求処理を設定します。
f) [Dot11v Bss Max Idle Protected] トグルボタンをクリックして、WLAN ごとの BSS 最大アイドル処理を設定します。
g) [Universal Admin] トグルボタンをクリックして、802.1x、WPA、または WPA2 で保護された WLAN でユニバーサル管理モードを有効にできるようにします。
h) [Opportunistic Key Caching] トグルボタンをクリックして、Opportunistic Key Caching を設定します。
i) [IP Source Guard] トグルボタンをクリックして、MAC 検証を設定します。
j) [Enable DHCP Option82 Remote ID suboption] トグル ボタンをクリックして、DHCP オプション 82 リモート ID オプションを設定します。
k) [VLAN Central Switching] トグルボタンをクリックして、VLAN 中央スイッチングを設定します。
l) [IP MAC Binding] トグルボタンをクリックして、IP MAC バインディング作成のサポートの制御を設定します。
m) [Idle threshold (0-4294967295 bytes)] フィールドに、アイドルしきい値を入力します。有効な範囲は 0 ～ 4,294,967,295 バイトです。デフォルト値は 0 です
n) [Reassociation Timeout time [1-100 seconds]] フィールドに、再関連付けのタイムアウト時間を入力します。有効な範囲は 1 ～ 100 秒です。デフォルト値は 20 秒です。
o) [mDNS Mode] ドロップダウンリストから、mDNS モードとして [Bridging]、[Drop]、または [Gateway] を選択します。

（注） これらのパラメータは、Cisco AireOS ワイヤレスコントローラ ではサポートされません。

ステップ 16 [Save] をクリックします。

作成した設計インスタンスが [Design Instances] ウィンドウの [Advanced SSID Configuration - Feature Templates] エリアに表示されます。

ステップ 17 （任意） 設計を編集するには、編集する設計の名前の横にあるチェックボックスをオンにして [Edit] をクリックします。変更を加えたら、[Save] をクリックします。

次のタスク

1. ワイヤレスコントローラに展開できるようにするために、作成した機能テンプレートをネットワークプロファイルに関連付けます。メインメニューから次を選択します。**[Design]** > **[Network Profiles]** の順に選択します。詳細については、ワイヤレス用のネットワークプロファイルの作成 （543 ページ）を参照してください。
2. ネットワークプロファイルで指定された機能テンプレートをネットワークデバイスにプロビジョニングします。メインメニューから次を選択します。**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。詳細については、Cisco AireOS コントローラのプロビジョニング （738 ページ）を参照してください。

Cisco CleanAir の機能テンプレートの作成

CleanAirは、共有ワイヤレススペクトラムに関する問題に予防的に対応するスペクトルインテリジェンスソリューションです。この機能を使用すると、共有スペクトラムの全ユーザーを確認できます（ネイティブデバイスと外部干渉源の両方）。また、ネットワークにおいて、これらの情報に基づいて対処できるようになります。たとえば、干渉デバイスを手動で排除することや、システムによって自動的にチャネルをステアリングして干渉を受けないようにすることができます。CleanAir は、スペクトラム管理と無線周波数（RF）の可視性を提供します。

[Default CleanAir 802.11a Design]、[Default CleanAir 802.11b Design]、および [Default CleanAir 6GHz Design] が、デフォルトの CleanAir 設定機能テンプレートです。デフォルト設計は編集や削除ができません。ただし、特定のネットワーク設計用にカスタムの機能テンプレートを作成できます。

始める前に

検出されたデバイスが [Inventory] ウィンドウに一覧表示されるように、[Discovery] 機能を使用してネットワーク内のデバイスを検出しておきます。

手順

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

ステップ 2 左側のペインで、[Wireless] を展開して選択します。 [CleanAir Configuration] を選択します。

または、[Search] フィールドに名前を入力して、機能テンプレートを検索することもできます。

ステップ 3 [Design Instances] ウィンドウで、[Add] をクリックします。

ステップ 4 [Add CleanAir Configuration] ウィンドウの [Design Name] フィールドに、設計の名前を入力します。

ステップ 5 機能テンプレートのすべてのプロパティをロックするには、[Lock all] をクリックします。特定のプロパティをロックするには、そのプロパティの横にある対応するロックアイコンをクリックします。

設計でロックされているプロパティは、デバイスのプロビジョニング中に変更できません。

ステップ 6 [Radio Band] ドロップダウンリストから [2.4 GHz] または [5 GHz] を選択します。

ステップ 7 [CleanAir Enable] トグルボタンをクリックして、2.4 GHz または 5 GHz の無線帯域で CleanAir 機能を有効にします。

[CleanAir Enable] トグルボタンが有効になっている場合は、そのトグルボタンをクリックして機能を無効にすることにより、スペクトル干渉を ワイヤレスコントローラ で検出しないようにします。

ステップ 8 [CleanAir Device Reporting Enable] トグルボタンをクリックして、干渉源が検出された場合に CleanAir システムから報告されるようにします。

[CleanAir Device Reporting Enable] トグルボタンが有効になっている場合は、トグルボタンをクリックして機能を無効にすることにより、干渉源が ワイヤレスコントローラ から報告されないようにします。

ステップ 9 CleanAir で検出できる永続型デバイスに関する情報を伝達できるように、[Persistent Device Propagation] トグルボックスをオンにします。

永続型デバイスの伝達を有効にすると、同じワイヤレスコントローラに接続されているネイバー AP に永続型デバイスの情報を伝達できます。永続型の干渉源は、常に検出できない場合でも、その場所に存在し、WLAN の動作に干渉します。

ステップ 10 [Enable Interferers Features] を展開し、CleanAir システムで検出および報告する必要がある干渉源の横にあるチェックボックスをオンにします。

- Ble Beacon
- Bluetooth Paging Inquiry
- Bluetooth SCO ACL
- Generic Dect
- Generic TDD
- Generic Waveform
- Jammer
- 電子レンジ
- Motorola Canopy
- SI FHSs
- Spectrum 802.11 FH
- Spectrum 802.11 Non STD Channel
- Spectrum 802.11 Spec Inverted
- Spectrum 802.11 Super AG SuperAG
- Spectrum 802.15.4
- ビデオ
- Wimax Fixed
- Wimax Mobile
- XBox

ステップ 11 [CleanAir Description] フィールドに説明を入力します。

ステップ 12 [Save] をクリックします。
作成した設計インスタンスが [Design Instances] ウィンドウの [CleanAir Configuration – Feature Templates] エリアに表示されます。

ステップ 13 （任意） 設計を編集するには、編集する設計の名前の横にあるチェックボックスをオンにして [Edit] をクリックします。変更を加えたら、[Save] をクリックします。

次のタスク

1. ワイヤレスコントローラ に展開できるようにするために、作成した機能テンプレートをネットワークプロファイルに関連付けます。メインメニューから次を選択します。**[Design]** > **[Network Profiles]** の順に選択します。詳細については、ワイヤレス用のネットワークプロファイルの作成 （543 ページ）を参照してください。
2. ネットワークプロファイルで指定された機能テンプレートをネットワークデバイスにプロビジョニングします。メインメニューから次を選択します。**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。詳細については、Cisco AireOS コントローラのプロビジョニング （738 ページ）を参照してください。

Dot11ax 設定用の機能テンプレートの作成

Dot11ax Configuration 機能テンプレートは、デバイスの 802.11ax パラメータを設定します。**[Default Dot11ax 6-GHz Design]**、**[Default Dot11ax 802.11a Design]**、および **[Default Dot11ax 802.11b Design]** が、デフォルトの 802.11ax 設定機能テンプレートです。デフォルト設計は編集や削除ができません。ただし、特定のネットワーク設計用にカスタムの機能テンプレートを作成できます。

Dot11ax 構成には、高効率（HE）ワイヤレスとも呼ばれる 802.11ax ワイヤレス仕様標準が含まれます。Dot11ax は 2.4 GHz、5 GHz および 6 GHz バンドを使用するデュアルバンドテクノロジーです。Dot11ax 構成パラメータは、Wi-Fi 6 をサポートしている Cisco Catalyst 9100 シリーズ アクセスポイントでのみ設定できます。

（注） BSS カラーは、重複する基本サービスセット（OBSS）を識別するために使用されます。BSS 構成は、Wi-Fi 6 対応 AP でのみプッシュされます。Cisco Catalyst 9100 シリーズ アクセスポイントは、高密度の高解像度アプリケーションに最適な次世代の Wi-Fi 802.11ax AP です。

始める前に

検出されたデバイスが [Inventory] ウィンドウに一覧表示されるように、[Discovery] 機能を使用してネットワーク内のデバイスを検出する必要があります。

手順

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

ステップ 2 左側のペインで、[Wireless] を展開して選択します。 [Dot11ax Configuration] の順に選択します。

または、[Search] フィールドに名前を入力して、機能テンプレートを検索することもできます。

ステップ 3 [Design Instances] ウィンドウで、[Add] をクリックします。

ステップ 4 **[Add Dot11ax Configuration]** ウィンドウの **[Design Name]** フィールドに、機能テンプレートの名前を入力します。

ステップ 5 機能テンプレートのすべてのプロパティをロックするには、[Lock all] をクリックします。特定のプロパティをロックするには、そのプロパティの横にある対応するロックアイコンをクリックします。

設計でロックされているプロパティは、デバイスのプロビジョニング中に変更できません。

ステップ 6 [BSS Color] トグルボタンをクリックして、BSS カラー機能を有効にします。デフォルト値は [disabled] です。

BSS カラー機能は、以下でサポートされています。

- Cisco AireOS 8.10 以降を搭載した Cisco AireOS ワイヤレスコントローラ
- Cisco IOS XE リリース 17.1 以降を搭載した シスコ ワイヤレス コントローラ

ステップ 7 [Target Wakeup Time] トグルボタンをクリックしてターゲットのウェイクアップ時間を有効にします。デフォルト値は [disabled] です。

目標のウェイクアップ時間は、以下でサポートされています。

- Cisco AireOS 8.10 以降を搭載した Cisco AireOS ワイヤレスコントローラ
- Cisco IOS XE リリース 17.1 以降を搭載した ワイヤレスコントローラ

ステップ 8 [Target Wakeup Time Broadcast] トグルボタンをクリックしてターゲットのウェイクアップ時間ブロードキャストを有効にします。デフォルト値は [disabled] です。

ターゲットウェイクアップ時間ブロードキャストは、以下でサポートされています。

- Cisco AireOS 8.10 以降を搭載した Cisco AireOS ワイヤレスコントローラ
- Cisco IOS XE リリース 17.3.1 以降を搭載した ワイヤレスコントローラ

（注） Cisco IOS XE リリース 17.3.1 と Cisco IOS XE リリース 17.6 の間のバージョンを実行しているワイヤレスコントローラの場合、ターゲット起動時間ブロードキャストの YANG のデフォルト値が有効になります。リリース 2.3.5 より前のリリースからこれらのワイヤレスコントローラを使用して Catalyst Center をアップグレードすると、YANG のデフォルト値が有効になっていても、デフォルト値は無効に設定されます。この違いは、属性の実際の値と目的の値の間におけるコンプライアンスの不一致として一覧表示されます。

ワイヤレスコントローラで目的の値を設定するには、アップグレード後にワイヤレスコントローラを再プロビジョニングします。

ステップ 9 [Multiple BSSID] トグルボタンをクリックして、複数の基本サービスセット識別子（BSSID）機能を有効にします。デフォルト値は [disabled] です。

複数の BSSID は、Cisco IOS XE 17.7.1 以降を搭載した ワイヤレスコントローラでのみサポートされています。

（注） この切り替えボタンは、[6 GHz] 無線帯域を選択した時にのみ有効です。

ステップ 10 [Radio Band] ドロップダウンリストから [2.4 GHz]、[5 GHz]、または [6 GHz] を選択します。デフォルト値は [disabled] です。

ステップ 11 [OBSS PD] トグルボタンをクリックして、オーバーラップ BSS パケット検出（OBSS-PD）機能を有効にします。

OBSS-PD は、Cisco IOS XE 17.4 以降を搭載した ワイヤレスコントローラ でのみサポートされています。

（注） このトグルボタンは、**6 GHz** 無線帯域には使用できません。

ステップ 12 [Non-SRG OBSS PD Max Threshold (dBm)] フィールドに、非空間再利用グループ（SRG）OBSS-PD 最大しきい値の値を dBm 単位で入力します。デフォルト値は -62 dBm です。

非 SRG OBSS-PD は、Cisco IOS XE 17.4 以降を搭載した ワイヤレスコントローラ でのみサポートされます。

（注） このトグルボタンは、**6 GHz** 無線帯域には使用できません。

ステップ 13 [Save] をクリックします。

作成した設計インスタンスが **[Design Instances]** ウィンドウの **[Dot11ax Configuration – Feature Templates]** エリアに表示されます。

ステップ 14 （任意） 設計を編集するには、編集する設計の名前の横にあるチェックボックスをオンにして [Edit] をクリックします。変更を加えたら、[Save] をクリックします。

次のタスク

1. AP に展開できるようにするために、作成した機能テンプレートをネットワークプロファイルにアタッチします。メインメニューから次を選択します。**[Design]** > **[Network Profiles]** の順に選択します。詳細については、「ワイヤレス用のネットワークプロファイルの作成」を参照してください。
2. ネットワークプロファイルで指定された機能テンプレートをネットワークデバイスにプロビジョニングします。メインメニューから次を選択します。**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。詳細については、Cisco AireOS コントローラのプロビジョニング （738 ページ）を参照してください。

Dot 11be ステータス設定用の機能テンプレートの作成

[Dot11be Status Configuration] 機能テンプレートは、2.4 GHz、5 GHz、および 6 GHz 無線帯域の 802.11be ステータスを設定します。802.11be 設定は、Cisco IOS XE リリース 17.15.2 を実行しているデバイスに適用されます。

[Default 802.11be Status 2.4GHz Design]、**[Default 802.11be Status 5GHz Design]**、および **[Default 802.11be Status 6GHz Design]** は、デフォルトの 802.11be ステータス設定機能テンプレートです。デフォルト設計は編集や削除ができません。ただし、特定のネットワーク設計用にカスタムの機能テンプレートを作成できます。

手順

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

ステップ 2 **左側のペインで、[Wireless] を展開して [Dot11be Status Configuration] を選択します。**

または、[Search] フィールドに名前を入力して、機能テンプレートを検索することもできます。

ステップ 3 [Design Instances] ウィンドウで、[Add] をクリックします。

ステップ 4 [Add 802.11be Status Configuration] スライドインペインの [Design Name] フィールドに、機能テンプレートの名前を入力します。

ステップ 5 機能テンプレートのすべてのプロパティをロックするには、[Lock all] をクリックします。特定のプロパティをロックするには、そのプロパティの横にある対応するロックアイコンをクリックします。

設計でロックされているプロパティは、デバイスのプロビジョニング中に変更できません。

ステップ 6 802.11be ステータスを有効または無効にするには、 [Dot11be Status] トグルボタンを使用します。

重要 802.11be ステータスを設定すると、WLAN が一時的に無効化され、対応する無線帯域のクライアントの接続が失われます。

ステップ 7 [Radio Band] ドロップダウンリストから、802.11be ステータスを設定する無線帯域（**2.4 GHz**、**5 GHz**、または **6 GHz**）を選択します。

ステップ 8 [Save] をクリックします。

作成した設計インスタンスが [Design Instances] ウィンドウの [Dot11be Status Configuration - Feature Templates] エリアに表示されます。

ステップ 9 （任意） 設計を編集するには、編集する設計の名前の横にあるチェックボックスをオンにして [Edit] をクリックします。変更を加えたら、[Save] をクリックします。

次のタスク

1. ワイヤレスコントローラ に展開できるようにするために、作成した機能テンプレートをネットワークプロファイルに関連付けます。メインメニューから次を選択します。**[Design]** > **[Network Profiles]** の順に選択します。詳細については、ワイヤレス用のネットワークプロファイルの作成 （543 ページ）を参照してください。
2. ネットワークプロファイルで指定された機能テンプレートをネットワークデバイスにプロビジョニングします。メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。詳細については、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のプロビジョニング （782 ページ）を参照してください。

イベント駆動型 RRM 設定の機能テンプレートの作成

[Event Driven RRM Configuration] 機能テンプレートを使用して、2.4 GHz および 5 GHz 無線のイベント駆動型 RRM パラメータを設定できます。[Default Event Driven 2.4GHz Design] と [Default Event Driven 5GHz Design] は、デフォルトのイベント駆動型 RRM 設定機能テンプレートです。デフォルト設計は編集や削除ができません。ただし、特定のネットワーク設計用にカスタムの機能テンプレートを作成できます。

始める前に

検出されたデバイスが [Inventory] ウィンドウに一覧表示されるように、[Discovery] 機能を使用してネットワーク内のデバイスを検出しておきます。

手順

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

ステップ 2 左側のペインで、[Wireless] を展開して選択します。 [Event Driven RRM Configuration] の順に選択します。

または、[Search] フィールドに名前を入力して、機能テンプレートを検索することもできます。

ステップ 3 [Design Instances] ウィンドウで、[Add] をクリックします。

ステップ 4 [Add Event Driven RRM Configuration] スライドインペインの [Design Name] フィールドに、機能テンプレートの名前を入力します。

ステップ 5 機能テンプレートのすべてのプロパティをロックするには、[Lock all] をクリックします。特定のプロパティをロックするには、そのプロパティの横にある対応するロックアイコンをクリックします。

設計でロックされているプロパティは、デバイスのプロビジョニング中に変更できません。

ステップ 6 [Radio Band] ドロップダウンリストから、無線帯域（[2.4GHz] または [5GHz]）を選択します。

ステップ 7 CleanAir 対応 AP が重大なレベルの干渉を検出したときに RRM を実行するには、[Event Driven RRM] トグルボタンをクリックします。

ステップ 8 [感度しきい値（Sensitivity Threshold）] ドロップダウンリストで、次のオプションから RRM をトリガーする感度しきい値レベルを選択します。

AP の干渉がしきい値レベルを上回ると、RRM はローカルの動的チャネル割り当て（DCA）の実行を開始し、ネットワーク パフォーマンスを改善できる場合は影響を受ける AP 無線のチャネルを変更します。

- [Low]：電波品質（AQ）値が示す非 Wi-Fi 干渉への感度を最低に指定します。
- [Medium]：電波品質（AQ）値が示す非 Wi-Fi 干渉への感度を中間に指定します。
- [High]：AQ 値によって示される非 Wi-Fi 干渉に対する最も高い感度を指定します。
- [Custom]：AQ 値によって示される非 Wi-Fi 干渉に対するカスタム感度を指定します。このオプションを選択した場合は、[Custom Threshold [1-99]] フィールドでカスタム値を指定する必要があります。

ステップ 9 **[Save]** をクリックします。

作成した設計インスタンスが [Design Instances] ウィンドウの [Event Driven RRM Configuration - Feature Templates] エリアに表示されます。

ステップ 10 （任意） 設計を編集するには、編集する設計の名前の横にあるチェックボックスをオンにして [Edit] をクリックします。変更を加えたら、[Save] をクリックします。

次のタスク

1. ワイヤレスコントローラ に展開できるようにするために、作成した機能テンプレートをネットワークプロファイルに関連付けます。メインメニューから次を選択します。**[Design]** > **[Network Profiles]** の順に選択します。詳細については、ワイヤレス用のネットワークプロファイルの作成 （543 ページ）を参照してください。
2. ネットワークプロファイルで指定された機能テンプレートをネットワークデバイスにプロビジョニングします。メインメニューから次を選択します。**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。詳細については、Cisco AireOS コントローラのプロビジョニング （738 ページ）を参照してください。

Flex 設定の機能テンプレートの作成

[Flex設定（Flex Configuration）] 機能テンプレートを使用して、Cisco IOS XE ベースのワイヤレスコントローラで FlexConnect 設定を構成します。

[Default Flex Configuration] は、デフォルトの FlexConnect 設定機能テンプレートです。デフォルト設計は編集や削除ができません。ただし、特定のネットワーク設計用にカスタムの機能テンプレートを作成できます。

始める前に

[Discovery] 機能を使用して、検出されたデバイスが [Inventory] ウィンドウに一覧表示されるように、ネットワーク内のデバイスを検出します。

手順

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

ステップ 2 左側のペインで、[Wireless] を展開して選択します。 [Flex Configuration] を選択します。

または、[Search] フィールドに名前を入力して、機能テンプレートを検索することもできます。

ステップ 3 [Design Instances] ウィンドウで、[Add] をクリックします。

ステップ 4 [Add Flex Configuration] スライドインペインの [Design Name] フィールドに、設計の名前を入力します。

ステップ 5 機能テンプレートのすべてのプロパティをロックするには、[Lock all] をクリックします。特定のプロパティをロックするには、そのプロパティの横にある対応するロックアイコンをクリックします。

設計でロックされているプロパティは、デバイスのプロビジョニング中に変更できません。

ステップ 6 [IPオーバーラップ（IP Overlap）] トグルボタンをクリックして、IP オーバーラップを設定します。

ステップ 7 [Apply] をクリックします。
作成した設計インスタンスが [設計インスタンス（Design Instances）] ウィンドウの [Flex設定-機能テンプレート（Flex Configuration - Feature Templates）] エリアに表示されます。

ステップ 8 （任意） 設計を編集するには、編集する設計の名前の横にあるチェックボックスをオンにして [Edit] をクリックします。変更を加えたら、[Save] をクリックします。

次のタスク

1. ワイヤレスコントローラに展開できるようにするために、作成した機能テンプレートをネットワークプロファイルに関連付けます。メインメニューから次を選択します。**[Design]** > **[Network Profiles]** の順に選択します。詳細については、ワイヤレス用のネットワークプロファイルの作成 （543 ページ）を参照してください。

   機能テンプレートをデバイスのグローバル設定として使用するには、デバイスサイトのネットワークプロファイルに追加します。SSID 固有の設定に機能テンプレートを使用するには、管理対象の AP の場所かサイトのネットワークプロファイルに追加します。

2. ネットワークプロファイルで指定された機能テンプレートをネットワークデバイスにプロビジョニングします。メインメニューから次を選択します。**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。詳細については、Cisco AireOS コントローラのプロビジョニング （738 ページ）を参照してください。

グローバル IPv6 設定の機能テンプレートの作成

[Global IPV6 Configuration] 機能テンプレートを使用して、デバイスで IPv6 をグローバルに有効にします。

[Default Global IPv6 Design] は、デフォルトのグローバル IPV6 設定の機能テンプレートです。デフォルト設計は編集や削除ができません。ただし、特定のネットワーク設計用にカスタムの機能テンプレートを作成できます。

始める前に

検出されたデバイスが [Inventory] ウィンドウに一覧表示されるように、[Discovery] 機能を使用してネットワーク内のデバイスを検出しておきます。

手順

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

ステップ 2 左側のペインで、[Wireless] を展開して選択します。 **グローバル IPv6 設定**を選択します。

または、[Search] フィールドに名前を入力して、機能テンプレートを検索することもできます。

ステップ 3 [Design Instances] ウィンドウで、[Add] をクリックします。

ウィンドウが表示されます。

ステップ 4 [Add Global IPV6 Configuration] スライドインペインの [Design Name] フィールドに、機能テンプレートの名前を入力します。

ステップ 5 機能テンプレートのすべてのプロパティをロックするには、[Lock all] をクリックします。特定のプロパティをロックするには、そのプロパティの横にある対応するロックアイコンをクリックします。

設計でロックされているプロパティは、デバイスのプロビジョニング中に変更できません。

ステップ 6 [Global IPV6 Config] トグルボタンをクリックして、IPv6 をデバイスでグローバルに有効にします。

ステップ 7 [Save] をクリックします。

作成した設計インスタンスが [Design Instances] ウィンドウの [Global IPV6 Configuration - Feature Templates] エリアに表示されます。

ステップ 8 （任意） 設計を編集するには、編集する設計の名前の横にあるチェックボックスをオンにして [Edit] をクリックします。変更を加えたら、[Save] をクリックします。

次のタスク

1. 作成した機能テンプレートをネットワークプロファイルに関連付けて、ワイヤレスコントローラに展開できるようにします。メインメニューから次を選択します。**[Design]**>**[Network**

Profiles] の順に選択します。詳細については、ワイヤレス用のネットワークプロファイルの作成 （543 ページ）を参照してください。

2. ネットワークプロファイルで指定された機能テンプレートをネットワークデバイスにプロビジョニングします。メインメニューから次を選択します。**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。詳細については、Cisco AireOS コントローラのプロビジョニング （738 ページ）を参照してください。

マルチキャストの機能テンプレートの作成

[Multicast Configuration] 機能テンプレートを使用して、デバイスでマルチキャストパラメータを設定します。

ネットワークがパケットのマルチキャストをサポートしている場合は、シスコ ワイヤレス コントローラが使用するマルチキャストの方法を設定できます。ワイヤレスコントローラは、次のいずれかのモードでマルチキャストを実行します。

- ユニキャストモード：このモードでは、ワイヤレスコントローラは、ワイヤレスコントローラに関連付けられているすべてのアクセスポイントにすべてのマルチキャストパケットをユニキャストします。このモードはそれほど効率的ではありませんが、マルチキャストをサポートしていないネットワークでは必要です。
- マルチキャストモード：このモードでは、ワイヤレスコントローラはマルチキャストパケットを CAPWAP マルチキャストグループに送信します。この方法では、ワイヤレスコントローラ プロセッサのオーバーヘッドが軽減され、パケットレプリケーションの処理がネットワークに移されます。この方式は、ユニキャスト方式より効率的です。

[Default Multicast Design] は、デフォルトのマルチキャスト設定機能テンプレートです。デフォルト設計は編集や削除ができません。ただし、特定のネットワーク設計用にカスタムの機能テンプレートを作成できます。

始める前に

検出されたデバイスが [Inventory] ウィンドウに一覧表示されるように、[Discovery] 機能を使用してネットワーク内のデバイスを検出しておきます。

手順

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

ステップ 2 左側のペインで、[Wireless] を展開して選択します。 [Multicast Configuration] を選択します。

または、[Search] フィールドに名前を入力して、機能テンプレートを検索することもできます。

ステップ 3 [Design Instances] ウィンドウで、[Add Design] をクリックします。

ステップ 4 [Add Multicast Configuration] の [Design Name] フィールドに、設計の名前を入力します。

ステップ 5 機能テンプレートのすべてのプロパティをロックするには、[Lock all] をクリックします。特定のプロパティをロックするには、そのプロパティの横にある対応するロックアイコンをクリックします。

設計でロックされているプロパティは、デバイスのプロビジョニング中に変更できません。

ステップ 6 [Enable Global Multicast Mode] トグルボタンをクリックして、マルチキャストパケットの送信を設定します。デフォルト値は [disabled] です。

ステップ 7 [AP Multicast Mode] ドロップダウンリストから、[UNICAST] または [MULTICAST] を選択します。

- ワイヤレスコントローラからユニキャスト方式でパケットをブロードキャストするように設定するには、[UNICAST] を選択します。
- ワイヤレスコントローラからマルチキャスト方式でCAPWAPマルチキャストグループにパケットをブロードキャストするように設定するには、[MULTICAST] を選択します。

ステップ 8 [IPV4 Multicast Group Address] を展開し、[IP Address] フィールドに IPv4 マルチキャストアドレスを入力します。

ステップ 9 [IPV6 Multicast Group Address] を展開し、[IP Address] フィールドに IPv6 マルチキャストアドレスを入力します。

ステップ 10 [Apply] をクリックします。

作成した設計インスタンスが [Design Instances] ウィンドウの [Multicast Configuration - Feature Templates] エリアに表示されます。

ステップ 11 （任意） 設計を編集するには、編集する設計の名前の横にあるチェックボックスをオンにして [Edit] をクリックします。変更を加えたら、[Save] をクリックします。

次のタスク

1. ワイヤレスコントローラ に展開できるようにするために、作成した機能テンプレートをネットワークプロファイルに関連付けます。メインメニューから次を選択します。**[Design]**>**[Network Profiles]** の順に選択します。詳細については、ワイヤレス用のネットワークプロファイルの作成 （543 ページ）を参照してください。
2. ネットワークプロファイルで指定された機能テンプレートをネットワークデバイスにプロビジョニングします。メインメニューから次を選択します。**[Provision]**>**[Network Devices]**>**[Inventory]** の順に選択します。詳細については、Cisco AireOS コントローラのプロビジョニング （738 ページ）を参照してください。

RRM FRA パラメータの機能テンプレートの作成

[RRM FRA Configuration] 機能テンプレートは、2.4 ～ 5 GHz および 5 ～ 6 GHz の無線帯域での無線リソース管理（RRM）用のフレキシブル ラジオ アサインメント（FRA）パラメータを設定します。

[Default FRA 2.4-5GHz Design] と **[Default FRA 5-6GHz Design]** は、デフォルトの FRA 機能テンプレートです。デフォルト設計は編集や削除ができません。ただし、特定のネットワーク設計用にカスタムの機能テンプレートを作成できます。

（注）
- Cisco AireOS ワイヤレスコントローラでは、6 GHz 無線帯域はサポートされていません。
- 6 GHz 無線帯域は、Cisco IOS XE 17.6 以降を搭載した Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ でサポートされています。

始める前に

検出されたデバイスが [Inventory] ウィンドウに一覧表示されるように、[Discovery] 機能を使用してネットワーク内のデバイスを検出する必要があります。

手順

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

ステップ 2 左側のペインで、[Wireless] を展開して選択します。 [RRM FRA Configuration] の順に選択します。

または、[Search] フィールドに名前を入力して、機能テンプレートを検索することもできます。

ステップ 3 [Design Instances] ウィンドウで、[Add] をクリックします。

ステップ 4 **[Add Flexible Radio Assignment (FRA) Configuration]** スライドインペイン の **[Design Name]** フィールドに、設計の名前を入力します。

ステップ 5 機能テンプレートのすべてのプロパティをロックするには、[Lock all] をクリックします。特定のプロパティをロックするには、そのプロパティの横にある対応するロックアイコンをクリックします。

設計でロックされているプロパティは、デバイスのプロビジョニング中に変更できません。

ステップ 6 [Radio Band] ドロップダウンリストから無線バンドを選択します。

ステップ 7 [FRA Freeze] トグルボタンを使い、FRA をフリーズする機能を有効にします。この機能は、デフォルトで無効になっています。

この機能は、Cisco IOS XE 17.6.1 以降を搭載した シスコ ワイヤレス コントローラ でサポートされています。

（注） このトグルボタンは、2.4 ～ 5 GHz の無線帯域でのみ使用できます。

ステップ 8 [FRA Status] トグルボタンを使い、FRA ステータス機能を有効にします。この機能はデフォルトでイネーブルになっています。

ステップ 9 [FRA Interval] ドロップダウンリストで、[FRA interval] を選択します。

ステップ 10 [FRA Sensitivity] ドロップダウンリストから、[FRA sensitivity value] を選択します。

このパラメータは FRA カバレッジのオーバーラップ感度を設定します。

（注） このドロップダウンリストは、**2.4 ～ 5 GHz** の無線バンドでのみ使用できます。

ステップ 11 [Save] をクリックします。

作成した設計インスタンスが [Design Instances] ウィンドウの [RRM FRA Configuration – Feature Templates] 領域に表示されます。

ステップ 12 （任意） 設計を編集するには、編集する設計の名前の横にあるチェックボックスをオンにして [Edit] をクリックします。変更を加えたら、[Save] をクリックします。

次のタスク

1. アクセスポイントに展開できるようにするために、作成した機能テンプレートをネットワークプロファイルにアタッチします。メインメニューから次を選択します。**[Design]** > **[Network Profiles]** の順に選択します。詳細については、ワイヤレス用のネットワークプロファイルの作成 （543 ページ）を参照してください。
2. ネットワークプロファイルで指定された機能テンプレートをネットワークデバイスにプロビジョニングします。メインメニューから次を選択します。**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。詳細については、Cisco AireOS コントローラのプロビジョニング （738 ページ）およびCisco Catalyst 9800 シリーズ ワイヤレス コントローラ のプロビジョニング （782 ページ）を参照してください。

RRM 一般パラメータの機能テンプレートの作成

[RRM General Configuration] 機能テンプレートは、2.4 GHz、5 GHz、および 6 GHz 無線の無線リソース管理（RRM）一般パラメータを設定します。

[Default RRM General 2.4 GHz Design]、**[Default RRM General 5 GHz Design]**、および **[Default RRM General 6 GHz Design]** が、デフォルトの RRM 一般設定機能テンプレートです。デフォルト設計は編集や削除ができません。ただし、特定のネットワーク設計用にカスタムの機能テンプレートを作成できます。

（注）
- Cisco AireOS ワイヤレスコントローラ では、6 GHz 無線帯域はサポートされていません。
- 6 GHz 無線帯域は、Cisco IOS XE リリース 17.6 以降を搭載した Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ でサポートされています。

始める前に

検出されたデバイスが [Inventory] ウィンドウに一覧表示されるように、[Discovery] 機能を使用してネットワーク内のデバイスを検出しておきます。

手順

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

ステップ 2 左側のペインで、[Wireless] を展開して選択します。 [RRM General Configuration] の順に選択します。

または、[Search] フィールドに名前を入力して、機能テンプレートを検索することもできます。

ステップ 3 [Design Instances] ウィンドウで、[Add] をクリックします。

ステップ 4 **[Add RRM General Configuration]** スライドインペイン の **[Design Name]** フィールドに、設計の名前を入力します。

ステップ 5 機能テンプレートのすべてのプロパティをロックするには、[Lock all] をクリックします。特定のプロパティをロックするには、そのプロパティの横にある対応するロックアイコンをクリックします。

設計でロックされているプロパティは、デバイスのプロビジョニング中に変更できません。

ステップ 6 [Radio Band] タブで、[Radio Band] ドロップダウンリストから無線帯域を [2.4 GHz]、[5 GHz]、または [6 GHz] から選択します。

ステップ 7 [Threshold] タブで、[Throughput Threshold (1000-10000000 Bps)] フィールドで選択した無線帯域のスループットしきい値を設定します。

ステップ 8 [Monitoring] タブで、モニタリングチャネルとネイバー探索タイプを設定します。

- [Monitoring Channels] ドロップダウンリストから次のオプションのいずれかを選択して、AP で RRM によるスキャンに使用されるチャネルのセットを指定します。デフォルトでは、モニタリングチャネルは [Country] に設定されています。
  - [All]：選択した無線でサポートされているすべてのチャネルで、RRM によるチャネルスキャンが実行されます。使用国で有効でないチャネルも対象となります。
  - [Country]：使用国内のデータチャネルのみで、RRM によるチャネルスキャンが実行されます。これはデフォルト値です。
  - [DCA]：RRM チャネルスキャンは、DCA アルゴリズムによって使用されるチャネルセットでのみ発生します。
- [Neighbor Discover Type] ドロップダウンリストから、ネイバー探索タイプを選択します。デフォルトでは、モードは [transparent] に設定されます。
  - [transparent]：ネイバー探索タイプを「transparent」に設定します。パケットはそのまま送信されます。
  - [protected]：ネイバー探索タイプを「protected」に設定します。パケットが暗号化されます。

ステップ 9 [Coverage] タブで、[Global Coverage Hole Detection Enabled] トグルボタンをクリックして、カバレッジホールの検出を有効にします。デフォルトで、この値が選択されています。

カバレッジホールの検出を有効にすると、カバレッジが不完全な領域に位置する可能性のあるクライアントを持つ AP があるかどうかを、AP から受信したデータに基づいて Cisco ワイヤレスコントローラが自動的に判断します。

ステップ 10 [Save] をクリックします。

作成した設計インスタンスが [Design Instances] ウィンドウの [RRM General Configuration - Feature Templates] 領域に表示されます。

ステップ 11 （任意） 設計を編集するには、編集する設計の名前の横にあるチェックボックスをオンにして [Edit] をクリックします。変更を加えたら、[Save] をクリックします。

次のタスク

1. ワイヤレスコントローラ に展開できるようにするために、作成した機能テンプレートをネットワークプロファイルに関連付けます。メインメニューから次を選択します。**[Design]** > **[Network Profiles]** の順に選択します。詳細については、ワイヤレス用のネットワークプロファイルの作成 （543 ページ）を参照してください。
2. ネットワークプロファイルで指定された機能テンプレートをネットワークデバイスにプロビジョニングします。メインメニューから次を選択します。**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。詳細については、Cisco AireOS コントローラのプロビジョニング （738 ページ）を参照してください。

不正な一般パラメータ用の機能テンプレートの作成

不正な一般設定およびクライアント除外ポリシーを設定するには、次の手順を実行します。

不正な一般設定のデフォルトの機能テンプレートには、次のようなものがあります。

- [Default Rogue General Configuration Critical]（デフォルトの不正な一般設定：クリティカル）
- [Default Rogue General Configuration Custom]（デフォルトの不正な一般設定：カスタム）
- [Default Rogue General Configuration High]（デフォルトの不正な一般設定：高）
- [Default Rogue General Configuration Low]（デフォルトの不正な一般設定：低）

デフォルト設計は編集や削除ができません。ただし、特定のネットワーク設計用にカスタムの機能テンプレートを作成できます。

始める前に

検出されたデバイスが [Inventory] ウィンドウに一覧表示されるように、[Discovery] 機能を使用してネットワーク内のデバイスを検出する必要があります。

手順

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

ステップ 2 左側のペインで、[Wireless] を展開して選択します。 [Rogue General Configuration] を選択します。

または、[Search] フィールドに名前を入力して、機能テンプレートを検索することもできます。

ステップ 3 [Add] をクリックして、新しい不正な一般設定プロファイルを作成します。

[不正な一般設定の追加（Add Rogue General Configuration）] スライドインペインが表示されます。

ステップ 4 [不正な一般設定の追加（Add Rogue General Configuration）] スライドインペインで、次の手順を実行します。

a) [Design Name] フィールドに設計の名前を入力します。

b) [General] タブで、ドロップダウンリストから [Rogue Detection Security Level] を選択します。

c) [Expiration timeout for Rogue APs] フィールドに、次のように、選択した不正検出セキュリティレベルの時間を秒単位で入力します。

- [LOW]：低セキュリティレベルを選択した場合、有効期限タイムアウトは240秒である必要があります。
- [HIGH]：高セキュリティレベルを選択した場合、有効期限タイムアウトは1200秒である必要があります。
- [CRITICAL]：クリティカルセキュリティ レベルを選択した場合、有効期限タイムアウトは3600秒である必要があります。
- [CUSTOM]：カスタムセキュリティレベルを選択した場合、有効期限タイムアウトは240～3500秒である必要があります。

d) 不正なクライアントを検証する場合は、[Validate Rogue Clients against AAA] トグルボタンを切り替えます。

e) アドホックネットワークを報告する場合は、[Detect and Report Adhoc Networks] トグルボタンを切り替えます。

f) 不正な AP を検証する場合は、[Validate Rogue APs against AAA] トグルボタンを切り替えます。

（注） [Validate Rogue APs against AAA] トグルボタンと [Rogue Polling Interval (seconds)] フィールドは、セキュリティレベルとしてカスタムを選択した場合にのみ表示されます。

g) [Rogue Polling Interval (seconds)] フィールドに、有効な不正ポーリング時間間隔を秒単位で入力します。

有効な不正ポーリング間隔の値の範囲は 60 ～ 86400 秒です。

h) [Rogue Detection Client Number Threshold] フィールドに、有効なしきい値（0 ～ 256）を入力します。

i) [Rogue Init Timer (seconds)] フィールドに、時間を秒単位で入力します。デフォルト値は 180 秒です。

j) [AP Authentication Alarm Threshold] フィールドに、有効なしきい値（1 ～ 255）を入力します。

k) システムログが生成される場合に通知を取得するには、[Syslog Notification] トグルボタンを切り替えます。

l) [MFP Key Refresh Interval (hours)] フィールドに、有効な時間間隔（1 ～ 24）を入力します。

m) （オプション）設計のすべてのプロパティをロックするには、[Lock all] をクリックします。特定のプロパティをロックするには、そのプロパティの横にある対応するロックアイコンをクリックします。

n) [Save] をクリックします。

次のタスク

1. （任意）ネットワークプロファイルへの機能テンプレートの追加については、ネットワークプロファイルへの機能テンプレートの追加 （549 ページ）を参照してください。

2. ネットワークプロファイルで指定された機能テンプレートをネットワークデバイスにプロビジョニングします。メインメニューから次を選択します。**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。

   詳細については、Cisco AireOS コントローラのプロビジョニング （738 ページ）を参照してください。



第 13 章

ソフトウェア イメージの管理

- ソフトウェアイメージ管理について （631 ページ）
- ソフトウェアイメージの完全性検証 （632 ページ）
- ソフトウェア イメージの表示 （632 ページ）
- 推奨されるソフトウェアイメージの使用 （637 ページ）
- ソフトウェアイメージのインポート （638 ページ）
- デバイスファミリに対するソフトウェアイメージの割り当ての管理 （640 ページ）
- イメージ更新のスケジュール （642 ページ）
- デバイスのソフトウェアイメージをインストールモードでアップロードする （644ページ）
- 標準ソフトウェアイメージについて （646 ページ）
- ソフトウェアイメージをスタンダードとしてマークする （646 ページ）
- 標準ソフトウェアイメージの管理 （649 ページ）
- イメージ配信サーバーの設定 （651 ページ）
- サイトへのイメージ配信サーバーの追加 （653 ページ）
- ソフトウェアイメージのプロビジョニング （653 ページ）

ソフトウェアイメージ管理について

Catalyst Center は、ネットワークにあるデバイスのすべてのソフトウェアイメージとソフトウェア メンテナンス アップデート（SMU）、サブパッケージ、ROMMON イメージなどを保存します。ソフトウェアイメージ管理には、次の機能があります。

- ソフトウェアイメージ管理：Catalyst Center はイメージタイプとバージョンに応じて、固有のソフトウェアイメージをすべて保存します。ユーザーはソフトウェア イメージの表示、インポート、および削除ができます。
- プロビジョニング：ソフトウェアイメージをネットワーク内のデバイスにプッシュできます。

ソフトウェアイメージ管理機能を使用する前に、Cisco Catalyst 3000、4000、および 6000 などの古いデバイスで Transport Layer Security（TLS）プロトコルを有効にする必要があります。システムアップグレード後は、TLS を再度有効にする必要があります。詳細については、Cisco

Catalyst Center 管理者ガイド [英語] の「Configure Security for Catalyst Center」を参照してください。

（注） リリース 2.3.3 以降、Catalyst Center では、IE3x00 シリーズおよび IE9x00 シリーズ スイッチのソフトウェアイメージ管理（SWIM）およびソフトウェア メンテナンス アップデート（SMU）のプライマリブートオプションとして内部ブートフラッシュのみをサポートします。

Catalyst Center の以前のリリース（リリース 2.3.3 より前）があり、ネットワーク内の IE3x00 または IE9x00 デバイスがセキュアデジタル（SD）フラッシュメモリモジュールですでに起動されている場合は、**boot flash-primary** コマンドを使用して、内部ブートフラッシュをデバイスのプライマリブートオプションとして設定してください。

実行コンフィギュレーションを SD フラッシュからブートフラッシュに保存して同期するには、**sync** コマンドを使用します。

ソフトウェアイメージの完全性検証

整合性検証アプリケーションでは、デバイスの感染を示す予期しない変更や無効な値がないか、Catalyst Center に格納されたソフトウェア イメージをモニターします。システムは、インポートプロセス中に、インポートしているイメージのソフトウェアおよびハードウェア プラットフォームのチェックサム値と、Known Good Values（KGV）ファイルのプラットフォームで識別されたチェックサム値を比較して、2 つの値の一致を確認することで、イメージの整合性を決定します。

完全性検証アプリケーションで現在の KGV ファイルを使用して選択したソフトウェアイメージを検証できない場合は、**[ソフトウェアイメージ管理（Software Image Management）]** ページにメッセージが表示されます。整合性検証アプリケーションおよびKGV ファイルのインポートの詳細については、*Cisco Catalyst Center* 管理者ガイド [英語] を参照してください。

ソフトウェア イメージの表示

ディスカバリを実行するか、手動でデバイスを追加した後、Catalyst Center は、デバイスのソフトウェア イメージ、SMU、およびサブパッケージに関する情報を自動的に保存します。

手順

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

ステップ 2 [概要（Overview）] タブは、次のセクションで構成されています。

- 上部セクションには、次の詳細情報が表示されます。

- [イメージ（Images）]：デバイスファミリのイメージ数を、重大および高レベルのアドバイザリとともに示します。
- [デバイス（Devices）]：タグ付けされたイメージ、更新の準備ができているイメージ、失敗した更新の準備状況、失敗したイメージ更新の数を示します。
- [更新（Updates）]：失敗したイメージ更新、進行中のイメージ更新、成功したイメージ更新の数を示します。

- 下部にある [イメージ更新ツール（Image Update Tools）] セクションでは、次のタスクを実行できます。
  - [イメージ更新のスケジュール（Schedule Image Update）]：選択したデバイスの特定の日時におけるソフトウェアイメージの更新をスケジュールします。詳細については、イメージ更新のスケジュール （642 ページ）を参照してください。
  - [イメージ更新ステータスの確認（Check Image Update Status）]：[更新ステータスの確認（Check Update Status）] をクリックし、事前チェック条件をトリガーしてイメージをデバイスと再同期します。[デバイスの更新（Devices Updates）] スライドインペインには、進行中の更新、待機中の更新、終了した更新、成功した更新、失敗した更新が表示されます。

    テーブルには、デバイス名、IPアドレス、更新日、更新の所要時間、ソフトウェアイメージバージョン、タスク名、更新ステータス、アクションの詳細が示されます。デバイス名をクリックし、詳細を表示します。[アクション（Actions）] 列では、デバイスの [再試行（Retry）] オプションをクリックして更新を再実行できます。

    [今後のタスク（Upcoming Tasks）] をクリックし、スケジュールされた更新を表示します。
  - [Download Update Readiness Report]：[準備状況レポートのダウンロード（Download Readiness Report）] をクリックし、すべてのデバイスのデバイス準備状況結果をCSVファイルにダウンロードします。
  - [Import Image]：[イメージのインポート（Import Image）] をクリックし、ソフトウェアイメージまたはソフトウェアイメージ更新をインポートします。詳細については、ソフトウェアイメージのインポート （638 ページ）を参照してください。

- [まだ送信されていないイメージ更新のフロー（Yet to be submitted Image Update flows）] セクションには、まだ送信されていない今後のタスクが表示されます。このセクションの省略記号アイコンをクリックすると、タスクを再開するのか削除するのかを決定できます。

ステップ 3 [イメージ（Images）] タブは、次のオプションで構成されています。

a) [イメージ（Images）] セクションには、デバイスファミリの総数、実行中のイメージ、標準、重大、高のアドバイザリがないデバイスファミリが表示されます。

右側の [イメージの概要を表示（Show images summary）] または [イメージの概要を非表示（Hide images summary）] をクリックし、概要を表示するか非表示にします。

b) 下部セクションには、イメージの製品ファミリ名の詳細が、各デバイスファミリのデバイス、イメージ、標準とマークされたイメージ、重大と高のアドバイザリの数とともに表示されます。

次のタスクを実行できます。

- [インポートされたイメージの表示（Show imported images）]：インポートされたソフトウェアイメージの詳細を表示する場合にクリックします。

  [Imported Image Family] ウィンドウの [Images] テーブルには、インポートされたすべてのソフトウェアイメージの [Image Name]、[Version]、[Device Series Assigned]、および [Action] が表示されます。

  [Action] 列で [Assign] をクリックして、ソフトウェアイメージをデバイスファミリに割り当てます。詳細については、デバイスファミリに対するソフトウェアイメージの割り当ての管理 （640 ページ）を参照してください。

- [タスクの表示（Show task）]：ソフトウェアイメージに関連するすべてのタスクのステータスを表示する場合にクリックします。

  [Recent Tasks] スライドインペインには、最近の 50 件のタスクのステータスが表示されます。[タスクステータス（Task Status）] ドロップダウンリストから、[すべて（All）]、[失敗（Failed）]、[進行中（In-Progress）]、または [成功（Successful）] を選択し、ステータスに基づいてタスクをフィルタ処理します。

- [イメージのインポート（Import images）]：ソフトウェアイメージまたはソフトウェアイメージ更新をインポートする場合にクリックします。詳細については、ソフトウェアイメージのインポート （638 ページ）を参照してください。

[製品ファミリ名（Product Family Name）] 列から、デバイス名をクリックして詳細を表示します。

- 選択したデバイスで使用可能なすべてのイメージを含む新しいウィンドウが開き、イメージ名とバージョンが表示されます。
- [属性（Attributes）]列には、イメージの詳細が表示されます。属性が [推奨（Recommended）]のイメージについては、Cisco.com からイメージをダウンロードできます。
- [アクション（Actions）] 列では、イメージを標準としてマークし、ダウンロードすることを選択できます。詳細については、ソフトウェアイメージをスタンダードとしてマークする （646 ページ）を参照してください。
  - [イメージの詳細情報なし（Image details not available）]：一致するイメージをダウンロードする場合にクリックします。
  - [ダウンロード可能（Available for download）]：イメージは Cisco.com でダウンロード可能です。イメージを標準としてマークし、Cisco.com からダウンロードできます。
  - [ダウンロード済み（Downloaded）]：最新のイメージがすでにダウンロードされています。イメージを標準または条件付き標準としてマークする場合にクリックします。
  - [標準としてマーク（Marked as standard）]：イメージは標準としてマークされています。ドロップダウン矢印をクリックして標準タグを削除するか、標準条件を編集します。

上部にある [同期の更新（Sync Updates）] オプションをクリックしてイメージの最新のステータスを表示します。

ステップ 4 [デバイス（Devices）] タブは、次のオプションで構成されています。

a) [デバイス（Devices）] セクションには、対象デバイスの総数とイメージステータスが異なるデバイスの数が表示されます。イメージステータスは、標準としてタグ付けされていないイメージ、更新の準備ができているイメージ、更新の準備に失敗、失敗したイメージ、イメージの更新が進行中、標準イメージで実行されているデバイスです。

右側の [デバイスの概要を表示（Show devices summary）] または [デバイスの概要を非表示（Hide devices summary）] をクリックし、概要を表示または非表示にします。

b) 下部セクションには、デバイス名、タグ、デバイスファミリ、ソフトウェアバージョン、イメージステータス、イメージ名、到達可能性、準備状況チェックステータス、管理アドレス、最新の更新ステータス、イメージの互換性の詳細が表示されます。

c) [タグ（Tag）] をクリックしてデバイスの新しいタグを作成するか、既存のタグを管理します。詳細については、デバイスのタグ付け （191 ページ）を参照してください。

d) 1 つ以上のデバイスを選択して [イメージ更新の準備状況の確認（Check Image Update Readiness）] をクリックし、事前チェック条件をトリガーしてイメージをデバイスと再同期します。このオプションを使用すると、[デバイス（Devices）] タブの [準備完了（Ready）] オプションをクリックしたときに最終再同期時刻を表示できます。[デバイスの更新（Devices Updates）] スライドインペインには、進行中の更新、待機中の更新、終了した更新、成功した更新、失敗した更新が表示されます。

e) [更新準備状況レポートのダウンロード（Download Update Readiness Report）] をクリックし、すべてのデバイスのデバイス準備状況結果を CSV ファイルにダウンロードします。

f) デバイスを選択し、[デバイスの更新（Update Devices）] をクリックしてイメージアップグレードプロセスを開始します。このオプションを使用すると、[イメージの更新（Image Update）] ウィンドウにリダイレクトされます。このイメージアップグレード手順では、特定の日時にイメージを更新するようにスケジュールすることもできます。詳細については、イメージ更新のスケジュール （642 ページ）を参照してください。

デバイス名をクリックし、そのデバイスの詳細を表示します。

[デバイスファミリ（Device Family）] 列から、デバイス名をクリックして詳細を表示します。

- 選択したデバイスで使用可能なすべてのイメージを含む新しいウィンドウが開き、イメージ名とバージョンが表示されます。
- [属性（Attributes）] 列には、イメージの詳細が表示されます。属性が [推奨（Recommended）] のイメージについては、Cisco.com からイメージをダウンロードできます。
- [アクション（Actions）] 列では、イメージを標準としてマークし、ダウンロードすることを選択できます。詳細については、ソフトウェアイメージをスタンダードとしてマークする （646 ページ）を参照してください。

上部にある [同期の更新（Sync Updates）] オプションをクリックしてイメージの最新のステータスを表示します。

ステップ 5 [更新（Updates）] タブには、失敗した、成功した、進行中、およびスケジュールが設定されている最近のイメージ更新の詳細が表示されます。タスクへのリンクをクリックすると、詳細情報を表示できます。

ステップ 6 Cisco.com ユーザーを設定済みの場合は、ステップ 3 に進みます。設定していない場合は、次の手順を実行します。

a) ブラウザでシークレット/プライベートウィンドウを開きます（以前にキャッシュされたログイン情報の使用を避けるため）。
b) 別の Catalyst Center GUI インスタンスを開いてログインします。
c) **[ソフトウェアイメージ管理（Software Image Management）]** ページの別のインスタンスを開きます。
d) 次のいずれかのタスクを完了します。

次の場合は...	次の操作...
Catalyst Center の新規インストールを完了した。	[Cisco.com ID] フィールドの [Add] リンクをクリックして、新しい Cisco.com ユーザーを設定します。
最新バージョンの Catalyst Center にアップグレードしており、以前に設定されたのと同じ Cisco.com ユーザーを使用する。	[Cisco.com ID] フィールドの [Re-Authenticate] リンクをクリックして該当ユーザーを再認証します。
最新バージョンの Catalyst Center にアップグレードしており、以前と同じ Cisco.com ユーザーを使用しない。	古い Cisco.com ユーザーを削除してから、新しいユーザーを設定します。 **1.** [Cisco.com ID] フィールドの [Delete] リンクをクリックします。 **2.** 表示されたダイアログボックスで、[Delete] をクリックして操作を確定します。 **3.** [Cisco.com ID] フィールドの [Add] リンクをクリックします。

e) [Information] ポップアップウィンドウで、次のチェックボックスの一方または両方をオンにして、[Authenticate] をクリックします。
   - （必須）[I am in private or incognito mode]
   - （オプション）[Save Credentials]

f) [Activate your device] ポップアップウィンドウで、アクティベーションコードが表示されていることを確認し、[Next] をクリックします。
g) [Log in] ポップアップウィンドウで、cisco.com ユーザの電子メールアドレスを入力し、[Next] をクリックします。
h) [Verify with your password] ポップアップウィンドウで、cisco.com ユーザーのパスワードを入力し、[Verify] をクリックします。

   [Device Activated] ポップアップウィンドウが表示されます。

i) [Device Activated] ポップアップウィンドウを閉じます。
j) **[ソフトウェアイメージ管理（Software Image Management）]** ページを更新します。
k) [Cisco.com ID] フィールドに、ユーザーに対して入力した電子メールアドレスが表示されていることを確認します。また、[Change] リンクが表示されていることを確認します。

ステップ 7 ウィンドウの上部にある [ルータ（Routers）]、[スイッチ（Switches）]、[ワイヤレスコントローラ（Wireless Controllers）]、[セキュリティおよびVPN（Security and VPN）]、[センサー（Sensors）]、または [仮想デバイス（Virtual Devices）] をクリックするか、[イメージ（Images）] タブの検索またはフィルタアイコンをクリックして、デバイスファミリをフィルタ処理します。

デフォルトでは、[イメージ（Images）] タブにすべてのデバイスファミリが表示されます。

（注） イメージのアクティブ化およびイメージの更新機能は、サードパーティ製デバイスではサポートされていないため、サードパーティ（シスコ以外）のデバイスは、**[イメージ（Images）]** ウィンドウに表示されません。

ステップ 8 [Sync Updates] をクリックし、後続の警告メッセージで [OK] をクリックして、Catalyst Center のすべての管理対象デバイスの cisco.com からのイメージ情報を同期します。

Cisco.com のログイン情報が設定されていない場合は、ログイン情報を指定するよう求められます。

[Show Tasks] でタスクの進捗状況を確認することができます。タスクが成功すると、すべてのデバイスファミリのイメージ情報が更新されます。

（注） イメージ情報を取得できるのは 1 時間に 1 回のみです。

推奨されるソフトウェアイメージの使用

Catalyst Center は、管理しているデバイスのシスコ推奨のソフトウェアイメージを表示します。ユーザーはそこから選択できます。

（注） シスコが推奨する最新のソフトウェアイメージのみをダウンロードできます。

手順

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

ステップ 2 cisco.com に接続するための正しいログイン情報が入力されていることを確認します。

ステップ 3 メインメニューから次を選択します。**[Provision]** > **[Software Image Management]**。

ステップ 4 [Images] をクリックします。

Catalyst Centerは、各製品ファミリと、それに対応するデバイス数、イメージ、標準としてマークされたイメージなどを表示します。

ステップ 5 [製品ファミリ名（Product Family Name）] で、製品ファミリをクリックして、使用可能なすべてのイメージを表示します。

この表には、一部のデバイスタイプとそのデバイスタイプがサポートしていないソフトウェアイメージが一覧表示されます。

デバイス タイプ	制限事項
Catalyst Center によって管理される AP	SWIM のアップグレードやダウングレードはサポートされていません。
Cisco Meraki デバイス	SWIM のアップグレードやダウングレードはサポートされていません。
サードパーティ製デバイス	SWIM のアップグレードやダウングレードはサポートされていません。
Cisco Catalyst 9400 シリーズ スイッチ	ブートローダーイメージのアップグレードやダウングレードはサポートされていません。
Cisco Catalyst 9800 シリーズ スイッチ	ROMMON イメージのアップグレードはサポートされています。しかし、イメージのダウングレードはサポートされていません。
Cisco ASR シリーズ ルータ	複合プログラマブル論理デバイス（CPLD）イメージのアップグレードはサポートされていません。
Cisco ISR シリーズ ルータ	CPLD イメージのアップグレードはサポートされていません。

ステップ 6 推奨イメージを標準としてマークします。

詳細については、ソフトウェアイメージをスタンダードとしてマークする （646 ページ）を参照してください。

ステップ 7 推奨のソフトウェアイメージをネットワーク内のデバイスにプロビジョニングします。

詳細については、ソフトウェアイメージのプロビジョニング （653 ページ）を参照してください。

ソフトウェアイメージのインポート

Catalyst Center がエアギャップ環境に展開されている場合、またはクラウドにアクセスできない場合は、ローカルコンピュータまたは URL から、ソフトウェアイメージおよびソフトウェ

アイメージ更新プログラムをインポートできます。それ以外の場合は、cisco.com からソフトウェアイメージをダウンロードすることを推奨します。

インポートされたイメージは、特定のデバイスファミリに存在するさまざまなスーパーバイザに基づいて分類されます。異なるスーパーバイザによる分類では、Cisco Catalyst 9400 シリーズ ファミリのみがサポートされます。

FTP を使用して FTP サーバからイメージをインポートする場合は、FTP 標準を使用します。

```
ftp://username:password@ip_or_hostname/path
```

手順

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

ステップ 2 [Images] タブをクリックし、[Import images] をクリックします。

または、[Overview] タブをクリックし、[Image Update Tools] セクションの [Import Image] をクリックします。

ステップ 3 **[Import Image]** スライドインペインで、次の手順を実行してソフトウェアイメージをインポートします。

1. [Upload Option] で、画像のアップロード方法を指定します。

   次の表に、アップロードオプションを示します。

オプション	説明
Select from computer	ローカルのソフトウェアイメージまたはソフトウェアイメージの更新ファイルをアップロードします。
Enter URL	HTTP または FTP ソースからソフトウェアイメージまたはソフトウェアイメージの更新プログラムをインポートします。 （注） ソフトウェアイメージは、連邦情報処理標準（FIPS）に準拠しています。Catalyst Center で FIPS モードが有効になっている場合、URL からイメージをインポートすることはできません。コンピュータまたは cisco.com からイメージをインポートします。
Select ISSU compatibility matrix	ローカルの互換性マトリックスファイルをアップロードします。 In-Service Software Upgrade（ISSU）互換性マトリックスは、現在のソフトウェアバージョンと目的のソフトウェア バージョンの間の互換性に関する情報を提供し、アップグレードが問題なく続行できるようにします。

2. 選択したオプションに基づいてファイルをアップロードします。

選択内容	結果
[Select from computer] または [Select ISSU compatibility matrix]	次のいずれかを実行できます。 • ファイルをドラッグアンドドロップする、または • [Choose a file] をクリックし、ローカルに保存されているファイルを選択する
Enter URL	[Enter Image URL (http or ftp)] フィールドに、イメージ URL を入力します。

3. [Source] で、イメージのソースを指定します。

   インポートするイメージがサードパーティベンダー向けの場合、[Third party] を選択します。その後 [Application Type] を選択して、デバイスの [Family] を示し、[Vendor] を特定します。

   （注） イメージのアクティブ化およびイメージの更新機能は、サードパーティのデバイスではサポートされていません。

4. [Import] をクリックします。

ステップ 4 [Show Tasks] をクリックして、イメージが正常にインポートされたことを確認します。

SMU をインポートした場合、Catalyst Center は自動的に SMU を適切なソフトウェアイメージに適用します。SMU を表示するには、[All available images] テーブルに戻り、SMU でイメージの行を展開します。

（注） Catalyst Center では、FMC によって管理される FTD デバイスのソフトウェアイメージをインポートすることはできません。インベントリに追加した FMC が [Managed] 状態になった場合は、[Software Image Management] ページに移動し、[Images] をクリックし、テーブル内の関連するハイパーリンクされた製品ファミリ名をクリックして、FMC で使用可能なソフトウェアイメージを表示します。

デバイスファミリに対するソフトウェアイメージの割り当ての管理

ローカルコンピュータまたは URL（cisco.com を除く）からソフトウェアイメージをインポートした後、使用可能なデバイスファミリに割り当てまたは再割り当てすることができます。インポートしたイメージは、いつでも複数のデバイスに割り当てることができます。

始める前に

ローカルコンピュータまたは URL（cisco.com を除く）からソフトウェアイメージをインポートしました。詳細については、ソフトウェアイメージのインポート（638ページ）を参照してください。

手順

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

ステップ 2 [Images] をクリックします。

ステップ 3 **[Show imported images]** をクリックします。

ステップ 4 この表の手順を使用して、インポートしたイメージを管理します。

実行する操作	結果
インポートしたイメージの割り当て	**1.** 対応するイメージ名の行の [Assign] をクリックします。 **2.** [Assign Device Family] スライドインペインで、[Cisco Devices Series] または [All Device Series] をクリックします。 [All Device Series] で、[Select a device type] ドロップダウンリストを使用して、デバイスタイプでテーブルをフィルタ処理できます。 （注） [Cisco Devices Series] には、インターネット接続がある場合にのみデバイスシリーズの情報が表示されます。 **3.** ソフトウェアイメージを割り当てるデバイスシリーズのチェックボックスをオンにします。 [Device Series] チェックボックスをオンにして、テーブル内のすべてのデバイスシリーズを選択できます。 **4.** デバイスシリーズがサイトに割り当てられていない場合は、[Select Site] をクリックし、[Select Site] ダイアログボックスで適切なサイトを選択して [Select] をクリックします。 **5.** [**Assign**] をクリックします。 （注） • デバイスシリーズがサイトに割り当てられていない場合、[Assign] は無効になります。 • Cisco.com クレデンシャルが設定されていない場合は、**[System]** > **[Settings]** > **[Cisco.com Credentials]**の順に選択して、クレデンシャルを指定します。

実行する操作	結果
インポートしたイメージの再割り当て	1. 対応するイメージ名の行の [Edit] をクリックします。 2. [Assign Device Family] スライドインペインで、[Cisco Devices Series] または [All Device Series] をクリックします。 3. ソフトウェアイメージを再割り当てするデバイスシリーズのチェックボックスをオンにします。 4. [Select Sites] をクリックします。 5. [Select Site] ダイアログボックスで、このデバイスファミリのサイト割り当てを更新し、[Select] をクリックします。 6. [**Assign**] をクリックします。

イメージ更新のスケジュール

選択したデバイスの特定の日時にソフトウェアイメージの更新をスケジュールするには、次の手順を実行します。

手順

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

ステップ 2 [Images] タブをクリックします。アップグレードするイメージを選択し、そのイメージを標準としてマークします。イメージをマークするには、ソフトウェアイメージをスタンダードとしてマークする （646 ページ） を参照してください。

ステップ 3 [Devices] タブで、イメージを使用して更新する必要があるデバイスを選択し、[Update Devices] をクリックします。

または、[Overview] タブに移動し、[Image Update Tools] セクションの [Schedule Update] をクリックします。[Image Upgrade] ワークフローにリダイレクトされます。

ステップ 4 [イメージの更新（Image Update）] ウィンドウが開き、イメージ更新のスケジュール手順が表示されます。

ステップ 5 [タスク名（Task Name）] ウィンドウで、スケジュールされた更新タスクの一意の名前を入力し、[次へ（Next）] をクリックします。

ステップ 6 [Select Devices] ウィンドウで、左側のパネルからデバイスの場所を選択します。[Devices] セクションで、イメージの更新をスケジュールするデバイスのチェックボックスをオンにして、 [Next]をクリックします。

（注） デバイスの事前チェックが成功すると、[Software Image] 列の [Outdated] リンクに緑色のチェックマークが付きます。デバイスのアップグレードを準備するための事前チェックでいずれかに失敗した場合、[Outdated] リンクのチェックマークが赤色に変わり、そのデバイスのソフトウェアイメージを更新できなくなります。先に進む前に [Outdated] リンクをクリックし、エラーを修正します。「デバイスのアップグレードの準備の事前チェックリスト」を参照してください。

ステップ 7 [Software Distribution Checks] ウィンドウで、ソフトウェア配布の事前チェックと事後チェックを有効にして、チェック順序を選択します。配布チェックを選択したら、[Next] をクリックします。

（注） 外部イメージ配信サーバをネットワーク階層に関連付けた場合、ネットワーク階層下のすべてのデバイスにイメージ配信サーバからイメージが配信されます。サイトへのイメージ配信サーバーの追加 （653 ページ）を参照してください。

現在のワークフローで実行する検証ツールを選択する、または新しいカスタムチェックを追加するには、次の手順を実行します。

a) 情報アイコンにマウスポインタを合わせると、検証に使用される検証基準と CLI コマンドが表示されます。
b) トグルボタンをクリックして、現在のワークフローで実行しない検証ツールをオフにします。
c) （任意）新しいカスタム事前チェックおよび事後チェックを追加するには、次の手順を実行します。

1. [Add a Custom Check] をクリックして、[New Custom Check] ウィンドウを開きます。
2. カスタムチェックの名前を [Name] に入力します。
3. [When] ドロップダウンリストで、[pre] か [post] またはその両方を選択します。
4. [Select a Test Device] ドロップダウンリストから、チェックを実行するデバイスを選択します。
5. [Open Command Runner] をクリックし、CLI コマンドを入力します。
6. [Add Known Command-Patterns to Ignore During Checks] を展開し、チェックで一致した出力を無視するために使用するコマンドパターンを追加します。

   コマンドパターンを追加するには、次の手順を実行します。

   - 新しいパターンを作成するには、目的の名前と文字列またはパターンを入力します。
   - 既存のパターンを使用するには、[Most Commonly Used Patterns] をクリックし、目的のパターンを選択して、[Add Selected] をクリックします。
   - [Test All Patterns] をクリックします。

7. [Additional Criteria] 領域を展開します。

   [Operation] ドロップダウンリストから、[Distribution]、[Activation]、または両方を選択します。

8. [Device Series] ドロップダウンリストから、目的のデバイスシリーズを選択し、[Save] をクリックします。

ステップ 8 [Software Activation Checks] ウィンドウで、ソフトウェアアクティベーションの事前チェックと事後チェックを有効にして、チェック順序を選択します。アクティベーション チェックを選択したら、 [Next] をクリックします。

ステップ 9 [Device Activation Order] ウィンドウでは、フィルタを使用してデバイスを並べ替え、アクティベーションの順序を並列または逐次から選べます。デバイスを並べ変えた後、また順番に戻すことができます。[Next] をクリックします。

ステップ 10 [Schedule Task and Clean Up] ウィンドウで、次のタスクをスケジュール設定します。

- [Software Distribution] セクションで、ソフトウェア配布のチェックを有効にします。
- [Software Activation] セクションで、[Now] または [Later] を選択して更新をスケジュール設定します。[Later] を選択した場合は、開始日時を設定し、更新を開始するタイムゾーンを選択します。デフォルトでは、選択したサイトのタイムゾーンに設定されます。
- [Initiate Flash Cleanup after Activation] チェックボックスをオンにして、実行中のイメージのみを保存し、デバイスに保存されている以前のイメージをすべて削除します。

設定を構成したら、[Next] をクリックします。

ステップ 11 [Summary] ウィンドウに、スケジュールされた更新の概要データが表示されます。詳細を確認し、必要に応じて [Edit] をクリックして設定を変更できます。[Submit] をクリックします。

デバイスのソフトウェアイメージをインストールモードでアップロードする

[ソフトウェアイメージ管理（Software Image Management）]ページでは、ソフトウェアイメージがインストールモードの状態として表示されることがあります。デバイスがインストールモードの場合、Catalyst Center はソフトウェアイメージをデバイスから直接アップロードできません。デバイスがインストールモードのときは、最初に手動でソフトウェアイメージを Catalyst Center リポジトリにアップロードしてから、イメージを標準としてマーキングします。

手順

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

ステップ 2 [Images] をクリックします。

ステップ 3 [製品ファミリ名（Product Family Name）] で、ハイパーリンクが設定されている製品ファミリ名をクリックして、使用可能なイメージを表示します。

ステップ 4 [イメージ名（Image Name）] で、[インストールモード（Install Mode）] で実行中のデバイスのソフトウェアイメージを検索します。

ステップ 5 [イメージの詳細情報なし（Image details not available）] ドロップダウンリストから、[一致するイメージのインポート（Import matching image）] を選択します。

ステップ 6 [イメージのインポート（Import Image）] スライドインペインで、次の手順を実行してイメージをインポートします。

1. [Upload Option] で、画像のアップロード方法を指定します。

   次の表に、アップロードオプションを示します。

オプション	説明
Select from computer	ローカルのソフトウェアイメージまたはソフトウェアイメージの更新ファイルをアップロードします。
Enter URL	HTTP または FTP ソースからソフトウェアイメージまたはソフトウェアイメージの更新プログラムをインポートします。 （注） ソフトウェアイメージは、連邦情報処理標準（FIPS）に準拠しています。Catalyst Center で FIPS モードが有効になっている場合、URL からイメージをインポートすることはできません。コンピュータまたは cisco.com からイメージをインポートします。
Select ISSU compatibility matrix	ローカルの互換性マトリックスファイルをアップロードします。

2. 選択したオプションに基づいてファイルをアップロードします。

選択内容	結果
[コンピュータから選択（Select from computer）] または [ISSU互換性マトリックスを選択（Select ISSU compatibility matrix）]	次のいずれかを実行できます。 • ファイルをドラッグアンドドロップする、または • [Choose a file] をクリックし、ローカルに保存されているファイルを選択する
Enter URL	[Enter Image URL (http or ftp)] フィールドに、イメージ URL を入力します。

3. [Source] で、イメージのソースを指定します。

   インポートするイメージがサードパーティベンダー向けの場合、[Third party] を選択します。その後 [Application Type] を選択して、デバイスの [Family] を示し、[Vendor] を特定します。

（注） イメージのアクティブ化およびイメージの更新機能は、サードパーティのデバイスではサポートされていません。

4. [Import] をクリックします。

ステップ 7 **[タスクの表示（Show task）]** をクリックして、インポートしたソフトウェアイメージが、正常にインポートされて Catalyst Center リポジトリに追加されたことを示す緑色であることを確認します。

ステップ 8 [Refresh] をクリックします。

デバイスファミリとその利用可能なイメージの ページが更新されます。Catalyst Center にソフトウェアイメージが表示されます。

標準ソフトウェアイメージについて

Catalyst Center では、ソフトウェアイメージと SMU を標準として指定できます。標準ソフトウェアイメージや SMU は、特定のデバイスタイプのコンプライアンス要件を満たす検証済みのイメージです。ソフトウェアイメージや SMU を標準として指定すると、反復的な設定変更の必要がなくなって時間が節約され、デバイス間の一貫性が確保されます。標準化されたイメージを作成するために、イメージと対応する SMU を標準として指定できます。特定のデバイスロールの標準イメージを指定することもできます。たとえば、Cisco 4431 シリーズ サービス統合型ルータデバイスファミリのイメージがある場合、アクセスロールだけを持つ Cisco 4431 デバイスに対する標準イメージを追加で指定できます。

対応するイメージも標準としてマークされていない限り、SMU を標準としてマークすることはできません。

ソフトウェアイメージをスタンダードとしてマークする

デバイスファミリまたは特定のデバイスロールのソフトウェアイメージを、スタンダードとしてマークできます。デバイスロールは、ネットワーク内での役目と配置に従ってデバイスを識別およびグループ分けします。

手順

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

ステップ 2 [Devices] をクリックします。

または、[Images] をクリックすることもできます。

ステップ 3 **[Device Family]** で、ソフトウェアイメージをスタンダードとしてマークする、ハイパーリンクされたデバイスファミリをクリックします。

または、[Images] を選択した場合は、ソフトウェアイメージをスタンダードとしてマークする [Product Family Name] の下で、ハイパーリンクされた製品ファミリをクリックします。

ステップ 4 条件の有無にかかわらず、ソフトウェアイメージをスタンダードとしてマークします。

次のテーブルを使用し、イメージが Catalyst Center リポジトリにアップロードされているかどうかに基づいて、イメージをダウンロードしてスタンダードとしてマークします。

ソフトウェアイメージの状態	実行する操作	結果
Catalyst Center リポジトリにアップロードされている	条件の有無にかかわらず、イメージをスタンダードとしてマークする	**1.** [Image Name] で、スタンダードとしてマークするイメージを見つけます。 **2.** イメージの対応する [Downloaded] ドロップダウンリストから、[Mark as standard] または [Mark as standard with conditions] を選択します。 **3.** [Mark as standard] スライドインペインで、必要に応じて、イメージをデバイスロール、デバイスタグ、または両方に割り当てるための詳細設定を行います。次に、[Confirm] をクリックします。 • [Device role]：ドロップダウンリストでロールを選択します。 • [Device tags]：ドロップダウンリストからデバイスタグのチェックボックスをオンにします。
Catalyst Center リポジトリにアップロードされていない	画像をダウンロードしてスタンダードとしてマークする	**1.** [Image Name] で、ダウンロードしてスタンダードとしてマークするイメージを見つけます。 **2.** イメージの対応する [Available for download] ドロップダウンリストから、[Mark as standard] を選択します。 **3.** [Mark as standard] スライドインペインで、[Confirm] をクリックします。 システムは自動的にイメージをダウンロードして、そのイメージをスタンダードとしてマークします。[Actions] にソフトウェアイメージのダウンロード進行中バーが表示されます。この処理には、しばらく時間がかかる場合があります。 （注） デバイスからソフトウェアイメージをインポートすることはできません。

ソフトウェアイメージの状態	実行する操作	結果
Catalyst Center リポジトリにアップロードされていない	イメージのダウンロードのみ	**1.** [Image Name] で、スタンダードとしてマークするイメージを見つけます。 **2.** イメージの対応する [Available for download] ドロップダウンリストから、[Download from Cisco.com] を選択します。 **3.** [Download Image] ダイアログボックスで、[Save] をクリックします。 [Actions] にソフトウェアイメージのダウンロード進行中バーが表示されます。この処理には、しばらく時間がかかる場合があります。 （注） デバイスからソフトウェアイメージをインポートすることはできません。

（注） イメージのダウンロードが失敗した場合は、[Show task] をクリックして [Recent Tasks] スライドインペインを表示します。[Task Status] ドロップダウンリストから [Failed] を選択します。[See why?] をクリックして失敗の詳細を表示します。

ステップ 5 スタンダードイメージのアドオンをダウンロードする場合は、次の手順を実行します。

1. [Image Name] で、アドオンを含むソフトウェアイメージを見つけ、そのイメージがスタンダードとしてマークされていることを確認します。

（注）
- ダウンロードするアドオンを含むソフトウェアイメージがスタンダードとしてマークされていない場合、まずそのイメージをスタンダードとしてマークする必要があります。
- [Add-ons] 列には、各ソフトウェアイメージのアドオンの数が一覧表示されます。

2. スタンダードイメージの行を展開します。

   アドオンは、展開されたイメージの行に表示されます。

3. そのアドオンの対応する [Available for download] ドロップダウンリストから、[Download from Cisco.com] を選択します。

（注）
- サブパッケージはダウンロードのみ可能です。
- 基本イメージ用の SMU、APSP、APDP、および PSIRT SMU のアップグレードがダウンロード可能であり、スタンダードとしてマークできます。

4. [Download Image] ダイアログボックスで、[Save] をクリックします。

   アドオンを使用してイメージの行を再展開し、[Actions] の下に進行状況スピナーを表示します。この処理には、しばらく時間がかかる場合があります。ダウンロードが完了すると、[Actions] の下に [Downloaded] と表示されます。

標準ソフトウェアイメージの管理

条件の有無にかかわらず標準としてマークされるソフトウェアイメージを管理できます。

始める前に

ソフトウェアイメージは、条件の有無にかからわず標準としてマークする必要があります。詳細については、ソフトウェアイメージをスタンダードとしてマークする（646ページ）を参照してください。

手順

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

ステップ 2 [Devices] をクリックします。

ステップ 3 [デバイスファミリ（Device Family）] で、標準イメージを管理する、ハイパーリンクが設定されたデバイスファミリをクリックします。

ステップ 4 次の表を使用して、条件の有無にかかわらず標準イメージを管理します。

実行する操作	結果
条件の有無にかかわらず標準ソフトウェアイメージを編集する	**1.** [イメージ名（Image Name）] で標準イメージを特定します。 **2.** 対象イメージの [標準としてマーク（Marked as standard）] または [条件付きで標準としてマーク（Conditionally marked as standard）] ドロップダウンリストから、[標準条件を編集（Edit standard conditions）] を選択します。 **3.** [標準としてマーク（Mark as standard）] スライドインペインで、詳細設定を更新してから [確認（Confirm）] をクリックします。 • [Device role]：ドロップダウンリストでロールを選択します。 • [デバイスタグ（Device tags）]：ドロップダウンリストからデバイスタグのチェックボックスをオンまたはオフにします。
条件なしでソフトウェアイメージの標準としてのマークを解除する	**1.** [イメージ名（Image Name）] で標準イメージを特定します。 **2.** 対象イメージの [標準としてマーク（Marked as standard）] ドロップダウンリストから、[標準を解除（Remove standard）] を選択します。 これでイメージはダウンロードされた状態になります。 （注） イメージが条件付きで標準としてマークされている場合は、最初に条件なしで標準としてマークする（つまり、条件を削除する）必要があります。その後、標準としてのマークを解除できます。
標準ソフトウェアイメージを置き換える	条件の有無にかかわらず、別のソフトウェアイメージを標準としてマークすると、現在の標準イメージが新しいイメージに置き換えられます。詳細については、ソフトウェアイメージをスタンダードとしてマークする （646 ページ）を参照してください。

イメージ配信サーバーの設定

イメージ配信サーバーは、ソフトウェアイメージの保管と配信に役立ちます。ソフトウェアイメージを配信するように最大3つの外部イメージ配信サーバーを設定できます。また、新しく追加されたイメージ配信サーバーに 1 つ以上のプロトコルを設定できます。

手順

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

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

[Image Distribution Servers] テーブルには、イメージ配信サーバーのホスト、ユーザー名、SFTP、SCP、および接続に関する詳細が表示されます。

ステップ 3 [Add] をクリックして新しいイメージ配信サーバを追加します。

[Add a New Image Distribution Server]スライドインペイン が表示されます。

ステップ 4 イメージ配信サーバーの次の項目を設定します。

- [Host]：イメージ配信サーバーのホスト名または IP アドレスを入力します。
- [Root Location] ：ファイル転送用の作業ルートディレクトリ。

（注） Cisco AireOS ワイヤレスコントローラ の場合、設定されたパスが 16 文字を超えると、イメージの配信は失敗します。

- [Username]：イメージ配信サーバーへのログインに使用されるユーザー名を入力します。ユーザー名には、サーバーの作業ルートディレクトリに対する読み取り/書き込み権限が必要です。
- [Password]：イメージ配信サーバーへのログインに使用されるパスワード。
- [ポート番号]：イメージ配信サーバーが実行されているポート番号を入力します。

ステップ 5 [Save] をクリックします。

ステップ 6 一部のワイヤレスコントローラの旧バージョンのソフトウェアでは、SFTPの暗号方式として弱い暗号方式（SHA1 ベースの暗号など）しかサポートされていないため、Catalyst Center でソフトウェアイメージの管理やワイヤレスアシュアランスの設定を行うには、ワイヤレスコントローラからの SFTP 接続に対して SFTP 互換モードを有効にする必要があります。Catalyst Center の SFTP サーバーでは、弱い暗号方式のサポートを最大90日間まで一時的に有効にすることができます。弱い暗号を許可するには、以下を実行します。

a) SFTP サーバーの IP アドレスの横にある [i] アイコンにカーソルを合わせ、[Click here] をクリックします。

b) [Compatibility Mode] スライドインペインで [Compatibility Mode] チェックボックスをオンにして期間（1 分～ 90 日）を入力します。
c) [Save] をクリックします。

ステップ 7 （任意） 設定を編集するには、対応するイメージ配信サーバーの横にある [Edit] アイコンをクリックし、必要な変更を行って [Save] をクリックします。

ステップ 8 （任意） イメージ配信サーバーを削除するには、イメージ配信サーバーの横にある [Delete] アイコンをクリックし、[Delete] をクリックします。

イメージ配信サーバーのプロトコル順序の変更

イメージ配信サーバーのプロトコル順序を変更できます。プロトコルの順序は、イメージ配信サーバーで検証チェックを実行するのに役立ちます。デフォルトでは、ソフトウェアイメージはプロトコル順序の最初のプロトコルを使用して配信されます。

手順

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

ステップ 2 [Image Distribution Servers] ウィンドウで、[Preferences] タブをクリックします。

デフォルトのプロトコル順序が表示されます。

ステップ 3 [Protocol Order] エリアで、[On/Off] プロトコルトグルボタンをクリックしてプロトコルを有効または無効にします。

- HTTPS：Catalyst Center はデバイスにログインし、Catalyst Center 認証局で TLS 1.2 を使用して **copy https://<Catalyst-Center-IP-address>/<Catalyst-Center-image-path>** コマンドを使用します。問題については、『Troubleshoot HTTPS Error in Cisco Catalyst Center for SWIM』を参照してください。
- SCP：Catalyst Center はデバイスにログインし、**SCP://sftpuser:randomised-password@<Catalyst-Center-IP-address>/<Catalyst-Center-image-path>** コマンドを使用します。問題が発生した場合は、TAC ケースをオープンする必要があります。
- SFTP—Catalyst Center はデバイスにログインし、「**SFTP://sftpuser:randomised-password@<Catalyst-Center-IP-address>/<Catalyst-Center-image-path>**」コマンドを使用します。問題が発生した場合は、TAC ケースをオープンする必要があります。

（注） イメージを配信するには HTTPS または SCP プロトコルを有効にする必要があります。レガシーデバイスをサポートするには、すべてのプロトコル順序で SFTP プロトコルを有効にする必要があります。

HTTPS プロトコルが無効になっているか、HTTPS プロトコル使用時にイメージ配信に失敗した場合、ソフトウェアイメージは SCP プロトコルを使用して配信されます。

ステップ 4 プロトコルをドラッグアンドドロップしてプロトコルの順序を変更します。
ステップ 5 [Save] をクリックします。

サイトへのイメージ配信サーバーの追加

地理的に異なる地域にある SFTP サーバを、サイト、ビルディング、およびフロアに関連付けることができます。ネットワーク階層内のすべてのデバイスは、ネットワークのアップグレードの際、関連付けられたイメージ配信サーバを使用します。

始める前に

イメージ配信サーバを設定する必要があります。『イメージ配信サーバーの設定 （651 ページ）』を参照してください。

手順

ステップ 1 メインメニューから次を選択します。 **[Design]** > **[Network Settings]** > **[Servers]** の順に選択します。
ステップ 2 [Image Distribution] 領域を展開して、イメージ配信サーバーとして機能する SFTP サーバーを選択します。
ステップ 3 [イメージ配信サーバーの追加（Add image distribution servers）] チェックボックスをオンにして、フィールドを表示します。
ステップ 4 [Primary] ドロップダウンリストから、プライマリとして設定するイメージ配信サーバを選択します。
ステップ 5 + アイコンをクリックして、[Secondary] ドロップダウンリストからセカンダリとして設定するイメージ配信サーバを選択します。
ステップ 6 [Save] をクリックします。

ソフトウェアイメージのプロビジョニング

Catalyst Center は、各デバイスのソフトウェアイメージを、その固有のデバイスタイプに対してスタンダードと指定したイメージと比較します。ソフトウェアイメージとスタンダードイメージに違いがある場合、Catalyst Center はデバイスのソフトウェアイメージを無効とします。この場合、古いソフトウェアイメージを更新できます。

ソフトウェアイメージをデバイスにプッシュする前に、Catalyst Center はデバイス管理ステータスの確認、ディスク容量の確認など、デバイスのアップグレード準備の事前チェックを実行します。事前チェックに失敗した場合は、ソフトウェアイメージのアップグレードを実行できません。デバイスのソフトウェアイメージをアップグレードする前に、問題を修正する必要があります。

すべての事前チェックに成功したら、新しいイメージをデバイスに配信（コピー）し、有効化（新しいイメージを実行中のイメージにすることが）できます。新しいイメージの有効化には、デバイスの再起動が必要です。再起動によって現在のネットワークアクティビティが中断される可能性があるため、後でプロセスをスケジュールすることができます。

ソフトウェアイメージが正常にアップグレードされると、Catalyst Center は CPU 使用率、ルートサマリの確認などのアップグレードの事後チェックを実行し、ネットワークの状態が変更されていないことを確認します。

始める前に

- デバイスタイプに指定されたスタンダードイメージがあることを確認します。ソフトウェアイメージをスタンダードとしてマークする （646 ページ）を参照してください。
- ソフトウェアイメージをすぐにアップグレードするには、[Automation Events for ITSM (ServiceNow)] バンドルを無効にする必要があります。バンドルにアクセスするには、**[Platform]** > **[Manage]** > **[Bundles]** > **[Automation Events for ITSM (ServiceNow)]** の順に選択します。

手順

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

ステップ 2 [Images] タブをクリックします。アップグレードするイメージを選択し、そのイメージを標準としてマークします。イメージをマークするには、ソフトウェアイメージをスタンダードとしてマークする （646 ページ） を参照してください。

ステップ 3 [Devices] タブで、イメージを使用して更新する必要があるデバイスを選択し、[Update Devices] をクリックします。

または、[Overview] タブに移動し、[Image Update Tools] セクションの [Schedule Update] をクリックします。[Image Upgrade] ワークフローにリダイレクトされます。

ステップ 4 [Image Update] ウィンドウが開き、イメージ更新の設定手順が表示されます。

ステップ 5 [Task Name] ウィンドウで、更新タスクの一意の名前を入力し、[Next] をクリックします。

ステップ 6 [Select Devices] ウィンドウで、左側のパネルからデバイスの場所を選択します。[Devices] セクションで、イメージの更新をスケジュールするデバイスのチェックボックスをオンにして、 [Next]をクリックします。

（注） デバイスの事前チェックが成功すると、[Software Image] 列の [Outdated] リンクに緑色のチェックマークが付きます。デバイスのアップグレードを準備するための事前チェックでいずれかに失敗した場合、[Outdated] リンクのチェックマークが赤色に変わり、そのデバイスのソフトウェアイメージを更新できなくなります。先に進む前に [Outdated] リンクをクリックし、エラーを修正します。「デバイスのアップグレードの準備の事前チェックリスト」を参照してください。

ステップ 7 [Software Distribution Checks] ウィンドウで、ソフトウェア配布の事前チェックと事後チェックを有効にして、チェック順序を選択します。配布チェックを選択したら、[Next] をクリックします。

（注） 外部イメージ配信サーバをネットワーク階層に関連付けた場合、ネットワーク階層下のすべてのデバイスにイメージ配信サーバからイメージが配信されます。サイトへのイメージ配信サーバーの追加 （653 ページ）を参照してください。

現在のワークフローで実行する検証ツールを選択する、または新しいカスタムチェックを追加するには、次の手順を実行します。

a) 情報アイコンにマウスポインタを合わせると、検証に使用される検証基準と CLI コマンドが表示されます。
b) トグルボタンをクリックして、現在のワークフローで実行しない検証ツールをオフにします。
c) （任意）新しいカスタム事前チェックおよび事後チェックを追加するには、次の手順を実行します。

1. [Add a Custom Check] をクリックして、[New Custom Check] ウィンドウを開きます。
2. カスタムチェックの名前を [Name] に入力します。
3. [When] ドロップダウンリストで、[pre] か [post] またはその両方を選択します。
4. [Select a Test Device] ドロップダウンリストから、チェックを実行するデバイスを選択します。
5. [Open Command Runner] をクリックし、CLI コマンドを入力します。
6. [Add Known Command-Patterns to Ignore During Checks] を展開し、チェックで一致した出力を無視するために使用するコマンドパターンを追加します。

   コマンドパターンを追加するには、次の手順を実行します。

   - 新しいパターンを作成するには、目的の名前と文字列またはパターンを入力します。
   - 既存のパターンを使用するには、[Most Commonly Used Patterns] をクリックし、目的のパターンを選択して、[Add Selected] をクリックします。
   - [Test All Patterns] をクリックします。

7. [Additional Criteria] 領域を展開します。

   [Operation] ドロップダウンリストから、[Distribution]、[Activation]、または両方を選択します。
8. [Device Series] ドロップダウンリストから、目的のデバイスシリーズを選択し、[Save] をクリックします。

ステップ 8 [Software Activation Checks] ウィンドウで、ソフトウェアアクティベーションの事前チェックと事後チェックを有効にして、チェック順序を選択します。アクティベーション チェックを選択したら、 [Next] をクリックします。

ステップ 9 [Device Activation Order] ウィンドウでは、フィルタを使用してデバイスを並べ替え、アクティベーションの順序を並列または逐次から選べます。デバイスを並べ変えた後、また順番に戻すことができます。[Next] をクリックします。

ステップ 10 [Schedule Task and Clean Up] ウィンドウで、次のタスクをスケジュール設定します。

- [Software Distribution] セクションで、ソフトウェア配布のチェックを有効にします。
- [Software Activation] セクションで、[Now] または [Later] を選択して更新をスケジュール設定します。[Later] を選択した場合は、開始日時を設定し、更新を開始するタイムゾーンを選択します。デフォルトでは、選択したサイトのタイムゾーンに設定されます。
- [Initiate Flash Cleanup after Activation] チェックボックスをオンにして、実行中のイメージのみを保存し、デバイスに保存されている以前のイメージをすべて削除します。

設定を構成したら、[Next] をクリックします。

ステップ 11 [Summary] ウィンドウに、スケジュールされた更新の概要データが表示されます。詳細を確認し、必要に応じて [Edit] をクリックして設定を変更できます。[Submit] をクリックします。

ISSU 互換性マトリックスのインポート

In-Service Software Upgrade（ISSU）は、サービスの中断なしで、または最小限に抑えて、デバイス上のイメージをアップグレードするプロセスです。ISSU は、長期リリース内または長期リリース間（17.3.x から 17.3.y や、17.3.x から 17.6.y など）でのみサポートされます。ISSU を使用してデバイスをアップグレードする際は、Catalyst Center でターゲットリリースに対応する ISSU 互換性マトリクスをダウンロードしてインポートできます。

手順

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

ステップ 2 [Images] タブをクリックし、[Import images] をクリックします。

または、[Overview] タブをクリックし、[Image Update Tools] セクションの [Import Image] をクリックします。

ステップ 3 **[イメージのインポート（Import Image）]** スライドインペインで、[ISSU互換性マトリックスの選択（Select ISSU compatibility matrix）] オプションボタンをクリックし、[ファイルの選択（Choose a file）] をクリックしてローカルに保存されている ISSU 互換性マトリックスファイルに移動します。

ステップ 4 [Import] をクリックします。

ステップ 5 [Show Tasks] をクリックして ISSU 互換性マトリクスファイルのインポートステータスを表示します。

（注） Catalyst Center 2.3.7 以降、互換性マトリックスファイルは、cisco.com で入手可能な ISSU 対応デバイスの標準タグ付きイメージと実行イメージに対して自動的にダウンロードされます。

ISSU または xFSU を使用したソフトウェアイメージのアップグレード

ISSU または xFSU を使用してデバイスをアップグレードすることを選択できます。ISSU は、デュアルスーパーバイザを備えたシャーシベースのスイッチ向けの設計となっており、ダウンタイムがほぼゼロのアップグレードを実現します。一方、xFSU は、Catalyst 9300 などのスタック可能なアクセススイッチに最適化されており、コントロールプレーンとデータプレーンのリロードを分離することでアップグレード中のダウンタイムを最小限に抑えます。

xFSU は、バージョン 17.18.2 以降を実行している Catalyst 9300 シリーズ デバイスでサポートされます。

始める前に

- ISSU または xFSU を使用してデバイスをアップグレードする前に、ISSU 互換性マトリックスファイルをインポートする必要があります。ISSU 互換性マトリックスのインポート（656 ページ）を参照してください。
- ソフトウェアイメージをすぐにアップグレードするには、[Automation Events for ITSM (ServiceNow)] バンドルを無効にする必要があります。バンドルにアクセスするには、**[Platform]** > **[Manage]** > **[Bundles]** > **[Automation Events for ITSM (ServiceNow)]** の順に選択します。

手順

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

ステップ 2 [Devices] タブで、イメージを使用して更新する必要があるデバイスを選択し、[Update Devices] をクリックします。

または、[Overview] タブに移動し、[Image Update Tools] セクションの [Schedule Update] をクリックします。[Image Upgrade] ワークフローにリダイレクトされます。

ステップ 3 [Image Update] ウィンドウが開き、イメージ更新の設定手順が表示されます。

ステップ 4 [Task Name] ウィンドウで、更新タスクの一意の名前を入力し、[Next] をクリックします。

ステップ 5 [Select Devices] ウィンドウで、左側のパネルからデバイスの場所を選択します。[Devices] セクションで、イメージの更新をスケジュールするデバイスのチェックボックスをオンにして、 [Next]をクリックします。

（注） デバイスの事前チェックが成功すると、[Software Image] 列の [Outdated] リンクに緑色のチェックマークが付きます。デバイスのアップグレードを準備するための事前チェックでいずれかに失敗した場合、[Outdated] リンクのチェックマークが赤色に変わり、そのデバイスのソフトウェアイメージを更新できなくなります。先に進む前に [Outdated] リンクをクリックし、エラーを修正します。「デバイスのアップグレードの準備の事前チェックリスト」を参照してください。

ステップ 6 [Software Distribution Checks] ウィンドウで、ソフトウェア配布の事前チェックと事後チェックを有効にして、チェック順序を選択します。配布チェックを選択したら、[Next] をクリックします。

（注） 外部イメージ配信サーバをネットワーク階層に関連付けた場合、ネットワーク階層下のすべてのデバイスにイメージ配信サーバからイメージが配信されます。サイトへのイメージ配信サーバーの追加 （653 ページ）を参照してください。

現在のワークフローで実行する検証ツールを選択する、または新しいカスタムチェックを追加するには、次の手順を実行します。

a) 情報アイコンにマウスポインタを合わせると、検証に使用される検証基準と CLI コマンドが表示されます。
b) トグルボタンをクリックして、現在のワークフローで実行しない検証ツールをオフにします。
c) （任意）新しいカスタム事前チェックおよび事後チェックを追加するには、次の手順を実行します。

1. [Add a Custom Check] をクリックして、[New Custom Check] ウィンドウを開きます。
2. カスタムチェックの名前を [Name] に入力します。
3. [When] ドロップダウンリストで、[pre] か [post] またはその両方を選択します。
4. [Select a Test Device] ドロップダウンリストから、チェックを実行するデバイスを選択します。
5. [Open Command Runner] をクリックし、CLI コマンドを入力します。
6. [Add Known Command-Patterns to Ignore During Checks] を展開し、チェックで一致した出力を無視するために使用するコマンドパターンを追加します。

   コマンドパターンを追加するには、次の手順を実行します。

   - 新しいパターンを作成するには、目的の名前と文字列またはパターンを入力します。
   - 既存のパターンを使用するには、[Most Commonly Used Patterns] をクリックし、目的のパターンを選択して、[Add Selected] をクリックします。
   - [Test All Patterns] をクリックします。

7. [Additional Criteria] 領域を展開します。

   [Operation] ドロップダウンリストから、[Distribution]、[Activation]、または両方を選択します。

8. [Device Series] ドロップダウンリストから、目的のデバイスシリーズを選択し、[Save] をクリックします。

ステップ 7 [Software Activation Checks] ウィンドウで、ソフトウェアアクティベーションの事前チェックと事後チェックを有効にして、チェック順序を選択します。[Next] をクリックします。

ステップ 8 [Device Activation Order] ウィンドウでは、フィルタを使用してデバイスを並べ替え、アクティベーションの順序を並列または逐次から選べます。デバイスを並べ変えた後、また順番に戻すことができます。

ステップ 9 ISSU でアップグレードする場合は、次の手順を実行します。

a) ISSU でアップグレードするデバイスを選択します。

（注） [イメージの更新（Update Image）] 列には ISSU 検証ステータスが表示されます。

- **オレンジ色で表示される ISSU**：選択したイメージに ISSU との互換性がないため、ISSU の検証に失敗しました。
- **灰色で表示される ISSU**：ISSU の検証が成功し、デバイスは ISSU をサポートしています。

b) [ISSU] ドロップダウンリストから [Enable ISSU Upgrade] を選択します。

c) [Next] をクリックします。

ステップ 10 xFSU でアップグレードする場合は、次の手順を実行します。

a) ISSU でアップグレードするデバイスを選択します。

（注） [イメージの更新（Update Image）] 列には XFSU 検証ステータスが表示されます。

- **オレンジ色で表示される xFSU**：選択したイメージに xFSU との互換性がないため、xFSU の検証に失敗しました。
- **グレーで表示される xFSU**：xFSU の検証が成功し、デバイスは xFSU をサポートしています。

b) [xFSU] ドロップダウンリストから [xFSUアップグレードの有効化（Enable xFSU Upgrade）] を選択します。

c) [Next] をクリックします。

ステップ 11 [Schedule Task and Clean Up] ウィンドウで、次のタスクをスケジュール設定します。

- [Software Distribution] セクションで、ソフトウェア配布のチェックを有効にします。
- [Software Activation] セクションで、[Now] または [Later] を選択して更新をスケジュール設定します。[Later] を選択した場合は、開始日時を設定し、更新を開始するタイムゾーンを選択します。デフォルトでは、選択したサイトのタイムゾーンに設定されます。

- [Initiate Flash Cleanup after Activation] チェックボックスをオンにして、実行中のイメージのみを保存し、デバイスに保存されている以前のイメージをすべて削除します。

設定を構成したら、[Next] をクリックします。

ステップ 12 [Summary] ウィンドウに、スケジュールされた更新の概要データが表示されます。詳細を確認し、必要に応じて [Edit] をクリックして設定を変更できます。[Submit] をクリックします。

デバイスのアップグレードの準備の事前チェックリスト

事前チェック	説明
ファイル転送のチェック	HTTPS と SCP を通じてデバイスに到達可能かどうかのチェック プロトコルのデフォルトの順序は、HTTPSが先で、SCP はその後です。 Catalyst Center が FQDN で設定されている場合、デバイスに関連付けられているネームサーバーが到達不能な場合、エラーメッセージが表示されます。
NTP クロックのチェック	デバイスの時間と Catalyst Center の時間を比較して、Catalyst Center 証明書が正常にインストールされていることを確認します。
フラッシュのチェック	アドオンを使用してスタンダードイメージにアップグレードするために必要なディスク容量を計算し、イメージを配信する前にフラッシュクリーンアップをプロアクティブに実行します。十分なディスク容量がない場合、警告またはエラー メッセージが返されます。自動フラッシュ クリーンアップでサポートされるデバイスとファイルの削除方法については、「自動フラッシュ クリーンアップ（Auto Flash cleanup）」を参照してください。
設定レジスタのチェック	設定レジスタの値を確認します。
暗号化 RSA チェック	RSA 証明書がインストールされているかどうかチェックします。
暗号化 TLS のチェック	デバイスが TLS 1.2 をサポートしているかどうかチェックします。
脆弱な暗号チェック	MD5 認証で追加された SNMP V3 ユーザーなどの脆弱な暗号を使用してデバイスが設定されているかどうかを確認します。ソフトウェアイメージバージョン 17.14 以降のデバイスでは、脆弱な暗号が原因でイメージのアップグレードがブロックされます。
IP ドメイン名のチェック	ドメイン名が設定されているかどうかチェックします。
スタートアップ設定のチェック	このデバイス用のスタートアップ設定があるかどうかを確認します。
NFVIS Flash のチェック	NFVIS デバイスでスタンダードイメージをアップグレードする準備ができているかどうかを確認します。
サービス契約のチェック	デバイスに有効なライセンスがあるかどうかを確認します。

事前チェック	説明
イメージの互換性チェック	スタンダードイメージがデバイスと互換性があるかどうかを確認します。
イメージバージョンのサポート	デバイスが互換性のあるスタンダードイメージのバージョンでタグ付けされているかどうかを確認します。タグ付けされたイメージのバージョンが互換性バージョンよりも低い場合、処理に失敗します。
ISSU の互換性	実行中のイメージとスタンダードイメージで一致する互換性マトリックスが使用可能かどうかを確認します。
Extended Fast Software Upgrade（xFSU）互換性チェック	デバイスは、現在の設定と状態に基づいて XFSU の適格性を自己評価し、レポートします。

イメージ更新ステータスの表示

手順

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

ステップ 2 [概要（Overview）] タブで、次の更新を確認できます。

- [更新（Updates）] : 失敗したイメージ更新、進行中のイメージ更新、成功したイメージ更新の数を示します。
- [イメージ更新ツール（Image Update Tools）] セクションで、[更新ステータスの確認（Check Update Status）] をクリックし、トリガーされるイメージ更新のステータスを確認します。[デバイスの更新（Devices Updates）] スライドインペインには、進行中の更新、待機中の更新、終了した更新、成功した更新、失敗した更新が表示されます。

  [今後のタスク（Upcoming Tasks）] をクリックし、スケジュールされた更新を表示します。
- [まだ送信されていないイメージ更新のフロー（Yet to be submitted Image Update flows）] セクションには、まだ送信されていない今後のタスクが表示されます。このセクションの省略記号アイコンをクリックすると、タスクを再開するのか削除するのかを選択できます。

ステップ 3 [デバイス（Devices）] タブで、チェックボックスをオンにしてタスクが失敗したデバイスを選択し、[再試行（Retry）] をクリックしてイメージの更新を再試行します。

ステップ 4 [更新（Updates）] タブには、失敗した、成功した、進行中、およびスケジュールが設定されている最近のイメージ更新の詳細が表示されます。タスクへのリンクをクリックすると、詳細情報を表示できます。

イメージ更新ワークフローの表示

手順

ステップ 1 メインメニューから次を選択します。、**[プロビジョニング（Provision）]** > **[ソフトウェアイメージ管理（Software Image Management）]**の順に選択します。[概要（Overview）] タブで、[イメージ更新ツール（Image Update Tools）] セクションの [更新のスケジュール（Schedule Update）] をクリックします。

または、**[ワークフロー（Workflows）]** > **[イメージの更新（Image Update）]** を選択することもできます。

ステップ 2 [タスク名（Task Name）] ウィンドウで、スケジュールされた更新タスクの一意の名前を入力し、[次へ（Next）] をクリックします。

ステップ 3 [Select Devices] ウィンドウで、左側のパネルからデバイスの場所を選択します。[Devices] セクションで、イメージの更新をスケジュールするデバイスのチェックボックスをオンにして、[Next]をクリックします。

（注） デバイスの事前チェックが成功すると、[Software Image] 列の [Outdated] リンクに緑色のチェックマークが付きます。デバイスのアップグレードを準備するための事前チェックでいずれかに失敗した場合、[Outdated] リンクのチェックマークが赤色に変わり、そのデバイスのソフトウェアイメージを更新できなくなります。先に進む前に [Outdated] リンクをクリックし、エラーを修正します。「デバイスのアップグレードの準備の事前チェックリスト」を参照してください。

ステップ 4 [Software Distribution Checks] ウィンドウで、ソフトウェア配布の事前チェックと事後チェックを有効にして、チェック順序を選択します。配布チェックを選択したら、[Next] をクリックします。

（注） 外部イメージ配信サーバをネットワーク階層に関連付けた場合、ネットワーク階層下のすべてのデバイスにイメージ配信サーバからイメージが配信されます。サイトへのイメージ配信サーバーの追加 （653 ページ）を参照してください。

現在のワークフローで実行する検証ツールを選択する、または新しいカスタムチェックを追加するには、次の手順を実行します。

a) 情報アイコンにマウスポインタを合わせると、検証に使用される検証基準と CLI コマンドが表示されます。
b) トグルボタンをクリックして、現在のワークフローで実行しない検証ツールをオフにします。
c) （任意）新しいカスタム事前チェックおよび事後チェックを追加するには、次の手順を実行します。

1. [Add a Custom Check] をクリックして、[New Custom Check] ウィンドウを開きます。
2. カスタムチェックの名前を [Name] に入力します。
3. [When] ドロップダウンリストで、[pre] か [post] またはその両方を選択します。

4. [Select a Test Device] ドロップダウンリストから、チェックを実行するデバイスを選択します。
5. [Open Command Runner] をクリックし、CLI コマンドを入力します。
6. [Add Known Command-Patterns to Ignore During Checks] を展開し、チェックで一致した出力を無視するために使用するコマンドパターンを追加します。

   コマンドパターンを追加するには、次の手順を実行します。

   - 新しいパターンを作成するには、目的の名前と文字列またはパターンを入力します。
   - 既存のパターンを使用するには、[Most Commonly Used Patterns] をクリックし、目的のパターンを選択して、[Add Selected] をクリックします。
   - [Test All Patterns] をクリックします。

7. [Additional Criteria] 領域を展開します。

   [Operation] ドロップダウンリストから、[Distribution]、[Activation]、または両方を選択します。
8. [Device Series] ドロップダウンリストから、目的のデバイスシリーズを選択し、[Save] をクリックします。

ステップ 5 [Software Activation Checks] ウィンドウで、ソフトウェア アクティベーションの事前チェックと事後チェックを有効にして、チェック順序を選択します。アクティベーション チェックを選択したら、 [Next] をクリックします。

ステップ 6 [Device Activation Order] ウィンドウでは、フィルタを使用してデバイスを並べ替え、アクティベーションの順序を並列または逐次から選べます。デバイスを並べ変えた後、また順番に戻すことができます。[Next] をクリックします。

ステップ 7 [Schedule Task and Clean Up] ウィンドウで、次のタスクをスケジュール設定します。

- [Software Distribution] セクションで、ソフトウェア配布のチェックを有効にします。
- [Software Activation] セクションで、[Now] または [Later] を選択して更新をスケジュール設定します。[Later] を選択した場合は、開始日時を設定し、更新を開始するタイムゾーンを選択します。デフォルトでは、選択したサイトのタイムゾーンに設定されます。
- [Initiate Flash Cleanup after Activation] チェックボックスをオンにして、実行中のイメージのみを保存し、デバイスに保存されている以前のイメージをすべて削除します。

設定を構成したら、[Next] をクリックします。

ステップ 8 [Summary] ウィンドウに、スケジュールされた更新の概要データが表示されます。詳細を確認し、必要に応じて [Edit] をクリックして設定を変更できます。[Submit] をクリックします。

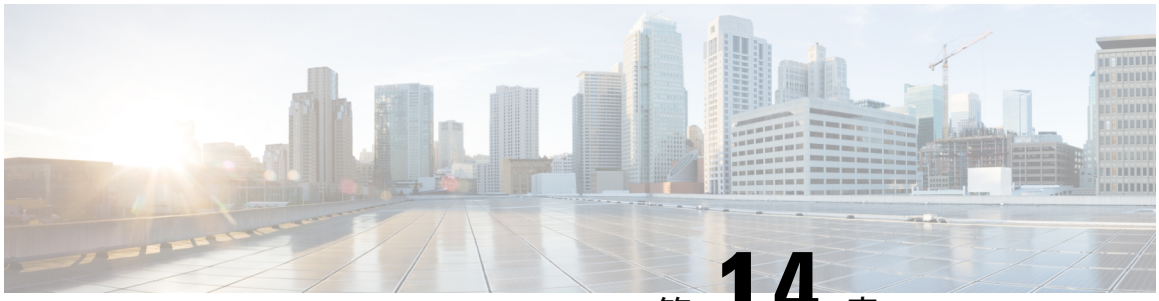
自動フラッシュクリーンアップ

デバイスのアップグレード準備の事前チェックの間、フラッシュのチェックにより、新しいイメージをコピーするための十分なスペースがデバイスにあるかどうかが確認されます。スペースが十分でない場合：

- **自動フラッシュクリーンアップをサポートしているデバイスの場合**：フラッシュのチェックが失敗し、警告メッセージが表示されます。このようなデバイスの場合、十分な容量を確保するために、イメージの配信プロセス中に自動クリーンアッププロセスが試行されます。自動フラッシュクリーンアップの一環として、Catalyst Center は未使用の .bin、.pkg、および .conf ファイルを特定し、デバイスに十分な空き容量ができるまでそれらのファイルの削除を繰り返します。イメージの配信はフラッシュ クリーンアップ後に試行されます。削除されたファイルは **[Activities]** > **[Audit Logs]** で確認できます。

（注） 自動フラッシュクリーンアップは、Nexus スイッチとワイヤレスコントローラを除くすべてのデバイスでサポートされています。

- **自動フラッシュクリーンアップをサポートしていないデバイスの場合**：フラッシュのチェックが失敗し、エラーメッセージが表示されます。イメージのアップグレードを開始する前に、デバイスのフラッシュからファイルを削除して、容量を確保できます。



第 14 章

ネットワークデバイスのコンプライアンス監査

- コンプライアンスの概要 （665 ページ）
- コンプライアンスカテゴリ （666 ページ）
- ネットワークのコンプライアンスの監視 （675 ページ）
- 設定コンプライアンスの管理 （676 ページ）
- コンプライアンス設定の構成 （678 ページ）
- コンプライアンスサマリーの表示 （680 ページ）
- 手動コンプライアンスの実行 （682 ページ）
- ネットワークデバイスのコンプライアンス監査レポートの生成 （683 ページ）
- コンプライアンス違反の確認 （683 ページ）
- デバイスのスタートアップ設定と実行中の設定の同期 （685 ページ）
- コンプライアンス違反の修正 （686 ページ）
- デバイスのアップグレード後のコンプライアンス動作 （687 ページ）
- CLI テンプレートコンプライアンスの制限事項 （688 ページ）

コンプライアンスの概要

Catalyst Center のコンプライアンスにより、管理者は、所定のポリシーや設定に対するネットワークの順守しているかどうかを効率的に監視、評価、および管理できます。最近の拡張機能により、コンプライアンス機能では、すべての管理対象デバイスにおけるコンプライアンス状況のネットワーク全体の包括的なビューを提供する強力な統合ダッシュボードが提供されるようになりました。

コンプライアンス ダッシュボードでは、次のことを行うことができます。

- **ネットワーク全体のコンプライアンスの概要**：非準拠のデバイスや未処理の違反に関する視覚的なインジケータを使用して、ネットワーク全体の正常性を単一のインターフェイスから表示します。

- **統合されたコンプライアンスカテゴリの確認**：コンプライアンスデータは、特定の問題に対処しやすくするために、構成コンプライアンス、ハードウェアおよびソフトウェアのコンプライアンス、脆弱性コンプライアンスの 3 つの主要カテゴリで構成されます。
- **コンプライアンスデータのフィルタ処理と分析**：サイト、デバイス、またはカテゴリ別にコンプライアンス結果をすばやくフィルタ処理し、ドリルダウンして、非準拠のデバイスと違反の特定の理由を確認できます。
- **一括コンプライアンス操作の実行**：ネットワーク全体または選択したデバイスの複数の違反を一度に効率的に確認または解除し、大規模なコンプライアンスワークフローを合理化します。
- **スタートアップ構成と実行中の構成の比較**：専用ビューを使用して、選択したデバイスのスタートアップ構成と実行中の構成を比較します。これは、保存されていない変更による不一致を特定して解決するのに役立ちます。

コンプライアンスチェックは次のように行うことができます。

- **自動**：最新の収集デバイスデータと Catalyst Center サービスからのリアルタイム通知を使用します。
- **手動**：管理者がオンデマンドでトリガーし、即時評価します。
- **定期実行**：毎日自動的に実行し、すべてのデバイスを少なくとも 7 日ごとに確認するジョブを使用します。

Catalyst Center は、アクティブに管理しているエンティティに対してのみコンプライアンスをレポートし、以前に管理していた構成要素の削除または変更にフラグを設定します。新しいアウトオブバンド追加は、Catalyst Center によって管理されるまで、コンプライアンスが報告されない場合があります。

コンプライアンスカテゴリ

コンプライアンスダッシュボードでは、デバイスのコンプライアンス違反を主に次の 3 つのタイプに分類します。

- [設定コンプライアンス（Configuration Compliance）]：ネットワーク設定やスタートアップ構成と実行中の構成の不一致など、意図した構成設定からの逸脱を追跡します。
- [ハードウェアおよびソフトウェアコンプライアンス（Hardware and Software Compliance）]：ソフトウェアイメージバージョンとハードウェアおよびモジュールの EOX（サポート終了/販売終了）ステータスを監視します。
- [脆弱性コンプライアンス（Vulnerability Compliance）]：優先順位の高いセキュリティアドバイザリの影響を受けたデバイスを強調表示します。これにより、優先順位を付けて修復できます。

コンプライアンスタイプ	コンプライアンスチェック	コンプライアンスステータス
設定コンプライアンス		
ネットワークプロファイル	Catalyst Center では、ネットワークプロファイルでインテント設定を定義して、そのインテントをデバイスにプッシュできます。もし、インバンド、アウトオブバンド、または他の Catalyst Center サービスによって引き起こされた変更により、任意の時点で違反が検出された場合、このチェックにより違反が特定され、評価され、フラグが立てられます。違反は、コンプライアンス サマリー ウィンドウの [Network Profiles] でユーザーに対して表示されます。 （注） ネットワーク プロファイル コンプライアンスは、ルータ、スイッチ、およびワイヤレスコントローラ に適用されます。	• [非準拠（Non-compliant）]：デバイスでプロファイルのインテント設定が実行されていません。 • [Compliant]：ネットワークプロファイルがデバイスに適用されており、同時に、Catalyst Center からプッシュされたデバイス設定がデバイスでアクティブに実行されています。 • [Error]：根本的なエラーのため、コンプライアンスがステータスを計算できませんでした。詳細については、エラーログを参照してください。
ネットワーク設定	Catalyst Center では、ネットワーク設定を使用してインテント設定を定義し、そのインテントをデバイスにプッシュできます。アウトオブバンドの変更またはその他の変更によって任意の時点で違反が検出された場合、コンプライアンスチェックによってそれを特定し、評価し、フラグを下げます。 [構成コンプライアンス（Configuration Compliance）] ウィンドウのポリシーで違反を表示できます。 （注） UI のアップグレード後、ネットワーク設定のコンプライアンスは 6 時間後にトリガーされます。	• [非準拠（Non-compliant）]：デバイスでインテント設定が実行されていません。 • [Compliant]：プッシュされたインテント設定が、デバイスでアクティブに実行されています。 • [NA]（該当なし）：ネットワーク設定を使用してデバイスが設定されていないか、デバイスがサイトに割り当てられていません。

コンプライアンスタイプ	コンプライアンスチェック	コンプライアンスステータス
ルールベースのコンプライアンス	Catalyst Center では、CLI 正規表現を使用してカスタム コンプライアンス ルールを定義できます。そのため、環境に固有の特定の構成パターンや値を柔軟に確認できます。	• [非準拠（Non-compliant）] : デバイスでインテント設定が実行されていません。 • [Compliant] : プッシュされたインテント設定が、デバイスでアクティブに実行されています。 • [NA]（該当なし）：ネットワーク設定を使用してデバイスが設定されていないか、デバイスがサイトに割り当てられていません。
スタートアップ設定と実行中の設定	このコンプライアンスチェックは、デバイスのスタートアップ設定と実行中の設定が同期しているかどうかを識別するために役立ちます。デバイスのスタートアップ設定と実行中の設定が同期していない場合は、コンプライアンスがトリガーされ、アウトオブバンド変更の詳細レポートが表示されます。スタートアップ設定と実行中の設定の比較に関するコンプライアンスは、アウトオブバンド変更の 2 分以内にトリガーされます。 （注） Syslog ベースの収集を機能させるには、**[Design]** > **[Network Settings]** > **[Telemetry]** > **[Syslogs]** ウィンドウで Catalyst Center を Syslog サーバーとして設定する必要があります。	• [非準拠（Non-compliant）] : スタートアップ設定と実行中の設定は同じではありません。詳細ビューには、スタートアップと実行中との違いか、または実行中と以前の実行中との違いが表示されます。 • [Compliant] : スタートアップ設定と実行中の設定は同じです。 • [NA (Not Applicable)] : このコンプライアンスタイプのデバイス（AireOS など）はサポートされていません。
ハードウェアおよびソフトウェアコンプライアンス		

コンプライアンスタイプ	コンプライアンスチェック	コンプライアンスステータス
ソフトウェアイメージ	このコンプライアンスチェックは、Catalyst Center のタグ付きのゴールデンイメージがデバイスで実行されているかどうかをネットワーク管理者が確認するために役立ちます。これにより、デバイスのゴールデンイメージと実行中のイメージとの違いがわかります。ソフトウェアイメージに変更があると、遅延なくすぐにコンプライアンスチェックがトリガーされます。	• [非準拠（Non-compliant）]：デバイスは、デバイスファミリのタグ付きのゴールデンイメージを実行していません。 • [Compliant]：デバイスは、デバイスファミリのタグ付きのゴールデンイメージを実行しています。 • [NA (Not Applicable)]：選択したデバイスファミリではゴールデンイメージを使用できません。
		ファブリックデバイスの場合： • [非準拠（Non-compliant）]：デバイスがデバイスファミリのタグ付きゴールデンイメージを実行していないか、ソフトウェアイメージの現在のバージョンにネットワークデバイスとの互換性がありません。 お使いのデバイスでサポートおよび推奨されるソフトウェアイメージのバージョンについては、*Cisco SD-Access* 互換性マトリックスを参照してください。 • [Compliant]：デバイスがデバイスファミリのタグ付きゴールデンイメージを実行しているか、ソフトウェアイメージの現在のバージョンにデバイスとの互換性があります。 • [NA (Not Applicable)]：選択したデバイスファミリではゴールデンイメージが使用できないか、デバイスがファブリックサイトに追加されていません。
	シスコのスイッチスタックの場合：Catalyst Center では、ネットワーク管理者は、タグ付きのゴールデンイメージがプライマリスイッチおよびスイッチスタックのメンバーで実行されているかどうかを確認できます。	

コンプライアンスタイプ	コンプライアンスチェック	コンプライアンスステータス
		• [非準拠（Non-compliant）]：タグ付きのゴールデンイメージが、プライマリスイッチおよびメンバースイッチで実行されていません。 また、ゴールデンタグ付けがデバイスに適用されず、メンバースイッチがプライマリスイッチと同じバージョンのイメージで実行されていない場合、デバイスは非準拠（Non-compliant）になります。 • [Compliant]：タグ付きのゴールデンイメージが、プライマリスイッチおよびメンバースイッチで実行されています。 また、ゴールデンタグ付けがデバイスに適用されず、メンバースイッチがプライマリスイッチと同じバージョンのイメージで実行されている場合、デバイスは準拠（Compliant）になります。 • [NA (Not Applicable)]：ゴールデンイメージがデバイスに適用されず、デバイスがスタック構成のスイッチではありません。
EoX - サポート終了	Catalyst Center では、EoX デバイスのハードウェア、ソフトウェア、およびモジュールのコンプライアンスステータスを確認できます。EoX コンプライアンスステータスは、[Compliance Summary] > [EoX - End of Life] タイルから確認できます。 [Inventory] ウィンドウの [EoX Status] 列で、デバイスの EoX ステータスを表示することもできます。 （注） EoX 機能へのアクセスを有効にするには、Catalyst Center ダッシュボードから「CX Cloud の接続への同意」（CX Cloud Consent to Connect）契約を承認します。	• [非準拠（Non-compliant）]：サポートの最終日を過ぎている場合、デバイスは非準拠の状態になります。 • [Compliant]：サポートの最終日まで十分な時間が残っている場合、デバイスは準拠の状態になります。 • [Compliant with Warning]：サポートの最終日が近づいている場合、デバイスは警告付き準拠の状態になります。
脆弱性に関するコンプライアンス		

コンプライアンスタイプ	コンプライアンスチェック	コンプライアンスステータス
重大なセキュリティ（PSIRT）	このコンプライアンスチェックでは、ネットワークデバイスが重大なセキュリティの脆弱性なしで実行されているかどうかを確認できます。	• [非準拠（Non-compliant）]：デバイスに重要なアドバイザリがあります。詳細レポートには、その他のさまざまな情報が表示されます。 • [Compliant]：デバイスに重大な脆弱性はありません。 • [NA (Not Applicable)]：Catalyst Center でネットワーク管理者がセキュリティ アドバイザリ スキャンを実行していないか、デバイスがサポートされていません。
インテントのコンプライアンス		
ファブリック（SDA） この機能はベータ版です。	ファブリック コンプライアンスは、ファブリック インテント違反（ファブリック関連の設定のアウトオブバンド変更など）の識別に役立ちます。 この機能はベータ段階であるため、ファブリックのコンプライアンスステータスは、デバイスの全体的なコンプライアンスステータスの決定には関与しません。	• [非準拠（Non-compliant）]：デバイスでインテント設定が実行されていません。 • [Compliant]：デバイスでインテント設定が実行されています。
SD-Accessのサポートされていない構成 この機能はベータ版です。	このコンプライアンスチェックにより、サポートされていない SD-Access 構成を特定できます。デバイスがファブリックサイトに追加されると、コンプライアンスチェックがすぐにトリガーされます。 非準拠デバイスのサポートされていない SD-Access 構成を表示するには、[Unsupported Configuration] をクリックします。[Unsupported Configuration] エリアで、サポートされていない SD-Access 構成が赤色で強調表示されます。 （注） ファブリックサイトに追加されていないデバイスの場合、このコンプライアンスチェックは使用されません。	• [非準拠（Non-compliant）]：デバイスは、SD-Access でサポートされていないいくつかの構成を実行しています。 • [Compliant]：デバイスは、SD-Access でサポートされている構成を実行しています。
ポリシー インテント コンプライアンス		

コンプライアンスタイプ	コンプライアンスチェック	コンプライアンスステータス
アプリケーションの可視性	Catalyst Center では、アプリケーション可視性インテントを作成して、CBAR および NBAR を介してデバイスにプロビジョニングできます。デバイスにインテント違反がある場合、このチェックにより、違反が識別されて、評価され、[Application Visibility] ウィンドウに準拠または非準拠として表示されます。 自動コンプライアンスチェックは、トラップの受信の 5 時間後に実行されるようにスケジュールされます。	• [非準拠（Non-compliant）]：デバイスで CBAR/NBAR 設定が実行されていません。 • [Compliant]：デバイスで CBAR/NBAR のインテント設定が実行されています。
モデル設定	このコンプライアンスチェックにより、ネットワーク管理者は、モデル設定の設計意図との不一致をチェックできます。違反は、[Compliance Summary] ウィンドウの [Network Profiles] に表示されます。	• [非準拠（Non-compliant）]：モデル設定の属性の実際の値と意図された値が一致しません。 • [Compliant]：モデル設計の属性が意図した値に一致します。

コンプライアンスタイプ	コンプライアンスチェック	コンプライアンスステータス
CLIテンプレート		• [非準拠（Non-compliant）]：CLI テンプレートとデバイスの実行コンフィギュレーションが一致しません。 • [Compliant]：CLI テンプレートとデバイスの実行コンフィギュレーションの間に不一致はありません。

コンプライアンスタイプ	コンプライアンスチェック	コンプライアンスステータス
	Catalyst Center ではネットワーク管理者は、CLI テンプレートをデバイスの実行コンフィギュレーションと比較できます。コンフィギュレーションの不一致にはフラグが立てられます。この不一致は、**[Compliance Summary]** ウィンドウの **[Network Profiles]** に表示されます。 フラグが設定された CLI コマンドを表示するには、次の手順を実行します。 1. **[Network Profile]** タイルをクリックします。 2. **[CLI Deviations]** エリアから、不一致を表示する CLI テンプレートを選択します。 3. CLI コマンドは **[Realize Template]**エリアに表示され、フラグが設定されたコマンドは赤で強調表示されます。 （注） コンプライアンスの問題を最小限に抑えるために CLI テンプレートで使用する必要があるベストプラクティスの一部を表示するには、**[View CLI Template Best Practices]** リンクをクリックします。 CLI テンプレート コンプライアンス用の実行コンフィギュレーションは、デバイスで使用可能な最新のアーカイブから取得されます。イベントベースのアーカイブは、トラップを受信してから更新されるまでに少なくとも 2 分かかります。正確な結果を得るには、設定の変更後にコンプライアンスを手動で実行する前に、少なくとも 2 分間待つことをお勧めします。 Syslog ベースの収集を機能させるには、**[Design]** > **[Network Settings]** > **[Telemetry]** > **[Syslogs]** ウィンドウで Catalyst Center を Syslog サーバーとして設定する必要があります。 （注） CLI テンプレート コンプライアンスにはいくつかの制限があります。「CLI テンプレート コンプライアンスの制限事項（688 ページ）」	

コンプライアンスタイプ	コンプライアンスチェック	コンプライアンスステータス
	を参照してください。	

ネットワークのコンプライアンスの監視

このダッシュボードを活用して、ネットワークのコンプライアンスステータスの概要を把握します。ダッシュボードは定期的に更新されますが、手動更新をトリガーして最新のデータを表示することもできます。

Before you begin

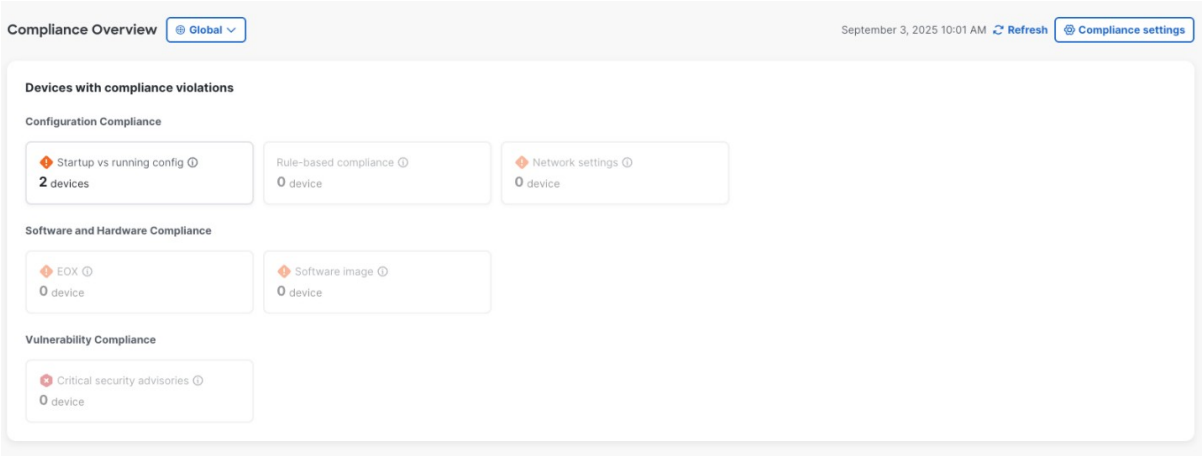
- 必要な管理者権限があることを確認してください。

ネットワークのコンプライアンスを監視するには、次の手順を実行します。

手順

ステップ 1 メインメニューから次を選択します。 **[ポリシー（Policy）] > [コンプライアンスの概要（Compliance Overview）]**。

図 *23 :* コンプライアンス概要ダッシュボード



ステップ 2 （オプション） [グローバル（Global）] セレクタをクリックして、特定のサイトでダッシュボードをフィルタ処理します。

[コンプライアンス違反のあるデバイス（Devices with compliance violations）] エリアでは、次の 3 つのプライマリカテゴリのコンプライアンス違反を表示できます。

- [設定コンプライアンス（Configuration Compliance）]：スタートアップ設定と実行中の設定の不一致、ネットワークプロファイル、およびグローバル設定など、確立された設定のベースラインからの逸脱を追跡します。
- [ソフトウェアおよびハードウェアコンプライアンス（Software and Hardware Compliance）]：ハードウェアおよびモジュールのソフトウェアイメージバージョンとEOX（サポート終了/販売終了）ステータスをモニターします。
- [脆弱性コンプライアンス（Vulnerability Compliance）]：重大なセキュリティアドバイザリの影響を受けるデバイスを強調表示します。

ステップ3 任意のコンプライアンスタイプをクリックすると、デバイステーブルに違反および非準拠デバイスのリストが表示されます。

設定コンプライアンスを管理する方法の詳細については、「設定コンプライアンスの管理」を参照してください。

ステップ4 （オプション）[更新（Refresh）] をクリックして、ダッシュボードを最新のコンプライアンスデータで更新します。

ステップ5 右上隅の [コンプライアンス設定（Compliance settings）] をクリックして設定ウィンドウを開きます。違反チェックの有効化または無効化、および異なるタイプのコンプライアンス違反に対して、カスタマイズされたコンプライアンスの重大度レベルを設定できます。

ダッシュボードには現在のコンプライアンスステータスが表示されるため、非準拠デバイスを対象に修復できます。

設定コンプライアンスの管理

ユーザーが設定のばらつきを効率的に特定し、進行中の違反と確認済みの違反を確認し、コンプライアンス監査を実行してネットワークアシュアランスを維持できるようにします。

Before you begin

- コンプライアンス設定を変更するには、ネットワーク管理者ロールを持っていることを確認してください。
- ダッシュボードの範囲をグローバルまたは特定のサイトに設定して、データに必要なネットワークセグメントが反映されるようにします。
- ダッシュボードの右上隅をチェックして、最後のコンプライアンス監査タイムスタンプが最新であることを確認します。

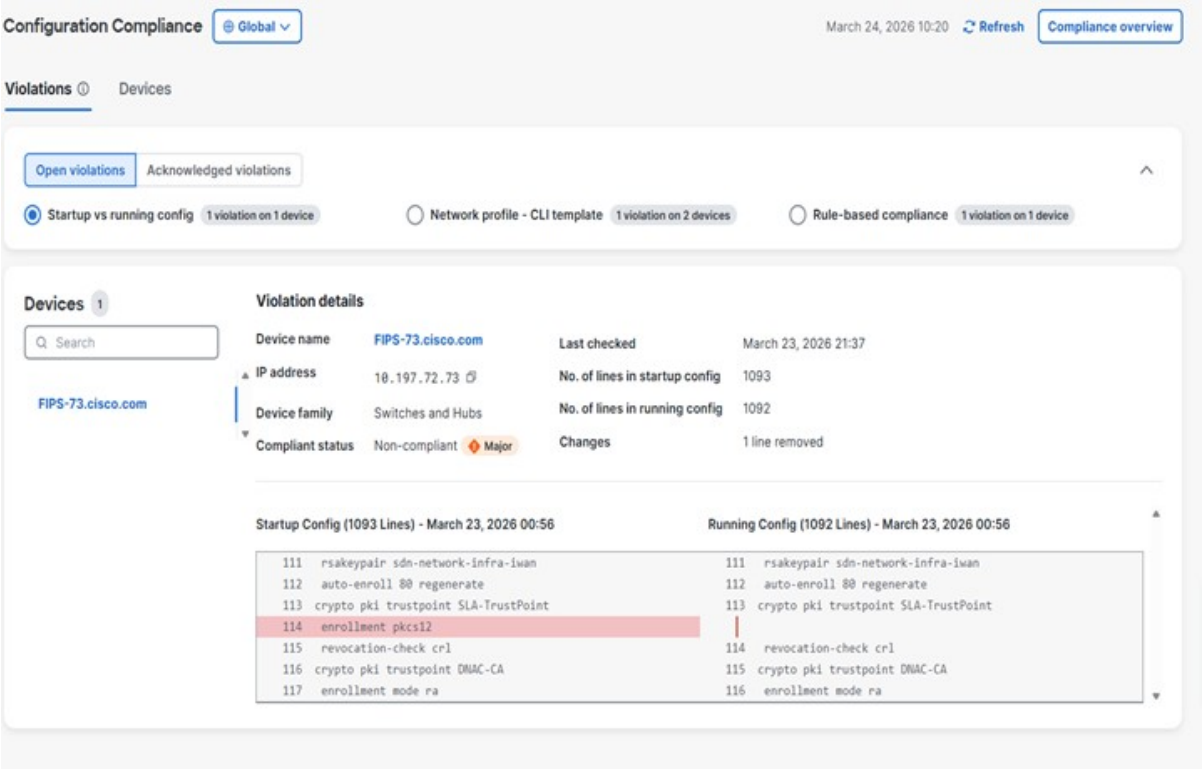
この手順を使用して、設定の違反を分析、確認、および監視します。

手順

ステップ 1 メインメニューから次を選択します。、**[ポリシー（Policies）]** > **[設定コンプライアンス（Configuration Compliance）]** を選択します。

コンプライアンス設定ダッシュボードが表示されます。

図 *24 :* 設定に関するコンプライアンス



ステップ 2 [違反（Violations）] タブをクリックして、違反を管理および表示します。

a) ルールベースのコンプライアンス、ネットワークプロファイル - CLI テンプレート、スタートアップ vs 実行コンフィギュレーションなどのオプションのリストからコンプライアンスタイプを選択します。

ステップ 3 [未解決の違反（Open violations）] と [確認済みの違反（Acknowledged violations）] トグルボタンを使用して、違反を確認します。

オプション	説明
未解決の違反	現在発生中であり、対応が必要な違反を表示します。
確認済みの違反	確認され、承認された違反を表示します。

a) 違反モデル名、影響を受けるデバイス、コンプライアンスタイプ、サブタイプ、属性、インテンド値、および現在の設定値について、表で違反の詳細を確認します。

b) [デバイス上（On devices）] 列の値をクリックすると、違反の影響を受けたデバイスが表示されます。

c) [インテンド値（Intended value）] 列の [詳細を表示（View details）] をクリックして、意図した設定を実際のデバイス設定と比較します。

ステップ 4 許容範囲内の逸脱を承認したり、以前の承認を元に戻すことによって、コンプライアンスアラートノイズを管理するには、次の手順を実行します。

a) [Open Violations] タブをクリックします。
b) 違反を選択し、表の上部にある [違反の承認（Acknowledge violations）] をクリックします。
c) 違反を一括で承認するには、表の上部にあるチェックボックスをオンにするか、複数の違反を選択して [違反の承認（Acknowledge violations）] をクリックします。
d) 確認ウィンドウで、[Confirm] をクリックします。違反は、[承認済みの違反（Acknowledged Violations）] タブに移動します。
e) [違反の承認の解除（Un-Acknowledge violations）] をクリックするとステータスが元に戻り、項目が [未解決の違反（Open violations）] リストに戻ります。

ステップ 5 デバイスレベルのコンプライアンスを監視し、個々のネットワークノードまで詳細に可視化するには、次の手順を行います。

a) [デバイス（Devices）] タブをクリックし、コンプライアンス タイプのフォーカスを選択して、コンプライアンス違反があるデバイスを表示して一括管理します。

ステップ 6 デバイステーブルを確認して、次のことを特定します。

a) デバイス名と IP アドレス：特定のネットワークノード。
b) コンプライアンスステータス：ドロップダウンリストを使用して、準拠、非準拠、エラー、該当なし、使用不可、中止、進行中、修復中などのコンプライアンスステータスをフィルタ処理できます。
c) シビラティ（重大度）：ドロップダウンリストを使用して、クリティカル、メジャー、マイナー、情報などのシビラティ（重大度）レベルをフィルタ処理できます。
d) 設定違反：ドロップダウンリストを使用して、設定違反のタイプをフィルタ処理できます。

ステップ 7 （オプション）デバイスを選択し、[コンプライアンスチェックの実行（Run compliance check）] をクリックすると、そのデバイス設定の即時手動監査がトリガーされます。

次のタスク

- 手動監査後もデバイスが非準拠のままの場合は、ハイパーリンクされたデバイス名をクリックして、デバイス 360 ビューを開きます。
- デバイス 360 ビューで、[準拠（Compliance）] タブに移動して、詳細な障害対応を実行し、設定の修復を開始します。

コンプライアンス設定の構成

コンプライアンス設定を構成する主な目的は、ネットワークの正常性とセキュリティに関する標準化されたフレームワークを確立することにあります。これらの設定をカスタマイズすることで、管理者は次のことが可能になります。

- 組織の標準の適用：すべてのネットワークデバイスを事前定義された設定、ソフトウェア、脆弱性ポリシーに準拠させることができます。
- リスクの軽減：セキュリティ脅威をもたらしたり動作を不安定にしたりする可能性がある非準拠デバイスを特定し、それらに対処できます。
- 可視性の最適化：コンプライアンスダッシュボードを調整して、特定のネットワークアーキテクチャにとって最も重要なメトリックに焦点を当てることにより、無関係なアラートからの「ノイズ」を削減できます。
- ガバナンスの自動化：手動の監査から自動化されたポリシー主導のモニタリングに移行し、ネットワーク インフラストラクチャ全体で一貫した監視を実現できます。

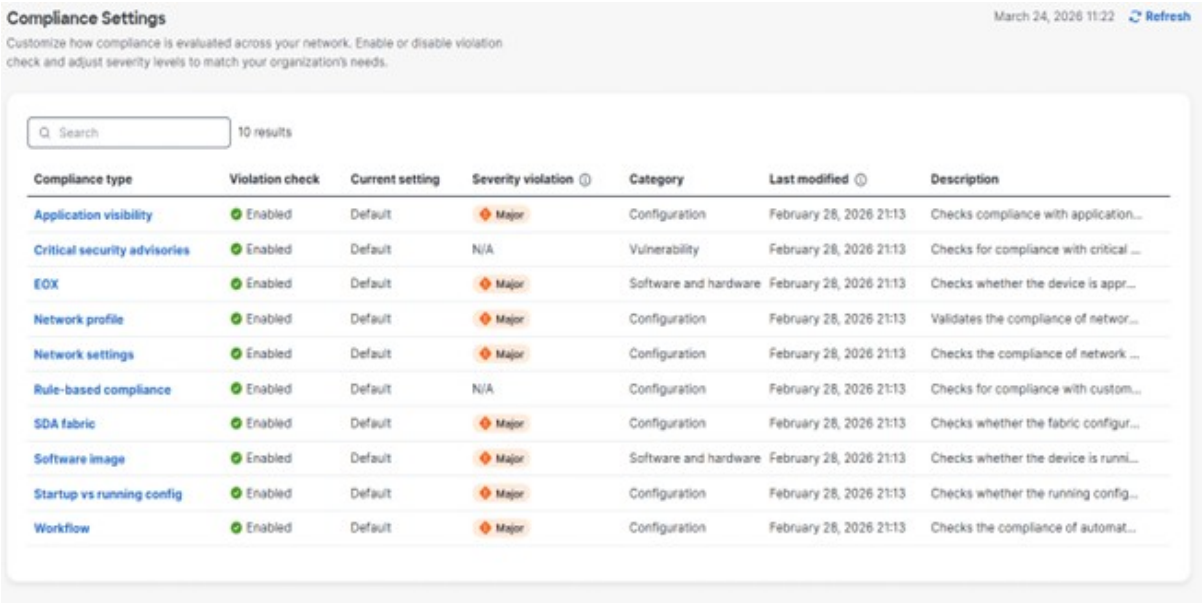
Before you begin

- コンプライアンス設定を変更するのに必要な管理者権限があることを確認します。
- これらの設定への変更が今後のネットワーク全体にわたるコンプライアンス監査のすべてに適用されることを理解しておきます。

手順

ステップ 1 メインメニューから次を選択します。、**[ポリシー（Policy）]** > **[コンプライアンス設定（Compliance Settings）]** の順に選択します。

図 *25 : [コンプライアンス設定（Compliance Settings）] ダッシュボード*



ステップ 2 （オプション）検索ボックスを使用して、特定のコンプライアンスタイプを特定します。

ステップ 3 各項目の [コンプライアンス設定（Compliance Settings）] テーブルを確認します。

- [違反チェック（Violation check）]：チェックが有効になっているか無効になっているかを示します。
- [現在の設定（Current setting）]：設定ステータスを表示します。
- [違反のシビラティ（Severity violation）]：割り当てられた影響レベルを表示します。
- [カテゴリ（Category）]：設定、脆弱性、ソフトウェア、ハードウェアなどのコンプライアンスエリアを示します。
- [最終変更日（Last modified）]：最終変更時刻を表示します。
- [説明（Description）]：コンプライアンスの説明。

ステップ 4 それぞれのコンプライアンスタイプの違反チェックを有効または無効にする、ハイパーリンクが設定されている[コンプライアンスタイプ（Compliance type）]をクリックすると、スライドインペインが開きます。

ステップ 5 設定スライドインペインでは、

違反チェックを有効または無効にできます（デフォルトでは、イネーブル）。違反チェックが有効になっている場合、シビラティレベルを[重大（Critical）]、[メジャー（Major）]（デフォルト設定）、[マイナー（Minor）]、[情報（Informational）]（違反なし）にカスタマイズできます。

a) [編集（Edit）]をクリックし、[違反チェック（Violation check）]を切り替えてチェックを有効または無効にします。チェックを無効にすると、対応するカテゴリはダッシュボード上の非準拠デバイス数に影響しなくなります。

b) [シビラティ（Severity）]違反レベルを調整します。

次のオプションがあります。

- [重大（Critical）]：優先順位の高い問題。
- [メジャー（Major）]（デフォルト）：シビラティの標準レベル。
- [マイナー（Minor）]：優先順位の低い問題。
- [情報（Informational）]：ステータス更新または重大ではないログ。

c) [保存（save）]をクリックして変更を適用します。

d) すべての設定を元の状態に戻す場合は、[デフォルトにリセット（Reset to default）]ボタンをクリックします。

コンプライアンスサマリーの表示

インベントリページには、デバイスごとにコンプライアンスの集約ステータスが表示されます。

手順

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

コンプライアンス列には、デバイスごとに集約コンプライアンスステータスが表示されます。

ステップ 2 コンプライアンスステータスをクリックすると、コンプライアンス サマリー ウィンドウが開きます。このウィンドウには、選択したデバイスに適用可能な次のコンプライアンスチェックが表示されます。

- スタートアップ設定と実行中の設定

  Catalyst Center では、スタートアップ コンフィギュレーションと実行コンフィギュレーションを比較しながらアウトオブバンド設定変更の詳細を表示できます。**[Change History]** エリアのバブルにカーソルを合わせると、詳細が表示されます。



  アウトオブバンドの変更については、次の詳細が表示されます。

  - [Lines Added, Removed, Modified]：追加、削除、または変更された行の数を示します。
  - [Triggered By]：設定変更イベントを表示します。イベントの詳細については、「Configuration Drift of a Device」を参照してください。
  - [Terminal Name, Login IP, Username]：ユーザーの端末名、ログイン IP、およびユーザー名を表示します。
  - [Config Method, Timestamp]：行った変更の設定方法とタイムスタンプを表示します。

  （注） [Config Method] がメモリの場合、デバイスによって設定が自己生成されたことを示します。

- ルールベースのコンプライアンスポリシー
- ソフトウェア イメージ
- 重大なセキュリティの脆弱性

- ネットワークプロファイル
- ネットワーク設定
- ファブリック
- SD-Accessのサポートされていない構成
- アプリケーションの可視性
- EoX - サポート終了
- Cisco Umbrella

（注） [ネットワーク設定（Network Settings）]、[ネットワークプロファイル（Network Profile）]、[ファブリック（Fabric）]、[SD-Accessのサポートされていない設定（SD-Access Unsupported Configuration）]、および [アプリケーションの可視性（Application Visibility）] はオプションであり、デバイスが必要なデータでプロビジョニングされている場合にのみ表示されます。

手動コンプライアンスの実行

Catalyst Center では、コンプライアンスチェックを手動でトリガーできます。

手順

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

ステップ 2 一括コンプライアンスチェックを実行するには、次の手順を実行します。

a) 該当するすべてのデバイスを選択します。

b) [Actions] ドロップダウンリストから、**[Compliance]** > **[Run Compliance]** の順に選択します。

ステップ 3 デバイスごとのコンプライアンスチェックを実行するには、次の手順を実行します。

a) コンプライアンスチェックを実行するデバイスを選択します。

b) [Actions] ドロップダウンリストから、**[Compliance]** > **[Run Compliance]** の順に選択します。

c) あるいは、[Compliance] 列（使用可能な場合）をクリックし、[Run Compliance] をクリックします。

ステップ 4 デバイスの最新のコンプライアンスステータスを表示するには、次の手順を実行します。

a) デバイスとインベントリを選択します。デバイス情報の再同期 （217 ページ）を参照してください。

b) [Actions] ドロップダウンリストから、**[Compliance]** > **[Run Compliance]** の順に選択します。

（注）

- 到達不能のデバイスやサポートされていないデバイスに対してコンプライアンスの実行をトリガーすることはできません。
- デバイスに対してコンプライアンスを手動で実行しない場合、コンプライアンスチェックはコンプライアンスのタイプに応じて一定期間後に実行されるように自動的にスケジュールされます。
- CLI テンプレート コンプライアンスは、実現されたテンプレートをデバイスの実行コンフィギュレーションと比較します。実行コンフィギュレーションは、デバイスで使用可能な最新のアーカイブから取得されます。
- イベントベースのアーカイブは、トラップを受信してから更新されるまでに少なくとも 2 分かかります。正確な結果を得るには、設定の変更後にコンプライアンスを手動で実行する前に、少なくとも 2 分間待つことをお勧めします。
- Syslog ベースの収集を機能させるには、[Design] > [Network Settings] > [Telemetry] > [Syslogs] ウィンドウで Catalyst Center を Syslog サーバーとして設定する必要があります。

ネットワークデバイスのコンプライアンス監査レポートの生成

Catalyst Center では、個々のネットワークデバイスのコンプライアンスステータスを示す統合されたコンプライアンス監査レポートを取得できます。このレポートを使用すると、ネットワークを完全に可視化できます。

詳細については、『*Cisco Catalyst Center Platform User Guide*』の「Run a Compliance Report」を参照してください。

コンプライアンス違反の確認

Catalyst Centerでは、デバイスに関する重要度の低いコンプライアンス違反を認識し、コンプライアンスステータスの計算から違反をオプトアウトできます。必要に応じて、コンプライアンスステータスの計算に違反をオプトインすることもできます。

手順

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

ステップ 2 デバイス名をクリックするとダイアログボックスが開き、そのデバイスの高度な情報が表示されます。ダイアログボックスの [View Device Details] リンクをクリックします。
デバイスの詳細ウィンドウが表示されます。

ステップ 3 左側のペインで、[Compliance] [Summary] を選択します。

ステップ 4 [Compliance Summary] ウィンドウで、違反を確認するコンプライアンスタイルをクリックします。

[未解決の違反（Open Violations）] および [確認済みの違反（Acknowledged Violations）] テーブルに次の情報が表示されます。

- モデル名
- 属性
- ステータス：この列には、次のいずれかのステータスが表示されます。
  - **Added**：デバイスに属性が追加されます。
  - **Changed**：インテント値とデバイス値が一致しません。
  - **Removed**：デバイスからインテントが削除されます。
- Intended Value：Catalyst Centerによって構成されたインテント値を示します。
- Actual Value：現在デバイスに構成されている値を表示します。
- Action：未解決の違反には [Acknowledge] リンクを表示し、確認済みの違反には [Move to Open Violations] リンクを表示します。

コンプライアンスステータスの計算から違反をオプトアウトするには、次の手順を実行します。

a) [Open Violations] タブをクリックします。
b) 違反を選択し、[Actions] 列で [Acknowledge] をクリックします。
c) 違反を一括で確認するには、表の上部にあるチェックボックスをオンにするか、複数の違反を選択して [Acknowledge] をクリックします。
d) 確認ウィンドウで、[Confirm] をクリックします。
違反は、[Acknowledged Violations] タブに移動します。

コンプライアンスステータスの計算に違反をオプトインするには、次の手順を実行します。

a) [Acknowledged Violations] タブをクリックします。
b) 違反を選択し、[Actions] 列で [Move to Open Violations] をクリックします。
c) 違反をまとめて移動するには、表の上部にあるチェックボックスをオンにするか、複数の違反を選択して [Move to Open Violations] をクリックします。
d) 確認ウィンドウで、[Confirm] をクリックします。
違反は [Open Violations] タブに移動します。

ステップ 5 コンプライアンスステータスの計算からオプトアウトした属性のリストを表示するには、[Compliance Summary] ウィンドウで [View Preference for Acknowledged Violations] リンクをクリックします。

ステップ 6 コンプライアンスステータスの計算に属性をオプトインするには、[違反の設定を認識（Acknowledge Violation Preferences）] スライドインペインで、次の手順を実行します。

a) 属性を選択し、[Actions] 列で [Unlist] をクリックします。
b) 一括で選択するには、表の上部にあるチェックボックスをオンにするか、複数の違反を選択して [Unlist] をクリックします。

[Models] タブに、モデル構成、ルーティング、ワイヤレス、アプリケーションの可視性、またはファブリックについて確認された属性が表示されます。確認済みのテンプレートは、[Templates] タブに表示されます。

（注）
- [Acknowledge Violation Preferences] ウィンドウで、空の（-）属性を持つモデルは、子属性を含むモデル全体が確認されていることを意味します。
- [Added] または [Removed] のステータスを持つ違反が確認されると、Catalyst Centerはそれと類似する属性とその子属性を自動的に認識します。
- [Added] または [Removed] のステータスを持つ類似した違反がオーバーライドしている場合、認識された子属性は [Open Violations] に移動できません。

デバイスのスタートアップ設定と実行中の設定の同期

デバイスのスタートアップコンフィギュレーションと実行コンフィギュレーションに不一致がある場合、修復同期を実行して設定を一致させることができます。

手順

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

ステップ 2 一括修復を行うには、次の手順を実行します。

a) 該当するすべてのデバイスを選択します。
b) [Actions] ドロップダウンリストから、**[Compliance]** > **[Write Running Config to Startup Config]** の順に選択します。

デバイスごとの修復を行うには、次の手順を実行します。

a) 修復同期を実行するデバイスを選択します。
b) [Actions] ドロップダウンリストから、**[Compliance]** > **[Write Running Config to Startup Config]** の順に選択します。

または、[Compliance] 列のリンクをクリックし、**[Compliance Summary]** > **[Startup vs Running Configuration]** > **[Sync Device Config]** の順に選択します。

ステップ 3 デバイスの修復ステータスを表示するには、次の手順を実行します。

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

b) [Actions] ドロップダウンリストから、**[Compliance]** > **[Check Startup Config Write Status]** の順に選択します。

コンプライアンス違反の修正

Catalyst Center では、デバイスのコンプライアンス違反の自動修正によって準拠ネットワークを維持できます。Catalyst Center のコンプライアンスチェックで特定されたデバイスのインテントからの逸脱は、この手順で修正されます。

手順

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

コンプライアンス列には、デバイスごとに集約コンプライアンスステータスが表示されます。

ステップ 2 コンプライアンスステータスをクリックして、[Compliance Summary] ウィンドウを起動します。

ステップ 3 ウィンドウの上部にある [Fix All Configuration Compliance Issues] リンクをクリックします。
[] スライドインペインが表示されます。

（注） コンプライアンス違反を修正するためのリンクは、サポートされているカテゴリに違反がある場合にのみ表示されます。それ以外の場合、リンクは表示されません。

ステップ 4 [Fix Configuration Compliance Issues] スライドインペインで、次の手順を実行します。

a) [Summary of Issues to be Fixed] エリアで、ネットワークデバイスのコンプライアンス違反を確認します。[Issues Identified] 列には、未解決の違反と認識済みの違反の合計数が表示されます。[Schedule the Fix] をクリックします。

b) 展開のためのタスクのスケジュールを設定します。

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

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 5 [Tasks] ウィンドウで、タスクの展開を監視します。

（注）

- HA の修復、ルーティング、ワイヤレスコントローラの HA の修復、ソフトウェアイメージ、セキュリティアドバイザリ、およびワークフローに関連するコンプライアンスの問題は、この修正では解消されません。これらに関しては、それぞれのセクションのアクションに従って個別に対処します。
- CLI テンプレートのコンプライアンスにはいくつかの制限があるため、一部の CLI テンプレートは非準拠のままになることがあります。詳細については、CLI テンプレートコンプライアンスの制限事項 （688 ページ）を参照してください。
- Catalyst Center リリース 2.3.7 以降では、次の変更については設定はデバイスに直接プッシュされず、Catalyst Center でインテントが更新されます。
  - IPDT でプロトコルエンドポイントが検出された場合。
  - SNMP トラップ設定の SNMP ユーザーグループの変更がシステムで検出された場合。

  デバイスロールの変更については、IPDT 設定はデバイスに直接プッシュされます。

デバイスのアップグレード後のコンプライアンス動作

- デバイスのアップグレードが正常に完了すると、該当するすべてのデバイス（システムでコンプライアンスが実行されたことがないデバイス）のコンプライアンスチェックがトリガーされます。
- コンプライアンスは、[Startup vs Running] タイプを除き、インベントリに含まれるデバイスのステータスを計算して表示します。
- アップグレード後、[Startup vs Running] タイルに [NA] が「Configuration data is not available」というテキストとともに表示されます。
- アップグレードが正常に完了してから 1 日後に、1 回限りのスケジューラが実行され、デバイスで構成データを使用できるようになります。[Startup vs Running] タイルに、正しいステータス（[Compliant]/[Non-Compliant]）と詳細データが表示され始めます。
- トラップを受信すると、設定アーカイブサービスが構成データを収集し、コンプライアンスチェックが再度実行されます。

（注）

アップグレードセットアップでは、[Flex Profile] インターフェイスのコンプライアンスの不一致は無視してください。インターフェイス名の場合、[1] が [management] にマッピングされます。

CLI テンプレートコンプライアンスの制限事項

Catalyst Center では、CLI テンプレートをデバイスの実行コンフィギュレーションと比較して、意図との不一致を識別することができます。コンパレータエンジンには、次のような制限事項があります。

- CLI テンプレートコンパレータは、変数と値の大文字の使用をサポートしています。ただし、コマンドキーワードには大文字を使用しないでください。
- CLI テンプレートコンパレータは、エイリアスの使用をサポートしています。
- 非準拠としてフラグが設定されている省略または短縮コマンドの使用は避けてください。
- コマンドが欠落していて、それがセクションレベルにある場合、欠落しているコマンドに続くセクションレベルのコマンドにもフラグが付けられます。この問題を回避するには、インデントを使用します。

  たとえば、次の CLI テンプレートコンパレータ出力は、インデントのないコマンドを示しています。

実現されたテンプレート	実行コンフィギュレーション	出力
#interface Vlan111 #description SVI interface kan-111 #ip address 111.2.3.4 255.255.255.0 #ip helper-address 7.7.7.8 #no mop enabled #no mop sysid #!	#interface Vlan111 # description SVI interface kan-111 # ip address 111.2.3.4 255.255.255.0 # ip helper-address 7.7.7.7 # ip helper-address 7.7.7.8 # no mop enabled # no mop sysid #!	以下のコマンドが欠落としてマークされています。 # ip helper-address 7.7.7.7 # ip helper-address 7.7.7.8 # no mop enabled # no mop sysid

  次の CLI テンプレートコンパレータ出力は、インデントを含むコマンドを示しています。

実現されたテンプレート	実行コンフィギュレーション	出力
#interface Vlan111 # description SVI interface kan-111 # ip address 111.2.3.4 255.255.255.0 # ip helper-address 7.7.7.8 # no mop enabled # no mop sysid #!	#interface Vlan111 # description SVI interface kan-111 # ip address 111.2.3.4 255.255.255.0 # ip helper-address 7.7.7.7 # ip helper-address 7.7.7.8 # no mop enabled # no mop sysid #!	コンパレーターは、欠落しているコマンドのみにフラグを立てます。 #ip helper-address 7.7.7.7

- 対話型およびイネーブルモードのコマンドは、コンプライアンスのために比較されません。コマンドですべてのオプションと値を指定することにより、対話型コマンドの代替形式を使用できます。

  たとえば、テンプレートコードが以下のように **#ENABLE** と **#INTERACTIVE** モードのコマンドを一緒に指定した場合、コマンドの比較は行われません。

```
#MODE_ENABLE
 #INTERACTIVE
    mkdir <IQ>Create directory<R>xyz
```

```
 #ENDS_INTERACTIVE
 #MODE_END_ENABLE
#end
```

- コンパレータによってフラグが設定されているコマンドでは範囲を使用しないでください。範囲は拡張形式で使用する必要があります。
- 同じテンプレート内のオーバーライドしているコマンドにフラグが付けられます。次の例に示すように、ignore-compliance シンタックスでコマンドを囲むことで、不一致を回避できます。

実現されたテンプレート	実行コンフィギュレーション	出力

`#no banner motd #Welcome to Cisco .:|:.#`
`#banner motd #Welcome to Cisco .:|:.#`
	`#banner motd ^CWelcome to Cisco .:|:.^C`	• 次のコマンドは、欠落としてフラグが付けられています。
		`no banner motd #Welcome to Cisco .:|:.#`
		• 実行中のコマンドはすでに前記のコマンドと比較されているため、次のコマンドも欠落としてマークされています。
		`banner motd #Welcome to Cisco .:|:.#`

不一致を回避するには、次の手順を実行します。

実現されたテンプレート	実行コンフィギュレーション	出力

`#! @start-ignore-compliance`
` #no banner motd #Welcome to Cisco .:|:#`
`#! @end-ignore-compliance`
`#banner motd #Welcome to Cisco .:|:.#`
	`#banner motd ^CWelcome to Cisco .:|:.^C`	シンタックスで囲まれたコマンドは比較されないため、不一致はありません。

- Cisco IOS XE の以降のリリースでは、一部のデフォルトコマンドは、**show run** コマンドではなく、**show run all** コマンドが発行された場合にのみ表示されます。したがって、これらのコマンドは実行コンフィギュレーションに表示されず、非準拠としてフラグが設定されます。

（注） コンプライアンスチェックでこれらのデフォルトコマンドを無視するには、Cisco Technical Assistance Center（TAC）でサポートケースを開きます。

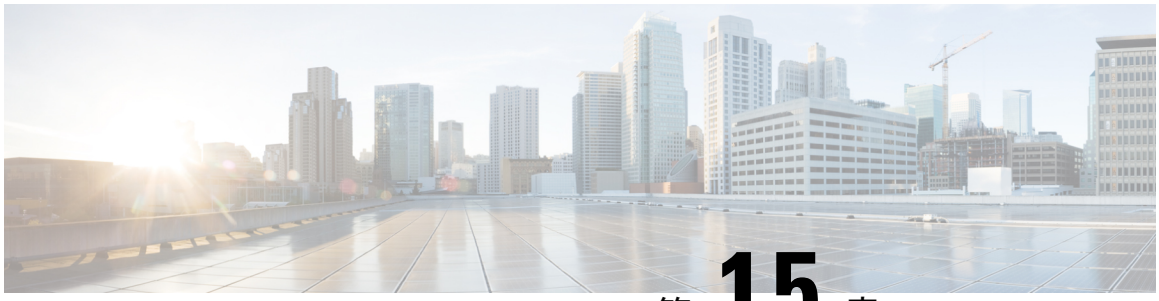
- パスワードを含むコマンドは、デバイスに暗号化された形式で保存されるため、コンパレータによってフラグが設定されます。

（注） 次の構文でコマンドを囲むことで、パスワードを含むコマンドと一部のデフォルトコマンドの不一致を回避できます。

```
! @start-ignore-compliance
! @end-ignore-compliance
```

次に、変更が表示されるようにテンプレートを再プロビジョニングします。

CLI テンプレートとデバイスの実行コンフィギュレーションとの不一致を避けるために、実行コンフィギュレーションと同様のコマンドを使用することをお勧めします。



第 15 章

デバイスの診断コマンドを実行

- コマンドランナーの概要 （691 ページ）
- デバイスの診断コマンドの実行 （691 ページ）

コマンドランナーの概要

コマンドランナー ツールでは、選択したデバイスに診断CLIコマンドを送信できます。現在、**show** とその他の読み取り専用コマンドが許可されています。

デバイスの診断コマンドの実行

コマンド ランナーを使用すると、選択したデバイスで診断 CLI コマンドを実行し、結果のコマンド出力を表示できます。コマンドランナーは、スタンドアロン端末の一部として使用可能なショートカットのサブセットのみをサポートします。

始める前に

コマンドランナーの使用を開始するには、次の手順を実行します。

1. メインメニューから次を選択します。**[System]** > **[Software Updates]** > **[Installed Apps]** の順に選択します。
2. [Command Runner] アプリケーションを検索し、[Install] をクリックします。
3. インストール後、ディスカバリ ジョブを実行し、デバイスにCatalyst Centerを入力します。これらデバイスの一覧が表示され、ここから診断 CLI コマンドを実行します。

手順

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

ステップ 2 [Command Runner] ウィンドウの [Search] フィールドで、ドロップダウン矢印をクリックして、[Device IP] または [Device Name] で検索します。

ステップ 3 診断 CLI コマンドを実行するデバイス（複数可）を選択します。

[Device List] に選択内容が表示されます。

ステップ 4 （任意） リストに追加する別のデバイスを選択します。到達可能なデバイスを 20 台まで選択できます。

（注） デバイス一覧にはインベントリで利用可能なデバイスがすべて表示されますが、コマンドランナーはワイヤレス アクセス ポイント デバイスおよび Cisco Meraki デバイスではサポートされていません。アクセス ポイント デバイスまたは Cisco Meraki デバイスを選択すると、コマンドが実行されないという警告メッセージが表示されます。

ステップ 5 [Select/Enter commands] フィールドに CLI コマンドを入力し、[Add] をクリックします。

コマンドランナーでは、先行入力がサポートされています。入力を開始すると、選択可能なコマンドがコマンドランナーによって表示されます。新しい有効なコマンドを入力することもできます。

ping や **traceroute** などの一部のコマンドは、インタラクティブモードまたは非インタラクティブモードで実行できます。ただし、コマンドランナーは非インタラクティブモードのみをサポートしています。インタラクティブモードでコマンドを実行すると、エラーが発生する場合があります。

ステップ 6 [コマンドの実行（Run Command(s)）] をクリックします。

成功すると、「コマンドは正常に実行されました」 というメッセージが表示されます。

ステップ 7 コマンド出力を表示するには、デバイスの下に表示されているコマンドをクリックします。

（注） [Command Runner] ウィンドウにすべてのコマンド出力が表示されます。パスワードなどの機密情報は、コマンド出力でマスクされます。

ステップ 8 （任意） [Export all CLI Output] をクリックすると、コマンド出力をテキストファイルにエクスポートしてローカルに保存できます。

ステップ 9 [Go Back] をクリックすると前のウィンドウに戻ります。

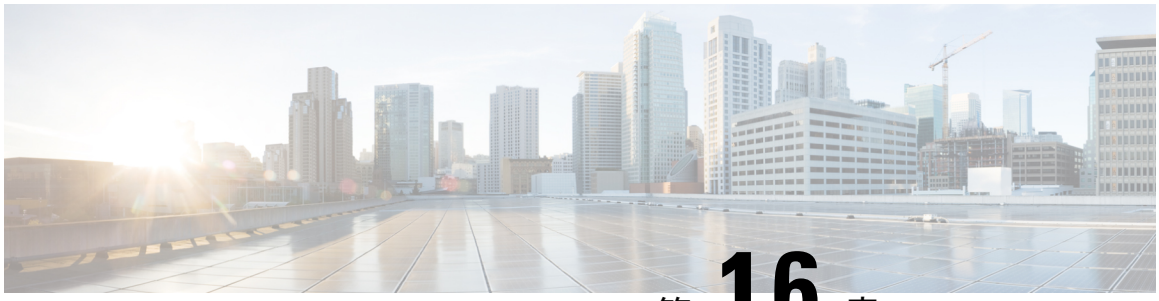
（注） 必要に応じて、デバイス名の横にある [x] をクリックすると、デバイス一覧からデバイスが削除されます。同様に、コマンドの横にある [x] をクリックすると、コマンド一覧からコマンドが削除されます。



第 V 部

ネットワークのプロビジョニング

- プラグアンドプレイを使用したデバイスのオンボーディングとプロビジョニング （695 ページ）
- ワイヤレスデバイスのプロビジョニング （735 ページ）
- ルーティングプロファイルのプロビジョニング （1185 ページ）
- ファイアウォール プロファイルのプロビジョニング （1189 ページ）
- LAN アンダーレイのプロビジョニング （1193 ページ）
- SD-Access LISP ファブリックネットワークのプロビジョニング （1213 ページ）
- キャンパスネットワークのプロビジョニング （1305 ページ）
- サービスのプロビジョニング （1327 ページ）



第 16 章

プラグアンドプレイを使用したデバイスのオンボーディングとプロビジョニング

- プラグアンドプレイ プロビジョニングの概要 （695 ページ）
- プラグ アンド プレイ プロビジョニングの前提条件 （698 ページ）
- プラグアンドプレイ展開のガイドライン （705 ページ）
- デバイスの表示 （706 ページ）
- デバイスの追加または編集 （710 ページ）
- デバイスの一括追加 （711 ページ）
- バーチャル アカウント プロファイルの登録または編集 （712 ページ）
- スマートアカウントからのデバイスの追加 （714 ページ）
- プラグアンドプレイ対応デバイスのプロビジョニング （716 ページ）
- デバイスの削除 （732 ページ）
- デバイスのリセット （733 ページ）

プラグアンドプレイ プロビジョニングの概要

プラグ アンド プレイ プロビジョニングは、最小限のネットワーク管理者およびフィールド担当者の関与で、新しいネットワーク デバイスを自動的かつリモートにプロビジョニングおよびオンボードする方法を提供します。

プラグ アンド プレイ プロビジョニングを使用すると、次の操作を実行できます。

- サイトの割り当て、サイト設定の展開、デバイス ソフトウェア イメージのインストール、およびカスタム オンボード設定の適用によって、デバイスをプロビジョニングする。
- インストールの前に、デバイス情報を入力し、プロビジョニング操作を選択してデバイスを計画します。デバイスはオンラインになると Catalyst Center に接続します。次に、デバイスのプロビジョニングとオンボーディングが自動で実行されます。
- 事前の計画なしにネットワーク上に表示される新しいデバイスである、要求されていないネットワーク デバイスをプロビジョニングします。

- Cisco スマート アカウントの Cisco Plug and Play Connect クラウド ポータルから、デバイス インベントリをプラグ アンド プレイに同期して、すべてのデバイスが Catalyst Center に表示されるようにします。
- ネットワーク デバイスの詳細なオンボーディング ステータスを表示します。

ここでは、プラグ アンド プレイ プロビジョニングの一般的なユースケースとワークフローについて説明します。

計画的なプロビジョニング

管理者は、新しいサイトまたはその他のネットワーク デバイス グループのプロビジョニングを計画できます。

（注） AP の計画済みステータスは、AP がプラグアンドプレイを介して Catalyst Center に接続したときに、ゼロタッチプロビジョニング（ZTP）のみを使用して AP を要求するための状態です。この計画は、AP がワイヤレスコントローラに直接関連付けられている場合、**[プロビジョニング（Provision）]** > **[インベントリ（Inventory）]** オプションを介した AP のプロビジョニングには適用されません。

計画的なプロビジョニングの手順は、次のとおりです。

1. ネットワーク階層内のサイトを定義することをお勧めします。ネットワーク階層 （271 ページ）を参照してください。
2. デバイスに適用する [オンボーディング設定（Onboarding Configuration）] テンプレートを定義します。このようなテンプレートには、ネットワーク上で管理できるようにデバイスをオンボードするための基本的なネットワーク設定コマンドが含まれています。多くの場合、Day-0 設定をカスタマイズする必要がない限り、このようなテンプレートは必要ありません。デバイス設定の変更を自動化するテンプレートの作成 （571 ページ）を参照してください。

（注） Day-0 テンプレートは、対話型コマンドをサポートしていません。

3. 展開するデバイスのタイプについて、ネットワークプロファイルを定義します。ネットワークプロファイルの概要 （535 ページ）を参照してください。
4. 展開するデバイスのデバイスログイン情報（CLI および SNMPv2c/SNMPv3）を定義することをお勧めします。SNMPv2c を使用している場合は、読み取りと書き込み両方のログイン情報を指定する必要があります。

（注） ログイン情報が不足していると、プロビジョニング後にデバイスをインベントリに追加できなくなります。

5. プロビジョニングするデバイスのソフトウェアイメージがアップロードされ、イメージリポジトリ内でゴールデンとしてマークされていることを確認します。ソフトウェアイメージのインポート （638 ページ）を参照してください。
6. CSV ファイルを使用して一度にまたは一括で、計画したデバイスに関する詳細を追加します。デバイスの追加または編集 （710 ページ）またはデバイスの一括追加 （711 ページ）を参照してください。
7. デバイスが起動し、自動的にプロビジョニングされます。

要求されていないプロビジョニング

計画前に新しいネットワークデバイスをネットワークに追加すると、そのネットワークデバイスは要求されていないデバイスとしてラベル付けされます。要求のないデバイスは、管理者が手動で追加することも、プラグ アンド プレイ プロビジョニングの前提条件 （698 ページ）で説明されているいずれかの検出方法を使用して自動的に追加することもできます。

管理者がデバイスをプロビジョニングする手順は、次のとおりです。

1. 要求のないデバイスでフィルタリングするか、名前で検索して、デバイス リストのデバイスを検索します。「デバイスの表示 （706 ページ）」を参照してください。
2. サイト、イメージ、設定テンプレート、またはプロファイルを割り当てて、デバイスを要求します。「プラグアンドプレイ対応デバイスのプロビジョニング （716 ページ）」を参照してください。サイトを割り当てずにデバイスを要求することもできます。

（注） サイトが割り当てられていないデバイスの場合、グローバルデバイスログイン情報が必要です。サイトが割り当てられているデバイスの場合、サイトレベルのグローバルデバイスログイン情報が必要です。

Cisco スマートアカウントの同期とプロビジョニング

ネットワーク デバイスは、シスコのプラグ アンド プレイ接続クラウド サービスによって Cisco スマート アカウントを通じて自動的に登録されます。管理者は Cisco Plug and Play Connect から Catalyst Center プラグ アンド プレイにデバイス インベントリを同期することができます。これにより、すべてのデバイスが Catalyst Center に表示されます。次に、これらのデバイスを要求してプロビジョニングすることができます。

1. スマートアカウントと同期するバーチャルアカウントを登録して同期します。「バーチャル アカウント プロファイルの登録または編集 （712 ページ）」を参照してください。

2. スマート アカウントからデバイス インベントリを同期します。スマートアカウントからのデバイスの追加 （714 ページ）を参照してください。
3. 要求のないデバイスでフィルタリングするか、名前で検索して、デバイス リストのデバイスを検索します。「デバイスの表示 （706 ページ）」を参照してください。
4. サイト、イメージ、設定テンプレート、またはプロファイルを割り当てて、デバイスを要求します。「プラグアンドプレイ対応デバイスのプロビジョニング （716 ページ）」を参照してください。
5. デバイスが起動し、自動的にプロビジョニングされます。

デバイスの要求と管理のシナリオ

- **要求されているデバイス**
  - デバイスが要求されて管理されると、PnP プロファイルがデバイスから削除されます。
  - デバイスは、工場出荷時設定へのリセット後にのみ PnP に再度接続しません。
- **インベントリ内の要求されていないデバイス**
  - ユーザーがすでにインベントリにあるデバイスを PnP を介して要求しようとすると、その要求はブロックされます。
  - Catalyst Center は、インベントリ通知を読み取って PnP を更新し、重複要求を防止します。
- **デバイスの工場出荷時設定へのリセット**
  - 管理対象デバイスが工場出荷時設定にリセットされると、要求されていない状態になります。
  - Catalyst Center はインベントリの存在をチェックし、デバイスがまだインベントリにある場合は新しい要求をブロックします。

プラグ アンド プレイ プロビジョニングの前提条件

プラグ アンド プレイ プロビジョニングを使用する前に、プロビジョニングするサイトとデバイスにアクセスできること、およびプラグ アンド プレイ プロビジョニングを実行するために必要な権限があることを確認してください。詳細については、ユーザープロファイルのロールおよび権限 （35 ページ）を参照してください。

すべてのデバイスタイプが必要な前提条件を満たしていることを確認します。さらに、ワイヤレスデバイスまたはセンサーデバイスを展開している場合は、それらの前提条件が満たされていることも確認してください。その他の前提条件はオプションですが、それらを実装すること

を選択した場合は、プラグアンドプレイを使用してデバイスをプロビジョニングする前に実行する必要があります。

すべてのデバイスの前提条件

すべてのデバイスタイプが次の前提条件を満たしていることを確認します。

- デバイスが、次のいずれかの方法で Catalyst Center コントローラを自動的に検出できることを確認します。
  - DHCP：DHCP コントローラディスカバリ （702 ページ）を参照してください。
  - DNS：DNS コントローラディスカバリ （704 ページ）を参照してください。
  - Cisco Plug and Play Connect クラウドサービス：Plug and Play Connect コントローラディスカバリ （704 ページ）を参照してください。
- **[System]** > **[Settings]** > **[Cisco.com Credentials]** を使用して、メインのCatalyst Center設定で cisco.com ログイン情報を設定します。

  必要に応じて、**[System]** > **[Settings]** > **[Smart Account]** で、Cisco スマートアカウントのログイン情報を設定します。
- プロビジョニングするシスコネットワークデバイスについて、サポートされているソフトウェアリリースがあり、工場出荷時のデフォルト状態になっていることを確認します。以前に設定されたネットワークデバイス、または不明な状態になっているネットワークデバイスを使用している場合は、*Cisco Catalyst Center* のネットワーク プラグアンドプレイのトラブルシューティング ガイド [英語] で、デバイスのクリーンアップとリセットの詳細を確認してください。

ワイヤレスデバイスまたはセンサーデバイスの前提条件

前述の前提条件に加えて、すべてのワイヤレスデバイスまたはセンサーデバイスが次の要件を満たしていることを確認してください。

- ワイヤレス AP デバイスの場合は、ワイヤレス AP を管理している シスコ ワイヤレス コントローラ がインベントリに追加され、プロビジョニングされ、ワイヤレス AP が割り当てられるサイトに割り当てられていることを確認します。この要件は、Mobility Express AP では必要ありません。
- ワイヤレス AP デバイスの場合は、ワイヤレス無線周波数プロファイルを定義します。ワイヤレス無線周波数プロファイルの作成（451ページ）を参照してください。この要件は、Mobility Express AP では必要ありません。
- Mobility Express AP の場合は、IP アドレスプールと管理インターフェイスを定義します。IP アドレスプールを設定する （397 ページ）を参照してください。
- ROW AP の場合は、必要な国コードを使用して AP プロファイルを作成し、カスタムサイトタグを設定することを推奨します。Cisco IOS XE デバイスの AP プロファイルの追加設定を行う （509 ページ）を参照してください。

- インテント AP の場合は、[**PnP AP Location**] ウィンドウで [**Configure AP Location**] チェックボックスを使用して、PnP オンボーディングのための AP の場所を設定できます。このチェックボックスは、デフォルトでオフになっています。必要に応じて、このチェックボックスをオンにして、PnP オンボーディング中の AP の場所として PnP 要求中に割り当てられるサイトを設定します。詳細については、『*Catalyst Center Administrator Guide*』の「Configure AP location for PnP onboarding」を参照してください。
- センサーの場合は、センサーが Catalyst Center エンタープライズ IP アドレス（private/enp9s0）を介して到達可能であることを確認します。DHCP オプション 43 の文字列を使用すると、デバイスが Catalyst Center の未要求モードで到達可能になります。ただし、デバイスを要求するには、インターフェイス enp9s0 IP アドレスから到達可能である必要があります。DHCP サーバーで ASCII 値「5A1D;B2;K4;I172.16.x.x;J80;」を使用して、NTP サーバー（DHCP オプション 42）とベンダー固有の DHCP オプション 43 を設定します。ここで、172.16.x.x は enp9s0 インターフェイスに関連付けられた Catalyst Center の仮想 IP アドレスです。
- PnP は、AP 検出の DHCP オプション 43、DNS オプション、または devicehelper メソッドをサポートしています。AP が DNS オプションを使用してワイヤレスコントローラに参加しているが、PnP 検出に DHCP オプション 43 が使用されている場合、競合が発生します。

ワイヤレスコントローラ のオプションの前提条件

プラグ アンド プレイ プロビジョニング プロセスを自動化するのに役立つオプションの前提条件には、次のようなものがあります。

- ネットワーク階層内のサイトを定義します。ネットワーク階層 （271 ページ）を参照してください。
- デバイスの CLI および SNMP ログイン情報を定義します。「グローバル デバイス クレデンシャルの設定 （379 ページ）」を参照してください。

（注） CLI、SNMPv2c、または SNMPv3 ログイン情報を使用して Cisco IOS XE コントローラを要求できます。SNMPv2c を使用している場合は、読み取りと書き込みの両方のログイン情報を指定します。

- イメージを展開する場合は、プロビジョニングされるデバイスのソフトウェアイメージをアップロードし、イメージリポジトリ内でゴールデンとしてマークされるようにします。ソフトウェアイメージのインポート （638 ページ）を参照してください。

（注） Day-0 プロビジョニング中にプラグアンドプレイで使用されるイメージ導入プロセスは、後でデバイスイメージの更新時に使用されるプロセスとは異なります。これについては、ソフトウェアイメージのプロビジョニング （653 ページ） で説明します。プラグアンドプレイ プロビジョニングでは、デバイスが工場出荷時のデフォルト状態にあると想定されているため、デバイスの事前チェック、自動フラッシュクリーンアップ、事後チェックは行われません。

- デバイスに適用する [Onboarding Configuration] テンプレートを定義します。このようなテンプレートには、ネットワーク上で管理できるようにデバイスをオンボードするための基本的なネットワーク設定コマンドが含まれています。デバイス設定の変更を自動化するテンプレートの作成 （571 ページ）を参照してください。

（注） [Onboarding Configuration] テンプレートで `ip http client source-interface` CLI コマンドを使用すると、Catalyst Center はその IP アドレスをデバイスの管理 IP アドレスとして使用でき、特に複数の IP または VRF のシナリオにおいて有用です。

- デバイスのネットワークプロファイルを定義します。ネットワークプロファイルの概要（535 ページ）を参照してください。

プラグアンドプレイのシステム証明書の要件

HTTP から HTTPS への安全な移行を容易にするために、PnP 検出プロセスには、有効なシステム証明書が必要です。システム証明書が正しく設定されていない場合、PnP 検出は失敗します。デバイスを正常に検出するには、次の要件を確認してください。

- システム証明書に、SAN IP および SAN FQDN を含む必要なすべての情報カテゴリ代替名（SAN）フィールドが含まれていることを確認します。
- DHCP オプション 43 文字列で設定された FQDN は、システム証明書に存在する FQDN と一致する必要があります。
- システム証明書で定義されているすべてのホスト名が、DNSインフラストラクチャ経由で解決可能であることを確認します。

証明書の設定と検出時に入力されたアドレスに不一致がある場合、デバイスはセキュアな接続を確立できず、検出に失敗します。

DHCP コントローラディスカバリ

シスコのネットワークデバイスは初回起動時にスタートアップ設定を使用しない場合、DHCP オプション 43 を使用して Catalyst Center コントローラの検出を試行します。

DHCP による検出方法の前提条件には、次が含まれます。

- 新しいデバイスが DHCP サーバにアクセスできる。
- DHCP サーバが Cisco Plug and Play のオプション 43 を使用して設定されている。DHCP オプション 43 を設定する場合は、Catalyst Center 企業 IP、企業仮想 IP（VIP）、または完全修飾ドメイン名（FQDN）を使用できます。FQDN を使用している場合は、ホスト名を正しい Catalyst Center クラスタアドレスに解決するように DNS サーバーが設定されていることを確認します。

  DHCP サーバが文字列「ciscopnp」を含むオプション 60 を使用してデバイスから DHCP の検出メッセージを受信すると、オプション 43 の情報を含む応答をデバイスに返します。デバイスの Cisco Plug and Play IOS エージェントは、応答から Catalyst Center コントローラの IP アドレスを抽出し、このアドレスを使用してコントローラと通信します。

（注） Lightweight AP の場合、オプション 60 には文字列 `ciscopnp` は含まれません。代わりに、Lightweight AP のベンダークラス識別子（VCI）が含まれています。プラグアンドプレイが Lightweight AP を検出できるように、必要に応じて DHCP サーバールールを設定します。詳細については、「Configure DHCP OPTION 43 for Lightweight Access Points」 [英語] を参照してください。

DHCP オプション 43 は、DHCP サーバとして機能する Cisco ルータ CLI で、次の例のように設定された文字列の値で構成されます。

```
ip dhcp pool pnp_device_pool          <-- Name of DHCP pool
network 192.168.1.0 255.255.255.0     <-- Range of IP addresses assigned to clients
default-router 192.168.1.1            <-- Gateway address
option 43 ascii "5A1N;B2;K4;I172.19.45.222;J80;"    <-- Option 43 string
```

このオプション 43 の文字列には、セミコロンで区切られた次のようなコンポーネントが含まれています。

- 5A1N;（プラグ アンド プレイ用の DHCP サブオプション、アクティブ動作、バージョン 1、デバッグ情報なし）。文字列のこの部分は変更する必要がありません。
- B2;（IP アドレスのタイプ）：
  - B1 = ホスト名
  - B2 = IPv4（デフォルト）

- I*xxx.xxx.xxx.xxx*：Catalyst Center コントローラのエンタープライズ IP またはエンタープライズ VIP アドレスまたはホスト名（大文字の i の後）。エンタープライズ VIP の設定は単一ノードの展開では任意ですが、3 ノードのクラスタでは必須です。この例では、IP アドレスは 172.19.45.222 です。
- J*xxxx*：Catalyst Center コントローラへの接続に使用するポート番号。HTTP にはポート 80 を使用する必要があります。

（注） PnP 検出中に信頼できる証明書をインストールした後、デバイスは自動的に HTTPS にポート 443 を使用するように切り替わります。

- K4;：デバイスとコントローラの間で使用されるトランスポート プロトコル。
  - K4 = HTTP（デフォルト）
  - K5 = HTTPS
- T*TrustedCertificateBundleURL*：デフォルト（Catalyst Center コントローラ）以外の別の場所から信頼できる証明書のバンドルを取得する場合は、このオプションパラメータを使用して信頼できる証明書のバンドルの外部 URL を指定します。APIC-EM コントローラは、Cisco InfoSec Cloud（http://www.cisco.com/security/pki/）からバンドルを取得します。たとえば、10.30.30.10 の TFTP サーバからバンドルをダウンロードするには、パラメータを「Tftp://10.30.30.10/ios.p7b」と指定します。

  信頼できる証明書のセキュリティを使用していて、T パラメータを指定しない場合、デバイスは Catalyst Center コントローラから信頼できる証明書のバンドルを取得します。
- Z*xxx.xxx.xxx.xxx*;（NTP サーバの IP アドレス）。信頼できる証明書のセキュリティを使用してすべてのデバイスを同期させる場合、このパラメータは必須です。

DHCP の設定の詳細については、『*Cisco IOS Command Reference*』を参照してください。

DHCP オプション 43 が設定されていない場合、デバイスが DHCP サーバに接続できない場合、またはこの方法が別の理由で失敗する場合は、ネットワークデバイスは DNS を使用して検出を試行します。詳細については、DNS コントローラディスカバリ （704 ページ）を参照してください。

Catalyst Center システム証明書に FQDN のみの SAN フィールドがある場合、PnP を開始する前に、シードデバイスの DHCP プールを編集して、FQDN、B2 ー B1、dns-server、および domain-name を含むオプション 43 文字列を含める必要があります。

DHCP プールがシスコスイッチまたはルータに依存している場合、次の設定例のようになります。

```
ip dhcp pool PnP_Pool
network 214.2.64.0255.255.255.0
default-router 214.2.64.1
option 43 ascii "5A1D;B1;K4;I<FQDN>;J80;"
```

```
domain-name sitdns.com
dns-server 17.1.104.100
```

DNS コントローラディスカバリ

DHCP ディスカバリが Catalyst Center コントローラの IP アドレスを取得できない場合、ネットワークデバイスは DNS ルックアップ方式にフォールバックします。DHCP サーバから返されたネットワークドメイン名に基づき、事前設定されたホスト名「pnpserver」を使用して、コントローラの完全修飾ドメイン名（FQDN）を作成します。NTP のサーバ名は、事前設定されたホスト名 pnpserver に基づいています。

たとえば、DHCP サーバからドメイン名「customer.com」が返された場合、ネットワークデバイスは「pnpserver.customer.com」というコントローラの FQDN を作成します。次に、この FQDN の IP アドレスを解決するために、ローカル ネーム サーバを使用します。NTP サーバ名の FQDN は pnpntpserver.customer.com です。

DNS による検出方法の前提条件には、次が含まれます。

- 新しいデバイスが DHCP サーバにアクセスできる。
- Catalyst Center コントローラがホスト名「pnpserver」を使用して展開されている。
- NTP のサーバ名はホスト名「pnpserver」で展開される。

Plug and Play Connect コントローラディスカバリ

DHCP または DNS による検出方法の使用がオプションでない場合は、Cisco Plug and Play Connect クラウド サービスによって、デバイスが Catalyst Center コントローラの IP アドレスを検出できます。ネットワークデバイスが起動すると、DHCP または DNS を介してコントローラを特定できない場合に、devicehelper.cisco.com に接続して Plug and Play Connect を試行し、組織に定義されている適切なコントローラの IP アドレスを取得します。通信を保護するために、デバイスは Plug and Play Connect に接続するときに、最初にシスコの信頼できる証明書のバンドルをダウンロードしてインストールします。

次の手順では、検出に Plug and Play Connect を使用して、Cisco Plug and Play でシスコのネットワークデバイスを展開する方法についての概要を説明します。

始める前に

シスコの各種ネットワークデバイスは、Cisco Plug and Play をサポートし、Cisco Plug and Play Connect クラウドサービスに接続している Cisco IOS イメージを実行しています。

手順

ステップ 1 ネットワーク管理者は、Cisco スマートアカウントの Web ポータルにある Plug and Play Connect を使用して、組織に適した Catalyst Center コントローラのコントローラ プロファイルを設定します。詳細については、web ポータルのスマートアカウントのマニュアルを参照してください。

ステップ 2 Cisco Commerce Workspace（CCW）を介してプラグアンドプレイ ネットワークデバイスを注文した場合、Cisco スマートアカウントが注文に割り当てられていれば、Plug and Play Connect を使用してネットワークデバイスが自動的に登録されます。Cisco Plug and Play で使用する各デバイスに、NETWORK-PNP-LIC オプションを追加します。

このオプションにより、デバイスのシリアル番号と PID がプラグアンドプレイ用にスマート アカウントで自動登録されます。デフォルト コントローラを指定済みの場合、注文の処理時にデバイスがそのコントローラに自動的に割り当てられます。

ステップ 3 または、Plug and Play Connect の Web ポータルからデバイスを手動で追加することもできます。

ステップ 4 Catalyst Center を、Cisco Plug and Play Connect のコントローラとして、リダイレクト サービス用に Cisco スマートアカウントに登録します。バーチャルアカウントプロファイルの登録または編集（712 ページ）を参照してください。

CCW を通してプラグアンドプレイ ネットワーク デバイスを注文し、これらのネットワークデバイスがスマートアカウント経由で Plug and Play Connect に自動登録される場合には、この手順が必須です。

ステップ 5 Cisco Plug and Play Connect クラウドポータルのスマートアカウントから、デバイス インベントリを Catalyst Center プラグ アンド プレイに同期します。

Plug and Play Connect の Web ポータルに登録されたデバイスがコントローラに同期され、SmartAccount のソースとともにプラグ アンド プレイのデバイス リストに表示されます。

ステップ 6 新しく同期されたデバイスを要求します。プラグアンドプレイ対応デバイスのプロビジョニング（716 ページ）を参照してください。

ステップ 7 デバイス インストーラによって、シスコ ネットワークデバイスがインストールされ、電源が投入されます。

ステップ 8 デバイスは、Plug and Play Connect サービスをクエリして Catalyst Center コントローラを検出し、Catalyst Center でプラグ アンド プレイのシリアル番号によってコントローラを識別します。次に、要求プロセス中に計画された内容に従ってプロビジョニングされます。

（注） デバイスが定義済みの NTP サーバ **time-pnp.cisco.com** または **pool.ntp.org** と同期できない場合、デバイスは Plug and Play Connect のコンタクトに失敗します。この問題を解決するには、これらの 2 つのホスト名への NTP トラフィックをブロック解除するか、これら 2 つの NTP ホスト名を DNS サーバーのローカル NTP サーバーアドレスにマッピングします。

プラグアンドプレイ展開のガイドライン

ルータ、スイッチ、ワイヤレスコントローラにプラグアンドプレイを使用する場合は、次の推奨事項に従ってください。

- デバイスの起動順序：一般に、ルーティングとアップストリームデバイスは最初に展開する必要があります。ルータおよびすべてのアップストリームデバイスがアップされてプロ

ビジョニングされると、スイッチとダウンストリームデバイスを展開できます。デバイスのプラグ アンド プレイ エージェントは最初のデバイスの起動時のみ、Catalyst Center コントローラの自動検出を試みます。現時点で、デバイスがコントローラに接続できない場合、デバイス プロビジョニングは失敗するため、アップストリーム デバイスは最初にプロビジョニングする必要があります。

- シスコのルータトランク/アクセスポートの構成：一般的なブランチネットワークには、ルータとスイッチが含まれます。1 つ以上のスイッチは WAN ルータに接続され、IP フォンやアクセス ポイントなどの他のエンドポイントはスイッチに接続します。スイッチがアップストリームルータに接続されると、次の展開モデルはプラグアンドプレイでサポートされます。
  - ダウンストリーム スイッチはルータのスイッチ ポートを使用してルータに接続されます。このタイプの接続では、ルータのスイッチ ポートをトランクまたはアクセスポートとして設定できます。
  - ルータのルーテッド ポートを使用してダウンストリーム スイッチをルータに接続する。この場合、ルーテッド ポートはサブインターフェイスを使用して複数の VLAN をサポートできます。プラグアンドプレイのプロセス中、スイッチはそのポートを自動的にトランクポートとして設定します。大規模ブランチの場合は、ルータとダウンストリーム スイッチ間に複数の VLAN を設置する必要があります。このような使用例をサポートするには、スイッチをルーテッド ポートに接続する必要があります。
- 非 VLAN 1 構成：プラグアンドプレイは、VLAN 1 を使用して、デフォルトでデバイスをサポートします。1 以外の VLAN を使用するには、隣接するアップストリームデバイスでサポート対象のリリースが実行されていなければなりません。また、そのアップストリームデバイスに「**pnp startup-vlan** *x*」グローバル CLI コマンドを設定して、以降のプラグアンドプレイデバイスにこの CLI をプッシュする必要があります。隣接するアップストリーム デバイスでこのコマンドを実行した場合、そのアップストリーム デバイスでは VLAN メンバーシップの変更は行われません。ただし、アップストリームに接続された、以降のプラグアンドプレイデバイス上のアクティブインターフェイスは、指定された VLAN に変更されます。このガイドラインは、ルータとスイッチの両方に適用され、アクセスモードではなくトランクモードのシナリオでのみ使用する必要があります。

デバイスの表示

[Plug and Play] ウィンドウでデバイスに関する情報を表示できます。

さらに、このウィンドウからいくつかのタスクを実行できます。詳細は、次のトピックを参照してください。

- デバイスの追加または編集 （710 ページ）
- デバイスの一括追加 （711 ページ）
- スマートアカウントからのデバイスの追加 （714 ページ）

- プラグアンドプレイ対応デバイスのプロビジョニング （716 ページ）
- デバイスのリセット （733 ページ）
- デバイスの削除 （732 ページ）

手順

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

[プラグアンドプレイ（Plug and Play）] ウィンドウには、次のデバイス情報を含むテーブルが表示されます。

表 *46* : デバイス情報

カラム	説明
#	行番号。
Device Name	デバイスのホスト名。このリンクをクリックすると、デバイスの詳細ウィンドウが開きます。スタック アイコンはスイッチ スタックを示します。
Serial Number	デバイスのシリアル番号。
Product ID	デバイスの製品 ID。
IP Address	デバイスの IP アドレス。
Source	デバイスエントリの送信元： • [User]：ユーザーが GUI または API を介してデバイスを追加しました。 • [Network]：コントローラに接続されたデバイスが要求解除されました。 • [SmartAccount]：デバイスはスマートアカウントから同期されました。
State	• [Unclaimed]：デバイスは正常に初期化が完了し、要求される準備ができているか、または [Planned] 状態になっています。 • [Planned]：ユーザーがデバイス構成またはプロビジョニングパラメータを指定し、デバイスをプロビジョニングする準備ができています。 • [Onboarding]：デバイスオンボーディングが進行中です。 • [Provisioned]：デバイスは正常にオンボーディングされ、インベントリに追加されています。AP とセンサーの場合、デバイスが ワイヤレスコントローラに正常に割り当てられると、状態が [Provisioned] に変わります。 • [Error]：デバイスにエラーがあり、プロビジョニングできませんでした。

カラム	説明
Onboarding State	デバイスのオンボーディング状態： • [Not Contacted]：デバイスが呼び出されていません。ユーザーがデバイスを追加またはリセットした可能性があります。 • [Connecting]：デバイスが呼び出されました。 • [Initializing]：システムワークフローを実行しています。基本的なデバイス情報が収集されます。スタックライセンスとバージョンの不一致が修正されます。 • [Initialized]：システムワークフローが完了しました。 • [Executing Workflow]：要求中に選択されたタスクは、この状態で適用されます。スタックは、製品およびイメージのバージョンに基づく番号の再割り当てとライセンスの更新をサポートしています。 • [Executed Workflow]：ユーザーワークフローが完了しました。 • [Connection Error]：接続を保護するための証明書をインストールできませんでした。 • [Authentication Error]：SUDI 証明書を検証できませんでした。 • [Authorization Error]: ユーザーが指定した SUDI シリアル番号を確認できませんでした。 • [Initialization Error]：システムワークフローの実行中にエラーが発生しました。 • [Workflow Execution Error]：ユーザーワークフローの実行中にエラーが発生しました。 • [Executing Reset]：リセットワークフローを実行しています。エラーが発生したデバイスを手動でリセットする必要があります。リセットすると、デバイスがリロードされます。 • [Reset Execution Error]：リセットワークフローの実行中にエラーが発生しました。 デバイスの履歴に移動するには、経過表示バーをクリックします。
サイト	デバイスが関連付けられているサイト。
Last Contact	デバイスが最後にプラグ アンド プレイに接続した日時。
Smart Account	デバイスが関連付けられている Cisco スマート アカウント。
Virtual Account	デバイスが関連付けられている（Cisco スマート アカウント内の）バーチャル アカウント。
Created	デバイスがプラグ アンド プレイに追加された日時。

デバイステーブルには、各デバイスについて、以下の表に示した情報が表示されます。一部の列はソートに対応しています。

（注）
- [Device Name] や [Serial Number] などの特定の列は、[Default] フォーカスビューに表示されます。
- [Devices]テーブルをカスタマイズして、列の表示と非表示を切り替えることができます。設定アイコン（⚙）をクリックして [Table Settings] スライドインペインを表示し、[Edit Table Columns] タブで表示する列や非表示にする列を選択します。[Apply] をクリックして、変更内容を保存します。

ステップ 2 [プラグアンドプレイ（Plug and Play）] ウィンドウから、次の方法でデバイス情報の表示を制御できます。

- 行を昇順または降順に並べ替えるには、キャロット矢印アイコン ▲ が付いている列ヘッダーをクリックします。
- 特定の状態のデバイスを表示するには、[Device Status] フィルタから、[Unclaimed]、[Error]、[Provisioned]、または [All] を選択します。
- ビューをフォーカスするには、[Focus] ドロップダウンリストから [Default] または [All] を選択します。
- テーブル情報の更新のタイミングを変更するには、[Auto-Refresh] ドロップダウンリストをクリックして、望ましい更新間隔を選択します。デフォルトでは、デバイステーブルは 30 秒ごとに更新されます。
- 特定のデバイスを見つけるには、[Filter] または [Find] オプションを使用します。
- デバイスの詳細を表示するには、デバイス名をクリックします。

  その他の詳細を表示するには、開いたウィンドウで、[Details]、[History]、または [Configuration] タブをクリックします。スイッチスタックの場合は、[Stack] タブをクリックすることもできます。一部のタブには、クリックしてさらに詳細を表示できる追加のリンクがあります。

（注） スイッチスタックからスタックメンバーを削除するには、[Stack] タブで、削除するメンバーの横にあるチェックボックスをオンにして、[Delete Member] をクリックします。

デバイスの追加または編集

この手順では、[Plug and Play Devices] リストからデバイスを追加または編集する方法について説明します。代わりに、[編集（Edit）] をクリックしてデバイスの詳細ウィンドウからデバイスを編集することもできます。

表 *47*：デバイスフィールド

フィールド	説明
[Serial Number]	デバイス シリアル番号（デバイスを編集している場合は読み取り専用）。
Product ID	デバイス製品 ID（デバイスを編集している場合は読み取り専用）。
[Device Name]	デバイス名
Enable SUDI Authorization	セキュアな固有デバイス識別子（SUDI）認証をサポートするデバイスで有効にします。有効にすると、デバイスがプラグアンドプレイサーバーに接続しようとしたときに、サーバーによって、SUDI 証明書のシリアル番号とユーザーが提供するシリアル番号が比較されます。シリアル番号が一致すると、デバイスが検証され、プラグアンドプレイサーバーに接続されます。
SUDI Serial Numbers	SUDI をサポートするデバイスには、シャーシのシリアル番号と SUDI シリアル番号（デバイス ラベルのライセンス SN と呼ばれる）の 2 つのシリアル番号があります。SUDI 認証を使用するデバイスを追加するときは、このフィールドに 1 つまたは複数の SUDI シリアル番号をカンマで区切って入力します。このフィールドは、[SUDI 認証の有効化（Enable SUDI Authorization）] がチェックされている場合にのみ表示されます。
This Device Represents a Stack	デバイスがスタックを表します（デバイスを編集している場合、この項目は読み取り専用です）。サポート対象のスタッカブルスイッチにのみ適用されます。

始める前に

デバイスにログイン情報が必要な場合は、グローバルデバイスログイン情報が **[Design]** > **[Network Settings]** > **[Device Credentials]** ページで設定されていることを確認します。詳細については、グローバル CLI クレデンシャルの追加 （379 ページ）を参照してください。

手順

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

ステップ 2 テーブル内のデバイスを表示します。

[Device State] のいずれかのボタンを使用してデバイスの状態でフィルタ処理したり、[Filter] オプションを使用して特定のデバイスを検索したりできます。[Refresh] をクリックしてデバイスリストを更新します。

ステップ 3 デバイスを追加または編集するには、次の手順を実行します。

- デバイスを追加するには、[Add Devices] をクリックし、[Single Device] をクリックします。
- デバイスを編集するには、編集するデバイス名の横にあるチェック ボックスをオンにして、デバイステーブルの上部にあるメニュー バーから **[Actions]** > **[Edit]** の順に選択します。[デバイスの編集（Edit Device）] ダイアログが表示されます。

ステップ 4 必要に応じてフィールドを設定します。詳細については上記の表を参照してください。

ステップ 5 次のいずれかのタスクを実行して、設定を保存します。

- デバイスを追加し、後で要求するには、[デバイスの追加（Add Device）] をクリックします。
- デバイスを追加し、すぐに要求するには、[追加 + 要求（Add + Claim）] をクリックします。デバイスの要求の詳細については、プラグアンドプレイ対応デバイスのプロビジョニング （716 ページ）を参照してください。
- デバイスを編集する場合は、[デバイスの編集（Edit Device）] をクリックします。

デバイスの一括追加

この手順では、CSV ファイルからデバイスを一括で追加する方法を示します。

手順

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

ステップ 2 [Add Devices] をクリックします。

[デバイスの追加（Add Device）] ダイアログが表示されます。

ステップ 3 [Bulk Devices] をクリックします。

ステップ 4 [Download File Template] をクリックしてファイルテンプレートをダウンロードします。

さまざまなデバイスの必須のフィールドとオプションのフィールドについては、ファイルテンプレートを参照してください。

ステップ 5 各デバイスの情報をファイルに追加し、ファイルを保存します。

デバイスタイプに基づいて、必須フィールドにデータを入力します。

（注） ファイルテンプレートを使用して追加されたサイトがネットワーク階層に存在しない場合、そのデバイスは削除されます。

ワイヤレスコントローラ の場合、Catalyst Center は IP アドレスタイプ（IPv4 アドレス、IPv6 アドレス、またはその両方）に基づいてデータを処理します。

ステップ 6 次のアクションのいずれかを実行して、CSV ファイルをアップロードします。

- ドラッグ アンド ドロップ エリアにファイルをドラッグアンドドロップします。
- [ファイルの選択（Choose a file）] をクリックし、CSV ファイルの保存場所を参照して [開く（Open）] をクリックします。

ステップ 7 **[デバイスのインポート（Import Devices）]** をクリックします。

CSV ファイル内のデバイスがテーブルにリストされます。

ステップ 8 インポートする各デバイスの横にあるチェックボックスをオンにするか、上部にあるチェックボックスをオンにしてすべてのデバイスを選択します。

ステップ 9 次のいずれかのタスクを実行して、デバイスを追加します。

- デバイスを追加し、それらを後で要求するには、**[デバイスの追加（Add Devices）]** をクリックします。
- デバイスを追加し、それらをすぐに要求するには、[追加 + 要求（Add + Claim）] をクリックします。デバイスの要求の詳細については、プラグアンドプレイ対応デバイスのプロビジョニング （716 ページ）を参照してください。

バーチャル アカウント プロファイルの登録または編集

リダイレクトサービスの場合、Cisco スマートアカウントで、Catalyst Centerを Cisco Plug and Play Connect のコントローラとして登録します。これにより、Cisco Plug and Play Connect クラウドポータルから Catalyst Centerの Cisco Plug and Play にデバイスインベントリを追加できます。

スマートアカウント、バーチャルアカウント、および関連するサーバーのプロファイル情報を、Plug and Play システムとデータベースに登録できます。登録された仮想アカウントのデバイスは、プラグ アンド プレイ データベースと同期されます。

表 *48 :* バーチャルアカウント フィールド

オプション	説明
スマートアカウントの選択	Cisco スマート アカウント名

オプション	説明
バーチャル アカウントの選択	バーチャルアカウント名バーチャルアカウントは、Cisco スマートアカウント内のサブアカウントです。
IP または **FQDN**	[IP]：この Catalyst Center コントローラの IPv4 アドレス、IPv6 アドレス、または両方のタイプの IP アドレス。 [FQDN]：この Catalyst Center コントローラの完全修飾ドメイン名。
プロファイル名	コントローラのプロファイル名
デフォルト コントローラ プロファイルとして使用	*[Default controller profile]* とは、仮想アカウントに追加された新しいデバイス、またはデフォルトのコントローラが割り当てられていない既存のデバイスは、このリダイレクトプロファイルに割り当てられることを意味します。

手順

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

ステップ 2 テーブル内のバーチャルアカウントを表示します。

このテーブルには、登録されている Plug and Play Connect のバーチャル アカウント プロファイルがすべて一覧表示されます。

ステップ 3 バーチャル アカウント プロファイルを登録または編集します。

- バーチャルアカウントを登録するには、[Register] をクリックします。[Register Virtual Account] ペインが表示されます。
- 登録済みのバーチャルアカウントプロファイルを編集するには、編集するプロファイル名の横にあるオプションボタンをクリックし、[Edit Profile] をクリックします。[Edit Profile] ペインが表示されます。

ステップ 4 必要に応じてフィールドを設定します。

ステップ 5 次のいずれかのタスクを実行して、設定を保存します。

- 新しいバーチャルアカウント プロファイルを登録する場合は、[Register] をクリックします。
- バーチャル アカウント プロファイルを編集している場合は、[Save] をクリックします。

次のタスク

Cisco Plug and Play Connect クラウド ポータルから、デバイス インベントリを Catalyst Center プラグ アンド プレイに同期します。詳細については、スマートアカウントからのデバイスの追加 （714 ページ）を参照してください。

スマートアカウントからのデバイスの追加

このタスクにより、Cisco Plug and Play Connect クラウド ポータルのスマート アカウントから Catalyst Center プラグ アンド プレイにデバイス インベントリを同期することができます。

バーチャル アカウント テーブルには、各プロファイルに関する次のような情報が表示されます。

表 *49* : バーチャルアカウント情報

カラム	説明
バーチャル アカウント	バーチャルアカウント名
スマート アカウント	バーチャルアカウントが関連付けられているスマートアカウント
プロファイル	プロファイル名
コントローラ	コントローラ IP アドレス

始める前に

Cisco プラグアンドプレイ接続クラウド ポータルからデバイスインベントリを同期する前に、バーチャルアカウントを登録する必要があります。バーチャル アカウント プロファイルの登録または編集 （712 ページ）を参照してください。**[Add Devices]** > **[Smart Account Devices]** ダイアログの **[PnP Connect]** リンクをクリックすると、[PnP Connect] 設定ページに直接移動できます。

手順

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

ステップ 2 [Add Devices] をクリックします。

ステップ 3 [Smart Account Add] をクリックし、[Add Devices from a Smart Account] スライドインペインを開きます。

ステップ 4 cisco.com ユーザーを設定済みの場合は、ステップ 5 に進みます。設定していない場合は、次の手順を実行します。

a) ブラウザでシークレット/プライベートウィンドウを開きます（以前にキャッシュされたログイン情報の使用を避けるため）。

b) 別の Catalyst Center GUI インスタンスを開いてログインします。

c) [Add Devices from a Smart Account] スライドインペインの別のインスタンスを開きます。

d) 次のいずれかのタスクを完了します。

次の場合は...	次の操作...
Catalyst Center 2.3.7.9 の新規インストールを完了します。	[Cisco.com ID] フィールドの [Add] リンクをクリックして、新しい cisco.com ユーザーを設定します。
Catalyst Center 2.3.7.9 にアップグレードし、以前に設定されたユーザーと同じcisco.com ユーザーを使用する場合：	[Cisco.com ID] フィールドの [Re-Authenticate] リンクをクリックして該当ユーザーを再認証します。
Catalyst Center 2.3.7.9 にアップグレードし、以前に設定されたユーザーと同じ cisco.com ユーザーを使用しない場合：	古い cisco.com ユーザーを削除してから、新しいユーザーを設定します。 **1.** [Cisco.com ID] フィールドの [Delete] リンクをクリックします。 **2.** 表示されたダイアログボックスで、[Delete] をクリックして操作を確定します。 **3.** [Cisco.com ID] フィールドの [Add] リンクをクリックします。

e) [Information] ポップアップウィンドウで、次のチェックボックスの一方または両方をオンにして、[Authenticate] をクリックします。

- （必須）[I am in private or incognito mode]
- （オプション）[Save Credentials]

f) [Activate your device] ポップアップウィンドウで、アクティベーションコードが表示されていることを確認し、[Next] をクリックします。

g) [Log in] ポップアップウィンドウで、cisco.com ユーザの電子メールアドレスを入力し、[Next] をクリックします。

h) [Verify with your password] ポップアップウィンドウで、cisco.com ユーザーのパスワードを入力し、[Verify] をクリックします。

[Device Activated] ポップアップウィンドウが表示されます。

i) [Device Activated] ポップアップウィンドウを閉じます。

j) [Plug and Play] ウィンドウを更新し、**[Add Devices]** > **[Smart Account Add]**をクリックし、[Add Devices from a Smart Account] スライドインペインを再度開きます。

k) [Cisco.com ID] フィールドに、ユーザーに対して入力した電子メールアドレスが表示されていることを確認します。また、[Change] リンクが表示されていることを確認します。

ステップ 5 プラグアンドプレイに登録するスマートアカウントとバーチャルアカウントを選択します。

PnP Connect バーチャル アカウント プロファイルを登録する必要がある場合は、[PnP Connect] リンクをクリックします。Cisco ID を変更する場合は、[Not me?] リンクをクリックします。

ステップ 6 [Devices] テーブルから、追加するデバイスを選択し、[Add Devices] をクリックします。

追加されたデバイスは、SmartAccount に設定されたソースとともに [Plug and Play Devices] テーブルに表示されます。

次のタスク

新しく追加されたデバイスを請求処理します。デバイスの要求の詳細については、プラグアンドプレイ対応デバイスのプロビジョニング （716 ページ）を参照してください。

プラグアンドプレイ対応デバイスのプロビジョニング

デバイスを要求すると、デバイスをプロビジョニングするプロセスが開始されます。デバイスがプロビジョニングされると、Catalyst Center は次のアクションを実行します。

1. イメージをデバイスに展開します。
2. 次の設定を構成するシステム構成 CLI コマンドを展開します。
   - デバイスのログイン情報（CLI および SNMP）
   - SSH v2 および SCP サーバの有効化
   - HTTP および HTTPS サーバの無効化
   - スイッチでは、vtp モードの透過が有効になっています
3. デバイスのタイプに対応するデバイスオンボーディング構成テンプレートを展開します。
   - 有線デバイスの場合、Catalyst Center は定義したオンボーディング設定（Day-0）テンプレートを展開します。
   - ワイヤレスデバイスの場合、Catalyst Center はサイトに割り当てられたネットワークプロファイルに基づいて構成を展開します。

   オンボーディング構成テンプレートに同じシステム構成 CLI コマンドのいずれかが含まれている場合、オンボーディング構成テンプレートはシステム構成 CLI コマンドの後にデバイスに適用されるため、システム構成 CLI コマンドはオーバーライドされます。
4. デバイスのプロビジョニング先のサイトで QoS ポリシーを設定した場合は、有線デバイスに Application Quality of Service（QoS）ポリシーを展開します。詳細については、アプリケーションポリシーの作成 （1470 ページ）を参照してください。
5. デバイスのオンボーディング中に、ポート 830 で NETCONF 設定をプッシュします。NETCONF ポート情報は、グローバルログイン情報とネットワーク設定に保存されます。

（注）
- 標準ポート 830 ではなく誤ったポートを通じて NETCONF がプッシュされた場合、デバイスはオンボーディングを正常に完了しますが、インベントリに追加することはできません。
- 要求プロセス時にデバイスがサイトに割り当てられていない場合、NETCONF はそのデバイスでは設定されません。
- 自動 NETCONF 有効化のサポートは、次でのみ使用できます。
  - Cisco IOS XE 17.3 以降のリリースを実行している Cisco Catalyst 9000 シリーズ スイッチ、および
  - Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ。

6. アプリケーションテレメトリおよびコントローラベースのアプリケーション認識（CBAR）が、該当するネットワークデバイスで有効になっています。
7. デバイスをインベントリに追加します。
8. PnP ラベルトラストポイントは、デバイスが Day-0 オンボーディングを正常に完了し、一覧で管理状態になり、サイトに割り当てられると、自動的に削除されます。

（注） あるデバイスについてデバイスの可制御性が有効になっている場合（デフォルトで有効）、デバイスがインベントリに追加された、またはサイトに割り当てられたときに、追加の設定がデバイスにプッシュされます。詳細については、*Cisco Catalyst Center Administrator Guide* の「Device Controllability」の項を参照してください。

まだ起動していないデバイスを初めて要求する場合、デバイスは起動時に自動的にプロビジョニングされます。このプロセスは、デバイスのプランニングと呼ばれます。

デバイスをプロビジョニングするための手順は、デバイスのタイプによって異なります。

- スイッチとルータの参照資料：スイッチまたはルータデバイスのプロビジョニング （717 ページ）
- シスコ ワイヤレス コントローラ、AP、およびセンサー：ワイヤレスコントローラ のプロビジョニング （722 ページ）

スイッチまたはルータデバイスのプロビジョニング

この手順では、[Plug and Play Devices] リストからデバイスを要求する方法について説明します。代わりに、[Claim] をクリックしてデバイスの [Details] ウィンドウからデバイスを要求することもできます。

始める前に

プラグ アンド プレイ プロビジョニングの前提条件が満たされていることを確認します。詳細については、プラグ アンド プレイ プロビジョニングの前提条件 （698 ページ）を参照してください。

手順

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

ステップ 2 テーブル内のデバイスを表示します。

デバイスを表示するには、[Focus] ドロップダウンリストから [Default] または [All] を選択します。

デフォルトでは、デバイステーブルは 30 秒ごとに更新されます。[Auto-Refresh] ドロップダウンリストをクリックして、更新間隔を選択します。

[Filter] または [Find] オプションを使用して、特定のデバイスを見つけます。

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

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

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

a) 必要に応じてデバイスのホスト名を変更します。

b) 次のいずれかのタスクを実行して、サイトを割り当てます。

- 各デバイスに異なるサイトを割り当てるには、[Assign] をクリックし、[Select a Site] ドロップダウンリストからサイトを選択します。
- 最初のデバイスと同じサイトを他のすべてのデバイスに割り当てるには、[Actions] 列で、省略記号アイコン ••• の上にカーソルを置き、[Apply Site to All] を選択します。
- あるデバイスのサイトを別のデバイスに割り当てるには、[Actions] 列で、省略記号アイコン ••• の上にカーソルを置き、[Assign this Site to Other Devices] をクリックし、デバイスを選択して [Assign] をクリックします。
- デバイスに割り当てられたサイトをクリアするには、[Clear Site] をクリックします。

（注） デバイスをサイトに割り当てていない場合は、ステップ 6 （718 ページ） でデバイスのテンプレートを選択する必要があります。

c) [Next] をクリックします。

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

a) [Configuration] 列で、設定するデバイスの [Assign] をクリックします。

b) デバイス構成を変更する必要がない場合は、[Cancel] をクリックして、次のステップに進みます。それ以外の場合は、次のいずれかの設定を変更または設定します。

- [Device Name]：必要に応じてデバイスのホスト名を変更します。
- [Image]：このドロップダウンリストで、デバイスに適用するゴールデン ソフトウェア イメージを選択します。イメージリポジトリにこのデバイスタイプのゴールデンイメージが 1 つしかない場合は、そのイメージがデフォルトで選択されます。

（注） デバイスのソフトウェア イメージ バージョンまたはゴールデンタグ付きバージョンが 17.14.1 以降の場合、選択したサイトで SNMP ログイン情報に MD5 認証が設定されていると、デバイス要求がブロックされます。

ゴールデンイメージが利用できず、イメージがイメージリポジトリ内で、このデバイスタイプの特定のデバイスロール（Border、Core など）でタグ付けされている場合、ドロップダウンリストに利用可能なイメージが表示されます。

デバイスを要求するには、SNMP ログイン情報に SHA 認証も設定する必要があります。あるいは、ソフトウェア イメージ バージョンが 17.14.1 より前である必要があります。SHA 認証の設定方法については、「グローバル デバイス クレデンシャルの編集 （394 ページ）」を参照してください。

- [Template]：このドロップダウンリストで、デバイスに適用するオンボーディング設定テンプレートを選択します。このデバイスタイプに対して定義されているオンボーディング設定テンプレートが 1 つしかない場合は、そのテンプレートがデフォルトで選択されます。

（注） デバイスをサイトに割り当てていない場合は、デバイスのテンプレートを選択する必要があります。選択するテンプレートには、デバイスにグローバル デバイス ログイン情報を設定するために必要な CLI コマンドを含める必要があります。それ以外の場合、デバイスは管理対象外の状態で一覧に追加されます。

- [Apply the PKCS12 device certificate on the device]：PKCS12 証明書をデバイスに展開するには、このチェックボックスをオンにします。このオプションは、ルータの場合にのみ使用可能です。
- [RTU License Level]：このドロップダウンリストから、[Lanbase] または [IP Services] を選択します。このオプションは、Cisco Industrial Ethernet（IE）4000 シリーズおよび 5000 シリーズ スイッチでのみ使用できます。
- [Select a Cabling Scheme]：スタックの番号を付け直す場合は、このドロップダウンリストで、スタックのケーブル配線スキームを選択します。

この項目は、スタック構成をサポートしているスイッチが次のいずれかのケーブル配線スキームに従って接続されている場合にのみ表示されます。

図 *26 :* ケーブル配線スキーム



- [Select a Top of Stack Serial Number]：スタックスイッチの先頭のシリアル番号は、ユーザが入力したスタックメンバーのシリアル番号が自動入力されます。自動入力されたシリアル番号を使用しない場合は、シリアル番号をクリックし、[Select a Top of Stack Serial Number] で、ドロップダウンリストをクリックします。[X] アイコンをクリックして、シリアル番号の選択を解除します。

  このオプションは、スタック構成をサポートしているスイッチがケーブル配線図に示すように接続されている場合にのみ表示されます。

  計画されているデバイスの場合、スタックスイッチの先頭のシリアル番号がデフォルトとして設定されています。必要に応じて、別のシリアル番号を指定できます。

  要求されていないデバイスの場合、スタックスイッチの先頭のシリアル番号はデフォルトとして設定されません。ドロップダウンリストからスタックスイッチの先頭のシリアル番号を選択します。

- [Select a License Level]：このドロップダウンリストで、スタックのライセンスレベルを選択します。[X] アイコンをクリックして、ライセンス レベルの選択を解除します。

  この項目は、スタック構成をサポートしているスイッチにのみ表示されます。

c) [Save] をクリックします。

d) [Clear Configuration] ドロップダウンリストから、次のオプションのいずれかを選択します。

- [Clear Device Certificates]：このオプションを選択し、証明書をクリアする各デバイスの横にあるチェックボックスをオンにして、[Clear] をクリックします。
- [Clear Images]：このオプションを選択し、イメージをクリアする各デバイスの横にあるチェックボックスをオンにして、[Clear] をクリックします。
- [Clear Templates]：このオプションを選択し、テンプレートをクリアする各デバイスの横にあるチェックボックスをオンにして、[Clear] をクリックします。
- [Clear License Levels]：このオプションを選択し、ライセンスレベルをクリアする各デバイスの横にあるチェックボックスをオンにして、[Clear] をクリックします。

e) あるデバイスのイメージまたはテンプレートを他のデバイスに適用するには、[Actions] 列で、省略記号アイコン ••• の上にカーソルを置き、[Apply Image to Other Devices] または [Apply Template to Other Devices] を選択します。

スタック構成のデバイスの場合は、[Apply License Level to Other Devices] をクリックして、デバイスのライセンスレベルを他のデバイスに適用できます。

f) プロビジョニングするデバイスを複数選択した場合は、リストにある次のデバイスの [Assign] クリックし、この設定手順を繰り返します。これを、すべてのデバイスに対して実行します。

g) すべてのデバイスを設定したら、[Next] をクリックします。

ステップ 7 すべてのデバイスのテンプレートパラメータ値をまとめて設定するには、次のステップに進みます。デバイスのテンプレートパラメータ値を 1 つずつ設定するには、[Provision Templates] ウィンドウから、次の手順を実行します。

a) 設定するデバイスの名前をクリックします。

b) デバイスに設定テンプレートが割り当てられている場合は、テンプレートで定義されたパラメータの値を指定します。

各デバイスのフィールドに各パラメータの値を入力します。レッド アスタリスクは必須フィールドを表します。

c) 選択したデバイスの起動構成に実行中の構成をコピーする場合、[Copy running config to startup config] チェックボックスをオンにします。

d) 複数のデバイスを選択してプロビジョニングした場合は、ウィンドウの左側にあるリストで次のデバイスをクリックし、パラメータ値を入力します。これを、すべてのデバイスに対して実行します。

e) [Next] をクリックします。

ステップ 8 すべてのデバイスのパラメータ値を一括で指定するには、[Provision Templates] ウィンドウで次の手順を実行します。

a) [Export] をクリックして、CSV テンプレートファイルを保存します。

b) 各パラメータの値をファイルに追加して、ファイルを保存します。

c) [Import] をクリックします。

d) ドラッグアンドドロップ エリアにファイルをドラッグアンドドロップするか、[click to select] をクリックしてファイルを選択します。

e) [Import] をクリックします。

f) [Next] をクリックします。

ステップ 9 [Summary] ウィンドウで、デバイスに関する詳細や構成プレビューステータスを確認できます。

ステップ 10 設定プレビューが成功したかどうかを確認するには、各デバイスの [Day-0 Config] 列を確認します。

プレビューにエラーが表示された場合は、表の上にあるエラーメッセージの [Actions] リンクをクリックして、実行する必要があるアクションを確認します。アクションをクリックすると、変更が必要なウィンドウで新しいタブを開くことができます。

プロビジョニングエラーを回避するには、デバイスを要求する前に問題がある場合は解決します。必要に応じて、[Provision Templates] のステップに戻ってパラメータ値やテンプレートを変更したり、[Design] エリアに再度アクセスしてネットワーク設計の設定を更新したり、ネットワーク接続の問題があれば解決します。

問題を解決したら、[Day-0 Config] 列に戻り、[Retrying get Day-0 configuration Preview for failed device(s)] をクリックし、[OK] をクリックします。

ステップ 11 [Day-0 Config] 列のリンクをクリックして、デバイス、その構成、構成プレビューエラーの詳細を確認します。

ステップ 12 [Claim] をクリックします。

ステップ 13 確認のダイアログボックスで [Yes] をクリックしてデバイスを要求します。

次のタスク

ネットワーク設定を構成している場合は、デバイスでこれらの設定をプロビジョニングします。詳細については、プロビジョニングプロセスの完了 （730ページ）を参照してください。

ワイヤレスコントローラ のプロビジョニング

この手順では、[Plug And Play Devices] リストからワイヤレスコントローラを要求する方法について説明します。代わりに、[Claim] をクリックしてデバイスの [Details] ウィンドウからデバイスを要求することもできます。

始める前に

プラグ アンド プレイ プロビジョニングの前提条件が満たされていることを確認します。詳細については、プラグ アンド プレイ プロビジョニングの前提条件 （698 ページ）を参照してください。

手順

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

ステップ 2 テーブル内のデバイスを表示します。

検索バーを使用して、特定のデバイスを検索できます。

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

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

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

a) 必要に応じてデバイスのホスト名を変更します。

b) 次のいずれかのタスクを実行して、サイトを割り当てます。

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

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

割り当てられたサイトに関連付けられているワイヤレス ネットワーク プロファイルにオンボーディング テンプレートがある場合、Catalyst Center はこのテンプレートを PnP オンボーディングに使用します。詳細については、ネットワークプロファイルへのテンプレートの追加 （549ページ）を参照してください。

c) [Next] をクリックします。

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

a) [Configuration] 列で、設定するデバイスの [Assign] をクリックします。

b) デバイス構成を変更する必要がない場合は、[Cancel] をクリックして、次の手順に進みます。それ以外の場合は、次のいずれかの設定を変更または設定します。

- [Device Name]：必要に応じてデバイスのホスト名を変更します。
- [Image]：このドロップダウンリストで、デバイスに適用するゴールデン ソフトウェア イメージを選択します。イメージリポジトリにこのデバイスタイプのゴールデンイメージが 1 つしかない場合は、そのイメージがデフォルトで選択されます。

（注） デバイスのソフトウェア イメージ バージョンまたはゴールデンタグ付きバージョンが 17.14.1 以降の場合、選択したサイトで SNMP ログイン情報に MD5 認証が設定されていると、デバイス要求がブロックされます。

デバイスを要求するには、SNMP ログイン情報に SHA 認証も設定する必要があります。あるいは、ソフトウェア イメージ バージョンが 17.14.1 より前である必要があります。SHA 認証の設定方法については、グローバル デバイス クレデンシャルの編集 （394 ページ）を参照してください。

- [Template]：このドロップダウンリストで、デバイスに適用するオンボーディング設定テンプレートを選択します。このデバイスタイプに対して定義されているオンボーディング設定テンプレートが 1 つしかない場合は、そのテンプレートがデフォルトで選択されます。

（注） デバイスをサイトに割り当てていない場合は、デバイスのテンプレートを選択する必要があります。選択するテンプレートには、デバイスにグローバル デバイス ログイン情報を設定するために必要な CLI コマンドを含める必要があります。それ以外の場合、デバイスは管理対象外の状態で一覧に追加されます。

アシュアランスの使用例とデバイスごとの設定を含む、非インテントベースのネットワーク展開での AP のオンボーディングについては、非インテントベースの展開に PnP を使用する AP のオンボーディング （1714 ページ） を参照してください。

- [Catalystワイヤレス LAN コントローラ設定（Catalyst Wireless LAN Controller Settings）]：Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の場合、必須フィールドである [ワイヤレス管理IP（Wireless Management IP）]、[サブネットマスク（Subnet Mask）]、[ゲートウェイ（Gateway）]、[ワイヤレス管理IP（IPv6）（Wireless Management IP (IPv6)）]、[プレフィックス（Prefix）]、[ゲートウェイ（IPv6）（Gateway (IPv6)）]、[IPインターフェイス名（IP Interface Name）] 、およびオプションで [VLAN ID] のフィールドにデータを入力します。

（注） 使用可能なフィールドは ワイヤレスコントローラ の IP アドレスタイプによって異なります。ワイヤレスコントローラに IPv4 アドレスタイプのみが含まれている場合、Catalyst Center には IPv4 アドレスのフィールドが表示されます。IPv6 アドレスタイプのみが含まれている場合、Catalyst Center には IPv6 アドレスのフィールドが表示されます。IPv4 と IPv6 の両方のアドレスタイプがある場合、Catalyst Center には IPv4 アドレスと IPv6 アドレスの両方のフィールドが表示されます。

- Mobility Express デバイスの場合は、[Wireless management IP]、[Subnet Mask]、および [Gateway] の各フィールドに値を入力します。
- 変更した場合は、[Save] をクリックします。それ以外の場合は、[Cancel] をクリックしてリストに戻り、他のデバイスを設定します。

c) [Clear Configuration] ドロップダウンリストから、次のオプションのいずれかを選択します。

- [Clear Device Certificates]：このオプションを選択し、証明書をクリアする各デバイスの横にあるチェックボックスをオンにして、[Clear] をクリックします。
- [Clear Images]：このオプションを選択し、イメージをクリアする各デバイスの横にあるチェックボックスをオンにして、[Clear] をクリックします。
- [Clear Templates]：このオプションを選択し、テンプレートをクリアする各デバイスの横にあるチェックボックスをオンにして、[Clear] をクリックします。

- [Clear License Levels]：このオプションを選択し、ライセンスレベルをクリアする各デバイスの横にあるチェックボックスをオンにして、[Clear] をクリックします。

d) あるデバイスのイメージまたはテンプレートを他のデバイスに適用するには、[Actions] 列で、省略記号アイコン ••• の上にカーソルを置き、[Apply Image to Other Devices] または [Apply Template to Other Devices] を選択します。

[ライセンスレベルを他のデバイスに適用（Apply License Level to Other Devices）] をクリックして、デバイスのライセンスレベルを他のデバイスに適用できます。

e) プロビジョニングするデバイスを複数選択した場合は、リストにある次のデバイスの [Assign] クリックし、この設定手順を繰り返します。これを、すべてのデバイスに対して実行します。

f) すべてのデバイスを設定したら、[Next] をクリックします。

ステップ 7 [Provision Templates] ウィンドウで、[Devices] エリアからテンプレートを選択し、[Domain] フィールドにドメイン名を入力して、[Next] をクリックします。

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

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

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

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

ステップ 11 [要求（Claim）] をクリックします。

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

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

次のタスク

ネットワーク設定を構成している場合は、デバイスでこれらの設定をプロビジョニングします。詳細については、プロビジョニングプロセスの完了（730ページ）を参照してください。

AP またはセンサーデバイスのプロビジョニング

[プラグアンドプレイデバイス（Plug and Play Devices）] リストから AP またはセンサーデバイスを要求するには、次の手順を実行します。代わりに、[Claim] をクリックしてデバイスの [Details] ウィンドウからデバイスを要求することもできます。

Before you begin

プラグ アンド プレイ プロビジョニングの前提条件が満たされていることを確認します。詳細については、「プラグ アンド プレイ プロビジョニングの前提条件 （698 ページ）」を参照してください。

手順

ステップ 1 **[プラグアンドプレイ（Plug and Play）]** に移動して、必要なデバイスを選択します。

a) メインメニューから次を選択します。**[Provision]** > **[Plug and Play]**。

b) テーブル内のデバイスを表示します。

検索バーを使用して、特定のデバイスを検索できます。

c) 要求するデバイスの横にあるチェックボックスをオンにします。

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

ステップ 2 （任意） [Assign Site] ウィンドウで、次の手順を実行します。

a) 必要に応じてデバイスのホスト名を変更します。

b) 次のいずれかのタスクを実行して、サイトを割り当てます。

- 各デバイスに異なるサイトを割り当てるには、[Assign] をクリックし、[Select a Site] ドロップダウンリストからサイトを選択します。
- 最初のデバイスと同じサイトを他のすべてのデバイスに割り当てるには、[Actions] 列で、省略記号アイコン ••• の上にカーソルを置き、[Apply Site to All] を選択します。
- あるデバイスのサイトを別のデバイスに割り当てるには、[Actions] 列で、省略記号アイコン ••• の上にカーソルを置き、[Assign this Site to Other Devices] をクリックし、デバイスを選択して [Assign] をクリックします。
- デバイスに割り当てられたサイトをクリアするには、[Clear Site] をクリックします。

割り当てられたサイトに関連付けられているワイヤレス ネットワーク プロファイルにオンボーディング テンプレートがある場合、Catalyst Center はこのテンプレートを PnP オンボーディングに使用します。詳細については、「ネットワークプロファイルへのテンプレートの追加 （549 ページ）」を参照してください。

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

- [Configure AP Location] チェックボックスがオンの場合、AP の設定 （1639 ページ） は PnP オンボーディング中にこのサイトを AP ロケーションとして割り当てます。
- [Configure AP Location] チェックボックスがオフの場合、Catalyst Center は PnP オンボーディング中にこのサイトを AP ロケーションとして設定しません。[Configure Access Points] ワークフローを使用して AP の場所を設定できます。詳細については、「AP の設定 （1639 ページ）」を参照してください。

詳細については、『*Cisco Catalyst Center Administrator Guide*』の「Configure AP location for PnP onboarding」を参照してください。

c) [Next] をクリックします。

ステップ 3 [Assign Configuration] ウィンドウで、次の手順を実行します。

a) [Configuration] 列で、設定するデバイスの [Assign] をクリックします。

b) デバイス構成を変更する必要がない場合は、[Cancel] をクリックして、次の手順に進みます。それ以外の場合は、次のいずれかの設定を変更または設定します。

- [Device Name]：必要に応じてデバイスのホスト名を変更します。
- [Template]：このドロップダウンリストで、デバイスに適用するオンボーディング設定テンプレートを選択します。このデバイスタイプに対して定義されているオンボーディング設定テンプレートが 1 つしかない場合は、そのテンプレートがデフォルトで選択されます。

（注） デバイスをサイトに割り当てていない場合は、デバイスのテンプレートを選択する必要があります。選択するテンプレートには、デバイスにグローバル デバイスログイン情報を設定するために必要な CLI コマンドを含める必要があります。それ以外の場合、デバイスは管理対象外の状態で一覧に追加されます。

アシュアランスのユースケースと デバイスごとの設定 を含む、非インテントベースのネットワーク展開での AP のオンボーディングについての詳細は、「非インテントベースの展開に PnP を使用する AP のオンボーディング （1714 ページ）」を参照してください。

- AP の場合、[APゾーン（AP Zone）] ドロップダウンリストから AP ゾーンを選択します。[RFプロファイル（RF Profile）] は自動的に入力され、SSID 数は選択した AP ゾーンに基づいて表示されます。デフォルトの AP ゾーンを選択する場合は、RF プロファイルを選択します。

- AP の場合、[無線周波数プロファイル（Radio Frequency Profile）] ドロップダウンリストで、デバイスに適用する無線周波数プロファイルを選択します。これは、1つのプロファイルをデフォルトとして指定した場合に設定できます。
- センサーの場合、[センサー設定（Sensor Settings）] ドロップダウンリストで、デバイスに適用するセンサー デバイス プロファイル（バックホール）を選択します。

（注） 1.3.1.2 よりも前の Cisco Aironet 1800s アクティブセンサーの場合は、センサー デバイス プロファイル **CiscoProvisioningSSID** を選択しないようにしてください。代わりに、バックホール用に独自の SSID を選択します。

- 変更した場合は、[Save] をクリックします。それ以外の場合は、[Cancel] をクリックしてリストに戻り、他のデバイスを設定します。

c) [Clear Configuration] ドロップダウンリストから、次のオプションのいずれかを選択します。
- [Clear Device Certificates]：このオプションを選択し、証明書をクリアする各デバイスの横にあるチェックボックスをオンにして、[Clear] をクリックします。
- [Clear Images]：このオプションを選択し、イメージをクリアする各デバイスの横にあるチェックボックスをオンにして、[Clear] をクリックします。
- [Clear Templates]：このオプションを選択し、テンプレートをクリアする各デバイスの横にあるチェックボックスをオンにして、[Clear] をクリックします。
- [Clear License Levels]：このオプションを選択し、ライセンスレベルをクリアする各デバイスの横にあるチェックボックスをオンにして、[Clear] をクリックします。

d) あるデバイスのイメージまたはテンプレートを他のデバイスに適用するには、[Actions] 列で、省略記号アイコン ••• の上にカーソルを置き、[Apply Image to Other Devices] または [Apply Template to Other Devices] を選択します。
e) プロビジョニングするデバイスを複数選択した場合は、リストにある次のデバイスの [Assign] クリックし、この設定手順を繰り返します。これを、すべてのデバイスに対して実行します。
f) すべてのデバイスを設定したら、[Next] をクリックします。

ステップ 4 [Provision Templates] ウィンドウで、[Devices] エリアからテンプレートを選択し、[Domain] フィールドにドメイン名を入力して、[Next] をクリックします。

（注） デバイスがサイトに割り当てられている場合は、[次へ（Next）] をクリックします。

ステップ 5 [Summary] ウィンドウで、デバイスに関する詳細や構成プレビューを確認できます。

ステップ 6 設定プレビューが成功したかどうかを確認するには、各デバイスの [デバイス設定（Device Configuration）] 列をチェックします。

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

ステップ 7 [Device Configuration] 列で、[Preview Configuration] をクリックして設定を確認します。

ステップ 8 [要求（Claim）] をクリックします。

ステップ 9 確認ダイアログボックスで [Yes] をクリックしてデバイスを要求し、プロビジョニングプロセスを開始します。

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

次のタスク

ネットワーク設定を構成している場合は、デバイスでこれらの設定をプロビジョニングします。詳細については、プロビジョニングプロセスの完了（730 ページ） を参照してください。

StackWise Virtual Link スイッチのプロビジョニング

PnP のオンボーディング中に、StackWise Virtual Link（SVL）を使用して、接続されたスイッチのペアを単一の論理デバイスとしてオンボーディングできます。現在、SVL PnP オンボーディングは、Catalyst 9500 シリーズ スイッチでのみサポートされています。

Before you begin

- 両方のスイッチが直接接続されていることを確認します。
- 最小速度 1 Gbps のリンクを使用してスイッチを接続し、インターフェイス速度が一致していることを確認します。
- スイッチが初期化状態にあることを確認します。

手順

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

ステップ 2 [SVL スイッチの要求（Claim a SVL switch）] をクリックします。

ステップ 3 [SVL スイッチとして要求（Claim as an SVL switch）] ポップアップウィンドウで、SVL オンボーディング設定に必要な値を入力します。

1. [アクティブスイッチ（Active Switch）]：スイッチの 1 つをアクティブスイッチとして選択します。
2. [スタンバイスイッチ（Standby Switch）]：スタンバイスイッチとして別のスイッチを選択します。
3. [StackWise Virtual Link]：SVLリンクを選択します。最大 8 つの SVL リンクを選択できます。
4. [デュアルアクティブ検出リンク（Dual-Active Detection Link）]：使用可能な場合、デュアルアクティブ検出リンクを選択します。
5. [ドメイン（Domain）]：ドメインに一意の値を割り当てます。

ステップ 4 [サイトの選択（Select Site）] を クリックし、SVL スイッチの目的のサイトを選択します。

ステップ 5 [テンプレートの管理（Manage Template）] をクリックし、SVL スイッチにプロビジョニングするテンプレートを選択します。

ステップ 6 （任意） SVL 作成後に適用する標準イメージを選択します。

デバイス上のイメージバージョンが異なる場合、PnP では標準イメージが強制的に選択され、SVL 生成の前に両方のデバイスに適用されます。

ステップ 7 [Claim] をクリックします。

PnP サーバーは SVL を作成し、デバイスをプロビジョニングします。

プロビジョニングプロセスの完了

プラグアンドプレイのプロビジョニング中に、デバイスのログイン情報とオンボーディング設定のみがデバイスにプッシュされます。他のネットワーク設定はプッシュされません。プラグアンドプレイのプロビジョニングが完了したら、[Design] 領域で構成されているネットワーク設定をプッシュすることで、プロビジョニングプロセスを完了できます。

ネットワーク設定には AAA サーバー設定が含まれます（設定されている場合）。Cisco ISE の場合、Catalyst Center は Cisco ISE のデバイスを RADIUS または TACACS の AAA クライアントとして設定します。

（注） Cisco Catalyst 9800 シリーズ ワイヤレス コントローラおよびCisco Catalyst 9000 シリーズ スイッチでは、デイゼロ設定中に NETCONF が有効になると、ローカル AAA 設定がデバイスにプッシュされます。

ワイヤレスおよびセンサーデバイスの場合、ネットワーク設定には、RF プロファイルやアンテナ無線プロファイルなどのワイヤレス設定が含まれます（設定されている場合）。詳細については、「ワイヤレスデバイスのプロビジョニングの概要（735 ページ）」を参照してください。

始める前に

- 次のいずれかの手順を使用して、デバイスがプロビジョニング（オンボード）されていることを確認します。
  - スイッチまたはルータデバイスのプロビジョニング （717 ページ）
  - ワイヤレスコントローラ のプロビジョニング （722 ページ）
- ネットワークの設定値を設定します。詳細については、ネットワークの設定（373 ページ）を参照してください。

手順

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

ステップ 2 デバイスを選択し、**[Actions]** > **[Provision]** > **[Provision Device]** を選択します。

ステップ 3 ワークフローの手順を進めます。

ステップ 4 [Summary] ウィンドウで、残りのネットワーク設定を確認します。変更を加えるには、関連するカテゴリの横にある [Edit] をクリックします。それ以外の場合は、[Deploy] をクリックします。

（注） デバイスのソフトウェア イメージ バージョンまたはゴールデンタグ付きバージョンが 17.14.1 以降の場合、選択したサイトで SNMP ログイン情報に MD5 認証が設定されていると、デバイス要求がブロックされます。

デバイスを要求するには、SNMP ログイン情報に SHA 認証も設定する必要があります。あるいは、ソフトウェア イメージ バージョンが 17.14.1 より前である必要があります。SHA 認証の設定方法については、「グローバルデバイス クレデンシャルの編集（394 ページ）」を参照してください。

ステップ 5 （任意）デバイスで構成を展開すると、[Task Progress] バーに、**[Activities]** > **[Tasks]**で進行中のプロビジョニングタスクの進行状況が表示されます（タスク名をクリックすると表示されます）。

デバイスの削除

デバイスを削除すると、デバイスはプラグアンドプレイのデータベースから削除されますが、リセットはされません。エラー状態のデバイスをリセットする場合は、[Reset] を使用します。

この手順では、[Plug and Play Devices] リストからデバイスを削除する方法について説明します。代わりに、[削除（Delete）] をクリックしてデバイスの詳細ウィンドウからデバイスを削除することもできます。

（注）
- デバイスがプロビジョニングの状態の場合は、[Inventory] タブからのみ削除できます。
- デバイスが一時的な状態（接続中や実行中など）の場合、そのデバイスは [プラグアンドプレイ デバイス（Plug and Play Devices）] リストから削除できません。

手順

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

ステップ 2 テーブル内のデバイスを表示します。

[Device State] のいずれかのボタンを使用してデバイスの状態でフィルタ処理したり、[Filter] オプションを使用して特定のデバイスを検索したりできます。[Refresh] をクリックしてデバイスリストを更新します。

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

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

ステップ 5 （任意）要求元不明デバイスの場合は、[インベントリ内のこのデバイスのプラグアンドプレイ機能を削除（Delete Plug and Play capabilities for this device in inventory）] チェックボックスをオンにします。

このオプションを選択すると、Catalyst Center はデバイスプロファイルを削除し、デバイスは PnP に再表示されません。

デバイスはインベントリに残り、引き続き管理できます。PnP 機能は後で再度有効にできます。

ステップ 6 [OK] をクリックします。

デバイスのリセット

デバイスのリセットはエラー状態のデバイスにのみ適用され、状態が [Unclaimed] にリセットされデバイスがリロードされますが、プラグアンドプレイ データベースからは削除されません。デバイスを削除する場合は、**[Ddelete]** を使用します。

（注） デバイスで保存された設定が工場出荷時のデフォルトまたは同様の最小限の設定である場合、このオプションを選択すると、デバイスはプロビジョニングプロセスを再起動します。ただし、デバイスに以前に保存されたスタートアップ コンフィギュレーションがある場合は、これによってデバイスのプロビジョニングプロセスの再起動を回避できますが、工場出荷時のデフォルトにリセットする必要があります。ワイヤレスデバイスおよびセンサーデバイスでは、デバイスの状態だけがリセットされ、デバイスはリロードされません。

この手順では、[Plug and Play Devices] リストからデバイスをリセットする方法を示します。代わりに、[Reset] をクリックしてデバイスの詳細ウィンドウからリセットすることもできます。

（注） デバイスが一時的な状態（接続中や実行中など）の場合、リセットすることはできません。

手順

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

ステップ 2 テーブル内のデバイスを表示します。

[Device State] のいずれかのボタンを使用してデバイスの状態でフィルタ処理したり、[Filter] オプションを使用して特定のデバイスを検索したりできます。[Refresh] をクリックしてデバイスリストを更新します。

ステップ 3 リセットする 1 個以上のデバイスの横にあるチェック ボックスをオンにします。

ステップ 4 デバイス テーブルの上にあるメニュー バーで、**[Actions（アクション）] > [Reset（リセット）]** をクリックします。

確認ダイアログボックスが表示されます。

ステップ 5 次のオプションのいずれかを選択します。

- [Reset and keep current claim parameters]：現在の請求パラメータが維持され、デバイスは [Planned] 状態になります。
- [Reset and remove all claim parameters]：現在の請求パラメータを削除し、デバイスが [Unclaimed] 状態になります。

ステップ 6 [リセット（**Reset**）] をクリックします。



第 17 章

ワイヤレスデバイスのプロビジョニング

- ワイヤレスデバイスのプロビジョニングの概要 （735 ページ）
- ワイヤレスデバイスと国コードについて （735 ページ）
- ロールベース アクセス コントロール （736 ページ）
- Cisco AireOS コントローラのプロビジョニングの前提条件 （736 ページ）
- Cisco AireOS コントローラのプロビジョニング （738 ページ）
- Day 1 の Cisco AP プロビジョニング （745 ページ）
- FlexConnect モードの AP における ICMP ping の有効化 （751 ページ）
- Cisco AireOS Mobility Express AP の Day-0 ワークフロー （752 ページ）
- Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの設定とプロビジョニング （754 ページ）
- Catalyst 9000 シリーズ スイッチ用 Cisco Catalyst 9800 組み込みワイヤレスコントローラの設定とプロビジョニング （790 ページ）
- ワイヤレスデバイスの AP LSC の更新 （799 ページ）
- Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の デバイスごとの設定 （801 ページ）
- リリース間コントローラモビリティの概要 （1171 ページ）
- Meraki デバイスをプロビジョニングするための前提条件 （1175 ページ）
- Meraki デバイスのプロビジョニング （1177 ページ）
- リモート テレワーカー デバイスのプロビジョニング （1178 ページ）

ワイヤレスデバイスのプロビジョニングの概要

以降のセクションでは、シスコのさまざまなワイヤレスデバイスをプロビジョニングする方法について説明します。

ワイヤレスデバイスと国コードについて

コントローラおよびアクセスポイントは、法的な規制基準の異なるさまざまな国で使用できるように設計されています。アクセスポイント内の無線は、製造時に特定の規制ドメインに割り

当てられています（ヨーロッパの場合はEなど）が、国コードを使用すると、規制ドメイン内で稼働する特定の国を指定できます（フランスの場合はFR、スペインの場合はESなど）。国番号を設定すると、各無線のブロードキャスト周波数帯域、インターフェイス、チャネル、および送信電力レベルが国別の規制に準拠していることを確認できます。

Catalyst Center は、割り当てられたサイトに応じて、国コードを使用してコントローラをプロビジョニングします。コントローラの場合は、複数のサイトに割り当てることができます。そのため、複数の国コードを割り当てることができます。Catalyst Center は、プロビジョニング中に、サイトをサイトの国コードとともにコントローラに割り当てます。たとえば、インドと米国の両方のサイトを管理するコントローラには、IN と US の国コードが割り当てられます。

アクセスポイントは、プロビジョニングされると、フロアに割り当てられます。アクセスポイントが ROW AP の場合、Catalyst Center は、サイトの国コードを取得して AP に割り当てます。同じフロア上の追加の AP には、同じ国コードが割り当てられます。

RF プロファイルを選択して AP をプロビジョニングする際、RF プロファイルで設定されたすべての DCA チャネルのうち、国コードに従ってサポートされているチャネルのみが動的チャネル割り当て（DCA）に対して考慮されます。サポートされていない DCA チャネルのリストは、Catalyst Center の AP 事前プロビジョニング ワークフローの AP 事前プロビジョニング手順の概要で確認できます。

国コード情報は、コントローラとアクセスポイントの [Device 360] ウィンドウに表示されます。

サポートされている国コードの製品ごとの完全なリストについては、https://www.cisco.com/c/dam/assets/prod/wireless/wireless-compliance-tool/index.html を参照してください。

ロールベース アクセス コントロール

Catalyst Center でのロールベース アクセス コントロールにより、ユーザーがアクセスできる機能と権限を定義することが可能です。ワイヤレスデバイスをプロビジョニングする前に、プロビジョニングするサイトとデバイスにアクセスできること、およびプロビジョニングの実行に必要な権限があることを確認してください。

詳細については、ユーザープロファイルのロールおよび権限 （35 ページ）を参照してください。

Cisco AireOS コントローラのプロビジョニングの前提条件

- シスコ ワイヤレス コントローラ をプロビジョニングする前に、次を含むグローバルネットワーク設定を定義したことを確認します。
  - AAA、DHCP、および DNS などのネットワーク サーバー。

詳細については、グローバル ネットワーク サーバーの設定（377ページ）を参照してください。

- CLI、SNMP、HTTP、HTTPS などのデバイス クレデンシャル。

  詳細については、グローバル CLI クレデンシャルの追加（379 ページ）、グローバル SNMPv2c ログイン情報の追加（380 ページ）、グローバル SNMPv3 ログイン情報の追加（382ページ）、およびグローバル HTTPS ログイン情報の追加（385 ページ）を参照してください。

- IP アドレス プール

  詳細については、「IP アドレスプールを設定する（397ページ）」を参照してください。

- SSID、ワイヤレス インターフェイス、およびワイヤレス無線周波数プロファイルなどのワイヤレス設定です。

（注） 以前のリリースからアップグレードする場合：

- WPA3-Enterprise SSID の場合、Catalyst Center は、SSID の Dot1x-SHA256 認証キー管理設定を有効にします。
- WPA2-WPA3-Enterprise SSID の場合、Catalyst Center は、SSID の Dot1x 認証キー管理設定と Dot1x-SHA256 認証キー管理設定の両方を有効にします。

この設定により、Cisco IOS XE リリース 17.6 以前を実行している Cisco AireOS ワイヤレスコントローラ および ワイヤレスコントローラ の意図した設定が変更される可能性があります。ワイヤレスコントローラを再プロビジョニングする前に、SSID の**認証キー管理**設定を更新できます。

詳細については、「グローバルワイヤレス設定の構成（414 ページ）」を参照してください。

- インベントリにワイヤレスコントローラがあることを確認します。ない場合は、[Discovery] 機能を使用してコントローラを検出します。
- サイトに ワイヤレスコントローラ が追加されたことを確認してください。詳細については、プロビジョニングされていないデバイスのサイトへの割り当て（189ページ）を参照してください。
- デバイスで既存の VLAN を再利用することはできません。デバイスにすでに存在する同じ VLAN を Catalyst Center がプッシュすると、プロビジョニングは失敗します。
- Catalyst Center によって管理されている ワイヤレスコントローラ の設定に手動で変更を加えることはできません。Catalyst Center GUI からすべての設定を実行する必要があります。

Cisco AireOS コントローラのプロビジョニング

始める前に

前提条件を満たしていることを確認します。詳細については、Cisco AireOS コントローラのプロビジョニングの前提条件 （736 ページ）を参照してください。

手順

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

[Inventory] ウィンドウが表示され、検出されたデバイスが一覧表示されます。

ステップ 2 左側のペインで [Global] サイトを展開し、関心のあるサイト、ビルディング、またはフロアを選択します。

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

ステップ 3 [Devices] テーブルで、[Search] フィールドをクリックします。[Quick Filters] タブで、次の手順を実行します。

a) [Device Family] で、[Wireless Controllers] をクリックして、検出された ワイヤレスコントローラ のリストを取得します。

b) [Reachability] で、[Reachable] をクリックして、検出された到達可能な ワイヤレスコントローラ のリストを取得します。

c) [適用（Apply）] をクリックします。

ステップ 4 プロビジョニングするデバイス名の横にあるチェックボックスをオンにします。

ステップ 5 [Actions] ドロップダウンリストから、**[Provision]** > **[Provision Device]** を選択します。

[Assign Site] ウィンドウが表示されます。

ステップ 6 [Choose a site] をクリックして ワイヤレスコントローラ にサイトを割り当てます。

ステップ 7 [Add Sites] ウィンドウで、ワイヤレスコントローラを関連付けるサイト名の横にあるチェックボックスをオンにして、[Save] をクリックします。

ステップ 8 [Apply] をクリックします。

ステップ 9 [Next] をクリックします。

[Configuration] ウィンドウが表示されます。

ステップ 10 ワイヤレスコントローラのロールを選択します（[Active Main WLC] または [Guest Anchor WLC]）。

ステップ 11 [Select Primary Managed AP Locations] をクリックして、ワイヤレスコントローラ の管理 AP の場所を選択します。

ステップ 12 [Managed AP Location] ウィンドウで、サイト名の横にあるチェックボックスをオンにします。親サイトまたは個々のサイトのいずれかを選択できます。親サイトを選択すると、その親サイトの下にある子は自動的に選択されます。

（注） 管理 AP の場所を継承することで、サイトをその下のビルディングやフロアとともに自動で選択できます。1 つの ワイヤレスコントローラ で管理できるのは 1 つのサイトのみです。

ステップ 13 [Save] をクリックします。

ステップ 14 （任意） [AP Authorization List] チェックボックスをオンにして、AP 認証の認証リストを選択し、次のタスクを実行します。

（注） このチェックボックスは、AP認証リストが使用可能な場合にのみ表示されます。AP認証リストの詳細については、AP 認証リストの作成 （492 ページ）を参照してください。

- [AP Authorization List Name] ドロップダウンリストから、AP 認証リストを選択します。AP 認証リストの内容に基づいて、Catalyst Centerは、それに対応するプライマリの認証タイプとフェールバックメカニズムを示したメッセージを表示します。
- （オプション）選択した AP 認証リストのエントリを表示するには、[View Entries] をクリックします。
- ワイヤレスコントローラ でメッシュ AP と非メッシュ AP の両方が管理されている場合、Catalyst Center には [Authorize Only Mesh Access Points] および [Authorize All Access Points] チェックボックスが表示されます。

  メッシュ AP の認証のみを有効にするには、[Authorize Only Mesh Access Points] チェックボックスをオンにします。

  すべての AP の認証を有効にするには、[Authorize All Access Points] チェックボックスをオンにします。

ステップ 15 [Interface and VLAN Configuration] で [+ Add] をクリックして、アクティブメイン ワイヤレスコントローラ のインターフェイスと VLAN の詳細を設定します。

インターフェイスおよび VLAN の設定は、非ファブリックの ワイヤレスコントローラ プロビジョニングにのみ適用できます。

[Configure Interface and VLAN] ウィンドウが表示されます。

ステップ 16 [インターフェイス名（Interface Name）] ドロップダウン リストからインターフェイス名を選択します。

（注） 追加インターフェイスの横に情報アイコン（ⓘ）が表示されます。追加インターフェイスの詳細については、ネットワークプロファイルの追加インターフェイスの構成（566 ページ）を参照してください。

ステップ 17 [VLAN ID] フィールドに、VLAN の値を入力します。

ステップ 18 [Interface IP Address] フィールドに、インターフェイス IP アドレスの値を入力します。

ステップ 19 [Interface Net Mask (in bits)] フィールドに、インターフェイスのサブネットマスクを入力します。

ステップ 20 [Gateway IP Address] フィールドにゲートウェイ IP アドレスを入力します。

ステップ 21 [LAG/Port Number] ドロップダウンリストから、リンク集約またはポート番号を選択します。

ステップ 22 [OK] をクリックします。

ステップ 23 （任意） ゲスト アンカー ワイヤレスコントローラの場合、[Assign Guest SSIDs to DMZ site] で [VLAN ID] を変更して、VLAN ID 構成を変更できます。

ステップ 24 [Next] をクリックします。

[Feature Templates] ウィンドウが表示されます。

ステップ 25 [Devices] ペインで、[Find] フィールドに機能テンプレートの名前を入力して検索するか、デバイスを展開して機能テンプレートを選択します。

選択した機能テンプレートが右側のペインに表示されます。

ステップ 26 プロビジョニングする機能テンプレートの [Design Name] の横にあるチェックボックスをオンにし、[Configure] をクリックして編集します。

この手順では、すべての設定を編集することはできません。

ステップ 27 必要な変更を加えて、[Apply] をクリックします。

ステップ 28 [Next] をクリックします。

[Advanced Configuration] ウィンドウが表示されます。ここでは、事前定義されたテンプレート変数の値を入力できます。

ステップ 29 [Devices] パネルでデバイスまたはテンプレートを検索します。

ステップ 30 [wlanid] フィールドに、事前定義されたテンプレート変数の値を入力します。

ステップ 31 [Next] をクリックします。

ステップ 32 [Summary] ステップでデバイスの詳細を確認し、[Next] をクリックしてデバイスをプロビジョニングします。

ステップ 33 展開のためのタスクのスケジュールを設定します。

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

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

（注）
- ワイヤレスコントローラ をプロビジョニングすると、Catalyst Center は設定を ワイヤレスコントローラ にプッシュし、ネットワークインテントに基づいて設定します。再プロビジョニング中に、ネットワークインテントの一部であるか、Catalyst Center によってプッシュされている設定と競合するアウトオブバンド設定が ワイヤレスコントローラ にある場合、Catalyst Center は ワイヤレスコントローラ のアウトオブバンド設定をネットワークインテント設定に上書きします。

  Catalyst Center のネットワークインテントを介してサポートされるすべての設定について、アウトオブバンド設定の代わりに使用することをお勧めします。
- デバイスで構成を展開すると、[Task Progress] バーに、**[Activities]** > **[Tasks]**で進行中のプロビジョニングタスクの進行状況が表示されます（タスク名をクリックすると表示されます）。

ステップ 34 [Tasks] ウィンドウで、タスクの展開を監視します。

ステップ 35 セカンダリコントローラをプロビジョニングします。

ステップ 36 展開が正常に完了すると、[Device Inventory] ウィンドウの [Status] 列に「SUCCESS」と表示されます。

プロビジョニング後に何らかの変更を行う場合は、[Design] をクリックしてサイトのプロファイルを変更し、もう一度 ワイヤレスコントローラ をプロビジョニングします。

ステップ 37 デバイスが正常に展開されると、[Provision Status] が [Configuring] から [Success] に変わります。

ステップ 38 [Device Inventory] ウィンドウで、[Provision Status] 列の [See Details] をクリックし、ネットワークインテントの詳細情報を取得するか、実行する必要があるアクションのリストを表示します。

ステップ 39 [Device Provisioning] の下の [See Details] をクリックします。

ステップ 40 [Deployment of network intent] の下の [View Details] をクリックし、デバイス名をクリックします。

ステップ 41 [Configuration Summary] エリアを展開して、操作の詳細、機能名、および管理機能を表示します。

[Configuration Summary] には、デバイスのプロビジョニング中に発生したエラーも表示されます。

ステップ 42 デバイスに送信される正確な設定の詳細を表示するには、[Provision Summary] エリアを展開します。

シスコ ワイヤレス コントローラ高可用性（HA）の設定

シスコ ワイヤレス コントローラ高可用性（HA）を Catalyst Center から設定できます。現在、ワイヤレスコントローラ HA の形成および中断の両方がサポートされています。スイッチオーバーオプションはサポートされていません。

シスコ ワイヤレス コントローラ 高可用性（HA）を設定するための前提条件

- ワイヤレスコントローラ 1 と ワイヤレスコントローラ 2 の検出機能とインベントリ機能が正常であること。デバイスが管理されていること。

- ワイヤレスコントローラ 1 と ワイヤレスコントローラ 2 のサービスポートおよび管理ポートが設定されていること。
- ワイヤレスコントローラ 1 と ワイヤレスコントローラ 2 の冗長ポートが物理的に接続されていること。
- ワイヤレスコントローラ 1 と ワイヤレスコントローラ 2 の管理アドレスが同じサブネット内にあること。ワイヤレスコントローラ 1 と ワイヤレスコントローラ 2 の冗長管理アドレスも同じサブネット内にあること。
- ワイヤレスコントローラ でこのブート変数を手動で設定します。

```
config t
boot system bootflash::<device_iosxe_image_filename>
config-register 0x2102

show boot.  (IOSXE cli)

BOOT variable = bootflash:<device_iosxe_image_filename>,12;
Configuration register is 0x2102
```

シスコ ワイヤレス コントローラ HA の設定

手順

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

[Inventory] ウィンドウが表示され、検出されたデバイスが一覧表示されます。

ステップ 2 プライマリコントローラとして設定する ワイヤレスコントローラ の名前の横にあるチェックボックスをオンにします。

ステップ 3 [Actions] ドロップダウンリストから、**[Provision]** > **[Configure WLC HA]** を選択します。

[高可用性（High Availability）] スライドインペインが表示されます。

（注） 選択した ワイヤレスコントローラ がサイトに割り当てられていない場合は、ペインの上部に警告が表示されます。Catalyst Center は、サイトに割り当てられるまでテレメトリ設定を ワイヤレスコントローラ にプッシュしません。

デフォルトでは、選択された ワイヤレスコントローラ がプライマリコントローラになり、[プライマリ C9800（Primary C9800）] フィールドが無効になります。

ステップ 4 [Redundancy Management IP] と [Peer Redundancy Management IP] のアドレスをそれぞれテキストボックスに入力します。

冗長性管理 IP およびピア冗長性管理 IP に使用される IP アドレスは、ワイヤレスコントローラ の管理インターフェイスと同じサブネットに設定する必要があります。これらの IP アドレスがこのサブネット範囲内で未使用の IP アドレスであることを確認します。

ステップ 5 [Select Secondary WLC] ドロップダウンリストから、セカンダリコントローラを選択します。

（注） プライマリコントローラのワイヤレス管理インターフェイス IP サブネットに基づいてセカンダリコントローラを選択すると、冗長性管理 IP が自動入力され、次のメッセージとともに [High Availability] ウィンドウの上部に **i** アイコンが表示されます。

冗長性管理 IP とピア冗長性管理 IP が他のネットワークエンティティに割り当てられていないことを確認します。IP が使用されている場合は、適宜 IP を変更して設定します。

ステップ 6 [Configure HA] をクリックします。

ステップ 7 展開のためのタスクのスケジュールを設定します。

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

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 8 [Tasks] ウィンドウで、タスクの展開を監視します。

ステップ 9 タスクが展開されると、HA 設定は、CLI コマンドを使用してバックグラウンドで開始されます。まずプライマリのワイヤレスコントローラが設定されます。成功すると、セカンダリのワイヤレスコントローラが設定されます。設定が完了すると、両方のワイヤレスコントローラが再起動します。このプロセスは、完了するまで最大 2.5 分かかります。

ステップ 10 HA 設定を確認するには、次の手順を実行します。

a) **[Provision]** > **[Inventory]** ウィンドウで、HA デバイスとして設定したデバイスをクリックします。高度なデバイス情報を含むダイアログボックスが開きます。

b) このダイアログボックスで、[View Details] をクリックします。

c) [Wireless Info] タブをクリックします。

[Redundancy Summary] タブには、**[Sync Status]** が **[In Progress]** として表示されます。Catalyst Center で HA のペアリングが成功したことが検出されると、[Sync Status] が [Complete] に変わります。

このプロセスは、インベントリポーラーまたは手動による再同期によってトリガーされます。これで、セカンダリ ワイヤレスコントローラ（ワイヤレスコントローラ 2）が Catalyst Center から削除されます。このフローは、ワイヤレスコントローラ での正常な HA 設定を示しています。

高可用性（HA）プロセス中および完了後に起こること

1. Cisco WLC-1 および WLC-2 は、冗長管理、冗長ユニット、および SSO とともに設定されます。ワイヤレスコントローラはロールをアクティブまたはスタンバイとしてネゴシエートするために再起動します。アクティブからスタンバイに構成が同期されます。

2. [冗長性の概要の表示（Show Redundancy Summary）] ウィンドウで、次の設定を確認できます。
   - SSO が有効になっています。
   - ワイヤレスコントローラがアクティブです。
   - ワイヤレスコントローラがホットスタンバイ状態になっています。
3. アクティブ ワイヤレス コントローラの管理ポートは、両方のコントローラによって共有され、アクティブコントローラを指します。スタンバイ ワイヤレス コントローラのユーザーインターフェイス、Telnet、および SSH は機能しません。コンソールとサービス ポート インターフェイスを使用して、スタンバイ ワイヤレス コントローラを制御できます。

高可用性を設定および確認するためのコマンド

Catalyst Center は、シスコ ワイヤレス コントローラ HA を設定するためのコマンドを送信します。

Catalyst Center は、以下のコマンドをワイヤレスコントローラ 1 に送信します。

- **config interface address redundancy-management 198.51.100.xx peer-redundancy-management 198.51.100.yy**
- **config redundancy unit primary**
- **config redundancy mode sso**

Catalyst Center は、以下のコマンドをワイヤレスコントローラ 2 に送信します。

- **config interface address redundancy-management 198.51.100.yy peer-redundancy-management 198.51.100.xx**
- **config redundancy unit secondary**
- **config port adminmode all enable**
- **config redundancy mode sso**

ワイヤレスコントローラから HA 設定を検証するには、次のコマンドを入力します。

- HA 関連の詳細情報を確認する場合：**config redundancy mode sso**
- 設定済みのインターフェイスを確認する場合：**show redundancy summary**

既存の展開での高可用性が設定されたデバイスの無効化

Catalyst Center の HA 無効化機能は、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ と Cisco AireOS ワイヤレスコントローラ でサポートされています。

始める前に

既存の展開の HA デバイスが Catalyst Center の外部で設定されていることを確認します。

手順

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

[Inventory] ウィンドウが表示され、検出されたデバイスが一覧表示されます。

ステップ 2 無効にする HA 機能を持つ ワイヤレスコントローラ の名前の横にあるチェックボックスをオンにします。

ステップ 3 [Actions] ドロップダウンリストから、**[Provision]** > **[Configure WLC HA]** を選択します。

[高可用性（High Availability）] スライドインペイン が表示されます。

[High Availability] スライドインペイン には、Catalyst Center の外部から設定された、選択された ワイヤレスコントローラ の **冗長性の概要** が表示されます。

ステップ 4 [HA の無効化（Disable HA）] をクリックします。

ステップ 5 **[Warning]** ダイアログボックスで **[OK]** をクリックします。

ステップ 6 展開のためのタスクのスケジュールを設定します。

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

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

ステップ 7 [Tasks] ウィンドウで、タスクの展開を監視します。

ステップ 8 タスクの展開後、選択された ワイヤレスコントローラ の HA 機能が正常に無効になったことを示す成功メッセージがウィンドウの下部に表示されます。

Day 1 の Cisco AP プロビジョニング

次の手順を使用して、AP をプロビジョニングします。

始める前に

- インベントリにシスコの AP があることを確認してください。ない場合は、ディスカバリ機能を使用して AP を検出します。詳細については、ネットワークの検出 （73 ページ）を参照してください。

- [License Manager] ウィンドウで、AP に必要なライセンスが有効になっていることを確認します。詳細については、『*Cisco Catalyst Center Administrator Guide*』の「Manage Licenses」を参照してください。
- 新しい AP ゾーンや SSID を追加する場合は、ワイヤレスコントローラ を再プロビジョニングする必要があります。詳細については、Cisco AireOS コントローラのプロビジョニング （738 ページ）およびCisco Catalyst 9800 シリーズ ワイヤレス コントローラ のプロビジョニング （782 ページ）を参照してください。
- AP ゾーンの設定を更新する場合は、ワイヤレスコントローラ を再プロビジョニングする必要があります。詳細については、Cisco AireOS コントローラのプロビジョニング （738 ページ）およびCisco Catalyst 9800 シリーズ ワイヤレス コントローラ のプロビジョニング （782 ページ）を参照してください。
- N+1 HA を使用していて、プライマリコントローラとセカンダリコントローラですでにプロビジョニングされている非 Flex SSID を Flex SSID に変更する場合（またはその逆の場合）は、WLAN の状態が、対応するサイト上のプライマリコントローラとセカンダリコントローラの両方で一貫していることを確認します。

  たとえば、*SSID1* は、ネットワークプロファイルで Flex SSID として設定され、プライマリコントローラとセカンダリコントローラの両方でプロビジョニングされ、後で非 Flex SSID に変更されます。セカンダリコントローラを再プロビジョニングせずにプライマリコントローラのみを再プロビジョニングすると、*SSID1* は、プライマリコントローラでは非 Flex SSID になりますが、セカンダリコントローラでは Flex SSID のままになります。この場合、プライマリコントローラとセカンダリコントローラの両方で共有されているサイトで AP をプロビジョニングすると、プロビジョニングは失敗します。一貫性を確保するには、セカンダリコントローラを再プロビジョニングする必要があります。セカンダリコントローラを再プロビジョニングすると、*SSID1* はセカンダリコントローラでも非 Flex SSID に変更され、AP をプロビジョニングする前の *SSID1* の状態は両方のコントローラで同じになります。
- ROW AP の場合は、必要な国コードを使用して AP プロファイルを作成し、カスタムサイトタグを設定することを推奨します。詳細については、Cisco IOS XE デバイスの AP プロファイルの追加設定を行う （509ページ）およびネットワークプロファイルへの AP グループ、Flex グループ、サイトタグ、およびポリシータグの追加 （563 ページ）を参照してください。

手順

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

ステップ 2 プロビジョニングする AP の横にあるチェックボックスをオンにします。

最大 500 の AP を同時に選択できます。

ステップ 3 [Actions] ドロップダウンリストから、**[Provision]** > **[Provision Device]** を選択します。

ステップ 4 ライセンス要件を満たしていない AP を選択すると、Catalyst Center は詳細を示すダイアログボックスを表示します。ダイアログボックスで、必要なオプションを選択します。

オプション	説明
ライセンス マネージャ	[License Manager] ウィンドウを開いて、対応するライセンスを有効にします。 ライセンスを有効にするには、『*Cisco Catalyst Center Administrator Guide*』の「Manage Licenses」を参照してください。
Continue with device provision	デバイスのプロビジョニングを続行します。 （注） ライセンス要件を満たしていない AP は、ワールドワイドセーフモード（WWSM）になります。
Cancel	ダイアログボックスを閉じて、別の AP を選択します。

ステップ 5 [Assign Site] ステップで、必要なパラメータを設定します。

a) [Choose a floor] をクリックし、サイトに AP を割り当てます。

b) [Choose a Floor] スライドインペインで、AP が存在するフロアをクリックし、[Save] をクリックします。

c) **[Next]** をクリックします。

（注） Catalyst Center では、このサイトは AP のプロビジョニング時に AP の場所として設定されません。[Configure Access Points] ワークフローを使用して AP の場所を設定できます。詳細については、AP の設定 （1639 ページ）を参照してください。

ステップ 6 [Configuration] ステップで、必要なパラメータを設定します。

a) [**Advanced Configuration**] をクリックして、アンテナスロットのアンテナ無線プロファイルを設定します。

（注） 高度な設定は、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ ソフトウェア リリース 17.6 以降を搭載した Cisco Catalyst 9130AXE ユニファイド アクセス ポイントでサポートされています。グローバルトライ無線モードは ワイヤレスコントローラ で有効化され、AP プロビジョニング中に設定されます。

アンテナ無線プロファイルの作成方法については、アンテナ無線プロファイルの作成 （520 ページ）を参照してください。

b) [Slot 1] および [Slot 2] ドロップダウンリストから、AP 無線スロットのビーム選択値を設定します。
c) [Save] をクリックします。
d) [AP Zone Name] ドロップダウンリストから、AP ゾーンを選択します。



（注） このドロップダウンリストは、サイトのネットワークプロファイルに AP ゾーンが追加されている場合にのみ有効になります。

AP ゾーンを選択した場合、RF プロファイルが AP ゾーン設定から継承されます。

e) [RF Profile] ドロップダウンリストから、デフォルト設定を使用するか、リストから別の値を選択します。

デフォルトの RF プロファイルは、**[Design]** > **[Network Settings]** > **[Wireless]** > **[RF Profiles]** > **[Basic RF Profile]** タブでデフォルトとマークしたカスタムプロファイルです。



（注） [AP Zone] ドロップダウンリストから AP ゾーンを選択した場合、このドロップダウンリストは無効になります。

f) [Mesh Role] ドロップダウンリストで、[Root] または [Mesh] を選択します。

ワイヤレス メッシュ ネットワークについての情報は ワイヤレス メッシュ ネットワークについて（531 ページ） を参照してください。

g) [Next] をクリックします。

ステップ 7 [Summary] ステップでデバイスの詳細を確認し、[Next] をクリックして AP をプロビジョニングします。

ステップ 8 展開のためのタスクのスケジュールを設定します。

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

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 9 [Tasks] ウィンドウで、タスクの展開を監視します。

ステップ 10 AP グループの作成または変更が進行中であることを示すメッセージに続き、プロビジョニング後に AP がリブートすることを示すメッセージが表示されます。[OK] をクリックします。

展開が正常に完了した場合、[Inventory] ウィンドウの [Last Sync Status] 列に「SUCCESS」と表示されます。

ワイヤレスコントローラ から別の ワイヤレスコントローラ に AP を移行する

次の手順を使用して、ネットワーク階層内の同じフロアにあるワイヤレスコントローラから別のワイヤレスコントローラに AP を移行します。

始める前に

- 古いワイヤレスコントローラ（例：WC1）が、プライマリ管理対象 AP の場所として必要なサイト（例：Building-1 の Floor-1、Floor-2、Floor-3）でプロビジョニングされていることを確認します。
- 移行する必要がある AP が、古いワイヤレスコントローラによって管理されているフロア（例：WC1 で管理されている Building-1/Floor-1、Building-1/Floor-2、Building-1/Floor-3）にプロビジョニングされていることを確認します。

手順

ステップ 1 新しい建物とフロアをネットワーク階層に追加します（例：Building-New と Floor-New）。詳細については、ビルディングの追加、編集、および削除（286 ページ）およびフロアの追加、編集、および削除（287 ページ）を参照してください。

ステップ 2 ワイヤレス ネットワーク プロファイルを作成し、新たに追加されたフロア（Floor-New）に割り当てます。詳細については、「ワイヤレス用のネットワークプロファイルの作成（543 ページ）」を参照してください。

ステップ 3 プライマリ管理対象 AP の場所として新たに追加されたフロア（Floor-New）を使用して古いワイヤレスコントローラを再プロビジョニングし、古いサイト（Floor-1、Floor-2、および Floor-3）を削除します。詳細については、Cisco AireOS コントローラのプロビジョニング（738 ページ）およびCisco Catalyst 9800 シリーズ ワイヤレス コントローラ のプロビジョニング（782 ページ）を参照してください。

ステップ 4 プライマリ管理対象 AP の場所として古いサイト（Floor-1、Floor-2、および Floor-3）を使用して、新しいワイヤレスコントローラ（WC2 など）をプロビジョニングします。詳細については、Cisco AireOS コントローラのプロビジョニング（738 ページ）およびCisco Catalyst 9800 シリーズ ワイヤレス コントローラ のプロビジョニング（782 ページ）を参照してください。

ステップ 5 [Configure Access Points] ワークフローを使用して、プライマリ ワイヤレスコントローラ名と IP アドレスを変更します。このワークフローの **[APパラメータの設定（Configure AP Parameters）]** ウィンドウで次の手順を実行します。

a) [High Availability] チェックボックスをオンにします。

b) [Select Primary Controller Name] ドロップダウンリストから、新しいワイヤレスコントローラ（WC2）を選択します。

c) [Primary Controller IP Address] フィールドに、新しいワイヤレスコントローラの IP アドレス（WC2 の IP アドレス）を入力します。

詳細については、「AP の設定（1639 ページ）」を参照してください。

ステップ 6 次の手順を実行して、AP が新しい ワイヤレスコントローラ（*WC2*）に参加していることを確認します。

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

b) [Inventory] ウィンドウの上部にある [Access Points] デバイスファミリボタンをクリックします。

c) [Focus] ドロップダウンリストにカーソルを合わせて、[Inventory] を選択します。

d) [Associated WLC IP] 列で、AP に対応する ワイヤレスコントローラ の IP アドレスを確認します。

この列が表示されない場合は、ウィンドウの右上隅にある歯車アイコンをクリックし、テーブル設定をカスタマイズして列を表示します。詳細については、「インベントリに関する情報の表示（102 ページ）」を参照してください。

（注） AP がフラッピングしていて、AUTO_INV_EVENT_SYNC_DISABLED または INV_EVENT_SYNC_DISABLED タグが割り当てられている場合、AP でのイベントの自動同期は無効になります。AP フラッピングの根本原因を解決したら、手動同期を実行して、最新の AP の詳細を表示することを推奨します。または、次にスケジュールされた同期による AP 情報の更新を待ちます。

ステップ 7 AP を再プロビジョニングして、最新の設定を展開します。詳細については、Day 1 の Cisco AP プロビジョニング （745 ページ）を参照してください。

AP のリセット

工場出荷時の状態へのリセット機能を使用すると、AP の設定をクリアし、デフォルト設定にリセットできます。AP の設定がクリアされると、AP が再起動します。

重要 AP をリセットすると、関連付けられているすべてのクライアントのネットワーク接続が中断されます。

始める前に

AP が到達可能であることを確認してください。

手順

ステップ 1 メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
[Inventory] ウィンドウに、検出されたデバイスのリストが表示されます。

ステップ 2 **[Devices]** テーブルで、**[Access Points]** デバイスファミリボタンをクリックして、使用可能な AP のリストを表示します。

ステップ 3 リセットする AP の横にあるチェックボックスをオンにします。

工場出荷時の状態にリセットする AP は、最大 100 個選択できます。

ステップ 4 **[Actions]** ドロップダウンリストから、**[Provision]** > **[Factory Reset]** を選択します。
[Factory Reset] スライドインペイン が開きます。

ステップ 5 [工場出荷時の状態へのリセット（Factory Reset）] で、次のいずれかのオプションを選択します。

- **[Clear all configuration]**：AP のすべての設定をクリアし、デフォルト設定にリセットします。
- **[Clear all configuration except static IP]**：静的 IP 設定を除き、AP のすべての設定をクリアします。

ステップ 6 [タスクのスケジュール（Schedule Task）] で、次の手順を実行します。

a) 次のオプションのいずれかを選択します。

- **[Now]**：AP をすぐにリセットします。
- **[Later]**：将来の日付または時刻で AP のリセットをスケジュールします。

b) （任意） [Task Name] フィールドで、タスク名を更新します。

c) [Later] を選択した場合は、次の手順を実行します。

- **[Start Date/Time]** で、タスクの開始日時を指定します。
- **[Time Zone]** ドロップダウンリストから、タスクのタイムゾーンを選択します。

ステップ 7 リセットするよう選択された AP を確認するには、**[Selected Devices]** ドロップダウンリストを展開します。

ステップ 8 [適用（Apply）] をクリックします。

AP のリセットのステータスを確認するには、**[Activities]** > **[Tasks]** ウィンドウに移動し、関連する作業項目を開きます。

FlexConnect モードの AP における ICMP ping の有効化

到達不能状態にある FlexConnect モードの AP への Internet Control Message Protocol（ICMP）ping を有効にすることができます。Catalyst Center は、ICMP を使用して、到達不能状態にある FlexConnect AP への ping を 5 分ごとに実行することで到達可能性を強化してから、[Inventory] ウィンドウの到達可能性ステータスを更新します。

手順

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

ステップ 2 [Enable ICMP ping for unreachable access Points in FlexConnect mode] チェックボックスをオンにして ICMP ping を有効にします。

ステップ 3 [保存（**Save**）] をクリックします。

「ICMP pingステータスが正常に更新されました（ICMP Ping status updated successfully）」という成功メッセージが表示されます。

Catalyst Centerは、シスコ ワイヤレス コントローラとの関連付けは解除されているが到達可能なFlexConnect APへのpingを開始します。到達可能性ステータスは[Inventory] ウィンドウで確認できます。

ステップ 4 到達可能性ステータスを確認するには、**[Provision]** > **[Inventory]** を選択します。

ステップ 5 デバイスがICMP pingによって到達可能である場合、[Reachability] 列に [Ping Reachable] と表示されます。

Cisco AireOS Mobility Express AP の Day-0 ワークフロー

始める前に

Cisco Mobility Express ワイヤレス ネットワーク ソリューションは、1 つ以上の 802.11ac Wave 2 Cisco Aironet シリーズのアクセスポイント（AP）と、ネットワーク内のその他の AP を管理する内蔵ソフトウェアベースのワイヤレスコントローラで構成されます。ワイヤレスコントローラとして機能している AP は、「プライマリ *AP*」と呼ばれます。このプライマリ AP によって管理される Cisco Mobility Express ネットワーク内のその他の AP は「従属 *AP*」と呼ばれます。

- サイト、ビルディング、フロアなどのネットワーク階層を設計します。詳細については、サイトの作成、編集、削除（285ページ）、ビルディングの追加、編集、および削除（286ページ）、およびフロアの追加、編集、および削除（287ページ）を参照してください。
- CLI、SNMP、HTTP、HTTPSなどのデバイスログイン情報をグローバルレベルで定義します。グローバルレベルで定義されたログイン情報は、サイトによって継承されます。詳細については、グローバルCLIクレデンシャルの追加（379ページ）、グローバルSNMPv2cログイン情報の追加（380ページ）、およびグローバルSNMPv3ログイン情報の追加（382ページ）を参照してください。
- WLAN、インターフェイス、RF プロファイルを作成します。
- DHCP サーバーにオプション #43 とオプション #60 を設定します。これは Catalyst Center プラグアンドプレイサーバーの IP アドレスです。この IP アドレスを使用して、AP は PnP サーバーに接続し、設定をダウンロードします。
- インベントリにMobility Express APがあることを確認してください。ない場合は、[Discovery] 機能を使用して検出します。詳細については、CDP を使用したネットワークの検出（86ページ）、IP アドレス範囲または CIDR を使用したネットワークの検出（90 ページ）、およびインベントリについて（100 ページ）を参照してください。
- AP は、シスコ ワイヤレス コントローラ 設定なしで初期設定へリセットされた状態である必要があります。

手順

ステップ 1 Cisco Mobility Express は DHCP サーバーに接続し、Catalyst Center プラグアンドプレイサーバーに接続します。

ステップ 2 DHCP サーバーは、Catalyst Center プラグアンドプレイサーバーの IP アドレスであるオプション #43 で IP アドレスを割り当てます。

ステップ 3 Mobility Express AP は PnP エージェントを開始し、PnP サーバーに接続します。

（注） ネットワーク内に一連の Mobility Express AP がある場合、内部プロトコルを通過します。プロトコルは 1 つの Mobility Express AP を選択します。これは、シスコ ワイヤレス コントローラで、PnP サーバーに到達するためのプライマリ AP として設定されます。

ステップ 4 **[Provision]** > **[Network Devices]** > **[Plug and Play]** タブで未要求 AP を検索します。

テーブルには、すべての未要求デバイスが一覧表示されます。[State] 列が [Unclaimed] として表示されます。[Filter] または [Find option] を使用して、特定のデバイスを検索することができます。

[Onbording Status] が [Initialized] になるまで待機する必要があります。

ステップ 5 この AP を要求するには、AP デバイス名の横にあるチェックボックスをオンにします。

ステップ 6 デバイステーブルの上にあるメニューバーで、**[Actions]** > **[Claim]** の順に選択します。

[デバイスの要求（Claim Devices）] ウィンドウが表示されます。

ステップ 7 [Site Assignement] ウィンドウで、[Site] ドロップダウンリストからサイトを選択します。

選択された AP のこの特定のサイトに対する要求は、関連付けられている構成にも適用されます。

ステップ 8 **[次へ (Next)]** をクリックします。

ステップ 9 デバイスを設定するには、[Configuratio] ウィンドウのデバイス名をクリックします。

ステップ 10 [Configuration for device name] ウィンドウで、デバイスの静的 IP の詳細を割り当てます。

- **[Management IP]**
- **[Subnet Mask]**
- **[Gateway]**

ステップ 11 [Save] をクリックします。

ステップ 12 [Next] をクリックします。

[Summary] ウィンドウが表示されます。

ステップ 13 [Summary] ウィンドウで [Claim] をクリックします。

Mobility Express AP が要求されると、設定された IP アドレスが Mobility Express AP に割り当てられます。

要求したデバイス（AP）とワイヤレスコントローラが **[Provision]** > **[Device Inventory]** > **[Inventory]** に表示されることを確認します。

ステップ 14 （任意） CSV ファイルからデバイスを一括して追加します。

詳細については、デバイスの一括追加 （711 ページ）を参照してください。

CSV ファイルを使用して Mobility Express AP を一括インポートすると、すべての Mobility Express AP が **[Device]** > **[Plug and Play]** ウィンドウに表示されます。VRRP プロトコルに基づいて、インポートされた Mobility Express AP のうち 1 台だけがプライマリ AP になります。残りの AP は従属 AP になります。プライマリ AP を要求した後、下位 AP を要求する必要はありません。Catalyst Center は、[Plug and Play] ウィンドウから下位 AP をクリアしません。これらの下位 AP は、**[Devices]** > **[Plug and Play]** ウィンドウから手動で削除する必要があります。

ステップ 15 シスコ ワイヤレス コントローラ をプロビジョニングするには、Cisco AireOS コントローラのプロビジョニング （738 ページ） を参照してください。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの設定とプロビジョニング

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの概要

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラは、インテントベース ネットワーク用に構築された次世代のワイヤレスコントローラです。Cisco Catalyst 9800 シリーズ ワイヤレス コントローラは Cisco IOS XE ベースであり、Aironet の優れた RF 性能と Cisco IOS XE のインテントベースのネットワーキング機能を統合して、組織にクラス最高水準のワイヤレスエクスペリエンスを生み出します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラはモジュール型オペレーティングシステムに基づいて構築され、オープンでプログラマブルな API 機能が搭載されていて、0 日目から *n* 日目のネットワーク運用を自動化できます。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラは、次のような複数のフォームファクタで使用できます。

- Catalyst 9800-40 ワイヤレスコントローラ。
- Catalyst 9800-80 ワイヤレスコントローラ。
- Catalyst 9800-CL Cloud ワイヤレスコントローラ：プライベートクラウド（ESXi、KVM、Cisco ENCS、および Hyper-V）に展開可能、Catalyst Center で管理可能。
- Catalyst 9300 シリーズ スイッチ、Catalyst 9400 シリーズ スイッチ、および Catalyst 9500H シリーズ スイッチ用 Catalyst 9800 組み込みワイヤレスコントローラ。

- Cisco Catalyst 9800-L ワイヤレスコントローラ：中小企業向けにシームレスなソフトウェアアップデートを提供します。Cisco Catalyst 9800-L ワイヤレスコントローラは 2 つのバリエーションで使用できます。銅線と光ファイバアップリンクのいずれかを選択でき、ネットワークの柔軟性が向上します。

次の表に、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラでサポートされている仮想プラットフォームおよびハードウェア プラットフォームを一覧表示します。

プラットフォーム	説明
Cisco Catalyst 9800-80 ワイヤレスコントローラ	最大 6000 アクセスポイントと 64,000 クライアントをサポートします。 最大 80 Gbps のスループットをサポートし、2 ラックユニットスペースを使用します。 最大 100-GE のアップリンクおよびシームレスなソフトウェアアップデートを搭載したモジュール型ワイヤレスコントローラ。
Cisco Catalyst 9800-40 ワイヤレスコントローラ	シームレスなソフトウェアアップデートを備えた、中小企業やキャンパスでの導入向けの固定ワイヤレスコントローラ。 最大 2000 アクセスポイントと 32,000 クライアントをサポートします。 最大 40 Gbps のスループットをサポートし、1 ラックユニットスペースを使用します。 4 つの 1-GE または 10-GE アップリンクポートを提供します。
Cisco Catalyst 9800-CL Cloud ワイヤレス コントローラ	Cisco Catalyst 9800-CL クラウド ワイヤレス コントローラは、プライベートクラウドまたはパブリッククラウドに Infrastructure as a Service（IaaS）として導入できます。 Cisco Catalyst 9800-CL クラウド ワイヤレス コントローラは、ハイアベイラビリティとセキュリティを実現するために構築された次世代のエンタープライズクラスの仮想ワイヤレスコントローラです。 Cisco Catalyst 9800-CL クラウド ワイヤレスコントローラの仮想フォームファクタは、ESXi、KVM、Cisco ENCS、および Hyper-V ハイパーバイザをサポートするプライベートクラウド向けです。
Catalyst 9000 シリーズスイッチ用 Cisco Catalyst 9800 組み込みワイヤレスコントローラ	Catalyst 9000 シリーズスイッチ用 Cisco Catalyst 9800 組み込みワイヤレスコントローラは、有線およびワイヤレス インフラストラクチャを一貫したポリシーと管理とともに提供します。 この導入モデルは、小規模キャンパスや分散型ブランチ向けの安全性に優れたソリューションである Cisco SD-Access でのみサポートされます。組み込みコントローラは、ファブリックモードでのみアクセスポイント（AP）をサポートします。

プラットフォーム	説明
Cisco Catalyst 9800-L ワイヤレス コントローラ	Cisco Catalyst 9800-L ワイヤレスコントローラは、中小企業向けにシームレスなソフトウェアアップデートを提供します。Cisco Catalyst 9800-L ワイヤレスコントローラは 2 つのバリエーションで使用できます。銅線と光ファイバアップリンクのいずれかを選択でき、ネットワークの柔軟性が向上します。 • Cisco Catalyst 9800-L Copper シリーズ ワイヤレス コントローラ（9800-L-C RJ45） • Cisco Catalyst 9800-L ファイバ シリーズ ワイヤレス コントローラ（9800-L-F SFP）

次の表に、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラでサポートされているホスト環境を一覧表示します。

ホスト環境	ソフトウェア バージョン
VMware ESXi	• VMware ESXi vSphere 6.0 • VMware ESXi vSphere 6.5[3] • VMware ESXi vCenter 6.0 • VMware ESXi VCenter 6.5
KVM	• Red Hat Enterprise Linux 7.1 および 7.2 をベースとした Linux KVM • Ubuntu 14.04.5 LTS、Ubuntu 16.04.5 LTS
NFVIS	Cisco ENCS 3.8.1 および 3.9.1

[3] ESXi vSphere を使用した C9800-CL の .ova ファイルのインストールは機能しません。これは C9800 ova に限定されませんが、他の製品に影響します。シスコと VMware は、問題解決に向けて積極的に取り組んでいます。問題が修正されたかどうかを確認するには、シスコのアカウント担当者にお問い合わせください。VMware 6.5 および C9800-CL OVA ファイルの展開に固有の問題があります。「必要なディスクイメージがありません。（A required disk image was missing）」という警告が表示され、「VM の展開に失敗しました：postNFCData に失敗しました：ディスク以外のファイルに POST できません。（Failed to deploy VM: postNFCData failed: Cannot POST to non-disk files.）」というエラーで展開が失敗します。VMware ESXi 6.5 に C9800-CL をインストールするには、次のいずれかを実行します。1）ESXi 組み込み GUI を使用して C9800-CL の .iso ファイルをインストールする（ESXI 6.5 クライアントバージョン 1.29.0 はテスト済みであり必須です）。2）OVF ツールを使用して C9800-CL の .ova ファイルをインストールする。

次の表に、Catalyst Center でサポートされている Cisco Enterprise Network Function Virtualization Infrastructure Software（NFVIS）のバージョンを示します。

（注） Cisco Enterprise NFVIS デバイスは、N-1 から N へのアップグレードパスのみをサポートします。たとえば、Cisco Enterprise NFVIS 3.11.x からは Cisco Enterprise NFVIS 3.12.x へのアップグレードのみがサポートされています。Cisco Enterprise NFVIS 3.11.x から Cisco Enterprise NFVIS 4.1.x へのアップグレードはサポートされていません。

Cisco Enterprise NFVIS バージョン	エンタープライズ ネットワーク コンピューティング システム デバイス プラットフォーム	注記
4.1.2 4.1.1 3.12.3 3.11.3 3.11.2 3.11.1	ENCS 5400 UCS-E UCS-C	Catalyst Center は、次の NFVIS アップグレードパスをサポートします。NFVIS v3.11.1 > 3.11.2 > 3.11.3 > 3.12.3 > 4.1.1 > 4.1.2。 Cisco Enterprise NFVIS 3.12.1 は、Catalyst Center のいずれのバージョンでもサポートされていません。 Catalyst Center を使用した、Cisco Enterprise NFVIS 3.11.x から Cisco Enterprise NFVIS 3.12.1 へのアップグレードはサポートされていません。 Catalyst Center を使用した、Cisco Enterprise NFVIS 3.12.1 から Cisco Enterprise NFVIS 3.12.2 へのアップグレードはサポートされていません。 Catalyst Center を使用した、Cisco Enterprise NFVIS 3.11.2 から 3.12.2 へのアップグレードはサポートされていません。 Cisco Enterprise NFVIS 3.12.2 は、Catalyst Center でサポートされています。
3.12.2 3.11.3 3.11.2 3.11.1	ENCS 5100	Cisco 5100 ENCS は、Cisco Enterprise NFVIS 3.10.x をサポートしていません。

Catalyst Center での Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の構成

1. Catalyst Center をインストールします。

   詳細については、『Cisco Catalyst Center Installation Guide』[英語] を参照してください。

2. ソフトウェアイメージのアップグレードに関する詳細については、Cisco Catalyst 9800 シリーズワイヤレスコントローラでのソフトウェアイメージのアップグレードのサポート（762 ページ） を参照してください。

3. Catalyst Center GUI にログインし、必要なアプリケーションが [Running] 状態であることを確認します。

   メインメニューから次を選択します。**[System Settings]** > **[Software Updates]** > **[Installed Apps]** の順に選択します。

4. Cisco Identity Services Engine と Catalyst Center を連動させます。統合後、関連する設定やデータとともに Catalyst Center が検出されたデバイスは、Cisco ISEにプッシュされます。

5. Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ を検出します。

   Cisco Catalyst 9800 シリーズ ワイヤレス コントローラを検出するには、NETCONF を有効にしてポートを 830 に設定する必要があります。NETCONF は、ネットワークデバイスの設定をインストール、操作、削除するためのメカニズムです。

   詳細については、CDP を使用したネットワークの検出 （86 ページ）またはIP アドレス範囲または CIDR を使用したネットワークの検出 （90 ページ）を参照してください。

   ワイヤレス管理 IP アドレスを手動で追加する必要があります。

（注） Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ では、プロビジョニングの失敗を防ぐために、ワイヤレス管理インターフェイスの静的 IP アドレスを設定する必要があります。

   [Discovery] ウィンドウで Cisco Discovery Protocol（CDP）または IP アドレス範囲を使用して検出を実行する場合は、[Preferred Management IP] ドロップダウンリストから [Use Loopback] を選択して、デバイスのループバック インターフェイスの IP アドレスを指定します。

6. 検出されたデバイスが [Device Inventory] ウィンドウに [Managed] 状態で表示されていることを確認します。

   詳細については、インベントリについて （100 ページ）およびインベントリに関する情報の表示 （102 ページ）を参照してください。

   デバイスが [Managed] 状態になるまで待機する必要があります。

7. Cisco Catalyst 9800 シリーズ ワイヤレス コントローラとのAssurance接続を確認するには、次のコマンドを使用します。

   - **#show crypto pki trustpoints | sec DNAC-CA**

```
Trustpoint DNAC-CA
    Subject Name:
    cn=kube-ca
          Serial Number (hex): 00E***************
    Certificate configured.
```

   - **#show crypto pki trustpoints | sec sdn-network**

```
Trustpoint sdn-network-infra-iwan:
    Subject Name:
    cn=sdn-network-infra-ca
        Serial Number (hex): 378***************
    Certificate configured.
```

- **#show telemetry ietf subscription all**

```
Telemetry subscription brief

  ID               Type        State       Filter type
  ------------------------------------------------------
  1011             Configured  Valid       tdl-uri
  1012             Configured  Valid       tdl-uri
  1013             Configured  Valid       tdl-uri
```

- **#show telemetry internal connection**

```
Telemetry connection

Address Port Transport State Profile
------------------------------------------------------------
IP address 25103 tls-native Active sdn-network-infra-iwan
```

- **#show network-assurance summary**

```
Network-Assurance                       : True
Server Url                              : https://10.***.***.***
ICap Server Port Number                 : 3***
Sensor Backhaul SSID                    :
Authentication                          : Unknown
```

8. 認証サーバーとポリシーサーバーの設定時に TACACS サーバーを設定します。

   Cisco Catalyst 9800 シリーズ ワイヤレス コントローラでユーザー名をローカルに設定している場合、TACACS の設定は必須ではありません。

9. サイト、ビルディング、フロアを追加してネットワーク階層を設計すると、後で設計の設定や構成を適用する場所を簡単に特定できるようになります。

   新しいネットワーク階層を作成します。または Cisco Prime Infrastructure に既存のネットワーク階層がある場合は、それを Catalyst Center にインポートできます。

   既存のネットワーク階層をインポートしてアップロードするには、Catalyst Center へのサイト階層のインポート （277 ページ）を参照してください。

   新しいネットワーク階層を作成するには、サイトの作成、編集、削除 （285 ページ）およびビルディングの追加、編集、および削除 （286 ページ）を参照してください。

10. AP の位置情報を追加し、フロアマップに配置して、ヒートマップカバレッジを可視化します。

    詳細については、「フロアマップでの AP の取り扱い （304 ページ）」を参照してください。

11. AAA（Cisco ISE がネットワークとクライアントエンドポイント向けに設定されている）、NetFlow コレクタ、NTP、DHCP、DNS、syslog、SNMP トラップなどのネットワーク設

定を定義します。これらのネットワークサーバーが、ネットワーク全体のデフォルトになります。AAA サーバーを追加するときに、TACACS サーバーを追加できます。

詳細については、ネットワーク設定の概要 （373 ページ）、グローバル ネットワーク サーバーの設定 （377 ページ）、および「AAA サーバーの追加」を参照してください。

12. カスタムとして、親プロファイルでワイヤレス無線周波数プロファイルを作成します。

    詳細については、「ワイヤレス無線周波数プロファイルの作成 （451 ページ）」を参照してください。

13. IP アドレスプールをグローバルレベルで作成します。

    Catalyst Center Cisco DNA Center は、IP アドレスプールを使用して、SD-Access ネットワークの設定と展開を自動化します。

    IP アドレスプールを作成するには、IP アドレスプールを設定する （397 ページ）を参照してください。

    プロビジョニングするビルディング用に IP アドレスプールを予約する必要があります。詳細については、「IP アドレスプールの予約」を参照してください。

14. エンタープライズおよびゲスト ワイヤレス ネットワークを作成します。グローバルワイヤレス設定を 1 回定義します。次に、Catalyst Centerは地理的な場所全体でさまざまなデバイスに設定をプッシュします。

    ワイヤレスネットワークの設計は、2 段階のプロセスです。まず SSID を作成し、次に作成した SSID をワイヤレス ネットワーク プロファイルに関連付ける必要があります。このプロファイルは、サイトにデバイスを展開するために使用されるトポロジを構築するのに役に立ちます。



（注） 以前のリリースからアップグレードする場合：

- WPA3-Enterprise SSID の場合、Catalyst Center は、SSID の Dot1x-SHA256 認証キー管理設定を有効にします。
- WPA2-WPA3-Enterprise SSID の場合、Catalyst Center は、SSID の Dot1x 認証キー管理設定と Dot1x-SHA256 認証キー管理設定の両方を有効にします。

この設定により、Cisco IOS XE リリース 17.6 以前を実行している Cisco AireOS ワイヤレスコントローラ および ワイヤレスコントローラ の意図した設定が変更される可能性があります。ワイヤレスコントローラ を再プロビジョニングする前に、SSID の**認証キー管理**設定を更新できます。

詳細については、エンタープライズ ワイヤレス ネットワーク用 SSID の作成 （415 ページ）およびゲスト ワイヤレス ネットワークの SSID の作成 （432 ページ）を参照してください。その他のワイヤレス設定については、グローバルワイヤレス設定の構成 （414 ページ）を参照してください。

15. バックホールの設定を行います。詳細については、「バックホール設定の管理（518ページ）」を参照してください。

16. Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の [Policy] ウィンドウで、次の設定を行います。

    - 仮想ネットワークを作成します。仮想ネットワークを使用して、物理ネットワークを複数の論理ネットワークにセグメント化できます。
    - グループベースのアクセス コントロール ポリシーを作成し、契約を追加する。詳細については、「グループベースのアクセス コントロール ポリシーの作成（1423ページ）」を参照してください。

17. 高可用性を設定します。

    詳細については、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の高可用性の設定 （763 ページ）」を参照してください。

18. 設計フェーズ中に追加された設定を使用して、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ をプロビジョニングします。

    詳細については、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のプロビジョニング （782 ページ）」を参照してください。

19. Cisco Catalyst 9800 シリーズ ワイヤレス コントローラでアプリケーションポリシーを設定および展開します。

    詳細については、アプリケーションポリシーの作成（1470ページ）、アプリケーションポリシーの展開（1476ページ）、およびアプリケーションポリシーの編集（1475ページ）を参照してください。

（注） アプリケーションポリシーを展開する前に、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラデバイスをプロビジョニングする必要があります。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ デバイスの場合、2 つの異なる SSID で異なるビジネスとの関連性を持つ2つの異なるポリシーは機能しません。関連性を設定するときは、最後に展開したポリシーが常に優先されます。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ デバイスの場合、アプリケーションのデフォルトのビジネスとの関連性を変更しても、FlexConnect モードでは機能しません。

非ファブリック SSID にのみアプリケーションポリシーを適用できます。

Cisco Catalyst 9800 シリーズ ワイヤレスコントローラでのソフトウェアイメージのアップグレードのサポート

始める前に

- Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ を検出します。

  Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ を検出するには、NETCONF を有効にしてポートを 830 に設定します。NETCONF は、ネットワークデバイスの設定をインストール、操作、削除するためのメカニズムです。これにより、コントローラでワイヤレスサービスが有効になります。

  詳細については、CDP を使用したネットワークの検出 （86 ページ）またはIP アドレス範囲または CIDR を使用したネットワークの検出 （90 ページ）を参照してください。

- デバイスが [Device Inventory] に [Managed] 状態で表示されていることを確認します。

  詳細については、インベントリについて （100 ページ）およびインベントリに関する情報の表示 （102 ページ）を参照してください。

手順

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

[Inventory] ウィンドウが表示され、検出されたデバイスが一覧表示されます。

ステップ 2 ローカルコンピュータまたは URL から、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ ソフトウェア イメージをインポートします。

詳細については、「ソフトウェアイメージのインポート （638 ページ）」を参照してください。

ステップ 3 ソフトウェアイメージをデバイスファミリに割り当てます。

詳細については、「デバイスファミリに対するソフトウェアイメージの割り当ての管理 （640 ページ）」を参照してください。

ステップ 4 デバイスファミリまたは特定のデバイスロールの星印をクリックして、ソフトウェアイメージをゴールデンとしてマークできます。

詳細については、「ソフトウェアイメージをスタンダードとしてマークする （646 ページ）」を参照してください。

ステップ 5 ソフトウェアイメージのプロビジョニング

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

ステップ 6 [Inventory] ウィンドウで、イメージをアップグレードする Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の横にあるチェックボックスをオンにします。

ステップ 7 [Actions] ドロップダウンリストから、**[Software Image]** > **[Image Update]** を選択します。

詳細については、ソフトウェアイメージのプロビジョニング （653 ページ）を参照してください。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の高可用性の設定

始める前に

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ で高可用性（HA）を設定するための前提条件は次のとおりです。

- 両方の Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ が同じソフトウェアバージョンを実行していて、プライマリ ワイヤレスコントローラ 上にアクティブなソフトウェアイメージがあります。
- Catalyst 9800 シリーズ ワイヤレス コントローラ 1 と Catalyst 9800 シリーズ ワイヤレス コントローラ 2 のサービスポートおよび管理ポートが設定されています。
- Catalyst 9800 シリーズ ワイヤレス コントローラ 1 および Catalyst 9800 シリーズ ワイヤレス コントローラ 2 の冗長ポートが物理的に接続されています。
- インターフェイス設定、ルート追加、SSH回線設定、NETCONF-YANG設定などの事前設定が、Catalyst 9800 シリーズワイヤレス コントローラアプライアンスで完了しています。
- Catalyst 9800 シリーズ ワイヤレス コントローラ 1 と Catalyst 9800 シリーズ ワイヤレス コントローラ 2 の管理インターフェイスは同じサブネット内にあります。
- Catalyst 9800 シリーズ ワイヤレス コントローラ 1 デバイスおよび Catalyst 9800 シリーズ ワイヤレス コントローラ 2 デバイスのディスカバリとインベントリは、Catalyst Centerから正常に実行されます。
- デバイスは到達可能で、[Managed] の状態になっています。

手順

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

[Inventory] ウィンドウが表示され、検出されたデバイスが一覧表示されます。

ステップ 2 特定のサイトで使用可能なデバイスを表示するには、左側のペインで [Global] サイトを展開し、関心のあるサイト、ビルディング、またはフロアを選択します。

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

ステップ 3 [Devices] テーブルで、[Search] フィールドをクリックします。[Quick Filters] タブで、次の手順を実行します。

1. [Device Family] で、[Wireless Controllers] をクリックして、検出された ワイヤレスコントローラ のリストを取得します。
2. [Reachability] で、[Reachable] をクリックして、検出された到達可能な ワイヤレスコントローラ のリストを取得します。
3. [適用（Apply）] をクリックします。

ステップ 4 [Inventory] ウィンドウで必要な Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ 名の隣にあるチェックボックスをオンにし、プライマリコントローラとしてプロビジョニングします。

ステップ 5 [Actions] にカーソルを合わせて **[Provision]** > **[Configure WLC HA]** を選択します。

[High Availability] スライドインペインが表示されます。

（注） 選択したコントローラがサイトに割り当てられていない場合は、ペインの上部に警告が表示されます。Catalyst Centerは、サイトに割り当てられるまでテレメトリ設定をコントローラにプッシュしません。

デフォルトでは、選択された Catalyst 9800 シリーズ ワイヤレス コントローラがプライマリコントローラになり、[Primary C9800] フィールドが無効になります。

ステップ 6 Cisco Catalyst 9800-CL ワイヤレス コントローラ の場合、[Select Primary Interface および [Select Secondary Interface] ドロップダウンリストから、HA 接続に使用するインターフェイスを選択します。

HA インターフェイスは次の目的で使用されます。

- IOSd が起動する前に、コントローラペア間の通信を有効にする。
- すべてのコントローラペアに IPC のトランスポートを提供する。
- コントローラペア間で交換される制御メッセージ全体の冗長性を有効にする。制御メッセージには、HA ロールの解決、キープアライブ、通知、HA 統計情報などがあります。

ステップ 7 [Select Secondary C9800] ドロップダウンリストから、HA ペアを作成するセカンダリコントローラを選択します。

（注） プライマリコントローラのワイヤレス管理インターフェイス IP サブネットに基づいてセカンダリコントローラを選択すると、冗長性管理 IP が自動入力され、次のメッセージとともに [High Availability] ウィンドウの上部に **i** アイコンが表示されます。

冗長性管理 IP とピア冗長性管理 IP が他のネットワークエンティティに割り当てられていないことを確認します。IP が使用されている場合は、適宜 IP を変更して設定します。

ステップ 8 各フィールドに [Redundancy Management IP] と [Peer Redundancy Management IP] のアドレスを入力します。

（注）
- 冗長性管理 IP およびピア冗長性管理 IP に使用される IP アドレスは、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の管理インターフェイスと同じサブネットに設定する必要があります。これらの IP アドレスがそのサブネット範囲内で未使用の IP アドレスであることを確認します。
- Catalyst Center は Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の管理 IP アドレスを Cisco ISE ネットワーク アクセス デバイス リストにプッシュするだけです。一方、スタンバイコントローラは冗長性管理 IP アドレスを使用して AAA 要求を開始します。したがって、シームレスなクライアント認証とスタンバイモニタリングのために、冗長性管理 IP アドレスを AAA サーバーに追加する必要があります。

ステップ 9 [Netmask] ドロップダウンリストで、ネットマスクアドレスを選択します。

ステップ 10 [Configure HA] をクリックします。

ステップ 11 展開のためのタスクのスケジュールを設定します。

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

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

（注） [Preview Configuration] ウィンドウには、プライマリ ワイヤレスコントローラとセカンダリ ワイヤレスコントローラの設定が表示されます。

ステップ 12 [Tasks] ウィンドウで、タスクの展開を監視します。

タスクが展開されると、HA 設定は、CLI コマンドを使用してバックグラウンドで開始されます。最初に、プライマリコントローラが設定されます。成功すると、セカンダリコントローラが設定されます。HA が有効になると、両方のデバイスが再起動します。このプロセスは、完了するまで最大 2.5 分かかります。

ステップ 13 HA 設定を確認するには、次の手順を実行します。

a) **[Provision]** > **[Inventory]** ウィンドウで、HA デバイスとして設定したデバイスをクリックします。高度なデバイス情報を含むダイアログボックスが開きます。

b) このダイアログボックスで、[View Details] をクリックします。

c) [Wireless Info] タブをクリックします。

[Redundancy Summary] タブには、[Sync Status] が [HA Pairing is in Progress] として表示されます。HA ペアリングが成功したことを Catalyst Center が検出すると、[Sync Status] が [Complete] になります。

このプロセスは、インベントリポーラーまたは手動による再同期によってトリガーされます。これで、セカンダリコントローラ（Catalyst 9800 シリーズ ワイヤレス コントローラ 2）が Catalyst Center から削除されます。このフローは、Catalyst 9800 シリーズ ワイヤレス コントローラ での正常な HA 設定を示しています。

ステップ 14 コントローラを手動で再同期するには、次の手順を実行します。

a) **[Provision]** > **[Inventory]** ウィンドウで、手動で同期するコントローラの横にあるチェックボックスをオンにします。

b) [Actions] ドロップダウンリストから [Inventory] > [Resync Device] の順に選択します。

次のタスク

HA プロセスが完了した後に発生するアクションを次に示します。

- Catalyst 9800 シリーズ ワイヤレス コントローラ 1 および Catalyst 9800 シリーズ ワイヤレス コントローラ 2 は、冗長性管理、冗長性単位、およびシングルサインオン（SSO）を使用して設定されます。デバイスが再起動し、そのロールをアクティブコントローラまたはスタンバイコントローラとしてネゴシエートします。構成はアクティブからスタンバイへと同期されます。

（注） Catalyst Center と HA セットアップでクライアントとエンドポイントの認証に AAA サーバーまたは Cisco ISE サーバーを設定した場合、アクティブコントローラとスタンバイコントローラの CTS ログイン情報が同期されるため、HA スイッチオーバー時に Catalyst Center は Cisco ISE でワイヤレスコントローラの CTS ログイン情報を更新しません。

- [冗長性の概要の表示（Show Redundancy Summary）] ウィンドウで、次の設定を確認できます。
  - SSO が有効になっています。
  - Catalyst 9800 シリーズ ワイヤレス コントローラ 1 はアクティブな状態です。
  - Catalyst 9800 シリーズ ワイヤレス コントローラ 2 はスタンバイ状態です。

高可用性（HA）に関する情報

高可用性（HA）によって、コントローラのフェールオーバーが原因で生じるワイヤレスネットワークのダウンタイムを短縮できます。Catalyst Center から Cisco Catalyst 9800 シリーズ ワイヤレス コントローラで HA を設定できます。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラで高可用性を設定するためのコマンド

手順

ステップ 1 次のコマンドを使用して、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのプライマリコントローラで HA を設定します。

- **chassis ha-interface GigabitEthernet <redundancy interface num> local-ip <redundancy ip> <netmask> remote-ip <peer redundancy ip>** コマンドを実行して、HA シャーシインターフェイスを設定します。

  次に、HA シャーシインターフェイスの設定例を示します。

  ```
  chassis ha-interface GigabitEthernet 3 local-ip 192.0.2.2 255.255.255.0
  remote-ip 192.0.2.3
  ```

- **reload** コマンドを実行して、変更が有効になるようにデバイスをリロードします。

ステップ 2 次のコマンドを使用して、Catalyst 9800 シリーズ ワイヤレス コントローラのセカンダリコントローラで HA を設定します。

- **chassis ha-interface GigabitEthernet <redundancy interface num> local-ip <redundancy ip> <netmask> remote-ip <peer redundancy ip>** コマンドを実行して、HA シャーシインターフェイスを設定します。

  次に、HA シャーシインターフェイスの設定例を示します。

  ```
  chassis ha-interface GigabitEthernet 2 local-ip 192.0.2.3 255.255.255.0
  remote-ip 192.0.2.2
  ```

ステップ 3 **chassis clear** コマンドを実行して、すべての HA 関連のパラメータ（ローカル IP、リモート IP、HA インターフェイス、マスク、タイムアウト、優先順位など）をクリアまたは削除します。

（注） **reload** コマンドを実行して、変更を反映するためにデバイスをリロードします。

ステップ 4 次のコマンドを使用して、Cisco Catalyst 9800-40 ワイヤレスコントローラおよび Cisco Catalyst 9800-80 ワイヤレス コントローラ デバイスのプライマリコントローラで HA を設定します。

- HA シャーシインターフェイスを設定するには、**chassis ha-interface local-ip <redundancy ip> <netmask> remote-ip <peer redundancy ip>** コマンドを実行します。

  次に、HA シャーシインターフェイスの設定例を示します。

  ```
  chassis ha-interface local-ip 192.0.2.2 255.255.255.0 remote-ip 192.0.2.3
  ```

- **reload** コマンドを実行して、変更が有効になるようにデバイスをリロードします。

ステップ 5 次のコマンドを使用して、Cisco Catalyst 9800-40 ワイヤレスコントローラおよび Cisco Catalyst 9800-80 ワイヤレス コントローラ デバイスのセカンダリコントローラで HA を設定します。

- HA シャーシインターフェイスを設定するには、**chassis ha-interface local-ip <redundancy ip> <netmask> remote-ip <peer redundancy ip>** コマンドを実行します。

  次に、HA シャーシインターフェイスの設定例を示します。

  ```
  chassis ha-interface local-ip 192.0.2.3 255.255.255.0 remote-ip 192.0.2.2
  ```

ステップ 6 **chassis clear** コマンドを実行して、すべての HA 関連のパラメータ（ローカル IP、リモート IP、HA インターフェイス、マスク、タイムアウト、優先順位など）をクリアまたは削除します。

（注） **reload** コマンドを実行して、変更を反映するためにデバイスをリロードします。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの高可用性を確認するためのコマンド

次のコマンドを使用して、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の高可用性構成を確認します。

- **config redundancy mode sso** コマンドを実行して、HA 関連の詳細情報を確認します。
- **show chassis** コマンドを実行して HA ペアのシャーシ設定を表示します。これには、MAC アドレス、ロール、スイッチプライオリティ、および冗長 HA ペア内の各コントローラデバイスの現在の状態が含まれています。
- **show ip interface brief** コマンドを実行して、プラットフォームで設定されている設定モードではなく、デバイスで実行されている実際に稼働中の冗長モードを表示します。
- **show redundancy states** コマンドを実行して、アクティブコントローラとスタンバイコントローラの冗長性状態を表示します。
- **show redundancy summary** コマンドを実行して、設定されているインターフェイスを確認します。
- ハイアベイラビリティ設定の詳細を確認するには、**show romvar** コマンドを実行します。

N+1 高可用性（HA）

N+1 高可用性（HA）の概要

Catalyst Center では、Cisco AireOS ワイヤレスコントローラおよび Cisco Catalyst 9800 シリーズ ワイヤレス コントローラでの N+1 高可用性（HA）がサポートされています。

Cisco AireOS ワイヤレスコントローラには、N+1 コントローラ向けの専用の型番（SKU）があります。Cisco Catalyst 9800 シリーズ ワイヤレス コントローラには専用の SKU がありません。

HA には同じモデルと PID を使用する必要があります。たとえば、Cisco Catalyst 9800-80 は別の 9800-80 とペアリングする必要があります。

N+1 HA アーキテクチャは、低い導入コストで、地理的に離れたデータセンター間のコントローラに冗長性をもたらします。

N+1 HA では、シスコ ワイヤレス コントローラを複数のプライマリコントローラのバックアップコントローラとして使用できます。これらのワイヤレスコントローラは互いに独立していて、インターフェイスの設定や IP アドレスを共有しません。AP フォールバックオプションが有効の場合、プライマリ ワイヤレスコントローラが動作を再開すると、AP はバックアップ ワイヤレスコントローラからプライマリ ワイヤレスコントローラに自動的にフォールバックします。

Catalyst Center Cisco DNA Center は、N+1 HA のプライマリおよびセカンダリコントローラの設定をサポートします。

N+1 HA は、グローバルレベルではなく AP レベルで設定されます。設定は AP に直接プッシュされます。

プライマリコントローラで高い優先順位が設定されている AP は、優先順位の低い AP が排除されることになっても、常に最初にバックアップコントローラに接続されます。

N+1 HA 設定には次の制限があります。

- VLAN ID の設定が原因で、セカンダリコントローラの自動プロビジョニングはサポートされていません。
- プライマリコントローラに変更を加えた場合、最新の設計の設定を使用してセカンダリコントローラを手動で再プロビジョニングする必要があります。
- Catalyst Center Cisco DNA Center では耐障害性はサポートされていません。
- アクセスポイントのステートフル スイッチ オーバー（AP SSO）機能は、N+1 HA ではサポートされていません。AP Control and Provisioning of Wireless Access Points（CAPWAP）ステートマシンは、プライマリコントローラに障害が発生したときに再起動されます。

Catalyst Center から N+1 高可用性を設定するための前提条件

- [Discovery] 機能を実行して、プライマリコントローラとセカンダリコントローラを検出します。

  詳細については、CDP を使用したネットワークの検出 （86 ページ）またはIP アドレス範囲または CIDR を使用したネットワークの検出 （90 ページ）を参照してください。

- ワイヤレスコントローラが到達可能で、[Managed] 状態である必要があります。

  詳細については、インベントリについて （100 ページ）およびインベントリに関する情報の表示 （102 ページ）を参照してください。

- デバイス間のネットワーク接続を確認します。プライマリコントローラがダウンしたときに、AP が N+1 の構成によってセカンダリコントローラに参加できるようにする必要があります。

- 2 つのビルディングを作成して、両方のデバイスのプライマリおよびセカンダリの場所を管理します。たとえば、ビルディング *A* とビルディング *B* という 2 つのビルディングを作成し、ビルディング A をコントローラ 1 のプライマリ管理場所かつコントローラ 2 のセカンダリ管理場所に設定し、ビルディング B をコントローラ 2 のプライマリ管理場所としてのみ設定できます。

  詳細については、サイトの作成、編集、削除 （285 ページ）およびビルディングの追加、編集、および削除 （286 ページ）を参照してください。

- 設計フェーズ中にカバレッジヒートマップが可視化されるようにするには、フロアマップに AP を追加して配置します。

  詳細については、「フロアマップでの AP の取り扱い （304 ページ）」を参照してください。

- 2つの SSID を作成し、バックホール SSID として関連付けます。

  詳細については、エンタープライズ ワイヤレス ネットワーク用 SSID の作成 （415 ページ）およびゲスト ワイヤレス ネットワークの SSID の作成 （432 ページ）を参照してください。

Catalyst Center からの N+1 高可用性の設定

この手順では、シスコ ワイヤレス コントローラ および Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ で N+1 高可用性（HA）を設定する方法を示します。

手順

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

[Inventory] ウィンドウが表示され、検出されたデバイスが一覧表示されます。

ステップ 2 プライマリコントローラとしてプロビジョニングするには、目的のコントローラの隣にあるチェックボックスをオンにします。

ステップ 3 [Actions] ドロップダウンリストから、**[Provision]** > **[Provision Device]** を選択します。

[Assign Site] ウィンドウが表示されます。

ステップ 4 プライマリコントローラのプライマリ管理対象 AP の場所を割り当てるには、**[Choose a site]** をクリックします。

ステップ 5 [Choose a site] ウィンドウで、サイトを選択して [Save] をクリックします。

ステップ 6 [Next] をクリックします。

[設定（Configuration）] ウィンドウが表示され、プライマリデバイスのプライマリ管理対象 AP の場所が表示されます。

ステップ 7 [Select Primary Managed AP Locations] をクリックして、プライマリコントローラの管理対象 AP のロケーションを追加または更新できます。

ステップ 8 [Managed AP Location] ウィンドウで、サイト名の隣にあるチェックボックスをオンにして、[Save] をクリックします。

親サイトまたは個々のサイトのいずれかを選択できます。

ステップ 9 インターフェイスと VLAN の詳細を設定します。

ステップ 10 **[Configure Interface and VLAN]** エリアで、IP アドレスとサブネットマスクの詳細を設定し、**[Next]** をクリックします。

ステップ 11 **[Advanced Configuration]** ウィンドウで、事前定義されたテンプレート変数の値を設定し、**[Next]** をクリックします。

ステップ 12 **[Summary]** ウィンドウでプライマリコントローラの管理対象 AP の場所およびその他の設定の詳細を確認し、**[Next]** をクリックします。

ステップ 13 展開のためのタスクのスケジュールを設定します。

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

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 14 [Tasks] ウィンドウで、タスクの展開を監視します。

ステップ 15 セカンダリコントローラをプロビジョニングするには、[Inventory] ウィンドウで目的のコントローラの横にあるチェックボックスをオンにし、セカンダリコントローラとしてプロビジョニングします。

ステップ 16 [Actions] ドロップダウンリストから、**[Provision]** > **[Provision Device]** を選択します。

[Assign Site] ウィンドウが表示されます。

ステップ 17 セカンダリコントローラの管理対象 AP の場所を割り当てるには、[Choose a site] をクリックします。

セカンダリコントローラの管理対象 AP の場所は、プライマリコントローラの管理対象 AP の場所と同じにする必要があります。

ステップ 18 [Choose a site] ウィンドウで、セカンダリコントローラを関連付けるサイト名の隣にあるチェックボックスをオンにして、[Save] をクリックします。

ステップ 19 **[Next]** をクリックします。

[設定（Configuration）] ウィンドウが表示され、セカンダリデバイスの管理対象のプライマリ AP とセカンダリ管理対象 AP の場所が表示されます。

ステップ 20 [Select Secondary Managed AP Locations] をクリックして、セカンダリコントローラの管理対象 AP の場所を追加または更新できます。

ステップ 21 [Managed AP Location] ウィンドウで、サイト名の隣にあるチェックボックスをオンにして、[Save] をクリックします。

親サイトまたは個々のサイトのいずれかを選択できます。

ステップ 22 セカンダリコントローラのインターフェイスと VLAN の詳細を設定します。

ステップ 23 [Configure Interface and VLAN] 領域で、セカンダリコントローラの IP アドレスとサブネットマスクの詳細を設定し、[Next] をクリックします。

ステップ 24 **[Advanced Configuration]** ウィンドウで、事前定義されたテンプレート変数の値を設定し、**[Next]** をクリックします。

ステップ 25 **[Summary]** ウィンドウでセカンダリコントローラの管理対象 AP の場所およびその他の設定の詳細を確認し、**[Next]** をクリックします。

ステップ 26 展開のためのタスクのスケジュールを設定します。

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

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 27 [Tasks] ウィンドウで、タスクの展開を監視します。

ステップ 28 プライマリコントローラおよびセカンダリコントローラの管理対象場所を確認するには、**[Provision]** > **[Inventory]** ウィンドウでプロビジョニングしたコントローラのデバイス名をクリックします。

ステップ 29 このダイアログボックスで、[View Device Details] をクリックします。

ステップ 30 デバイスの詳細ウィンドウで **[Wireless Info]** タブをクリックし、プライマリおよびセカンダリの管理対象場所の詳細を表示します。

ステップ 31 プライマリコントローラの AP をプロビジョニングします。詳細については、Day 1 の Cisco AP プロビジョニング （745 ページ）を参照してください。

モビリティ設定の概要

Catalyst Center のモビリティ設定では、一連の シスコ ワイヤレス コントローラ をモビリティグループにグループ化して、ワイヤレスクライアントのシームレスなローミング体験を実現できます。

モビリティグループを作成すると、ネットワーク内で複数のワイヤレスコントローラを有効にして、コントローラ間またはサブネット間のローミングが発生した際に、動的に情報を共有してデータトラフィックを転送できます。異なるモビリティグループ名を同じ無線ネットワーク内の異なるワイヤレスコントローラに割り当てると、モビリティグループによって、1つの企業内の異なるフロア、ビルディング、キャンパス間でのローミングを制限できます。

Catalyst Center では、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラや Cisco AireOS コントローラなどのさまざまなプラットフォーム間でモビリティグループを作成できます。

モビリティ設定には、次の注意事項および制限事項があります。

- [Provision] ウィンドウでは、モビリティを設定するために複数のコントローラを選択することはできません。

- グループ名をデフォルトにしてモビリティグループを作成することはできません。これにより、モビリティおよびRFグループ名がデフォルトとしてリセットされ、すべてのピアが削除されます。
- アンカーコントローラでモビリティグループ名を設定することはできません。
- Cisco AireOSコントローラでモビリティグループを設定しているときに仮想IPアドレスが変更された場合は、ワイヤレスコントローラを手動で再起動する必要があります。
- 同じモビリティグループ名を持つワイヤレスコントローラは、自動的に1つのモビリティグループにグループ化され、互いにピアとして追加されます。
- Cisco AireOS コントローラでモビリティグループを設定するときに、ワイヤレスコントローラ に IP アドレス 192.0.2.1 がない場合、Catalyst Center は仮想 IP アドレス 192.0.2.1 をすべての ワイヤレスコントローラ にプッシュします。
- ゲストアンカーコントローラをモビリティグループに明示的に追加しないでください。プロビジョニングされたゲストアンカーコントローラは、[Mobility Configuration] ウィンドウでピアを追加している間、ドロップダウンリストに表示されません。
- ワイヤレスコントローラをゲストアンカーとしてプロビジョニングする場合は、それがモビリティグループに追加されていないことを確認します。

モビリティ設定ワークフロー

次に、シスコ ワイヤレス コントローラ でモビリティを設定するために使用できるワークフローを示します。

- モビリティを設定するには、モビリティグループ名、RF グループ名、およびモビリティピアを使用して ワイヤレスコントローラ をプロビジョニングする必要があります。
- ワイヤレスコントローラのプロビジョニング中に適用される設定は、そのグループに設定されているすべてのモビリティピアに自動的に複製されます。
- ワイヤレスコントローラ を再同期して、最新のトンネルステータスを取得します。

モビリティ設定のユースケース

次のユースケースでは、コントローラ間のモビリティの設定手順について説明します。

ユースケース 1

この使用例では、ワイヤレスコントローラ 1、ワイヤレスコントローラ 2、およびワイヤレスコントローラ 3 がモビリティグループ名「Default」で Catalyst Center に新たに追加されると想定しています。これらのワイヤレスコントローラはまだプロビジョニングされていません。

1. モビリティグループ名、RF グループ名を設定し、ワイヤレスコントローラ 2 およびワイヤレスコントローラ 3 をピアとして追加して、ワイヤレスコントローラ 1 をプロビジョニングします。
2. ワイヤレスコントローラ 2 をプロビジョニングします。

[Provision] ウィンドウでは、ワイヤレスコントローラ 2 のモビリティ設定がグループ名とピアとともに自動的に入力されます。

3. ワイヤレスコントローラ 3 をプロビジョニングします。
4. すべてのワイヤレスコントローラをプロビジョニングした後、ワイヤレスコントローラを再同期して、最新のトンネルステータスを受信します。

使用例 2

この使用例では、ワイヤレスコントローラ 1、ワイヤレスコントローラ 2、およびワイヤレスコントローラ 3 が異なるモビリティグループ名で Catalyst Center にすでに追加されていると想定としています。これらのワイヤレスコントローラはプロビジョニングされています。

1. モビリティグループ名、RF グループ名を設定し、ワイヤレスコントローラ 2 およびワイヤレスコントローラ 3 をピアとして追加して、ワイヤレスコントローラ 1 をプロビジョニングします。
2. モビリティ設定は、ワイヤレスコントローラ 2、ワイヤレスコントローラ 3 などの他のピア間で自動的に複製されます。
   - ワイヤレスコントローラ 1 のプロビジョニングが成功すると、ワイヤレスコントローラ 2 とワイヤレスコントローラ 3 がピアとしてワイヤレスコントローラ 1 に追加されます。
   - ワイヤレスコントローラ 2 では、ワイヤレスコントローラ 1 とワイヤレスコントローラ 3 が、ピアとして追加されます。
   - ワイヤレスコントローラ 3 では、ワイヤレスコントローラ 1 とワイヤレスコントローラ 2 が、ピアとして追加されます。

モビリティグループの設定

手順

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

[インベントリ（Inventory）] ウィンドウが表示され、検出されたすべてのデバイスが一覧表示されます。

ステップ 2 モビリティを設定する Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の名前の横にあるチェックボックスをオンにします。

ステップ 3 [Actions] ドロップダウンリストから、**[Provision]** > **[Configure WLC Mobility]** を選択します。

[モビリティグループの設定（Configure Mobility Group）] スライドインペインが表示されます。

詳細については、「モビリティ設定の概要 （772 ページ）」を参照してください。

ステップ 4 [Mobility Group Name] ドロップダウンリストで、[+] をクリックして新しいモビリティグループを追加するか、既存のモビリティグループの中から選択できます。

既存のモビリティピア情報は、Catalyst Centerで使用可能なインテントからロードされます。



（注） ドロップダウンリストからデフォルトのモビリティグループを選択した場合、モビリティピアは追加できません。

ステップ 5 [RF Group Name] フィールドに RF グループの名前を入力します。

ステップ 6 Datagram Transport Layer Security（DTLS）を使いデータを暗号化するには、[Data Link Encryption] ボタンをクリックします。

ステップ 7 モビリティの暗号化設定を有効または無効にするには、[DTLS High Cipher Only] ボタンをクリックします。

暗号方式の設定は、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ リリース 17.5 以降に適用されます。変更を有効にするには、デバイスを手動で再起動する必要があります。

ステップ 8 DTLS暗号構成を変更した後にデバイスを手動で再起動して、プロビジョニング後に変更を有効にするには、[Restart for DTLS Ciphers to take effect] トグルボタンを使用します。

ステップ 9 [Mobility Peers] で [Add] をクリックして、モビリティピアを設定します。最大 24 個のピアデバイスをモビリティグループに追加できます。

ステップ 10 [モビリティピアの追加（Add Mobility Peer）] スライドインペインで、次の設定を行います。

a) 次のタイプのモビリティピアのいずれかを選択します。

- Catalyst Centerによって管理されるモビリティピアを含めるには、[Managed WLC] をクリックします。
- Catalyst Centerによって管理されていないモビリティピアを含めるには、[External WLC] をクリックします。

b) [Managed WLC] を選択した場合は、[Device Name] ドロップダウンリストからコントローラを選択します。

デバイスがプロビジョニングされると、Catalyst Center はデバイスにモビリティグループを作成し、RF グループを割り当て、ピアのすべての終端を設定します。モビリティグループの設定は、選択したすべてのピアデバイスに自動的に展開されます。

c) [外部WLC（External WLC）] を選択した場合は、次の設定を行います。

- [Device Name] フィールドに、デバイス名を入力します。
- （オプション）[Device Series] ドロップダウンリストから、デバイスシリーズを選択します。
- [プライベートIPv4/IPv6アドレス（Private IPv4/IPv6 Address）] フィールドに、プライベート IPv4 または IPv6 アドレスを入力します。

- （オプション）[パブリックIPv4/IPv6アドレス（Public IPv4/IPv6 Address）] フィールドに、パブリック IPv4 または IPv6 アドレスを入力します。
- [MAC Address] フィールドに、デバイスの MAC アドレスを入力します。
- [Mobility Group Name] フィールドに、モビリティグループ名を入力します。
- （オプション）[Hash] フィールドに、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのハッシュを入力します。

（注） このフィールドは、Cisco Catalyst 9800-CL ワイヤレスコントローラでのみ使用できます。

d) [Save] をクリックします。

ステップ 11 [Configure Mobility] をクリックします。

ステップ 12 （任意） モビリティグループ名と RF グループ名をリセットするには、次のいずれかの方法を実行します。

- [Configure Mobility Group] スライドインペインで、[Mobility Group Name] ドロップダウンリストから [default] を選択します。
- [Configure Mobility Group] スライドインペインで、[Reset Mobility] をクリックします。

この手順により、[RF Group Name] が自動的に [default] に設定され、すべてのピアが削除されます。プロビジョニングが完了すると、デバイスのモビリティが設定され、そのデバイスは他のすべてのピアから削除されます。

ステップ 13 展開のためのタスクのスケジュールを設定します。

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

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 14 [Tasks] ウィンドウで、タスクの展開を監視します。

AP 偽装の設定

Catalyst Center では、AP 偽装を有効または無効にできます。AP 偽装は、フィッシングインシデントを検出して報告するための迅速かつ効果的な手段を提供するグローバルな設定です。AP 偽装は、Catalyst 9800コントローラでサポートされます。

手順

ステップ 1 メインメニューから次を選択します。 **[Design]** > **[Network settings]** の順にクリックします。

ステップ 2 **[Wireless]** > **[Security Settings]**の順にクリックします。

ステップ 3 左側の階層ツリーでは、[Global] がデフォルトで選択されています。[Global] サイトを展開し、目的のサイト、建物、またはフロアを選択します。

（注） サイト、ビルディング、フロアは、グローバルレベルから設定が継承されます。

ステップ 4 [AP Impersonation] タブをクリックします。

ステップ 5 [AP偽装の有効化（Enable AP Impersonation）] チェックボックスをオンにして AP 偽装を有効にします。

ステップ 6 タイプとして [Auth IE] または [Infra MFP] を選択します。

（注） [Infra MFP] タイプがデフォルトで選択されています。

ステップ 7 [Save] をクリックします。

ステップ 8 （オプション）AP 偽装を無効にするには、[AP偽装の有効化（Enable AP Impersonation）] チェックボックスをオフにします。

DTLS 暗号スイートについて

暗号スイートは、無線 LAN 上の無線通信を保護するように設計された暗号と完全性アルゴリズムのセットです。

リリース 17.5 以降を実行している Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ、Catalyst 9000 シリーズスイッチ用 Cisco Catalyst 9800 組み込みワイヤレスコントローラ、および Catalyst アクセスポイント上の Cisco Embedded Wireless Controller プラットフォームでは複数の DTLS（Data Datagram Transport Layer Security）暗号スイートを設定できます。

複数の DTLS 暗号スイートの設定

DTLS 暗号スイートは、グローバルレベルまたはサイトレベルで設定できます。

始める前に

- **[System]** > **[Settings]** > **[Device Settings]** > **[Device Controllability]** ウィンドウでデバイス可制御性機能が有効になっていることを確認します。

- 検出されたデバイスが [Inventory] ウィンドウに一覧表示されるように、[Discovery] 機能を使用してネットワーク内の Cisco Catalyst 9800 シリーズ ワイヤレス コントローラを検出します。

手順

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

ステップ 2 同じ DTLS 暗号スイート構成ですべてのサイトを設定するには、左側の階層ツリーから、以下を選択します[Global] を選択します。

DTLS暗号スイートをサイトレベルで設定するには、左側の階層ツリーから、以下を選択しますサイトを選択します。DTLS暗号スイートの設定は、その特定のサイトで使用可能なコントローラにプッシュされます。

ステップ 3 [Security Settings] をクリックします。

ステップ 4 [Configure DTLS Ciphersuites] タブをクリックします。

ステップ 5 暗号スイートをデバイスの可制御性の一部として設定するには、[Skip DTLS Ciphersuite Config] チェックボックスをオフにします。

ステップ 6 デフォルト暗号スイートまたはカスタム暗号スイートを設定します。

デフォルトでは、**デフォルト**暗号スイートが選択されています。

[Default Ciphersuite] ボックスにはデフォルト暗号スイートのリストが示され、これらの暗号スイートが、デバイスでデフォルトとして設定されています。これらのデフォルト暗号スイートの優先順位は変更できません。

ステップ 7 カスタム暗号スイートを設定するには、[Custom] ボタンをクリックします。

カスタム暗号スイートは、優先順位に従ってデフォルト暗号スイートを上書きします。

ステップ 8 [Version] ドロップダウンリストから、DTLS のバージョンを選択します。

Catalyst Center は、DTLS のバージョンに基づいて、使用可能な暗号スイートを表示します。

ステップ 9 暗号スイートを適用しない場合は、その暗号スイートの横にある青色のトグルボタンをクリックします。

ステップ 10 暗号スイートの優先順位を変更するには、各暗号スイートをドラッグします。

ステップ 11 [**保存（Save）**] をクリックします。

「DTLS Ciphersuite Config Saved successfully」というメッセージが表示されます。

ステップ 12 暗号スイートの設定を適用するには、デバイスをプロビジョニングする必要があります。

詳細については、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のプロビジョニング （782 ページ）を参照してください。

N+1 ローリング AP アップグレードについて

ローリング AP アップグレード機能は、N+1 HA 設定の Cisco Catalyst 9800 シリーズ ワイヤレス コントローラでサポートされています。この機能は、ワイヤレス LAN ネットワーク内の Cisco Catalyst 9800 シリーズ ワイヤレス コントローラに関連付けられている AP のソフトウェアイメージをアップグレードするのに便利です。ゼロダウンタイムを実現するために、N+1 ローリング AP アップグレード機能を使用して、段階的に AP をアップグレードすることができます。

プライマリコントローラは、無線リソース管理ネイバー AP マップを使用して、候補の AP を識別します。アップグレードプロセスは、イメージが候補の AP に事前ダウンロードされている間に、ソフトウェアイメージをプライマリコントローラにダウンロードすることから始まります。候補の AP がアップグレードされて再起動されると、これらの AP は、セカンダリコントローラに段階的に参加します。すべての AP がセカンダリコントローラに参加した後、プライマリコントローラは再起動します。これらの AP は、再起動された後、段階的にプライマリコントローラに再度参加します。

次に、ローリング AP アップグレード機能を設定するための前提条件を示します。

- 2 つのワイヤレスコントローラの N+1 ハイアベイラビリティを設定し、1 つはプライマリコントローラ、もう 1 つはセカンダリコントローラとして使用します。
- プライマリコントローラと N+1 コントローラは、同じ構成を使用し、ネットワーク内の同じ場所を管理します。
- N+1 コントローラではすでにゴールデンイメージが実行されているため、ローリング AP アップグレードはダウンタイムなしで動作します。

  ゴールデンイメージは、ネットワークデバイスの標準化されたイメージであり、Catalyst Center は cisco.com からイメージを自動的にダウンロードします。イメージの標準化は、デバイスのセキュリティと、デバイスのパフォーマンスの最適化に役立ちます。
- N+1 コントローラは到達可能であり、Catalyst Center で [Managed] 状態になっています。
- 両方のコントローラが同じモビリティグループの一部であり、プライマリコントローラと N+1 コントローラの間にモビリティトンネルが確立されます。プライマリコントローラと N+1 コントローラ間のアップグレード情報は、モビリティトンネルを介して交換されます。



（注） ワイヤレスコントローラ 1 がワイヤレスコントローラ 2 に対して N+1、およびワイヤレスコントローラ 2 がワイヤレスコントローラ 1 に対して N+1 となっている循環型 N+1 展開がある場合、両方のデバイスでローリング AP アップグレードを実行することはできません。その代わりに、1 つのコントローラで通常のアップグレードを行う必要があります。最初のコントローラがローリング AP アップグレードなしでアップグレードされると、もう一方のコントローラでローリング AP アップグレードを実行できます。

ローリング AP アップグレードを設定するワークフロー

この手順では、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラでローリング AP アップグレードを設定する方法を示します。

（注） N+1 ローリング AP アップグレードは、ファブリックおよび非ファブリックの展開でサポートされています。

手順

ステップ 1 Catalyst Center をインストールします。

詳細については、*Cisco Catalyst Center* 設置ガイド [英語] を参照してください。

ステップ 2 Catalyst Center GUI にログインし、必要なアプリケーションが**実行**状態であることを確認します。

メインメニューから次を選択します。**[System]** > **[Software Updates]** > **[Installed Apps]** の順に選択します。

ステップ 3 ディスカバリ機能を使用して ワイヤレスコントローラを検出します。

Catalyst 9800 シリーズ ワイヤレス コントローラを検出するには、NETCONF を有効にしてポートを 830 に設定する必要があります。NETCONF は、ネットワークデバイスの構成をインストール、操作、削除するメカニズムです。

詳細については、CDP を使用したネットワークの検出 （86 ページ）またはIP アドレス範囲または CIDR を使用したネットワークの検出 （90 ページ）を参照してください。

ステップ 4 検出されたデバイスが [Device Inventory] ウィンドウに [Managed] 状態で表示されていることを確認します。

詳細については、インベントリについて （100 ページ）およびインベントリに関する情報の表示 （102 ページ）を参照してください。

デバイスが [Managed] になるまで待機する必要があります。

ステップ 5 サイト、ビルディング、フロアを追加してネットワーク階層を設計すると、後で設計の設定や構成を適用する場所を簡単に特定できるようになります。

新しいネットワーク階層を作成します。または Cisco Prime Infrastructure に既存のネットワーク階層がある場合は、それを Catalyst Center にインポートできます。

既存のネットワーク階層をインポートしてアップロードするには、Catalyst Center へのサイト階層のインポート （277 ページ）を参照してください。

新しいネットワーク階層を作成するには、サイトの作成、編集、削除 （285 ページ）およびビルディングの追加、編集、および削除 （286 ページ）を参照してください。

ステップ 6 AP の位置情報を追加し、フロアマップに配置して、ヒートマップカバレッジを可視化します。

詳細については、「フロアマップでの AP の取り扱い （304 ページ）」を参照してください。

ステップ 7 プライマリ管理対象 AP の場所、およびローリング AP アップグレードが有効になっていて、モビリティグループがセカンダリコントローラをピアとして設定されている状態で、プライマリコントローラをプロビジョニングします。

これを行うには、**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択し、プライマリコントローラ名の横にあるチェックボックスをオンにします。

ステップ 8 モビリティグループ設定で、モビリティピアとして N+1 コントローラを設定します。

詳細については、「モビリティ設定の概要 （772 ページ）」を参照してください。

ステップ 9 プライマリコントローラのプライマリ管理対象 AP の場所を N+1 コントローラのセカンダリ管理対象 AP の場所として設定することによって、N+1 HA コントローラをプロビジョニングします。これにより、セカンダリコントローラが N+1 コントローラとして設定されます。

詳細については、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のプロビジョニング （782 ページ）」を参照してください。

ステップ 10 プライマリコントローラに関連付けられている AP をプロビジョニングします。

ステップ 11 ソフトウェアイメージをリポジトリにインポートします。

詳細については、「ソフトウェアイメージのインポート （638 ページ）」を参照してください。

ステップ 12 ソフトウェアイメージをデバイスファミリに割り当てます。

詳細については、「デバイスファミリに対するソフトウェアイメージの割り当ての管理 （640 ページ）」を参照してください。

ステップ 13 デバイスファミリまたはデバイスロールの星印をクリックして、ソフトウェアイメージをゴールデンとしてマークします。

詳細については、ソフトウェアイメージをスタンダードとしてマークする （646 ページ）を参照してください。

ステップ 14 イメージをアップグレードする前に、両方のデバイスでイメージの準備状況チェックが成功していることを確認してください。

また、[N+1 Device Check] と [Mobility Tunnel Check] のステータスに緑色のチェックマークが付いていることも確認してください。

- イメージ更新の準備状況チェックを実行するには、**[Provision]** > **[Network Devices]** > **[Software Images]** の順に選択します。
- [Focus] ドロップダウンリストから [Software Images] を選択します。イメージをアップグレードするデバイスを選択します。
- デバイスの事前チェックが成功すると、[Image Precheck Status] 列の [Status] リンクに緑色のチェックマークが付きます。デバイスのアップグレード準備状況の事前チェックのいずれかが失敗した場合、[Image Precheck Status] リンクのマークが赤色に変わり、そのデバイスの OS イメージは更新できません。先に進む前に [Status] リンクをクリックし、エラーを修正します。

ステップ 15 プライマリコントローラでアップグレードを開始します。

ステップ 16 [Software Images] ウィンドウで、プライマリコントローラの横にあるチェックボックスをオンにします。

ステップ 17 [Actions] ドロップダウンリストから、**[Software Image]** > **[Update Image]** の順に選択します。

詳細については、ソフトウェアイメージのプロビジョニング （653 ページ）を参照してください。

ステップ 18 イメージのアップグレードの進行状況をモニターするには、[Software Image] 列で [In Progress] をクリックします。

[Device Status] ウィンドウに、次の情報が表示されます。

- [Distribution Operation]：イメージ配信プロセスに関する情報が表示されます。イメージは Catalyst Center からプライマリデバイスにコピーされます。配信プロセスが完了すると、アクティブ化操作が開始されます。
- [Activate Operation]：アクティブ化操作の詳細が表示されます。このプロセス中に、ローリング AP アップグレードが開始されます。
- [Rolling AP Upgrade Operation]：ローリング AP アップグレードタスクが完了したかどうか、保留中の AP の数、再起動中の AP の数、N+1 コントローラに参加している AP の数など、ローリング AP アップグレードの概要が表示されます。

  [View AP Status] をクリックすると、プライマリコントローラ、N+1 コントローラ、デバイス名、現在のステータス、および反復に関する詳細が表示されます。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のプロビジョニング

次の手順を使用して、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ をプロビジョニングします。

始める前に

Catalyst Center での Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の構成 （757 ページ）に示された手順を完了したことを確認します。

手順

ステップ 1 メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。

ステップ 2 [Devices] テーブルで、プロビジョニングする ワイヤレスコントローラ 名の横にあるチェックボックスをオンにします。

ステップ 3 [Actions] ドロップダウンリストから、**[Provision]** > **[Provision Device]** を選択します。

ステップ 4 ワイヤレスコントローラ がライセンス要件を満たしていない AP を管理している場合、Catalyst Center は詳細を示すダイアログボックスを表示します。ダイアログボックスで、必要なオプションをクリックします。

オプション	説明
ライセンス マネージャ	[License Manager] ウィンドウを開いて、対応するライセンスを有効にします。 ライセンスを有効にするには、『*Cisco Catalyst Center Administrator Guide*』の「Manage Licenses」を参照してください。
Continue with device provision	デバイスのプロビジョニングを続行します。 （注） ライセンス要件を満たしていない AP は、ワールドワイドセーフモード（WWSM）になります。
Cancel	ダイアログボックスを閉じて、別の ワイヤレスコントローラを選択します。

ステップ 5 [Assign Site] ウィンドウで、ワイヤレスコントローラ にサイトを割り当てます。

a) [Choose a Site] をクリックします。

b) [Choose a site] スライドインペインで、ワイヤレスコントローラ に割り当てるサイト名をクリックし、[Save] をクリックします。

c) [Next] をクリックします。

ステップ 6 [Configuration] ウィンドウで、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のロール [Active Main WLC] または [Anchor] を選択します。

ステップ 7 管理対象 AP の場所を選択します。

- プライマリコントローラの管理対象 AP の場所を選択するには、[Select Primary Managed AP Locations] をクリックします。
- セカンダリコントローラの管理対象 AP の場所を選択するには、[Select Secondary Managed AP Locations] をクリックします。

ステップ 8 管理対象 AP の場所の親サイトまたは個々のサイトのいずれかを選択し、[Save] をクリックします。

親サイトを選択すると、その親サイトの下にあるすべての子も選択されます。チェックボックスをオフにして、子サイトの選択を解除できます。

（注） 管理対象 AP の場所を継承することで、サイトおよび特定のサイトのビルディングとフロアを自動的に選択できます。1 つのサイトは 1 つの ワイヤレスコントローラ によってのみ管理されます。

ステップ 9 （任意） [AP Authorization List] チェックボックスをオンにして、AP の認証リストを選択し、AP 認証設定を構成します。



（注） このチェックボックスは、AP認証リストが使用可能な場合にのみ表示されます。AP認証リストの詳細については、「AP 認証リストの作成 （492 ページ）」を参照してください。

- [AP Authorization List Name] ドロップダウンリストから、AP 認証リストを選択します。AP 認証リストの内容に基づいて、Catalyst Centerは、それに対応するプライマリの認証タイプとフェールバックメカニズムを示したメッセージを表示します。
- （オプション）選択した AP 認証リストのエントリを表示するには、[View Entries] をクリックします。
- ワイヤレスコントローラ でメッシュ AP と非メッシュ AP の両方が管理されている場合、Catalyst Center には [Authorize Only Mesh Access Points] および [Authorize All Access Points] チェックボックスが表示されます。

  メッシュ AP の認証のみを有効にするには、[Authorize Only Mesh Access Points] チェックボックスをオンにします。

  すべての AP の認証を有効にするには、[Authorize All Access Points] チェックボックスをオンにします。

ステップ 10 アクティブなメインワイヤレスコントローラでは、インターフェイスと VLAN の詳細を設定します。

ステップ 11 （任意） [VLANの設定（Configure VLAN）] エリアで、VLAN の設定を行います。

動的インターフェイスには、最大 8 つの IPv6 アドレスと 1 つの IPv4 アドレスを設定できます。動的インターフェイスを設定するには、「ネットワークプロファイルの追加インターフェイスの構成 （566 ページ）」を参照してください。



（注） FlexConnect SSID の場合、プロビジョニング中に Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ で VLAN が自動的に作成されません。ワイヤレス ネットワーク プロファイルにマッピングされたインターフェイスと VLAN は、AP のプロビジョニング時に Flex プロファイルに作成されます。

必要な VLAN を選択し、[編集（Edit）] をクリックします。[VLANの設定（Configure VLAN）] スライドインペインで、次の設定を完了します。

a) （任意） [IPv4] タブで、次のフィールドにデータを入力します。

- [インターフェイスIPアドレス（Interface IP Address）]：このインターフェイスの IPv4 アドレスを入力します。
- [ゲートウェイIPアドレス（Gateway IP Address）]：インターフェイスのゲートウェイ IPv4 アドレスを入力します。

- [Subnet Mask (in bits)]：インターフェイスのサブネットマスクの詳細を入力します。

b) （任意） [IPv6] タブで、[IPv6アドレスの追加（Add IPv6 Address）] をクリックし、次の設定を完了します。

- インターフェイスの IPv6 アドレスを入力します。
- [プレフィックス長（Prefix Length）] ドロップダウンリストから、プレフィックス長を選択します。

ステップ 12 （任意） [Skip AP Provision] チェックボックスをオンにして、ワイヤレスコントローラ のプロビジョニング中に AP 関連コマンドの設定をスキップします。

詳細については、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのプロビジョニング中に AP プロビジョニングをスキップする （1707 ページ） を参照してください。

（注） ワイヤレスコントローラを再プロビジョニングする際に、AP インテント設定に変更がない場合、Catalyst Center は AP 関連コマンドの設定をスキップします。インテント設定に変更がある場合、このチェックボックスを使用して、AP 関連の設定をスキップできます。

検出された AP 設定変更の詳細については、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのプロビジョニング中に AP プロビジョニングをスキップする （1707 ページ）」を参照してください。

ステップ 13 （任意） N+1 HA セットアップでローリング AP アップグレード機能を有効にするには、[Rolling AP Upgrade] チェックボックスをオンにします。

（オプション）このチェックボックスをオンにする場合は、最小限のクライアント中断で再起動が可能となるように、[AP Reboot %] ドロップダウンリストから AP のパーセンテージを選択します。

詳細については、ローリング AP アップグレードを設定するワークフロー （780 ページ） を参照してください。

（注） 設定すると、同じ AP 再起動パーセンテージ値が、ローリング AP アップグレードプロセスと段階的 AP LSC 更新プロセスの両方に適用されます。たとえば、AP の再起動パーセンテージを 25% に設定すると、ローリング AP アップグレードおよび段階的 AP LSC 更新の両方で、一度に 25% の AP のみが再起動されます。

ステップ 14 （任意） 有効期限が切れる前に、関連する AP のローカルで有効な証明書（LSC）を更新するには、[AP LSC Certificate Renewal] チェックボックスをオンにします。

デフォルトでは、ワイヤレスコントローラ は毎日午前 12:00 に段階的な方法で AP LSC を更新します。

このチェックボックスをオンにする場合は、次の設定を行います。

- [Renewal Profile] ドロップダウンリストから、AP LSC 更新プロファイルを選択します。

AP LSC 更新プロファイルを作成する場合は、「AP LSC 更新プロファイルの作成 （495 ページ）」を参照してください。

- （オプション）段階的な更新に AP LSC 更新プロファイルを選択する場合は、最小限のクライアント中断で再起動が可能となるように、[AP Reboot %] ドロップダウンリストから AP のパーセンテージを選択します。デフォルトは 25% です。

（注） 設定すると、同じ AP 再起動パーセンテージ値が、ローリング AP アップグレードプロセスと段階的 AP LSC 更新プロセスの両方に適用されます。たとえば、AP の再起動パーセンテージを 25% に設定すると、ローリング AP アップグレードおよび段階的 AP LSC 更新の両方で、一度に 25% の AP のみが再起動されます。

ステップ 15 [Next] をクリックします。

ステップ 16 [Feature Templates] ウィンドウの [Devices] ペインで、機能テンプレートを選択します。

[Find] フィールドに機能テンプレートの名前を入力して検索するか、デバイスを展開して機能テンプレートを選択します。選択した機能テンプレートが右側のペインに表示されます。

ステップ 17 プロビジョニングする機能テンプレートの [Design Name] の横にあるチェックボックスをオンにし、[Configure] をクリックして編集します。

この手順では、すべての設定を編集することはできません。

ステップ 18 必要な変更を加えて、[Apply] をクリックします。

ステップ 19 [Next] をクリックします。

ステップ 20 [Advanced Configuration] ウィンドウの [Devices] ペインで、デバイスまたはテンプレートを検索します。

ステップ 21 [wlanid] フィールドに、事前定義されたテンプレート変数の値を入力し、[Next] をクリックします。

ステップ 22 [Summary] ウィンドウで設定を確認し、[Next] をクリックします。

ステップ 23 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 24 [Tasks] ウィンドウで、タスクの展開を監視します。

（注） ワイヤレスコントローラ をプロビジョニングすると、Catalyst Center は設定を ワイヤレスコントローラ にプッシュし、ネットワークインテントに基づいて設定します。

再プロビジョニング中に、ネットワークインテントの一部であるか、Catalyst Center によってプッシュされている設定と競合するアウトオブバンド設定が ワイヤレスコントローラ にある場合、Catalyst Center は ワイヤレスコントローラ のアウトオブバンド設定をネットワークインテント設定に上書きします。

選択的 AP グループリソース向けサービス（RFS）変換機能により、AP 関連の設定（AP タグマッピング、RF タグ、Flex または RF プロファイルなど）の再プロビジョニングが最適化されます。AP 関連設定へのアウトオブバンド変更は、規則遵守レポートで明示的にフラグが付けられていない限り、再プロビジョニング中に自動的に修正されません。ネットワークインテントに一致するように AP 関連のアウトオブバンド設定を修正するには、ワイヤレスコントローラ 再同期およびコンプライアンス実行を行います。たとえば、静的 AP タグマッピングを手動で更新する場合は、次のとおりです。

- 再同期とコンプライアンス実行を行った場合、手動での変更がインテント設定と一致するように修正されます。
- 再同期とコンプライアンス実行を行わなかった場合、手動での変更は修正されず、新しいインテントの変更のみが適用されます。

選択的 AP グループ RFS 変換機能を無効にする場合は、Cisco Technical Assistance Center （TAC）にお問い合わせください。

Catalyst Center のネットワークインテントを介してサポートされるすべての設定について、アウトオブバンド設定の代わりに使用することをお勧めします。

ステップ 25 Catalyst Center からデバイスにプッシュされる設定を確認するには、ワイヤレスコントローラ で show コマンドを使用します。

- **#show wlan summary**
- **#show run | sec line**
- **#show running-configuration**

ステップ 26 デバイスが正常に展開されると、[Provision Status] が [Configuring] から [Success] に変わります。

ステップ 27 [Inventory] ウィンドウで、[Focus] ドロップダウンリストから [Provision] を選択します。

ステップ 28 [Provision Status] カラムで、対応するデバイスの [See Details] リンクをクリックし、ネットワークインテントの詳細情報またはアクションのリストを表示します。

ステップ 29 デバイス スライドインペイン で、[Device Provisioning] の [See Details] をクリックします。

ステップ 30 [Deployment of network intent] の下の [View Details] をクリックし、デバイス名をクリックします。

ステップ 31 デバイス名をクリックして展開します。

ステップ 32 [Configuration Summary] エリアを展開して、操作の詳細、機能名、および管理機能を表示します。

[Configuration Summary] には、デバイスのプロビジョニング中に発生したエラーも（エラー理由とともに）表示されます。

ステップ 33 デバイスに送信される正確な設定の詳細を表示するには、[Provision Summary] エリアを展開します。

ステップ 34 AP をプロビジョニングします。

Catalyst アクセスポイント上の Cisco Embedded Wireless Controller の Day-0 ワークフロー

Catalyst アクセスポイント上の Cisco Embedded Wireless Controller（EWC-AP）は、次世代の Wi-Fi ソリューションであり、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ に Cisco Catalyst 9100 シリーズアクセスポイントを統合し、進化および成長し続ける組織にそのクラスで最高のワイヤレスエクスペリエンスをもたらします。

始める前に

- サイト、ビルディング、フロアなどのネットワーク階層を設計します。

  詳細については、サイトの作成、編集、削除（285 ページ）およびビルディングの追加、編集、および削除（286 ページ）を参照してください。

- デバイスを要求するサイトのデバイスログイン情報（CLI、SNMP、HTTP、HTTPS など）を定義します。

  詳細については、グローバル CLI クレデンシャルの追加（379 ページ）、グローバル SNMPv2c ログイン情報の追加（380 ページ）、およびグローバル SNMPv3 ログイン情報の追加（382 ページ）を参照してください。

- SSID、ワイヤレスインターフェイス、および無線周波数プロファイルを作成します。

  詳細については、エンタープライズ ワイヤレス ネットワーク用 SSID の作成（415 ページ）、ゲスト ワイヤレス ネットワークの SSID の作成（432 ページ）、ワイヤレスインターフェイスの作成（449 ページ）、およびワイヤレス無線周波数プロファイルの作成（451 ページ）を参照してください。

（注） Catalyst アクセスポイント上の Cisco Embedded Wireless Controller では、Flex ベースの SSID の作成のみがサポートされています。

- Catalyst アクセスポイント上の Cisco Embedded Wireless Controller が接続されているスイッチでオプション #43 を使用して DHCP サーバーを設定します。この IP アドレスは Catalyst Center プラグアンドプレイ（PnP）サーバーの IP アドレスです。この IP アドレスを使用すると、AP は PnP サーバーに接続しますが、[Unclaimed] 状態のままになります。

- インベントリに Catalyst アクセスポイント上の Cisco Embedded Wireless Controller があることを確認します。ない場合は、[Discovery] 機能を使用して検出します。詳細については、

CDP を使用したネットワークの検出 （86 ページ）、IP アドレス範囲または CIDR を使用したネットワークの検出 （90 ページ）、およびインベントリについて （100 ページ）を参照してください。

- AP は、シスコ ワイヤレス コントローラ 設定なしで初期設定へリセットされた状態である必要があります。

Catalyst アクセスポイント上の Cisco Embedded Wireless Controller は、次のような複数のフォームファクタで使用できます。

- Catalyst 9115AX アクセスポイント上の Cisco 組み込みワイヤレスコントローラ
- Catalyst 9117AX アクセスポイントの Cisco 組み込みワイヤレスコントローラ
- Catalyst 9120AX アクセスポイントの Cisco 組み込みワイヤレスコントローラ
- Catalyst 9130AX アクセスポイントの Cisco 組み込みワイヤレスコントローラ

手順

ステップ 1 Catalyst アクセスポイント上の Cisco Embedded Wireless Controller が DHCP サーバーと通信します。

DHCP サーバーからの応答で、IP アドレスとともに、Cisco プラグアンドプレイサーバーの IP アドレスを含むオプション #43 が返されます。

ステップ 2 オプション #43 に基づいて、 Catalyst アクセスポイント上の Cisco Embedded Wireless Controller はプラグアンドプレイ エージェントをオンにし、Catalyst Center プラグアンドプレイサーバーに接続します。

（注） ネットワーク内に Catalyst アクセスポイント上の Cisco Embedded Wireless Controller のセットがある場合、それらは内部プロトコルを通過します。プロトコルは、PnP サーバーに到達するために シスコ ワイヤレス コントローラ 上でプライマリ AP として設定されている 1 つの Catalyst アクセスポイント上の Cisco Embedded Wireless Controller を選択します。

ステップ 3 **[Provision]** > **[Plug and Play]** タブで、要求されていない Catalyst アクセスポイント上の Cisco Embedded Wireless Controller を見つけます。

テーブルには、すべての未要求デバイスが一覧表示されます。[State] 列が [Unclaimed] として表示されます。[Filter] または [Find option] を使用して、特定のデバイスを検索することができます。

[Onboarding State] 列の下でオンボーディングステータスが [Initialized] になるまで待つ必要があります。

ステップ 4 Catalyst アクセスポイント上の Cisco Embedded Wireless Controller を要求するには、AP デバイス名の横にあるチェックボックスをオンにします。

ステップ 5 デバイス表の上にあるメニューバーで、**[Actions]** > **[Claim]** の順に選択します。

[デバイスの要求（Claim Devices）] ウィンドウが表示されます。

ステップ 6 [Assign Site] ウィンドウの [Site] ドロップダウンリストからサイトを選択します。

選択された AP のこの特定のサイトに対する要求は、関連付けられている構成にも適用されます。

ステップ 7 **[次へ (Next)]** をクリックします。

ステップ 8 デバイスを設定するために、[Assign Configuration] ウィンドウで対応する [Assign] オプションをクリックします。

ステップ 9 [デバイス名の設定（Configuration for device name）] スライドインペインで、次のタスクを実行します。

- [Wireless Management IP] フィールドに、ワイヤレス管理 IP アドレスを入力します。

  PnP サーバーに接続するために AP で使用される IP アドレスと同じ IP アドレスは使用できません。

- [Subnet Mask] フィールドにサブネット マスクを入力します。
- [Gateway] フィールドに、ゲートウェイ IP アドレスを入力します。

ステップ 10 [Save] をクリックします。

ステップ 11 [Next] をクリックします。

[概要（Summary）] ウィンドウが表示されます。

ステップ 12 [Claim] をクリックします。

Catalyst アクセスポイント上の Cisco Embedded Wireless Controller 要求が成功すると、設定されたワイヤレス管理アドレス、サブネットマスク、およびゲートウェイが Cisco Embedded Wireless Controller に割り当てられます。

要求されたデバイスが **[Provision]** > **[Inventory]** ウィンドウに表示され、[Managed] 状態に移行します。デバイスは自動的にプロビジョニングされます。プロビジョニングが完了すると、**[Provision]** > **[Plug and Play]** ウィンドウの [Provisioned] タブでデバイスを確認できます。

Catalyst 9000 シリーズ スイッチ用 Cisco Catalyst 9800 組み込みワイヤレスコントローラの設定とプロビジョニング

サポートされているハードウェア プラットフォーム

デバイス ロール	プラットフォーム
組み込みワイヤレスコントローラ	Cisco Catalyst 9300 シリーズ スイッチ Cisco Catalyst 9400 シリーズ スイッチ Cisco Catalyst 9500-H シリーズ スイッチ
ファブリックエッジ	Cisco Catalyst 9300 シリーズ スイッチ

デバイス ロール	プラットフォーム
	Cisco C9350 シリーズ スマートスイッチ Cisco Catalyst 9400 シリーズ スイッチ Cisco Catalyst 9500-H シリーズ スイッチ Cisco Catalyst 3600 シリーズ スイッチ Cisco Catalyst 3850 シリーズ スイッチ
AP	Cisco 802.11ac Wave 2 AP： • Cisco Aironet 1810 シリーズ OfficeExtend アクセス ポイント • Cisco Aironet 1810W シリーズ アクセス ポイント • Cisco Aironet 1815i アクセスポイント • Cisco Aironet 1815w アクセスポイント • Cisco Aironet 1815m アクセスポイント • Cisco 1830 Aironet シリーズ アクセスポイント • Cisco Aironet 1850 シリーズ アクセス ポイント • Cisco Aironet 2800 シリーズ アクセス ポイント • Cisco Aironet 3800 シリーズ アクセスポイント • Cisco Aironet 4800 シリーズ アクセスポイント Cisco 802.11ac Wave 1 AP • Cisco Aironet 1700 シリーズ アクセス ポイント • Cisco Aironet 2700 シリーズ アクセスポイント • Cisco Aironet 3700 シリーズ アクセスポイント Cisco Catalyst 9105 シリーズ Wi-Fi 6 アクセスポイント Cisco Catalyst 9115 シリーズ Wi-Fi 6 アクセスポイント Cisco Catalyst 9117 シリーズ Wi-Fi 6 アクセスポイント Cisco Catalyst 9120 シリーズ Wi-Fi 6 アクセスポイント Cisco Catalyst 9124 シリーズ Wi-Fi 6 アクセスポイント Cisco Catalyst 9130 シリーズ Wi-Fi 6 アクセスポイント Cisco Catalyst 9136 シリーズ Wi-Fi 6 アクセスポイント Cisco Catalyst Wireless 9136I Wi-Fi 6 アクセスポイント

デバイス ロール	プラットフォーム
	Cisco Catalyst Wireless 9163E Wi-Fi 6 アクセスポイント Cisco Catalyst Wireless 9166D Wi-Fi 6 アクセスポイント Cisco Catalyst Wireless 9166I Wi-Fi 6 アクセスポイント Cisco Catalyst Wireless 9162I Wi-Fi 6 アクセスポイント Cisco Catalyst Wireless 9164I Wi-Fi 6 アクセスポイント Cisco Catalyst Wireless 9167 シリーズ Wi-Fi 6 アクセスポイント Cisco Wireless 9171I シリーズ Wi-Fi 7 アクセスポイント Cisco Wireless 9172H シリーズ Wi-Fi 7 アクセスポイント Cisco Wireless 9172I シリーズ Wi-Fi 7 アクセスポイント Cisco Catalyst Wireless 9176 シリーズ Wi-Fi 6 アクセスポイント Cisco Catalyst 9176D1 シリーズ Wi-Fi 7 アクセスポイント Cisco Catalyst 9176I シリーズ Wi-Fi 7 アクセスポイント Cisco Catalyst Wireless 9178 シリーズ Wi-Fi 6 アクセスポイント Cisco Catalyst 9178I シリーズ Wi-Fi 7 アクセスポイント

事前設定

Catalyst 9300 シリーズ スイッチ用 Cisco Catalyst 9800 組み込みワイヤレス コントローラ で、スイッチが **aaa new-model** ですでに設定されている場合は、次のコマンドが存在することを確認してください。

```
aaa new-model
aaa authentication login default local
aaa authorization exec default local
aaa session-id common
```

これは、NETCONF の設定では必須です。プロビジョニングに自動アンダーレイを使用している場合、これらの設定は必要ありません。

Catalyst 9000 スイッチ用 Cisco Catalyst 9800 組み込みワイヤレスコントローラの設定

1. Catalyst Center をインストールします。

詳細については、『Cisco Catalyst Center Installation Guide』[英語] を参照してください。

2. Catalyst Center GUI にログインし、必要なアプリケーションが**実行**状態であることを確認します。

   メインメニューから次を選択します。**[System]** > **[Software Updates]** > **[Installed Apps]** の順に選択します。

3. Cisco Identity Services Engine と Catalyst Center を連動させます。Cisco ISE が Catalyst Center に登録されると、Catalyst Center が検出するすべてのデバイスが、関連する設定データやその他のデータとともに Cisco ISE にプッシュされます。

4. Cisco Catalyst 9000 シリーズスイッチおよびエッジスイッチを検出します。

   Catalyst 9000 シリーズ スイッチの Cisco Catalyst 9800 組み込みワイヤレスコントローラを検出するには、NETCONF を有効にし、ポートを 830 に設定する必要があります。

   エッジスイッチを検出するために NETCONF を有効にする必要はありません。

   詳細については、CDP を使用したネットワークの検出 （86 ページ）およびIP アドレス範囲または CIDR を使用したネットワークの検出 （90 ページ）を参照してください。

   [Preferred Management IP] を [Use Loopback] に変更します。

5. デバイスが [Device Inventory] に [Managed] 状態で表示されていることを確認します。

   詳細については、インベントリについて （100 ページ）およびインベントリに関する情報の表示 （102 ページ）を参照してください。

   デバイスが**管理対象**状態になっていることを確認します。

6. ネットワークの地理的な場所を表すネットワーク階層を設計します。サイト、ビルディング、フロアを作成すると、後で設計の設定や構成を適用する場所を簡単に特定できるようになります。

   新しいネットワーク階層を作成します。または Cisco Prime Infrastructure に既存のネットワーク階層がある場合は、それを Catalyst Center にインポートできます。

   既存のネットワーク階層をインポートしてアップロードするには、Catalyst Center へのサイト階層のインポート （277 ページ）を参照してください。

   新しいネットワーク階層を作成するには、サイトの作成、編集、削除 （285 ページ）およびビルディングの追加、編集、および削除 （286 ページ）を参照してください。

7. 非ファブリックネットワークで設計フェーズ中にヒートマップの可視化を取得するには、フロアマップに AP を追加して配置します。

   ファブリックネットワークの場合、設計時にフロアマップに AP を配置することはできません。AP は、ファブリックネットワークにデバイスを追加した後にオンボードされます。

   詳細については、「フロアマップでの AP の取り扱い （304 ページ）」を参照してください。

8. AAA（Cisco ISE がネットワークおよびクライアントエンドポイント用に設定されている）、NetFlow コレクタ、NTP、DHCP、DNS、syslog、および SNMP トラップなどのネットワーク設定を定義します。これらのネットワークサーバーが、ネットワーク全体のデフォルトになります。

   SSID の作成時に、[Wireless] ウィンドウで最大 6 つの AAA サーバーを設定できます。

   詳細については、ネットワーク設定の概要 （373 ページ）、グローバル ネットワーク サーバーの設定 （377 ページ）、および「AAA サーバーの追加」を参照してください。

9. CLI、SNMP、HTTP などのデバイスのログイン情報を設定します。

   詳細については、グローバルデバイス クレデンシャルの設定 （379 ページ）、グローバル CLI クレデンシャルの追加 （379 ページ）、グローバル SNMPv2c ログイン情報の追加 （380 ページ）、グローバル SNMPv3 ログイン情報の追加 （382 ページ）、グローバル HTTPS ログイン情報の追加 （385 ページ）を参照してください。

10. IP アドレスプールをグローバルレベルで設定します。

    IP アドレスプールを設定するには、IP アドレスプールを設定する （397 ページ）を参照してください。

    プロビジョニングするビルディングの IP アドレスプールを予約するには、「IP アドレスプールの予約」を参照してください。

11. エンタープライズおよびゲスト ワイヤレス ネットワークを作成します。グローバルワイヤレス設定を 1 回定義すると、Catalyst Center はあらゆる場所にあるさまざまなデバイスに構成をプッシュします。

    ワイヤレスネットワークの設計は、2 段階のプロセスです。初めに、[Wireless] ウィンドウで SSID を作成する必要があります。次に、作成した SSID をワイヤレス ネットワーク プロファイルに関連付けます。このプロファイルは、サイトにデバイスを展開するために使用されるトポロジを構築するのに役に立ちます。

    詳細については、エンタープライズ ワイヤレス ネットワーク用 SSID の作成 （415 ページ）およびゲスト ワイヤレス ネットワークの SSID の作成 （432 ページ）を参照してください。

12. バックホールの設定を行います。

13. [Policy] ウィンドウで、次の設定を行います。

    - 仮想ネットワークを作成します。仮想ネットワークを使用して、物理ネットワークを複数の論理ネットワークにセグメント化できます。
    - グループベースのアクセス コントロール ポリシーを作成し、契約を追加します。詳細については、「グループベースのアクセス コントロール ポリシーの作成 （1423 ページ）」を参照してください。

14. 設計フェーズ中に追加された設定を使用して、Cisco Catalyst 9000 シリーズスイッチとエッジノードスイッチをプロビジョニングします。

    - ファブリックサイトを作成します。

- CP+ボーダー+エッジまたはCP+ボーダーを作成して、デバイスをファブリックネットワークに追加します。
- Catalyst 9000 シリーズ スイッチの Cisco Catalyst 9800 組み込みワイヤレスコントローラで、組み込みワイヤレス機能を有効にします。
- ファブリックドメインで AP をオンボードします。

詳細については、SD-Access LISP ファブリックネットワークのプロビジョニング （1213 ページ）を参照してください。

デバイスが正常に展開されると、展開ステータスが [Configuring] から [Success] に変わります。

Cisco Catalyst 9000 シリーズ スイッチでの組み込みワイヤレスのプロビジョニング

始める前に

Catalyst 9000 シリーズ スイッチの Cisco Catalyst 9800 組み込みワイヤレスコントローラをプロビジョニングする前に、Catalyst 9000 スイッチ用 Cisco Catalyst 9800 組み込みワイヤレスコントローラの設定 （792 ページ）の手順を完了していることを確認します。

この手順では、Cisco Catalyst 9300 シリーズ スイッチ、Cisco Catalyst 9400 シリーズ スイッチ、および Cisco Catalyst 9500H シリーズ スイッチに組み込みワイヤレスをプロビジョニングする方法について説明します。

手順

ステップ 1 メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。

[Inventory] ウィンドウが表示され、検出されたデバイスが一覧表示されます。

ステップ 2 Catalyst 9000 シリーズ スイッチデバイスと、サイトに関連付けるエッジスイッチの横にあるチェックボックスをオンにします。

ステップ 3 [Actions] ドロップダウンリストから、**[Provision]** > **[Assign Device to Site]** の順に選択します。デバイスをサイトに割り当てます。詳細については、プロビジョニングされていないデバイスのサイトへの割り当て （189 ページ）を参照してください。
次の手順では、設計フェーズ中に追加された設定を使用して、Catalyst 9000 シリーズ スイッチとエッジノードをプロビジョニングします。

ステップ 4 **[Provision]** > **[Inventory]** ウィンドウで、プロビジョニングするデバイス名の横にあるチェックボックスをオンにします。

a) [Actions] ドロップダウンリストから、**[Provision]** > **[Provision Device]** を選択します。
b) **[Next]** をクリックします。

c) **[Summary]** ウィンドウで設定を確認し、**[Next]** をクリックします。
d) 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

e) [Tasks] ウィンドウで、タスクの展開を監視します。

ステップ 5 エッジスイッチをプロビジョニングするには、プロビジョニングするエッジスイッチの横にあるチェックボックスをオンにします。

a) [Actions] ドロップダウンリストから、[Provision] を選択します。
b) **[Next]** をクリックします。
c) [Summary] ウィンドウで設定を確認し、[Deploy] をクリックします。

デバイスが正常に展開されると、[Provision Status] が [Configuring] から [Success] に変わります。

ステップ 6 ファブリックサイトにデバイスを追加するには、メニューアイコンをクリックして次を選択します。**[Provision]** > **[Fabric Sites]**の順に選択します。

ステップ 7 ファブリックサイトを作成します。詳細については、「ファブリックサイトの追加 （1229ページ）」を参照してください。

ステップ 8 IP トランジットネットワークを追加します。

ステップ 9 デバイスを追加して、ファブリックサイトに仮想ネットワークを関連付けます。

ステップ 10 Cisco Catalyst 9000 シリーズ スイッチをコントロールプレーン、ボーダーノード、およびエッジノードか、またはコントロールプレーンとボーダーノードとして追加します。

a) デバイスをクリックし、[Add as CP+Border+Edge] または [Add as CP+Border] を選択します。
b) エッジノードをクリックして、[Add to Fabric] を選択します。
c) **[Save]** をクリックします。

ステップ 11 デバイス上で組み込みのワイヤレスを有効にするには、**[Edge]**、**[CP+Border+Edge]** または **[CP+Border]** として追加されたデバイスをクリックし、**[Embedded Wireless LAN Controller]** トグルボタンをクリックします。

a) ワイヤレス機能を有効にする前に Cisco Catalyst 9000 シリーズ スイッチにワイヤレスパッケージをインストールしなかった場合、この機能を有効にするには組み込みの ワイヤレスコントローラ ソフトウェアイメージが必要であることを示す警告メッセージが Catalyst Center に表示されます。[Warning] ダイアログボックスで [OK] をクリックして、イメージを手動でインストールします。
b) [Download Image] ウィンドウで、[Choose File] をクリックしてローカルに保存されているソフトウェアイメージに移動するか、または [Enter image URL] でソフトウェアイメージのインポート元となる HTTP または FTP を指定します。
c) [Import] をクリックします。

イメージのインポートの進捗状況が表示されます。ウィンドウを閉じてインポートの進行状況を表示し、後でインストールをスケジュールする場合は、[Close] をクリックします。

d) イメージのインポートが完了したら、[Download Image] ウィンドウの [Schedule Image Installation] で、次のいずれかのオプションを選択します。

- [Now]：イメージをすぐにインストールします。
- [Later]：将来の日付と時刻でイメージのインストールをスケジュールします。

e) [Task Name] フィールドで、必要に応じてタスク名を更新します。

f) [Later] を選択した場合は、次の手順を実行します。

- [Start Date/Time] で、イメージのインストールの開始日時を指定します。
- イメージのインストールにデフォルトのサイトのタイムゾーンを使用するには、[Site Settings] チェックボックスをオンにします。タイムゾーンを選択するには、[Site Settings] チェックボックスをオフにして、ドロップダウンリストからタイムゾーンを選択します。

g) [適用（Apply）] をクリックします。

イメージのインストールのステータスを表示するには、**[Activities]** > **[Tasks]** ウィンドウに移動し、関連する作業項目を開きます。

h) 組み込みの ワイヤレスコントローラ ソフトウェアイメージが配信され、スイッチでアクティブ化されたら、**[Provision]** > **[Inventory]** > **[Resync]** オプションを使用してデバイスを再同期します。

ステップ 12 [Manage Scope] ウィンドウで、次の手順を実行します。

- [Primary] タブで、必要なサイト名の横にあるチェックボックスをオンにします。
- [Secondary] タブで、必要なサイト名の横にあるチェックボックスをオンにします。

親サイトまたは個々のサイトを選択できます。親サイトを選択すると、その下にあるすべての子も選択されます。このチェックボックスをオフにすると、個々のサイトの選択を解除できます。

また、[Search Hierarchy] 検索フィールドまたはフィルタアイコンを使用してサイトを検索できます。

ステップ 13 [Next] をクリックします。

ステップ 14 [Advanced] ウィンドウで、必要な設定を行います。

- ローリング AP アップグレード機能を有効にするには、[Rolling AP Upgrade] チェックボックスをオンにします。

  （オプション）このチェックボックスをオンにする場合は、最小限のクライアント中断で再起動が可能となるように、[AP Reboot Percentage] ドロップダウンリストから AP のパーセンテージを選択します。デフォルトは 25% です。

- 有効期限が切れる前に、関連する AP のローカルで有効な証明書（LSC）を更新するには、[AP LSC Certificate Renewal] チェックボックスをオンにします。

  このチェックボックスをオンにする場合は、次の設定を行います。

  - [Renewal Profile] ドロップダウンリストから、AP LSC 更新プロファイルを選択します。

    AP LSC 更新プロファイルを作成する場合は、AP LSC 更新プロファイルの作成 （495 ページ）を参照してください。

- （オプション）段階的な更新に AP LSC 更新プロファイルを選択する場合は、最小限のクライアント中断で再起動が可能となるように、[AP Reboot %] ドロップダウンリストから AP のパーセンテージを選択します。デフォルトは 25% です。



（注） 設定すると、同じ AP 再起動パーセンテージ値が、ローリング AP アップグレードプロセスと段階的 AP LSC 更新プロセスの両方に適用されます。たとえば、AP の再起動パーセンテージを 25% に設定すると、ローリング AP アップグレードおよび段階的 AP LSC 更新の両方で、一度に 25% の AP のみが再起動されます。

ステップ 15 [Next] をクリックします。

ステップ 16 **[Summary]** ウィンドウで設定を確認し、**[Save]** をクリックします。

ステップ 17 [Modify Fabric] ステップで、[Now] をクリックして変更を確定し、[Apply] をクリックして設定を適用します。
次の手順では、ファブリックサイトで AP をオンボードします。

ステップ 18 Catalyst Center GUI でメニューアイコンをクリックして、**[Provision]** > **[Fabric Sites]**。

ファブリックサイトのリストが表示されます。

ステップ 19 作成したファブリックサイトを選択し、[Host Onboarding] タブをクリックして、AP の IP プールを有効にします。

ステップ 20 ファブリックサイト内のデバイスに適用される認証テンプレートを選択します。次に [Save] をクリックします。

ステップ 21 [Virtual Networks] の下で、[INFRA_VN] をクリックして、選択した仮想ネットワークに 1 つ以上の IP プールを関連付けます。

ステップ 22 [Virtual Network] の下で、ゲスト仮想ネットワークをクリックして、選択したゲスト仮想ネットワークの IP プールを関連付けます。

ステップ 23 設計フェーズ中に AP 用に作成された [IP Pool Name] チェックボックスをオンにします。

ステップ 24 [Update] をクリックして設定を保存します。

AP は指定したプールから IP アドレスを取得します。このプールは AP VLAN に関連付けられており、いずれかの検出方法を通じて ワイヤレスコントローラ に登録されます。

ステップ 25 ホストがアクセスできるネットワーク内のワイヤレス SSID を指定します。[Wireless SSID] セクションで、ゲスト SSID または企業 SSID を選択してアドレスプールを割り当ててから、[Save] をクリックします。

ステップ 26 **[Inventory]** > **[Resync]**の順に選択して手動で再同期をトリガーし、組み込みのワイヤレス用の Catalyst Center で AP を確認します。
検出された AP が [Provision] ウィンドウの [Inventory] に表示され、[Status] は [Not Provisioned] として表示されます。

ステップ 27 AP をプロビジョニングします。

詳細については、Day 1 の Cisco AP プロビジョニング （745 ページ）を参照してください。

ステップ 28 アプリケーションポリシーを設定および展開します。詳細については、アプリケーションポリシーの作成（1470ページ）、アプリケーションポリシーの展開（1476ページ）、およびアプリケーションポリシーの編集（1475 ページ）を参照してください。

アプリケーションポリシーを展開する前に、Catalyst 9300 シリーズ スイッチおよび Cisco Catalyst 9500H シリーズ スイッチをプロビジョニングします。

2 つの異なる SSID で異なるビジネスとの関連性を持つ 2 つの異なるポリシーは機能しません。関連性を設定するときは、最後に展開したポリシーが優先されます。

アプリケーションのデフォルトのビジネスとの関連性を変更しても、FlexConnect モードでは機能しません。

非ファブリック SSID にのみアプリケーションポリシーを適用できます。

ワイヤレスデバイスの AP LSC の更新

Before you begin

デバイスで Cisco IOS XE リリース 17.1.7.1 以降が実行されていることを確認します。

ワイヤレスデバイスの AP のローカルで有効な証明書（LSC）を期限切れになる前に更新するには、次の手順を実行します。

次のデバイスの AP LSC を更新できます。

- Cisco Catalyst 9800 シリーズ ワイヤレス コントローラについて
- ワイヤレス対応スイッチ

更新の期限が切れる AP の証明書は、期限切れの時間、サイトタグ、または手動選択に基づいて更新できます。

手順

ステップ 1 インベントリ内のデバイスに移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、ビルディング、またはフロアを選択します。
c) AP LSC を更新するデバイスを選択します。

ステップ 2 [アクション（Actions）] ドロップダウンリストから、**[プロビジョニング（Provision）]** > **[AP LSC証明書の更新（Renew AP LSC Certificate）]** の順に選択します。

ステップ 3 [アクセスポイント証明書の更新（Renew Access Point Certificate）] ウィンドウで、次の設定を完了します。

a) AP LSC を更新するオプションを選択します。

表 *50 : AP* 選択オプション

オプション	説明
[証明書の更新期限が切れるすべてのAP（All APs due for certificate renewal）]	期限切れまでの日数に基づいて、更新の期限が切れるすべての AP の証明書を更新します。 [期限（Due Time）] フィールドに、AP LSC の有効期限までの日数を入力します。有効な範囲は 0 ～ 60 日です。
[選択したサイトタグで設定された、証明書の更新の期限が切れるAP（APs configured with selected site tags and due for certificate renewal）]	サイトタグに基づいて、更新の期限が切れるすべての AP の証明書を更新します。 • [サイトタグ（Site tags）] ドロップダウンリストから、1 つまたは複数のサイトタグを選択します。 • [期限（Due Time）] フィールドに、AP LSC の有効期限までの日数を入力します。有効な範囲は 0 ～ 60 日です。
[APを手動で選択（Manually select APs）]	選択内容に基づいて、更新の期限が切れるすべての AP の証明書を更新します。 テーブルで必要な AP を選択します。 （注） テーブルの各列の検索フィールドを使用して AP を検索できます。検索フィールドに値を手動で入力し、Enter を押します。 検索結果には、列全体で値が強調表示された状態で対応する AP が表示されます。

b) [Submit] をクリックします。

ステップ 4 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

ステップ 5 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のデバイスごとの設定

Catalyst Center では デバイスごとの設定 機能を使用して Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の個々の機能またはパラメータをカスタマイズできます。デバイスごとの設定 を使用して、ワイヤレスコントローラ のデバイスレベルの設定を作成、編集、複製、および削除できます。

これらの設定を使用して、新しい ワイヤレスコントローラ を Catalyst Center にオンボーディングし、その設定を管理できます。これらの ワイヤレスコントローラ に関連付けられている AP を管理することもできます。

デフォルトステータス

デフォルトでは、デバイスごとの設定 機能は Catalyst Center で無効になっています。設定を有効にするには、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の デバイスごとの設定 を有効にします。 （802 ページ）」を参照してください。

制限事項

- 次の場合、デバイスごとの設定 はサポートされていません。
  - 以前に Catalyst Center に追加され、サイトベースのネットワークプロファイルがあるインテントベースのワイヤレスネットワーク設定を使用している ワイヤレスコントローラ（これらの ワイヤレスコントローラ では、デバイスごとの設定 は読み取り専用モードで利用可能です）、および
  - SD-Access ワイヤレス設定。
- AI 拡張 RRM 設定の場合、デバイスごとの設定 は [デバイスプロビジョニングなしで有効化（Enable Without Device Provisioning）] 展開タイプのアシュアランスユースケースでのみサポートされます。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のための デバイスごとの設定 の前提条件

- ワイヤレスコントローラ で Cisco IOS XE リリース 17.12 以降が実行されていることを確認します。
- ワイヤレスコントローラを Catalyst Center に追加します。
  - 単一のデバイスを手動で追加することも、ディスカバリを使用するか、[インベントリ（Inventory）] ウィンドウで CSV ファイルをインポートすることによって複数のデバイスを追加することもできます。詳細については、Catalyst Center インベントリへのデバイスの追加 （155 ページ）を参照してください。

- Prime Data Migration Tool（PDMT）を使用して、Cisco Prime Infrastructure からデバイスを移行できます。詳細については、『*Cisco Prime Infrastructure to Cisco Catalyst Center Prime Data Migration Guide*』を参照してください。

- デバイスが [インベントリ（Inventory）] ウィンドウに [管理対象（Managed）] 状態で表示されていることを確認します。

  詳細については、インベントリについて（100 ページ）およびインベントリに関する情報の表示 （102 ページ）を参照してください。

- エリア、ビルディング、フロアなどのネットワーク階層を設計します。この構造によって、後で設定を適用するサイトを特定しやすくなります。

  次のいずれかを行うことができます。

  - 新しいネットワーク階層を作成する（「サイトの作成、編集、削除 （285 ページ）」および「ビルディングの追加、編集、および削除 （286 ページ）」を参照）、または
  - Cisco Prime Infrastructure の既存のネットワーク階層（あれば）を Catalyst Center にインポートする（「Catalyst Center へのサイト階層のインポート （277 ページ）」を参照）

- AP の位置情報を追加し、フロアマップに配置して、ヒートマップカバレッジを可視化します。

  詳細については、「フロアマップでの AP の取り扱い （304 ページ）」を参照してください。

- 国コードが設定されていることを確認してください。

  詳細については、ワイヤレスデバイスと国コードについて （735 ページ）を参照してください。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の デバイスごとの設定 を有効にします。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の デバイスごとの設定 機能を有効にするには、次の手順を実行します。

（注） ワイヤレスコントローラがサイトベースのネットワークプロファイルを備えたインテントベースのワイヤレスネットワーク設定を使用して管理されている場合、デバイスごとの設定 は ワイヤレスコントローラ に対して読み取り専用モードで使用できます。

始める前に

前提条件を満たしていることを確認します。Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のための デバイスごとの設定 の前提条件 （801 ページ）を参照してください。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、[デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 デバイスの詳細ウィンドウの右上隅から、[デバイスごとの設定の有効化（Enable Per-Device Configuration）] をクリックします。

ステップ 4 [デバイスごとの設定（Per-device configuration）] ダイアログボックスで、詳細を表示し、[有効（Enable）] をクリックします。

次のタスク

他の操作を実行する前に、ワイヤレスコントローラ が再同期されていることを確認してください。ワイヤレスコントローラ の手動での再同期の詳細については、「デバイス情報の再同期（217 ページ）」を参照してください。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のデバイスごとの機能を設定する

デバイスごとの設定を使用して ワイヤレスコントローラ の個々の機能を設定およびプロビジョニングするには、次の手順を実行します。

（注） Catalyst Center 以外で設定変更を行った場合（CLI や WebUI を介してなど）、これらの変更は次のインベントリ同期時に検出され、インポートされます。このプロセスにより競合が発生する可能性があります。一貫性を維持し、予測可能なネットワークの動作を確保するために、サポートされているすべての設定変更に Catalyst Center を使用することを推奨します。

始める前に

次の内容を確認してください。

- 前提条件が満たされていること（「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのための デバイスごとの設定 の前提条件 （801 ページ）」を参照）
- デバイスごとの設定 が ワイヤレスコントローラ で有効になっていること（「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の デバイスごとの設定 を有効にします。 （802 ページ）」を参照）。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、[デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 （任意）デバイスの詳細ウィンドウの右上隅から、[APの管理（Manage APs）]をクリックして、ワイヤレスコントローラ に関連付けられている AP の AP 設定を変更します。

詳細については、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ に関連付けられた AP の管理 （805 ページ）を参照してください。

ステップ 4 [設定（Configuration）] タブで、 は、ワイヤレスコントローラ に必要な機能を設定およびプロビジョニングします。

- [SSID]：「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の SSID の設定 （813 ページ）」を参照してください。
- [RF]：「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の RF 設定 （852 ページ）」を参照してください。
- [AP]：「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の AP 設定 （867 ページ）」を参照してください。
- [タグマッピング（Tag Mapping）]：「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のタグマッピング設定 （909 ページ）」を参照してください。
- [セキュリティ（Security）]：「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のセキュリティ設定 （918 ページ）」を参照してください。
- [グローバルワイヤレス（Global Wireless）]：「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のグローバルワイヤレス設定 （1002 ページ）」を参照してください。

- [サービス（Services）]：「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのサービス設定 （1093 ページ）」を参照してください。
- [レイヤ2（Layer 2）]：「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のレイヤ 2 設定 （1122 ページ）」を参照してください。
- [ネットワークの設定（Network Settings）]：「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのネットワーク設定 （1139 ページ）」を参照してください。
- [レイヤ3（Layer 3）]：「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のレイヤ 3 の設定 （1162 ページ）」を参照してください。
- [管理（Administration）]：「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の管理設定 （1166 ページ）」を参照してください。

設定を検索するには、デバイスの詳細ウィンドウの左側のペインで[機能の検索（Search Features）]フィールドをクリックし、設定の名前を入力します。

（注） 使用可能な設定とそのオプションは、ワイヤレスコントローラ で実行されている Cisco IOS XE リリースによって異なる場合があります。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ に関連付けられた AP の管理

デバイスごとの設定を介してワイヤレスコントローラに関連付けられた AP を管理するには、次の手順を使用します。ワイヤレスコントローラに関連付けられた AP に対し、タグ（サイトタグ、ポリシータグ、および RF タグ）とタグマッピングプロファイルを設定できます。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 デバイスの詳細ウィンドウの 右上隅 から、[APの管理（Manage APs）] をクリックします。

ステップ 4 （任意）[アクセスポイント（Access Points）] スライドインペインで、[運用アクセスポイント（Operational Access Points）] の AP 設定セットを編集します。

1. 必要な AP 名の横にあるチェックボックスをオンにします。

2. [AP設定セットの編集（Edit AP Configuration Set）] をクリックします。

   [Edit AP Configuration Set] スライドインペイン が開きます。

3. **[Policy Tag]** ドロップダウンリストからポリシータグを選択します。
4. **[Site Tag]** ドロップダウンリストからサイトタグを選択します。
5. **[RF Tag]** ドロップダウンリストから RF タグを選択します。
6. ステップ 7（806 ページ）から ステップ 9（807 ページ）まで入力して、設定をプロビジョニングします。

ステップ 5 （任意） AP をサイトに割り当てます。

1. 必要な AP 名の横にあるチェックボックスをオンにします。
2. **[Assign AP to Site]** をクリックします。

   [Assign AP to Site] スライドインペイン が開きます。

3. 必要なサイトを選択します。

（注） [検索（Search）] フィールドに名前を入力してサイトを検索するか、[グローバル（Global）] を展開してサイトを選択することができます。

4. [**Assign**] をクリックします。

ステップ 6 （任意） [APおよび無線パラメータの設定（Configure AP and Radio Parameters）] をクリックして、AP および無線パラメータを設定します。

詳細については、AP の設定 （1639 ページ）を参照してください。

ステップ 7 [Review and Provision] をクリックします。

ステップ 8 ワイヤレスコントローラ がライセンス要件を満たしていない AP を管理している場合、Catalyst Center は詳細を示すダイアログボックスを表示します。ダイアログボックスで、必要なオプションを選択します。

オプション	説明
ライセンス マネージャ	[License Manager] ウィンドウを開いて、対応するライセンスを有効にします。 ライセンスを有効にするには、『*Cisco Catalyst Center Administrator Guide*』の「Manage Licenses」を参照してください。
[デバイスプロビジョニングに進む（Continue to device provision）]	デバイスのプロビジョニングを続行します。 （注） ライセンス要件を満たしていない AP は、ワールドワイドセーフモード（WWSM）になります。

オプション	説明
Cancel	ダイアログボックスを閉じます。

ステップ 9 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 10 [Tasks] ウィンドウで、タスクの展開を監視します。

デバイスごとの設定のテーブル設定のカスタマイズ

デバイスの詳細ウィンドウにテーブルが表示される場合に機能のデバイスごとの設定テーブル設定をカスタマイズするには、次の手順を実行します。

（注） この手順は、ウィンドウに [エアタイムフェアネス（Air Time Fairness）] などの機能のテーブルが表示されない場合は適用されません。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、 で、必要な設定をクリックします。

ステップ 4 対応する設定テーブルで、右上隅にある歯車アイコンをクリックします。
[Table Settings] スライドインペインが開きます。

ステップ 5 **[Table Appearance]** をクリックし、テーブルの密度とストライピングを調整します。

a) [Table Density] で、[Default] または [Compact] オプションを選択します。

b) テーブルストライピングを適用するには、[Table Striping] の下にあるトグルボタンをクリックします。
c) [Apply] をクリックします。

ステップ 6 （任意） テーブル設定をリセットするには、[Reset All Settings] をクリックします。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ 用の デバイスごとの設定 の編集

デバイスの詳細ウィンドウにテーブルが表示される場合に機能のデバイスごとの設定を編集するには、次の手順を実行します。

（注） この手順は、ウィンドウに [エアタイムフェアネス（Air Time Fairness）] などの機能のテーブルが表示されない場合は適用されません。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。
a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。
a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、[デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、必要なデバイスごとの機能をクリックします。
ステップ 4 編集する設定の横にあるチェックボックスをオンにします。
ステップ 5 **[Actions]** にカーソルを合わせ、**[Edit]** をクリックします。
ステップ 6 スライドインペイン で、必要な設定を編集します。
ステップ 7 [Review and Provision] をクリックします。
ステップ 8 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

ステップ 9 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の デバイスごとの設定 の複製

デバイスの詳細ウィンドウにテーブルが表示される場合、この手順を使用して機能のデバイスごとの設定 を複製するには、次の手順を実行します。

（注） この手順は、ウィンドウに [エアタイムフェアネス（Air Time Fairness）] などの機能のテーブルが表示されない場合は適用されません。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、必要なデバイスごとの機能をクリックします。

ステップ 4 複製する設定の横にあるチェックボックスをオンにします。

ステップ 5 **[Actions]** にカーソルを合わせ、**[Clone]** をクリックします。

ステップ 6 スライドインペイン で、必要な設定を完了します。

ステップ 7 （任意） その他の必要な設定を編集します。

ステップ 8 [Review and Provision] をクリックします。

ステップ 9 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 10 [Tasks] ウィンドウで、タスクの展開を監視します。

別の Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ から デバイスごとの設定 を複製

次の機能について、別の Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ から デバイスごとの設定 を複製するには、次の手順を使用します。

- WLAN プロファイル
- ポリシープロファイル
- AP 加入プロファイル
- RF プロファイル
- Flex プロファイル
- サイト タグ

別の Cisco IOS XE リリースを実行している ワイヤレスコントローラ から設定を複製する場合、一部のオプションが使用できないか、正しくない場合があります。このような場合、Catalyst Center は、ワイヤレスコントローラ に適用されるデフォルトを選択します。続行する前に、値を確認してください。

（注） 設定の復元元となる ワイヤレスコントローラ がマスターキーで暗号化されている場合、正常にプロビジョニングできるように、WLAN プロファイルおよび AP 加入プロファイルの複製プロセス中にパスワード（クリアテキストまたは暗号化）を設定する必要があります。

始める前に

複製する ワイヤレスコントローラ がすでに Catalyst Center に追加されており、管理状態になっていることを確認してください。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、[デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、対応するデバイスごとの機能をクリックします。

ステップ 4 [別のWLCから複製（Clone from another WLC）] をクリックします。

ステップ 5 スライドインペイン で、次の手順を実行します。

a) ドロップダウンリストから、設定を複製する ワイヤレスコントローラ を選択します。

選択した ワイヤレスコントローラ に関連付けられている設定のリストが表示されます。

b) 必要な設定を選択します。

c) [Clone] をクリックします。

ステップ 6 警告ダイアログボックスで [OK] をクリックします。

ステップ 7 スライドインペイン には、選択した ワイヤレスコントローラ から複製された設定が表示されます。

（注） 機能の複製を実行すると、送信元 ワイヤレスコントローラ から設定がコピーされます。ターゲット ワイヤレスコントローラ との互換性を確保するため、適用前に設定を確認してください。

ステップ 8 必要な設定を編集します。

（注） 左側のペインの警告アイコンは、設定の競合を示します。競合を確認し、適切な値を選択して次のウィンドウに進みます。

ステップ 9 [Review and Provision] をクリックします。

ステップ 10 ワイヤレスコントローラ がライセンス要件を満たしていない AP を管理している場合、Catalyst Center は詳細を示すダイアログボックスを表示します。ダイアログボックスで、必要なオプションを選択します。

オプション	説明
ライセンス マネージャ	[License Manager] ウィンドウを開いて、対応するライセンスを有効にします。 ライセンスを有効にするには、『*Cisco Catalyst Center Administrator Guide*』の「Manage Licenses」を参照してください。
[デバイスプロビジョニングに進む（Continue to device provision）]	デバイスのプロビジョニングを続行します。 （注） ライセンス要件を満たしていない AP は、ワールドワイドセーフモード（WWSM）になります。
Cancel	ダイアログボックスを閉じます。

ステップ 11 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 12 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の デバイスごとの設定 を削除

デバイスの詳細ウィンドウにテーブルが表示される場合、機能の デバイスごとの設定 を削除するには、この手順を実行します。

（注） この手順は、ウィンドウに [エアタイムフェアネス（Air Time Fairness）] などの機能のテーブルが表示されない場合は適用されません。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、[デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、必要なデバイスごとの機能をクリックします。

ステップ 4 削除する設定の横にあるチェックボックスをオンにします。

ステップ 5 **[Actions]** にカーソルを合わせ、**[Delete]** をクリックします。

ステップ 6 ダイアログボックスで、**Yes** をクリックします。

ステップ 7 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。

- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 8 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の SSID の設定

このセクションでは、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のデバイスごとの SSID 設定に関する情報を示します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の WLAN プロファイルの作成

この手順を使用して、ワイヤレスコントローラ の WLAN プロファイルを作成し、プロビジョニングします。WLAN プロファイルで Wi-Fi 設定を構成し、ユーザーがワイヤレスネットワークに接続できるようにします。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、 [SSID] を展開し、[WLANプロファイル（WLAN Profiles）] をクリックします。

ステップ 4 [Add] をクリックします。

ステップ 5 [WLANプロファイルの作成（Create WLAN Profile）] スライドインペインの [一般（General）] タブで、次の設定を完了します。

a) [ワイヤレス ネットワーク名（SSID）（Wireless Network Name (SSID)）] フィールドに、SSID の一意の名前を入力します。
b) [WLAN ID] フィールドでは、WLAN ID は次に使用可能な番号に基づいて自動的に入力されます。

必要に応じて、WLAN ID を更新します。有効な範囲は 1 ～ 4096 です。

c) [WLANプロファイル名（WLAN Profile Name）] フィールドに、WLAN プロファイル名に基づいて WLAN プロファイル名が自動的に入力されます。

必要に応じて、名前を更新します。

（注） WLAN プロファイル名が一意であり、既存の RLAN プロファイル名と一致していないことを確認してください。そうでない場合、WLAN プロファイルの作成タスクは失敗します。

d) [SSID状態（SSID State）] で、トグルボタンを使用して対応するステータスを有効または無効にします。

- [管理ステータス（Admin Status）]：WLAN の管理ステータスを有効または無効にします。

  このトグルボタンを無効にすると、対応する SSID は AP ビーコンでブロードキャストされません。

- [ブロードキャストSSID（Broadcast SSID）]：範囲内のすべてのワイヤレスクライアントに対して SSID の可視性を有効または無効にします。

e) [Wi-Fi 7の互換性（Wi-Fi 7 Compatibility）] で、Wi-Fi 7 の互換性情報を表示します。

詳細を表示するには、[詳細を表示（Show Details）] をクリックします。

Wi-Fi 7の互換性を確保するには、ステップ 6 （816 ページ） で次の設定を行います。

- WPA3 を有効にします。
- サポートされている暗号および認証キー管理の組み合わせを、次の中から選択します。
  - AES および 802.1X-SHA256 または FT-802.1X
  - GCMP256 および SAE-EXT-KEY、FT-SAE-EXT-KEY、または OWE
  - GCMP256 および 802.1X-SHA256 または FT-802.1X
  - GCMP256 および Suite-B-192
- [保護された管理フレーム（PMF）（Protected Management Frame（PMF）] は、[必須（Required）] または [任意（Optional）] に設定する必要があります

f) [Wi-Fi 7帯域ごとのステータス（Wi-Fi 7 Per Band Status）] では、Wi-Fi 7 設定の帯域ごとのステータスを表示します。

各帯域の詳細を表示するには、[詳細を表示（Show Details）] をクリックします。

各帯域ごとに Wi-Fi 7 を有効にするには、次の設定を行います。

- [無線ポリシー（Radio Policy）]でバンドを有効にします。
- 各帯域に対して Global 11be を有効にします。詳細については、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の高スループットパラメータの設定 （1006 ページ） を参照してください。
- 選択した 802.11be プロファイルのマルチリンク動作（MLO）グループで帯域を有効にします。詳細については、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の 802.11be プロファイルの設定 （849 ページ） を参照してください。

g) [無線ポリシー（Radio Policy）]で、次の設定を行います。

- 802.11 帯域ごとにサポートされる無線スロットを示します。対応する帯域のスロット設定を表示するには、[スロット設定を表示（Show Slot Configuration）] をクリックします。

（注） スロット設定で、スロットの横にチェックボックスがオンになっている場合、それを使用して、対応する帯域のスロットを有効または無効にできます。

- [6 GHz]、[5 GHz]、[2.4 GHz] トグルボタンを使用して、対応する帯域の無線ポリシーを有効または無効にします。

（注） 6 GHz 帯域は次の場合にのみサポートされます。

  - WPA2 が無効であり、
  - WPA3、保護された管理フレーム、および 802.11ax 設定が有効になっている場合。

- [Bgポリシー（Bg Policy）] ドロップダウンリストから、ポリシーを選択します。

（注） このドロップダウンリストは、[2.4 GHz] トグルボタンを有効にした場合にのみ使用できます。

- （任意）対応する設定を有効にするには、必要なチェックボックスをオンにします。

チェックボックス	説明
Band Select	[2.4 GHz] トグルボタンを有効にした場合にのみ使用できます。
[6 GHzクライアントのステアリング（6 Ghz Client Steering）]	[6 GHz] トグルボタンを有効にした場合にのみ使用できます。

- [最小2.4 GHzデータレート（Minimum 2.4 GHz Data Rate）] および [最小5 GHzデータレート（Minimum 5 GHz Data Rate）] ドロップダウンリストから、その帯域に接続するクライアントでサポートされる最小データレートを選択します。

  値を大きくすると、ネットワークパフォーマンスが向上し、レガシーデバイスからの干渉を減らすことができますが、古くて遠隔なクライアントが接続できなくなることがあります。互換性を最大化する場合は小さい値を選択し、スループットを最適化してエアタイム効率を向上させる場合は大きい値を選択します。

（注） AP のスロットの可用性は、AP モデルによって異なります。フレキシブル ラジオ アサインメント（FRA）機能を備えたスロットの場合、FRA は帯域を動的に変更できます。この設定は、設定された帯域内で動作する場合にのみスロットに適用されます。必要に応じて、この設定を使用して帯域およびスロットごとに WLAN ブロードキャストを制限します。帯域全体で 1 つ以上のスロットが有効になっていることを確認します。

ステップ 6 [セキュリティ（Security）] で [レイヤー2（Layer 2）] をクリックし、セキュリティポリシーを設定します。

（注） 同じ SSID を持つ WLAN には、一意のレイヤ 2 セキュリティポリシーが必要です。

- 認証用の 802.1X サーバーでユーザーログイン情報の検証を設定するには、[エンタープライズ（Enterprise）] をクリックし、次の手順を実行します。

1. （オプション）[MACオーバーライド承認リスト（MAC Override Authorization List）] フィールドに、WLAN のデフォルトリストを上書きする MAC アドレス承認リストの名前を入力します。

   グローバルまたはデフォルトのリストとは異なる認証ポリシーが必要な場合は、このフィールドを使用します。

2. （オプション）[WLAN承認リスト（WLAN Authorization List）] フィールドに、WLAN に使用する承認リストの名前を入力します。

   このフィールドで承認リストを指定しない場合、WLAN はデフォルトのリストを使用します。

3. （オプション）[MACフィルタリング（MAC Filtering）] チェックボックスをオンにして、ワイヤレスネットワークで MAC ベースのアクセス制御またはセキュリティを有効にします。

   このチェックボックスをオンにした場合は、[MAC Authorization List] ドロップダウンリストから認証リストを選択します。

   承認リストの作成については、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の認証方式リストの作成 （929 ページ）」を参照してください。

4. （オプション）ロビーアンバサダーアカウントへのアクセスを有効にするには、[ロビー管理アクセス（Lobby Admin Access）] チェックボックスをオンにします。

5. [WPAパラメータ（WPA Parameters）] で、対応する設定を行うために必要なチェックボックスをオンにします。

   - [WPA]：WPA サポートを設定します。

（注） [WPA3] または [OSEN Policy] チェックボックスをオンにすると、このチェックボックスはグレー表示になります。

- [WPA2]：WPA2 サポートを設定します。
- [WPA3]：WPA3 サポートを設定します。

（注） [WPA]、[GTK Randomize]、または [OSEN Policy] チェックボックスをオンにすると、このチェックボックスはグレー表示になります。

WPA3 を有効にする場合は、必要に応じて次のチェックボックスをオンにして、対応する設定を構成できます。

- [移行の無効化（Transition Disable）]：WPA3 から WPA2 への移行を防止します。
- [ビーコン保護（Beacon Protection）]：ビーコン保護を有効にします。

- [GTKランダム化（GTK Randomize）]：ホール 196 の緩和のためにランダム化 Group Temporal Key（GTK）を有効にします。

  ホール 196 は WPA2 脆弱性の名前です。

（注） [WPA3] チェックボックスをオンにすると、このチェックボックスはグレー表示になります。

- [OSENポリシー（OSEN Policy）]：暗号化を使用したオンライン サブスクリプション（OSEN）サポートを設定します。

（注） [WPA] または [WPA3] チェックボックスをオンにすると、このチェックボックスはグレー表示になります。

6. [WPA暗号化（WPA Encryption）]エリアが表示された場合は、必要なチェックボックスをオンにして、WPA に対応する暗号サポートを有効にします。

   少なくとも 1 つの暗号のサポートを有効にする必要があります。

7. [WPA2/WPA3暗号化（WPA2/WPA3 Encryption）] エリアが表示されたら、次の設定を行います。

- Cisco IOS XE リリース 17.15 より前のリリースを実行している ワイヤレスコントローラの場合、必要な暗号化タイプを選択します。
- Cisco IOS XE リリース 17.15 以降を実行している ワイヤレスコントローラ の場合、必要な暗号化タイプの横にあるチェックボックスをオンにします。

8. [認証キー管理（Auth Key Management）] エリアが表示されたら、対応する認証キー管理タイプを選択するために必要なチェックボックスをオンにします。

このエリアで使用可能なタイプは、[WPA]、[WPA2]、または [WPA3] の暗号化設定によって異なります。

[CCKM] チェックボックスをオンにした場合は、[CCKM TSF許容度（CCKM TSF Tolerance）] フィールドに CCKM 許容度レベルをミリ秒単位で入力します。

このフィールドの有効な範囲は 1000 ～ 5000 です。デフォルト値は 1000 です。認証されたクライアントデバイスでは、再関連付け中に遅延を感じることなく、AP間でローミングできます。

9. [Protected Management Frame (802.11w)] の [Status] ドロップダウンリストから、使用可能なステータスを選択します。

[オプション（Optional）] または [必須（Required）] を選択した場合は、次の設定を行います。

- [SA Query Time(msec)] フィールドに、セキュリティ アソシエーション（SA）クエリの再試行タイムアウトをミリ秒単位で入力します。

  有効な範囲は 100 ～ 500 です。デフォルト値は 200 です。

- [Association Comeback Timer(sec)] フィールドに、アソシエーション復帰時間をミリ秒単位で入力します。

  有効な範囲は、1 ～ 20 です。デフォルト値は 1 です。

10. [Fast Transition (802.11r)] の [Fast Transition Mode] ドロップダウンリストから、使用可能なモードを選択します。

[有効（Enabled）] または [適応型有効（Adaptive Enabled）] を選択した場合は、次の設定を行います。

- 分散システム経由の高速移行を有効にするには、[Over the DS] チェックボックスをオンにします。
- [Reassociation Timeout] フィールドに、再関連付けのタイムアウトを秒単位で入力します。

  有効な範囲は 1 ～ 100 です。デフォルト値は 20 です。

- パスワード（WPA2 暗号化を使用した PSK）を使用したユーザーログイン情報の検証を設定するには、[パーソナル（Personal）] をクリックし、次の設定を行います。

1. （オプション）[MACオーバーライド承認リスト（MAC Override Authorization List）] フィールドに、WLAN のデフォルトリストを上書きする MAC アドレス承認リストの名前を入力します。

グローバルまたはデフォルトのリストとは異なる認証ポリシーが必要な場合は、このフィールドを使用します。

2. （オプション）[WLAN承認リスト（WLAN Authorization List）] フィールドに、WLAN に使用する承認リストの名前を入力します。

   このフィールドで承認リストを指定しない場合、WLANはデフォルトのリストを使用します。

3. （オプション）[MACフィルタリング（MAC Filtering）] チェックボックスをオンにして、ワイヤレスネットワークで MAC ベースのアクセス制御またはセキュリティを有効にします。

   このチェックボックスをオンにした場合は、[MAC Authorization List] ドロップダウンリストから認証リストを選択します。

   承認リストの作成については、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の認証方式リストの作成 （929 ページ）」を参照してください。

4. （オプション）ロビーアンバサダーアカウントへのアクセスを有効にするには、[ロビー管理アクセス（Lobby Admin Access）] チェックボックスをオンにします。

5. [WPAパラメータ（WPA Parameters）] で、対応する設定を行うために必要なチェックボックスをオンにします。

   - [WPA]：WPA サポートを設定します。

   （注） [WPA3] チェックボックスをオンにすると、このチェックボックスはグレー表示になります。

   - [WPA2]：WPA2 サポートを設定します。
   - [WPA3]：WPA3 サポートを設定します。

   （注） [WPA] または [GTK Randomize] チェックボックスをオンにすると、このチェックボックスはグレー表示になります。

   WPA3 を有効にする場合、必要なチェックボックスをオンにして、対応する設定を有効にできます（任意）。

   - [移行の無効化（Transition Disable）]：WPA3 から WPA2 への移行を防止します。
   - [ビーコン保護（Beacon Protection）]：ビーコン保護を有効にします。

   - [GTKランダム化（GTK Randomize）]：ホール 196 の緩和のために GTK を有効にします。

     ホール 196 は WPA2 脆弱性の名前です。

（注） [WPA3] チェックボックスをオンにすると、このチェックボックスはグレー表示になります。

6. [WPA暗号化（WPA Encryption）]エリアが表示された場合は、必要なチェックボックスをオンにして、WPA に対応する暗号サポートを有効にします。

   少なくとも 1 つの暗号のサポートを有効にする必要があります。

7. [WPA2/WPA3暗号化（WPA2/WPA3 Encryption）]エリアが表示される場合は、[AES(CCMP128)] チェックボックスをオンにしてこの暗号化タイプを選択します。

8. [認証キー管理（Auth Key Management）] エリアが表示されたら、対応する認証キー管理タイプを選択するために必要なチェックボックスをオンにします。

   このエリアで使用可能なオプションは、[WPA]、[WPA2]、または [WPA3] の暗号化設定によって異なります。

   選択したオプションに基づいて、追加の設定がある場合は、それらの設定を完了します。

   - （任意）[PSK Format] ドロップダウンリストから、認証の事前共有キー（PSK）形式を選択します。
   - （任意）[PSKタイプ（PSK Type）] ドロップダウンリストから [非暗号化（Unencrypted）] を選択します。
   - [Pre-shared Key] フィールドに、PSK 値を入力します。

     16 進数キー形式の場合、PSK の長さは 64 文字にする必要があります。ASCII キー形式の場合、PSK の長さは 8 ～ 63 の範囲にする必要があります。
   - [Anti Clogging Threshold] フィールドに、Simultaneous Authentication of Equals（SAE）アンチロギングしきい値を入力します。

     有効な範囲は 0 ～ 3000 です。デフォルト値は 1500 です
   - [Max Retries] フィールドに、SAE 再送信の最大数を入力します。

     有効な範囲は 1 ～ 10 です。デフォルト値は 5 です。
   - [Retransmit Timeout] フィールドに、SAE 再送信タイムアウトを入力します。

     有効な範囲は 1 ～ 10000 です。デフォルト値は 400 です。
   - （任意）[SAEパスワード要素（SAE Password Element）] ドロップダウンリストから、SAE パスワード要素モードを選択します。

9. [Protected Management Frame (802.11w)] の [Status] ドロップダウンリストから、使用可能なステータスを選択します。

   [オプション（Optional）] または [必須（Required）] を選択した場合は、これらのフィールドにデータを入力します。

- [アソシエーション復帰タイマー（秒）（Association Comeback Timer(sec)）] フィールドに、アソシエーション復帰時間を秒単位で入力します。

  有効な範囲は、1 ～ 20 です。デフォルト値は 1 です。

- [SAクエリ時間（ミリ秒）（SA Query Time(msec)）] フィールドに、セキュリティ アソシエーション（SA）クエリの再試行タイムアウトをミリ秒単位で入力します。

  有効な範囲は 100 ～ 500 です。デフォルト値は 200 です。

10. [Fast Transition (802.11r)] の [Fast Transition Mode] ドロップダウンリストから、使用可能なモードを選択します。

[有効（Enabled）] または [適応型有効（Adaptive Enabled）] を選択した場合は、次の設定を行います。

- 分散システム経由の高速移行を有効にするには、[Over the DS] チェックボックスをオンにします。
- [Reassociation Timeout] フィールドに、再関連付けのタイムアウトを秒単位で入力します。

  有効な範囲は 1 ～ 100 です。デフォルト値は 20 です。

11. （オプション）[MPSK] で、[MPSK有効化（Enable MPSK）] チェックボックスをオンにして、複数事前共有キー（MPSK）サポートを設定し、次の設定を行います。

（注） MPSK と Easy-PSK は同時に有効にできません。

実行する操作	結果
MPSK の追加 （注） 最大 5 つの MPSK を追加できます。	**1.** [Add] をクリックします。 **2.** [MPSK設定の追加（Add MPSK Configuration）] ダイアログボックスの [優先順位（Priority）] フィールドに、優先順位を入力します。 有効な範囲は 0 ～ 4 です。 **3.** （任意）[Key Format] ドロップダウンリストから形式を選択します。 **4.** （任意）[パスワードタイプ（Password Type）] ドロップダウンリストから [非暗号化（Unencrypted）] を選択します。 **5.** （任意）[Pre-Shared Key] フィールドに、MPSK キーを入力します。 **6.** [Save] をクリックします。

実行する操作	結果
MPSK の編集	1. 編集するMPSKの横にあるチェックボックスをオンにします。 2. [Actions] にカーソルを合わせて [Edit] を選択します。 3. 必要な設定を編集します。 4. [Save] をクリックします。
MPSK の削除	1. 削除するMPSKの横にあるチェックボックスをオンにします。 2. [Actions] にカーソルを合わせて [Delete] を選択します。 3. ダイアログボックスで、**Yes** をクリックします。

- 静的 Wired Equivalent Privacy（WEP）を使用した認証用の 802.1X サーバーでユーザーログイン情報の検証を設定するには、[静的WEP（Static WEP）] をクリックし、次の設定を行います。

1. （オプション）[MACオーバーライド承認リスト（MAC Override Authorization List）] フィールドに、WLAN のデフォルトリストを上書きする MAC アドレス承認リストの名前を入力します。

   グローバルまたはデフォルトのリストとは異なる認証ポリシーが必要な場合は、このフィールドを使用します。

2. （オプション）[WLAN承認リスト（WLAN Authorization List）] フィールドに、WLAN に使用する承認リストの名前を入力します。

   このフィールドで承認リストを指定しない場合、WLAN はデフォルトのリストを使用します。

3. （オプション）[MACフィルタリング（MAC Filtering）] チェックボックスをオンにして、ワイヤレスネットワークで MAC ベースのアクセス制御またはセキュリティを有効にします。

   このチェックボックスをオンにした場合は、[MAC Authorization List] ドロップダウンリストから認証リストを選択します。

   承認リストの作成については、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の認証方式リストの作成 （929 ページ）」を参照してください。

4. （オプション）ロビーアンバサダーアカウントへのアクセスを有効にするには、[ロビー管理アクセス（Lobby Admin Access）] チェックボックスをオンにします。

5. [静的WEPパラメータ（Static WEP Parameters）] で、次の設定を行います。

   - [Key Size] ドロップダウンリストからキーサイズを選択します。
   - [Key Index] フィールドに、静的 WEP 認証に使用するキーを示す WEP キーインデックスを入力します。

     有効な範囲は 1 ～ 4 です。

   - [Key Format] ドロップダウンリストから WEP キー形式を選択します。

- [WEP Key Type] ドロップダウンリストから WEP キー暗号化タイプを選択します。
- [Wep Key] フィールドに静的 WEP キーを入力します。

  キーの長さは、[Key Size] ドロップダウンリストから選択したキーサイズによって異なります。

6. （オプション）[Fast Transition] で [静的WEP Fast Transition（Static WEP Fast Transition）] チェックボックスをオンにして、Fast Transition を有効にします。

- オープンでセキュアな認証を使用したユーザーログイン情報の検証を設定するには、[オープンセキュア（Open Secured）] をクリックし、次の設定を行います。

1. （オプション）[MACオーバーライド承認リスト（MAC Override Authorization List）] フィールドに、WLAN のデフォルトリストを上書きする MAC アドレス承認リストの名前を入力します。

   グローバルまたはデフォルトのリストとは異なる認証ポリシーが必要な場合は、このフィールドを使用します。

2. （オプション）[WLAN承認リスト（WLAN Authorization List）] フィールドに、WLAN に使用する承認リストの名前を入力します。

   このフィールドで承認リストを指定しない場合、WLAN はデフォルトのリストを使用します。

3. （オプション）[MACフィルタリング（MAC Filtering）] チェックボックスをオンにして、ワイヤレスネットワークで MAC ベースのアクセス制御またはセキュリティを有効にします。

   このチェックボックスをオンにした場合は、[MAC Authorization List] ドロップダウンリストから認証リストを選択します。

   承認リストの作成については、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の認証方式リストの作成 （929 ページ）」を参照してください。

4. （オプション）ロビーアンバサダーアカウントへのアクセスを有効にするには、[ロビー管理アクセス（Lobby Admin Access）] チェックボックスをオンにします。

5. [WPA3] チェックボックスをオンにして、WPA3 サポートを設定します。

6. [WPA2/WPA3暗号化（WPA2/WPA3 Encryption）] で、[AES(CCMP128)] チェックボックスをオンにしてこの暗号化タイプを選択します。

7. [認証キー管理（Auth Key Management）] で、対応する認証キー管理タイプを選択するために必要なチェックボックスをオンにします。

   このエリアで使用可能なオプションは、[WPA3] の暗号化設定によって異なります。

   [OWE] チェックボックスをオンにした場合は、[Transition Mode WLAN ID] フィールドに Opportunistic Wireless Encryption（OWE）移行モードの WLAN ID を入力します。

   この WLAN ID の有効な範囲は 0 ～ 4096 です。デフォルト値は 0 です

8. [Protected Management Frame (802.11w)] の [Status] ドロップダウンリストから、使用可能なステータスを選択します。

[オプション（Optional）] または [必須（Required）] を選択した場合は、次の設定を行います。

- [Association Comeback Timer(sec)] フィールドに、アソシエーション復帰時間をミリ秒単位で入力します。

  有効な範囲は、1 ～ 20 です。デフォルト値は 1 です。

- [SA Query Time(msec)] フィールドに、セキュリティ アソシエーション（SA）クエリの再試行タイムアウトをミリ秒単位で入力します。

  有効な範囲は 100 ～ 500 です。デフォルト値は 200 です。

- [オープン（Open）] をクリックしてオープン認証を設定し、必要なチェックボックスをオンにして対応する設定を有効にします。

  - （オプション）[MACオーバーライド承認リスト（MAC Override Authorization List）] フィールドに、WLANのデフォルトリストを上書きするMACアドレス承認リストの名前を入力します。

    グローバルまたはデフォルトのリストとは異なる認証ポリシーが必要な場合は、このフィールドを使用します。

  - （オプション）[WLAN承認リスト（WLAN Authorization List）] フィールドに、WLANに使用する承認リストの名前を入力します。

    このフィールドで承認リストを指定しない場合、WLAN はデフォルトのリストを使用します。

  - （オプション）[MACフィルタリング（MAC Filtering）]：ワイヤレスネットワークでMACベースのアクセス制御またはセキュリティを有効にします。

    このチェックボックスをオンにした場合は、[MAC Authorization List] ドロップダウンリストから認証リストを選択します。

    承認リストの作成については、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の認証方式リストの作成 （929 ページ）」を参照してください。

  - （オプション）ロビー アンバサダー アカウントへのアクセスを有効にするには、[ロビー管理アクセス（Lobby Admin Access）] チェックボックスをオンにします。

  - （オプション）[OWE移行モード（OWE Transition Mode）]：OWE 移行モードを設定します。

    このチェックボックスをオンにした場合は、[Transition Mode WLAN ID] フィールドに OWE 移行モードの WLAN ID を入力します。

    この WLAN ID の有効な範囲は 0 ～ 4096 です。デフォルト値は 0 です

ステップ 7 （任意） [セキュリティ（Security）] で、[レイヤ3（Layer 3）] をクリックして、次の設定を行います。

a) Web認証ポリシーを設定するには、[Webポリシー（Web Policy）]チェックボックスをオンにします。

b) ドロップダウンリストから必要なオプションを選択します。

- [Web認証パラメータマップ（Web Auth Parameter Map）]：Web 認証のパラメータマップを選択します。Web 認証パラメータマップを作成するには、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの Web 認証プロファイルの作成 （970 ページ）」を参照してください。

- [認証リスト（Authentication List）]：認証リストを選択します。

  認証リストの作成については、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の認証方式リストの作成 （928 ページ）」を参照してください。

c) 対応する設定を有効にするには、必要なチェックボックスをオンにします。

- [MACフィルタの障害時（On MAC Filter Failure）]：MAC フィルタの障害時に Web 認証を有効にします。
- [スプラッシュWebリダイレクト（Splash Web Redirect）]：スプラッシュページ Web リダイレクトを設定します。

d) （任意） [Web承認リスト（Web Authorization List）] フィールドに、WLAN のWeb 承認リストの名前を入力します。

このリストは、Web 認証セッション中のクライアントアクセスを許可または拒否します。

e) [事前認証ACL（Preauthentication ACL）] で、対応するドロップダウンリストから IPv4 ACL と IPv6 ACL を選択します。

IPv4 ACL の作成については、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の IPv4 ACL の作成 （940 ページ）」を参照してください。IPv6 ACL の作成については、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の IPv6 ACL の作成 （949 ページ）」を参照してください。

ステップ 8 （任意） [セキュリティ（Security）] で、[AAA] をクリックして、次の設定を行います。

a) [Authentication List] ドロップダウンリストから認証リストを選択します。

dot1x タイプ認証リストの作成については、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の認証方式リストの作成 （928 ページ）」を参照してください。

b) WLAN でローカル Extensible Authentication Protocol（EAP; 拡張可能認証プロトコル）認証を有効にするには、[ローカルEAP認証（Local EAP Authentication）] チェックボックスをオンにします。

このチェックボックスをオンにする場合は、[EAPプロファイル名（EAP Profile Name）] ドロップダウンリストからローカル EAP プロファイルを選択します。ローカル EAP プロファイルを作成するには、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のローカル EAP プロファイルの作成 （958 ページ）」を参照してください。

ステップ 9 （任意） [詳細設定（Advanced）] で、[11be] をクリックし、WLAN の 802.11be プロファイルを選択します。

802.11be プロファイルの作成については、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の 802.11be プロファイルの設定 （849 ページ）」を参照してください。

ステップ 10 （任意） [詳細設定（Advanced）] で、[11ax] をクリックして、次の設定を行います。

a) 対応する設定を有効にするには、必要なチェックボックスをオンにします。

- [11axの有効化（Enable 11ax）]：802.11ax 設定を有効にします。

- [ダウンリンクMU-MIMO（Downlink MU-MIMO）]：802.11axマルチユーザーMIMO（MU-MIMO）ダウンリンク設定を有効にします。
- [ダウンリンクOFDMA（Downlink OFDMA）]：802.11ax直交周波数分割多重（OFDMA）ダウンリンク設定を有効にします。
- [アップリンクMU-MIMO（Uplink MU-MIMO）]：802.11ax MU-MIMO アップリンク設定を有効にします。
- [アップリンクOFDMA（Uplink OFDMA）]：802.11ax OFDMA アップリンク設定を有効にします。
- [BSSターゲット起動時間（BSS Target Wake Up Time）]：802.11ax ターゲット起動時間のサポートを有効にします。
- [HE BSSカラー有効（HE BSS Color Enable）]：802.11ax 基本サービスセット（BSS）カラー設定を有効にします。

  このチェックボックスをオンにする場合は、[HE BSS Color] フィールドに BSS カラー値を入力します。

  有効範囲は 0 ～ 255 です。デフォルト値は 0 です
- [HE TWT有効（HE TWT Enable）]：802.11ax ターゲット起動時間を有効にします。
- [BSSターゲット起動時間ブロードキャスト（BSS Target Wake Up Time Broadcast）]：802.11ax ターゲット起動時間ブロードキャストのサポートを有効にします。

ステップ 11 （任意） [詳細設定（Advanced）] で、[11k] をクリックして、次の設定を行います。

a) [経由ローミング（Assisted Roaming）] で、対応する設定の適切なステータスを示すために必要なチェックボックスをオンにします。

- [予測最適化（Prediction Optimization）]：WLAN の ワイヤレスコントローラ で 11k 経由ローミング予測最適化が有効になっているかどうかを示します。
- [ネイバーリスト（Neighbor List）]：WLAN の ワイヤレスコントローラ で 11k ネイバーリストが有効になっているかどうかを示します。
- [デュアルバンドネイバーリスト（Dual Band Neighbor List）]：WLAN の ワイヤレスコントローラ で 11k デュアルバンド ネイバー リストが有効になっているかどうかを示します。

b) [ビーコン無線測定（Beacon Radio Measurement）] で、必要なチェックボックスをオンにして対応する設定を行います。

- [関連付けでのクライアントスキャンレポート（Client Scan Report on Association）]：クライアント関連付け後にビーコン測定要求を送信します。
- [ローミングでのクライアントスキャンレポート（Client Scan Report on Roam）]：クライアントローミング時にビーコン測定要求を送信します。

ステップ 12 （任意） [詳細（Advanced）] で [11v BSS] をクリックし、次の設定を行います。

a) 必要なチェックボックスをオンにして、対応する設定を行います。

- [BSS移行（BSS Transition）]：WLAN ごとに BSS 移行を有効にします。
- [BSS最大アイドル保護（BSS Max Idle Protected）]：WLAN ごとに BSS 最大アイドル処理の保護モードを有効にします。
- [デュアルネイバーリスト（Dual Neighbor List）]：WLAN の 802.11v BSS 移行でデュアルバンドネイバー リストが有効になっているかを確認します。
- [Directed Multicast Service]：WLAN ごとに Directed Multicast Service（DMS）処理を設定します。
- [BSS最大アイドルサービス（[BSS Max Idle Service]）]：WLAN ごとに BSS 最大アイドル処理を有効にします。
- [802.11vの関連付け解除強制切断（802.11v Disassociate Imminent）]：WLAN ごとに緊急の BSS 移行の関連付け解除強制切断を有効にします。
- [802.11v TFS]：WLAN ごとに TFS 処理を有効にします。
- [802.11v WNMスリープモード（802.11v WNM Sleep Mode）]：WLAN ごとにワイヤレスネットワーク管理（WNM）スリープモードを有効にします。

b) [802.11v Disassociate Timer] フィールドに、緊急の 802.11v 関連付け解除タイマーを秒単位で入力します。

有効な範囲は 0 ～ 3000 です。デフォルト値は 200 です。

c) [802.11v関連付け解除タイマー最適化ローミング（802.11v Disassociate Timer Optimized Roaming）] フィールドに、緊急の 802.11v 最適化ローミング関連付け解除タイマーを秒単位で入力します。

有効な範囲は 0 ～ 40 です。デフォルト値は 40 です。

ステップ 13 （任意）[詳細設定（Advanced）] で、[デバイス分析（Device Analytics）] をクリックし、必要なチェックボックスをオンにして、対応する設定を有効にします。

- [サポートのアドバタイズ（Advertise Support）]：デバイス分析サポートを有効にします。
- [クライアントとデータを共有（Share Data with Client）]：シスコデバイスデータをクライアントと共有できるようにします。
- [PC分析サポートのアドバタイズ（Advertise PC Analytics Support）]：PC 分析サポートを有効にします。

ステップ 14 （任意）[詳細設定（Advanced）]で、[最大クライアント数（Max Clients）] をクリックし、以下のフィールドにデータを入力します。

- [WLANごと（Per WLAN）]：WLAN ごとのクライアント接続の最大数を入力します。

  有効な範囲は 0 ～ 32000 です。デフォルト値は 0 です
- [WLANでのAPごと（Per AP Per WLAN）]：WLAN で設定可能な AP ごとのクライアント接続の最大数を入力します。

有効な範囲は 0 ～ 1200 です。デフォルト値は 0 です

- [WLANでのAP無線ごと（Per AP Radio Per WLAN）]：WLAN で設定可能な AP 無線ごとのクライアント接続の最大数を入力します。

  有効な範囲は 0 ～ 500 です。デフォルト値は 200 です。

ステップ 15 [詳細設定（Advanced）] で、[オフチャネルスキャン（Off Channel Scan）] をクリックして、次の設定を行います。

a) [遅延優先順位（Defer Priority）] で、必要な RRM オフチャネルスキャン遅延優先順位値の横にあるチェックボックスをオンにします。

b) [Scan Defer Time (msec)] フィールドに、必要なスキャン遅延時間をミリ秒単位で入力します。

有効な範囲は 0 ～ 60000 です。デフォルト値は 100 です。

ステップ 16 [詳細設定（Advanced）] で、[その他（Miscellaneous）] をクリックして、次の設定を行います。

a) [Peer-to-Peer Blocking] ドロップダウンリストから、WLAN のピアツーピアブロッキングの設定を選択します。

b) 必要なオプションを使用して、対応する設定を行います。

- [カバレッジホール検出（Coverage Hole Detection）]：ワイヤレスコントローラ でカバレッジホール検出（CHD）を有効にします。
- [Fastlane+ (ASR)]：WLAN で高度なスケジューリング要求処理を有効にします。
- [Aironet IE]：Cisco Compatible Extensions オプションのサポートを有効にし、WLAN で Aironet 情報要素（IE）のサポートを設定します。
- [AP名のアドバタイズ（Advertise AP Name）]：WLAN の AP 名のステータスをアドバタイズします。
- [LAA（RCM）クライアントを拒否（Deny LAA (RCM) Clients）]：ローカルで管理されているアドレス（ランダム MAC アドレス）へのクライアントの接続を拒否します。
- [IP送信元ガード（P Source Guard）]：IP 送信元ガード（IPSG）を有効にします。

  IPSG は、ワイヤレスコントローラが認識していない送信元 IP アドレスを持つパケットを転送することを防ぐレイヤ 2 セキュリティ機能です。
- [遅延測定に関するアナウンス（Latency Measurements Announcements）]：現在の無線帯域が過負荷状態になった場合に、クライアントが遅延の少ない無線帯域に移動できるように、無線帯域に関する遅延情報を提供します。
- [マルチキャストバッファ（Multicast Buffer）]：WLAN の 802.11a 無線のマルチキャストバッファ調整モードを設定します。

  このチェックボックスをオンにする場合は、[Multicast Buffer Value] フィールドに値を入力します。

  有効な範囲は 30 ～ 60 です。
- [Opportunistic Key Caching（OKC）]：Opportunistic Key Caching を有効にします。

OKC を使用すると、ワイヤレスクライアントと WLAN インフラストラクチャは、複数の AP 間でローミングしている場合でも、この WLAN とのクライアント アソシエーションの存続期間中、1 つのペアワイズマスターキー（PMK）のみをキャッシュできます。

- [負荷分散（Load Balance）]：WLAN の負荷分散を有効にします。
- [メディアストリームマルチキャストダイレクト（Media Stream Multicast-Direct）]：WLAN 用の信頼性の高いマルチキャストストリーム配信。
- [802.11ac MU-MIMO]：WLAN で 802.11ac MU-MIMO を設定します。
- [ユニバーサル管理（Universal Admin）]：802.1X、WPA、または WPA2 対応 WLAN でユニバーサル管理モードを有効にします。
- [MBO]：Wi-Fi Alliance Agile Multiband（MBO）サポートを有効にします。

（注） WPA2 対応 WLAN の MBO の場合、[Protected Management Frame (802.11w)] を [Required] または [Optional] に設定する必要があります。

- [Wi-Fi からセルラーへのステアリング（Wi-Fi to Cellular Steering）]：WLAN で Wi-Fi からセルラーへのステアリングを有効にします。

  Wi-Fi からのセルラーステアリングを有効にするには、MBO を有効にする必要があります。

c) （任意） [Wi-Fi Direct Client] ドロップダウンリストから、WLAN の Wi-Fi Direct 関連ポリシーを選択します。

d) （任意） 必要なチェックボックスをオンにして、対応する設定を行います。

- [RSN IE Lenを無視（Ignore RSN IE Len）]：Robust Secure Network Information Element（RSN IE）検証を有効にします。
- [ローミングクライアントのリアンカー（RE Anchor Roam Clients）]：ローミング音声クライアントのリアンカーポリシーを設定します。
- [静的IPトンネリング（Static IP Tunneling）]：WLAN で静的 IP クライアントトンネリングのサポートを有効にします。
- [UAPSD準拠（UAPSD Compliant）]：WLAN の Wi-Fi マルチメディア（WMM）不定期自動省電力配信（U-APSD）準拠クライアントのサポートを有効にします。

e) [Fine Timing Measurementレスポンダーの有効化（Enable Fine Timing Measurement Responder）] トグルボタンを使用して、Fine Timing Measurement（FTM）レスポンダーとして機能するように AP を設定します。

このオプションは、ロケーションベースのサービスに使用されます。これにより、互換性のあるクライアントは AP からの距離を測定して、正確な屋内位置を特定できます。

f) [APの場所をアドバタイズ（Advertise AP Location）] トグルボタンを使用して、ビーコンおよびプローブ応答フレームで AP の物理的な場所をブロードキャストします。

クライアントおよびロケーションベースのサービスは、この情報を使用して、デバイスの位置情報とナビゲーションの精度を向上できます。

g) [WMMポリシー（WMM Policy）] ドロップダウンリストから、ポリシーのオプションを選択します。
h) [mDNSモード（mDNS Mode）] ドロップダウンリストから、mDNS 動作モードを選択します。
i) [DTIM期間（ビーコン間隔）（DTIM Period (in Beacon Intervals)）] の [5 GHz帯域（5 GHz Band）] および [2.4 GHz帯域（2.4 GHz Band）] フィールドに、対応する Delivery Traffic Indication Map（DTIM）期間を入力します。

有効な範囲は 1 ～ 255 です。デフォルト値は 1 です。これらのフィールドは、各 802.11 ネットワークの WLAN ごとの DTIM 設定を表します。

ステップ 17 [Review and Provision] をクリックします。

ステップ 18 ワイヤレスコントローラ がライセンス要件を満たしていない AP を管理している場合、Catalyst Center は詳細を示すダイアログボックスを表示します。ダイアログボックスで、必要なオプションを選択します。

オプション	説明
ライセンス マネージャ	[License Manager] ウィンドウを開いて、対応するライセンスを有効にします。 ライセンスを有効にするには、『*Cisco Catalyst Center Administrator Guide*』の「Manage Licenses」を参照してください。
[デバイスプロビジョニングに進む（Continue to device provision）]	デバイスのプロビジョニングを続行します。 （注） ライセンス要件を満たしていない AP は、ワールドワイドセーフモード（WWSM）になります。
Cancel	ダイアログボックスを閉じます。

ステップ 19 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 20 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のポリシープロファイルの作成

ワイヤレスコントローラ のポリシープロファイルを作成してプロビジョニングするには、次の手順を実行します。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、 で [SSID] を展開して [ポリシープロファイル（Policy Profiles）] をクリックします。

ステップ 4 [Add] をクリックします。

ステップ 5 [ポリシープロファイルの作成（Create Policy Profile）] スライドインペインの [一般（General）] タブで、必要な設定を完了します。

a) [ポリシープロファイル名（Policy Profile Name）] フィールドに、ポリシープロファイルの一意の名前を入力します。

ポリシープロファイル名には最大32文字を含めることができます。Catalyst Center では、ポリシープロファイル名の先頭または末尾にスペースを含めることはできません。

b) （任意） [Description] フィールドに、説明を入力します
c) トグルボタンを使用して必要な設定を有効または無効にします。

トグルボタン	説明
Status	ポリシープロファイルを有効または無効にします。
IP MAC バインディング	IP-MAC アドレスバインディング作成のサポートに対する制御を設定します。
Passive Client	ポリシーのパッシブ クライアント サポートを有効または無効にします。
暗号化トラフィック分析	WLAN で暗号化トラフィック分析機能を有効にします。

d) [WLANスイッチングポリシー（WLAN Switching Policy）] で、トグルボタンを使用して必要な設定を有効または無効にします。

- **[Central Switching]**
- **[Central DHCP]**（ローカルでスイッチされるクライアント用）
- **[Central Authentication]**

- **[Flex NAT/PAT]**

（注） このオプションを有効にする前に、必要なローカルスイッチング、中央 DHCP、IPv4 DHCP を有効にする必要があります。

e) （任意）[CTSポリシー（CTS Policy）] で、必要な Cisco TrustSec（CTS）ポリシーを設定します。

- [インラインタギング（Inline Tagging）] チェックボックスをオンにして、クライアントのインラインタギングを有効にします。
- [SGACL適用（SGACL Enforcement）] チェックボックスをオンにして、デバイスにおける CTS ポリシーのセキュリティグループ ACL（SGACL）の適用を有効にします。
- [Default SGT] フィールドに、デフォルトのセキュリティグループタグ（SGT）値を入力します。

  有効な範囲は 2 ～ 65519 です。デフォルト値は 2 です。

ステップ 6 （任意）[アクセスポリシー（Access Policies）] をクリックし、必要なアクセスポリシーを設定します。

a) 対応する設定を有効にするには、必要なチェックボックスをオンにします。

b) [WLANローカルプロファイリング（WLAN Local Profiling）] の [ローカルサブスクライバポリシー名（Local Subscriber Policy Name）] フィールドに、ポリシーマップの名前を入力します。

ポリシーマップの作成については、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のポリシーマップの作成 （1094 ページ）」を参照してください。

c) [VLAN]で必要な設定を完了します。

- [VLAN/VLANグループ（VLAN/VLAN Group）] フィールドに、VLAN または VLAN グループを検索するテキストを入力します。ドロップダウンリストから、VLAN または VLAN グループを選択します。
- [Multicast VLAN] フィールドに、WLAN に関連付けられているマルチキャスト VLAN ID を入力します。

  有効な範囲は 1 ～ 4094 です。
- [OSEN暗号化VLAN（OSEN Encryption VLAN）] フィールドに、この WLAN で OSEN 暗号化トラフィックに使用する VLAN ID を入力します。

  この VLAN には最大 8 文字を含めることができます。

d) [WLAN ACL] で、次の設定を完了します。

- [IPv4 ACL] ドロップダウンリストから、IPv4 ACL を選択します。

  ACL の作成については、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の IPv4 ACL の作成 （940 ページ）」を参照してください。
- [IPv6 ACL] ドロップダウンリストから、IPv6 ACL を選択します。

ACL の作成については、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の IPv6 ACL の作成 （949 ページ）」を参照してください。

- [レイヤ2ACL（Layer 2 ACL）] フィールドに、WLAN のレイヤ 2 ACL の名前を入力します。

e) [URLフィルタ（URL Filters）] で、対応するドロップダウンリストから事前認証および認証後 URL フィルタを選択します。

（注） 拡張 URL フィルタは、FlexConnect ローカルスイッチングを展開する場合にのみ使用することを推奨します。

URL フィルタの作成については、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の基本的な URL フィルタの作成 （962 ページ）」と「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの拡張 URL フィルタの作成 （964 ページ）」を参照してください。

ステップ 7 [QoSとAVC（QoS and AVC）] をクリックし、必要な設定を完了します。

a) [自動QoS（Auto QoS）] ドロップダウンリストから、WLAN の auto-QoS モードを選択します。

b) （任意） [Re-anchor Classmap Name] フィールドに、選択的リアンカーリングのプロトコルを含むクラスマップの名前を入力します。

c) （任意） [NBARプロトコル検出（NBAR Protocol Discovery）] チェックボックスをオンにし、WLAN の Network Based Application Recognition（NBAR）プロトコル検出を有効にします。

d) （任意） [QBSS負荷（QBSS Load）] チェックボックスをオンにし、QoS 拡張 BSS 負荷 IE をアドバタイズします。

e) （任意） auto-QoS モード [なし（None）] を選択した場合は、[QoS SSIDポリシー（QoS SSID Policy）] と [QoSクライアントポリシー（QoS Client Policy）] の [出力（Egress）] および [入力（Ingress）] ドロップダウンリストから QoS SSID ポリシー名を選択します。

QoS ポリシーの作成については、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の QoS ポリシーの作成 （1097 ページ）」を参照してください。

f) [フローモニターIPv4（Flow Monitor IPv4）] と [フローモニターIPv6（Flow Monitor IPv6）] の [出力（Egress）] および [入力（Ingress）] ドロップダウンリストからフローモニターを選択します。

フローモニターの作成については、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのフローモニターの作成 （1105 ページ）」を参照してください。

ステップ 8 [SIP-CAC] で、必要なチェックボックスをオンにして対応する設定を有効にします。

チェックボックス	説明
コール スヌーピング	ポリシープロファイルにマッピングされた WLAN のコールスヌープを有効にします。 （注） コールスヌープを有効にする場合は、Platinum SSID ポリシーを設定する必要があります。

チェックボックス	説明
Send 486 Busy	SIP CAC が 486 ビジーを送信できるようにします。
Send Disassociate	SIP CAC 送信の関連付け解除を有効にします。

ステップ 9 （任意）[モビリティ（Mobility）] をクリックし、モビリティアンカーを設定します。

a) [モビリティアンカー（Mobility Anchors）] で必要な設定を完了します。

- ポリシーにマッピングされた WLAN がアンカー WLAN であることを示すには、[エクスポートアンカー（Export Anchor）] チェックボックスをオンにします。

（注） このオプションを有効にすると、中央スイッチングが有効になります。リンクローカルブリッジング機能を無効にする必要があります。

- 静的 IP モビリティを有効にするには、[静的IPモビリティ（Static IP Mobility）] チェックボックスをオンにします。

（注） 静的 IP モビリティとモビリティアンカーを同時に有効にすることはできません。

b) [アンカー（Anchors）] で、モビリティアンカーを追加または削除します。

（注） このアクションにより、有効になっている WLAN が一時的に無効になり、一部のクライアントの接続が失われます。

実行する操作	結果
アンカーの追加	**1.** [Add] をクリックします。 **2.** [追加（Add）] ダイアログボックスで次の操作を実行します。 • [アンカーIP（Anchor IP）] ドロップダウンリストからモビリティアンカー IP を選択します。 • [Anchor Priority] ドロップダウンリストから、モビリティアンカーの優先順位を選択します。 **3.** [Save] をクリックします。

実行する操作	結果
アンカーの編集	**1.** アンカー IP の横にあるチェックボックスをオンにします。 **2.** [Actions] にカーソルを合わせて [Edit] を選択します。 **3.** 必要な設定を編集します。 **4.** [Save] をクリックします。
アンカーの削除	**1.** アンカー IP の横にあるチェックボックスをオンにします。 **2.** [Actions] にカーソルを合わせて [Delete] を選択します。 **3.** ダイアログボックスで、**Yes** をクリックします。

ステップ 10 [詳細設定（Advanced）] で、[WLANスケジューラ（WLAN Scheduler）] をクリックして WLAN のスケジューラを設定します。

実行する操作	結果
WLAN スケジューラを追加する	**1.** [Add] をクリックします。 **2.** [WLANスケジューラの追加（Add Wlan Scheduler）] ダイアログボックスで次の操作を実行します。 • [予定表プロファイル名（Calendar Profile Name）] ドロップダウンリストから、予定表プロファイルを選択します。 • [クライアントセッションの無効化（Client Session Disable）] トグルボタンを使用し、予定表プロファイルに基づいてクライアントセッションを有効または無効にします。 • [WLANの有効化（Wlan Enable）] トグルボタンを使用し、予定表プロファイルに基づいてポリシープロファイルを有効または無効にします。 **3.** [Save] をクリックします。
WLAN スケジューラを編集する	**1.** WLAN スケジューラの横にあるチェックボックスをオンにします。 **2.** [Actions] にカーソルを合わせて [Edit] を選択します。 **3.** 必要な設定を編集します。 **4.** [Save] をクリックします。

実行する操作	結果
WLAN スケジューラを削除する	1. WLANスケジューラの横にあるチェックボックスをオンにします。 2. [Actions] にカーソルを合わせて [Delete] を選択します。 3. ダイアログボックスで、**Yes** をクリックします。

ステップ 11 [詳細設定（Advanced）] で [WLANタイムアウト（WLAN Timeout）] をクリックし、クライアントの WLAN タイムアウトを設定します。

a) [Session Timeout (sec)] フィールドに、クライアントセッションタイムアウトを秒単位で入力します。

有効な範囲は 0 ～ 86400 です。デフォルト値は 28,800 です。

b) [Idle Timeout (sec)] フィールドに、アイドルタイムアウトの期間を秒単位で入力します。

有効な範囲は 15 ～ 100000 です。デフォルト値は 300 です。

c) [Idle Threshold (bytes)] フィールドに、アイドルしきい値をバイト単位で入力します。

デフォルト値は 0 です

d) [Client Exclusion Timeout] フィールドに、クライアント除外タイムアウト値を入力します。

0 ～ 2147483647 の範囲の値を指定できます。デフォルト値は 60 です。

e) （任意） ゲスト LAN のセッションタイムアウトを有効にするには、[ゲストLANのセッションタイムアウト（Guest LAN Session Timeout）] チェックボックスをオンにします。

f) （任意） WLAN のクライアント除外を有効にするには、[クライアント除外（Client Exclusion）] チェックボックスをオンにします。

ステップ 12 （任意） [詳細設定（Advanced）] で [WLAN Flexポリシー（WLAN Flex Policy）] をクリックし、WLAN Flex ポリシーを設定します。

a) [VLAN中央スイッチング（VLAN Central Switching）] チェックボックスをオンにし、VLAN 中央スイッチングを設定します。

（注） AAA オーバーライドが無効の場合、VLANベースの中央スイッチングはサポートされません。

b) [Split MAC ACL] フィールドに、スプリット MAC ACL 名を入力します。

ACL の作成については、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の IPv4 ACL の作成（940 ページ）」を参照してください。

ステップ 13 （任意） [詳細設定（Advanced）] で [AAAポリシー（AAA Policy）] をクリックし、AAA ポリシーを設定します。

a) AAA オーバーライドを有効にするには、[AAAオーバーライド（AAA Override）] チェックボックスをオンにします。

b) AAA オーバーライドを有効にする場合は、[NAC状態（NAC State）] チェックボックスを使用してネットワーク アドミッション コントロール（NAC）を有効または無効にします。

このチェックボックスをオンにする場合は、[NACタイプ（NAC Type）] ドロップダウンリストからオプションを選択します。

c) オーバーライド VLAN が使用できない場合にポリシープロファイル VLAN へのフォールバックを有効にするには、[VLANフォールバック（VLAN Fallback）] チェックボックスをオンにします。

d) [AAA Policy Name] ドロップダウンリストから、AAA ポリシーを選択します。

AAA ポリシーの作成については、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の AAA ポリシーの作成 （939 ページ）」を参照してください。

e) [Accounting List] ドロップダウンリストから、アカウンティングリストを選択します。

アカウンティングリストの作成については、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのアカウンティング方式リストの作成 （931 ページ）」を参照してください。

f) 中間アカウンティングメッセージを有効にするには、[中間アカウンティング（Interim Accounting）] チェックボックスをオンにします。

ステップ 14 （任意） [詳細設定（Advanced）] で [DHCP] をクリックし、ワイヤレスクライアントの DHCP を設定します。

a) WLAN 上のすべてのクライアントに DHCP を適用するには、[IPv4 DHCPが必要（IPv4 DHCP Required）] チェックボックスをオンにします。

（注） [Flex NAT/PAT] オプションを有効にする前に、このオプションを有効にする必要があります。

b) [DHCP Server IP Address] フィールドに、WLAN の IPv4 DHCP サーバーを入力します。

c) [DHCPサーバーVRF（DHCP Server VRF）] ドロップダウンリストから、IPv4 DHCP サーバーの VRF 名を選択します。

VRF インターフェイスの作成については、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの VRF インターフェイスの作成 （1134 ページ）」を参照してください。

d) [DHCPオプションの無効化（Disable DHCP Option）] トグルボタンを使用して、この WLAN に関する DHCP 要求の追加 DHCP オプションの包含を有効または無効にします。

e) 対応する DHCP オプション 82 の設定を有効にするには、必要なチェックボックスをオンにします。

ステップ 15 （任意） [詳細設定（Advanced）] で [DNS レイヤセキュリティ（DNS Layer Security）] を クリックし、DNS レイヤセキュリティを設定します。

a) [DNS Layer Security Parameter Map] フィールドに、マップ名を入力します。

アカウンティングリストの作成については、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのアカウンティング方式リストの作成 （931 ページ）」を参照してください。

b) [Flex DNS トラフィックリダイレクト（Flex DNS Traffic Redirect）] ドロップダウンリストから、Cisco Umbrella DNA トラフィック リダイレクト オプションを選択します。

c) DNS DHCP オプションを有効にするには、[DNSのFlex DHCPオプション（Flex DHCP Option for DNS）] チェックボックスをオンにします。

ステップ 16 （任意）[詳細設定（Advanced）] で[その他（Miscellaneous）] をクリックし、ユーザー定義（プライベート）ネットワーク、Air Time Fairness などのその他のワイヤレスプロファイル設定を構成します。

a) [mDNS Service Policy] フィールドに、サービスポリシーの名前を入力します。

サービスポリシー名は最大 64 文字で指定できます。サービスポリシーの作成については、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の mDNS サービスポリシーの作成（1072 ページ）」を参照してください。

b) [Hotspot Server] ドロップダウンリストからサーバーを選択します。

c) 対応する設定を有効にするには、必要なチェックボックスをオンにします。

- [リンクローカルブリッジング（Link Local Bridging）]：リンクローカルブリッジングを有効にします。

（注） リンクローカルブリッジングを有効にする場合は、WLAN モビリティポリシーアンカーを無効にする必要があります。

- [マルチキャストフィルタ（Multicast Filter）]：すべてのマルチキャスト ダウンストリーム パケットをドロップするフィルタを有効にします。
- [レートなし（Rate None）]：クライアントの Address Resolution Protocol（ARP）レート制限を有効にします。

d) [Burst Interval] フィールドに、バースト間隔を秒単位で入力します。

有効な範囲は 3 ～ 255 です。デフォルト値は 5 です。

e) [Rate Pps] フィールドに、許可される ARP パケットレートの値を入力します。

有効な範囲は 15 ～ 1500 です。デフォルト値は 100 です。

f) [L3アクセス（L3 Access）] トグルボタンを使用して、レイヤ 3 アクセスを有効または無効にします。

g) [ユーザー定義（プライベート）ネットワーク（User Defined (Private) Network）] で、対応する設定を有効にするために必要なチェックボックスをオンにします。

- [ステータス（Status）]：ユーザー定義（プライベート）ネットワークを有効にします。
- [ユニキャストのドロップ（Drop Unicast）]：ユーザー定義（プライベート）ネットワークのユニキャストトラフィックをドロップするようにアクションを設定します。

h) [Air Time Fairness Policies] の [2.4 GHz Policy] および [5 GHz Policy] ドロップダウンリストから、対応するポリシーを選択します。

i) [WGBパラメータ（WGB Parameters）] で必要な設定を完了します。

- ワークグループブリッジ（WGB）ブロードキャストタギングを有効にするには、[ブロードキャストタギング（Broadcast Tagging）] チェックボックスをオンにします。
- クライアント VLAN サポートを有効にするには、[WGB VLAN] チェックボックスをオンにします。
- [外部APへのマルチキャスト転送（Multicast Forwarding for Foreign APs）] トグルボタンを使用して、ゲストまたはモビリティシナリオで外部 AP に接続されているクライアントのマルチキャストトラフィック転送を有効または無効にします。

j) [ポリシープロキシ設定（Policy Proxy Settings）] で必要な設定を完了します。

- ARP プロキシ機能を有効にするには、[ARPプロキシ（ARP Proxy）] チェックボックスをオンにします。
- [IPv6 Proxy] ドロップダウンリストから、IPv6 ネイバー探索（ND）プロキシ機能を選択します。

k) [EoGRE Tunnel Profile] の [Tunnel Profile] ドロップダウンリストからトンネルプロファイルを選択します。

トンネルプロファイルの作成については、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの EoGRE トンネルプロファイルの作成 （1110 ページ）」を参照してください。

ステップ 17 [Review and Provision] をクリックします。

ステップ 18 ワイヤレスコントローラ がライセンス要件を満たしていない AP を管理している場合、Catalyst Center は詳細を示すダイアログボックスを表示します。ダイアログボックスで、必要なオプションを選択します。

オプション	説明
ライセンス マネージャ	[License Manager] ウィンドウを開いて、対応するライセンスを有効にします。 ライセンスを有効にするには、『*Cisco Catalyst Center Administrator Guide*』の「Manage Licenses」を参照してください。
[デバイスプロビジョニングに進む（Continue to device provision）]	デバイスのプロビジョニングを続行します。 （注） ライセンス要件を満たしていない AP は、ワールドワイドセーフモード（WWSM）になります。
Cancel	ダイアログボックスを閉じます。

ステップ 19 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。

- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 20 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のリモート LAN プロファイルの作成

この手順を使用して、ワイヤレスコントローラ のリモート LAN（RLAN）プロファイルを作成し、プロビジョニングします。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[SSID] を展開し、[リモート LAN プロファイル（Remote LAN Profiles）] をクリックします。

ステップ 4 [Add] をクリックします。

ステップ 5 [リモートLANプロファイルの作成（Create Remote LAN Profile）] スライドインペインの [一般（General）] タブで、次の設定を完了します。

a) [RLANプロファイル名（RLAN Profile Name）] フィールドに、RLANプロファイルの一意の名前を入力します。

（注） RLAN プロファイル名が既存の WLAN プロファイル名と一致していないことを確認してください。そうでない場合、RLAN プロファイルの作成タスクは失敗します。

b) [RLAN ID] フィールドに、RLAN プロファイル ID を入力します。

有効な範囲は 1 ～ 128 です。デフォルト値は 1 です。

c) [ステータス（Status）] トグルボタンを使用して、RLAN プロファイルを有効または無効にします。

d) （任意） [Client Association Limit] フィールドに、RLAN ごとのクライアント接続の最大数を入力します。デフォルト値は 0 です

e) [mDNS Mode] ドロップダウンリストから、RLAN のモードを選択します。

ステップ 6 [セキュリティ（Security）] で [レイヤ 2（Layer 2）] をクリックし、RLAN のレイヤ 2 セキュリティポリシーを設定します。

a) （任意） [802.1X] チェックボックスをオンにして、802.1X を有効にします。

b) （任意） [MAC Filtering] ドロップダウンリストからオプションを選択します。

認証リストの作成については、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の認証方式リストの作成 （929 ページ）を参照してください。

c) （任意） [Authentication List] ドロップダウンリストからタイプ [DOT1x] の認証リストを選択します。

認証リストの作成については、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の認証方式リストの作成 （928 ページ）を参照してください。

d) [Fallback Mechanism] ドロップダウンリストから、RLAN フォールバック認証タイプを選択します。

e) （任意） [EAPアイデンティティ要求の再試行ステータス（EAP-Identity-Request Retries Status）] チェックボックスをオンにして、EAP アイデンティティ要求の再試行設定を有効にします。

- [EAP-Identity-Request Max Retries] フィールドに、EAP アイデンティティ要求の最大再送信回数を入力します。

  有効な範囲は、1 ～ 20 です。

- [EAP-Identity-Request Timeout (sec)] フィールドに、EAP アイデンティティ要求のタイムアウト値を秒単位で入力します。

  有効な範囲は 1 ～ 120 です。

f) （任意） [EAP要求の再試行ステータス（EAP-Request Retries Status）] チェックボックスをオンにして、EAP 要求の再試行設定を有効にします。

- [EAP-Request Max Retries] フィールドに、EAP 要求の最大再送信回数を入力します。

  有効な範囲は、1 ～ 20 です。

- [EAP-Request Timeout (sec)] フィールドに、EAP 要求のタイムアウト値を秒単位で入力します。

  有効な範囲は 1 ～ 120 です。

ステップ 7 （任意） [セキュリティ（Security）] で [レイヤ 3（Layer 3）] をクリックし、RLAN のレイヤ 3 ポリシーと ACL を設定します。

a) [Web認証（Web Auth）] チェックボックスをオンにして、セキュリティ Web 認証を有効にします。

（注） Web 認証と 802.1X は同時に有効にできません。

b) [Web Auth Parameter Map] ドロップダウンリストから、マップを選択します。

Web 認証プロファイルの作成については、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの Web 認証プロファイルの作成 （970 ページ）」を参照してください。

RLAN プロファイルを Web 認証に関連付けると、 Web ポータルを介したユーザー認証が可能になり、セキュリティが強化され、ワイヤレスネットワークに対するアクセス制御が向上します。

c) [Authentication List] ドロップダウンリストからタイプ [login] の認証リストを選択します。

認証リストの作成については、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の認証方式リストの作成 （928 ページ）を参照してください。

d) [事前認証ACL（Preauthentication ACL）] で、対応するドロップダウンリストから必要な ACL を選択します。

- [IPv4]（IPv4 ACL の作成については、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの IPv4 ACL の作成 （940 ページ）」を参照してください）
- [IPv6]（IPv6 ACL の作成については、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの IPv6 ACL の作成 （949 ページ）」を参照してください）

ステップ 8 （任意） [セキュリティ（Security）] で、[AAA] をクリックし、[ローカルEAP認証（Local EAP Authentication）] チェックボックスをオンにして、RLAN で EAP プロファイルを有効にします。

このチェックボックスをオンにする場合は、[EAP Profile Name] ドロップダウンリストから EAP プロファイル名を選択します。

RLAN プロファイルをローカル EAP に関連付けると、ワイヤレスネットワーク環境でのセキュリティ、アクセス制御、コンプライアンス、ネットワークパフォーマンス、ユーザー管理、障害対応、および拡張性が向上します。

ステップ 9 [Review and Provision] をクリックします。

ステップ 10 ワイヤレスコントローラ がライセンス要件を満たしていない AP を管理している場合、Catalyst Center は詳細を示すダイアログボックスを表示します。ダイアログボックスで、必要なオプションを選択します。

オプション	説明
ライセンス マネージャ	[License Manager] ウィンドウを開いて、対応するライセンスを有効にします。 ライセンスを有効にするには、『*Cisco Catalyst Center Administrator Guide*』の「Manage Licenses」を参照してください。
[デバイスプロビジョニングに進む（Continue to device provision）]	デバイスのプロビジョニングを続行します。 （注） ライセンス要件を満たしていない AP は、ワールドワイドセーフモード（WWSM）になります。
Cancel	ダイアログボックスを閉じます。

ステップ 11 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 12 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のリモート LAN ポリシーの作成

この手順を使用して、ワイヤレスコントローラ のリモート LAN (RLAN) ポリシーを作成し、プロビジョニングします。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、 [SSID] を展開し、[リモートLANポリシー（Remote LAN Policies）] をクリックします。

ステップ 4 [Add] をクリックします。

ステップ 5 [リモートLANポリシーの作成（Create Remote LAN Policy ）] スライドインペイン の [一般（General）] タブで、必要な設定を完了します。

a) [RLAN Policy Name] フィールドに RLAN ポリシーの名前を入力します。

   RLAN ポリシー名は最大 32 文字で指定できます。

b) （任意） [Description] フィールドに、説明を入力します
c) [ステータス（Status）] トグルボタンを使用して、RLAN ポリシーを有効または無効にします。
d) （任意） [PoE] チェックボックスをオンにして、Power over Ethernet（PoE）を有効にします。
e) [電力レベル（Power Level）] ドロップダウンリストから、AP PoE ポートの電力レベルを選択します。
f) [RLANスイッチングポリシー（RLAN Switching Policy）] で、[セントラルスイッチング（Central Switching）] と [セントラルDHCP（Central DHCP）] トグルボタンを使用して、対応する設定を有効または無効にします。

ステップ 6 [アクセスポリシー（Access Policies）] をクリックし、必要な設定を完了します。

a) （任意） [事前認証（Pre-Authentication）] チェックボックスをオンにして、事前認証を有効にします。

b) （任意） [VLAN] ドロップダウンリストから、VLAN を検索するテキストを入力します。ドロップダウンリストから [VLAN] を選択します。

VLAN の作成については、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の VLAN プロファイルの作成 （1126 ページ）を参照してください。

c) [ホストモード（Host Mode）] ドロップダウンリストから、RLAN のホストモードを選択します。

d) （任意） [RLAN ACL] で、ドロップダウンリストから [IPv4 ACL] と [IPv6 ACL] を選択します。

- IPv4 ACL（IPv4 ACL を作成するには、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の IPv4 ACL の作成 （940 ページ）」を参照してください）
- IPv6 ACL（IPv6 ACL を作成するには、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の IPv6 ACL の作成 （949 ページ）」を参照してください）

ステップ 7 [詳細設定（Advanced）] をクリックし、必要な設定を完了します。

a) [違反モード（Violation Mode）] ドロップダウンリストから、RLAN の違反モードを選択します。

b) （任意） [Session Timeout (sec)] フィールドに、セッションタイムアウトの値を秒単位で入力します。

有効な範囲は 0 ～ 86400 です。デフォルト値は 28,800 です。

（注） セッションタイムアウトを無効にするには、0 を入力します。

c) （任意） [mDNSサービスポリシー（mDNS-AP Service Policy）] ドロップダウンリストから、mDNS サービス ポリシー名を選択します。

mDNS サービスポリシーの作成については、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の mDNS サービスポリシーの作成 （1072 ページ）を参照してください。

d) （任意） [ユーザー定義（プライベート）ネットワーク（User Defined (Private) Network）] で、対応する設定を有効にするために必要なチェックボックスをオンにします。

- [ステータス（Status）] : ユーザー定義（プライベート）ネットワークを有効にします。
- [ユニキャストのドロップ（Drop Unicast）] : ユーザー定義（プライベート）ネットワークのユニキャストトラフィックをドロップするようにアクションを設定します。

e) （任意） [AAAポリシー（AAA Policy）] で必要な設定を完了します。

- AAA オーバーライドを有効にするには、[AAAオーバーライド（AAA Override）] チェックボックスをオンにします。
- [AAA Policy Name] ドロップダウンリストから、AAA ポリシーを選択します。

AAA ポリシーの作成については、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の AAA ポリシーの作成 （939 ページ）を参照してください。

- [Accounting List] ドロップダウンリストから、アカウンティングリストを選択します。

  アカウンティングリストの作成については、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のアカウンティング方式リストの作成 （931 ページ）を参照してください。

f) （任意） [スプリットトンネル（Split Tunnel）] で、必要な設定を完了します。

- [ステータス（Status）] チェックボックスをオンにして、スプリットトンネルを有効にします。
- [ACL] ドロップダウンリストから、ACL を選択します。

  IPv4 ACL の作成については、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の IPv4 ACL の作成 （940 ページ）を参照してください。

g) （任意） [除外リスト（Exclusionlist）] で、必要な設定を完了します。

- クライアント除外を無効にするには、[ステータス（Status）]チェックボックスをオフにします。
- [Exclusionlist Timeout] フィールドに、クライアントを除外する時間を入力します。

  0 ～ 2147483647 の範囲の値を指定できます。デフォルト値は 60 です。

h) （任意） [DHCP] で、必要な設定を完了します。

- リモート LAN 上のすべてのクライアントに DHCP を強制するには、[IPv4 DHCPが必要（IPv4 DHCP Required）] チェックボックスをオンにします。
- [DHCP Server IP Address] フィールドに、リモート LAN の IPv4 DHCP サーバーを入力します。
- [DHCPサーバーVRF（DHCP Server VRF）] ドロップダウンリストから、リモート LAN の IPv4 DHCP サーバー VRF 名を選択します。

i) [その他（Miscellaneous）] で、対応する設定を有効にするために必要なチェックボックスをオンにします。

チェックボックス	説明
[ARPレートなし（ARP Rate None）]	クライアントの Address Resolution Protocol（ARP）レート制限を有効にするには、このチェックボックスをオンにします。 このチェックボックスをオンにする場合は、次の設定を行います。 • [ARPレートPPS（ARP Rate PPS）] フィールドに、許可される ARP パケットレートの値を入力します。 有効な範囲は 15 ～ 1500 です。デフォルト値は 100 です。 • [ARP Burst Interval] フィールドに、バースト間隔を秒単位で入力します。 有効な範囲は 3 ～ 255 です。デフォルト値は 5 です。

チェックボックス	説明
[NDPレートなし（NDP Rate None）]	クライアントのネイバー探索プロトコル（NDP）レート制限を有効にするには、このチェックボックスをオンにします。 このチェックボックスをオンにする場合は、次の設定を行います。 • [NDPレート PPS（NDP Rate PPS）] フィールドに、許可されるNDP パケットレートの値を入力します。 有効な範囲は 15 ～ 1500 です。デフォルト値は 100 です。 • [NDP Burst Interval] フィールドに、バースト間隔を秒単位で入力します。 有効な範囲は 3 ～ 255 です。デフォルト値は 5 です。

ステップ 8 [Review and Provision] をクリックします。

ステップ 9 ワイヤレスコントローラ がライセンス要件を満たしていない AP を管理している場合、Catalyst Center は詳細を示すダイアログボックスを表示します。ダイアログボックスで、必要なオプションを選択します。

オプション	説明
ライセンス マネージャ	[License Manager] ウィンドウを開いて、対応するライセンスを有効にします。 ライセンスを有効にするには、『*Cisco Catalyst Center Administrator Guide*』の「Manage Licenses」を参照してください。
[デバイスプロビジョニングに進む（Continue to device provision）]	デバイスのプロビジョニングを続行します。 （注） ライセンス要件を満たしていないAPは、ワールドワイドセーフモード（WWSM）になります。
Cancel	ダイアログボックスを閉じます。

ステップ 10 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 11 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のポリシータグの作成

ワイヤレスコントローラ に関連付けられている AP のポリシータグを作成してプロビジョニングするには、次の手順を実行します。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。

b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。

c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。

b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、で、[SSID] を展開して [ポリシータグ（Policy Tags）] をクリックします。

ステップ 4 [Add] をクリックします。

ステップ 5 [ポリシータグの作成（Create Policy Tags）] スライドインペインの [タグ名（Tag Name）] フィールドに、ポリシータグの一意の名前を入力します。

ステップ 6 （任意） [Description] フィールドに、説明を入力します

ステップ 7 （任意） [WLANプロファイルからポリシープロファイルへのマッピング（WLAN Profile - Policy Profile Mapping）] で、WLAN プロファイルからポリシープロファイルへのマッピングを設定します。

実行する操作	結果
WLAN プロファイルからポリシープロファイルへのマッピングを追加する	**1.** [Add] をクリックします。 **2.** [WLAN Profile] ドロップダウンリストから、WLAN プロファイルを選択します。 **3.** [Policy Profile] ドロップダウンリストから、ポリシープロファイルを選択します。 **4.** [Save] をクリックします。
WLAN プロファイルからポリシープロファイルへのマッピングを編集する	**1.** 必要な WLAN プロファイル名の横にあるチェックボックスをオンにします。 **2.** [Actions] にカーソルを合わせて [Edit] を選択します。 **3.** 必要な設定を編集します。 **4.** [Save] をクリックします。

実行する操作	結果
WLAN プロファイルからポリシープロファイルへのマッピングを削除する	**1.** 必要な WLAN プロファイル名の横にあるチェックボックスをオンにします。 **2.** [アクション（Actions）] にカーソルを合わせて [削除（Delete）] を選択します。 **3.** ダイアログボックスで、**Yes** をクリックします。

ステップ 8 （任意）[RLANプロファイルからRLANポリシーへのマッピング（RLAN Profile - RLAN Policy Mapping）] で、RLAN プロファイルから RLAN ポリシーへのマッピングを設定します。

実行する操作	結果
RLAN プロファイルから RLAN ポリシーへのマッピングを追加する	**1.** [Add] をクリックします。 **2.** [Port ID] ドロップダウンリストから、AP の RLAN ポート ID 値を選択します。 **3.** [RLAN Profile] ドロップダウンリストから、RLAN プロファイルを選択します。 **4.** [RLAN Policy Profile] ドロップダウンリストから、RLAN ポリシープロファイルを選択します。 **5.** [Save] をクリックします。
RLAN プロファイルから RLAN ポリシーへのマッピングを編集する	**1.** 必要なポート ID の横にあるチェックボックスをオンにします。 **2.** [Actions] にカーソルを合わせて [Edit] を選択します。 **3.** 必要な設定を編集します。 **4.** [Save] をクリックします。
RLAN プロファイルから RLAN ポリシーへのマッピングを削除する	**1.** 必要なポート ID の横にあるチェックボックスをオンにします。 **2.** [アクション（Actions）] にカーソルを合わせて [削除（Delete）] を選択します。 **3.** ダイアログボックスで、**Yes** をクリックします。

ステップ 9 [Review and Provision] をクリックします。

ステップ 10 ワイヤレスコントローラ がライセンス要件を満たしていない AP を管理している場合、Catalyst Center は詳細を示すダイアログボックスを表示します。ダイアログボックスで、必要なオプションを選択します。

オプション	説明
ライセンス マネージャ	[License Manager] ウィンドウを開いて、対応するライセンスを有効にします。 ライセンスを有効にするには、『*Cisco Catalyst Center Administrator Guide*』の「Manage Licenses」を参照してください。
[デバイスプロビジョニングに進む（Continue to device provision）]	デバイスのプロビジョニングを続行します。 （注） ライセンス要件を満たしていないAPは、ワールドワイドセーフモード（WWSM）になります。
Cancel	ダイアログボックスを閉じます。

ステップ 11 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 12 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の 802.11be プロファイルの設定

次の手順を使用して、ワイヤレスコントローラの802.11beプロファイルを設定または作成し、プロビジョニングします。802.11be プロファイルは、Cisco IOS XE リリース 17.15.1 以降を実行している ワイヤレスコントローラ にのみ適用されます。

Cisco IOS XE リリース 17.18.1 より前のバージョンを実行している ワイヤレスコントローラ では、単一の 802.11be プロファイル（default-dot11be-profile）が使用されます。Cisco IOS XE リリース 17.18.1 以降を実行している ワイヤレスコントローラ は、カスタム 802.11be プロファイルをサポートしています。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。

b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[SSID] を展開し、[802.11be プロファイル（802.11be Profiles）] をクリックします。

ステップ 4 次の該当する設定のいずれかを完了します。

実行する操作	結果
Cisco IOS XE リリース 17.18.1 より前のバージョンを実行しているワイヤレスコントローラの802.11beプロファイルを設定する	**1.** デフォルトの802.11beプロファイルの横にあるオプションボタンをクリックします。 **2.** **[Actions]** にカーソルを合わせ、**[Edit]** をクリックします。
Cisco IOS XE リリース 17.18.1 以降を実行しているワイヤレスコントローラ の 802.11be プロファイルを作成する	[Add] をクリックします。

ステップ 5 [**Profile Name**] フィールドに、Cisco IOS XE リリース 17.18.1 以降を実行しているワイヤレスコントローラの 802.11be プロファイルの一意の名前を入力します。

プロファイル名には最大 32 文字を含めることができます。Catalyst Center では、プロファイル名の先頭と末尾にスペースを含めることはできません。

ステップ 6 （任意） [説明（Description）] フィールドで、説明を更新します。

説明には最大 64 文字を使用できます。

ステップ 7 （任意） 利用可能なトグルボタンを使用して、対応するパラメータを有効または無効にします。

- [ダウンリンクOFDMA（Downlink OFDMA）]：Cisco IOS XE リリース 17.18.1 より前のバージョンを実行している ワイヤレスコントローラ でOFDMA を使用するためのダウンリンク接続を有効にします。
- [アップリンクOFDMA（Uplink OFDMA）]：Cisco IOS XE リリース 17.18.1 より前のバージョンを実行している ワイヤレスコントローラ で OFDMA を使用するためのアップリンク接続を有効にします。
- [ダウンリンクMU-MIMO（Downlink MU-MIMO）]：Cisco IOS XE リリース 17.18.1 より前のバージョンを実行している ワイヤレスコントローラ で MU-MIMO を使用するためのダウンリンク接続を有効にします。
- [アップリンクMU-MIMO（Uplink MU-MIMO）]：Cisco IOS XE リリース 17.18.1 より前のバージョンを実行している ワイヤレスコントローラ で MU-MIMO を使用するためのアップリンク接続を有効にします。

- [OFDMA Multi-RU]：OFDMA を使用した単一ユーザーへの複数リソースユニット（RU）の同時割り当てを有効にします。

（注） Cisco IOS XE リリース 17.18.1 以降を実行している ワイヤレスコントローラ の OFDMA および MU-MIMO を設定するには、WLAN プロファイルの**[詳細設定（Advanced）]**>**[11ax]**タブを使用します。詳細については、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の WLAN プロファイルの作成 （813 ページ）を参照してください。

ステップ 8 （任意） トグルボタンを使用して、Cisco IOS XE リリース 17.18.1 以降を実行している ワイヤレスコントローラ の MLO グループ設定を有効または無効にします。

- [Primary 2.4GHz]：MLO グループで 2.4 GHz 帯域を設定します。
- [Primary 5GHz]：MLO グループで 5 GHz 帯域を設定します。
- [Secondary 5GHz]：MLO グループでセカンダリ 5 GHz 帯域を設定します。
- [Primary 6GHz]：MLO グループで 6 GHz 帯域を設定します。

ステップ 9 [Review and Provision] をクリックします。

ステップ 10 ワイヤレスコントローラ がライセンス要件を満たしていない AP を管理している場合、Catalyst Center は詳細を示すダイアログボックスを表示します。ダイアログボックスで、必要なオプションを選択します。

オプション	説明
ライセンス マネージャ	[License Manager] ウィンドウを開いて、対応するライセンスを有効にします。 ライセンスを有効にするには、『*Cisco Catalyst Center Administrator Guide*』の「Manage Licenses」を参照してください。
[デバイスプロビジョニングに進む（Continue to device provision）]	デバイスのプロビジョニングを続行します。 （注） ライセンス要件を満たしていない AP は、ワールドワイドセーフモード（WWSM）になります。
Cancel	ダイアログボックスを閉じます。

ステップ 11 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 12 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の RF 設定

このセクションでは、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のデバイスごとの RF 設定に関する情報を示します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の RF プロファイルの作成

ワイヤレスコントローラ の RF プロファイルを作成してプロビジョニングするには、次の手順を実行します。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、で、[RF] を展開して [RFプロファイル（RF Profiles）] をクリックします。

ステップ 4 [Add] をクリックします。

ステップ 5 [RFプロファイルの作成（Create RF Profiles）] スライドインペインの [一般（General）] タブで、必要なパラメータを設定します。

a) [RFプロファイル名（RF Profile Name）] フィールドに、RF プロファイルの一意の名前を入力します。

プロファイル名には最大 32 文字を含めることができます。Catalyst Center では、プロファイル名に ? は使用できません。

b) （任意） [Description] フィールドに、説明を入力します
c) [無線帯域（Radio Band）] ドロップダウンリストから、RF プロファイルの無線帯域を選択します。

[6 GHz] を選択した場合は、必要に応じて AP が標準電力モードで動作するようにできます。標準電力モードを有効にするには、[標準電力モードを許可（Allow Standard Power Mode）] チェックボックスをオンにします。

d) [ステータス（Status）] トグルボタンを使用して、RF プロファイルを有効または無効にします。
e) [NDPモード（NDP Mode）] ドロップダウンリストから、動作モードを選択します。

ステップ 6 [802.11] をクリックし、次の手順を実行します。

a) [動作データレート（Operational Data Rates）] で、ドロップダウンリストから対応するデータレートの必要な設定を選択します。

b) 5-GHz および 2.4-GHz 帯域の場合、[802.11n MCS レート（802.11n MCS Rates）] で、必要な変調符号化スキーム（MCS）インデックスのチェックボックスをオンにします。

ステップ 7 [RRM] で、[トラップしきい値（Trap Thresholds）] をクリックして必要な設定を完了します。

a) [Interference (%)] フィールドに、干渉しきい値の割合を入力します。

有効範囲は 0 ～ 100 です。デフォルト値は 10 です。

干渉がこのしきい値を超えると、トラップが生成されます。

b) [Clients] フィールドに、トラップをトリガーする AP 無線ごとのクライアント数のしきい値を入力します。

有効値は 1 ～ 200 です。デフォルト値は 12 です。

c) [Noise (dBm)] フィールドに、ノイズのしきい値を dBm 単位で入力します。

有効な範囲は -127 ～ 0 です。デフォルト値は -70 です。

d) [Utilization (%)] フィールドに、AP が使用する帯域幅のしきい値の割合を入力します。

有効範囲は 0 ～ 100 です。デフォルト値は 80 です。

ステップ 8 [RRM] で、[カバレッジ（Coverage）] をクリックして必要な設定を完了します。

a) [Minimum Client Level (clients)] フィールドに、最小のクライアント例外レベルを入力します。

有効値は 1 ～ 200 です。デフォルト値は 3 です。

b) [Data RSSI Threshold (dBm)] フィールドに、データパケットの受信信号強度表示（RSSI）しきい値を dBm 単位で入力します。

有効な範囲は -90 ～ -60 です。デフォルト値は -80 です。

c) [Voice RSSI Threshold (dBm)] フィールドに、音声パケットの RSSI しきい値を dBm 単位で入力します。

有効な範囲は -90 ～ -60 です。デフォルト値は -80 です。

d) [Exception Level (%)] フィールドに、カバレッジ例外レベルの割合を入力します。

有効な範囲は 1 ～ 100 です。デフォルト値は 25 です。

ステップ 9 [RRM] で、[TPC] をクリックして必要な設定を完了します。

a) [Maximum Power Level (dBm)] フィールドに、送信電力の上限を dBm 単位で入力します。

有効な範囲は -10 ～ 30 です。デフォルト値は 30 です。

802.11 ネットワークの場合、この設定は、伝送パワーコントロール（TPC）が自動モードまたは 1 回実行モードの場合にのみ受け入れられます。

b) [Minimum Power Level (dBm)] フィールドに、送信電力の下限を dBm 単位で入力します。

有効な範囲は -10 ～ 30 です。デフォルト値は -10 です。

802.11 ネットワークの場合、この設定は TPC が自動モードまたは 1 回実行モードの場合にのみ受け入れられます。

c) [Power Control Threshold (dBm)] フィールドに、RRM の TPC バージョン 1 しきい値を dBm 単位で入力します。

有効な範囲は -80 ～ -50 です。デフォルト値は -70 です。

d) [Tx Power V2 Threshold] フィールドに、RRM の TPC バージョン 2 しきい値を dBm 単位で入力します。

有効な範囲は -80 ～ -50 です。デフォルトは -67 です。

ステップ 10 [RRM] で、[DCA] をクリックして必要な設定を完了します。

a) （任意）RFプロファイルの動的チャネル割り当て（DCA）を設定するには、[APの外部AP干渉の回避（Avoid AP Foreign AP Interference）] チェックボックスをオンにします。

DCA を設定すると、チャネルを割り当てるときに、デバイスの RRM アルゴリズムは、ワイヤレスネットワークに含まれていない外部 AP からの 802.11 トラフィックも考慮に入れます。

b) [DCAチャネル（DCA Channels）] で、必要なチャネル番号のチェックボックスをオンにします。

c) （任意） 802.11a Zero Wait DFS 機能を有効にするには、[ゼロ待機DFS（Zero Wait DFS）] チェックボックスをオンにします。

（注） この機能は、5-GHz 帯域にのみ適用されます。

d) [Channel Width] ドロップダウンリストから、RF プロファイルの DCA チャネル幅を選択します。

（注） このドロップダウンリストは、6-GHz および 5-GHz 帯域でのみ使用できます。

e) 6 GHz バンドを選択した場合は、[**Channel Width Min**] および [**Channel Width Max**] ドロップダウンリストから、DBS で許可される最小および最大チャネル幅を選択します。

f) （任意） 6-GHz DCA の優先チャネルスキャン（PSC）を有効にするには、[PSCの適用（PSC Enforcement）] チェックボックスをオンにします。

g) [高速ローミング（High Speed Roam）] で、次の設定を完了します。

- 2.4-GHz および 5-GHz 帯域の場合は、次の設定を完了します。
  - （オプション）RFプロファイルの高速ローミング（HSR）モードを設定するには、[モードの有効化（Mode Enable）] チェックボックスをオンにします。
  - [ネイバータイムアウト（Neighbor Timeout）] フィールドに、RFプロファイルのネイバーのタイムアウト間隔を入力します。

    有効な範囲は 5 ～ 60 です。デフォルト値は 5 です。

- [クライアントネットワーク設定（Client Network Preference）] ドロップダウンリストから、クライアントネットワーク設定を選択します。
  - [接続（Connectivity）] : RRM アルゴリズムでは、ネットワーク設定としてクライアントの接続が使用されます。
  - [スループット（Bps）（Throughput (Bps)）] : RRM アルゴリズムでは、ネットワーク設定としてクライアントの高スループットが使用されます。
  - [デフォルト（Default）] : RRM アルゴリズムではネットワーク設定は使用されません。

ステップ 11 2.4-GHz 帯域を選択した場合は、[RRM] で [帯域選択（Band Select）] をクリックし、次の設定を完了します。

a) （任意） 802.11ax ブロードキャストプローブ応答を有効にするには、[帯域選択プローブ応答（Band Select Probe Response）] チェックボックスをオンにします。

b) [Client RSSI (dBm)] フィールドに、最小モバイルステーションの RSSI しきい値を dBm 単位で入力します。

有効な範囲は -90 ～ -20 です。デフォルト値は -80 です。

c) [Client Mid-RSSI (dBm)] フィールドに、中規模モバイルステーションの RSSI しきい値を dBm 単位で入力します。

有効な範囲は -90 ～ -20 です。デフォルト値は -80 です。

d) [Cycle Count (cycles)] フィールドに、新しいクライアントの抑制サイクルの回数を入力します。

有効な範囲は 1 ～ 10 です。デフォルト値は 2 です。

e) [Cycle Threshold (msec)] フィールドに、バンドセレクトのスキャンサイクルしきい値をミリ秒単位で入力します。

有効な範囲は 1 ～ 1000 です。デフォルト値は 200 です。

f) [Expire Dual Band (sec)] フィールドに、デュアル帯域の有効期限を秒単位で入力します。

有効な範囲は 10 ～ 300 です。デフォルト値は 60 です。

g) [Expire Suppression (sec)] フィールドに、抑制の有効期限を秒単位で入力します。

有効な範囲は 10 ～ 200 です。デフォルト値は 20 です。

ステップ 12 [802.11ax] をクリックし、必要な設定を完了します。

a) 6-GHz 帯域を選択した場合は、次の設定を完了します。

- [6 GHz検出フレーム（6 GHz Discovery Frames）] ドロップダウンリストから、802.11ax 6-GHz 帯域の検出フレームを選択します。
- [He Bcast Probe Resp Intvl] フィールドに、802.11ax ブロードキャストプローブ応答間隔を入力します。

有効な範囲は 5 ～ 25 です。デフォルト値は 20 です。

- [Multi BSSID Profile] ドロップダウンリストから、マルチ BSSID プロファイルを選択します。

  マルチ BSSID プロファイルの作成については、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のマルチ BSSID プロファイルの作成 （864 ページ）」を参照してください。

b) [空間再利用（Spatial Reuse）] で、必要な設定を完了します。

- （オプション）オーバーラップ BSS パケット検出（OBSS-PD）空間再利用を有効にするには、[OBSS PD] チェックボックスをオンにします。
- [Non-SRG OBSS PD Max Threshold (dBm)] フィールドに、非空間再利用グループ（SRG）OBSS-PD 最大しきい値の値を dBm で入力します。

  有効な範囲は -82 ～ -62 です。デフォルト値は -62 です。
- （オプション）SRG OBSS-PD 空間再利用を有効にするには、[SRG OBSS PD] チェックボックスをオンにします。
- [SRG OBSS PD Min Threshold (dBm)] フィールドに、SRG OBSS-PD 最小しきい値の値を dBm で入力します。

  有効な範囲は -82 ～ -62 です。デフォルト値は -82 です。
- [SRG OBSS PD Max Threshold (dBm)] フィールドに、SRG OBSS-PD 最大しきい値の値を dBm で入力します。

  有効な範囲は -82 ～ -62 です。デフォルト値は -62 です。

ステップ 13 [詳細設定（Advanced）] をクリックし、必要な設定を完了します。

a) （任意）[A-MPDU Window Size] フィールドに、Aggregated MAC Protocol Data Unit（A-MPDU）ウィンドウサイズを入力します。

有効な範囲は 1 ～ 255 です。デフォルト値は 255 です。

b) [高密度パラメータ（High Density Parameters）] で、必要な設定を完了します。

- [Max Clients] フィールドに、高密度環境における AP あたりのクライアントの最大数を入力します。

  有効な範囲は 0 ～ 500 です。デフォルト値は 200 です。
- [Multicast Data Rate (Mbps)] ドロップダウンリストから、マルチキャストクライアントを AP に関連付けられる最小データレートを選択します。

（注） 値 0 は、AP が自動的にデータレートを調整することを示します。

- [Rx SOP Threshold (dBm)] ドロップダウンリストから [Receiver Start of Packet Detection (RX SOP)] 感度しきい値（dBm 単位）を選択します。

[カスタム（Custom）] RX SOP しきい値を選択すると、[RX-SOPしきい値（dBm）カスタム値（RX-SOP Threshold (dBm) Custom Value）] フィールドが表示されます。このフィールドには、RX SOP しきい値のカスタム値を dBm 単位で入力します。値の範囲は -85 ～ -60 です。

c) [クライアントの分布（Client Distribution）] で、必要な設定を完了します。

- [Load Balancing Window] フィールドに、AP 間で負荷分散するクライアントの数を入力します。

  有効な範囲は 0 ～ 20 です。デフォルト値は 5 です。

- [Load Balancing Denial Count] フィールドに、AP の負荷分散の拒否カウントを入力します。

  有効な範囲は 1 ～ 10 です。デフォルト値は 3 です。

d) [ATF設定（ATF Configuration）] で、必要な設定を完了します。

[ATF最適化（ATF Optimization）] ドロップダウンリストから、RF プロファイルの Air Time Fairness を有効または無効にするオプションを選択します。Air Time Fairness 最適化が有効になっている場合、ワイヤレスコントローラ は十分に活用されていないクライアントからより多くの帯域幅を必要とするクライアントに通信時間を動的に再割り当てします。この最適化により、ネットワーク効率が向上します。

5-GHz および 2.4-GHz 帯域の場合は、次の設定を完了します。

- [ステータス（Status）] ドロップダウンリストから、Air Time Fairness 動作モードを設定します。
- デフォルトの RF ポリシーで通信時間割り当てモードを有効にするには、[ブリッジクライアントアクセス（Bridge Client Access）] チェックボックスをオンにします。

  このチェックボックスをオンにした場合は、[通信時間割り当て（Airtime Allocation）] フィールドに、必要に応じて通信時間割り当ての重みの割合を入力します。

  有効な範囲は 5 ～ 90 です。デフォルト値は 5 です。

e) [FRA] で、必要な設定を完了します。

帯域	操作
6 GHz	• [クライアントのリセット回数（Client Reset Count）] フィールドに、デュアルバンド無線のクライアント認識 FRA クライアント数を入力して、6-GHz 帯域から 5-GHz 帯域に切り替えます。 有効な範囲は 1 ～ 10 です。デフォルト値は 1 です。 • [クライアント使用率しきい値（%）（Client utilization threshold (%)）] フィールドに、デュアルバンド無線のクライアント認識 FRA 使用率しきい値を入力して、6-GHz 帯域から 5-GHz 帯域に切り替えます。

帯域	操作
5 GHz	クライアント認識 FRA を有効または無効にするには、[クライアント認識（Client Aware）] チェックボックスを使用します。 クライアント認識 FRA により、デュアルバンド無線は、専用 5-GHz 帯域の負荷に応じて 5-GHz またはモニターモードで動作できます。 このチェックボックスをオンにした場合は、次のフィールドにデータを入力します。 • [クライアント選択（Client Select）] : デュアルバンド無線をモニターモードからクライアントサービスモードに移行するためのクライアント認識 FRA 使用率しきい値を入力します。 有効範囲は 0 ～ 100 です。デフォルト値は 50 です。 • [クライアント選択（Client Select）] : デュアルバンド無線をクライアントサービスモードからモニターモードに移行するためのクライアント認識 FRA 使用率しきい値を入力します。 有効範囲は 0 ～ 100 です。デフォルト値は 5 です。
2.4 GHz	[FRAアクション（FRA Action）] ドロップダウンリストから、デュアルバンド無線の FRA アクションを選択します。

f) [RSSI設定（RSSI Settings）] で、必要な設定を完了します。

- （オプション）最適化されたローミング機能を有効にするには、[RSSI Low Check] チェックボックスをオンにして RSSI Low Check を有効にしておく必要があります。
- [RSSI Threshold (dBm)] フィールドに、最適化されたローミングの最小 RSSI しきい値を入力します。

  有効な範囲は -127 ～ 0 です。デフォルト値は -127 です。

g) [UNII帯域設定（UNII Band Settings）] で、[UNII-3低電力チャネル（UNII-3 Low Power Channels）] チェックボックスを使用して、RF プロファイルの 5-GHz 帯域内における UNII-3 低電力チャネルの使用を有効または無効にします。

有効にすると、AP はこれらのチャネルを使用して干渉を減らし、ネットワークパフォーマンスを向上させることができます。



（注） このチェックボックスは、6-GHz および 2.4-GHz 帯域には適用されません。

h) （任意） [再試行制限（Retry Limits）] で、次のフィールドにデータを入力します。

- [集約再試行（Aggregate Retries）] : ドロップするまでの集約データフレームの最大再送信試行回数を入力します。

有効な範囲は -1 ～ 255 です。デフォルト値は -1 です。

- [管理再試行（Management Retries）]：ドロップするまでの管理フレームの最大再送信試行回数を入力します。

  有効な範囲は -1 ～ 255 です。デフォルト値は -1 です。

- [非集約再試行（Non-Aggregate Retries）]：ドロップするまでの非集約データフレームの最大再送信試行回数を入力します。

  有効な範囲は -1 ～ 255 です。デフォルト値は -1 です。

ステップ 14 [802.11be] をクリックし、[プリアンブルパンクチャ（Preamble Puncture）] トグルボタンを使用してプリアンブル パンクチャリングを有効または無効にします。

プリアンブル パンクチャリングは、より広範な帯域幅を維持しながら、干渉があるチャネルの一部を除外することにより、スペクトル効率を向上させます。

（注） このタブは、2.4-GHz 帯域では使用できません。

ステップ 15 [Review and Provision] をクリックします。

ステップ 16 ワイヤレスコントローラ がライセンス要件を満たしていない AP を管理している場合、Catalyst Center は詳細を示すダイアログボックスを表示します。ダイアログボックスで、必要なオプションを選択します。

オプション	説明
ライセンス マネージャ	[License Manager] ウィンドウを開いて、対応するライセンスを有効にします。 ライセンスを有効にするには、『*Cisco Catalyst Center Administrator Guide*』の「Manage Licenses」を参照してください。
[デバイスプロビジョニングに進む（Continue to device provision）]	デバイスのプロビジョニングを続行します。 （注） ライセンス要件を満たしていない AP は、ワールドワイドセーフモード（WWSM）になります。
Cancel	ダイアログボックスを閉じます。

ステップ 17 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 18 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの無線アンテナプロファイルの作成

ワイヤレスコントローラの無線アンテナプロファイルを作成してプロビジョニングするには、次の手順を実行します。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラのリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、[デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[RF] を展開して **[無線アンテナプロファイル（Radio Antenna Profiles）]** をクリックします。

ステップ 4 [Add] をクリックします。

ステップ 5 **[無線アンテナプロファイルの作成（Create Radio Antenna Profile）]** スライドインペインの [一般（General）] タブで、次の設定を完了します。

a) **[無線アンテナプロファイル名（Radio Antenna Profile Name）]** フィールドに、無線アンテナプロファイルの一意の名前を入力します。

プロファイル名には最大 32 文字を含めることができます。Catalyst Center では、プロファイル名の先頭と末尾にスペースを含めることはできません。

b) （任意） [Description] フィールドに、説明を入力します
c) [Antenna Beam] ドロップダウンリストから、AP スロットのビームステアリングモードを選択します。
d) （任意） [Number of Antennas to be Enabled] フィールドに、AP スロットに対して有効にするアンテナの数を入力します。

有効な範囲は 0 ～ 8 です。

e) （任意） 対応する設定を有効にするには、必要なチェックボックスをオンにします。

チェックボックス	説明
Mesh Backhaul	この無線でメッシュバックホールを有効にします。

チェックボックス	説明
Mesh Designated Downlink	この無線を指定メッシュ ダウンリンク バックホールとして使用します。 指定されたダウンリンクバックホールが使用可能な場合、アップリンク無線はダウンリンク無線として使用されません。

f) **[WAT無線管理状態（WAT Radio Administrative State）]** ドロップダウンリストから、必要な状態を選択します。

[常時有効（Always Enabled）] を選択すると、ワイヤレスアクティブテスト（WAT）で常に無線を選択できます。

g) [DTIM Period] の [6 GHz Band] フィールドに、6 GHz 帯域の Delivery Traffic Indication Map（DTIM）間隔を入力します。

有効な範囲は 1 ～ 255 です。デフォルト値は 1 です。

ステップ 6 [Review and Provision] をクリックします。

ステップ 7 ワイヤレスコントローラ がライセンス要件を満たしていない AP を管理している場合、Catalyst Center は詳細を示すダイアログボックスを表示します。ダイアログボックスで、必要なオプションを選択します。

オプション	説明
ライセンス マネージャ	[License Manager] ウィンドウを開いて、対応するライセンスを有効にします。 ライセンスを有効にするには、『*Cisco Catalyst Center Administrator Guide*』の「Manage Licenses」を参照してください。
[デバイスプロビジョニングに進む（Continue to device provision）]	デバイスのプロビジョニングを続行します。 （注） ライセンス要件を満たしていない AP は、ワールドワイドセーフモード（WWSM）になります。
Cancel	ダイアログボックスを閉じます。

ステップ 8 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

ステップ 9 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の RF タグの作成

次の手順を使用して、ワイヤレスコントローラ に関連付けられた AP の RF タグを作成し、プロビジョニングします。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[RF] を展開し、[RFタグ（RF Tags）] をクリックします。

ステップ 4 [Add] をクリックします。

ステップ 5 [RFタグの作成（Create RF Tag）] スライドインペインの [タグ名（Tag Name）] フィールドに、RF タグの一意の名前を入力します。

名前には最大 32 文字を使用できます。

ステップ 6 （任意） [Description] フィールドに、説明を入力します

ステップ 7 （任意） 次のドロップダウンリストから、対応するバンドに必要な RF プロファイルを選択します。

- [6 GHz RFプロファイル（6 GHz RF Profile）]（6 GHz RF プロファイルの作成については、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の RF プロファイルの作成 （852 ページ）」を参照してください）
- [5 GHz RFプロファイル（5 GHz RF Profile）]（5 GHz RF プロファイルの作成については、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の RF プロファイルの作成 （852 ページ）」を参照してください）
- [2.4 GHz RFプロファイル（2.4 GHz RF Profile）]（2.4 GHz RF プロファイルの作成については、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の RF プロファイルの作成 （852 ページ）」を参照してください）

ステップ 8 [APのビーム状態（AP Beam State）] ドロップダウンリストから、AP のビームフォーミング状態を選択します。

ステップ 9 （任意）[スロット設定を表示（Show Slot Configuration）] をクリックしてスロット設定を表示および更新します。

次のドロップダウンリストから、対応するバンドとスロットに必要な無線アンテナプロファイルを選択します。

- [6 GHzスロット2無線プロファイル（6 GHz Slot 2 Radio Profile）]
- [6 GHzスロット3無線プロファイル（6 GHz Slot 3 Radio Profile）]
- [6 GHzスロット1無線プロファイル（6 GHz Slot 1 Radio Profile）]
- [5 GHzスロット1無線プロファイル（5 GHz Slot 1 Radio Profile）]
- [5 GHzスロット2無線プロファイル（5 GHz Slot 2 Radio Profile）]
- [5 GHzスロット0無線プロファイル（5 GHz Slot 0 Radio Profile）]
- [2.4 GHzスロット0無線プロファイル（2.4 GHz Slot 0 Radio Profile）]
- [2.4 GHzスロット2無線プロファイル（2.4 GHz Slot 2 Radio Profile）]

無線アンテナプロファイルを作成するには、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの無線アンテナプロファイルの作成 （860 ページ）」を参照してください。

ステップ 10 [Review and Provision] をクリックします。

ステップ 11 ワイヤレスコントローラ がライセンス要件を満たしていない AP を管理している場合、Catalyst Center は詳細を示すダイアログボックスを表示します。ダイアログボックスで、必要なオプションを選択します。

オプション	説明
ライセンス マネージャ	[License Manager] ウィンドウを開いて、対応するライセンスを有効にします。 ライセンスを有効にするには、『*Cisco Catalyst Center Administrator Guide*』の「Manage Licenses」を参照してください。
[デバイスプロビジョニングに進む（Continue to device provision）]	デバイスのプロビジョニングを続行します。 （注） ライセンス要件を満たしていない AP は、ワールドワイドセーフモード（WWSM）になります。
Cancel	ダイアログボックスを閉じます。

ステップ 12 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。

- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 13 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のマルチ BSSID プロファイルの作成

次の手順を使用して、ワイヤレスコントローラ の複数の基本サービスセット識別子（BSSID）プロファイルを作成し、プロビジョニングします。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、 [RF] を展開し、[マルチBSSIDプロファイル（Multi BSSID Profiles）] をクリックします。

ステップ 4 [Add] をクリックします。

ステップ 5 [マルチBSSIDプロファイルの作成（Create Multi BSSID Profile）] スライドインペインの[マルチBSSIDプロファイル名（Multi BSSID Profile Name）] フィールドに、マルチ BSSID プロファイルの名前を入力します。

ステップ 6 （任意） [Description] フィールドに、説明を入力します

ステップ 7 （任意） [802.11ax] の下で、利用可能なチェックボックスを使用して対応するパラメータを有効にします。

ステップ 8 （任意） [802.11be] の下で、利用可能なチェックボックスを使用して対応するパラメータを有効にします。

（注） Cisco IOS XE リリース 17.18.1 以降を実行する ワイヤレスコントローラ の場合、ステップ 7（864 ページ） の [802.11ax] の下にある [ダウンリンクOFDMA（Downlink OFDMA）]、[アップリンクOFDMA（Uplink OFDMA）]、[ダウンリンクMU-MIMO（Downlink MU-MIMO）]、および [アップリンクMU-MIMO（Uplink MU-MIMO）] チェックボックスを使用して、対応するパラメータを設定します。

ステップ 9 [Review and Provision] をクリックします。

ステップ 10 ワイヤレスコントローラ がライセンス要件を満たしていない AP を管理している場合、Catalyst Center は詳細を示すダイアログボックスを表示します。ダイアログボックスで、必要なオプションを選択します。

オプション	説明
ライセンス マネージャ	[License Manager] ウィンドウを開いて、対応するライセンスを有効にします。 ライセンスを有効にするには、『*Cisco Catalyst Center Administrator Guide*』の「Manage Licenses」を参照してください。
[デバイスプロビジョニングに進む（Continue to device provision）]	デバイスのプロビジョニングを続行します。 （注） ライセンス要件を満たしていない AP は、ワールドワイドセーフモード（WWSM）になります。
Cancel	ダイアログボックスを閉じます。

ステップ 11 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する（238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 12 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のデフォルト RF 設定の編集

この手順を使用して、ワイヤレスコントローラ のデフォルト RF 設定を編集し、プロビジョニングします。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、[デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[RF] を展開して、[RF デフォルト（RF Defaults）]をクリックします。

ステップ 4 必要なバンドを選択します。[Actions] にカーソルを合わせて [Edit] を選択します。

または、必要なバンドをクリックします。

ステップ 5 [RFデフォルトの編集（Edit RF Defaults）] スライドインペイン の [ローミングおよびクライアント設定（Roaming & Client Settings）] で、次の設定を完了します。

- [無線あたりの最大クライアント数（Maximum Clients per Radio）] フィールドに、このバンドを使用する AP の各無線への接続を許可するクライアントの最大数を入力します。

  有効な範囲は 0 ～ 500 です。

- [クライアントネットワーク設定（Client Network Preference）] ドロップダウンリストから、このバンドに関連付けられているクライアントに推奨されるネットワーク動作を選択します。
  - [接続最適化（Connectivity Optimized）] : 安定した接続を優先します。
  - スループット最適化（Throughput Optimized） : データレートを最大化します。
  - [デフォルト（コントローラ決定）（Default（Controller Decision）] : ワイヤレスコントローラ のデフォルト設定を使用します。

ステップ 6 [Review and Provision] をクリックします。

ステップ 7 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

ステップ 8 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の AP 設定

このセクションでは、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のデバイスごとの AP 設定に関する情報を示します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの AP 参加プロファイルの作成

ワイヤレスコントローラの AP 参加プロファイルを作成してプロビジョニングするには、次の手順を実行します。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[AP] を展開して [AP参加プロファイル（AP Join Profiles）] をクリックします。

ステップ 4 [Add] をクリックします。

ステップ 5 [AP参加プロファイルの作成（Create AP Join Profile）] スライドインペインの [一般（General）] タブで、次の設定を完了します。

a) [AP参加プロファイル名（AP Join Profile Name）] フィールドに、AP 参加プロファイルの一意の名前を入力します。

AP 参加プロファイル名には最大 32 文字を含めることができます。Catalyst Center では、AP 参加プロファイル名の先頭と末尾にスペースを含めることはできません。

b) （任意） [Description] フィールドに、説明を入力します
c) [Country Code] ドロップダウンリストから、AP の国コードを選択します。

重要 エンドユーザーライセンス契約（EULA）の要件に従って適切な国コードを選択し、ネットワークが地域や国の規制に準拠するようにします。不適切な国コードを割り当てると、ワイヤレス通信が中断され、不適切な国コードでデバイスを使用しているワイヤレス ネットワーク オペレータに、政府から罰則や制裁が課される可能性があります。

d) [タイムゾーン（Time Zone）] ドロップダウンリストから、タイムゾーンのオプションを選択します。

[オフセット（Offset）] エリアで [WLCとの差（Delta From WLC）] を選択した場合は、次のフィールドにデータを入力します。

- [HH]：タイムゾーンのオフセット時間を入力します。

  有効な範囲は -12 ～ 14 です。デフォルト値は 0 です

- [MM]：タイムゾーンのオフセット分を入力します。

  有効な範囲は 0 ～ 59 です。デフォルト値は 0 です

e) [展開モード（Deployment Mode）] ドロップダウンリストから、AP 展開モードを選択します。

（注） 展開モードを変更すると、AP が再参加し、関連付けられているクライアントの接続が失われる可能性があります。

f) 対応する設定を有効にするには、必要なチェックボックスをオンにします。

- [LED状態（LED State）]：LED ステータスを有効にします。
- [USBの有効化（USB Enable）]：USB を有効にします。
- [LAGモード（LAG Mode）]：AP LAG モードを有効にします。
- [アプリケーションホスティング（Apphost）]：IOX アプリケーション ホスティングを有効にします。

g) （任意） [NTPサーバー（NTP Server）] フィールドに、有効な NTP サーバーの IP アドレスを入力します。

h) （任意） 対応する設定を有効にするには、必要なチェックボックスをオンにします。

- [DHCPへのフォールバック（Fallback to DHCP）]：DHCP への AP のフォールバックを有効にします。

  このチェックボックスをオンにすると、静的 IP アドレスを介した接続に失敗した AP は DHCP にフォールバックします。

- [GAS APレート制限（GAS AP Rate Limit）]：AP で Generic Advertisement Services（GAS） レート制限を有効にします。

このチェックボックスをオンにした場合は、次のフィールドにデータを入力します。

- [GAS要求制限間隔（ミリ秒）（GAS Request limit interval (msec)）]：GAS 要求レート制限を定義する間隔をミリ秒単位で入力します。

  有効な範囲は 100 ～ 10000 です。

- [許可されるGAS/ANQP要求の最大数（Maximum Allowed GAS/ANQP Requests）]：一定の間隔で AP スロットごとに許可される GAS 要求の最大数を入力します。

  有効な範囲は 1 ～ 100 です。

i) （任意） 次のフィールドにデータを入力します。

- [NTPサーバー情報キー（NTP Server Info Key）]：NTP 認証キーを識別するキー ID を入力します。

  値の範囲は 1 ～ 65535 です。デフォルト値は 1 です。

- [NTPサーバー信頼キー（NTP Server Trust Key）]：NTP 認証で使用する信頼キーを入力します。

j) [NTPサーバーキータイプ（NTP Server Key type）] ドロップダウンリストから、信頼キーをローカルに保存するときに使用する暗号化を選択します。

k) （任意） [LEDフラッシュ（秒）（Led Flash (sec)）] フィールドに、AP の LED フラッシュタイマーの持続時間を秒単位で入力します。

有効な範囲は 0 ～ 3600 です。デフォルト値は 0 です。

l) （任意） [DHCPサーバーの有効化（DHCP Server Enable）] チェックボックスをオンにして、DHCP サーバーを有効にします。

m) （任意） [Fast Channel] フィールドに、高速チャネルモード番号の値を入力します。

有効な範囲は 0 ～ 4294967295 です。

n) [OfficeExtend AP設定（OfficeExtend AP Configuration）] で、必要なチェックボックスをオンにして対応する設定を有効にします。

- [ローカルアクセス（Local Access）]：Office Extended AP（OEAP）でローカルアクセスを有効にします。
- [不正検出（Rogue Detection）]：OEAP で不正検出を有効にします。
- [リンク暗号化（Link Encryption）]：OEAP でデータ暗号化を有効にします。
- [SSIDのプロビジョニング（Provisioning SSID）]：OEAP で暫定 SSID を有効にします。

o) [アンテナモニタリング（Antenna Monitoring）] で、次の設定を完了します。

- （オプション）[アンテナモニタリング（Antenna Monitoring）] チェックボックスをオンにしてアンテナモニタリングを有効にします。

- [RSSI Fail Threshold (dB)] フィールドに、アンテナモニタリングの RSSI 障害しきい値を dB 単位で入力します。

  有効な範囲は 10 ～ 90 です。デフォルト値は 40 です。

- [Weak RSSI (dBm)] フィールドに、アンテナモニタリングの弱い RSSI 値を入力します。

  有効な範囲は -90 ～ -10 です。デフォルト値は -60 です。

- [Detection Time (min)] フィールドに、アンテナモニタリングの検出時間を入力します。

  有効な範囲は 9 ～ 180 です。デフォルト値は 12 です。

ステップ 6 [クライアント（Client）] をクリックし、次の設定を完了します。

a) [Maximum Client Limit] フィールドに、AP 設定ごとのクライアントの最大数を入力します。

   有効な範囲は 0 ～ 1200 です。デフォルト値は 0 です

b) [Statistics Timer (sec)] フィールドに、AP から ワイヤレスコントローラ に 802.11 統計情報を送信する時間を秒単位で入力します。

c) （任意） [RSSIクライアント統計（RSSI Client Statistics）] チェックボックスをオンにして AP からのクライアント RSSI 統計レポートを有効にします。

d) （任意） [RSSI Statistics Interval] フィールドに、AP から ワイヤレスコントローラ に送信されるクライアント RSSI 統計のレポート間隔を入力します。

   有効な範囲は 30 ～ 300 です。デフォルト値は 30 です。

e) [TCP MSS設定（TCP MSS Configuration）] で、次の設定を完了します。

   - （オプション）[MSS調整の有効化（Enable Adjust MSS）] チェックボックスを使用して、TCP MSS 調整を有効または無効にします。

   - [Adjust MSS] フィールドに、グローバル AP TCP MSS 値を入力します。

     有効な範囲は 536 ～ 1363 です。デフォルト値は 1,250 です。

ステップ 7 [CAPWAP] で、[高可用性（High Availability）] をクリックして次の設定を完了します。

a) [CAPWAPタイマー（CAPWAP Timers）] で、次のフィールドにデータを入力します。

   - [高速ハートビートタイムアウト（秒）（Fast Heartbeat Timeout (sec)）]：AP すべてのハートビートタイマーのタイムアウト値を秒単位で入力します。

     有効な範囲は 0 ～ 10 です。デフォルト値は 0 です

   - [ハートビートタイムアウト（秒）（Heartbeat Timeout (sec)）]：AP 検出のハートビートタイマーのタイムアウト値を秒単位で入力します。

     有効な範囲は 0 ～ 30 です。デフォルト値は 30 です。

   - [検出タイムアウト（秒）（Discovery Timeout (sec)）]：AP 検出のタイムアウト値を秒単位で入力します。

     有効な範囲は 1 ～ 10 です。デフォルト値は 10 です。

- [プライマリ検出タイムアウト（Primary Discovery Timeout (sec)）]：プライマリ AP 検出のタイムアウト値を秒単位で入力します。

  有効な範囲は 30 ～ 3000 です。デフォルト値は 120 です。

- [準備参加タイムアウト（秒）（Primed Join Timeout (sec)）]：AP 検出の準備参加タイムアウト値を秒単位で入力します。

  有効な範囲は 0 ～ 43200 です。デフォルト値は 0 です

b) [再送信タイマー（Retransmit Timers）] で、次のフィールドにデータを入力します。

- [カウント（Count）]：再送信タイマーカウントを入力します。

  有効な範囲は 3 ～ 8 です。デフォルト値は 5 です。

- [間隔（秒）（Interval (sec)Interval (sec)）]：再送信タイマーの間隔を秒単位で入力します。

  有効な範囲は 2 ～ 5 です。デフォルト値は 3 です。

c) [プライマリコントローラへのAPのフォールバック（AP Fallback to Primary Controller）] で、[有効化（Enable）] チェックボックスを使用して、バックアップコントローラへのフォールバックを有効または無効にします。

フォールバックはプライマリコントローラに適用され、バックアップ プライマリ コントローラには適用されません。

d) （任意）[バックアッププライマリコントローラ（Backup Primary Controller）] と [バックアップセカンダリコントローラ（Backup Secondary Controller）] で、次のフィールドにデータを入力します。

- [名前（Name）]：AP のコントローラ名を入力します。
- [IPv4/IPv6アドレス（IPv4/IPv6 Address）]：AP のコントローラの IP アドレスを入力します。

ステップ 8 [CAPWAP] で、[詳細設定（Advanced）] をクリックして次の設定を完了します。

a) 対応する設定を有効にするには、必要なチェックボックスをオンにします。

[データ暗号化の有効化（Enable Data Encryption）]：AP のデータ暗号化を有効にします

- [ジャンボMTUの有効化（Enable Jumbo MTU）]：AP のジャンボ MTU を有効にします

b) [リンク遅延（Link Latency）] ドロップダウンリストから、リンク監査オプションを選択します。

c) [優先モード（Preferred Mode）] ドロップダウンリストから、CAPWAP の優先モードを選択します。

d) [CAPWAP Window Size] フィールドに、マルチウィンドウキューのリクエストパケットの CAPWAP ウィンドウサイズを入力します。

有効な範囲は 1 ～ 50 です。デフォルト値は 1 です。

e) [検出（Discovery）] で、次の設定を完了します。

- [プライベート（Private）] チェックボックスを使用して、プライベート IP アドレスからの検出応答を有効または無効にします。

- [パブリック（Public）]チェックボックスを使用して、パブリック IP アドレスからの検出応答を有効または無効にします。
- [オンボーディング設定（Onboarding Configuration）] ドロップダウンリストから、AP の CAPWAP 検出オンボーディング設定を選択します。

ステップ 9 [AP] で [一般（General）] をクリックし、次の設定を完了します。

a) [Power over Ethernet] で、次の設定を完了します。

- （任意）対応する設定を有効にするには、必要なチェックボックスをオンにします。
  - [スイッチフラグ（Switch Flag）]：802.3af スイッチを有効にします
  - [パワーインジェクタの状態（Power Injector State）]：パワーインジェクタが使用されている場合。
- [パワーインジェクタタイプ（Power Injector Type）] ドロップダウンリストから、パワーインジェクタのタイプを選択します。

  [インストール済み（Installed）] か [オーバーライド（Override）] を選択した場合は、[インジェクタスイッチMAC（Injector Switch MAC）] フィールドにパワーインジェクタスイッチの MAC アドレスを入力します。

b) [AP EAP認証（AP EAP Authentication）] で、次の設定を完了します。

[EAPタイプ（EAP Type）] で認証方式を選択します。

- [No-Auth]：デフォルトの認証方式。
- [EAP-TLS]：EAP-Transport Level Security（EAP-TLS）では、証明書ベースの認証を使用します。

  [EAP-TLS] を選択した場合は、ユーザー名を入力します。Catalyst Center によって証明書が生成され、PnP 要求プロセス中にその証明書が適用されます。
- [EAP-PEAP]：EAP-Protected Extensible Authentication Protocol（EAP-PEAP）では、相互認証が提供され、脆弱なユーザーログイン情報の機密性と整合性が保証されます。またこのプロトコルでは、自身をパッシブ（盗聴）およびアクティブ（中間者）攻撃から保護し、セキュアに暗号キー関連情報を生成します。EAP-PEAP は、IEEE 802.1X 標準および RADIUS プロトコルと互換性があります。

  [EAP-PEAP] を選択した場合は、ユーザー名とパスワードを入力します。Catalyst Center によって証明書が生成され、PnP 要求プロセス中にその証明書が適用されます。
- [EAP-FAST]：EAP-Flexible Authentication through Secure Tunneling（EAP-FAST）では、相互認証が提供され、共有秘密を使用してトンネルが確立されます。このトンネルは、パスワードに基づく弱い認証方式を保護するために使用されます。Protected Access Credentials（PAC）キーと呼ばれる共有秘密は、トンネルのセキュリティを確保するときにクライアントとサーバを相互認証するために使用されます。

  [EAP-FAST] を選択した場合は、PnP 要求プロセス中に適用されるユーザー名とパスワードを入力します。

この認証方式は、AP PnP 要求時と n 日目の認証時に使用されます。認証方式を変更すると、PnP 要求プロセスでオンボードされた AP のサービスに影響します。認証方式を変更する場合は、PnP 要求プロセスでオンボードされた AP の工場出荷時設定へのリセットを実行します。AP が別の Extensible Authentication Protocol（EAP; 拡張可能認証プロトコル）方式で参加する場合、EAP 方式は選択した認証方式によって変わります。

[AP承認タイプ（AP Authorization Type）] ドロップダウンリストから、ローカルで有効な証明書（LSC）AP 承認タイプを選択します。

c) [クライアント統計レポート間隔（Client Statistics Reporting Interval）] の [5 GHz（秒）（5 GHz (sec)）] および [2.4 GHz（秒）（2.4 GHz (sec)）] フィールドに、対応する帯域に接続されているすべてのクライアントのクライアント統計を AP から送信するレポート間隔を（秒単位で）入力します。

有効な範囲は 5 ～ 90 です。デフォルトは 90 です。

d) （任意） [拡張モジュール（Extended Module）] で、[有効化（Enable）] チェックボックスをオンにして AP 拡張モジュールを有効にします。

e) （任意） [Mesh] の [Mesh Profile Name] フィールドに、メッシュプロファイル名を入力します。

メッシュプロファイルの作成については、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのメッシュプロファイルの作成 （892 ページ）を参照してください。

f) （任意） [インターフェイス設定（Interface Settings）] の [AP静的MTUサイズ（AP Static MTU Size）] フィールドに、AP の最大伝送ユニット（MTU）サイズを入力します。

有効な値は 0（無効化）、または 576 ～ 1485 です。

g) （任意） [MACsec暗号化（MACsec Encryption）] で、次の設定を完了します。

- [MACsec暗号化の有効化（Enable MACsec Encryption）] チェックボックスをオンにして、AP の Media Access Control Security（MACsec）を有効にします。このオプションでは、レイヤ 2 暗号化によって有線接続のセキュリティが強化され、AP と ワイヤレスコントローラ 間で転送中のデータが保護されます。
- [MACsec事前共有キーチェーン（MACsec Pre-shared Key Chain）] ドロップダウンリストから、キーチェーンを選択します。

  キーチェーンの作成については、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のキーチェーンの作成 （996 ページ）」を参照してください。
- [MACsecリプレイウィンドウサイズ（MACsec Replay Window Size）] フィールドに、MACsec のリプレイ保護ウィンドウのサイズを指定する数値を入力します。

  この値は、受け入れられる順序が不正なパケットの数を決定します。これは、ネットワークジッターを調整しながら、リプレイ攻撃を防ぐのに役立ちます。

h) （任意） [高度なAP機能（Advanced AP Features）] で、必要なチェックボックスをオンにして対応する設定を有効にします。

- [RLANファストスイッチング（RLAN Fast Switching）]：リモート LAN（RLAN）インターフェイスのファストスイッチングを有効または無効にします。有効にすると、APはRLANトラフィックを効率的に切り替えて遅延を短縮できます。

- [NSIポート（NSIポート）]：AP のネットワーク サービス インターフェイス（NSI）を有効または無効にします。

  NSI ポートは、高度なネットワークサービスおよび診断に使用されます。

- [CAPWAPパケットアグリゲーション（CAPWAP Packet Aggregation）]：AP の CAPWAP アグリゲーションを有効または無効にします。

  アグリゲーションによって CAPWAP トンネルのオーバーヘッドが削減され、パフォーマンスが向上します。

- [加速度センサー（Accelerometer Sensor）]：AP の加速度センサーを有効または無効にします。有効にすると、AP は動作または改ざんイベントを検出できます。

ステップ 10 （任意） [AP] で、[電源管理（Power Management）] をクリックして次の設定を完了します。

a) [Regular Power Profile] の [Regular Power Profile] ドロップダウンリストから、AP に適用する電力プロファイルを選択します。

必要な電力が供給されていない場合、AP は電力プロファイルにおける一連のルールの定義に従い、ディレーティング状態で機能します。

電力プロファイルの作成については、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の電力プロファイルの作成 （896 ページ）を参照してください。

b) [予定表プロファイル-電力プロファイルマッピング（Calendar Profile - Power Profile Mapping）] で、電力プロファイルマッピングを設定します。

実行する操作	結果
電力プロファイルマッピングを追加する	**1.** [マッピングの追加（Add Mappin）] をクリックします。 **2.** [Add Calendar Profile - Power Profile Mapping] ダイアログボックスで、[Calendar Profile] ドロップダウンリストからカレンダープロファイルを選択します。 カレンダープロファイルの作成については、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のカレンダープロファイルの作成 （908 ページ）を参照してください。 **3.** [電力プロファイル（Power Profile）] ドロップダウンリストから電力プロファイルを選択します。 電力プロファイルの作成については、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の電力プロファイルの作成 （896 ページ）を参照してください。 **4.** [Save] をクリックします。

実行する操作	結果
電力プロファイルマッピングを編集する	1. 必要な予定表プロファイルの横にあるチェックボックスをオンにします。 2. [アクション（Actions）] にカーソルを合わせて [編集（Edit）] を選択します。 3. マッピングを編集します。 4. [Save] をクリックします。
電力プロファイルマッピングを削除する	1. 必要な予定表プロファイルの横にあるチェックボックスをオンにします。 2. [アクション（Actions）] にカーソルを合わせて [削除（Delete）] を選択します。 3. ダイアログボックスで、**Yes** をクリックします。

ステップ 11 [AP] で [Hyperlocation] をクリックし、次の設定を完了します。

a) （任意）[Hyperlocationの有効化（Enable Hyperlocation）] チェックボックスをオンにして、Hyperlocationを有効にします。

b) [Hyperlocationの有効化（Enable Hyperlocation）] チェックボックスをオフにした場合は、次のフィールドにデータを入力します。

- [検出しきい値（dBm）（Detection Threshold (dBm)）]：RSSI が低いパケットを除外する値を入力します。

  有効な範囲は -100 ～ -50 です。デフォルト値は -100 です。

- [トリガーしきい値（サイクル）（Trigger Threshold (cycles)）]：ライアントに BAR を送信するまでのスキャンサイクル数を設定する値を入力します。

  有効な範囲は 1 ～ 100 です。デフォルト値は 10 です。

- [リセットしきい値（Reset Threshold）]：トリガー後にスキャンサイクルの値をリセットする値を入力します。

  有効な範囲は 0 ～ 99 です。デフォルト値は 8 です。

ステップ 12 [AP] で [AP統計（AP Statistics）] をクリックし、次の設定を完了します。

a) [システムモニタリング（System Monitoring）] で、次の設定を完了します。

- （オプション）AP 統計の収集と処理を有効にするには、[リアルタイム統計のモニタリング（Monitor Real Time Statistics）] チェックボックスをオンにします。
- （オプション）AP 統計アラームを有効にするには、[APのアラームのトリガー（Trigger Alarm for AP）] チェックボックスをオンにします。

- [CPU Threshold to Trigger Alarm (%)] フィールドと [Memory Threshold to Trigger Alarm (%)] フィールドに、それぞれ CPU とメモリ使用量のしきい値の割合を入力します。

  有効範囲は 0 ～ 100 です。デフォルト値は 0 です

  SNMP トラップは、このしきい値を超えたときに送信されます。

- [Interval to Hold Alarm (sec)] フィールドに、アラームがトリガーされる前の保持時間を秒単位で入力します。

  有効な範囲は 0 ～ 3600 です。デフォルト値は、6 です。

- [Trap Retransmission Time (sec)] フィールドに、アラームの再送信間隔を秒単位で入力します。

  有効な範囲は 0 ～ 65535 です。デフォルト値は 0 です

- [サンプリング間隔（秒）（Sampling Interval (sec)）] フィールドに、AP からのデータ収集の頻度を定義する値を秒単位で入力します。

  有効な範囲は 2 ～ 900 です。デフォルト値は 30 です。

- [Statistics Interval (sec)] フィールドに、AP 統計の計算間隔を定義する値を秒単位で入力します。

  有効な範囲は 120 ～ 900 です。デフォルト値は 300 です。

- （オプション）定義されたサンプリング間隔における CPU とメモリの使用量が高い場合に AP を自動的にリロードするには、[APのリロード（Reload the AP）] チェックボックスをオンにします。

b) [無線モニタリング（Radio Monitoring）] で、次の設定を完了します。

- （オプション）AP 無線統計の収集と処理を有効にするには、[AP無線スタックのモニタリング（Monitoring of AP Radio Stuck）] チェックボックスをオンにします。
- （オプション）統計に増分がない場合に AP 無線のアラームを生成するには、[AP無線スタックのアラーム（Alarms for AP Radio Stuck）] チェックボックスをオンにします。
- （オプション）統計に増分がない場合に AP 無線のリセットを有効にして無線を回復するには、[スタック状態のAP無線のリセット（Reset the Stuck AP Radio）] チェックボックスをオンにします。
- [Sampling Interval (sec)] フィールドに、無線からのデータ収集頻度を定義する値を秒単位で入力します。

  有効な範囲は 720 ～ 3600 です。デフォルト値は 720 です。

ステップ 13 [管理（Management）] で、[デバイス（Device）] をクリックして次の設定を完了します。

a) （任意）[TFTPダウングレード（TFTP Downgrade）] で、次のフィールドにデータを入力します。

- [IPv4/IPv6アドレス（IPv4/IPv6 Address）]：TFTP サーバーの TFTP ダウングレード IP アドレスを入力します。
- [イメージファイル名（Image File Name）]：TFTP ダウングレードファイルの名前を入力します。

b) [システムログ（System Log）] で、次の設定を完了します。

- [ファシリティ値（Facility Value）] ドロップダウンリストから、ファシリティ値を選択します。
- （オプション）[ホストIPv4/IPv6アドレス（Host IPv4/IPv6 Address）] フィールドに、ホストの IPv4 または IPv6 アドレスを入力します。
- [ログトラップ値（Log Trap Value）] ドロップダウンリストから、ログレベルを選択します。
- （オプション）セキュア syslog の TLS モードを有効にするには、[セキュア（Secured）] チェックボックスをオンにします。

c) [Telnet/SSH] で、次の設定を完了します。

- [Telnet] チェックボックスを使用して、AP への Telnet セッションを有効または無効にします。
- [SSH] チェックボックスを使用して、AP への SSH セッションを有効または無効にします。
- [シリアルコンソール（Serial Console）] チェックボックスを使用して、シリアルコンソール経由の AP へのアクセスを有効または無効にします。
- [コンソールポート速度（Console Port Speed）] ドロップダウンリストから、シリアルアクセス用の端末またはコンソールサーバーの設定に一致する AP コンソールポートのボーレートを選択します。

d) [APコアダンプ（AP Core Dump）] で、次の設定を完了します。

- [カーネルコアダンプ（Kernel Core Dump）] ドロップダウンリストから、カーネルコアダンプのタイプを選択します。

（注） カーネルコアダンプのタイプを変更すると、APが再参加し、関連付けられているクライアントの接続が失われる可能性があります。

- [Max AP Kernel Core Dumps] フィールドに、カーネルコアダンプの最大数を入力します。

  有効な範囲は 1 ～ 5 です。デフォルト値は 5 です。

- （オプション）[無線コアダンプ（Radio Core Dump）] チェックボックスをオンにして、AP コアダンプを有効にします。

  APコアダンプを有効にする場合は、次の設定を完了します。

  - （オプション）[ファイル圧縮の有効化（Enable File Compression）] チェックボックスをオンにして、ファイル圧縮を有効にします。
  - [TFTP Server (IPv4/IPv6)] フィールドに、コアダンプを移動する TFTP サーバーのアドレスを入力します。
  - [File Name] フィールドに、コアファイル名を入力します。

- [カーネルコアダンプファイル制限（Kernel Coredump File Limit）] フィールドに、AP で保持するコアダンプファイルの最大数を入力します。上限に達すると、古いファイルが削除されます。

  有効な範囲は 15 ～ 25 です。デフォルト値は 25 です。

ステップ 14 [管理（Management）] で、[ユーザー（User）] をクリックして次の設定を完了します。

- （オプション）[ユーザー名（Username）] フィールドに、AP ユーザー管理のユーザー名を入力します。

  最大 32 文字を入力することができます。

- [パスワードタイプ（Password Type）] ドロップダウンリストから、AP ユーザー管理のパスワードタイプのタイプを選択します。
- （オプション）[パスワード（Password）] フィールドに、AP ユーザー管理のパスワードを入力します。
- [シークレットタイプ（Secret Type）] ドロップダウンリストから、AP ユーザー管理のシークレットのタイプを選択します。
- （オプション）[シークレット（Secret）] フィールドに、AP ユーザー管理のシークレットを入力します。

ステップ 15 [管理（Management）] で、[ログイン情報（Credentials）] をクリックして次の設定を完了します。

- （オプション）[Dot1xユーザー名（Dot1x Username）] フィールドに、AP Dot1x 認証のユーザー名を入力します。

  最大 32 文字を入力することができます。

- （オプション）[Dot1xパスワード（Dot1x Password）] フィールドに、AP Dot1x 認証のパスワードを入力します。
- [Dot1xパスワードタイプ（Dot1x Password Type）] ドロップダウンリストから、AP Dot1x 認証のパスワードのタイプを選択します。

ステップ 16 （任意）[管理（Management）] で [CDP] をクリックし、[CDP状態（CDP State）] チェックボックスをオンにして AP の CDP を有効にします。

ステップ 17 [セキュリティ（Security）] をクリックし、次の設定を完了します。

a) [不正検出（Rogue Detection）] で、次の設定を完了します。

- （任意）対応する設定を有効にするには、必要なチェックボックスをオンにします。
  - [不正検出（Rogue Detection）]：システム管理者の承認を得ずにセキュアなネットワークにインストールされている AP を検出します。
  - [不正封じ込め自動レート選択（Rogue Containment Automatic Rate Selection）]：不正封じ込め自動レート選択を有効にします。
  - [FlexConnectスタンドアロンでの自動封じ込め（Auto Containment on FlexConnect Standalone）]：FlexConnect モードの不正封じ込めを有効にします。

- 次のフィールドにデータを入力します。
  - [不正検出最小RSSI（Rogue Detection Minimum RSSI）]：AP 不正検知の最小 RSSI を入力します。

    有効な範囲は -128 ～ -70 です。デフォルトは -90 です。
  - [不正検出一時間隔（秒）（Rogue Detection Transient Interval (sec)）]：不正 AP が検出されてから ワイヤレスコントローラ がレポートされるまでの一時的な間隔を秒単位で入力します。

    有効な値は 0、または 120 ～ 1800 です。デフォルト値は 0 です
  - [不正検出レポート間隔（秒）（Rogue Detection Report Interval (sec)）]：AP 不正検出のモニターモードレポートが生成される間隔を秒単位で入力します。

    有効な範囲は 10 ～ 300 です。
- （オプション）[不正検出プロファイル名（Rogue Detection Profile Name）] フィールドに、不正検出プロファイルの名前を入力します。

b) （任意） [PMF-拒否（PMF-Denial）] で、[不正封じ込めPMF-拒否（Rogue Containment PMF-Denial）] チェックボックスをオンにして、802.11w で保護された管理フレーム（PMF）拒否不正 AP 封じ込めを有効にします。

このチェックボックスをオンにした場合、必要に応じて、次のチェックボックスを使用して対応する設定を有効または無効にできます。

- [不正封じ込めPMF-認証解除（Rogue Containment PMF-Deauth）]：認証解除を使用した PMF 拒否不正 AP 封じ込め。
- [不正検出PMFオフチャネル（Rogue Detection PMF Off-Channel）]：オフチャネル PMF 不正 AP 封じ込め。

c) （任意） [aWIPSおよびフォレンジックキャプチャ（aWIPS and Forensic Capture）] で、[aWIPS] チェックボックスをオンにして、Advanced Wireless Intrusion Prevention System（aWIPS）を有効にします。

aWIPS を有効にすると、[Forensic Capture] チェックボックスが表示されます。aWIPS フォレンジックキャプチャを有効にするには、[Forensic Capture] チェックボックスをオンにします。

ステップ 18 （任意） [iCAPクライアントテレメトリ（iCAP Client Telemetry）] で [フルパケットトレース（Full Packet Trace）] をクリックし、次の手順を完了します。

a) 必要なチェックボックスをオンにして、対応する設定を有効にします。
- [トピックステータス（Topic Status）]：インテリジェントキャプチャ（iCAP）クライアントのフル パケット トレース サブスクリプションを有効にします。
- [トレースの集約（Aggregate Trace）]：フルパケットトレースの集約を有効にします。

b) [Client MAC Filters] の [MAC Address] フィールドに、クライアント MAC アドレスを入力します。

ステップ 19 （任意） [iCAPクライアントテレメトリ（iCAP Client Telemetry）] で [部分パケットトレース（Partial Packet Trace）] をクリックし、次の手順を完了します。

a) [トピックステータス（Topic Status）] チェックボックスをオンにして、iCAP クライアントの部分パケット トレース サブスクリプションを有効にします。

b) [Client MAC Filters] の [MAC Address] フィールドに、クライアント MAC アドレスを入力します。

追加の MAC アドレスを含めるには、プラスアイコンをクリックします。

c) [プロトコルフィルタ（Protocol Filters）] で、次の設定を完了します。

- すべてのプロトコルの部分的なパケットトレースを収集するには、[プロトコルフィルタタイプ（Protocol Filter Type）] で [すべて（All）] チェックボックスをオンにします。
- [Management Type] で、部分的なパケットトレースを収集するために必要な管理プロトコル（[All]、[Assoc]、および [Auth]）の横にあるチェックボックスをオンにします。
- [Data Type] で、部分的なパケットトレースを収集するために必要なデータプロトコル（[All]、[ARP]、[DHCP]、[DHCPv6]、[DNS]、[EAP]、[ICMP]、および [ICMPv6]）の横にあるチェックボックスをオンにします。
- [Cisco Type] で、部分的なパケットトレースを収集するために必要な Cisco プロトコル（[All] および [NDP]）の横にあるチェックボックスをオンにします。

ステップ 20 [iCAPクライアントテレメトリ（iCAP Client Telemetry）] で [異常検出（Anomaly Detection）] をクリックし、次の手順を完了します。

a) （任意） 対応する設定を有効にするには、必要なチェックボックスをオンにします。

- [トピックステータス（Topic Status）] : iCAP クライアントの異常検出サブスクリプションを有効にします。
- [APパケットトレーストリガー（Packet Trace Trigger AP）] : 異常検出時に AP パケットトレースをトリガーします

b) （任意） [Client MAC Filters] の [MAC Address] フィールドに、クライアント MAC アドレスを入力します。

追加の MAC アドレスを含めるには、プラスアイコンをクリックします。

c) [Timeout] の [DHCP Frequency (sec)] フィールドに、異常検出に関する DHCP タイムアウトを秒単位で入力します。

有効な範囲は 1 ～ 120 です。デフォルト値は 5 です。

ステップ 21 [iCAPクライアントテレメトリ（iCAP Client Telemetry）] で [統計（Statistics）] をクリックし、次の手順を完了します。

a) [クライアント統計サブスクリプション（Client Statistics Subscription）] で、次の設定を完了します。

- （オプション）iCAP クライアントのクライアント統計サブスクリプションを有効にするには、[トピックステータス（Topic Status）] チェックボックスをオンにします。
- [Frequency (sec)] フィールドに、クライアント統計の収集頻度を秒単位で入力します。

有効な範囲は 30 ～ 3600 です。デフォルト値は 30 です。

b) [クライアントフィルタ統計サブスクリプション（Client Filter Statistics Subscription）] で、次の設定を完了します。

- （オプション）iCAP フィルタ処理済みクライアントのクライアント統計サブスクリプションを有効にするには、[トピックステータス（Topic Status）] チェックボックスをオンにします。
- [Frequency (sec)] フィールドに、フィルタ処理されたクライアント統計の収集頻度を秒単位で入力します。

  有効な範囲は 5 ～ 3600 です。デフォルト値は 5 です。

c) （任意） [Client MAC Filters] の [MAC Address] フィールドに、クライアント MAC アドレスを入力します。

追加の MAC アドレスを含めるには、プラスアイコンをクリックします。

ステップ 22 [iCAPテレメトリサブスクリプション（iCAP AP Telemetry Subscriptions）] をクリックし、次の設定を完了します。

a) 対応する設定を有効にするには、必要なチェックボックスをオンにします。

- [RFスペクトル（RF Spectrum）] : RF スペクトルの iCAP AP テレメトリ サブスクリプションを有効にします。
- [スロット0（Slot 0）] : RF スペクトルの測定に無線スロット 0 を使用します。
- [スロット1（Slot 1）] : RF スペクトルの測定に無線スロット 1 を使用します。
- [スロット2（Slot 2）] : RF スペクトルの測定に無線スロット 2 を使用します。
- [スロット3（Slot 3）] : RF スペクトルの測定に無線スロット 3 を使用します。

b) （任意） 統計サブスクリプションを設定します。

- 必要なチェックボックスをオンにして、対応するAP統計サブスクリプションを有効にします。
- 対応する [頻度（秒）（Frequency (sec)）] フィールドに、対応する AP 統計の収集頻度を秒単位で入力します。

  有効な範囲は 30 ～ 3600 です。デフォルト値は 30 です。

ステップ 23 （任意） [QoS] をクリックし、次の設定を完了します。

a) 必要なチェックボックスを使用して、対応する設定を有効または無効にします。

- [アクションフレーム（Action Frame）] : DSCP からユーザー優先順位（UP）へのマッピングが変更された場合に 802.11 QoS マップアクションフレームを送信します。
- [DSCPアップストリームを信頼（Trust DSCP Upstream）] : UP ではなくアップストリーム DSCP を信頼するように AP を設定します。

b) [DSCPからUPの範囲（SCP to UP Range）] で、DSCP から UP の範囲マッピングを設定します。

実行する操作	結果
DSCP から UP への範囲マッピングを追加する	**1.** [Add] をクリックします。 **2.** [DSCPからUPへの範囲の追加（Add DSCP to UP Range）] ダイアログボックスで、[ユーザー優先順位（User Priority）] ドロップダウンリストからユーザー優先順位を選択します。 **3.** [UP to DSCP Upstream] フィールドに、AP アップストリーム トラフィックの UP から DSCP へのマッピングを入力します。 有効な範囲は 0 ～ 63 です。デフォルト値は 0 です **4.** [Lower DSCP Range] フィールドに、DSCP 範囲の下限を入力します。 有効な範囲は 0 ～ 63 です。デフォルト値は 0 です **5.** [Upper DSCP Range] フィールドに、DSCP 範囲の上限を入力します。 有効な範囲は 0 ～ 63 です。デフォルト値は 0 です **6.** [Save] をクリックします。
DSCP から UP への範囲マッピングを編集する	**1.** 必要なユーザー優先順位の横にあるチェックボックスをオンにします。 **2.** [Actions] にカーソルを合わせて [Edit] を選択します。 **3.** 必要な設定を編集します。 **4.** [Save] をクリックします。
DSCP から UP への範囲マッピングを削除する	**1.** 必要なユーザー優先順位の横にあるチェックボックスをオンにします。 **2.** [アクション（Actions）] にカーソルを合わせて [削除（Delete）] を選択します。 **3.** ダイアログボックスで、**Yes** をクリックします。

c) [DSCPからUPへの例外（DSCP to UP Exception）] で、DSCP から UP への例外マッピングを設定します。

実行する操作	結果
DSCP から UP への例外マッピングを追加する	**1.** [Add] をクリックします。 **2.** [DSCPからUPへの例外の追加（Add DSCP to UP Exception）] ダイアログボックスの [DSCP] フィールドに、UP にマッピングする DSCP を入力します。 有効な範囲は 0 ～ 63 です。 **3.** [User Priority] ドロップダウンリストからユーザー優先順位を選択します。 **4.** [Save] をクリックします。
DSCP から UP への例外マッピングを編集する	**1.** 必要な DSCP の横にあるチェックボックスをオンにします。 **2.** [Actions] にカーソルを合わせて [Edit] を選択します。 **3.** 必要な設定を編集します。 **4.** [Save] をクリックします。
DSCP から UP への例外マッピングを削除する	**1.** 必要な DSCP の横にあるチェックボックスをオンにします。 **2.** [アクション（Actions）] にカーソルを合わせて [削除（Delete）] を選択します。 **3.** ダイアログボックスで、**Yes** をクリックします。

ステップ 24 [地理位置情報（Geolocation）] をクリックし、必要な設定を構成します。

[詳細時間測定（Fine Timing Measurement）] で、次の設定を完了します。

- [FTMの有効化（FTM Enabled）] チェックボックスを使用して、詳細時間測定（FTM）を有効または無効にします。
- [FTMイニシエータバースト期間（FTM Initiator Burst Duration）] ドロップダウンリストから期間を選択します。
- [FTMイニシエータバーストサイズ（FTM Initiator Burst Size）] フィールドに、FTM イニシエータバーストサイズを入力します。

  有効な範囲は 2 ～ 31 です。デフォルト値は 16 です。

[超広帯域（UWB）（Ultra-Wide Band (UWB)）] で、次の設定を完了します。

- [UWB] チェックボックスを使用して、AP ロケーショントラッキングの超高帯域（UWB）を有効または無効にします。
- [UWBバースト期間（UWB Burst Duration）] フィールドに、最適化された AP ロケーショントラッキングの UWB バースト期間を入力します。

有効な範囲は 5 ～ 30 です。デフォルト値は 10 です。

- [UWBバーストサイズ（UWB Burst Size）] フィールドに、最適化された AP ロケーショントラッキングの UWB バーストサイズを入力します。

  有効な範囲は 10 ～ 100 です。デフォルト値は 32 です。

- [UWB Wi-Fiブロッキング（UWB Wi-Fi Blocking）] チェックボックスを使用して、超高帯域（UWB）操作中の Wi-Fi 送信のブロッキングを有効または無効にします。

  UWB と Wi-Fi 間の干渉を減らすには、この設定を有効にします。これは、特定のロケーションベースサービスで必要になる場合があります。

  このチェックボックスをオンにした場合は、[UWB Wi-Fiブロック期間（UWB Wi-Fi Block Duration）] ドロップダウンリストから、AP での UWB 操作中に Wi-Fi をブロックする期間を選択します。

  期間を長くすると UWB の精度は向上しますが、Wi-Fi 接続に一時的に影響が生じる可能性があります。

ステップ 25 [その他（Miscellaneous）] をクリックし、次の設定を完了します。

- （オプション）[パケット キャプチャ プロファイル（Packet Capture Profile）] フィールドに、パケット キャプチャ プロファイルの名前を入力します。
- （オプション）[APトレースプロファイル（AP Trace Profile）] フィールドで、AP トレースプロファイルを選択します。
- （オプション）[ビーコン電力（Beacon Power）] フィールドに、Bluetooth Low Energy（BLE）ビーコン電力値を入力します。

  有効な範囲は 40 ～ 100 です。デフォルト値は 59 です。

- （オプション）[ビーコン間隔（Beacon Interval）] フィールドに、AP の BLE ビーコン間隔を入力します。

  有効な範囲は 1 ～ 10 です。デフォルト値は 1 です。

- （オプション）[SSID統計の有効化（SSID Statistics Enable）] チェックボックスをオンにして、AP で BSSID 統計を有効にします。

  （注） AP で BSSID 統計とクライアントトラフィック分散ステータスを同時に有効にすることはできません。

- （オプション）[SSIDプロファイル統計頻度（SSID Profile Statistics Frequency）] フィールドに、AP で BSSID 統計を送信する頻度を入力します。

  有効な範囲は 1 ～ 180 です。デフォルト値は 30 です。

- （オプション）[SSIDネイバー統計の有効化（SSID Neighbor Statistics Enable）] チェックボックスをオンにして、AP で BSSID ネイバー統計を有効にします。

- （オプション）[SSIDネイバー統計頻度（SSID Neighbor Statistics Frequency）] フィールドに、AP から送信される連続した BSSID ネイバー統計の更新間隔を入力します。

  有効な範囲は 0 ～ 180 です。デフォルト値は 180 です。

- （オプション）[個別のICAPの有効化（ICAP Individual Enable）] チェックボックスを使用して、個別の異常の異常検出レポートを有効にします。

- （オプション）[個別のICAPのスロットル（ICAP Individual Throttle）] フィールドに、個別の異常検出レポートにおける 5 分あたりのイベント数を入力します。

  有効な範囲は 0 ～ 500 です。デフォルト値は 5 です。

- （オプション）[ICAPサマリーの有効化（ICAP Summary Enable）]チェックボックスをオンにして、異常検出レポートのサマリーを有効にします。

- （オプション）[ICAPサマリー頻度（ICAP Summary Frequency）] フィールドに、異常検出サマリーレポートの頻度を入力します。

  有効な範囲は 3 ～ 60 です。デフォルト値は 5 です。

- （オプション）[部分トレース管理プローブ（Partial Trace Management Probe）] チェックボックスをオンにして、管理プロトコルをプローブするために部分的なパケットトレースを収集します。

- （オプション）[AUX LAN ID] フィールドに、補助クライアントトラフィックを割り当てる VLAN ID を入力します。

  有効な範囲は 0 ～ 4094 です。デフォルト値は 0 です

- [Press Sense Config State] ドロップダウンリストから、AP 圧力センサーの設定状態を選択します。

- （オプション）[プロキシホスト名（Proxy Hostname）] フィールドに、HTTP プロキシホスト名を入力します。

- （オプション）[プロキシリスト（Proxy List）] フィールドに、プロキシから除外する URL のリストを入力します。

- （オプション）[プロキシポート（Proxy Port）] フィールドに、HTTP プロキシポート番号を入力します。

  有効な範囲は 0 ～ 65535 です。

- （オプション）[プロキシユーザー名（Proxy Username）] フィールドに、プロキシサーバーで AP を認証するためのプロキシユーザー名を入力します。

  ユーザー名には最大 64 文字を含めることができます。

- （オプション）[プロキシパスワード暗号化タイプ（Proxy Password Encryption Type）] ドロップダウンリストから、プロキシパスワードを保存してセキュリティを強化するための暗号化方式を選択します。

- （オプション）[プロキシパスワード（Proxy Password）] フィールドに、プロキシサーバーで AP を認証するためのプロキシパスワードを入力します。

  パスワードがプロキシサーバーで設定したログイン情報と一致していることを確認してください。

- （オプション）[アカウンティング方式リスト（Accounting Method List）] フィールドから、アカウンティング方式リスト名を選択します。

  アカウンティング方式リストの作成については、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のアカウンティング方式リストの作成 （931 ページ）」を参照してください。

- （オプション）[AP管理IPv4 ACL名（AP Management IPv4 ACL Name）] フィールドに、AP への管理アクセスを制限する IPv4 ACL の名前を入力します。

  ACL 名には最大 32 文字を含めることができます。この ACL で許可されたデバイスのみが、IPv4 を介して AP を管理できます。

- （オプション）[AP管理IPv6 ACL名（AP Management IPv6 ACL Name）] フィールドに、AP への管理アクセスを制限する IPv6 ACL の名前を入力します。

  ACL 名には最大 32 文字を含めることができます。この ACL で許可されたデバイスのみが、IPv6 を介して AP を管理できます。

- （オプション）[トラフィック分散ステータス（Traffic Distribution Status）] チェックボックスをオンにして、クライアントトラフィック分散統計を有効にします。

  （注） AP で BSSID 統計とクライアントトラフィック分散ステータスを同時に有効にすることはできません。

- （オプション）[トラフィック分散間隔（Traffic Distribution Interval）] フィールドに、AP から統計を送信する間隔を入力します。

  有効な範囲は 30 ～ 3600 です。デフォルト値は 300 です。

- （オプション）[セッション制限（Session Limit）] フィールドに、AP ごとに許可される Dot1x セッションの最大数を入力します。

  デフォルト値は 0 です

- [Tunnel UDP Lite] ドロップダウンリストから、IPv6 CAPWAP データチェックサムタイプを選択します。

- （オプション）必要なチェックボックスをオンにして、対応する設定を有効または無効にします。
  - [GPRCの有効化（GPRC Enable）]：AP で gRPC サーバーを有効にするには、このチェックボックスをオンにします。
  - [TLS設定制御設定（TLS Config Control Preference）]：ワイヤレスコントローラで定義された暗号スイートに関する設定を構成します。
  - [BLEスキャン状態（BLE scan state）]：BLE スキャン状態を有効にします。
  - [永続的SSIDブロードキャストの有効化（Persistent SSID Broadcast Enable）]：永続的 SSID ブロードキャストを有効にします。
  - **[個別のADRの集約を有効化]**：個別の異常検出レポートの集約を有効にします。

- [Adr Individual Pc Throttle] フィールドに、個別の異常検出レポートにおけるクライアントごとの 5 分あたりのイベント数を入力します。

  有効な範囲は 0 ～ 50 です。デフォルト値は 5 です。

- [Adr Individual Pt Throttle] フィールドに、個別の異常検出レポートにおけるタイプごとの 5 分あたりのイベント数を入力します。

  有効範囲は 0 ～ 100 です。デフォルト値は 5 です。

- （オプション）[BLEビーコン（BLE Beacons）] で、BLE ビーコン設定を表示します。

  Cisco Connected Mobile Experiences（CMX）と Cisco Spaces での空間マッピングを介して BLE ビーコン設定を管理できます。これらの属性は、可視性を確保するとともにロケーションベースサービスとの整合性を保つために読み取り専用となっています。

ステップ 26 [Review and Provision] をクリックします。

ステップ 27 ワイヤレスコントローラ がライセンス要件を満たしていない AP を管理している場合、Catalyst Center は詳細を示すダイアログボックスを表示します。ダイアログボックスで、必要なオプションを選択します。

オプション	説明
ライセンス マネージャ	[License Manager] ウィンドウを開いて、対応するライセンスを有効にします。 ライセンスを有効にするには、『*Cisco Catalyst Center Administrator Guide*』の「Manage Licenses」を参照してください。
[デバイスプロビジョニングに進む（Continue to device provision）]	デバイスのプロビジョニングを続行します。 （注） ライセンス要件を満たしていない AP は、ワールドワイドセーフモード（WWSM）になります。
Cancel	ダイアログボックスを閉じます。

ステップ 28 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 29 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のグローバル メッシュ パラメータの設定

次の手順を使用して、ワイヤレスコントローラ のグローバル メッシュ パラメータを設定し、プロビジョニングします。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、 [AP] を展開して [メッシュ（Mesh）] をクリックします。

ステップ 4 [Global] タブをクリックします。

ステップ 5 （任意） [全般（General）] で、チェックボックスを使用して対応する設定を有効または無効にします。

- [イーサネットブリッジングによるBPDUの許可（Ethernet Bridging Allow BPDU）] : イーサネットブリッジングが有効な場合にメッシュネットワークで BPDU パケットを許可します。
- [サブセットチャネル同期（Subset Channel Sync）] : モビリティグループ全体でメッシュルート AP（RAP）チャネルの同期を有効にします。
- [公共安全が有効（Public Safety Enabled）] : 公共安全帯域を有効にします。
- [自動DCA RF ASCI AP（Auto DCA RF ASCI APs）] : RF ASIC 統合メッシュ RAP のバックホール無線で RRM DCA を常に有効にする必要があることを示します。
- メッシュ AP（MAP）でコールアドミッション制御（CAC）を有効にするには、[CAC有効（CAC Enabled）] チェックボックスをオンにします。

ステップ 6 （任意） [バックホール（Backhaul）] で、チェックボックスを使用して対応する設定を有効または無効にします。

- [拡張UNII-Bドメインチャネル（Extended UNII B Domain Channels）] : MAP のバックホール無線で UNII B ドメインチャネルを有効にします。
- [RRM] : 子 MAP を持たないルート MAP のバックホール無線で RRM を有効にします。

ステップ 7 （任意） [セキュリティ（Security）] で、MAP の PSK プロビジョニングを有効にするには、[PSKプロビジョニング（PSK Provisioning）] チェックボックスをオンにします。

- （オプション）MAP のデフォルト PSK を有効にするには、[デフォルトPSK（Default PSK）] チェックボックスをオンにします。
- [使用中PSKインデックス（PSK Inuse Index）] ドロップダウンリストから、使用中の PSK キーインデックスを選択します。

  PSK キーの作成については、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のメッシュ PSK の作成 （890 ページ）を参照してください。

ステップ 8 [アラーム（Alarm）] で、これらのフィールドにデータを入力します。

- [最大ホップ数（Max Hop Count）]：メッシュアラームを生成するための MAP ノードから RAP ノードまでのホップ数のしきい値を入力します。

  有効範囲は 1 ～ 16 です。
- [MAPの推奨最大子MAP数（Recommended Max Children for MAP）]：メッシュアラームを生成する親 MAP の子 MAP 数のしきい値を入力します。

  有効な範囲は 1 ～ 50 です。
- [RAPの推奨最大子RAP数（Recommended Max Children for MAP）]：メッシュアラームを生成する親 RAP の子 RAP 数のしきい値を入力します。

  有効な範囲は 1 ～ 50 です。
- [親変更回数（Parent Change Count）]：メッシュアラームを生成するために子メッシュノードが親ノードを変更する回数のしきい値を入力します。

  有効な範囲は 1 ～ 30 です。
- [低リンクSNR（Low Link SNR（dB）]：メッシュアラームを生成するための子メッシュノードにおけるバックホールリンクの低 SNR のしきい値を入力します。

  有効な範囲は 1 ～ 30 です。
- [高リンクSNR（High Link SNR（dB）]：メッシュアラームを生成するための子メッシュノードにおけるバックホールリンクの高 SNR のしきい値を入力します。

  有効な範囲は 31 ～ 100 です。
- [関連付け数（Association Count）]：アラームを生成するための親メッシュノードでの累積関連付け数のしきい値を入力します。

  有効な範囲は 1 ～ 30 です。

ステップ 9 [Review and Provision] をクリックします。

ステップ 10 ワイヤレスコントローラ がライセンス要件を満たしていない AP を管理している場合、Catalyst Center は詳細を示すダイアログボックスを表示します。ダイアログボックスで、必要なオプションを選択します。

オプション	説明
ライセンス マネージャ	[License Manager] ウィンドウを開いて、対応するライセンスを有効にします。 ライセンスを有効にするには、『*Cisco Catalyst Center Administrator Guide*』の「Manage Licenses」を参照してください。
[デバイスプロビジョニングに進む（Continue to device provision）]	デバイスのプロビジョニングを続行します。 （注） ライセンス要件を満たしていないAPは、ワールドワイドセーフモード（WWSM）になります。
Cancel	ダイアログボックスを閉じます。

ステップ 11 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 12 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のメッシュ PSK の作成

ワイヤレスコントローラのメッシュ事前共有キー（PSK）を作成してプロビジョニングするには、次の手順を実行します。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[AP] を展開して [メッシュ（Mesh）] をクリックします。

ステップ 4 [PSK Keys] タブをクリックします。

ステップ 5 [Add] をクリックします。

（注） 5 個の PSK キーがすでに作成されている場合、このオプションは使用できません。

ステップ 6 [メッシュプロファイルキーの作成（Create Mesh Profile Key）] スライドインペインの [インデックス（Index）] ドロップダウンリストから、PSK のインデックスを選択します。

ステップ 7 [Psk Key] フィールドに、PSK を入力します。

PSK は 3 ～ 32 文字で指定できます。

ステップ 8 [Psk Key Type] ドロップダウンリストから、PSK タイプを選択します。

ステップ 9 （任意） [Description] フィールドに、PSK の説明を入力します。

ステップ 10 [Review and Provision] をクリックします。

ステップ 11 ワイヤレスコントローラ がライセンス要件を満たしていない AP を管理している場合、Catalyst Center は詳細を示すダイアログボックスを表示します。ダイアログボックスで、必要なオプションを選択します。

オプション	説明
ライセンス マネージャ	[License Manager] ウィンドウを開いて、対応するライセンスを有効にします。 ライセンスを有効にするには、『*Cisco Catalyst Center Administrator Guide*』の「Manage Licenses」を参照してください。
[デバイスプロビジョニングに進む（Continue to device provision）]	デバイスのプロビジョニングを続行します。 （注） ライセンス要件を満たしていない AP は、ワールドワイドセーフモード（WWSM）になります。
Cancel	ダイアログボックスを閉じます。

ステップ 12 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 13 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのメッシュプロファイルの作成

ワイヤレスコントローラのメッシュプロファイルを作成してプロビジョニングするには、次の手順を実行します。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。

b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。

c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。

b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[AP] を展開して [メッシュ（Mesh）] をクリックします。

ステップ 4 [Mesh Profiles] タブをクリックします。

ステップ 5 [Add] をクリックします。

ステップ 6 [メッシュプロファイルの作成（Create Mesh Profile）] スライドインペインの [一般（General）] タブで、次の設定を完了します。

a) [Mesh Profile Name] フィールドに、メッシュプロファイルの名前を入力します。

b) （任意） [Description] フィールドに、説明を入力します

c) [Range (Root AP to Mesh AP)] フィールドに、屋外 RAP と MAP 間の最大範囲を入力します。

有効な範囲は 150 ～ 132000 です。デフォルト値は 12,000 です。

d) [マルチキャストモード（Multicast Mode）] ドロップダウンリストから、メッシュネットワーク上のイーサネット ブリッジ マルチキャスト トラフィックのマルチキャストモードを選択します。

e) （任意） 対応する設定を有効にするには、必要なチェックボックスをオンにします。

- [IDS（不正/署名検出）（IDS (Rogue/Signature Detection)）] : MAP がワイヤレスコントローラに IDS および不正レポートを送信できるようにします。
- [バックホールクライアントアクセス（Backhaul Client Access）] : MAP のバックホール無線でクライアントアクセスを有効にします。
- [バックグラウンドスキャン（Background Scanning）] : MAP のバックホール無線でバックグラウンドスキャンを有効にします。
- [APのバッテリ状態（Battery State for an AP）] : MAP の外部バッテリ状態を有効にします。
- [チャネル変更通知（Channel Change Notification）] : 親 MAP から子 MAP へのチャネル変更通知の送信を可能にします。

- [フルセクターDFSステータス（Full Sector DFS Status）]：メッシュネットワークでフルセクターの動的周波数選択（DFS）を有効にします。
- [LSC]：MAP に対するローカルで有効な証明書（LSC）認証を有効にします。
- [デイジーチェーンSTP冗長性（Daisychain STP Redundancy）]：MAP でデイジーチェーンのスパニングツリープロトコル（STP）冗長性を有効にします。
- [バックホールamsdu（Backhaul amsdu）]：MAP のバックホール無線で Aggregated MAC Service Data Unit（A-MSDU）を有効にします。
- [MAP高速祖先検索（Map Fast Ancestor Find）]：MAP のバックホール無線で MAP 高速先祖検索機能を有効にします。
- [RAPイーサネットデイジーチェーン（RAP Ethernet Daisy Chain）]：RAP の RAP イーサネットデイジー チェーンを有効にします。

f) [コンバージェンス方式（Convergence Method）] ドロップダウンリストから、MAP で使用するコンバージェンス方式を選択します。

ステップ 7 [詳細設定（Advanced）] をクリックして、次の設定を完了します。

a) [Channel Width] フィールドに、バックホールチャネル幅を入力します。

b) （任意） 対応する設定を有効にするには、必要なチェックボックスをオンにします。

- [ワイヤレス接続の維持（Keep Wireless Connection）]：有線チャネルに切り替えずに親 AP とのワイヤレス接続を AP が維持できるようにします。
- [最小輻輳チャネルスキャン（Least Congested Channel Scan）]：最小輻輳チャネルスキャンを有効にします。
- [Unii3バイアス（Unii3 Bias）]：他のチャネルよりも UNII-3 チャネルに 20% のバイアスを追加します。
- [Unii2の使用（Use Unii2）]：最小輻輳チャネルスキャンで UNII-2 帯域のチャネルを考慮に入れます。

c) [セキュリティ（Security）]で、対応するドロップダウンリストから必要なオプションを選択します。

ドロップダウンリストで...	選択...
Method	MAP に使用されるセキュリティ方式
（オプション）**Authentication Method**	AAA 認証方式リスト 認証方式リストの作成については、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの認証方式リストの作成（928 ページ）」を参照してください。

ドロップダウンリストで...	選択...
（オプション）**Authorization Method**	AAA 承認方式リスト 認証方式リストの作成については、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の認証方式リストの作成（929ページ）を参照してください。

d) （任意）[イーサネットブリッジング（Ethernet Bridging）] で、必要なチェックボックスをオンにし、対応する設定を有効にします。

- [VLANトランスペアレント（VLAN Transparent）]：MAP 上のイーサネットブリッジングで VLAN 設定を使用する必要があることを示します。
- [イーサネットブリッジング（Ethernet Bridging）]：MAP のイーサネットブリッジングを有効にします。

e) （任意） [ブリッジグループ（Bridge Group）] で、次の設定を完了します。

- [Bridge Group Name] フィールドに、ブリッジグループの名前を入力します。
- [完全一致（Strict Match）] チェックボックスをオンにして、親を選択するために MAP のブリッジグループ名の完全一致を有効にします。

f) [5 GHz帯域バックホール（5 GHz Band Backhaul）] で、次の設定を完了します。

- [5 GHz Band Rate Types] ドロップダウンリストから、バックホール データレート タイプを選択します。
- [dot11abg] バックホールのデータレートタイプを選択した場合は、[Rate (Mbps)] ドロップダウンリストから、メッシュバックホール 802.11 伝送の列挙値を選択します。
- [dot11n] バックホールのデータレートタイプを選択した場合は、[Dot11n MCS index] フィールドに、メッシュバックホール伝送の 802.11n MCS インデックスを入力します。

  有効な範囲は 0 ～ 31 です。デフォルト値は 0 です
- [dot11ac] バックホール データ レート タイプを選択した場合は、次のオプション設定も構成できます。
  - [Dot11ac MCSインデックス（Dot11ac MCS index）] フィールドに、メッシュバックホール伝送の 802.11ac MCS インデックスを入力します。

    有効な範囲は 0 ～ 9 です。デフォルト値は 0 です
  - [AC Spatial Stream] フィールドに、メッシュバックホール伝送の 802.11ac 空間ストリーム値を入力します。

    有効な範囲は 1 ～ 4 です。デフォルト値は 1 です。

- [dot11ax] バックホールデータ レート タイプを選択した場合は、次のオプション設定も構成できます。
  - [Dot11ax MCSインデックス（Dot11ax MCS index）] フィールドに、メッシュバックホール伝送の 802.11ax MCS インデックスを入力します。

    有効な範囲は 0 ～ 11 です。デフォルト値は 0 です
  - [AX Spatial Stream] フィールドに、メッシュバックホール伝送の 802.11ax 空間ストリーム値を入力します。

    有効な範囲は 1 ～ 8 です。デフォルト値は 1 です。

g) [2.4 GHz帯域バックホール（2.4 GHz Band Backhaul）] で、次の設定を完了します。

- [2.4 GHz Band Rate Types] ドロップダウンリストから、バックホールのデータレートタイプを選択します。
- [dot11abg] バックホールのデータレートタイプを選択した場合は、[Rate (Mbps)] ドロップダウンリストから、メッシュバックホール 802.11 伝送の列挙値を選択します。
- [dot11n] バックホールのデータレートタイプを選択した場合は、[Dot11n MCS index] フィールドに、メッシュバックホール伝送の 802.11n MCS インデックスを入力します。

  有効な範囲は 0 ～ 31 です。デフォルト値は 0 です
- [dot11ax] バックホールデータ レート タイプを選択した場合は、次のオプション設定も構成できます。
  - [Dot11ax MCSインデックス（Dot11ax MCS index）] フィールドに、メッシュバックホール伝送の 802.11ax MCS インデックスを入力します。

    有効な範囲は 0 ～ 11 です。デフォルト値は 0 です
  - [AX Spatial Stream] フィールドに、メッシュバックホール伝送の 802.11ax 空間ストリーム値を入力します。

    有効な範囲は 1 ～ 4 です。デフォルト値は 1 です。

h) （任意）[高速ローミング（Fast Roaming）] で、[高速ティアダウン（Fast Teardown）] チェックボックスをオンにして高速ティアダウンを有効にし、次のフィールドにデータを入力します。

- [再試行回数（Number of Retries）]：ゲートウェイが到達不能とみなされるまでの再試行回数を入力します。

  有効な範囲は 1 ～ 10 です。デフォルト値は 4 です。
- [間隔（秒）（Interval (seconds)）]：再試行間隔を入力します。

  有効な範囲は 1 ～ 10 です。デフォルト値は 1 です。
- [遅延しきい値（ミリ秒）（Latency Threshold (milliseconds)）]：ping 遅延しきい値をミリ秒単位で入力します。

有効な範囲は 1 ～ 500 です。デフォルト値は 10 です。

- [遅延超過しきい値（秒）（Latency Exceeded Threshold (seconds)）]：しきい値の時間内に少なくとも 1 つの ping が成功する必要がある間隔を秒単位で入力します。

  有効な範囲は 1 ～ 30 です。デフォルト値は 8 です。

- [アップリンク回復間隔（秒）（Uplink Recovery Interval (seconds)）]：子接続を受け入れるために RAP アップリンクが安定している必要がある時間を秒単位で入力します。

  有効な範囲は 1 ～ 3600 です。デフォルト値は 60 です。

ステップ 8 [Review and Provision] をクリックします。

ステップ 9 ワイヤレスコントローラ がライセンス要件を満たしていない AP を管理している場合、Catalyst Center は詳細を示すダイアログボックスを表示します。ダイアログボックスで、必要なオプションを選択します。

オプション	説明
ライセンス マネージャ	[License Manager] ウィンドウを開いて、対応するライセンスを有効にします。 ライセンスを有効にするには、『*Cisco Catalyst Center Administrator Guide*』の「Manage Licenses」を参照してください。
[デバイスプロビジョニングに進む（Continue to device provision）]	デバイスのプロビジョニングを続行します。 （注） ライセンス要件を満たしていない AP は、ワールドワイドセーフモード（WWSM）になります。
Cancel	ダイアログボックスを閉じます。

ステップ 10 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 11 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の電力プロファイルの作成

この手順を使用して、ワイヤレスコントローラの電力プロファイルを作成し、プロビジョニングします。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[AP] を展開して [電力プロファイル（Power Profiles）] をクリックします。

ステップ 4 [Add] をクリックします。

ステップ 5 [電力プロファイルを作成（Create Power Profile）] スライドインペインの [プロファイル名（Profile Name）] フィールドで、電力プロファイルの名前を入力します。

ステップ 6 （任意） [Description] フィールドに、説明を入力します

ステップ 7 （任意） [省電力クライアントしきい値（Power Save Client Threshold）] フィールドに、AP が省電力モードを維持できるしきい値を入力します。

有効な範囲は 1 ～ 32 です。デフォルト値は 1 です。

ステップ 8 （任意） [ルール（Rules）] で、[追加（Add）] をクリックしてルールを追加します。

a) [Sequence] フィールドに一意のインターフェイスシーケンス番号を入力します。

有効な範囲は 0 ～ 4294967295 です。

b) [インターフェイス（Interface）] ドロップダウンリストでインターフェイスを選択します。

次を選択できます。	下記を実行
Ethernet	次の設定を完了します。 • [Interface ID] ドロップダウンリストからインターフェイス ID を選択します。 • [Parameter Value] ドロップダウンリストからパラメータ値を選択します。

次を選択できます。	下記を実行
無線機	次の設定を完了します。 • [Parameter] ドロップダウンリストからパラメータを選択します。 • [Interface ID] ドロップダウンリストからインターフェイス ID を選択します。 • [Parameter Value] ドロップダウンリストからパラメータ値を選択します。 （注） [ステート（State）] パラメータを選択すると、このドロップダウンリストは無効になります。

c) [Save] をクリックします。

ステップ 9 （任意） ルールを削除するには、次の手順を実行します。

1. 必要なルールの横にあるチェックボックスをオンにします。
2. **[Actions]** にカーソルを合わせ、**[Delete]** をクリックします。
3. ダイアログボックスで、**Yes** をクリックします。

ステップ 10 [Review and Provision] をクリックします。

ステップ 11 ワイヤレスコントローラ がライセンス要件を満たしていない AP を管理している場合、Catalyst Center は詳細を示すダイアログボックスを表示します。ダイアログボックスで、必要なオプションを選択します。

オプション	説明
ライセンス マネージャ	[License Manager] ウィンドウを開いて、対応するライセンスを有効にします。 ライセンスを有効にするには、『*Cisco Catalyst Center Administrator Guide*』の「Manage Licenses」を参照してください。
[デバイスプロビジョニングに進む（Continue to device provision）]	デバイスのプロビジョニングを続行します。 （注） ライセンス要件を満たしていない AP は、ワールドワイドセーフモード（WWSM）になります。
Cancel	ダイアログボックスを閉じます。

ステップ 12 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 13 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の Flex プロファイルの作成

この手順を使用して、ワイヤレスコントローラ の Flex プロファイルを作成し、プロビジョニングします。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[AP] を展開し、[Flex プロファイル（Flex Profiles）] をクリックします。

ステップ 4 [Add] をクリックします。

ステップ 5 [Flexプロファイルの作成（Create Flex Profile）] スライドインペインの [一般（General）] タブで、次の設定を完了します。

a) [Flexプロファイル名（Flex Profile Name）] フィールドに、Flex プロファイルの一意の名前を入力します。

   プロファイル名は最大 32 文字で指定できます。

b) （任意） [Description] フィールドに、説明を入力します
c) [Native VLAN ID] フィールドに、AP の VLAN ID を入力します。

   有効な範囲は 1 ～ 4094 です。デフォルト値は 1 です。

d) （任意） [mDNS Flexプロファイル（mDNS Flex Profile）] ドロップダウンリストから、mDNS Flex プロファイル名を選択します。

mDNS Flex プロファイルの作成については、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの mDNS Flex プロファイルの作成 （1075 ページ）」を参照してください。

e) （任意） 次のフィールドにデータを入力します。

- [HTTPプロキシポート（HTTP Proxy Port）]：HTTP プロキシポートを入力します。

  有効な範囲は 0 ～ 65535 です。デフォルト値は 0 です

- [HTTPプロキシ IP アドレス（HTTP Proxy IP Address）]：HTTP プロキシ IP アドレスを入力します。

f) （任意） 対応する設定を有効にするには、必要なチェックボックスをオンにします。

- [フォールバック無線シャットダウン（Fallback Radio Shut）]：ワイヤレスコントローラ に接続されている AP の FlexConnect イーサネットフォールバック機能を有効にします。
- [OfficeExtend AP]：このプロファイルに接続されている AP をホーム AP として使用します。
- [復元力のあるFlex（Flex Resilient）]：リモートエッジ AP（REAP）でスタンドアロンモードのサポートを有効にします。
- [最小遅延接続（Join Minimum Latency）]：REAP AP が最小の遅延で ワイヤレスコントローラ に接続できるようにします。
- [ARPキャッシング（ARP Caching）]： ワイヤレスコントローラ に接続されている FlexConnect AP の ARP キャッシュを有効にします。
- [IPオーバーラップ（IP Overlap）]：サイトの IP オーバーラップのサポートを有効にします。
- [効率的なイメージアップグレード（Efficient Image Upgrade）]：効率的な AP イメージのアップグレードのサポートを有効にします。
- [PMK配布方法（Pmk Dist Method）]：AP でペアワイズマスターキー（PMK）の配布を有効にします。

g) （任意） [最大再試行回数（セカンダリ）（Maximum Retry Attempts (Secondary)）] フィールドには、接続を確立または維持する際のセカンダリデバイスの最大再試行回数を入力します。

値を大きくすると、不安定な環境での信頼性が向上しますが、障害の検出が遅延する場合があります。

h) （任意） [CTSポリシー（CTS Policy）] で、次の設定を行います。

- [インラインタギング（Inline Tagging）]チェックボックスをオンにして、ワイヤレスコントローラ に接続されている FlexConnect AP の Cisco TrustSec （CTS）インラインタギングを有効にします。
- [SGACLの適用（SGACL Enforcement）]チェックボックスをオンにして、ワイヤレスコントローラ に接続されている FlexConnect AP のロールベースの適用を有効にします。
- [CTS Profile Name] ドロップダウンリストから、CTS プロファイルを選択します。

プロファイルを作成する場合は、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの SXP AP プロファイルの作成 （981 ページ） 」参照してください。

ステップ 6 （任意） [ローカル認証（Local Authentication）] をクリックして、これらの設定を完了します。

a) [RADIUS Server Group] ドロップダウンリストから RADIUS サーバーグループを選択します。

RADIUS サーバーグループの作成については、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の RADIUS サーバーグループの作成 （921 ページ） 」を参照してください。

b) [Local Accounting RADIUS Server Group] ドロップダウンリストから RADIUS サーバーグループを選択します。

RADIUS サーバーグループの作成については、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の RADIUS サーバーグループの作成 （921 ページ） 」を参照してください。

c) [EAP-FAST Profile（EAP Fast プロファイル）] のドロップダウンリストから、EAP Fast プロファイル名を選択します。

EAP Fast プロファイルを作成するには、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の EAP-FAST プロファイルの作成 （959 ページ） 」を参照してください。

d) 対応する設定を有効にするには、必要なチェックボックスをオンにします。

- [ローカルクライアントローミング（Local Client Roaming）]：ローカルローミング用に AP で分散クライアントデータのキャッシングを有効にします。
- [LEAP]：Lightweight Extensible Authentication Protocol（LEAP）を有効にします。
- [TLS]：TLSを有効にします。
- [PEAP]：Protected Extensible Authentication Protocol（PEAP）を有効にします。
- [RADIUS]：RADIUS を有効にします。

e) [ユーザー（Users）] で、ユーザーを追加、編集、または削除します。

実行する操作	結果
Flex ローカル認証ユーザーの追加	[追加（Add）] をクリックして、次の手順を実行します。 **1.** [Username] フィールドに、グループ内の AP に関連付けられているクライアントを認証するためのユーザー名を入力します。 **2.** [パスワードタイプ（Password Type）] ドロップダウンリストから、グループ内の AP に関連付けられているクライアントを認証するためのパスワード暗号化タイプを選択します。 **3.** [Password] フィールドに、グループ内の AP に関連付けられているクライアントを認証するためのパスワードを入力します。 **4.** [Save] をクリックします。
Flex ローカル認証ユーザーの編集	**1.** 必要なユーザー名の横にあるチェックボックスをオンにします。 **2.** [アクション（Actions）] にカーソルを合わせて [編集（Edit）] をクリックします。 **3.** 必要な設定を編集します。 **4.** [Save] をクリックします。
Flex ローカル認証ユーザーの削除	**1.** 必要なユーザー名の横にあるチェックボックスをオンにします。 **2.** [アクション（Actions）] にカーソルを合わせて [削除（Delete）] をクリックします。 **3.** ダイアログボックスで、**Yes** をクリックします。

ステップ 7 （任意） [ポリシーACL（Policy ACL）] をクリックし、ACL を設定します。

実行する操作	結果
ポリシー ACL の追加	[追加（Add）] をクリックして、次の手順を完了します。 **1.** [ACL Name] ドロップダウンリストから、ACL を選択します。 ACL を作成する場合は、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の IPv4 ACL の作成 （940 ページ）」を参照してください。 **2.** ACL の中央 Web 認証を有効にするには、[Central Web Authentication] チェックボックスをオンにします。 **3.** [URL Filter] フィールドに、ACL の URL フィルタリストを入力します。 URL フィルタの作成については、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の基本的な URL フィルタの作成 （962 ページ）」および「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の拡張 URL フィルタの作成 （964 ページ）」を参照してください。 **4.** [Save] をクリックします。
ポリシー ACL の編集	**1.** 必要なポリシー ACL の横にあるチェックボックスをオンにします。 **2.** [アクション（Actions）] にカーソルを合わせて [編集（Edit）] をクリックします。 **3.** 必要な設定を編集します。 **4.** [Save] をクリックします。
ポリシー ACL の削除	**1.** 必要なポリシー ACL の横にあるチェックボックスをオンにします。 **2.** [アクション（Actions）] にカーソルを合わせて [削除（Delete）] をクリックします。 **3.** ダイアログボックスで、**Yes** をクリックします。

ステップ 8 （任意） [VLAN] をクリックして、VLAN を設定します。

実行する操作	結果
VLAN の追加	[追加（Add）] をクリックして、次の手順を完了します。 **1.** [VLAN Name] ドロップダウンリストから、VLAN 名を選択します。 VLAN を作成する場合は、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の VLAN プロファイルの作成 （1126 ページ）」を参照してください。 **2.** [ID] フィールドに、VLAN 名で識別される AP の ACL にマッピングする VLAN ID を入力します。 有効な範囲は 1 ～ 4096 です。デフォルト値は 1 です。 **3.** [Direction] で [Unidirectional] または [Bidirectional] オプションボタンをクリックします。 **4.** [単一方向（Unidirectional）] を選択した場合は、対応するドロップダウンリストから入力 ACL と出力 ACL を選択します。 • [入力ACL（Ingress ACL）]（ACL の作成については、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の IPv4 ACL の作成 （940 ページ）」を参照してください） • [出力ACL（Egress ACL）]（ACL の作成については、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の IPv4 ACL の作成 （940 ページ）」を参照してください） **5.** [双方向（Bidirectional）] を選択した場合は、[ACL名（Acl Name）] ドロップダウンリストから ACL を選択します。 ACL を作成する場合は、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の IPv4 ACL の作成 （940 ページ）」を参照してください。 **6.** [Save] をクリックします。
VLAN の編集	**1.** 必要な VLAN の横にあるチェックボックスをオンにします。 **2.** [アクション（Actions）] にカーソルを合わせて [編集（Edit）] をクリックします。 **3.** 必要な設定を編集します。 **4.** [Save] をクリックします。

実行する操作	結果
VLAN の削除	**1.** 必要な VLAN の横にあるチェックボックスをオンにします。 **2.** [アクション（Actions）] にカーソルを合わせて [削除（Delete）] をクリックします。 **3.** ダイアログボックスで、**Yes** をクリックします。

ステップ 9 （任意） [DNSレイヤセキュリティ（DNS Layer Security）] をクリックし、パラメータマップを設定します。

実行する操作	結果
パラメータマップの追加	[追加（Add）] をクリックして、次の手順を完了します。 **1.** [Parameter Map Name] フィールドに、Cisco Umbrella プロファイル名を入力します。 **2.** [Save] をクリックします。
パラメータマップの編集	**1.** 必要なパラメータマップの横にあるチェックボックスをオンにします。 **2.** [アクション（Actions）] にカーソルを合わせて [編集（Edit）] をクリックします。 **3.** 必要な設定を編集します。 **4.** [Save] をクリックします。
パラメータマップの削除	**1.** 必要なパラメータマップの横にあるチェックボックスをオンにします。 **2.** [アクション（Actions）] にカーソルを合わせて [削除（Delete）] をクリックします。 **3.** ダイアログボックスで、**Yes** をクリックします。

ステップ 10 [Review and Provision] をクリックします。

ステップ 11 ワイヤレスコントローラ がライセンス要件を満たしていない AP を管理している場合、Catalyst Center は詳細を示すダイアログボックスを表示します。ダイアログボックスで、必要なオプションを選択します。

オプション	説明
ライセンス マネージャ	[License Manager] ウィンドウを開いて、対応するライセンスを有効にします。 ライセンスを有効にするには、『*Cisco Catalyst Center Administrator Guide*』の「Manage Licenses」を参照してください。
[デバイスプロビジョニングに進む（Continue to device provision）]	デバイスのプロビジョニングを続行します。 （注） ライセンス要件を満たしていないAPは、ワールドワイドセーフモード（WWSM）になります。
Cancel	ダイアログボックスを閉じます。

ステップ 12 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 13 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のサイトタグの作成

この手順を使用して、ワイヤレスコントローラに関連付けられた AP のサイトタグを作成し、プロビジョニングします。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[AP]を展開し、[サイトタグ（Site Tags）] をクリックします。

ステップ 4 [Add] をクリックします。

ステップ 5 [サイトタグの作成（Create Site Tag）] スライドインペインの [サイトタグ名（Site Tag Name）] フィールドに、サイトタグの一意の名前を入力します。

サイトタグ名には、最大 32 文字の英数字と特殊文字を使用できます。 Catalyst Center は、サイトタグ名の先頭と末尾のスペースをサポートしていません。

ステップ 6 （任意） [Description] フィールドに、説明を入力します

説明には、最大 64 文字の英数字と特殊文字を使用できます。

ステップ 7 [AP Join Profile] ドロップダウンリストから、AP 接続プロファイルを選択します。

AP 参加プロファイルを作成するには、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの AP 参加プロファイルの作成 （867 ページ）」を参照してください。

ステップ 8 [ローカルサイト（Local Site）] チェックボックスをオンにして、ローカルサイトを有効にします。

このチェックボックスをオフにする場合、[フレックスプロファイル（Flex Profile）] ドロップダウンリストから、フレックスプロファイルを選択します。

フレックスプロファイルを作成するには、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの Flex プロファイルの作成 （899 ページ）」を参照してください。

ステップ 9 [Load] フィールドに、サイトによる相対的負荷の見積を入力します。

有効な範囲は 0 ～ 1000 です。デフォルト値は 0 です

AP 数を概算値として使用できます。

ステップ 10 [Review and Provision] をクリックします。

ステップ 11 ワイヤレスコントローラ がライセンス要件を満たしていない AP を管理している場合、Catalyst Center は詳細を示すダイアログボックスを表示します。ダイアログボックスで、必要なオプションを選択します。

オプション	説明
ライセンス マネージャ	[License Manager] ウィンドウを開いて、対応するライセンスを有効にします。 ライセンスを有効にするには、『*Cisco Catalyst Center Administrator Guide*』の「Manage Licenses」を参照してください。
[デバイスプロビジョニングに進む（Continue to device provision）]	デバイスのプロビジョニングを続行します。 （注） ライセンス要件を満たしていない AP は、ワールドワイドセーフモード（WWSM）になります。
Cancel	ダイアログボックスを閉じます。

ステップ 12 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 13 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のカレンダープロファイルの作成

カレンダープロファイルには、毎日、毎週、または毎月の繰り返しスケジュールを設定できます。電源ポリシーに関連付けられている場合、この設定により AP に接続されているインターフェイスの電源切断が自動化されます。この手順を使用して、ワイヤレスコントローラのカレンダープロファイルを作成し、プロビジョニングします。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[AP] を展開して [カレンダープロファイル（Calendar Profiles）] をクリックします。

ステップ 4 [Add] をクリックします。

ステップ 5 [カレンダープロファイルの作成（Create Calendar Profile）] スライドインペインの [プロファイル名（Profile Name）] フィールドに、カレンダープロファイルの名前を入力します。

ステップ 6 [周期（Recurrence）] で、カレンダープロファイルの繰り返し頻度を選択します。

- [毎日（Daily）] : 毎日カレンダー プロファイル ルールを適用します。
- [毎週（Weekly）] : 毎週選択した曜日にカレンダー プロファイル ルールを適用します。目的の曜日をクリックして選択します。
- [毎月（Monthly）] : 毎月選択した日にカレンダープロファイル ルールを適用します。目的の日付をクリックして選択します。

ステップ 7 [開始時刻（Start Time）] と [終了時刻（End Time）] で、繰り返しスケジュールの開始時刻と終了時刻を指定します。

ステップ 8 [Review and Provision] をクリックします。

ステップ 9 ワイヤレスコントローラ がライセンス要件を満たしていない AP を管理している場合、Catalyst Center は詳細を示すダイアログボックスを表示します。ダイアログボックスで、必要なオプションを選択します。

オプション	説明
ライセンス マネージャ	[License Manager] ウィンドウを開いて、対応するライセンスを有効にします。 ライセンスを有効にするには、『*Cisco Catalyst Center Administrator Guide*』の「Manage Licenses」を参照してください。
[デバイスプロビジョニングに進む（Continue to device provision）]	デバイスのプロビジョニングを続行します。 （注） ライセンス要件を満たしていない AP は、ワールドワイドセーフモード（WWSM）になります。
Cancel	ダイアログボックスを閉じます。

ステップ 10 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 11 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のタグマッピング設定

このセクションでは、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のデバイスごとのタグマッピング設定に関する情報を説明します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の AP プライミングプロファイルの作成

この手順を使用して、ワイヤレスコントローラ の AP プライミングプロファイルを作成し、プロビジョニングします。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[タブマッピング（Tag Mapping）] を展開し、[AP プライミング（AP Priming）] をクリックします。

ステップ 4 [Add] をクリックします。

ステップ 5 [APプライミングの作成（Create AP Priming）] スライドインペイン の [プロファイル名（Profile Name）] フィールドで、プライミングプロファイルの名前を入力します。

ステップ 6 （任意） 必要に応じて、ワイヤレスコントローラ 設定名と、これらのコントローラの AP に対応する ワイヤレスコントローラ IP アドレスを入力します。

- プライマリコントローラ
- セカンダリコントローラ
- ターシャリコントローラ

ステップ 7 （任意） [地理位置情報（Geolocation）]チェックボックスをオンにして、APプライミングプロファイルの地理的な場所を有効にします。

プロファイルの地理的場所を有効にする場合、必要に応じて次の両方のフィールドにデータを入力できます。

- **[Height (meters)]**：地上からの高さをメートル単位で入力します（最も近い整数に丸めます）。

  有効な範囲は 100 ～ 1000 です。

- **[Height Uncertainty (meters)]**：高さの不確実性をメートル単位で入力します。

  有効な範囲は 1 ～ 100 です。

ステップ 8 （任意） 設定済みのすべてのプライミングプロファイル属性を AP にプッシュするには、[プライミングのオーバーライド（Priming Override）] スライダを使用します。

ステップ 9 [Review and Provision] をクリックします。

ステップ 10 ワイヤレスコントローラ がライセンス要件を満たしていない AP を管理している場合、Catalyst Center は詳細を示すダイアログボックスを表示します。ダイアログボックスで、必要なオプションを選択します。

オプション	説明
ライセンス マネージャ	[License Manager] ウィンドウを開いて、対応するライセンスを有効にします。 ライセンスを有効にするには、『*Cisco Catalyst Center Administrator Guide*』の「Manage Licenses」を参照してください。
[デバイスプロビジョニングに進む（Continue to device provision）]	デバイスのプロビジョニングを続行します。 （注） ライセンス要件を満たしていないAPは、ワールドワイドセーフモード（WWSM）になります。
Cancel	ダイアログボックスを閉じます。

ステップ 11 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 12 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のタグ優先順位の設定

次の手順を使用して、ワイヤレスコントローラのタグ優先順位を設定し、プロビジョニングします。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラのリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、[デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[タグマッピング（Tag Mapping）] を展開して [タグマッピング（Tag Mapping）] をクリックします。

ステップ 4 （任意） [タグの優先順位（Tag Priority）] タブで、トグルボタンを使用して必要な設定を有効または無効にします。

- [ルールベース（Rule-Based）]：ルールベースのタグ優先順位設定の有効化または無効化
- [AP]：AP ベースのタグ優先順位設定の有効化または無効化

ステップ 5 （任意） [APタグの永続性（AP Tag Persistency）] チェックボックスをオンにして永続的な AP タグを有効にします。

ステップ 6 [Review and Provision] をクリックします。

ステップ 7 ワイヤレスコントローラ がライセンス要件を満たしていない AP を管理している場合、Catalyst Center は詳細を示すダイアログボックスを表示します。ダイアログボックスで、必要なオプションを選択します。

オプション	説明
ライセンス マネージャ	[License Manager] ウィンドウを開いて、対応するライセンスを有効にします。 ライセンスを有効にするには、『*Cisco Catalyst Center Administrator Guide*』の「Manage Licenses」を参照してください。
[デバイスプロビジョニングに進む（Continue to device provision）]	デバイスのプロビジョニングを続行します。 （注） ライセンス要件を満たしていない AP は、ワールドワイドセーフモード（WWSM）になります。
Cancel	ダイアログボックスを閉じます。

ステップ 8 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

ステップ 9 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの静的タグマッピングの作成

ワイヤレスコントローラ に関連付けられている AP の静的タグマッピングを作成してプロビジョニングするには、次の手順を実行します。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。

b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。

c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。

b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[タグマッピング（Tag Mapping）] を展開して [タグマッピング（Tag Mapping）] をクリックします。

ステップ 4 [静的（Static）] タブをクリックします。

ステップ 5 [Add] をクリックします。

ステップ 6 [アクセスポイントの追加（Add Access Point）] スライドインペインの [APイーサネットMACアドレス（AP Ethernet MAC Address）] フィールドに、AP のイーサネット MAC アドレスを入力します。

ステップ 7 次のドロップダウンリストから必要なタグを選択します。

- [ポリシータグ（Policy Tag）]：AP のポリシータグを選択します。
- [サイトタグ（Site Tag）]：AP のサイトタグを選択します。
- [RFタグ（RF Tag）]：AP の RF タグを選択します。

ステップ 8 [プライミングプロファイル（Priming Profile）] ドロップダウンリストから、APプライミングプロファイルを選択します。

AP プライミングプロファイルの作成については、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の AP プライミングプロファイルの作成 （909 ページ）」を参照してください。

ステップ 9 [Review and Provision] をクリックします。

ステップ 10 ワイヤレスコントローラ がライセンス要件を満たしていない AP を管理している場合、Catalyst Center は詳細を示すダイアログボックスを表示します。ダイアログボックスで、必要なオプションを選択します。

オプション	説明
ライセンス マネージャ	[License Manager] ウィンドウを開いて、対応するライセンスを有効にします。 ライセンスを有効にするには、『*Cisco Catalyst Center Administrator Guide*』の「Manage Licenses」を参照してください。

オプション	説明
[デバイスプロビジョニングに進む（Continue to device provision）]	デバイスのプロビジョニングを続行します。 （注） ライセンス要件を満たしていないAPは、ワールドワイドセーフモード（WWSM）になります。
Cancel	ダイアログボックスを閉じます。

ステップ 11 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 12 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のロケーションベースのタグマッピングルールの作成

次の手順を使用して、ワイヤレスコントローラに関連付けられたAPのロケーションベースのタグマッピングルールを作成し、プロビジョニングします。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[タグマッピング（Tag Mapping）] を展開して [タグマッピング（Tag Mapping）] をクリックします。

ステップ 4 [場所（Locations）] タブをクリックします。

ステップ 5 [Add] をクリックします。

ステップ 6 [ロケーションルールの作成（Create Location Rule）] スライドインペインの [一般（General）] タブで、次の設定を完了します。

a) [Location Name] フィールドに、AP ロケーションの名前を入力します。

b) （任意） [Description] フィールドに、説明を入力します

c) ドロップダウンリストから必要なタグを選択します。

- [サイトタグ（Site Tag）]：AP ロケーションのサイトタグを選択します。
- [ポリシータグ（Policy Tag）]：AP ロケーションのポリシータグを選択します。
- [RFタグ（RF Tag）]：AP ロケーションの RF タグを選択します。

ステップ 7 （任意） [APのプロビジョニング（AP Provisioning）] をクリックし、次の設定を完了します。

実行する操作	結果
非稼働 AP をルールに追加	**1.** [追加（Add）] にカーソルを合わせて [非稼働 AP（Non-Operational APs）] をクリックします。 **2.** [APの追加（Add AP）] ダイアログボックスの [AP MAC] フィールドに、AP の MAC アドレスを入力します。 **3.** [Save] をクリックします。
稼働 AP をルールに追加	**1.** [追加（Add）] にカーソルを合わせて [稼働AP（Operational APs）] をクリックします。 **2.** [APの追加（Add AP）] ダイアログボックスで、追加する AP の横にあるチェックボックスをオンにします。 特定の AP を検索するには、[検索（Search）] フィールドをクリックし、必要なフィルタオプションを選択します。次に、[Apply] をクリックします。 **3.** [Save] をクリックします。
ルールから AP を削除	**1.** 削除する AP の横にあるチェックボックスをオンにします。 **2.** [Actions] にカーソルを合わせて [Delete] を選択します。 **3.** ダイアログボックスで、**Yes** をクリックします。

ステップ 8 [Review and Provision] をクリックします。

ステップ 9 ワイヤレスコントローラ がライセンス要件を満たしていない AP を管理している場合、Catalyst Center は詳細を示すダイアログボックスを表示します。ダイアログボックスで、必要なオプションを選択します。

オプション	説明
ライセンス マネージャ	[License Manager] ウィンドウを開いて、対応するライセンスを有効にします。 ライセンスを有効にするには、『*Cisco Catalyst Center Administrator Guide*』の「Manage Licenses」を参照してください。
[デバイスプロビジョニングに進む（Continue to device provision）]	デバイスのプロビジョニングを続行します。 （注） ライセンス要件を満たしていないAPは、ワールドワイドセーフモード（WWSM）になります。
Cancel	ダイアログボックスを閉じます。

ステップ 10 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 11 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のルールベース タグマッピング プロファイルの作成

この手順を使用して、ワイヤレスコントローラ に関連付けられた AP のルールベースのタグマッピングプロファイルを作成し、プロビジョニングします。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。

b) デバイス情報を含むダイアログボックスで、[デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[タグマッピング（Tag Mapping）] を展開して [タグマッピング（Tag Mapping）] をクリックします。

ステップ 4 [Rule-Based] タブをクリックします。

ステップ 5 [Add] をクリックします。

ステップ 6 [正規表現ルールプロファイルの追加（Add Regex Rule Profile ）] スライドインペインの [ルール名（Rule Name）] フィールドに、ルールの名前を入力します。

ステップ 7 [AP Name Regex] フィールドに、AP 名をフィルタリングするための正規表現を入力します。

たとえば、AP 名が *ap-lab-12* の場合、AP 名に一致するように、**ap-lab** などの正規表現を使用してフィルタを設定できます。

ステップ 8 （任意） [アクティブ（Active）] トグルボタンを使用して、ルールを有効または無効にします。

ルールを有効にする場合、[優先順位（Priority）] フィールドにルールの優先順位を入力します。

0 を入力すると、ルールは非アクティブになります。アクティブなルールには有効な優先順位値を入力する必要があります。

ステップ 9 [タイプ（Type）] ドロップダウンリストから、プライミングタイプまたはタグタイプを選択します。

a) プライミングタイプの場合は、[プライミングプロファイル（Priming Profile）] ドロップダウンリストから AP のプライミングプロファイルを選択します。

（注） AP プライミングプロファイルを作成するには、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の AP プライミングプロファイルの作成 （909 ページ）」を参照してください。

b) タグタイプの場合は、次のドロップダウンリストから必要なタグを選択します。

- [ポリシータグ（Policy Tag）] : AP のポリシータグを選択します。
- [サイトタグ（Site Tag）] : AP のサイトタグを選択します。
- [RFタグ（RF Tag）] : AP の RF タグを選択します。

ステップ 10 [Review and Provision] をクリックします。

ステップ 11 ワイヤレスコントローラ がライセンス要件を満たしていない AP を管理している場合、Catalyst Center は詳細を示すダイアログボックスを表示します。ダイアログボックスで、必要なオプションを選択します。

オプション	説明
ライセンス マネージャ	[License Manager] ウィンドウを開いて、対応するライセンスを有効にします。 ライセンスを有効にするには、『*Cisco Catalyst Center Administrator Guide*』の「Manage Licenses」を参照してください。

オプション	説明
[デバイスプロビジョニングに進む（Continue to device provision）]	デバイスのプロビジョニングを続行します。 （注） ライセンス要件を満たしていないAPは、ワールドワイドセーフモード（WWSM）になります。
Cancel	ダイアログボックスを閉じます。

ステップ 12 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 13 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のセキュリティ設定

このセクションでは、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のデバイスごとのセキュリティ設定に関する情報を示します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の RADIUS サーバーの作成

次の手順を使用して、ワイヤレスコントローラ の RADIUS サーバーを作成し、プロビジョニングします。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。

b) デバイス情報を含むダイアログボックスで、[デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、[セキュリティ（Security）] を展開し、[AAA] をクリックします。

ステップ 4 [Servers/Groups] にカーソルを合わせ [RADIUS] の [Servers] をクリックします。

ステップ 5 [Add] をクリックします。

ステップ 6 [RADIUSサーバーの作成（Create RADIUS Server）] スライドインペインの [サーバー名（Server Name）] フィールドに、RADIUS サーバーグループの名前を入力します。

ステップ 7 [タイプ（Type）] ドロップダウンリストから、必要なタイプを選択します。

ステップ 8 RADIUS サーバーのタイプに応じて、対応するフィールドにデータを入力します。

- [サーバーIPアドレス（Server IP Address）] フィールドが表示される場合は、RADIUS サーバーの IPv4 アドレスを入力します。
- [サーバーIPv6アドレス（Server IPv6 Address）] フィールドが表示される場合は、RADIUS サーバーの IPv6 アドレスを入力します。
- [サーバーFQDN（Server FQDN）] フィールドが表示される場合は、RADIUS サーバーの FQDN を入力します。

ステップ 9 （任意） キーからプロキシ自動設定（PAC）キーに移行するには、[PACキー（PAC Key）] チェックボックスをオンにします。

ステップ 10 これらの設定を完了します。

次の場合は...	次の操作...
PAC キーを有効化	• [PACキータイプ（PAC Key Type）] ドロップダウンリストから、キータイプを選択します。 • [PACキー（PAC Key）] フィールドに、セキュア RADIUS サーバー認証用の PAC キーを入力します。 • [PACキーの確認（Confirm PAC Key）] フィールドで、PAC キーを確認します。
PAC キーを有効にしなかった	• [キータイプ（Key Type）] ドロップダウンリストから、キータイプを選択します。 • [キー（Key）] フィールドに、セキュア RADIUS サーバー認証用のキーを入力します。 • [キーの確認（Confirm Key）] フィールドで、キーを確認します。

ステップ 11 （任意） 次のフィールドにデータを入力します。

- [認証ポート（Authentication Port）]：認証要求と応答に使用する UDP ポート番号を入力します。

有効な値の範囲は 0 ～ 65534 です。デフォルト値は 1812 です。

- [アカウンティングポート（Accounting Port）]：アカウンティング要求と応答に使用する UDP ポート番号を入力します。

  有効な値の範囲は 0 ～ 65534 です。デフォルト値は 1813 です。

- [サーバータイムアウト（秒）（Server Timeout (sec)）]：RADIUS サーバーからの応答を待機する時間を秒単位で入力します。

  有効な範囲は 1 ～ 1000 です。

- [再試行回数（Retry Count）]：クライアントが RADIUS サーバーへの要求の再送信を試行できる回数を入力します。

  有効範囲は 0 ～ 100 です。

ステップ 12 （任意）ユーザーセッションに対する動的更新で認可変更（CoA）キーの変更を有効にするには、[CoA のサポート（Support for CoA）] チェックボックスをオンにします。

（注） タイプに [ホスト名（Hostname）] を選択した場合、このチェックボックスは使用できません。

（オプション）このチェックボックスをオンにする場合は、[CoAサーバーキータイプ（CoA Server Key Type）] ドロップダウンリストからオプションを選択します。

CoA サーバーキータイプを選択した場合は、これらのフィールドにデータを入力します。

- [CoAサーバーキー（CoA Server Key）]：CoA サーバーキーを入力します。
- [CoAサーバーキーの確認（Confirm CoA Server Key）]：キーを確認します。

ステップ 13 （任意）[自動テストツール（Automate Tester）] チェックボックスをオンにして、自動ネットワークテストを設定します。

このチェックボックスをオンにする場合は、次の設定を行います。

- [ユーザー名（Username）] フィールドに、RADIUS 要求に含めるテストユーザー名を入力します。
- （任意）対応する設定を有効にするには、必要なチェックボックスをオンにします。
  - [認証ポートを無視（Ignore Auth Port）]：サーバーの認証ポートのテストを無視します
  - [アカウンティングポートを無視（Ignore Acct Port）]：サーバーのアカウンティングポートのテストを無視します
  - [プローブの有効化（Enable Probe）]：プローブを有効にし、パケットを送信してサーバーステータスを確認します

    プローブを有効にしなかった場合、[アイドル時間（分）（Idle Time (minutes)）] フィールドに、サーバーの状態を確認する必要があるまでの時間を分単位で入力します。

    有効な範囲は 1 ～ 35791 です。

ステップ 14 [Review and Provision] をクリックします。

ステップ 15 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 16 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の RADIUS サーバーグループの作成

次の手順を使用して、ワイヤレスコントローラ の RADIUS サーバーグループを作成します。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、 [セキュリティ（Security）] を展開し、[AAA] をクリックします。

ステップ 4 [Servers/Groups] にカーソルを合わせ [RADIUS] で [Server Groups] をクリックします。

ステップ 5 [Add] をクリックします。

ステップ 6 [RADIUSサーバーグループの作成（Create RADIUS Server Group）] スライドインペインの [サーバーグループ名（Server Group Name）]フィールドに、RADIUS サーバーグループの名前を入力します。

ステップ 7 [MACデリミタ（MAC Delimiter）] ドロップダウンリストから、RADIUS 互換性モードの文字を選択します。

ステップ 8 [MACフィルタリング（MAC Filtering）] ドロップダウンリストから MAC フィルタリングオプションを選択します。

ステップ 9 （任意） [デッドタイム（分）（Dead Time (min)）] フィールドに、応答のないサーバーの使用を停止するまでの時間（単位）を入力します。

有効な範囲は 0 ～ 1440 です。

ステップ 10 （任意）RADIUS サーバーグループでのロードバランシングを有効にするには、[負荷分散（Load Balance）] チェックボックスをオンにします。

ステップ 11 ドロップダウンリストから、適切な IPv4 および IPv6 送信元インターフェイスを選択します。

RADIUS トラフィック用に、物理インターフェイス、論理インターフェイス、または SVI インターフェイスを選択できます。

ステップ 12 ドロップダウンリストから適切な IPv4 および IPv6 VRF を選択します。

ステップ 13 [サーバー（Servers）] で、次のいずれかのオプションを使用してサーバーを追加します。

- 必要なサーバーの横にあるプラスアイコンをクリックします。
- 必要なサーバーをクリックし、[選択項目を追加（Add Selected）] をクリックします。

  複数のサーバーを選択するには、[Shift] キーを押しながらサーバーをクリックし、[選択項目を追加（Add Selected）] をクリックします。
- すべてのサーバーを追加するには、[すべて追加（Add All）] をクリックします。

  [検索（Search）] フィールドを使用して、サーバーをフィルタ処理できます。

ステップ 14 [Review and Provision] をクリックします。

ステップ 15 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 16 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の TACACS+ サーバーの作成

次の手順を使用して、ワイヤレスコントローラの TACACS+ サーバープロファイルを作成します。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。

b) デバイス情報を含むダイアログボックスで、[デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、[セキュリティ（Security）] を展開し、[AAA] をクリックします。

ステップ 4 [Servers/Groups] にカーソルを合わせ、[TACACS+] で [Servers] をクリックします。

ステップ 5 [Add] をクリックします。

ステップ 6 [TACACS+サーバーの作成（Create TACACS+ Server）] スライドインペインの [サーバー名（Server Name）] フィールドに、TACACS+ サーバーの名前を入力します。

ステップ 7 [タイプ（Type）] ドロップダウンリストから、必要なタイプを選択します。

ステップ 8 TACACS+ サーバーのタイプに応じて、対応するフィールドにデータを入力します。

- [サーバーIPアドレス（Server IP Address）] フィールドが表示される場合は、TACACS+ サーバーの IPv4 アドレスを入力します。
- [サーバーIPv6アドレス（Server IPv6 Address）] フィールドが表示される場合は、TACACS+ サーバーの IPv6 アドレスを入力します。
- [サーバーFQDN（Server FQDN）] フィールドが表示される場合は、TACACS+ サーバーの FQDN を入力します。

ステップ 9 [キータイプ（Key Type）] ドロップダウンリストから、キータイプを選択します。

ステップ 10 [キー（Key）] フィールドに、セキュア認証のための TACACS+ サーバーのキーを入力します。

ステップ 11 [キーの確認（Confirm Key）] フィールドで、TACACS+ サーバーのキーを確認します。

ステップ 12 （任意） [Port] フィールドに、着信要求をリッスンするポート番号を入力します。

有効な範囲は 0 ～ 65535 です。デフォルト値は 49 です。

ステップ 13 （任意） [Server Timeout (sec)] フィールドに、TACACS+ サーバーからの応答を待機する時間を秒単位で入力します。

有効な範囲は 1 ～ 1000 です。

ステップ 14 [Review and Provision] をクリックします。

ステップ 15 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 16 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の TACACS+ サーバーグループの作成

次の手順を使用して、ワイヤレスコントローラのTACACS+サーバーグループを作成し、プロビジョニングします。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、 [セキュリティ（Security）] を展開し、[AAA] をクリックします。

ステップ 4 [サーバー/グループ（Servers/Groups）] にカーソルを合わせ、[TACACS+] で [サーバーグループ（Server Groups）] をクリックします。

ステップ 5 [Add] をクリックします。

ステップ 6 [TACACS+サーバーグループの作成（Create TACACS+ Server Group）]スライドインペイン の [サーバーグループ名（Server Group Name）] フィールドに、サーバーグループの名前を入力します。

ステップ 7 ドロップダウンリストから、適切な IPv4 および IPv6 送信元インターフェイスを選択します。

TACACS+トラフィック用に、物理インターフェイス、論理インターフェイス、またはSVIインターフェイスを選択できます。

ステップ 8 ドロップダウンリストから適切な IPv4 および IPv6 VRF を選択します。

ステップ 9 [サーバー（Servers）] で、次のいずれかのオプションを使用してサーバーを追加します。

- 必要なサーバーの横にあるプラスアイコンをクリックします。
- 必要なサーバーをクリックし、[選択項目を追加（Add Selected）] をクリックします。

  複数のサーバーを選択するには、[Shift] キーを押しながらサーバーをクリックし、[選択項目を追加（Add Selected）] をクリックします。
- すべてのサーバーを追加するには、[すべて追加（Add All）] をクリックします。

  [検索（Search）] フィールドを使用して、サーバーをフィルタ処理できます。

ステップ 10 [Review and Provision] をクリックします。

ステップ 11 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 12 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の LDAP サーバーの作成

この手順を使用して、ワイヤレスコントローラのLDAPサーバーを作成し、プロビジョニングします。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、 [セキュリティ（Security）] を展開し、[AAA] をクリックします。

ステップ 4 [サーバー/グループ（Servers/Groups）] にカーソルを合わせ、[LDAP] で [サーバー（Servers）] をクリックします。

ステップ 5 [Add] をクリックします。

ステップ 6 [LDAPサーバーの作成（Create LDAP Serve）] スライドインペインの [サーバー名（Server Name）] フィールドに、LDAP サーバーの名前を入力します。

ステップ 7 [タイプ（Type）] ドロップダウンリストから、必要なタイプを選択します。

ステップ 8 LDAP サーバーのタイプに応じて、対応するフィールドにデータを入力します。

- [サーバーIPアドレス（Server IP Address）] フィールドが表示される場合は、LDAP サーバーの IPv4 アドレスを入力します。
- [サーバーIPv6アドレス（Server IPv6 Address）] フィールドが表示される場合は、LDAP サーバーの IPv6 アドレスを入力します。

- [サーバーFQDN（Server FQDN）] フィールドが表示される場合は、LDAP サーバーの FQDN を入力します。

ステップ 9 （任意）[認証（Authenticate）] チェックボックスをオンにして、ワイヤレスコントローラと LDAP サーバー間のセキュアでコンプライアンスに準拠した接続を有効にします。

このチェックボックスをオンにした場合は、次のフィールドにデータを入力します。

- [バインドユーザー名（Bind Username）]：LDAP バインド操作のユーザー名を入力します。
- [バインドパスワード（Bind Password）]：LDAP バインド操作のパスワードを入力します。
- [バインドパスワードの確認（Confirm Bind Password）]：LDAP バインド操作用のパスワードを確認します。

ステップ 10 [ポート（Port）] フィールドに、サーバーの Listening ポート番号を入力します。

値の範囲は 1 ～ 65535 です。デフォルト値は 389 です。

ステップ 11 [ユーザーベースDN（User Based DN）] フィールドに、ベース識別名（DN）を入力します。

ステップ 12 （任意）[サーバータイムアウト（秒）（Server Timeout (sec)）] フィールドに、再送信の前に LDAP サーバーからの応答を待機する時間を秒単位で入力します。

値の範囲は 1 ～ 65535 です。デフォルト値は 30 です。

ステップ 13 （任意）[セキュアモード（Secure Mode）] チェックボックスをオンにして、ワイヤレスコントローラと LDAP サーバー間の通信が暗号化されていることを確認します。

（オプション）このチェックボックスをオンにする場合は、[トラストポイント名（Trustpoint Name）] ドロップダウンリストからトラストポイントを選択します。

ステップ 14 （任意）[ユーザーオブジェクトタイプ（User Object Types）] で、ユーザーオブジェクトタイプを設定します。

実行する操作	結果
ユーザーオブジェクトタイプの追加	**1.** [Add] をクリックします。 **2.** [ユーザーオブジェクトタイプ（User Object Type）] フィールドに、オブジェクトタイプ属性名を入力します。 **3.** [Save] をクリックします。
ユーザーオブジェクトタイプの削除	**1.** 削除するユーザーオブジェクトタイプの横にあるチェックボックスをオンにします。 **2.** **[Actions]** にカーソルを合わせ、**[Delete]** をクリックします。 **3.** ダイアログボックスで、**Yes** をクリックします。

ステップ 15 [Review and Provision] をクリックします。

ステップ 16 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 17 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の LDAP サーバーグループの作成

次の手順を使用して、ワイヤレスコントローラ のLDAPサーバーグループを作成し、プロビジョニングします。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、 [セキュリティ（Security）] を展開し、[AAA] をクリックします。

ステップ 4 [サーバー/グループ（Servers/Groups）] にカーソルを合わせ、[LDAP] で [サーバーグループ（Server Groups）] をクリックします。

ステップ 5 [Add] をクリックします。

ステップ 6 [LDAPサーバーグループの作成（Create LDAP Server Group）] スライドインペインの [サーバーグループ名（Server Group Name）] フィールドに、サーバーグループの名前を入力します。

ステップ 7 [サーバー（Servers）] で、次のいずれかのオプションを使用してサーバーを追加します。

- 必要なサーバーの横にあるプラスアイコンをクリックします。
- 必要なサーバーをクリックし、[選択項目を追加（Add Selected）] をクリックします。

  複数のサーバーを選択するには、[Shift] キーを押しながらサーバーをクリックし、[選択項目を追加（Add Selected）] をクリックします。

- すべてのサーバーを追加するには、[すべて追加（Add All）] をクリックします。

  [検索（Search）] フィールドを使用して、サーバーをフィルタ処理できます。

ステップ 8 [Review and Provision] をクリックします。

ステップ 9 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 10 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の認証方式リストの作成

次の手順を使用して、ワイヤレスコントローラ の認証方式リストを作成し、プロビジョニングします。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、 [セキュリティ（Security）] を展開し、[AAA] をクリックします。

ステップ 4 [AAA Method List] にカーソルを合わせ [Authentication] をクリックします。

ステップ 5 [追加（Add）] にカーソルを合わせて認証タイプを選択します。

- [タイプ-ログイン（Type - Login）]：AAA 認証用
- [タイプ- Dot1x（Type - Dot1x）]：Web 認証または TACACS 用

ステップ 6 [認証方式リストプロファイルの作成（Create Authentication Method List Profile）]スライドインペイン の [メソッドリスト名（Method List Name）] フィールドに、認証方式リストプロファイルの名前を入力します。

ステップ 7 [Group Type] ドロップダウンリストからオプションを選択します。

- [グループ（Group）]：AAA 認証用
- [ローカル（Local）]：ローカルデバイスの認証用

ステップ 8 （任意） [グループ（Group）] を選択した場合は、ローカルへのフォールバック（Fallback to Local）] チェックボックスをオンにして、ローカルユーザー名認証へのフォールバックを使用します。

ステップ 9 （任意） [サーバーグループ（Server Groups）] ドロップダウンリストからサーバーグループを選択します。

サーバーグループの作成については、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の RADIUS サーバーグループの作成 （921 ページ）」と「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の TACACS+ サーバーの作成 （922 ページ）」を参照してください。

ステップ 10 [Review and Provision] をクリックします。

ステップ 11 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

ステップ 12 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の認証方式リストの作成

次の手順を使用して、ワイヤレスコントローラ の認証方式リストを作成し、プロビジョニングします。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、[デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、[セキュリティ（Security）] を展開し、[AAA] をクリックします。

ステップ 4 [AAA Method List] にカーソルを合わせ [Authorization] をクリックします。

ステップ 5 [追加（Add）] にカーソルを合わせて認証タイプを選択します。

- [タイプ：ネットワーク（Type - Network）]
- [タイプ：EXEC（Type - Exec）]
- [タイプ：クレデンシャルダウンロード（Type - Credential-download）

MAC フィルタ認証の場合は、[タイプ：ネットワーク（Type - Network）]を選択します。

ステップ 6 [認証方式リストプロファイルの作成（Create Authorization Method List Profile）]スライドインペイン の [メソッドリスト名（Method List Name）] フィールドに、認証方式リストプロファイルの名前を入力します。

Catalyst Center では、方式リスト名にスペースまたは？を使用できません。

ステップ 7 [Group Type] ドロップダウンリストからオプションを選択します。

- [グループ（Group）]：AAA 認証用
- [ローカル（Local）]：ローカルデバイスでの認証用

ステップ 8 （任意） [グループ（Group）] を選択した場合は、ローカルへのフォールバック（Fallback to Local）] チェックボックスをオンにして、ローカルユーザー名認証へのフォールバックを使用します。

ステップ 9 （任意） 認証が完了したら、[認証済み（Authenticated）] チェックボックスをオンにして、成功を示します。

ステップ 10 （任意） [サーバーグループ（Server Groups）] ドロップダウンリストからサーバーグループを選択します。

サーバーグループの作成方法については、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の RADIUS サーバーグループの作成 （921 ページ）およびCisco Catalyst 9800 シリーズ ワイヤレス コントローラ の TACACS+ サーバーの作成 （922 ページ）を参照してください。

ステップ 11 [Review and Provision] をクリックします。

ステップ 12 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

ステップ 13 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のアカウンティング方式リストの作成

この手順を使用して、ワイヤレスコントローラ のアカウンティング方式リストを作成し、プロビジョニングします。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、 [セキュリティ（Security）] を展開し、[AAA] をクリックします。

ステップ 4 [AAA方式リスト（AAA Method List）] にカーソルを合わせて [アカウンティング（Accounting）] を選択します。

ステップ 5 [追加（Add）] にカーソルを合わせて AAA アカウンティングタイプを選択します。

- [タイプ：EXEC（Type - Exec）]
- [タイプ：ネットワーク（Type - Network）]
- **タイプ - アイデンティティ**
- **タイプ - コマンド**

AAA ベースのアカウンティングの場合は、[タイプ - アイデンティティ（Type - Identity）] を選択します。

ステップ 6 [アカウンティング方式リストプロファイルの作成（Create Accounting Method List Profile]スライドインペイン の [メソッドリスト名（Method List Name）] フィールドに、アカウンティング方式リストプロファイルの名前を入力します。

ステップ 7 [サーバーグループ（Server Groups）] ドロップダウンリストからアカウンティングのサーバーグループを選択します。

サーバーグループの作成については、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の RADIUS サーバーグループの作成 （921 ページ）」と「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の TACACS+ サーバーの作成 （922 ページ）」を参照してください。

ステップ 8 [Review and Provision] をクリックします。

ステップ 9 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 10 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のグローバル AAA パラメータの設定

ワイヤレスコントローラ のグローバル AAA パラメータを設定してプロビジョニングするには、次の手順を実行します。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、[デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、[セキュリティ（Security）] を展開し、[AAA] をクリックします。

ステップ 4 [AAAの詳細設定（AAA Advanced）] にカーソルを合わせ、[グローバル設定（Global Configuration）] を選択します。

ステップ 5 [グローバル設定（Global Configurations）] で、次の設定を完了します。

- [システム認証制御（System Auth Control）] チェックボックスを使用して、システム認証制御を有効または無効にします。
- [ローカル認証（Local Authentication）] ドロップダウンリストから認証を選択します。

選択内容	結果
なし（None）	ローカル承認には [なし（None）] を選択してください。

選択内容	結果
方式リスト	[認証方式リスト（Authentication Method List）] ドロップダウンリストから認証方式リストを選択します。 認証方式リストの作成については、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の認証方式リストの作成 （928 ページ）」を参照してください。

- [ローカル承認（Local Authorization）] ドロップダウンリストから承認を選択します。

選択内容	結果
なし（None）	ローカル認証には [なし（None）] を選択してください。
方式リスト	[承認方式リスト（Authorization Method List）] ドロップダウンリストから承認方式リストを選択します。 認証方式リストの作成については、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の認証方式リストの作成 （929 ページ）を参照してください。

- [RADIUSサーバーのロードバランシング（RADIUS Server Load Balance）] チェックボックスを使用して、RADIUS サーバーのロードバランシングを有効または無効にします。
- [中間更新（Interim Update）] チェックボックスを使用して、中間アカウンティング更新を有効または無効にします。

ステップ 6 [RADIUS属性-アカウンティング（RADIUS Attributes - Accounting）] で、次の設定を完了します。

- [Called-station-id] ドロップダウンリストから、Called-Station-ID として追加される属性を選択します。
- [Called-station-idの大文字小文字の設定（Called-station-id Case）] ドロップダウンリストから、Called-Station-ID で送信される値の大文字小文字オプションを選択します。
- （オプション）[MACデリミタ（MAC Delimiter）] ドロップダウンリストから、アカウンティングレコード内の MAC アドレスのオクテットを区切るために使用する文字を選択します。
- [ユーザー名の大文字小文字の設定（Username Case）] ドロップダウンリストから、ユーザー名の大文字小文字オプションを選択します。
- [ユーザー名デリミタ（Username Delimiter）] ドロップダウンリストから、ユーザー名のデリミタを選択します。

ステップ 7 [RADIUS属性-認証（RADIUS Attributes - Authentication）] で、次の設定を完了します。

- [Called-station-id] ドロップダウンリストから、Called-Station-ID として追加される属性を選択します。
- [Called-station-idの大文字小文字の設定（Called-station-id Case）] ドロップダウンリストから、Called-Station-ID で送信される値の大文字小文字オプションを選択します。

- [MACデリミタ（MAC Delimiter）] ドロップダウンリストから、アカウンティングレコード内の MAC アドレスのオクテットを区切るために使用する文字を選択します。

ステップ 8 [Review and Provision] をクリックします。

ステップ 9 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 10 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のパスワードポリシーの作成

この手順を使用して、ワイヤレスコントローラのパスワードポリシーを作成し、プロビジョニングします。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、 [セキュリティ（Security）] を展開し、[AAA] をクリックします。

ステップ 4 [AAA詳細設定（AAA Advanced）] にカーソルを合わせ、[パスワードポリシー（Password Policy）] を選択します。

ステップ 5 [Add] をクリックします。

ステップ 6 [パスワードポリシーの作成（Create Password Policy）] スライドインペイン の次のフィールドにデータを入力します。

- [パスワードポリシー名（Password Policy Name）] : パスワードポリシーの名前を入力します。
- [最小長（Minimum Length）] : パスワードの最小長を入力します。

有効な範囲は 1 ～ 127 です。デフォルト値は 1 です。

- [最大長（Maximum Length）]：パスワードの最大長を入力します。

  有効な範囲は 1 ～ 127 です。デフォルト値は 127 です。

- [大文字の数（Upper Count）]：パスワードに使用できる大文字の数を入力します。

  有効な範囲は 0 ～ 127 です。デフォルト値は 0 です

- [小文字の数（Lower Count）]：パスワードに使用できる小文字の数を入力します。

  有効な範囲は 0 ～ 127 です。デフォルト値は 0 です

- [数字の数（Numeric Count）]：パスワードで使用できる数字の数を入力します。

  有効な範囲は 0 ～ 127 です。デフォルト値は 0 です

- [特殊文字の数（Special Count）]：パスワードに使用できる特殊文字の数を入力します。

  有効な範囲は 0 ～ 127 です。デフォルト値は 0 です

- [文字変更の数（Character Changes）]：古いパスワードから新しいパスワードへ変更する際、変更する必要がある文字数を入力します。

  有効な範囲は 1 ～ 127 です。デフォルト値は 4 です。

- （オプション）[文字の最大連続重複制限（Max Number of Character Repetition）]：パスワード内の 1 つの文字を連続して繰り返す最大回数を入力します。

  有効な値は 0 および 2 ～ 5 です。デフォルト値は 0 ですこのルールを無効にするには、0 を入力します。

ステップ 7 （任意）パスワードでの、キーボード上の連続した文字または数字の使用を禁止するには、[キーボード配列の4文字連続並びの禁止（Prohibit Consecutive Four Keyboard Letters）] チェックボックスをオンにします。

このチェックボックスをオンにすると、キーボードの両方向で連続した 4 文字または数字をパスワードに含めることはできません。

ステップ 8 [有効性（Validity）] ドロップリストから、パスワードの有効性を選択します。

ユーザー定義の有効期限については、次のフィールドにデータを入力してください。

- [年（Years）]：パスワードの期限切れまでの年数を入力します。

  有効な範囲は 0 ～ 99 です。

- [月（Months）]：パスワードの期限切れまでの月数を入力します。

  有効な範囲は 0 ～ 11 です。

- [日（Days）]：パスワードの期限切れまでの日数を入力します。

  有効な範囲は 0 ～ 30 です。

- [時間（Hours）]：パスワードの期限切れまでの時間数を入力します。

有効な範囲は 0 ～ 23 です。

- [分（Minutes）] : パスワードの有効期限を分単位で入力します。

  有効な範囲は 0 ～ 59 です。

- [秒（Seconds）] : パスワードの期限切れまでの秒数を入力します。

  有効な範囲は 0 ～ 59 です。

ステップ 9 [Review and Provision] をクリックします。

ステップ 10 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 11 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の RADIUS フォールバックの設定

ワイヤレスコントローラ の RADIUS フォールバックを設定してプロビジョニングするには、次の手順を実行します。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラのリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、[デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、[セキュリティ（Security）] を展開し、[AAA] をクリックします。

ステップ 4 [AAA詳細設定（AAA Advanced）] にカーソルを合わせ、[RADIUSフォールバック（RADIUS Fallback）] を選択します。

ステップ 5 （任意） 次のフィールドにデータを入力します。

- [再送信回数（Retransmit Count）]：アクティブサーバーへの再試行回数を入力します。

  有効範囲は 0 ～ 100 です。

- [タイムアウト間隔（秒）（Timeout Interval (sec)）]：RADIUS サーバーが応答するまで待機する時間を秒単位で入力します。

  有効な範囲は 1 ～ 1000 です。

- [デッドタイム（分）（Dead Time (min)）]：応答のないサーバーの使用を停止するまでの時間を分単位で入力します。

  有効な範囲は 1 ～ 1440 です。

- [デッド条件時間（秒）（Dead Criteria Time (sec)）]：ネットワークの認証とアクセスが中断されないように、システムがバックアップサーバーに切り替える時間を決定するタイミングを秒単位で入力します。

  有効な範囲は 1 ～ 120 です。

- [デッド条件再試行回数（Dead Criteria Retries）]：RADIUS サーバーを非アクティブとしてマークするために、RADIUS サーバーからルータへの必要な連続応答失敗回数を入力します。

  有効な範囲は 1 ～ 100 です。

ステップ 6 [Review and Provision] をクリックします。

ステップ 7 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

ステップ 8 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の属性リストの作成

この手順を使用して、ワイヤレスコントローラの属性リストを作成し、プロビジョニングします。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。

b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。

c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、[デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、[セキュリティ（Security）] を展開し、[AAA] をクリックします。

ステップ 4 [AAA 詳細設定（AAA Advanced）] にカーソルを合わせ、[属性リスト（Attribute Lists）] を選択します。

ステップ 5 [Add] をクリックします。

ステップ 6 [属性リストの作成（Create Attribute List）] スライドインペイン の [属性リスト名（Attribute List Name）] フィールドに、属性リストの名前を入力します。

ステップ 7 （任意） [属性（Attributes）] で、必要な属性を設定します。

実行する操作	結果
属性の追加	**1.** [Add] をクリックします。 **2.** [属性の追加（Add Attribute）] ダイアログボックスで、次のフィールドにデータを入力します。 • [属性タイプ（Attribute Type）]：合理化されたユーザーアクセス制御の属性タイプの名前を入力します。 または、入力を開始すると、使用可能な属性タイプのリストが表示されます。このリストから必要な属性タイプを選択できます。 • [属性値（Attribute Value）]：選択した属性タイプに関連付けられる値を入力します。 または、[属性値（Attribute Value）] ドロップダウンリストが表示された場合は、必要な値を選択します。 **3.** [Save] をクリックします。
属性の削除	**1.** 必要な属性の横にあるチェックボックスをオンにします。 **2.** [アクション（Actions）] にカーソルを合わせて [削除（Delete）] を選択します。 **3.** ダイアログボックスで、**Yes** をクリックします。

ステップ 8 [Review and Provision] をクリックします。

ステップ 9 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 10 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の AAA ポリシーの作成

この手順を使用して、ワイヤレスコントローラ の AAA ポリシープロファイルを作成し、プロビジョニングします。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラのリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[セキュリティ（Security）] を展開し、[AAAポリシー（AAA Policy）] をクリックします。

ステップ 4 [Add] をクリックします。

ステップ 5 [AAAポリシープロファイルの作成（Create AAA Policy Profile）] スライドインペインの [ポリシー名（Policy Name）] フィールドに AAA ポリシーの名前を入力します。

ステップ 6 NAS ID オプションのドロップダウンリストから、必要な RADIUS NAS ID オプションを選択します。

ステップ 7 [Review and Provision] をクリックします。

ステップ 8 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 9 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の IPv4 ACL の作成

この手順を使用して、ワイヤレスコントローラのIPv4 ACLを作成し、プロビジョニングします。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、[セキュリティ（Security）] を展開し、[ACL] をクリックします。

ステップ 4 [IPv4/IPv6] にカーソルを合わせ、[IPv4] で、[標準（Standard）] を選択します。

ステップ 5 [Add] をクリックします。

ステップ 6 [IPv4標準ACLの作成（Create IPv4 Standard ACL）] スライドインペインの [ACL名（ACL Name）] フィールドに、IPv4 ACL の一意の名前を入力します。

ACL 名には最大 231 文字の英数字と特殊文字を含めることができます。数字のみを入力する場合、有効な範囲は 1 ～ 99 および 1300 ～ 1999 のいずれかです。ACL 名に特殊文字が含まれている場合は、アルファベットで始める必要があります。Catalyst Center では、ACL 名に ? とスペースは使用できません。

ステップ 7 （任意） [ルール（Rules）] で、必要なルールを設定します。

a) ルールを作成するには、次の手順を完了します。

1. [Add] をクリックします。
2. [ルールの追加（Add Rule）] ダイアログボックスの [シーケンス（Sequence）] フィールドに、ルールインデックスの一意の整数を入力します。

   1 ～ 2147483647 の範囲の値を指定できます。
3. [Action] ドロップダウンリストからアクションを選択します。

   • [許可（permit）] : トラフィックを許可します

   • [拒否（deny）] : トラフィックをブロックします

4. [送信元タイプ（Source Type）] ドロップダウンリストから、ルールに適用するトラフィック送信元を選択します。
   - [すべて（Any）]：すべての送信元 IPv4 アドレスからのトラフィックに適用されます。
   - [ホスト（Host）]：特定の IPv4 アドレスからのトラフィックに適用されます。

     [ホスト（Host）] を選択した場合は、[送信元IP（Source IP）] フィールドに送信元ホストの IP アドレスを入力します。Catalyst Center は、送信元ホストの IP アドレスとして 0.0.0.0 をサポートしていません。
   - [ネットワーク（Network）]：ネットワークからのトラフィックに適用されます。

     [ネットワーク（Network）] を選択した場合は、次のフィールドにデータを入力します。
     - [サブネットIP（Subnet IP）]：サブネット IP アドレスを入力します。Catalyst Center は、サブネット IP アドレスとして 0.0.0.0 をサポートしていません。
     - [送信元ワイルドカード（Source Wildcard）]：送信元に適用するワイルドカードビットを入力します。Catalyst Center は、ワイルドカードとして 0.0.0.0 をサポートしていません。
5. （オプション）このエントリに対する一致のログを作成するには、[ログ（Log）] チェックボックスをオンにします。
6. [Save] をクリックします。

b) ルールを編集するには、次の手順を実行します。
1. 必要なルールの横にあるチェックボックスをオンにします。
2. [アクション（Actions）] にカーソルを合わせて [編集（Edit）] を選択します。
3. 必要な設定を編集します。
4. [Save] をクリックします。

c) ルールを削除するには、次の手順を実行します。
1. 必要なルールの横にあるチェックボックスをオンにします。
2. [アクション（Actions）] にカーソルを合わせて [削除（Delete）] を選択します。
3. ダイアログボックスで、**Yes** をクリックします。

ステップ 8 [Review and Provision] をクリックします。

ステップ 9 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。

- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 10 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の IPv4 ロールベース ACL の作成

この手順を使用して、ワイヤレスコントローラの IPv4 ロールベース ACLを作成し、プロビジョニングします。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、[セキュリティ（Security）] を展開し、[ACL] をクリックします。

ステップ 4 [IPv4/IPv6] にカーソルを合わせ、[IPv4] で、[ロールベース（Role-based）] を選択します。

ステップ 5 [Add] をクリックします。

ステップ 6 [IPv4ロールベースACLの作成（Create IPv4 Role-based ACL）] スライドインペインの [ACL名（ACL Name）] フィールドに、IPv4 ACL の一意の名前を入力します。

ACL 名には最大 229 文字の英数字と特殊文字を含めることができます。ACL 名に特殊文字が含まれている場合は、アルファベットで始める必要があります。Catalyst Center では、ACL 名に ? とスペースは使用できません。

ステップ 7 （任意） [ルール（Rules）] で、必要なルールを設定します。

a) ルールを作成するには、次の手順を完了します。

1. [Add] をクリックします。
2. [ルールの追加（Add Rule）] ダイアログボックスの [シーケンス（Sequence）] フィールドに、ルールインデックスの一意の整数を入力します。

   有効な範囲は 1 ～ 2147483647 です。
3. [Action] ドロップダウンリストからアクションを選択します。

   - [許可（permit）]：トラフィックを許可します

- [拒否（deny）]：トラフィックをブロックします

4. [プロトコル（Protocol）]フィールドで、ルールに適用するプロトコルを指定します。0 ～ 255 の範囲の数値、または bgp、tcp、udp などの IOS キーワードを入力できます。

   TCP または UDP を使用する場合、次のドロップダウンリストからポート番号の評価方法を指定するポート演算子を選択します。

   - [送信元ポート演算子（Source Port Operator）]：送信元ポート演算子を選択します。

次を選択できます。	下記を実行
eq、**gt**、**lt**、または **neq**	[送信元ポート（Source Port）] フィールドに、送信元ポート番号、または bgp、bootpc、tacacs などの IOS サービスキーワードを入力します。 ポート番号と IOS サービスキーワードの両方が同じ数値範囲に対して検証されます。有効な範囲は 0 ～ 65535 です。
range	次のフィールドにポート番号の範囲を入力します。 • [開始送信元ポート（Start Source Port）]：開始送信元ポート番号、または bgp、bootpc、tacacs などの IOS サービスキーワードを入力します。 ポート番号と IOS サービスキーワードの両方が同じ数値範囲に対して検証されます。有効な範囲は 0 ～ 65535 です。 • [終了送信元ポート（End Source Port）]：終了送信元ポート番号、または bgp、bootpc、tacacs などの IOS サービスキーワードを入力します。 ポート番号と IOS サービスキーワードの両方が同じ数値範囲に対して検証されます。有効な範囲は 0 ～ 65535 です。

   - [接続先ポート演算子（Destination Port Operator）]：接続先ポート演算子を選択します。

次を選択できます。	下記を実行
eq、**gt**、**lt**、または **neq**	[宛先ポート（Destination Port）] フィールドに、宛先ポート番号、または bgp、bootpc、tacacs などの IOS サービスキーワードを入力します。 ポート番号と IOS サービスキーワードの両方が同じ数値範囲に対して検証されます。有効な範囲は 0 ～ 65535 です。

次を選択できます。	下記を実行
range	次のフィールドにポート番号の範囲を入力します。 • [開始宛先ポート（Start Destination Port）]：開始宛先ポート番号、またはbgp、bootpc、tacacsなどのIOSサービスキーワードを入力します。 ポート番号とIOSサービスキーワードの両方が同じ数値範囲に対して検証されます。有効な範囲は0 ～ 65535です。 • [終了宛先ポート（End Destination Port）]：終了宛先ポート番号、またはbgp、bootpc、tacacsなどのIOSサービスキーワードを入力します。 ポート番号とIOSサービスキーワードの両方が同じ数値範囲に対して検証されます。有効な範囲は0 ～ 65535です。

5. （オプション） [DSCP] ドロップダウンリストから、ルールの DSCP 値を選択します。
6. （オプション）このエントリに対する一致のログを作成するには、[ログ（Log）] チェックボックスをオンにします。
7. [Save] をクリックします。

b) ルールを編集するには、次の手順を実行します。

1. 必要なルールの横にあるチェックボックスをオンにします。
2. [アクション（Actions）] にカーソルを合わせて [編集（Edit）] を選択します。
3. 必要な設定を編集します。
4. [Save] をクリックします。

c) ルールを削除するには、次の手順を実行します。

1. 必要なルールの横にあるチェックボックスをオンにします。
2. [アクション（Actions）] にカーソルを合わせて [削除（Delete）] を選択します。
3. ダイアログボックスで、**Yes** をクリックします。

ステップ 8 [Review and Provision] をクリックします。

ステップ 9 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。

- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 10 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの IPv4 拡張 ACL の作成

ワイヤレスコントローラ の IPv4 拡張 ACL を作成してプロビジョニングするには、次の手順を実行します。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、[セキュリティ（Security）] を展開し、[ACL] をクリックします。

ステップ 4 [IPv4/IPv6] にカーソルを合わせ、[IPv4] で [拡張（Extended）] を選択します。

ステップ 5 [Add] をクリックします。

ステップ 6 [IPv4拡張ACLの作成（Create IPv4 Extended ACL）] スライドインペインの [ACL名（ACL Name）] フィールドに、IPv4 拡張 ACL の一意の名前を入力します。

ACL 名には最大 231 文字の英数字と特殊文字を含めることができます。数字のみを入力する場合、有効な範囲は 1 ～ 99 または 1300 ～ 1999 です。ACL 名に特殊文字が含まれている場合は、アルファベットで始める必要があります。Catalyst Center では、ACL 名に ? とスペースは使用できません。

ステップ 7 （任意） [ルール（Rules）] で、必要なルールを設定します。

a) ルールを作成するには、次の手順を完了します。

1. [Add] をクリックします。
2. [ルールの追加（Add Rule）] ダイアログボックスの [シーケンス（Sequence）] フィールドに、ルールインデックスの一意の整数を入力します。

   有効な範囲は 1 ～ 2147483647 です。
3. [Action] ドロップダウンリストからアクションを選択します。

   - [許可（permit）] : トラフィックを許可します

- [拒否（deny）]：トラフィックをブロックします

4. [送信元タイプ（Source Type）] ドロップダウンリストから、ルールに適用するトラフィック送信元を選択します。
   - [すべて（Any）]：すべての送信元 IPv4 アドレスからのトラフィックに適用されます。
   - [ホスト（Host）]：特定の IPv4 アドレスからのトラフィックに適用されます。

     [ホスト（Host）] を選択した場合は、[送信元IP（Source IP）] フィールドに送信元ホストの IP アドレスを入力します。Catalyst Center は、送信元ホストの IP アドレスとして 0.0.0.0 をサポートしていません。
   - [ネットワーク（Network）]：ネットワークからのトラフィックに適用されます。

     [ネットワーク（Network）] を選択した場合は、次のフィールドにデータを入力します。
     - [サブネットIP（Subnet IP）]：サブネット IP アドレスを入力します。Catalyst Center は、サブネット IP アドレスとして 0.0.0.0 をサポートしていません。
     - [送信元ワイルドカード（Source Wildcard）]：送信元に適用するワイルドカードビットを入力します。Catalyst Center は、ワイルドカードとして 0.0.0.0 をサポートしていません。

5. [接続先タイプ（Destination Type）] ドロップダウンリストから、ルールに適用するトラフィック接続先を選択します。
   - [任意（Any）]：任意の宛先 IPv4 アドレスへのトラフィックに適用されます。
   - [ホスト（Host）]：特定の IPv4 アドレスへのトラフィックに適用されます。

     [ホスト（Host）] を選択した場合は、[宛先IP（Destination IP）] フィールドに宛先ホストの IP アドレスを入力します。Catalyst Center は、宛先ホストの IP アドレスとして 0.0.0.0 をサポートしていません。
   - [ネットワーク（Network）]：ネットワークへのトラフィックに適用されます。

     [ネットワーク（Network）] を選択した場合は、次のフィールドにデータを入力します。
     - [サブネットIP（Subnet IP）]：サブネット IP アドレスを入力します。Catalyst Center は、サブネット IP アドレスとして 0.0.0.0 をサポートしていません。
     - [宛先ワイルドカード（Destination Wildcard）]：送信元に適用するワイルドカードビットを入力します。Catalyst Center は、ワイルドカードとして 0.0.0.0 をサポートしていません。

6. [プロトコル（Protocol）] フィールドで、ルールに適用するプロトコルを指定します。0 ～ 255 の範囲の数値、または bgp、tcp、udp などの IOS キーワードを入力できます。

   TCP または UDP を使用する場合、次のドロップダウンリストからポート番号の評価方法を指定するポート演算子を選択します。

- [送信元ポート演算子（Source Port Operator）]：送信元ポート演算子を選択します。

次を選択できます。	下記を実行
eq、**gt**、**lt**、または **neq**	[送信元ポート（Source Port）] フィールドに、送信元ポート番号、または bgp、bootpc、tacacs などの IOS サービスキーワードを入力します。 ポート番号と IOS サービスキーワードの両方が同じ数値範囲に対して検証されます。有効な範囲は 0 ～ 65535 です。
range	次のフィールドにポート番号の範囲を入力します。 • [開始送信元ポート（Start Source Port）]：開始送信元ポート番号、または bgp、bootpc、tacacs などの IOS サービスキーワードを入力します。 ポート番号と IOS サービスキーワードの両方が同じ数値範囲に対して検証されます。有効な範囲は 0 ～ 65535 です。 • [終了送信元ポート（End Source Port）]：終了送信元ポート番号、または bgp、bootpc、tacacs などの IOS サービスキーワードを入力します。 ポート番号と IOS サービスキーワードの両方が同じ数値範囲に対して検証されます。有効な範囲は 0 ～ 65535 です。

- [接続先ポート演算子（Destination Port Operator）]：接続先ポート演算子を選択します。

次を選択できます。	下記を実行
eq、**gt**、**lt**、または **neq**	[宛先ポート（Destination Port）] フィールドに、宛先ポート番号、または bgp、bootpc、tacacs などの IOS サービスキーワードを入力します。 ポート番号と IOS サービスキーワードの両方が同じ数値範囲に対して検証されます。有効な範囲は 0 ～ 65535 です。

次を選択できます。	下記を実行
range	次のフィールドにポート番号の範囲を入力します。 • [開始宛先ポート（Start Destination Port）]：開始宛先ポート番号、またはbgp、bootpc、tacacsなどのIOSサービスキーワードを入力します。 ポート番号とIOSサービスキーワードの両方が同じ数値範囲に対して検証されます。有効な範囲は0 ～ 65535です。 • [終了宛先ポート（End Destination Port）]：終了宛先ポート番号、またはbgp、bootpc、tacacsなどのIOSサービスキーワードを入力します。 ポート番号とIOSサービスキーワードの両方が同じ数値範囲に対して検証されます。有効な範囲は0 ～ 65535です。

7. （オプション）[DSCP] ドロップダウンリストから、ルールの DSCP 値を選択します。
8. [Save] をクリックします。

b) ルールを編集するには、次の手順を実行します。

1. 必要なルールの横にあるチェックボックスをオンにします。
2. [アクション（Actions）] にカーソルを合わせて [編集（Edit）] を選択します。
3. 必要な設定を編集します。
4. [Save] をクリックします。

c) ルールを削除するには、次の手順を実行します。

1. 必要なルールの横にあるチェックボックスをオンにします。
2. [アクション（Actions）] にカーソルを合わせて [削除（Delete）] を選択します。
3. ダイアログボックスで、**Yes** をクリックします。

ステップ 8 [Review and Provision] をクリックします。

ステップ 9 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 10 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の IPv6 ACL の作成

次の手順を実行して、ワイヤレスコントローラ の IPv6 ACL を作成し、プロビジョニングします。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、[セキュリティ（Security）] を展開し、[ACL] をクリックします。

ステップ 4 [IPv4/IPv6] にカーソルを合わせ、[IPv6] で、[IPv6] を選択します。

ステップ 5 [Add] をクリックします。

ステップ 6 [IPv6 ACLの作成（Create IPv6 ACL）] スライドインペインの [ACL名（ACL Name）] フィールドに、IPv6 ACL の一意の名前を入力します。

ACL名には最大233文字の英数字と特殊文字を含めることができます。数値で始めることはできません。Catalyst Center は ACL 名に？とスペースをサポートしていません。

ステップ 7 （任意） [ルール（Rules）] で、必要なルールを設定します。

a) ルールを作成するには、次の手順を完了します。

1. [Add] をクリックします。
2. [ルールの追加（Add Rule）] ダイアログボックスの [シーケンス（Sequence）] フィールドに、ルールインデックスの一意の整数を入力します。

   有効な範囲は 1 ～ 4294967294 です。
3. [Action] ドロップダウンリストからアクションを選択します。

   • [許可（permit）] : トラフィックを許可します

   • [拒否（deny）] : トラフィックをブロックします

4. [送信元タイプ（Source Type）] ドロップダウンリストから、ルールに適用するトラフィック送信元を選択します。
   - [任意（Any）]：任意の送信元 IPv6 アドレスからのトラフィックに適用されます。
   - [ホスト（Host）]：特定の IPv6 アドレスからのトラフィックに適用されます。

     [ホスト（Host）] を選択した場合は、[宛先IP（Source IP）] フィールドに、送信元ホストの有効な IPv6 アドレスを入力します。Catalyst Center は、IPv6 アドレスとして 0000:0000:0000:0000:0000:0000:0000:0000 または :: をサポートしていません。
   - [ネットワーク（Network）]：ネットワークからのトラフィックに適用されます。

     [ネットワーク（Network）] を選択した場合は、次のフィールドにデータを入力します。
     - [送信元IP（Source IP）]：送信元サブネット IP アドレスを入力します。Catalyst Center は、IPv6 アドレスとして 0000:0000:0000:0000:0000:0000:0000:0000 または :: をサポートしていません。
     - [送信元ワイルドカードビット（Source Wildcard Bits）]：送信元に適用するワイルドカードビットを入力します。Catalyst Center は、このフィールドの値として 0000:0000:0000:0000:0000:0000:0000:0000 または :: をサポートしていません。

5. [接続先タイプ（Destination Type）] ドロップダウンリストから、ルールに適用するトラフィック接続先を選択します。
   - [任意（Any）]：任意の宛先 IPv6 アドレスへのトラフィックに適用されます。
   - [ホスト（Host）]：特定の IPv6 アドレスへのトラフィックに適用されます。

     [ホスト（Host）] を選択した場合は、[宛先IP（Source IP）] フィールドに、宛先ホストの IP アドレスを入力します。Catalyst Center は、IPv6 アドレスとして 0000:0000:0000:0000:0000:0000:0000:0000 または :: をサポートしていません。
   - [ネットワーク（Network）]：ネットワークへのトラフィックに適用されます。

     [ネットワーク（Network）] を選択した場合は、次のフィールドにデータを入力します。
     - [宛先IP（Destination IP）]：宛先サブネット IP アドレスを入力します。Catalyst Center は、IPv6 アドレスとして 0000:0000:0000:0000:0000:0000:0000:0000 または :: をサポートしていません。
     - [宛先ワイルドカードビット（Destination Wildcard Bits）]：宛先に適用するワイルドカードビットを入力します。Catalyst Center は、このフィールドの値として 0000:0000:0000:0000:0000:0000:0000:0000 または :: をサポートしていません。

6. [プロトコル（Protocol）] フィールドで、ルールに適用するプロトコルを指定します。0 ～ 255 の範囲の数値、または bgp、tcp、udp などの IOS キーワードを入力できます。

   TCP または UDP を使用する場合、次のドロップダウンリストからポート番号の評価方法を指定するポート演算子を選択します。

- [送信元ポート演算子（Source Port Operator）]：送信元ポート演算子を選択します。

次を選択できます。	下記を実行
eq、**gt**、**lt**、または **neq**	[送信元ポート（Source Port）] フィールドに、送信元ポート番号、またはbgp、bootpc、tacacs などのIOSサービスキーワードを入力します。 ポート番号とIOSサービスキーワードの両方が同じ数値範囲に対して検証されます。有効な範囲は 0 ～ 65535 です。
range	次のフィールドにポート番号の範囲を入力します。 • [開始送信元ポート（Start Source Port）]：開始送信元ポート番号、または bgp、bootpc、tacacs などの IOS サービスキーワードを入力します。 ポート番号とIOSサービスキーワードの両方が同じ数値範囲に対して検証されます。有効な範囲は 0 ～ 65535 です。 • [終了送信元ポート（End Source Port）]：終了送信元ポート番号、またはbgp、bootpc、tacacs などのIOSサービスキーワードを入力します。 ポート番号とIOSサービスキーワードの両方が同じ数値範囲に対して検証されます。有効な範囲は 0 ～ 65535 です。

- [接続先ポート演算子（Destination Port Operator）]：接続先ポート演算子を選択します。

次を選択できます。	下記を実行
eq、**gt**、**lt**、または **neq**	[宛先ポート（Destination Port）] フィールドに、宛先ポート番号、またはbgp、bootpc、tacacs などのIOSサービスキーワードを入力します。 ポート番号とIOSサービスキーワードの両方が同じ数値範囲に対して検証されます。有効な範囲は 0 ～ 65535 です。

次を選択できます。	下記を実行
range	次のフィールドにポート番号の範囲を入力します。 • [開始宛先ポート（Start Destination Port）]：開始宛先ポート番号、またはbgp、bootpc、tacacsなどのIOSサービスキーワードを入力します。 ポート番号とIOSサービスキーワードの両方が同じ数値範囲に対して検証されます。有効な範囲は0 ～ 65535です。 • [終了宛先ポート（End Destination Port）]：終了宛先ポート番号、またはbgp、bootpc、tacacsなどのIOSサービスキーワードを入力します。 ポート番号とIOSサービスキーワードの両方が同じ数値範囲に対して検証されます。有効な範囲は0 ～ 65535です。

7. （オプション） [DSCP] ドロップダウンリストから、ルールの DSCP 値を選択します。
8. （オプション）このエントリに対する一致のログを作成するには、[ログ（Log）] チェックボックスをオンにします。
9. [Save] をクリックします。

b) ルールを編集するには、次の手順を実行します。

1. 必要なルールの横にあるチェックボックスをオンにします。
2. [アクション（Actions）] にカーソルを合わせて [編集（Edit）] を選択します。
3. 必要な設定を編集します。
4. [Save] をクリックします。

c) ルールを削除するには、次の手順を実行します。

1. 必要なルールの横にあるチェックボックスをオンにします。
2. [アクション（Actions）] にカーソルを合わせて [削除（Delete）] を選択します。
3. ダイアログボックスで、**Yes** をクリックします。

ステップ 8 [Review and Provision] をクリックします。

ステップ 9 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。

- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 10 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の IPv6 ロールベース ACL の作成

この手順を使用して、ワイヤレスコントローラの IPv6 ロールベース ACLを作成し、プロビジョニングします。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、[セキュリティ（Security）] を展開し、[ACL] をクリックします。

ステップ 4 [IPv4/IPv6] にカーソルを合わせ、[IPv6] で、[ロールベース（Role-based）] を選択します。

ステップ 5 [Add] をクリックします。

ステップ 6 [IPv6ロールベースACLの作成（Create IPv6 Role-based ACL）] スライドインペインの [ACL名（ACL Name）] フィールドに、IPv6 ACL の一意の名前を入力します。

ACL名には最大222文字の英数字と特殊文字を含めることができます。数値で始めることはできません。Catalyst Center は ACL 名に？とスペースをサポートしていません。

ステップ 7 （任意） [ルール（Rules）] で、必要なルールを設定します。

a) ルールを作成するには、次の手順を完了します。

1. [Add] をクリックします。
2. [ルールの追加（Add Rule）] ダイアログボックスの [シーケンス（Sequence）] フィールドに、ルールインデックスの一意の整数を入力します。

   有効な範囲は 1 ～ 4294967294 です。
3. [Action] ドロップダウンリストからアクションを選択します。

   - [許可（permit）]：トラフィックを許可します

- [拒否（deny）]：トラフィックをブロックします

4. [プロトコル（Protocol）]フィールドで、ルールに適用するプロトコルを指定します。0 ～ 255 の範囲の数値、または bgp、tcp、udp などの IOS キーワードを入力できます。

   TCP または UDP を使用する場合、次のドロップダウンリストからポート番号の評価方法を指定するポート演算子を選択します。

   - [送信元ポート演算子（Source Port Operator）]：送信元ポート演算子を選択します。

次を選択できます。	下記を実行
eq、**gt**、**lt**、または **neq**	[送信元ポート（Source Port）] フィールドに、送信元ポート番号、または bgp、bootpc、tacacs などの IOS サービスキーワードを入力します。 ポート番号と IOS サービスキーワードの両方が同じ数値範囲に対して検証されます。有効な範囲は 0 ～ 65535 です。
range	次のフィールドにポート番号の範囲を入力します。 • [開始送信元ポート（Start Source Port）]：開始送信元ポート番号、または bgp、bootpc、tacacs などの IOS サービスキーワードを入力します。 ポート番号と IOS サービスキーワードの両方が同じ数値範囲に対して検証されます。有効な範囲は 0 ～ 65535 です。 • [終了送信元ポート（End Source Port）]：終了送信元ポート番号、または bgp、bootpc、tacacs などの IOS サービスキーワードを入力します。 ポート番号と IOS サービスキーワードの両方が同じ数値範囲に対して検証されます。有効な範囲は 0 ～ 65535 です。

   - [接続先ポート演算子（Destination Port Operator）]：接続先ポート演算子を選択します。

次を選択できます。	下記を実行
eq、**gt**、**lt**、または **neq**	[宛先ポート（Destination Port）] フィールドに、宛先ポート番号、または bgp、bootpc、tacacs などの IOS サービスキーワードを入力します。 ポート番号と IOS サービスキーワードの両方が同じ数値範囲に対して検証されます。有効な範囲は 0 ～ 65535 です。

次を選択できます。	下記を実行
range	次のフィールドにポート番号の範囲を入力します。 • [開始宛先ポート（Start Destination Port）]：開始宛先ポート番号、またはbgp、bootpc、tacacsなどのIOSサービスキーワードを入力します。 ポート番号とIOSサービスキーワードの両方が同じ数値範囲に対して検証されます。有効な範囲は0 ～ 65535です。 • [終了宛先ポート（End Destination Port）]：終了宛先ポート番号、またはbgp、bootpc、tacacsなどのIOSサービスキーワードを入力します。 ポート番号とIOSサービスキーワードの両方が同じ数値範囲に対して検証されます。有効な範囲は0 ～ 65535です。

5. （オプション） [DSCP] ドロップダウンリストから、ルールの DSCP 値を選択します。
6. （オプション）このエントリに対する一致のログを作成するには、[ログ（Log）] チェックボックスをオンにします。
7. [Save] をクリックします。

b) ルールを編集するには、次の手順を実行します。

1. 必要なルールの横にあるチェックボックスをオンにします。
2. [アクション（Actions）] にカーソルを合わせて [編集（Edit）] を選択します。
3. 必要な設定を編集します。
4. [Save] をクリックします。

c) ルールを削除するには、次の手順を実行します。

1. 必要なルールの横にあるチェックボックスをオンにします。
2. [アクション（Actions）] にカーソルを合わせて [削除（Delete）] を選択します。
3. ダイアログボックスで、**Yes** をクリックします。

ステップ 8 [Review and Provision] をクリックします。

ステップ 9 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。

- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 10 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の MAC ベースの ACL の作成

次の手順を実行して、ワイヤレスコントローラ の MAC ベースの ACL を作成し、プロビジョニングします。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、[セキュリティ（Security）] を展開し、[ACL] をクリックします。

ステップ 4 [MACベース（MAC-Based）] タブをクリックします。

ステップ 5 [Add] をクリックします。

ステップ 6 [MACベースACLの作成（Create MAC-Based ACL）] スライドインペインの [ACL名（ACL Name）] フィールドに、MAC ベース ACL の一意の名前を入力します。

ACL 名には最大 230 文字の英数字と特殊文字を含めることができます。Catalyst Center では ACL 名に ? とスペースを使用できません。ACL 名に英数字または特殊文字が含まれている場合は、英字で始める必要があります。

ステップ 7 （任意） [ルール（Rules）] で、必要なルールを設定します。

a) ルールを作成するには、次の手順を完了します。

1. [Add] をクリックします。
2. [Action] ドロップダウンリストからアクションを選択します。
   - [許可（permit）]：トラフィックを許可します
   - [拒否（deny）]：トラフィックをブロックします

3. [送信元タイプ（Source Type）] ドロップダウンリストから、ルールに適用するトラフィック送信元を選択します。
   - [任意（Any）]：任意の送信元 MAC アドレスからのトラフィックに適用されます。
   - [ホスト（Host）]：特定の MAC アドレスからのトラフィックに適用されます。

     [ホスト（Host）] を選択した場合、[送信元MAC（Source MAC）] フィールドに送信元 MAC アドレスを入力します。*xxxx.xxxx.xxxx*、*xx-xx-xx-xx-xx-xx*、または *xx:xx:xx:xx:xx:xx* のいずれかの形式で MAC アドレスを入力します。
   - [ネットワーク（Network）]：ネットワークからのトラフィックに適用されます。

     [ネットワーク（Network）] を選択した場合は、次のフィールドにデータを入力します。
     - [送信元MAC（Source MAC）]：送信元の MAC アドレスを入力します。*xxxx.xxxx.xxxx*、*xx-xx-xx-xx-xx-xx*、または *xx:xx:xx:xx:xx:xx* のいずれかの形式で MAC アドレスを入力します。
     - [送信元MACワイルドカード（Source MAC Wildcard）]：送信元に適用するワイルドカードビットを入力します。*xxxx.xxxx.xxxx*、*xx-xx-xx-xx-xx-xx*、または *xx:xx:xx:xx:xx:xx* のいずれかの形式で MAC アドレスを入力します。

4. [接続先タイプ（Destination Type）] ドロップダウンリストから、ルールに適用するトラフィック接続先を選択します。
   - [任意（Any）]：任意の接続先 MAC アドレスへのトラフィックに適用されます。
   - [ホスト（Host）]：特定の MAC アドレスへのトラフィックに適用されます。

     [ホスト（Host）] を選択した場合、[接続先MAC（Destination MAC）] フィールドに接続先の MAC アドレスを入力します。*xxxx.xxxx.xxxx*、*xx-xx-xx-xx-xx-xx*、または *xx:xx:xx:xx:xx:xx* のいずれかの形式で MAC アドレスを入力します。
   - [ネットワーク（Network）]：ネットワークへのトラフィックに適用されます。

     [ネットワーク（Network）] を選択した場合は、次のフィールドにデータを入力します。
     - [接続先MAC（Destination MAC）]：接続先の MAC アドレスを入力します。*xxxx.xxxx.xxxx*、*xx-xx-xx-xx-xx-xx*、または *xx:xx:xx:xx:xx:xx* のいずれかの形式で MAC アドレスを入力します。
     - [接続先MACワイルドカード（Destination MAC Wildcard）]：宛先に適用されるワイルドカードビットを入力します。*xxxx.xxxx.xxxx*、*xx-xx-xx-xx-xx-xx*、または *xx:xx:xx:xx:xx:xx* のいずれかの形式で MAC アドレスを入力します。

5. [Save] をクリックします。

b) ルールを編集するには、次の手順を実行します。

1. 必要なルールの横にあるチェックボックスをオンにします。

2. [アクション（Actions）] にカーソルを合わせて [編集（Edit）] を選択します。
3. 必要な設定を編集します。
4. [Save] をクリックします。

c) ルールを削除するには、次の手順を実行します。

1. 必要なルールの横にあるチェックボックスをオンにします。
2. [アクション（Actions）] にカーソルを合わせて [削除（Delete）] を選択します。
3. ダイアログボックスで、**Yes** をクリックします。

ステップ 8 [Review and Provision] をクリックします。

ステップ 9 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 10 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のローカル EAP プロファイルの作成

この手順を使用して、ワイヤレスコントローラのローカル EAP プロファイルを作成し、プロビジョニングします。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、[デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[セキュリティ（Security）] を展開し、[EAP] をクリックします。

ステップ 4 [Local EAP Profiles] タブで [Add] をクリックします。

ステップ 5 [ローカルEAPプロファイルの作成（Create Local EAP Profiles）] スライドインペイン の [ローカルEAPプロファイル名（Local EAP Profile Name）] フィールドに、ローカル EAP プロファイルの名前を入力します。

プロファイル名には最大 63 文字の英数字と特殊文字を含めることができます。

ステップ 6 （任意） 対応する EAP メソッドを許可するために、必要なチェックボックスをオンにします。

ステップ 7 （任意） 選択した EAP メソッドに基づいて、次の設定を完了します。

選択内容	結果
EAP-TLS、EAP-FAST、または PEAP	[トラストポイント名（Trustpoint Name）] ドロップダウンリストからデフォルトの Public Key Infrastructure（PKI）トラストポイントを選択します。
EAP-FAST	[EAP FASTプロファイル（EAP-FAST Profile）] ドロップダウンリストから、EAP FAST プロファイルを選択します。 EAP-FAST プロファイルの作成については、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の EAP-FAST プロファイルの作成（959 ページ）」を参照してください。

ステップ 8 [Review and Provision] をクリックします。

ステップ 9 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 10 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の EAP-FAST プロファイルの作成

この手順を使用して、ワイヤレスコントローラ の EAP-FAST プロファイルを作成し、プロビジョニングします。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラのリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、[デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[セキュリティ（Security）] を展開し、[EAP] をクリックします。

ステップ 4 [EAP-FAST Profiles] タブをクリックします。

ステップ 5 [Add] をクリックします。

ステップ 6 [EAP-FASTプロファイルの作成（Create EAP-FAST Profiles）] スライドインペインで、次のフィールドにデータを入力します。

- [EAP-FASTプロファイル名（EAP-FAST Profile Name）] フィールドに、EAP-FAST プロファイルの固有名を入力します。

  プロファイル名には最大 63 文字の英数字と特殊文字を含めることができます。

- [サーバーキー（Server Key）]：プロファイルのローカルキーを入力します。
- [サーバーキーの確認（Confirm Server Key）]：同じプロファイルのローカルキーを再入力します。
- [存続可能時間（秒）（Time to Live (sec)）]：Protected Access Credential（PAC）の存続可能時間を秒単位で入力します。

  有効な範囲は 1 ～ 700,000,000 です。デフォルト値は 86400 です。

- （オプション）[認証局ID（Authority ID）]：プロファイルの認証局 ID を入力します。

  認証局 ID には最大 231 文字の英数字と特殊文字を含めることができます。

- （オプション）[認証局ID情報（Authority ID Information）]：認証局 ID 情報を入力します。

  認証局 ID 情報には、最大 228 文字の英数字および特殊文字を含めることができます。

- （オプション）[説明（Description）]：説明を入力します。

  説明には最大 241 文字の英数字および特殊文字を含めることができます。

ステップ 7 [Review and Provision] をクリックします。

ステップ 8 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

ステップ 9 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の高度な EAP の設定

この手順を使用して、ワイヤレスコントローラ に高度な EAP プロファイルを設定し、プロビジョニングします。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[セキュリティ（Security）] を展開し、[EAP] をクリックします。

ステップ 4 [Advanced] タブをクリックします。

ステップ 5 次のフィールドにデータを入力します。

- [EAPアイデンティティ要求タイムアウト（秒）（EAP-Identity-Request Timeout (sec)）]：EAP アイデンティティ要求のタイムアウトを秒単位で入力します。

  有効な範囲は 1 ～ 120 です。デフォルト値は 40 です。

- [EAPアイデンティティ要求の最大再試行数（EAP-Identity-Request Max Retries）]：EAP アイデンティティ要求の最大再送信回数を入力します。

  有効な範囲は、1 ～ 20 です。デフォルト値は 2 です。

ステップ 6 （任意） [EAP最大ログインID応答無視（EAP Max-Login Ignore Identity Response）] チェックボックスをオンにして、同じユーザー名でデバイスに接続できるクライアントの数を制限します。

ステップ 7 次のフィールドにデータを入力します。

- [EAP要求タイムアウト（秒）（EAP-Request Timeout (sec)）]：EAP 要求の再送信タイムアウトを秒単位で入力します。

  有効な範囲は 1 ～ 120 です。デフォルト値は 30 です。

- [EAP要求最大試行回数（EAP-Request Max Retries）]：EAP 要求の最大再送信回数を入力します。

  有効な範囲は 0 ～ 20 です。デフォルト値は 2 です。

- [EAPOLキータイムアウト（ミリ秒）（EAPOL-Key Timeout (msec)）] フィールドに、EAP over LAN（EAPOL）キー再送信タイムアウトをミリ秒単位で入力します。

  有効な範囲は 200 ～ 5000 です。デフォルト値は 1000 です。

- [EAPOLキー最大試行回数（EAPOL-Key Max Retries ）] フィールドに、EAPOL キーの最大再試行回数を入力します。

  有効な範囲は 0 ～ 4 です。デフォルト値は 2 です。

- [EAPブロードキャストキー間隔（秒）（EAP-Broadcast Key Interval (sec)）] フィールドに、EAP ブロードキャストキーの更新間隔を秒単位で入力します。

  有効な範囲は 120 ～ 86400 です。デフォルト値は 3600 です。

ステップ 8 [Review and Provision] をクリックします。

ステップ 9 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 10 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の基本的な URL フィルタの作成

ワイヤレスコントローラ の基本的な URL フィルタを作成してプロビジョニングするには、次の手順を実行します。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、[デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[セキュリティ（Security）] を展開して [URLフィルタ（URL Filters）] をクリックします。

ステップ 4 [Basic] タブで [Add] をクリックします。

ステップ 5 [基本的なURLフィルタの作成（Create Basic URL Filter）] スライドインペインの [URLリスト名（Url List Name）] フィールドに、URL フィルタの一意の名前を入力します。

URL フィルタ名には最大 32 文字を含めることができます。Catalyst Center では、URL フィルタ名に ? # % + ' またはスペースを含めることはできません。

ステップ 6 [フィルタタイプ（Filter Type）] ドロップダウンリストから、URL フィルタに使用する認証を選択します。

[事後認証（POST-AUTH）] を選択した場合は、次のフィールドにデータを入力します。

- [IPv4リダイレクトサーバー（IPv4 Redirect Server）] : リダイレクトサーバーの IPv4 アドレスを入力します。
- [IPv6リダイレクトサーバー（IPv6 Redirect Server）] : リダイレクトサーバーの IPv6 アドレスを入力します。

ステップ 7 [アクション（Action）] ドロップダウンリストから、URL フィルタ内の URL を許可またはブロックするかどうかを示すアクションを選択します。

ステップ 8 （任意） [URL（URLs）] で、URL フィルタの URL ドメイン名を設定します。

実行する操作	結果
URL フィルタに URL ドメイン名を追加する	**1.** [Add] をクリックします。 **2.** [Add URL] ダイアログボックスの [Url Name] フィールドに、URL フィルタのドメイン名を入力します。 ドメイン名には最大 255 文字を含めることができます。Catalyst Center では、ドメイン名に特殊文字 - _ . * を含めることができます。* はワイルドカード文字として使用されます（*cisco.com など）。Catalyst Center はバックスラッシュ（/）を使用したサブドメインをサポートしていません。 **3.** [Save] をクリックします。
URL フィルタからドメイン名を削除する	**1.** 削除するドメイン名の横にあるチェックボックスをオンにします。 **2.** [Actions] にカーソルを合わせて [Delete] を選択します。 **3.** ダイアログボックスで、**Yes** をクリックします。

ステップ 9 [Review and Provision] をクリックします。

ステップ 10 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 11 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の拡張 URL フィルタの作成

拡張 URL フィルタは、ワイヤレスネットワークに適用される完全修飾ドメイン名（FQDN）ACL です。

次の手順を使用して、ワイヤレスコントローラ の拡張 URL フィルタを作成し、プロビジョニングします。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[セキュリティ（Security）] を展開して [URLフィルタ（URL Filters）] をクリックします。

ステップ 4 [拡張（Enhanced）] タブをクリックします。

ステップ 5 [Add] をクリックします。

ステップ 6 [拡張URLフィルタを作成（Create Enhanced URL Filter）] スライドインペイン の [URLリスト名（Url List Name）] フィールドに、URL フィルタの一意の名前を入力します。

URL フィルタ名には最大 32 文字を含めることができます。Catalyst Center では、URL フィルタ名に ? # % + ' またはスペースを含めることはできません。

ステップ 7 （任意） [ルール（Rules）] で、URL フィルタのルールを設定します。

実行する操作	結果
ルールの追加	1. [Add] をクリックします。 2. [**Add URL**] ダイアログボックスの [**URL**] フィールドに、拡張URLルールの URL、FQDN、またはドメイン名を入力します。 ドメイン名には最大 255 文字を含めることができます。Catalyst Center では、ドメイン名に特殊文字 - _ . * を含めることができます。* はワイルドカード文字として使用されます（*cisco.com など）。Catalyst Center はバックスラッシュ（/）を使用したサブドメインをサポートしていません。 3. [Preference] フィールドに、ルールの優先順位を入力します。 有効な範囲は 0 ～ 65535 です。 4. [Save] をクリックします。 5. [Action] ドロップダウンリストからアクションを選択します。
ルールの編集	1. 必要なルールの横にあるチェックボックスをオンにします。 2. [Actions] にカーソルを合わせて [Edit] を選択します。 3. [Action] ドロップダウンリストから、ルールのアクションを更新します。 4. [Save] をクリックします。
ルールの削除	1. 削除するルールの横にあるチェックボックスをオンにします。 2. [Actions] にカーソルを合わせて [Delete] を選択します。 3. ダイアログボックスで、**Yes** をクリックします。

ステップ 8 [Review and Provision] をクリックします。

ステップ 9 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 10 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のゲストユーザーの作成

次の手順を使用して、ワイヤレスコントローラ のゲストユーザーを作成し、プロビジョニングします。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。

b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。

c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。

b) デバイス情報を含むダイアログボックスで、[デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、[セキュリティ（Security）] を展開し、[ゲストユーザー（Guest User）] をクリックします。

ステップ 4 [Add] をクリックします。

ステップ 5 [ゲストユーザーの作成（Create Guest User）] スライドインペイン の、[一般（General）] で次の設定を完了します。

- [User Name] フィールドに、ゲストユーザーのユーザー名を入力します。
- （オプション）[パスワードの生成（Generate Password）] チェックボックスをオンにして、ゲストユーザーのパスワードを生成します。
- [Password] フィールドに、ゲストユーザーのパスワードを入力します。



（注） [Generate Password] チェックボックスをオンにすると、このフィールドは自動的に入力されます。

- **[Confirm Password]** フィールドにパスワードを再入力します。



（注） [Generate Password] チェックボックスをオンにすると、このフィールドは自動的に入力されます。

- [Description] フィールドに、説明を入力します

- [No. of Simultaneous User Logins] フィールドに、ゲストユーザーに許可される同時ログイン試行の最大数を入力します。

  有効な範囲は 0 ～ 64 です。

ステップ 6 [有効期間（Lifetime）] で、次のフィールドにデータを入力します。

- [年（Years）] : ゲストユーザーログイン情報を使用できる年数を入力します。

  有効な範囲は 0 ～ 1 です。デフォルト値は 0 です

- [月（Months）] : ゲストユーザーログイン情報を使用できる月数を入力します。

  有効な範囲は 0 ～ 11 です。デフォルト値は 0 です

- [日（Days）] : ゲストユーザーログイン情報を使用できる日数を入力します。

  有効な範囲は 0 ～ 30 です。デフォルト値は 1 です。

- [時間（Hours）] : ゲストユーザーログイン情報を使用できる時間数を入力します。

  有効な範囲は 0 ～ 23 です。デフォルト値は 0 です

- （オプション）[分（Minutes）] : ゲストユーザーログイン情報を使用できる分数を入力します。

  有効な範囲は 0 ～ 59 です。デフォルト値は 0 です

ステップ 7 [Review and Provision] をクリックします。

ステップ 8 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

ステップ 9 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の Web 認証パラメータの設定

ワイヤレスコントローラ の Web 認証パラメータを設定してプロビジョニングするには、次の手順を実行します。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。

b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、[デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[セキュリティ（Security）] を展開して [Web認証（Web Auth）] をクリックします。

ステップ 4 [グローバル（Global）] タブで、次の設定を完了します。

a) [一般（General）] で、次の設定を完了します。

- （任意）[Maximum HTTP connections] フィールドに、クライアントごとに許可する HTTP 接続の最大数を入力します。

  有効値は 1 ～ 200 です。

- [Init-State Timeout(secs)] フィールドに、タイムアウトを秒単位で入力します。

  有効な範囲は 60 ～ 3932100 です。

- [タイプ（Type）] ドロップダウンリストから認証タイプを選択します。
- （オプション）認証タイプ [承認（consent）] を選択した場合、電子メールによる承認を有効にするには、[電子メールを使用した承認の有効化（Turn-On Consent with Email）] チェックボックスをオンにします。
- （任意）対応する設定を有効にするには、必要なチェックボックスをオンにします。
  - [キャプティブバイパスポータル（Captive Bypass Portal）]：Web 認証のキャプティブバイパスを有効にします
  - [成功ウィンドウの無効化（Disable Success Window）]：Web 認証に成功した後に、ワイヤレスコントローラのデフォルトの成功ウィンドウを無効にします。
  - [ログアウトウィンドウの無効化（Disable Logout Window）]：Web 認証のログアウトウィンドウを無効にします。
  - [シスコのロゴの無効化（Disable Cisco Logo）]：内部 HTML ウィンドウでシスコのロゴを無効にします。
- （オプション）次のフィールドにデータを入力します。
  - [スリープ状態のクライアントのタイムアウト（分）（Sleeping Client Timeout (Minutes)）]：クライアントのスリープタイムアウトを分単位で入力します。

    有効な範囲は 10 ～ 43200 です。
  - [トラストポイント（Trustpoint）]：トラストポイント名を入力します。
  - [仮想IPv4アドレス（Virtual IPv4 Address）]：仮想 IPv4 アドレスを入力します。

- [仮想IPv6アドレス（Virtual IPv6 Address）]：仮想 IPv6 アドレスを入力します。

- （任意）対応する設定を有効にするには、必要なチェックボックスをオンにします。
  - [Web認証代行受信HTTPS（Web Auth intercept HTTPS）]：HTTPS トラフィックの代行受信を有効にします。
  - [Web認証用HTTPS サーバーの有効化（Enable HTTP server for Web Auth）]：Web 認証用の HTTPS サーバーを設定します。
  - [Web認証用HTTPS サーバーの無効化（Disable HTTP server for Web Auth）]：Web 認証用の HTTPS サーバーを無効にします。

b) （任意）[バナー設定（Banner Configuration）] で、次の設定を完了します。

- [Banner Title] フィールドに、バナータイトルのテキストを入力します。

  最大 127 文字を入力することができます。例：*c* **banner-title-text** *c*、*c* はデリミタです。

- [バナータイプ（Banner Type）] で、必要なオプションの横にあるオプションボタンをクリックします。

選択内容	結果
バナー テキスト（Banner Text）	[バナーテキスト（Banner Text）] フィールドに、バナーに表示するテキストを入力します。 最大 400 文字を入力できます。例：*c* **banner-text** *c*、*c* はデリミタです。
ファイル名	[読み取り元ファイル（Read from File）] フィールドに、バナーテキストの読み取り元ファイルの名前を入力します。

c) （任意）[外部サーバーへのリダイレクト（Redirect to external server）] で、外部 Web 認証用のデータを次のフィールドに入力します。

- [ログイン用のリダイレクトURL（Redirect URL for login）]：ログイン要求のためにユーザーをリダイレクトする URL を入力します。

  最大 230 文字を入力できます。

- [成功時のリダイレクト（Redirect On-Success）] フィールドに、ログインが成功した後にユーザーをリダイレクトする URL を入力します。

  最大 230 文字を入力できます。

- [失敗時のリダイレクト（Redirect On-Failure）] フィールドに、ログインが失敗した後にユーザーをリダイレクトする URL を入力します。

  最大 230 文字を入力できます。

- [AP MACアドレスのリダイレクト付加（Redirect Append for AP MAC Address）]：リダイレクトに付加する AP の MAC アドレスを入力します。
- [クライアントMACアドレスのリダイレクト付加（Redirect Append for Client MAC Address）]：リダイレクトに付加するクライアントの MAC アドレスを入力します。
- [WLAN SSIDのリダイレクト付加（Redirect Append for WLAN SSID）]：リダイレクトに付加する WLAN SSID を入力します。
- [ポータルIPv4アドレス（Portal IPV4 Address）]：リダイレクトを送信するポータルの IPv4 アドレスを入力します。
- [ポータルIPv6アドレス（Portal IPV6 Address）]：リダイレクトを送信するポータルの IPv6 アドレスを入力します（IPv6 アドレスを使用する場合）。

d) （任意）[カスタマイズされたページ（Customized page）] で、カスタマイズされた Web 認証用のデータを次のフィールドに入力します。

- [ログインページ（Login Page）]：Web 認証用にカスタマイズされたログインウィンドウのファイル詳細を *bootflash:filename* 形式で入力します。
- [ログアウトページ（Logout Page）]：Web 認証用にカスタマイズされたログアウトウィンドウのファイル詳細を *bootflash:filename* 形式で入力します。
- [ログイン成功ページ（Login Successful Page）]：ログイン成功時のカスタマイズされたウィンドウのファイル詳細を *bootflash:filename* 形式で入力します。
- [ログイン失敗ページ（Login Failed Page）]：ログイン失敗時のカスタマイズされたウィンドウのファイル詳細を *bootflash:filename* 形式で入力します。

ステップ 5 [Review and Provision] をクリックします。

ステップ 6 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

ステップ 7 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの Web 認証プロファイルの作成

ワイヤレスコントローラ の Web 認証プロファイルを作成してプロビジョニングするには、次の手順を実行します。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラのリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、 [セキュリティ（Security）] を展開して [Web認証（Web Auth）] をクリックします。

ステップ 4 [Web Auth Profiles] タブをクリックします。

ステップ 5 [Add] をクリックします。

ステップ 6 [WLAN認証の作成（Create Web Auth）] スライドインペインの [一般（General）] タブで、次の設定を完了します。

- [Parameter Map Name] フィールドに、Web 認証プロファイルの名前を入力します。
- （オプション）[最大HTTP接続数（Maximum HTTP connections）] フィールドに、許可する HTTP 接続の最大数を入力します。

  有効値は 1 ～ 200 です。
- [Type] ドロップダウンリストから、認証タイプ（[authbypass]、[webauth]、[consent]、または [webconsent]）を選択します。
- （オプション）[初期状態タイムアウト（Init-State Timeout(secs)）] フィールドに、 Web 認証タイムアウトを秒単位で入力します。

  有効な範囲は 60 ～ 3932100 です。
- （オプション）[スリープ状態のクライアントステータス（Sleeping Client Status）] チェックボックスをオンにして、スリープ状態のクライアントの認証を有効にします。

ステップ 7 [Review and Provision] をクリックします。

ステップ 8 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

ステップ 9 [Tasks] ウィンドウで、タスクの展開を監視します。

次のタスク

web 認証プロファイルの追加パラメータを設定する場合は、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの web 認証プロファイルの設定（972 ページ）」を参照してください。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの web 認証プロファイルの設定

ワイヤレスコントローラの web 認証プロファイルの追加パラメータを設定してプロビジョニングするには、次の手順を実行します。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラのリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、[デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、[セキュリティ（Security）] を展開して [Web認証（Web Auth）] をクリックします。

ステップ 4 追加パラメータを設定する web 認証プロファイルを選択します。

a) [Web Auth Profiles] タブをクリックします。
b) 必要な web 認証プロファイルのチェックボックスをオンにします。
c) [Actions] にカーソルを合わせて [Edit] を選択します。

ステップ 5 [**Edit Web Auth**] スライドインペインの [**General**] タブで、次の設定を完了します。

a) [**General**] で、次の設定を完了します。

- （オプション）[最大HTTP接続数（Maximum HTTP connections）] フィールドに、許可する HTTP 接続の最大数を入力します。

  有効値は 1 ～ 200 です。

- [Type] ドロップダウンリストから、認証タイプ（[authbypass]、[webauth]、[consent]、または [webconsent]）を選択します。

- （オプション）[初期状態タイムアウト（Init-State Timeout(secs)）] フィールドに、 Web 認証タイムアウトを秒単位で入力します。

有効な範囲は 60 ～ 3932100 です。

- （任意）対応する設定を有効にするには、必要なチェックボックスをオンにします。
  - [キャプティブバイパスポータル（Captive Bypass Portal）]：Web 認証のキャプティブバイパスを有効にします
  - [成功ウィンドウの無効化（Disable Success Window）]：Web 認証に成功した後に、ワイヤレスコントローラのデフォルトの成功ウィンドウを無効にします。
  - [ログアウトウィンドウの無効化（Disable Logout Window）]：Web 認証のログアウトウィンドウを無効にします。
  - （オプション）[スリープ状態のクライアントステータス（Sleeping Client Status）] チェックボックスをオンにして、スリープ状態のクライアントの認証を有効にします。

    このオプションを有効にすると、[**Sleeping Client Timeout (minutes)**] フィールドに、スリープタイムアウト（分単位）を任意で入力できます。

    有効な範囲は 10 ～ 43200 分です。

b) （任意） [バナー設定（Banner Configuration）] で、次の設定を完了します。

- [Banner Title] フィールドに、バナータイトルのテキストを入力します。

  タイトルには最大 127 文字を使用できます。

- [**Banner Type**] で必須オプション（[**None**]、[**Banner Text**]、または [**File Name**]）を選択します。

選択内容	結果
バナー テキスト（Banner Text）	[バナーテキスト（Banner Text）] フィールドに、バナーに表示するテキストを入力します。 例：*c* **banner-text** *c*、*c* はデリミタです。
ファイルから読み取る	[**File Name**] フィールドに、バナーテキストの読み取り元となるファイルの名前を入力します。 ファイル名には最大 61 文字を使用できます。

ステップ 6 [**Advanced**] タブで、次の設定を完了します。

a) （任意） [外部サーバーへのリダイレクト（Redirect to external server）] で、外部 Web 認証用のデータを次のフィールドに入力します。

- [ログイン用のリダイレクトURL（Redirect URL for login）]：ログイン要求のためにユーザーをリダイレクトする URL を入力します。

  最大 230 文字を入力できます。 Catalyst Center では、URL にスペースは使用できません。

- [成功時のリダイレクト（Redirect On-Success）] フィールドに、ログインが成功した後にユーザーをリダイレクトする URL を入力します。

最大 230 文字を入力できます。 Catalyst Center では、URL にスペースは使用できません。

- [失敗時のリダイレクト（Redirect On-Failure）] フィールドに、ログインが失敗した後にユーザーをリダイレクトする URL を入力します。

  最大 230 文字を入力できます。 Catalyst Center では、URL にスペースは使用できません。

- [**Redirect Append for AP MAC Address**]：リダイレクト ACL に付加する AP MAC アドレスのリダイレクト付加を入力します。

  最大 227 文字を入力できます。Catalyst Center では、リダイレクト付加にスペースと？は使用できません。

- [**Redirect Append for Client MAC Address**]：リダイレクト ACL に付加するクライアント MAC アドレスのリダイレクト付加を入力します。

  最大 223 文字を入力できます。Catalyst Center では、リダイレクト付加にスペースと？は使用できません。

- [**Redirect Append for WLAN SSID**]：リダイレクト ACL に付加する WLAN SSID のリダイレクト付加を入力します。

  最大 224 文字を入力できます。Catalyst Center では、リダイレクト付加にスペースと？は使用できません。

- [ポータルIPv4アドレス（Portal IPV4 Address）]：リダイレクトを送信するポータルの IPv4 アドレスを入力します。

  IP アドレスを *xxx.xxx.xxx.xxx* の形式で入力します。

- [ポータルIPv6アドレス（Portal IPV6 Address）]：リダイレクトを送信するポータルの IPv6 アドレスを入力します（IPv6 アドレスを使用する場合）。

  IP アドレスを *X:X:X:X:X:X:X:X* の形式で入力します。

b) （任意）[カスタマイズされたページ（Customized page）] で、カスタマイズされた Web 認証用のデータを次のフィールドに入力します。

- [ログインページ（Login Page）]：Web 認証用にカスタマイズされたログインウィンドウのファイル詳細を *bootflash:filename* 形式で入力します。

  ファイル詳細は *bootflash:*、*harddisk:*、または *flash:* で始まる必要があります。

- [ログアウトページ（Logout Page）]：Web 認証用にカスタマイズされたログアウトウィンドウのファイル詳細を *bootflash:filename* 形式で入力します。

  ファイル詳細は *bootflash:*、*harddisk:*、または *flash:* で始まる必要があります。

- [ログイン成功ページ（Login Successful Page）]：ログイン成功時のカスタマイズされたウィンドウのファイル詳細を *bootflash:filename* 形式で入力します。

  ファイル詳細は *bootflash:*、*harddisk:*、または *flash:* で始まる必要があります。

- [ログイン失敗ページ（Login Failed Page）]：ログイン失敗時のカスタマイズされたウィンドウのファイル詳細を *bootflash:filename* 形式で入力します。

ファイル詳細は *bootflash:*、*harddisk:*、または *flash:* で始まる必要があります。

ステップ 7 [Review and Provision] をクリックします。

ステップ 8 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

ステップ 9 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の CTS の設定

Cisco TrustSec は、ネットワーク内のユーザー、ホスト、およびネットワーク デバイスを強力に識別する機能に基づいた、シスコ ネットワーク デバイスのセキュリティを改善します。TrustSec は、特定の役割についてデータ トラフィックを一意に分類することで、トポロジに依存しない、スケーラブルなアクセス コントロールを実現します。TrustSec は、認証されたピアおよびこれらのピアとの暗号化リンク間で信頼を確立することで、データの機密保持および整合性を保証します。

この手順を使用して、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の Cisco TrustSec（CTS）を設定し、設定をプロビジョニングします。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[セキュリティ（Security）] を展開して [TrustSec] をクリックします。

ステップ 4 [グローバル（Global）] タブで、Cisco TrustSec（CTS）パラメータを設定します。

ステップ 5 （任意） [CTSデバイスID（CTS Device ID）] フィールドに、TrustSec ネットワーク アクセス デバイスの名前を入力します。

名前には最大 32 文字を使用できます。名前は、Cisco Identity Services Engine で設定された名前と同じである必要があります。

ステップ 6 （任意） [CTSパスワード（CTS Password）] に、CTS のパスワードを入力します。

パスワードは 162 文字以内で指定できます。Catalyst Center では、パスワードに？やスペースの使用をサポートしていません。

ステップ 7 （任意） [CTS承認リスト（CTS Authorization List）] ドロップダウンリストから、TrustSec デバイスの AAA サーバーのリストを選択します。

認証リストの作成については、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の認証方式リストの作成 （929 ページ）を参照してください。

ステップ 8 （任意） [CTSデバイスSGT（CTS Device SGT）] フィールドに、ローカル デバイス セキュリティ グループの番号を入力します。

有効な範囲は 2 ～ 65519 です。Cisco IOS XE リリース 17.17.1 以降の場合、有効な範囲は 2 ～ 65521 です。

ステップ 9 （任意） [ポリシーサーバー設定（Policy Server Configuration）] で、次の設定を完了します。

- [デバイス名（Device Name）] フィールドに、Cisco ISEで使用されるデバイス名を入力します。
- [ユーザ名（Username）] フィールドに、ユーザ名を入力します。

  ユーザー名には最大 32 文字を使用できます。
- [暗号化（Encryption）] ドロップダウンリストから、パスワードの暗号化タイプを選択します。
- [Password] フィールドにパスワードを入力します。

  パスワードには最大 24 文字を使用できます。

ステップ 10 [Review and Provision] をクリックします。

ステップ 11 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 12 [Tasks] ウィンドウで、タスクの展開を監視します。

次のタスク

[ポリシーサーバー（Policy Servers）] テーブルでは、ポリシーサーバーを追加、編集、または削除できます。ポリシーサーバーを追加するには、「CTS 設定用のポリシーサーバーの作成（977 ページ）」を参照してください。

CTS 設定用のポリシーサーバーの作成

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の CTS ポリシーサーバー設定のポリシーサーバーを作成し、プロビジョニングするには、この手順を使用します。

ワイヤレスコントローラ の CTS 設定については、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の CTS の設定 （975 ページ）」を参照してください。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラのリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、[デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[セキュリティ（Security）] を展開して [TrustSec] をクリックします。

ステップ 4 [グローバル（Global）] タブの [ポリシーサーバー（Policy Servers）] テーブルで、[追加（Add）] をクリックします。

ステップ 5 [ポリシーサーバーの作成（Create Policy Server）] スライドインペインの [ポリシーサーバープロファイル（Policy Server Profile）] で、次の設定を完了します。

- [ポリシーサーバー名（Policy Server Name）] フィールドに、ポリシーサーバープロファイルの一意の名前を入力します。

  プロファイル名には最大 255 文字を含めることができます。Catalyst Center ではプロファイル名に疑問符（?）とスペースを含めることはできません。この名前はワイヤレスコントローラ内のポリシーサーバー設定を識別します。

- （オプション） [ドメイン名（Domain Name）] フィールドに、ポリシーサーバーの完全修飾ドメイン名（FQDN）を入力します。DNS解決を使用するには、IPアドレスの代わりにこの名前を使用します。

  ドメイン名には最大 128 文字を使用できます。

- （オプション） [サーバーポート（Server Port）] フィールドに、ポリシーサーバーに接続するために使用するポート番号を入力します。

有効な範囲は 1025 ～ 65535 です。このポートがポリシーサーバーで設定されたリスニングポートと一致していることを確認します。

- （オプション）[再送信試行回数（Retransmit Attempts）] フィールドには、応答を受信しなかった場合に、ワイヤレスコントローラ がポリシーサーバーへの要求の送信を再試行する回数を入力します。

  有効な範囲は 0 ～ 5 です。値が大きいほど信頼性が高くなりますが、障害の検出が遅延する場合があります。

- （オプション）[タイムアウト（秒）（Timeout (seconds)）] フィールドに、この試行を失敗と見なす前に ワイヤレスコントローラ が待機する時間を秒単位で入力します。

  有効な範囲は 1 ～ 60 です。

- [TLSサーバートラストポイント（TLS Server Trustpoint）] ドロップダウンリストから TLS サーバートラストポイントを選択します。

- （オプション）使用可能な場合は、[JSONコンテンツタイプの使用（Use JSON Content Type）] トグルボタンを使用して、ポリシーサーバーとの通信用のコンテンツタイプとして JSON を使用することを有効または無効にします。

ステップ 6 [IPアドレス（IP Address）] で、IPアドレスを設定します。

実行する操作	結果
IP アドレスの追加	**1.** [Add] をクリックします。 **2.** [IPアドレスの追加（Add IP Address）] ダイアログボックスの [IP アドレス（IP Address）] フィールドに、有効な IPv4 または IPv6 アドレスを入力します。
IP アドレスの削除	**1.** 削除する IP アドレスの横にあるチェックボックスをオンにします。 **2.** [Actions] にカーソルを合わせて [Delete] を選択します。 **3.** ダイアログボックスで、**Yes** をクリックします。

ステップ 7 [Review and Provision] をクリックします。

ステップ 8 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

ステップ 9 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の SXP の設定

ワイヤレスコントローラ の Cisco TrustSec（CTS）SGT Exchange Protocol（SXP）を設定してプロビジョニングするには、次の手順を実行します。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[セキュリティ（Security）] を展開して [TrustSec] をクリックします。

ステップ 4 （任意） [SXP] タブで、次の設定を完了します。

a) [SXPステータス（SXP Status）] トグルボタンを使用して、CTS SXP のサポートを有効または無効にします。
b) 次のパラメータを設定します。

- [デフォルトSXP送信元IPv4アドレス（Default SXP Source IPv4 Address）]：デフォルトの SXP 送信元 IPv4 アドレスを入力します。
- [デフォルトSXPパスワードタイプ（Default SXP Password Type）]：デフォルトの SXP パスワードタイプを選択します。
- [デフォルトSXPパスワード（Default SXP Password）]：デフォルトの SXP パスワードを入力します。

  パスワードには最大 162 文字を含めることができます。
- [調整期間（秒）（Reconciliation Period (sec)）]：調整時間を秒単位で入力します。

  値の範囲は 0 ～ 64000 です。
- [再試行期間（秒）（Retry Period (sec)）]：SXP 接続の再試行期間を秒単位で入力します。

  値の範囲は 0 ～ 64000 です。
- [送信元IPv6（Source Ipv6）]：有効な送信元 IPv6 アドレスを入力します。

ステップ 5 [Review and Provision] をクリックします。

ステップ 6 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

ステップ 7 [Tasks] ウィンドウで、タスクの展開を監視します。

次のタスク

[ピア接続（Peer Connections）] テーブルで CTS SXP のサポートを有効にすると、必要に応じてピア接続を追加、編集、または削除できます。

ピア接続を追加するには、[追加（Add）] をクリックして次の設定を完了します。

1. [ローカルデバイスのモード（Mode of Local Device）] ドロップダウンリストから、ローカルデバイスのロールを選択します。
2. [IPタイプ（IP Type）] ドロップダウンリストから、IP アドレスタイプを選択します。
3. [**Peer IP**] フィールドに、選択した IP アドレスタイプに基づいて SXP ピア IP アドレスを入力します。
4. （オプション）[**Source IP**] フィールドに、選択した IP アドレスタイプに基づいて SXP 送信元 IP アドレスを入力します。
5. [Password] ドロップダウンリストから、パスワードタイプを選択します。
6. 「ステップ 5 （980 ページ）」から「ステップ 7 （980 ページ）」までを完了します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の CTS リンク設定の作成

この手順を使用して、ワイヤレスコントローラ の CTS リンク設定を作成し、プロビジョニングします。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。

b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[セキュリティ（Security）] を展開して [TrustSec] をクリックします。

ステップ 4 [CTSリンク設定（CTS Link Configuration）] タブで、[追加（Add）] をクリックします。

ステップ 5 [CTSリンク設定の作成（Create CTS Link Configuration）] スライドインペインで、次の設定を完了します。

a) （任意） [Interface Name] ドロップダウンリストから、インターフェイスを選択します。

b) [CTS手動（CTS Manual）] トグルボタンを使用して、CTS 手動モードを有効または無効にします。

CTS 手動モードを有効にする場合は、必要な設定を完了します。

- [ポートSGT（Port SGT）] フィールドに、タグなしまたは信頼できない着信トラフィックに適用する送信元セキュリティグループタグ（SGT）番号を入力します。

  有効な範囲は 2 ～ 65519 です。

- （オプション）ピアが送信に使用する送信元SGTを信頼するには、[信頼できる（Trusted）]チェックボックスをオンにします。

- [SGTの伝達（Propagate SGT）] トグルボタンを使用して、CTS SGT 伝達の設定を行います。

（注） [信頼できる（Trusted）]チェックボックスをオンにすると、このオプションはグレー表示になります。

ステップ 6 [Review and Provision] をクリックします。

ステップ 7 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。

- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

ステップ 8 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの SXP AP プロファイルの作成

ワイヤレスコントローラの CTS SXP AP プロファイルを作成してプロビジョニングするには、次の手順を実行します。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[セキュリティ（Security）] を展開して [TrustSec] をクリックします。

ステップ 4 [AP] タブをクリックします。

ステップ 5 [Add] をクリックします。

ステップ 6 [SXP APプロファイルの作成（Create SXP AP Profiles）] スライドインペインの [プロファイル名（Profile Name）] フィールドで、プロファイルの一意の名前を入力します。

プロファイル名には最大 31 文字を含めることができます。Catalyst Center では、プロファイル名の先頭と末尾にスペースを含めることはできません。

ステップ 7 （任意） [ステータス（Status）] トグルボタンをクリックし、CTS SXP 設定を有効にします。

ステップ 8 次のフィールドにデータを入力します。

- （オプション）[デフォルトパスワード（Default Password）]：CTS SXP のデフォルトパスワードを入力します。

  パスワードには最大 80 文字を含めることができます。

- [CTSリスナーの最小値（秒）（CTS Listener Minimum (sec)）]：CTS SXP リスナーの最小ホールド時間を秒単位で入力します。

  値の範囲は 1 ～ 65534 です。デフォルトは 90 です。

- [CTSリスナーの最大値（秒）（CTS Listener Maximum (sec)）]：CTS SXP リスナーの最大ホールド時間を秒単位で入力します。

  値の範囲は 1 ～ 65534 です。デフォルト値は 120 です。

- [CTSスピーカーの秒数（秒）（CTS Speaker Seconds (sec)）]：CTS SXP スピーカーのホールド時間を秒単位で入力します。

  値の範囲は 1 ～ 65534 です。デフォルト値は 120 です。

- [CTS調整期間（秒）（CTS Recon Period (sec)）]：CTS SXP の調整期間を秒単位で入力します。

  値の範囲は 0 ～ 64000 です。デフォルト値は 120 です。

- [CTS再試行期間（秒）（CTS Retry Period (sec)）]：CTS SXP の再試行期間を秒単位で入力します。値の範囲は 0 ～ 64000 です。デフォルト値は 120 です。

ステップ 9 （任意）[CTS SXPプロファイル接続（CTS SXP Profile Connections）] で、CTS SXP プロファイル接続を設定します。

実行する操作	結果
CTS SXP プロファイル接続を追加する	**1.** [Add] をクリックします。 **2.** [Add CTS SXP Profile Connections] ダイアログボックスの [Peer IP] フィールドに、SXP 接続のピア IP アドレスを入力します。 **3.** [接続モード（Connection Mode）] ドロップダウンリストから、SXP 接続モードを選択します。 **4.** [パスワードタイプ（Password Type）] ドロップダウンリストから、SXP 接続のパスワードタイプを選択します。 **5.** [Save] をクリックします。
CTS SXP プロファイル接続を編集する	**1.** 編集するピアの IP アドレスの横にあるチェックボックスをオンにします。 **2.** [Actions] にカーソルを合わせて [Edit] を選択します。 **3.** 必要な設定を編集します。 **4.** [Save] をクリックします。
CTS SXP プロファイル接続を削除する	**1.** 削除するピアの IP アドレスの横にあるチェックボックスをオンにします。 **2.** [Actions] にカーソルを合わせて [Delete] を選択します。 **3.** ダイアログボックスで、**Yes** をクリックします。

ステップ 10 [Review and Provision] をクリックします。

ステップ 11 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 12 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の不正ポリシーの設定

次の手順を使用して、ワイヤレスコントローラ の不正 AP を検出する不正ポリシーを設定し、プロビジョニングします。

デフォルトの AP プロファイルと次のグローバル不正パラメータは、不正 AP 検知セキュリティレベル（[低（Low）]、[高（High）]、または [重大（Critical）]）に対して自動的に設定され、編集できません。

- **Adhoc Rogue AP**
- **Auto Containment Level**
- **Detect and Report Adhoc Networks**
- **Expiration timeout for Rogue APs (seconds)**
- **Rogue AP Expiration Timeout (sec)**
- **Rogue Auto Contain Ad Hoc**
- **Rogue Init Timer (sec)**
- **Rogue Polling Interval (sec)**
- **Using our SSID**
- **Valid client on Rogue AP**
- **Validate Rogue Clients Against AAA**
- **Validate Rogue APs Against AAA**

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[セキュリティ（Security）] を展開して [ワイヤレス保護ポリシー（Wireless Protection Policies）] をクリックします。

ステップ 4 [不正ポリシー（Rogue Policies）] タブの [一般（General）] で、 必要な設定を行います。

a) [不正AP検知セキュリティレベル（Rogue Detection Security Level）] のドロップダウンリストから、セキュリティレベルを選択します。

[カスタム（Custom）] セキュリティレベルを選択した場合は、次の設定を完了します。

- [Rogue AP Expiration Timeout (sec)] フィールドに、不正 AP のタイムアウト値を秒単位で入力します。

  有効な範囲は 240 ～ 3600 です。デフォルト値は 1200 です。

- [AAAに対する不正クライアントの検証（Validate Rogue Clients Against AAA）] チェックボックスを使用して、AAA サーバーに対する不正クライアントの検証を有効または無効にします。

- [AAAに対する不正APの検証（Validate Rogue APs Against AAA）] チェックボックスを使用して、AAA サーバーに対する不正 AP の検証を有効または無効にします。

- [Rogue Polling Interval (sec)] フィールドに、不正情報について AAA サーバーにポーリングする間隔を入力します。

  有効な範囲は 60 ～ 86400 です。デフォルト値は 3600 です。

- [アドホックネットワークの検出とレポート（Detect and Report Adhoc Networks）] チェックボックスをオンにして、アドホック不正検出およびレポートを有効にします。

- [Rogue Init Timer (sec)] フィールドに、不正 AP の初期タイマーを秒単位で入力します。

  有効な範囲は 0 ～ 360 です。デフォルト値は 60 です。

  不正APが検出されると、初期タイマーが開始され、タイマーが期限切れになるとルールが適用されます。

b) [Rogue Detection Client Number Threshold] フィールドに、不正な AP SNMP トラップごとの不正なクライアントのしきい値を入力します。

有効な範囲は 0 ～ 256 です。デフォルト値は 56 です。

c) [AP認証（AP Authentication）] チェックボックスを使用して、AP 認証を有効または無効にします。

（注） ステップ 6 （986 ページ） でグローバル MFP が有効になっている場合、AP 認証を有効にすることはできません。

d) [AP Authentication Alarm Threshold] フィールドに、AP 認証アラームのしきい値を入力します。

有効な範囲は 1 ～ 255 です。デフォルト値は 22 です。

e) [syslog通知（Syslog Notification）] チェックボックスを使用して、syslog を介した不正イベント通知を有効または無効にします。

ステップ 5 [カスタム（Custom）] セキュリティレベルを選択した場合は、[自動封じ込め（Auto Contain）] で次の設定を行います。

- [自動封じ込めレベル（Auto Containment Level）] ドロップダウンリストから、不正 AP の自動封じ込めレベルを選択します。
- 次のチェックボックスを使用して、対応する設定を有効または無効にします。
  - [モニターモードAPのみの自動封じ込め（Auto Containment only for Monitor mode APs）]：モニターモードの AP に対してのみ自動封じ込めを設定します。
  - [自分のSSIDの使用（Using Our SSID）]：自分の SSID をアドバタイズしている不正 AP の自動封じ込めを設定します。
  - [不正AP上の有効なクライアント（Valid client on Rogue AP）]：不正 AP を使用している有効なクライアントの自動封じ込めを設定します。
  - [アドホック不正AP（Adhoc Rogue AP）]：アドホック不正 AP の自動封じ込めを設定します。

ステップ 6 [MFP設定（MFP Configuration）] で、次の設定を完了します。

- [グローバルMFP状態（Global MFP State）]チェックボックスを使用して、管理フレーム保護（MFP）をグローバルに有効または無効にします。

（注） AP 認証が有効になっている場合、グローバル MFP を有効にすることはできません。

- [AP偽装検出（AP Impersonation Detection）] チェックボックスを使用して、AP 偽装検出を有効または無効にします。
- [MFPキーリフレッシュ間隔（時間）（MFP Key Refresh Interval (hours)）] フィールドで、MFP キーのリフレッシュ間隔を時間単位で入力します。

  有効な範囲は 1 ～ 24 です。

ステップ 7 [不正デバイスの承認（Rogue Device Authorization）] で、[不正承認モード（Rogue Authorization Mode）] チェックボックスを使用して、ネットワーク上の不正デバイスを特定して管理するための承認モードを有効または無効にします。

ステップ 8 [Review and Provision] をクリックします。

ステップ 9 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 10 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの不正 AP ルールの作成

ワイヤレスコントローラ の不正 AP ルールを作成してプロビジョニングするには、次の手順を実行します。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[セキュリティ（Security）] を展開して [ワイヤレス保護ポリシー（Wireless Protection Policies）] をクリックします。

ステップ 4 [不正APルール（Rogue AP Rules）] タブをクリックします。

ステップ 5 [Add] をクリックします。

ステップ 6 [不正APルールの作成（Create Rogue AP Rules）] スライドインペインの [ルール名（Rule Name）] フィールドに、不正 AP ルールの一意の名前を入力します。

ルール名には最大 32 文字の英数字と特殊文字を含めることができます。ルール名には、少なくとも 1 つの英数字、ピリオド（.）、下線（_）、またはハイフン（-）を含める必要があります。Catalyst Center では、ルール名に ? とスペースは使用できません。

ステップ 7 [優先順位（Priority）] フィールドに、不正 AP ルールの優先順位を示す番号を入力します。

有効な範囲は 1 ～ 512 です。値が小さいほど、プライオリティが高いことを示します。

ステップ 8 [タイプ（Type）] ドロップダウンリストから、分類タイプを選択します。

ステップ 9 分類タイプに基づいて、次の設定を完了します。

選択内容	結果
[フレンドリー（Friendly）] または [悪意のある（Malicious）]	[状態（State）] ドロップダウンリストから、不正 AP ルールの状態を選択します。

選択内容	結果
Custom	• [状態（State）] ドロップダウンリストから、不正 AP ルールの状態を選択します。 • [シビラティスコア（Severity Score）] フィールドに、分類タイプのスコアを入力します。 有効な範囲は 1 ～ 100 です。 • （オプション）[カスタム名（Custom Name）] フィールドに、分類タイプのカスタム名を入力します。

ステップ 10 [Review and Provision] をクリックします。

ステップ 11 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 12 [Tasks] ウィンドウで、タスクの展開を監視します。

次のタスク

ルールの追加パラメータの設定については、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の不正 AP ルールの設定 （988 ページ）」を参照してください。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の不正 AP ルールの設定

この手順を使用して、ワイヤレスコントローラ の不正 AP ルールの追加パラメータを設定し、プロビジョニングします。

Before you begin

不正 AP ルールを作成します。不正 AP ルールを作成するには、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの不正 AP ルールの作成 （987 ページ）」を参照してください。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。

b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。

c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラのリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、で [セキュリティ（Security）] を展開し、**[ワイヤレス保護ポリシー（Wireless Protection Policies）] > [不正APルール（Rogue AP Rules）]** をクリックします。

ステップ 4 設定するルールの横にあるチェックボックスをオンにします。[Actions] にカーソルを合わせて [Edit] を選択します。

ステップ 5 （任意） [不正APルールの編集（Edit Rogue AP Rules）] スライドインペインの [優先順位（Priority）] フィールドで、不正 AP ルールの既存の優先順位を更新します。

有効な範囲は 1 ～ 512 です。値が小さいほど、プライオリティが高いことを示します。

ステップ 6 [ルールの有効化（Enable Rule）] チェックボックスを使用して、ルールを有効または無効にします。

（注） ルールを有効にすると、[優先順位（Priority）] フィールドのみ編集できます。他のオプションは無効になっています。

ルールを無効にする場合は、次の設定を完了します。

a) [タイプ（Type）] ドロップダウンリストから、分類タイプを [フレンドリー（Friendly）]、[悪意のある（Malicious）]、[削除（Delete）]、または [カスタム（Custom）] から選択します。

分類タイプに基づいて、次の設定を完了します。

選択内容	結果
[フレンドリー（Friendly）] または [悪意のある（Malicious）]	[状態（State）] ドロップダウンリストから、不正 AP ルールの状態を選択します。
Custom	• [状態（State）] ドロップダウンリストから、不正 AP ルールの状態を選択します。 • [シビラティスコア（Severity Score）] フィールドに、分類タイプのスコアを入力します。有効な指定範囲は 1 ～ 100 です。 • （オプション）[カスタム名（Custom Name）] フィールドに、分類タイプのカスタム名を入力します。 名前には、最大 215 文字の英数字と特殊文字を使用できます。

b) [マッチ動作（Match Operation）] ドロップダウンリストから、不正 AP がルールの分類タイプを採用する基準を選択します。

- [すべて（All）]：検出された不正 AP は、ルールで指定されたすべての条件を満たしている必要があります。
- [いずれか（Any）]：検出された不正 AP は、ルールで指定されたいずれかの条件を満たしている必要があります。

c) （任意）[条件（Conditions）] で、必要なチェックボックスをオンにして、該当する条件にルールの分類タイプを適用するように設定します。

- [クライアント数（Client Count）]：この条件では、不正 AP に最小数のクライアントがアソシエートされている必要があります。

  このオプションをオンにする場合は、[不正クライアントの最小数（Minimum Number of Rogue Clients）] フィールドに、不正 AP にアソシエートされたクライアントの最小数を入力します。有効な範囲は 1 ～ 10 です。デフォルト値は 0 です

  接続されたクライアント数が指定された制限を超える場合、ルールの分類タイプが採用されます。

- [期間（duration）]：この条件では不正 AP が最小期間検出される必要があります。

  このオプションをオンにする場合は、[期間（Time Duration）] フィールドに最小検出期間の値を秒単位で入力します。指定できる範囲は 0 ～ 86400 です。デフォルト値は 0 です

- [暗号化（encryption）]：この条件では、WLAN が指定された暗号化を使用している必要があります。

  このチェックボックスをオンにすると、必要に応じてチェックボックスを使用して、対応する暗号化タイプを選択できます。

- [インフラストラクチャ（infrastructure）]：この条件では、不正 AP の SSID がワイヤレスコントローラに既知である必要があります。

  このチェックボックスをオンにすると、必要に応じて、[SSIDの管理（Manage SSID）] チェックボックスをオンにして、不正 AP の SSID が管理対象 SSID と一致するかどうかを確認できます。

- [rssi]：この条件では、不正 AP には、最小の受信信号強度表示（RSSI）値が必要です。

  このチェックボックスをオンにする場合は、[最大RSSI（Maximum RSSI）] フィールドに最大 RSSI 値を入力します。有効な範囲は 0 ～ –128 です。

- [チャネル幅（channel-width）]：この条件では、不正 AP は指定された無線バンドのチャネル幅を使用する必要があります。

  チェックボックスをオンにした場合は、次のドロップダウンリストから必要なオプションを選択してください。

  - [バンド（Band）]：不正 AP 無線バンドを選択します。
  - [最大チャンネル幅（Maximum Channel Width）]：無線バンドの最大チャンネル幅を選択します。

- [ssid]：この条件では、不正 AP には特定のユーザー設定 SSID が必要です。

  このチェックボックスをオンにした場合、[ユーザー設定SSID（User Configured SSID）] フィールドに SSID を入力します。回線ごとに 1 つの SSID を入力できます。

- [部分一致 - ssid（substring-ssid）]：この条件では、不正 AP には特定のユーザー設定 SSID の部分一致が必要です。ワイヤレスコントローラは、発生パターンを分析し、SSID の文字列に部分一致が見つかった場合はその一致を特定します。

  このチェックボックスをオンにした場合、[ユーザー設定部分一致 SSID（User Configured Substring-SSID）] フィールドに、SSID の部分一致を入力します。回線ごとに 1 つの SSID の部分一致を入力できます。

ステップ 7 [Review and Provision] をクリックします。

ステップ 8 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

ステップ 9 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のクライアント除外ポリシーの設定

この手順を使用して、ワイヤレスコントローラのクライアント除外ポリシーを設定し、プロビジョニングします。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラのリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[セキュリティ（Security）] を展開して [ワイヤレス保護ポリシー（Wireless Protection Policies）] をクリックします。

ステップ 4 [Client Exclusion Policies] タブをクリックします。

ステップ 5 （任意） 該当するイベントのクライアントを除外するために、必要なチェックボックスをオンにします。

- [すべてのイベントを選択（Select All Events）]：すべてのイベントをクライアント除外用に選択します。
- [過剰な802.11のアソシエーションの失敗（Excessive 802.11 Association Failures）]：802.11 関連付けの失敗が繰り返される場合にクライアントを除外します。
- [過剰な802.1X認証エラー（Excessive Web Authentication Failures）]：802.1X 認証の失敗が繰り返される場合にクライアントを除外します。
- [過剰な802.11認証タイムアウト（Excessive 802.11 Authentication Timeout）]：802.11 認証のタイムアウトが繰り返される場合にクライアントを除外します。
- [IP盗難またはIP再使用（IP Theft or IP Reuse）]：IP アドレスが再利用され、IP 盗難の可能性が示されている場合にクライアントを除外します。
- [過剰なWeb認証エラー（Excessive Web Authentication Failures）]：Web 認証の失敗が繰り返される場合にクライアントを除外します。

ステップ 6 [Review and Provision] をクリックします。

ステップ 7 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

ステップ 8 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の LSC プロビジョニングパラメータの設定

この手順を使用して、ワイヤレスコントローラ の AP のローカルで有効な証明書（LSC）のプロビジョニングに関するパラメータを設定し、その設定をプロビジョニングします。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。

b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラのリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[セキュリティ（Security）] を展開して [LSC] をクリックします。

ステップ 4 [LSCプロビジョン（LSC Provision）] タブに移動し、[プロビジョニングの設定（Provisioning Configuration）] で、LSC を使用した AP 参加の試行を設定します。

- [ステータス（Status）] ドロップダウンリストから、LSC プロビジョニングのステータスを選択します。

  ステータスを有効にすると、AP は LSC プロビジョニングを使用できます。ステータスを無効にすると、AP は製造元でインストールされる証明書（MIC）または自己署名証明書（SSC）にフォールバックします。

- （オプション）[トラストポイント名（Trustpoint Name）] フィールドに、AP および ワイヤレスコントローラ に証明書を提供する認証局（CA）サーバーのトラストポイントを入力します。

- （オプション）[結合の試行回数（Number of Join Attempts）] フィールドに、MIC にフォールバックする前に、AP が LSC を使用して行う結合の試行回数を入力します。

  有効範囲は 0 ～ 255 です。

- [キーサイズ（Key Size）] ドロップダウンリストから、LSC プロビジョニングに使用するキーのサイズを選択します。

ステップ 5 （任意） [サブジェクト名パラメータ（Subject Name Parameters）] で、AP から送信される証明書署名リクエストに含まれる必須パラメータを入力します。

必要な国、州、都市、部門、組織、および電子メールアドレスを設定します。

ステップ 6 （任意） [LSC更新設定（LSC Renewal Configuration）] で、[LSC自動更新（LSC Auto-Renewal）] チェックボックスを使用して、AP 参加中の LSC の更新を有効または無効にします。

AP 参加中に LSC の更新を有効にする場合は、次の設定を完了します。

- [期限切れ時間（日）（Due Time (Days)）] フィールドに、LSC が期限切れになる日数を入力し、更新を開始します。

  値の範囲は 5 ～ 365 です。

- （オプション）[更新スケジュール（Renewal Schedule）] ドロップダウンリストから、カレンダープロファイルを選択します。

  カレンダープロファイルの作成については、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のカレンダープロファイルの作成 （908 ページ）を参照してください。

- LSC 更新に関する定期的な syslog メッセージの有効化または無効化を設定するには、[syslog] トグルボタンを使用します。
- [更新モード（Renewal Mode）] ドロップダウンリストから、更新モードを選択します。
  - [ワンショット（One Shot）]：対象となるすべての AP の証明書を一斉に更新します。
  - [スタッガード（Staggered）]：対象 AP の証明書をグループに分けて更新します。

スタッガード更新を選択した場合は、[スタッガード更新の設定（Staggered Renewal Configuration）] で次の設定を行います。

（注） AP アップグレードの設定を行うには、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の AP アップグレード設定をします。 （1170 ページ）」を参照してください。

- [アカウンティングアクション（Accounting Action）] ドロップダウンリストから、アカウンティング中に AP が欠落したときに実行するアクションを選択します。
- （オプション） [アカウンティングの割合（Accounting Percent）] フィールドに、アカウンティング中に再度参加する必要がある AP の割合を入力します。

  有効範囲は 0 ～ 100 です。
- [イテレーション有効期限（分）（Iteration Expiry (Minutes)）] フィールドに、AP での LSC プロビジョニングのために、時間差のイテレーションの有効期限が切れるまでの時間（分）を入力します。

  有効範囲は 0 ～ 255 です。

ステップ 7 [Review and Provision] をクリックします。

ステップ 8 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

ステップ 9 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの LSC プロビジョニングエントリの作成

ワイヤレスコントローラのローカルで有効な証明書（LSC）プロビジョニングエントリを作成し、その設定をプロビジョニングするには、次の手順を実行します。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラのリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[セキュリティ（Security）] を展開して [LSC] をクリックします。

ステップ 4 [LSCプロビジョニングエントリ（LSC Provisioning Entries）] タブをクリックします。

ステップ 5 [追加（Add）] にカーソルを合わせ、必要なオプションを選択します。

- [単一のAP MACの追加（Add Single AP MAC）] : LSC プロビジョニングエントリの単一の MAC アドレスを設定します。
- [複数のAP MACの追加（CSVのアップロード）（Add Multiple AP MACs(Upload CSV)）] : カンマ区切り値（CSV）ファイルをアップロードして、LSC プロビジョニングエントリの複数の MAC アドレスを設定します。

次を選択できます。	下記を実行
単一のAP MACを追加	[LSCプロビジョニングエントリの作成（Create LSC Provisioning Entries）] スライドインペインの [AP MACアドレス（AP MAC Address）] フィールドに、LSC をプロビジョニングする AP イーサネット MAC アドレスを入力します。 xxxx.xxxx.xxxx、xx-xx-xx-xx-xx-xx、xxxx-xxxx-xxxx、または xxxx:xxxx:xxxx の形式で MAC アドレスを入力します。

次を選択できます。	下記を実行
複数のAP MACを追加(CSVのアップロード)	**1.** [サンプルCSV（sample CSV）] をクリックして、サンプル CSV ファイルをダウンロードします。 **2.** LSC をプロビジョニングする MAC アドレスを CSV ファイルに入力します。 xxxx.xxxx.xxxx、xx-xx-xx-xx-xx-xx、xxxx-xxxx-xxxx、または xxxx:xxxx:xxxx の形式で MAC アドレスを入力します。 **3.** CSV ファイルをドラッグアンドドロップ領域にドラッグアンドドロップするか、[ファイルを選択（Choose a file）] をクリックして CSV ファイルの場所を参照し、[開く（Open）] をクリックします。 **4.** [Upload] をクリックします。 Catalyst Center で検証チェックが実行されます。アップロードした CSV ファイルが要件を満たしていない場合は、エラーメッセージが表示されます。

ステップ 6 [Review and Provision] をクリックします。

ステップ 7 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

ステップ 8 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のキーチェーンの作成

この手順を使用して、Cisco IOS XE リリース 26.1.1 以降を実行している ワイヤレスコントローラ のキーチェーンを作成し、プロビジョニングします。

キーチェーンは、ルーティング認証などのセキュア通信プロトコルの認証キーをグループ化するために使用されます。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[セキュリティ（Security）] を展開し、[MACsecキーチェーン（MACsec Key Chain）] をクリックします。

ステップ 4 [Add] をクリックします。

ステップ 5 [キーチェーン設定の作成（Create Key Chain Configuration）] スライドインペイン で、次の設定を完了します。

a) [キーチェーン名（Key Chain Name）] フィールドに、キーチェーンの一意の名前を入力します。
b) キーチェーンの設定

実行する操作	結果
キーチェーンの追加	**1.** [Add] をクリックします。 **2.** [キーチェーンの追加（Add Key Chain）] ダイアログボックスの [キー ID（Key ID）] フィールドに、キー識別子を入力します。 通常のキーチェーンの場合、0 ～ 2147483674 の数値を入力します。Media Access Control Security（MACsec）キーチェーンの場合、桁数が偶数の 16 進数を入力します。 **3.** （オプション）[MACsec暗号化アルゴリズム（MACsec Cryptographic Algorithm）] ドロップダウンリストから、MACsec のアルゴリズムを選択します。 **4.** （オプション）[キー文字列（Key String）] フィールドに、認証または暗号化用の 16 進数のキー文字列を入力します。 AES 128 ビット暗号ベースメッセージ認証コード（CMAC）の場合、このフィールドに 32 文字の文字列を入力します。AES 256 ビット CMAC の場合、このフィールドに 64 文字の文字列を入力します。 **5.** （オプション）[キー文字列暗号化タイプ（Key String Encryption Type）] ドロップダウンリストから、キー文字列を保存するための暗号化メソッドを選択します。 **6.** [Save] をクリックします。

実行する操作	結果
キーチェーンの編集	1. 編集するキーチェーンのチェックボックスをオンにします。 2. [Actions] にカーソルを合わせて [Edit] を選択します。 3. 必要な設定を編集します。 4. [Save] をクリックします。
キーチェーンの削除	1. 削除するキーチェーンのチェックボックスをオンにします。 2. [Actions] にカーソルを合わせて [Delete] を選択します。 3. ダイアログボックスで、**Yes** をクリックします。

ステップ 6 [Review and Provision] をクリックします。

ステップ 7 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

ステップ 8 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の AP 証明書ポリシーを設定します。

この手順を使用して、ワイヤレスコントローラの AP 証明書ポリシーを設定し、プロビジョニングします。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラのリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。

b) デバイス情報を含むダイアログボックスで、[デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[セキュリティ（Security）] を展開して [AP証明書ポリシー（AP Certificate Policy）] をクリックします。

ステップ 4 [MIC APを許可（Allow MIC APs）] トグルボタンを使用して、AP が ワイヤレスコントローラに参加するための Manufacturing Installed Certificate（MIC）の使用を有効または無効にします。

ステップ 5 （任意） [MIC APのトラストポイント名（Trustpoint Name for MIC APs）] ドロップダウンリストから、ワイヤレス管理インターフェイスの認証局とのセキュア通信を指定するトラストポイントを選択します。

ステップ 6 [Review and Provision] をクリックします。

ステップ 7 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

ステップ 8 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の MAC アドレスを使用した AP 証明書ポリシーの作成

MAC アドレスを使用して ワイヤレスコントローラ の AP 証明書ポリシーを作成してプロビジョニングするには、次の手順を実行します。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラのリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、[デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[セキュリティ（Security）] を展開して [AP証明書ポリシー（AP Certificate Policy）] をクリックします。

ステップ 4 [MAC/シリアル番号（MAC/Serial Number）] にカーソルを合わせ、[MAC] を選択します。

ステップ 5 [追加（Add）] にカーソルを合わせ、必要な方式を選択します。

- [単一エントリの追加（Add Single Entry）]：単一の MAC アドレスを使用して AP 証明書ポリシーを作成します。
- [CSVのアップロード（Upload CSV）]：カンマ区切り値（CSV）ファイルに記載されている MAC アドレスを使用して AP 証明書ポリシーを作成します。

次を選択できます。	下記を実行
単一エントリの追加	[AP証明書ポリシーMACの作成（Create AP Certificate Policy MAC）] スライドインペインの [APイーサネットMACアドレス（AP Ethernet MAC Address）] フィールドに、このポリシーを適用する AP のイーサネット MAC アドレスを入力します。 xxxx.xxxx.xxxx、xx-xx-xx-xx-xx-xx、または xx:xx:xx:xx:xx:xx のいずれかの形式で MAC アドレスを入力します。
CSVをアップロード	[CSVのアップロード（Upload CSV）] スライドインペインで、次の設定を完了します。 **1.** [サンプルCSV（sample CSV）] をクリックして、サンプル CSV ファイルをダウンロードします。 **2.** このポリシーを適用する AP のイーサネット MAC アドレスを入力します。 xxxx.xxxx.xxxx、xx-xx-xx-xx-xx-xx、または xx:xx:xx:xx:xx:xx のいずれかの形式で MAC アドレスを入力します。 **3.** CSV ファイルをドラッグアンドドロップ領域にドラッグアンドドロップするか、[ファイルを選択（Choose a file）] をクリックして CSV ファイルの場所を参照し、[開く（Open）] をクリックします。 **4.** [Upload] をクリックします。 Catalyst Center で検証チェックが実行されます。アップロードした CSV ファイルが要件を満たしていない場合は、エラーメッセージが表示されます。

ステップ 6 [Review and Provision] をクリックします。

ステップ 7 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

ステップ 8 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のシリアル番号を使用した AP 証明書ポリシーの作成

この手順を使用して、シリアル番号を使用してワイヤレスコントローラの AP 証明書ポリシーを作成し、プロビジョニングします。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラのリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[セキュリティ（Security）] を展開して [AP証明書ポリシー（AP Certificate Policy）] をクリックします。

ステップ 4 [MAC/シリアル番号（MAC/Serial Number）] にカーソルを合わせ、[シリアル番号（Serial Number）] を選択します。

ステップ 5 [追加（Add）] にカーソルを合わせ、必要な方式を選択します。

- [単一エントリの追加（Add Single Entry）]：単一のシリアル番号を使用して AP 証明書ポリシーを作成します。
- [CSVのアップロード（Upload CSV）]：カンマ区切り値（CSV）ファイルに記載されているシリアル番号を使用して AP 証明書ポリシーを作成します。

次を選択できます。	下記を実行
単一エントリの追加	[AP証明書ポリシーシリアル番号の作成（Create AP Certificate Policy Serial Number）] スライドインペインの [トラストアンカーシリアル番号（Trust Anchor Serial Number）] フィールドに、AP に関連付けられたトラストアンカー証明書のシリアル番号を入力します。 シリアル番号には 11 文字の数字を含める必要があります。 （注） シリアル番号が認証局によって発行されたシリアル番号と一致していることを確認してください。

次を選択できます。	下記を実行
CSVをアップロード	[CSVのアップロード（Upload CSV）] スライドインペインで、次の設定を完了します。 1. [サンプルCSV（sample CSV）] をクリックして、サンプルCSVファイルをダウンロードします。 2. APに関連付けられたトラストアンカー証明書のシリアル番号を入力します。 シリアル番号には 11 文字の数字を含める必要があります。 （注） シリアル番号が認証局によって発行されたシリアル番号と一致していることを確認してください。 3. CSV ファイルをドラッグアンドドロップ領域にドラッグアンドドロップするか、[ファイルを選択（Choose a file）] をクリックしてCSVファイルの場所を参照し、[開く（Open）] をクリックします。 4. [Upload] をクリックします。 Catalyst Center で検証チェックが実行されます。アップロードしたCSV ファイルが要件を満たしていない場合は、エラーメッセージが表示されます。

ステップ 6 [Review and Provision] をクリックします。

ステップ 7 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

ステップ 8 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のグローバルワイヤレス設定

このセクションでは Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のデバイスごとのグローバルワイヤレス設定に関する情報を示します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の CleanAir の設定

Cisco CleanAir テクノロジーは、シリコンレベルのインテリジェンスを使用して、スペクトル対応、自己回復、自己最適化型のワイヤレスネットワークを構築し、ワイヤレス干渉の影響を軽減します。

次の手順を使用して、ワイヤレスコントローラ の CleanAir パラメータを設定し、プロビジョニングします。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[グローバルワイヤレス（Global Wireless）] を展開し、[CleanAir] をクリックします。

ステップ 4 [6GHz] タブで、次の設定を完了します。

a) [Enable CleanAir] トグルボタンを使用して、6 GHz 帯域で CleanAir を有効または無効にします。
b) [干渉源のレポート（Report Interferers）] チェックボックスをオンにして、干渉源のレポートを有効にします。
c) [トラップの設定（Trap Configuration）] で、次の設定を完了します。

- （オプション）[電波品質の指標のトラップを有効化（Enable Air Quality Index (AQI)Trap）] チェックボックスをオンにして、この帯域で電波品質通知を有効にします。
- [AQI Alarm Threshold] フィールドに、AQI トラップのしきい値を入力します。

  有効な範囲は 1 ～ 100 です。デフォルト値は 10 です。
- この帯域で干渉デバイスレポート（IDR）通知を有効にするには、[セキュリティアラーム用干渉の有効化（Enable Interference for Security Alarm）] チェックボックスをオンにします。

d) [CleanAir詳細設定（Advanced CleanAir Configuration）] で、次の設定を完了します。

- [未分類カテゴリの電波品質アラーム（Air Quality Alarm for Unclassified category）] トグルボタンを使用して、未分類カテゴリの電波品質アラームを有効または無効にします。

- （オプション）[未分類カテゴリの電波品質アラームしきい値（Air Quality Alarm Threshold for Unclassified category）] フィールドに、未分類カテゴリの電波品質アラームのしきい値を入力します。

  有効な範囲は 1 ～ 100 です。

e) [検出する干渉タイプ（Interference Types to Detect）] および [トラップの対象とする干渉タイプ（Interference Types to Trap）] で、必要な干渉タイプの横にあるチェックボックスをオンにします。

f) ステップ 7 （1005 ページ） から ステップ 10 （1006 ページ） まで入力して、設定をプロビジョニングします。

ステップ 5 [5GHz] タブで、次の設定を完了します。

a) [Enable CleanAir] トグルボタンを使用して、5 GHz 帯域で CleanAir を有効または無効にします。

b) （任意）[スペクトルインテリジェンス（SI）の有効化（Enable Spectrum Intelligence (SI)）] チェックボックスをオンにして、この帯域でスペクトルインテリジェンス（SI）を有効にします。

c) （任意）[干渉源のレポート（Report Interferers）] チェックボックスをオンにして、干渉源のレポートを有効にします。

d) [トラップの設定（Trap Configuration）] で、次の設定を完了します。

- （オプション）[電波品質の指標のトラップを有効化（Enable Air Quality Index (AQI)Trap）] チェックボックスをオンにして、この帯域で電波品質通知を有効にします。
- [AQI Alarm Threshold] フィールドに、AQI トラップのしきい値を入力します。

  有効な範囲は 1 ～ 100 です。デフォルト値は 10 です。
- [セキュリティアラーム用干渉の有効化（Enable Interference for Security Alarm）] チェックボックスをオンにして、この帯域で IDR 通知を有効にします。

e) [CleanAir詳細設定（Advanced CleanAir Configuration）] で、次の設定を完了します。

- [未分類カテゴリの電波品質アラーム（Air Quality Alarm for Unclassified category）] トグルボタンを使用して、未分類カテゴリの電波品質アラームを有効または無効にします。
- （オプション）[未分類カテゴリの電波品質アラームしきい値（Air Quality Alarm Threshold for Unclassified category）] フィールドに、未分類カテゴリの電波品質アラームのしきい値を入力します。

  有効な範囲は 1 ～ 100 です。

f) [検出する干渉タイプ（Interference Types to Detect）] および [トラップの対象とする干渉タイプ（Interference Types to Trap）] で、必要な干渉タイプの横にあるチェックボックスをオンにします。

g) ステップ 7 （1005 ページ） から ステップ 10 （1006 ページ） まで入力して、設定をプロビジョニングします。

ステップ 6 [2.4 GHz] タブで、次の設定を完了します。

a) [Enable CleanAir] トグルボタンを使用して、2.4 GHz 帯域で CleanAir を有効または無効にします。

b) （任意）[スペクトルインテリジェンス（SI）の有効化（Enable Spectrum Intelligence (SI)）] チェックボックスをオンにして、この帯域でスペクトルインテリジェンス（SI）を有効にします。

c) [干渉源のレポート（Report Interferers）] チェックボックスをオンにして、干渉源のレポートを有効にします。

d) [トラップの設定（Trap Configuration）] で、次の設定を完了します。

- [電波品質の指標のトラップを有効化（Enable Air Quality Index (AQI) Trap）] チェックボックスをオンにして、この帯域で電波品質通知を有効にします。
- [AQI Alarm Threshold] フィールドに、AQI トラップのしきい値を入力します。

  有効な範囲は 1 ～ 100 です。デフォルト値は 10 です。
- [セキュリティアラーム用干渉の有効化（Enable Interference for Security Alarm）] チェックボックスをオンにして、この帯域で IDR 通知を有効にします。

e) [CleanAir詳細設定（Advanced CleanAir Configuration）] で、次の設定を完了します。

- [未分類カテゴリの電波品質アラーム（Air Quality Alarm for Unclassified category）] トグルボタンを使用して、未分類カテゴリの電波品質アラームを有効または無効にします。
- （オプション）[未分類カテゴリの電波品質アラームしきい値（Air Quality Alarm Threshold for Unclassified category）] フィールドに、未分類カテゴリの電波品質アラームのしきい値を入力します。

  有効な範囲は 1 ～ 100 です。

f) [検出する干渉タイプ（Interference Types to Detect）] および [トラップの対象とする干渉タイプ（Interference Types to Trap）] で、必要な干渉タイプの横にあるチェックボックスをオンにします。

g) ステップ 7（1005 ページ） から ステップ 10（1006 ページ） まで入力して、設定をプロビジョニングします。

ステップ 7 [Review and Provision] をクリックします。

ステップ 8 ワイヤレスコントローラ がライセンス要件を満たしていない AP を管理している場合、Catalyst Center は詳細を示すダイアログボックスを表示します。ダイアログボックスで、必要なオプションを選択します。

オプション	説明
ライセンス マネージャ	[License Manager] ウィンドウを開いて、対応するライセンスを有効にします。 ライセンスを有効にするには、『*Cisco Catalyst Center Administrator Guide*』の「Manage Licenses」を参照してください。
[デバイスプロビジョニングに進む（Continue to device provision）]	デバイスのプロビジョニングを続行します。 （注） ライセンス要件を満たしていない AP は、ワールドワイドセーフモード（WWSM）になります。
Cancel	ダイアログボックスを閉じます。

ステップ 9 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 10 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の高スループットパラメータの設定

次の手順を使用して、ワイヤレスコントローラ の高スループットパラメータを設定します。



重要 運用帯域で高いスループットを設定すると、クライアント接続が失われます。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[グローバルワイヤレス（Global Wireless）] を展開して [高スループット（High Throughput）] をクリックします。

ステップ 4 [6 GHz] タブでは、6 GHz 帯域の高スループットパラメータを設定します。

a) （任意） [11ax] で、次の設定を完了します。

- [SS/MCS] で、必要なチェックボックスをオンにして、対応する空間ストリーム（SS）または変調および符号化スキーム（MCS）の設定を選択します。
- [ビームフォーミングサポート（Beamforming Support）] ドロップダウンリストから、WLAN のビームフォーミングを有効または無効にするステータスを選択します。

  ビームフォーミングは、接続されているクライアントに信号を向けることで信号の品質を向上させて範囲を広げます。

- [HEダイナミックフラグメンテーション（HE Dynamic Fragmentation）] トグルボタンを使用して、高効率（HE）802.11ax 伝送のダイナミック フラグメンテーションを有効または無効にします。

b) （任意） [11be] で、次の設定を行います。

- [11beの有効化（Enable 11be）] トグルボタンを使用して、ワイヤレスコントローラ を有効または無効にし、802.11be ネットワークを管理します。
- [SS/MCS] で、必要なチェックボックスをオンにして、対応する SS または MCS の設定を選択します。

c) ステップ 7 （1009 ページ） から ステップ 10 （1009 ページ） まで入力して、設定をプロビジョニングします。

ステップ 5 [5 GHz] タブでは、5 GHz 帯域の高スループットパラメータを設定します。

a) （任意） [11n] で、次の設定を行います。

- [Enable 11n] トグルボタンを使用して、ワイヤレスコントローラ を有効または無効にし、802.11n ネットワークを管理します。
- [Dot11nショートガード有効（Dot11n Short Guard Enabled）] トグルボタンを使用して、この帯域での 802.11n ガード間隔のサポートを有効または無効にします。
- [MCS/（データレート）（MCS/(Data Rate)）] で、必要なチェックボックスをオンにして、対応する MCS またはデータレート設定を選択します。

b) （任意） [11ac] で、次の設定を行います。

- [Enable 11ac] トグルボタンを使用して、ワイヤレスコントローラ を有効または無効にし、802.11ac ネットワークを管理します。
- [SS/MCS/（データレート）（SS/MCS/(Data Rate)）] で、必要なチェックボックスをオンにして、対応する SS、MCS またはデータレート設定を選択します。

c) （任意） [11ax] で、次の設定を行います。

- [Enable 11ax] トグルボタンを使用して、ワイヤレスコントローラ を有効または無効にし、802.11ax ネットワークを管理します。
- [SS/MCS] で、必要なチェックボックスをオンにして、対応する SS または MCS の設定を選択します。
- [ビームフォーミングサポート（Beamforming Support）] ドロップダウンリストから、WLAN のビームフォーミングを有効または無効にするステータスを選択します。

  ビームフォーミングは、接続されているクライアントに信号を向けることで信号の品質を向上させて範囲を広げます。
- [RIFS伝送ステータス（RIFS Transmission Status）] トグルボタンを使用して、伝送での Reduced Interframe Spacing（RIFS）の使用を有効または無効にします。

- [HEダイナミックフラグメンテーション（HE Dynamic Fragmentation）] トグルボタンを使用して、高効率（HE）802.11ax 伝送のダイナミック フラグメンテーションを有効または無効にします。

d) （任意） [11be] で、次の設定を行います。

- [11beの有効化（Enable 11be）] トグルボタンを使用して、ワイヤレスコントローラ を有効または無効にし、802.11be ネットワークを管理します。
- [SS/MCS] で、必要なチェックボックスをオンにして、対応する SS または MCS の設定を選択します。

e) ステップ 7（1009 ページ）から ステップ 10（1009 ページ）まで入力して、設定をプロビジョニングします。

ステップ 6 [2.4 GHz] タブでは、2.4 GHz 帯域の高スループットパラメータを設定します。

a) （任意） [11n] で、次の設定を行います。

- [Enable 11n] トグルボタンを使用して、ワイヤレスコントローラ を有効または無効にし、802.11n ネットワークを管理します。
- [Dot11nショートガード有効（Dot11n Short Guard Enabled）] トグルボタンを使用して、この帯域での 802.11n ガード間隔のサポートを有効または無効にします。
- [MCS/（データレート）（MCS/(Data Rate)）] で、必要なチェックボックスをオンにして、対応する MCS またはデータレート設定を選択します。

b) （任意） [11ax] で、次の設定を行います。

- [Enable 11ax] トグルボタンを使用して、ワイヤレスコントローラ を有効または無効にし、802.11ax ネットワークを管理します。
- [SS/MCS] で、必要なチェックボックスをオンにして、対応する SS または MCS の設定を選択します。
- [ビームフォーミングサポート（Beamforming Support）] ドロップダウンリストから、WLAN のビームフォーミングを有効または無効にするステータスを選択します。

  ビームフォーミングは、接続されているクライアントに信号を向けることで信号の品質を向上させて範囲を広げます。
- [RIFS伝送ステータス（RIFS Transmission Status）] トグルボタンを使用して、伝送での Reduced Interframe Spacing（RIFS）の使用を有効または無効にします。
- [HEダイナミックフラグメンテーション（HE Dynamic Fragmentation）] トグルボタンを使用して、高効率（HE）802.11ax 伝送のダイナミック フラグメンテーションを有効または無効にします。

c) （任意） [11be] で、次の設定を行います。

- [11beの有効化（Enable 11be）] トグルボタンを使用して、ワイヤレスコントローラ を有効または無効にし、802.11be ネットワークを管理します。
- [SS/MCS] で、必要なチェックボックスをオンにして、対応する SS または MCS の設定を選択します。

d) ステップ 7（1009 ページ）から ステップ 10（1009 ページ）まで入力して、設定をプロビジョニングします。

ステップ 7 [Review and Provision] をクリックします。

ステップ 8 ワイヤレスコントローラ がライセンス要件を満たしていない AP を管理している場合、Catalyst Center は詳細を示すダイアログボックスを表示します。ダイアログボックスで、必要なオプションを選択します。

オプション	説明
ライセンス マネージャ	[License Manager] ウィンドウを開いて、対応するライセンスを有効にします。 ライセンスを有効にするには、『*Cisco Catalyst Center Administrator Guide*』の「Manage Licenses」を参照してください。
[デバイスプロビジョニングに進む（Continue to device provision）]	デバイスのプロビジョニングを続行します。 （注） ライセンス要件を満たしていない AP は、ワールドワイドセーフモード（WWSM）になります。
Cancel	ダイアログボックスを閉じます。

ステップ 9 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する（238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 10 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のメディアパラメータの設定

この手順を使用して、ワイヤレスコントローラ のビデオおよび音声メディアパラメータを設定し、設定をプロビジョニングします。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、[デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[グローバルワイヤレス（Global Wireless）] を展開して [メディアパラメータ（Media Parameters）] をクリックします。

ステップ 4 [6 GHz]、[5 GHz]、または [2.4 GHz] にカーソルを合わせ [メディア（Media）] をクリックして、必要なパラメータを設定します。

a) （任意）[メディア（Media）] で [ユニキャスト ビデオ リダイレクト（Unicast Video Redirect）] チェックボックスをオンにして、ユニキャストまたはマルチキャストのみのビデオストリームをベストエフォートベースでリダイレクトします。
b) （任意）[マルチキャスト ダイレクト アドミッション コントロール（Multicast Direct Admission Control）] で、次の設定を完了します。

- ビデオアクセスカテゴリのアドミッションコントロールを有効にするには、[メディア ストリーム アドミッション コントロール（ACM）（Media Stream Admission Control (ACM)）] チェックボックスをオンにします。
- 次のフィールドにデータを入力します。
  - [最大メディアストリームRF帯域幅（%）（Maximum Media Streams RF Bandwidth (%)）]：この無線帯域でメディアアプリケーション用に割り当てられる最大帯域幅の割合を入力します。

    有効な範囲は 5 ～ 85 です。デフォルト値は 5 です。
  - [最大メディア帯域幅（%）（Maximum Media Bandwidth (%)）] メディアトラフィックに許可される最大帯域幅の割合を入力します。

    有効な範囲は 5 ～ 85 です。デフォルト値は 85 です。
- [Client Minimum Phy Rate (kbps)] ドロップダウンリストから、マルチキャスト ダイレクト ストリームの最小クライアントレートを選択します。
- [Maximum Retry Percentage (%)] フィールドに、マルチキャスト ダイレクト ストリームの最大再試行率を入力します。

  有効範囲は 0 ～ 100 です。デフォルト値は 80 です。

c) （任意）[メディアストリーム-マルチキャストダイレクト（Media Stream - Multicast Direct）] で、必要なパラメータを設定します。

- 必要なチェックボックスをオンにして、対応する設定を行います。
  - [マルチキャストダイレクトの有効化（Enable Multicast Direct）]：無線でマルチキャスト ダイレクト ストリームを許可します。
  - [ベストエフォートQoSアドミッション（Best Effort QoS Admission）]：ベストエフォートキューでメディアストリームを許可します。
- 次のフィールドにデータを入力します。
  - [無線ごとの最大ストリーム数（Maximum Stream Per Radio）]：無線ごとのメディアストリームの最大許可数を選択します。
  - [クライアントごとの最大ストリーム数（Maximum Stream Per Client）]：クライアントごとのメディアストリームの最大許可数を選択します。

d) （任意）[コールアドミッション制御（CAC）詳細（Call Admission Control（CAC）Advanced）] で、次の設定を完了します。

- 5 GHz バンドの場合、[デフォルトの802.11a/n QoSパケット最大（バイト）（Default 802.11a/n QoS Packet Maximum (bytes)）] フィールドに、802.11a/n ネットワークでの QoS の最大許容パケットサイズ（バイト単位）を入力します。

  有効な範囲は 15000 ～ 400000000 です。
- [CACの最大同時通話数（CAC Maximum Concurrent Calls）] フィールドに、AP または無線帯域で許可される同時音声またはビデオ通話の最大数を入力します。

  有効な範囲は 0 ～ 4294967295 です。制限を設定しない場合は、このフィールドを空白のままにします。

e) ステップ6（1012ページ）から ステップ9（1013ページ）まで入力して、設定をプロビジョニングします。

ステップ5 [6 GHz]、[5 GHz]、または [2.4 GHz] にカーソルを合わせ [音声（Voice）] をクリックして、必要なパラメータを設定します。

a) （任意）[音声（Voice）] で [コールアドミッション制御（ACM）（Call Admission Control (ACM)）] チェックボックスをオンにして、音声アクセスカテゴリのアドミッションコントロールを有効にします。

このチェックボックスをオンにする場合は、次の設定を行います。

- [負荷ベースのCAC（Load-Based CAC）] チェックボックスをオンにして、負荷ベースのチャネル可用性チェック（CAC）を有効にします。
- 次のフィールドにデータを入力します。
  - [最大RF帯域幅（Maximum RF bandwidth (%)）]：802.11e クライアントに割り当てられる最大帯域幅の割合を入力します。

有効な範囲は 5 ～ 85 です。デフォルト値は 75 です。

- [予約済みローミング帯域幅（%）（Reserved Roaming Bandwidth (%)）]：音声トラフィック用のローミングクライアントに割り当てられる最大帯域幅の割合を入力します。

  有効な範囲は 0 ～ 25 です。デフォルト値は、6 です。

- [緊急帯域幅（Expedited Bandwidth）] チェックボックスをオンにして、帯域幅要求の迅速化をサポートを有効にします。
- [SIP CACおよび帯域幅（SIP CAC and Bandwidth）] で、[SIP CACサポート（SIP CAC Support）] チェックボックスをオンにして、SIP CAC サポートを有効にします。

  SIP CAC サポートを有効にする場合は、必要な設定を行います。

  - [SIP帯域幅（kbps）（SIP Bandwidth (kbps)）] フィールドに、このコントローラに関連付けられた AP の dot11 帯域の SIP CAC 設定に対する帯域幅を kbps 単位で入力します。

    有効な範囲は 8 ～ 64 です。デフォルト値は 64 です。

  - [SIP音声サンプリング間隔（ミリ秒）（SIP Voice Sample Interval (ms)）] ドロップダウンリストから、このコントローラに関連付けられた AP の dot11 帯域に対する SIP CAC 設定の音声サンプル間隔をミリ秒単位で選択します。

b) （任意）[トラフィック ストリーム メトリック（Traffic Stream Metrics）] で、必要な設定を行います。

- 対応する設定を有効にするには、必要なチェックボックスをオンにします。
  - [メトリックコレクション（Metrics Collection）]：802.11a トラフィック ストリーム メトリックのサポートを有効にします。

    メトリックを有効にすると、関連付けられた AP は 802.11a インターフェイス上のトラフィックに関する統計データを 90 秒ごとにコントローラに送信します。

  - [無通信タイムアウト（Inactivity Timeout]：通信仕様（TSPEC）の非通信タイムアウト処理モードを有効にします。

- 次のフィールドにデータを入力します。
  - [ストリームサイズ（Stream Size）]：メディアストリームの最大許容データレートを入力します。

    有効な範囲は 84,000 ～ 92,100 です。

  - [最大ストリーム数（Maximum Streams）]：TSPEC ごとのメディアストリームの最大数を入力します。

    有効な範囲は 1 ～ 5 です。

c) ステップ 6（1012 ページ）から ステップ 9（1013 ページ）まで入力して、設定をプロビジョニングします。

ステップ 6 [Review and Provision] をクリックします。

ステップ 7 ワイヤレスコントローラ がライセンス要件を満たしていない AP を管理している場合、Catalyst Center は詳細を示すダイアログボックスを表示します。ダイアログボックスで、必要なオプションを選択します。

オプション	説明
ライセンス マネージャ	[License Manager] ウィンドウを開いて、対応するライセンスを有効にします。 ライセンスを有効にするには、『*Cisco Catalyst Center Administrator Guide*』の「Manage Licenses」を参照してください。
[デバイスプロビジョニングに進む（Continue to device provision）]	デバイスのプロビジョニングを続行します。 （注） ライセンス要件を満たしていない AP は、ワールドワイドセーフモード（WWSM）になります。
Cancel	ダイアログボックスを閉じます。

ステップ 8 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

ステップ 9 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の Air Time Fairness の設定

次の手順を使用して、ワイヤレスコントローラ の Air Time Fairness（ATF）パラメータを設定します。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。

b) デバイス情報を含むダイアログボックスで、[デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、c を展開して、[Air Time Fairness] をクリックします。

ステップ 4 [5 GHz] または [2.4 GHz] のいずれかのタブをクリックし、これらの設定を完了します。

a) バンドの ATF を有効または無効にするには、[ステータス（Status）] トグルボタンを使用します。

b) [モード（Mode）] ドロップダウンリストから、ATF 動作モードを選択します。

[強制（Enforced）] モードを選択した場合、必要に応じて [最適化（Optimization）] チェックボックスをオンにして、ATF 最適化を有効にできます。

c) デフォルトの RF ポリシーで通信時間割り当てモードを有効にするには、[ブリッジクライアントアクセス（Bridge Client Access）] チェックボックスをオンにします。

[ブリッジ クライアント アクセス（Bridge Client Access）] チェックボックスをオンにした場合は、[通信時間割り当て（Airtime Allocation）] フィールドに、必要に応じて通信時間割り当ての重みの割合を入力します。

有効な範囲は 5 ～ 90 です。デフォルト値は 5 です。

ステップ 5 [Review and Provision] をクリックします。

ステップ 6 ワイヤレスコントローラ がライセンス要件を満たしていない AP を管理している場合、Catalyst Center は詳細を示すダイアログボックスを表示します。ダイアログボックスで、必要なオプションを選択します。

オプション	説明
ライセンス マネージャ	[License Manager] ウィンドウを開いて、対応するライセンスを有効にします。 ライセンスを有効にするには、『*Cisco Catalyst Center Administrator Guide*』の「Manage Licenses」を参照してください。
[デバイスプロビジョニングに進む（Continue to device provision）]	デバイスのプロビジョニングを続行します。 （注） ライセンス要件を満たしていない AP は、ワールドワイドセーフモード（WWSM）になります。
Cancel	ダイアログボックスを閉じます。

ステップ 7 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

ステップ 8 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の Air Time Fairness ポリシーの作成

ワイヤレスコントローラ の Air Time Fairness（ATF）ポリシーを作成してプロビジョニングするには、次の手順を実行します。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、 で、[グローバルワイヤレス（Global Wireless）] を展開して [Air Time Fairness（Airtime Fairness）] をクリックします。

ステップ 4 [Policy] タブをクリックします。

ステップ 5 [Add] をクリックします。

ステップ 6 [ATFポリシーの作成（Create ATF Policy）] スライドインペインの [ATFポリシー名（ATF Policy Name）] フィールドに、ATF ポリシーの一意の名前を入力します。

ステップ 7 [ID] フィールドに ATF ポリシーの一意の ID を入力します。

有効な範囲は 0 ～ 511 です。

ステップ 8 [Weight] フィールドに、ATF ポリシーのポリシーの重みを入力します。

有効な範囲は 5 ～ 100 です。デフォルト値は 10 です。

ステップ 9 （任意） [クライアント共有（Client Sharing）] チェックボックスをオンにし、ATF ポリシーの公平なクライアント共有を有効にします。

ステップ 10 [Review and Provision] をクリックします。

ステップ 11 ワイヤレスコントローラ がライセンス要件を満たしていない AP を管理している場合、Catalyst Center は詳細を示すダイアログボックスを表示します。ダイアログボックスで、必要なオプションを選択します。

オプション	説明
ライセンス マネージャ	[License Manager] ウィンドウを開いて、対応するライセンスを有効にします。 ライセンスを有効にするには、『*Cisco Catalyst Center Administrator Guide*』の「Manage Licenses」を参照してください。
[デバイスプロビジョニングに進む（Continue to device provision）]	デバイスのプロビジョニングを続行します。 （注） ライセンス要件を満たしていないAPは、ワールドワイドセーフモード（WWSM）になります。
Cancel	ダイアログボックスを閉じます。

ステップ 12 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 13 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のネットワークパラメータの設定

次の手順を使用して、ワイヤレスコントローラのネットワークパラメータを設定し、設定をプロビジョニングします。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[グローバルワイヤレス（Global Wireless）] を展開して [ネットワークパラメータ（Network Parameters）] をクリックします。

ステップ 4 [6 GHz] タブで、6 GHz 帯域の必要なパラメータを設定します。

a) [一般（General）] で、次の設定を完了します。

- （オプション）[6 GHzネットワークステータス（6 GHz Network Status）] チェックボックスをオンにして、6 GHz 帯域を有効にします。

（注） この帯域が動作している場合、[Beacon Interval (msec)]、[Fragmentation Threshold (bytes)]、または [DTPC Support] を設定すると、クライアントの接続が失われます。

- 次のフィールドにデータを入力します。
  - [ビーコン間隔（ミリ秒）（Beacon Interval（msec）] フィールドに、AP 無線が、ビーコン送信のスケジューリングに使用できる時間をミリ秒単位で入力します。

    有効な範囲は 20 ～ 1000 です。デフォルト値は 100 です。
  - [フラグメンテーションしきい値（バイト）（Fragmentation Threshold (bytes)）] フィールドに、パケットをフラグメント化するサイズをバイト単位で入力します。

    有効な範囲は 256 ～ 2346 です。デフォルト値は 2346 です。

- [DTPCサポート（DTPC Support）] チェックボックスをオンにして、すべての 802.11b/g 帯域でダイナミック伝送パワーコントロール（DTPC）を有効にします。

  FTPC が有効になっている場合、無線の送信電力レベルがビーコンにアドバタイズされ、プローブが応答します。

（注） DTPC を有効にする場合、5 GHz 帯域の電力制限値は設定できません。詳細については、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のグローバル無線パラメータの設定 （1023 ページ）を参照してください。

b) （任意） [CCXロケーション測定（CCX Location Measurement）] で [モード（Mode）] チェックボックスをオンにして、802.11 Cisco Client Extensions（CCX）クライアントロケーション測定のサポートを有効にします。

この測定を有効にする場合は、[Interval] フィールドに、802.11 CCX クライアントロケーション測定間隔を入力します。

この間隔の有効な範囲は 10 ～ 32400 です。デフォルト値は 60 です。

c) （任意） A-MPDU Tx および A-MSDU Tx で、集約 MAC プロトコルデータユニット（A-MPDU）と集約MACサービスデータユニット（A-MSDU）の送信優先順位を有効にする必要な優先順位レベルを選択します。

d) [802.11一般パラメータ（General 802.11 Parameters）] で、[ワールドモード（IE）の有効化（Enable World Mode (IE)）] トグルボタンを使用して、AP のビーコンフレームにワールドモード情報要素（IE）含めることを有効または無効にします。

異なる規制ドメインのクライアントにネットワークサービスを提供する場合、または国際無線規格に確実に準拠する場合は、このオプションをオンにします。

e) ステップ 7（1022 ページ）から ステップ 10（1022 ページ）まで入力して、設定をプロビジョニングします。

ステップ 5 [5 GHz] タブで、5 GHz 帯域の必要なパラメータを設定します。

a) [一般（General）] で、次の設定を完了します。

- （オプション）[5 GHzネットワークステータス（5 GHz Network Status）] チェックボックスをオンにして、5 GHz 帯域を有効にします。

（注） この帯域が動作している場合、[Beacon Interval (msec)]、[Fragmentation Threshold (bytes)]、[DTPC Support]、またはデータレートを設定すると、クライアントの接続が失われます。

- 次のフィールドにデータを入力します。
  - [ビーコン間隔（ミリ秒）（Beacon Interval（msec）] フィールドに、AP 無線が、ビーコン送信のスケジューリングに使用できる時間をミリ秒単位で入力します。

    有効な範囲は 20 ～ 1000 です。デフォルト値は 100 です。
  - [フラグメンテーションしきい値（バイト）（Fragmentation Threshold (bytes)）] フィールドに、パケットをフラグメント化するサイズをバイト単位で入力します。

    有効な範囲は 256 ～ 2346 です。デフォルト値は 2346 です。
  - [RSSIしきい値（dBm）（RSSI Threshold (dBm)）] : 最適化されたローミングが発生する最小 RSSI しきい値を入力します。

    有効な範囲は -127 ～ 0 です。デフォルト値は -127 です。

- （オプション）必要なチェックボックスをオンにして、対応する設定を行います。
  - [DTPCサポート（DTPC Support）] : すべての 802.11b/g バンドで DTPC を有効にします。

    FTPCが有効になっている場合、無線の送信電力レベルがビーコンにアドバタイズされ、プローブが応答します。

（注） DTPC を有効にする場合、5 GHz 帯域の電力制限値は設定できません。詳細については、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のグローバル無線パラメータの設定（1023 ページ）を参照してください。

- [トライ無線モード（Tri Radio Mode）]：トライ無線モードを有効にします。
- [RSSI Low Check]：最適化されたローミングが発生する前に RSSI しきい値が有効になっているか確認します。

b) （任意）[CCXロケーション測定（CCX Location Measurement）] で、[モード（Mode）] チェックボックスをオンにして、802.11 CCX クライアントロケーション測定のサポートを有効にします。

この測定を有効にする場合は、[Interval] フィールドに、802.11 CCX クライアントロケーション測定間隔を入力します。

この間隔の有効な範囲は 10 ～ 32400 です。デフォルト値は 60 です。

c) [データレート（Data Rates）] で、データレートのドロップダウンリストから、対応するデータレートの設定を選択します。

オプション	説明
必須	ワイヤレスコントローラ で AP に関連付けるには、クライアントがこのデータレートをサポートする必要があります。
サポートあり	このデータレートをサポートする、関連付けられた任意のクライアントは、そのレートを使用して AP と通信できる可能性があります。
無効	通信に使用するデータレートは、クライアントが指定します。

d) （任意） [A-MPDU Tx] で、次の設定を完了します。

- [Ampduウィンドウサイズ（Ampdu Window Size）] フィールドに、A-MPDU のウィンドウサイズを入力します。

  有効な範囲は 1 ～ 255 です。

- [集約スケジューラ（Aggregation Scheduler）] トグルボタンを使用して、802.11n A-MPDU スケジューラを有効または無効にします。
- [フレームバースト（Frame Burst）] ドロップダウンリストから、802.11n A-MPDU のバーストに必要な設定を選択します。
- [リアルタイム トラフィック タイムアウト（Realtime Traffic Timeout）] フィールドに、A-MPDU 送信集約スケジューラのリアルタイム トラフィック タイムアウトをミリ秒単位で入力します。

  有効な範囲は 1 ～ 1000 です。

- A-MSDU 送信の優先順位を有効にする必要な優先順位レベルを選択します。

e) （任意）[A-MSDU Tx] で、A-MSDU 送信の優先順位を有効にする必要な優先順位レベルを選択します。

f) [802.11一般パラメータ（General 802.11 Parameters）] で、[ワールドモード（IE）の有効化（Enable World Mode (IE)）] トグルボタンを使用して、AP のビーコンフレームにワールドモード情報要素（IE）含めることを有効または無効にします。

異なる規制ドメインのクライアントにネットワークサービスを提供する場合、または国際無線規格に確実に準拠する場合は、このオプションをオンにします。

g) ステップ 7（1022 ページ）から ステップ 10（1022 ページ）まで入力して、設定をプロビジョニングします。

ステップ 6 [2.4 GHz] タブで、2.4-GHz 帯域の必要なパラメータを設定します。

a) [一般（General）] で、次の設定を完了します。

- （オプション）[2.4 GHz ネットワークステータス（2.4 GHz Network Status）] チェックボックスをオンにして、2.4 GHz 帯域を有効にします。

（注） この帯域が動作している場合、[802.11g Network Status]、[Beacon Interval (msec)]、[Short Preamble]、[Fragmentation Threshold (bytes)]、[DTPC Support]、またはデータレートを設定すると、クライアントの接続が失われます。

- [802.11gネットワークステータス（802.11g Network Status）] トグルボタンを使用して、802.11b ネットワークで 802.11g サポートを有効または無効にします。
- 次のフィールドにデータを入力します。
  - [ビーコン間隔（ミリ秒）（Beacon Interval（msec）] フィールドに、AP 無線が、ビーコン送信のスケジューリングに使用できる時間をミリ秒単位で入力します。

    有効な範囲は 20 ～ 1000 です。デフォルト値は 100 です。
  - [フラグメンテーションしきい値（バイト）（Fragmentation Threshold (bytes)）] フィールドに、パケットをフラグメント化するサイズをバイト単位で入力します。

    有効な範囲は 256 ～ 2346 です。デフォルト値は 2346 です。
  - [RSSIしきい値（dBm）（RSSI Threshold (dBm)）]：最適化されたローミングの最小 RSSI しきい値を入力します。

    有効な範囲は -127 ～ 0 です。デフォルト値は -127 です。
- 必要なチェックボックスをオンにして、対応する設定を行います。
  - [ショートプリアンブル（Short Preamble）]：無線プリアンブルの短いバージョンの送信を有効にします。

- [DTPCサポート（DTPC Support）]：すべての 802.11b/g バンドで DTPC を有効にします。

  FTPCが有効になっている場合、無線の送信電力レベルがビーコンにアドバタイズされ、プローブが応答します。

（注） DTPC を有効にする場合、5 GHz 帯域の電力制限値は設定できません。詳細については、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のグローバル無線パラメータの設定（1023 ページ）を参照してください。

- [RSSI Low Check]：最適化されたローミングが発生する前に RSSI しきい値が有効になっているか確認します。

b) （任意）[CCXロケーション測定（CCX Location Measurement）]で、[モード（Mode）]チェックボックスをオンにして、802.11 CCX クライアントロケーション測定のサポートを有効にします。

この測定を有効にする場合は、[Interval] フィールドに、802.11 CCX クライアントロケーション測定間隔を入力します。

この間隔の有効な範囲は 10 ～ 32400 です。デフォルト値は 60 です。

c) [データレート（Data Rates）] で、データレートのドロップダウンリストから、対応するデータレートの設定を選択します。

オプション	説明
必須	ワイヤレスコントローラ で AP に関連付けるには、クライアントがこのデータレートをサポートする必要があります。
サポートあり	このデータレートをサポートする、関連付けられた任意のクライアントは、そのレートを使用して AP と通信できる可能性があります。
無効	通信に使用するデータレートは、クライアントが指定します。

d) （任意） [A-MPDU Tx] で、次の設定を完了します。

- [Ampduウィンドウサイズ（Ampdu Window Size）] フィールドに、A-MPDU のウィンドウサイズを入力します。

  有効な範囲は 1 ～ 255 です。

- [集約スケジューラ（Aggregation Scheduler）] トグルボタンを使用して、802.11n A-MPDU スケジューラを有効または無効にします。

- [リアルタイム トラフィック タイムアウト（Realtime Traffic Timeout）] フィールドに、A-MPDU 送信集約スケジューラのリアルタイム トラフィック タイムアウトをミリ秒単位で入力します。

  有効な範囲は 1 ～ 1000 です。

- A-MSDU 送信の優先順位を有効にする必要な優先順位レベルを選択します。

e) （任意）[A-MSDU Tx] で、A-MSDU 送信の優先順位を有効にする必要な優先順位レベルを選択します。

f) [802.11一般パラメータ（General 802.11 Parameters）] で、[ワールドモード（IE）の有効化（Enable World Mode (IE)）] トグルボタンを使用して、AP のビーコンフレームにワールドモード情報要素（IE）含めることを有効または無効にします。

異なる規制ドメインのクライアントにネットワークサービスを提供する場合、または国際無線規格に確実に準拠する場合は、このオプションをオンにします。

g) ステップ 7（1022 ページ）から ステップ 10（1022 ページ）まで入力して、設定をプロビジョニングします。

ステップ 7 [Review and Provision] をクリックします。

ステップ 8 ワイヤレスコントローラ がライセンス要件を満たしていない AP を管理している場合、Catalyst Center は詳細を示すダイアログボックスを表示します。ダイアログボックスで、必要なオプションを選択します。

オプション	説明
ライセンス マネージャ	[License Manager] ウィンドウを開いて、対応するライセンスを有効にします。 ライセンスを有効にするには、『*Cisco Catalyst Center Administrator Guide*』の「Manage Licenses」を参照してください。
[デバイスプロビジョニングに進む（Continue to device provision）]	デバイスのプロビジョニングを続行します。 （注） ライセンス要件を満たしていない AP は、ワールドワイドセーフモード（WWSM）になります。
Cancel	ダイアログボックスを閉じます。

ステップ 9 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 10 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のグローバル無線パラメータの設定

ワイヤレスコントローラ のグローバル無線パラメータを設定し、その設定をプロビジョニングするには、次の手順を実行します。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。

b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。

c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。

b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[グローバルワイヤレス（Global Wireless）] を展開して [グローバルパラメータ（Global Parameters）] をクリックします。

ステップ 4 [6 GHz] タブで、6-GHz 帯域の必要なパラメータを設定します。

a) [EDCA] で、次の設定を完了します。

（注） この帯域が動作している場合、拡張型分散チャネルアクセス（EDCA）プロファイルまたは DFS チャネル スイッチ アナウンス モードを設定すると、クライアントの接続が失われます。

- [EDCAプロファイル（EDCA Profile）] ドロップダウンリストから、EDCA パラメータセット要素で使用する EDCA プロファイルを選択します。

  EDCA パラメータで、音声、ビデオ、およびその他の Quality of Service（QoS）トラフィックに対して、優先的なワイヤレスチャネルアクセスを提供します。

- （オプション） [クライアントの負荷ベースの設定（Client Load Based Configuration）] チェックボックスをオンにして、クライアントの負荷ベースの EDCA を有効にし、アクティブなクライアントと負荷に基づいてクライアントの EDCA パラメータを動的に変更することでコリジョンを減らします。

b) [802.11ax] で、必要なチェックボックスをオンにして必要な設定を有効にします。

- [ターゲット起動時間（Target Wake Up Time）] : AP が Wi-Fi ネットワーク内のアクティビティを管理できるようにします。

  AP は以下の方法でアクティビティを管理します。

- ステーション（STA）間の媒体の競合を最小限に抑える。
- 省電力モードの STA が起動する必要がある時間を短縮する。

- [Multiple BSSID]：802.11ax の複数の基本サービスセット識別子（BSSID）機能を有効にします。
- [Target Wake up time broadcast]：802.11ax ターゲット起動時間のブロードキャストを有効にします。
- [BSS Color]：802.11ax BSS カラー機能を有効にします。

c) ステップ 7（1026 ページ）から ステップ 10（1027 ページ）まで入力して、設定をプロビジョニングします。

ステップ 5 [5 GHz] タブで、5 GHz 帯域の必要なパラメータを設定します。

a) [EDCA] で、次の設定を完了します。

（注） この帯域が動作している場合、EDCA プロファイル、DFS チャネル スイッチ アナウンス モード、またはオーバーラップ BSS パケット検出（OBSS-PD）を設定すると、クライアントの接続が失われます。

- [EDCAプロファイル（EDCA Profile）] ドロップダウンリストから、EDCA パラメータセット要素で使用する EDCA プロファイルを選択します。

  EDCA パラメータで、音声、ビデオ、およびその他の Quality of Service（QoS）トラフィックに対して、優先的なワイヤレスチャネルアクセスを提供します。

- （オプション）[クライアントの負荷ベースの設定（Client Load Based Configuration）] チェックボックスをオンにして、クライアントの負荷ベースの EDCA を有効にし、アクティブなクライアントと負荷に基づいてクライアントの EDCA パラメータを動的に変更することでコリジョンを減らします。

b) [802.11ax] で、次の設定を完了します。

- （任意）対応する設定を有効にするには、必要なチェックボックスをオンにします。
  - [ターゲット起動時間（Target Wake Up Time）]：AP が Wi-Fi ネットワーク内のアクティビティを管理できるようにします。

    AP は以下の方法でアクティビティを管理します。
    - ステーション（STA）間の媒体の競合を最小限に抑える。
    - 省電力モードの STA が起動する必要がある時間を短縮する。

  - [BSS Color]：802.11ax BSS カラー機能を有効にします。
  - [Target Wake up time broadcast]：802.11ax ターゲット起動時間のブロードキャストを有効にします。

- [OBSS PD]：OBSS-PD 空間再利用を有効にします。

- [Non-SRG OBSS PD Max Threshold (dBm)] フィールドに、非空間再利用グループ（SRG）OBSS PD 最大しきい値を dBm 単位で入力します。

  有効な範囲は -82 ～ -62 です。

- （オプション）[SRG OBSS PD] チェックボックスをオンにして、SRG OBSS-PD 機能を有効にします。

- 次のフィールドにデータを入力します。

  - [SRG OBSS PD Min Threshold (dBm)]：SRG OBSS-PD 最小しきい値を dBm 単位で入力します。

    有効な範囲は -82 ～ -62 です。

  - [SRG OBSS PD Max Threshold (dBm)]：SRG OBSS-PD 最大しきい値を dBm 単位で入力します。

    有効な範囲は -82 ～ -62 です。

c) [DFS (802.11h)] で、次の設定を完了します。

- [チャネルスイッチステータス（Channel Switch Status）] チェックボックスをオンにして、チャネルスイッチ機能を有効にします。

- [スマートDFS（Smart DFS）] チェックボックスをオンにして動的周波数選択（DFS）を有効にし、レーダー信号による干渉を回避します。

- [Channel Switch Announcement Mode] ドロップダウンリストからモードを選択します。

- [Power Constraint] フィールドに、電力制限値を入力します。

  有効な範囲は 0 ～ 30 です。

d) ステップ 7（1026 ページ）から ステップ 10（1027 ページ）まで入力して、設定をプロビジョニングします。

ステップ 6 [2.4 GHz] タブで、2.4-GHz 帯域の必要なパラメータを設定します。

a) [EDCA] で、次の設定を完了します。

（注） この帯域が動作している場合、EDCA プロファイルまたは OBSS-PD を設定すると、クライアントの接続が失われます。

- [EDCAプロファイル（EDCA Profile）] ドロップダウンリストから、EDCA パラメータセット要素で使用する EDCA プロファイルを選択します。

  EDCA パラメータで、音声、ビデオ、およびその他の Quality of Service（QoS）トラフィックに対して、優先的なワイヤレスチャネルアクセスを提供します。

- （オプション）[クライアントの負荷ベースの設定（Client Load Based Configuration）] チェックボックスをオンにして、クライアントの負荷ベースの EDCA を有効にし、アクティブなクライアントと負荷に基づいてクライアントの EDCA パラメータを動的に変更することでコリジョンを減らします。

b) [802.11ax] で、次の設定を完了します。

- （任意）対応する設定を有効にするには、必要なチェックボックスをオンにします。
  - [ターゲット起動時間（Target Wake Up Time）]：AP が Wi-Fi ネットワーク内のアクティビティを管理できるようにします。

    AP は以下の方法でアクティビティを管理します。
    - ステーション（STA）間の媒体の競合を最小限に抑える。
    - 省電力モードの STA が起動する必要がある時間を短縮する。
  - [BSS Color]：802.11ax BSS カラー機能を有効にします。
  - [Target Wake up time broadcast]：802.11ax ターゲット起動時間のブロードキャストを有効にします。
  - [OBSS PD]：OBSS-PD 空間再利用を有効にします。
- [Non-SRG OBSS PD Max Threshold (dBm)] フィールドに、非 SRG OBSS PD 最大しきい値を dBm 単位で入力します。

  有効な範囲は -82 ～ -62 です。
- （オプション）[SRG OBSS PD] チェックボックスをオンにして、SRG OBSS-PD 機能を有効にします。
- 次のフィールドにデータを入力します。
  - [SRG OBSS PD Min Threshold (dBm)]：SRG OBSS-PD 最小しきい値を dBm 単位で入力します。

    有効な範囲は -82 ～ -62 です。
  - [SRG OBSS PD Max Threshold (dBm)]：SRG OBSS-PD 最大しきい値を dBm 単位で入力します。

    有効な範囲は -82 ～ -62 です。

c) ステップ 7（1026 ページ）から ステップ 10（1027 ページ）まで入力して、設定をプロビジョニングします。

ステップ 7 [Review and Provision] をクリックします。

ステップ 8 ワイヤレスコントローラ がライセンス要件を満たしていない AP を管理している場合、Catalyst Center は詳細を示すダイアログボックスを表示します。ダイアログボックスで、必要なオプションを選択します。

オプション	説明
ライセンス マネージャ	[License Manager] ウィンドウを開いて、対応するライセンスを有効にします。 ライセンスを有効にするには、『*Cisco Catalyst Center Administrator Guide*』の「Manage Licenses」を参照してください。
[デバイスプロビジョニングに進む（Continue to device provision）]	デバイスのプロビジョニングを続行します。 （注） ライセンス要件を満たしていないAPは、ワールドワイドセーフモード（WWSM）になります。
Cancel	ダイアログボックスを閉じます。

ステップ 9 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 10 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの 6 GHz 帯域における RRM の設定

ワイヤレスコントローラ の 6 GHz 帯域で無線リソース管理（RRM）パラメータを設定し、その設定をプロビジョニングするには、次の手順を実行します。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、[デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[グローバルワイヤレス（Global Wireless）] を展開して [RRM] をクリックします。

ステップ 4 [6 GHz] にカーソルを置き、[一般（General）] を選択して次の設定を完了します。

a) [トラップのプロファイルしきい値（Profile Threshold for Traps）] で、次の設定を完了します。

- [Throughput (Bps)] フィールドに、802.11a スループットしきい値を入力します。

  有効な範囲は 1000 ～ 10000000 です。デフォルト値は 1,000,000 です。

- （オプション）[自動CFG（Automatic CFG）] チェックボックスをオンにして、パフォーマンスプロファイルモードを有効にします。

b) [ノイズ/干渉/不正/CleanAir/SIモニタリングチャネル（Noise/Interference/Rogue/CleanAir/SI Monitoring Channels）] セクションで、必要なオプションを選択します。

（注） CleanAir および SI モニタリングは、AP がモニターモードの場合にのみ実行されます。

- [チャネルリスト（Channel List）]：監視するチャネルを選択します。
- [RRMネイバー検出タイプ（RRM Neighbor Discover Type）]：ネイバー検出プロトコル（NDP）のモードを選択します。

c) [監視間隔（Monitor Intervals）] で、次の設定を完了します。

- 次のフィールドにデータを入力します。
  - [ネイバーパケット頻度（秒）（Neighbor Packet Frequency (sec)）]：各 AP で新しい信号強度、ノイズ、干渉測定値を受信する頻度を指定する間隔を秒単位で入力します。

    有効な範囲は 60 ～ 3600 です。デフォルト値は 180 です。

  - [レポート間隔（秒）（Reporting Interval (sec)）]：各測定レポートの間隔を秒単位で入力します。

    有効な範囲は 60 ～ 3600 です。デフォルト値は 180 です。

  - [ネイバータイムアウト係数（Neighbor Timeout Factor）]：ネイバーパケットを受信しなかった場合にネイバーが期限切れになるまでの時間を指定する、ネイバータイムアウト係数を入力します。

    有効な範囲は 5 ～ 60 です。デフォルト値は 20 です。

  - [カバレッジ監視間隔（Monitor Coverage Interval）]：各 AP で新しいカバレッジ測定値を受信する間隔を秒単位で入力します。

    有効な範囲は 60 ～ 3600 です。

  - [負荷監視間隔（Monitor Load Interval）]：各 AP で新しい負荷測定値を受信する間隔を秒単位で入力します。

    有効な範囲は 60 ～ 3600 です。

- （任意）対応する設定を有効にするには、必要なチェックボックスをオンにします。
  - [チャネル監視ステータス（Channel Monitor Status）]：ネイバーモニタリングモードを有効にします。
  - [RSSI監視正規化（Monitor RSSI Normalization）]：802.11 ネイバー探索 RSSI 正規化を有効にします。
  - [システムログ負荷（Sys Log Load）]：負荷プロファイルのロギングモードを有効にします。
  - [システムログチャネル（Sys Log Channel）]：ダイナミックチャネル変更のロギングモードを有効にします。
  - [システムログパフォーマンス（Sys Log Performance）]：パフォーマンスプロファイルのロギングモードを有効にします。
  - [システムログカバレッジ（Sys Log Coverage）]：カバレッジプロファイルのロギングモードを有効にします。
  - [システムログ外部（Sys Log Foreign）]：外部プロファイルのロギングモードを有効にします。
- [イベントノイズのログ記録（Log Noise Events）] トグルボタンを使用して、RRM システムによって検出されたノイズ関連のイベントをログに記録します。

  ノイズイベントのロギングは、ワイヤレス干渉の問題の監視と障害対応に役立ちます。

d) ステップ 10（1032 ページ）から ステップ 13（1033 ページ）まで入力して、設定をプロビジョニングします。

ステップ 5 [6 GHz] にカーソルを合わせて [カバレッジ（Coverage）] を選択し、次の設定を完了します。

a) [カバレッジホール検出の有効化（Enable Coverage Hole Detection）] トグルボタンを使用して、カバレッジホール検出（CHD）を有効または無効にします。

b) 次のフィールドにデータを入力します。

- [データパケット数（Data Packet Count）]：CHD アルゴリズムがトリガーされる、データパケット数の最小しきい値を入力します。

  有効な範囲は 1 ～ 255 です。
- [音声パケット数（Voice Packet Count）]：CHD アルゴリズムがトリガーされる、音声パケット数の最小しきい値を入力します。

  有効な範囲は 1 ～ 255 です。
- [データパケットパーセンテージ（Data Packet Percentage）]：CHD アルゴリズムがトリガーされる、ドロップされるデータパケットの割合のしきい値を入力します。

  有効な範囲は 1 ～ 100 です。
- [音声パケットパーセンテージ（Voice Packet Percentage）]：CHD アルゴリズムがトリガーされる、ドロップされる音声パケットの割合のしきい値を入力します。

有効な範囲は 1 ～ 100 です。

c) ステップ 10 （1032 ページ） から ステップ 13 （1033 ページ） まで入力して、設定をプロビジョニングします。

ステップ 6 [6 GHz] にカーソルを合わせて [DCA] を選択し、次の設定を完了します。

a) [チャネル割り当てモード（Channel Assignment Mode）] ドロップダウンリストからモードを選択します。

[自動（Automatic）] を選択した場合は、対応するドロップダウンリストから必要なオプションを選択します。

- [間隔（Interval）]：DCA の間隔を選択します。
- [アンカー時間（Anchortime）]：DCA のアンカー時間を選択します。

b) [DCAチャネル感度（DCA Channel Sensitivity）] ドロップダウンリストから、DCA 感度レベルを選択します。

c) [Dynamic Bandwidth Selection Max Channel Width] ドロップダウンリストから、DBS の最大の最適チャネル幅を選択します。

d) （任意） [チャネル通知の有効化（Notification Channel Enable）] チェックボックスをオンにして、チャネル変更通知モードを有効にします。

e) （任意） [DCAアグレッシブスタートアップ（DCA Aggr Startup）] チェックボックスをオンにして、アグレッシブ DCA アルゴリズムを有効にします。

f) [DCA Update Interval Sec] フィールドに、AP におけるチャネル割り当ての更新試行頻度を指定する間隔を秒単位で入力します。

有効な範囲は 0 ～ 4294967295 です。

g) [Optimized Roaming Data Rate Threshold (mbps)] ドロップダウンリストから、802.11 の最適化されたローミングのデータレートしきい値を選択します。

h) [DCAに干渉を含める（Include Interference in DCA）] トグルボタンを使用して、AP のチャネルを選択するときに検出された干渉を考慮するように DCA アルゴリズムを設定します。

このオプションにより、チャネル割り当てを最適化し、同一チャネル干渉を減らすことができます。

i) （任意） [チャネル通知しきい値（Notification Channel Threshold）] フィールドに、チャネル変更通知をトリガーするためのしきい値を入力します。

有効な範囲は 1 ～ 1000 です。

j) （任意） [イベント駆動型RRM（Event Driven RRM）] で [イベント駆動型RRMの有効化（Enable Event Driven RRM）] チェックボックスをオンにして、この帯域でイベント駆動型 RRM を有効にします。

このチェックボックスをオンにする場合は、次の設定を完了します。

- [感度しきい値（Sensitivity Threshold）] ドロップダウンリストから、イベント駆動型 RRM のしきい値レベルを選択します。

[カスタム（Custom）] を選択した場合は、[カスタムしきい値（Custom Threshold）] フィールドにイベント駆動型 RRM のカスタムしきい値を入力します。

有効な範囲は 1 ～ 99 です。

- （オプション）[不正コントリビューション（Rogue contribution）] チェックボックスをオンにして、この帯域でイベント駆動型 RRM 不正コントリビューションを有効にします。

  このチェックボックスをオンにする場合は、[Rogue Duty-Cycle] フィールドに、イベント駆動型 RRM 不正コントリビューションのデューティサイクルしきい値を入力します。

  有効な範囲は 1 ～ 99 です。デフォルト値は 80 です。

k) ステップ 10 （1032 ページ）から ステップ 13 （1033 ページ） まで入力して、設定をプロビジョニングします。

ステップ 7 [6 GHz] にカーソルを合わせて [TPC] を選択し、次の設定を完了します。

a) [電力割り当て方式（Power Assignment Method）] ドロップダウンリストから、電力割り当て方式を選択します。

[固定（Fixed）] を選択した場合は、[デフォルト送信電力レベル（Default Tx Power Level）] ドロップダウンリストから、データの送信に使用する電力レベルを選択します。

b) （任意） [TCPチャネル対応（TPC Channel Aware）] チェックボックスをオンにして、伝送パワーコントロール（TPC）アルゴリズムがチャネル対応であることを示します。

c) 次のフィールドにデータを入力します。

- [最大送信電力通知しきい値（Notification Max Tx Power Threshold）]：TPC アルゴリズムで各無線に割り当てられる最大しきい値を入力します。

  有効な範囲は 3 ～ 30 です。

- [最小送信電力通知しきい値（Notification Min Tx Power Threshold）]：TPC アルゴリズムで各無線に割り当てられる最小しきい値を入力します。

  有効な範囲は 3 ～ 30 です。

d) （任意） 対応する設定を有効にするには、必要なチェックボックスをオンにします。

- [システムログ送信電力（Sys Log Tx Power）]：送信電力変更のロギングモードを有効にします。
- [送信電力通知の有効化（Notification Tx Power Enable）]：送信電力変更通知モードを有効にします。

e) ステップ 10 （1032 ページ）から ステップ 13 （1033 ページ） まで入力して、設定をプロビジョニングします。

ステップ 8 [6 GHz] にカーソルを合わせて [RFグループ化（RF Grouping）] を選択し、次の設定を完了します。

a) [グループ化モード（Grouping Mode）] ドロップダウンリストから RF グループ化モードを選択します。

b) [リーダー（Leader）] グループ化モードを選択した場合は、[静的メンバー（Static Members）] で次の設定を完了します。

実行する操作	結果
静的メンバーを追加する	**1.** [Add] をクリックします。 **2.** [IPv4/IPv6アドレス（IPv4/IPv6 Address）] フィールドに、有効な IPv4 アドレスまたは IPv6 アドレスを入力します。 **3.** [コントローラ名（Controller Name）] フィールドに、静的メンバーの名前を入力します。 **4.** [Save] をクリックします。
静的メンバーを削除する	**1.** 削除する静的メンバーのチェックボックスをオンにします。 **2.** [Actions] にカーソルを合わせて [Delete] を選択します。 **3.** ダイアログボックスで、**Yes** をクリックします。

c) （任意）[RRMグループ更新間隔（秒）（RRM Group Update Interval (seconds)）] フィールドに、RRM グループ情報が更新される間隔を秒単位で入力します。

この間隔に基づいて ワイヤレスコントローラ は再計算を行い、AP グループ全体に RRM 設定を適用します。間隔を短くするとすぐに適応しますが、システムオーバーヘッドが大きくなる可能性があります。

d) ステップ 10（1032 ページ）から ステップ 13（1033 ページ）まで入力して、設定をプロビジョニングします。

ステップ 9 [6 GHz] にカーソルを合わせて [空間再利用（Spatial Reuse）] を選択し、次の設定を完了します。

a) [BSSカラー割り当てモード（BSS Color Assignment Mode）] ドロップダウンリストから、BSS カラー最適化（BCO）モードを選択します。

- [オフ（Off）]：BSS カラーは動的に選択されず、手動で設定する必要があります。
- [自動（Automatic）]：BSS カラーは、この動作を許可するすべての AP で定期的に更新されます。

（注） このモードの場合、DCA チャネル割り当てモードが「ステップ 6（1030 ページ）」で [自動（automatic）] になっている必要があります。

b) ステップ 10（1032 ページ）から ステップ 13（1033 ページ）まで入力して、設定をプロビジョニングします。

ステップ 10 [Review and Provision] をクリックします。

ステップ 11 ワイヤレスコントローラ がライセンス要件を満たしていない AP を管理している場合、Catalyst Center は詳細を示すダイアログボックスを表示します。ダイアログボックスで、必要なオプションを選択します。

オプション	説明
ライセンス マネージャ	[License Manager] ウィンドウを開いて、対応するライセンスを有効にします。 ライセンスを有効にするには、『*Cisco Catalyst Center Administrator Guide*』の「Manage Licenses」を参照してください。
[デバイスプロビジョニングに進む（Continue to device provision）]	デバイスのプロビジョニングを続行します。 （注） ライセンス要件を満たしていないAPは、ワールドワイドセーフモード（WWSM）になります。
Cancel	ダイアログボックスを閉じます。

ステップ 12 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 13 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の 5 GHz 帯域での RRM の設定

この手順を使用して、ワイヤレスコントローラ の 5 GHz 帯域で RRM パラメータを設定し、プロビジョニングします。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、[デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[グローバルワイヤレス（Global Wireless）] を展開して [RRM] をクリックします。

ステップ 4 5 GHz にカーソルを合わせ、[一般（General）] を選択して、次の設定を完了します。

a) [トラップのプロファイルしきい値（Profile Threshold for Traps）] で、次の設定を完了します。

- 次のフィールドにデータを入力します。
  - [干渉パーセンテージ（Interference Percentage）] フィールドに、干渉しきい値の割合を入力します。

    有効範囲は 0 ～ 100 です。デフォルト値は 10 です。

    干渉がこの値を超えると、トラップが生成されます。
  - [クライアント（Clients）]：トラップがトリガーされる、AP 無線ごとのクライアント数のしきい値を入力します。

    有効値は 1 ～ 200 です。デフォルト値は 12 です。
  - [ノイズ（Noise）]：ノイズのしきい値を入力します。

    有効な範囲は -127 ～ 0 です。デフォルト値は -70 です。
  - [使用率（Utilization Percentage）]：AP が使用する帯域幅のしきい値をパーセンテージで入力します。

    有効範囲は 0 ～ 100 です。デフォルト値は 80 です。
  - [スループット（Throughput (Bps)）]：802.11a スループットしきい値を入力します。

    有効な範囲は 1000 ～ 10000000 です。デフォルト値は 1,000,000 です。
- （オプション）[自動CFG（Automatic CFG）] チェックボックスをオンにして、パフォーマンスプロファイルモードを有効にします。

b) [ノイズ/干渉/不正/CleanAir/SIモニタリングチャネル（Noise/Interference/Rogue/CleanAir/SI Monitoring Channels）] セクションで、必要なオプションを選択します。

- [チャネルリスト（Channel List）]：チャネルオプションを選択します。
- [RRMネイバー検出タイプ（RRM Neighbor Discover Type）]：NDP のモードを選択します。
- [RRMネイバー検出モード（RRM Neighbor Discover Mode）]：NDP の動作モードを選択します。

c) [監視間隔（Monitor Intervals）] で、次の設定を完了します。

- 次のフィールドにデータを入力します。
  - [ネイバーパケット頻度（秒）（Neighbor Packet Frequency (sec)）]：各 AP で新しい信号強度、ノイズ、干渉測定値を受信する頻度を指定する間隔を秒単位で入力します。

    有効な範囲は 60 ～ 3600 です。デフォルト値は 180 です。

- [レポート間隔（秒）（Reporting Interval (sec)）]：各測定レポートの間隔を秒単位で入力します。

  有効な範囲は 60 ～ 3600 です。デフォルト値は 180 です。

- [ネイバータイムアウト係数（Neighbor Timeout Factor）]：ネイバーパケットを受信しなかった場合にネイバーが期限切れになるまでの時間を指定する、ネイバータイムアウト係数を入力します。

  有効な範囲は 5 ～ 60 です。デフォルト値は 20 です。

- [カバレッジ監視間隔（Monitor Coverage Interval）]：各 AP で新しいカバレッジ測定値を受信する間隔を秒単位で入力します。

  有効な範囲は 60 ～ 3600 です。

- [負荷監視間隔（Monitor Load Interval）]：各 AP で新しい負荷測定値を受信する間隔を秒単位で入力します。

  有効な範囲は 60 ～ 3600 です。

- （任意）対応する設定を有効にするには、必要なチェックボックスをオンにします。
  - [チャネル監視ステータス（Channel Monitor Status）]：ネイバーモニタリングモードを有効にします。
  - [RSSI監視正規化（Monitor RSSI Normalization）]：802.11 ネイバー探索 RSSI 正規化を有効にします。
  - [システムログ負荷（Sys Log Load）]：負荷プロファイルのロギングモードを有効にします。
  - [システムログチャネル（Sys Log Channel）]：ダイナミックチャネル変更のロギングモードを有効にします。
  - [システムログパフォーマンス（Sys Log Performance）]：パフォーマンスプロファイルのロギングモードを有効にします。
  - [システムログカバレッジ（Sys Log Coverage）]：カバレッジプロファイルのロギングモードを有効にします。
  - [システムログ外部（Sys Log Foreign）]：外部プロファイルのロギングモードを有効にします。

- [イベントノイズのログ記録（Log Noise Events）] トグルボタンを使用して、RRM システムによって検出されたノイズ関連のイベントをログに記録します。

  ノイズイベントのロギングは、ワイヤレス干渉の問題の監視と障害対応に役立ちます。

d) [UNII-3] で、[Unii3 Lpチャネル（Unii3 Lp Channels）] チェックボックスを使用して、5 GHz 帯域幅の UNII-3 低電力チャネルを有効または無効にします。

e) ステップ 10 （1040 ページ）から ステップ 13 （1041 ページ）まで入力して、設定をプロビジョニングします。

ステップ 5 [5GHz] にカーソルを合わせて、[カバレッジ（Coverage）] を選択し、次の設定を完了します。

a) [カバレッジホール検出の有効化（Enable Coverage Hole Detection）] トグルボタンを使用して、カバレッジホール検出（CHD）を有効または無効にします。

b) 次のフィールドにデータを入力します。

- [データRSSIしきい値（Data RSSI Threshold）]：ワイヤレスコントローラ で、CHD アルゴリズムがトリガーされる、データパケットの RSSI しきい値を入力します。

  有効な範囲は -90 ～ -60 です。デフォルト値は -80 です。

- [音声RSSIしきい値（Voice RSSI Threshold）]：ワイヤレスコントローラ で、CHD アルゴリズムがトリガーされる、音声パケットの RSSI しきい値を入力します。

  有効な範囲は -90 ～ -60 です。デフォルト値は -80 です。

- [APあたりの失敗クライアントの最小数（Minimum Failed Client per AP）]：CHD アルゴリズムがトリガーされる、クライアントの最小数を入力します。

  有効値は 1 ～ 200 です。デフォルト値は 3 です。

- [APあたりのカバレッジ例外レベル（Percent Coverage Exception Level per AP）]：カバレッジホールの例外がトリガーされる、AP のカバレッジ ホール リージョン内のクライアントの最小パーセンテージを入力します。

  有効な範囲は 1 ～ 100 です。デフォルト値は 25 です。

- [データパケット数（Data Packet Count）]：CHD アルゴリズムがトリガーされる、データパケット数の最小しきい値を入力します。

  有効な範囲は 1 ～ 255 です。デフォルト値は 50 です。

- [音声パケット数（Voice Packet Count）]：CHD アルゴリズムがトリガーされる、音声パケット数の最小しきい値を入力します。

  有効な範囲は 1 ～ 255 です。デフォルト値は 100 です。

- [データパケットパーセンテージ（Data Packet Percentage）]：CHD アルゴリズムがトリガーされる、ドロップされるデータパケットの割合のしきい値を入力します。

  有効な範囲は 1 ～ 100 です。デフォルト値は 50 です。

- [音声パケットパーセンテージ（Voice Packet Percentage）]：CHD アルゴリズムがトリガーされる、ドロップされる音声パケットの割合のしきい値を入力します。

  有効な範囲は 1 ～ 100 です。デフォルト値は 50 です。

c) ステップ 10 （1040 ページ） から ステップ 13 （1041 ページ） まで入力して、設定をプロビジョニングします。

ステップ 6 [5GHz] にカーソルを合わせて [DCA] を選択し、次の設定を完了します。

a) [動的チャネル割り当てアルゴリズム（Dynamic Channel Assignment Algorithm）] で、次の設定を完了します。

- ドロップダウンリストから必要なオプションを選択します。

- [チャネル割り当てモード（Channel Assignment Mode）]：モードを選択します。

  [自動（Automatic）] を選択した場合、ドロップダウンリストから必要なオプションを選択します。

  - [間隔（Interval）]：DCA の間隔を選択します。
  - [アンカー時間（Anchortime）]：DCA のアンカー時間を選択します。

- [DCAチャネル感度（DCA Channel Sensitivity）]：DCA 感度レベルを選択します。
- [チャネル幅（Channel Width）]：チャネル幅を選択します。
- [ダイナミック帯域幅選択の最大チャネル幅（Dynamic Bandwidth Selection Max Channel Width）]：DBS の最大の最適チャネル幅を選択します。

- （任意）対応する設定を有効にするには、必要なチェックボックスをオンにします。
  - [外部AP干渉の回避（Avoid Foreign AP Interference）]：ワイヤレスコントローラで干渉検出を有効にします。
  - [永続的な非Wi-Fi干渉の回避（Avoid Persistent Non-Wi-Fi Interference）]：ワイヤレスコントローラでデバイス検出を有効にします。
  - [Cisco AP負荷の回避（Avoid Cisco AP load）]：ワイヤレスコントローラで負荷検出を有効にします。
  - [ゼロ待機DFS（Zero Wait DFS）]：ゼロ待機 DFS 機能を有効にします。
  - [非5 GHzノイズの回避（Avoid Non 5 GHz Noise）]：ワイヤレスコントローラでノイズ検出を有効にします。
  - [チャネル通知の有効化（Notification Channel Enable）]：チャネル変更通知モードを有効にします。
  - [起動時のDCAアグレッシブネス（DCA Aggr Startup）]：アグレッシブ DCA アルゴリズムを有効にします。

- [DCA Min Metric RSSI] フィールドに、DCA でチャネルを変更するために必要な最小 RSSI エネルギーメトリックを入力します。

  有効な範囲は -100 ～ -60 です。

- （オプション）[DCA更新間隔（秒）（DCA Update Interval Sec）] フィールドに、AP におけるチャネル割り当ての更新試行頻度を指定する間隔を秒単位で入力します。

  有効な範囲は 0 ～ 4294967295 です。

- [Optimized Roaming Data Rate Threshold (mbps)] ドロップダウンリストから、802.11 の最適化されたローミングのデータレートしきい値を選択します。

b) [DCAに干渉を含める（Include Interference in DCA）] トグルボタンを使用して、AP のチャネルを選択するときに検出された干渉を考慮するように DCA アルゴリズムを設定します。

このオプションにより、チャネル割り当てを最適化し、同一チャネル干渉を減らすことができます。

c) （任意）[チャネル通知しきい値（Notification Channel Threshold）] フィールドに、チャネル変更通知をトリガーするためのしきい値を入力します。

有効な範囲は 1 ～ 1000 です。

d) （任意）[自動RFチャネルリスト（Auto-RF Channel List）] で、必要な RF チャネルの横にあるチェックボックスをオンにします。

e) （任意）[イベント駆動型RRM（Event Driven RRM）] で [イベント駆動型RRMの有効化（Enable Event Driven RRM）] チェックボックスをオンにして、帯域でイベント駆動型 RRM を有効にします。

イベント駆動型 RRM を有効にする場合は、次の設定を完了します。

- [感度しきい値（Sensitivity Threshold）] ドロップダウンリストから、イベント駆動型 RRM の感度レベルを選択します。

  カスタム感度しきい値を選択した場合は、[カスタムしきい値（Custom Threshold）] フィールドに、イベント駆動型 RRM のカスタムしきい値を入力します。

  有効な範囲は 1 ～ 99 です。デフォルト値は 1 です。

- （オプション）[不正コントリビューション（Rogue contribution）] チェックボックスをオンにして、帯域での不正コントリビューションを有効にします。

  不正コントリビューションを有効にする場合は、[Rogue Duty-Cycle] フィールドに、不正コントリビューションのデューティサイクルしきい値を入力します。

  有効な範囲は 1 ～ 99 です。デフォルト値は 80 です。

f) ステップ 10 （1040 ページ） から ステップ 13 （1041 ページ） まで入力して、設定をプロビジョニングします。

ステップ 7 [5GHz] にカーソルを合わせて、[TPC] を選択し、次の設定を完了します。

a) [電力割り当て方式（Power Assignment Method）] ドロップダウンリストから、電力割り当て方式を選択します。

[固定（Fixed）] を選択した場合は、[デフォルト送信出力レベル（Default Tx Power Level）] フィールドから、データの送信に使用する電力レベルを選択します。

b) 次のフィールドにデータを入力します。

- [最大送信出力レベル割り当て（dBm）（Maximum Power Level Assignment (dBm)）]：送信電力の上限を dBm 単位で入力します。

  有効な範囲は -10 ～ 30 です。デフォルト値は 30 です。

- [最小送信出力レベル割り当て（dBm）（Minimum Power Level Assignment (dBm)）]：送信電力の下限を dBm 単位で入力します。

  有効な範囲は -10 ～ 30 です。デフォルト値は -10 です。

- [パワー制御しきい値（dBm）（Power Control Threshold (dBm)）]：RRM アルゴリズムの TPC しきい値を入力します。

有効な範囲は -80 ～ -50 です。デフォルト値は -70 です。

c) （任意） [TCPチャネル対応（TPC Channel Aware）] チェックボックスをオンにして、TPC アルゴリズムがチャネル対応であることを示します。

d) 次のフィールドにデータを入力します。

- [最大送信電力通知しきい値（Notification Max Tx Power Threshold）]：TPC アルゴリズムで各無線に割り当てられる最大しきい値を入力します。

  有効な範囲は 3 ～ 30 です。

- [最小送信電力通知しきい値（Notification Min Tx Power Threshold）]：TPC アルゴリズムで各無線に割り当てられる最小しきい値を入力します。

  有効な範囲は 3 ～ 30 です。

e) （任意） 対応する設定を有効にするには、必要なチェックボックスをオンにします。

- [システムログ送信電力（Sys Log Tx Power）]：送信電力変更のロギングモードを有効にします。
- [送信電力通知の有効化（Notification Tx Power Enable）]：送信電力変更通知モードを有効にします。

f) ステップ 10（1040 ページ）から ステップ 13（1041 ページ）まで入力して、設定をプロビジョニングします。

ステップ 8 [5 GHz] にカーソルを合わせて、[RFグループ化（RF Grouping）]を選択し、次の設定を完了します。

a) [グループ化モード（Grouping Mode）] ドロップダウンリストから RF グループ化モードを選択します。

b) [リーダー（Leader）] グループ化モードを選択した場合は、[静的メンバー（Static Members）] で次の設定を完了します。

実行する操作	結果
静的メンバーを追加する	**1.** [Add] をクリックします。 **2.** [IPv4/IPv6アドレス（IPv4/IPv6 Address）] フィールドに、有効な IPv4 アドレスまたは IPv6 アドレスを入力します。 **3.** [コントローラ名（Controller Name）] フィールドに、静的メンバーの名前を入力します。 **4.** [Save] をクリックします。
静的メンバーを削除する	**1.** 削除する静的メンバーのチェックボックスをオンにします。 **2.** [Actions] にカーソルを合わせて [Delete] を選択します。 **3.** ダイアログボックスで、**Yes** をクリックします。

c) （任意）[RRMグループ更新間隔（秒）（RRM Group Update Interval (seconds)）] フィールドに、RRM グループ情報が更新される間隔を秒単位で入力します。

この間隔に基づいて ワイヤレスコントローラ は再計算を行い、AP グループ全体に RRM 設定を適用します。間隔を短くするとすぐに適応しますが、システムオーバーヘッドが大きくなる可能性があります。

d) ステップ 10（1040 ページ）から ステップ 13（1041 ページ）まで入力して、設定をプロビジョニングします。

ステップ 9 [5 GHz] にカーソルを合わせて [空間再利用（Spatial Reuse）] を選択し、次の設定を完了します。

a) [BSSカラー割り当てモード（BSS Color Assignment Mode）] ドロップダウンリストから、BSS カラー最適化モードを選択します。

- [オフ（Off）]：BSS カラーは動的に選択されず、手動で設定する必要があります。
- [自動（Automatic）]：BSS カラーは、この動作を許可するすべての AP で定期的に更新されます。

（注） このモードの場合、DCA チャネル割り当てモードが「ステップ 6（1036 ページ）」で [自動（automatic）] になっている必要があります。

b) ステップ 10（1040 ページ）から ステップ 13（1041 ページ）まで入力して、設定をプロビジョニングします。

ステップ 10 [Review and Provision] をクリックします。

ステップ 11 ワイヤレスコントローラ がライセンス要件を満たしていない AP を管理している場合、Catalyst Center は詳細を示すダイアログボックスを表示します。ダイアログボックスで、必要なオプションを選択します。

オプション	説明
ライセンス マネージャ	[License Manager] ウィンドウを開いて、対応するライセンスを有効にします。 ライセンスを有効にするには、『*Cisco Catalyst Center Administrator Guide*』の「Manage Licenses」を参照してください。
[デバイスプロビジョニングに進む（Continue to device provision）]	デバイスのプロビジョニングを続行します。 （注） ライセンス要件を満たしていない AP は、ワールドワイドセーフモード（WWSM）になります。
Cancel	ダイアログボックスを閉じます。

ステップ 12 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 13 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の 2.4 GHz 帯域での RRM の設定

この手順を使用して、ワイヤレスコントローラ の 2.4 GHz 帯域で RRM パラメータを設定し、プロビジョニングします。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、 [グローバルワイヤレス（Global Wireless）] を展開して [RRM] をクリックします。

ステップ 4 2.4 GHz にカーソルを合わせ、[一般（General）] を選択して、次の設定を完了します。

a) [トラップのプロファイルしきい値（Profile Threshold for Traps）] で、次の設定を完了します。
   - 次のフィールドにデータを入力します。
     - [干渉パーセンテージ（Interference Percentage）] フィールドに、干渉しきい値の割合を入力します。

       有効範囲は 0 ～ 100 です。デフォルト値は 10 です。

       干渉がこの値を超えると、トラップが生成されます。
     - [クライアント（Clients）] : トラップがトリガーされる、AP 無線ごとのクライアント数のしきい値を入力します。

       有効値は 1 ～ 200 です。デフォルト値は 12 です。

- [ノイズ（Noise）]：ノイズのしきい値を入力します。

  有効な範囲は -127 ～ 0 です。デフォルト値は -70 です。

- [使用率（Utilization Percentage）]：AP が使用する帯域幅のしきい値をパーセンテージで入力します。

  有効範囲は 0 ～ 100 です。デフォルト値は 80 です。

- [スループット（Throughput (Bps)）]：802.11a スループットしきい値を入力します。

  有効な範囲は 1000 ～ 10000000 です。デフォルト値は 1,000,000 です。

- （オプション）[自動CFG（Automatic CFG）] チェックボックスをオンにして、パフォーマンスプロファイルモードを有効にします。

b) [ノイズ/干渉/不正/CleanAir/SIモニタリングチャネル（Noise/Interference/Rogue/CleanAir/SI Monitoring Channels）] で、これらの設定を完了します。

- [チャンネルリスト（Channel List）] ドロップダウンリストから、チャネルオプションを選択します。
- [RRMネイバー検出タイプ（RRM Neighbor Discover Type）] ドロップダウンリストから、NDP のモードを選択します。
- [RRMネイバー検出モード（RRM Neighbor Discover Mode）] ドロップダウンリストから、NDP の動作モードを選択します。

c) [監視間隔（Monitor Intervals）] で、次の設定を完了します。

- 次のフィールドにデータを入力します。
  - [ネイバーパケット頻度（秒）（Neighbor Packet Frequency (sec)）]：各 AP で新しい信号強度、ノイズ、干渉測定値を受信する頻度を指定する間隔を秒単位で入力します。

    有効な範囲は 60 ～ 3600 です。デフォルト値は 180 です。

  - [レポート間隔（秒）（Reporting Interval (sec)）]：各測定レポートの間隔を秒単位で入力します。

    有効な範囲は 60 ～ 3600 です。デフォルト値は 180 です。

  - [ネイバータイムアウト係数（Neighbor Timeout Factor）]：ネイバーパケットを受信しなかった場合にネイバーが期限切れになるまでの時間を指定する、ネイバータイムアウト係数を入力します。

    有効な範囲は 5 ～ 60 です。デフォルト値は 20 です。

  - [カバレッジ監視間隔（Monitor Coverage Interval）]：各 AP で新しいカバレッジ測定値を受信する間隔を秒単位で入力します。

    有効な範囲は 60 ～ 3600 です。

- [負荷監視間隔（Monitor Load Interval）]：各 AP で新しい負荷測定値を受信する間隔を秒単位で入力します。

  有効な範囲は 60 ～ 3600 です。デフォルト値は 360 です。

- （任意）対応する設定を有効にするには、必要なチェックボックスをオンにします。
  - [チャネル監視ステータス（Channel Monitor Status）]：ネイバーモニタリングモードを有効にします。
  - [RSSI監視正規化（Monitor RSSI Normalization）]：802.11 ネイバー探索 RSSI 正規化を有効にします。
  - [システムログ負荷（Sys Log Load）]：負荷プロファイルのロギングモードを有効にします。
  - [システムログチャネル（Sys Log Channel）]：ダイナミックチャネル変更のロギングモードを有効にします。
  - [システムログパフォーマンス（Sys Log Performance）]：パフォーマンスプロファイルのロギングモードを有効にします。
  - [システムログカバレッジ（Sys Log Coverage）]：カバレッジプロファイルのロギングモードを有効にします。
  - [システムログ外部（Sys Log Foreign）]：外部プロファイルのロギングモードを有効にします。

- [イベントノイズのログ記録（Log Noise Events）] トグルボタンを使用して、RRM システムによって検出されたノイズ関連のイベントをログに記録します。

  ノイズイベントのロギングは、ワイヤレス干渉の問題の監視と障害対応に役立ちます。

d) ステップ 10（1048 ページ）から ステップ 13（1048 ページ）まで入力して、設定をプロビジョニングします。

ステップ 5 [2.4GHz] にカーソルを合わせて、[カバレッジ（Coverage）] を選択し、次の設定を完了します。

a) [カバレッジホール検出の有効化（Enable Coverage Hole Detection）] トグルボタンを使用して、カバレッジホール検出（CHD）を有効または無効にします。

b) 次のフィールドにデータを入力します。

- [データRSSIしきい値（Data RSSI Threshold）]：ワイヤレスコントローラ で、CHD アルゴリズムがトリガーされる、データパケットの RSSI しきい値を入力します。

  有効な範囲は -90 ～ -60 です。デフォルト値は -80 です。

- [音声RSSIしきい値（Voice RSSI Threshold）]：ワイヤレスコントローラ で、CHD アルゴリズムがトリガーされる、音声パケットの RSSI しきい値を入力します。

  有効な範囲は -90 ～ -60 です。デフォルト値は -80 です。

- [APあたりの失敗クライアントの最小数（Minimum Failed Client per AP）]：CHD アルゴリズムがトリガーされる、クライアントの最小数を入力します。

有効値は 1 ～ 200 です。デフォルト値は 3 です。

- [APあたりのカバレッジ例外レベル（Percent Coverage Exception Level per AP）]：カバレッジホールの例外がトリガーされる、AP のカバレッジ ホール リージョン内のクライアントの最小パーセンテージを入力します。

  有効な範囲は 1 ～ 100 です。デフォルト値は 25 です。

- [データパケット数（Data Packet Count）]：CHD アルゴリズムがトリガーされる、データパケット数の最小しきい値を入力します。

  有効な範囲は 1 ～ 255 です。デフォルト値は 50 です。

- [音声パケット数（Voice Packet Count）]：CHD アルゴリズムがトリガーされる、音声パケット数の最小しきい値を入力します。

  有効な範囲は 1 ～ 255 です。デフォルト値は 100 です。

- [データパケットパーセンテージ（Data Packet Percentage）]：CHD アルゴリズムがトリガーされる、ドロップされるデータパケットの割合のしきい値を入力します。

  有効な範囲は 1 ～ 100 です。デフォルト値は 50 です。

- [音声パケットパーセンテージ（Voice Packet Percentage）]：CHD アルゴリズムがトリガーされる、ドロップされる音声パケットの割合のしきい値を入力します。

  有効な範囲は 1 ～ 100 です。デフォルト値は 50 です。

c) ステップ 10（1048 ページ）から ステップ 13（1048 ページ）まで入力して、設定をプロビジョニングします。

ステップ 6 [2.4GHz] にカーソルを合わせて [DCA] を選択し、次の設定を完了します。

a) [動的チャネル割り当てアルゴリズム（Dynamic Channel Assignment Algorithm）] で、次の設定を完了します。

- ドロップダウンリストから必要なオプションを選択します。
  - [チャネル割り当てモード（Channel Assignment Mode）]：モードを選択します。

    [自動（Automatic）] を選択した場合、ドロップダウンリストから必要なオプションを選択します。
    - [間隔（Interval）]：DCA の間隔を選択します。
    - [アンカー時間（Anchortime）]：DCA のアンカー時間を選択します。
  - [DCAチャネル感度（DCA Channel Sensitivity）]：DCA 感度レベルを選択します。
  - [ダイナミック帯域幅選択の最大チャネル幅（Dynamic Bandwidth Selection Max Channel Width）]：DBS の最大の最適チャネル幅を選択します。
- （任意）対応する設定を有効にするには、必要なチェックボックスをオンにします。

- [外部AP干渉の回避（Avoid Foreign AP Interference）]：ワイヤレスコントローラで干渉検出を有効にします。
- [永続的な非Wi-Fi干渉の回避（Avoid Persistent Non-Wi-Fi Interference）]：ワイヤレスコントローラでデバイス検出を有効にします。
- [Cisco AP負荷の回避（Avoid Cisco AP load）]：ワイヤレスコントローラで負荷検出を有効にします。
- [非5 GHzノイズの回避（Avoid Non 5 GHz Noise）]：ワイヤレスコントローラでノイズ検出を有効にします。
- [チャネル通知の有効化（Notification Channel Enable）]：チャネル変更通知モードを有効にします。
- [起動時のDCAアグレッシブネス（DCA Aggr Startup）]：アグレッシブ DCA アルゴリズムを有効にします。

- [DCA Min Metric RSSI] フィールドに、DCA でチャネルを変更するために必要な最小 RSSI エネルギーメトリックを入力します。

  有効な範囲は -100 ～ -60 です。

- （オプション）[DCA更新間隔（秒）（DCA Update Interval Sec）] フィールドに、AP におけるチャネル割り当ての更新試行頻度を指定する間隔を秒単位で入力します。

  有効な範囲は 0 ～ 4294967295 です。

- [Optimized Roaming Data Rate Threshold (mbps)] ドロップダウンリストから、802.11 の最適化されたローミングのデータレートしきい値を選択します。

b) [DCAに干渉を含める（Include Interference in DCA）] トグルボタンを使用して、AP のチャネルを選択するときに検出された干渉を考慮するように DCA アルゴリズムを設定します。

このオプションにより、チャネル割り当てを最適化し、同一チャネル干渉を減らすことができます。

c) （任意）[チャネル通知しきい値（Notification Channel Threshold）] フィールドに、チャネル変更通知をトリガーするためのしきい値を入力します。

有効な範囲は 1 ～ 1000 です。

d) （任意）[自動RFチャネルリスト（Auto-RF Channel List）] で、必要な RF チャネルの横にあるチェックボックスをオンにします。

e) [イベント駆動型RRM（Event Driven RRM）] で [イベント駆動型RRMの有効化（Enable Event Driven RRM）] チェックボックスをオンにして、帯域でイベント駆動型 RRM を有効にします。

イベント駆動型 RRM を有効にする場合は、次の設定を完了します。

- [感度しきい値（Sensitivity Threshold）] ドロップダウンリストから、イベント駆動型 RRM の感度レベルを選択します。

  カスタム感度しきい値を選択した場合は、[カスタムしきい値（Custom Threshold）] フィールドに、イベント駆動型 RRM のカスタムしきい値を入力します。

有効な範囲は 1 ～ 99 です。デフォルト値は 1 です。

- （オプション）[不正コントリビューション（Rogue contribution）] チェックボックスをオンにして、帯域での不正コントリビューションを有効にします。

  不正コントリビューションを有効にする場合は、[Rogue Duty-Cycle] フィールドに、不正コントリビューションのデューティサイクルしきい値を入力します。

  有効な範囲は 1 ～ 99 です。デフォルト値は 80 です。

f) ステップ 10（1048 ページ）から ステップ 13（1048 ページ）まで入力して、設定をプロビジョニングします。

ステップ 7 [2.4GHz] にカーソルを合わせて、[TPC] を選択し、次の設定を完了します。

a) [電力割り当て方式（Power Assignment Method）] ドロップダウンリストから、電力割り当て方式を選択します。

[固定（Fixed）] を選択した場合は、[デフォルト送信電力レベル（Default Tx Power Level）] ドロップダウンリストから、データ送信用の電力レベルを選択します。

b) 次のフィールドにデータを入力します。

- [最大送信出力レベル割り当て（dBm）（Maximum Power Level Assignment (dBm)）]：送信電力の上限を dBm 単位で入力します。

  有効な範囲は -10 ～ 30 です。デフォルト値は 30 です。

- [最小送信出力レベル割り当て（dBm）（Minimum Power Level Assignment (dBm)）]：送信電力の下限を dBm 単位で入力します。

  有効な範囲は -10 ～ 30 です。デフォルト値は -10 です。

- [パワー制御しきい値（dBm）（Power Control Threshold (dBm)）]：RRM アルゴリズムの TPC しきい値を入力します。

  有効な範囲は -80 ～ -50 です。デフォルト値は -70 です。

c) （任意）[TCPチャネル対応（TPC Channel Aware）] チェックボックスをオンにして、TPC アルゴリズムがチャネル対応であることを示します。

d) [Notification Max Tx Power Threshold] フィールドに、TPC アルゴリズムで各無線に割り当てられる最大しきい値を入力します。

有効な範囲は 3 ～ 30 です。

e) [Notification Min Tx Power Threshold] フィールドに、TPC アルゴリズムで各無線に割り当てられる最小しきい値を入力します。

有効な範囲は 3 ～ 30 です。

f) （任意）送信電力変更のロギングモードを有効にするには、[システムログ送信電力（Sys Log Tx Power）] チェックボックスをオンにします。

g) （任意）送信電力変更通知モードを有効にするには、[送信電力通知の有効化（Notification Tx Power Enable）] チェックボックスをオンにします。

h) ステップ 10（1048 ページ）から ステップ 13（1048 ページ）まで入力して、設定をプロビジョニングします。

ステップ 8 [2.4GHz] にカーソルを合わせて、[RFグループ化（RF Grouping）]を選択し、次の設定を完了します。

a) [グループ化モード（Grouping Mode）] ドロップダウンリストから RF グループ化モードを選択します。

b) [リーダー（Leader）] グループ化モードを選択した場合は、[静的メンバー（Static Members）] で次の設定を完了します。

実行する操作	結果
静的メンバーを追加する	**1.** [Add] をクリックします。 **2.** [IPv4/IPv6アドレス（IPv4/IPv6 Address）] フィールドに、有効な IPv4 アドレスまたは IPv6 アドレスを入力します。 **3.** [コントローラ名（Controller Name）] フィールドに、静的メンバーの名前を入力します。 **4.** [Save] をクリックします。
静的メンバーを削除する	**1.** 削除する静的メンバーのチェックボックスをオンにします。 **2.** [Actions] にカーソルを合わせて [Delete] を選択します。 **3.** ダイアログボックスで、**Yes** をクリックします。

c) （任意）[RRMグループ更新間隔（秒）（RRM Group Update Interval (seconds)）] フィールドに、RRM グループ情報が更新される間隔を秒単位で入力します。

この間隔に基づいて ワイヤレスコントローラ は再計算を行い、AP グループ全体に RRM 設定を適用します。間隔を短くするとすぐに適応しますが、システムオーバーヘッドが大きくなる可能性があります。

d) ステップ 10（1048 ページ）から ステップ 13（1048 ページ）まで入力して、設定をプロビジョニングします。

ステップ 9 [2.4 GHz] にカーソルを合わせて [空間再利用（Spatial Reuse）] を選択し、次の設定を完了します。

a) [BSSカラー割り当てモード（BSS Color Assignment Mode）] ドロップダウンリストから、BSS カラー最適化モードを選択します。

- [オフ（Off）]：BSS カラーは動的に選択されず、手動で設定する必要があります。
- [自動（Automatic）]：BSS カラーは、この動作を許可するすべての AP で定期的に更新されます。

（注） このモードの場合、DCA チャネル割り当てモードが「ステップ 6（1044 ページ）」で [自動（automatic）] になっている必要があります。

b) ステップ 10（1048 ページ）から ステップ 13（1048 ページ）まで入力して、設定をプロビジョニングします。

ステップ 10 [Review and Provision] をクリックします。

ステップ 11 ワイヤレスコントローラ がライセンス要件を満たしていない AP を管理している場合、Catalyst Center は詳細を示すダイアログボックスを表示します。ダイアログボックスで、必要なオプションを選択します。

オプション	説明
ライセンス マネージャ	[License Manager] ウィンドウを開いて、対応するライセンスを有効にします。 ライセンスを有効にするには、『*Cisco Catalyst Center Administrator Guide*』の「Manage Licenses」を参照してください。
[デバイスプロビジョニングに進む（Continue to device provision）]	デバイスのプロビジョニングを続行します。 （注） ライセンス要件を満たしていない AP は、ワールドワイドセーフモード（WWSM）になります。
Cancel	ダイアログボックスを閉じます。

ステップ 12 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する（238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 13 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の RRM FRA パラメータの設定

この手順を使用して、ワイヤレスコントローラ の RRM FRA パラメータを設定し、構成をプロビジョニングします。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[グローバルワイヤレス（Global Wireless）] を展開して [RRM] をクリックします。

ステップ 4 [FRA] タブをクリックします。

ステップ 5 [5/6GHzフレキシブル ラジオ アサインメント（5/6 GHz Flexible Radio Assignment）] で、次の設定を完了します。

a) [FRAステータス（FRA Status）] トグルボタンを使用して、5/6 GHz デュアルバンド（XOR）モデルのすべての AP でフレキシブル ラジオ アサインメント（FRA）を有効または無効にします。
b) （任意） [FRA凍結（FRA Freeze）]チェックボックスをオンにして、5/6 GHz デュアルバンド（XOR）モデルのすべての AP で FRA 凍結を有効にします。
c) [FRA間隔（FRA Interval）] ドロップダウンリストから、5/6 GHz デュアルバンド（XOR）モデルの FRA 間隔を選択します。

ステップ 6 [2.4/5GHzフレキシブルラジオアサインメント（2.4/5 GHz Flexible Radio Assignment）] で、次の設定を完了します。

a) [FRAステータス（FRA Status）] トグルボタンを使用して、すべての AP で FRA を有効または無効にします。
b) （任意） [FRA凍結（FRA Freeze）] チェックボックスをオンにして、すべての AP で FRA 凍結を有効にします。
c) [FRA Interval] ドロップダウンリストで、[FRA interval] を選択します。
d) [FRA Sensitivity] ドロップダウンリストから、FRA カバレッジオーバーラップ感度を選択します。
e) （任意） [クライアント対応（Client Aware）] チェックボックスをオンにして、デュアルバンドが 5 GHz 帯域の負荷に基づいて 5 GHz またはモニターモードで動作できるようにします。
f) [FRAアクション（FRA Action）] ドロップダウンリストから、デュアルバンド無線の FRA アクションを選択します。
g) [Client Select Threshold] フィールドに、デュアルバンド無線をモニターモードからクライアントサービスモードに移行するための FRA 使用率のしきい値を入力します。

有効範囲は 0 ～ 100 です。

（注） クライアント選択しきい値は、クライアントリセットしきい値より大きくする必要があります。

h) [Client Reset Threshold] フィールドに、デュアルバンド無線をクライアントサービスモードからモニターモードに移行するための FRA 使用率のしきい値を入力します。

有効範囲は 0 ～ 100 です。

（注） クライアントのリセットしきい値は、クライアント選択のしきい値より小さくする必要があります。

i) ドロップダウンリストから、[FRAセンサーのしきい値（FRA Sensor Threshold）] を選択します。

j) ドロップダウンリストから、[FRAサービスの優先順位（FRA Service Priority）] を選択します。

ステップ 7 [Review and Provision] をクリックします。

ステップ 8 ワイヤレスコントローラ がライセンス要件を満たしていない AP を管理している場合、Catalyst Center は詳細を示すダイアログボックスを表示します。ダイアログボックスで、必要なオプションを選択します。

オプション	説明
ライセンス マネージャ	[License Manager] ウィンドウを開いて、対応するライセンスを有効にします。 ライセンスを有効にするには、『*Cisco Catalyst Center Administrator Guide*』の「Manage Licenses」を参照してください。
[デバイスプロビジョニングに進む（Continue to device provision）]	デバイスのプロビジョニングを続行します。 （注） ライセンス要件を満たしていない AP は、ワールドワイドセーフモード（WWSM）になります。
Cancel	ダイアログボックスを閉じます。

ステップ 9 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 10 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のグローバル ワイヤレス パラメータの設定

次の手順を使用して、ワイヤレスコントローラのグローバルワイヤレスパラメータを設定し、構成をプロビジョニングします。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[グローバルワイヤレス（Global Wireless）] を展開し、[詳細設定（Advanced）] をクリックします。

ステップ 4 [グローバル（Global）] タブの次のフィールドにデータを入力します。

- [RFグループ名（RF Group Name）]：RF グループの名前を入力します。
- [ユーザーあたりの最大ログイン数（Maximum Login Sessions Per User）]：単一ユーザーに許可される同時ログインの最大数を入力します。

  有効な範囲は 0 ～ 8 です。

ステップ 5 対応する設定を有効にするには、必要なチェックボックスをオンにします。

- [ワイヤレスパスワードポリシー（Wireless Password Policy）]：AP 参加プロファイル（管理ユーザーパスワード）およびフレックスプロファイル（ローカル認証ユーザーパスワード）のワイヤレスパスワードポリシーを有効にします。
- [ワイヤレスによる管理（Management via Wireless）]：ワイヤレスクライアントからの管理アクセスを有効にします。
- [AP LAGモード（AP Lag Mode）]：グローバル LAG を有効にします。
- [Dot15無線（Dot15 Radio）]：グローバル 802.15 無線スイッチを有効にします。
- [デバイス分類子（Device Classifier）]：接続されているデバイスの分類を有効にします。

ステップ 6 [アシステッドローミング（Assisted Roaming）] で、次のフィールドにデータを入力します。

- [最大拒否回数（Denial Maximum）]：アソシエーション拒否の最大回数を入力します。

  有効な範囲は 1 ～ 10 です。

- [フロアバイアス（dBm）（Floor Bias（dBm）]：同じフロアにある AP の RSSI バイアスのデフォルト値を dBm 単位で入力します。

  有効な範囲は 5 ～ 25 です。

- [予測の最小数（Prediction Minimum）]：経由ローミング予測が機能するために最適化された AP の最小数を入力します。

  有効な範囲は 2 ～ 6 です。

- [XORから専用モードへのRSSIしきい値（RSSI Threshold for XOR to Dedicated Mode）]：AP がデュアルバンド（XOR）モードから専用モードに切り替わる最小 RSSI 値を dBm 単位で入力します。

  有効な範囲は -128 ～ 0 です。値を小さくすると、AP モード移行が微弱な信号の影響を受けにくくなります。

ステップ 7 （任意） [APイメージのアップグレード（AP Image Upgrade）] で、次の設定を完了します。

- [HTTPSメソッド（HTTPS Method）] トグルボタンを使用して、HTTPS を有効または無効にします。
- [HTTPSポート（HTTPS Port）] フィールドに、HTTPS ファイル転送用のカスタムポート番号を入力します。

  有効な範囲は 0 ～ 65535 です。

ステップ 8 （任意） [AP地理位置情報（AP Geolocation）] で、[測距を使用した地理位置情報の導出（Geolocation Derivation Using Ranging）] トグルボタンを使用して、AP のロケーションの精度を向上させるために、測距を使用した地理位置情報の導出を有効または無効にします。

ステップ 9 （任意） [クライアントイベントとロギング（Client Events & Logging）] で、次のトグルボタンを使用して、対応する設定を有効または無効にします。

- [クライアントオンボーディングイベントの有効化（Enable Client Onboarding Event）]：新しいクライアントデバイスがワイヤレスネットワークに参加したときのイベントの生成を有効または無効にします。
- [詳細なクライアントSyslogを有効化（Enable Detailed Client Syslog）]：クライアントイベントの詳細な Syslog メッセージを有効または無効にします。

ステップ 10 （任意） [プローブ要求管理（Probe Request Management）] で、次の設定を完了します。

- [プローブ要求制限（Probe Request Limit）]：アクション実行前に、クライアントから許可されるプローブ要求の最大数を入力します。

  有効な範囲は 1 ～ 100 です。

- [プローブ要求間隔（ms）（Probe Request Interval (ms)）]：同じクライアントからのプローブ要求間の最小間隔をミリ秒単位で入力します。

有効な範囲は 100 ～ 64000 です。

- [プローブ要求フィルタリングの有効化（Enable Probe Request Filtering）]：クライアントからのプローブ要求のフィルタリングを有効または無効にします。

  フィルタリングを有効にすると、ワイヤレスコントローラ は不要なプローブ要求をフィルタ処理してパフォーマンスを向上し、干渉を減らします。

ステップ 11 （任意）[Web認証（Web Authentication）] で、[Web認証の最大試行回数（Web Authentication Max Retries）] フィールドに、失敗後にクライアントが Web 認証を再試行できる最大回数を入力します。

有効な範囲は 0 ～ 20 です。

ステップ 12 （任意）[XORローミングとロードバランシング（XOR Roaming & Load Balancing）] で、必要な設定を完了します。

- [XOR RSSIしきい値専用（dBm）（Dedicated to XOR RSSI Threshold (dBm)）]：専用デュアルバン（XOR）操作の RSSI しきい値を dBm 単位で入力します。

  有効な範囲は -128 ～ 0 です。

- [XORローミングの最小クライアント数（Minimum Clients for XOR Roaming）]：XOR ローミング機能をアクティブ化する前に必要なクライアントの最小数を入力します。

  有効値は 0 ～ 200 です。

- [ロードバランシング ウィンドウ（Load Balancing Window）]： ロード バランシング計算に使用される時間を秒単位で入力します。

  有効値は 0 ～ 200 です。

- [XORローミングプローブ抑制モード（XOR Roam Probe Suppression Mode）]：XOR ローミング中のプローブ抑制の動作モードを選択します。

- [プローブ抑制の積極性（Probe Suppression Aggressiveness）]：XOR ローミング中のプローブ抑制の積極性レベルを示す数値を入力します。

  有効範囲は 0 ～ 255 です。値が大きいほど抑制が強化され、プローブトラフィックが減少します。

ステップ 13 （任意）[アクセスポイントの機能（Access Point Features）] で、次の設定を完了します。

- [LEDの明るさレベル（LED Brightness Level）]：AP LED の明るさレベルを示す数値を入力します。

  有効な範囲は 1 ～ 8 です。数字が大きいほど明るさが増します。

- [ローカル管理 MAC アドレスの使用（Use Locally Administered MAC Address）]：AP のローカルに管理された MAC アドレスの使用を有効または無効にします。

  ネットワークポリシーまたはプライバシーのデフォルトのハードウェア MAC アドレスを上書きするには、このオプションを有効にします。

ステップ 14 （任意）[AP監査およびVLAN（AP Audit & VLAN）] で、次の設定を完了します。

- [AP監査レポートの有効化（Enable AP Audit Report）]： AP からの定期的な監査レポートを有効または無効にします。
- [AP監査レポート間隔（秒）（AP Audit Report Interval (seconds)）]：AP が監査レポートを ワイヤレスコントローラに送信する頻度を示す時間を秒単位で入力します。

  有効な範囲は 10 ～ 43200 です。
- [永続的VLAN割り当て（Persistent VLAN Assignment）]：クライアントの永続的 VLAN 割り当てを有効または無効にします。

  有効にすると、クライアントは再関連付けしても VLAN 割り当てを保持します。

ステップ 15 （任意）[セキュアネットワーク（Secure Network）] で、次の設定を完了します。

- [セキュアネットワーク名（Secure Network Name）]：AP 認証または暗号化に使用するセキュアネットワークの一意の名前を入力します。

  名前には最大 64 文字を使用できます。
- [セキュアネットワーク名暗号化タイプ（Secure Network Name Encryption Type）]：セキュアネットワーク名を保存または送信する暗号化タイプを選択します。

（注） クリアテキスト暗号化タイプの場合、セキュアネットワーク名には最大19文字を使用できます。AES暗号化タイプの場合、セキュアネットワーク名は 12 ～ 64 文字をを使用する必要があります。

ステップ 16 [Review and Provision] をクリックします。

ステップ 17 ワイヤレスコントローラ がライセンス要件を満たしていない AP を管理している場合、Catalyst Center は詳細を示すダイアログボックスを表示します。ダイアログボックスで、必要なオプションを選択します。

オプション	説明
ライセンス マネージャ	[License Manager] ウィンドウを開いて、対応するライセンスを有効にします。 ライセンスを有効にするには、『*Cisco Catalyst Center Administrator Guide*』の「Manage Licenses」を参照してください。
[デバイスプロビジョニングに進む（Continue to device provision）]	デバイスのプロビジョニングを続行します。 （注） ライセンス要件を満たしていない AP は、ワールドワイドセーフモード（WWSM）になります。
Cancel	ダイアログボックスを閉じます。

ステップ 18 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 19 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のロードバランシングの設定

次の手順を使用して、ワイヤレスコントローラ の 5 GHz および 2.4 GHz 帯域のロードバランシング パラメータを設定し、設定をプロビジョニングします。

6 GHz 帯域の場合、[Aggressive Load Balancing Window] や [Aggressive Load Balancing Denial Count] などのグローバルパラメータは、RF プロファイルで設定します。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラのリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[グローバルワイヤレス（Global Wireless）] を展開し、[詳細設定（Advanced）] をクリックします。

ステップ 4 [Load Balancing] タブをクリックします。

ステップ 5 [5 GHz] および [2.4 GHz] にある、次のフィールドにデータを入力します。

- [アグレッシブロードバランシングウィンドウ（クライアント数）（Aggressive Load Balancing Window（clients）] : アグレッシブ ロード バランシング ウィンドウのクライアント数を入力します。

  有効な範囲は 0 ～ 20 です。

- [アグレッシブロードバランシング拒否カウント（Aggressive Load Balancing Denial Count）] : アグレッシブ ロード バランシング ウィンドウの拒否カウントを入力します。

  有効な範囲は 1 ～ 10 です。

ステップ 6 [Review and Provision] をクリックします。

ステップ 7 ワイヤレスコントローラ がライセンス要件を満たしていない AP を管理している場合、Catalyst Center は詳細を示すダイアログボックスを表示します。ダイアログボックスで、必要なオプションを選択します。

オプション	説明
ライセンス マネージャ	[License Manager] ウィンドウを開いて、対応するライセンスを有効にします。 ライセンスを有効にするには、『*Cisco Catalyst Center Administrator Guide*』の「Manage Licenses」を参照してください。
[デバイスプロビジョニングに進む（Continue to device provision）]	デバイスのプロビジョニングを続行します。 （注） ライセンス要件を満たしていない AP は、ワールドワイドセーフモード（WWSM）になります。
Cancel	ダイアログボックスを閉じます。

ステップ 8 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

ステップ 9 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の帯域選択の設定

この手順を使用して、WLAN ごとに ワイヤレスコントローラ のバンド選択パラメータを設定し、設定をプロビジョニングします。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、[デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[グローバルワイヤレス（Global Wireless）] を展開し、[詳細設定（Advanced）] をクリックします。

ステップ 4 [Band Select] タブをクリックします。

ステップ 5 （任意） 次のフィールドにデータを入力します。

- [サイクル数（Cycle Count）]：クライアントの抑制サイクルの最大回数を入力します。

  有効な範囲は 1 ～ 10 です。

- [サイクルしきい値（ミリ秒）（Cycle Threshold (msec)）]：バンド選択のサイクルしきい値を入力します。

  有効な範囲は 1 ～ 1000 です。

- [抑制エージアウト（秒）Age Out Suppression (sec)）]：抑制の有効期限を秒単位で入力します。

  有効な範囲は 10 ～ 200 です。

- [デュアルバンドエージアウト（秒）Age Out Dual Band (sec)）]：デュアルバンドの有効期限を入力します。

  有効な範囲は 10 ～ 300 です。

- [クライアントRSSI（dBm）（Client RSSI (dBm)）]：モバイルステーション RSSI しきい値の最小値を入力します。

  有効な範囲は -90 ～ -20 です。

- [クライアント中間RSSI（dBm）（Client Mid RSSI (dBm)）]：中規模モバイルステーションの RSSI しきい値を入力します。

  有効な範囲は -90 ～ -20 です。

ステップ 6 [Review and Provision] をクリックします。

ステップ 7 ワイヤレスコントローラ がライセンス要件を満たしていない AP を管理している場合、Catalyst Center は詳細を示すダイアログボックスを表示します。ダイアログボックスで、必要なオプションを選択します。

オプション	説明
ライセンス マネージャ	[License Manager] ウィンドウを開いて、対応するライセンスを有効にします。 ライセンスを有効にするには、『*Cisco Catalyst Center Administrator Guide*』の「Manage Licenses」を参照してください。

オプション	説明
[デバイスプロビジョニングに進む（Continue to device provision）]	デバイスのプロビジョニングを続行します。 （注） ライセンス要件を満たしていない AP は、ワールドワイドセーフモード（WWSM）になります。
Cancel	ダイアログボックスを閉じます。

ステップ 8 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

ステップ 9 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の最適化されたローミングの設定

次の手順を使用して、ワイヤレスコントローラ の最適化されたローミングパラメータを設定し、構成をプロビジョニングします。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、[デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[グローバルワイヤレス（Global Wireless）] を展開し、[詳細設定（Advanced）] をクリックします。

ステップ 4 [Optimized Roaming] タブをクリックします。

ステップ 5 [6 Ghz]、[5 Ghz]、および [2.4 Ghz] で、次の設定を完了します。

a) 対応する帯域で最適化されたローミングを有効または無効にするには、[最適化されたローミングモード（Optimized Roaming Mode）] トグルボタンを使用します。

b) [Optimized Roaming Data Rate Threshold (mbps)] ドロップダウンリストから、802.11 の最適化されたローミングのデータレートしきい値を選択します。

このしきい値は、クライアントが接続を維持するために必要な最小データレートを設定し、クライアントがより良いカバレッジエリアに移動できるようにします。

（注） データレートしきい値の設定を誤ると、クライアント接続に問題が発生することがあります。この機能を有効にした後で、意図せずにクライアントが切断される問題が発生する場合は、データレートしきい値を下げるか、無効にしてください。

c) [最適化ローミングヒステリシス（Optimized Roaming Hysteresis）] フィールドに、クライアントローミングに必要な信号強度マージンを入力します。

有効な範囲は 0 ～ 10 です。

ステップ 6 [Review and Provision] をクリックします。

ステップ 7 ワイヤレスコントローラ がライセンス要件を満たしていない AP を管理している場合、Catalyst Center は詳細を示すダイアログボックスを表示します。ダイアログボックスで、必要なオプションを選択します。

オプション	説明
ライセンス マネージャ	[License Manager] ウィンドウを開いて、対応するライセンスを有効にします。 ライセンスを有効にするには、『*Cisco Catalyst Center Administrator Guide*』の「Manage Licenses」を参照してください。
[デバイスプロビジョニングに進む（Continue to device provision）]	デバイスのプロビジョニングを続行します。 （注） ライセンス要件を満たしていない AP は、ワールドワイドセーフモード（WWSM）になります。
Cancel	ダイアログボックスを閉じます。

ステップ 8 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

ステップ 9 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の高密度パラメータの設定

この手順を使用して、ワイヤレスコントローラ の 5 GHz および 2.4 GHz 帯域の高密度パラメータを設定し、構成をプロビジョニングします。

6 GHz 帯域の場合、Rx SOP しきい値やマルチキャストデータレートなどのグローバル高密度パラメータは、RF プロファイルで設定します。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[グローバルワイヤレス（Global Wireless）] を展開し、[詳細設定（Advanced）] をクリックします。

ステップ 4 [High Density] タブをクリックします

ステップ 5 [Rx SOP しきい値（Rx SOP Threshold）] で、ドロップダウンリストから必要なオプションを選択します。

- [5 GHz（dBm）] : 5 GHz 帯域のしきい値を選択します。

  [カスタム（Custom）] を選択した場合、[カスタム5 GHz（dBm）（Custom 5 GHz (dBm)）] フィールドに、Rx SOP しきい値のカスタム値を dBm 単位で入力します。

  有効な範囲は -85 ～ -60 です。デフォルト値は -85 です。

- [2.4 GHz（dBm）] : 2.4 GHz 帯域のしきい値を選択します。

  [カスタム（Custom）] を選択する場合、[カスタム2.4 GHz（dBm）（Custom 2.4 GHz (dBm)）] フィールドに、Rx SOP しきい値のカスタム値を dBm 単位で入力します。

  有効な範囲は -85 ～ -60 です。デフォルト値は -85 です。

ステップ 6 [マルチキャストデータレート（Multicast Data Rate）] で、ドロップダウンリストから必要なオプションを選択します。

- [5 GHz（dBm）] : 5 GHz 帯域の AP に関連付けられるマルチキャストクライアントの最小データレートを選択します。

- [2.4 GHz（dBm）]：2.4 GHz 帯域の AP に関連付けられるマルチキャストクライアントの最小データレートを選択します。

ステップ 7 [Review and Provision] をクリックします。

ステップ 8 ワイヤレスコントローラ がライセンス要件を満たしていない AP を管理している場合、Catalyst Center は詳細を示すダイアログボックスを表示します。ダイアログボックスで、必要なオプションを選択します。

オプション	説明
ライセンス マネージャ	[License Manager] ウィンドウを開いて、対応するライセンスを有効にします。 ライセンスを有効にするには、『*Cisco Catalyst Center Administrator Guide*』の「Manage Licenses」を参照してください。
[デバイスプロビジョニングに進む（Continue to device provision）]	デバイスのプロビジョニングを続行します。 （注） ライセンス要件を満たしていない AP は、ワールドワイドセーフモード（WWSM）になります。
Cancel	ダイアログボックスを閉じます。

ステップ 9 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 10 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の優先コールの追加

次の手順を使用して、ワイヤレスコントローラ の優先コールを追加し、プロビジョニングします。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。

c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[グローバルワイヤレス（Global Wireless）] を展開し、[詳細設定（Advanced）] をクリックします。

ステップ 4 [Preferred Calls] タブをクリックします。

ステップ 5 [Add] をクリックします。

ステップ 6 [優先コールの作成（Create Preferred Calls）] スライドインペイン の [コールインデックス（Call Index）] フィールド に、コールの SIP インデックスを入力します。

有効な範囲は 1 ～ 6 です。

ステップ 7 [コール番号（Call Number）] フィールドに、SIP 優先コール番号を入力します。

SIP 優先コール番号には最大 28 文字を使用できます。Catalyst Center では、コール番号に ? とスペースは使用できません。

ステップ 8 [Review and Provision] をクリックします。

ステップ 9 ワイヤレスコントローラ がライセンス要件を満たしていない AP を管理している場合、Catalyst Center は詳細を示すダイアログボックスを表示します。ダイアログボックスで、必要なオプションを選択します。

オプション	説明
ライセンス マネージャ	[License Manager] ウィンドウを開いて、対応するライセンスを有効にします。 ライセンスを有効にするには、『*Cisco Catalyst Center Administrator Guide*』の「Manage Licenses」を参照してください。
[デバイスプロビジョニングに進む（Continue to device provision）]	デバイスのプロビジョニングを続行します。 （注） ライセンス要件を満たしていない AP は、ワールドワイドセーフモード（WWSM）になります。
Cancel	ダイアログボックスを閉じます。

ステップ 10 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。

- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 11 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の RFID の設定

ワイヤレスコントローラ の電波による固体識別（RFID）パラメータを設定し、その設定をプロビジョニングするには、次の手順を実行します。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[グローバルワイヤレス（Global Wireless）] を展開し、[詳細設定（Advanced）] をクリックします。

ステップ 4 [RFID] タブをクリックします。

ステップ 5 [RFIDの状態（RFID State）] トグルボタンを使用して、RFID タグトラッキングを有効または無効にします。

ステップ 6 [RFID Timeout (sec)] フィールドに、古い RFID エントリをクリーンアップするタイムアウト値を秒単位で入力します。

有効な範囲は 60 ～ 7200 です。

ステップ 7 [Review and Provision] をクリックします。

ステップ 8 ワイヤレスコントローラ がライセンス要件を満たしていない AP を管理している場合、Catalyst Center は詳細を示すダイアログボックスを表示します。ダイアログボックスで、必要なオプションを選択します。

オプション	説明
ライセンス マネージャ	[License Manager] ウィンドウを開いて、対応するライセンスを有効にします。 ライセンスを有効にするには、『*Cisco Catalyst Center Administrator Guide*』の「Manage Licenses」を参照してください。

オプション	説明
[デバイスプロビジョニングに進む（Continue to device provision）]	デバイスのプロビジョニングを続行します。 （注） ライセンス要件を満たしていないAPは、ワールドワイドセーフモード（WWSM）になります。
Cancel	ダイアログボックスを閉じます。

ステップ 9 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 10 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のセルラーステアリングの設定

次の手順を使用して、ワイヤレスコントローラのセルラーステアリングパラメータを設定し、設定をプロビジョニングします。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラのリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、[デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[グローバルワイヤレス（Global Wireless）] を展開し、[詳細設定（Advanced）] をクリックします。

ステップ 4 [Cellular Steering] タブをクリックします。

ステップ 5 RSSI しきい値を dBm 単位で入力して、次の Wi-Fi からセルラーへのステアリングをトリガーします。

- 6 GHz 帯
- 5 GHz 帯
- 2.4 GHz 帯

有効な範囲は -90 ～ -80 dBm です。

ステップ 6 [Review and Provision] をクリックします。

ステップ 7 ワイヤレスコントローラ がライセンス要件を満たしていない AP を管理している場合、Catalyst Center は詳細を示すダイアログボックスを表示します。ダイアログボックスで、必要なオプションを選択します。

オプション	説明
ライセンス マネージャ	[License Manager] ウィンドウを開いて、対応するライセンスを有効にします。 ライセンスを有効にするには、『*Cisco Catalyst Center Administrator Guide*』の「Manage Licenses」を参照してください。
[デバイスプロビジョニングに進む（Continue to device provision）]	デバイスのプロビジョニングを続行します。 （注） ライセンス要件を満たしていない AP は、ワールドワイドセーフモード（WWSM）になります。
Cancel	ダイアログボックスを閉じます。

ステップ 8 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

ステップ 9 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの 6 GHz クライアントステアリングの設定

ワイヤレスコントローラ の WLAN ごとに 6-GHz クライアントステアリングのパラメータを設定し、その設定をプロビジョニングするには、次の手順を実行します。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、[デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[グローバルワイヤレス（Global Wireless）] を展開し、[詳細設定（Advanced）] をクリックします。

ステップ 4 [6 GHz Client Steering] タブをクリックします。

ステップ 5 （任意） 次のフィールドにデータを入力します。

- [6 GHz移行の最小クライアント数（6 GHz Transition Minimum Client Count）]：6-GHz クライアントステアリングの最小クライアント数を入力します。

  有効値は 0 ～ 200 です。

- [6 GHz移行の最小ウィンドウサイズ（6 GHz Transition Minimum Window Size）]：クライアントステアリングの最小ウィンドウサイズを設定する値を入力します。

  有効値は 0 ～ 200 です。

- [6 GHz移行の最大使用率の差（%）（6 GHz Transition Max Utilization Difference (%)）]：クライアントを誘導するための最大チャネル使用率の差を設定する値をパーセンテージで入力します。

  有効範囲は 0 ～ 100 です。

- [6 GHz移行の最小2.4 GHz RSSIしきい値（dBm）（6 GHz Transition Min 2.4 GHz RSSI Threshold (dBm)）]：クライアントを誘導するための最小受信 2.4-GHz RSSI しきい値を入力します。

  有効な範囲は -70 ～ -20 です。

- [6 GHz移行の最小5 GHz RSSIしきい値（dBm）（6 GHz Transition Min 5 GHz RSSI Threshold (dBm)）]：クライアントを誘導するための最小受信 5-GHz RSSI しきい値を入力します。

  有効な範囲は -75 ～ -20 です。

ステップ 6 [Review and Provision] をクリックします。

ステップ 7 ワイヤレスコントローラ がライセンス要件を満たしていない AP を管理している場合、Catalyst Center は詳細を示すダイアログボックスを表示します。ダイアログボックスで、必要なオプションを選択します。

オプション	説明
ライセンス マネージャ	[License Manager] ウィンドウを開いて、対応するライセンスを有効にします。 ライセンスを有効にするには、『*Cisco Catalyst Center Administrator Guide*』の「Manage Licenses」を参照してください。
[デバイスプロビジョニングに進む（Continue to device provision）]	デバイスのプロビジョニングを続行します。 （注） ライセンス要件を満たしていない AP は、ワールドワイドセーフモード（WWSM）になります。
Cancel	ダイアログボックスを閉じます。

ステップ 8 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

ステップ 9 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の mDNS の設定

ワイヤレスコントローラ のマルチキャスト ドメイン ネーム システム（mDNS）ゲートウェイを設定してプロビジョニングするには、次の手順を実行します。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、[デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[グローバルワイヤレス（Global Wireless）] を展開して [mDNS] をクリックします。

ステップ 4 [Global] タブで [mDNS Gateway] トグルボタンを使用して、mDNS ゲートウェイを有効または無効にします。

ステップ 5 mDNS ゲートウェイを有効にする場合は、次の設定を完了します。

- [トランスポート（Transport）] ドロップダウンリストから、mDNS メッセージ処理のトランスポート方式を選択します。
- [Active-Query Timer (Minutes)] フィールドに、分単位で時間を入力します。

  有効な範囲は 1 ～ 120 です。デフォルト値は 30 です。
- （任意）[mDNS-AP Service Policy] ドロップダウンリストから、mDNS サービスポリシーを選択します。

  mDNS サービスポリシーの作成については、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の mDNS サービスポリシーの作成 （1072 ページ）を参照してください。

ステップ 6 [Review and Provision] をクリックします。

ステップ 7 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

ステップ 8 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の mDNS サービス定義の作成

この手順を使用して、ワイヤレスコントローラ の mDNS サービス定義を作成し、プロビジョニングします。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、[デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[グローバルワイヤレス（Global Wireless）] 展開して [mDNS] をクリックします。

ステップ 4 [サービスポリシー（Service Policy）] にカーソルを合わせ [サービス定義（Service Definition）] を選択します。

ステップ 5 [Add] をクリックします。

ステップ 6 [サービス定義の作成（Create Service Definition）]スライドインペインの [サービス定義名（Service Definition Name ）] フィールドに、サービス定義の名前を入力します。

サービスの定義には最大 164 文字を使用できます。先頭は英数字にする必要があります。

ステップ 7 （任意） [Description] フィールドに、説明を入力します

説明には最大 164 文字を使用できます。

ステップ 8 [サービスタイプ（Service Types）] で、サービスタイプを設定します。

実行する操作	結果
サービスタイプの追加	**1.** [Add] をクリックします。 **2.** [Add Service Type] ダイアログボックスの [Service Type] フィールドに、サービスタイプの文字列を入力します。最大 164 文字を入力できます。 Catalyst Center では、サービスタイプに特殊文字 ?、<、>、& は使用できません。 **3.** [Save] をクリックします。
サービスタイプの削除	**1.** 削除するサービスタイプの横にあるチェックボックスをオンにします。 **2.** [Actions] にカーソルを合わせて [Delete] を選択します。 **3.** ダイアログボックスで、**Yes** をクリックします。

ステップ 9 [Review and Provision] をクリックします。

ステップ 10 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 11 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の mDNS サービスリストの作成

入力方向と出力方向の mDNS サービスリストを作成できます。次の手順を使用して、ワイヤレスコントローラ の mDNS サービスリストを作成してプロビジョニングします。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[グローバルワイヤレス（Global Wireless）] 展開して [mDNS] をクリックします。

ステップ 4 [サービスポリシー（Service Policy）] にカーソルを合わせ、[サービスリスト（Service List）] を選択します。

ステップ 5 [追加（Add）] にカーソルを合わせて、方向のいずれかを選択します。

- [方向 - イン（Direction - IN）]：入力方向のサービスリストを作成します。
- [方向 - アウト（Direction - OUT）]：出力方向のサービスリストを作成します。

ステップ 6 [サービスリストの作成（Create Service List）] スライドインペイン の [サービスリスト名（Service List Name）] フィールドに、サービスリストの名前を入力します。

名前には最大 164 文字を使用できます。

IN 方向の場合、Catalyst Center では default-mdns-in-service-list 名は使用できません。**OUT** 方向の場合、Catalyst Center では default-mdns-out-service-list 名は使用できません。

ステップ 7 （任意） すべてのサービスをサービスリストに割り当てるには、[すべてのサービスの割り当て（Assign All Services）] トグルボタンをクリックします。

選択内容	結果
方向 - イン	[メッセージタイプ（Message Type）] ドロップダウンリストからメッセージタイプを選択します。

選択内容	結果
方向 - アウト	[有線フィルタ（Wired Filter）] ドロップダウンリストから、有線フィルタを選択します。 有線フィルタの作成については、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の mDNS 有線フィルタの作成（1074 ページ）を参照してください。

ステップ 8 （任意）[すべてのサービスの割り当て（Assign All Services）] トグルボタンが有効になっていない場合は、[割り当てられたサービス（Assigned Services）] で次の手順を実行します。

実行する操作	結果
利用可能サービスの追加	**1.** [Add] をクリックします。 **2.** [利用可能サービスの追加（Add Available Service）] の [サービス（Services）] ドロップダウンリストから、サービスの定義を選択します。 Catalyst Center は、[サービス文字列（Service String）] フィールドのサービス定義に基づき、 文字列を自動的に入力します。 **3.** 選択した方向に基づいて、次の設定を完了します。 • [方向 - イン（Direction - IN）] を選択した場合は、[メッセージタイプ（Message Type）] ドロップダウンリストからメッセージタイプを選択します。 • [方向 - アウト（Direction - OUT）] を選択した場合は、[有線フィルタ（Wired Filter）] ドロップダウンリストから有線フィルタを選択します。 有線フィルタの作成については、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の mDNS 有線フィルタの作成（1074 ページ）を参照してください。 **4.** [Save] をクリックします。
利用可能なサービスの編集	**1.** 編集するサービスの横にあるチェックボックスをオンにします。 **2.** [Actions] にカーソルを合わせて [Edit] を選択します。 **3.** 必要な設定を編集します。 **4.** [Save] をクリックします。

実行する操作	結果
利用可能なサービスの削除	1. 削除するサービスの横にあるチェックボックスをオンにします。 2. [Actions] にカーソルを合わせて [Delete] を選択します。 3. ダイアログボックスで、**Yes** をクリックします。

ステップ 9 [Review and Provision] をクリックします。

ステップ 10 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 11 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の mDNS サービスポリシーの作成

ワイヤレスコントローラ の mDNS サービスポリシーを作成してプロビジョニングするには、次の手順を実行します。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[グローバルワイヤレス（Global Wireless）] を展開して [mDNS] をクリックします。

ステップ 4 [サービスポリシー（Service Policy）] にカーソルを合わせ、[サービスポリシー（Service Policy）] を選択します。

ステップ 5 [Add] をクリックします。

ステップ 6 [サービスポリシーの作成（Create Service Policy）] スライドインペインの[サービスポリシー名（Service Policy Name）] フィールドに、サービスポリシーの一意の名前を入力します。

サービスポリシー名は最大 164 文字で指定できます。

ステップ 7 （任意） ドロップダウンリストから必要なオプションを選択します。

- [サービスリスト入力（Service List Input）]：入力サービスリストを選択します。

  入力サービスリストの作成については、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の mDNS サービスリストの作成 （1070 ページ）を参照してください。

- [サービスリスト出力（Service List Output）]：出力サービスリストを選択します。

  出力サービスリストの作成については、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の mDNS サービスリストの作成 （1070 ページ）を参照してください。

- [場所（Location）]：mDNS ロケーションベース フィルタリングのオプションを選択します。
  - [ap-location]：AP ロケーションを使用したロケーションベースのフィルタリング。
  - [ap-name]：AP 名を使用したロケーションベースのフィルタリング。
  - [location-group]：ロケーショングループを使用したロケーションベースのフィルタリング。
  - [lss]：Location Specific Services（LSS）を使用したロケーションベースのフィルタリング。
  - [regex]：正規表現文字列を使用したロケーションベースのフィルタリング。
  - [site-tag]：サイトタグを使用したロケーションベースのフィルタリング。
  - [ssid]：SSID を使用したロケーションベースのフィルタリング。

ステップ 8 正規表現文字列を使用したロケーションベースのフィルタリングで [正規表現（regex）] オプションを選択した場合は、次の設定を完了します。

- [AP正規表現（AP Regex）] ドロップダウンリストから、対応するロケーション フィルタリング オプションを選択します。
- [Regex Pattern] フィールドに、正規表現文字列を入力します。

  正規表現パターンには最大 164 文字を使用できます。Catalyst Center では、このフィールドに ? は使用できません。このフィールドに %、+、または * を入力する場合は、それらの文字の後に文字を入力しないでください。

ステップ 9 [Review and Provision] をクリックします。

ステップ 10 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。

- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 11 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の mDNS 有線フィルタの作成

ワイヤレスコントローラ の mDNS 有線フィルタを作成してプロビジョニングするには、次の手順を実行します。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[グローバルワイヤレス（Global Wireless）] を展開して [mDNS] をクリックします。

ステップ 4 [サービスポリシー（Service Policy）] にカーソルを合わせ、[有線フィルタ（Wired Filter）] を選択します。

ステップ 5 [Add] をクリックします。

ステップ 6 [有線フィルタの作成（Create Wired Filter）] スライドインペインの [有線フィルタ名（Wired Filter Name）] フィールドに、有線フィルタの一意の名前を入力します。

有線フィルタ名には最大 64 文字を含めることができます。

ステップ 7 （任意） [VLAN List] フィールドに、VLAN ID のリストを入力します。

VLAN ID の有効な範囲は 1 ～ 4094 です。次のように入力できます。

- カンマで区切った複数の VLAN ID（20,30,40 など）
- VLAN ID の範囲（20 ～ 25 など）
- カンマで区切った最大 16 個の VLAN のリスト（10-20,30,40-50 など）

ステップ 8 [MACアドレス（MAC Address）] で、MAC アドレスを設定します。

実行する操作	結果
MAC アドレスを追加する	1. [Add] をクリックします。 2. [MACアドレスの追加（Add MAC Address）] ダイアログボックスの [MACアドレス（Add MAC Address）] フィールドに、mDNS サービスプロバイダーの MAC アドレスを入力します。 MAC アドレスを xxxx.xxxx.xxxx の形式で入力します。 3. [Save] をクリックします。
MAC アドレスを削除する	1. 削除する MAC アドレスの横にあるチェックボックスをオンにします。 2. [Actions] にカーソルを合わせて [Delete] を選択します。 3. ダイアログボックスで、**Yes** をクリックします。

ステップ 9 [Review and Provision] をクリックします。

ステップ 10 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 11 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの mDNS Flex プロファイルの作成

ワイヤレスコントローラの mDNS Flex プロファイルを作成してプロビジョニングするには、次の手順を実行します。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、[デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[グローバルワイヤレス（Global Wireless）] を展開して [mDNS] をクリックします。

ステップ 4 [mDNS Flex Profile] タブをクリックします。

ステップ 5 [Add] をクリックします。

ステップ 6 [mDNS Flexプロファイルの作成（Create mDNS Flex Profile）] スライドインペインの [mDNS Flexプロファイル名（mDNS Flex Profile Name）] フィールドに、mDNS Flex プロファイルの一意の名前を入力します。

mDNS Flex プロファイル名には最大 164 文字を使用できます。Catalyst Center では、プロファイル名に ? とスペースを使用することはできません。プロファイル名の先頭は英数字にする必要があります。

ステップ 7 （任意） 次のフィールドにデータを入力します。

- [サービスキャッシュ更新タイマー（Service Cache Update Timer）]：mDNS サービスキャッシュ更新タイマーの値を入力します。

  有効な範囲は 1 ～ 100 です。デフォルト値は 1 です。

- [統計更新タイマー（Statistics Update Timer）]：mDNS 統計更新タイマーの値を入力します。

  有効な範囲は 1 ～ 100 です。

- [VLANリスト（VLAN List）]：VLAN ID のリストを入力します。

  VLAN ID の有効な範囲は 1 ～ 4094 です。次のように入力できます。

  - カンマで区切った複数の VLAN ID（20,30,40 など）
  - VLAN ID の範囲（20 ～ 25 など）
  - カンマで区切った最大 16 個の VLAN のリスト（10-20,30,40-50 など）

ステップ 8 （任意） [Wired Service Policy] ドロップダウンリストから、サービスポリシーを選択します。

サービスポリシーの作成については、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の mDNS サービスポリシーの作成 （1072 ページ）を参照してください。

ステップ 9 [Review and Provision] をクリックします。

ステップ 10 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 11 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のマルチキャストの設定

次の手順を使用して、ワイヤレスコントローラ のグローバル ワイヤレス マルチキャスト パラメータを設定し、設定をプロビジョニングします。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[グローバルワイヤレス（Global Wireless）] を展開して [マルチキャスト（Multicast）] をクリックします。

ステップ 4 [一般（General）] タブで [グローバルワイヤレスマルチキャスト（Global Wireless Multicast）] トグルボタンをクリックして、グローバル ワイヤレス マルチキャストを有効または無効にします。

グローバルワイヤレスマルチキャストを有効にする場合、必要に応じて、[ワイヤレスmDNSブリッジング（Wireless mDNS Bridging）] チェックボックスをオンにして、mDNS ブリッジングを有効にできます。

ステップ 5 [AP CAPWAPマルチキャスト（AP CAPWAP Multicast）] ドロップダウンから、マルチキャストの配信メカニズムを選択します。

[マルチキャスト（Multicast）] オプションを選択した場合、必要に応じて、これらのフィールドにデータを入力できます。

- [AP CAPWAP IPv4マルチキャストグループアドレス（AP CAPWAP IPv4 Multicast group Address）]：AP が使用する CAPWAP の IPv4 マルチキャスト グループ アドレスを入力します。
- [AP CAPWAP IPv6マルチキャストグループアドレス（AP CAPWAP IPv6 Multicast group Address）]：AP が使用する CAPWAP の IPv6 マルチキャスト グループ アドレスを入力します。

ステップ 6 トグルボタンを使用して次の設定を有効または無効にします。

- [ワイヤレス非IPマルチキャスト（Wireless Non-IP Multicast）]：管理者は、非 IP アプリケーションのマルチキャスト トラフィックを有効または無効にできます。

- [ワイヤレスブロードキャスト（Wireless Broadcast）]：ワイヤレスネットワーク内のブロードキャストトラフィック伝送。

ステップ 7 [Review and Provision] をクリックします。

ステップ 8 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

ステップ 9 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の IGMP スヌーピングの設定

ワイヤレスコントローラ の Internet Group Management Protocol（IGMP）スヌーピングを設定し、その設定をプロビジョニングするには、次の手順を実行します。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラのリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、[デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[グローバルワイヤレス（Global Wireless）] を展開して [マルチキャスト（Multicast）] をクリックします。

ステップ 4 [IGMPスヌーピング（IGMP Snooping）] タブをクリックします。

ステップ 5 （任意） [IGMPスヌーピング（IGMP Snooping）] チェックボックスをオンにして、VLAN の IGMP スヌーピングを有効にします。

IGMP スヌーピングを有効にする場合は、次の設定を完了します。

- [Last Member Query Interval (msec)] フィールドに、最後のメンバークエリ間隔をミリ秒単位で入力します。

有効な範囲は 100 ～ 32767 です。

- （オプション）[VLAN] で、必要な VLAN を有効または無効にします。

  VLAN を有効または無効にするには、必要な VLAN の横にあるチェックボックスをオンにし、[アクション（Actions）] にカーソルを合わせて [有効化（Enable）] または [無効化（Disable）] を選択します。

ステップ 6 （任意） VLAN に IGMP メンバーシップクエリの送信に使用できるマルチキャストルータがない場合は、[IGMPスヌーピングクエリア（IGMP Snooping Querier）] チェックボックスをオンにしてクエリアを有効にします。

ステップ 7 [Review and Provision] をクリックします。

ステップ 8 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

ステップ 9 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の MLD スヌーピングの設定

次の手順を使用して、ワイヤレスコントローラ のグローバルなマルチキャストリスナー検出（MLD）スヌーピングを設定し、設定をプロビジョニングします。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[グローバルワイヤレス（Global Wireless）] を展開して [マルチキャスト（Multicast）] をクリックします。

ステップ 4 [MLD Snooping] タブをクリックします。

ステップ 5 （任意） [Snooping] チェックボックスをオンにして、VLAN のグローバル MLD スヌーピングを有効にします。

MLD スヌーピングを有効にする場合は、次の設定を完了します。

- [MLD Query Interval (msec)] フィールドに、最後のリスナークエリ間隔をミリ秒単位で入力します。

  有効な範囲は 0 または 100 ー 32768 のいずれかです。

- （オプション）[VLAN] で、必要な VLAN を有効または無効にします。

  VLAN を有効または無効にするには、必要な VLAN の横にあるチェックボックスをオンにし、[アクション（Actions）] にカーソルを合わせて [有効化（Enable）] または [無効化（Disable）] を選択します。

ステップ 6 [Review and Provision] をクリックします。

ステップ 7 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

ステップ 8 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の PIM とマルチキャストルーティングの設定

この手順を使用して、ワイヤレスコントローラ のプロトコル非依存型マルチキャスト（PIM）とマルチキャストルーティングをグローバルに設定し、その設定をプロビジョニングします。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、[デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[グローバルワイヤレス（Global Wireless）] を展開して [マルチキャスト（Multicast）] をクリックします。

ステップ 4 [PIMおよびマルチキャストルーティング（PIM and Multicast-Routing）] タブをクリックします。

ステップ 5 [PIM設定（PIM Configuration）] セクションで、次のパラメータを設定します。

- [PIM RPアドレス（PIM RP-Address）]：RP アドレスを静的に設定するためのランデブーポイント（RP）アドレスを入力します。この設定は、受信機がネットワーク内のマルチキャスト送信元を検出できるようにするために必要です。
- [Auto RPリスナー（Auto RP Listener）]：PIM-SM ネットワーク内の RP を動的に検出するには、Auto RP リスナーを有効にします。

ステップ 6 [マルチキャストルーティング設定（Multicast Routing Configuration）] セクションで、次の設定を構成します。

- [分散型マルチキャストルーティング（Distributed Multicast-Routing）]：このボタンを切り替えて、マルチキャスト設定をグローバルに有効または無効にします。
- [VRF環境における分散型マルチキャストルーティング（VRF with Distributed Multicast-Routing）]：使用可能な VRF のリストから、分散型マルチキャストルーティングに使用する VRF を追加または削除します。このオプションにより、複数の仮想ネットワークにまたがるマルチキャスト トラフィックのセグメンテーションが有効になります。VRF インターフェイスを作成する場合は、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの VRF インターフェイスの作成（1134 ページ）」を参照してください。

ステップ 7 [Review and Provision] をクリックします。

ステップ 8 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する（238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 9 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの VRF - RP アドレスマップの作成

ワイヤレスコントローラの VRF-ランデブーポイント（RP）アドレスマップを作成してプロビジョニングするには、次の手順を実行します。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラのリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、[デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[グローバルワイヤレス（Global Wireless）] を展開して [マルチキャスト（Multicast）] をクリックします。

ステップ 4 [VRF - RPアドレスマップ（VRF - RP Address Map）] タブをクリックします。

ステップ 5 [Add] をクリックします。

ステップ 6 [VRF - RPアドレスマップの作成（Create VRF - RP Address Map）] スライドインペインで、次の設定を完了します。

- [VRF] ドロップダウンリストから VRF を選択します。

  VRF の作成については、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の VRF インターフェイスの作成 （1134 ページ）」を参照してください。

- [RPアドレス（RP Address）] フィールドに、グループの RP の IP アドレスを入力します。

ステップ 7 [Review and Provision] をクリックします。

ステップ 8 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

ステップ 9 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のためのワイヤレス ブロード キャストおよび非 IP マルチキャストの作成

この手順を使用して、ワイヤレスコントローラ の VLAN ブロードキャストおよび非 IP マルチキャストを作成し、設定をプロビジョニングします。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、 [グローバルワイヤレス（Global Wireless）] を展開して [マルチキャスト（Multicast）] をクリックします。

ステップ 4 [ワイヤレスブロードキャストおよびワイヤレス非IPマルチキャスト（Wireless Broadcast and Wireless Non-IP Multicast）] タブをクリックします。

[その他（More）] ドロップダウンリストが表示されている場合は、カーソルを [その他（More）] に合わせ、[ワイヤレスブロードキャストおよびワイヤレス非IPマルチキャスト（Wireless Broadcast and Wireless Non-IP Multicast）] を選択します。

ステップ 5 [VLANブロードキャストおよび非IPマルチキャストの作成（Create VLAN Broadcast and Non-IP Multicast）] スライドインペイン の [VLAN ID] フィールドに、VLAN ID を入力します。

有効な範囲は 1 ～ 4094 です。

ステップ 6 トグルボタンを使用して次の設定を有効または無効にします。

- [非IPマルチキャスト（Non-IP Multicast）] : VLAN の非 IP マルチキャストを有効にします。
- [ブロードキャスト（Broadcast）] : ワイヤレス クライアントへのブロードキャスト パケットを許可します。

ステップ 7 [Review and Provision] をクリックします。

ステップ 8 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。

- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 9 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のロケーションの設定

次の手順を使用して、ワイヤレスコントローラのロケーションパラメータを設定し、設定をプロビジョニングします。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、[デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[グローバルワイヤレス（Global Wireless）] を展開し、[ロケーション（Location）] をクリックします。

ステップ 4 [アルゴリズム（Algorithm）] ドロップダウンリストから、RSSI および SNR 値の平均化に使用するアルゴリズムを選択します。

- [平均（Average）]：プローブ RSSI 測定の更新を、CPU のオーバーヘッドがより高くなる、より正確なアルゴリズムに設定します。
- [シンプル（Simple）]：プローブ RSSI 測定の更新を、より高速なアルゴリズムに設定します。CPU のオーバーヘッドは小さくなりますが、精度は低くなります。

ステップ 5 次のフィールドにデータを入力します。

- [調整クライアントの期限しきい値（秒）（Expiry Calibrating Client Threshold (sec)）]：クライアントを調整するためのタイムアウトを秒単位で入力します。

  有効な範囲は 1 ～ 3600 です。

- [クライアント期限切れのしきい値（秒）（Expiry Client Threshold (sec)）]：RSSI 値のタイムアウトを秒単位で入力します。

  有効な範囲は 5 ～ 3600 です。

- [クライアント通知しきい値（dB）（Notify Client Threshold (dB)）]：クライアントのネットワーク モビリティ サービス プロトコル（NMSP）通知 RSSI しきい値を dB 単位で入力します。

  有効な範囲は 0 ～ 10 です。

  このしきい値は、通知をトリガーするクライアント RSSI の変化を定義します。たとえば、このフィールドに 5 と入力すると、クライアントの RSSI が 5 dB 変化したときに NMSP は通知を送信します。

- [タグの有効期限（秒）（Expiry Tags (sec)）]：RFID RSSI の有効期限を秒単位で入力します。

  有効な範囲は 5 ～ 300 です。

  RSSI 値が期限切れになると、RFID RSSI はクリーンアップされます。

- [タグの通知しきい値（dB）（Notify Threshold Tags (dB)）]：RSSI 測定のロケーション コントロール プロトコル（LOCP）通知しきい値を入力します。

  有効な範囲は 1 ～ 10 です。

ステップ 6 ドロップダウンリストから必要なオプションを選択します。

- [RSSIハーフライフ調整クライアントしきい値（秒）（RSSI Half Life Calibrating Client Threshold (sec)）]：クライアントを調整するための RSSI 半減期のしきい値を選択します。
- [RSSIハーフライフクライアントしきい値（秒）（RSSI Half Life Client Threshold (sec)）]：クライアントの NMSP 通知しきい値を選択します。
- [RSSIハーフライフ不正APしきい値（秒）（RSSI Half Life Rogue AP Threshold (sec)）]：不正 AP の RSSI 半減期のしきい値を選択します。
- [RSSIハーフライフタグしきい値（秒）（RSSI Half Life Tags (sec)）]：RFID タグの RSSI 半減期のしきい値を選択します。

  RFID RSSI 半減期は、RFID タグの 2 つの RSSI 読み取り値を平均した場合の半減期を表します。

ステップ 7 [Review and Provision] をクリックします。

ステップ 8 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

ステップ 9 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの国コードの設定

ワイヤレスコントローラの国コードを設定してプロビジョニングするには、次の手順を実行します。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラのリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、[デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[グローバルワイヤレス（Global Wireless）] を展開して [国（Country）] をクリックします。

ステップ 4 国コードを設定します。

国コードを管理するには、次のオプションを使用します。

実行する操作	結果
国コードを検索する	[検索（Search）] フィールドに、国の名前の一部または完全な名前を入力し、Enter を押します。
国コードを追加する	次のいずれかのオプションを使用します。 • 必要な国コードの横にあるプラスアイコンをクリックします。 • 国コードをクリックし、[選択項目を追加（Add Selected）] をクリックします。 （注） 複数の国コードを選択して追加するには、Shift キーを押しながら国コードをクリックし、[選択項目を追加（Add Selected）] をクリックします。

実行する操作	結果
国コードを削除する	次のいずれかのオプションを使用します。 • 必要な国コードの横にある [X] アイコンをクリックします。 • 国コードをクリックし、[選択項目を削除（Remove Selected）] をクリックします。 （注） 複数の国コードを選択して削除するには、Shift キーを押しながら国コードをクリックし、[選択項目を削除（Remove Selected）] をクリックします。 • [すべて削除（Remove All）] をクリックし、すべての国コードを削除します。

ステップ 5 [Review and Provision] をクリックします。

ステップ 6 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

ステップ 7 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の Cisco DNA 統合設定

この手順を使用して、ワイヤレスコントローラ の Cisco DNA 統合設定を行い、その設定をプロビジョニングします。

Cisco DNA gRPC とネットワークアシュアランス gRPC は同時に動作可能です。Cisco Spaces IoT サービスと Catalyst Center gRPC も同時に実行できます。

（注） クリアテキストトークンの設定は、wsaCfgIcapPort が有効になっている場合にのみ使用できます。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、[デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[グローバルワイヤレス（Global Wireless）] を展開し、[Cisco DNA 統合設定（Cisco DNA Integration Settings）] をクリックします。

ステップ 4 [クリアテキストトークン（Clear Text Token）] フィールドに、AP 参加トークンをクリアテキスト形式で入力します。

トークンタイプが [クリア（Clear）] の場合、または暗号化されていないトークンから暗号化されたトークンに移行する場合に、このフィールドを使用します。

（注） クリアテキストトークンの安全性は低くなります。

ステップ 5 [Review and Provision] をクリックします。

ステップ 6 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

ステップ 7 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の AP ポリシーの設定

この手順を使用して、ワイヤレスコントローラ の AP ポリシーを設定し、プロビジョニングします。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラのリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[グローバルワイヤレス（Global Wireless）] をクリックし、[APポリシー（AP Policy）] をクリックします。

ステップ 4 [APポリシー（AP Policy）] タブをクリックします。

ステップ 5 （任意） 必要なチェックボックスをオンにして、対応するポリシーを設定します。

- [MACに基づくAPを認可（Authorize APs against MAC）]：MAC アドレスを使用して AP 認可ポリシーを設定します。
- [シリアル番号に対してAPを認可（Authorize APs against Serial Number）]：シリアル番号を使用して AP 認可ポリシーを設定します。

ステップ 6 [承認方式リスト（Authorization Method List）] ドロップダウンリストから承認方式リストを選択します。

「タイプ - ログイン情報ダウンロード」の承認方式リストの作成については、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の認証方式リストの作成 （929 ページ）」を参照してください。

ステップ 7 [Review and Provision] をクリックします。

ステップ 8 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

ステップ 9 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のデバイス認証シリアル番号の作成

この手順を使用して、ワイヤレスコントローラ のデバイス認証シリアル番号を作成し、プロビジョニングします。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。

b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。

c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。

b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[グローバルワイヤレス（Global Wireless）] をクリックし、[APポリシー（AP Policy）] をクリックします。

ステップ 4 [デバイス認証（Device Authentication）] にカーソルを合わせ、[シリアル番号（Serial Numbers）] を選択します。

ステップ 5 [Add] をクリックします。

ステップ 6 [デバイス認証シリアル番号の作成（Create Device Authentication Serial Number）] スライドインペインの [シリアル番号（Serial Number）] フィールドに、デバイス認証シリアル番号を入力します。

最大 255 文字を使用できます。Catalyst Center は、シリアル番号で ? とスペースをサポートしていません。

ステップ 7 （任意） [属性リスト名（Attribute List Name）] ドロップダウンリストから、属性リストを選択します。

属性リストの作成については、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の属性リストの作成 （937 ページ）」を参照してください。

ステップ 8 [Review and Provision] をクリックします。

ステップ 9 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 10 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のデバイス認証 MAC アドレスの作成

ワイヤレスコントローラ のデバイス認証 MAC アドレスを作成してプロビジョニングするには、次の手順を実行します。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[グローバルワイヤレス（Global Wireless）] を展開し、[APポリシー（AP Policy）] をクリックします。

ステップ 4 [デバイス認証（Device Authentication）] にカーソルを合わせ、[MACアドレス（MAC Addresses）] を選択します。

ステップ 5 [Add] をクリックします。

ステップ 6 [デバイス認証MACアドレスの作成（Create Device Authentication MAC Address）] スライドインペインの [MACアドレス（MAC Address）] フィールドに、デバイス認証 MAC アドレスを入力します。

最大 64 文字を含めることができます。MAC アドレスは、*xx:xx:xx:xx:xx:xx*、*xxxx.xxxx.xxxx*、*xx-xx-xx-xx-xx-xx*、または *xxxxxxxxxxxx* 形式で入力できます。

ステップ 7 （任意） [属性リスト名（Attribute List Name）] ドロップダウンリストから、属性リストを選択します。

属性リストの作成については、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の属性リストの作成 （937 ページ）」を参照してください。

ステップ 8 （任意） [Description] フィールドに、説明を入力します

最大 128 文字を入力できます。Catalyst Center では、説明に ? は使用できません。

ステップ 9 （任意） [WLANプロファイル名（WLAN Profile Name）] ドロップダウンリストから、WLAN プロファイルを選択します。

WLAN プロファイルの作成については、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の WLAN プロファイルの作成 （813 ページ）」を参照してください。

ステップ 10 [Review and Provision] をクリックします。

ステップ 11 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 12 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のワイヤレス地理位置情報設定の構成

ワイヤレスコントローラ に関連付けられている AP のワイヤレス地理位置情報設定を構成し、ロケーションベースサービスとトラッキング機能を有効にしてからプロビジョニングするには、次の手順を実行します。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、[デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、で、[グローバルワイヤレス（Global Wireless）] を展開して [ワイヤレス地理位置情報設定（Wireless Geolocation Settings）] をクリックします。

ステップ 4 [地理位置情報導出の有効化（Enable Geolocation Derivation）] トグルボタンを使用して、AP の地理的な場所の自動更新および導出を有効または無効にします。

このオプションを有効にすると、ワイヤレスコントローラは利用可能なネットワークデータを使用して AP の地理的な場所を自動的に導出して更新します。このオプションにより、ロケーションベースサービスとレポートが改善されます。このオプションを無効にする場合は、各 AP の地理位置情報設定を手動で構成する必要があります。

ステップ 5 [Review and Provision] をクリックします。

ステップ 6 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

ステップ 7 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのサービス設定

このセクションでは、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのデバイスごとのサービス設定に関する情報を示します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のサービステンプレートの作成

次の手順を使用して、ワイヤレスコントローラ のローカルポリシーのサービステンプレートを作成し、プロビジョニングします。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラのリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[サービス（Services）] を展開し、[ローカルポリシー（Local Policy）] をクリックします。

ステップ 4 [Service Template] タブで [Add] をクリックします。

ステップ 5 [サービステンプレートの作成（Create Service Template）] スライドインペイン の次のフィールドにデータを入力します。

- [**Service Template Name**]：サービステンプレートの一意の名前を入力します。

  名前には最大 48 文字を使用できます。

- （オプション）[VLAN ID]：VLAN ID を入力します。

  有効な範囲は 1 ～ 4094 です。

- （オプション）[セッションタイムアウト（秒）（Session Timeout (sec)）]：セッションタイムアウトを秒単位で入力します。

  有効な範囲は 1 ～ 1073741823 です。

ステップ 6 （任意） ドロップダウンリストから必要なオプションを選択します。

- [アクセス制御リスト（Access Control List）]（ACL の作成については、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の IPv4 ACL の作成 （940 ページ）」を参照してください）
- [入力QoS（Ingress QoS）]（QoS の作成については、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の QoS ポリシーの作成 （1097 ページ）」を参照してください）
- [出力QoS（Egress QoS）]（QoS の作成については、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の QoS ポリシーの作成 （1097 ページ）」を参照してください）
- [mDNSサービスポリシー（mDNS Service Policy）]（mDNS サービスポリシーの作成については、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の mDNS サービスポリシーの作成 （1072 ページ）」を参照してください）

ステップ 7 [Review and Provision] をクリックします。

ステップ 8 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

ステップ 9 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のポリシーマップの作成

次の手順を使用してポリシーマップを作成し、ワイヤレスコントローラ上のローカルポリシーのサービステンプレートにマッピングし、プロビジョニングします。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。

b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。

c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[サービス（Services）] を展開し、[ローカルポリシー（Local Policy）] をクリックします。

ステップ 4 [Policy Map] タブをクリックします。

ステップ 5 [Add] をクリックします。

ステップ 6 [**Create Policy Map**] スライドインペインの [**Policy Map Name**] フィールドに、ポリシーマップの名前を入力します。

ステップ 7 （任意） [一致条件リスト（Match Criteria List）] で、必要な一致条件リストを設定します。

（注） 一致基準リストを少なくとも 1 つ設定します。最大 254 件の一致基準リストを設定できます。

実行する操作	結果
一致条件リストの追加	**1.** [Add] をクリックします。 **2.** [追加の一致条件リスト（Add Match Criteria List）] ダイアログボックスの [サービステンプレート（Service Template）] ドロップダウンリストから、ローカルポリシーのサービステンプレートを選択します。 サービステンプレートの作成については、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のサービステンプレートの作成 （1093 ページ）を参照してください。 **3.** （オプション）一致条件リストに対応するフィルタを含めるには、必須のチェックボックスをオンにします。 • **Device Type** • **ユーザ ロール** • User Name • **OUI** • **MAC Address** **4.** いずれかのフィルタのチェックボックスをオンにした場合は、これらの設定を行います。 • 対応する [Condition] ドロップダウンリストから、フィルタの条件（[equals]、[does not equal] または [regex]）を選択します。 • フィルタの対応するフィールドにデータを入力します。 • [**Device Type**]：デバイス名を入力します。 • [**User Role**]：ユーザーロールを入力します。 • [**Username**]：ユーザー名を入力します。 • [**OUI**]：組織固有識別子（OUI）を、ピリオド区切りの 16 進数形式で入力します。たとえば、*xx.xx.xx* となります。 • [**MAC Address**]：MAC アドレスを *xxxx.xxxx.xxxx* の形式で入力します。 **5.** [Save] をクリックします。

実行する操作	結果
一致条件リストの編集	1. 編集するシーケンスの横にあるチェックボックスをオンにします。 2. [Actions] にカーソルを合わせて [Edit] を選択します。 3. 必要な設定を編集します。 4. [Save] をクリックします。
一致条件リストの削除	1. 削除するシーケンスの横にあるチェックボックスをオンにします。 2. [Actions] にカーソルを合わせて [Delete] を選択します。 3. ダイアログボックスで、**Yes** をクリックします。

ステップ 8 [Review and Provision] をクリックします。

ステップ 9 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 10 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の QoS ポリシーの作成

この手順を使用して、ワイヤレスコントローラ の QoS ポリシーを作成し、プロビジョニングします。

（注） 少なくとも 1 つのクラスマップを追加するか、QoS ポリシーのクラスのデフォルトを設定する必要があります。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。

b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[サービス（Services）] を展開し、[QoS] をクリックします。

ステップ 4 [Add] をクリックします。

ステップ 5 [**Create QoS Policy**] スライドインペインの [**Policy Name**] フィールドに、QoS ポリシーの一意の名前を入力します。

Catalyst Center では、ポリシー名に ? とスペースは使用できません。

ステップ 6 （任意） [Description] フィールドに、説明を入力します

説明には最大 200 文字を使用できます。

ステップ 7 [クラスのデフォルト（Class Default）] で、次の設定を完了します。

a) [**Mark Type**] ドロップダウンリストから、必須オプション（[**None**]、[**DSCP**]、または [**User Priority**]）を選択します。

マーキングは、次のいずれかに使用できます。

- パケットヘッダー内の特定のフィールドまたはビットの設定
- デバイスの内部にあるパケット構造の特定のフィールドの設定

選択内容	結果
DSCP	[マーク値（Mark Value）] ドロップダウンリストから、IPv4 および IPv6 パケットに DSCP を設定するために必要なオプションを選択します。
ユーザー優先度	[マーク値（Mark Value）] ドロップダウンリストから、必要なオプションを選択して、WLAN ユーザーの優先順位を設定します。

b) （任意） [ポリシング（Kbps）（Police (kbps)）] フィールドに、コミットされた情報レートを入力します。

指定できる範囲は 8 ～ 10000000 です。

ステップ 8 （任意） [クラスマップ（Class Maps）] で、クラスマップを設定します。

a) [追加（Add）] をクリックして、クラスマップを追加します。

[クラスマップの追加（Add Class Map）] ダイアログボックスで、次の設定を行います。

1. [**Class Type**] ドロップダウンリストから、クラスマップタイプ（[**AVC**] または [**User Defined**]）を選択します。
2. [**Match**] ドロップダウンリストから、一致タイプ（[**Any**] または [**All**]）を選択します。
3. [**Drop**] ドロップダウンリストから、特定の送信元からの通信をドロップするための必須オプション（[**Disabled**] または [**Enabled**]）を選択します。

   [無効（Disabled）] を選択した場合は、次の設定を行います。

   - [**Mark Type**] ドロップダウンリストから、必須オプション（[**None**]、[**DSCP**]、または [**User Priority**]）を選択します。

選択内容	結果
DSCP	[マーク値（Mark Value）] ドロップダウンリストから、IPv4 および IPv6 パケットに DSCP を設定するために必要なオプションを選択します。
ユーザー優先度	[マーク値（Mark Value）] ドロップダウンリストから、必要なオプションを選択して、WLAN ユーザーの優先順位を設定します。

   - （オプション）[ポリシング（Kbps）（Police (kbps)）] フィールドに、コミットされた情報レートを入力します。

     指定できる範囲は 8 ～ 10000000 です。

4. [マッチタイプ（Match Type）] ドロップダウンリストから、必要な一致パラメータを選択します。

選択内容	結果
AVC クラスタイプ	次のいずれかの方法を使用して、一致タイプに基づいて一致するパラメータを追加します。 • 必要な一致パラメータの横にあるプラスアイコンをクリックします。 • 必要な一致パラメータをクリックし、[選択項目を追加（Add Selected）] をクリックします。 複数の一致パラメータを選択するには、Shift キーを押しながら一致パラメータをクリックし、[選択項目を追加（Add Selected）] をクリックします。 • すべての一致パラメータを追加するには、[すべて追加（Add All）] をクリックします。 [検索（Search）] フィールドを使用して、一致パラメータをフィルタリングできます。 少なくとも 1 つの一致パラメータを追加します。一致パラメータを最大 256 個まで追加できます。 たとえば、[プロトコル（Protocol）] マッチタイプを選択した場合は、少なくとも 1 つのプロトコルを選択します。
ユーザー定義クラスタイプ	[マッチ値（Match Value）] ドロップダウンリストから、必要な一致パラメータを選択します。

5. [Save] をクリックします。

b) クラスマップを削除するには、次の手順を実行します。

1. 必要なクラスマップの横にあるチェックボックスをオンにします。
2. [Actions] にカーソルを合わせて [Delete] を選択します。
3. ダイアログボックスで、**Yes** をクリックします。

ステップ 9 [Review and Provision] をクリックします。

ステップ 10 ワイヤレスコントローラ がライセンス要件を満たしていない AP を管理している場合、Catalyst Center は詳細を示すダイアログボックスを表示します。ダイアログボックスで、必要なオプションを選択します。

オプション	説明
ライセンス マネージャ	[License Manager] ウィンドウを開いて、対応するライセンスを有効にします。 ライセンスを有効にするには、『*Cisco Catalyst Center Administrator Guide*』の「Manage Licenses」を参照してください。

オプション	説明
[デバイスプロビジョニングに進む（Continue to device provision）]	デバイスのプロビジョニングを続行します。 （注） ライセンス要件を満たしていないAPは、ワールドワイドセーフモード（WWSM）になります。
Cancel	ダイアログボックスを閉じます。

ステップ 11 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 12 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのカスタムアプリケーションの作成

ワイヤレスコントローラのカスタムアプリケーションを作成してプロビジョニングするには、次の手順を実行します。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、で、[サービス（Services）] を展開し、[アプリケーションの可視性（Application Visibility）] をクリックします。

ステップ 4 [カスタムアプリケーション（Custom Applications）] タブで、[追加（Add）] をクリックします。

ステップ 5 [**Create Custom Application**] スライドインペインの [**Application Name**] フィールドに、アプリケーションの一意の名前を入力します。

アプリケーション名の長さは 3 ー 24 文字にする必要があります。Catalyst Center では、アプリケーション名に英数字、-、および _ を使用できます。Catalyst Center では、アプリケーション名にスペースおよび他の特殊文字は使用できません。

ステップ 6 [**Type**] ドロップダウンリストから、アプリケーションタイプ（[**URL**]、[**Server Name**]、[**Protocol**]、または [**DSCP**]）を選択します。

ステップ 7 アプリケーションのタイプに基づいて、次の設定を完了します。

a) [URL] を選択した場合は、[URL] フィールドに URL を入力します。

Catalyst Center では URL にスペースは使用できません。

b) [サーバー名（Server Name）] を選択した場合は、[サーバー名（Server Name）] フィールドにサーバー名を入力します。

最大 30 文字を入力できます。

c) [プロトコル（Protocol）] を選択した場合は、次の設定を完了します。

- [**IP Address**] フィールドに、カスタムアプリケーションの有効な IP アドレスを *x.x.x.x* 形式で入力します。
- （オプション）[**Subnet (0-32)**] フィールドに、カスタムアプリケーションのサブネットマスクを入力します。

  有効な範囲は 0 ～ 32 です。
- [**Protocol Type**] で、必要なプロトコル（[**TCP**] および [**UDP**]）の横にあるチェックボックスをオンにします。
- [ポートの値（Port Values）] で、必要なオプションを選択します。
  - [個別の値（Individual Values）] を選択した場合は、次の設定を完了します。

実行する操作	結果
ポート番号を追加する	**1.** [Add] をクリックします。 **2.** [ポート番号の追加（Add Port Number）] ダイアログボックスの [ポート番号（Port Number）] フィールドに、ポート番号を入力します。 値の範囲は 1 ～ 65535 です。 **3.** [Save] をクリックします。

実行する操作	結果
ポート番号を削除する	1. 削除するポート番号の横にあるチェックボックスをオンにします。 2. [Actions] にカーソルを合わせて [Delete] を選択します。 3. ダイアログボックスで、**Yes** をクリックします。

- [範囲（Range）] を選択した場合は、対応するフィールドにポート番号の開始範囲と終了範囲を入力します。

  値の範囲は 1 ～ 65535 です。

d) [DSCP] を選択した場合は、次のいずれかの方法を使用して DSCP を追加します。

（注） DSCP を少なくとも 1 つ追加します。

- 必要な DSCP の横にあるプラスアイコンをクリックします。
- 必要な DSCP をクリックし、[選択項目を追加（Add Selected）] をクリックします。

  複数の DSCP を選択するには、Shift を押しながら DSCP をクリックし、[選択項目を追加（Add Selected）] をクリックします。
- すべての DSCP を追加するには、[すべて追加（Add All）] をクリックします。

  [検索（Search）] フィールドを使用して、DSCP をフィルタ処理できます。

ステップ 8 [トラフィッククラス（Traffic Class）] または [同様の設定（Similar To）] を選択します。

選択内容	結果
[Traffic Class]	[トラフィッククラス（Traffic Class）] ドロップダウンリストからクラスを選択します。
Similar To	[同様の設定（Similar To）] ドロップダウンリストから必要なオプションを選択します。

ステップ 9 [**Business Relevance**] ドロップダウンリストから、オプション（[**Relevant**]、[**Irrelevant**]、または [**Default**]）を選択します。

ステップ 10 [Review and Provision] をクリックします。

ステップ 11 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 12 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のエクスポータの作成

ワイヤレスコントローラのフローエクスポータを作成してプロビジョニングするには、次の手順を実行します。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラのリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、[デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、で、[サービス（Services）] を展開し、[アプリケーションの可視性（Application Visibility）] をクリックします。

ステップ 4 [**Flow Monitors**] にカーソルを合わせて [**Exporter**] をクリックします。

ステップ 5 [エクスポータ（Exporter）] ウィンドウで、[追加（Add）] をクリックします。

ステップ 6 [**Create Exporter**] スライドインペインで、次の設定を完了します。

a) [**Exporter Name**] フィールドに、フローエクスポータの一意の名前を入力します。

最大 60 文字を入力できます。Catalyst Center では、エクスポータ名に英数字、-、および _ を使用できます。Catalyst Center では、エクスポータ名にスペースおよび他の特殊文字は使用できません。

b) （任意） [**Description**] フィールドに、フローエクスポータの説明を入力します。

最大 80 文字を入力できます。Catalyst Center では、エクスポータに特殊文字 ?、<、>、および & は使用できません。

c) [**Exporter Type**] ドロップダウンリストからエクスポータのタイプ（[**External Collector**] または [**Local**]）を選択します。

[**External Collector**] を選択した場合は、次の設定を完了します。

- [宛先IP（Destination IP）]：接続先の IP アドレスを入力すると、フローレコードがこの接続先デバイスに送信されます。IP アドレスを *xxx.xxx.xxx.xxx* の形式で入力します。
- [VRF]：ドロップダウンリストから [VRF] を選択します。フローモニターは、選択した VRF に関連付けられています。
- [ポート（Port）]：UDP のポート番号を入力します。

  値の範囲は 1 ～ 65535 です。デフォルト値は 9995 です。

ステップ 7 [Review and Provision] をクリックします。

ステップ 8 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

ステップ 9 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのフローモニターの作成

ワイヤレスコントローラのフローモニターを作成してプロビジョニングするには、次の手順を実行します。

始める前に

フローモニターにバインドされるフローエクスポータを作成していることを確認します。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラのリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、[デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、で、[サービス（Services）] を展開し、[アプリケーションの可視性（Application Visibility）] をクリックします。

ステップ 4 [**Flow Monitors**] にカーソルを合わせ、[**Monitor**] をクリックします。

ステップ 5 **[モニター（Monitor）]** ウィンドウで、[追加（Add）] をクリックします。

ステップ 6 [モニターの作成（Create Monitor）] スライドインペインで、次の構成設定を入力します。

- [**Flow Monitor Name**]：フローモニターの一意の名前を入力します。

  最大 40 文字を入力できます。Catalyst Center では、- _ @ [ ] { } ( ) および . の特殊文字をフローモニター名で使用できます。

- （オプション）[**Description**]：フローモニターの説明を入力します。

  最大 80 文字を入力できます。Catalyst Center では、フローモニター名で ? は使用できません。

- [**Flow Exporters**]：次の方法のいずれかを使用して、使用可能なリストから必要なフローエクスポータを追加します。

  - 必要なフローエクスポータの横にあるプラスアイコンをクリックします。
  - 必要なフローエクスポータをクリックし、[**Add Selected**] をクリックします。

    複数のフローエクスポータを選択するには、**Shift** を押しながらフローエクスポータをクリックし、[**Add Selected**] をクリックします。
  - すべてのフローエクスポータを追加するには、[**Add All**] をクリックします。

    [**Search**] フィールドを使用して、フローエクスポータをフィルタ処理できます。

ステップ 7 [Review and Provision] をクリックします。

ステップ 8 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

ステップ 9 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の EoGRE グローバルパラメータの設定

次の手順を使用して、ワイヤレスコントローラ の EoGRE グローバルパラメータを設定し、設定をプロビジョニングします。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラのリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[サービス（Services）] を展開して [EoGRE] をクリックします。

ステップ 4 [グローバル（Global）] タブの次のフィールドにデータを入力します。

- [ハートビート間隔（秒）（Heartbeat Interval (sec)）]：トンネルゲートウェイに対するキープアライブのハートビート間隔を秒単位で入力します。

  有効な範囲は 60 ～ 600 です。

- [最大ハートビートスキップカウント（Max Heartbeat Skip Count）]： フトンネルゲートウェイに対するキープアライブの最大ハートビート スキップ カウントを指定します。

  有効な範囲は 3 ～ 10 です。

ステップ 5 [Interface Name] ドロップダウンリストから、インターフェイスを選択します。

物理インターフェイスの管理については、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのイーサネットポートの設定 （1133 ページ）」を参照してください。

SVI プロファイルの作成については、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の SVI プロファイルの作成 （1122 ページ）」を参照してください。

ステップ 6 [Review and Provision] をクリックします。

ステップ 7 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

ステップ 8 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の EoGRE ゲートウェイの作成

ワイヤレスコントローラ の EoGRE トンネルゲートウェイを作成してプロビジョニングするには、次の手順を実行します。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。

b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。

c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。

b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[サービス（Services）] を展開して [EoGRE] をクリックします。

ステップ 4 [Gateways] タブをクリックします。

ステップ 5 [Add] をクリックします。

ステップ 6 **[ゲートウェイの作成（Create Gateway）]** スライドインペインの [トンネルID（Tunnel ID）] フィールドに、トンネル ID を入力します。

ステップ 7 [宛先IPアドレス（Destination IP Address）] で、IP アドレスオプションを選択します。

ステップ 8 （任意） [Source Interface] ドロップダウンリストからインターフェイスを選択します。

物理インターフェイスの管理については、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのイーサネットポートの設定 （1133 ページ）」を参照してください。

SVI プロファイルの作成については、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の SVI プロファイルの作成 （1122 ページ）」を参照してください。

ステップ 9 （任意） 選択した宛先 IP アドレスオプションに基づいて、次の設定を完了します。

選択内容	結果
Ipv4	[宛先IPアドレス（IPv4）（Destination IP Address(IPv4)）] フィールドに、宛先の IPv4 アドレスまたはホスト名を入力します。
Ipv6	[宛先IPアドレス（IPv6）（Destination IP Address(IPv6)）] フィールドに、宛先の IPv6 アドレスまたはホスト名を入力します。

ステップ 10 （任意） [AAAプロキシ（AAA Proxy）] トグルボタンをクリックして AAA プロキシを有効にし、次の設定を完了します。

- [暗号化タイプ（Encryption Type）] ドロップダウンリストから暗号化タイプを選択します。

- 次のフィールドにデータを入力します。
  - [キーフレーズ（Key Phrase）]：AAA キーフレーズを入力します。

    最大 128 文字を入力できます。
  - [認証ポート（Auth Port）]：AAA 認証または許可ポートを入力します。

    有効な範囲は 0 ～ 65535 です。
  - [アカウンティングポート（Acct Port）]：AAA アカウンティングポートを入力します。

    有効な範囲は 0 ～ 65535 です。

ステップ 11 [Review and Provision] をクリックします。

ステップ 12 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 13 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの EoGRE ドメインの作成

ワイヤレスコントローラの EoGRE トンネルドメインを作成してプロビジョニングするには、次の手順を実行します。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。

b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。

c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。

b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[サービス（Services）] を展開して [EoGRE] をクリックします。

ステップ 4 [Domains] タブをクリックします。

ステップ 5 [Add] をクリックします。

ステップ 6 [ドメインの作成（Create Domain）] スライドインペインの [ドメイン名（Domain Name）] フィールドに、トンネルドメインの名前を入力します。

ステップ 7 （任意） [ステータス（Status）] トグルボタンをクリックしてトンネルドメインを有効にします。

ステップ 8 （任意） 対応するドロップダウンリストからプライマリおよびセカンダリ トンネル ゲートウェイを選択します。

ステップ 9 （任意） [リバーティブ冗長性（Revertive Redundancy）] チェックボックスをオンにして、リバーティブ冗長性モデルを有効にします。

ステップ 10 [Review and Provision] をクリックします。

ステップ 11 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 12 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の EoGRE トンネルプロファイルの作成

ワイヤレスコントローラ の EoGRE ワイヤレス トンネル プロファイルを作成してプロビジョニングするには、次の手順を実行します。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[サービス（Services）] を展開して [EoGRE] をクリックします。

ステップ 4 [Tunnel Profiles] タブをクリックします。

ステップ 5 [Add] をクリックします。

ステップ 6 [トンネルプロファイルの作成（Create Tunnel Profile）] スライドインペインの [一般（General）] タブで、次の設定を完了します。

a) [Tunnel Profile Name] フィールドに、トンネルプロファイルの名前を入力します。

トンネルプロファイル名には最大 128 文字を使用できます。

b) （任意） [ステータス（Status）] トグルボタンをクリックしてトンネルプロファイルを有効にします。

c) [集中転送（Centralized Forwarding）] トグルボタンを使用して、すべてのワイヤレスクライアントトラフィックが中央のコントローラを介してルーティングされるのか、ローカルで AP に転送されるのかを示します。

d) [DHCPオプション82（DHCP Option-82）] で次の設定を完了します。

- （オプション）[DHCPオプション82ステータス（DHCP Option-82 Status）] トグルボタンをクックして DHCP オプション 82 を有効にします。
- （オプション）[ASCII] トグルボタンをクリックして DHCP オプション 82 を ASCII 形式で有効にします。

  ASCII 形式を使用しない場合は、バイナリ形式が使用されます。
- （任意）[Delimiter] フィールドに、DHCP オプション 82 のデリミタ文字を入力します。

  単一のデリミタ文字を入力できます。
- ドロップダウンリストから必要なオプションを選択します。
  - [MAC形式（MAC Format）] : DHCP オプション 82 の MAC 形式を選択します。
  - （オプション）[回線ID（Circuit ID）] : DHCP オプション 82 の回線 ID を選択します。
  - （オプション）[リモートID（Remote ID）] : DHCP オプション 82 のリモート ID を選択します。

e) （任意） [AAA] で、必要なチェックボックスをオンにして対応する設定を有効にします。

- [RADIUSプロキシ（RADIUS Proxy）] : AAA プロキシを有効にします。

  AAA プロキシを有効にする場合、必要に応じて、[アカウンティングプロキシ（Accounting Proxy）] チェックボックスをオンにして AAA アカウンティングプロキシを有効にできます。
- [オーバーライド（Override）] : AAA オーバーライドを有効にします。

ステップ 7 （任意） [ルール（Rules）] タブをクリックし、必要なルールを設定します。

実行する操作	結果
ルールの追加	**1.** [Add] をクリックします。 **2.** [ルールの追加（Add Rule）] ダイアログボックスの [優先順位（Priority）] フィールドに、ルールの優先順位の番号を入力します。 有効な範囲は 1 ～ 100 です。 **3.** [Realm] フィールドに、照合するルールレルムを入力します。 ルールレルムには最大 128 文字を使用できます。Catalyst Center では、レルムの先頭または末尾にスペースを含めることはできません。 **4.** [Domain Name] ドロップダウンリストから、ルールの接続先ドメインを選択します。 **5.** [VLAN ID] フィールドに、ルールの VLAN ID を入力します。 有効な範囲は 1 ～ 4094 です。 **6.** **[Save]** をクリックします。
ルールの編集	**1.** 編集するルールの横にあるチェックボックスをオンにします。 **2.** [Actions] にカーソルを合わせて [Edit] を選択します。 **3.** 必要な設定を編集します。 **4.** [Save] をクリックします。
ルールの削除	**1.** 削除するルールの横にあるチェックボックスをオンにします。 **2.** [Actions] にカーソルを合わせて [Delete] を選択します。 **3.** ダイアログボックスで、**Yes** をクリックします。

ステップ 8 [Review and Provision] をクリックします。

ステップ 9 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 10 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのメディアストリームの設定

ワイヤレスコントローラ のメディア ストリーム パラメータを設定し、その設定をプロビジョニングするには、次の手順を実行します。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。

b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。

c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラのリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。

b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[サービス（Services）] を展開して [メディアストリーム（Media Stream）] をクリックします。

ステップ 4 [一般（General）] タブで、[マルチキャストダイレクトの有効化（Enable Multicast Direct）] トグルボタンを使用してマルチキャストダイレクト設定を有効または無効にします。

ステップ 5 （任意） [セッションメッセージ設定（Session Message Configuration）] で、次の設定を完了します。

a) [セッションアナウンス状態（Session Announcement State）] チェックボックスをオンにして、メディアストリームの Session Description Protocol（SDP）メッセージを有効にします。

b) 次のフィールドにデータを入力します。

- [セッションアナウンスURL（Session Announcement URL）] : メディアストリームの SDP URL を入力します。

  URL には最大 128 文字を使用できます。

- [セッションアナウンス電子メール（Session Announcement Email）] : メディアストリームの SDP 電子メール ID を入力します。

  電子メール ID には最大 64 文字を使用できます。

- [セッションアナウンス電話（Session Announcement Phone）] : メディアストリームの SDP 電話番号を入力します。

  電話番号には最大 30 個の数字とハイフンを使用できます。

- [セッションアナウンスメモ（Session Announcement Note）] : メディアストリームの SDP アナウンスメモを入力します。

  アナウンスメモには最大 128 文字を使用できます。

ステップ 6 [Review and Provision] をクリックします。

ステップ 7 ワイヤレスコントローラ がライセンス要件を満たしていない AP を管理している場合、Catalyst Center は詳細を示すダイアログボックスを表示します。ダイアログボックスで、必要なオプションを選択します。

オプション	説明
ライセンス マネージャ	[License Manager] ウィンドウを開いて、対応するライセンスを有効にします。 ライセンスを有効にするには、『*Cisco Catalyst Center Administrator Guide*』の「Manage Licenses」を参照してください。
[デバイスプロビジョニングに進む（Continue to device provision）]	デバイスのプロビジョニングを続行します。 （注） ライセンス要件を満たしていない AP は、ワールドワイドセーフモード（WWSM）になります。
Cancel	ダイアログボックスを閉じます。

ステップ 8 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

ステップ 9 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のメディア ストリーム プロファイルの作成

この手順を使用して、ワイヤレスコントローラのメディアストリームプロファイルを作成し、プロビジョニングします。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。

b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[サービス（Services）] を展開して [メディアストリーム（Media Stream）] をクリックします。

ステップ 4 [Streams] タブをクリックします。

ステップ 5 [Add] をクリックします。

ステップ 6 [メディア ストリームプロファイルの作成（Create Media Stream Profile）] スライドインペインの [メディアストリーム名（Media Stream Name）] フィールドに、メディアストリームグループの名前を入力します。

メディアストリームグループ名には最大 64 文字を使用できます。

ステップ 7 [Maximum Expected Bandwidth (Kbps)] に、メディア ストリームの予想帯域幅を入力します。

有効な範囲は 1 ～ 35000 です。デフォルト値は 1000 です。

ステップ 8 [**Multicast Destination**] で、次のフィールドに有効な IPv4 アドレスまたは IPv6 アドレスを入力します。

- [開始IPv4/IPv6アドレス（Start IPv4/IPv6 Address）]：メディアストリームグループの開始 IP アドレスを入力します。
- [終了IPv4/IPv6アドレス（End IPv4/IPv6 Address ）]：メディアストリームグループの終了 IP アドレスを入力します。

  開始 IP アドレスと終了 IP アドレスは同じタイプである必要があります。

ステップ 9 [リソース予約コントロール（RRC）パラメータ（Resource Reservation Control（RRC）Parameters）]で、ドロップダウンリストから、次の設定を完了します。

a) [Average Packet Size (bytes)] フィールドに、ストリームの予想パケットサイズを入力します。

有効な範囲は 100 ～ 1500 です。デフォルト値は 1200 です。

b) ドロップダウンリストから必要なオプションを選択します。

- [**Policy**]：ストリームのアクション（[**Admit**] または [**Deny**]）を選択します。
- [優先順位（Priority）]：ストリームの優先順位を選択します。値は 1 ～ 8 から選択できます。
- [QoS]：ストリームの QoS 値を選択します。
- [**RRC re-evaluation**]：RRC 評価のオプション（[**Periodical**] または [**Initial**]）を選択します。
- [**Violation**]：RRC 違反に対するアクション（[**Fallback**] または [**Drop**]）を選択します。

ステップ 10 [Review and Provision] をクリックします。

ステップ 11 ワイヤレスコントローラ がライセンス要件を満たしていない AP を管理している場合、Catalyst Center は詳細を示すダイアログボックスを表示します。ダイアログボックスで、必要なオプションを選択します。

オプション	説明
ライセンス マネージャ	[License Manager] ウィンドウを開いて、対応するライセンスを有効にします。 ライセンスを有効にするには、『*Cisco Catalyst Center Administrator Guide*』の「Manage Licenses」を参照してください。
[デバイスプロビジョニングに進む（Continue to device provision）]	デバイスのプロビジョニングを続行します。 （注） ライセンス要件を満たしていない AP は、ワールドワイドセーフモード（WWSM）になります。
Cancel	ダイアログボックスを閉じます。

ステップ 12 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 13 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のゲスト LAN プロファイルの作成

この手順を使用して、ワイヤレスコントローラ のゲスト LAN プロファイルを作成し、プロビジョニングします。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、 [サービス（Services）] を展開して [ゲストLAN（Guest LAN）] をクリックします。

ステップ 4 [Guest LAN Profiles] タブで [Add] をクリックします。

ステップ 5 [ゲストLANプロファイルの作成（Create Guest LAN Profile）] スライドインペイン の [一般（General）] タブで、次の設定を完了します。

a) [**Guest LAN Profile Name**] フィールドに、ゲスト LAN プロファイルの一意の名前を入力します。

プロファイル名は最大 32 文字で指定できます。

b) [ID] フィールドに、ゲスト LAN プロファイルの ID を入力します。

有効な範囲は 1 ～ 5 です。

c) [Client Association Limit] フィールドに、ゲスト LAN ごとのクライアント接続の最大数を入力します。

有効な範囲は 1 ～ 2000 です。デフォルト値は 2000 です。

d) [mDNS Mode] ドロップダウンリストから、ゲスト LAN の mDNS モード（[Bridging]、[Drop]、または [Gateway]）を選択します。

e) ゲスト LAN の有線 VLAN ID を有効または無効にするには、[有線VLANステータス（Wired VLAN Status）] トグルボタンを使用します。

（注） 有線 VLAN ID はゲスト フォーリン コントローラに設定する必要があります。

有線 VLAN ID が有効になっている場合は、[有線VLAN ID（Wired VLAN ID）] フィールドに、ゲスト フォーリン コントローラのゲスト LAN の VLAN ID を入力します。

有効な範囲は 0 ～ 4094 です。デフォルト値は 0 です

f) ゲスト LAN を有効または無効にするには、[ステータス（Status）] トグルボタンを使用します。

ステップ 6 （任意） [セキュリティ（Security）] タブをクリックして、次の設定を行います。

a) セキュリティWeb認証を設定するには、[Web認証（Web Auth）]チェックボックスをオンにします。

b) ドロップダウンリストから必要なオプションを選択します。

- [Web認証パラメータマップ（Web Auth Parameter Map）]（Web 認証プロファイルの作成については、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの Web 認証プロファイルの作成（970 ページ）」を参照してください）
- [認証リスト（Authentication List）]（認証リストの作成については、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の認証方式リストの作成 （928 ページ）」を参照してください）
- [認可リスト（Authorization List）]（認可リストの作成については、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の認証方式リストの作成 （929 ページ）」を参照してください）

ステップ 7 [Review and Provision] をクリックします。

ステップ 8 ワイヤレスコントローラ がライセンス要件を満たしていない AP を管理している場合、Catalyst Center は詳細を示すダイアログボックスを表示します。ダイアログボックスで、必要なオプションを選択します。

オプション	説明
ライセンス マネージャ	[License Manager] ウィンドウを開いて、対応するライセンスを有効にします。 ライセンスを有効にするには、『*Cisco Catalyst Center Administrator Guide*』の「Manage Licenses」を参照してください。
[デバイスプロビジョニングに進む（Continue to device provision）]	デバイスのプロビジョニングを続行します。 （注） ライセンス要件を満たしていないAPは、ワールドワイドセーフモード（WWSM）になります。
Cancel	ダイアログボックスを閉じます。

ステップ 9 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 10 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのゲスト LAN マップの作成

ワイヤレスコントローラ のゲスト LAN マップを作成してプロビジョニングするには、次の手順を実行します。

（注） ワイヤレスコントローラの単一ゲスト LAN マップを作成できます。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。

b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[サービス（Services）] を展開して [ゲストLAN（Guest LAN）] をクリックします。

ステップ 4 [ゲストLANマップ（Guest LAN Map）] タブをクリックします。

ステップ 5 [Add] をクリックします。

ステップ 6 [ゲストLANマップの作成（Create Guest LAN Map）] スライドインペインの [マップ名（Map Name）] フィールドに、ゲスト LAN マップの一意の名前を入力します。

マップ名には最大 32 文字を使用できます。

ステップ 7 （任意） [ゲストLAN/ポリシーマップ（Guest LAN - Policy Map）] で、ゲスト LAN/ポリシーマッププロファイルを設定します。

（注） 最大 5 つのゲスト LAN およびポリシープロファイルマップを設定できます。

実行する操作	結果
ゲスト LAN/ポリシープロファイルマップを追加する	**1.** [Add] をクリックします。 **2.** [ゲストLAN/ポリシーマップの追加（Add Guest LAN - Policy Map）] ダイアログボックスの [ゲストLANプロファイル名（Guest LAN Profile Name）] ドロップダウンリストから、ゲスト LAN プロファイルを選択します。 **3.** [Policy Profile Name] ドロップダウンリストから、ポリシープロファイルを選択します。 **4.** [Save] をクリックします。
ゲスト LAN/ポリシープロファイルマップを編集する	**1.** 必要なプロファイル名の横にあるチェックボックスをオンにします。 **2.** [Actions] にカーソルを合わせて [Edit] を選択します。 **3.** 必要な設定を編集します。 **4.** [Save] をクリックします。

実行する操作	結果
ゲスト LAN/ポリシープロファイル マップを削除する	1. 必要なプロファイル名の横にあるチェックボックスをオンにします。 2. [Actions] にカーソルを合わせて [Delete] を選択します。 3. ダイアログボックスで、**Yes** をクリックします。

ステップ 8 [Review and Provision] をクリックします。

ステップ 9 ワイヤレスコントローラ がライセンス要件を満たしていない AP を管理している場合、Catalyst Center は詳細を示すダイアログボックスを表示します。ダイアログボックスで、必要なオプションを選択します。

オプション	説明
ライセンス マネージャ	[License Manager] ウィンドウを開いて、対応するライセンスを有効にします。 ライセンスを有効にするには、『*Cisco Catalyst Center Administrator Guide*』の「Manage Licenses」を参照してください。
[デバイスプロビジョニングに進む（Continue to device provision）]	デバイスのプロビジョニングを続行します。 （注） ライセンス要件を満たしていない AP は、ワールドワイドセーフモード（WWSM）になります。
Cancel	ダイアログボックスを閉じます。

ステップ 10 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 11 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の 除外クライアントを追加

除外されたクライアントは、障害対応またはセキュリティ目的で使用できます。必要なクライアントを除外することで、特定のデバイスがネットワークにアクセスできないようにできます。

この手順を使用して、ワイヤレスコントローラ の除外クライアントを追加し、プロビジョニングします。

（注） [アシュアランス（Assurance）] ウィンドウからクライアントのリストを変更する場合、ワイヤレスコントローラ が再同期された後にのみ [除外クライアント（Excluded Clients）] テーブルにそれらのリストが表示されます。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[サービス（Services）] を展開し、[除外クライアント（Excluded Clients）] をクリックします。

ステップ 4 [Add] をクリックします。

ステップ 5 [クライアント除外の作成（Create Client Exclusion）] スライドインペイン で、次のフィールドにデータを入力します。

- [クライアントデバイスの MAC アドレス（Client device MAC Address）]：除外するクライアントの MAC アドレスを入力します。

  xxxx.xxxx.xxxx、*xx-xx-xx-xx-xx-xx*、*xxxx-xxxx-xxxx*、*xxxx:xxxx:xxxx*、または *xx:xx:xx:xx:xx:xx* の形式で MAC アドレスを入力します。クライアントがすでに除外リストに含まれていないことを確認します。

- [説明（Description）]：MAC アドレスの説明または除外の理由を入力します。

ステップ 6 [Review and Provision] をクリックします。

ステップ 7 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

ステップ 8 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のレイヤ 2 設定

このセクションでは、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ におけるデバイスごとのレイヤ 2 設定に関する情報を示します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の SVI プロファイルの作成

次の手順を使用して、ワイヤレスコントローラのスイッチドVLANインターフェイス（SVI）プロファイルを作成し、プロビジョニングします。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラのリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、[デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[レイヤ 2（Layer 2）] を展開し、[VLAN] をクリックします。

ステップ 4 [SVI] タブで [Add] をクリックします。

ステップ 5 [SVIの作成（Create SVI）] スライドインペインの [一般（General）] タブで、次の設定を完了します。

a) [VLAN番号（VLAN Number）] フィールドに、SVI の VLAN ID を入力します。

有効な範囲は 1 ～ 4094 です。

b) （任意） [Description] フィールドに、説明を入力します
c) [管理ステータス（Admin Status）] トグルボタンを使用して、VLAN を有効または無効にします。
d) （任意） [VRF] ドロップダウンリストから VRF を選択します。



重要 VRF を変更すると、IPv4 および IPv6 アドレスが削除されます。

e) （任意） [MTU（バイト）（MTU (bytes)）] フィールドに、IP MTU の値を入力します。

有効な範囲は 68 ～ 18000 です。デフォルト値は 1500 です

f) （任意） [PIMスパースモード（PIM Sparse Mode）] チェックボックスをオンにして、プロトコル非依存型マルチキャスト（PIM）スパースモードを有効にし、効率的なマルチキャストルーティングを実現します。

受信者が分散しているネットワークでは、このモードが推奨されます。

g) （任意） [IGMPバージョン（IGMP Version）] ドロップダウンリストから、IGMP バージョンを選択します。

h) （任意） [自動ステート（Autostate）] チェックボックスをオンにして、VLAN の状態の自動判定を有効にします。

i) （任意） [IPv4] チェックボックスをオンにして、VLAN インターフェイスで IPv4 アドレスを有効にし、これらの設定を完了します。

- [タイプ（Type）] ドロップダウンリストから、VLAN インターフェイスが IP 設定を受信する方法を選択します。
- [静的（Static）] を選択した場合、次の手順を行います。
  - [IP Address] フィールドに、IPv4 アドレスを入力します。
  - [Subnet Mask] フィールドにサブネットマスクを入力します。
  - [セカンダリ（Secondary）] チェックボックスをオンにして、セカンダリ IP アドレスを追加します。

    このチェックボックスをオンにした場合は、セカンダリ IP アドレスとサブネットマスクを対応するフィールドに入力します。
- [DHCP] を選択した場合、[ホスト名（Host Name）] フィールドにホスト名を入力します。
- [OSPF] の下で、これらの設定を完了します。
  - [プロセスID（Process ID）] ドロップダウンリストから、[Open Shortest Path First (OSPF)] プロセス ID を選択します。
  - [BFD] チェックボックスをオンにして、Bidirectional Forwarding Detection（BFD）を有効にします。
  - [メッセージダイジェスト認証（Message Digest Authentication）] チェックボックスをオンにして、メッセージダイジェスト認証を使用します。
  - [メッセージダイジェスト認証 - キーマップ（Message Digest Authentication - Key Map(s)）] の下で、メッセージダイジェスト認証キーマップを設定します。

実行する操作	結果
メッセージダイジェスト認証キーマップの追加	**1.** [Add] をクリックします。 **2.** [キー（Key）] フィールドにキーを入力します。 **3.** [パスワードタイプ（Password Type）] フィールドに暗号化タイプを入力します。 **4.** [パスワード（Password）] フィールドに OSPF キーを入力します。 **5.** [Save] をクリックします。
メッセージダイジェスト認証キーマップの削除	**1.** 削除するキーの横にあるチェックボックスをオンにします。 **2.** [Actions] にカーソルを合わせて [Delete] を選択します。 **3.** ダイアログボックスで、**Yes** をクリックします。

j) （任意） [IPv6] チェックボックスをオンにして、VLAN インターフェイスで IPv6 アドレスを有効にし、これらの設定を完了します。

- IPv6 静的アドレスを設定します。

実行する操作	結果
IPv6 静的アドレスの追加	**1.** [Add] をクリックします。 **2.** [IPv6静的アドレスの追加（Add IPv6 Static）] ダイアログボックスの [タイプ（Type）] ドロップダウンリストから、タイプを選択します。 **3.** [アドレス（Address）] フィールドに、VLAN インターフェイスのアドレスを入力します。 **4.** [Save] をクリックします。
IPv6 静的アドレスの削除	**1.** 削除する IPv6 アドレスの横にあるチェックボックスをオンにします。 **2.** [Actions] にカーソルを合わせて [Delete] を選択します。 **3.** ダイアログボックスで、**Yes** をクリックします。

- （任意）対応する設定を有効にするには、必要なチェックボックスをオンにします。
  - [リンクローカル（Link Local）] : リンクローカルアドレスを使用します。

このチェックボックスをオンにした場合は、[アドレス（Address）]フィールドにリンクローカルアドレスを入力します。

- [DHCP]：SVI が IPv6 アドレスを動的に取得できるように、DHCP を有効にします。

  DHCP を有効にする場合、必要に応じて [高速コミット（Rapid Commit）] チェックボックスをオンにして、プレフィックス委任の高速コミットを有効にできます。

- [自動設定（Autoconfig）]：VLAN インターフェイスで自動アドレス割り当てを有効にします。

  このチェックボックスをオンにすると、必要に応じて、[デフォルト（Default）] チェックボックスをオンにしてデフォルトルートを挿入できます。

- [IPv6 DHCPクライアントとして動作（Act as an IPv6 DHCP client）]：DHCP サーバーからの自動 IPv6 アドレス割り当てを有効にします。

  このチェックボックスをオンにすると、必要に応じて、[プレフィックス名（Prefix Name）] フィールドにプレフィックス名を入力できます。

  プレフィックス名は 200 文字まで入力できます。

ステップ 6 （任意） [詳細設定（Advanced）] タブをクリックして、次の設定を完了します。

a) [アクセスリスト（Access Lists）] で、対応するドロップダウンリストからインバウンドおよびアウトバウンド IPv4 および IPv6 ACL を選択します。

ACL の作成については、『Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の IPv4 ACL の作成 （940 ページ）』と『Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の IPv6 ACL の作成 （949 ページ）』を参照してください。

b) [DHCPリレー （DHCP Relay）] で、次の設定を完了します。

- [リレー情報オプション（Relay Information Optio）] チェックボックスをオンにして、受信した DHCP でのリレー情報オプションを有効にします。TranslatorEnglish

- [加入者ID（Subscriber ID）] フィールドに、加入者 ID サブオプションを入力します。
- [送信元インターフェイスVLAN（Source-Interface VLAN）] ドロップダウンリストから SVI を選択します。

  SVI プロファイルの作成については、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の SVI プロファイルの作成 （1122 ページ）」を参照してください。

- [サーバーIDオーバーライド（Server Id Override）] チェックボックスをオンにして、サーバー ID オーバーライドおよびリンク選択サブオプションを挿入します。
- [オプションの挿入（Option Insert）] チェックボックスをオンにして、アウトバウンドパケットに DHCP オプションを挿入できるようにします。

c) [ヘルパーアドレス（Helper Address(es)）] で、IPv4 ヘルパーアドレスを設定します。

実行する操作	結果
ヘルパーアドレスの追加	1. [Add] をクリックします。 2. [ヘルパーアドレスの追加（Add Helper Address）] ダイアログボックスの [IPv4ヘルパーアドレス（IPv4 Helper Address）] フィールドに、DHCP サーバーの IP アドレスを入力します。 3. [Save] をクリックします。
ヘルパーアドレスの削除	1. 削除するヘルパーアドレスの横にあるチェックボックスをオンにします。 2. [Actions] にカーソルを合わせて [Delete] を選択します。 3. ダイアログボックスで、**Yes** をクリックします。

d) [mDNSゲートウェイ（mDNS Gateway）] チェックボックスをオンにして、mDNS ゲートウェイを有効にします。

mDNS ゲートウェイがグローバル コンフィギュレーション モードで設定されていることを確認してください。詳細については、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の mDNS の設定 （1067 ページ）を参照してください。

（オプション）このチェックボックスをオンにした場合、[mDNSサービスポリシー（mDNS Service Policy）] ドロップダウンリストから mDNS サービスポリシーを選択します。mDNS サービスポリシーの作成については、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の mDNS サービスポリシーの作成 （1072 ページ）を参照してください。

ステップ 7 [Review and Provision] をクリックします。

ステップ 8 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

ステップ 9 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の VLAN プロファイルの作成

この手順を使用して、ワイヤレスコントローラ の VLAN プロファイルを作成し、プロビジョニングします。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[レイヤ2（Layer 2）] を展開し、[VLAN] をクリックします。

ステップ 4 [VLAN] タブをクリックします。

ステップ 5 [Add] をクリックします。

ステップ 6 [VLANの作成（Create VLAN）] スライドインペイン の [VLAN ID] フィールドに、VLAN ID を入力します。

有効な範囲は 1 ～ 4094 です。

ステップ 7 [VLAN名（VLAN Name）] フィールドに、VLAN 名を入力します。

ステップ 8 [状態（State）] ドロップダウンリストから、VLAN の動作状態を選択します。

ステップ 9 [Review and Provision] をクリックします。

ステップ 10 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 11 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の VLAN グループプロファイルの作成

この手順を使用して、ワイヤレスコントローラ の VLAN プロファイルを作成し、プロビジョニングします。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[レイヤ2（Layer 2）] を展開し、[VLAN] をクリックします。

ステップ 4 [VLAN Group] タブをクリックします。

ステップ 5 [Add] をクリックします。

ステップ 6 [VLANグループの作成（Create VLAN Group）] スライドインペイン の [VLANグループ名（VLAN Group Name）] フィールドに、VLAN グループ名を入力します。

ステップ 7 [VLAN List] フィールドに、VLAN リストの値を入力します。

次のいずれかを入力できます。

- VLAN ID（VLAN ID の有効な範囲は 1 ～ 4094 ）
- カンマ区切りの VLAN ID の範囲（たとえば、1-20,30,40-50）

ステップ 8 [Review and Provision] をクリックします。

ステップ 9 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 10 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのポート チャネル インターフェイスの作成

ワイヤレスコントローラのポート チャネル インターフェイスを作成してプロビジョニングするには、次の手順を実行します。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。

b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。

c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラのリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。

b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[レイヤ2（Layer 2）] を展開して [インターフェイス（Interfaces）] をクリックします。

ステップ 4 [論理（Logical）] にカーソルを合わせ、[ポートチャネル（Port Channel）] を選択します。

ステップ 5 [Add] をクリックします。

ステップ 6 [ポートチャネルの作成（Create Port Channel）] スライドインペインで、必要な設定を完了します。

a) [Port Channel Number] フィールドに、ポートチャネル番号を入力します。

有効な範囲は 1 ～ 64 です。

b) （任意） [Description] フィールドに、説明を入力します

200 文字まで入力できます。Catalyst Center では説明に ? は使用できません。

c) [管理ステータス（Admin Status）] トグルボタンを使用して、インターフェイスを有効または無効にします。

d) [レイヤ3アドレス（Layer 3 Address）] トグルボタンを使用して、ポートチャネルタイプをレイヤ 2 からレイヤ 3、またはレイヤ 3 からレイヤ 2 に変更します。

（注） ポートチャネルタイプを変更すると、ポートメンバーが削除されます。ポートメンバーを再選択する必要があります。

e) [ポートメンバー（Port Members）] で、ポートチャネルタイプのポートメンバーを設定します。

実行する操作	結果
ポートメンバーを検索する	[検索（Search）] フィールドに、ポートメンバーの名前の一部または完全な名前を入力し、Enter を押します。

実行する操作	結果
ポート メンバーを追加する	次のいずれかのオプションを使用します。 • 必要なポートメンバーの横にあるプラスアイコンをクリックします。 • ポートメンバーをクリックし、[選択項目を追加（Add Selected）] をクリックします。 （注） 複数のポートメンバーを選択して追加するには、Shift を押しながらポートメンバーをクリックし、[選択項目を追加（Add Selected）] をクリックします。
ポートメンバーを削除する	次のいずれかのオプションを使用します。 • 必要なポートメンバーの横にある [X] アイコンをクリックします。 • ポートメンバーをクリックし、[選択項目を削除（Remove Selected）] をクリックします。 （注） 複数のポートメンバーを選択して削除するには、Shift を押しながらポートメンバーをクリックし、[選択項目を削除（Remove Selected）] をクリックします。 • [すべて削除（Remove All）] をクリックし、すべてのポートメンバーを削除します。

ステップ 7 [Review and Provision] をクリックします。

ステップ 8 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

ステップ 9 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのループバック インターフェイスの作成

ループバック インターフェイスは、ワイヤレスコントローラで管理とルーティングの目的で使用されます。

ワイヤレスコントローラのループバックインターフェイスを作成してプロビジョニングするには、次の手順を実行します。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラのリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[レイヤ2（Layer 2）] を展開して [インターフェイス（Interfaces）] をクリックします。

ステップ 4 [論理（Logical）] タブにカーソルを合わせ、[ループバック（Loopback）] をクリックします。

ステップ 5 [Add] をクリックします。

ステップ 6 [ループバックの作成（Create Loopback）] スライドインペインで、次の設定を完了します。

a) ループバック インターフェイスを識別するために使用される [ループバック番号（Loopback Number）] として一意の番号を入力します。
b) （任意） [Description] フィールドに、説明を入力します
c) （任意）[管理ステータス（Admin Status）] トグルボタンを使用して、選択したインターフェイスを有効または無効にします。
d) （任意） [VRF] ドロップダウンリストから、ループバック インターフェイスが選択した VRF テーブルに関連付けられるように VRF を選択します。これにより、ループバック インターフェイス上のトラフィックが VRF のルーティングテーブルに従ってルーティングされます。
e) 受信した DHCP パケットがゲートウェイ IP アドレス（giaddr）フィールドを設定しないように、[リレー情報オプション（Relay Information Option）] を有効にします。この設定は、リレーエージェントがゲートウェイ IP アドレスを指定せずに DHCP サーバーに追加情報を提供する必要があるネットワークで使用されます。これにより、DHCP サーバーは、リレーエージェント情報オプションの情報を使用して IP アドレスとその他の設定パラメータを割り当てることができるようになります。
f) [IPオプション（IP Options）] で、必要なオプションを選択します。
g) [IPv4] を選択した場合は、次の設定を構成します。

- [IPv4 Type] ドロップダウンリストから IP アドレスタイプを選択します。

- [IP address] フィールドに、ループバック インターフェイスに割り当てる IPv4 アドレスを入力します。
- [Subnet Mask] フィールドにサブネット マスクを入力します。
- （オプション）[セカンダリIP（Secondary IP）] チェックボックスをオンにして、ループバック インターフェイスにセカンダリ IP アドレスを割り当てます。[セカンダリIP（Secondary IP）] アドレスと [セカンダリIPマスク（Secondary IP Mask）] を入力します。

h) [IPv6] を選択した場合は、次の設定を構成します。

- 次の IPv6 設定の少なくとも 1 つを選択します。
  - [DHCP]：ループバック インターフェイスの DHCPv6 を有効にします。選択した場合は、必要に応じて [高速コミット（Rapid Commit）] を有効にし、プレフィックスを委任できます。
  - [自動設定（Autoconfig）]：ループバック インターフェイスを自動的に設定します。選択した場合は、[自動設定（Autoconfig）] ドロップダウンリストから挿入する自動設定を選択します。
  - [IPv6 DHCPクライアントとして動作（Act as an IPv6 DHCP client）]：IPv6 アドレスの自動割り当てを有効にします。選択した場合は、[IPv6 DHCPクライアントとして動作（Act as an IPv6 DHCP client）] フィールドにプレフィックス名を入力します。
- [静的リスト（Static lists）] で、静的リストを設定します。

実行する操作	結果
静的リストを追加する	**1.** [Add] をクリックします。 **2.** [静的リストの追加（Add Static List）] ダイアログボックスの [静的（Static）] ドロップダウンリストから、静的リストを選択します。 **3.** 静的リストに基づいて、対応するフィールドに有効な IPv6 アドレスを入力します。 **4.** [Save] をクリックします。
静的リストを削除する	**1.** 削除する静的リストの横にあるチェックボックスをオンにします。 **2.** [Actions] にカーソルを合わせて [Delete] を選択します。 **3.** ダイアログボックスで、**Yes** をクリックします。

ステップ 7 [Review and Provision] をクリックします。

ステップ 8 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

ステップ 9 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのイーサネットポートの設定

ワイヤレスコントローラのイーサネットポートを設定してその設定をプロビジョニングするには、次の手順を実行します。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[レイヤ2（Layer 2）] を展開して [インターフェイス（Interfaces）] をクリックします。

ステップ 4 [Ethernet] タブで、設定するイーサネットポートの横にあるオプションボタンをクリックします。

ステップ 5 [Actions] にカーソルを合わせて [Edit] を選択します。

ステップ 6 （任意） [イーサネットポートの編集（Edit Ethernet Ports）] スライドインペインの [一般（General）] タブで、[説明（Description）] フィールドにポートの説明を入力します。

ステップ 7 （任意） [詳細設定（Advanced）] タブで、対応するドロップダウンリストからインバウンドとアウトバウンドの IPv4 および IPv6 ACL を選択します。

IPv4 ACL の作成については、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の IPv4 ACL の作成（940 ページ）を参照してください。

IPv6 ACL の作成については、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の IPv6 ACL の作成 （949 ページ）」を参照してください。

ステップ 8 [Review and Provision] をクリックします。

ステップ 9 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する（238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 10 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の VRF インターフェイスの作成

Virtual Routing and Forwarding（VRF）インターフェイスは、ワイヤレスコントローラ内の複数のルーティング テーブル インスタンスをセグメント化するために使用されます。

次の手順を実行して、ワイヤレスコントローラのVRFインターフェイスを作成し、プロビジョニングします。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラのリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、[デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[レイヤ2（Layer 2）] を展開して [インターフェイス（Interfaces）] をクリックします。

ステップ 4 [VLAN] タブで、[追加（Add）] をクリックします。

ステップ 5 [VRFの作成（Create VRF）] スライドインペイン で、次の設定を完了します。

- 次のオプションからプロトコルを選択します。IPv4、IPv6、または IPv4/IPv6。選択したプロトコルに基づいてルーティングテーブルが作成されます。
- [VRF名（VRF name）] フィールドに、VRF の名前を入力します。
- [Route Distinguisher] フィールドに、ルート識別子の詳細を ASN:nn 形式で入力します。これは、異なる VRF 内のルートを区別するために使用される一意の ID です。

- ルートターゲットインポートの場合、[追加（Add）] をクリックして、VRF がインポートするルートターゲット拡張コミュニティ属性を指定します。これにより、VRF は、一致するルートターゲット属性を持つ他の VRF からのルートを受け入れることができます。
- ルートターゲットエクスポートの場合、[追加（Add）] をクリックして、VRF がエクスポートするルートターゲット拡張コミュニティ属性を指定します。これにより、VRF は、ルートターゲット属性が一致する他の VRF にそのルートをアドバタイズできます。

ステップ 6 [Review and Provision] をクリックします。

ステップ 7 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

ステップ 8 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのワイヤレス管理インターフェイスの設定

ワイヤレス管理インターフェイスは、ワイヤレスコントローラ と AP 間のすべての通信に使用されます。ワイヤレスコントローラには単一のワイヤレス管理インターフェイスがあります。

ワイヤレスコントローラ のワイヤレス管理インターフェイスを設定してプロビジョニングするには、次の手順を実行します。

（注） インターフェイスまたはトラストポイントを変更すると、AP が切断され、クライアント接続が中断されます。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、[デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[レイヤ2（Layer 2）] を展開して [インターフェイス（Interfaces）] をクリックします。

ステップ 4 [Wireless] タブをクリックします。

ステップ 5 （任意） 次の設定を完了します。

a) [Interface Name] ドロップダウンリストから、インターフェイスを選択します。

SVI インターフェイスの作成については、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの SVI プロファイルの作成（1122 ページ）」を参照してください。イーサネットポートの作成については、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのイーサネットポートの設定（1133 ページ）」を参照してください。

b) [Trustpoint] フィールドに、ワイヤレス管理トラストポイント名を入力します。
c) [NAT IPv4/IPv6 Server Address] フィールドに、NAT IP アドレスを入力します。
d) トグルボタンを使用して次の設定を有効または無効にします。

- [L3インターフェイスキャッシュでのNATの有効化（Enable NAT on L3 Interface Cache）]：レイヤ 3 インターフェイス キャッシュ データのネットワークアドレス変換（NAT）を有効または無効にします。
- [プライベートIP検出（Private IP Discovery）]：ワイヤレスコントローラがクライアントデバイスに関連付けられているプライベート IP アドレスを検出してログに記録できるようにするオプションを有効または無効にします。
- [パブリックIP検出（Public IP Discovery）]：ワイヤレスコントローラがクライアントデバイスに関連付けられているパブリック IP アドレスを検出してログに記録できるようにするオプションを有効または無効にします。

ステップ 6 [コントローラ管理セキュリティ（Controller Management Security）] で、次の設定を完了します。

- [SSC認証トークン（SSC Authentication Token）] フィールドに、ワイヤレスコントローラ とのセキュアな管理通信に使用するセキュアソケット通信（SSC）トークンを入力します。

（注） このトークンが機密扱いになっており、ピアデバイスまたは管理システムで期待される値と一致していることを確認します。

- [SSC認証トークンタイプ（SSC Auth Token Type）] ドロップダウンリストから、SSC 認証トークンの保存と送信に使用する暗号化またはハッシュ方式を選択します。

（注） トークンタイプを変更する場合は、接続されているすべてのシステムでトークンを更新する必要がある場合があります。

ステップ 7 [SSC信頼ハッシュ（SSC Trust Hashes）] で、SSC 信頼ハッシュを設定します。

実行する操作	結果
SSC 信頼ハッシュの追加	**1.** [Add] をクリックします。 **2.** [SSC信頼ハッシュの追加（Add SSC Trust Hash）] ダイアログボックスの [SSC証明書フィンガープリント（SSC Certificate Fingerprint）] フィールドに、ワイヤレスコントローラとのセキュア通信のために AP で使用される SSC のフィンガープリントまたはハッシュを入力します。 **3.** [Save] をクリックします。
SSC 信頼ハッシュの編集	**1.** 編集する SSC 信頼ハッシュの横にあるチェックボックスをオンにします。 **2.** [Actions] にカーソルを合わせて [Edit] を選択します。 **3.** 設定を編集します。 **4.** [Save] をクリックします。
SSC 信頼ハッシュの削除	**1.** 削除する SSC 信頼ハッシュのチェックボックスをオンにします。 **2.** [Actions] にカーソルを合わせて [Delete] を選択します。 **3.** ダイアログボックスで、**Yes** をクリックします。

ステップ 8 [Review and Provision] をクリックします。

ステップ 9 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 10 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の検出プロトコルの設定

次の手順を使用して、ワイヤレスコントローラの検出プロトコルを設定し、その設定をプロビジョニングします。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、[デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[レイヤ2（Layer 2）] を展開し、[検出プロトコル（Discovery Protocols）] をクリックします。

ステップ 4 [CDP] で、次の設定を完了します。

a) [CDPステータス（CDP Status）] トグルボタンを使用して、Cisco Discovery Protocol（CDP）を有効または無効にします。

CDP を有効にする場合は、次のフィールドにデータを入力します。

- [ホールド時間（Hold Time）] : CDP パケットで送信されるまでのホールド時間（秒単位）を入力します。

  有効な範囲は 10 ～ 255 です。

- [タイマー（Timer）] : CDP パケットが送信されるレート（秒単位）を入力します。

  有効な範囲は 5 ～ 254 です。

b) [CDPアドバタイズメント バージョン（CDP Advertisement Version）] ドロップダウンリストから、必要なバージョンを選択します。

ステップ 5 [LLDP] で、次の設定を完了します。

a) [LLDPステータス（LLDP Status）] トグルボタンを使用して、Link Layer Discovery Protocol（LLDP）を有効または無効にします。
b) （任意） 次のいずれかの方法を使用して、タイプ、長さ、および値（TLV）を追加します。

- 必要な TLV の横にあるプラスアイコンをクリックします。
- 必要な TLV をクリックし、[Add Selected] をクリックします。

  複数の AP エントリを選択するには、Shift を押しながら TLV をクリックし、[Add Selected] をクリックします。

- すべての TLV を追加するには、[Add All] をクリックします。

  [Search] フィールドを使用して、TLV をフィルタ処理できます。

ステップ 6 [Review and Provision] をクリックします。

ステップ 7 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

ステップ 8 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のネットワーク設定

このセクションでは、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のデバイスごとのネットワーク設定に関する情報を示します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの DNS ループバックの設定

ワイヤレスコントローラにおける DNS ベースのホスト名からアドレスへの変換を設定してその設定をプロビジョニングするには、次の手順を実行します。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラのリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、[デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、**[ネットワーク設定（Network Settings）]** を展開して [DNS] をクリックします。

ステップ 4 [DNSループバック（DNS Loopback）] トグルボタンを使用して、DNS ベースのアドレスからホスト名への変換を有効または無効にします。

ステップ 5 [Review and Provision] をクリックします。

ステップ 6 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

ステップ 7 [Tasks] ウィンドウで、タスクの展開を監視します。

次のタスク

DNS ループバックを有効にすると、[DNS] テーブルで DNS サーバーを追加、編集、または削除できます。DNS サーバーの追加については、「DNS ループバック用の DNS サーバーの追加（1140 ページ）」を参照してください。

DNS ループバック用の DNS サーバーの追加

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のアドレス変換に DNS ベースのホスト名用の DNS サーバーを追加するには、この手順を使用します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の DNS ループバックを有効にする場合は、少なくとも 1 台の DNS サーバーを追加する必要があります。DNS ループバックを設定するには、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの DNS ループバックの設定（1139 ページ）」を参照してください。

（注） 長いフォーマットで作成された DNS IPv6 サーバーアドレスは、デバイスの再同期後に短縮されたフォーマットに変換されます。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、[デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、**[ネットワーク設定（Network Settings）]** を展開して [DNS] をクリックします。

ステップ 4 [DNS] テーブルで、[追加（Add）] をクリックします。

ステップ 5 [DNSの作成（Create DNS）] スライドインペインで、次の設定を完了します。

a) （任意） VRF を有効にするには、[VRF] チェックボックスをオンにします。

b) VRF を有効にする場合は、[VRF名（VRF Name）] ドロップダウンリストから、VRF を選択します。

（注） VRF が有効になっている場合、Catalyst Center は VRF [なし（None）] をサポートしません。

VRF インターフェイスを作成する場合は、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の VRF インターフェイスの作成 （1134 ページ）」を参照してください。

c) DNS サーバーを設定します。

実行する操作	結果
DNS サーバーの追加	**1.** [Add] をクリックします。 **2.** [DNSサーバーの追加（IPv4/IPv6）（Add DNS Server (IPv4 / IPv6)）] ダイアログボックスの [DNSサーバー（IPv4/IPv6）（DNS Server (IPv4 / IPv6)）] フィールドに、DNS サーバーの有効な IPv4 または IPv6 アドレスを入力します。 **3.** [Save] をクリックします。
DNS サーバーの削除	**1.** 削除する DNS サーバーの横にあるチェックボックスをオンにします。 **2.** [**Actions**] にカーソルを合わせ、[**Delete**] を選択します。 **3.** ダイアログボックスで、**Yes** をクリックします。

ステップ 6 [Review and Provision] をクリックします。

ステップ 7 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

ステップ 8 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の IPv4 DHCP プールの作成

この手順を使用して、ワイヤレスコントローラ の IPv4 DHCP プールを作成し、プロビジョニングします。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。

b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。

c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。

b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[ネットワーク設定（Network Settings）] を展開して [DHCPプール（DHCP Pools）] をクリックします。

ステップ 4 [DHCPプール（DHCP Pools）] にカーソルを合わせ [IPv4] をクリックします。

ステップ 5 [Add] をクリックします。

ステップ 6 [DHCPプールの作成（Create DHCP Pools）] スライドインペインの [一般（General）] タブで、次の設定を完了します。

a) [**DHCP Pool Name**] フィールドに、DHCP プールの一意の名前を入力します。

DHCP プール名には最大 236 文字を使用できます。Catalyst Center は、DHCP プール名で ? またはスペースをサポートしていません。

b) （任意） VRF を有効にするには、[VRF] チェックボックスをオンにします。

VRF を有効にする場合は、[VRF名（VRF Name）] ドロップダウンリストから、 DHCP プールに関連付ける VRF を選択します。

c) [**Network**] フィールドに、有効なネットワーク IP アドレスを入力します。

d) [Subnet Mask] ドロップダウンリストから、サブネットマスクを選択します。

e) [リース（Lease）] ドロップダウンリストから、リースの有効期限に関するオプションを選択します。

[ユーザー定義（User Defined）] オプションを選択した場合は、次のフィールドにデータを入力します。

- [日（Days）]（有効な範囲は 0 ～ 365 です。）
- [時（Hours）]（有効な範囲は 0 ～ 23 です。）
- [分（Minutes）]（有効な範囲は 0 ～ 59 です。）

ステップ 7 （任意） [詳細（Advanced）] タブで、次の設定を完了します。

a) [Domain] フィールドに、ドメイン名を入力します。

Cisco IOS XE リリース 17.15.1 以降を実行しているワイヤレスコントローラの場合、ドメイン名には最大 255 文字を使用できます。Catalyst Center は、ドメイン名で ? またはスペースをサポートしていません。

b) （任意） [デフォルトルータ（Default Router）] で、デフォルトルータを設定します。

実行する操作	結果
デフォルトルータの追加	**1.** [Add] をクリックします。 **2.** [デフォルトルータ追加（Add Default Router(s)）] ダイアログボックスの [デフォルトルータ（Default routers）] フィールドに、デフォルトルータの IP アドレスを入力します。 **3.** [Save] をクリックします。 （注） デフォルトルータは、DHCP プールと同じサブネット内にある必要があります。
デフォルトルータの削除	**1.** 削除するデフォルトルータの横にあるチェックボックスをオンにします。 **2.** [Actions] にカーソルを合わせて [Delete] を選択します。 **3.** ダイアログボックスで、**Yes** をクリックします。

c) （任意） [DNS サーバー（DNS Server）] で、DNS サーバーを設定します。

実行する操作	結果
DNS サーバーの追加	**1.** [Add] をクリックします。 **2.** [DNSサーバーの追加（Add DNS Server）] ダイアログボックスの [DNSサーバーリスト（DNS Server List）] フィールドに、DNS サーバーの IPv4 アドレスを入力します。 **3.** [Save] をクリックします。
DNS サーバーの削除	**1.** 削除する DNS サーバーの横にあるチェックボックスをオンにします。 **2.** **[Actions]** にカーソルを合わせ、**[Delete]** をクリックします。 **3.** ダイアログボックスで、**Yes** をクリックします。

ステップ 8 [Review and Provision] をクリックします。

ステップ 9 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 10 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の IPv6 DHCP プールの作成

この手順を使用して、ワイヤレスコントローラ の IPv6 DHCP プールを作成し、プロビジョニングします。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[ネットワーク設定（Network Settings）] を展開して [DHCPプール（DHCP Pools）] をクリックします。

ステップ 4 [DHCP プール（DHCP Pools）] にカーソルを合わせ [IPv6] をクリックします。

ステップ 5 [Add] をクリックします。

ステップ 6 [**Create DHCP Pools**] スライドインペインの [**DHCP Pool Name**] フィールドに、DHCP プールの一意の名前を入力します。

DHCP プール名には最大 232 文字を使用できます。Catalyst Center では、DHCP プール名に ? またはスペースは使用できません。

ステップ 7 （任意） [ドメイン名（Domain Names）]で、ドメイン名を設定します。

実行する操作	結果
ドメイン名の追加	**1.** [Add] をクリックします。 **2.** [ドメイン名の追加（Add Domain Names）] ダイアログボックスの [ドメイン名（Domain Name）] フィールドに、ドメイン名を入力します。 ドメイン名には最大 225 文字を使用できます。 **3.** [Save] をクリックします。
ドメイン名の削除	**1.** 削除するドメイン名の横にあるチェックボックスをオンにします。 **2.** [Actions] にカーソルを合わせて [Delete] を選択します。 **3.** ダイアログボックスで、**Yes** をクリックします。

ステップ 8 [DNS サーバー（DNS Server）] で、DNS サーバーを設定します。

実行する操作	結果
DNS サーバーの追加	**1.** [Add] をクリックします。 **2.** [ドメイン名の追加（Add Domain Names）] ダイアログボックスの [DNS サーバーリスト（DNS Server List）] フィールドに、DNS サーバーの IPv6 アドレスを入力します。 **3.** [Save] をクリックします。
DNS サーバーの削除	**1.** 削除する DNS サーバーの横にあるチェックボックスをオンにします。 **2.** [Actions] にカーソルを合わせて [Delete] を選択します。 **3.** ダイアログボックスで、**Yes** をクリックします。

ステップ 9 [IPv6アドレスの割り当て（IPV6 Address Allocation）] で、IPv6 アドレスの割り当てを設定します。

実行する操作	結果
IPv6 アドレスの追加	**1.** [Add] をクリックします。 **2.** [IPv6アドレス割り当ての追加（Add IPV6 Address Allocation）] ダイアログボックスの [IPv6アドレス（IPv6 Address）] フィールドに、IPv6 アドレスを入力します。 **3.** [Save] をクリックします。

実行する操作	結果
IPv6 アドレスの削除	1. 削除する IPv6 アドレスの横にあるチェックボックスをオンにします。 2. [Actions] にカーソルを合わせて [Delete] を選択します。 3. ダイアログボックスで、**Yes** をクリックします。

ステップ 10 [Review and Provision] をクリックします。

ステップ 11 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 12 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの DHCP パーシステンスの設定

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの DHCP パーシステンスを設定してその設定をプロビジョニングするには、次の手順を実行します。

始める前に

DHCP プールがすでに作成されていることを確認します。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラのリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、[デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[ネットワーク設定（Network Settings）] を展開して [DHCPプール（DHCP Pools）] をクリックします。

ステップ 4 [DHCPパーシステンス（DHCP Persistence）] タブをクリックします。DHCP パーシステンスを設定するインターフェイスを選択します。

ステップ 5 [アクション（Actions）] にカーソルを合わせて [編集（Edit）] をクリックします。

または、インターフェイス名をクリックします。

ステップ 6 [DHCPパーシステンスの編集（Edit DHCP Persistence）] スライドインペインで、次のパラメータを設定します。

- [インターフェイス（Interface）]：IPアドレスを割り当てる必要があるクライアントインターフェイスを表示します。
- [プール名（Pool Name）]：ドロップダウンリストから DHCP プール名を選択します。デフォルトでは、DHCP プール [なし（None）] が選択されています。

  DHCP プールの作成については、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の IPv4 DHCP プールの作成 （1142 ページ）」と「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の IPv6 DHCP プールの作成 （1144 ページ）」を参照してください。

  （注） DHCP プール名を変更するには、まず DHCP プール [なし（None）] を選択して設定をプロビジョニングします。プロビジョニングが完了したら、必要な DHCP プールを選択します。

- [予約済みIPアドレス（Reserved IP Address）]：予約済み IP アドレスを入力します。

  この IP アドレスを使用することで、これらの IP アドレスが他のデバイスに動的に割り当てられなくなります。

  （注） DHCP プール [なし（None）] を選択すると、このフィールドは無効になります。

ステップ 7 [Review and Provision] をクリックします。

ステップ 8 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

ステップ 9 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の HTTP および HTTPS の設定

次の手順を使用して、ワイヤレスコントローラ の HTTP および HTTPS を設定し、構成をプロビジョニングします。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、[ネットワーク設定（Network Settings）] を展開し、[HTTP/HTTPS] をクリックします。

ステップ 4 対応する設定を有効にするには、必要なチェックボックスをオンにします。

- [HTTPアクセス（HTTP Access）] : HTTP サーバーを有効にします。

  このチェックボックスをオンにする場合は、[HTTP Port] フィールドに HTTP ポート番号を入力します。

  有効な値は、80、または 1024 ～ 65535 までの任意の値です。

  （注） HTTP ポート番号と HTTPS ポート番号は異なるものである必要があります。HTTPS ですでに使用されているポートに切り替えるには、新しいポートをHTTPS用にプロビジョニングしてから、そのポートをHTTPに使用します。

  たとえば、HTTPS がポート 1028 を使用するように設定されていて、HTTP でもポート 1028 を使用したい場合は、最初に HTTPS ポートを別の番号に変更して設定をプロビジョニングしてから、ポート1028をHTTP に割り当てます。

- [HTTPSアクセス（HTTPS Access）] : HTTPS セキュアサーバーを有効にします。

このチェックボックスをオンにする場合は、[**HTTPS Port**] フィールドに HTTPS ポート番号を入力します。

有効な値は、443 、または 1025 ～ 65535 までの任意の値です。



（注） HTTP ポート番号と HTTPS ポート番号は異なるものである必要があります。HTTP ですでに使用されているポートに切り替えるには、新しいポートをHTTP用にプロビジョニングしてから、そのポートをHTTPS用に使用します。

たとえば、HTTP がポート 1026 を使用するように設定されていて、HTTPS でもポート 1026 を使用したい場合は、最初に HTTP ポートを別の番号に変更して設定をプロビジョニングしてから、ポート1026をHTTPS に割り当てます。

- [個人ID検証（Personal Identity Verification）]：個人 ID 検証を有効にします。



（注） ワイヤレスコントローラにトラストポイント、CA サーバー証明書を設定します。クライアント証明書がブラウザ上の CA サーバーによって署名されていることを確認します。そうでない場合、ワイヤレスコントローラ UI にアクセスすることはできません。

個人 ID 検証を有効にする場合、必要に応じて、[個人ID検証承認のみ（Personal Identity Verification Authorization only）] チェックボックスをオンにして、Web UI のみに検証を設定できます。

ステップ 5 [認証（Authentication）] ドロップダウンリストから、認証方式を選択します。

[aaa] を選択した場合、これらのドロップダウンリストから、必要に応じて必要なオプションを選択できます。

- [承認リスト（Authorization List）]（承認方式リストの作成については、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の認証方式リストの作成 （929 ページ）」を参照してください）
- [認証リスト（Authentication List）]（タイプ LOGIN の認証方式リストの作成については、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の認証方式リストの作成 （928 ページ）」を参照してください）

ステップ 6 （任意）[HTTPプロキシ設定（HTTP Proxy Configuration）] で、次の両方のフィールドにデータを入力します。

- [クライアントプロキシサーバー（Client Proxy Server）]：クライアント プロキシ サーバーを入力します。

  IPv4 アドレス、IPv6 アドレス、またはホスト名を入力できます。

- [クライアントプロキシポート（Client Proxy Port）]：クライアントプロキシポートを入力します。

値の範囲は 1 ～ 65535 です。

（注） これらのフィールドのいずれかにデータを入力する場合は、もう一方のフィールドにもデータを入力する必要があります。Catalyst Center は、両方のフィールドを合わせて 215 文字までサポートします。

ステップ 7 [HTTPトラストポイント（HTTP Trustpoint）] で、[トラストポイントの有効化（Enable TrustPoint）] トグルボタンを使用して、HTTP トラストポイントを有効または無効にします。

HTTP トラストポイントを有効にする場合、[セキュアなトラストポイント（Secure Trustpoint）] ドロップダウンリストから、セキュアなサーバー証明書トラストポイントを選択します。

（注） HTTP インターフェイスでセキュアトラストポイントの設定を変更すると、ワイヤレスコントローラ UI へのアクセスが中断され、管理機能に影響を与える可能性があります。

ステップ 8 [タイムアウトポリシー（Timeout Policy）] で、次のフィールドにデータを入力します。

- [HTTPタイムアウトポリシー（秒）（HTTP Timeout-policy (secs)）]：HTTP サーバー接続のアイドルタイムアウトを秒単位で入力します。

  有効な範囲は 1 ～ 600 です。
- [セッション アイドル タイムアウト（秒）（Session Idle Timeout (secs)）]：HTTP サーバーセッションのアイドルタイムアウトを秒単位で入力します。

  有効な範囲は 180 ～ 1200 です。
- [サーバーライフタイム（秒）（Server Life Time (secs)）]：HTTP サーバー接続の有効期間を秒単位で入力します。

  有効な範囲は 1 ～ 86400 です。
- [最大リクエスト数（Max number of requests）]：HTTP サーバー接続で許可されるリクエストの最大数を入力します。

  有効な範囲は 1 ～ 86400 です。

ステップ 9 [Review and Provision] をクリックします。

ステップ 10 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 11 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の一般的な SNMP パラメータの設定

ワイヤレスコントローラ の一般的な SNMP パラメータを設定し、その設定をプロビジョニングするには、次の手順を実行します。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[ネットワーク設定（Network Settings）] を展開して [SNMP] をクリックします。

ステップ 4 （任意） [一般（General）] タブの次のフィールドにデータを入力します。

- [システムの場所（System Location）] : デバイスの場所を入力します。

  システムの場所には最大 234 文字を含めることができます。 Catalyst Center では、システムの場所に ? は使用できません。

- [システム連絡先（System Contact）] : デバイス管理者の連絡先の詳細を入力します。

  連絡先の詳細には最大 235 文字を含めることができます。Catalyst Center では、連絡先の詳細に ? は使用できません。

ステップ 5 [Review and Provision] をクリックします。

ステップ 6 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

ステップ 7 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の SNMP ワイヤレストラップの設定

次の手順を使用して、ワイヤレスコントローラのSNMPワイヤレストラップを設定し、構成をプロビジョニングします。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラのリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、[デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[ネットワーク設定（Network Settings）] を展開して [SNMP] をクリックします。

ステップ 4 [Wireless Traps] タブをクリックします。

ステップ 5 各エリアの下にある [有効（Enable）] トグルボタンを使用して、対応するトラップを有効または無効にします。

- **汎用コントローラ**
- [メッシュ（Mesh）]
- **RF**
- **Rogue**
- **RRM**
- **Wireless Client**
- **ワイヤレスモビリティ**

ステップ 6 [Review and Provision] をクリックします。

ステップ 7 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

ステップ 8 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の SNMP コミュニティ文字列の追加

SNMPコミュニティ文字列は、管理対象デバイスへのアクセスを認証するために使用されるパスワードです。デバイス検出にも使用できます。

（注） デバイス検出に使用される SNMP コミュニティ文字列が削除されると、デバイスは Catalyst Center で管理対象外状態になります。

この手順を使用して、ワイヤレスコントローラ の SNMP コミュニティ文字列を追加し、プロビジョニングします。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[ネットワーク設定（Network Settings）] を展開して [SNMP] をクリックします。

ステップ 4 [コミュニティストリング（Community Strings）] タブをクリックします。

ステップ 5 [Add] をクリックします。

ステップ 6 [コミュニティ文字列の追加（Add Community String）] スライドインペインの [コミュニティ名（Community Name）] フィールドに、SNMP コミュニティ文字列を入力します。

SNMP コミュニティ文字列は、管理対象デバイスへのアクセスを認証するためのパスワードです。文字列には最大 128 文字を含めることができます。Catalyst Center は、文字列内の？、バックスラッシュ（\）、およびスペースをサポートしていません。

ステップ 7 [アクセスモード（Access Mode）] ドロップダウンリストから、SNMP 管理ステーションがデバイスから情報を取得できるモードを選択します。

- [読み取り専用（Read Only）]：ネットワークデバイスから情報を表示または取得します。
- [読み取り/書き込み（Read/Write）]：情報を表示し、デバイス設定と構成を変更します。

ステップ 8 [Review and Provision] をクリックします。

ステップ 9 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 10 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの SNMPv3 ユーザーグループの作成

ワイヤレスコントローラ の SNMPv3 ユーザーグループを作成して設定をプロビジョニングするには、次の手順を実行します。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[ネットワーク設定（Network Settings）] を展開して [SNMP] をクリックします。

ステップ 4 [V3ユーザーグループ（V3 User Groups）] タブをクリックします。

ステップ 5 [Add] をクリックします。

ステップ 6 [V3ユーザーグループの作成（Create V3 User Groups）] スライドインペインの [グループ名（Group Name）] フィールドに、SNMPv3 ユーザーグループの一意の名前を入力します。

ユーザーグループ名には最大 32 文字を含めることができます。

ステップ 7 [セキュリティレベル（Security Level）] で、ユーザーグループのセキュリティのレベルを設定します。

実行する操作	結果
セキュリティレベルを追加する	**1.** [Add] をクリックします。 **2.** [セキュリティレベルの追加（Add Security Level）] ダイアログボックスの [セキュリティレベル（Security Level）] ドロップダウンリストから、セキュリティレベルを選択します。 • [AUTH]：メッセージは認証されますが、暗号化されません。 • [NOAUTH]：セキュリティは適用されません。 • [PRIV]：メッセージは認証され、暗号化されます。 （注） セキュリティレベルタイプは、ユーザーグループ内で一意である必要があります。 **3.** （オプション）[読み取りビュー（Read View）] フィールドで、グループの読み取りビューを指定します。 **4.** （オプション）[書き込みビュー（Write View）] フィールドで、グループの書き込みビューを指定します。
セキュリティレベルを編集する	**1.** セキュリティレベルのチェックボックスをオンにします。 **2.** [Actions] にカーソルを合わせて [Edit] を選択します。 **3.** 必要な設定を更新します。 **4.** [Save] をクリックします。
セキュリティレベルを削除する	**1.** 削除するセキュリティレベルのチェックボックスをオンにします。 **2.** [Actions] にカーソルを合わせて [Delete] を選択します。 **3.** ダイアログボックスで、**Yes** をクリックします。

ステップ 8 [Review and Provision] をクリックします。

ステップ 9 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 10 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの SNMPv3 ユーザーの作成

ワイヤレスコントローラの SNMPv3 ユーザーを作成してプロビジョニングするには、次の手順を実行します。SNMPv3 は、認証とプライバシーをサポートすることにより、ネットワーク管理のセキュリティを強化します。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラのリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、[デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[ネットワーク設定（Network Settings）] を展開して [SNMP] をクリックします。

ステップ 4 [V3ユーザー（V3 Users）] タブをクリックします。

ステップ 5 [Add] をクリックします。

ステップ 6 [V3ユーザーグループの作成（Create V3 User Groups）] スライドインペインで、次の設定を完了します。

a) [ユーザー名（Username）] フィールドに、SNMPv3 ユーザーの一意の名前を入力します。

ユーザーグループ名には最大 32 文字を含めることができます。

b) [グループ名（Group Name）] ドロップダウンリストから、SNMPv3 ユーザーグループを選択します。

SNMPv3 ユーザーグループの作成については、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの SNMPv3 ユーザーグループの作成 （1154 ページ）」を参照してください。

c) [セキュリティモード（Security Mode）] ドロップダウンリストから、認証とプライバシーのセキュリティレベルを選択します。

次を選択できます。	下記を実行
AuthPriv	• [プライバシープロトコル（Privacy Protocol）] ドロップダウンリストから、データ暗号化のプロトコルを選択します。 • [プライバシー暗号化（Privacy Encryption）] ドロップダウンリストから、プライバシーパスワードの暗号化方式を選択します。 （注） 暗号化タイプ [6] または [7] を使用するには、デバイスがプレーンテキストのパスワードを受け入れるか、事前暗号化されたパスワードを提供するように設定されていることを確認します。それ以外の場合は、暗号化タイプ [0] を選択します。 • [プライバシーパスワード（Privacy Password）] フィールドに、プライバシーパスワードを入力します。
[AuthPriv] または [AuthNoPriv]	• [認証プロトコル（Authentication Protocol）] ドロップダウンリストから、認証のプロトコルを選択します。 [SHA2] を選択した場合は、[認証アルゴリズム（Authentication Algorithm）] ドロップダウンリストから SHA-2 認証アルゴリズムのビット長を選択します。 • [認証暗号化（Authentication Encryption）] ドロップダウンリストから、認証パスワードの暗号化方式を選択します。 （注） 暗号化タイプ [6] または [7] を使用するには、デバイスがプレーンテキストのパスワードを受け入れるか、事前暗号化されたパスワードを提供するように設定されていることを確認します。それ以外の場合は、暗号化タイプ [0] を選択します。 • [認証パスワード（Authentication Password）] フィールドに、認証パスワードを入力します。 • （オプション）[ACL IPv6] ドロップダウンリストから、IPv6 ACL を選択します。 IPv6 ACL の作成については、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の IPv6 ACL の作成 （949 ページ）」を参照してください。

次を選択できます。	下記を実行
[AuthPriv]、[AuthNoPriv]、または [NoAuthNoPriv]	（オプション）[ACL IPv4] ドロップダウンリストから、IPv4 ACL を選択します。 IPv4 ACL の作成については、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の IPv4 ACL の作成 （940 ページ）を参照してください。

ステップ 7 [Review and Provision] をクリックします。

ステップ 8 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

ステップ 9 [Tasks] ウィンドウで、タスクの展開を監視します。

[V3ユーザー（V3 Users）]テーブルには、暗号化されたパスワードを持つSNMPv3ユーザーのみが表示されます。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の SNMP ホストの作成

この手順を使用して、ワイヤレスコントローラ の SNMP ホストを作成し、プロビジョニングします 。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[ネットワーク設定（Network Settings）] を展開して [SNMP] をクリックします。

ステップ 4 [ホスト（Hosts）] タブをクリックします。

ステップ 5 [Add] をクリックします。

ステップ 6 [IPアドレス（IP Address）] フィールドの [SNMPホストの作成（Create SNMP Host）] スライドインペイン に、ホストの IP アドレスを入力します。

ステップ 7 [バージョン（Version）] ドロップダウンリストから、トラップを送信する SNMP バージョンを選択します。

次を選択できます。	下記を実行
V1 または V2C	[コミュニティ文字列（Community String）] ドロップダウンリストから、SNMP コミュニティ文字列を選択します。 コミュニティ文字列を追加するには、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の SNMP コミュニティ文字列の追加（1153 ページ）」を参照してください。
[V3]	次の設定を完了します。 • [V3ユーザー（V3 User）] フィールドに、SNMPv3 認証および暗号化用のユーザー名を入力します。 • [セキュリティレベル（Security Level）] のドロップダウンリストから、セキュリティレベルを選択します。

ステップ 8 （任意） [UDPポート（UDP Port）] フィールドに、SNMP 宛て先ポートの番号を入力します。

有効な範囲は 0 ～ 65535 です。デフォルト値は 162 です。

ステップ 9 [タイプ（Type）] のドロップダウンリストから、SNMP 通知のタイプを選択します。

- [トラップ（traps）]：SNMP 通知の受信確認はありません。
- [インフォーム（informs）]：SNMP 通知の受信確認があります。

ステップ 10 [Review and Provision] をクリックします。

ステップ 11 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 12 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の NTP サーバープロファイルの作成

この手順を使用して、ワイヤレスコントローラ の Network Time Protocol（NTP）サーバープロファイルを作成し、プロビジョニングします。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[ネットワーク設定（Network Settings）] を展開し、[NTP] をクリックします。

ステップ 4 [NTP] タブで [Add] をクリックします。

ステップ 5 [NTPサーバープロファイルの作成（Create NTP Server ProfileCreate NTP Server Profile）] スライドインペインの ホスト名フィールドに、[ホスト名（Host Name）] を入力します。

IPv4 アドレス、IPv6 アドレス、または完全修飾ドメイン名（FQDN）を入力できます。

ステップ 6 （任意） この NTP サーバープロファイルをデフォルトで使用するには、[優先（Prefer）] チェックボックスをオンにします。

ステップ 7 [DNS解決用のIP（IP for DNS Resolution）] ドロップダウンリストから、ドメイン名システム（DNS）解決に使用する IP アドレスのタイプを選択します。

ステップ 8 [送信元アドレス（Source Address）] ドロップダウンリストから、NTP サーバーとの通信に使用するインターフェイスを選択します。

選択内容	結果
VLAN	[VLAN] ドロップダウンリストから、NTP サーバーと通信する VLAN を選択します。
Interface	[インターフェイス（Interface）] ドロップダウンリストから、NTP サーバーとの通信に使用するインターフェイスを選択します。

ステップ 9 （任意） [認証の有効化（Enable Authentication）] チェックボックスをオンにして、NTP サーバーに対する認証を有効にします。

このチェックボックスをオンにする場合は、[Key] ドロップダウンリストから、認証に使用するキーインデックスを選択します。

認証キープロファイルの作成については、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の認証キープロファイルの作成 （1161 ページ）を参照してください。

ステップ 10 （任意） [VRF] チェックボックスをオンにして、VRF ごとに NTP サーバーを設定し、隔離されたルーティングドメイン内で正確に時刻同期されるようにします。これにより、特定のセグメントのネットワーク信頼性とイベントロギングが向上します。

このチェックボックスをオンにした場合は、DNS 解決用に選択した IP アドレスオプションに基づいて、対応するドロップダウンリストから VRF インターフェイスを選択します。VRF を作成するには、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の VRF インターフェイスの作成 （1134 ページ）を参照してください。

ステップ 11 [Review and Provision] をクリックします。

ステップ 12 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

ステップ 13 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の認証キープロファイルの作成

この手順を使用して、ワイヤレスコントローラ の NTP サーバーに対する認証用の認証キープロファイルを作成し、プロビジョニングします。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。

b) デバイス情報を含むダイアログボックスで、[デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[ネットワーク設定（Network Settings）] を展開し、[NTP] をクリックします。

ステップ 4 [Authentication Keys] タブをクリックします。

ステップ 5 [Add] をクリックします。

ステップ 6 [認証キーの作成（Create Authentication Key）] スライドインペイン の [認証キー番号（Authentication Key Number）] フィールドに、一意の認証キー番号を入力します。

有効な範囲は 1 ～ 4294967295 です。

ステップ 7 [認証キー（Authentication Key）] フィールドに、MD5 認証用の認証キーを入力します。

認証キーは最大 32 文字です。Catalyst Center は ? とスペースを認証キーでサポートしていません。

ステップ 8 [Review and Provision] をクリックします。

ステップ 9 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 10 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のレイヤ 3 の設定

このセクションでは、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ におけるデバイスごとのレイヤ 3 設定に関する情報を示します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のスタティックルートの作成

この手順を使用して、ワイヤレスコントローラのスタティックルートを作成し、プロビジョニングします。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。

b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラのリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[レイヤ3（Layer 3）] を展開し、[ルーティング（Routing）] をクリックします。

ステップ 4 [静的（Static）] タブで、カーソルを [追加（Add）] に移動し、必要なスタティック ルート オプションを選択します。

ステップ 5 [IPv4] を選択した場合、[スタティックルートの作成（Create Static Route）] スライドインペインで 、次の設定を行います。

a) [プレフィック（Prefix）] フィールドに、スタティックルートのプレフィックスを入力します。
b) [プレフィックスマスク（Prefix Mask）] フィールドに、スタティックルート プレフィックスマスクを入力します。
c) （任意） [VRF] チェックボックスをオンにして Virtual Routing and Forwarding (VRF) を有効にします。

このチェックボックスをオンにした場合、[VRF名（VRF Name）] ドロップダウンリストから VRF を選択します。VRF を作成するには、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の VRF インターフェイスの作成 （1134 ページ）」を参照してください。

d) （任意）[DHCP] チェックボックスをオンにして、DHCP からデフォルトゲートウェイを取得します。

このチェックボックスをオンにする場合は、[メトリック（Metric）] フィールドに値を入力します。

有効な範囲は 1 ～ 255 です。デフォルト値は 1 です。

e) （任意） [ルートパスリスト（Route Path List）] で、ルートパスリストを設定します。

実行する操作	結果
ルートパスリストの追加	**1.** [Add] をクリックします。 **2.** [ルートパスリストの追加（Add Route Path List）] ダイアログボックスの [ルートパス（Route Path）] ドロップダウンリストから、ルートパスを選択します。 [インターフェイス（Interface）] を選択した場合、[インターフェイス（Interface）] ドロップダウンリストからインターフェイスを選択します。 **3.** [ネクストホップIP（Next Hop IP）] フィールドに次のホップの IP アドレスを入力します。 [インターフェイス（Interface）] を選択した場合、このフィールドは任意です。 **4.** [メトリック（Metric）] フィールドに、値を入力します。 有効な範囲は 1 ～ 255 です。デフォルト値は 1 です。 **5.** **[保存（Save）]** をクリックします。
ルートパスリストの削除	**1.** 必要なルートパスの横にあるチェックボックスをオンにします。 **2.** [Actions] にカーソルを合わせて [Delete] を選択します。 **3.** ダイアログボックスで、**Yes** をクリックします。

ステップ 6 [IPv6] を選択した場合、[スタティックルートの作成（Create Static Route）] スライドインペインで 、次の設定を行います。

a) [プレフィック（Prefix）] フィールドに、スタティックルートの IPv6 プレフィックスを入力します。

b) [プレフィックス長（Prefix Length）] フィールドにプレフィックス長を入力します。

c) （任意） [VRF] チェックボックスをオンにして Virtual Routing and Forwarding (VRF) を有効にします。

このチェックボックスをオンにした場合、[VRF名（VRF Name）] ドロップダウンリストから VRF を選択します。VRF を作成するには、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の VRF インターフェイスの作成 （1134 ページ）」を参照してください。

d) （任意） [ルートパスリスト（Route Path List）] で、ルートパスリストを設定します。

実行する操作	結果
ルートパスリストの追加	**1.** [Add] をクリックします。 **2.** [ルートパスリストの追加（Add Route Path List）] ダイアログボックスの [ルートパス（Route Path）] ドロップダウンリストから、ルートパスを選択します。 [インターフェイス（Interface）] を選択した場合、[インターフェイス（Interface）] ドロップダウンリストからインターフェイスを選択します。 **3.** [ネクストホップIP（Next Hop IP）] フィールドに次のホップの IP アドレスを入力します。 [インターフェイス（Interface）] を選択した場合、このフィールドは任意です。 **4.** （オプション） [アドミニストレーティブディスタンス（Administrative Distance）] フィールドに値を入力します。 有効な範囲は 1 ～ 254 です。デフォルト値は 1 です。 **5.** **[保存（Save）]** をクリックします。
ルートパスリストの削除	**1.** 必要なルートパスの横にあるチェックボックスをオンにします。 **2.** [Actions] にカーソルを合わせて [Delete] を選択します。 **3.** ダイアログボックスで、**Yes** をクリックします。

ステップ 7 [Review and Provision] をクリックします。

ステップ 8 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

ステップ 9 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の管理設定

このセクションでは、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のデバイスごとの管理設定について説明します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のデバイス管理設定の構成

ワイヤレスコントローラ のデバイス管理設定を構成し、その設定をプロビジョニングするには、次の手順を実行します。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、[デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、で、[管理（Administration）] を展開して [デバイス（Device）] をクリックします。

ステップ 4 [一般（General）] タブで、次の設定を完了します。

- [IPルーティング（IP Routing）] トグルボタンを使用して、IP ルーティングを有効または無効にします。
- [Host Name] フィールドにホスト名を入力します。

  ホスト名に使用できるのは、大文字と小文字、数字、ハイフン（-）、下線（_）、ピリオド（.）です。ホスト名に数字のみを含めることはできません。
- （オプション）[バナー（Banner）] フィールドに、必要なデータを入力します。

ステップ 5 [Review and Provision] をクリックします。

ステップ 6 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

ステップ 7 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のデバイス FTP/SFTP/TFTP 設定

ネットワークでは、次のいずれかの転送プロトコルを設定することにより、デバイス間でファイルをセキュアに転送できます。

- File Transfer Protocol（FTP）：ネットワークを介してクライアントとサーバー間でファイルを転送するために使用されます。
- Secure File Transfer Protocol（SFTP）：暗号化されたファイル転送にセキュアシェル（SSH）を使用します。
- Trivial File Transfer Protocol（TFTP）：ファイルを転送するためのよりシンプルで軽量なプロトコルで、多くの場合、ネットワークの起動やファームウェアのアップグレードに使用されます。

この手順を使用して、ワイヤレスコントローラのFTP、SFTP、およびTFTPを設定し、設定をプロビジョニングします。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラ のリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、 [デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[管理（Administration）] を展開して [デバイス（Device）] をクリックします。

ステップ 4 [FTP/SFTP/TFTP] タブをクリックします。

ステップ 5 [FTP設定（FTP Settings）] で、次の設定を完了します。

- [送信元インターフェイス（Source Interface）] ドロップダウンリストからインターフェイスを選択します。
- [ユーザー名（Username）]：FTP 接続のユーザー名を入力します。

  ユーザー名は最大 237 文字です。Catalyst Center では、? とスペースをユーザー名に含めることはできません。

- [パスワード（Username）]：FTP 接続のパスワードを入力します。

  パスワードは25 文字以内で指定できます。少なくとも 1 つの英数字を含める必要があります。Catalyst Center では、? をパスワードに含めることはできませ n。

ステップ 6 [SFTP設定（SFTP Settings）] で、[送信元インターフェイス（Source Interface）] ドロップダウンリストからインターフェイスを選択します。

ステップ 7 [TFTP設定（TFTP Settings）] で、[送信元インターフェイス（Source Interface）] ドロップダウンリストからインターフェイスを選択します。

ステップ 8 [Review and Provision] をクリックします。

ステップ 9 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 10 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のユーザー管理設定を設定します。

次の手順を使用して、ワイヤレスコントローラ のユーザー管理設定を設定し、設定をプロビジョニングします。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラのリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、[デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[管理（Administration）] を展開し、[ユーザー管理（User Administration）] をクリックします。

ステップ 4 [Add] をクリックします。

ステップ 5 [ユーザー管理の作成（Create User Administration）] スライドインペインでは、パラメータを設定してユーザーロールと権限を定義します。

a) [**User Name**]：新しいアカウントの一意のユーザー名を入力します。

名前には最大 64 文字を使用できます。Catalyst Center は、ユーザー名で ? をサポートしていません。

b) [ポリシー（Policy）]：ドロップダウンリストからパスワードポリシーを選択します。このポリシーはユーザーに関連付けられています。

c) [詳細モード（Advanced Mode）]：このオプションを切り替えて、権限レベルを詳細モードに切り替えます。

d) [権限（Privilege）]：モードに基づいてユーザー権限レベルを選択します。[詳細（Advanced）] モードを有効にしていない場合、権限は基本モードに設定されます。

e) 基本モードを選択した場合、次の権限オプションを使用できます。

- [管理者（Admin）]：ユーザーは GUI のすべてのセクションにアクセスできます。
- [読み取り専用（Read Only）]：ユーザーはダッシュボードとモニタリングセクションにのみアクセスできます。
- [アクセスなし（No Access）]：ユーザーは GUI にアクセスできません。
- [ロビー管理者（Lobby Admin）]：ゲストユーザーアカウントのみを作成できるユーザー。

（注） ロビー管理者から別のロールに権限を変更する場合、または別のロールからロビー管理者に権限を変更する場合、既存のエントリを削除し、必要な権限を持つ新しいエントリを追加します。

f) 詳細モードを選択した場合は、権限レベルを 0 ～ 15 から選択します。

- 権限 15 は管理者ユーザーです。
- 権限 1 ～ 14 は読み取り専用ユーザーと見なされます。
- 権限 0 はアクセスできません。

g) [パスワード（Password）]：ユーザーアカウントのパスワードを入力し、確認のために [パスワードの確認（Confirm Password）] フィールドに再入力します。

パスワードには最大 127 文字を使用できます。[**Confirm Password**] フィールドのパスワードが、[**Password**] フィールドのパスワードと一致している必要があります。

ステップ 6 [Review and Provision] をクリックします。

ステップ 7 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。

- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 8 [Tasks] ウィンドウで、タスクの展開を監視します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の AP アップグレード設定をします。

この手順を使用して、ワイヤレスコントローラ の APアップグレード設定をし、プロビジョニングします。

手順

ステップ 1 インベントリで必要な ワイヤレスコントローラ に移動します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
b) 左上の [グローバル（Global）] をクリックし、必要なエリア、建物、またはフロアを選択します。
c) [Wireless Controllers] デバイスファミリーボタンをクリックして、使用可能な ワイヤレスコントローラのリストを表示します。

ステップ 2 必要な ワイヤレスコントローラ のデバイスの詳細ウィンドウを開きます。

a) デバイス名をクリックします。
b) デバイス情報を含むダイアログボックスで、[デバイスの詳細の表示（View Device Details）] をクリックしてデバイスの詳細ウィンドウを開きます。

ステップ 3 [設定（Configuration）] タブで、、[管理（Administration）] を展開し、[AP アップグレード設定（AP Upgrade Configuration）] をクリックします。

ステップ 4 [反復あたりのアップグレードするAPの割合（AP Upgrade Percentage per Iteration）] ドロップダウンリストから、反復あたりの AP アップグレードの割合または AP アップグレードモードに必要なオプションを選択します。

次のオプションを使用できます。

- [段階的なアップグレード（Staggered upgrade）]：選択した割合に基づいて、ワイヤレスコントローラに関連付けられた AP を分割してアップグレードします。
- [ワンタイムアップグレード（One-time upgrade）]：ワイヤレスコントローラに関連付けられたすべての A Pを一度にアップグレードします。
- [シリアルアップグレード（Serial upgrade）]：ワイヤレスコントローラに関連付けられた AP を 1 つずつアップグレードします。

ワイヤレスコントローラに関連付けられた AP の、段階的なアップグレードの割合、ワンタイムアップグレード、またはシリアルアップグレードを選択できます。

ステップ 5 次のチェックボックスを使用して、対応する設定を有効または無効にします。

- [クライアントステアリング（Client Steering）]：アップグレード中は、クライアントをAPから遠ざけます。
- [クライアントの認証解除（Client Deauthentication）]：アップグレード中にAPに接続されていたクライアントをリロードする前に認証解除します。

ステップ6 [Review and Provision] をクリックします。

ステップ7 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

ステップ8 [Tasks] ウィンドウで、タスクの展開を監視します。

リリース間コントローラモビリティの概要

リリース間コントローラモビリティ（IRCM）は、異なるソフトウェアバージョンのさまざまなシスコ ワイヤレス コントローラ で実行されるシームレスなモビリティとワイヤレスサービスをサポートします。

Catalyst Center は、次のデバイスの組み合わせでゲストアンカー機能をサポートしています。

- アンカーコントローラとしてのCisco AireOS コントローラとフォーリンコントローラとしての Cisco AireOS コントローラの設定。
- フォーリンコントローラとしての Cisco Catalyst 9800 シリーズ ワイヤレス コントローラとゲストアンカーコントローラとしての Cisco AireOS コントローラの設定。
- アンカーコントローラとしての Cisco Catalyst 9800 シリーズ ワイヤレス コントローラとフォーリンコントローラとしての Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの設定。

コントローラデバイスでの IRCM の設定には、次のような制限事項があります。

- フォーリンコントローラとしてのCisco AireOS コントローラの設定、およびアンカーコントローラとしての Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの設定はサポートされていません。
- ファブリックゲストアンカーの設定はサポートされていません。
- ゲスト SSID のみがサポートされています。

- ゲストアンカーモードでの非ゲストアンカー SSID のブロードキャストはサポートされていません。

ゲストアンカーの設定とプロビジョニングプロセス

ゲストアンカー シスコ ワイヤレス コントローラを設定するには、次の手順を実行します。

手順

ステップ 1 サイト、ビルディング、フロアなどのネットワーク階層を設計します。詳細については、サイトの作成、編集、削除（285 ページ）およびビルディングの追加、編集、および削除（286 ページ）を参照してください。

ステップ 2 AAA、DHCP、DNS サーバーなどのネットワーク サーバーを設定します。詳細については、グローバル ネットワーク サーバーの設定（377 ページ）およびCisco ISE またはその他の AAA サーバーの追加（375 ページ）を参照してください。

ステップ 3 Cisco Identity Services Engine を設定し、外部 Web 認証と中央 Web 認証を使用してゲスト ワイヤレス ネットワークの SSID を作成します。詳細については、「ゲスト ワイヤレス ネットワークの SSID の作成（432 ページ）」を参照してください。

ステップ 4 Cisco Discovery Protocol（CDP）または IP アドレス範囲を使用してワイヤレスコントローラを検出し、そのデバイスが **[Devices]** > **[Inventory]** ウィンドウに [Managed] 状態で表示されていることを確認します。詳細については、「検出の概要（73 ページ）」を参照してください。

ステップ 5 アクティブなメイン ワイヤレスコントローラ として外部 ワイヤレスコントローラ をプロビジョニングします。「Cisco AireOS コントローラのプロビジョニング（738 ページ）」を参照してください。

（注） 外部ワイヤレスコントローラのプロビジョニング時に複数のネットワークプロファイルを持つサイトを選択する場合は、ネットワークプロファイルのアンカーグループの総数が 3 以下であることを確認してください。

ステップ 6 ゲスト アンカーとして ワイヤレスコントローラ のロールを選択し、ゲスト アンカー コントローラをプロビジョニングします。詳細については、「Cisco AireOS コントローラのプロビジョニング（738 ページ）」を参照してください。

（注）
- SSID に指定されているように、アンカー ワイヤレスコントローラの管理対象 AP の場所と同じサイトを選択する必要があります。
- アンカー ワイヤレスコントローラのインターフェイス構成を変更した場合は、再プロビジョニングする必要があります。

ステップ 7 CLI、SNMP、HTTP、HTTPS などのデバイス クレデンシャルを設定します。詳細については、グローバル CLI クレデンシャルの追加 （379 ページ）、グローバル SNMPv2c ログイン情報の追加 （380 ページ）、グローバル SNMPv3 ログイン情報の追加 （382 ページ）、およびグローバル HTTPS ログイン情報の追加 （385 ページ）を参照してください。

シスコのコントローラデバイスで IRCM を設定するための前提条件

- Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ および Cisco AireOS コントローラを検出します。

  Catalyst 9800 シリーズ ワイヤレス コントローラを検出するには、NETCONF を有効にしてポートを 830 に設定する必要があります。NETCONF は、ネットワークデバイスの構成をインストール、操作、削除するメカニズムです。

  詳細については、CDP を使用したネットワークの検出 （86 ページ）またはIP アドレス範囲または CIDR を使用したネットワークの検出 （90 ページ）を参照してください。

- サイト、ビルディング、フロアを追加してネットワーク階層を設計すると、後で設計の設定や構成を適用する場所を簡単に特定できるようになります。

  新しいネットワーク階層を作成するには、サイトの作成、編集、削除 （285 ページ）およびビルディングの追加、編集、および削除 （286 ページ）を参照してください。

- AP の位置情報を追加し、フロアマップに配置して、ヒートマップカバレッジを可視化します。

  詳細については、「フロアマップでの AP の取り扱い （304 ページ）」を参照してください。

- AAA（Cisco ISE がネットワークとクライアントエンドポイント向けに設定されている）、NetFlow コレクタ、NTP、DHCP、DNS、syslog、SNMP トラップなどのネットワーク設定を定義します。これらのネットワークサーバーが、ネットワーク全体のデフォルトになります。AAA サーバーを追加するときに、TACACS サーバーを追加できます。

  詳細については、ネットワーク設定の概要 （373 ページ）、グローバル ネットワーク サーバーの設定 （377 ページ）、および「AAA サーバーの追加」を参照してください。

- ゲスト ワイヤレス ネットワークの SSID を作成します。

  詳細については、「ゲスト ワイヤレス ネットワークの SSID の作成 （432 ページ）」を参照してください。

- フォーリンコントローラとアンカーコントローラの WLAN プロファイル名は、モビリティに対して同じにする必要があります。

Cisco AireOS コントローラおよび Cisco Catalyst 9800 シリーズ ワイヤレス コントローラでの IRCM の設定

始める前に

IRCM を設定するための前提条件が満たされていることを確認します。詳細については、シスコのコントローラデバイスで IRCM を設定するための前提条件（1173 ページ）を参照してください。

手順

ステップ 1 メインメニューから次を選択します。**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。

[インベントリ（Inventory）] ウィンドウが表示され、検出されたデバイスが一覧表示されます。

ステップ 2 フォーリンコントローラとしてプロビジョニングする Catalyst 9800 シリーズ ワイヤレス コントローラの横にあるチェックボックスをオンにします。

ステップ 3 [Actions] ドロップダウンリストから、**[Provision]** > **[Provision]** を選択します。

ステップ 4 [Assign Site] ウィンドウで、[Choose a Site] をクリックして Catalyst 9800 シリーズ ワイヤレス コントローラ デバイスにサイトを割り当てます。

ステップ 5 [Add Sites] ウィンドウで、サイト名の横にあるチェックボックスをオンにして Catalyst 9800 シリーズ ワイヤレス コントローラ を関連付けます。

ステップ 6 **[Save]** をクリックします。

ステップ 7 [Apply] をクリックします。

ステップ 8 [Next] をクリックします。

ステップ 9 Catalyst 9800 シリーズ ワイヤレス コントローラ のロールを [Active Main WLC] として選択します。

ステップ 10 アクティブなメイン ワイヤレスコントローラ では、インターフェイスと VLAN の詳細を設定する必要があります。

ステップ 11 [インターフェイスの割り当て（Assign Interface）] エリアで、次の操作を実行します。

a) [VLAN ID]：VLAN ID の値を入力します。
b) [IP Address]：インターフェイス IP アドレスを入力します。
c) [Gateway IP Address]：ゲートウェイ IP アドレスを入力します。
d) [Subnet Mask (in bits)]：インターフェイスのネットマスクの詳細を入力します。

（注） Catalyst 9800 シリーズ ワイヤレス コントローラ では、IP アドレス、ゲートウェイ IP アドレス、およびサブネットマスクを割り当てる必要はありません。

ステップ 12 [Next] をクリックします。

ステップ 13 [Summary] ウィンドウで、設定を確認します。

ステップ 14 [Deploy] をクリックし、Catalyst 9800 シリーズ ワイヤレス コントローラ をフォーリンコントローラとしてプロビジョニングします。

ステップ 15 **[Devices]** > **[Inventory]** ウィンドウで、ゲストアンカーコントローラとしてプロビジョニングする Cisco AireOS コントローラの横にあるチェックボックスをオンにします。

ステップ 16 手順 3 ～ 8 を繰り返します。

ステップ 17 Cisco AireOS コントローラのロールを [Guest Anchor] として選択します。

ステップ 18 ゲスト アンカー ワイヤレスコントローラの場合は、インターフェイスと VLAN の詳細を設定する必要があります。

ステップ 19 手順 11 ～ 14 を繰り返します。

Merakiデバイスをプロビジョニングするための前提条件

- Meraki ダッシュボードを Catalyst Center と統合します。Cisco Meraki ダッシュボードの統合 （180 ページ）を参照してください。
- SSID を作成します。エンタープライズ ワイヤレス ネットワーク用 SSID の作成 （415 ページ）を参照してください。

（注） Cisco Meraki ダッシュボードは、次の種類の SSID をサポートしています。

- [Open]：この SSID は、Meraki ダッシュボードの [Open] に対応しています。
- [WPA2 Personal]：この SSID は、Meraki ダッシュボードの [preshared key with WAP2] に対応しています。
- [WPA2 Enterprise]：この SSID は、Cisco Meraki ダッシュボードの Meraki 認証またはマイ Radius サーバーを使用した WAP-2 暗号化に対応しています。Catalyst Center における建物レベルのクライアントおよびエンドポイントの認証用に AAA サーバーまたは Cisco ISE サーバーを定義している場合は、その設定が Meraki ダッシュボードの [my Radius server] にプロビジョニングされます。それ以外の場合は、Merakiデバイスによる認証に [Meraki Radius] が使用されます。

すべての SSID に対して、インターフェイス名を選択できます。Catalyst Center で [Management] インターフェイスを選択した場合、VLAN ID は 0 です。つまり、Cisco Meraki ダッシュボードではサポートされないため、Cisco Meraki ダッシュボードでは VLAN タギングは無効になります。Catalyst Center で SSID のカスタムインターフェイスを作成すると、Cisco Meraki ダッシュボードで、カスタムインターフェイス名と VLAN ID を使用して AP タグが作成されます。

- ネットワークプロファイルを作成し、SSID がプロビジョニングされるサイトに割り当てます。

（注） Catalyst Center のネットワーク階層 **[Sites]** > **[Buildings]** は、Meraki ダッシュボードの **[Organization]** > **[Network]** に対応しています。ワークフローの [Add Sites to Profile] ウィンドウで、[Buildings] を選択することをお勧めします。

（注） Catalyst Center Meraki ネットワークを作成して、SSID をネットワークにプロビジョニングします。Meraki ダッシュボードは、Meraki ネットワーク構成を Meraki デバイスにプロビジョニングします。

Meraki デバイスのプロビジョニング

この手順では、Meraki ダッシュボードによって管理されている Cisco Meraki デバイスの SSID をプロビジョニングする方法について説明します。

始める前に

前提条件を満たしていることを確認します。詳細については、Merakiデバイスをプロビジョニングするための前提条件 （1175 ページ）を参照してください。

手順

ステップ 1 メインメニューから次を選択します。**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。

[Inventory] ウィンドウが表示され、検出されたデバイスが一覧表示されます。

ステップ 2 Cisco Meraki ダッシュボードを表示するには、左側のペインで [グローバル（Global）] サイトを展開し、ビルディングを選択します。

選択したビルディングで使用可能なすべての Cisco Meraki ダッシュボードが表示されます。

ステップ 3 プロビジョニングする Meraki ダッシュボードの横にあるチェックボックスをオンにします。

ステップ 4 [Actions] ドロップダウンリストから、**[Provision]** > **[Provision Device]** を選択します。

[サイトの割り当て（Assign Site）] ウィンドウが表示され、Cisco Meraki ダッシュボードと関連付けられたビルディングを確認できます。

ステップ 5 関連付けられたビルディングを変更するには、[Choose a site] をクリックします。

ステップ 6 [Choose a site] ウィンドウで、ビルディングを選択して [Save] をクリックします。

ステップ 7 [Next] をクリックします。

[Configuration] ウィンドウが表示されます。管理ビルディングは、プライマリロケーションで表示できます。

ステップ 8 Cisco Meraki ダッシュボードのセカンダリ管理ロケーションを選択するには、[セカンダリ管理対象APロケーションの選択（Select Secondary Managed AP Locations）] をクリックします。

ステップ 9 [Managed AP Location] ウィンドウで、ビルディング名の横にあるチェックボックスをオンにします。

ステップ 10 [Save] をクリックします。

ステップ 11 [Next] をクリックします。
[Summary] ウィンドウで、設定を確認します。変更するには、[Edit] をクリックします。

（注） Meraki 展開では、各ネットワークで最大 15 の SSID がサポートされています。

ステップ 12 [展開（Deploy）] をクリックします。

ステップ 13 [デバイスのプロビジョニング（Provision Devices）] ウィンドウで、次の手順を実行して CLI 設定をプレビューします。

a) [Generate Configuration Preview] オプションボタンをクリックします。
b) **[Task Name]** フィールドに、CLI プレビュータスクの名前を入力し、**[Apply]** をクリックします。
c) [Task Submitted] ダイアログボックスで、[Work Items] リンクをクリックします。

（注） このダイアログボックスは表示されてから数秒で表示されなくなります。[Tasks] ウィンドウに移動するには、メニューアイコンをクリックして次を選択します。 **[Activities]** > **[Tasks]** の順に選択します。

d) **[Tasks]** ウィンドウで、設定プレビュー要求を送信した CLI プレビュータスクをクリックします。
e) CLI 構成の詳細を表示し、[Deploy] をクリックします。
f) 即座にデバイスを展開するには、[Now] オプションボタンをクリックし、[Apply] をクリックします。
g) 将来の日付と時刻でデバイスの展開をスケジュールするには、[Later] オプションボタンをクリックし、展開する日時を定義します。
h) [Information] ダイアログボックスで、次の手順を実行します。

1. **[Tasks]** ウィンドウから CLI プレビュータスクを削除する場合は、**[Yes]** をクリックします。
2. **[Tasks]** ウィンドウでタスクを保持する場合は、**[No]** をクリックします。

（注） CLI タスクは、**[Tasks]** ウィンドウで完了済みとしてマークされます。このタスクの CLI 設定は表示することはできますが、再度展開することはできません。

（注） デバイスで構成を展開すると、[Task Progress] バーに、**[Activities]** > **[Tasks]**で進行中のプロビジョニングタスクの進行状況が表示されます（タスク名をクリックすると表示されます）。

展開が正常に完了すると、[デバイスインベントリ（Device Inventory）] ウィンドウの [プロビジョニング ステータス （Provision Status）] 列に「成功（SUCCESS）」と表示されます。

リモート テレワーカー デバイスのプロビジョニング

次のトピックでは、リモートテレワーカーサイトのコンポーネントとリモート テレワーカー デバイスをプロビジョニングする手順について説明します。

リモートテレワーカーの導入の概要

導入コンポーネント

Cisco リモートテレワーカーの導入は、シスコ ワイヤレスコントローラ、Cisco OfficeExtend アクセスポイント（AP）、および企業ファイアウォールの 3 つの主要コンポーネントを中心に構築されています。次のモデルがこの導入でサポートされています。

- **ワイヤレスコントローラ**：Cisco 5520 ワイヤレスコントローラ、Cisco 8540 ワイヤレスコントローラ、Cisco 3504 ワイヤレスコントローラ[4]Cisco Catalyst 9800-40 ワイヤレスコントローラ、Cisco Catalyst 9800-80 ワイヤレスコントローラ、Cisco Catalyst 9800-CL ワイヤレスコントローラ、および Cisco Catalyst 9800-L ワイヤレスコントローラ。
- **アクセス ポイント**：Cisco Aironet 1815T（テレワーカー）アクセス ポイント、Cisco Aironet 1815I アクセス ポイント、Cisco Aironet 1815W アクセス ポイント、Cisco Aironet 1840I アクセス ポイント、Cisco Aironet 2800 シリーズ アクセス ポイント、Cisco Aironet 3800 シリーズ アクセス ポイント、Cisco Aironet 4800 、Cisco Catalyst 9115 アクセス ポイント、Cisco Catalyst 9120 アクセス ポイント、および Cisco Catalyst 9130 アクセス ポイント。

シスコ ワイヤレス コントローラについて

Cisco のコントローラは、システム全体のワイヤレス WLAN 機能（セキュリティポリシー、侵入防御、RF 管理、Quality of Service（QoS）、モビリティなど）を担っています。シスコの AP と連携して動作し、テレワーカーのビジネスクリティカルなワイヤレスアプリケーションをサポートします。コントローラは、ネットワーク管理者が安全かつスケーラブルなテレワーカー環境を構築するために必要な制御、スケーラビリティ、セキュリティ、および信頼性を提供します。

ユーザーが会社のデバイスを組織のオンサイト ワイヤレス ネットワークに接続できるようにするために、リモート テレワーク ソリューションは、組織内でデータと音声をサポートするものと同じワイヤレス Secure Set Identifier（SSID）をテレワーカーの自宅で提供します。

Cisco OfficeExtend アクセス ポイント

AP をコントローラから独立して動作させることはできません。AP は、コントローラリソースと通信するときに、必要に応じてその設定をダウンロードし、ソフトウェアまたはファームウェアイメージを同期します。AP は、コントローラへのセキュアな Datagram Transport Layer Security（DTLS）接続を構築し、企業のオフィスと同じプロファイルを使用してリモート WLAN 接続を確立します。セキュアなトンネリングにより、すべてのトラフィックを一元化されたセキュリティ ポリシーに対して検証でき、家庭用のファイアウォールに関連する管理オーバーヘッドを最小限に抑えられます。

企業向けファイアウォール

コントローラは緩衝地帯（DMZ）に配置する必要があり、企業ファイアウォールは、ファイアウォール経由でのコントローラへの CAPWAP 制御とデータトラフィックを許可する必要があ

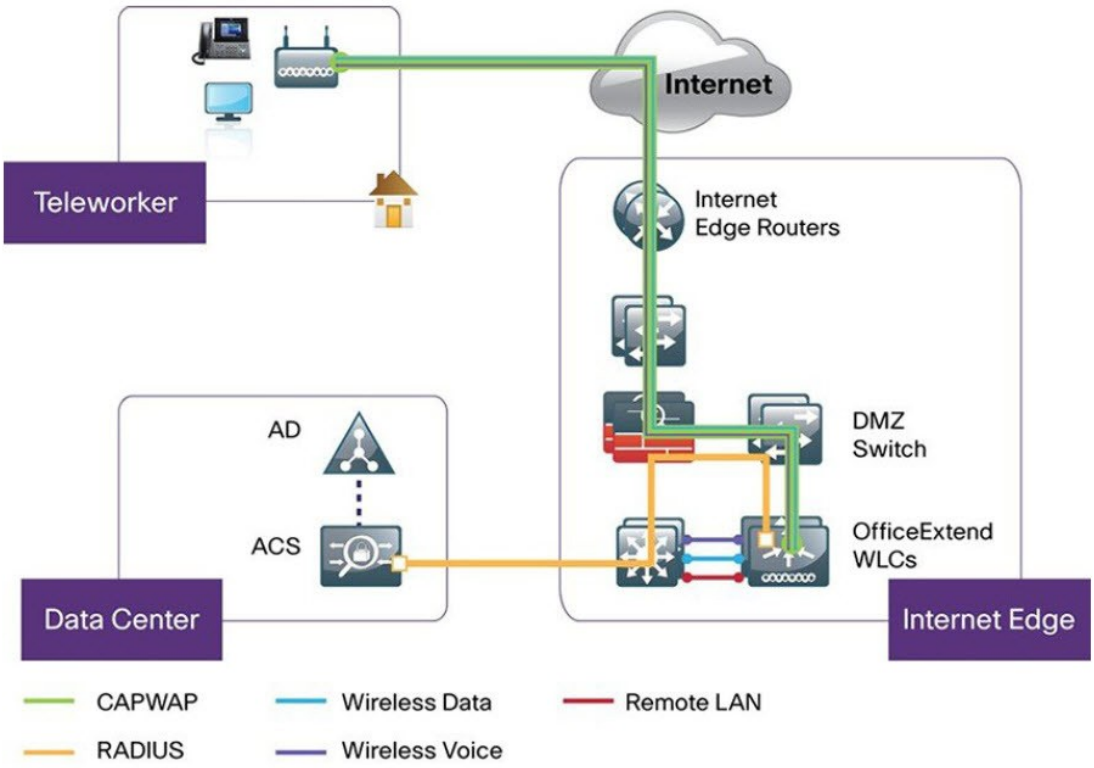
[4] Cisco Aironet 1815 テレワーカー アクセス ポイントのみでサポートされます。

ります。ファイアウォールの一般設定では、ファイアウォール経由での CAPWAP 制御および CAPWAP 管理ポート番号が許可されます。コントローラと AP の間の通信用に、ファイアウォールで UDP 5246 および 5247 ポートを開く必要があります。

展開設定

最も柔軟で安全なリモートテレワーカー構成を実現するには、専用のコントローラペアをインターネットエッジ DMZ 専用に展開します。インターネットからのトラフィックは、内部ネットワークではなく DMZ で終端しますが、リモート AP は引き続き内部ネットワークに直接接続されています。

図 *27*：サンプルのリモートテレワーカー導入シナリオ



リモートテレワーカーサイトの作成

リモートテレワーカーサイトは、ワイヤレスコントローラとリモート テレワーカー アクセス ポイント（AP）を管理するためだけに使用される専用サイトです。リモートテレワーカーサイトを作成するには、サイトでリモートテレワーカー機能を有効にする必要があります。有効にすると、リモートテレワーカー機能は、サイトの階層内のサイト、ビルディング、またはフロアに対して個別に無効化できません。サイトでは、リモートテレワーカー機能のみを管理できます。

テレワーカーサイトでは、切り替えはコントローラから集中的に実行されます。ローカルスイッチングを使用して FlexConnect のネットワークプロファイルを設定することはできません。

始める前に

- テレワーカーの展開で使用されるサポート対象デバイスを理解します。
- インベントリに シスコ ワイヤレス コントローラとシスコの AP があることを確認してください。ない場合は、デバイスを検出するか、手動で追加します。詳細については、ネットワークの検出 （73 ページ） または ネットワークデバイスの追加 （157 ページ） を参照してください。
- ネットワークに適したグローバル ワイヤレス ネットワーク設定を構成します。詳細については、「グローバルワイヤレス設定の構成 （414 ページ）」を参照してください。
- リモートテレワーカー AP の場合は、リモートテレワーカーを有効にして AP プロファイルを作成し、カスタムサイトタグを設定することをお勧めします。詳細については、Cisco IOS XE デバイスの AP プロファイルの追加設定を行う （509 ページ）およびネットワークプロファイルへの AP グループ、Flex グループ、サイトタグ、およびポリシータグの追加 （563 ページ）を参照してください。
- Cisco AireOS デバイスの場合は、リモートテレワーカー AP に使用されるサイトのカスタム AP グループに AP プロファイルをマッピングする必要があります。詳細については、ワイヤレス用のネットワークプロファイルの作成 （543 ページ）およびネットワークプロファイルへの AP グループ、Flex グループ、サイトタグ、およびポリシータグの追加 （563 ページ）を参照してください。

手順

ステップ 1 リモートテレワーカー AP を管理するためのサイトを作成します。「サイトの作成、編集、削除 （285 ページ）」を参照してください。

ステップ 2 建物とフロアを追加します。「ビルディングの追加、編集、および削除 （286 ページ）」を参照してください。

ステップ 3 リモートテレワーカーサイトのワイヤレスネットワーク設定を構成します。

a) メインメニューから次を選択します。**[Design]** > **[Network Settings]** > **[Wireless]** の順に選択します。
b) 左側の階層ツリーから、以下を選択しますリモートテレワーカーサイトを選択します。
c) [Remote Teleworker] をクリックします。
d) [Enable Remote Teleworker] チェックボックスをオンにします。
e) **[Save]** をクリックします。

ステップ 4 コントローラをサイトに割り当てます。「プロビジョニングされていないデバイスのサイトへの割り当て （189 ページ）」を参照してください。

ステップ 5 AP をサイトに割り当てます。「プロビジョニングされていないデバイスのサイトへの割り当て （189 ページ）」を参照してください。

シリアル番号または MAC アドレスを使用できますが、両方を混在させることはできません。または、CSV ファイルをアップロードすることがきます。

ステップ 6 ワイヤレスネットワーク設定で、AP を承認済み AP リストに追加します。

a) 左側の階層ツリーから、以下を選択します [Global] を選択します。
b) メインメニューから次を選択します。**[Design]** > **[Network Settings]** > **[Wireless]** の順に選択します。
c) [Security Settings] をクリックします。
d) [AP Authorization List] タブをクリックし、コントローラへの参加を許可する AP を追加します。詳細については、AP 認証リストの作成 （492 ページ）を参照してください。

コントローラは、認証リストに含まれている AP からの CAPWAP 要求にのみ応答します。

ステップ 7 コントローラをプロビジョニングします。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。

[Inventory] ウィンドウが表示され、検出されたデバイスが一覧表示されます。

b) プロビジョニングするコントローラを見つけます。
c) デバイス名の横にあるチェックボックスをオンにします。
d) [Actions] ドロップダウンリストから、**[Provision]** > **[Provision Device]** を選択します。
e) [Assign Site] ウィンドウで、割り当てられたサイトを選択して [Save] をクリックします。
f) [Next] をクリックします。
g) （任意） [Configuration] ウィンドウの [NAT Address for Remote Teleworker] で、[Enable NAT Address] チェックボックスをオンにして、NAT IP アドレスを入力します。

（注） Catalyst Center は次のアドレスをサポートしていないことに注意してください。

- IPv6 ドキュメントアドレス：2001:db8::/322
- IPv6 サイトローカルアドレス：fec0::/103
- IPv6 リンクローカルアドレス：fe80::/104
- IPv6 ループバックアドレス：::1
- IPv6 マルチキャストアドレス：FF00::/8

h) [Next] をクリックします。
i) [Feature Templates] ウィンドウで [Next] をクリックします。
j) [Advanced Configuration] ウィンドウで [Next] をクリックします。
k) [Summary] ウィンドウで設定を確認し、[Deploy] をクリックします。
l) [Provision Device] スライドインペインで、[Now] を選択し、[Apply] をクリックします。

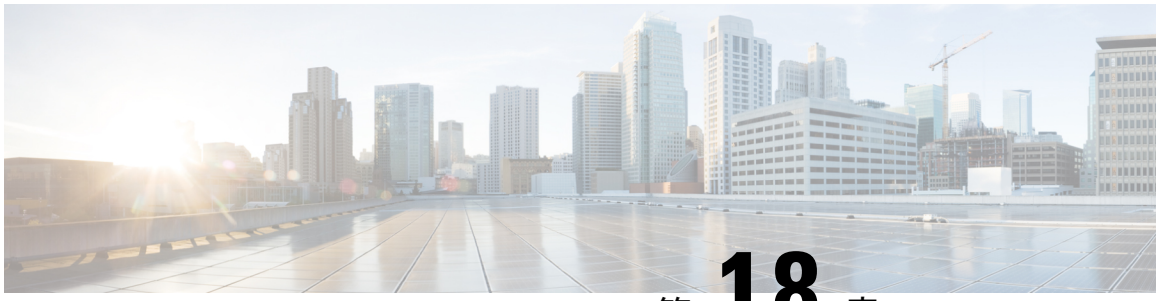
（注） デバイスで構成を展開すると、[Task Progress] バーに、**[Activities]** > **[Tasks]**で進行中のプロビジョニングタスクの進行状況が表示されます（タスク名をクリックすると表示されます）。

ステップ 8 シスコ ワイヤレス コントローラがプロビジョニングされたら、AP をプロビジョニングできます。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。

[Inventory] ウィンドウが表示され、検出されたデバイスが一覧表示されます。

b) プロビジョニングする AP を見つけます。
c) デバイス名の横にあるチェックボックスをオンにします。
d) [Actions] ドロップダウンリストから、**[Provision]** > **[Provision Device]** を選択します。
e) [Assign Site] ウィンドウで、[Choose a floor] をクリックし、AP をフロアに割り当てます。
f) [Save] をクリックします。
g) [Next] をクリックします。
h) [Configuration] ウィンドウで [Next] をクリックします。
i) [Summary] ウィンドウで設定を確認し、[Deploy] をクリックします。
j) [Provision Device] スライドインペインで、[Now] を選択し、[Apply] をクリックします。



第 18 章

ルーティングプロファイルのプロビジョニング

- ルータのプロビジョニング （1185 ページ）
- VPC インベントリ収集 （1187 ページ）

ルータのプロビジョニング

始める前に

ルーティングプロファイルをプロビジョニングする前に、次を含むグローバルネットワーク設定を定義したことを確認します。

- AAA、DHCP、および DNS などのネットワーク サーバー。詳細については、グローバル ネットワーク サーバーの設定 （377 ページ）を参照してください。
- CLI、SNMP、HTTP、HTTPS などのデバイス クレデンシャル。詳細については、グローバル CLI クレデンシャルの追加 （379 ページ）、グローバル SNMPv2c ログイン情報の追加 （380 ページ）、グローバル SNMPv3 ログイン情報の追加 （382 ページ）、およびグローバル HTTPS ログイン情報の追加 （385 ページ）を参照してください。
- IP アドレス プール詳細については、「IP アドレスプールを設定する （397 ページ）」を参照してください。
- サービスプロバイダーのプロファイル。詳細については、サービス プロバイダ プロファイルの設定 （413 ページ）を参照してください。

手順

ステップ 1 メインメニューから次を選択します。**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。

[Inventory] ウィンドウが表示され、検出されたデバイスが一覧表示されます。

ステップ 2 特定のサイトで使用可能なデバイスを表示するには、**[Global]** をクリックして目的のサイト、ビルディング、またはフロアを選択します。

選択したサイトで使用可能なすべてのデバイスが [インベントリ（Inventory）] ウィンドウに表示されます。

ステップ 3 **[Inventory]** ウィンドウの上部で、**[Routers]** をクリックします。

ステップ 4 プロビジョニングするデバイスの横にあるチェックボックスをオンにします。

ステップ 5 サイトの **[Assign]** をクリックし、**[Assign Device to Site]** ウィンドウで **[Choose a site]** をクリックします。

ステップ 6 [Actions] ドロップダウンリストから、**[Provision]** > **[Provision Device]** を選択します。

ステップ 7 ルータをプロビジョニングするには、次の手順を実行します。

1. [Confirm Profile] ページで詳細を確認し、[Next] をクリックします。
2. **[Router WAN Configuration]** ページで詳細を確認します。

   仮想ルータをプロビジョニングしている場合、このページは表示されません。

   1. 回線インターフェイスとしてギガビットイーサネットを選択した場合は、接続アイコン[ ]をクリックします。静的 IP アドレスを選択した場合は、WAN IP アドレスを入力します。DHCP を選択した場合は、DHCP サーバーの IP アドレスを入力します。プライマリ WAN がすでに PnP を使用して設定されている場合は、**[Do not Change]** を選択できます。**[Interface Name]** ドロップダウンリストから、プライマリ WAN として設定するインターフェイスを選択します。
   2. 回線インターフェイスとしてセルラーを選択した場合は、接続アイコン [ ] をクリックして [ネゴシエートされたIPアドレス（IP Negotiated）] を選択し、ドロップダウンリストから [インターフェイス名（Interface Name）] を選択して [アクセスポイント名（Access Point Name (APN)）] を入力します。サービスプロバイダに応じて、**[PAP]** チェックボックスまたは **[CHAP]** チェックボックスをオンにします。
   3. 複数のサービスプロバイダを利用している場合は、バックアップ WAN インターフェイスの **[IP SLA Address]** を入力します。
   4. [Next] をクリックします。
3. **[Router LAN Configuration]** ページで詳細を確認します。
   1. ドロップダウンリストから [Interface] を選択します。
   2. ドロップダウンリストから **[IP-Pool/IP]** を選択します。
   3. [IP Address Pool] ドロップダウンリストからプールを選択します。
   4. [Next] をクリックします。
4. **[Integrated Switch Configuration]** ページで詳細を確認します。

   設定によっては、このページが表示されない場合があります。
5. さまざまな仕様、設定、構成のドロップダウンメニューを展開し、**[Summary]** ページで詳細を確認します。

ステップ 8 [展開（Deploy）] をクリックします。

ステップ 9 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 10 [Tasks] ウィンドウで、タスクの展開を監視します。

または、[デバイスインベントリ（Device Inventory）] ウィンドウからタスク展開をモニターできます。展開が正常に完了すると、[プロビジョニングステータス （Provision Status）] 列に [成功（SUCCESS）] と表示されます。[SUCCESS] をクリックして詳細なプロビジョニング ログ ステータスを確認します。

VPC インベントリ収集

クラウドインベントリ収集が正常に完了すると、[Provision] セクションの [Cloud] タブに、収集した AWS VPC インベントリのビューが表示されます。左側のナビゲーションを展開して、クラウドプロファイルまたはアクセスキーのクラウド領域を表示できます。左側のナビゲーション項目をキーワードでフィルタ処理してクリックすると、選択した領域またはアクセスキーに対してのみ VPC が表示されます。

[VPC Inventory] ビューでは、VPC をクリックして、その VPC のサブネットや仮想インスタンスなどの詳細を確認することもできます。AWS VPC インベントリ収集は、すべてのインベントリ収集のデフォルト間隔で行われるようにスケジュールされており、クラウドアクセスキーの歯車メニューの [Sync] アクションを使用して、オンデマンドでトリガーすることもできます。インベントリ収集のステータスを表示するには、[VPC Inventory] ビューで [Show Sync Status] をクリックします。



第 19 章

ファイアウォール プロファイルのプロビジョニング

- Firewall Threat Defense デバイスのプロビジョニング （1189 ページ）
- ファイアウォール適応型セキュリティアプライアンスデバイスのプロビジョニング （1191 ページ）

Firewall Threat Defense デバイスのプロビジョニング

この手順では、Firepower Management Center（FMC）によって管理される Firepower Threat Defense（FTD）デバイスをプロビジョニングする方法について説明します。

始める前に

- FMC と Catalyst Center を統合します。Firepower Management Center の統合 （181 ページ）を参照してください。
- ネットワーク階層内でサイトを作成します。サイトの作成、編集、削除 （285 ページ）を参照してください。
- Routed FTD または Transparent FTD のネットワークプロファイルを作成し、FTD デバイスが割り当てられるサイトに割り当てます。ファイアウォール用のネットワークプロファイルの作成 （537 ページ）を参照してください。

手順

ステップ 1 メインメニューから次を選択します。**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。

[Inventory] ページには、ディスカバリプロセス中に収集されたデバイス情報が表示されます。

ステップ 2 プロビジョニングする FTD デバイスの横にあるチェックボックスをオンにして、[Site] 列の下にある [Assign] をクリックします。

ステップ 3 [Assign Device to Site] ウィンドウで、[Choose a Site] をクリックします。

ステップ 4 [Choose a Site] ウィンドウで、階層からサイトを選択して [Save] をクリックします。

ステップ 5 [Next] をクリックします。

ステップ 6 [Now] をクリックしてデバイスをサイトにすぐに割り当てるか、[Later] をクリックして特定の時間にスケジュールします。

ステップ 7 [**Assign**] をクリックします。

（注） **[Activities]** > **[Tasks]** で、サイトへのデバイスの割り当てのステータスを確認できます。

ステップ 8 [Actions] ドロップダウンリストから、**[Provision]** > **[Provision Device]** を選択します。

[Provision Firewall Profile] ウィンドウが表示されます。

ステップ 9 [Confirm Profile] ページで詳細を確認し、[Next] をクリックします。

ステップ 10 [Firewall Type] ページで詳細を確認し、[Next] をクリックします。

[FTD Configuration] ページが表示されます。

ステップ 11 ルーテッドモードのファイアウォールをサイトに関連付けている場合は、次の手順を実行します。

a) [Outside Interface] エリアを展開し、[Select Physical Interface] ドロップダウンリストから外部インターフェイスを選択して、[Static IP] または [DHCP] オプションボタンを選択します。

- [Static IP]：IP アドレスおよびサブネットマスクを入力します。
- [DHCP]：IP アドレスは DHCP から取得されます。

b) [Inside Interface] エリアを展開し、[Select Physical Interface] ドロップダウンリストから内部インターフェイスを選択して、[Static IP] または [DHCP] オプションボタンを選択します。

- [Static IP]：IP アドレスおよびサブネットマスクを入力します。
- [DHCP]：IP アドレスは DHCP から取得されます。

ステップ 12 トランスペアレントモードのファイアウォールをサイトに関連付けている場合は、次の手順を実行します。

a) [Outside Interface] エリアを展開し、[Select Physical Interface] ドロップダウンリストから外部インターフェイスを選択します。

b) [Inside Interface] エリアを展開し、[Select Physical Interface] ドロップダウンリストから内部インターフェイスを選択します。

c) [ブリッジ仮想インターフェイス（Bridge Virtual Interface）] エリアを展開し、次のタスクを実行します。

- [Bridge Group Number]：ブリッジグループ番号を入力します。有効な値は 1 ー 250 です。
- [IP]：FTD デバイスの IP アドレスを入力します。
- [Subnet Mask]：サブネットマスクを入力します。

ステップ 13 [Next] をクリックします。

ステップ 14 [Summary] ウィンドウで、デバイス仕様を確認します。

ステップ 15 続行するには、[Deploy] をクリックします。

[Provision Firewall device(s)] ダイアログボックスが表示されます。

ステップ 16 [Now]、[Later]、または [Generate configuration preview] オプションボタンをクリックします。

- [Now]：プロビジョニングがすぐに開始されます。
- [Later]：特定の時間にプロビジョニングがスケジュールされます。
- [設定プレビューの生成（Generate configuration preview）]：選択したデバイスに展開するために後で使用できるプレビューを生成します。

ステップ 17 [Apply] をクリックします。

（注） **[アクティビティ（Activities）]>[タスク（Tasks）]** で、プロビジョニングステータスを確認できます。[ファイアウォールデバイスのプロビジョニング（Provision Firewall device(s)）] ダイアログボックスで [設定プレビューの生成（Generate configuration preview）] を選択した場合は、**[アクティビティ（Activities）]>[タスク（Tasks）]** で作業項目のステータスを確認できます。

ファイアウォール適応型セキュリティアプライアンスデバイスのプロビジョニング

この手順では、ファイアウォール適応型セキュリティアプライアンス（ASA）デバイスをプロビジョニングする方法について説明します。

Before you begin

- ASA デバイスを Catalyst Centerと統合します。
- ASAデバイスのファイアウォールのネットワークプロファイルを作成し、サイトに割り当てます。ファイアウォール用のネットワークプロファイルの作成（537ページ） を参照してください。

手順

ステップ 1 メインメニューから次を選択します。**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。

[インベントリ（Inventory）] ページには、検出プロセス中に収集されたデバイス情報が表示されます。

ステップ 2 ASA デバイスを選択します。[Actions] ドロップダウンリストから、**[Provision]** > **[Provision Device]** を選択します。

[Provision Firewall Profile] ウィンドウが表示されます。

ステップ 3 [プロファイルの確認（Confirm Profile）] ウィンドウで詳細を確認します。**[次へ（Next）]** をクリックします。

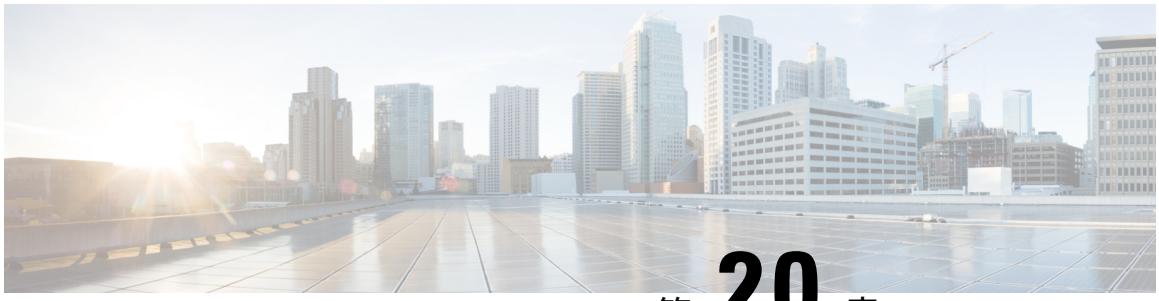
ステップ 4 [ファイアウォールタイプ（Firewall Type）] ウィンドウで詳細を確認します。[Next] をクリックします。

ステップ 5 [カスタム設定（Custom Configuration）] ウィンドウで詳細を確認します。[Next] をクリックします。

ステップ 6 **[サマリー（Summary）]** ウィンドウでデバイス仕様を確認します。[Deploy] をクリックします。

[構成の可視性と制御（Visibility and Control of Configurations）] の設定に応じて、次のいずれかを実行できます。

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。



第 20 章

LAN アンダーレイのプロビジョニング

- LAN の自動化 （1193 ページ）
- LAN 自動化によるネットワークのプロビジョニングの前提条件 （1195 ページ）
- LAN 自動化によるネットワークのプロビジョニング （1196 ページ）
- LAN 自動化のピアデバイスのユースケース （1204 ページ）
- LAN 自動化のステータスの確認 （1206 ページ）
- インターフェイス間のリンクを作成 （1206 ページ）
- インターフェイス間のリンクの削除 （1207 ページ）
- LAN 自動化デバイスのホスト名とループバック IP アドレスの編集 （1208 ページ）
- Strict 検出モードのデバイスの管理 （1209 ページ）

LAN の自動化

Catalyst Center は、新しいネットワークの手動展開に代わるものとして LAN 自動化を提供します。この自動化により、ネットワークの運用を簡素化し、エラーのない標準的なネットワークを構築できます。LAN 自動化では、IS-IS ルーティングプロトコルを使用してレイヤ 3 ルーテッドアクセス設計が展開されます。

[LAN Automation] には、次の機能が用意されています。

- LAN 自動化によるネットワークのプロビジョニング
- LAN 自動化セッションの履歴の表示
- LAN 自動化デバイスの概要の表示

メインメニューから次を選択します。**Provision** > **LAN Automation** の順に選択してこのウィンドウを表示します。

- [Start LAN Automation]：このオプションを使用して、ネットワーク上で LAN 自動化セッションを開始します。
- [Overview]：このセクションを展開し、LAN 自動化によるネットワークのプロビジョニングの前提条件と詳細情報を表示します。

- [Sessions]：このセクションは、LAN 自動化セッションの履歴（[History]）と LAN 自動化デバイスのリスト（[LAN Automated Devices]）で構成されています。

n 日目の運用

0 日目に [Start LAN Automation] をクリックし、LAN 自動化によるネットワークのプロビジョニングを開始します。詳細については、LAN 自動化によるネットワークのプロビジョニング（1196 ページ）を参照してください。

0 日目には、Catalyst Center の [Sessions] セクションにデータは表示されません。

n 日目の運用

n 日目に [Start LAN Automation] をクリックすることにより、別の LAN 自動化セッションを開始できます。サイト間で最大 5 つの LAN 自動化セッションを同時に実行できます。詳細については、LAN 自動化によるネットワークのプロビジョニング（1196ページ）を参照してください。

LAN 自動化セッションが進行中の場合は、Catalyst Center の [LAN Automation] ウィンドウにセッションのタイルが表示されます。セッションの詳細を表示するには、タイルの [See Session Details] をクリックします。セッションの LAN 自動化を停止するには、タイルの [Stop LAN Automation] をクリックします。

[History] タブには、ネットワーク内の LAN 自動化セッションの履歴が表示されます。[Search] フィールドを使用して特定のテキストを検索できます。セッションの詳細を表示するには、ハイパーリンクが設定された日付をクリックします。セッションのログを表示するには、セッションの詳細ウィンドウで [View Session Logs] をクリックします。

[LAN Automated Devices] タブには、LAN 自動デバイスの詳細が表示されます。検索フィールドを使用して、特定のテキストに基づいてデータをフィルタ処理できます。データをフィルタ処理するには、次のトグルボタンのいずれかをクリックします。

- [Seed Devices]：シードデバイスのデータを表示します。
- [Discovered]：検出されたデバイスのデータを表示します。
- [Provisioned]：プロビジョニングされたデバイスのデータを表示します。
- [Error]：エラーのあるデバイスのデータを表示します。

[LAN Automated Devices] タブでは、次の操作も可能です。

- デバイス名のハイパーリンクをクリックしてデバイスの詳細を表示する。
- [Add Link] をクリックして 2 つのデバイス間のインターフェイスをプロビジョニングする。詳細については、インターフェイス間のリンクを作成（1206ページ）を参照してください。
- [Delete Link] をクリックして 2 つのデバイス間のインターフェイスを削除する。詳細については、インターフェイス間のリンクの削除 （1207 ページ）を参照してください。

- [デバイスの編集（Edit Device）]オプションを使用して、デバイスのホスト名とループバック IP アドレスをカスタマイズします。詳細については、LAN 自動化デバイスのホスト名とループバック IP アドレスの編集 （1208 ページ）を参照してください。

（注）

- *n* 日目にデバイスのホスト名とループバック IP アドレスを編集するには、デバイスがインベントリで **[Managed]** の状態になっている必要があります。
- 単一の *n* 日目ワークフローで最大 25 のデバイスのループバック IP アドレスを編集できます。

LAN 自動化によるネットワークのプロビジョニングの前提条件

LAN 自動化によってネットワークをプロビジョニングする前に、次の前提条件を満たしていることを確認してください。

- ネットワーク階層を設定します。（ネットワーク階層の作成 （285 ページ） を参照）。
- 次のグローバルネットワーク設定を定義します。
  - AAA、DHCP、DNS サーバーなどのネットワークサーバー（グローバル ネットワーク サーバーの設定 （377 ページ） を参照）。
  - CLI、SNMP、HTTP、HTTPS のログイン情報などのデバイスのログイン情報(グローバル CLI クレデンシャルの追加 （379 ページ）、グローバル SNMPv2c ログイン情報の追加 （380 ページ）、グローバル SNMPv3 ログイン情報の追加 （382 ページ）、グローバル HTTPS ログイン情報の追加 （385 ページ）を参照)。

（注）

SNMPv2 書き込みログイン情報は必要ありません。設定されている場合、LAN の自動化中にデバイスにプッシュされません。

  - IP アドレスプール（IP アドレスプールを設定する （397 ページ） を参照）。
- インベントリに少なくとも 1 つのデバイスがあることを確認します。デバイスがない場合は、ディスカバリ機能を使用して検出します。（ディスカバリの実行 （86 ページ） およびプロビジョニングされていないデバイスのサイトへの割り当て （189ページ） を参照。）

（注） 検出されたサイトの CLI ログイン情報にユーザー名「cisco」が設定されている場合、LAN 自動化はブロックされます。

- ネットワークに Cisco Catalyst 9400 スイッチが設定されている場合は、LAN 自動化で 40G ポートが自動的に有効になるように、スイッチで次の操作が完了している必要があります。
  - Day-0 設定はスイッチで実行されます。

    詳細については、*Cisco Catalyst 9400 シリーズ スイッチハードウェア設置ガイド* [英語] の「Initial Configuration for the Switch」を参照してください。
  - 40G Quad Small Form-Factor Pluggable（QSFP）トランシーバはスーパバイザのポート 9 またはポート 10 のいずれかに挿入されます。スーパバイザ上の 1 ～ 8 のポートには、10G または 1G Small Form-Factor Pluggable（SFP）トランシーバは挿入されません。デュアル スーパーバイザ エンジンがある場合は、40G QSFP がポート 9 に挿入されていることを確認します。

    Catalyst 9400 シリーズ スーパーバイザの詳細については、*Cisco Catalyst 9400 シリーズ スーパーバイザ インストール ノート* [英語] の「Uplink Ports」を参照してください。
- LAN の自動化の詳細については、「*Cisco Catalyst Center SD-Access LAN Automation Deployment Guide*」を参照してください。

LAN 自動化によるネットワークのプロビジョニング

始める前に

前提条件が満たされていることを確認してください。詳細については、LAN 自動化によるネットワークのプロビジョニングの前提条件 （1195 ページ）を参照してください。

手順

ステップ 1 プロビジョニングするサイト用に IP アドレスプールを予約します。

（注） LAN 自動化 IP アドレスプールのサイズは、25 ビットのネットマスク以上である必要があります。

a) メインメニューから次を選択します。**[Design]** > **[Network Settings]** > **[IP Address Pools]** の順に選択します。
b) 左側の階層ツリーから、以下を選択します必要なサイトを選択します。
c) [Reserve] をクリックします。[Reserve IP Pool] リンクをクリックします。
d) [Reserve IP Pool] スライドインペインで以下のフィールドに入力し、使用可能なグローバル IP アドレスプールのすべてまたは一部を特定のサイト用に予約します。

- [IP Address Pool Name]：予約した IP アドレスプールの一意の名前。
- [Type]：IP アドレスプールのタイプ。
  - [LAN]：該当するアンダーレイの LAN インターフェイスに IP アドレスを割り当てます。LAN 自動化では、このオプションを選択します。
  - [Management]：IP アドレスを管理インターフェイスに割り当てます。
  - [Service]：IP アドレスをサービスインターフェイスに割り当てます。
  - [WAN]：IP アドレスを WAN インターフェイスに割り当てます。
  - [Generic]：他のすべてのネットワークタイプで使用されます。 これがデフォルトのオプションです。
- [**IP Address Space**]：[**IPv4**] または [**IPv6**] のチェックボックスをオンにしてアドレスプールを作成します。デュアルスタックプールを作成するには、[**IPv4**] と [**IPv6**] の両方のチェックボックスをオンにします。デフォルトでは、[IPv4] のチェックボックスはオンになっています。
- [Global IP Pool]：IP アドレスのすべてまたは一部を予約する IPv4 アドレスプール。 検索フィールドにテキストを入力して、ドロップダウンリストに表示される結果を絞り込めます。

（注） LAN 自動化では、IPv4 サブネットのみが使用されます。

- [Prefix length / Number of IP Addresses]：予約する IP アドレスの選択方法を次から指定します。

実行する操作	結果...
特定の IP ルートプレフィックスでアドレスを予約する	**1.** [Prefix length] ラジオボタンをクリックします。 **2.** ドロップダウンリストから適切なプレフィックス長の値を選択します。 **3.** [IPv4 Subnets] フィールドに、使用するサブネットアドレスを入力します。

実行する操作	結果...
特定の数のアドレスを予約する	**1.** [Number of IP Addresses] ラジオボタンをクリックします。 **2.** [Total host] フィールドに、予約する IP アドレスの数を入力します。

- [Gateway]：ゲートウェイ IP アドレス。 このフィールドは、[Prefix length] ラジオボタンが選択されている場合にのみ表示されます。
- [Overlapping]：Classless Interdomain Routing（CIDR）のオーバーラップを有効にするかどうかを指定します。

状況	結果...
複数の並列 IPv4 および IPv6 アドレス空間における IP プールの配置を有効にしない	[Off] ラジオボタンがすでに選択されていることを確認してください。これはデフォルト設定です。
CIDR 重複を有効にする	**1.** [On] ラジオボタンをクリックします。 **2.** 使用するアドレス空間識別子を指定します。[Create new] ラジオボタンをクリックして識別子を入力するか、[Select existing] ラジオボタンをクリックしてドロップダウンリストから識別子を選択します。 **重要** 新しいアドレス空間識別子の名前を入力する場合は、注意してください。後で名前を変更することはできません。

- [DHCP Server(s)]：Catalyst Center の展開で使用される DHCP サーバの IP アドレス。
- [DNS Server(s)]：Catalyst Center の展開で使用される DNS サーバーの IP アドレス。

e) [予約（Reserve）] をクリックします。

ステップ 2 デバイスの検出とプロビジョニングを開始するには、次の手順を実行します。

a) メインメニューから次を選択します。**[Provision]** > **[LAN Automation]**。

b) [LAN Automation] ウィンドウで、[Start LAN Automation] をクリックします。

ワークフローが設定プロセスを導きます。

c) [**Seed Devices**] ウィンドウで、シードデバイスのサイトを選択し、必要に応じてテーブルに記載されている属性を設定します。

属性	説明
Primary Seed Device	Catalyst Center が新しいデバイスを検出してプロビジョニングする起点として使用するプライマリデバイスを選択します。 [**Select interfaces**] で、デバイスのインターフェイスを選択します。
Secondary Seed Device	セカンダリシードデバイスを選択します。 [**Select interfaces**] で、デバイスのインターフェイスを選択します。
Discovery Depth	デバイスは、プライマリシードデバイスより下の指定されたレベルまで LAN 自動化されます。[検出深さ（Discovery Depth）] のデフォルト値は 2 で、最大値は 5 です。

d) [Sessions Attributes] ウィンドウで、次の手順を実行します。

1. 新しく検出されたすべてのデバイスが割り当てられるサイトを選択します。このサイトは、プライマリサイトおよびピアサイトとは異なる場合があります。
2. 必要に応じて、次の表に記載されているセッション属性を設定します。

属性	説明
Principal IP Address Pool	LAN 自動化用に予約された IP アドレスプール。ドロップダウンリストで IP アドレスプールを選択します。

属性	説明
Link Overlapping IP Pool	他のサイトと共有される IP アドレスプール。アンダーレイでポイントツーポイントリンクに対する /31 IP アドレスを設定するために使用されます。 • IP プールを重複するリンクには、親サイトから継承されるサブプールか他のサイトで定義されているサブプールを指定できます。 • IP プールを重複するリンクを使用すると、マルチサイト展開で /31 IP アドレスの重複が可能になります。異なるサイトのホストにおいて、/31 リンクで IP アドレスを再利用できます。 • IP プールを重複するリンクを定義した場合、[Principal IP Pool] フィールドで定義されたアドレスが管理 IP（ループバックアドレスや VLAN アドレスなど）に使用されます。 （注） IPv6 アドレスプールの場合、 [ポイントツーポイント IPv6 リンクローカルアドレッシング（Point-to-point IPv6 Link-Local addressing）] チェックボックスを使用してポイントツーポイントリンクを設定します。
ポイントツーポイント IPv6 リンクローカルアドレッシング	このオプションは、IPv6 アドレスプールを選択すると表示されます。アンダーレイのポイントツーポイントリンクのリンクローカルアドレッシングを有効にするには、チェックボックスを選択します。
IS-IS Domain Password	LAN 自動化用の IS-IS パスワードを入力します。パスワードがすでにシードデバイスに存在する場合は、そのパスワードが再使用され、上書きされることはありません。パスワードを入力せず、デバイスにパスワードがない場合は、デフォルトのドメインパスワードが使用されます。プライマリシードデバイスとセカンダリシードデバイスの両方のドメインパスワードが一致するようにします。

属性	説明
OSPF	Open Shortest Path First（OSPF）ルーティングプロトコルを選択した場合は、次のフィールドを設定します。 • Process Id：OSPF ルーティングプロセス識別子を入力します。 • Area Id：ネットワークの OSPF エリア識別子を指定します。 • Authentication key：OSPF メッセージ認証に使用されるパスワードまたはキーを入力します。
Session Timeout	LAN 自動化セッションのタイムアウト値を指定します。指定した時間制限に達すると、LAN 自動化が自動的に停止します。値は分単位で指定し、有効な範囲は 20 ～ 10,080 です。
Advertise LAN Automation Summary Route into BGP	LAN 自動化によって [Principal IP pool] をプライマリおよびピアシードデバイスの BGP にアドバタイズさせる場合は、このチェックボックスをオンにします。LAN 自動化は、シードデバイスで BGP が構成されている場合にのみ、シードデバイスにサマリールートをアドバタイズします。 このチェックボックスはデフォルトでは無効になっています。プライマリまたはピアシードデバイスに自律システム（AS）番号が設定されている場合にのみ有効になります。
Enable Multicast	このチェックボックスをオンにすると、アンダーレイ ネイティブ マルチキャストが有効になります。LAN 自動化によって、シードデバイスを RP とし、検出されたデバイスをサブスクライバとするマルチキャストツリーが作成されます。

属性	説明

Choose a File	[Choose a File] ドロップダウンからホスト名マップファイルを選択するか、ストレージデバイスからCSV ファイルをアップロードできます。
	
	選択したCSVファイルに記述されているシリアル番号とホスト名のマッピングを使用して、検出されたデバイスに対してユーザーが指定した名前が設定されます。検出されたデバイスがスタックの場合、スタックのすべてのシリアル番号が CSV ファイルで指定されます。または、デバイスごとにカスタマイズされたループバックIPアドレスを設定することもできます。LAN自動化プロセスでは、対応するデバイスに、指定したループバックIPアドレスが割り当てられます。CSVファイルにループバックIPアドレス情報が含まれていない場合、IPプールからランダムなIPアドレスがデバイスに割り当てられます。
	
	（注）
	デバイスのループバック IP アドレスには、そのデバイスと同じサイト内にある任意の IP アドレスプールのアドレスを指定できます。
	
	デバイス照合の厳密モードでは、CSVファイルにサイト名も含まれている必要があります。
	
	サンプルの CSV ファイルは次のとおりです。
	
	`standalone-switch,FCW2212L0NF,10.1.1.4`
	`stack-switch,"FCW2212E00Y,FCW2212L0GV"`

検出されたデバイスのホスト名プレフィックス	プロビジョニングしているデバイスの名前プレフィックス。Catalyst Centerが各デバイスをプロビジョニングするときに、ここで指定されたテキストでデバイスにプレフィックスを付与し、末尾に一意の番号を追加します。たとえば、名前プレフィックスとして「Access」を入力した場合、連続する各デバイスがプロビジョニングされると、Access-1、Access-2、Access-3のように名前が付けられます。

属性	説明
デバイスの照合	次のデバイス検出のオプションを選択します。 • [Relaxed]：デバイスのシリアル番号がアップロードされたデバイスリストと一致する場合、検出されたデバイスにホスト名とループバック IP が割り当てられます。 • [Strict]：デバイス検出は、指定されたデバイスのリストに制限されます。最大 50 台のデバイスを検出できます。デバイスを追加または編集するには、Strict 検出モードのデバイスの管理 （1209 ページ）を参照してください。

e) [Review] ウィンドウで、すべての LAN 自動化セッションの設定を調べます。変更するには、[Edit] をクリックします。

ステップ 3 [Review] ウィンドウで、[Start] をクリックします。

Catalyst Center は、新規デバイスの検出とプロビジョニングを開始します。

LAN 自動化では、VLAN 1 のシードデバイスで IP アドレスを設定します。シードデバイスのこの VLAN 1 IP アドレスが Catalyst Center から到達できない場合は、[LAN Automation Status] ウィンドウにエラーメッセージが表示されます。エラーの詳細および可能な修復アクションを表示するには、このウィンドウの [See Details] リンクにマウスカーソルを合わせます。

ステップ 4 プロビジョニングしているデバイスの進行状況をモニターして確認します。

[LAN Automation] ウィンドウで、ステータス ペインの [See Session Details] をクリックします。

ステータス表示をフィルタリングして、検出されたデバイス、プロビジョニングされたデバイス、またはエラーメッセージの詳細を表示できます。[**View Session Logs**] をクリックすると、セッションログが表示されます。デバイス名のハイパーリンクをクリックすると、デバイスの詳細が表示されます。

（注） 新しいデバイスのプロビジョニングには数分かかる場合があります。

ステップ 5 すべてのデバイスが検出されてインベントリに追加されたら、LAN 自動化セッションを停止します。デバイスが到達可能であり、管理対象の状態になっていることを確認します。

a) [LAN Automation Status] ウィンドウで、[Stop LAN Automation] をクリックします。

LAN 自動化を停止すると、[Review LAN Automation Session] ワークフローがトリガーされます。このワークフローでは、LAN 自動化セッション中に検出されたデバイスを確認し、展開前に変更を加えることができます。

b) [Review Discovered Devices] ウィンドウでは、デバイスのループバック IP アドレス（管理 IP アドレス）を編集できます。

c) [Validate] をクリックして、編集した IP アドレスを検証します。

d) 検証に成功した場合は、[**Apply**] をクリックすると、LAN 自動化設定が展開されます。

ステップ 6 （オプション）複数の LAN 自動化セッション（最大 5 つのセッション）を並行して実行できます。各セッションの詳細は、[**LAN Automation**] ウィンドウの個別のタイルに表示されます。

同時 LAN 自動化セッションを開始する前に、次の側面を考慮してください。

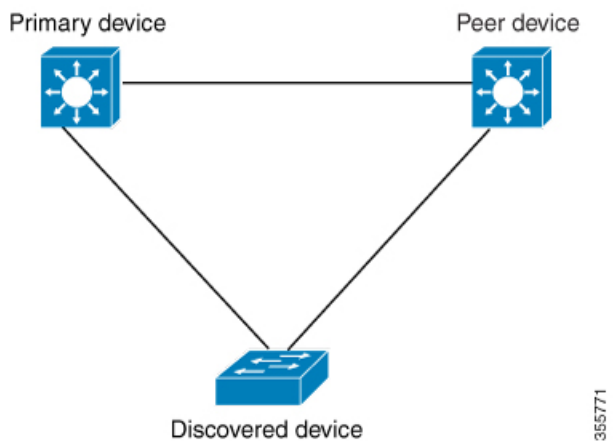
- 複数のセッションで同じシードデバイスを使用することはできません。
- 並行セッションに同じサイトを使用することはできません。
- 並列セッションに同じ IP プールを使用することはできません。

ステップ 7 （オプション）[**History**] タブで、完了した LAN 自動化セッションのステータスを確認できます。また、[**LAN Automated Devices**] タブで検出されたデバイスのリストを確認できます。

LAN 自動化のピアデバイスのユースケース

デュアルホーム スイッチのプロビジョニング

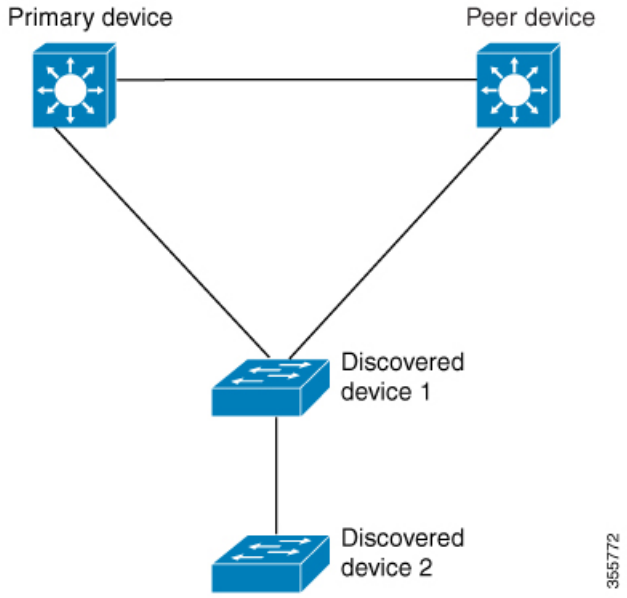
デュアル ホームのスイッチのプロビジョニングのために、常にピア デバイスを選択する必要があります。



Catalyst Center プライマリ デバイスで DHCP サーバーを設定します。Catalyst Center が検出されたデバイスがプライマリ デバイスとピア デバイスの両方に接続されていることを理解しているため、LAN 自動化タスクが停止されると、2 つのレイヤー 3 ポイントツーポイント接続を設定します。1 つの接続は、検出されたデバイスとプライマリ デバイスの間で確立されます。もう 1 つの接続は検出されたデバイスとピア デバイスの間で確立されます。

（注） LAN 自動化ジョブが実行される前に、プライマリ デバイスとピア デバイスの間のリンクが設定される場合、ピア デバイスを Catalyst Center のLAN 自動化設定の一部としてピア デバイスに接続するプライマリ デバイスのインターフェイスを選択する必要があります。

LAN 自動化の 2 段階制限



前述のトポロジの場合、Catalyst Center は次のリンクを設定します。

- ポイントツーポイントのレイヤ 3 は 検出されたデバイス *1* から プライマリ デバイス に接続するためにルートする
- ポイントツーポイントのレイヤ 3 は 検出されたデバイス *1* から ピア デバイス に接続するためにルートする
- ポイントツーポイントのレイヤ 3 は 検出されたデバイス *1* から 検出されたデバイス *2* に接続するためにルートする

検出されたデバイス *3*という名前のデバイスが以下の検出されたデバイス *2*に直接接続されるシナリオを考えてください。検出されたデバイス *2* と検出されたデバイス *3* の間の接続は、LAN 自動化ジョブの一部として設定されません。プライマリデバイスから 2 段階以上離れているためです。

LAN 自動化のステータスの確認

進行中の LAN 自動化セッションのステータスと、完了したセッションの履歴をログとともに表示します。

手順

ステップ 1 メインメニューから次を選択します。**[Provision]** > **[LAN Automation]**。

[LAN自動化（LAN Automation）] ウィンドウには、進行中のセッション、過去のセッションの履歴、および LAN 自動化されたデバイスのステータスペインが表示されます。

ステップ 2 ステータスペインで、[セッションの詳細を表示（See Session Details）] をクリックして、LAN 自動化の全体的なステータス（進行中または完了）とセッションログを表示します。

ステップ 3 完了したセッションの履歴を表示するには、[履歴（History）] タブを選択します。セッションのハイパーリンクをクリックして、詳細とログを表示します。

ステップ 4 LAN 自動化デバイスを確認するには、[LAN自動化されたデバイス（LAN Automated Devices）] タブを選択します。デバイス名をクリックして、デバイス固有のログと構成を表示します。

インターフェイス間のリンクを作成

LAN 自動化を介してインターフェイス間にリンクを追加するには：

手順

ステップ 1 メインメニューから次を選択します。**[Provision]** > **[LAN Automation]**。

ステップ 2 **[LAN 自動化（LAN Automation）]** ウィンドウの [LAN 自動化デバイス（LAN Automated Devices）] タブで、[リンクの追加（Add Link）] をクリックします。

または、**[Workflows]** > **[Add Link]**からリンクを作成できます。

ステップ 3 [Add Link] のワークフローで次の手順に従います。

a) サイトを選択します。

b) リンクを確立する 2 つのデバイスを選択します。

c) LAN 内の IP アドレスプールを選択します。

IP アドレスプールが Catalyst Center から到達可能であることを確認します。

IPv6 の場合、[ポイントツーポイントIPv6リンクローカルアドレッシング（Point-to-point IPv6 Link-Local addressing）]チェックボックスを選択すると、リンクローカルアドレッシングを使用してポイントツーポイントリンクを設定できます。

d) 接続を確立する両方のデバイスのインターフェイスを選択します。
e) [Now] か [Later] をクリックし、リンクをプロビジョニングするタイミングを指定します。
f) 表示されるフィールドにタスクの名前を入力します。
g) [Summary] ウィンドウで、設定を確認します。変更するには、[Edit] をクリックします。
h) [Start Add Link] をクリックします。

[Link Configuration Started Successfully] ウィンドウが表示されます。

ステップ 4 （任意） 設定のステータスを表示するには、[View Status in Activities] をクリックします。

また、**[アクティビティ（Activities）]** > **[タスク（Task）]** でステータスを表示することもできます。

インターフェイス間のリンクの削除

LAN 自動化中に、またはリンクの追加操作を実行して作成されたインターフェイスリンクを削除するには、次の手順を実行します。

手順

ステップ 1 メインメニューから次を選択します。**[Provision]** > **[LAN Automation]**。

ステップ 2 **[LAN自動化（LAN Automation）]** ウィンドウの [LAN自動化デバイス（LAN Automation Devices）] タブで、**[リンクの削除（Delete Link）]** をクリックします。

または、**[Workflows]** > **[Delete Link]** からリンクを削除できます。

ステップ 3 [Delete Link] のワークフローの手順に従います。

a) サイトと 2 つのデバイスを選択します。
b) リンクを削除するこれら両方のデバイスのインターフェイスを選択します。
c) [Now] または [Later] をクリックし、削除プロセスを開始するタイミングを指定します。
d) 表示されるフィールドにタスクの名前を入力します。
e) [Summary] ウィンドウで、設定を確認します。変更するには、[Edit] をクリックします。
f) [Start Delete Link] をクリックします。

[LAN Automation configuration has been removed from the selected interfaces] ウィンドウが表示されます。

ステップ 4 （任意） リンク削除タスクのステータスを表示するには、[View Status in Activities] をクリックします。

また、**[アクティビティ（Activities）]** > **[タスク（Task）]** でステータスを表示することもできます。

LAN 自動化デバイスのホスト名とループバック IP アドレスの編集

LAN タイプの予約済み IP アドレスプールを使用して、LAN 自動化で検出されたデバイスのホスト名とループバック IP アドレスをカスタマイズできます。

（注）
- *n* 日目にデバイスのホスト名とループバック IP アドレスを編集するには、デバイスがインベントリで **[Managed]** の状態になっている必要があります。
- 単一の *n* 日目ワークフローで最大 25 のデバイスのループバック IP アドレスを編集できます。

始める前に

- LAN 自動化でデバイスを検出します。詳細については、LAN 自動化によるネットワークのプロビジョニング （1196 ページ）を参照してください。
- [LAN] タイプの必要な IP アドレスプールを予約します。詳細については、IP アドレスプールの予約 （399 ページ）を参照してください。

手順

ステップ 1 メインメニューから次を選択します。**[Provision]** > **[LAN Automation]**。

ステップ 2 **[LAN Automation]** ウィンドウの **[LAN Automated Devices]** タブで、編集するデバイスの横にあるチェックボックスをオンにします。

ステップ 3 [Edit Device] をクリックします。

ステップ 4 [Edit Devices] ウィンドウで、次の手順を実行します。

a) **[Device Name]** フィールドに、デバイスのホスト名を入力します。

b) [IP Address Pool] ドロップダウンリストから、IP アドレスプールを選択します。

c) [IP Address] フィールドに IPv4 アドレス（サブネットマスクなし）を入力します。

（注） IP アドレスは、選択した IP アドレスプールの範囲内にある必要があります。

d) 必要に応じて、[リセット（Reset）] または [すべてをリセット（Reset All）] オプションを使用して変更を元に戻します。

e) デバイスごとにステップ4.a（1208ページ）、ステップ4.b（1208ページ）、ステップ4.c（1208ページ）を繰り返します。

f) **[検証 (Validate)]** をクリックします。

指定されたIPアドレスを割り当てられない場合、Catalyst Centerにエラーメッセージが表示されます。[IP Address] フィールドに有効な IPv4 アドレスを入力します。

g) [Next] をクリックします。

ステップ 5 [Schedule Edit Device Deployment] ウィンドウで、次のいずれかを実行します。

- **[Now]** オプションボタンをクリックし、タスクに名前を付けて、**[Apply]** をクリックします。
- **[Later]** オプションボタンをクリックし、タスクに名前を付け、開始日、開始時刻、およびタイムゾーンを指定して、**[Apply]** をクリックします。

Strict 検出モードのデバイスの管理

Catalyst Center リリース 2.3.7.5 以降では、検出時のデバイスの照合用に [Relaxed] モードまたは [Strict] モードのいずれかを選択できます。[Strict] モードでは、デバイスの検出を、定義されたリストに制限します。検出リストからデバイスを追加・編集・削除するには、次の手順を実行します。

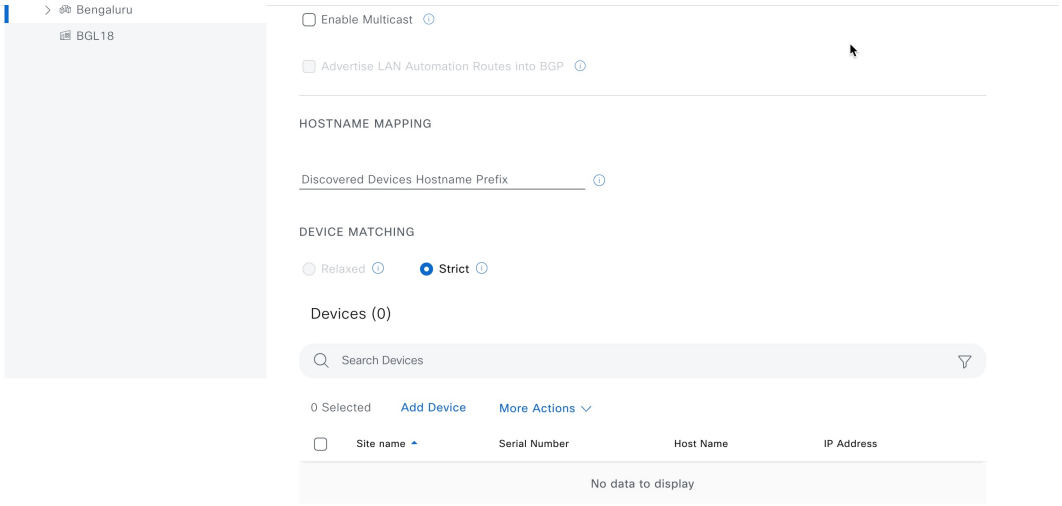
手順

ステップ 1 [LAN Automation] ウィンドウで、[Start LAN Automation] をクリックします。

ステップ 2 シードデバイスを追加し、[Next] をクリックします。

ステップ 3 [Session Attributes] ウィンドウの左側のペインで、建物またはフロアを選択します。

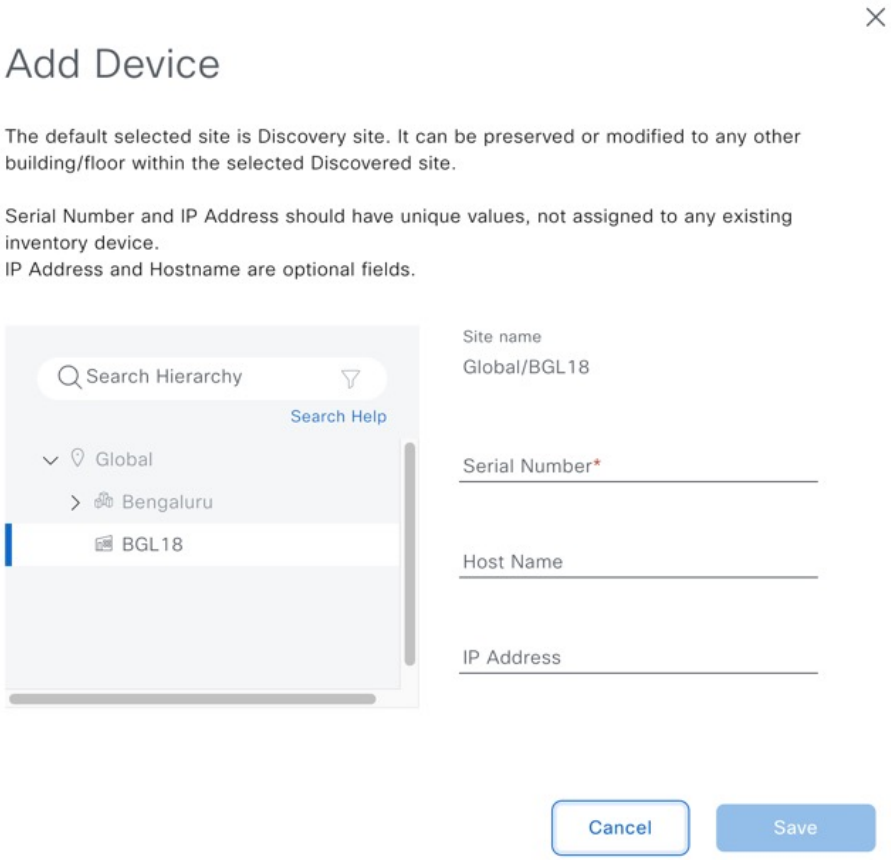
ステップ 4 [Device Matching] で、[Strict] オプションを選択します。



（注） サイトとしてエリアを選択する場合は、デバイスリストを追加する必要があります。この場合、[Strict] モードが自動的に選択され、[Relaxed] モードが無効になります。

ステップ 5 検出リストに対して次のいずれかのオプションを使用して、デバイスを追加します。

- [Add Device]：単一のデバイスを追加するには、このオプションを使用します。
  - [Devices] テーブルで、[Add Device] をクリックして、次の手順を実行します。
    1. エリアを選択した場合は、サイトとして建物またはフロアを選択します。
    2. デバイスの [Serial Number] を入力します。
    3. （オプション）デバイスの [Host Name] と [IP Address] を入力します。
    4. [Save] をクリックします。

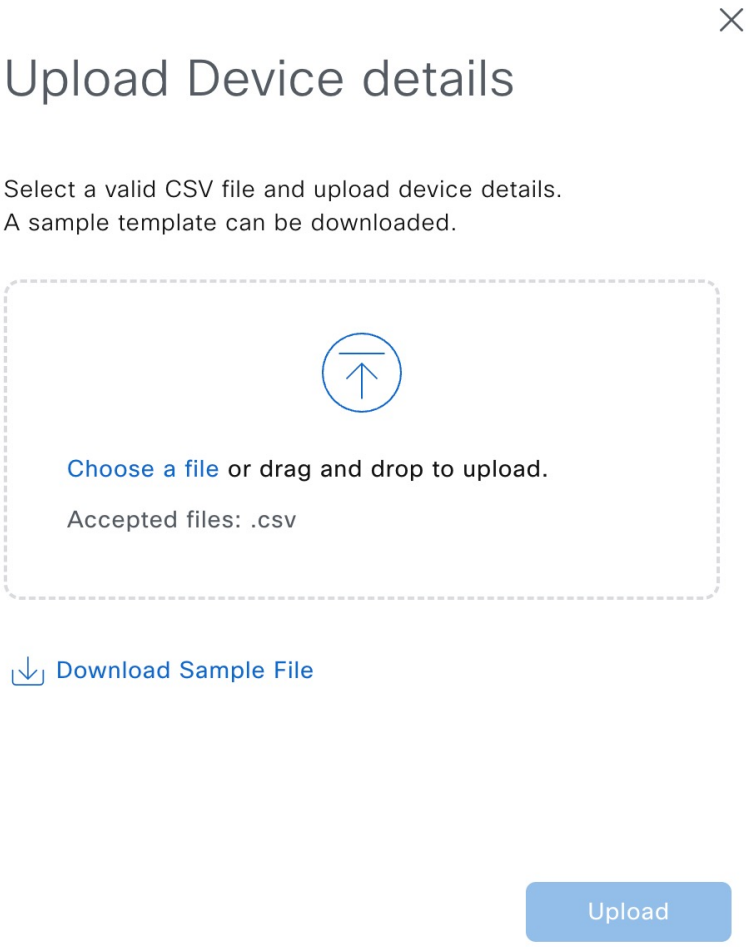


• [Upload Device]：CSV ファイルからデバイスを追加するには、このオプションを使用します。

1. [**Devices**] テーブルで、[**More Actions**] をクリックし、デバイス CSV ファイルをアップロードするためのオプションを選択します。
2. CSV ファイルをアップロードします。

   CSV ファイルをボックスエリアにドラッグアンドドロップするか、[**Choose a File**] をクリックして CSV ファイルを参照します。

   サンプル テンプレートをダウンロードすることもできます。



ステップ 6 検出リストのデバイスを編集するには、次の手順を実行します。

a) 編集するデバイスの隣にあるチェックボックスをオンにし、**[More Actions]** > **[Edit Device]** を選択します。

b) 必要に応じて、デバイスの詳細を編集します。

一度に編集できるデバイスは 1 つだけです。

c) [Save] をクリックします。

ステップ 7 検出リストからデバイスを削除するには、次の手順を実行します。

a) 削除するデバイスの隣にあるチェックボックスをオンにし、**[More Actions]** > **[Delete Device]** を選択します。

複数の削除するデバイスを選択できます。

b) [Delete] アイコンをクリックして、削除アクションを確認します。



第 21 章

SD-Access LISP ファブリックネットワークのプロビジョニング

- Cisco SD-Access ゼロトラスト セキュリティソリューション （1214 ページ）
- ファブリックネットワークについて （1222 ページ）
- Cisco SD-Access のロールベース アクセス コントロール （1228 ページ）
- ファブリックサイトの追加 （1229 ページ）
- ファブリックサイトの移動 （1232 ページ）
- ファブリックサイトの設定 （1234 ページ）
- デバイスをファブリックに追加 （1235 ページ）
- ファブリックからデバイスを削除 （1239 ページ）
- ボーダーノードとしてのデバイスの追加 （1240 ページ）
- LISP Pub/Sub の設定 （1245 ページ）
- ファブリックの再設定 （1246 ページ）
- IP トランジットの作成 （1247 ページ）
- SD-Access トランジットの作成 （1248 ページ）
- ファブリックサイトの認証テンプレートの設定 （1250 ページ）
- ファブリックサイト内のポートの設定 （1252 ページ）
- ファブリックネットワークのワイヤレス SSID の設定 （1254 ページ）
- ファブリックでのワイヤレス メッシュ アクセス ポイントの設定 （1255 ページ）
- ファブリックサイトでのセキュリティサービスの挿入の設定 （1256 ページ）
- 仮想ネットワーク （1256 ページ）
- ファブリックゾーンの設定 （1270 ページ）
- 拡張ノードデバイスの設定 （1278 ページ）
- サプリカントベースの拡張ノードの設定 （1289 ページ）
- ポートチャネルの設定 （1296 ページ）
- マルチキャスト （1299 ページ）
- ファブリックサイトの BGP AS 番号の編集 （1302 ページ）

Cisco SD-Access ゼロトラストセキュリティソリューション

ネットワークは、外部および内部の脅威から守らなければなりません。Cisco SD-Access は、職場にゼロトラストのセキュリティソリューションを提供します。Cisco SD-Access のゼロトラスト セキュリティ ソリューションは、ネットワーク上のあらゆる場所からすべてのユーザとデバイスへセキュアなアクセスを実現します。

Cisco SD-Access ゼロトラストセキュリティ ソリューションには、次の機能が含まれています。

- すべてのエンドポイントの識別と検証：接続している各エンドポイントとの初期レベルの信頼を確立します。
- ポリシーとセグメンテーションの確立：エンドポイントとユーザータイプに基づいて、最小限の特権アクセスを保証します。
- エンドポイントの継続的な監視：エンドポイントを継続的に監視してコンプライアンスを確保します。
- 脅威の軽減：非準拠または悪意のある動作を示すエンドポイントを隔離できます。

Cisco SD-Access ゼロトラスト セキュリティ ソリューションは、職場でのネットワーク設定とお使いのサービスに応じて、柔軟にゼロトラストワークプレイスの実現を支援します。ユーザのネットワークへの接続を、ダイナミックなルールとセグメンテーションの自動化を用いて細かに設定できます。

Cisco SD-Access ゼロトラストセキュリティ ソリューションは、次の機能を使用してネットワーク アクセス ポリシーを自動化します。

- エンドポイントの可視性：エンドポイントを識別してグループ化できます。トラフィックフロー分析を通じて相互作用をマッピングし、アクセスポリシーを定義します。
- トラストモニタリング：エンドポイントの動作を継続的に監視し、脆弱性をスキャンし、持続的なアクセスの信頼性を検証し、不正なエンドポイントや侵害されたエンドポイントを隔離します。
- ネットワーク セグメンテーション：マルチレベルでのセグメンテーションを通じて、グループベースのアクセスポリシーとセキュアなネットワークを確立します。

Cisco SD-Access ゼロトラスト セキュリティ ソリューションで、職場でのネットワーク設定とお使いのサービスに応じて、ゼロトラストワークプレイスを実現するあらゆる方法を模索できます。ネットワークの現状に応じて、ゼロトラストワークプレイスへ移行する最適な道筋を見つけ、それぞれのステップでもたらされる利点を検証できます。

[Zero Trustの概要（Zero-Trust Overview）] ダッシュボード

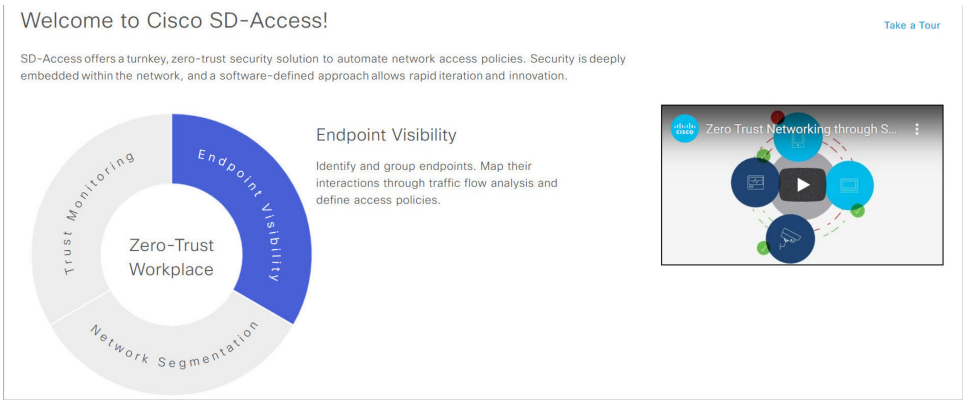
SD-Access の [Zero Trust Overview] ダッシュボードには、Zero Trust ワークプレイスへの移行の概要が示されます。このダッシュボードを表示するには、メインメニューから次を選択します。**[Provision]** > **[Zero Trust Overview]** の順に選択します。

Zero Trust ワークプレイスへの移行には、次のフェーズがあります。

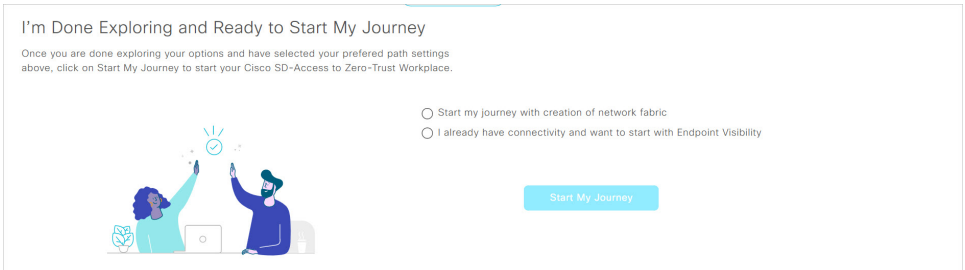
- 0 日目：Zero Trust ワークプレイスジャーニーの開始日。詳細については、[Zero Trustの概要（Zero-Trust Overview）] ダッシュボードの Day-0 ビュー （1215 ページ）を参照してください。
- n 日目：Zero Trust ワークプレイスジャーニーの継続的な監視と設定変更。詳細については、[Zero Trustの概要（Zero Trust Overview）] ダッシュボードの Day-n ビュー （1218 ページ）を参照してください。

[ZeroTrustの概要（Zero-TrustOverview）]ダッシュボードのDay-0ビュー

SD-Access Zero Trust ワークプレイスへの移行の開始前、[Zero Trustの概要（Zero-Trust Overview）] ダッシュボードの Day-0 ビューは、次のセクションで構成されます。







- [Welcome to Cisco SD-Access!]：このセクションには、完全な SD-Access Zero Trust ワークプレイスへの複数の道筋を簡潔に示す概要ビデオが用意されています。また、SD-Access Zero Trust ワークプレイスの中心となる次の項目を含む円もあります。

- エンドポイントの可視性
- 信頼のモニタリング
- ネットワークのセグメント化

各項目にカーソルを合わせると、詳細が表示されます。

- [Explore and start your journey to SD-Access Zero-Trust Workplace]：このセクションでは、ネットワーク設定とサービスに基づいて Zero Trust ワークプレイスへのさまざまな道筋を調べて、ネットワークに最適な道筋を特定できます。このセクションは、ネットワーク接続（Network Connectivity）とサービス（Services）のオプション、および道筋に関する詳細を含む円形のジャーニーマップで構成されています。ネットワーク接続とサービスについて選択したオプションに基づいて、ジャーニーマップには、Zero Trust ワークプレイスへの移行に利用できる道筋が表示されます。

  ジャーニーマップの各推奨ステップに関する詳細を表示するには、ジャーニーマップの周囲にある目的のステップにカーソルを合わせます。

- [I'm Done Exploring and Ready to Start My Journey]：道筋を調べて望ましい設定を選択した後、このセクションを使用して、Zero Trust ワークプレイスへの移行を開始できます。

SD-Access Zero Trust ワークプレイスへの移行の開始

手順

ステップ 1 メインメニューから次を選択します。**[Provision]** > **[Zero Trust Overview]** の順に選択します。

ステップ 2 [SD-Accessゼロトラストワークプレイスの調査と移行の開始（Explore and start your journey to SD-Access Zero-Trust Workplace）] で、次の手順を実行します。

a) [Network Connectivity] 設定で、必要なオプションを選択します。

- Zero Trust ワークプレイスへの移行でワイヤレスデバイスを使用するには、[With Wireless] を有効にします。
- Zero Trust ワークプレイスへの移行で、Cisco Catalyst 9000 シリーズ デバイスを使用するには [With CAT9K] を有効にし、Catalyst Center トラフィック テレメトリ アプライアンス を使用するには [With Traffic Telemetry Appliance] を有効にします。

b) [Services] 設定で、必要なオプションを選択します。

- Zero Trust ワークプレイスジャーニーで Cisco Identity Services Engine を使用するには、**[With ISE]** を有効にします。
- Zero Trust ワークプレイスジャーニーで Talos インテリジェンスを使用するには、**[With Talos]** を有効にします。

- Zero Trust ワークプレイスジャーニーでコントローラベースのアプリケーション認識（CBAR）を使用するには、**[With CBAR Enabled]** を有効にします。

c) （任意） ジャーニーマップの各推奨ステップに関する詳細を表示するには、ジャーニーマップの周囲にある目的のステップにカーソルを合わせます。

ステップ 3 [調査終了、移行開始準備完了（I'm Done Exploring and Ready to Start My Journey）] で、次のオプションのいずれかを選択します。

- ファブリックネットワークを作成し、Zero Trust ワークプレイスへの移行を開始するには、[Start my journey with creation of network fabric] をクリックします。
- すでにファブリックネットワーク接続があり、エンドポイントの可視性から Zero Trust ワークプレイスへの移行を開始する場合は、[I already have connectivity and want to start with Endpoint Visibility] をクリックします。

ステップ 4 [Start My Journey] をクリックします。

ステップ 5 [移行マップの変更（Modify Journey Map）] ダイアログボックスで、次の手順を実行します。

a) ジャーニーマップの設定を確認します。

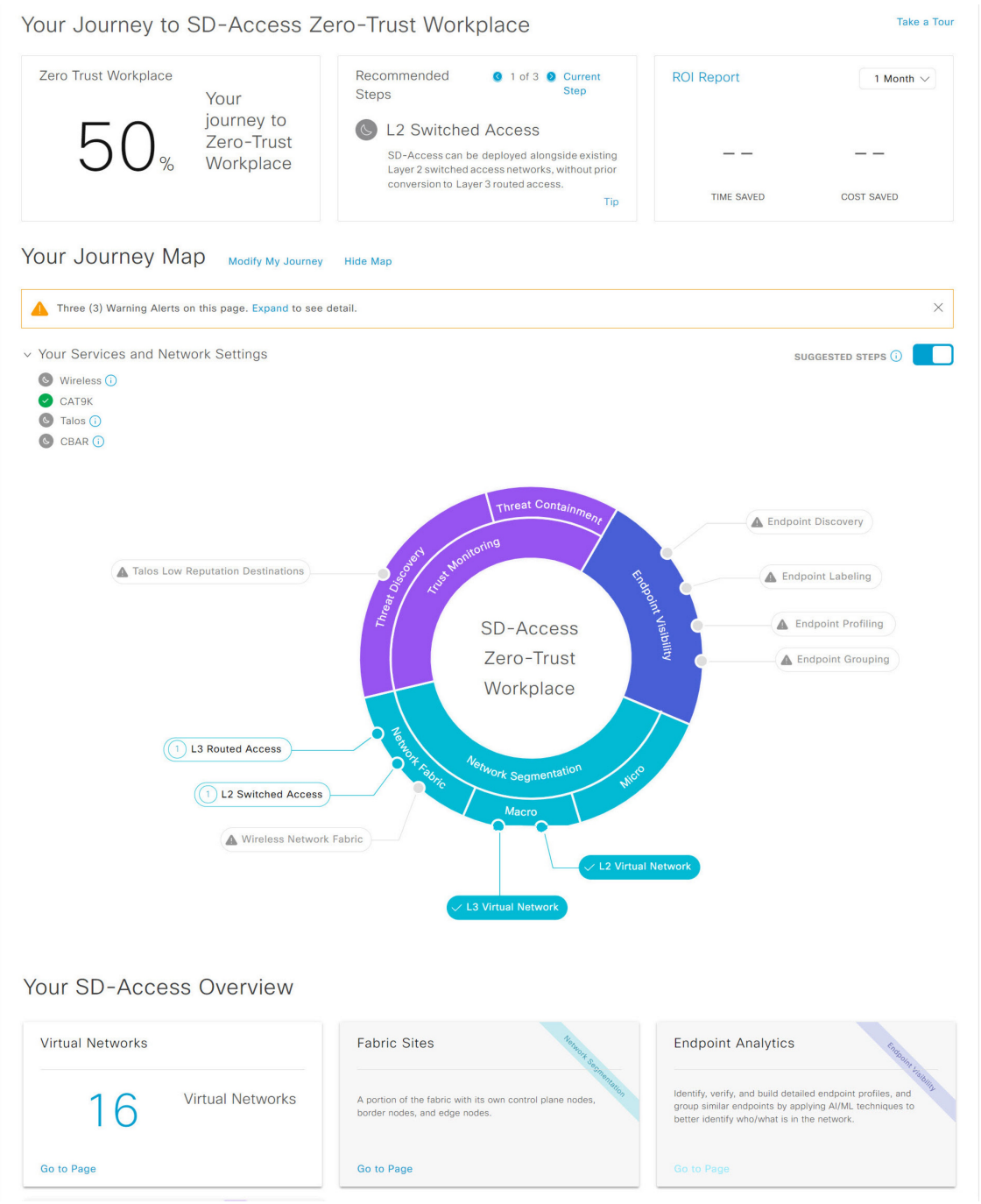
（注）
- Catalyst Center では、ネットワーク用に選択されたサービスが検出されない場合、メッセージが表示されます。
- Catalyst Center では、移行で選択されなかった追加のサービスが検出された場合、メッセージが表示されます。

b) （任意） 選択したサービスをジャーニーマップの設定から削除するには、該当するチェックボックスをオフにします。

c) [Confirm] をクリックします。

[Zero Trustの概要（Zero Trust Overview）] ダッシュボードの Day-n ビュー

SD-Access Zero Trust ワークプレイスへの移行の開始後、[Zero Trustの概要（Zero Trust Overview）] ダッシュボードの Day-n ビューは、次のセクションで構成されます。



- [SD-Access Zero Trustワークプレイスへの移行（Your Journey to SD-Access Zero-Trust Workplace）]：このセクションは、次のようなダッシュレットで構成されています。
  - [Zero Trust Workplace] ダッシュレットには、Zero Trust ワークプレイスへの移行の進行状況がパーセンテージで表示されます。
  - [Recommended Steps] ダッシュレットには、Zero Trust ワークプレイスへの移行で推奨される次のステップが表示されます。すべてのステップをスクロールするには、矢印

ボタン（ と ）を使用します。このダッシュレットには、一部のステップに関するヒントも表示されます。利用可能な場合は、[Tip] をクリックすると、該当するステップのヒントが表示されます。

- [ROI Report] ダッシュレットには、Zero Trust ワークプレイスへの移行を進めるうえで実行されたステップに基づいて、節約された時間とコストが表示されます。レポートの期間を選択するには、このダッシュレットのドロップダウンを使用します。レポートを表示するには、[ROI Report] をクリックします。

- [Your Journey Map]：このセクションには、Zero Trust ワークプレイスへの移行のネットワーク接続とサービス設定の詳細が表示されます。Zero Trust ワークプレイスへの移行を変更するには、[Modify My Journey] をクリックします。ジャーニーマップを非表示にするには、[Hide Map] をクリックします。

  このセクションには、進めている移行に関する警告アラートが表示されます（アラートがある場合）。アラートの詳細を表示するには、[Expand] をクリックします。選択したサービスがネットワークで現在利用できない場合に、そのサービスを移行から削除するには、該当する [Remove From Journey] オプションをクリックします。ネットワークで現在利用できないサービスを利用可能にするには、該当するハイパーリンクをクリックしてそのサービスを取得します。

  移行用に選択したサービスのリストを表示するには、[Your Services and Network Settings] ドロップダウンを展開します。サービスの横にある アイコンは、そのサービスがネットワークで現在利用可能であることを示しています。サービスの横にある アイコンは、そのサービスがネットワークで現在利用できないことを示しています。 該当する アイコンにカーソルを合わせると、利用できないサービスに関する詳細を含む [Update Needed] ダイアログボックスが表示されます。[必要な更新（Update Needed）] ダイアログボックスで、次のタスクを実行します。

  - 移行からサービスを削除するには、[Remove From Journey] をクリックします。
  - ネットワークで利用できないサービスを取得するには、該当するハイパーリンクをクリックします。

  ジャーニーマップの周囲にあるステップについて推奨される順番を表示するには、[Suggested Steps] トグルボタンを有効にします。

  ジャーニーマップの各ステップに関する詳細を表示するには、ステップにカーソルを合わせます。

  ステップの横にある アイコンは、その構成が未完了であることを示しています。ステップの横にある数字（例：）は、ジャーニーマップにおける推奨ステップの順番を提案しています。ステップの横にある アイコンは、その構成が完了していることを示しています。

- [Your SD-Access Overview]：このセクションは、Zero Trust ワークプレイスへの移行の各機能領域のダッシュレットで構成されています。関連するウィンドウを開くには、該当する

[Go to Page] オプションをクリックします。各ダッシュレットの右上には、Zero Trust ワークプレイスへの移行の対応する中心項目が示されています。

SD-Access Zero Trust ワークプレイスへの移行の変更

手順

ステップ 1 メインメニューから次を選択します。**[Provision]** > **[Zero Trust Overview]** の順に選択します。

ステップ 2 [Your Journey Map] で、[Modify My Journey] をクリックします。

ステップ 3 [SD-Accessゼロトラストワークプレイスの調査と移行の開始（Explore and start your journey to SD-Access Zero-Trust Workplace）] で、次の手順を実行します。

a) [Network Connectivity] 設定で、必要なオプションを選択します。

- Zero Trust ワークプレイスへの移行でワイヤレスデバイスを使用するには、[With Wireless] を有効にします。
- Zero Trust ワークプレイスへの移行で、Cisco Catalyst 9000 シリーズ デバイスを使用するには [With CAT9K] を有効にし、Catalyst Center トラフィック テレメトリ アプライアンス を使用するには [With Traffic Telemetry Appliance] を有効にします。

b) [Services] 設定で、必要なオプションを選択します。

- Zero Trust ワークプレイスジャーニーで Cisco Identity Services Engine を使用するには、**[With ISE]** を有効にします。
- Zero Trust ワークプレイスジャーニーで Talos インテリジェンスを使用するには、**[With Talos]** を有効にします。
- Zero Trust ワークプレイスジャーニーでコントローラベースのアプリケーション認識（CBAR）を使用するには、**[With CBAR Enabled]** を有効にします。

c) （任意） ジャーニーマップの各推奨ステップに関する詳細を表示するには、ジャーニーマップの周囲にある目的のステップにカーソルを合わせます。

ステップ 4 [調査終了、移行開始準備完了（I'm Done Exploring and Ready to Start My Journey）] で、次のオプションのいずれかを選択します。

- ファブリックネットワークを作成し、Zero Trust ワークプレイスへの移行を開始するには、[Start my journey with creation of network fabric] をクリックします。
- すでにファブリックネットワーク接続があり、エンドポイントの可視性から Zero Trust ワークプレイスへの移行を開始する場合は、[I already have connectivity and want to start with Endpoint Visibility] をクリックします。

ステップ 5 [Modify My Journey] をクリックします。

ステップ 6 [移行マップの変更（Modify Journey Map）] ダイアログボックスで、次の手順を実行します。

a) ジャーニーマップの設定を確認します。

（注）
- Catalyst Center では、ネットワーク用に選択されたサービスが検出されない場合、メッセージが表示されます。
- Catalyst Center では、移行で選択されなかった追加のサービスが検出された場合、メッセージが表示されます。

b) （任意） 選択したサービスをジャーニーマップの設定から削除するには、該当するチェックボックスをオフにします。

c) [Confirm] をクリックします。

ファブリックネットワークについて

ファブリックネットワークは、1 つまたは複数の場所で単一のエンティティとして管理されるデバイスの論理グループです。ファブリックネットワークを使用すると、仮想ネットワークやユーザーおよびデバイスグループの作成、高度なレポート作成などが可能になります。その他の機能には、アプリケーション認識、トラフィック分析、トラフィックの優先順位付け、最適なパフォーマンスと運用効率のためのステアリングのインテリジェントサービスがあります。

Catalyst Center では、デバイスをファブリックネットワークに追加できます。これらのデバイスは、ファブリックネットワーク内のコントロールプレーン、ボーダーデバイスまたはエッジデバイスとして機能するように設定できます。

ファブリックサイト

ファブリックサイトは、コントロールプレーン、ボーダー、エッジ、ワイヤレスコントローラ、ISE PSN のネットワークデバイスの固有のセットを持つ独立したファブリック領域です。異なるレベルの冗長性とスケールは、DHCP、AAA、DNS、インターネットなどのローカルリソースを含むことにより、サイトごとに設計することができます。

ファブリックサイトは、単一の物理的ロケーション、複数のロケーション、またはロケーションのサブセットのみをカバーすることができます。

- 単一の場所: ブランチ、キャンパスまたはメトロ キャンパス
- 複数の場所: メトロ キャンパス + 複数ブランチ
- ロケーションのサブセット: キャンパス内での構築または領域

Software-Defined Access ファブリックネットワークは、複数のサイトで構成されることがあります。各サイトは、優れた拡張性、復元力、生存性、およびモビリティを備えます。ファブ

リックサイトの全体的な集約は、多数のエンドポイントに対応し、モジュール方式で（または水平方向に）拡張します。複数のファブリックサイトは、トランジットを使用して相互接続されます。

トランジット

トランジットとは、2 つ以上のファブリックサイトを相互接続したり、ファブリックサイトと外部ネットワーク（インターネット、データセンターなど）を接続するサイトです。トランジットネットワークには 2 つのタイプがあります。

- IP トランジット：通常の IP ネットワークを使用して、外部ネットワークに接続するか 2 つ以上のファブリックサイトを接続します。IP トランジットは、従来型の IP ベース（VRF-LITE、MPLS）ネットワークを利用します。これには、サイト間での VRF と SGT の再マッピングが必要です。
- SD-Access トランジット：LISP/VxLAN のカプセル化を使用して 2 つのファブリックサイトを接続します。SD-Access トランジットエリアは、独自のコントロールプレーンノードを持つがエッジノードやボーダーノードはないファブリックの一部として定義できます。ただし、外部ボーダーを持つファブリックを使用することもできます。SD-Access トランジットを使用すると、エンドツーエンドポリシープレーンは SGT グループタグを使用して維持されます。

ファブリックの準備状況、イメージの互換性、およびコンプライアンスのチェック

ファブリックの準備状況チェック

ファブリックの準備状況チェックは、デバイスがファブリックに追加される準備が整っていることを確認するために、デバイス上で実行される事前プロビジョニングチェックのセットです。ファブリックの準備状況チェックは、デバイスのプロビジョニング時に自動的に実行されるようになりました。インターフェイス VLAN とマルチ VRF の設定チェックは、ファブリックの準備状況チェックの一環としては行われません。

ファブリックの準備状況チェックには、次の項目が含まれます。

- 接続チェック：エッジノードからマップサーバーへの接続、エッジノードからボーダーへの接続など、デバイス間で必要な接続を確認します。
- 既存の設定チェック：SD-Access を介してプッシュされる設定と競合する設定がデバイスにあり、それが後でエラーになる可能性がないかを確認します。
- ハードウェアバージョン：デバイスのハードウェアバージョンがサポートされているかどうかを確認します。
- イメージタイプ：サポートされているイメージタイプ（IOS XE、IOS、NXOS、Cisco Controller）を使用してデバイスが実行されているかどうかを確認します。

- ループバック インターフェイス：デバイス上のループバック インターフェイスの設定を確認します。SDA アプリケーションを使用するには、デバイスが番号 0 のループバック インターフェイスを持ち、デバイスに IP アドレスが設定されている必要があります。番号 0 のループバック インターフェイスがないと、Loopback0 がデフォルトでルーティング ロケータ（RLOC）として使用されるため、ファブリック プロビジョニング エラーが発生する可能性があります。
- ソフトウェアライセンス：デバイスが適切なソフトウェアライセンスを使用して実行されているかどうかを確認します。

ファブリックの準備状況チェックの実行中にエラーが検出された場合、エラー通知が [topology] エリアに表示されます。問題を修正し、デバイスのプロビジョニング ワークフローを続行できます。

イメージの互換性チェック

ネットワークデバイス（ファブリック展開の前後）に、Catalyst Center パッケージバージョンに基づいて推奨されるまたはサポートされているソフトウェアイメージのバージョンと互換性があることを確認するために、Catalyst Center はイメージ互換性チェックを実行してネットワークデバイスを評価します。

ネットワークデバイスが互換性のないソフトウェアイメージを実行している場合は、**[Provision]** > **[Inventory]** > **[Image Compatibility]** 列に アイコンが表示されます。*Cisco SD-Access* 互換性マトリックスで、デバイスでサポートされているソフトウェアイメージのバージョンを確認し、デバイスのプロビジョニング ワークフローを続行できます。

ファブリック コンプライアンス チェック

ファブリック コンプライアンスとは、ファブリック プロビジョニング中に設定されたユーザー インテントに従って動作するデバイスの状態です。ファブリック コンプライアンス チェックは、次の条件に基づいてトリガーされます。

- 有線デバイスの場合は 24 時間ごと、ワイヤレスデバイスの場合は 6 時間ごと。
- 有線デバイスで設定が変更された場合。

  有線デバイスの設定変更によって SNMP トラップがトリガーされ、それによってコンプライアンスチェックがトリガーされます。Catalyst Center サーバーが SNMP サーバーとして設定されていることを確認します。

次のコンプライアンスチェックを実行し、デバイスがファブリックに準拠していることを確認します。

- 仮想ネットワーク：Catalyst Center 上の仮想ネットワークのユーザーインテントの現在の状態に準拠するように、必要な VRF がデバイスに設定されているかどうかを確認します。
- ファブリックロール：デバイスの設定が Catalyst Center のファブリックロールのユーザーインテントに準拠しているかどうかを確認します。
- セグメント：セグメントの VLAN 設定と SVI 設定を確認します。

- ポートの割り当て：VLAN および認証プロファイルのインターフェイス設定を確認します。

ファブリックの正常性チェック

SD-Access アプリケーションの正常性は、アプリケーションのステータスを示すために定期的にチェックされます。SD-Access の正常性チェックには、SD-Access アプリケーションの古いデータベースエントリのチェックも含まれ、これによりファブリックのプロビジョニングが中断される可能性があります。

SD-Access アプリケーションのステータスは、**[System]** > **[System 360]** > **[System Health]** ページで確認できます。アプリケーションの正常性をチェックする方法の詳細については、『Cisco Catalyst Center Administrator Guide』の「Use System 360」および「Monitor System Health」を参照してください。

検証ツールを使用して、SD-Access アプリケーションの正常性ステータスに登録することで、同じチェックを実行することもできます。検証ツールは、**[System]** > **[System 360]** > **[System Health]** ページで使用できます。新しい検証を実行する場合は、**[Validation Set(s) selection]** フィールドの **[Application Health Status]** チェックボックスをオンにしてください。検証ツールにアクセスして実行する方法の詳細については、『Cisco Catalyst Center Administrator Guide』の「Use the Validation Tool」を参照してください。

SD-Access アプリケーションのステータスには、次の 3 つの値があります。

- **HEALTHY**：SD-Access アプリケーションが期待どおりに動作しており、すべてのプロビジョニング アクティビティが許可されていることを示します。
- **UNHEALTHY**：依存サービスが正常でないために SD-Access アプリケーションが動作していないことを示します。この状態では、SD-Access ファブリックのすべてのプロビジョニング アクティビティがブロックされる可能性があります。
- **DEGRADED**：すべての依存サービスが動作しているものの、SD-Access アプリケーションにデータベースの不整合があることを示します。この状態は、1 つ以上のファブリックサイトの機能またはプロビジョニングに影響を与える可能性があります。

  SD-Access アプリケーションが DEGRADED 状態である場合は、Cisco TAC に連絡して問題を解決してください。

ファブリックのスケールチェック

スケールチェックは、ファブリックサイトのエンティティに対して定義されたスケール制限またはしきい値をモニターします。定義されたスケール制限に近づいている、または制限を超えているファブリックエンティティの数を可視化します。スケールチェックは、エンティティがファブリックサイトでプロビジョニングされるたびに実行されます。

（注） スケールチェックは、潜在的なスケール違反を可視化するためのガイドラインとして機能するものであり、追加のファブリックエンティティのプロビジョニングを妨げるような強制はしません。

スケールチェックのステータスは、**[Provision]** > **[SD-Access]** > **[Fabric Sites]** ウィンドウの **[Application Checks]** 列で確認できます。[アプリケーションチェック（Application Checks）] 列には、スケールチェックの結果に基づいて次の状態が表示されます。

- [Critical]：ファブリックエンティティが定義されたスケール制限の 95% を超えたことを示します。
- [Warning]：ファブリックエンティティが定義されたスケール制限の 75% を超えたことを示します。
- 緑色のチェックマーク：SD-Access アプリケーションに問題がないことを示します。
- [Not Applicable]：ファブリックサイトに関連付けられたエンティティがないことを示します。

[Critical] および [Warning] ステータスの場合、インジケータをクリックすると、スケールチェックの詳細情報を確認できます。

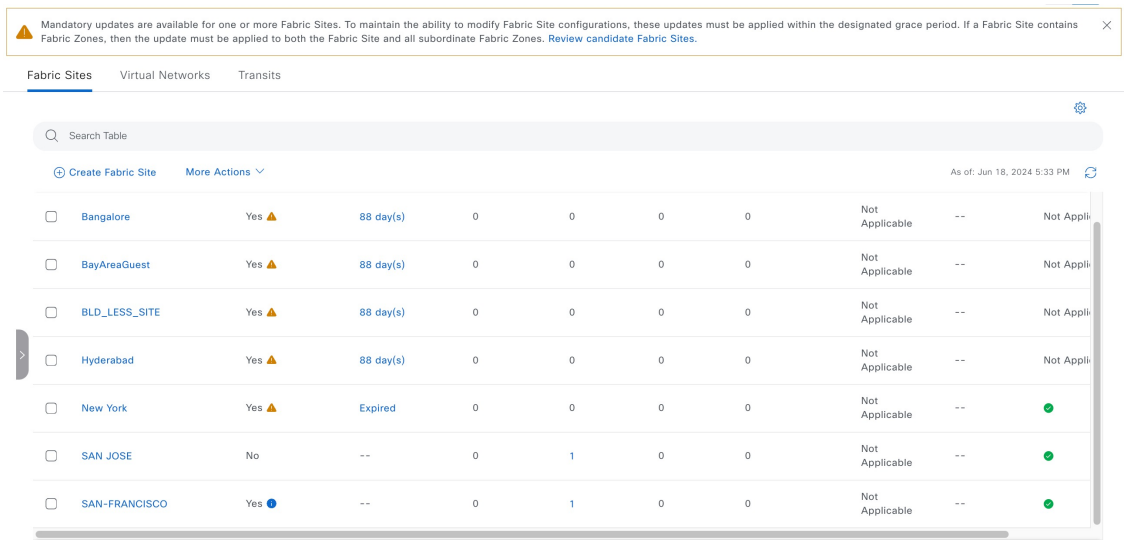
ファブリックサイトごとのスケールしきい値の詳細については、*Cisco Catalyst Center データシート*の「アプライアンスのスケール」を参照してください。

ファブリックサイトの更新

ファブリックサイトの概要ページには、ファブリックサイトで使用可能な設定の更新と、それらの更新を適用するための猶予期間に関する情報が表示されます。指定された猶予期間内は、サイトで使用可能な必須の設定更新を適用するためのバナーメッセージが表示されます。猶予期間（デフォルトでは 180 日）が終了すると、更新が適用されるまでファブリックサイトで設定を行うことはできません。バナーの **[Review candidate Fabric Sites]** リンクをクリックすると、必須の更新が必要なファブリックサイトを表示できます。

[ファブリックサイト（Fabric Sites）] テーブルの列には、次を含む設定の更新情報が表示されます。

- **[Outstanding Updates]**：サイトとその関連ゾーンで使用可能な更新に基づいて、**[Yes]** または **[No]** が表示されます。
- **[Update Grace Period]**：ファブリックサイトとその関連ゾーンの中で、更新を適用するための最短の残り時間（日数）を表示します。値をクリックすると、サイトとその関連ゾーンの個々の猶予期間を表示できます。





次の表で、これらの列に表示される値について説明します。

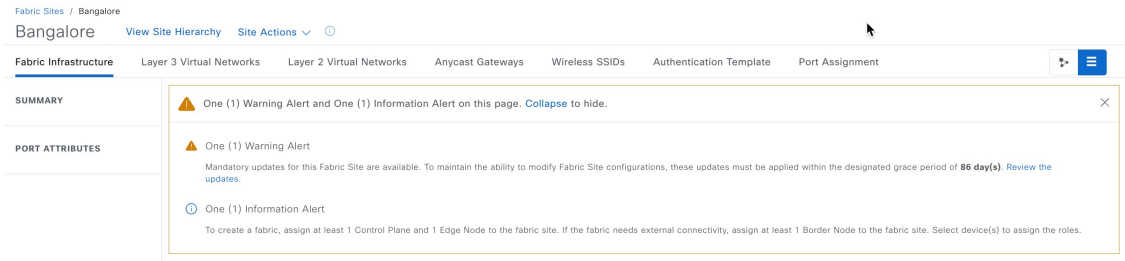
未処理の更新	猶予期間の更新	説明
情報アイコン付きの **[Yes]**。	空白の値を表示します。	更新は利用可能ですが、前提条件が満たされていないため、更新の適用に関するタイマーがないことを示します。猶予期間タイマーは、前提条件が満たされ、更新を適用する準備が整うと開始されます。

未処理の更新	猶予期間の更新	説明
警告アイコン付きの **[Yes]**。	ファブリックサイトとその関連ゾーンの中で、更新を適用するための最短の残り時間（日数）を表示します。サイトまたはそのいずれかの関連ゾーンの猶予期間が終了した場合、列には **[Expired]** と表示されます。	サイトまたはその関連ゾーンに未処理の更新があることを示します。値をクリックすると、サイトとその関連ゾーンの個々の猶予期間が表示されます。
なし	空白の値を表示します。	サイトとその関連ゾーンに未処理の更新がないことを示します。

未処理の更新があるサイトをクリックすると、更新の可用性と猶予期間に基づいて、ファブリックサイトのウィンドウに次のような設定の更新に関するアラートが表示されます。

- アクティブな猶予期間のある準備の整った更新：警告ポップアップウィンドウと、更新の可用性と更新を適用する猶予期間に関するアラートが表示されます。
- 猶予期間が終了している準備の整った更新：エラー ポップアップ ウィンドウと、更新の猶予期間が終了しており、すべてのファブリックサイト設定が一時停止されていることを示すクリティカルアラートが表示されます。
- 準備が整っていない更新：サイトの更新は利用可能ですが、前提条件を満たしていないことを示す情報アラートが表示されます。利用可能な更新を確認して、導入の準備ができます。

アラートダイアログボックスで、**[Expand]** をクリックしてアラートの詳細を表示し、**[Review the updates]** リンクをクリックして、使用可能な更新を表示して適用します。



Cisco SD-Access のロールベース アクセス コントロール

Catalyst Center でのロールベース アクセス コントロールにより、ユーザーがアクセスできる機能と権限を定義するカスタムロールを作成できます。Cisco SD-Access の場合、Catalyst Center では、次のような **SD-Access** 機能を持つカスタムロールを作成することが可能です。

- Cisco SD-Access ファブリックのロールベース アクセス コントロール設定を簡素化する。

- カスタムロールを割り当てられたユーザーが SD-Access ファブリックを作成して管理できるようにする。
- 依存機能に対するアクセス権限を手動で設定できないようにする。**SD-Access** のアクセス権限を設定すると、デバイス検出、デバイスプロビジョニング、PnP、コンプライアンス、SWIM をはじめとする、他のすべての依存機能が必要な権限とともに自動的に選択されます。これらの権限を手動で再設定しないことを推奨します。

Catalyst Center のカスタムロールの詳細については、「*Cisco Catalyst Center Administrator Guide*」を参照してください。

ファブリックサイトの追加

始める前に

IP デバイストラッキング（IPDT）がすでにサイトに設定されている場合にのみ、ファブリックサイトを作成できます。IPDTを有効にするには、**[設計（Design）]** > **[ネットワーク設定（Network Settings）]** > **[テレメトリ（Telemetry）]** に移動し、[有線エンドポイントデータコレクション（Wired Endpoint Data Collection）] エリアで、[このサイトでのCatalyst Center有線エンドポイントデータ収集の有効化（Enable Catalyst Center Wired Endpoint Data Collection At This Site）] オプションボタンをクリックします。

IPv6 アンダーレイのサポートについて、以下の要件が満たされていることを確認してください。

- サポートされているプラットフォーム：Cisco IOS XE 26.1.1 以降、Cisco ISE リリース 3.5 パッチ 3。
- サポートされている製品：Cisco Catalyst 9000 シリーズ スイッチ。

  Cisco Catalyst 9200、IE9300、IE3500 シリーズ スイッチは、ファブリックエッジロールではサポートされていませんが、拡張ノードおよびポリシー拡張ノードロールではサポートされています。Cisco Catalyst 9200 シリーズ スイッチは、サプリカントベースの拡張ロールでサポートされています。

  Cisco Catalyst C9350、C9610、9550、9600x、および 9500x シリーズ スイッチは、IPv6 アンダーレイファブリックのファブリックロールと、IPv4 ファブリックサイトのデュアルスタック ボーダー ロールではサポートされません。
- ファブリックサイトは、IPv4 または IPv6 のいずれかのアンダーレイをサポートしますが、両方をサポートすることはできません。
- IPv6 アンダーレイは、LISP Pub/Sub SDA ファブリックでのみサポートされます。
- IPv6 オーバーレイマルチキャストは、IPv4 と IPv6 両方のアンダーレイ ファブリック サイトで、HER/ユニキャストモードでサポートされます。

手順

ステップ 1 メインメニューから次を選択します。 **[Provision]** > **[Fabric Sites]**.

ステップ 2 [SUMMARY] で、ファブリックサイトの数を示す数字をクリックします。

結果のウィンドウには、すでに作成されているすべてのファブリックサイトとその情報（正常性スコア、ファブリックゾーン、ファブリックデバイス、ファブリックロール、接続されたトランジットなど）が表形式で表示されます。

選択した列のみを表示するようにテーブルビューをカスタマイズできます。ウィンドウの右上隅にある歯車アイコンを使用して、[Table Settings] を編集し、[Apply] をクリックして変更を適用します。

ステップ 3 [Create Fabric Sites] をクリックします。

または、最初の 3 つの手順の代わりに、メニューアイコンをクリックして次を選択します。**[Workflow]** > **[Create Fabric Sites and Fabric Zones]** の順に選択します。

ステップ 4 [Create Fabric Sites] ウィンドウで、[Let's Do it] をクリックして、ワークフローに直接移動します。

ステップ 5 [Fabric Site Location] ウィンドウで、ファブリックサイトとして追加するエリア、建物、またはフロアを選択します。

ステップ 6 [Wired Endpoint Data Collection] ウィンドウで、[Wired Endpoint Data Collection] チェックボックスがオンになっていることを確認します。

ステップ 7 ファブリックの [アンダーレイIPアドレッシング（Underlay IP Addressing）] を選択します。

- デュアルスタック Catalyst Center 展開の場合、[IPv4] または [IPv6] のいずれかを選択できます。
- シングルスタック Catalyst Center 展開の場合、アンダーレイ IP アドレッシングタイプとして [IPv4] または [IPv6] のいずれかがデフォルトで選択されます。

ステップ 8 [Authentication Template] ウィンドウで、次の手順を実行します。

a) ファブリックサイトの認証テンプレートを選択します。

テンプレートオプション	説明
クローズド認証	認証前のすべてのトラフィック（DHCP、DNS、ARP など）が廃棄されます。
オープン認証	ホストには、802.1X 認証を受ける必要なくネットワークアクセスが許可されます。
影響小	スイッチポートに ACL を適用することでセキュリティを追加して、認証前に非常に制限されたネットワークアクセスを許可します。ホストが正常に認証されると、追加のネットワーク アクセスが許可されます。
なし（None）	なし。

b) （オプション）[Closed Authentication]、[Open Authentication]、または [Low Impact] を選択した場合は、[Edit] をクリックして認証設定を編集します。

設定	タスク
[First Authentication Method]	[802.1x] または [MAC Authentication Bypass (MAB)] を選択します。
[802.1x Timeout (in seconds)]	スライダを使用して、802.1x タイムアウトを秒単位で指定します。
Wake On LAN	[はい（Yes）] または [いいえ（No）] を選択します。
ホスト数	[Unlimited] または [Single] を選択します。
音声 VLAN	このチェックボックスを使用して、サイトのデフォルトの音声 VLAN（VLAN 2046）を有効または無効にします。
BPDU ガード	このチェックボックスを使用して、すべての [Closed Authentication] ポートでブリッジプロトコル データ ユニット（BPDU）ガードを有効または無効にします。
[Pre-Authentication Access Control List]	IPv4 および IPv6 用の事前認証アクセス制御リスト（ACL）を設定できます。 **1.** トグルボタンを有効にして、[Low Impact] 認証の事前認証制御を設定します。 **2.** [Implicit Action] ドロップダウンリストから、暗黙的なアクションを選択し、ルールの説明を入力します。 **3.** アクセスコントラクトを追加するには、[Add Contract Action] をクリックし、ルールを選択して、[Apply Table] をクリックします。

ステップ 9 （オプション）[Fabric Zones] ウィンドウで、次のいずれかのオプションを選択します。

オプション	タスク
後でファブリックゾーンを指定する場合	[Setup Fabric Zones Later] をクリックします。
ファブリックゾーンを指定し、範囲指定されたサブネットを作成する場合	[Setup Fabric Zones Now] をクリックし、表示されているネットワーク階層からファブリックサイトを選択します。

ステップ 10 [Summary] ウィンドウで、ファブリックサイトの設定を確認します。

ここでファブリックサイトまたはゾーン設定を編集できます。

ステップ 11 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 12 [Tasks] ウィンドウで、タスクの展開を監視します。

ステップ 13 サイトとゾーンがプロビジョニングされるまでに数秒かかります。サイトの作成が成功すると、「Fabric Site Creation Completed」というメッセージが表示されます。

次に、新しいファブリックサイトを作成するか [Tasks] ウィンドウでアクティビティを表示するかを選択できます。

ファブリックサイトの移動

ファブリックサイトを作成した後、次の方法でサイト階層を変更できます。

- ファブリックサイトを別のファブリックサイトの下に移動することはできず、ファブリックサイトのネストは許可されません。
- サイト、ビルディング、またはフロアが（ファブリックゾーンまたはファブリックサイトのメンバーとして）ファブリックサイトの一部になると、そのファブリックサイトの階層内にとどまる必要があります。外部に移動することはできません。
- 移動中の競合を防ぐため、現在の親サイトと新しい親サイト間でネットワーク設定とネットワークプロファイルが一致していることが検証されます。

図 *28* : サンプルのサイト階層

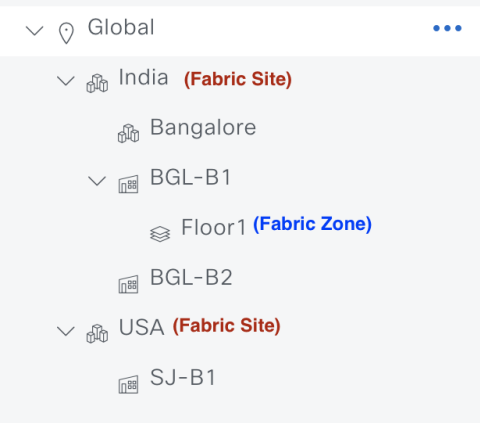


表 *51* : サンプルのサイト移動操作

移動操作	可/不可	Reason
サイト *India* を *Global* の下に作成されたサイト *Asia* に移動	対応	新しい親または新しい先祖がファブリックサイトではないため、サイトを移動できる
既存のファブリックサイト *USA* の下にサイト *India* を移動	非対応	新しいファブリックサイトの下にサイトを移動することはできない
ビルディング *BGL-B1* を *USA* に移動	非対応	あるファブリックサイトから別のファブリックサイトにビルディングを移動することはできない
ビルディング *BGL-B1* を *Global* の下に作成された新しいサイト *Asia* に移動	非対応	ファブリックサイトの外にビルディングを移動することはできない
既存のファブリックサイト内の新しいビルディング *BGL-B2* にフロア *Floor1* を移動	対応	ファブリックサイト内でゾーンを移動できる
フロア *Floor1* を別のファブリックサイトの新しいビルディング *SJ-B1* に移動	非対応	ゾーンを別のファブリックサイトに移動することはできない
ビルディング *BGL-B1* を *Bangalore* に移動	対応	*India* ファブリックサイト内でビルディングを移動できる

ファブリックサイトの設定

ファブリックサイトを作成したら、ホストがファブリックサイトに接続するためのデバイス、仮想ネットワーク、および認証方式を設定できます。

[Provision（プロビジョニング）]>**[SD-Access]**>**[ファブリックサイト（Fabric Sites）]**メニューでファブリックサイトを選択し、次のタブを使用します。

- [Fabric Infrastructure]：デバイスをファブリックロールに割り当てます。
- [Layer 3 Virtual Networks]：ファブリックサイトのレイヤ 3 仮想ネットワークを作成するか、既存のレイヤ 3 仮想ネットワークをファブリックサイトに割り当てます。
- [Layer 2 Virtual Networks]：ファブリックサイトのレイヤ 2 仮想ネットワークを作成するか、既存のレイヤ 2 仮想ネットワークをファブリックサイトに割り当てます。
- [Anycast Gateways]：ファブリックサイトのレイヤ 3 仮想ネットワークのエニーキャストゲートウェイを作成します。
- [Authentication Template] ：ファブリック用の認証テンプレートを選択します。
- [Wireless SSIDs] ：ホストがアクセスできるネットワーク内のワイヤレス SSID を指定します。ゲスト SSID またはエンタープライズ SSID を選択し、アドレスプールを割り当てることができます。
- [Port Assignment] ：ファブリックサイトに接続するデバイスのタイプに応じて、各ポートに固有の設定を適用します。

これらの各操作については、後のセクションで説明します。

（注） 制約事項は次のとおりです。

- Cisco SD-Access 展開環境では、AP、拡張ノード、およびユーザーデバイス（単一のコンピュータまたは単一のコンピュータと電話機など）と、トランクポートを必要とするデバイス（単一サーバーなど）のみがサポートされます。
- 内部スイッチまたは仮想スイッチを備えたサーバーはサポートされていません。
- その他のネットワーキング機器（ハブ、ルータ、スイッチなど）はサポートされていません。

デバイスをファブリックに追加

ファブリックサイトを作成すると、そのファブリックサイトにデバイスを追加できます。デバイスがコントロールプレーンノード、エッジノード、またはボーダーノードとして機能する必要があるかどうかも指定できます。

IP デバイストラッキング（IPDT）がファブリックサイトに設定されている場合にのみ、新しいデバイスをファブリックサイトに追加できます。IPDTを有効にするには、**[設計（Design）]**> **[ネットワーク設定（Network Settings）]** > **[テレメトリ（Telemetry）]**に移動し、[有線エンドポイント データ収集（Wired Endpoint Data Collection）] エリアで、[このサイトでのCatalyst Center 有線エンドポイントデータ収集の有効化（Enable Catalyst Center Wired Endpoint Data Collection At This Site）] オプションボタンをクリックします。

アクセスロールが割り当てられ、サイトで IPDT を有効にする前にプロビジョニングされたデバイスは、ファブリックに追加できません。このようなデバイスは、ファブリックサイトに追加する前に再プロビジョニングしてください。プロビジョニング ワークフローを調べて、デバイスでの [Deployment of IPDT] のステータスを確認します。

（注）

- ファブリックサイト内のデバイスをコントロールプレーンノードまたはボーダーノードとして指定する手順はオプションです。それらのロールがないデバイスもあります。ただし、各ファブリックサイトには、少なくとも 1 つのコントロール プレーン ノード デバイスと 1 つのボーダーノードデバイスが存在する必要があります。有線ファブリックの現在のリリースでは、冗長性を確保するために最大 6 つのコントロール プレーン ノードを追加できます。
- 現在、シスコ ワイヤレス コントローラは 2 つのコントロールプレーンノードとのみ通信します。
- ファブリックに追加された後にデバイスのロールを変更することはできません。ロールを変更するには、ファブリックからデバイスを削除して再度追加します。

始める前に

デバイスをプロビジョニングします（まだプロビジョニングしていない場合）。

- **[Provision]** > **[Network Devices]** > **[Inventory]** ウィンドウに、検出されたデバイスが表示されます。
- ファブリックの準備状況チェックに合格し、プロビジョニングする準備が整ったら、トポロジビューにデバイスが灰色で表示されます。
- ファブリックの準備状況チェックの実行中にエラーが検出された場合、エラー通知が [topology] エリアに表示されます。[See more details] をクリックして、結果のウィンドウに一覧表示された問題のあるエリアを確認します。問題を修正し、[Re-check] をクリックして問題が解決されていることを確認します。

- 問題解決の一環としてデバイス構成を更新する場合は、そのデバイスに対して **[Inventory] [Resync]** を実行して、デバイス情報を再同期してください。

（注） ファブリックの準備状況チェックに失敗しても、デバイスのプロビジョニングを続行できます。

手順

ステップ 1 メインメニューから次を選択します。**[Provision]** > **[Fabric Sites]**。

ステップ 2 [SUMMARY] で、ファブリックサイトの数を示す数字をクリックします。

ステップ 3 デバイスを追加するファブリックサイトを選択します。

インベントリされたネットワーク内のすべてのデバイスが結果のトポロジビューに表示されます。トポロジ表示では、ファブリックに追加されるすべてのデバイスは青です。

ステップ 4 [Fabric Infrastructure] タブの [List] ビューで、デバイスをクリックします。スライドインペイン に、次の [Fabric] オプションが表示されます。

オプション	説明
エッジノード	選択したデバイスをエッジノードとして有効にするには、このオプションの横にあるボタンをトグルします。
ボーダー ノード	選択したデバイスをボーダーノードとして有効にするには、このオプションの横にあるボタンをトグルします。
コントロール プレーン ノード	選択したデバイスをコントロールプレーンノードとして有効にするには、このオプションの横にあるボタンをトグルします。

デバイスをファブリックインアボックスとして設定するには、[Control Plane Node]、[Border Node]、および [Edge Node] オプションを選択します。

デバイスをコントロールプレーンおよびボーダーノードとして設定するには、[Control Plane Node] と [Border Node] の両方を選択します。

ステップ 5 （任意） デバイスのワイヤレス機能を有効にするには、[Capability] で [Embedded Wireless LAN Controller] トグルボタンをクリックして、次の手順を実行します。

トグルボタンがすでに有効になっている場合は、代わりに [Configure] をクリックしてワイヤレス設定を設定できます。

a) デバイスにワイヤレスパッケージをまだインストールしていない場合、機能を有効にするには組み込みの ワイヤレスコントローラ ソフトウェアイメージが必要であることを示す警告メッセージが Catalyst Center に表示されます。[Warning] ダイアログボックスで [OK] をクリックして、イメージを手動でインストールします。

b) [Download Image] で [Choose File] をクリックしてローカルに保存されているソフトウェアイメージに移動するか、または [Enter image URL] でソフトウェアイメージのインポート元となる HTTP または FTP ソースを指定します。

c) [Import] をクリックします。

イメージのインポートの進捗状況が表示されます。ウィンドウを閉じてインポートの進行状況を表示し、後でインストールをスケジュールする場合は、[Close] をクリックします。

d) イメージのインポートが完了したら、[Download Image] ウィンドウの [Schedule Image Installation] で、次のいずれかのオプションを選択します。

- [Now]：イメージをすぐにインストールします。
- [Later]：将来の日付と時刻でイメージのインストールをスケジュールします。

e) [Task Name] フィールドで、必要に応じてタスク名を更新します。

f) [Later] を選択した場合は、次の手順を実行します。

- [Start Date/Time] で、イメージのインストールの開始日時を指定します。
- イメージのインストールにデフォルトのサイトのタイムゾーンを使用するには、[Site Settings] チェックボックスをオンにします。タイムゾーンを選択するには、[Site Settings] チェックボックスをオフにして、ドロップダウンリストからタイムゾーンを選択します。

g) [適用（Apply）] をクリックします。

イメージのインストールのステータスを表示するには、**[Activities]** > **[Tasks]** ウィンドウに移動し、関連する作業項目を開きます。ソフトウェアイメージが配信され、スイッチでアクティブ化されたら、**[Provision]** > **[Inventory]** > **[Resync]** オプションを使用してデバイスを再同期する必要があります。

h) [Manage Scope] で、組み込みワイヤレスコントローラの管理対象 AP の場所を割り当てます。

- [Primary] タブで、必要なサイト名の横にあるチェックボックスをオンにします。
- [Secondary] タブで、必要なサイト名の横にあるチェックボックスをオンにします。

親サイトまたは個々のサイトを選択できます。親サイトを選択すると、その下にあるすべての子も選択されます。このチェックボックスをオフにすると、個々のサイトの選択を解除できます。

また、[Search Hierarchy] 検索フィールドまたはフィルタアイコンを使用してサイトを検索できます。

i) [Next] をクリックします。

j) [Advanced] ウィンドウで、必要な設定を行います。

- ローリング AP アップグレード機能を有効にするには、[Rolling AP Upgrade] チェックボックスをオンにします。

  （オプション）このチェックボックスをオンにする場合は、最小限のクライアント中断で再起動が可能となるように、[AP Reboot Percentage] ドロップダウンリストから AP のパーセンテージを選択します。デフォルトは 25% です。

- 有効期限が切れる前に、関連する AP のローカルで有効な証明書（LSC）を更新するには、[AP LSC Certificate Renewal] チェックボックスをオンにします。

  このチェックボックスをオンにする場合は、次の設定を行います。

  - [Renewal Profile] ドロップダウンリストから、AP LSC 更新プロファイルを選択します。

    AP LSC 更新プロファイルを作成する場合は、AP LSC 更新プロファイルの作成 （495 ページ） を参照してください。

  - （オプション）段階的な更新に AP LSC 更新プロファイルを選択する場合は、最小限のクライアント中断で再起動が可能となるように、[AP Reboot %] ドロップダウンリストから AP のパーセンテージを選択します。デフォルトは 25% です。



（注） 設定すると、同じ AP 再起動パーセンテージ値が、ローリング AP アップグレードプロセスと段階的 AP LSC 更新プロセスの両方に適用されます。たとえば、AP の再起動パーセンテージを 25% に設定すると、ローリング AP アップグレードおよび段階的 AP LSC 更新の両方で、一度に 25% の AP のみが再起動されます。

k) [Next] をクリックします。
l) [Summary] で設定を確認します。
m) [Save] をクリックします。

デバイスのワイヤレス機能が有効になっており、ワイヤレスネットワーク設定に変更がある場合、変更をデバイスにプッシュするには、[Configure] をクリックして設定を保存する必要があります。

ステップ 6 [Add] をクリックして設定を保存します。

ステップ 7 [Fabric Infrastructure] タブで [Deploy] をクリックして、デバイスを設定します。

ステップ 8 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。



（注） デバイスは、Catalyst Center リリースと互換性のあるソフトウェアリリースを実行している場合にのみ、ファブリックに追加されます。ファブリックデバイスの互換性については、「Cisco SD-Access Compatibility Matrix」を参照してください。

特定のファブリックロールについて、デバイスのソフトウェアイメージが Catalyst Center リリースと互換性がない場合、デバイスはファブリックに追加されず、エラーメッセージが表示されます。

ステップ 9 [Tasks] ウィンドウで、タスクの展開を監視します。

次のタスク

デバイスがファブリックに追加されると、ファブリック コンプライアンス チェックが自動的に実行され、デバイスがファブリックに準拠していることが確認されます。トポロジには、ファブリック コンプライアンス チェックに失敗したデバイスが青色で、横に十字マークが付いた状態で表示されます。エラー通知の [詳細の表示（See more details）] をクリックして問題領域を特定し、修正します。

ファブリックからデバイスを削除

次の手順を使用して、ファブリックサイトから 1 つ以上のデバイスを削除します。

（注） ファブリックサイトのボーダーノードがサービス挿入サイトに関連付けられている場合、サービス挿入サイトとの関連付けを削除して、ファブリックサイトからデバイスを削除します。詳細については、「サービス挿入サイトの編集 （1391 ページ）」を参照してください。

手順

ステップ 1 メインメニューから次を選択します。**[Provision]** > **[Fabric Sites]**。

ステップ 2 [Fabric Sites] タブ の [SUMMARY] で、ファブリックサイトの数を示す数字をクリックします。

ステップ 3 [Fabric Sites] ウィンドウで、ファブリックサイトを選択します。

ステップ 4 次のいずれかのオプションを使用して、[ファブリックインフラストラクチャ（Fabric Infrastructure）] タブの [リスト（List）] ビューから、ファブリックの一部である（[ファブリックロール（Fabric Role）] を持つ）デバイスを選択します。

- デバイス名をクリックします。
- デバイスのチェックボックスをオンにして、**[その他のアクション（More Actions）]** > **[ファブリックロールの編集（Edit Fabric Role）]** の順に選択します。複数のデバイスを選択できます。

トポロジ表示では、ファブリックに追加されるすべてのデバイスは青です。

ステップ 5 スライドインペインの [ファブリック（Fabric）] タブで、[ファブリックから削除（Remove From Fabric）] をクリックします。

ステップ 6 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

ステップ 7 [Tasks] ウィンドウで、タスクの展開を監視します。

次のタスク

タスクの展開が成功したら、ワイヤレスロールが有効になっている Cisco Catalyst 9000 シリーズスイッチで組み込みワイヤレスコントローラを使用する場合、各スイッチを再起動することを推奨します。再起動によって最適な機能が確保されます。たとえば、同じファブリックサイトにワイヤレスロールが有効になっている複数の Catalyst 9000 シリーズ スイッチがあって再起動しない場合、モビリティトンネルの制限などの問題が発生する可能性があります。

各スイッチを再起動するには、次の手順を実行します。

1. [ファブリックインフラストラクチャ（Fabric Infrastructure）] タブで、スイッチ名をクリックします。
2. スライドインペイン で、[リブート（Reboot）] をクリックします。
3. [Warning] ダイアログボックスで、[Yes] をクリックします。

ボーダーノードとしてのデバイスの追加

ファブリックにデバイスを追加する場合、「デバイスをファブリックに追加 （1235ページ）」[英語]で説明したように、コントロールプレーン、ボーダーノード、またはエッジノードとして動作するようにさまざまな組み合わせで追加できます。

この項では、デバイスをボーダーノードとして追加し、次を設定する方法について説明します：

- ボーダーノードタイプ：内部、外部、または内部と外部（ステップ 9 （1241 ページ））
- ボーダーノードの優先順位（ステップ 10 （1242 ページ））
- ボーダーノードアフィニティ ID（ステップ 10 （1242 ページ））
- ボーダーノードのスイッチ仮想インターフェイス（SVI）の TCP MSS 調整値（ステップ 10 （1242 ページ））
- AS パスのプリペンド（ステップ 10 （1242 ページ））
- 関連するトランジット：SD-Access トランジットまたは IP ベースのトランジット（ステップ 11 （1243 ページ））
- レイヤ 3 ハンドオフの IP アドレスプールの割り当て（ステップ 11 （1243 ページ））

始める前に

ボーダーノードアフィニティ ID 機能を使用するには、SD-Access LISP Pub/Sub トランジットを作成していることを確認します。詳細については、SD-Access トランジットの作成（1248 ページ）を参照してください。ローカルファブリックサイトに最初のコントロールプレーンノードを追加するときは、必ず LISP Pub/Sub コントロールプレーンプロトコルを選択してください。詳細については、LISP Pub/Sub の設定（1245 ページ）を参照してください。ボーダーノードは、Cisco IOS XE リリース 17.8.1 以降を実行している必要があります。

手順

ステップ 1 メインメニューから次を選択します。**[Provision]** > **[Fabric Sites]**。

ステップ 2 [Fabric Sites] タブ の [SUMMARY] で、ファブリックサイトの数を示す数字をクリックします。

ステップ 3 [Fabric Sites] ウィンドウで、ボーダーノードを設定するファブリックサイトを選択します。
ネットワークインベントリ内のすべてのデバイスが結果のトポロジビューに表示されます。トポロジビューでは、ファブリックロールで動作するすべてのデバイスは青色で表示されます。

ステップ 4 [Fabric Infrastructure] タブで、デバイスをクリックします。

ステップ 5 スライドインペインで、[Border Node] トグルボタンをクリックします。

ステップ 6 表示されたスライドインペインで、[Layer 3 Handoff] タブをクリックします。

ステップ 7 [Enable Layer-3 Handoff] チェックボックスを選択します。

ステップ 8 デバイスの [ローカル自律番号（Local Autonomous Number）] を入力します。

ローカル自律番号がデバイスですでに設定されている場合は、その番号が表示され、このフィールドは無効になります。デバイスですでに設定されているローカル自律番号は変更することができません。

ステップ 9 ボーダーノードのタイプを設定します。デフォルトでは、ボーダーノードは外部専用ボーダーノードとして指定され、外部ルートをインポートせずに、ファブリックサイトへのデフォルトゲートウェイとして機能します。

ボーダーノードは、デフォルトゲートウェイではなく、外部ルートのみをインポートする内部専用ボーダーノードとして設定できます。ボーダーノードには、内部ボーダーおよび外部ボーダーを組み合わせたロールを設定することもできます。

- ボーダーを外部専用ボーダーノードとして指定するには、[Default to all virtual networks] および [Do not import external routes] の両方のチェックボックスをオンにします。
- ボーダーを内部専用ボーダーノードとして指定するには、[Default to all virtual networks] および [Do not import external routes] の両方のチェックボックスをオフにします。
- ボーダーノードを内部および外部ボーダーとして指定するには、[Default to all virtual networks] チェックボックスをオンにします。このノードはファブリックのデフォルトゲートウェイとして機能し、BGP で学習したルートをファブリックサイトもインポートします（[Do not import external routes] チェックボックスはオンにしないでください）。

ボーダーノードタイプの詳細については、『Cisco SD-Access Solution Design Guide』[英語] を参照してください。

ステップ 10 SD-Access トランジットでボーダーノードの優先順位、アフィニティ ID、AS パスのプリペンド、TCP MSS 調整値およびネイティブマルチキャストを設定するには、[Advanced] をクリックして、次を設定します。

a) ボーダーノードの優先順位を変更するには、[Modify Border Priority] チェックボックスをオンにして、新しい優先順位値を入力します。

- 優先度の範囲は、1 ～ 10 です。
- 1 は最高の優先順位を示します。
- 10 は最も低い優先順位を示します。
- デフォルトの優先順位値は 10 です。

ファブリックサイトに 2 つ以上のボーダーノードが設定されている場合、トラフィックは優先順位の高いボーダーノードを介してルーティングされます。優先順位値が同じ場合、トラフィックはボーダーノード間で負荷分散されます。

b) （オプション）ボーダーノードアフィニティ ID を設定するには、[Modify Border Node Affinity-ID] チェックボックスをオンにして、次のフィールドに値を入力します。

- [Affinity-ID Prime]：相対的な prime 値が小さいほど、優先順位が高くなります。
- [Affinity-ID Decider]：2 つのボーダーノードの prime 値が同じ場合、ボーダーノードの優先順位を決定するタイブレーカーとして decider 値が使用されます。

アフィニティ ID は、他の利用可能なすべてのボーダーノードから受信した値の中でこのボーダーノードの値を考慮した相対値です。アフィニティ ID の相対値が低いほど、宛先ボーダーノードの優先順位が高くなります。デフォルトでは、アフィニティ ID 値はプロビジョニングされません。

受信したアフィニティ ID が等しい場合、優先順位を使用してボーダーノードの優先順位が決まります。



（注） アフィニティ ID 機能を適切に機能させるために、同じ SD-Access トランジットに接続されているすべてのボーダーノードにアフィニティ ID を設定していることを確認します。

c) BGP AS_PATH リストに付加する AS パスの数を定義するには、[AS Path Prepending] チェックボックスをオンにして、1 ～ 10 の値を入力します。

AS パスのプリペンドは、入力境界の選択に役立ちます。

d) レイヤ 3 ハンドオフ SVI の TCP 最大セグメントサイズ（MSS）値をカスタマイズするには、[TCP MSS Adjustment] チェックボックスをオンにして、必要な値を入力します。

[TCP MSS Adjustment] には 500 ～ 1440 の範囲内で値を入力できます。[TCP MSS Adjustment] の値は、IPv4 と IPv6 の両方の TCP セッションに適用されます。

（注） 境界デバイスがレイヤ 3 ハンドオフ用に設定されている場合にのみ、TCP MSS 値をカスタマイズできます。

e) IPv6 アンダーレイボーダーの場合、BGP ルータのカスタム識別子を設定できます。[カスタムBGP ルータID（Custom BGP Router ID）] チェックボックスを選択し、必要な値を入力します。値は IPv4 形式である必要があります。

f) （オプション）SD-Access トランジットに接続されている複数のサイトでネイティブマルチキャストを設定するには、[Enable Multicast over SD-Access Transit] チェックボックスをオンにします。

（注） SD-Access トランジットでも同様のチェックボックスを有効にしてください。

[Activities] > **[Audit Logs]** でボーダーノードの優先順位とアフィニティ ID の展開ログを表示できます。

ステップ 11 [Add Transit Site] にカーソルを合わせ、このボーダーノードに接続するトランジットを選択します。

[IP:BGP IP TRANSIT] では、仮想ネットワークの IP アドレスの割り当てを自動化するか、仮想ネットワークのローカルおよびピア IP アドレスを手動で割り当てるかを選択できます。両方を行うことはできません。

a) （オプション）Catalyst Center でボーダーノードとピア間の接続に IP アドレスを割り当てることができるようにするには、[Select IP Address Pool] ドロップダウンリストから IP アドレスプールを選択します。

（注） ローカルおよびピア IP アドレスを手動で割り当てた場合は、[Select IP Address Pool] が無効になります。

b) ハンドオフインターフェイスを設定するには、[Add External Interface] をクリックします。

表示されるウィンドウで、次の手順を実行します。

1. [External Interface] ドロップダウンメニューからインターフェイスを選択します。
2. [Remote AS Number] は、選択したトランジットまたはピアネットワークから自動的に導出されます。
3. （オプション）[Interface Description] フィールドに、インターフェイスの説明を入力します。
4. （オプション）[Actions] ドロップダウンリストから、[Enable All] または [Disable All] を選択します。

5. 仮想ネットワークの [Enable Layer 3 Handoff] トグルボタンをクリックします。この仮想ネットワークは、ボーダーノードによって BGP 経由でピアにアドバタイズされます。1 つ、複数、またはすべての仮想ネットワークを選択できます。
6. [VLAN ID] フィールドに、選択した仮想ネットワークの VLAN ID を入力します。
7. （オプション）選択した仮想ネットワークの IPv4 および IPv6 の [Local IP Address] および [Peer IP Address] を手動で割り当てるには、IP アドレスとサブネットマスクを CIDR 表記（IP アドレス/プレフィックス長）で入力します。

（注） すでに IP プールを選択している場合、[Local IP Address] および [Peer IP Address] フィールドは無効になっています。

8. **[Save]** をクリックします。

c) [Add] をクリックします。

SDA トランジットを設定する場合、外部ボーダーノードでデュアルスタックサポートを有効にできます。手順は次のとおりです。

a) [詳細属性（Advanced attributes）] トグルボタンをクリックします。
b) [デュアルスタックRLOC登録（Dual stack RLOC registration）] チェックボックスを選択します。
c) SDA トランジットを接続するためのアンダーレイ IP アドレスタイプを選択します—IPv4 または IPv6。

ステップ 12 （オプション）ファブリックサイトに従来のネットワークを接続している場合、または従来のネットワークから SD-Access ネットワークに移行する場合にのみ、この手順を実行します。[Layer 2 Handoff] タブをクリックします。

仮想ネットワークのリストと、各仮想ネットワークの IP アドレスプールの数が表示されます。

a) ハンドオフする仮想ネットワークをクリックします。

仮想ネットワークに存在する IP アドレスプールのリストと、従来のネットワークに接続できるインターフェイスのリストが表示されます。

b) [External Interface] ドロップダウンから、インターフェイスを選択します。
c) [Interface Description] に、オプションでインターフェイスの説明を入力します。
d) [External VLAN] フィールドに、ファブリックを拡張する必要がある VLAN 番号を入力します。

仮想ネットワークは単一のインターフェイスまたは複数のインターフェイスでハンドオフできます。セグメントのレイヤ 2 ハンドオフを 2 つの異なるデバイスで実行することもできます。いずれの場合も、ネットワークにループが形成されていないことを確認します。

ボーダーノードは従来のネットワークに接続されているため、ブロードキャストストーム、レイヤ 2 ループ、およびレイヤ 2 スイッチド アクセス ネットワークで発生する可能性のあるスパニングツリーの問題の影響を受けます。コントロールプレーンのノードサービスまたは他の外部ネットワークに接続するボーダーノードサービスの中断を防ぐため、ボーダーノードはレイヤ 2 ハンドオフ機

能専用にすべきであり、他のファブリックロールまたはサービスと同じ場所に配置しないでください。

e) **[Save]** をクリックします。

ステップ 13 [Add] をクリックして設定を保存します。

ステップ 14 [Fabric Infrastructure] タブで [Deploy] をクリックして、ボーダーノードを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

（注） デバイスは、Catalyst Center リリースと互換性のあるソフトウェアリリースを実行している場合にのみ、ボーダーノードとして設定されます。デバイスが互換性のないソフトウェアを実行している場合、エラーメッセージが表示され、デバイスはファブリックボーダーノードとして設定されません。ソフトウェアの互換性については、「Cisco SD-Access Compatibility Matrix」を参照してください。

ステップ 15 [Tasks] ウィンドウで、タスクの展開を監視します。

LISP Pub/Sub の設定

最初のコントロールプレーンをファブリックに追加する場合にのみ、ファブリックサイトで LISP Pub/Sub を設定できます。

始める前に

ファブリックデバイスが Cisco IOS XE リリース 17.6.1 以降で動作することを確認します。

手順

ステップ 1 メインメニューから次を選択します。 **[Provision]** > **[Fabric Sites]**.

ステップ 2 [SUMMARY] で、ファブリックサイトの数を示す数字をクリックします。

ステップ 3 デバイスを追加するファブリックサイトを選択します。

インベントリされたネットワーク内のすべてのデバイスが結果のトポロジビューに表示されます。トポロジ表示では、ファブリックに追加されるすべてのデバイスは青です。

ステップ 4 [Fabric Infrastructure] タブの [List] ビューで、コントロールプレーンとして設定するデバイスをクリックします。

ステップ 5 スライドインペインで、[Control Plane Node] トグルボタンを有効にして、このプレーンを設定します。

ステップ 6 [Configure Control Plane] スライドインペインで、[LISP Pub/Sub] ルート配布プロトコルを選択し、[Add] をクリックします。

ステップ 7 [Fabric Infrastructure] タブで [Deploy] をクリックして、LISP Pub/Sub コントロールプレーンを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

ステップ 8 [Tasks] ウィンドウで、タスクの展開を監視します。

ステップ 9 ファブリックサイトの LISP Pub/Sub の設定を確認するには、[SITE SUMMARY] ウィンドウで LISP Pub/Sub のステータスを確認します。

ファブリックの再設定

ファブリックで使用されている IP アドレスプールを変更すると、ファブリックは無効になります。ファブリックサイトのデバイスに IP アドレスプールの変更を設定するには、この手順を使用してファブリックを更新します。

ファブリックの再設定にかかる時間は、デバイスの数によって異なります。

（注） ファブリックが再設定されて IP アドレスプールの変更内容によってデバイスが更新されるまで、ファブリックデバイスで他の操作を実行できません。

手順

ステップ 1 メインメニューから次を選択します。**[Provision]** > **[Fabric Sites]**。

ステップ 2 [Fabric Sites] タブ の [SUMMARY] で、ファブリックサイトの数を示す数字をクリックします。

ステップ 3 [Fabric Sites] ウィンドウで、変更された IP アドレスプールを使用するファブリックサイトを選択します。

ステップ 4 **[Fabric Infrastructure]** タブの警告アラートで、**[Reconfigure Fabric]** をクリックします。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。

- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 5 [Tasks] ウィンドウで、タスクの展開を監視します。

IP トランジットの作成

次の手順を使用して、IP トランジットを作成します。

手順

ステップ 1 メインメニューから次を選択します。 **[Workflows]** > **[Create Transits]** の順に選択します。

または、**[Provision]** > **[Transits]** に移動し、[Create Transit] をクリックします。

ステップ 2 タスクの概要ウィンドウが表示されたら、[Let's Do It] をクリックして、ワークフローに直接移動します。

ステップ 3 [Transit Name and Type] ウィンドウで次の手順を実行します。

a) [Transit Name] フィールドに、トランジットの名前を入力します。

b) [Transit Type] ドロップダウンリストから [IP-Based] を選択します。

ルーティング プロトコルが BGP にデフォルトとして設定されます。

c) [Remote BGP Autonomous System Number] フィールドに、トランジットの自律システム番号（ASN）を入力します。

d) [詳細属性（Advanced attributes）] トグルボタンをクリックして、詳細属性を有効または無効にします。

e) [Select Site] ドロップダウンリストで、トランジットのサイトを選択します。

選択したサイトがファブリックサイトレベル以上にあることを確認します。

トランジットの作成後にサイトマッピングを編集できます。編集するには、[Transits] ウィンドウで、**[More Actions]** > **[Edit Transit]**をクリックし、必要に応じてサイトの選択を更新します。

トランジットが以下の場合...	結果
ファブリックサイトに関連付けられている場合	関連するすべてのファブリックサイトに共通の親であるサイトを選択します。
ファブリックサイトに関連付けられていない場合	ファブリックサイトのレベル以上のサイトを選択できます。

ステップ 4 [Transit Control Plane Nodes] ウィンドウで [Next] をクリックします。

ステップ 5 [Summary] ウィンドウで、設定を確認します。変更するには、[Edit] をクリックします。

ステップ 6 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

ステップ 7 [Tasks] ウィンドウで、タスクの展開を監視します。

SD-Access トランジットの作成

次の手順を使用して、SD-Access トランジットを作成します。

手順

ステップ 1 メインメニューから次を選択します。 **[Workflows]** > **[Create Transits]** の順に選択します。

または、**[Provision]** > **[Transits]** の順に移動し、[トランジットの作成（Create Transit）] をクリックします。

ステップ 2 タスクの概要ウィンドウが表示されたら、[Let's Do It] をクリックして、ワークフローに直接移動します。

ステップ 3 [トランジットの名前とタイプ（Transit Name and Type）] ウィンドウで、次の手順を実行します。

a) [Transit Name] フィールドに、トランジットの名前を入力します。

b) [Transit Type] ドロップダウンリストから、トランジットタイプを選択します。

- LISP Pub/Sub コントロールプレーンのないファブリックサイトのトランジットを設定する場合は、[SD-Access (LISP/BGP)] を選択してください。
- LISP Pub/Sub コントロールプレーンのあるファブリックサイトのトランジットを設定する場合は、[SD-Access (LISP Pub/Sub)] を選択してください。

  このオプションを選択した場合、トランジットを介したネイティブマルチキャストを有効にするには、[Native Multicast Over SD-Access Transit] チェックボックスをオンにします。

（注） SD-Access トランジットに接続されている複数のサイトでネイティブマルチキャストを完全に設定するには、ボーダーノードで SD-Access トランジットを介するマルチキャストを有効にする必要があります。

[SD-Access (LISP Pub/Sub)] トランジットを他の Catalyst Center クラスタと共有する場合は、[Yes, Share] を選択してください。共有しない場合は、[No, keep it local] を選択してください。

（注） [Yes, Share] オプションは、**複数の Catalyst Center** パッケージがすべての Catalyst Center クラスタにインストールされている場合にのみ表示されます。

c) [詳細属性（Advanced attributes）] をオンにし、[サイト（Site）] ドロップダウンリストでトランジットのサイトを選択します。

選択したサイトがファブリックサイトの上のレベルにあることを確認します。デフォルトでは、[グローバル（Global）] に設定されています。

トランジットの作成後にサイトマッピングを編集できます。編集するには、[Transits] ウィンドウで、**[More Actions]** > **[Edit Transit]**をクリックし、必要に応じてサイトの選択を更新します。

トランジットが以下の場合...	結果
ファブリックサイトに関連付けられている場合	関連するすべてのファブリックサイトおよび関連するトランジット コントロール プレーン ノードに共通の親であるサイトを選択します。
ファブリックサイトに関連付けられていない場合	関連するトランジットコントロールプレーン ノードに共通の親であるサイトを選択できます。

ステップ 4 [Transit Control Plane Nodes] ウィンドウで次の手順を実行します。

a) [Select a Site] ドロップダウンリストから、コントロールプレーンノードがあるサイトを選択します。

（注） LISP/BGP コントロールプレーンを使用するファブリックサイトには [SD-Access (LISP Pub/Sub)] トランジットを追加できません。LISP Pub/Sub コントロールプレーンを使用するファブリックサイトには [SD-Access (LISP/BGP)] トランジットを追加できません。

b) [Transit Control Plane Node] ドロップダウンリストから、コントロールプレーンノードを選択します。

c) （オプション）追加のノードを設定するには、プラスアイコンをクリックし、「4.a （1249 ページ）」と「4.b （1249 ページ）」を繰り返します。

ステップ 5 [Summary] ウィンドウで、設定を確認します。変更するには、[Edit] をクリックします。

ステップ 6 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

ステップ 7 [Tasks] ウィンドウで、タスクの展開を監視します。

次のタスク

ファブリックサイトを SD-Access トランジットと相互接続するには、トランジットをファブリックボーダーノードに追加します。

ファブリックサイトの認証テンプレートの設定

次の手順を使用して、ファブリックサイト内のすべてのデバイスに適用される認証テンプレートを設定します。

（注） ファブリック内の既存のスイッチのいずれかに1つ以上のスタックメンバーまたはラインカードが追加されると、これらの新しいスタックメンバーまたはラインカードでも認証テンプレートを設定するように警告アラートが表示されます。警告アラートの[修正の適用（Apply Fix）]をクリックして、設定を適用し、ファブリックを更新します。

手順

ステップ 1 メインメニューから次を選択します。**[Provision]** > **[Fabric Sites]**。

ステップ 2 [SUMMARY] で、ファブリックサイトの数を示す数字をクリックします。

ステップ 3 [fabric site] をクリックします。

ステップ 4 [Authentication Template] タブをクリックします。

ステップ 5 [認証テンプレートの選択（Select Authentication Template）] で、サイトの認証テンプレートを選択します。

- **オープン認証（Open Authentication）**：ホストには、802.1X 認証を受ける必要なくネットワーク アクセスが許可されます。
- **クローズ認証（Closed Authentication）**：認証前のすべてのトラフィック（DHCP、DNS、ARP を含む）は廃棄されます。
- [低インパクト（Low Impact）]：スイッチポートに ACL を適用することでセキュリティを追加して、認証前に制限されたネットワークアクセスを許可します。ホストが正常に認証されると、追加のネットワークアクセスが許可されます。
- なし（None）

[クローズド認証（Closed Authentication）]、[オープン認証（Open Authentication）]、および [低インパクト（Low Impact）] テンプレートでは、次の設定を構成できます。

- [音声VLAN（Voice VLAN）]：このチェックボックスを使用して、サイトのデフォルトの音声 VLAN（VLAN 2046）を有効または無効にします。

- [BPDUガード（BPDU Guard）]（クローズド認証）：このチェックボックスを使用して、すべての [クローズド認証（Closed Authentication）] ポートでブリッジ プロトコル データ ユニット（BPDU）ガードを有効または無効にします。

選択した認証テンプレートの設定を編集して、サイト固有の認証要件に対応することができます。

サイトレベルの認証を変更する前に、マクロまたは Autoconf を使用して AP がオンボーディングされ、かつまだ定期的な再同期が行われていないファブリックデバイスがあれば再同期する必要があります。

ステップ 6 （オプション）選択した認証方式の設定を編集するには、[Edit] をクリックします。

a) スライドインペインで、必要な設定を編集します。

- [First Authentication Method]：[802.1x] または [MAC Authentication Bypass（MAB）] を選択します
- [802.1x Timeout（in seconds）]：スライダを使用して、802.1x タイムアウトを秒単位で指定します。
- [Wake on LAN]：[Yes] または [No] を選択します。

  Wake on LAN（WoL）は、次の場合にのみサポートされます。

  - 送信元（WoL イニシエータ）と宛先（スリープ状態のホスト）の両方が同じサブネット内にあり、レイヤ 2 フラッディングが有効になっている。
  - 送信元が、SD-Access ファブリックの外部にあるが、レイヤ 3 ハンドオフを介してファブリックに接続されているネットワーク内にある。宛先が、IP ダイレクトブロードキャストが有効になっている SD-Access サブネット内にある。

  （注） 次のトポロジは WoL をサポートしていません。

  - WoL イニシエータとスリープ状態のホストが、同じレイヤ 3 仮想ネットワーク内の異なるサブネット上にある。
  - WoL イニシエータが、SD-Access トランジットを介してスリープ状態のホストにルーティングする。

- [Number of Hosts]：[Unlimited] または [Single] を選択します。

  （注） [Number of Hosts] は、1 つのポートに接続できるデータホストの数を指定します。[Single] の場合、ポートでは 1 つのデータクライアントのみを保持できます。[Unlimited] の場合、ポートで複数のデータクライアントと 1 つの音声クライアントを保持できます。

- [Pre-Authentication Access Control List]：トグルボタンを有効にして、[Low Impact] 認証の事前認証制御を構成します。[Implicit Action] ドロップダウンリストから、暗黙的なアクションを選択します。ルールの説明を入力します。アクセスコントラクトを追加するには、[Add Contract Action] をクリックし、ルールを選択して、[Apply Table] をクリックします。

b) **[Save]** をクリックします。

保存された変更は、認証テンプレートが編集されているサイトにのみ適用されます。

ステップ 7 [Select Authentication Template] タブで [Deploy] をクリックして、すべてのノードの認証テンプレートを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

ヒットレス認証変更機能を使用すると、ファブリックからデバイスを削除することなく、1 つの認証方式から別の認証方式に切り替えることができます。

ステップ 8 [Tasks] ウィンドウで、タスクの展開を監視します。

ファブリックサイト内のポートの設定

[Port Assignment] タブで、ファブリックサイトの各アクセスデバイスを設定できます。デバイスの各ポートのネットワーク動作設定を指定できます。

個々のポートの認証テンプレートを設定しない場合、ポートは、グローバル認証テンプレートの設定からそれらの設定を継承します。[ポート（Ports）]テーブルで、対応するポートの認証テンプレート名の横に継承アイコンが表示されます。

手順

ステップ 1 メインメニューから次を選択します。**[Provision]** > **[Fabric Sites]**。

ステップ 2 [Fabric Sites] タブ の [SUMMARY] で、ファブリックサイトの数を示す数字をクリックします。

ステップ 3 [Fabric Sites] ウィンドウで、ポート割り当てを設定するファブリックサイトをクリックします。

ステップ 4 [Port Assignment] タブをクリックします。

ステップ 5 ファブリックデバイスのリストからデバイスを選択し、[Configure] をクリックします。

ステップ 6 [Configure Port Assignments] スライドインペインで、接続されるデバイスのタイプをクリックします。

オプション	説明
ユーザーデバイスとエンドポイント	ホストデバイスに接続するポートを設定します。
アクセス ポイント（AP）	アクセスポイントに接続するポートを設定します。
トランク	ポートをトランク ポートとして設定します。

オプション	説明
サプリカントベースの拡張ノード	サプリカントベースの拡張ノードを受信するようにポートを設定します。

- ホストデバイスを接続するには、[ユーザーデバイスとエンドポイント（User Devices and Endpoints）] をクリックし、次の手順を実行します。
  1. [VLAN Name (Data)] ドロップダウンリストからデータの VLAN 名を選択します。
  2. [Security Group] ドロップダウンリストからセキュリティグループを選択します。

     セキュリティグループは、[None] 認証テンプレートでのみサポートされます。
  3. [VLAN Name (Voice)] ドロップダウンリストから音声の VLAN 名を選択します。
  4. [Authentication Template] ドロップダウンリストから認証タイプを選択します。
  5. コネクテッドデバイスに関する [Description] を入力します。
- アクセスポイントを接続するには、[アクセスポイント（Access Point）] をクリックし、次の手順を実行します。
  1. [VLAN Name (Data)] ドロップダウンリストから VLAN 名を選択します。
  2. [Authentication Template] ドロップダウンリストから認証タイプを選択します。
  3. コネクテッドデバイスに関する [Description] を入力します。
- サプリカントベースの拡張ノードデバイスを接続するには、[Supplicant-Based Extended Node] をクリックします。
- トランクポートを接続するには、[Trunk] をクリックし、ポートの説明を [Description] に入力します。

  トランクポートの [ネイティブVLAN（Native VLAN）] と [許可VLAN（Allowed VLANs）] を設定します。
  - [ネイティブVLAN（Native VLAN）] フィールドに、ネイティブ VLAN の値を入力します。

    有効な範囲は 1 ～ 4094 です。デフォルト値は 1 です。
  - [許可VLAN（Allowed VLANs）] フィールドでは、すべての VLAN、1 ～ 4094 の特定の VLAN ID を許可することを選択するか、または VLAN の範囲を指定できます。たとえば、100、200、または 300-400 と入力できます。デフォルト値は [すべて（All）] です。



（注） テンプレートでデフォルト値をオーバーライドする場合は、テンプレートの各ポートに指定される値と一致するようにトランク設定を更新します。

ステップ 7 [Configure Port Assignment] スライドインペイン の [Update] をクリックして設定を保存します。

ステップ 8 [Port Assignment] タブの [Deploy All] をクリックしてポート割り当てを更新します。

ステップ 9 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 10 [Tasks] ウィンドウで、タスクの展開を監視します。

ファブリックネットワークのワイヤレス SSID の設定

始める前に

ワイヤレスデバイスをファブリックサイトに追加してください。

手順

ステップ 1 メインメニューから次を選択します。**[Provision]** > **[Fabric Sites]**。

ステップ 2 [SUMMARY] で、ファブリックサイトの数を示す数字をクリックします。

ステップ 3 [fabric site] をクリックします。

ステップ 4 [Wireless SSID] タブをクリックし、ホストがアクセス可能なネットワーク内のワイヤレス SSID を指定します。

ステップ 5 [Choose Pool] ドロップダウンリストから、SSID 用に予約されている IP アドレスプールを選択します。

このドロップダウンリストでは、レイヤ 3 およびレイヤ 2 セグメント用に設定されたワイヤレス IP アドレスプールを選択できます。

ステップ 6 [Assign SGT] ドロップダウンリストから、SSID のセキュリティグループを選択します。

ステップ 7 SSID でワイヤレスマルチキャストを有効にするには、[Enable Wireless Multicast] チェックボックスをオンにします。

ステップ 8 [Deploy] をクリックします。

ステップ 9 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。

- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 10 [Tasks] ウィンドウで、タスクの展開を監視します。

ファブリックでのワイヤレス メッシュ アクセス ポイントの設定

Catalyst Center リリース 2.3.7 以降、SD-Access ファブリックでワイヤレスメッシュ AP をオンボードできます。メッシュ AP は、ネットワーク要件に応じて、メッシュアクセスポイント（MAP）またはルートアクセスポイント（RAP）としてプロビジョニングできます。詳細については、「ワイヤレス メッシュ ネットワークについて」を参照してください。

始める前に

- 認証済みのアクセスポイント（AP）のリストを定義します。シスコ ワイヤレス コントローラのプロビジョニング中に AP 認証リストを選択できます。シスコ ワイヤレス コントローラは、AP 認証リストに含まれている AP からの要求にのみ応答します。認証された AP のリストを作成する方法については、「AP 認証リストの作成」を参照してください。
- メッシュ AP を管理およびプロビジョニングするための AP プロファイルを定義します。「Cisco IOS XE デバイスの AP プロファイルのメッシュ設定を行う」を参照してください。

手順

ステップ 1 メッシュネットワークモードで使用する既存の AP がある場合は、最初に [Configure Access Point] ワークフローを使用して AP モードを [Bridge] に変更する必要があります。詳細については、「AP の設定」を参照してください。

ステップ 2 メッシュ AP をオンボードするには、AP 認証リストを使用してファブリック対応ワイヤレスコントローラをプロビジョニングします。「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのプロビジョニング」を参照してください。

次のタスク

AP をオンボードし、MAP または RAP のロールでプロビジョニングします。

ファブリックサイトでのセキュリティサービスの挿入の設定

ファブリックサイトでサービスの挿入を設定するには、次の手順を実行します。

手順

ステップ 1 メインメニューから次を選択します。**[Provision]** > **[Fabric Sites]**。

ステップ 2 [SUMMARY] で、ファブリックサイトの数を示す数字をクリックします。

ステップ 3 [ファブリックサイト（Fabric Sites）] ウィンドウで、セキュリティサービスの挿入を設定するファブリックサイトを選択します。

ステップ 4 対応するファブリック サイト ウィンドウで、[サイトアクション（Site Actions）] にカーソルを合わせて [サービスの挿入の有効化（Enable Service Insertion）] を選択します。

ステップ 5 次の設定を完了し、このファブリックサイトでサービス挿入サイトを有効にします。

サービス挿入サイトの状態	結果
どのファブリックサイトでもまだ有効になっていない	セキュリティサービスの挿入を有効にするには、「デイゼロでサービス挿入サイトを有効にするための事前チェック（1388 ページ）」を参照してください。
別のファブリックサイトですでに有効になっている	このファブリックサイトをサービス挿入サイトとして設定するには、「サービス挿入サイトの有効化（1389 ページ）」を参照してください。
このサイトですでに有効になっている	サービス挿入サイトの設定を編集するには、「サービス挿入サイトの編集（1391 ページ）」を参照してください。

仮想ネットワーク

仮想ネットワークは、共通物理ネットワークインフラストラクチャ内でトラフィックをセグメント化するために使用されるオーバーレイです。これは「マクロセグメンテーション」とも呼ばれます。レイヤー 2 仮想ネットワークはスイッチドトラフィックをセグメント化し、レイヤー 3 仮想ネットワークはルーテッドトラフィックをセグメント化します。Cisco SD-Access ファブリックに接続されている各エンドポイントは、静的エッジポート構成または Cisco Identity Service Engine からの動的ポリシーに基づいて、特定の仮想ネットワークに割り当てられます。

仮想ネットワークのエンドポイントは、マイクロセグメンテーションポリシーによって明示的にブロックされていない限り、相互に通信できます。異なる仮想ネットワークにまたがるエンドポイントは、デフォルトでは、相互に通信できません。仮想ネットワーク間トラフィックの場合は、接続ポリシーをCisco SD-Accessファブリックの外部（フュージョンデバイス上など）で実装する必要があります。

仮想ネットワークの一般的な使用例は、社内エンドポイントとビルディング管理システムの両方を含むオフィスビルです。社内エンドポイントは、照明、暖房、換気、空調などのビルディングシステムとは別にセグメント化する必要があります。このようなシナリオでは、ネットワーク管理者は、マクロセグメンテーションを使用して2つ以上の仮想ネットワークで社内エンドポイントとビルディングシステムをセグメント化することにより、ビルディングシステムと社内エンドポイントの間の不正アクセスをブロックできます。

レイヤ3仮想ネットワークは、複数のファブリックサイトやネットワークドメイン（ワイヤレス LAN、キャンパス LAN、および WAN）にまたがる場合があります。レイヤ 2 仮想ネットワークは、単一のファブリックサイト内に存在します。

レイヤ 3 仮想ネットワークの作成

手順

ステップ 1 メインメニューから次を選択します。**[Workflows]** > **[Create Layer 3 Virtual Networks]** の順に選択します。

または、**[Provision]** > **[Virtual Networks]** で [Layer 3] タブに移動し、[Create Layer 3 Virtual Networks] をクリックすることもできます。

ステップ 2 タスクの概要ウィンドウが開いたら、[Let's Do it] をクリックして、ワークフローに直接移動します。

ステップ 3 [Layer 3 Virtual Networks] ウィンドウで、次の手順を実行します。

a) [Layer 3 Virtual Network name] フィールドに、レイヤー 3 仮想ネットワークの名前を入力します。

b) （任意） 別のレイヤ 3 仮想ネットワークを作成するには、プラスアイコンをクリックし、レイヤ 3 仮想ネットワークの名前を入力します。

ステップ 4 [Fabric Sites and Fabric Zones (Optional)] ウィンドウで、次のように構成します。

a) [Select Fabric Sites] をクリックして、ファブリックサイトを選択します。

仮想ネットワークは複数のファブリックサイトに割り当てることができます。ファブリックサイトを選択するには、次のいずれかのタスクを実行します。

- 必要なファブリックサイトの横にあるプラスアイコンをクリックします。
- ファブリックサイト名をクリックし、[Add Selected] をクリックします。

（注） 複数のファブリックサイトを選択するには、**Shift**キーを押しながらファブリックサイト名をクリックし、[Add Selected] をクリックします。

- すべてのファブリックサイトを選択するには、[Add All] をクリックします。

作成したすべてのレイヤ 3 仮想ネットワークについて、この関連付けを繰り返します。

b) [**Assign**] をクリックします。

c) [Select Fabric Zones] をクリックして、次のいずれかのタスクを実行します。

- 必要なファブリックゾーンの横にあるプラスアイコンをクリックします。
- ファブリックゾーン名をクリックし、[Add Selected] をクリックします。



（注） 複数のファブリックゾーンを選択するには、Shift キーを押しながらファブリック ゾーン名をクリックし、[Add Selected] をクリックします。

- すべてのファブリック ゾーンを選択するには、[Add All] をクリックします。

d) [**Assign**] をクリックします。

ステップ 5 [Summary] ウィンドウで、レイヤー 3 仮想ネットワークの設定を確認します。

ステップ 6 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

ステップ 7 [Tasks] ウィンドウで、タスクの展開を監視します。

レイヤ 2 仮想ネットワークの作成

手順

ステップ 1 メインメニューから次を選択します。**[Workflows]** > **[Create Layer 2 Virtual Networks]** の順に選択します。

または、**[Provision]** > **[Virtual Networks]** で [Layer 2] タブに移動し、[Create Layer 2 Virtual Networks] をクリックすることもできます。

ステップ 2 タスクの概要ウィンドウが開いたら、[Let's Do it] をクリックして、ワークフローに直接移動します。

ステップ 3 [設定属性（Configuration Attributes）] ウィンドウで、必要なレイヤ 2 仮想ネットワーク属性を設定します。

a) [VLAN Name] フィールドに、VLAN 名を入力します。

b) [VLAN ID] フィールドに、VLAN ID を入力します。有効な VLAN ID の範囲は 2 ～ 4093 です。

（注） 1002 ～ 1005 および 2046 の VLAN ID は、予約済みの VLAN ID です。

c) [Traffic Type] エリアから、[Data] または [Voice] を選択します。

d) [Fabric-Enabled Wireless] チェックボックスをオンにして、ワイヤレスを有効にします。
レイヤー 2 仮想ネットワークでは、[Layer 2 Flooding] チェックボックスがデフォルトで有効になっています。

e) [Layer 2 Flooding] の場合、フラッディングアドレスタイプを選択し、必要に応じてカスタムフラッディング IP アドレスを割り当てることができます。

- **フラッディングアドレス割り当て**: [Shared] または [Custom] を選択します。
- **フラッディングアドレス**: [Custom] を選択した場合、レイヤ 2 フラッディングのフラッディング IP アドレスを入力します。サポートされている IP アドレスの範囲は、IPv4 の場合は 239.0.0.0/8、IPv6 の場合は FF30::/96 です。[Shared] アドレスタイプのフラッディングアドレスは編集できません。

レイヤ 2 フラッディングは、次の方法でアンカーおよび継承された仮想ネットワークでサポートされます。

- アンカー仮想ネットワークで**レイヤ 2 フラッディング**が無効になっている場合、継承した仮想ネットワークでも無効になります。
- アンカー仮想ネットワークで**レイヤ 2 フラッディング**が有効になっている場合、継承した仮想ネットワークで有効または無効にできます。有効になっている場合、フラッディングアドレス割り当てタイプとフラッディングアドレスはアンカーされた仮想ネットワークと同じである必要があります。

f) [Flood Access Tunnel] チェックボックスをオンにして、フラッドアクセストンネルを有効にします。
[ファブリック対応ワイヤレス（Fabric-Enabled Wireless）] が有効になっている場合、レイヤ 2 仮想ネットワークに対してデフォルトで有効になっています。

g) ファブリック内の SSDP トラフィックをブロックするには、[Resource Guard] チェックボックスをオンにします。

h) 別のレイヤー 2 仮想ネットワークを追加するには、プラスアイコンをクリックして、3.a （1258 ページ）から 3.d （1259 ページ） までを繰り返します。

ステップ 4 [Fabric Sites and Advanced Attributes] ウィンドウで、[Fabric Zones] ドロップダウンからレイヤー 2 仮想ネットワークのファブリックサイトを選択します。必要に応じて、次の手順にしたがって、このレイヤー 2 仮想ネットワークに関連付けるファブリックゾーンを選択することもできます。

a) [Select Fabric Zones] をクリックして、次のいずれかのオプションを選択してファブリックゾーンを追加します。

- 必要なファブリックゾーンの横にあるプラスアイコンをクリックします。
- ファブリックゾーン名をクリックし、[Add Selected] をクリックします。

（注） 複数のファブリックゾーンを選択するには、Shift キーを押しながらファブリック ゾーン名をクリックし、[Add Selected] をクリックします。

- すべてのファブリック ゾーンを選択するには、[Add All] をクリックします。

b) [**Assign**] をクリックします。

作成したすべてのレイヤ 2 仮想ネットワークについて、この関連付けを繰り返します。

ステップ 5 （オプション）[Fabric Sites and Advanced Attributes] ウィンドウで、[Advanced Attributes] トグルボタンをクリックして、レイヤ 3 仮想ネットワークをこのレイヤ 2 仮想ネットワークに関連付けます。

ステップ 6 [Summary] ウィンドウで、レイヤ 2 仮想ネットワークの設定を確認します。

ステップ 7 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

ステップ 8 [Tasks] ウィンドウで、タスクの展開を監視します。

ステップ 9 成功メッセージが表示されたら、[エニーキャストゲートウェイを表示（View Anycast Gateway）] をクリックして、ゲートウェイの作成を確認します。

[Virtual Networks] ウィンドウの [Anycast Gateway] タブに、ファブリックに含まれるすべてのエニーキャストゲートウェイの詳細が表示されます。

ファブリックサイトへのレイヤ 3 仮想ネットワークの関連付け

手順

ステップ 1 メインメニューから次を選択します。**[Provision]** > **[Virtual Networks]**。

ステップ 2 [SUMMARY] で、[Layer 3 Virtual Networks] の数を示す数字をクリックします。

表示されるウィンドウに、グローバルレベルで作成されたすべてのレイヤ 3 仮想ネットワークが示されます。

ステップ 3 [Layer 3] タブで、ファブリックサイトの関連付けを編集したいレイヤ 3 仮想ネットワークの横にあるチェックボックスをオンにします。

（注） 最大 5 つのレイヤ 3 仮想ネットワークを編集できます。

ステップ 4 [More actions] にカーソルを合わせ、[Edit Fabric Site and Fabric Zone Associations] を選択します。

ステップ 5 [Fabric Sites and Fabric Zones (Optional)] ウィンドウで、次のように構成します。

a) [Select Fabric Sites] をクリックして、ファブリックサイトを選択します。

仮想ネットワークは複数のファブリックサイトに割り当てることができます。ファブリックサイトを選択するには、次のいずれかのタスクを実行します。

- 必要なファブリックサイトの横にあるプラスアイコンをクリックします。
- ファブリックサイト名をクリックし、[Add Selected] をクリックします。

（注） 複数のファブリックサイトを選択するには、**Shift**キーを押しながらファブリックサイト名をクリックし、[Add Selected] をクリックします。

- すべてのファブリックサイトを選択するには、[Add All] をクリックします。

すべてのレイヤー 3 仮想ネットワークについて、この関連付けを繰り返します。

b) [**Assign**] をクリックします。

c) [Select Fabric Zones] をクリックして、次のいずれかのタスクを実行します。

- 必要なファブリックゾーンの横にあるプラスアイコンをクリックします。
- ファブリックゾーン名をクリックし、[Add Selected] をクリックします。

（注） 複数のファブリックゾーンを選択するには、Shift キーを押しながらファブリック ゾーン名をクリックし、[Add Selected] をクリックします。

- すべてのファブリック ゾーンを選択するには、[Add All] をクリックします。

d) [**Assign**] をクリックします。

ステップ 6 [Summary] ウィンドウで、レイヤー 3 仮想ネットワークサイトを確認します。

ステップ 7 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。

- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238ページ）を参照してください。

ステップ 8 [Tasks] ウィンドウで、タスクの展開を監視します。

エニーキャストゲートウェイの作成

始める前に

レイヤ 3 仮想ネットワークが作成されていることを確認します。詳細については、レイヤ 3 仮想ネットワークの作成（1257 ページ）を参照してください。

手順

ステップ 1 メインメニューから次を選択します。**[Provision]** > **[Virtual Networks]**。

ステップ 2 [SUMMARY] で、[Anycast Gateways] の数を示す数字をクリックします。

ステップ 3 [Anycast Gateway] タブで、[Create Anycast Gateway] をクリックします。

または、メニューアイコンをクリックして**[Workflows]** > **[Create Anycast Gateways]**の順に選択します。

ステップ 4 タスクの概要ウィンドウが開いたら、[Let's Do it] をクリックして、ワークフローに直接移動します。

ステップ 5 [Layer 3 Virtual Networks] ウィンドウで、ゲートウェイを追加する仮想ネットワークを 1 つ以上選択します。

- 必要なファブリックサイトの横にあるプラスアイコンをクリックします。
- ファブリックサイト名をクリックし、[Add Selected] をクリックします。

（注） 複数のファブリックサイトを選択するには、**Shift**キーを押しながらファブリックサイト名をクリックし、[Add Selected] をクリックします。

- すべてのファブリックサイトを選択するには、[Add All] をクリックします。

ステップ 6 [Configuration Attributes] ウィンドウの左側のペインで、エニーキャストゲートウェイを作成するレイヤー 3 仮想ネットワークを選択し、必要な属性を設定します。

a) [IP Address Pool] ドロップダウンリストから、IP アドレスプールを選択します。

エニーキャストゲートウェイのセカンダリ IP アドレスプールを設定できます。

- セカンダリ IP プールを追加するには、次の手順を実行します。

1. [追加のIPアドレスプールの追加（Add additional IP addresses pool）] をクリックします。

2. [IPプールの選択（Select IP Pools）] ウィンドウで、最大 4 つの IP アドレスプールを選択し、[保存（Save）] をクリックします。

- セカンダリ IP プールを編集するには、次の手順を実行します。

1. [追加のIPアドレスプールの編集（Edit additional IP addresses pools）] をクリックします。
2. 必要に応じて IP アドレスプールを編集または削除し、[保存（Save）] をクリックします。



（注） INFRA_VN でエニーキャストゲートウェイを作成する場合、（IPv4 アドレスと IPv6 アドレスの両方を含む）デュアルスタック IP アドレスプールはサポートされません。ファブリック アンダーレイ タイプに対応するシングルスタック IP アドレスプールを選択します。IPv4 アンダーレイファブリックには IPv4 専用プールを、IPv6 アンダーレイファブリックには IPv6 専用プールを使用します。

b) INFRA_VN の場合、次の属性を設定します。

- [Pool Type] ドロップダウンリストから [AP] または [Extended Node] を選択します。
- [VLAN Name] に有効な VLAN 名を入力するか、[Auto generate VLAN name] チェックボックスをオンにします。
- [VLAN ID] に仮想ネットワークのカスタム VLAN ID を入力します。
- サプリカントベースの拡張ノードをオンボードするには、[Supplicant-Based Extended Node Onboarding] チェックボックスをオンにします。



（注） このチェックボックスは、拡張ノードプールタイプを選択した場合にのみアクティブになります。

- サプリカントベースの拡張ノードの MACsec 暗号化オンボーディングでは、[MACsec暗号化（MACsec Encrypted）] チェックボックスをオンにします。



（注） [MACsec暗号化（MACsec Encrypted）] チェックボックスは、[サプリカントベースの拡張ノードのオンボーディング（Supplicant-Based Extended Node Onboarding）] オプションを選択した場合にのみアクティブになります。

- **[Enforcement]** チェックボックスを使用して、ネットワークへのグループベースのポリシーの適用を有効または無効にします。[適用（Enforcement）]チェックボックスは、デフォルトでオンになっています。

（注） グループベースのポリシーの適用を無効にするオプションは、デフォルトポリシーが拒否に設定されているネットワークでデバイスをオンボーディングするときに便利です。[適用（Enforcement）] オプションは、チェックボックスをオフにすると使用できなくなります。

c) IP ダイレクトブロードキャスト機能を有効にするには、[IP-Directed Broadcast] チェックボックスをオンにします。

（注）
- ダイレクトブロードキャストを有効にすると、Catalyst Centerのレイヤ 2 フラッディングが自動的に有効になります。
- ルータおよび Cisco Nexus 7000 シリーズ スイッチは、ダイレクトブロードキャストをサポートしていません。
- ダイレクトブロードキャストを有効にする前に、アンダーレイマルチキャストが有効になっていることを確認してください。

d) サブネット内ルーティングを有効にするには、[Intra-Subnet Routing] チェックボックスをオンにします。

（注） イントラサブネット ルーティングを有効にすると、Catalyst Centerの [Fabric-Enabled Wireless] チェックボックスと [Layer 2 Flooding] チェックボックスが自動的に無効になります。

e) [TCP MSS Adjustment] チェックボックスをオンにして、エニーキャストゲートウェイの TCP 最大セグメントサイズ（MSS）値をカスタマイズし、必要な値を入力します。

[TCP MSSの調整（TCP MSS Adjustment）] 値を 500 ～ 1440 の範囲で設定できます。この値は、IPv4 および IPv6 の両方を介した TCP セッションに適用されます。

[TCP MSS Adjustment] の値は、すべてのエニーキャスト ゲートウェイ スイッチ仮想インターフェイス（SVI）に適用されます。

f) エニーキャストゲートウェイでサイレントホスト検出を有効にするには、[**Silent Host Discovery**] チェックボックスをオンにします。

事前認証 VLAN を使用したサイレントホスト検出を有効にするには、[**Edit Pre-Auth VLANs**] をクリックします。[Edit] ウィンドウで、事前認証 VLAN を選択します。カスタム事前認証 VLAN（VLAN 1 以外）を使用している場合は、[**Candidate Pre-Auth VLAN**] を有効にした状態でエニーキャストゲートウェイを作成します（手順 *l* を参照）。

（注） 事前認証 VLAN を使用した**サイレントホスト検出**で、事前認証された通信フローを許可するには、[**Authentication Control Direction**] が [**In**] に設定された状態で、ファブリックの認証テンプレートが [Open]、[Closed]、または [Low Impact] モードであることを確認します。

g) [VLAN Name] に有効な VLAN 名を入力するか、[Auto generate VLAN name] チェックボックスをオンにします。

h) [VLAN ID] に仮想ネットワークのカスタム VLAN ID を入力します。

（注）
- VLAN ID 1、1002 ー 1005、2046、および 4095 は予約済みで、使用できません。
- カスタム VLAN ID を指定しない場合は、Catalyst Center が 1021 ー 2020 の範囲の VLAN ID を生成します。

i) [Traffic Type] から、[Data] または [Voice] を選択します。

j) [Security Group] ドロップダウンリストからセキュリティグループを選択します。

k) [Critical VLAN] チェックボックスをオンにして、この IP プールをクリティカル IP アドレスプールに含めます。

認証サーバーを使用できない場合、クリティカルプールがクローズド認証プロファイルに使用されます。認証サーバーがない場合、クリティカルプールにクリティカル VLAN が割り当てられ、未認証のすべてのホストがそのクリティカル VLAN に配置されます。

（注） クリティカル VLAN を有効にすると、Catalyst Centerが VLAN 名を自動的に生成します。

l) [**Candidate Pre-Auth VLAN**] チェックボックスをオンにして、エニーキャストゲートウェイを事前認証 VLAN として使用できるようにします。このチェックボックスをオンにする場合は、必ず VLAN ID を設定してください。

[**Candidate Pre-Auth VLAN**] を有効にすると、サイレントホスト検出機能の設定時に、VLAN ID を事前認証 VLAN として選択できます。

m) ファブリック内の SSDP トラフィックをブロックするには、[Resource Guard] チェックボックスをオンにします。

n) この IP プールをワイヤレス IP アドレスプールとして有効にするには、[Fabric-Enabled Wireless] チェックボックスをオンにします。

o) レイヤ 2 フラッディングを有効にするには、[Layer 2 Flooding] チェックボックスをオンにします。

（注） レイヤ 2 フラッディングにはアンダーレイマルチキャストが必要であり、これは LAN 自動化中に設定されます。LAN 自動化でアンダーレイをプロビジョニングしない場合は、アンダーレイマルチキャストを手動で設定します。

p) [レイヤ2フラッディング（Layer 2 Flooding）] の場合、フラッディング アドレス タイプを選択し、必要に応じてカスタムフラッディング IP アドレスを割り当てます。

- **フラッディングアドレス割り当て**: [Shared] または [Custom] を選択します。
- **フラッディングアドレス**: [Custom] を選択した場合、レイヤ 2 フラッディングのフラッディング IP アドレスを入力します。サポートされている IP アドレスの範囲は、IPv4 の場合は 239.0.0.0/8、IPv6 の場合は FF30::/96 です。[Shared] アドレスタイプのフラッディングアドレスは編集できません。

レイヤ2フラッディングは、次の方法でアンカーおよび継承された仮想ネットワークでサポートされます。

- アンカー仮想ネットワークで **レイヤ 2 フラッディング**が無効になっている場合、継承した仮想ネットワークでも無効になります。
- アンカー仮想ネットワークで **レイヤ 2 フラッディング**が有効になっている場合、継承した仮想ネットワークで有効または無効にできます。有効になっている場合、フラッディングアドレス割り当てタイプとフラッディングアドレスはアンカーされた仮想ネットワークと同じである必要があります。

（注） **IP ダイレクトブロードキャスト**機能は、レイヤ2フラッディングの**フラッディングアドレス割り当て**および**フラッディングアドレス**の設定を採用します（設定されている場合）。

q) ファブリック対応のワイヤレスネットワークに接続されているブリッジモードの仮想マシンのオンボーディングを有効にするには、[Fabric Enabled Wireless] と [Multiple IP-to-MAC Addresses] チェックボックスをオンにします。

r) 1 つの有線ホストに複数の IPv4 アドレス（IP エイリアシング）を持たせるには、[Multiple IP-to-MAC Addresses] チェックボックスのみをオンにします。

1 つの MAC アドレスに最大 1000 個の IPv4 アドレスを設定できます。

s) [Flood Access Tunnel] チェックボックスをオンにして、フラッドアクセストンネルを有効にします。このオプションは、[ファブリック対応ワイヤレス（Fabric-Enabled Wireless）] が有効になっている場合にのみ使用できます。

t) IP プールをさらに関連付けるには、プラスアイコンをクリックして上記の手順を繰り返します。

ステップ 7 [Fabric Zones] （オプション）ウィンドウで、ファブリックゾーンを追加します。

a) [Select Fabric Zones] をクリックして、次のいずれかのオプションを選択してファブリックゾーンを追加します。

- 必要なファブリックゾーンの横にあるプラスアイコンをクリックします。
- ファブリックゾーン名をクリックし、[Add Selected] をクリックします。



（注） 複数のファブリックゾーンを選択するには、Shift キーを押しながらファブリック ゾーン名をクリックし、[Add Selected] をクリックします。

- すべてのファブリックゾーンを選択するには、[Add All] をクリックします。

b) [**Assign**] をクリックします。

ステップ 8 [Summary] ウィンドウでエニーキャストゲートウェイの設定を確認します。

ステップ 9 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 10 [Tasks] ウィンドウで、タスクの展開を監視します。

エクストラネットポリシー

レイヤ3仮想ネットワーク（VN）間でフュージョンデバイスを使用せずにルートリークできるエクストラネットポリシーを設定します。エクストラネットポリシーを使用し、Catalyst Centerの自動化を介してエンドポイント（ホストやユーザー）にDHCP、DNS、インターネットなどの共有サービスへのアクセスを提供します。共有サービスはプロバイダーVNに接続します。共有サービスを使用するエンドポイントは、サブスクライバーVNに常駐します。エクストラネットポリシーは、プロバイダー VN とサブスクライバ VN 間の通信を確立します。

次の展開に関して、エクストラネットポリシーを作成、編集、および削除することができます。

- IP トランジットを使用した単一サイトファブリック
- SDA トランジットを使用したマルチサイトファブリック

エクストラネットポリシー管理

Catalyst Center は、従来のポリシーベースルーティング設定から移行して、ボーダーデバイスにエクストラネットポリシーを展開するための新しいCLI設定をサポートします。新しいCLI

設定は、Cisco IOS XE リリース 17.18.1 以降を実行しているボーダーデバイスでのみサポートされます。下位バージョンを実行しているデバイスは、ポリシーベースルーティング設定を引き続きサポートします。

エクストラネットポリシーのステータスは、ファブリックサイトテーブルの [エクストラネットポリシー（Extranet Policy）] 列で確認できます。設定オプションを使用して、テーブルでの [エクストラネットポリシー（Extranet Policy）] 列の表示を有効にします。

エクストラネットポリシー移行のシナリオ

Catalyst Center は、ボーダーデバイスのサポートに基づいて、ポリシーベースルーティング設定から新しい CLI アプローチへのファブリックサイトの移行をサポートします。

サイトの移行準備が整うと、ファブリックウィンドウに情報バナーが表示されます。

（注） ファブリック内のすべてのデバイスが新しいCLIベースのエクストラネットポリシーに移行された後は、ポリシーベースルーティング設定に戻したり、IOS XE バージョン 17.18.1 より前のバージョンを実行しているファブリックにボーダーデバイスを追加したりすることはできません。

次の表に、新規と既存のファブリックサイトの移行シナリオを示します。

ファブリック内のすべてのボーダーデバイスが 17.18.1 以降のバージョンである新しいサイトの場合。	移行は自動的に行われます。エクストラネットポリシーを作成すると、新しい CLI 設定を使用してファブリック内のすべてのボーダーデバイスに展開されます。
ファブリック内のすべてのボーダーデバイスが 17.18.1 以降のバージョンにアップグレードされた既存のサイトの場合。	サイトの移行準備が整っており、更新を適用できることを示す情報バナーが表示されます。

エクストラネットポリシーの設定に関するガイドライン

エクストラネットポリシーを設定する前に、次のガイドラインを考慮してください。

- エクストラネットポリシーを設定するには、Cisco IOS XE 17.9.1 以降のリリースがデバイスで動作している必要があります。
- エクストラネットポリシーは、LISP Pub/Sub コントロールプレーンがあるファブリックサイトでのみサポートされます。
- SD-Access トランジットを使用するマルチサイトファブリックでエクストラネットポリシーを設定するには、すべてのサイトにプロバイダー VN がある必要があります。
- ネットワークで複数の VN ポリシーを設定する場合、同じ VN を複数のポリシーでプロバイダー VN にすることはできません。
- エクストラネットポリシーは、重複する IP プールをサポートしていません。

- ポリシー内のプロバイダー VN は、別の VN ポリシー内のサブスクライバ VN として設定することはできません。また、その逆もできません。
- エクストラネットポリシーが適用されるすべてのファブリックサイトにプロバイダー VN を追加してください。
- プロバイダー VN がファブリック外で互いにリークしないようにしてください。そうしないと、サブスクライバ VN 間でルートリークが発生する可能性があります。
- エクストラネットポリシーはルータデバイスではサポートされていません。
- エクストラネットポリシーを介した VN 間マルチキャストはサポートされていません。エクストラネットポリシーを介して相互接続されているレイヤ 3 仮想ネットワーク間ではマルチキャストをルーティングできません。

エクストラネットポリシーの作成

エクストラネットポリシーを作成するには、次の手順を実行します。

手順

ステップ 1 メインメニューから次を選択します。**[Workflows]** > **[Create Extranet Policy]**の順に選択します。

または、**[Provision]** > **[Virtual Networks]**の [Extranet Policies] タブに移動します。[Extranet Policies] ウィンドウで、[Create Extranet Policy] をクリックします。

ステップ 2 画面上のガイダンスに従ってポリシーの名前を指定し、プロバイダー VN とサブスクライバ VN を選択します。

このエクストラネットポリシーを 1 つ以上のファブリックサイトに割り当てることができます。

SD-Access トランジットでファブリックサイトに接続するマルチサイト展開では、SD-Access トランジットによって接続されているすべてのファブリックサイトを選択してください。

ステップ 3 [概要（Summary）] ページで、エクストラネットポリシー設定を確認します。

変更を加えるには、変更する設定のグループの横にある [Edit] をクリックします。

ステップ 4 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

ステップ 5 [Tasks] ウィンドウで、タスクの展開を監視します。

エクストラネットポリシーの編集

エクストラネットポリシーを編集して、サブスクライバ VN の追加または削除、ファブリックサイトへのポリシーの割り当て、ファブリックサイトからのポリシーの削除を行うことができます。

手順

ステップ 1 メインメニューから次を選択します。**[Provision]** > **[Virtual Networks]** の順に選択します。

ステップ 2 [Extranet Policies] タブで、編集するポリシーを選択し、**[More Actions]** > **[Edit Extranet Policy]** の順にクリックします。

ステップ 3 画面上のガイダンスに従ってポリシーを編集します。

エクストラネットポリシーの削除

エクストラネットポリシーを削除するには、次の手順を実行します。

手順

ステップ 1 メインメニューから次を選択します。**[Provision]** > **[Virtual Networks]** の順に選択します。

ステップ 2 [Extranet Policies] タブで、削除するポリシーを選択し、**[More Actions]** > **[Delete Extranet Policy]** の順にクリックします。

ステップ 3 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

ステップ 4 [Tasks] ウィンドウで、タスクの展開を監視します。

ファブリックゾーンの設定

ファブリックサイト（親サイト）は、ネットワークを簡単に管理できるように、より小さなサブネットによるファブリックゾーンに分割できます。ファブリックゾーンは、独自のエッジノードと拡張ノードを持つことができますが、コントロールプレーンとボーダーのために親サイトに接続します。以前の Catalyst Center のリリースから現在のリリースに移行した場合は、

既存のファブリックサイトにファブリックゾーンを作成することができます。このファブリックゾーンは、親サイトのすべてのプロパティを継承します。

はじめる前に

- ネットワーク階層がグローバルサイトの下に作成されていることを確認します。
- 階層の最下位に位置していない親サイトを選択します。

次に、ファブリックゾーンを設定するためのワークフローの概要を示します。

1. 次のいずれかの方法でファブリックゾーンを作成します。
   - [Create a Fabric Site] ワークフローを使用して、ファブリックサイトとそのゾーンを作成します。詳細については、ファブリックサイトとファブリックゾーンの作成（1271ページ）を参照してください。
   - 既存のファブリックサイトを編集して、ファブリックゾーンを追加します。詳細については、ファブリックサイト内のファブリックゾーンの作成（1273ページ）を参照してください。
2. ファブリックゾーンにエッジノードと拡張ノードを追加します。詳細については、デバイスをファブリックに追加（1235ページ）を参照してください。
3. ファブリックゾーンにレイヤ3仮想ネットワークとセグメントを割り当てます。詳細については、ファブリックゾーンへのレイヤ3仮想ネットワークの関連付け（1274ページ）を参照してください。

（注） ファブリックゾーンで使用できるのは親サイトの仮想ネットワークとセグメントのみです。

（注） ファブリックゾーンに追加されたセグメントは、親サイトでは更新できません。

親サイトのファブリックゾーンのエッジノードおよび拡張ノードは編集できません。

ファブリックゾーンのエッジノードは、親サイトのコントロールプレーンまたはボーダーとして設定できます。

ファブリックサイトとファブリックゾーンの作成

手順

ステップ1 メインメニューから次を選択します。**[Provision]** > **[Fabric Sites]**。

ステップ2 [Create Fabric Site] をクリックします。

または、メニューアイコンをクリックして**[Workflows]** > **[Create Fabric Site]**の順に選択します。

ステップ 3 タスクの概要ウィンドウが表示されたら、[Let's Do It] をクリックして、ワークフローに直接移動します。

ステップ 4 [Fabric Site Location] ウィンドウで、ファブリックゾーンとして追加するエリア、建物、またはフロアを選択します。

ステップ 5 [Wired Endpoint Data Collection] ウィンドウで、[Wired Endpoint Data Collection] チェックボックスがオンになっていることを確認します。

ステップ 6 [認証テンプレート（Authentication Template）] ウィンドウで、次のタスクを実行します。

a) ファブリックサイトの認証テンプレートを選択します。

- [Closed Authentication]：認証前のすべてのトラフィック（DHCP、DNS、ARP など）が廃棄されます。
- [Open Authentication]：ホストには、802.1X 認証を受ける必要なくネットワーク アクセスが許可されます。
- [Low Impact]：スイッチポートに ACL を適用することでセキュリティを追加して、認証前に制限されたネットワークアクセスを許可します。ホストが正常に認証されると、追加のネットワーク アクセスが許可されます。
- なし（None）

b) （オプション）[Closed Authentication]、[Open Authentication]、または [Low Impact] を選択した場合は、[Edit] をクリックして認証設定を編集します。

- [First Authentication Method]：[802.1x] または [MAC Authentication Bypass（MAB）] を選択します
- [802.1x Timeout（in seconds）]：スライダを使用して、802.1x タイムアウトを秒単位で指定します。
- [Wake on LAN]：[Yes] または [No] を選択します。
- [Number of Hosts]：[Unlimited] または [Single] を選択します。
- [BPDU Guard]：このチェックボックスを使用して、すべての [Closed Authentication] ポートでブリッジ プロトコル データ ユニット（BPDU）ガードを有効または無効にします。
- [Pre-Authentication Access Control List]：トグルボタンを有効にして、[Low Impact] 認証の事前認証制御を構成します。[Implicit Action] ドロップダウンリストから、暗黙的なアクションを選択します。ルールの説明を入力します。アクセスコントラクトを追加するには、[Add Contract Action] をクリックし、ルールを選択して、[Apply Table] をクリックします。

ステップ 7 [Fabric Zones] ウィンドウで、ファブリックゾーンを指定し、範囲指定されたサブネットを作成するには、[Setup Fabric Zones Now] をクリックします。

ファブリックゾーンを有効にするには、ネットワーク階層でファブリックサイトを選択します。

ステップ 8 [Summary] ウィンドウで、ファブリックサイトの設定を確認します。

ここでファブリックサイトまたはゾーン設定を編集できます。

ステップ 9 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 10 [Tasks] ウィンドウで、タスクの展開を監視します。

ステップ 11 サイトとゾーンがプロビジョニングされるまでに数秒かかります。作成を確認する成功メッセージが表示されます。

サイト階層ペインでは、新しく作成されたファブリックゾーンに「FZ」というタグが付けられます。

ファブリックサイト内のファブリックゾーンの作成

手順

ステップ 1 メインメニューから次を選択します。**[Provision]** > **[Fabric Sites]**。

ステップ 2 [SUMMARY] で、ファブリックサイトの数を示す数字をクリックします。

ステップ 3 ファブリックゾーンを指定するファブリックサイトの [アクション（Actions）] 列で、省略記号アイコン（ ••• ）にカーソルを合わせて [ファブリックゾーンの編集（Edit Fabric Zone）] を選択します。

ステップ 4 [Edit Fabric Zones] ウィンドウで、エリア、建物、またはフロアを選択します。

ステップ 5 [Summary] ウィンドウでファブリックサイトの設定を確認します。

ここでファブリックサイトまたはゾーン設定を編集できます。

ステップ 6 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 7 [Tasks] ウィンドウで、タスクの展開を監視します。

ステップ 8 ファブリックサイトとファブリックゾーンがプロビジョニングされるまでに数秒かかります。プロビジョニングを確認する成功メッセージが表示されます。

サイト階層ペインでは、新しく作成されたファブリックゾーンが「FZ」になります。

次のタスク

- 新しく作成したファブリックゾーンにエッジノードデバイスと拡張ノードデバイスのみを追加します。

  ファブリックゾーンに割り当てられている親サイトデバイスに割り当てることはできません。ただし、ファブリックゾーンへのエッジノードデバイスの割り当てを親サイトのコントロールプレーンまたはボーダーノードして設定することは可能です。

- ファブリックゾーンに IP プールと仮想ネットワークを割り当てます。

ファブリックゾーンへのレイヤ 3 仮想ネットワークの関連付け

始める前に

ファブリックゾーンが作成されていることを確認します。

（注） ファブリックゾーンに追加できるのは親サイトのレイヤ 3 仮想ネットワークのみです。

手順

ステップ 1 メインメニューから次を選択します。**[Provision]** > **[Virtual Networks]**。

ステップ 2 [SUMMARY] で、[Layer 3 Virtual Networks] の数を示す数字をクリックします。

表示されるウィンドウに、グローバルレベルのすべてのレイヤ 3 仮想ネットワークが示されます。

ステップ 3 [Layer 3] タブで、ファブリックゾーンの関連付けを編集するレイヤー 3 仮想ネットワークの横にあるチェックボックスをオンにします。

（注） 最大 5 つのレイヤ 3 仮想ネットワークを編集できます。

ステップ 4 [More actions] にカーソルを合わせ、[Edit Fabric Site and Fabric Zone Associations] を選択します。

ステップ 5 [Fabric Sites and Fabric Zones (Optional)] ウィンドウで、次のように構成します。

a) [Select Fabric Zones] をクリックして、ファブリックゾーンを選択します。

仮想ネットワークは、ファブリックサイトの複数のファブリックゾーンに割り当てることができます。ファブリックゾーンを選択するには、次のいずれかのタスクを実行します。

- 必要なファブリックゾーンの横にあるプラスアイコンをクリックします。
- ファブリックゾーン名をクリックし、[Add Selected] をクリックします。

（注） 複数のファブリックゾーンを選択するには、Shift キーを押しながらファブリック ゾーン名をクリックし、[Add Selected] をクリックします。

- すべてのファブリック ゾーンを選択するには、[Add All] をクリックします。

b) [**Assign**] をクリックします。
c) すべてのレイヤー 3 仮想ネットワークについて、この関連付けを繰り返します。

ステップ 6 [Summary] ウィンドウで、レイヤー 3 仮想ネットワークゾーンを確認します。

ステップ 7 [Created and Deploy（Step 1 of 2）] ウィンドウで、[Update] をクリックします。

ステップ 8 [Created and Deploy（Step 2 of 2）] ウィンドウで、[Deploy] をクリックして、レイヤ 3 仮想ネットワークをデプロイします。

ステップ 9 仮想ネットワークを確認するには、[View Layer 3 Virtual Networks] をクリックします。

[Virtual Networks] ウィンドウの [Layer 3] タブに、すべてのレイヤー 3 仮想ネットワークの詳細情報が表示されます。

ファブリックゾーンへのレイヤ 2 仮想ネットワークの関連付け

始める前に

（注） ファブリックゾーンに追加されたゲートウェイは、親サイトでは編集できません。

手順

ステップ 1 メインメニューから次を選択します。**[Provision]** > **[Virtual Networks]**。

ステップ 2 [SUMMARY] で、[Layer 2 Virtual Networks] の数を示す数字をクリックします。

表示されるウィンドウに、グローバルレベルのすべてのレイヤ 2 仮想ネットワークが示されます。

ステップ 3 [Global] ファブリックサイトをクリックします。

ステップ 4 [Select Fabric Site] スライドインペインで、ファブリックサイトを選択し、[Select] をクリックします。

ステップ 5 [レイヤー2] タブで、ファブリックゾーンの関連付けを編集したいレイヤ2仮想ネットワークのチェックボックスをオンにします。

（注） 最大 5 つのレイヤー 2 仮想ネットワークを編集できます。

ステップ 6 [More actions] にカーソルを合わせ、[Edit Layer 2 Fabric Zone Associations] を選択します。

ステップ 7 **[関連付けられたファブリックサイトおよびファブリックゾーン（Associated Fabric Sites and Fabric Zones）]** ウィンドウで、次の設定を行います。

a) [Select Fabric Zones] をクリックして、ファブリックゾーンを選択します。

仮想ネットワークは、ファブリックサイトの複数のファブリックゾーンに割り当てることができます。ファブリックゾーンを選択するには、次のいずれかのタスクを実行します。

- 必要なファブリックゾーンの横にあるプラスアイコンをクリックします。
- ファブリックゾーン名をクリックし、[Add Selected] をクリックします。

（注） 複数のファブリックゾーンを選択するには、Shift キーを押しながらファブリック ゾーン名をクリックし、[Add Selected] をクリックします。

- すべてのファブリック ゾーンを選択するには、[Add All] をクリックします。

b) [**Assign**] をクリックします。

c) すべてのレイヤ 2 仮想ネットワークに、この関連付けを繰り返します。

ステップ 8 [Summary] ウィンドウで、レイヤ 2 仮想ネットワークの設定を確認して、[Create] をクリックします。

ステップ 9 [Create] ウィンドウで、[Deploy] をクリックして、レイヤー 2 仮想ネットワークを展開します。

レイヤ 2 仮想ネットワークがプロビジョニングされると、成功メッセージが表示されます。

ステップ 10 仮想ネットワークの作成を確認するには、[View Layer 2 Virtual Networks] をクリックします。[Virtual Networks] ウィンドウの [Layer 2] タブに、すべてのレイヤー 2 仮想ネットワークの詳細情報が表示されます。

ファブリックゾーンへのエニーキャストゲートウェイの関連付け

始める前に

ファブリックゾーンが作成されていることを確認します。

（注） 親サイトのエニーキャストゲートウェイのみをファブリックゾーンに追加できます。

ファブリックゾーンに追加されたエニーキャストゲートウェイは、親サイトでは更新できません。

手順

ステップ 1 メインメニューから次を選択します。**[Provision]** > **[Virtual Networks]**。

ステップ 2 [SUMMARY] で、[Anycast Gateways] の数を示す数字をクリックします。

表示されるウィンドウに、グローバルレベルのすべてのエニーキャストゲートウェイが示されます。

ステップ 3 [Global] ファブリックサイトをクリックします。

ステップ 4 [Select Fabric Site] スライドインペインで、ファブリックサイトを選択し、[Select] をクリックします。

ステップ 5 [Anycast Gateway] タブで、ファブリックゾーンの関連付けを編集するエニーキャストゲートウェイの横にあるチェックボックスをオンにします。

（注） 最大 5 つのエニーキャストゲートウェイを編集できます。

ステップ 6 [More actions] にカーソルを合わせ、[Edit Fabric Zone Associations] を選択します。

ステップ 7 **[ファブリックゾーン（Fabric Zones）]（オプション）**ウィンドウで、次の手順を実行します。

a) [Select Fabric Zones] をクリックして、次のいずれかのタスクを実行します。

- 必要なファブリックゾーンの横にあるプラスアイコンをクリックします。
- ファブリックゾーン名をクリックし、[Add Selected] をクリックします。

（注） 複数のファブリックゾーンを選択するには、Shift キーを押しながらファブリック ゾーン名をクリックし、[Add Selected] をクリックします。

- すべてのファブリック ゾーンを選択するには、[Add All] をクリックします。

b) [**Assign**] をクリックします。

ステップ 8 [Summary] ウィンドウでエニーキャストゲートウェイの設定を確認します。

ステップ 9 [Create] ウィンドウで、[Deploy] をクリックします。

ステップ 10 成功メッセージが表示された後にゲートウェイの作成を確認するには、[View Anycast Gateway] をクリックします。

[Virtual Networks] ウィンドウの [Anycast Gateway] タブに、すべてのエニーキャストゲートウェイの詳細が表示されます。

拡張ノードデバイスの設定

拡張ノードは、自動化されたワークフローによって設定されます。設定後、拡張ノードデバイスがファブリックトポロジビューに表示されます。[Port Assignment] タブを使用して、拡張ノードにポートを割り当てることができます。

（注） 拡張ノードは、GUI ベースのプロビジョニング ワークフローではオンボードできません。拡張ノードをオンボーディングするには、デバイス設定を工場出荷時の初期状態にリセットしてデバイスの電源をオンにした後に、SD-Access 自動化ワークフローを使用する必要があります。

デバイスは、拡張ノードネイバーのライセンスとデバイス自体のライセンスに従ってオンボードされます。

- ネイバーが Essentials ライセンスで動作している場合、デバイスのライセンスに関係なく、そのデバイスは標準の拡張ノードとしてオンボードされます。
- ネイバーが Advantage ライセンスで動作していて、デバイスに Essentials ライセンスがある場合、そのデバイスは標準の拡張ノードとしてオンボードされます。
- ネイバーが Advantage ライセンスで動作していて、デバイスに Advantage ライセンスがある場合、そのデバイスはポリシー拡張ノードとしてオンボードされます。
- デバイスに複数のネイバーがあり、各ネイバーのライセンスレベルが異なる場合、デバイスのライセンスに関係なく、そのデバイスは標準の拡張ノードとしてオンボードされます。

拡張ノードデバイスは、マルチキャストトラフィックをサポートします。

ポリシー拡張ノードは、仮想ネットワーク内のセキュリティポリシーをサポートする拡張ノードです。ポリシー拡張ノードのポート割り当て時に、[グループ（Group）] を選択できます。

ポリシー拡張ノードデバイスには、Cisco IOS XE リリース 17.1.1s 以降を実行している Cisco Catalyst Industrial Ethernet（IE）3400、IE 3400 Heavy Duty シリーズ スイッチ、および Cisco Catalyst 9000 シリーズ スイッチがあります。

シスコ デジタルビルディング シリーズ スイッチ、Cisco Catalyst 3560-CX スイッチ、および Cisco Industrial Ethernet 4000、4010、5000 シリーズ スイッチは、ポリシー拡張ノードとして構成することはできません。

拡張ノードの設定

Cisco Catalyst 9300、Cisco Catalyst 9400、および Cisco Catalyst 9500 シリーズスイッチは、ファブリックエッジとして設定されたときに拡張ノードをサポートします。

（注） ファブリックエッジノードとして設定されている Cisco Catalyst 9200 シリーズ スイッチは、拡張ノードデバイスをサポートしていません。

拡張ノードでサポートされている最小ソフトウェアバージョンは次のとおりです。

- Cisco Industrial Ethernet 4000、4010、5000 シリーズ スイッチ：15.2(7)E0s（LAN ベースライセンスが有効になっている）

  IP サービスライセンスがある場合は、Switch Database Management（SDM）テンプレートを `dual-ipv4-and-ipv6 default` に手動で変更する必要があります。

- Cisco Catalyst IE 3400、3400 Heavy Duty（X-coded および D-coded）シリーズ スイッチ：Cisco IOS XE リリース 17.1.1s。
- Cisco Catalyst IE 3100、3200 シリーズ スイッチ：Cisco IOS XE リリース 17.15.x。
- Cisco Catalyst IE 3300 シリーズ スイッチは、Essentials ライセンス（Cisco IOS XE リリース 16.12.1s）を実行している場合、拡張ノードとして動作できます。
- Cisco Digital Building シリーズ スイッチ、Cisco Catalyst 3560-CX スイッチ：リリース 15.2(7)E0s。

ポリシー拡張ノードデバイス、およびポリシー拡張ノードをサポートするエッジノードデバイスで必要な最小ソフトウェアバージョンは Cisco IOS XE リリース 17.1.1 s です。

この設定手順は、標準の拡張ノードとポリシー拡張ノードの両方に適用されます。

始める前に

ポリシー拡張ノードとしてデバイスを設定するには、デバイスとそれをサポートするエッジノードの両方で、Network Advantage と Advantage のライセンスレベルが有効になっている必要があります。

手順

ステップ 1 拡張ノードのネットワーク範囲を設定します。IP アドレスプールを設定する （397 ページ） を参照してください。この手順では、IP アドレスプールを追加し、サイトレベルで IP プールを予約します。CLI および SNMP クレデンシャルが設定されていることを確認します。

ステップ 2 拡張 IP アドレスプールを INFRA_VN に割り当てます。エニーキャストゲートウェイの作成 （1262 ページ） を参照してください。[Pool Type] として [Extended Node] を選択します。

Catalyst Center Cisco DNA Center は、サポートされているファブリックエッジデバイスで拡張 IP アドレスプールと VLAN を設定します。これにより、拡張ノードのオンボーディングが有効になります。

ステップ 3 拡張 IP アドレスプールとオプション 43 を使用して DHCP サーバーを設定します。拡張 IP アドレスプールが Catalyst Center から到達可能であることを確認します。



（注） オプション 43 の詳細については、DHCP コントローラディスカバリ （702 ページ）を参照してください。

ステップ 4 ファブリックエッジデバイスに拡張ノードデバイスを接続します。拡張ノードデバイスからファブリックエッジへ複数のリンクを設定できます。

ステップ 5 拡張ノードに接続されているファブリックエッジノードでポートチャネルを作成します。リングまたはデイジーチェーン内の後続の拡張ノードに関して、それが接続している、前の拡張ノードでポートチャネルを作成します。



（注） この手順は、ファブリックのグローバル認証モードが [Open Authentication]、[Low Impact]、または [Closed Authentication] の場合にのみ完了してください。ファブリックサイトが [None] 認証モードに設定されている場合、ポートチャネルは、プラグ アンド プレイ プロビジョニングを使用した拡張ノードのオンボーディング中に自動的に作成されます。

ポートチャネルを作成するには、次の手順を実行します。

a) メインメニューから次を選択します。**[Provision]** > **[Fabric Sites]**。
b) [Fabric Sites] タブで、ファブリックサイトの数を示す数字をクリックします。
c) [fabric site] をクリックします。
d) [ポートの割り当て（Port Assignment）] タブで、**[その他のアクション（More Actions）]** > **[ポートチャネルの作成（Create Port Channel）]**を選択します。
e) 次のタスクを完了します。

- ポートチャネルを作成する必要があるファブリックデバイスを選択します。
- [Connected Device Type] ドロップダウンリストから [Extended Node] を選択します。
- 説明を入力します。
- [Port Aggregation Protocol (PAgP Desirable)] を選択します。

  Cisco IOS XE リリース 17.1.1s 以降、IE 3300 および IE 3400 デバイスは PAgP をサポートしています。
- Cisco IOS XE リリース 17.1.1s よりも前のバージョンを実行している場合は、IE 3300 および IE 3400 デバイスの [On] を選択します。

（注） 拡張ノードのオンボーディングでは Link Aggregation Control Protocol（LACP）は機能しません。

- ポートチャネルとしてバンドルするポートを選択します。

f) [Done] をクリックします。

これで、ファブリックエッジノード（または拡張ノード）にポートチャネルが作成され、拡張デバイスがオンボードされます。

ステップ 6 以前の設定がない場合は、拡張ノードデバイスの電源をオンにします。拡張ノードデバイスに構成がある場合は、デバイス構成を工場出荷時のデフォルトにリセットしてリロードします。

Catalyst Centerは、拡張ノードデバイスをインベントリに追加し、同じサイトをファブリックエッジとして割り当てます。これで拡張ノードデバイスがファブリックに追加され、オンボードされ、管理できるようになります。

（注） 拡張ノードデバイスは、Catalyst Center リリースと互換性のあるソフトウェアリリースを実行している場合にのみ、ファブリックに追加されます。デバイスが互換性のないソフトウェアリリースを実行している場合は、オンボードされません。ファブリックデバイスの互換性については、「Cisco SD-Access Compatibility Matrix」を参照してください。

設定が完了すると、拡張ノードがファブリックトポロジに、拡張ノードであることを示すタグ（X）とともに表示されます。

拡張ノードのポリシー拡張ノードへのアップグレード

Cisco SD-Access の自動化では、Essentials ライセンスを持つポリシー拡張ノード対応デバイスが拡張ノードとしてオンボーディングされます。ライセンスを Advantage にアップグレードすることで、この拡張ノードデバイスをポリシー拡張ノードに変換できます。

デイジーチェーンでは、アップストリームデバイスが拡張ノードである場合、拡張ノードをポリシー拡張ノードにアップグレードすることはできません。

リングでは、ネイバーが両方とも拡張ノードである場合、拡張ノードをポリシー拡張ノードにアップグレードすることはできません。

ポリシー拡張ノードにアップグレードされたノードを、拡張ノードとして再設定することはできません。

拡張ノードをポリシー拡張ノードに変換するには、次の手順を実行します。

始める前に

- 拡張ノードがすでにオンボーディングされていることを確認してください。
- Catalyst Center でスマートライセンス認証情報を更新します。

手順

ステップ 1 Catalyst Center ライセンスマネージャを使用して、デバイスのライセンスレベルを Essentials から Advantage に変更します。

a) メインメニューから次を選択します。**[Tools]** > **[License Manager]** の順に選択します。
b) [Devices] タブで、デバイスの横にあるチェックボックスをオンにします。
c) **[Actions]** > **[Change License]** > **[Change Cisco License]** を選択します。
d) [Change Cisco License Level] ウィンドウで、[Advantage] をクリックします。
e) ライセンスタイプを選択します。

必要なライセンスタイプ（[すべて（All）]、[DNA]、または [CNS]）をクリックします。

f) [Continue] をクリックします。
g) ライセンスレベルが更新されたときにデバイスを再起動するには、[更新時にデバイスを再起動（Reboot device on update）] チェックボックスをオンにします。
h) （任意） [Task Name] フィールドで、タスク名を更新します。
i) ライセンスレベルを更新するスケジュールを選択します。

- [Now]：ライセンスレベルをただちに更新し、デバイスを再起動します。
- [Later]：日付と時刻をスケジュールし、ライセンスレベルを更新してデバイスを再起動するためのタイムゾーンを定義します。

j) [Confirm] をクリックします。

ステップ 2 ノードが [Reachable] になり、[Managed] 状態になるのを待ちます。

[Provision] > **[Inventory]** ウィンドウに、すべてのデバイスの到達可能性ステータスが表示されます。

ステップ 3 「Netconf Connection Refused」エラーが表示された場合は、デバイスを再同期します。エラーが表示されなくなるまで、再同期プロセスを繰り返します。

a) **[プロビジョニング（Provision）]** > **[インベントリ（Inventory）]** ウィンドウで、デバイスを選択します。
b) **[Actions]** > **[Inventory]** > **[Resync Device]** の順に選択します。

ステップ 4 ポリシー拡張ノードにアップグレードします。

a) **[Provision]** > **[Fabric Sites]** ウィンドウで、デバイスがオンボーディングされているサイトを選択します。
b) [Fabric Infrastructure] タブで、デバイスをクリックしてその属性を編集します。

c) [ファブリック（Fabric）] タブで、[拡張ノード属性（Extended Node Attributes）] の下にある **[ポリシー拡張ノード（Policy Extended Node）]** トグルボタンをクリックします。次に、[追加（Add）] をクリックします。

d) **[ポリシー拡張ノードアップグレード（Policy Extended Node Upgrade）]** ダイアログボックスで、[アップグレード（Upgrade）] をクリックします。

e) [ENからPENへのアップグレード（EN to PEN Upgrade）] スライドインペインで、展開するタスクをスケジュールします。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

f) [Tasks] ウィンドウで、タスクの展開を監視します。

拡張ノードの削除

このタスクでは、拡張ノード、ポリシー拡張ノード、および認証済み拡張ノードを削除する手順について説明します。

手順

ステップ 1 ファブリックから拡張ノードデバイスを削除します。

a) メインメニューから次を選択します。**[Provision]** > **[Fabric Sites]**。

b) [Fabric Sites] タブで、ファブリックサイトの数を示す数字をクリックします。

c) 拡張ノードデバイスを含むファブリックサイトを選択します。

d) [Fabric Infrastructure] タブで、拡張ノードデバイスをクリックします。

e) スライドインペインで、[Remove From Fabric] をクリックします。

f) [Add] をクリックします。

ステップ 2 デバイスを [Inventory] から削除します。

インベントリからデバイスを削除する手順については、ネットワークデバイスの削除 （218 ページ）を参照してください。

ステップ 3 サプリカントベースの拡張ノードデバイスの場合、ファブリックエッジノードまたは FIAB でポート割り当て設定を削除します。

拡張ノードおよびポリシー拡張ノードの REP リングトポロジの設定

Resilient Ethernet Protocol（REP）はネットワークループの制御、リンク障害の処理、コンバージェンス時間の改善を実現します。

特に明記されていないかぎり、「拡張ノード」という用語はポリシー拡張ノードも表します。

REP リングで設定できるデバイスは次のとおりです。

- 拡張ノード：

  Cisco IOS 15.2(7)E3 以降のリリースが動作する Cisco Industrial Ethernet (IE) 4000、4010、5000 シリーズ スイッチ。

  Cisco IOS XE 17.3.3 以降のリリースが動作する CATALYST IE3100、3200、3300、3500、9300 シリーズ スイッチ。

- ポリシー拡張ノード：

  Cisco IOS XE 17.3.3 以降のリリースが動作する Cisco Catalyst IE3400、IE3400H シリーズ スイッチ。

REP リングの制約事項

- 特定の REP リング内の複数のリングおよびリングのリングはサポートされていません。
- REP リング内のノードには、デイジーチェーン方式で他のノードを接続できます。ただし、デイジーチェーンのノードには、ノードのリングを接続することはできません。
- REP リングまたはデイジーチェーンでは、拡張ノードとポリシー拡張ノードを混在させることはできません。REP リングまたはデイジーチェーンは、拡張ノードのみで、またはポリシー拡張ノードのみで構成されている必要があります。
- デフォルトでは、1 つの REP リングに最大 18 台のデバイスをオンボードできます。19 台以上のデバイスをオンボードするには、**spanning-tree vlan** *infra VN VLAN* **max-age 40** コマンドを使用して BPDU タイマーを増やします。Catalyst Center テンプレートを使用して、コマンドを設定します。
- REP リング内のデバイスが到達不能な場合、Catalyst Center は REP リングを削除できません。

（注） リングの最後の 2 つのノードが同時にオンボードを試みると、まれに、これらのノード間にポートチャネルが作成されない場合があります。REP リングが作成されると、リングの最後の 2 つのノード間にポートチャネルが確立されます。

特に明記されていないかぎり、次の手順は拡張ノードとポリシー拡張ノードの両方に適用されます。

始める前に

ファブリックエッジノードと拡張ノードがオンボードされていることを確認します。

REP リングの終端となっているファブリックエッジノードとそのインターフェイスを特定します。

（注） REP リング設定手順により、ネットワークトラフィックが短時間中断される可能性があります。

手順

ステップ 1 メインメニューから次を選択します。**[Workflows]**。次に、[REPリングの設定（ファブリック）（Configure REP ring (Fabric)）] カードを見つけて、[開始（Start）] をクリックします。

または、次の手順を使用することもできます。

1. ファブリック サイト トポロジ ビューに移動します。
2. REP リングを作成するファブリックエッジノードまたはFIAB ノードをクリックして、詳細を表示します。
3. [REPリング（REP Rings）] をクリックし、次に [REPリングを作成（Create REP Ring）] をクリックします。

ステップ 2 タスクの概要ウィンドウが表示されたら、[Let's Do It] をクリックして、ワークフローを開始します。

ステップ 3 **[ファブリックサイトを選択（Select a fabric site）]** ウィンドウで、エッジノードと拡張ノードの両方があるサイトを選択します。その後、[次へ（Next）] をクリックします。

ステップ 4 [Select a fabric edge node] ウィンドウで、ファブリックエッジノードを選択します。その後、[次へ（Next）] をクリックします。

ステップ 5 **[ファブリックエッジに接続する拡張ノードの選択（Select extended nodes connected to fabric edge）]** ウィンドウで、ファブリックエッジノードに接続する 2 つの拡張ノードを選択します。

a) 1 つ目の拡張ノードを選択し、[次へ（Next）] をクリックします。
b) 2 つ目の拡張ノードを選択し、[次へ（Next）] をクリックします。

ステップ 6 [REPリング検出選択の確認（Review your REP Ring discovery selections）] ウィンドウで、次のタスクを完了します。

a) 設定する REP リングの名前を入力します。
b) 選択したファブリックサイトとデバイスが表示されていることを確認します。
c) 必要に応じて、適切な [編集（Edit）] リンクをクリックして変更を加えます。

ステップ 7 [プロビジョニング（Provision）] をクリックして REP リングの設定を開始します。

[REP Ring Configuration Status] ウィンドウで、設定の進捗状況の詳細なステータスを確認できます。

ステップ 8 [REP Ring Summary] ウィンドウに、作成された REP リングの詳細情報が、検出されたデバイスとともに表示されます。

ステップ 9 REP リングの作成後、成功メッセージが表示されます。

REP リングの作成を確認するには、ファブリック サイト ウィンドウに移動し、ファブリックエッジノードをクリックします。

スライドインウィンドウの [REP Ring] タブで、そのエッジノードに存在するすべての REP リングのリストを確認できます。

リスト内の REP リング名をクリックすると、リングに存在するデバイス、リングに接続する各デバイスのポートなどの詳細情報が表示されます。

REP リングステータスの表示

REP リング内のデバイスのステータスを表示するには、次の手順を実行します。

手順

ステップ 1 メインメニューから次を選択します。**[Provision]** > **[Fabric Sites]**。

ステップ 2 [Fabric Sites] タブで、ファブリックサイトの数を示す数字をクリックします。

ステップ 3 [fabric site] をクリックします。

ステップ 4 [Fabric Infrastructure] タブで、ファブリックエッジノードまたはファブリックインアボックス（FIAB）クリックします。

スライドインペイン に、選択したファブリックエッジノードまたは FIAB の詳細が表示されます。

ステップ 5 [REP Rings] タブで、[View] をクリックして [REP Ring Topology Status] を表示します。

[REP Topology Status] セクションには、REP リング内のすべてのデバイスの現在の状態が表示されます。[Role] 列に表示される状態は、[Open]、[Fail]、または [Alt] です。

[Open] は、デバイスリンクがアップしていて、トラフィックを転送していることを示します。

[Fail] は、デバイスリンクがダウンしていることを示します。

[Alt] は、デバイスリンクがアップしているが、ポートがトラフィックを転送できないことを示します。

REP リングの削除

手順

ステップ 1 メインメニューから次を選択します。**[Provision]** > **[Fabric Sites]**。

ステップ 2 [ファブリックインフラストラクチャ（Fabric Infrastructure）] タブで、REP リングの終端となるファブリックエッジノードをクリックします。

スライドインウィンドウに、選択したファブリックエッジノードの詳細が表示されます。

ステップ 3 [REPリング（REP Rings）] タブで、目的の REP リングの **[アクション（Actions (…)）]** > **[削除（Delete）]** をクリックします。

これにより、REP リングが削除されます。

REP リングへのノードの追加

Before you begin

デバイスをCatalyst Centerに追加してください。デバイスを追加する方法については、デバイスの追加または編集 （710 ページ）を参照してください。

（注） この機能は次のプラットフォームをサポートしています。Cisco IE 2000 シリーズ スイッチ、Cisco Catalyst IE 3200 高耐久性シリーズ スイッチ、Cisco Catalyst IE 3300 高耐久性シリーズ スイッチ、Cisco Catalyst IE 3400 高耐久性シリーズ スイッチ、Cisco Catalyst IE 3400 Heavy Duty シリーズ スイッチ、Cisco IE 4000 シリーズ スイッチ、Cisco IE 4010 シリーズ スイッチ、Cisco IE 5000 シリーズ スイッチ、Cisco IE 9300 シリーズ スイッチ、Cisco Catalyst ESS3300 エンベデッド シリーズ スイッチ。

既存の REP リングに単一ノードを追加するには、次の手順を実行します。ノードは 1 つずつ追加する必要があります。

手順

ステップ 1 [プラグアンドプレイ（Plug and Play）] ワークフローを使用してデバイスの導入準備をして、要求します。

a) メインメニューから次を選択します。、[プロビジョニング（Provision）]>[プラグアンドプレイ（Plug and Play）] の順に選択します。

オンボーディングされたデバイスは、[プラグアンドプレイ（Plug and Play）] ウィンドウに表示されます。

b) [Actions] ドロップダウンリストから、[Claim] をクリックします。
c) [サイトの割り当て（Assign Site）] ウィンドウで、[割り当て（Assign）] をクリックしてノードを追加するサイトにデバイスを割り当て、[次へ（Next）] をクリックします。
d) 設定をデバイスに展開するには、[Assign] をクリックし、[Next] をクリックします。



（注） プラグアンドプレイ プロビジョニングにより、デバイスタイプ向けのデバイス オンボーディングテンプレートが自動的に展開されます。詳細については、プラグアンドプレイ プロビジョニングの概要 （695 ページ）を参照してください。

e) [Provision Templates] ウィンドウで、[Preview Configuration] をクリックして設定を確認し、[Claim] をクリックします。
f) [OK] をクリックし、[Yes] をクリックします。

デバイスを要求すると、成功のメッセージが表示されます。

g) [Refresh] をクリックします。デバイス オンボーディング プロセスが完了するまでに時間がかかる場合があります。

デフォルトでは、デバイステーブルは 30 秒ごとに更新されます。[Auto-Refresh] ドロップダウンリストをクリックして、更新間隔を選択します。

プロセスが完了すると、デバイスは [プロビジョニング済み（Provisioned）] タブに移動します。

ステップ 2 デバイスがインベントリで管理対象状態になっていることを確認します。

a) メインメニューから次を選択します。[Provision] > [Inventory] の順に選択します。
b) [更新（Refresh）] をクリックして、デバイスステータスを更新します。デバイスが管理対象状態になるまで待ちます。

ステップ 3 デバイスを REP リングに追加します。

a) メインメニューから次を選択します。[プロビジョニング（Provision）]>[ファブリックサイト（Fabric Sites）] の順に選択します。
b) [ファブリックサイト（Fabric Sites）] タブで、デバイスを含むファブリックサイトをクリックします。
c) [ファブリック インフラストラクチャ（Fabric Infrastructure）] タブで、REP リングのエッジノードをクリックします。

スライドインペインに、選択したノードの詳細が表示されます。

d) [REPリング（REP Rings）] タブで、目的の REP リングについて、アクション列で省略記号（…）をクリックし、[再検出（Rediscover）] を選択します。
デバイスが REP に正常に追加されると、ノード挿入ステータスが [Success] になります。
e) （任意） [REPリング（REP Rings）] タブで、REP リンクをクリックして、実行された手順を表示します。障害が発生した場合は、デバイスの挿入が失敗した手順を表示できます。

必要に応じて、失敗したノードの挿入を再検出します。

REP リングからのノードの削除

このタスクでは、REP リングから 1 つまたは複数の拡張ノードを削除する手順について説明します。



（注） 拡張ノードが削除された後、ダウンサイジングされた REP リングは既存のインターフェイスを使用して隣接デバイスへのリンクを作成する必要があります。

始める前に

ノードが属する REP リングが不完全でないことを確認してください。

手順

ステップ 1 拡張ノードデバイスをネットワークから手動で削除します。

または、REP リング内のデバイスがダウンすると、[Fabric Infrastructure] ウィンドウに通知が表示されます。

ステップ 2 メインメニューから次を選択します。**[Provision]** > **[Fabric Sites]**。

ステップ 3 [ファブリックインフラストラクチャ（Fabric Infrastructure）] タブで、REP リングの終端となるファブリックエッジノードをクリックします。

スライドインペインに、選択したファブリックエッジノードの詳細が表示されます。

ステップ 4 [REP Rings] タブで、目的の REP リングについて、**[Actions (…)]** > **[Rediscover]**を選択します。

REP リングから拡張ノードデバイスが削除され、REP リングの更新情報が表示されます。

サプリカントベースの拡張ノードの設定

Authenticated Extended Node（AEN）とも呼ばれるサプリカントベースの拡張ノードは、IEEE 802.1x（Dot1x）サプリカント設定を受け取り、完全な認証と承認の後にのみ SD-Access ネットワークにオンボードされる拡張ノードデバイスです。サプリカントベースの拡張ノードデバイスをオンボードするには、ファブリックエッジのオーセンティケータポートをクローズド認証テンプレートで設定する必要があります。

次のプラットフォームは、サプリカントベースの拡張ノードのオンボーディングをサポートしています。

ファブリックエッジまたは FIAB：

Cisco Catalyst 9000 シリーズ：Cisco IOS XE 17.7.1 以降で動作する C9300、C9400、C9500、および C9500H スイッチ。

サプリカントベースの拡張ノード：

Cisco Catalyst 9000 シリーズ：Cisco IOS XE 17.7.1 以降で動作する C9200、C9300、C9400、C9500、および C9500H スイッチ。

サプリカントベースの拡張ノードの設定手順

始める前に

- Cisco ISE を構成して、リリース 3.1 以降で動作することを確認します。「サプリカントベースの拡張ノードをオンボードするための Cisco Identity Services Engine の設定 （1293 ページ）」を参照してください。
- ファブリックエッジノードまたは FIAB デバイスをファブリックに追加し、それが Cisco IOS XE 17.7.1 以降で動作することを確認します。
- ファブリックエッジノードと Cisco ISE の間のパスに適切なパス MTU を設定します。値は 9100 をお勧めします。

（注） パス MTU は、LAN 自動化中、またはアンダーレイの構成時に、ファブリック内のすべてのデバイスに設定されます。

手順

ステップ 1 Catalyst Center で AAA サーバー設定を構成します。

a) **[System]** > **[Settings]** > **[External Services]** > **[Authentication and Policy Servers]** ウィンドウで、デバイス認証用の AAA サーバーとして Cisco ISE を定義します。

詳細な手順については、*Cisco Catalyst Center Administrator Guide*の「Configure Authentication and Policy Servers」を参照してください。

b) Cisco ISE サーバーをグローバルサイトに追加します。詳細については、Cisco ISE またはその他の AAA サーバーの追加 （375 ページ）を参照してください。

ステップ 2 （オプション）オンボーディング前にデバイスを認証するように Catalyst Center を構成します。

a) メインメニューから次を選択します。 **[System]** > **[Settings]** > **[Device Settings]** > **[PnP Device Authorization]** の順に選択します。

b) [Device Authorization] チェックボックスをオンにしてデバイスで許可を有効にします。

c) [Save] をクリックします。

ステップ 3 PKI 証明書を管理するように Catalyst Center アプライアンスを構成します。

a) メインメニューから次を選択します。**[System]** > **[Settings]** > **[Certificate]** > **[Certificate Authority]** の順に選択します。
b) [Certificate Authority] ウィンドウで、[Use Cisco DNA Center] をクリックします。
c) [CA Management] タブで [Download] をクリックして、CA 証明書をダウンロードします。
d) Cisco ISE の信頼できる証明書ストアに証明書を追加します。詳細については、『Cisco Identity Services Engine Administrator Guide』を参照してください。

外部証明書を使用する場合は、その証明書を Cisco ISE の信頼できる証明書ストアに追加します。

ステップ 4 拡張 IP アドレスプールとオプション 43 を使用して DHCP サーバーを設定します。拡張 IP アドレスプールが Catalyst Center から到達可能であることを確認します。

オプション 43 の詳細については、DHCP コントローラディスカバリ （702 ページ）を参照してください。

ステップ 5 ファブリックサイトで [Closed Authentication] を有効にし、ブリッジプロトコルデータユニット（BPDU）ガードを無効にします。

デフォルトでは、[Closed Authentication] を選択すると、すべてのダウンリンクアクセスポートに BPDU ガード設定がプッシュされます。拡張ノードのようなリモートスイッチが接続されている場合、BPDU ガードはポートをエラーディセーブルモードにプッシュします。BPDU ガードを無効にするには、クローズド認証の設定時に、[Enable BPDU Guard] チェックボックスをオフにします。

詳細については、「認証テンプレートの選択」 を参照してください。

ステップ 6 エニーキャストゲートウェイの作成 （1262 ページ）に記載されているように、拡張 IP アドレスプールを INFRA_VN に割り当てます。

[Create Anycast Gateways] ワークフローで、[Pool Type] として [Extended Node] を選択し、[Supplicant-Based Extended Node Onboarding] チェックボックスをオンにします。

Catalyst Center Cisco DNA Center は、サポートされているファブリックエッジデバイスで拡張 IP アドレスプールと VLAN を設定します。これにより、拡張ノードのオンボーディングが有効になります。

（注） 拡張 IP アドレスプールは、ファブリックエッジデバイスが Cisco IOS XE 17.7.1 以降で動作している場合にのみ正常に割り当てられます。Catalyst Center の以前のリリースからアップグレードした場合は、拡張 IP アドレスプールを構成する前に、サプリカントベースの拡張ノードの移行を完了する必要があります。

ステップ 7 ファブリックエッジデバイスまたは FIAB に拡張ノードデバイスを接続します。

オンボーディングの前にデバイスを認証することを選択した場合（ステップ 2）、電源をオンにした後、拡張ノードデバイスは [Pending Authorization] 状態になります。**[Provision]** > **[Plug and Play]** ウィンドウでデバイスのステータスを確認できます。

ステップ 8 （オプション）デバイスを認証します。

この手順は、デバイスが [Pending Authorization] 状態の場合にのみ実行してください。

a) メインメニューから次を選択します。**[Provision]** > **[Plug and Play]**。

b) [Plug and Play] ウィンドウで、サプリカントベースの拡張ノードデバイスを選択し、**[Actions]** > **[Authorize]** の順に選択します。

認証プロセスは、Cisco ISE で証明書ベースの EAP-TLS 認証を完了するために、サプリカントベースの拡張ノードデバイスをプロビジョニングします。認証後、Cisco ISE はサプリカントベースの拡張ノードデバイスに完全なアクセスを許可します。サプリカントベースの拡張ノードデバイスは、SD-Access ファブリックに完全にオンボードされます。

サプリカントベースの拡張ノードデバイスがファブリックにオンボードされた後は、ファブリック エッジサプリカント ポートへのアクセスは認証ステータスのみに基づきます。デバイスまたはポートがダウンすると、認証セッションがクリアされ、ポートでトラフィックが許可されなくなります。ポートが再び起動すると、IEEE 802.1x（Dot1x）認証プロセスを経て、SD-Access ネットワークへのアクセスが回復します。

障害のあるポートの交換

オーセンティケータ（ファブリックエッジまたは FIAB）ポートとサプリカントポート間のリンクがダウンした場合、障害のあるポートを交換し、[Port Assignment] メニューから新しいポートを設定できます。

手順

ステップ 1 サプリカントポートを交換するには、次の手順に従います。

a) 新しいサプリカントポートの設定をクリアします。

b) 既存の設定を現在のサプリカントポートから新しいサプリカントポートにコピーして、802.1X 認証を可能にします。

ステップ 2 オーセンティケータポートを交換するには、次の手順に従います。

a) サプリカントポートをオーセンティケータの新しいインターフェイスに割り当てます。ポートの割り当てについては、「ファブリックサイト内のポートの設定 （1252 ページ）」を参照してください。[Connected Device Type] として [Supplicant-Based Extended Node] を選択します。

b) オーセンティケータの古いインターフェイスの既存のポート割り当てをクリアします。

ステップ 3 オーセンティケータとサプリカントの古いポート間の物理接続を切断します。オーセンティケータとサプリカントの新しいポート間をケーブルで接続します。このリンクを確立します。

ステップ 4 オーセンティケータとサプリカントの新しいポート間のリンクが確立されたら、次の手順を実行します。

a) オーセンティケータとサプリカントの両方に対して **[Inventory]** > **[Resync Device]** を実行して、Catalyst Center のデバイス情報を再同期します。デバイス情報の再同期 （217 ページ）を参照してください。

b) 新しいサプリカントポートをオーセンティケータに割り当てます。ポートの割り当てについては、「ファブリックサイト内のポートの設定 （1252ページ）」を参照してください。[Connected Device Type] として [Authenticator Switch] を選択します。

c) 古いサプリカントポートのポート割り当てをクリアします。

サプリカントベースの拡張ノードをオンボードするためのCiscddentity Services Engine の設定

このタスクでは、Cisco Identity Services Engine（ISE）でサプリカントベースの拡張ノード（SBEN）デバイスをプロファイリングする方法について説明します。以下にリストされている手順は、Cisco ISE 設定手順の一部です。詳細については、『Cisco Identity Services Engine Administrator Guide』を参照してください。

始める前に

Catalyst Center から CA 証明書をダウンロードします。

手順

ステップ 1 CA 証明書を Cisco ISE にインポートします。

Cisco ISE ホームページから、**[Administration]** > **[System]** > **[Certificates]** > **[System Certificate]** > **[Import]** を選択します。[インポート（Import）] ウィンドウで、[クライアント認証とsyslogの信頼（Trust for client authentication and Syslog）] チェックボックスがオンになっていることを確認します。詳細については、『Cisco Identity Services Engine Administrator Guide』の「Import the Root Certificates to the Trusted Certificate Store」セクションを参照してください。

ステップ 2 RADIUS 属性を使用して、次の認証プロファイルを設定します。

Cisco ISE メインメニューから、**[Policy]** > **[Policy Elements]** > **[Results]** > **[Authorization]** > **[Authorization Profiles]** を選択します。

次のプロファイルを設定します。

```
SBEN-DHCP:
Access Type = ACCESS_ACCEPT
Filter-ID = SBEN_DHCP_ACL.in

SBEN_LIMITED_ACCESS_AUTHZ:
Access Type = ACCESS_ACCEPT
Filter-ID = SBEN_MAB_ACL.in
cisco-av-pair = interface-template-name=SWITCH_SBEN_MAB_TEMPLATE

SBEN_FULL_ACCESS_AUTHZ :
Access Type = ACCESS_ACCEPT
cisco-av-pair = interface-template-name=SWITCH_SBEN_FULL_ACCESS_TEMPLATE
```

Macsec 暗号化オンボーディング

```
SBEN_FULL_ACCESS :
Access Type = ACCESS_ACCEPT
cisco-av-pair = interface-template-name=SWITCH_SBEN_FULL_ACCESS_TEMPLATE
```

ステップ 3 [共通タスク（Common Tasks）] で、Macsec 暗号化 SBEN オンボーディング用に次の設定を構成します。

a) [再認証（Reauthentication）] オプションを有効にします。

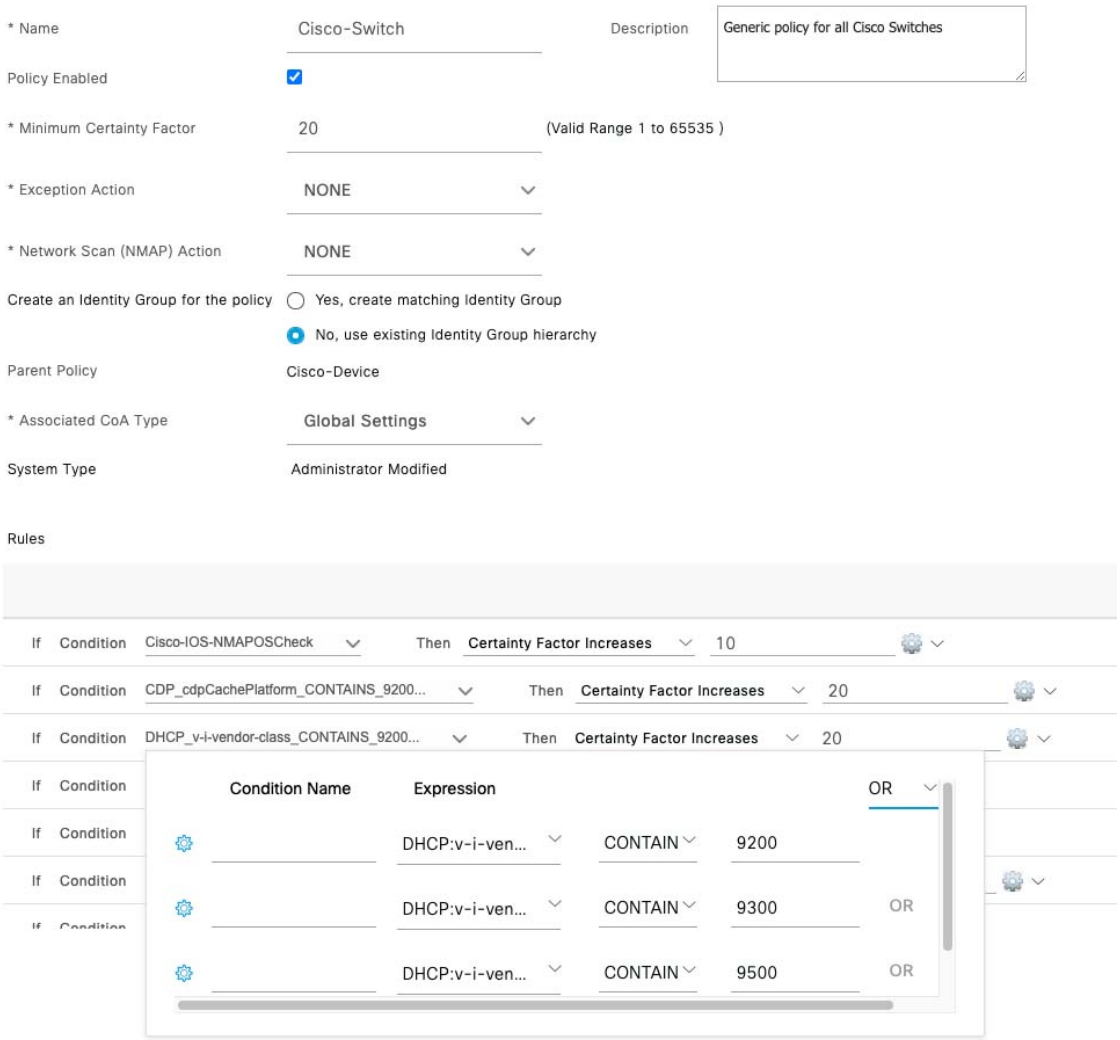
b) [Macsecポリシー（Macsec policy）] オプションを有効にします。

- SBEN のオンボーディング中に [推奨される保護（should-secure）] オプションを選択します。
- SBEN のオンボーディング後に [必須の保護（must-secure）] オプションを選択します。

ステップ 4 [Profiling Policies] ウィンドウでデバイス プロファイリング ポリシーを定義します。

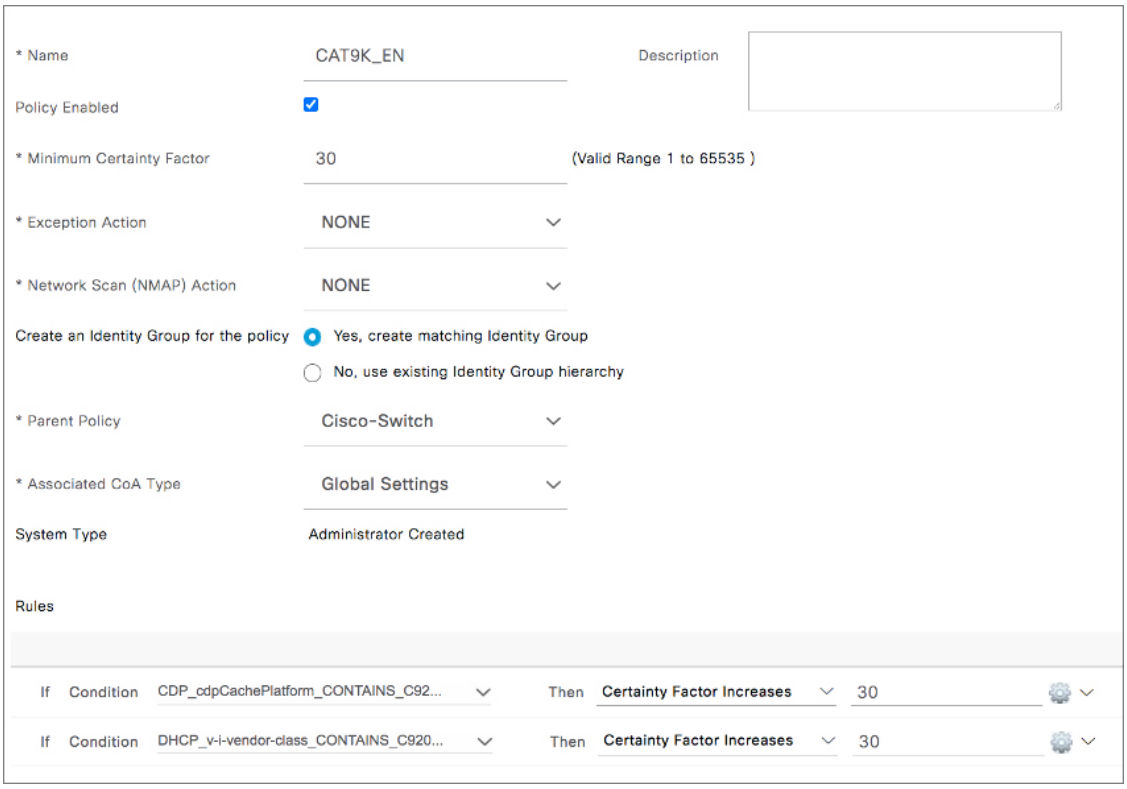
a) Cisco ISE のメインメニューから、**[Policy]** > **[Profiling]** > **[Profiling Policies]**を選択します。

b) [Profiling Policies] ウィンドウで、[Cisco-Device]：[Cisco-Switch] ポリシーの新しい [DHCP-v-i-vendor-class] 条件を追加します。



c) サプリカントデバイスの新しい子ポリシーを [Cisco-Switch] の下に作成し、[CdpCachePlatform] および [V-I-Vendor-Class] 条件を適用します。

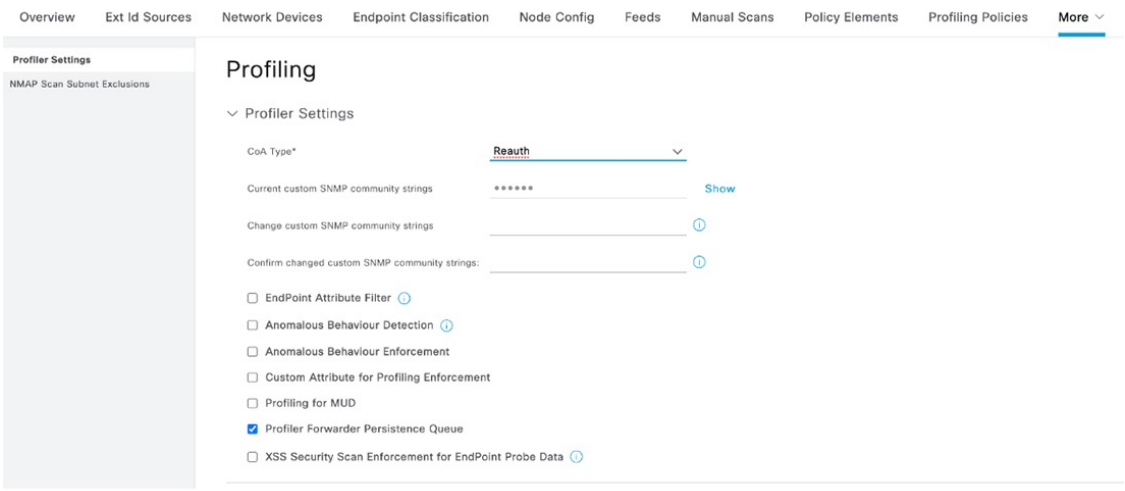
子ポリシーの [Minimum Certainty Factor] の値が親ポリシーの値よりも高いことを確認してください。



ステップ 5 グローバル認可変更（CoA）タイプを [Reauth] に設定します。

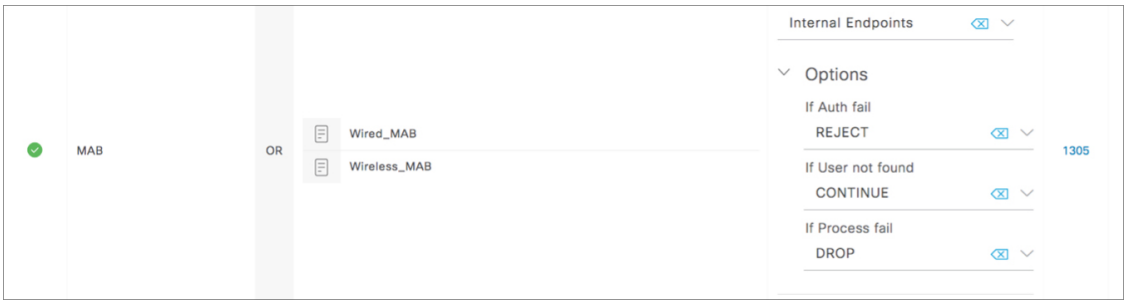
[CoA Type] を設定するには、Cisco ISE ホームページから、**[Work Centers]** > **[Profiler]** > **[Settings]**の順に移動します。

[CoA Type] ドロップダウンリストから [Reauth] を選択します。

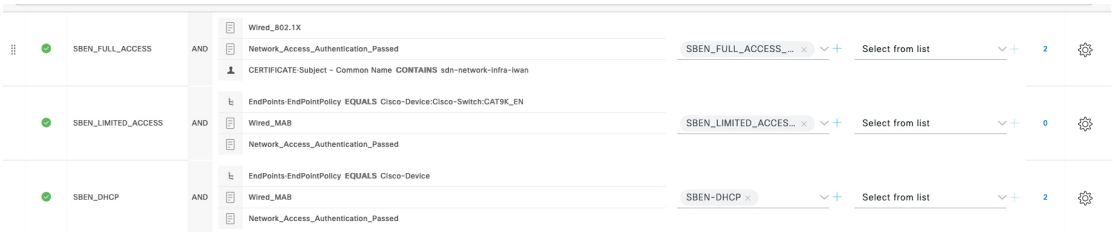


ステップ 6 [Authorization Policy] ウィンドウで認証ポリシーを定義します。

a) Cisco ISE ホームページから、**[Policy]** > **[Policy Sets]** > **[Default]** > **[Authorization Policy]**を選択します。
b) デフォルト MAB ポリシーの [If User not found] フィールドが [CONTINUE] オプションに設定されていることを確認します。



c) [Authorization Policy] ウィンドウで、サプリカントデバイスの認証ポリシーを構成し、ポリシーを以前に作成した認証プロファイル（SBEN-DHCP、SBEN_LIMITED_ACCESS_AUTHZ、SBEN_FULL_ACCESS_AUTHZ）に関連付けます。



ポートチャネルの設定

単一のエンティティとして機能するようにバンドルされたポートのグループは、ポートチャネルと呼ばれます。ファブリックエッジと、拡張ノードやサーバーなどリモート接続されたデバイスとの間のポートチャネルでは、接続の復元力と帯域幅が増加します。

ポートチャネルの作成

始める前に

認証はクローズド認証（[Closed Authentication]）である必要があります。

（注） 他の認証モードでは、次の手順は自動化されています。

手順

ステップ 1 メインメニューから次を選択します。**[Provision]** > **[Fabric Sites]**。

ステップ 2 [Fabric Sites] タブ の [SUMMARY] で、ファブリックサイトの数を示す数字をクリックします。

ステップ 3 [Fabric Sites] ウィンドウで、ポートチャネルを設定するファブリックサイトをクリックします。

ステップ 4 [Port Assignment] タブで、[More Actions] にカーソルを合わせ、[Create Port Channel] をクリックします。

ステップ 5 [Select your fabric devices] ウィンドウで、ポートチャネルを作成する必要があるファブリックデバイスを選択します。

ステップ 6 ポートチャネルの数を指定し、各ポートチャネルを設定するには、**[ポートチャネルの数の決定（Determine number of port channels）]** ウィンドウで次のタスクを実行します。

a) [Connected Device Type] ドロップダウンリストから、接続済みのデバイスのタイプを選択します。

- ファブリックエッジノードと拡張ノードの間または 2 つの拡張ノードの間にポートチャネルを作成する場合は、[Extended Node] を選択します。
- 片側にファブリックエッジノードまたは拡張ノードがあり、反対側にサードパーティデバイスまたはサーバーポートがあるポートチャネルを作成するには、[Trunk] を選択します。

  トランクポートの [ネイティブVLAN（Native VLAN）] と [許可VLAN（Allowed VLANs）] の値を設定します。

  - [ネイティブVLAN（Native VLAN）] フィールドに、ネイティブ VLAN の値を入力します。

    有効な範囲は 1 ～ 4094 です。デフォルト値は 1 です。

  - [許可VLAN（Allowed VLANs）] フィールドでは、すべての VLAN、1 ～ 4094 の特定の VLAN ID を許可することを選択するか、または VLAN の範囲を指定できます。たとえば、100、200、または 300-400 と入力できます。デフォルト値は [すべて（All）] です。

（注） テンプレートでデフォルト値をオーバーライドする場合は、テンプレートの各ポートに指定される値と一致するようにトランク設定を更新します。

b) 新しいポートチャネルの説明を [Description] に入力します。

c) プロトコルを選択します。

- Cisco IOS XE リリース 16.12.1s および以前のリリースを実行する拡張ノードの場合は、プロトコルとして [On] を選択します。
- Cisco IOS XE リリース 17.1.1s および以降のリリースを実行する拡張ノードの場合は、プロトコルとして [Port Aggregation Protocol (PAgP)] を選択します。
- [Link Aggregation Control Protocol (LACP)] を拡張ノードのプロトコルとして選択しないでください。LACP モードでは、トランクポートまたはサーバーポートのみを接続できます。

ステップ 7 使用可能なインターフェイスのリストから、ポートチャネルとしてバンドルするインターフェイスを選択します。



（注） LACPモードで接続されたポートチャネルには、16を超えるメンバーを含めることはできません。

PAgP モードで接続されたポートチャネルには 8 つを超えるメンバーを含めることはできません。

ステップ 8 [Summary] ウィンドウで、作成されたポートチャネルを確認します。

ステップ 9 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 10 [Tasks] ウィンドウで、タスクの展開を監視します。

ポートチャネルの更新

始める前に

ポートチャネルを更新する前に、少なくとも 1 つのメンバーインターフェイスが存在することを確認します。

手順

ステップ 1 メインメニューから次を選択します。**[Provision]** > **[Fabric Sites]**。

ステップ 2 [Fabric Sites] タブ の [SUMMARY] で、ファブリックサイトの数を示す数字をクリックします。

ステップ 3 [Fabric Sites] ウィンドウで、ポートチャネルを更新するファブリックサイトをクリックします。

ステップ 4 [ポートの割り当て（Port Assignment）] タブで、更新するポートチャネルをクリックします。

ステップ 5 [More Actions] にカーソルを合わせ、[Edit Port Channel] をクリックします。

ステップ 6 画面上のガイドラインに従って、ポートチャネル設定を更新します。

ポートチャネルにインターフェイスを追加したり、ポートチャネルの既存のインターフェイスを削除したりできます。

ステップ 7 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

ステップ 8 [Tasks] ウィンドウで、タスクの展開を監視します。

ポートチャネルの削除

手順

ステップ 1 メインメニューから次を選択します。**[Provision]** > **[Fabric Sites]**。

ステップ 2 [SUMMARY] で、ファブリックサイトの数を示す数字をクリックします。

ステップ 3 [fabric site] をクリックします。

ステップ 4 [ポートの割り当て（Port Assignment）] タブで、削除するポートチャネルをクリックします。

ステップ 5 [その他のアクション（More Actions）] にカーソルを合わせ、[ポートチャネルの削除（Delete Port Channel）] をクリックします。

ステップ 6 プロンプトで [Yes] をクリックします。

ステップ 7 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

ステップ 8 [Tasks] ウィンドウで、タスクの展開を監視します。

マルチキャスト

マルチキャスト トラフィックは、次のような異なる方法で転送されます。

- ランデブー ポイントを使用した共有ツリー経由。この場合、PIM SM が使用されます。

- 最短パス ツリー（SPT）経由。PIM Source Specific Multicast（SSM）では SPT だけが使用されます。PIM SM は、受信側が接続しているエッジ ルータで送信元が認識されると SPT に切り替わります。

『IP マルチキャスト ルーティング テクノロジーの概要（IP Multicast Technology Overview）』を参照してください。

マルチキャストの設定

Catalyst Center には、仮想ネットワークでグループ通信またはマルチキャストトラフィックを有効にするためのワークフローが用意されています。このワークフローでは、ネットワークでのマルチキャスト実装（ネイティブマルチキャストまたはヘッドエンド レプリケーション）を選択することもできます。

（注） ボーダーがマルチサイト リモート ボーダーとして機能する仮想ネットワークでマルチキャストを有効にすることができます。このような仮想ネットワークでマルチキャストを設定すると、継承された仮想ネットワークにすでにセグメントが含まれている場合は、継承された仮想ネットワークのデバイスにもマルチキャストが設定されます。継承された仮想ネットワークにセグメントがない場合、マルチキャストは、最初のセグメントが作成された後にのみ展開されます。仮想ネットワークとその継承ネットワークが同じタイプのマルチキャスト実装を展開していることを確認してください。継承された仮想ネットワークのエッジノードデバイスをランデブーポイント（RP）として設定することはできません。

手順

ステップ 1 メインメニューから次を選択します。[Workflows] > [Configure Multicast] の順に選択します。

ステップ 2 タスクの概要ウィンドウが表示されたら、[Let's Do It] をクリックして、ワークフローに直接移動します。

ステップ 3 [Fabric Site] ウィンドウのサイト階層ペインでサイトを選択します。

ステップ 4 [Replication Mode] ウィンドウで、ネットワークのマルチキャスト実装方式を次の中から選択します。

- **Native Multicast**
- **Head-end replication**

ステップ 5 [Virtual Networks] ウィンドウで、マルチキャストを設定する仮想ネットワークを選択します。

（注） 継承された仮想ネットワークを選択してマルチキャストを設定することはできません。

ステップ 6 [Multicast pool mapping] ウィンドウで、[IP Pools] ドロップダウンリストから IP アドレスプールを選択します。選択した IP アドレスプールは、選択した仮想ネットワークに関連付けられます。

ステップ 7 [Multicast Mode] ウィンドウで、実装するマルチキャストのタイプを選択します。

- **SSM**（送信元特定マルチキャスト）
- **ASM**（任意の固有のマルチキャスト）
- [SSM] と [ASM] を選択して両方を一緒に設定します。

ステップ 8 次の手順を実行します。

a) [SSM] を選択した場合は、仮想ネットワークごとに IP グループの範囲を追加して、SSM リストを設定します。仮想ネットワークに複数の IP グループ範囲を追加できます。

1. デフォルトでは、IPv4 アドレスの 232.0.0.0/8 の範囲が選択されています。必要に応じて IPv4 アドレスの範囲を変更できます。

   225.0.0.0 ～ 239.255.255.255 の IP グループ範囲を選択します。

2. IPv6 アドレスの場合、FF3x::/32 は SSM 用に予約されています。

b) [ASM] を選択したら、[Multicast Group to Rendezvous Point Mapping] ウィンドウで各仮想ネットワークのランデブーポイントを設定します。

1. ランデブーポイントのタイプ（[External] または [Fabric]）を選択します。
2. それぞれのタブでランデブーポイント（[IPv4 RP] と [IPv6 RP]）を選択します。
3. 任意の数の外部ランデブーポイントを定義できます。
4. 必要に応じて、グループからランデブーポイントへのマッピングを定義できます。ランデブーポイントに関連付けられている 1 つか複数の IPv4/IPv6 マルチキャストグループが存在する場合があります。
5. マッピングなし、またはありのランデブーポイントを設定できます。両方を一緒に設定することはできません。
6. IPv6 および IPv4 FF00:/8 と 225.0.0.0/8 ～ 239.0.0.0/8 それぞれのマルチキャストグループの範囲が許可されます。

ステップ 9 [Summary] ウィンドウで、マルチキャスト設定を確認します。設定を変更するには、[Edit] をクリックします。

ステップ 10 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 11 [Tasks] ウィンドウで、タスクの展開を監視します。

ファブリックサイトの BGP AS 番号の編集

ファブリックサイトのBGP自律システム（AS）番号を編集するには、次の手順を実行します。

BGP AS 番号を変更すると、BGP ピアリングが一時的に中断され、ボーダーノードおよびコントロールプレーンノードのカスタム BGP 設定が削除されるため、テンプレートの更新とカスタム設定の再設定が必要です。BGP AS 番号を変更すると、すべての仮想ネットワークで外部接続が一時的に停止し、管理アクセスが中断される可能性があります。

手順

ステップ 1 メインメニューから次を選択します。**[Provision]** > **[Fabric Sites]**。

ステップ 2 [SUMMARY] で、ファブリックサイトの数を示す数字をクリックします。

ステップ 3 **[ファブリックサイト（Fabric Sites）]** ウィンドウで、BGP AS 番号を編集するファブリックサイトを選択します。

ステップ 4 対応するファブリックサイトウィンドウで、[サイトアクション（Site Actions）] の上にカーソルを合わせ、[BGP AS番号の編集（Edit BGP AS Number）] を選択します。

ステップ 5 [BGP AS番号の編集（Edit BGP AS Number）] ダイアログボックスで情報を確認し、[編集（Edit）] をクリックします。

ステップ 6 [新しいローカルBGP AS番号（New Local BGP AS Number）] フィールドに、新しい BGP AS 番号を入力します。

有効範囲は 1 ～ 4294967295 です。

ステップ 7 [Deploy] をクリックします。



重要 展開を成功させるには、デバイスが到達可能であることを確認します。

ステップ 8 展開のためのタスクのスケジュールを設定します。

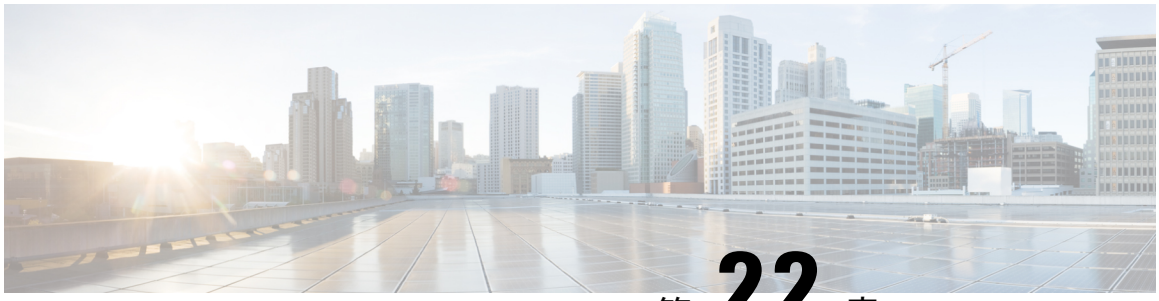
[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

ステップ 9 [Tasks] ウィンドウで、タスクの展開を監視します。

次のタスク

CLIテンプレートを使用してBGPのカスタマイズを設定した場合は、対応するCLIテンプレートの AS 番号を更新してから再適用します。



第 22 章

キャンパスネットワークのプロビジョニング

- キャンパスネットワーク （1305 ページ）
- ネットワークの管理 （1306 ページ）
- 設定プロファイルの管理 （1309 ページ）
- スイッチング デバイス グループの管理 （1312 ページ）
- デバイスの管理 （1317 ページ）
- デバイス設定の比較 （1323 ページ）

キャンパスネットワーク

キャンパスネットワーク機能を使用すると、Cisco Catalyst スイッチ（Cisco Catalyst 9000 シリーズ スイッチおよび Cisco Catalyst 産業用イーサネット（IE）スイッチ）と Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のキャンパス環境全体で設定を管理し、標準化できます。この機能は、設定の一貫性を維持し、複数のサイトに展開を拡張するのに役立ちます。

キャンパスネットワークでは、ネットワークは管理対象デバイスの論理的なコンテナとして機能します。設定の一貫性をサポートするために、Catalyst Center は設定プロファイルを使用します。これらのプロファイルを使用すると、他のデバイスに一貫性のある標準化された設定を展開できます。デバイス設定を設定プロファイルと比較することで逸脱を特定できます。

（注） この機能はベータ版です。

スイッチ

Catalyst Center は、同様の設定を持つデバイスのコレクションであるスイッチング デバイス グループの作成をサポートしています。ネットワークには、複数のデバイスグループと個別に管理されるデバイスを含めることができるため、サイト全体でのスイッチの展開と管理に柔軟性がもたらされます。スイッチの新しい設定プロファイルを作成したり、既存のデバイスからデバイス設定を学習したりできます。

ワイヤレスコントローラについて

Catalyst Center では、既存のワイヤレスコントローラから設定を学習し、それらを設定プロファイルとして保存できます。

（注） この機能はベータ版であり、機能を有効にする必要があります。機能を有効にするには、Cisco Technical Assistance Center（TAC）にお問い合わせください。この機能が有効になっていない場合、ワイヤレスコントローラ関連の設定のオプションは使用できないか、グレー表示されます。

ワイヤレスコントローラ のキャンパスネットワーク設定の詳細については、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのキャンパスネットワーク設定のユースケース （1716 ページ）」を参照してください。

ネットワークの管理

Catalyst Center でネットワークを表示して管理するには、次の手順を実行します。

手順

ステップ 1 メインメニューから次を選択します。**[プロビジョニング（Provision）]>[キャンパスネットワーク（Campus Network）] > [ネットワークおよび設定プロファイル（Networks & Configuration Profiles）]** の順に選択します。

既存のネットワークがない場合は、[Create Network] オプションを使用して新しいネットワークを作成します。詳細については、「ネットワークの作成 （1308 ページ）」を参照してください。

既存のネットワークの場合、ネットワークのリストには、デバイスグループとデバイスの数、ネットワークに関連付けられているサイトなどの詳細が表示されます。

目的	手順
ネットワークの編集または削除	必要に応じて、省略記号アイコンにカーソルを合わせ、[ネットワーク名の編集（Edit network name）] または [ネットワークの削除（Delete network）] を選択します。 デバイスグループが関連付けられているネットワークは削除できません。
ネットワークの追加	[ネットワークの作成（Create Network）] をクリックします。ネットワークの作成 （1308 ページ）を参照してください。

目的	手順
ネットワークの詳細の表示	ネットワークをクリックします。 次のステップを参照してください。

ステップ 2 ネットワークをクリックしてネットワークの詳細を表示します。

このウィンドウには、次の詳細情報が表示されます。

名前	説明
デバイスグループ	このタブには、ネットワークに関連付けられているすべてのデバイスグループが、デバイスグループのタイプやデバイスグループ内のデバイス数などの詳細とともに表示されます。 [**Create switching device group**] をクリックして、新しいスイッチングデバイス グループを追加します。作成ウィンドウで、デバイスグループ名を入力してデバイスを追加（オプション）し、作成オプションをクリックします。 省略記号アイコンにカーソルを合わせ [Edit] または [Delete] を選択します。デバイスが割り当てられているデバイス グループを削除することはできません。 デバイスグループの詳細を表示するには、デバイスグループ名をクリックします。詳細については、スイッチングデバイス グループの管理（1312ページ）を参照してください。
[デバイス （Devices）]	このタブには、ネットワークに関連付けられているネットワークデバイスのリストが、IP アドレス、管理性ステータス、属するデバイスグループなどの詳細とともに表示されます。デバイスの詳細を表示するには、デバイス名をクリックします。 デバイスの管理（1317ページ）を参照してください。

ネットワークの作成

手順

ステップ 1 メインメニューから次を選択します。**[プロビジョニング（Provision）]**>**[キャンパスネットワーク（Campus Network）]** > **[ネットワークおよび設定プロファイル（Networks & Configuration Profiles）]** の順に選択します。

次の表は、既存のネットワークの有無に基づいて発生する内容を示します。

問題	結果
既存のネットワークがない	**[ネットワークの作成（Create Network）]** オプションが表示されます。
既存のネットワークがある	使用可能なネットワークのリストと、新しいネットワークを追加するための **[ネットワークの作成（Create Network）]** オプションが表示されます。

ステップ 2 [ネットワークの作成（Create Network）] をクリックします。

ステップ 3 **[ネットワークの作成（Create Network）]** ウィンドウで、次のフィールドを設定します。

ネットワークの詳細

- [ネットワーク名（Network name）]：ネットワークの名前を入力します。
- [サイト（Site）]：ネットワークのサイトを選択します。サイトおよびその下のレベルに関連付けられているすべてのデバイスがネットワークに追加されます。

デバイスグループを作成したり、個々のデバイスをネットワークに追加したりできます。利用可能なオプションから選択します。

オプション	Action
スイッチデバイスグループの作成	[デバイスグループ名（Device group name）] を入力します。必要に応じて、デバイスをデバイスグループに追加します。
WLCの追加	ネットワークに追加するワイヤレスコントローラを選択します。 （注） この機能はベータ版であり、機能を有効にする必要があります。この機能が有効になっていない場合、このオプションはグレー表示されます。
[後で実行（Do this later）]	デバイスグループの作成をスキップする場合に選択します。

ステップ 4 [ネットワークの作成（Create Network）] をクリックします。

設定プロファイルの管理

設定プロファイルを作成するか、既存のデバイスから学習して、ネットワーク全体のデバイスグループとデバイスにこれらのプロファイルを割り当てることができます。設定プロファイルを追加、編集、削除するには、次の手順を実行します。

手順

ステップ 1 メインメニューから次を選択します。**[プロビジョニング（Provision）]**>**[キャンパスネットワーク（Campus Network）]** > **[ネットワークおよび設定プロファイル（Networks & Configuration Profiles）]**。

ステップ 2 次の表を使用して、設定プロファイルを設定します。

（注） ワイヤレスコントローラの場合、この機能はベータ版であり、機能の有効化が必要です。この機能が有効になっていない場合、これらのオプションは使用できません。

表 *52*: プロファイルの切り替え

目的	手順
設定プロファイル の作成	[新規作成（Create new）] をクリックします。詳細については、デバイスグループを切り替えるための設定プロファイルの作成（1310 ページ） を参照してください。
既存デバイスからのプロファイルの学習	[スイッチから学習（Learn from a switch）] をクリックします。詳細については、スイッチから設定プロファイルを学習 （1315 ページ） を参照してください。
プロファイルの編集	プロファイル名をクリックし、必要な更新を行います。
プロファイルの削除	[アクション（Actions）] 列で [削除（Delete）] を選択します。
プロファイルの複製	[アクション（Actions）] 列で [重複（Duplicate）] を選択し、設定プロファイルの名前を入力します。

表 *53* : ワイヤレスプロファイル

目的	手順
ワイヤレスコントローラからのプロファイルの学習	[WLCから学習（Learn from a WLC）] をクリックします。詳細については、ワイヤレスコントローラ から 設定プロファイルを学習する （1311 ページ） を参照してください。
プロファイルの編集	プロファイル名をクリックし、必要な更新を行います。
プロファイルの削除	1. [アクション（Actions）] で、対応する省略記号アイコンをクリックし、[削除（Delete）] を選択します。 2. ダイアログボックスで、[Delete] をクリックします。
プロファイルの複製	1. [アクション（Actions）] で、対応する省略記号アイコンをクリックし、[複製（Duplicate）] を選択します。 2. [設定プロファイルの複製（Duplicate configuration profile）] ダイアログボックスに、設定プロファイルの一意の名前を入力します。 3. [Duplicate] をクリックします。

デバイスグループを切り替えるための設定プロファイルの作成

デバイスグループを切り替えるための設定プロファイルを作成するには、次の手順を実行します。

手順

ステップ 1 メインメニューから次を選択します。**[プロビジョニング（Provision）]>[キャンパスネットワーク（Campus Network）] > [ネットワークおよび設定プロファイル（Networks & Configuration Profiles）]**。

ステップ 2 [設定プロファイル（Configuration profiles）] をクリックします。

ステップ 3 [切り替え（Switching）] タブの左ペインでプロファイルのタイプを選択し、[新規作成（Create New）] をクリックします。

ステップ 4 [設定プロファイル名（Configuration profile name）] を入力し、必要に応じて [設定プロファイルの説明（Configuration profile description）] を入力します。

ステップ 5 設定のタイプに基づいてプロファイル属性を設定します。

設定の情報については、「Cisco Catalyst スイッチのデバイスごとの設定を管理する （123 ページ）」を参照してください。

ステップ 6 必要なプロファイル設定が完了したら、**[設定プロファイルの作成（Create configuration profile）]** をクリックします。

ワイヤレスコントローラ から 設定プロファイル を学習する

設定プロファイル は設定を標準化します。また、複数の ワイヤレスコントローラ にわたるプロビジョニングも可能です。

Catalyst Center は、ワイヤレスコントローラから学習したデバイス設定を 設定プロファイル として保存します。ネットワーク全体で 設定プロファイル を ワイヤレスコントローラ に割り当てることができます。設定プロファイルは、デバイスごとの設定を使用してプロビジョニングされた、またはインテントベースのネットワーク設定を使用してプロビジョニングされた、またはプロビジョニングされずにインベントリに登録されている、ワイヤレスコントローラから学習できます。

ワイヤレスコントローラからデバイス設定を学習して設定プロファイルとして保存するには、次の手順を実行します。

Before you begin

- この機能はベータ版であり、機能を有効にする必要があります。この機能が有効になっていない場合、このオプションはグレー表示されます。
- Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ で Cisco IOS XE リリース 17.12 以降が実行されていることを確認します。
- 設定プロファイル はバージョン固有です。特定の Cisco IOS XE リリースを実行している ワイヤレスコントローラ から学習した 設定プロファイル は、同じバージョンを実行している ワイヤレスコントローラ にのみ適用できます。

手順

ステップ 1 メインメニューから次を選択します。**[プロビジョニング（Provision）]**>**[キャンパスネットワーク（Campus Network）]** > **[ネットワークおよび設定プロファイル（Networks & Configuration Profiles）]**。

ステップ 2 **[設定プロファイル（Configuration profiles）]** > **[ワイヤレス（Wireless）]** の順にクリックします。

ステップ 3 [WLCから学習（Learn from a WLC）] をクリックし、ワイヤレスコントローラ から 設定プロファイル を学習します。

ステップ 4 [デバイスの選択（Select device）] ウィンドウで、設定を学習する ワイヤレスコントローラ を選択します。

学習デバイス設定でサポートされていない ワイヤレスコントローラ の詳細を表示するには、[お探しのデバイスが見つからない場合（Can't find a device you're looking for?）] をクリックします。

ステップ 5 [**Configurations to learn**] ウィンドウに、特定された設定が表示されます。必要に応じて、設定プロファイル の名前を更新します。

ステップ 6 [確認（レビュー）] ウィンドウで、設定プロファイル に保存される設定を確認します。

（注） このウィンドウで設定を編集することはできません。

ステップ 7 [設定プロファイルの作成（Create configuration profile）] をクリックして、設定を保存します。

スイッチング デバイス グループの管理

スイッチング デバイス グループを表示および管理するには、次の手順を実行します。

始める前に

デバイスグループを含むネットワークが作成されていることを確認します。詳細については、ネットワークの作成 （1308 ページ）を参照してください。

手順

ステップ 1 メインメニューから次を選択します。**[プロビジョニング（Provision）]>[キャンパスネットワーク（Campus Network）] > [ネットワークおよび設定プロファイル（Networks & Configuration Profiles）]** の順に選択します。

ステップ 2 [ネットワーク（Networks）] ウィンドウでネットワーク名をクリックします。

ステップ 3 次のオプションを使用してデバイスグループを管理します。

実行する操作	結果
デバイスグループの作成	[**Create device group**] をクリックします。 **1.** 作成ウィンドウで、デバイスグループ名を入力します。 **2.** デバイスを選択します。 **3.** [**Create device group**] をクリックします。
デバイスグループの編集または削除	省略記号アイコンをクリックし、必要に応じて [**Edit device group name**] か [**Delete**] を選択します。
デバイスグループの詳細の表示	デバイスグループ名をクリックし、次の手順に進みます。

ステップ 4 デバイスグループ名をクリックします。

ウィンドウには、デバイスグループに関連付けられている [**Configurations**] と [**Devices**] が表示されます。

[設定（Configurations）] タブには、デバイスグループに関連付けられている設定プロファイルが表示されます。

次の表で説明されているオプションを使用して設定プロファイルを管理します。

表 *54* : コンフィギュレーション

オプション	説明
設定プロファイルの作成	設定プロファイルを作成するには、このオプションを使用します。
設定プロファイルの割り当て	デバイスグループに割り当てられている既存のプロファイルがない場合は、このオプションを使用します。 **1.** 必要なプロファイルタイプ（レイヤ 2、レイヤ 3、セキュリティ、ネットワーク設定）のドロップダウンリストからプロファイル名を選択します。 **2.** ポートプロファイルを選択します。 　**1.** デバイスモデルまたは個々のデバイスを選択します。 　**2.** 選択したデバイスで 1 つ以上のポートを選択します。 **3.** 設定プロファイルをプロビジョニングします。
設定プロファイルの割り当ての編集	[設定プロファイル（Configuration profile）] エリアで、[編集（Edit）] オプションを使用してプロファイルを変更およびプロビジョニングします。また、[削除（Delete）] オプションを使用して、デバイスグループから関連付けられているプロファイルを削除することもできます。 [編集（Edit）] ウィンドウで、必要なプロファイルを選択するか、既存の割り当てを削除します。必要な編集を行った後、変更をプロビジョニングします。

オプション	説明
ポートプロファイルの割り当ての編集	[ポートプロファイル（Port Profiles）]エリアで[ポートプロファイルの割り当ての編集（Edit port profile assignment）]をクリックし、ポートプロファイルを編集してプロビジョニングします。また、[割り当ての削除（Delete assignment）]オプションを使用して、デバイスグループから関連付けられているプロファイルを削除することもできます。 [編集（Edit）] ウィンドウで、必要なプロファイルを選択するか、既存の割り当てを削除します。必要な編集を行った後、変更をプロビジョニングします。

[デバイス（Device）] タブには、デバイスグループに割り当てられているネットワークデバイスのリストが表示されます。デバイステーブルには、デバイス名、IP アドレス、管理性のステータス、稼働時間などの情報が含まれています。デバイスをクリックすると、設定の詳細が表示されます。

デバイスがない場合は、[デバイスの割り当て（Assign devices）] オプションが表示されます。

次のオプションを使用してデバイスを管理します。

表 *55* : デバイス

オプション	説明
設定の比較	デバイス設定を既存の設定プロファイルと比較します。 • **[設定の比較（Compare configuration）] > [すべてのデバイスの設定を比較（Compare configurations of all devices）]** の順に選択し、すべてのデバイスの設定を比較します。 • 比較するデバイスを選択し、[設定の比較（Compare configuration）] をクリックして選択したデバイスの設定を比較します。 デバイス設定の比較（1323 ページ） を参照してください。

オプション	説明
デバイスの割り当て	デバイスグループにデバイスを割り当てます。 [デバイスの割り当て（Assign devices）] ウィンドウで、割り当てるデバイスの横にあるチェックボックスをオンにし、[デバイスの割り当て（Assign devices）] をクリックします。 （注） デバイスはネットワークに関連付けられているサイトからのみ割り当てることができます。
デバイスの削除	デバイスグループからデバイスを削除します。 削除するデバイスの横にあるチェックボックスをオンにし、[デバイスの削除（Remove devices）] をクリックします。
プロファイルの学習	デバイスの設定を学習して設定プロファイルを作成します。 学習するデバイスの横にあるチェックボックスをオンにし、[プロファイルの学習（Learn profiles）] をクリックします。 （注） 設定学習オプションは、Cisco Catalyst 9000 シリーズ スイッチでのみ使用できます。 「スイッチから設定プロファイルを学習 （1315 ページ）」を参照してください。

スイッチから設定プロファイルを学習

次の手順を実行して、デバイスから設定を学習し、スイッチング設定プロファイルを作成します。

始める前に

ネットワークとデバイスグループを作成し、デバイスをデバイスグループに割り当てていることを確認します。ネットワークの管理 （1306 ページ）およびスイッチング デバイス グループの管理 （1312 ページ）を参照してください。

手順

ステップ 1 メインメニューから次を選択します。**[プロビジョニング（Provision）]**>**[キャンパスネットワーク（Campus Network）]** > **[ネットワークおよび設定プロファイル（Networks & Configuration Profiles）]**.

ステップ 2 デバイスからプロファイルを学習するには、次の手順を実行します。

オプション 1：

a) [ネットワーク（Network）] をクリックします。

b) ネットワーク内のデバイスを表示するには、次のいずれかのオプションを使用します。

- [デバイスグループ（Device Group）] タブで、デバイスグループをクリックします。

  [デバイスグループ（Device Group）] ウィンドウで、[デバイス（Devices）] タブをクリックします。

- [Devices] タブをクリックします。

c) 目的のデバイスを選択し、[プロファイルの学習（Learn profiles）] をクリックします。

（注） [**Learn profiles**] オプションは、Cisco Catalyst 9000 シリーズ スイッチでのみサポートされています。

オプション 2：

a) **[設定プロファイル（Configuration profiles）]** > **[スイッチング（Switching）]**をクリックします。

b) [スイッチから学習（Learn from a switch）] をクリックします。

c) 学習するデバイスを選択します。

ステップ 3 設定のタイプを選択します。

- [デバイス設定（Device configurations）] の場合、学習する設定を選択します。各設定はプロファイルとして保存できます。
  - **レイヤ 2**
  - **レイヤ 3**
  - **セキュリティ**
  - **ネットワーク設定**
  - **ポート プロファイル**
- [ポート設定（Port configurations）] の場合、学習するポートを選択します。

ステップ 4 [Next] をクリックします。

デバイスから学習した設定が表示されます。

ステップ 5 設定を表示し、必要に応じて編集します。

ステップ 6 [構成プロファイルの作成（Create Configuration Profiles）] をクリックします。

デバイスの管理

Before you begin

ネットワークを作成し、デバイスをネットワークに割り当てます。詳細については、ネットワークの作成 （1308 ページ） を参照してください。

キャンパス ネットワーク内のデバイスを表示および管理するには、次の手順を使用します。

（注） ワイヤレスコントローラの場合、この機能はベータ版であり、機能の有効化が必要です。この機能が有効になっていない場合、これらのオプションは使用できません。

手順

ステップ 1 メインメニューから次を選択します。**[プロビジョニング（Provision）]>[キャンパスネットワーク（Campus Network）] > [ネットワークおよび設定プロファイル（Networks & Configuration Profiles）]**。

ステップ 2 ネットワーク名をクリックすると、ネットワークの詳細が表示されます。

ステップ 3 [Devices] タブをクリックします。

ステップ 4 必要なデバイスタイプを選択します。

- スイッチを管理する場合は [**switches**] をクリックします。
- ワイヤレスコントローラを管理する場合は [**wireless controllers**] をクリックします。

ステップ 5 ネットワークにデバイスが割り当てられていない場合は、[デバイスの割り当て（Assign devices）] をクリックします。

スイッチの割り当てについては、「スイッチングデバイス グループの管理 （1312 ページ）」を参照してください。ワイヤレスコントローラの割り当てについては、「既存のネットワークに対する ワイヤレスコントローラ の割り当て （1319 ページ）」を参照してください。

ステップ 6 （任意） [エクスポート（Export）] をクリックして、ネットワークとそのデバイスの詳細を含むカンマ区切り値（CSV）ファイルをダウンロードします。

ステップ 7 （任意） 次の設定を使用してスイッチを管理します。

実行する操作	結果
デバイスから 設定プロファイル を学習	設定を学習するデバイスのチェックボックスをオンにして、[プロファイルの学習（Learn profiles）] をクリックします。 （注） このオプションは、Cisco Catalyst 9000 シリーズ スイッチでのみ使用できます。
ネットワークからのデバイスの削除	1. ネットワークから削除するデバイスのチェックボックスをオンにします。 2. [ネットワークから削除（Remove from network）] をクリックします。 3. ダイアログボックスで、[デバイスの削除（Remove device）] をクリックします。
ネットワークへのデバイスの割り当て	スイッチング デバイス グループの管理 （1312 ページ） を参照してください。
デバイス設定の比較	スイッチング デバイス グループの管理 （1312 ページ） を参照してください。

ステップ 8 （任意） 次の設定を使用して ワイヤレスコントローラ を管理します。

実行する操作	結果
ネットワークに ワイヤレスコントローラ を追加	[WLCの追加（Add WLC）] をクリックします。 既存のネットワークに対する ワイヤレスコントローラ の割り当て （1319 ページ） を参照してください。
設定プロファイル の ワイヤレスコントローラ の割り当てを管理	省略記号アイコンをクリックし、[デバイスのプロビジョニング（Provision Device）] を選択します。 または、デバイスのチェックボックスをオンにして、**[デバイスのプロビジョニング（Provision Device）]** をクリックします。 「設定プロファイル の ワイヤレスコントローラ への割り当て （1320 ページ）」、「設定プロファイル の ワイヤレスコントローラ 割り当ての編集 （1321 ページ）」、および「ワイヤレスコントローラからの設定プロファイルの削除 （1323 ページ）」を参照してください。

実行する操作	結果
デバイス設定の比較	省略記号アイコンをクリックし、[設定の比較（Compare configuration）] を選択します。 または、デバイスのチェックボックスをオンにして、[設定の比較（Compare configuration）] をクリックします。 デバイス設定の比較 （1323 ページ） を参照してください。
以前の比較結果を表示	省略記号アイコンをクリックし、[前回の実行結果との比較を表示（view last run comparison）] を選択します。
ネットワークからのデバイスの削除	1. 省略記号アイコンをクリックし、[ネットワークから削除（Remove from network）] を選択します。 または、デバイスのチェックボックスをオンにして、[ネットワークから削除（Remove from network）] をクリックします。 2. ダイアログボックスで、[デバイスの削除（Remove device）] をクリックします。

既存のネットワークに対する ワイヤレスコントローラ の割り当て

既存のネットワークに ワイヤレスコントローラ を追加するには、次の手順を実行します。

Before you begin

- この機能はベータ版であり、機能を有効にする必要があります。この機能が有効になっていない場合、これらのオプションは使用できません。
- ワイヤレスコントローラがキャンパスネットワークの対応するサイトに割り当てられていることを確認してください。

手順

ステップ 1 メインメニューから次を選択します。**[プロビジョニング（Provision）]>[キャンパスネットワーク（Campus Network）] > [ネットワークおよび設定プロファイル（Networks & Configuration Profiles）]**。

ステップ 2 ネットワーク名をクリックすると、ネットワークの詳細が表示されます。

ステップ 3 [Devices] タブをクリックします。

ステップ 4 [ワイヤレスコントローラ（wireless controllers）] をクリックします。

ステップ 5 次のいずれかの設定を完了します。

- ネットワークにワイヤレスコントローラが割り当てられていない場合は、[デバイスの割り当て（Assign devices）] をクリックして ワイヤレスコントローラ を割り当てます。
- ワイヤレスコントローラ がネットワークにすでに割り当てられている場合は、[WLCの追加（Add WLC）] をクリックします。

ステップ 6 [デバイスの追加（Add device）] ウィンドウで、必要な ワイヤレスコントローラ を選択します。

ステップ 7 [デバイスの割り当て（Assign devices）] をクリックします。

設定プロファイル の ワイヤレスコントローラ への割り当て

設定プロファイル が ワイヤレスコントローラ に割り当てられていない場合は、この手順を使用して 設定プロファイル を ワイヤレスコントローラ に割り当てます。

Before you begin

- この機能はベータ版であり、機能を有効にする必要があります。この機能が有効になっていない場合、これらのオプションは使用できません。
- 設定プロファイルが ワイヤレスコントローラ で使用可能であることを確認します。詳細については、「ワイヤレスコントローラ から 設定プロファイル を学習する （1311 ページ）」を参照してください。

手順

ステップ 1 メインメニューから次を選択します。**[プロビジョニング（Provision）]>[キャンパスネットワーク（Campus Network）] > [ネットワークおよび設定プロファイル（Networks & Configuration Profiles）]**。

ステップ 2 ネットワーク名をクリックすると、ネットワークの詳細が表示されます。

ステップ 3 [Devices] タブをクリックします。

ステップ 4 [ワイヤレスコントローラ（wireless controllers）] をクリックします。

ステップ 5 デバイス名をクリックします。

ステップ 6 [設定プロファイルの割り当て（Assign configuration profile）] をクリックし、**[設定プロファイルの割り当てとプロビジョニング（Assign Configuration Profiles and Provision）]** ウィンドウで次の設定を行います。

a) **[設定プロファイルの割り当て（Assign configuration profiles）]** ウィンドウで、対応するドロップダウンリストから必要な 設定プロファイル タイプごとに 設定プロファイル を選択します。

（注） 同じ Cisco IOS XE リリースを実行している ワイヤレスコントローラ から学習した 設定プロファイル のみを割り当てることができます。

b) **[レビュー（Review）]** ウィンドウでデバイス設定を確認します。

プロビジョニングに影響する問題がある場合、Catalyst Centerには アイコンが表示されます。エラーの詳細を表示するには、このアイコン付きの機能をクリックします。続行する前に、対応する 設定プロファイルを編集して問題を解決してください。詳細については、設定プロファイルの管理 （1309ページ）を参照してください。

c) 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

d) [Tasks] ウィンドウで、タスクの展開を監視します。

設定プロファイル の ワイヤレスコントローラ 割り当ての編集

設定プロファイル がすでに ワイヤレスコントローラ に割り当てられている場合は、この手順を使用して 設定プロファイル 割り当てを編集し、ワイヤレスコントローラ をプロビジョニングします。

Before you begin

- この機能はベータ版であり、機能を有効にする必要があります。この機能が有効になっていない場合、これらのオプションは使用できません。
- 必要な 設定プロファイル が割り当てに利用できることを確認してください。詳細については、ワイヤレスコントローラから設定プロファイルを学習する （1311ページ） を参照してください。

手順

ステップ 1 メインメニューから次を選択します。**[プロビジョニング（Provision）]>[キャンパスネットワーク（Campus Network）] > [ネットワークおよび設定プロファイル（Networks & Configuration Profiles）]**。

ステップ 2 ネットワーク名をクリックすると、ネットワークの詳細が表示されます。

ステップ 3 [Devices] タブをクリックします。

ステップ 4 [ワイヤレスコントローラ（wireless controllers）] をクリックします。

ステップ 5 デバイス名をクリックします。

ステップ 6 [設定プロファイルの編集（Edit configuration profile）] をクリックし、**[設定プロファイルの割り当てとプロビジョニング（Assign Configuration Profiles and Provision）]** ウィンドウで次の設定を行います。

a) **[設定プロファイルの編集（Edit configuration profiles）]** ウィンドウで、必要な 設定プロファイル タイプごとに 設定プロファイル を選択します。

同じ Cisco IOS XE リリースを実行している ワイヤレスコントローラ から学習した 設定プロファイル のみを割り当てることができます。

実行する操作	結果
プロファイルが割り当てられていない設定プロファイル タイプへの 設定プロファイル の割り当て	対応するドロップダウンリストから必要な 設定プロファイル を選択します。
設定プロファイル タイプからの 設定プロファイル の削除	**1.** 対応する [割り当ての削除（Delete assignment）] オプションをクリックします。 **2.** ダイアログボックスで、**Yes** をクリックします。
すでにプロファイルが割り当てられている設定プロファイル タイプには、別の 設定プロファイル を選択してください。	**1.** 割り当てられた 設定プロファイル を削除します。 **2.** 対応するドロップダウンリストから必要な 設定プロファイル を選択します。

b) **[レビュー（Review）]** ウィンドウでデバイス設定を確認します。

プロビジョニングに影響する問題がある場合、Catalyst Center には アイコンが表示されます。エラーの詳細を表示するには、このアイコン付きの機能をクリックします。続行する前に、対応する 設定プロファイル を編集して問題を解決してください。詳細については、設定プロファイルの管理（1309 ページ）を参照してください。

c) 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する（238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

d) [Tasks] ウィンドウで、タスクの展開を監視します。

ワイヤレスコントローラからの 設定プロファイル の削除

ワイヤレスコントローラから 設定プロファイル 割り当てを削除するには、この手順を使用します。

（注） この機能はベータ版であり、機能を有効にする必要があります。この機能が有効になっていない場合、これらのオプションは使用できません。

削除後は、ワイヤレスコントローラに別の設定プロファイルを割り当てることができます。

（注） ワイヤレスコントローラから設定プロファイルを削除しても、Catalyst Centerはワイヤレスコントローラでプロビジョニングされた、対応する設定を削除しません。

手順

ステップ 1 メインメニューから次を選択します。**[プロビジョニング（Provision）]>[キャンパスネットワーク（Campus Network）] > [ネットワークおよび設定プロファイル（Networks & Configuration Profiles）]**。

ステップ 2 ネットワーク名をクリックすると、ネットワークの詳細が表示されます。

ステップ 3 [Devices] タブをクリックします。

ステップ 4 [ワイヤレスコントローラ（wireless controllers）] をクリックします。

ステップ 5 デバイス名をクリックします。

ステップ 6 [割り当ての削除（Delete assignment）] オプションをクリックして、設定プロファイルタイプの設定プロファイルの割り当てを削除します。

ステップ 7 ダイアログボックスで、[Delete] をクリックします。

デバイス設定の比較

デバイス設定を設定プロファイルと比較して逸脱を特定するには、次の手順を実行します。

始める前に

スイッチ

ネットワークとデバイスグループを作成し、デバイスをデバイスグループに割り当てていることを確認します。「ネットワークの管理 （1306ページ）」と「スイッチングデバイス グループの管理 （1312 ページ）」を参照してください。

ワイヤレスコントローラ

（注） この機能はベータ版であり、機能を有効にする必要があります。この機能が有効になっていない場合、このオプションは使用できません。

- ワイヤレスコントローラがネットワークに割り当てられていることを確認します。詳細については、「既存のネットワークに対するワイヤレスコントローラの割り当て（1319ページ）」を参照してください。
- 設定プロファイルが使用可能であることを確認します。詳細については、「ワイヤレスコントローラ から 設定プロファイル を学習する （1311 ページ）」を参照してください。

手順

ステップ 1 メインメニューから次を選択します。**[プロビジョニング（Provision）]>[キャンパスネットワーク（Campus Network）] > [ネットワークおよび設定プロファイル（Networks & Configuration Profiles）]**.

ステップ 2 ネットワークをクリックします。

ステップ 3 次の手順を実行してデバイス設定を比較します。

スイッチ

a) **[デバイスグループ（Device Groups）]** タブで、デバイスグループをクリックします。

b) **[デバイスグループ（Device Group）]** ウィンドウで、必要なオプションを選択します。

目的	手順
すべてのデバイスのデバイス設定を比較する	**[設定の比較（Compare configuration）] > [すべてのデバイスの設定を比較（Compare configurations of all devices）]** の順に選択します。
選択したデバイスのデバイス設定の比較	必要なデバイスのチェックボックスをオンにして、[設定の比較（Compare configuration）] をクリックします。

ワイヤレスコントローラについて

a) [デバイス（Devices）] タブで、[ワイヤレスコントローラ（wireless controllers）] をクリックします。

b) 省略記号アイコンをクリックし、[設定の比較（Compare configuration）] を選択します。

または、デバイスのチェックボックスをオンにして、[設定の比較（Compare configuration）] をクリックします。

ステップ 4 [設定の比較（Compare configuration）] ダイアログボックスで、次の手順を実行します。

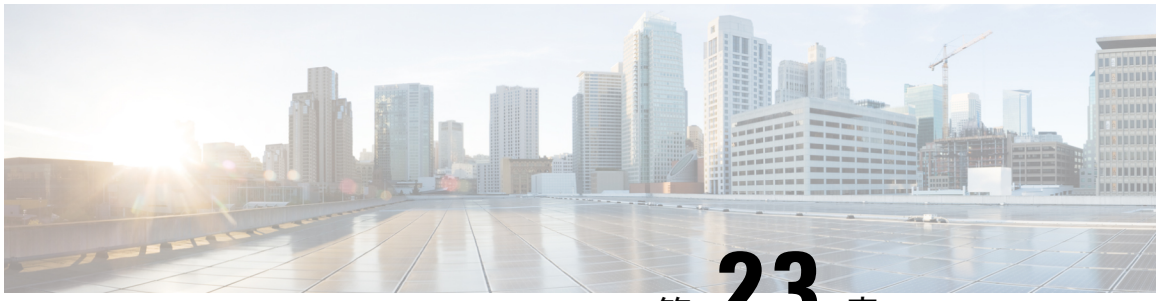
a) [プロファイルタイプの選択（Select profile type）] ドロップダウンリストから、設定プロファイルのタイプを選択します。

b) [プロファイルの選択（Select profile）] ドロップダウンリストから、設定を比較するプロファイルを選択します。
c) [Compare（比較）] をクリックします。

[比較結果（Comparison results）] ウィンドウには、次の比較結果のデバイス数が表示されます。

- [一致（Match）]：設定が一致するデバイス。
- [不一致（Does not match）]：設定が設定プロファイルと一致しないデバイス。
- [比較に失敗（Comparison failed）]：比較に失敗したデバイス。

比較された特定のデバイスとそれらの個別の比較結果を表示することもできます。



第 23 章

サービスのプロビジョニング

- アプリケーション （1327 ページ）
- アプリケーション ホスティング （1352 ページ）
- Cisco Catalyst 9100 シリーズ アクセスポイントでのアプリケーション ホスティング （1368 ページ）
- サイト間 VPN の設定 （1372 ページ）
- Cisco Umbrella の設定 （1374 ページ）
- セキュアトンネルの作成 （1383 ページ）
- SD-Access へのセキュリティサービスの挿入 （1386 ページ）
- Secure Equipment Access （1397 ページ）
- Cisco Cyber Vision Center と Catalyst Center の統合 （1403 ページ）

アプリケーション

このセクションでは、アプリケーションについて説明します。

アプリケーションの可視性について

アプリケーション可視性サービスを使用すると、組み込みアプリケーション、カスタムアプリケーション、およびアプリケーションセットを管理できます。

アプリケーション可視性サービスは、Catalyst Center 内でアプリケーションスタックとしてホストされているため、特定のデバイスでコントローラベースのアプリケーション認識（CBAR）機能を有効にして、数千のネットワークと自社製のアプリケーションおよびネットワークトラフィックを分類することができます。

次のパッケージをインストールできます。

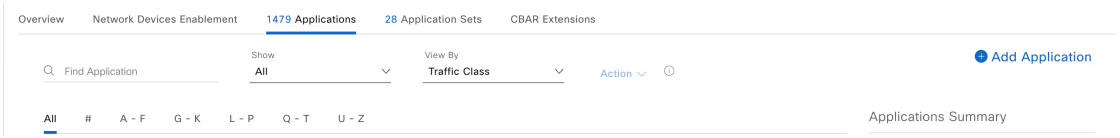
- [Application Policy]：キャンパスやブランチ内の LAN、WAN、およびワイヤレスで QoS ポリシーを自動化できます。
- [Application Registry]：アプリケーションとアプリケーションセットを表示、管理、および作成できます。

- [Application Visibility Service]：Network-Based Application Recognition（NBAR）およびCBARの技術を使用してアプリケーションを分類できます。

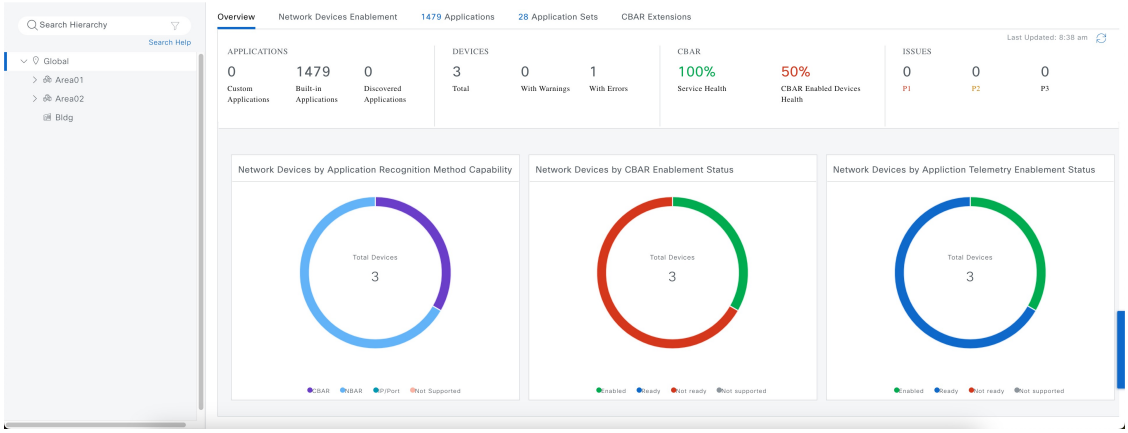
  NBAR は、Cisco Catalyst 9000 デバイスでの最大 450 のインターフェイスのプロビジョニングをサポートしています。Catalyst Center のアプリケーション可視性は、この 450 インターフェイスの制限を超えません。

（注） 互換性を確保するには、上記のパッケージのパッケージバージョンが同じである必要があります。

アプリケーションレジストリ、またはアプリケーションレジストリとアプリケーションポリシーの両方をインストールする場合、メニューアイコンをクリックして次を選択します。**[Provision]** > **[Application Visibility]**を選択すると、[Applications] タブと [Application Sets] タブが表示されます。



アプリケーションレジストリとアプリケーション可視性サービス、またはアプリケーションレジストリ、アプリケーションポリシー、およびアプリケーション可視性サービスをインストールする場合、メニューアイコンをクリックして次を選択します。 **[Provision]** > **[Application Visibility]**を選択すると、[Applications]、[Application Sets]、[Network Devices Enablement]、[CBAR Extensions] の各タブが表示されます。



アプリケーション可視性ビュー

次の表で、**[Provision（プロビジョニング）]** > **[Services（サービス）]** > **[アプリケーション可視性（Application Visibility）]** の [概要（Overview）] タブで使用可能なダッシュレットとチャートについて説明します。

アイテム	説明
アプリケーション	このチャートには、Catalyst Center アプリケーション内のアプリケーションのうち、アプリケーションポリシーで使用できるアプリケーションの数が表示されます。アプリケーションは次のように分類されます。 • [Custom]：ユーザーによって追加されたアプリケーション • [Built-in]: インストールされているアプリケーション Catalyst Center • [Discovered]：さまざまな認識方法で検出され、アプリケーションレジストリにインポートされたアプリケーション （注） このチャートには、CBAR が有効なデバイスでのみ観察されたアプリケーションが表示されます。
デバイス	デバイス、警告のあるデバイス、およびエラーのあるデバイスの総数が表示されます。
CBAR	このウィジェットには、すべての CBAR 対応デバイスのサービス正常性と平均正常性スコアが表示されます。デバイスに未処理のエラーまたは警告がない場合、そのデバイスは正常です。 CBAR 正常性スコアは、すべての CBAR 対応デバイスで計算されます。 各 CBAR 対応デバイスの CBAR 正常性を確認できます。0% の CBAR 正常性スコアは、デバイスに少なくとも 1 つのエラー（P1）があることを示します。50% の CBAR 正常性スコアは、デバイスにエラーはないが、少なくとも 1 つの警告（P2）があることを示します。100% の CBAR 正常性スコアは、正常なデバイスを示します。
問題	すべての問題は、次のように優先順位によって分類されます。 • エラー（P1） • 警告（P2） • その他 （P3） [P1]、[P2]、および [P3] タブをクリックすると、デバイスの問題と修復の詳細が表示されます。

アイテム	説明
アプリケーション認識方式別のネットワークデバイス	このチャートには、各アプリケーション認識方式によって分類されたデバイスの数が表示されます。 • [CBAR]：CBAR 対応デバイス（ルータ、スイッチなど） • [NBAR]：NBAR ベースのデバイス（ルータ、スイッチ、シスコ ワイヤレス コントローラ、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラなど） • [IP/port]：IP/ポートベースのデバイス（スイッチなど） • [Not supported]：上記のいずれの方式でもサポートされていないデバイス
CBAR 有効化ステータス別のネットワークデバイス	このチャートには、各 CBAR の準備状況ステータスのデバイス数が表示されます。 • [Enabled]：CBAR が有効になっているデバイス • [Ready]：CBAR を有効にする準備が整っているデバイス （注） [Ready] ステータスの横にある情報アイコンは、それぞれのデバイスがワイヤレス対応であることを示しています。 • [Not Ready]：CBAR をサポートしているが、いくつかの問題により CBAR を有効にする準備ができていないデバイス • [Not Supported]：CBAR をサポートしていないデバイス
アプリケーションテレメトリ有効化ステータス別のネットワークデバイス	このチャートには、デバイス アプリケーション テレメトリ有効化ステータスが表示されます。 • [Enabled]：アプリケーションテレメトリが有効になっているデバイス • [Ready]：アプリケーションテレメトリを有効にする準備が整っているデバイス • [Not Ready]：アプリケーションテレメトリをサポートしているが、いくつかの問題によりアプリケーションテレメトリを有効にする準備ができていないデバイス • [Not Supported]：アプリケーションテレメトリをサポートしていないデバイス

次の表に、[ネットワークデバイスの有効化（Network Devices Enablement）] タブの [サイトデバイス（Site Devices）] テーブルに表示されるデバイス情報およびステータスを示します。

カラム	説明
[Device Name]	デバイスの名前。デバイス名をクリックして、CBARサービスのステータスを表示します。
[Management IP]	デバイスの IP アドレス。
Device Type	ルータ、スイッチとハブ、ワイヤレス コントローラなど、関連するデバイスのグループ。
Site	デバイスに割り当てられているサイト。
Fabric	デバイスが割り当てられているファブリックドメイン。
Role	スキャン プロセス中に、検出された各デバイスに割り当てられているロール。デバイス ロールは、ネットワーク内での役目と配置に従って、デバイスを識別およびグループ分けするために使用されます。Catalyst Center でデバイスロールを特定できない場合、デバイスロールは不明に設定されます。
Active Recognition Method	デバイス認識方式（CBAR、NBAR、IP/Port、または Not supported）が表示されます。
[OS Version]	デバイスで現在実行されている Cisco IOS ソフトウェア。
CBAR Readiness Status	ステータスが [有効（Enabled）] の場合、情報アイコンにカーソルを合わせると、CBARがワイヤレスモード、有線モード、またはファブリック SSID タイプに対して有効になっているかどうかについての詳細が表示されます。 ステータスが [準備完了（Ready）] の場合は、情報アイコンにカーソルを合わせると、修復メッセージが表示されます。
Protocol Pack Version	デバイスにインストールされているプロトコルパックの現在のバージョンと、プロトコルパックの更新ステータスが表示されます。
Device Registry Status	デバイスとアプリケーションレジストリとの同期ステータスが表示されます。情報アイコンまたはエラーアイコンにカーソルを合わせると、同期ステータスに関する詳細が表示されます。
CBAR Deployment Status	CBAR の展開ステータスが表示されます。 詳細については、ネットワークデバイスでのCBARの再設定（1339ページ）を参照してください。

カラム	説明
Service Health Status	[Service Health Status] 列の [Issues] をクリックすると、[CBAR Service Status] ページが開きます。このページには、問題の完全なリストとデバイスのサービスステータス情報が表示されます。Cisco Catalyst 9K デバイスの名前をクリックすると、CBAR サービスのフットプリント（サービス負荷、CPU、フロー）を確認できます。
Application Telemetry Readiness Status	アプリケーションテレメトリのデバイス準備状況が表示されます。
Application Telemetry Deployment Status	デバイスのアプリケーションテレメトリ展開ステータスが表示されます。展開が失敗した場合、リンクをクリックすると、失敗の詳細が表示されます。
Application QoS Policy	デバイスに適用されているアプリケーションポリシー。シスコワイヤレス コントローラに複数のアプリケーションポリシーがある場合は、適用されているアプリケーションポリシーの数と適用されているすべてのアプリケーションポリシーの名前が表示されます。
WAN Interfaces	WAN インターフェイスの数が表示されます。[WAN interface details] をクリックすると、デバイスの WAN 接続設定が表示されます。
Trunk Interfaces	トランクインターフェイスの数が表示されます。[Trunk interface details] をクリックすると、デバイスのトランク接続設定が表示されます。

CBAR クラウドの設定

アプリケーション可視性サービスでは、CBAR クラウドを使用してプロトコルパックを拡充し、クラウドからデータを送受信することによって不明なアプリケーションの可視性を強化します。

手順

ステップ 1 メインメニューから次を選択します。**[Provision]** > **[Application Visibility]**の順に選択します。

ステップ 2 [CBAR拡張（CBAR Extensions）] タブをクリックします。

ステップ 3 [Cisco Cloud Services] リンクをクリックします。

ステップ 4 **[システム（System）]** > **[設定（Settings）]** > **[外部サービス（External Services）]** > **[Cisco Catalyst Cloud]** ページが新しいブラウザタブで開きます。

a) [**Cisco Catalyst Cloud**] ページで、[**Register**] をクリックします。

b) [**Activate your device**] ポップアップウィンドウで、[**Next**] をクリックして続行します。

（注） [**Activation code**] フィールドは事前に入力されています。

c) [**Sign in**] ポップアップウィンドウで、Cisco アカウントにサインインします。

Catalyst Center が登録され、[**Cisco Catalyst Cloud**] ページに登録情報が表示されます。

ステップ 5 **[プロビジョニング（Provision）] > [アプリケーションの可視性（Application Visibility）]** に戻り、**[CBAR 拡張（CBAR Extensions）]** を選択します。[CBAR拡張（CBAR Extensions）] ページを更新します。

ステップ 6 [CBAR Cloud] タブで、使用可能な **CBAR ダイナミック アプリケーション フィード**のリストを表示できます。すべてのアプリケーションフィードを有効にするには、[All] オプションボタンをクリックします。

（注） すべてのフィードを選択すると、新しく導入されたアプリケーションフィードがネットワークで自動的に有効になります。

必要なアプリケーションフィードを有効にするには、次の手順を実行します。

1. [Selected only] オプションボタンをクリックします。
2. 選択するアプリケーションフィードの横にあるチェックボックスをオンにします。
3. [Apply] をクリックします。

（注） [選択内容のみ（Selected only）] モードでは、新しく導入されたアプリケーションフィードは、手動で選択するまでネットワークにインポートされません。

CBAR クラウドの有効化または無効化

始める前に

Catalyst Center と Cisco Cloud Services の間で接続が確立されていることを確認します。詳細については、CBAR クラウドの設定 （1332 ページ）を参照してください。

手順

ステップ 1 メインメニューから次を選択します。**[Provision] > [Application Visibility]** の順に選択します。

ステップ 2 [CBAR Extensions] > [CBAR Cloud] タブをクリックします。

ステップ 3 次のいずれか 1 つのタスクを実行します。

- CBAR クラウドを有効にするには、[有効化（Enable）] トグルボタンをクリックします。
- CBAR クラウドを無効にするには、[有効化（Enable）] トグルボタンをクリックし、表示されるダイアログボックスで [はい（Yes）] をクリックします。

ネットワークデバイスでの CBAR の有効化

始める前に

- デバイスがサイトに割り当てられている必要があります。
- ネットワークデバイスでCBARを有効にする前に、CBARクラウドを設定することをお勧めします。詳細については、CBARクラウドの設定（1332ページ）を参照してください。

手順

ステップ 1 メインメニューから次を選択します。**[Provision]** > **[Application Visibility]** > **[Network Devices Enablement]** タブを選択します。

[サイトデバイス（Site Devices）] テーブルが表示されます。すべての列を表示するには、縦の省略記号をクリックし、[すべて（All）] をクリックします。

ステップ 2 選択したデバイスまたはすべてのデバイスで CBAR を有効にします。

以下で CBAR を有効にする場合	結果
すべてのデバイス	1. [CBAR] ドロップダウンリストから、[すべての対応デバイスでCBARを有効化（Enable CBAR on all ready devices）] を選択します。 2. 警告ダイアログボックスで、[Yes] をクリックします。
選択されたデバイス	1. デバイス名の横にあるチェックボックスをオンにして、デバイスを選択します。 2. [CBAR] ドロップダウンリストから、[選択したデバイスでCBARを有効化（Enable CBAR on selected devices）] を選択します。 3. 警告ダイアログボックスで、[Yes] をクリックします。

ステップ 3 確認したら、[CBARの有効化] スライドインペインでデバイスの詳細を確認し、[有効化（Enable）] をクリックします。

ステップ 4 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

ステップ 5 [Tasks] ウィンドウで、タスクの展開を監視します。

ネットワークデバイスでの CBAR の無効化

手順

ステップ 1 メインメニューから次を選択します。**[Provision]** > **[Application Visibility]** > **[Network Devices Enablement]** タブを選択します。

[サイトデバイス（Site Devices）] テーブルが表示されます。すべての列を表示するには、縦の省略記号をクリックし、[すべて（All）] をクリックします。

ステップ 2 選択したデバイスまたはすべてのデバイスで CBAR を無効にします。

CBAR を無効化する場合	結果
すべてのデバイス	1. [CBAR] ドロップダウンリストから、[すべてのデバイスでCBARを無効化（Disable CBAR on all devices）] を選択します。 2. 警告ダイアログボックスで、[Yes] をクリックします。
選択されたデバイス	1. デバイス名の横にあるチェックボックスをオンにして、デバイスを選択します。 2. [CBAR] ドロップダウンリストから、[選択したデバイスでCBARを無効化（Disable CBAR on selected devices）] を選択します。 3. 警告ダイアログボックスで、[Yes] をクリックします。

ステップ 3 確認後、**[CBARの無効化（Disable CBAR）]** スライドインペインで、展開のタスクをスケジュールします。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

ステップ 4 [Tasks] ウィンドウで、タスクの展開を監視します。

アプリケーションテレメトリの有効化

アプリケーションテレメトリを有効にして、アプリケーションの可視性とモニタリング用のトラフィックテレメトリデータを送信するようにデバイスでNetFlowコレクタ設定を行います。詳細については、テレメトリの設定について （59 ページ）を参照してください。

始める前に

アプリケーションテレメトリを有効にする前に、CBARクラウドを設定することをお勧めします。詳細については、CBAR クラウドの設定 （1332 ページ）を参照してください。

手順

ステップ 1 メインメニューから次を選択します。**[Provision]** > **[Application Visibility]** の順に選択します。

ステップ 2 [Network Devices Enablement] タブをクリックします。

ステップ 3 [サイトデバイス（Site Devices）] テーブルで、次の手順を実行してアプリケーションテレメトリを有効にします。

a) デバイスを選択します。

b) [Application Telemetry] ドロップダウンリストから、[Enable Application Telemetry] を選択します。

c) [アプリケーションテレメトリの有効化（Enable Application Telemetry ）] ウィンドウで、次の手順を実行します。

- **[Generate Configure Preview]** オプションボタンをクリックし、**[Preview]** をクリックします。
- **[Enable Application Telemetry Task]** ウィンドウで、Catalyst Center は、最初にリストされたデバイスの実行中の設定と計画された設定の並列比較を表示します。
- デバイス設定を確認し、準備ができたら **[Deploy]** をクリックします。
- **[Now]** または **[Later]** のスケジューリングオプションを選択し、**[Deploy]** をクリックします。

（注） **[Application Telemetry]** 列には、アプリケーションテレメトリの展開ステータスが表示されます。

デバイスのアプリケーションテレメトリの展開が失敗した場合は、**[Application Telemetry Deployment Status]** 列のリンクをクリックして失敗の理由を確認します。

アプリケーションテレメトリの無効化

手順

ステップ 1 メインメニューから次を選択します。**[Provision]** > **[Application Visibility]** の順に選択します。

ステップ 2 [Network Devices Enablement] タブをクリックします。

ステップ 3 アプリケーションテレメトリを無効にするには、次の手順を実行します。

1. [Site Devices] テーブルでデバイスを選択します。
2. [Application Telemetry] ドロップダウンリストから、[Disable Application Telemetry] を選択し、表示される警告ダイアログボックスで [Yes] をクリックします。

CBAR 対応デバイスでのプロトコルパックの更新

CBAR をサポートする任意のデバイスのプロトコルパックを最新または特定のプロトコルパックにアップグレードできます。プロトコルパックを手動で更新することも、プロトコルパックの自動更新を有効にすることもできます。

（注）
- CBAR クラウドコネクタが無効になっている場合、プロトコルパック自動更新メニューは無効になります。
- プロトコルパック自動更新が有効になっている場合、プロトコルパック手動更新メニューは無効になります。

始める前に

- [System Settings] で Cisco ログイン情報を設定します。シスコのログイン情報の設定に関する詳細については、*Cisco Catalyst Center* アドミニストレーション ガイド [英語] を参照してください。
- デバイスは CBAR をサポートしている必要があります。
- デバイスで CBAR が有効になっている必要があります。
- デバイスのプロトコルパックは cisco.com で使用可能である必要があります。

手順

ステップ 1 メインメニューから次を選択します。**[Provision]** > **[Services]** > **[Application Visibility]** の順に選択します。

ステップ 2 [Network Devices Enablement] タブをクリックします。

ステップ 3 [Site Devices] テーブルの [Protocol Pack Version] 列に表示されているステータスを確認します。

[Outdated] ステータスをクリックすると、[Update Protocol Pack] ウィンドウに該当するプロトコルパックのリストが表示されます。

ステップ 4 [Update Protocol Pack] ウィンドウで、必要なプロトコルパックのバージョンに対応する [Update] をクリックします。

[Protocol Pack Version] カラムに [In progress] ステータスが表示されます。現在更新中のバージョンを表示するには、情報アイコンをクリックします。[Protocol Pack Version] カラムに [Update failed] ステータスが表示されたら、エラーアイコンをクリックして失敗の原因を確認します。

ステップ 5 すべてのデバイスまたは選択したデバイスを最新のプロトコルパックに手動で更新する場合は、次のタスクを実行します。

該当するすべての CBAR 対応デバイスでプロトコルパックを更新するには、次のようにします。

- [Update Protocol Pack] ドロップダウンリストから、[Update All Devices] を選択し、後続の警告ダイアログボックスで [Yes] をクリックします。

選択したデバイスでプロトコルパックを更新するには、次のようにします。

- [Site Devices] テーブルでデバイスを選択します。
- [Update Protocol Pack] ドロップダウンリストから、[Update Selected Devices] を選択し、後続の警告ダイアログボックスで [Yes] をクリックします。

ファイルから選択したデバイスでプロトコルパックを更新するには、次のようにします。

- [Site Devices] テーブルでデバイスを選択します。
- [Update Protocol Pack] ドロップダウンリストから、[Update Selected Devices From File] を選択します。

- [Update Protocol Pack From File] スライドインペインで、CSV ファイルをドラッグアンドドロップ領域にドラッグアンドドロップするか、[Choose a file] をクリックして CSV ファイルの場所を参照し、[Open] をクリックします。
- [Import] をクリックします。

ステップ 6 すべてのデバイスのプロトコルパックを自動更新する場合は、次のタスクを実行します。

- [Update Protocol Pack] ドロップダウンリストから、[Auto Update] トグルボタンを有効にして、後続の警告ダイアログボックスで [Yes] をクリックします。

（注） デフォルトでは、すべての準備完了デバイスが自動更新に含まれます。

選択したデバイスをプロトコルパック自動更新から除外するには、次の手順を行います。

- [Site Devices] テーブルでデバイスを選択します。
- [Update Protocol Pack] ドロップダウンリストから、[Exclude Selected Devices] を選択し、後続の警告ダイアログボックスで [Yes] をクリックします。

選択したデバイスをプロトコルパックの自動更新に含めるには、次の手順を行います。

- [Site Devices] テーブルでデバイスを選択します。
- [Update Protocol Pack] ドロップダウンリストから、[Include Selected Devices] を選択し、後続の警告ダイアログボックスで [Yes] をクリックします。

ネットワークデバイスでの CBAR の再設定

[Application Visibility] > [Network Devices Enablement] ウィンドウで、インターフェイスを [Site Devices] テーブルに含めたり、テーブルから除外したりできます。

手順

ステップ 1 メインメニューから次を選択します。**[Provision]** > **[Services]** > **[Application Visibility]** の順に選択します。

ステップ 2 [Network Devices Enablement] タブをクリックします。

ステップ 3 [サイトデバイス（Site Devices）] テーブルで、設定するデバイスの [CBAR展開ステータス（CBAR Deployment status）] 列で [再設定（Re-Configure）] をクリックし、次の手順を実行します。

a) [Enable CBAR] スライドインペインで、デバイス名を検索するかデバイスを見つけて [View Interfaces] をクリックします。
b) 除外するインターフェイスを見つけます。

c) [Status] 列で、トグルボタンをクリックしてインターフェイスを無効にし、[Save] をクリックします。

ステップ 4 インターフェイスを含めるには、[Excluded Interfaces] を選択し、目的のインターフェイスの横にあるトグルボタンをオンにして [Save] をクリックします。

ステップ 5 [有効（Enable）] をクリックします。

ステップ 6 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

ステップ 7 [Tasks] ウィンドウで、タスクの展開を監視します。

アプリケーションおよびアプリケーションセット

アプリケーションは、ネットワーク内で使用されているソフトウェアプログラムまたはネットワーク シグナリング プロトコルです。Catalyst Center は、約 1400 の異なるアプリケーションから成る Cisco Next Generation Network-Based Application Recognition（NBAR2）ライブラリの全アプリケーションをサポートしています。

アプリケーションは、アプリケーションセットと呼ばれる論理グループに分類されています。アプリケーションセットには、ポリシー内でのビジネスとの関連性を割り当てることができます。

アプリケーションは、同様のトラフィック処理要件が規定されている RFC 4594 の定義に従い、業界標準ベースのトラフィッククラスにマッピングされています。トラフィッククラスでは、割り当てられているビジネスとの関連性グループに基づいて、アプリケーショントラフィックに適用される処理（Differentiated Services Code Point（DSCP）マーキング、キューイング、破棄など）を定義します。

Catalyst Center に含まれていない追加のアプリケーションがある場合は、カスタム アプリケーションとして追加して、アプリケーション セットに割り当てることができます。

単方向と双方向のアプリケーション トラフィック

一部のアプリケーションは、完全な左右対称であり、接続の両端に同一の帯域幅プロビジョニングを必要とします。このようなアプリケーションのトラフィックを、双方向のトラフィックと呼びます。たとえば、100 kbps の低遅延キューイング（LLQ）が一方向の音声トラフィックに割り当てられている場合、逆方向の音声トラフィックにも 100 kbps の LLQ をプロビジョニングする必要があります。このシナリオは、同じ Voice over IP（VoIP）コーダ/デコーダ（コーデック）が両方の方向で使用されており、マルチキャスト保留音（MOH）のプロビジョニングが考慮されていないことが前提となっています。ただし、ストリーミングビデオやマルチ

キャストMoHなどの特定のアプリケーションは、ほとんどの場合、単方向です。したがって、ブランチからキャンパスに向かう方向のトラフィックフローでは、ブランチルータでこのようなトラフィック向けの帯域幅保証をプロビジョニングするのは、不要であるばかりか非効率的となる可能性があります。

Catalyst Center では、アプリケーションが特定のポリシーに関して単方向か双方向かを指定できます。

スイッチおよびワイヤレスコントローラでは、NBAR2 やカスタムアプリケーションがデフォルトで単方向となっています。ただし、ルータでは、NBAR2 アプリケーションはデフォルトで双方向です。

カスタムアプリケーション

カスタム アプリケーションは、Catalyst Center に追加するアプリケーションです。使用可能なカスタムアプリケーションの数は、[Overview] ウィンドウで確認できます。有線デバイスについては、サーバー名、IP アドレスとポート、または URL に基づいてアプリケーションを定義できます。Cisco AireOS コントローラではなく、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラに対してカスタムアプリケーションを定義できます。

IP アドレスとポートに従ってアプリケーションを定義する場合は、DSCP 値とポート分類を定義することもできます。

設定プロセスを簡素化するために、類似のトラフィックおよびサービスレベル要件を持つ別のアプリケーションに基づいてアプリケーションを定義できます。Catalyst Center は、他のアプリケーションのトラフィック クラス設定を、定義しているアプリケーションにコピーします。

Catalyst Center は、カスタムアプリケーションの一部として定義される場合でも、ポート番号 80、443、53、5353、および 8080 の ACL を設定しません。カスタム アプリケーションでトランスポート IP が定義されている場合、Catalyst Center はデバイス上のアプリケーションを設定します。

（注） ポリシーが展開されているときにデバイス上のカスタムアプリケーションをプログラムする場合は、そのカスタム アプリケーションを、ポリシーで定義されているいずれかのアプリケーション セットに割り当てる必要があります。

検出されたアプリケーション

検出されるアプリケーションには、Infoblox DNS サーバーなどの推奨されるカスタマイズからインポートされたアプリケーションと、推奨される未分類のアプリケーションフローからインポートされたアプリケーションがあります。

未分類のトラフィックには、CBAR 対応デバイスで識別されるフローからのトラフィックのうち、NBARエンジンでは認識されないフローからのトラフィックが含まれます。このような場合、意味のあるビットレートを持つアプリケーションが未分類として報告され、Catalyst Center でインポートしてアプリケーションとして使用することができます。

アプリケーション可視性サービスでは、Catalyst Center を、CBAR クラウドを介して外部の信頼できるソースに接続して、未分類のトラフィックを分類したり、改善されたシグニチャを生成したりできます。

使用可能な外部の信頼できるソースは、Google Meet、Service Now、Sugarcrm、Telegram、SAP、Microsoft Office 365 クラウドコネクタ、Box、RingCentral、Github、Crashplan、Intuit、Workday、Zscaler、Atlassian、Amazon Chime、Zoom、Dropbox、Webex、Whatsapp、Cisco Meraki、および Salesforce です。このリストは動的です。新しいソースがクラウドに追加されると、リストが更新されます。リストを表示するには、**[Application Visibility]** > **[CBAR Extensions]** > **[CBAR Cloud]**の順に選択します。

（注） アプリケーションを設定する前に、CBAR クラウドコネクタを設定する必要があります。

検出されたアプリケーションはアプリケーションレジストリにインポートされます。

お気に入りのアプリケーション

Catalyst Center では、他のすべてのアプリケーションよりも先に設定するアプリケーションにフラグを付けることができます。お気に入りとしてアプリケーションにフラグを付けることで、デバイス上のお気に入りのアプリケーションに対して QoS ポリシーが設定されていることを確認できるようにします。詳細については、リソースが制限されているデバイスの処理順（1462 ページ）を参照してください。

カスタムアプリケーションを作成すると、お気に入りのアプリケーションとしてマークされます。

お気に入りとしてマークできるアプリケーションの数に制限はありませんが、お気に入りのアプリケーションをごく少数にとどめると（たとえば、25 未満）、ネットワークデバイスの TCAM（Ternary Content Addressable Memory）が限られている展開で、お気に入りのアプリケーションがビジネス関連の観点から正しく処理されるようになります。

お気に入りのアプリケーションは、ビジネス関連のグループまたはトラフィック クラスに属させることが可能で、ポリシー単位ではなくシステム全体で設定されます。たとえば、お気に入りとして cisco-jabber-video アプリケーションにフラグを付けた場合、そのアプリケーションはすべてのポリシーでお気に入りのフラグが付きます。

ビジネス関連のアプリケーションだけでなく、ビジネスに関係のないアプリケーションにもお気に入りのフラグを付けられることに注意してください。たとえば、ネットワーク上に大量の望ましくない Netflix トラフィックがある場合、Netflix にお気に入りのアプリケーションとしてフラグを付けることができます（Netflix がビジネスに関係のないアプリケーションとして割り当てられている場合でも可能）。この場合、Netflix は、その他のビジネスに関係のないアプリケーションより先にデバイスポリシーに組み込まれるようになり、このアプリケーションを制御するビジネス上の目的が確実に実現されます。

アプリケーションおよびアプリケーションセットの設定

次のサブセクションでは、アプリケーションとアプリケーションセットのコンテキストで実行できるさまざまなタスクについて説明します。

（注） 編集または削除できるのは、カスタムアプリケーションと検出されたアプリケーションだけです。また、一度に編集または削除できる数は、カスタムアプリケーションと検出されたアプリケーションの合計で最大100個までです。編集または削除する対象としてアプリケーションを選択した場合、選択したアプリケーションの数を除く、編集または削除が可能なアプリケーションの数を示す通知メッセージが表示されます。

アプリケーション設定の変更

既存のCBARアプリケーション、カスタムアプリケーション、検出されたアプリケーションのアプリケーションセットやトラフィッククラスを変更できます。

手順

ステップ1 メインメニューから次を選択します。**[Provision]** > **[Services]** > **[Application Visibility]** の順に選択します。

ステップ2 [Applications] タブをクリックします。

ステップ3 [Search]、[Show]、または [View By] フィールドを使用して、変更するアプリケーションを見つけます。

名前、ポート番号、およびトラフィッククラスに基づいてアプリケーションを検索できます。

ステップ4 [アプリケーション名（Application Name）] をクリックします。

ステップ5 ダイアログボックスで、1 つまたは両方の設定を変更します。

- [Traffic Class]：ドロップダウンリストからトラフィッククラスを選択します。有効なトラフィック クラスは、BROADCAST_VIDEO、BULK_DATA、MULTIMEDIA_CONFERENCING、MULTIMEDIA_STREAMING、NETWORK_CONTROL、OPS_ADMIN_MGMT、REAL_TIME_INTERACTIVE、SIGNALING、TRANSACTIONAL_DATA、VOIP_TELEPHONY です。
- [Application Set]：ドロップダウンリストからアプリケーションの設定を選択します。有効なアプリケーションセットは、認証サービス、バックアップおよびストレージ、コラボレーションアプリケーション、コンシューマ ブラウジング、コンシューマ ファイル シェアリング、コンシューマゲーミング、コンシューマメディア、コンシューマ misc、コンシューマ ソーシャル ネットワーキング、データベースアプリケーション、デスクトップ仮想化、電子メール、企業 ipc、ファイル共有、一般的なブラウジング、一般的なメディア、一般的な misc、トンネリング、ローカルサービス、ネーミングサービス、ネットワーク制御、ネットワーク管理、リモートアクセス、saas アプリケーション、シグナリング、ソフトウェア開発ツール、ソフトウェアアップデート、ストリーミングメディアです。

ステップ6 [Save] をクリックします。

サーバー名に基づくカスタムアプリケーションの作成

Catalyst Centerに存在しないアプリケーションがある場合、カスタム アプリケーションとして追加することができます。

手順

ステップ 1 メインメニューから次を選択します。**[Provision]** > **[Services]** > **[Application Visibility]** の順に選択します。

ステップ 2 [Application] タブをクリックします。

ステップ 3 ウィンドウの右上隅にある [Add Application] をクリックします。

ステップ 4 スライドインペインで、次のフィールドに必要な情報を入力します。

- **[Application Name]**：カスタムアプリケーションの名前。名前には、下線とハイフンも含めて最大 24 文字の英数字を指定できます。アプリケーション名で使用できる特殊文字は、下線とハイフンのみです。
- [Type]：ユーザーがアプリケーションにアクセスするための方法。サーバー経由でアクセス可能なアプリケーションの [サーバー名（Server Name）] を選択します。
- [Server name]：アプリケーションをホストするサーバーの名前。
- [Similar To]：類似のトラフィック処理要件を持つアプリケーション。オプションボタンをクリックしてこのオプションを選択し、ドロップダウンリストからアプリケーションを選択します。Catalyst Centerは、他のアプリケーションのトラフィッククラスを、定義しているアプリケーションにコピーします。
- **[Traffic Class]**：アプリケーションが属するトラフィッククラス。有効な値は BULK_DATA、TRANSACTIONAL_DATA、OPS_ADMIN_MGMT、NETWORK_CONTROL、VOIP_TELEPHONY、MULTIMEDIA_CONFERENCING、MULTIMEDIA_STREAMING、BROADCAST_VIDEO、REAL_TIME_INTERACTIVE、および SIGNALING です。
- [Application set]：アプリケーションを配置するアプリケーションセット。有効なアプリケーションセットは、認証サービス、バックアップおよびストレージ、コラボレーション アプリケーション、コンシューマブラウジング、コンシューマ ファイル シェアリング、コンシューマゲーミング、コンシューマメディア、コンシューマ misc、コンシューマ ソーシャル ネットワーキング、カスタムアプリケーション、データベース アプリケーション、デスクトップ仮想化、電子メール、企業 ipc、ファイル共有、一般的なブラウジング、一般的なメディア、一般的な misc、トンネリング、ローカルサービス、ネーミングサービス、ネットワーク制御、ネットワーク管理、リモートアクセス、saasアプリケーション、シグナリング、ソフトウェア開発ツール、ソフトウェアアップデート、ストリーミングメディアです。

ステップ 5 [Save] をクリックします。

IP アドレスおよびポートに基づくカスタムアプリケーションの作成

Catalyst Centerに存在しないアプリケーションがある場合、カスタム アプリケーションとして追加することができます。

手順

ステップ 1 メインメニューから次を選択します。**[Provision]** > **[Services]** > **[Application Visibility]** の順に選択します。

ステップ 2 [Application] タブをクリックします。

ステップ 3 [アプリケーションの追加（Add Application）] をクリックします。

ステップ 4 [Application Name] フィールドに、アプリケーションの名前を入力します。名前には、下線とハイフンも含めて最大 24 文字の英数字を指定できます。アプリケーション名で使用できる特殊文字は、下線とハイフンのみです。

ステップ 5 [種類（Type）] エリアで、[サーバー IP/ポート（Server IP/Port）] ラジオボタンをクリックして、アプリケーションが IP アドレスとポートを通じてアクセスできます。

ステップ 6 [DSCP] チェックボックスをオンにして、DSCP 値を定義します。値を定義しない場合のデフォルト値は [Best Effort] です。ベストエフォートサービスとは原則的に、いずれの QoS も適用されないネットワークデバイスのデフォルト動作です。

ステップ 7 [IP/Port Classifiers] チェックボックスをオンにして、アプリケーションの IP アドレスおよびサブネット、プロトコル、ポートまたはポート範囲を選択します。有効なプロトコルは、[IP]、[TCP]、[UDP]、[TCP/UDP] です。[IP] プロトコルを選択した場合は、ポート番号または範囲は定義しません。 をクリックして、さらに分類子を追加します。

ステップ 8 次のいずれかの方法を使用して、アプリケーション トラフィック処理要件を定義します。

- [Similar To]：お使いのアプリケーションに既存のアプリケーションと同様のトラフィック処理要件がある場合は、[Similar To] オプションボタンをクリックし、ドロップダウンリストからアプリケーションを選択します。Catalyst Center は、他のアプリケーションのトラフィッククラスを、定義しているアプリケーションにコピーします。
- [Traffic Class]：アプリケーションに定義するトラフィッククラスがわかっている場合は、[Traffic Class] オプションボタンをクリックし、ドロップダウンリストからトラフィッククラスを選択します。有効な値は BULK_DATA、TRANSACTIONAL_DATA、OPS_ADMIN_MGMT、NETWORK_CONTROL、VOIP_TELEPHONY、MULTIMEDIA_CONFERENCING、MULTIMEDIA_STREAMING、BROADCAST_VIDEO、REAL_TIME_INTERACTIVE、および SIGNALING です。

ステップ 9 [Application Set] ドロップダウンリストから、アプリケーションが属するアプリケーションセットを選択します。有効なアプリケーションセットは、認証サービス、バックアップおよびストレージ、コラボレーションアプリケーション、コンシューマブラウジング、コンシューマファイルシェアリング、コンシューマゲーミング、コンシューマメディア、コンシューマ misc、コンシューマ ソーシャル ネットワーキング、カスタムアプリケーション、データベース アプリケーション、デスクトップ仮想化、電子メール、企業 ipc、ファイル共有、一般的なブラウジング、一般的なメディア、一般的な misc、トンネリング、ローカルサービス、ネーミングサービス、ネットワーク制御、ネットワーク管理、リモートアクセス、

saasアプリケーション、シグナリング、ソフトウェア開発ツール、ソフトウェアアップデート、ストリーミングメディアです。

ステップ 10 [Save] をクリックします。

URL に基づくカスタム アプリケーションの作成

Catalyst Centerに存在しないアプリケーションがある場合、カスタム アプリケーションとして追加することができます。

手順

ステップ 1 メインメニューから次を選択します。**[Provision]** > **[Services]** > **[Application Visibility]** の順に選択します。

ステップ 2 [Application] タブをクリックします。

ステップ 3 [アプリケーションの追加（Add Application）] をクリックします。

[アプリケーションの追加（Add Application）] ダイアログボックスが表示されます。

ステップ 4 [アプリケーション名（Application Name）] フィールドに、アプリケーションの名前を入力します。名前には、下線とハイフンも含めて最大24文字の英数字を指定できます。（アプリケーション名で使用できる特殊文字は、下線とハイフンのみです。）

ステップ 5 **タイプ**については、[**URL**] オプションボタンをクリックします。

ステップ 6 [**Url**] フィールドに、アプリケーションに到達するために使用する url を入力します。

ステップ 7 トラフィック クラスの設定:

- 同様のトラフィック処理要件を持つ別のアプリケーションと同じトラフィッククラスを使用するには、オプションボタンをクリックして、ドロップダウンリストからアプリケーションを選択します。
- トラフィッククラスを指定するには、[**トラフィッククラス (Traffic class)**] オプションボタンをクリックし、ドロップダウンリストからトラフィッククラスを選択します。有効な値は BULK_DATA、TRANSACTIONAL_DATA、OPS_ADMIN_MGMT、NETWORK_CONTROL、VOIP_TELEPHONY、MULTIMEDIA_CONFERENCING、MULTIMEDIA_STREAMING、BROADCAST_VIDEO、REAL_TIME_INTERACTIVE、および SIGNALING です。

ステップ 8 [**アプリケーションセット (Application set)**] ドロップダウンリストから、アプリケーションを配置するアプリケーションセットを選択します。

ステップ 9 [Save] をクリックします。

カスタムアプリケーションの編集または削除

必要な場合は、カスタム アプリケーションを変更または削除できます。

（注） アプリケーション ポリシーによって直接参照されているカスタム アプリケーションを削除することはできません。通常、アプリケーションポリシーはアプリケーションセットを参照し、個々のアプリケーションを参照しません。ただし、ポリシーにアプリケーションの特別な定義（コンシューマまたはプロデューサの割り当てや双方向の帯域幅プロビジョニングなど）が設定されている場合、ポリシーはそのアプリケーションを直接参照します。そのため、アプリケーションを削除する前に、特別な定義を削除するか、またはアプリケーションへの参照を削除する必要があります。

手順

ステップ 1 メインメニューから次を選択します。**[Provision]** > **[Services]** > **[Application Visibility]** の順に選択します。

ステップ 2 [Application] タブをクリックします。

ステップ 3 [Search]、[Show]、または [View By] フィールドを使用して、変更するアプリケーションを見つけます。

名前、ポート番号、およびトラフィッククラスに基づいてアプリケーションを検索できます。

ステップ 4 アプリケーションを編集するには、次の手順を実行します。

a) アプリケーション名をクリックして、必要な変更を行います。フィールドの詳細については、サーバー名に基づくカスタムアプリケーションの作成（1344 ページ）、IP アドレスおよびポートに基づくカスタムアプリケーションの作成（1345 ページ）、またはURL に基づくカスタム アプリケーションの作成（1346 ページ）を参照してください。

b) [Save] をクリックします。

または、アプリケーションを選択し、[Actions] ドロップダウンリストから [Edit] をクリックしてアプリケーションを編集します。

（注） ポリシーを再展開しても、編集したカスタムアプリケーションは再設定されません。Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ

ステップ 5 アプリケーションを削除するには、アプリケーションボックスにある  をクリックし、次に [OK] をクリックして確定します。

または、次の手順を実行してアプリケーションを削除することもできます。

a) アプリケーション名の横にあるチェックボックスをオンにします。複数のアプリケーションを選択することもできます。

b) [Actions] ドロップダウンリストから、[Delete] オプションをクリックします。

c) [OK] をクリックして確定します。

アプリケーションをお気に入りにする

アプリケーションをお気に入りとしてマークして、アプリケーションの QoS 設定を、他のアプリケーションの QoS 設定の前にデバイスに展開する必要あることを指定できます。お気に入りとしてマークされたアプリケーションには、その横に黄色の星が付いています。

ポリシーを追加または編集すると、お気に入りとしてマークされたアプリケーションがアプリケーションセットの上部に表示されます。

アプリケーションは、個々のポリシーベースではなくシステム全体で設定されます。詳細については、「お気に入りのアプリケーション （1342 ページ）」を参照してください。

手順

ステップ 1 メインメニューから次を選択します。**[Provision]** > **[Services]** > **[Application Visibility]** の順に選択します。

ステップ 2 [Application] タブをクリックします。

ステップ 3 お気に入りとしてマークするアプリケーションを特定します。

ステップ 4 スターアイコンをクリックします。

カスタム アプリケーション セットの作成

使用したいアプリケーションセットがない場合、カスタム アプリケーション セットを作成できます。

手順

ステップ 1 メインメニューから次を選択します。**[Provision]** > **[Services]** > **[Application Visibility]** の順に選択します。

ステップ 2 [Application Sets] タブをクリックします。

ステップ 3 [Add Application Set] をクリックします。

ステップ 4 スライドインペインに、新しいアプリケーション設定の名前を入力します。

Catalyst Center で新しいアプリケーションセットが作成されますが、アプリケーションは含まれません。

ステップ 5 ドロップダウンリストから [Default Business Relevance] を選択します。デフォルトのビジネス関連性（Default Business Relevance）は、具体的なアプリケーション QoS がない場合のビジネス関連性レベルです。このレベルは、ポリシーに割り当てられていないサイトのAssuranceに表示されます。

ステップ 6 [Save] をクリックします。

ステップ 7 [Search] を使用して [Show] または [View By] フィールドを使用して、アプリケーション設定を見つけます。

名前、ポート番号、およびトラフィッククラスに基づいてアプリケーションを検索できます。

ステップ 8 新しいアプリケーション設定に移動させるアプリケーションを見つけます。

ステップ 9 移動させるアプリケーションの横にあるチェック ボックスをオンにします。

ステップ 10 新しいアプリケーション設定にアプリケーションをドラッグ アンド ドロップします。

カスタム アプリケーション セットの編集または削除

必要な場合は、カスタム アプリケーションを変更または削除できます。



（注） アプリケーション ポリシーによって参照されているカスタム アプリケーション セットを削除することはできません。アプリケーション セットを削除する前に、ポリシーからアプリケーション セットを削除する必要があります。

手順

ステップ 1 メインメニューから次を選択します。**[Provision]** > **[Services]** > **[Application Visibility]** の順に選択します。

ステップ 2 [Application Sets] タブをクリックします。

ステップ 3 [検索（Search）]、[表示（Show）]、または [表示方法（View By）] フィールドを使用して、変更するアプリケーション セットを見つけます。

名前、ポート番号、およびトラフィッククラスに基づいてアプリケーションを検索できます。

ステップ 4 次のいずれか 1 つのタスクを実行します。

- アプリケーション設定するには、アプリケーション設定に、またはアプリケーション設定からアプリケーションをドラッグアンドドロップします。[OK] をクリックして、それぞれの変更を確定します。
- アプリケーション設定を削除するには、アプリケーション設定ボックスにある をクリックし、次に [OK] をクリックして確定します。

未分類アプリケーションの検出

Catalyst Center のアプリケーション可視性サービスは、分類済みと未分類のドメインおよびソケットに関する情報をデバイスから取得し、その情報を [Observed Traffic] チャートに表示します。アプリケーション可視性サービスによって検出された未分類のサーバー名と IP/ポートの数は、[Recommendations] の下に表示されます。

未分類のサーバー名と IP/ポートはアプリケーションレジストリに追加できます。



（注） 最大 1100 の検出されたアプリケーションをアプリケーションレジストリに追加できます。

手順

ステップ 1 メインメニューから次を選択します。**[Provision]** > **[Services]** > **[Application Visibility]** の順に選択します。

ステップ 2 [CBAR Extensions] > [Discovered Applications] タブをクリックします。

ステップ 3 表に、未分類の検出されたサーバーまたはIP/ポートのリストが表示されます。表内で選択したサーバーまたはIP/ポートを非表示にする場合は、サーバーを選択して [Hide Ignored Applications] チェックボックスをオンにします。

ステップ 4 アプリケーションレジストリでアプリケーションとしてインポートするサーバーまたはIP/ポートを選択します。

ステップ 5 ドロップダウンリストから、必要な [Application]、[Application Set]、および [Traffic Class] を選択します。

ステップ 6 [Import] をクリックします。

ステップ 7 [Applications] タブをクリックし、[Show] ドロップダウンリストから [Discovered] を選択して、インポートされたアプリケーションを表示します。

Catalyst Center トラフィック テレメトリ アプライアンス のアプリケーション可視性サービスのサポート

Catalyst Center トラフィック テレメトリ アプライアンスは、ミラーリングされた IP ネットワークトラフィックからエンドポイントテレメトリを生成し、エンドポイントの可視性とセグメンテーションのために Catalyst Center とテレメトリデータを共有します。

Catalyst Center トラフィック テレメトリ アプライアンスで CBAR を有効にするための前提条件には、次のものが含まれます。

- デバイスをサイトに割り当てる必要があります。
- デバイスロールを [Distribution] モードに設定する必要があります。

QoS ポリシーを設定せずに、Catalyst Center トラフィック テレメトリ アプライアンス で属性セットとマップを使用してカスタムアプリケーションを設定することができます。詳細については、アプリケーションポリシーの作成（1470ページ）およびアプリケーションポリシーの展開 （1476 ページ）を参照してください。

Infoblox アプリケーションの検出

Catalyst Center を組織の Infoblox DNS サーバーと統合して、未分類のトラフィックをサーバー名に基づいて解決することができます。

始める前に

- バージョン 1.5 以降の Infoblox WAPI が必要です。Infoblox WAPI のバージョンを確認するには、Infoblox サーバーにログインし、**[Help]** > **[Documentation]** > **[WAPI Documentation]** の順に選択します。
- 少なくとも読み取り専用権限を持つロールを作成し、そのロールを Infoblox ユーザーに割り当てます。詳細については、*Cisco Catalyst Center* 管理者ガイド [英語] の「Manage Users」を参照してください。

手順

ステップ 1 メインメニューから次を選択します。**[Provision]** > **[Services]** > **[Application Visibility]** の順に選択します。

ステップ 2 [CBAR Extensions] > [Infoblox] タブをクリックします。

ステップ 3 [Infoblox] の [Here] リンクをクリックして、Catalyst Center で IPAM/DNS サーバーのログイン情報を設定します。

ステップ 4 IPAM の設定を行います。詳細については、*Cisco Catalyst Center* 管理者ガイド [英語] の「Configure an IP Address Manager」を参照してください。

ステップ 5 [Infoblox] に戻り、⚙ アイコンをクリックして次の設定を完了します。

- [All DNS Zones] チェックボックスをオンにするか、[DNS Zones to Inspect] ドロップダウンリストから必要な DNS ゾーンを選択します。ドロップダウンリストには、Infoblox サーバーで定義されている DNS ゾーンが表示されます。
- [Inspect] ドロップダウンリストから必要な検査レコードを選択します。
- [Read Application name from] チェックボックスをオンにし、[Extensible Attribute] または [AVC RRTYPE format] のいずれかのオプションボタンをクリックします。[Extensible Attribute] オプションボタンをクリックした場合は、わかりやすいアプリケーション名を含む拡張機能属性名を入力します。
- [Default Traffic Class] から、Infoblox アプリケーションを分類するためのデフォルトのトラフィッククラスを選択します。
- [Default Application Set] から、Infoblox アプリケーションを分類するためのデフォルトのアプリケーションセットを選択します。

ステップ 6 **[保存（Save）]** をクリックします。

ステップ 7 インポートするアプリケーションを選択し、次のタスクを完了します。

- アプリケーションの名前が Infoblox サーバーで定義された名前と異なる場合は、アプリケーション名を編集します。
- [Infoblox] に定義されているデフォルトのアプリケーションセットとトラフィッククラスを変更する場合は、ドロップダウンリストから必要なアプリケーションセットとトラフィッククラスを選択します。

ステップ 8 [Import] をクリックします。

ステップ 9 [Applications] タブをクリックして [Show] ドロップダウンリストから [Discovered] を選択し、インポートされた Infoblox アプリケーションを確認して必要に応じて編集します。

アプリケーションのインポート後にアプリケーションのサーバー名を変更すると、[Infoblox] ウィンドウの [Application Status] 列に、アプリケーションのステータスが [Updated] と表示されます。[Application Status] 列に表示されるアプリケーション名は、アプリケーションの新しいサーバー名です。アプリケーションの古いサーバー名を表示するには、情報アイコンをクリックします。

検出されたアプリケーションの編集と削除

必要に応じて、検出されたアプリケーションを編集または削除できます。

手順

ステップ 1 メインメニューから次を選択します。**[Provision]** > **[Services]** > **[Application Visibility]** の順に選択します。

ステップ 2 [アプリケーション（Applications）] タブをクリックします。

ステップ 3 [Search]、[Show]、[View By] のいずれかのフィールドを使用して、変更する検出済みのアプリケーションを見つけます。

名前、ポート番号、およびトラフィッククラスに基づいてアプリケーションを検索できます。

ステップ 4 次のいずれか 1 つのタスクを実行します。

- アプリケーションを編集するには、次の手順を実行します。
  1. アプリケーション名をクリックして、必要な変更を行います。

     検出済みのアプリケーションの場合、[Attribute Set] と [Traffic Class] のみを編集できます。
  2. [Save] をクリックします。
- アプリケーションを削除するには、次の手順を行います。
  1. アプリケーションを選択し、ウィンドウの上部にある [アクション（Action）] ドロップダウンリストから [削除（Delete）] オプションを選択します。
  2. 次にウィンドウに表示される警告ダイアログボックスで [OK] をクリックします。

アプリケーション ホスティング

ここでは、アプリケーション ホスティングについて説明します。

アプリケーション ホスティングについて

アプリケーション ホスティングを使用すると、Catalyst Center によって管理されているデバイス上のサードパーティ製アプリケーションのライフサイクルを管理できます。

次のプラットフォームでサードパーティの Docker アプリケーションをホストできます。

- Cisco Catalyst 9300 シリーズ スイッチ（Cisco IOS-XE ソフトウェアバージョン 16.12.1s 以降）。
- Cisco Catalyst 9100 シリーズ アクセスポイント（Cisco IOS-XE ソフトウェアバージョン 17.3.1 以降）。
- Cisco Catalyst 9400 シリーズ スイッチ（Cisco IOS-XE ソフトウェアバージョン 17.1 以降）。
- Cisco Catalyst IE3200、IE3300（4 GB）、IE3400、IE3400H シリーズ スイッチ（Cisco IOS-XE ソフトウェアバージョン 17.3 以降）。
- Cisco Catalyst IE3100 および IE 3105 高耐久性シリーズ スイッチ（Cisco IOS-XE ソフトウェアバージョン 17.15 以降）。
- Cisco Catalyst IE9300 シリーズ スイッチ（Cisco IOS-XE ソフトウェアバージョン 17.9 以降）。

（注）
- Catalyst Center では、ホストされるアプリケーションに割り当てられるディスク容量は 5 GB に制限されています。
- アプリケーション ホスティングは、モビリティエージェント（MA）、N+1 冗長性、または高可用性（HA）構成をサポートしていません。この機能を使用して展開されたアプリケーションは、特定のホストデバイスにバインドされます。そのため、冗長ハードウェアに自動的に移行したり、デバイスの障害やメンテナンスイベント中にフェールオーバーしたりすることはありません。高可用性を必要とする重要なサービスは、専用インフラストラクチャでホストされるようにします。

有線またはワイヤレス ワークフロー オプションでは、次のナビゲーションパスを使用できます。

- 有線/スイッチライフサイクル：**[プロビジョニング（Provision）]**>**[サービス（Services）]**>**[アプリケーションホスティング（Application Hosting）]** の順に移動します。
- ワイヤレス/AP ライフサイクル：**[プロビジョニング（Provision）]**>**[サービス（Services）]**>**[IoTサービス（IoT Services）]** の順に移動します。

アプリケーション ホスティング サービス パッケージのインストールと更新

始める前に

SUPER-ADMIN-ROLE 権限を持つユーザのみがこの手順を実行することができます。

手順

ステップ 1 メインメニューから次を選択します。**[System]** > **[Software Management]** の順に選択します。または、クラウドアイコンをクリックし、[ソフトウェア管理に移動（Go to Software Management）] リンクをクリックします。

ステップ 2 [リリースで使用可能なアプリケーション（Available Application for the release）] で、[アプリケーションホスティングパッケージ（Application Hosting package）] を選択し、[インストール（Install）] をクリックします。

アプリケーションホスティングの前提条件

Cisco Catalyst 9000 デバイスでアプリケーションホスティングを有効にするには、次の前提条件を満たしている必要があります：

- ディスカバリの前に、デバイスの NETCONF ポートを設定します。
- アプリケーションをホストするデバイスでセキュア HTTP サーバーを設定します。

  セキュア HTTP サーバーを無効にすると、デバイスが Catalyst Center で [準備中（Not Ready）] と表示され、アプリケーションのインストールなどのアプリケーションホスティング操作が失敗することがあります。
- デバイス上の HTTPS ユーザー認証用にローカルまたは AAA 認証サーバーを設定します。ユーザー名およびパスワードは特権レベル 15 で設定する必要があります。
- Cisco Catalyst 9300 シリーズ スイッチが Cisco IOS XE 16.12.x 以降のバージョンを実行し、Cisco Catalyst 9400 シリーズ スイッチが Cisco IOS XE 17.1.x 以降のバージョンを実行していることを確認します。
- デバイスに着脱可能な USB SSD 外部ストレージがあることを確認します（9300 ファミリのスイッチの場合のみ）。
- スイッチ上の設定が正しいことを確認します。スイッチで WebUI を開き、HTTPS ユーザーとしてログインします。Catalyst Center

  次の例は、スイッチの動作設定を示しています。

```
prompt# sh run | sec ip http
ip http server
```

```
ip http authentication local
ip http secure-server
ip http max-connections 16
ip http client source-interface GigabitEthernet0/0
```

17.3 より前のリリースの Cisco IOS XE を搭載するスイッチの追加設定：

```
ip http secure-active-session-modules dnac
ip http session-module-list dnac NG_WEBUI
ip http active-session-modules none
```

- Catalyst Center で、デバイスを手動で追加するときに HTTPS ログイン情報を設定します。アプリケーション ホスティングには、HTTPS ユーザー名、パスワード、およびポート番号が必須です。デフォルトのポート番号は 443 です。デバイスログイン情報を編集することもできます。ネットワーク デバイス クレデンシャルの更新（164 ページ）を参照してください。すでに管理されているデバイスを編集する場合は、インベントリでそのデバイスを再同期してから、アプリケーション ホスティング関連のアクションに使用します。

次のチェックを使用してログイン情報の不一致または準備の失敗をトラブルシュートします。

- HTTPS ポート設定とユーザー権限レベルを検証します。
- インベントリデータベースのログイン情報を更新します。
- デバイスを再同期して準備状況チェックを再実行します。
- 一般的な準備失敗コードを解釈してそれらに対処します。

（注）
- アプリケーション ホスティングの HA は、3 ノードの Catalyst Center クラスタではサポートされていません。
- アプリケーション ホスティングは、返品許可（RMA）ワークフローをサポートしていません。

アプリケーションをホストするデバイスの準備状況の表示

スイッチにアプリケーションをインストールする前に、Cisco Catalyst 9300 シリーズ スイッチのアプリケーションをホスティングするための準備状況を確認する必要があります。

手順

ステップ 1 メインメニューから次を選択します。**[Provision]** > **[Services]** > **[Application Hosting]**

ステップ 2 [All Devices] をクリックします。

ステップ 3 アプリケーションをホストできるデバイスのリストが表示されます。[App Hosting Status] は、デバイスがアプリケーションをホストするための準備状況を示します。[See Details] をクリックして、デバイスで実行された準備状況チェックのリストを表示します。

アプリケーション ホスティングの準備状況チェック

準備状況チェックは、診断デバイスの適格性検証であり、次のことを行います。

- ネットワークデバイスがアプリケーションホスティング操作に適しているかどうかを確認します。
- 展開の失敗を減らすために、すべての前提条件が満たされていることを確認します。
- デバイスの準備状況を示す結果ステータスである、[成功（Passed）]、[失敗（Failed）]、または [スキップ（Skipped）] を表示します。

スイッチチェックには、標準アプリケーションホスティング基準とスイッチ固有のインタラクティブな HTTPS 検証が含まれます。

アクセスポイント（AP）チェックには、HTTP または HTTPS ログイン情報が必要です。これらのチェックでは、HTTPS クレデンシャルの検証は、個別の準備状況チェックとして表示されません。

スイッチと AP の両方に関する特定の準備状況チェックには、以下が含まれます。

1. HTTPS ログイン情報がインベントリに入力されているか。
2. IOS-XEバージョンがアプリケーション ホスティングをサポートしているか。
3. アプリケーション ホスティングがデバイスと同期しているか。
4. アプリケーション ホスティングがインベントリと同期しているか。
5. インベントリでデバイスが管理対象状態になっているか。
6. デバイスシリーズが Catalyst Center のアプリケーション ホスティングでサポートされているか。
7. HTTPS ユーザー名がデバイスに設定されているか。
8. デバイスにセキュアな HTTP サーバが設定されているか。

表 *56 :* スイッチ固有のインタラクティブな *HTTPS* 検証

Check	操作
HTTPS ログイン情報は有効か	UI に用意されている [ここをクリック（Click here）] リンクを使用して、デバイス用に設定されている HTTPS ログイン情報を検証します。

AP 固有の考慮事項

すべての AP ワークフローに、HTTP または HTTPS の前提条件が必要です。

インタラクティブな HTTPS ログイン情報は有効かのチェックは、AP の別個の準備状況行として表示されません。

各準備状況チェックは、次のいずれかのステータスを返します。

- [成功（Passed）]：チェックが正常に完了し、条件が満たされました。
- [失敗（Failed）]： 条件が満たされていないため、修正処置が必要です。
- [スキップ（Skipped）]：現在のコンテキストにチェックを適用できないか、手動の検証トリガーが必要です。

準備状況チェック結果をトラブルシュートするための運用ガイドラインは、次のとおりです。

- [アプリケーションホスティングがデバイスと同期しているか（Is App Hosting in Sync with the Device）]が、検出処理中メッセージが原因で[失敗（Failed）]ステータスを返す場合。プロセスが完了するのを待ってから、再試行してください。
- [アプリケーションホスティングがデバイスと同期しているか（Is App Hosting in Sync with the Device）]が[スキップ（Skipped）]ステータスを返し、インフラストラクチャが有効になっていないことを示すメッセージが表示されたら、インストールを続行します。インフラストラクチャが有効になり、チェックが再実行されます。
- チェックが失敗し続ける場合、インベントリから再同期を実行して、準備状態を再チェックします。

選択したアプリケーションのデバイスとステータスの表示

選択したアプリケーションがインストールされているすべてのデバイスを表示するには、次の手順を実行します。また、各デバイスにおける現在のアプリケーションの状態を監視することもできます。**[アプリケーション（App）]**>**[管理（Manage）]**のアプリケーション中心のビューは、**[すべてのデバイス（All Devices）]**>**[デバイスの選択（Select Device）]**>**[インストールされているアプリケーションの表示（View Installed Apps）]**のデバイス中心のワークフローを補完します。

Before you begin

次の要件が満たされていることを確認する必要があります。

- スイッチの場合、アプリケーションホスティングサービスを有効にする必要があります。
- AP の場合、IoT サービスを有効にする必要があります。
- アプリケーションを Catalyst Center に正常にアップロードする必要があります。

- アプリケーションは、少なくとも1台のターゲットデバイスにインストールする必要があります。

手順

ステップ1 メインメニューから次を選択します。 次のいずれかのパスを選択します。

- スイッチ：**[プロビジョニング（Provision）]** > **[サービス（Services）]** > **[アプリケーションホスティング（Application Hosting）]** の順に移動します。
- アクセスポイント：**[プロビジョニング（Provision）]** > **[サービス（Services）]** > **[IoTサービス（IoT Services）]** の順に移動します。

ステップ2 リストから必要なアプリケーションを選択します。

ステップ3 [Manage] をクリックします。

ステップ4 [デバイス（Devices）] ビューで、各デバイスのアプリケーションのステータスを確認します。

ステップ5 必要に応じて、[すべて（ALL）]、[実行中（RUNNING）]、[停止（STOPPED）]、[失敗（FAILED）]、[進行中（IN-PROGRESS）] などのステータスフィルタを使用して結果を絞り込みます。

ステップ6 [概要（Summary）] をクリックし、すべてのデバイスの選択したアプリケーションのステータス概要を表示します。

ステップ7 1つ以上のデバイスを選択し、[アクション（Actions）] を使用してライフサイクル操作を実行します。

ステップ8 デバイスの [ホスト名（Hostname）] をクリックし、デバイスレベルのアプリケーションビューを開きます。

各デバイスの [管理（Manage）] ビューに次の情報が表示されます。

- [ホスト名（Hostname）]：デバイスの名前。
- [デバイスIP（Device IP）]：デバイスの IP アドレス。
- [アプリケーションバージョン（App Version）]：現在インストールされているアプリケーションのバージョン。
- [アプリケーションステータス（App Status）]：アプリケーションの現在の動作状態。
- [最後に検知（Last Heard）]：デバイスからの最後の通信に関するタイムスタンプ。
- [アクションステータス（Action Status）]：アプリケーションで実行された最新のライフサイクル操作のステータス。

アプリケーションの追加

シスコパッケージまたは Docker アプリケーションを追加できます。

始める前に

- [Cisco Package]：IOS SDK ツールを使用してアプリケーションをパッケージ化し、アプリケーションが IOS XE オペレーティングシステムと互換性を持つようにする必要があります。
- [Docker]：Docker イメージを tar ファイルとして保存する必要があります。Docker イメージを tar ファイルとして保存するには、次のコマンドを入力します。

```
docker save -o <path for generated tar file> <image name:tag>
Example: docker save -o alpine-tcpdump.tar itsthenetwork/alpine-tcpdump:latest
```

（注） 詳細については、「Cisco Package Format」と「Docker Save Command」を参照してください。

手順

ステップ 1 **[Provision]** > **[Services]** > **[Application Hosting]**メインメニューから次を選択します。。

ステップ 2 [New Application] をクリックします。

ステップ 3 ドロップダウンリストからアプリケーションとカテゴリを選択します。

ステップ 4 [Select] をクリックして、アップロードするアプリケーションを選択します。

アップロードダイアログでは、アップロード要求を開始する前に、ファイルが .tar または .tar.gz 形式であり、2 GB を超えていないことを検証します。

ステップ 5 [Upload] をクリックします。

新しく追加されたアプリケーションは、[App Hosting] ページで確認できます。

ThousandEyes Enterprise Agent アプリケーションの自動ダウンロード

ThousandEyes Enterprise Agent アプリケーションを使用すると、ネットワークをモニターし、内部、外部、キャリア、およびインターネットネットワーク全体のネットワーク トラフィック パスをリアルタイムで監視できます。ThousandEyes Enterprise Agent アプリケーションの利点は、Catalyst Center アプリケーション ホスティング サービスにこのアプリケーションを手動でインポートする必要がないことです。

これらの条件が満たされると、アプリケーション ホスティング サービスの開始から 10 分以内に、ThousandEyes Enterprise Agent アプリケーションが自動的にダウンロードされます。

- 少なくとも 1 つの管理対象デバイスがインベントリ内に存在し、管理性エラーがない。
- 管理対象デバイスでインベントリの再同期に少なくとも 1 回成功している。

アプリケーションを手動でダウンロードするには、ThousandEyes Enterprise Agent .tar ファイルへの次のリンクをクリックします。

thousandeyes-enterprise-agent.cat9k.tar

インターネット接続がない場合は、次のコマンドを使用してコンソールからプロキシ接続を設定できます。

```
magctl service setenv app-hosting http_proxy <proxy-value>
```

ThousandEyes Enterprise Agent アプリケーションに接続するプロキシ値を設定します。

Catalyst Center は、CPU アーキテクチャ全体で ThousandEyes のマルチバリアント アプリケーション パッケージをサポートしています。ThousandEyes の場合、Catalyst Center は、x86_64 や aarch64 など、同じアプリケーションファミリのアーキテクチャ固有のバリアントを認識できます。インストールまたはアップグレード中にデバイスごとに適切なバリアントを自動的に解決し、バリアントを認識したライフサイクル運用を提供します。

アプリケーションの更新

Catalyst Center で追加されたアプリケーションを更新できます。

手順

ステップ 1 **[Provision]** > **[Services]** > **[Application Hosting]**メインメニューから次を選択します。。

使用可能なアプリケーションは、[App Hosting] ウィンドウで確認できます。

ステップ 2 更新するアプリケーションを選択します。

ステップ 3 [Update App] をクリックします。

ステップ 4 アップロードする新しいバージョンのアプリケーションを選択します。

ステップ 5 [Upload] をクリックします。

アプリケーションの起動

Catalyst Center でアプリケーションを起動できます。

手順

ステップ 1 **[Provision]** > **[Services]** > **[Application Hosting]**メインメニューから次を選択します。。

ステップ 2 アプリケーションを選択し、[Manage] をクリックして、アプリケーションを使用するデバイスを表示します。

ステップ 3 起動するアプリケーションがあるデバイスを選択します。

ステップ 4 [Actions] ドロップダウンリストから [Start App] を選択します。

アプリケーションの停止

Catalyst Center でアプリケーションを停止できます。

手順

ステップ 1 **[Provision]** > **[Services]** > **[Application Hosting]**メインメニューから次を選択します。。

ステップ 2 アプリケーションを選択し、[Manage] をクリックして、アプリケーションを使用するデバイスを表示します。

ステップ 3 停止するアプリケーションがあるデバイスを選択します。

ステップ 4 [Actions] ドロップダウンリストから [Stop App] を選択します。

デバイスでホストされているアプリケーションの表示

始める前に

「アプリケーション ホスティングの前提条件」の前提条件を満たします。

手順

ステップ 1 **[Provision]** > **[Services]** > **[Application Hosting]**メインメニューから次を選択します。。

ステップ 2 すべてのデバイスを表示するには、右上隅の [All Devices] をクリックします。特定のアプリケーションを使用するデバイスのみを表示するには、アプリケーションを選択して [Manage] をクリックします。

すべてのデバイスを表示することを選択した場合、[すべてのデバイス（All Devices）] ウィンドウには、アプリケーションをホストできるデバイスに関する情報（[ホスト名（Hostname）]、[IPアドレス（IP Address）]、[イメージバージョン（Image Version）]、[アプリケーションホスティングステータス（App Hosting Status）]、[最終更新日（Last Updated）] など）が表示されます。

特定のアプリケーションのデバイスリストを表示することを選択した場合、[デバイス（Devices）] ウィンドウには、アプリケーションをホストできるデバイスに関する情報（[ホスト名（Hostname）]、[デバイス IP（Device IP）]、[アプリケーションバージョン（App Version）]、[アプリケーションステータス（App Status）]、[最後に検知したプラットフォームバージョン（Last Heard, Platform Version）]、[アクションステータス（Action Status）] など）が表示されます。

ステップ 3 [Devices] ウィンドウで [Summary] をクリックすると、デバイス上で失敗または停止したアプリケーション、および実行中のアプリケーションの概要が表示されます。

ステップ 4 アプリケーションでアクションを実行するには、[Action] ドロップダウンリストをクリックし、[Start]、[Stop]、[Edit]、[Upgrade]、または [Uninstall] を選択します。

ステップ 5 インストールされているホスティング アプリケーションを表示するデバイスリンクをクリックします。

[Applications] ウィンドウには、インストールされているアプリケーションの**名前**、**バージョン**、**アプリケーションステータス**、**モニタリング アプリケーション**、**正常性**、および**詳細情報**が表示されます。

（注） **モニタリングアプリケーション**には、アプリケーション モニタリング ダッシュボードへのリンクが含まれています。このリンクは、the Catalyst Center application package controller .yaml ファイルで提供されます。このファイルにアプリケーション ダッシュボード URL が含まれていない場合、**モニタリングアプリケーション**の列（[Monitor App]）は適用されません。

ステップ 6 [Details] 列で [View] をクリックすると、デバイスのアプリケーションステータスに関する詳細情報が表示されます。

ステップ 7 特定のアプリケーションのログをダウンロードするには、アプリケーションを選択して [Application Logs] をクリックします。

ステップ 8 デバイスからテクニカルサポートログをダウンロードするには、[Tech Support logs] をクリックします。

アプリケーションホスティングを使用したアプリケーションのインストール

Catalyst Center を使用すると、スイッチにアプリケーションをインストールできます。サポートされているスイッチの詳細については、「アプリケーション ホスティングについて （1353 ページ）」を参照してください。

始める前に

- 前提条件を満たします。詳細については、アプリケーションホスティングの前提条件（1354 ページ） を参照してください。
- アプリケーションを Catalyst Center に追加します。詳細については、アプリケーションの追加 （1358 ページ） を参照してください。
- アプリケーションをホストするためのスイッチの準備状況を確認します。詳細については、アプリケーションをホストするデバイスの準備状況の表示（1355 ページ） を参照してください。

手順

ステップ 1 **[Provision]** > **[Services]** > **[Application Hosting]**メインメニューから次を選択します。。

ステップ 2 アプリケーションを選択し、[Install] をクリックします。

ステップ 3 [Get Started] ウィンドウで、[Task Name] フィールドにワークフローの一意の名前を入力し、[Next] をクリックします。

ステップ 4 [Select Site] ウィンドウで、アプリケーションを有効にするサイトを選択し、[Next] をクリックします。

ステップ 5 [Select Switches] ウィンドウで、アプリケーションのインストール先デバイスを選択し、[Next] をクリックします。

ステータスが [Ready] および [Partially Ready] のデバイスを選択できます。[See Details] をクリックして、デバイスで実行された準備状況チェックのリストを表示します。

[Partially Ready] ステータスのデバイスの場合は、[Readiness Check] ウィンドウの [Check Now] リンクをクリックして、HTTPS ログイン情報を検証します。

[Devices] テーブルに目的のデバイスがない場合は、[Import] をクリックして CSV ファイルからデバイスを追加します。

ステップ 6 [設定アプリ（Configuration App）] ウィンドウで、次の設定を実行します。

- **[Network Settings]**：
  - [アプリケーションネットワーク（App-Network）] ドロップダウンリストから、アプリケーションを設定する VLAN を選択します。
  - [Address Type] ドロップダウンリストから [Static] または [Dynamic] を選択します。[静的（Static）] を選択した場合は、[エクスポート（Export）] をクリックして CSV テンプレートをダウンロードします。CSV テンプレートに詳細を入力します。[インポート（Import）] をクリックして CSV ファイルをアップロードします。[動的（Dynamic）] を選択した場合は、アプリケーションの [IPアドレス（IP Address）]、[ゲートウェイ（Gateway）]、[プレフィックス/マスク（Prefix/Mask）]、および [DNS] を入力します。
- [App Resources]：[Allocate all resources available on a device] または [Customize resource allocation] チェックボックスをオンにします。[Customize resource allocation] チェックボックスをオンにすると、[CPU]、[Memory]、および [Persistent Storage] の最大値を低い値に変更できます。
- [Custom Settings]：シスコ パッケージ アプリケーションにのみ適用されます。アプリケーションによって指定された属性の設定の詳細を入力します。
- [App Data]：アプリケーション固有のファイルを参照してアップロードします。必要なアプリケーション固有のファイルの特定方法については、関連するアプリケーションのドキュメントを参照してください。
- [Docker Runtime Options]：アプリケーションに必要な Docker ランタイムオプションを入力します。

ステップ 7 [Summary] ウィンドウで、アプリケーション構成の設定を確認します。

ステップ 8 （任意） [Configuration Preview] をクリックし、選択したデバイスに設定をプッシュするために使用される設定テンプレートを確認します。

ステップ 9 [Provision] をクリックします。

ステップ 10 確認ウィンドウで [Yes] をクリックして、選択したデバイスでのアプリケーションのインストールを完了します。

（注） アプリケーションをインストールすると、デバイスの Cisco IOS-XE 設定も変更されます。実行中の設定に対するこの変更は、ルータのリロード後にアプリケーションが期待どおりに機能するように、スタートアップ設定にコピーする必要があります。アプリケーションのインストールが完了したら、[CLI Templates] を使用して実行中の設定をスタートアップ設定にコピーします。

CSV ファイルを使用したアプリケーションの一括インストール

Catalyst Center では、複数の AP でのアプリケーションの一括インストールが可能になります。

デバイス IP のリストを含む CSV ファイルをインポートし、アプリケーションのインストールを単一のワークフローで続行できます。

始める前に

- Cisco Catalyst 9100 シリーズ アクセスポイントを検出するには、NETCONF を有効にし、ポートを 830 に設定します。
- Cisco Catalyst 9100 シリーズ アクセスポイントで IP が Catalyst Center に直接到達できることを確認します。
- Cisco Catalyst 9800 シリーズ ワイヤレス コントローラで Cisco IOS XE 17.3.x 以降のソフトウェアが実行されていることを確認します。
- Catalyst Center アプライアンスが最新の Catalyst Center ISO を実行していることを確認します。
- USB ドングルが AP に挿入されていることを確認します。

手順

ステップ 1 メインメニューから次を選択します。**[Provision]** > **[Services]** > **[IoT Services]** の順に選択します。

ステップ 2 AP にインストールするアプリケーションをクリックします。

ステップ 3 [Install] をクリックします。

ステップ 4 [開始（Get Started）] ウィンドウで、タスクの名前を入力し、[次へ（Next）] をクリックします。

ステップ 5 [入力元の選択（Input Source Selection）] ウィンドウで、[CSVアップロード（CSV Upload）] をクリックします。

ステップ 6 [サンプルCSVテンプレート（Sample CSV Template）] をクリックして、ファイルテンプレートをダウンロードします。

ステップ 7 デバイス IP のリストを追加します。または、インベントリから AP の詳細をエクスポートします。

- アプリケーションの一括インストール用に、単一の CSV ファイルで最大 500 個の AP IP アドレスのアップロードがサポートされます。
- CSV アップロードの制限を超える大規模な AP 展開、または展開リスクを管理するために、単一の大規模な一括アップロードではなく、フェーズ展開をバッチで実行することを推奨します。

ステップ 8 CSV ファイルをアップロードするには、次のいずれかのオプションを使用します。

- ドラッグ アンド ドロップ エリアにファイルをドラッグ アンド ドロップします。
- [ファイルを選択（Choose a file）] と表示されている場所をクリックし、ファイルを選択します。

ステップ 9 成功メッセージを展開して IP アドレス検証の詳細を表示し、[次へ（Next）] をクリックします。

重複する IP はウィンドウの下部に表示されます。すべてのデバイス IP のプレビューは、ウィンドウの右側に表示されます。

ステップ 10 [アクセスポイントの選択（Select Access Points）] ウィンドウで、アプリケーションをホストする AP を選択し、[次へ（Next）] をクリックします。

アップロードされた CSV ファイル内の無効な IP の数が表示されます。[IPの表示（View IPs）] をクリックすると、無効な IP を表示できます。

ステップ 11 [アプリケーションの設定（Configure App）] ウィンドウで、アプリケーション固有の設定を行い、[次へ（Next）] をクリックします。

ステップ 12 [概要（Summary）] ウィンドウでアプリケーションの展開設定を確認し、[プロビジョニング（Provision）] をクリックします。

設定を変更する場合は、[編集（Edit）] をクリックして必要な変更を加えます。

ステップ 13 [Track Provisioning Status] ウィンドウで展開の進捗状況を追跡できます。[View Details] をクリックして、プロビジョニングステータスを確認し、[Next] をクリックします。

ステップ 14 タスク完了Task Completed] ウィンドウが表示されます。[Manage IoT Application] をクリックして、Day-*N* タスクを実行します。

Cisco Catalyst 9300 デバイスからのアプリケーションのアンインストール

Cisco Catalyst 9300 シリーズ スイッチからアプリケーションをアンインストールできます。

手順

ステップ 1 **[Provision]** > **[Services]** > **[Application Hosting]**メインメニューから次を選択します。。

ステップ 2 アプリケーションを選択し、[Manage] をクリックして、アプリケーションを使用するデバイスを表示します。

ステップ 3 アンインストールするアプリケーションがあるデバイスを選択します。

ステップ 4 [Actions] ドロップダウンリストから [Uninstall App] を選択します。

Cisco Catalyst 9300 デバイスでのアプリケーション設定の編集

アプリケーションに package_config.ini ファイルが含まれており、Cisco Catalyst 9300 シリーズスイッチで稼働させるための設定が必要な場合は、アプリケーション設定を編集できます。

手順

ステップ 1 **[Provision]** > **[Services]** > **[Application Hosting]**メインメニューから次を選択します。。

ステップ 2 アプリケーションを選択し、[Manage] をクリックして、アプリケーションを使用するデバイスを表示します。

ステップ 3 編集するアプリケーションがあるデバイスを選択します。

ステップ 4 [Actions] ドロップダウンリストから、[Edit App Config] を選択します。

アプリケーションの削除

Catalyst Center からアプリケーションを削除できます。

始める前に

アプリケーションを使用しているすべてのデバイスからアプリケーションをアンインストールする必要があります。詳細については、Cisco Catalyst 9300 デバイスからのアプリケーションのアンインストール （1365 ページ）を参照してください。

手順

ステップ 1 **[Provision]** > **[Services]** > **[Application Hosting]**メインメニューから次を選択します。。

ホストされている削除可能なアプリケーションは、[App Hosting] ウィンドウで確認できます。

ステップ 2 削除するアプリケーションを選択します。

ステップ 3 [Delete Application] をクリックします。

ステップ 4 確認ダイアログボックスで、[OK] をクリックします。

アプリケーションが削除されるのは、Catalyst Centerによって管理されているいずれのデバイスでも使用されていない場合のみです。

それ以外の場合、エラーメッセージに、アプリケーションを使用しているデバイスの数が表示されます。確認ダイアログボックスで [Cancel] をクリックし、アプリケーションをアンインストールします。詳細については、Cisco Catalyst 9300 デバイスからのアプリケーションのアンインストール（1365 ページ）を参照してください。

アプリケーションログのダウンロード

アプリケーションログは Catalyst Center からダウンロードできます。

手順

ステップ 1 メインメニューから次を選択します。**[Provision]** > **[Services]** > **[IoT Services]** の順に選択します。

ステップ 2 [All Devices] をクリックします。

アプリケーションをホストできるデバイスのリストが表示されます。

ステップ 3 [APp logs] をクリックして、Catalyst Center からアプリケーションログをダウンロードします。

ステップ 4 [App Logs] ポップアップウィンドウで、ダウンロードするアプリケーション ログ ファイルを選択し、[Download] をクリックします。

デバイスのテクニカルサポートログのダウンロード

トラブルシューティングを行うために、Catalyst Center からデバイスのテクニカルサポートのログをダウンロードできます。

手順

ステップ 1 メインメニューから次を選択します。**[Provision]** > **[Services]** > **[IoT Services]** の順に選択します。

ステップ 2 [All Devices] をクリックします。

アプリケーションをホストできるデバイスのリストが表示されます。

ステップ 3 [Tech Support logs] をクリックして、デバイスのテクニカルサポートログをダウンロードします。

Cisco Catalyst 9100 シリーズ アクセスポイントでのアプリケーション ホスティング

ここでは、Cisco Catalyst 9100 シリーズ アクセスポイントでのアプリケーション ホスティングについて説明します。

Cisco Catalyst 9100 シリーズ アクセス ポイントでのアプリケーション ホスティングについて

仮想環境への移行により、再利用可能なポータブルかつスケーラブルなアプリケーションを構築する必要性が高まりました。アプリケーションのホスティングによって、管理者には独自のツールやユーティリティを利用するためのプラットフォームが与えられます。ネットワークデバイスでホストされるアプリケーションは、自動化、設定管理のモニタリング、既存のツールチェーンとの統合など、さまざまな目的で使用できます。

アプリケーション ホスティングを使用すると、Catalyst Center によって管理されているデバイス上のサードパーティ製アプリケーションのライフサイクルを管理できます。このリリースでは、Cisco IOS-XE ソフトウェアバージョン 17.3 以降を搭載した Cisco Catalyst 9100 シリーズ アクセスポイントでサードパーティ製 SES-imagotag IoT Connector アプリケーションを利用できます。

Cisco Catalyst 9100 シリーズ アクセスポイントの SES-imagotag IoT Connector は、あらゆる Electronic Shelf Label（ESL）通信に対応しています。

（注） アクセスポイントは、同じ IoT 機能を必要とする 2 つのアプリケーションをサポートすることはできません。特定の IoT 機能を使用するアプリケーションが AP ですでに実行されている場合、同じ機能を必要とする別のアプリケーションをアクティブ化すると、必要なデバイスが使用できないため失敗します。

たとえば、AP の IoT 無線機能を使用するアプリケーションがすでにインストールされ実行されている場合、その IoT 無線機能も必要とする別のアプリケーションをアクティブ化しようとすると失敗します。

Cisco Catalyst 9100 シリーズ アクセス ポイントでの USB アプリケーションのインストールと管理のアプリケーション ホスティング ワークフロー

始める前に

デバイスでアプリケーション ホスティングを有効にするには、次の前提条件を満たしている必要があります。

- Cisco Catalyst 9100 シリーズ アクセスポイントを検出するには、NETCONF を有効にし、ポートを 830 に設定します。
- Cisco Catalyst 9100 シリーズ アクセスポイントで IP が Catalyst Center に直接到達できることを確認します。
- Cisco Catalyst 9800 シリーズ ワイヤレス コントローラで Cisco IOS XE 17.3.x 以降のソフトウェアが実行されていることを確認します。
- Catalyst Center アプライアンスが最新の Catalyst Center ISO を実行していることを確認します。
- USB ドングルが AP に挿入されていることを確認します。これは、SES-imagotag Connector アプリケーションを実行するために必要です。

手順

ステップ 1 Cisco Catalyst 9800 シリーズ ワイヤレス コントローラと Cisco Catalyst 9100 シリーズ アクセス ポイントのアプリケーションをホスティングするための準備状況を確認してから、アプリケーションをインストールください。

詳細については、アプリケーションをホストするデバイスの準備状況の表示（1355 ページ）を参照してください。

ステップ 2 Catalyst Center にアプリケーション ホスティング サービスをインストールします。

詳細については、アプリケーション ホスティング サービス パッケージのインストールと更新 （1354 ページ）を参照してください。

ステップ 3 Cisco Catalyst 9800 シリーズ ワイヤレス コントローラを Catalyst Center に追加します。

詳細については、ネットワークデバイスの追加 （157 ページ）を参照してください。

（注） NETCONF が有効になっていることを確認し、ポートを 830 に設定します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラが [Managed] 状態になるまで待機する必要があります。

ステップ 4 [Network Hierarchy] ウィンドウで AP をフロアに割り当てます。

詳細については、フロアマップでの AP の取り扱い （304 ページ）を参照してください。

ステップ 5 USB アプリケーション（SES-imagotag コネクタ）を Catalyst Center にアップロードします。

詳細については、アプリケーションの追加 （1358 ページ）を参照してください。

ステップ 6 IoT サービスを有効にします。

詳細については、Cisco Catalyst 9100 シリーズ アクセス ポイントでの IoT サービスの有効化 （1637 ページ）を参照してください。

ステップ 7 『Application Hosting on Catalyst APs Deployment Guide』の説明に従って、コンテナを設定します。

Cisco Catalyst 9100 シリーズ アクセスポイントにインストールされているホスティングアプリケーションの表示

始める前に

前提条件が満たされていることを確認してください。詳細については、「アプリケーション ホスティングの前提条件」を参照してください。

手順

ステップ 1 メインメニューから次を選択します。**[Provision]** > **[Services]** > **[IoT Services]** の順に選択します。

ステップ 2 すべてのデバイスを表示するには、右上隅の [All Devices] をクリックします。特定のアプリケーションを使用するデバイスのみを表示するには、アプリケーションを選択して [Manage] をクリックします。

すべてのデバイスを表示することを選択した場合、[All Devices] ページには、アプリケーションをホストできるデバイスに関する情報（[Hostname]、[IP Address]、[Image Version]、[App Hosting Status]、[Last Updated]）が表示されます。

（注） AP の [App Hosting Status] が [Ready] の場合、AP で更新を設定するには、必要なホスト名の横にあるチェックボックスをオンにして、[Resync] をクリックします。

特定のアプリケーションのデバイスのリストを表示することを選択した場合、[Devices] ウィンドウには、アプリケーションをホストできるデバイスに関する次の情報（[Hostname]、[Device IP]、[App Version]、[App Status]、[Last Heard, Platform Version]、および [Action Status] が表示されます。

ステップ 3 [Devices] ウィンドウで [Summary] をクリックすると、デバイス上で失敗または停止したアプリケーション、および実行中のアプリケーションの概要が表示されます。

ステップ 4 [Action] ドロップダウンリストをクリックして、アプリケーションを開始、停止、編集、アップグレード、およびアンインストールします。

ステップ 5 インストールされているホスティング アプリケーションを表示するデバイスリンクをクリックします。

[Applications]ページには、インストールされているアプリケーションの**名前**、**バージョン**、**アプリケーションステータス**、**IP アドレス**、**正常性**、および**詳細情報**が表示されます。

ステップ 6 [Details] 列で [View] をクリックすると、デバイスのアプリケーションステータスに関する詳細情報が表示されます。

[App Details] ウィンドウには、アプリケーションの**リソース**および**ネットワーク**情報が表示されます。

ステップ 7 アプリケーションログをダウンロードするには、アプリケーションログをダウンロードするアプリケーションを選択し、[Application Logs] をクリックします。

ステップ 8 テクニカルサポートログをダウンロードするには、テクニカルサポートログをダウンロードするアプリケーションを選択し、[Tech Support Logs] をクリックします。

Cisco Catalyst 9100 デバイスからのアプリケーションのアンインストール

Cisco Catalyst 9100 シリーズ AP からアプリケーションをアンインストールできます。

手順

ステップ 1 メインメニューから次を選択します。**[Provision]** > **[Services]** > **[IoT Services]** の順に選択します。

ステップ 2 アプリケーションを選択し、[Manage] をクリックして、そのアプリケーションを使用するデバイスを表示します。

ステップ 3 アンインストールするアプリケーションがあるデバイスを選択します。

ステップ 4 [Actions] ドロップダウンリストから [Uninstall App] を選択します。

Cisco Catalyst 9100 デバイスからのアプリケーションの削除

Cisco Catalyst 9100 シリーズ AP からアプリケーションを削除できます。

始める前に

アプリケーションを使用しているすべてのデバイスからアプリケーションをアンインストールする必要があります。詳細については、「Cisco Catalyst 9100 デバイスからのアプリケーションのアンインストール」を参照してください。

手順

ステップ 1 メインメニューから次を選択します。**[Provision]** > **[Services]** > **[IoT Services]** の順に選択します。

[IoTサービス（IoT Services）] ウィンドウで使用可能なホストされているアプリケーションを表示できます。

ステップ 2 削除するアプリケーションを選択します。

ステップ 3 [Delete Application] をクリックします。

ステップ 4 確認ダイアログボックスで、[OK] をクリックします。

アプリケーションが削除されるのは、Catalyst Centerによって管理されているいずれのデバイスでも使用されていない場合のみです。

それ以外の場合、エラーメッセージに、アプリケーションを使用しているデバイスの数が表示されます。[Cancel] をクリックし、アプリケーションをアンインストールします。詳細については、「Cisco Catalyst 9100 デバイスからのアプリケーションのアンインストール」を参照してください。

サイト間 VPN の設定

サイト間 VPN を作成し、既存のサイト間 VPN を編集または削除できます。

Catalyst Center は次のデバイスでサイト間 VPN をサポートしています。

- Cisco ASR 1000
- Cisco CSR
- Cisco ISR 4000

サイト間 VPN の作成

この手順では、サイト間 VPN を作成する方法を示します。

始める前に

- ネットワーク階層内のサイトを定義します。ネットワーク階層（271 ページ）を参照してください。

- VPN トンネルに使用する IP アドレスプールを設定します。IP アドレスプールには、少なくとも 6 つの空き IP アドレスが必要です。IP アドレスプールを設定する （397 ページ）を参照してください。

手順

ステップ 1 メインメニューから次を選択します。**[Provision]** > **[Site to Site VPN]**。

サイト間 VPN は、このほかに **[Workflows]** > **[Site to Site VPN]** ウィンドウからも作成できます。

ステップ 2 VPN を作成するには、[Add] をクリックします。
[サイトの選択（Choose Your Sites）] ワークフローが表示されます。

ステップ 3 [サイトの選択（Choose Your Sites）] ワークフローで、次の手順を実行します。

a) 最初のフィールドに VPN 名を入力します。

b) [Site 1] ドロップダウンリストから、最初のサイト、そのサイトのデバイス、およびそのデバイスの WAN インターフェイスを選択します。WAN インターフェイスは、デバイスがプロビジョニングされている場合はデフォルトで設定されます。

c) [Site 2] ドロップダウンリストから、2 番目のサイト、そのサイトのデバイス、およびそのデバイスの WAN インターフェイスを選択します。WAN インターフェイスは、デバイスがプロビジョニングされている場合はデフォルトで設定されます。

ステップ 4 [ネットワークの選択（Select Networks）] ウィンドウで、次の手順を実行します。

a) [Tunnel IP Pool] ドロップダウンリストから、IP アドレスプールを選択します。

b) それぞれのサイトについて、使用するサブネットの横にあるチェックボックスをオンにします。

c) （オプション）サイトのカスタムネットワークを追加する場合は、下部にある [Add Custom Networks] リンクをクリックし、必要なフィールドに入力します。

ステップ 5 [VPNの設定（Configure VPN）] ウィンドウで、次の手順を実行します。

a) 暗号化の事前共有キーを入力します。

b) 必要に応じて、暗号化アルゴリズムと整合性アルゴリズムを設定します。デフォルトの設定を使用することを推奨します。設定を変更した場合にデフォルトの選択に戻すには、[Use Cisco recommended IKEV2 & Transform Set Values] チェックボックスをオンにします。

ステップ 6 [Summary] ウィンドウで、VPN 設定を確認します。変更するには、[Edit] をクリックします。

ステップ 7 続行するには、[Create VPN] をクリックします。

次のステータス画面では、完了した順に各ステップの横にチェックマークが表示されます。[Services] をクリックして [Site to Site VPN] ウィンドウに戻ると、新しく作成した VPN が表示されます。

サイト間 VPN の編集

手順

ステップ 1 メインメニューから次を選択します。**[Provision]** > **[Site to Site VPN]**。

ステップ 2 編集する VPN の横にあるチェックボックスをオンにします。

ステップ 3 リストの上方にあるメニューバーで [Edit] をクリックします。

ステップ 4 [Summary] ウィンドウで、VPN 設定を確認します。変更するには、[Edit] をクリックします。

ステップ 5 [Edit VPN] をクリックして変更を送信します。

次のステータス画面では、完了した順に各ステップの横にチェックマークが表示されます。[Services]をクリックして [Site to Site VPN] 画面に戻ります。

サイト間 VPN の削除

手順

ステップ 1 メインメニューから次を選択します。**[Provision]** > **[Site to Site VPN]**。

ステップ 2 削除する VPN の横にあるチェックボックスをオンにします。

ステップ 3 リストの上方にあるメニューバーで [Delete] をクリックします。

確認ダイアログボックスが表示されます。

ステップ 4 [Yes] をクリックして、VPN を削除することを確認します。

Cisco Umbrella の設定

このセクションでは、Cisco Umbrella と Catalyst Center との統合について説明します。

Cisco Umbrella について

Cisco Umbrella の DNS レイヤセキュリティにより、最も迅速かつ簡単にネットワークのセキュリティを強化できます。セキュリティの可視性を向上させ、侵害されたシステムを検出します。脅威がネットワークやエンドポイントに到達する前に阻止することにより、あらゆるポートやプロトコルでネットワーク内外を問わずユーザーを保護します。

Catalyst Center は、次のデバイス上の Cisco Umbrella 設定をサポートします。

- Cisco IOS-XE ソフトウェアバージョン 16.12 以降を搭載した Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ
- Cisco Catalyst 9100 シリーズ AP
- Cisco IOS-XE ソフトウェアバージョン 17.3.1 以降を搭載した Cisco Catalyst 9200 アクセス スイッチ
- Cisco IOS-XE ソフトウェアバージョン 17.3.1 以降を搭載した Cisco Catalyst 9300 アクセス スイッチ

Cisco Umbrella のロールベース アクセス コントロールの設定

Catalyst Center で Cisco Umbrella を設定したり、ネットワークデバイスで Cisco Umbrella をプロビジョニングしたりするには、必要な RBAC 権限を持つ Cisco Umbrella のユーザーロールを作成する必要があります。詳細については、*Catalyst Center* 管理者ガイド [英語] の「Manage Users」を参照してください。

表 *57 : Cisco Umbrella* の *RBAC* 権限マトリックス

機能	アクセス	権限
Catalyst Center での Cisco Umbrella の設定	[Network Design] > [Advanced Network Settings]	書き込み
システム 360 での Cisco Umbrella ダッシュレットの追加	[Network Design] > [Advanced Network Settings]	書き込み
ネットワークデバイスでの Cisco Umbrella のプロビジョニング	[Network Provision] > [Provision]	書き込み
	[Network Design] > [Network Hierarchy]	読み取り
	[Network Provision] > [Inventory Management]	読み取り
	[System]	読み取り
	[Network Provision] > [Scheduler]	書き込み
	[Network Services] > [Umbrella]	書き込み

Catalyst Center での Cisco Umbrella の設定

始める前に

- Cisco Umbrella アカウントを作成します。

- *login.umbrella.com* にログインし、API キー、レガシートークン、管理キー、シークレットなどの必要なキーを作成します。
- Cisco Umbrella ログイン URL の組織 ID をメモします。
- Cisco Umbrella でローカルバイパスドメインを作成します。
- Catalyst Center と管理しているネットワークデバイスやソフトウェアアップデートをダウンロードする Cisco cloud との間にプロキシサーバーがある場合は、プロキシサーバーへのアクセスを設定する必要があります。詳細については、『Catalyst Center Administrator Guide』の「Configure the Proxy」セクションを参照してください。
- Catalyst Center で Cisco Umbrella パッケージをインストールします。『Catalyst Center Administrator Guide』の「Download and Install Packages and Updates」セクションを参照してください。
- 必要な RBAC 権限を持つ Cisco Umbrella のユーザーロールを作成します。Cisco Umbrella のロールベース アクセス コントロールの設定 （1375 ページ）を参照してください。

（注） IPv6 で設定された Catalyst Center クラスタに Cisco Umbrella パッケージをインストールすることはできません。

手順

ステップ 1 メインメニューから次を選択します。**[System]** > **[Settings]** > **[External Services]** > **[Umbrella]** の順に選択します。

ステップ 2 Cisco Umbrella から手動で取得した次の詳細を入力します。

- **Organization ID**
- **Network Device Registration API Key**
- **Network Device Registration Secret**
- **Management API Key**
- **Management Secret**
- **Legacy Device Registration Token**

ステップ 3 [Save] をクリックします。

Cisco Umbrella ダッシュレットの追加

[System 360] ウィンドウに [Umbrella] ダッシュレットを追加できます。[Umbrella] ダッシュレットには、Catalyst Center での Cisco Umbrella の構成ステータスが表示されます。

始める前に

Cisco Umbrella パッケージをインストールする必要があります。

手順

ステップ 1 メインメニューから次を選択します。**[System]** > **[System 360]** の順に選択します。

ステップ 2 [Actions] メニューから、[Edit Dashboard] を選択し、[Add Dashlet] をクリックします。

ステップ 3 [Umbrella Dashlet] を選択し、[Add] をクリックします。

[Umbrella] ダッシュレットが **[System 360]** ウィンドウの [外部接続されたシステム（Externally Connected Systems）] に表示されます。Cisco Umbrella が Catalyst Center で設定されていれば、[Umbrella] ダッシュレットにステータスが [Available] と表示され、組織 ID が表示されます。

Cisco Umbrella が Catalyst Center で設定されていない場合は、[Configure] リンクをクリックし、**[System]** > **[Settings]** > **[External Services]** > **[Umbrella]** のフィールドに値を入力できます。Catalyst Center での Cisco Umbrella の設定 （1375 ページ）を参照してください。

Cisco Umbrella でキーが変更された場合は、[Update] リンクをクリックし、**[System]** > **[Settings]** > **[External Services]** > **[Umbrella]** のキーを更新できます。Catalyst Center での Cisco Umbrella の設定 （1375 ページ）を参照してください。

Cisco Umbrella サービス統計ダッシュボードの表示

[Umbrella Service Stats] ダッシュボードを表示するには、メインメニューから次を選択します。**[Provision]** > **[Services]** > **[Umbrella]** の順に選択します。

ダッシュボードには、次のダッシュレットが表示されます。

- [Total Umbrella DNS Queries]：選択したサイトでブロックされた DNS クエリと許可された DNS クエリの数を示します。
- [Blocked Umbrella DNS Queries]：選択したサイトでセキュリティポリシーおよびコンテンツポリシーによってブロックされた DNS クエリの数を示します。

デフォルトでは、このダッシュレットには過去 3 時間の統計情報が表示されます。過去 24 時間または 7 日間の統計を表示するには、[Cisco Umbrellaサービス統計（Umbrella Service Stats）] ウィンドウの左上隅にあるドロップダウンリストからその目的の時間を選択します。

ネットワークデバイスでの Cisco Umbrella のプロビジョニングの前提条件

ネットワークデバイスで Cisco Umbrella をプロビジョニングする前に、次の点を確認します。

- Cisco Umbrella が Catalyst Center で設定されている。
- Cisco Umbrella をプロビジョニングするデバイスについて、ワイヤレスプロビジョニングが完了している。
- SSID 設定が非ファブリックである。
- デバイスが FlexConnect モードの非ファブリック SSID として設定されている場合、AP がプロビジョニングされている。
- デバイスからダイレクト インターネット アクセスで Cisco Umbrella への接続が確立されている。
- Cisco Umbrella ルート証明書は、 Catalyst Center 信頼できる証明書バンドルで入手できます。*Cisco Catalyst Center Administrator Guide* のトピック「信頼できる証明書の設定」を参照してください。
- デバイスの Cisco Umbrella 設定が Catalyst Center から設定されていない場合は、デバイスから Cisco Umbrella 設定を削除し、デバイスを Catalyst Center と再同期する。

ネットワークデバイスでの Cisco Umbrella のプロビジョニング

始める前に

前提条件が満たされていることを確認してください。詳細については、ネットワークデバイスでの Cisco Umbrella のプロビジョニングの前提条件 （1378 ページ）を参照してください。

（注） 組織のネットワークでの Cisco Umbrella の展開は、*login.umbrella.com* からのみモニタできます。

手順

ステップ 1 メインメニューから次を選択します。**[Workflows]** > **[Umbrella Deployment]** の順に選択します。

または、以下の手順を実行します。

a) メインメニューから次を選択します。**[Provision]** > **[Umbrella]** の順に選択します。
b) Cisco Umbrella を展開するサイトをネットワーク階層から選択します。
c) [Select Devices] ウィンドウが表示されます。手順 4 に進んで展開ワークフローを続けます。

ステップ 2 タスクの概要ウィンドウが表示されたら、[Let's Start] をクリックして、ワークフローに直接移動します。

ステップ 3 [Choose Site] ウィンドウが表示されます。

a) 各サイトのデバイスの準備状況が次のステータスで示されます。

- [Eligible Devices]：Cisco Umbrella の構成に適格なデバイス。ネットワークデバイスでの Cisco Umbrella のプロビジョニングの前提条件 （1378 ページ）を参照してください。
- [Enabled Devices]：Catalyst Center からすでに設定されているデバイス。

b) 展開するサイトを選択し、[Next] をクリックします。

（注） 一度に選択できるサイトは 1 つだけです。親サイトを選択すると、すべての子サイトに同時に Cisco Umbrella を展開できます。

ステップ 4 [Select Device Type] ウィンドウで、[Switches] または [Wireless Controllers] を選択します。

ステップ 5 [Select Device Type] ウィンドウで [Switches] を選択した場合は、次の手順を実行します。

a) [Select Devices] ウィンドウで、有線デバイスを選択します。

b) [Configure Interface] ウィンドウで、次の手順を実行します。

1. 設定するポートを選択し、[Define Umbrella Interfaces] をクリックします。
2. [Select Configuration] ダイアログボックスで、[Define Umbrella Interfaces] ドロップダウンリストをクリックし、[IN(LAN)]、[OUT(WAN)]、または [Disable Umbrella] を選択し、[Save] をクリックします。

（注） 次の手順に進むには、少なくとも 1 つの [IN] インターフェイスと 1 つの [OUT] インターフェイスを選択する必要があります。

c) [Define Umbrella Policy Mapping (Wired)] ウィンドウで、グローバルレベルまたはインターフェイスレベルの Umbrella ポリシーを選択します。

d) [Configure Policies for Your Devices] ウィンドウで、[IN(LAN)] インターフェイスを選択し、[Define Umbrella Policies] をクリックします。

e) [Select Policy] ダイアログボックスで、選択したインターフェイスのポリシーを選択し、[Save] をクリックします。

ステップ 6 [Select Device Type] ウィンドウで [Wireless Controllers] を選択した場合は、次の手順を実行します。

a) [Select Devices] ウィンドウで、ワイヤレスデバイスを選択します。

b) SSID を選択し、各 SSID に必要な Cisco Umbrella ポリシーを選択します。

（注）
- このページには、非ファブリック SSID のみが表示されます。
- SSID は選択し、Cisco Umbrella ポリシーは選択しない場合には、デフォルトポリシーが SSID にマッピングされます。
- 複数のポリシーを選択した場合に、ポリシーが適用される順序は、Cisco Umbrella クラウドポータルに定義されています。

c) [Umbrella Policy Association (Wireless)] ウィンドウで、SSID に適用されるデフォルトのポリシーを確認します。

SSID に関連付けられているポリシーを変更する場合は、[Cisco Umbrella] リンクをクリックします。Catalyst Center からの Cisco Umbrella の展開が完了すると、Cisco Umbrella コンソールにネットワーク アイデンティティが表示されます。Cisco IOS-XE ソフトウェアバージョン 16.xx を搭載したデバイスの場合、ネットワーク アイデンティティはグローバルと表示されます。Cisco IOS-XE ソフトウェアバージョンが 16.xx 以降のデバイスの場合、ネットワーク アイデンティティは、サイトと SSID 名に基づいて作成されたカスタム名として表示されます。

ステップ 7 [Review Internal Domains] ウィンドウで、内部ドメインのリストを追加または削除します。[Internal Domain] リストのドメインに一致する DNS クエリは、Cisco Umbrella ではなくローカル DNS サーバーに転送されます。

ステップ 8 [DNS Crypt] ウィンドウが表示されます。[Enable DNS Packet Encryption] オプションがデフォルトで選択されています。

a) [DNS Crypt] ウィンドウで、[Next] をクリックします。
b) DNS パケット暗号化を使用しない場合は、[Enable DNS Packet Encryption] チェックボックスをオフにします。

ステップ 9 [Summary] ウィンドウで、詳細を確認します。変更するには、[Edit] をクリックします。

ステップ 10 続行するには、[Deploy] をクリックします。

ステップ 11 [Schedule] ウィンドウで、構成を今すぐ展開するか、後でスケジュールするかを選択します。

ステップ 12 続行するには、[Apply] をクリックします。

ステップ 13 **[Deployment]** ウィンドウで **[View Status]** をクリックし、展開ステータスを確認します。

デバイスの Cisco Umbrella 展開ステータスと Cisco Umbrella でのデバイス構成ステータスを確認できます。Cisco Umbrella の展開ログは [Audit Logs] ウィンドウでも確認できます。

ネットワークデバイスでの Cisco Umbrella の無効化

手順

ステップ 1 メインメニューから次を選択します。**[Workflows]** > **[Umbrella Deployment]** の順に選択します。

または、以下の手順を実行します。

a) メインメニューから次を選択します。**[Provision]** > **[Services]** > **[Umbrella]** の順に選択します。
b) Cisco Umbrella を無効にするサイトをネットワーク階層から選択します。
c) [Select Devices] ウィンドウが表示されます。手順 4 に進んで無効化ワークフローを続けます。

ステップ 2 タスクの概要ウィンドウが表示されたら、[Let's Start] をクリックして、ワークフローに直接移動します。

ステップ 3 [Choose Site] ウィンドウが表示されます。

a) 各サイトのデバイスの準備状況が次のステータスで示されます。

- [Ready Devices]：Cisco Umbrella 構成の前提条件を満たしているデバイス。ネットワークデバイスでの Cisco Umbrella のプロビジョニングの前提条件 （1378 ページ）を参照してください。
- [Not Ready Devices]：前提条件を満たしていないデバイス。
- [Enabled Devices]：Catalyst Center からすでに設定されているデバイス。

b) 無効にするサイトを選択し、[Next] をクリックします。

（注） 一度に選択できるサイトは 1 つだけです。親サイトを選択すると、すべての子サイトで同時に Cisco Umbrella が無効になります。

ステップ 4 [Select Device Type] ウィンドウで、[Switches] または [Wireless Controllers] を選択します。

ステップ 5 [Select Devices] ウィンドウで、[Enabled] タブをクリックし、デバイスを選択します。

ステップ 6 [Disable] オプションボタンをクリックし、デバイスを選択します。

ステップ 7 [Summary] ウィンドウで、詳細を確認します。変更するには、[Edit] をクリックします。

ステップ 8 続行するには、[Deploy] をクリックします。

ステップ 9 [Schedule] ウィンドウで、構成を今すぐ展開するか、後でスケジュールするかを選択します。

ステップ 10 続行するには、[Apply] をクリックします。

ステップ 11 **[Deployment]** ウィンドウで **[View Status]** をクリックし、展開ステータスを確認します。

Cisco Umbrella の展開ログは [Audit Logs] ウィンドウで確認できます。

ネットワークデバイスでの Cisco Umbrella 設定の更新

手順

ステップ 1 メインメニューから次を選択します。**[Workflows]** > **[Umbrella Deployment]** の順に選択します。

または、以下の手順を実行します。

a) メインメニューから次を選択します。**[Provision]** > **[Services]** > **[Umbrella]** の順に選択します。
b) Cisco Umbrella 構成を更新するサイトをネットワーク階層から選択します。
c) [デバイスの選択（Select devices）] ウィンドウが表示されます。手順 4 に進んで更新ワークフローを続けます。

ステップ 2 タスクの概要ウィンドウが表示されたら、[開始（Let's Start）] をクリックして、ワークフローに直接移動します。

ステップ 3 [Choose Site] ウィンドウが表示されます。

a) 各サイトのデバイスの準備状況が次のステータスで示されます。
   - [Ready Devices]：Cisco Umbrella 構成の前提条件を満たしているデバイス。ネットワークデバイスでの Cisco Umbrella のプロビジョニングの前提条件 （1378 ページ）を参照してください。
   - [Not Ready Devices]：前提条件を満たしていないデバイス。
   - [Enabled Devices]：Catalyst Center からすでに設定されているデバイス。

b) 更新するサイトを選択し、[Next] をクリックします。

（注） 一度に選択できるサイトは 1 つだけです。親サイトを選択すると、すべての子サイトで同時に Cisco Umbrella が更新されます。

ステップ 4 [Select Device Type] ウィンドウで、[Switches] または [Wireless Controllers] を選択します。

ステップ 5 [Select Device Type] ウィンドウで [Switches] を選択した場合は、次の手順を実行します。

a) [Select Devices] ウィンドウで、有線デバイスを選択し、[Update] オプションボタンをクリックします。
b) [Configure Interface] ウィンドウで、次の手順を実行します。
   1. ポートを選択し、[Define Umbrella Interfaces] をクリックします。
   2. [Select Configuration] ダイアログボックスで、[Define Umbrella Interfaces] ドロップダウンリストをクリックし、[IN(LAN)]、[OUT(WAN)]、または [Disable Umbrella] を選択し、[Save] をクリックします。

（注） 次の手順に進むには、少なくとも 1 つの [IN] インターフェイスと 1 つの [OUT] インターフェイスを選択する必要があります。

c) [Define Umbrella Policy Mapping (Wired)] ウィンドウで、グローバルレベルまたはインターフェイスレベルの Umbrella ポリシーを選択し、[Next] をクリックします。
d) [Configure Policies for Your Devices] ウィンドウで、[IN(LAN)] インターフェイスを選択し、[Define Umbrella Policies] をクリックします。
e) [Select Policy] ダイアログボックスで、選択したインターフェイスのポリシーを選択し、[Save] をクリックします。

ステップ 6 [Select Device Type] ウィンドウで [Wireless Controllers] を選択した場合は、次の手順を実行します。

a) [Select Devices] ウィンドウで、ワイヤレスデバイスを選択し、[Update] オプションボタンをクリックします。
b) [Umbrellaポリシーマップの定義（ワイヤレス）（Define Umbrella Policy Map (Wireless)）] ウィンドウで SSID を選択し、マッピングする Cisco Umbrella ポリシーを選択するか、SSID の選択を解除して Cisco Umbrella を無効にします。

ステップ 7 [Review Internal Domains] ウィンドウで、内部ドメインのリストを追加または削除します。[Internal Domain] リストのドメインに一致する DNS クエリは、Cisco Umbrella ではなくローカル DNS サーバーに転送されます。

ステップ 8 [DNS Crypt] ウィンドウが表示されます。[Enable DNS Packet Encryption] オプションがデフォルトで選択されています。

DNS パケット暗号化を使用しない場合は、[Enable DNS Packet Encryption] チェックボックスをオフにします。

ステップ 9 [Summary] ウィンドウで、詳細を確認します。変更するには、[Edit] をクリックします。

ステップ 10 続行するには、[Deploy] をクリックします。

ステップ 11 [Schedule] ウィンドウで、構成を今すぐ展開するか、後でスケジュールするかを選択します。

ステップ 12 続行するには、[Apply] をクリックします。

ステップ 13 **[Deployment]** ウィンドウで **[View Status]** をクリックし、展開ステータスを確認します。

Cisco Umbrella の展開ログは [Audit Logs] ウィンドウで確認できます。

セキュアトンネルの作成

Catalyst Center では、企業とブランチ拠点間のセキュアな接続を確立する VPN トンネルのプランニングと展開が可能です。

（注） この機能は、現在、Cisco Catalyst 9300X シリーズ スイッチでのみサポートされています。

セキュアトンネルの設定

この手順を使用して、*n* 日目にセキュアトンネルを計画および展開できます。

手順

ステップ 1 メインメニューから次を選択します。**[Provision]** > **[Secure Tunnels]** の順に選択します。

または、[Workflows] > [Create Secure Tunnel] ウィンドウからセキュアトンネルを作成することもできます。

ステップ 2 [Secure Tunnel] ウィンドウで、[Create Secure Tunnel] をクリックします。

ステップ 3 タスクの概要ウィンドウが開いたら、[Let's Do it] をクリックして、ワークフローに直接移動します。

ステップ 4 [Select Tunnel Type] ウィンドウで、[Site To Secure Access Service Edge (SIG/SASE)] タイルをクリックして、作成するセキュアトンネルのタイプを選択します。

これにより、Cisco Catalyst 9300X シリーズ スイッチとセキュア インターネット ゲートウェイの間にセキュアトンネルが作成されます。

ステップ 5 **[セキュア インターネット ゲートウェイを選択（Select Secure Internet Gateway）]** ウィンドウで、ドロップダウンリストをクリックして [セキュア インターネット ゲートウェイ（Secure Internet Gateway）] を選択します。

選択したセキュア インターネット ゲートウェイについて、次のいずれかを実行します。

- [Umbrella]：Cisco Umbrella でトンネルを作成したことを確認します。後続の手順でトンネル ID と事前共有キーが必要になります。詳細については、Catalyst Center での Cisco Umbrella の設定 （1375 ページ）を参照してください。Cisco Umbrella ポータルにトンネルが作成されている場合は、確認チェックボックスをオンにします。
- [Zscaler]：Zscaler ポータルでトンネルがすでに作成されていることを確認します。Zscaler でトンネルを作成した後、選択した Cisco Catalyst 9300X シリーズ スイッチでトンネルパラメータを設定するために、事前共有キーと定義済みの FQDN が必要になります。Zscaler ポータルにトンネルが作成されている場合は、確認チェックボックスをオンにします。

ステップ 6 **[サイトとデバイスを選択（Choose Site and Device）]** ウィンドウで、サイトとトンネルのマッピングについて次の手順を実行します。

1. [Site] のドロップダウンリストからサイトを選択します。
2. [Device] のドロップダウンリストからデバイスを選択します。
3. [Number of Tunnels] のドロップダウンリストから作成するトンネルの数を選択します。

4. Zscaler の場合、[Tunnel Type] のドロップダウンリストからトンネルタイプを選択します。
5. [Tunnel Name] にトンネル名を入力します。
6. [Tunnel Source Interface] を選択します。
7. トンネル IP に同じインターフェイスを使用する場合は、チェックボックスをオンにします。同じインターフェイスを使用しない場合は、チェックボックスをオフにして、[Interface] を選択します。
8. [Data Center Location] にデータセンターの位置を入力します。

ステップ 7 [トンネル設定の定義（Define Tunnel Settings）] ウィンドウで、次の手順を実行します。

1. Umbrella の場合、[Pre-Shared Key (PSK)] に認証用の事前共有キー（PSK）を入力します。
2. セキュア インターネット ゲートウェイの統合が完了していない場合は、次の手順を実行します。
    1. [トンネル ID（Tunnel ID）] にトンネル ID を入力し、次のいずれかを選択します。
        1. [Fully Qualified Domain Name (FQDN)]：Cisco Umbrella で生成された**トンネル ID** または Zscaler で生成された**ユーザー ID** を使用します。
        2. [IP Address]：接続先にする IP アドレスを使用します。
3. シスコ推奨の設定を使用するには、チェックボックスをオンにします。値をカスタマイズするには、チェックボックスをオフにします。

ステップ 8 **[トンネルトラフィックの設定（Configure Tunnel Traffic）]** ウィンドウで、トラフィックをルーティングするためのオプションを次から選択します。

- [Send all traffic]：すべてのトラフィックを IPSec トンネル経由で Umbrella に送信します。
- [Send Selected Traffic]：サブネットとサブネットの入力インターフェイスを入力します。 をクリックすると、さらにサブネットを追加できます。

ステップ 9 [Schedule Task] ウィンドウで、トンネルを今すぐ作成するか、後でスケジュールするかを選択します。[Generate CLI Preview] を選択することもできます。

ステップ 10 [Summary] ウィンドウで、設定を確認します。変更するには、[Edit] をクリックします。

ステップ 11 [Create Secure Tunnel] をクリックします。

[Done!] ウィンドウが表示されます。

ステップ 12 [View all Tunnels] タブをクリックして、トンネル作成のステータスを表示します。

この処理には、しばらく時間がかかる場合があります。[Refresh] をクリックします。トンネルが起動すると、ステータスが [Provision] から [Up] に変わります。

SD-Access へのセキュリティサービスの挿入

セキュリティサービスの挿入により、定義済みのポリシーに基づいてファイアウォールを介してトラフィックがステアリングされ、SD-Access ファブリックネットワークのセキュリティが強化されます。セキュリティサービスの挿入により、ネットワークは適切なトラフィックを特定してファイアウォールにリダイレクトすることでセキュリティイネーブラとして機能し、ゼロトラスト セキュリティ ソリューションをサポートします。

セキュリティサービスの挿入は、有線展開とワイヤレス展開の両方をサポートしています。シスコとサードパーティのファイアウォールと互換性があります。

セキュリティサービスの挿入を許可するために、Catalyst Center は以下を実行します。

- ネットワーク自動化を実行して、トラフィックをファイアウォールにリダイレクトします。
- トラフィック ステアリング ポリシーを設定して、ファイアウォールへのトラフィックのステアリングを決定します。
- トラフィック ステアリング ポリシーを Cisco ISE とデバイスにプッシュします。

（注） トラフィックをリダイレクトするトラフィック ステアリング ポリシーが設定されている場合、ファイアウォール IP に到達できなければ、トラフィックはドロップされます。

ファブリックの正常性のモニタリングとトラブルシューティングについては、『*Cisco Catalyst Assurance User Guide*』の「Monitor and Troubleshoot SD-Access Health」を参照してください。

メインメニューから次を選択します。、**[プロビジョニング（Provision）]**>**[セキュリティサービスの挿入（Security Service Insertion）]**の順に選択し、[セキュリティサービスの挿入（Security Service Insertion）] ウィンドウを表示します。次の詳細が表示されます。

以下の場合	ウィンドウに次の情報が表示されます。
Day-0	• サービス挿入サイトを有効にするための事前チェック • [サービス挿入サイトの有効化（Enable a Service Insertion Site）] オプション
Day-n	• [サービス挿入サイト（Service insertion sites）] タブ • [ステアリングコントラクト（Steering contracts）] タブ • [サービス挿入の有効化（Enable Service Insertion）] オプション

サービス挿入サイト

サービス挿入サイトは、仮想ネットワークとファイアウォールがトラフィックをステアリングするように設定されているネットワーク内のファブリックサイトです。セキュリティサービスの挿入を使用するには、サービス挿入サイトを有効にする必要があります。

Day-0

サービス挿入サイトを有効にするには、デイゼロで次の手順を実行します。

1. デイゼロでサービス挿入サイトを有効にするための事前チェック （1388 ページ）
2. サービス挿入サイトの有効化 （1389 ページ）

Day-n

メインメニューから次を選択します。、**[プロビジョニング（Provision）]**>**[セキュリティサービス挿入（Security Service Insertion）]** > **[サービス挿入サイト（Service insertion sites）]**を選択し、Day-n のサービス挿入サイトを表示および設定します。

[サービス挿入サイト（Service insertion sites）] タブには、次のエリアが表示されます。

- [概要（Summary）]：次の項目の総数を表示します。
  - サービス挿入サイト
  - 使用されている仮想ネットワーク
  - トラフィック ステアリング ポリシー
  - トラフィック ステアリング コントラクト
- [設定別の統計（Statistics by configuration）]：次の情報を表示します。
  - 上位 5 つのファイアウォール IP アドレス
  - 上位 5 つのトラフィック ステアリング コントラクト
  - 上位 5 つのノード
- [サービス挿入サイト（Service insertion sites）]：設定されたサービス挿入サイトの詳細を記載した表を表示します。

  検索バーを使用して、サービス挿入サイトを検索できます。

  サービス挿入サイト名をクリックして、サービス挿入サイトに関連付けられた仮想ネットワークとトラフィック ステアリング ポリシーを表示、編集できます。詳細については、サービス挿入サイトの編集 （1391 ページ） を参照してください。
- [ワークフローライブラリ（Workflow library）]：セキュリティサービス挿入に使用可能なワークフローを表示します。

[サービス挿入の有効化（Enable Service Insertion）] をクリックして、サービス挿入サイトを有効にします。詳細については、サービス挿入サイトの有効化（1389ページ）を参照してください。

デイゼロでサービス挿入サイトを有効にするための事前チェック

デイゼロで手順を使用して、サービス挿入サイトを有効にするための前提条件が満たされていることを確認します。

手順

ステップ1 メインメニューから次を選択します。**[プロビジョニング（Provision）]** > **[セキュリティサービスの挿入（Security Service Insertion）]**の順に選択します。

ステップ2 [**Software-Defined Access and Access Control Application package**] で、次の設定を確認します。

確認事項	非該当時の対応
SD-Access およびアクセス コントロール アプリケーション パッケージ バージョン 2.2 以降がインストールされているかどうか。	[ACAパッケージのインストール（Install ACA package）] をクリックして、必要なパッケージをインストールします。
仮想ネットワークが必須のファブリックサイトで設定されているかどうか。 ⚠ アイコンは、仮想ネットワークがファブリックサイトで設定されていないことを示します。	[ファブリックサイト（Fabric sites）] をクリックして、ファブリックサイトのレイヤ 3 仮想ネットワークを設定します。 詳細については、レイヤ 3 仮想ネットワークの作成（1257 ページ） を参照してください。

データを更新するには、ツールバーの [Refresh] をクリックします。

ステップ3 [ISE統合（ISE Integration）] で、次の設定を確認します。

確認事項	非該当時の対応
Cisco ISE が Catalyst Center と統合されているかどうか。	[ISE統合（Integrate ISE）] をクリックして Cisco ISE を Catalyst Center と統合します。
Cisco ISE がバージョン 3.4 以降を実行しているかどうか。	[ISEの更新（Update ISE）] をクリックして、Cisco ISE を必要なバージョンに更新します。
Cisco ISE が同期されているかどうか。	[ISEの同期（Sync ISE）] をクリックして Cisco ISE を同期します。

データを更新するには、ツールバーの [Refresh] をクリックします。

ステップ4 [セキュリティグループ（Security groups）] で、次の設定を確認します。

確認事項	非該当時の対応
セキュリティグループが利用可能かどうか。	[セキュリティグループの作成（Create security group）]をクリックして、必要なセキュリティグループを作成します。 詳細については、セキュリティグループの作成（1416 ページ） を参照してください。
Catalyst Center がセキュリティグループを部分的または完全に管理しているかどうか。	Cisco ISE がセキュリティグループを完全に管理している場合、Catalyst Center でのセキュアサービス挿入にそれらを使用することはできません。

次のタスク

サービス挿入サイトの有効化 （1389 ページ）

サービス挿入サイトの有効化

ファブリックサイトでサービス挿入サイトを有効にしてセキュリティ サービス ポリシーを展開するには、次の手順を実行します。

始める前に

Day-0 では、「デイゼロでサービス挿入サイトを有効にするための事前チェック （1388 ページ）」を参照してください。

手順

ステップ 1 メインメニューから次を選択します。 **[プロビジョニング（Provision）]** > **[セキュリティサービスの挿入（Security Service Insertion）]** の順に選択します。

ステップ 2 セキュリティサービスの挿入を有効にします。

- Day-0 では、[サービス挿入サイトの有効化（Enable a Service Insertion Site）] をクリックします。
- Day-n では、[サービス挿入の有効化（Enable Service Insertion）] をクリックします。

ステップ 3 タスクの概要ウィンドウが開いたら、[Let's Do It] をクリックして、ワークフローに直接移動します。

ステップ 4 **[ファブリックサイトの選択（Select a fabric site）]** ウィンドウで、サービス挿入サイトとして有効にするファブリックサイトを選択します。

- 選択したファブリックサイトに関連付けられている仮想ネットワークとデバイスを表示します。
- 仮想ネットワークに関連付けられているすべてのデバイスが準備完了状態であることを確認します。

（注） ⚠ アイコンは、仮想ネットワークに準備完了状態ではないデバイスがあることを示します。これらの仮想ネットワークには、ステアリングポリシーを設定できません。

ステップ 5 **[サービス挿入の展開（Service insertion deployment）]** ウィンドウで、次の設定を完了します。

a) [仮想ネットワーク（Virtual network）] ドロップダウンリストから仮想ネットワークを選択します。

b) [ファイアウォールIP/マスク（Firewall IP/mask）] フィールドにファイアウォールの IP アドレスとサブネットマスクを入力します。

仮想ネットワークとファイアウォールの IP アドレスに基づいて、Catalyst Center はファイアウォール名を自動的に生成します。

c) [関連付けられているボーダーノード（Associated border nodes）] ドロップダウンリストから、必要なボーダーノードを選択します。

d) （任意） 別の仮想ネットワークを必要なボーダーノードに関連付けるには、[+] アイコンをクリックし、「5.a （1390 ページ）」から「5.c （1390 ページ）」までを繰り返します。

ステップ 6 **[ステアリングポリシーの設定（Configure steering policies）]** ウィンドウで、必要なステアリングポリシーを選択します。

ステアリングポリシーがない場合は、[ポリシーの追加（Add policy）] をクリックしてステアリングポリシーを追加します。詳細については、Day N におけるトラフィック ステアリング ポリシーの作成 （1511 ページ）を参照してください。

ステアリングポリシーを追加するには、少なくとも 1 つのステアリングコントラクトが必要です。

実行する操作	結果
ステアリングコントラクトの作成	[ステアリングコントラクトの作成（Create steering contract）] をクリックします。 詳細については、トラフィック ステアリング コントラクトの作成 （1515 ページ）を参照してください。
セキュリティグループの作成	[アクション（Actions）] にカーソルを合わせて [セキュリティグループの作成（Create security group）] を選択します。 詳細については、セキュリティグループの作成 （1416ページ）を参照してください。

ステップ 7 [Summary] ウィンドウで、設定を確認します。

変更するには、[Edit] をクリックします。

ステップ 8 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。

- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238ページ）を参照してください。

ステップ 9 [Tasks] ウィンドウで、タスクの展開を監視します。

サービス挿入サイトの編集

サービス挿入サイトを編集するには、次の手順を実行します。

手順

ステップ 1 メインメニューから次を選択します。**[プロビジョニング（Provision）]** > **[セキュリティサービスの挿入（Security Service Insertion）]** の順に選択します。

ステップ 2 [サービス挿入サイト（Service insertion sites）] タブで、サービス挿入サイト名をクリックします。

ステップ 3 サービス挿入サイトに影響を与える SD-Access アクティビティ（ボーダーノードの追加など）がある場合は、サービス挿入サイトに変更を組み込みます。

a) ファブリックサイトへの変更の詳細を表示するには、警告メッセージを確認します。

b) 対応するリンクをクリックします。

c) 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する（238ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238ページ）を参照してください。

d) [Tasks] ウィンドウで、タスクの展開を監視します。

変更がプロビジョニングされると、成功メッセージが表示されます。

ステップ 4 （任意）[仮想ネットワーク（Virtual Networks）] タブで、サービス挿入サイトのレイヤ 3 仮想ネットワークを設定します。

実行する操作	結果
仮想ネットワークを追加する	サービス挿入サイトへの仮想ネットワークの追加（1392ページ）を参照してください。
仮想ネットワークを編集する	サービス挿入サイトに関連付けられている仮想ネットワークの編集（1393ページ）を参照してください。
仮想ネットワークを削除する	サービス挿入サイトからの仮想ネットワークの削除（1393ページ）を参照してください。

ステップ 5 （任意）[ステアリングポリシー（Steering policies）] タブで、ステアリングポリシーを設定します。

実行する操作	結果
トラフィック ステアリング ポリシーを表示する	トラフィック ステアリング ポリシー（1510 ページ）を参照してください。
トラフィック ステアリング ポリシーを作成する	Day N におけるトラフィック ステアリング ポリシーの作成（1511 ページ）を参照してください。
トラフィック ステアリング ポリシーの編集	トラフィック ステアリング ポリシーの編集（1513 ページ）を参照してください。
トラフィック ステアリング ポリシーの削除	トラフィック ステアリング ポリシーの削除（1514 ページ）を参照してください。
トラフィック ステアリング ポリシーの展開	トラフィック ステアリング ポリシーの展開（1515 ページ）を参照してください。

サービス挿入サイトへの仮想ネットワークの追加

既存のサービス挿入サイトに仮想ネットワークを追加するには、次の手順を実行します。

手順

ステップ 1 メインメニューから次を選択します。**[プロビジョニング（Provision）] > [セキュリティサービスの挿入（Security Service Insertion）]** の順に選択します。

ステップ 2 サービス挿入サイト名をクリックします。

ステップ 3 [仮想ネットワーク（Virtual networks）] タブで、[新しい仮想ネットワークの追加（Add new virtual network）] をクリックします。

ステップ 4 [仮想ネットワーク（Virtual network）] ドロップダウンリストから仮想ネットワークを選択します。

ステップ 5 [ファイアウォールIP/マスク（Firewall IP/mask）] フィールドにファイアウォールの IP アドレスとサブネットマスクを入力します。

仮想ネットワークとファイアウォールの IP アドレスに基づいて、Catalyst Center はファイアウォール名を自動的に生成します。

ステップ 6 [関連付けられているボーダーノード（Associated border nodes）] ドロップダウンリストから、ボーダーノードを選択します。

ステップ 7 （任意）別の仮想ネットワークを追加するには、[+] アイコンをクリックし、「ステップ 4（1392 ページ）」から「ステップ 6（1392 ページ）」までを繰り返します。

ステップ 8 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

ステップ 9 [Tasks] ウィンドウで、タスクの展開を監視します。

サービス挿入サイトに関連付けられている仮想ネットワークの編集

既存のサービス挿入サイトに関連付けられている仮想ネットワークを編集するには、次の手順を実行します。

始める前に

関連付けられているトラフィック ステアリング ポリシーを削除します。詳細については、トラフィック ステアリング ポリシーの削除 （1514 ページ）を参照してください。

手順

ステップ 1 メインメニューから次を選択します。 **[プロビジョニング（Provision）]** > **[セキュリティサービスの挿入（Security Service Insertion）]** の順に選択します。

ステップ 2 [サービス挿入サイト（Service insertion sites）] タブで、サービス挿入サイト名をクリックします。

ステップ 3 [仮想ネットワーク（Virtual Networks）] タブで、編集するネットワークの横にあるチェックボックスをオンにします。

ステップ 4 [編集（Edit）] をクリックします。

ステップ 5 [仮想ネットワークの編集（Edit virtual networks）] スライドインペインで、必要な設定を編集します。

詳細については、サービス挿入サイトへの仮想ネットワークの追加 （1392 ページ）を参照してください。

ステップ 6 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

ステップ 7 [Tasks] ウィンドウで、タスクの展開を監視します。

サービス挿入サイトからの仮想ネットワークの削除

この手順を使用して、既存のサービス挿入サイトから仮想ネットワークを削除します。

サービス挿入サイトから仮想ネットワークを削除しても、ファブリックサイトからは削除されません。

始める前に

1. サービスの挿入サイトに関連付けられているトラフィック ステアリング ポリシーを削除します。

   詳細については、サービス挿入サイトの編集（1391ページ）またはトラフィック ステアリング ポリシーの削除（1514ページ）を参照してください。

2. デバイスに更新を展開します。

   詳細については、サービス挿入サイトの編集（1391ページ）またはトラフィック ステアリング ポリシーの展開（1515ページ）を参照してください。

手順

ステップ 1 メインメニューから次を選択します。**[プロビジョニング（Provision）]** > **[セキュリティサービスの挿入（Security Service Insertion）]** の順に選択します。

ステップ 2 [サービス挿入サイト（Service insertion sites）] タブで、サービス挿入サイト名をクリックします。

ステップ 3 [仮想ネットワーク（Virtual networks）] タブで、削除するネットワークの横にあるチェックボックスをオンにします。

ステップ 4 [Delete] をクリックします。

ステップ 5 [注意（Warning）] ダイアログボックスで [削除（Remove）] をクリックします。

ステップ 6 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する（238ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238ページ）を参照してください。

ステップ 7 [Tasks] ウィンドウで、タスクの展開を監視します。

サービス挿入サイトに関連付けられているデバイスの管理

サービス挿入サイトとして設定されているファブリックサイトでは、次のことができます。

- ファブリックサイトへのエッジノードの追加（「デバイスをファブリックに追加（1235ページ）」を参照）
- ファブリックサイトからのエッジノードの削除（「ファブリックからデバイスを削除（1239ページ）」を参照）

（注） ファブリックサイトで少なくとも 1 つのエッジノードを使用できることを確認してください。

- ファブリックサイトへのボーダーノードの追加（「ボーダーノードとしてのデバイスの追加 （1240 ページ）」を参照）
- ファブリックサイトからのボーダーノードの削除（「ファブリックからデバイスを削除（1239 ページ）」を参照）

（注） ボーダーノードがサービス挿入サイトに関連付けられている場合、ファブリックサイトから削除することはできません。

サービス挿入サイトに関連付けられているエッジノードとボーダーノードを管理できます。サービス挿入サイトに関連付けられているデバイスを管理するには、次の手順を実行します。

手順

ステップ 1 メインメニューから次を選択します。**[プロビジョニング（Provision）] > [セキュリティサービスの挿入（Security Service Insertion）]** の順に選択します。

ステップ 2 [サービス挿入サイト（Service insertion sites）] タブで、サービス挿入サイト名をクリックします。

ステップ 3 エッジノードがファブリックサイトに追加されたか、ファブリックサイトから削除された場合は、次の設定を完了します。

a) サービス挿入サイトを削除します。詳細については、「サービス挿入サイトの削除（1396ページ）」を参照してください。

b) サービス挿入サイトを有効にして、エッジノードの変更を含めます。詳細については、「サービス挿入サイトの有効化 （1389 ページ）」を参照してください。

ステップ 4 ボーダーノードがファブリックサイトに追加された場合は、次の設定を完了します。

a) 警告メッセージの対応するリンクをクリックして、サービス挿入サイトの変更内容を組み込みます。

詳細については、「サービス挿入サイトの編集 （1391 ページ）」を参照してください。

b) 仮想ネットワークを編集して、ボーダーノードをサービス挿入サイトに関連付けます。

詳細については、「サービス挿入サイトに関連付けられている仮想ネットワークの編集（1393ページ）」を参照してください。

ステップ 5 ボーダーノードがファブリックサイトから削除された場合は、警告メッセージの対応するリンクをクリックして、サービス挿入サイトの変更内容を組み込みます。

詳細については、「サービス挿入サイトの編集 （1391 ページ）」を参照してください。

サービス挿入サイトの削除

サービス挿入サイトを削除するには、次の手順を実行します。

始める前に

1. トラフィック ステアリング ポリシーがサービス挿入サイトに関連付けられている場合は、これらのポリシーを削除します。

   詳細については、トラフィック ステアリング ポリシーの削除 （1514 ページ） を参照してください。

2. トラフィック ステアリング ポリシーを削除した後、サービス挿入サイトに関連付けられているデバイスに更新を展開します。

   詳細については、トラフィック ステアリング ポリシーの展開 （1515 ページ） を参照してください。

3. 仮想ネットワークがサービス挿入サイトに関連付けられている場合は、サービス挿入サイトから仮想ネットワークを削除します。

   詳細については、サービス挿入サイトからの仮想ネットワークの削除 （1393 ページ） を参照してください。

手順

ステップ 1 メインメニューから次を選択します。 **[プロビジョニング（Provision）] > [セキュリティ サービスの挿入（Security Service Insertion）]** の順に選択します。

ステップ 2 [サービス挿入サイト（Service insertion sites）] タブで、サービス挿入サイト名をクリックします。

ステップ 3 [サイトの削除（Delete site）] をクリックします。

ステップ 4 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ） を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ） を参照してください。

ステップ 5 [Tasks] ウィンドウで、タスクの展開を監視します。

トラフィック ステアリング コントラクトの設定

この手順を使用して、セキュリティサービスの挿入用のトラフィック ステアリング コントラクトを設定します。

手順

ステップ 1 メインメニューから次を選択します。**[プロビジョニング（Provision）]** > **[セキュリティサービスの挿入（Security Service Insertion）]**の順に選択します。

ステップ 2 [ステアリングコントラクト（Steering contracts）] タブをクリックします。

ステップ 3 （任意） トラフィック ステアリング コントラクトを設定します。

実行する操作	結果
トラフィック ステアリング コントラクトの作成	[ステアリングコントラクトの作成（Create steering contract）] をクリックします。 詳細については、トラフィック ステアリング コントラクトの作成（1515 ページ）を参照してください。
トラフィック ステアリング コントラクトの編集	[その他のアクション（More Actions）] にカーソルを合わせて [編集（Edit）] を選択します。 詳細については、トラフィック ステアリング コントラクトの編集または複製 （1517 ページ）を参照してください。
トラフィック ステアリング コントラクトの複製	[その他のアクション（More Actions）] にカーソルを合わせ、[複製（Duplicate）]を選択します。 詳細については、トラフィック ステアリング コントラクトの編集または複製 （1517 ページ）を参照してください。
トラフィック ステアリング コントラクトの削除	[その他の操作（More Actions）]にカーソルを合わせて [削除（Delete）] を選択します。 詳細については、トラフィック ステアリング コントラクトの削除（1518 ページ）を参照してください。

Secure Equipment Access

Cisco Secure Equipment Access（SEA）は、産業用 OT 資産へのセキュアなリモートアクセスを可能にします。ゼロトラスト ネットワーク アクセス（ZTNA）をスイッチやルータに組み込み、セキュアなリモートアクセス機能を簡単かつ大規模に展開できるようにします。これは、

Cisco IoT Operations ダッシュボード（IoT OD）のコンポーネントの 1 つです。IoT OD は、次のようなクラウドベースのダッシュボードです。

- オペレーションズチームが業務の合理化に役立つ洞察を明らかにできるようにします。
- すべての産業用資産のセキュアで包括的な 1 つのビューで事業継続性を高めます。

SEA API は、ネットワークデバイスとネットワーク資産を簡単に統合して制御できるようにすることにより、産業用資産の合理的な管理を可能にします。RESTful 機能により、デバイスの追加、監視、削除などの機能を向上させると同時に、IoT OD 内でのセキュアなアクセスとデータ管理を実現します。

アプリケーション ホスティングは、Catalyst Center によって管理されるスイッチでの SEA のインストールをサポートします。詳細については、アプリケーションホスティングを使用したアプリケーションのインストール （1362 ページ）を参照してください。

SEA のインストールは、次のスイッチでサポートされています。

- Cisco Catalyst IE3300、IE3400、IE3400H シリーズ スイッチ（Cisco IOS-XE ソフトウェアバージョン 17.3 以降）。
- Cisco Catalyst IE9300 シリーズ スイッチ（Cisco IOS-XE ソフトウェアバージョン 17.9 以降）。
- Cisco Catalyst 9300 および Catalyst 9400 シリーズ スイッチ（Cisco IOS-XE ソフトウェアバージョン 17.3 以降）。

Catalyst Center の展開で使用する SEA を有効にして設定する方法については、このセクションのトピックを参照してください。

Cisco IoT ダッシュボードのセットアップ

Cisco IoT ダッシュボードを設定し、Secure Equipment Access（SEA）を有効にするには、次の手順を実行します。

手順

ステップ 1 まだ作成していない場合は、Cisco スマートアカウントを作成します。続行する前に、スマートアカウントのログイン情報とバーチャルアカウントを控えておいてください。

（注） EDM 管理型 IR1101 および IR1800 の場合、PnP リダイレクトにはスマートアカウントを使用する必要があります。さらに、スマートアカウントを使用すると、購入した IR1101 および IR1800 デバイスを、製造から IoT OD 組織へ自動的に登録する設定を行うことができます。

ステップ 2 iotod-account-request@cisco.com 宛てに電子メールを送り、

- 組織へのアクセスを追加して有効にし、
- SEA エージェントのインストールを有効にします（Catalyst Centerを経由）。

次のタスク

Cisco IoT ダッシュボードへのログイン （1399 ページ）。

Cisco IoT ダッシュボードへのログイン

Cisco IoT ダッシュボードにログインするには、次の手順を実行します。

始める前に

- Cisco IoT ダッシュボードのセットアップ （1398 ページ）。
- ダッシュボードは、次のブラウザの最新バージョンをサポートしています：
  - Google Chrome
  - Microsoft Edge
  - Mozilla Firefox

これらのブラウザのいずれかを使用してログインします。

手順

ステップ 1 サポートされているブラウザで、次の URL の 1 つを開きます。

- https://us.ciscoiot.com/
- https://eu.ciscoiot.com/

ステップ 2 E メールアドレスを入力し、[次へ（Next）] をクリックします。

続行するには、この手順を繰り返す必要がある場合があります。

ステップ 3 **[組織の選択（Select your organization）]** ウィンドウで、組織名をクリックします。

ステップ 4 **[Catalyst Centerとの組織の接続（Connect Organization with Catalyst Center）]** 画面で、[接続（Connect）] をクリックします。

次のタスク

Secure Equipment Access の設定 （1400 ページ）。

Secure Equipment Access の設定

SEA API の使用を有効にするには、次の手順を完了します。

始める前に

Cisco IoT ダッシュボードへのログイン （1399 ページ）

手順

ステップ 1 Catalyst Center で、[Secure Equipment Access] ウィンドウを開きます。メインメニューから、次のいずれかの手順を実行します。

- **[プロビジョニング（Provision）] > [サービス（Services）] > [Secure Equipment Access]** の順に選択します。
- **[プロビジョニング（Provision）] > [サービス（Services）] > [サービスカタログ（Service Catalog）]** の順に選択し、[Secure Equipment Access] タイルをクリックします。

ステップ 2 SEA サービスの API キーを設定します。

次を行う場合...	結果...
Catalyst Center に API キーを設定させる	**1.** [サービス接続方式（Service Connection Method）] ドロップダウンリストで、[自動（推奨）（Auto (recommended)）] を選択します。 **2.** [SEAクラスター（SEA Cluster）] ドロップダウンリストで、使用するクラスターを選択して [接続（Connect）] をクリックします。 まだリストされていないクラスターを選択するには、[その他（Other）] を選択してからクラスターの URL を入力します。
API キーを手動で生成する	**1.** [サービス接続方式（Service Connection Method）] ドロップダウンリストで、[手動（Manual）] を選択します。 **2.** Cisco IoT ダッシュボードを起動したブラウザウィンドウで、「API キーの生成 （1403 ページ）」に記載されている手順を完了します。 **3.** Catalyst Center の **[Secure Equipment Access]** ウィンドウに戻り、コピーした API キーを [APIキーシークレット（API Key Secret）] フィールドに貼り付けてから、[接続（Connect）] をクリックします。

ステップ 3 以下を確認します。

- SEA サービスのプロビジョニングが正常に完了していること。
- 組織が [SEA組織（SEA Organization）] エリアに表示されていること。

ステップ 4 以下の手順で [リモートアクセスの有効化（Enable Remote Access）] ウィザードを完了します。

a) ウィザードを開始します。[製品ファミリの選択（Select product family）] エリアで、シスコデバイスのプロセッサタイプを選択し、[SEAエージェントのプロビジョニング（Provision SEA Agents）] をクリックします。

b) デバイスが存在するサイトを選択し、[次へ（Next）] をクリックします。

（注） サイトがグレー表示されている場合、SEAエージェントを展開できるデバイスがそのサイトに含まれていないことを示します。

c) SEAエージェントを展開するデバイスのチェックボックスをオンにしてから、[次へ（Next）]をクリックします。

（注）
- デバイスがグレー表示されている場合、展開の準備ができていません。デバイスの準備が整うまで待ってから、ウィザードを再度完了する必要があります。[準備中（Not Ready）] ステータスをクリックしてエラーを確認します。
- 一度に最大 10 台のデバイスにエージェントを展開できます。

d) SEA エージェントをブートストラップするように次の設定を構成してから、[次へ（Next）] をクリックします。

- [HTTP接続プロキシの有効化（Enable HTTP Connect Proxy）] : このオプションが選択されていることを確認します。
- [プロキシURL（Proxy URL）] : プロキシサーバーの URL を入力します。
- [VLAN ID] : （エージェント、デバイス、Catalyst Center が使用する）管理インターフェイスの VLAN ID を入力します。
- [IP割り当て（IP Assignment）] : [動的（Dynamic）] または [静的（Static）] を選択します。[静的（Static）] を選択した場合は、詳細を含む CSV ファイルをアップロードする必要があります。

e) ウィザードの [概要（Summary）] ウィンドウで、指定した設定を確認してから [アプリケーションの展開（Deploy App）] をクリックします。

[SEAエージェントの管理（Manage SEA Agents）] ウィンドウが開きます。

f) 展開が完了したら、各デバイスの [アクションステータス（Action Status）] 列に [実行中（Running）] と表示されていることを確認します。

ステップ 5 選択したデバイスで実行されている SEA エージェントと Catalyst Center 間の接続が動作していることを確認します。

a) Cisco IoT Operations ダッシュボードを起動したブラウザウィンドウに戻ります。
b) メインメニューから [システム管理（System Management）] をクリックし、**[システム管理（System Management）]** ウィンドウを開きます。
c) エージェントを展開したデバイスがウィンドウの下部に表示されていることを確認します。
d) [SEAエージェント接続（SEA Agent Connection）] 列で、これらの各デバイスに対して `Up` と表示されていることを確認します。

ステップ 6 運用テクノロジー（OT）資産を追加します。

a) **[システム管理（System Management）]** ウィンドウで、適切なデバイスのリンクをクリックします。
b) [資産（Assets）] エリアで [+資産の追加（+ Add Asset）] をクリックして、[資産の追加（Add Asset）] スライドインペインを開きます。
c) 次の設定を構成してから、[追加（Add）] をクリックします。
   - [資産名（Asset Name）]：資産の名前を入力します。
   - [IPアドレス（IP Address）]：資産の IP アドレスを入力します。
   - （オプション）[説明（Description）]：資産の説明を入力します。
d) 追加した資産が [資産（Assets）] エリアに表示されていることを確認します。
e) 追加する OT 資産ごとに手順 6a ～ 6d を繰り返します。

ステップ 7 追加した OT 資産のアクセス方法を設定します。

a) 資産のリンクをクリックします。
b) [アクセス方法（Access Methods）] エリアで [+アクセス方法の追加（+ Add Access Method）] をクリックし、[アクセス方法の追加（Add Access Method）] スライドインペインを開きます。
c) 次の設定を構成してから、[追加（Add）] をクリックします。
   - [アクセス方法（Access Method）]：ドロップダウンリストから使用するアクセス方法を選択します。
   - [ポート（Port）]：使用するポートを入力します。
   - [セッションタイムアウト（Session Timeout）]：非アクティブ状態が原因でセッションタイムアウトになるまでに経過する必要がある時間を指定します。
   - [ユーザー名（Username）] と [パスワード（Password）]：適切なログイン情報を入力します。
   - [名前（Name）]：設定しているアクセス方法の名前を入力します。
   - （オプション）[説明（Description）]：アクセス方法の説明を入力します。
d) 追加したアクセス方法が [アクセス方法（Access Methods）] エリアに表示されていることを確認します。
e) 追加するアクセス方法ごとに手順 8a ～ 8d を繰り返します。

ステップ 8 作成したいずれかのアクセス方法を使用してリモートセッションを確立します。

a) Cisco IoT Operations ダッシュボードのメインメニューから、[リモートセッション（Remote Sessions）] をクリックします。
b) 使用するアクセス方法のタイルで、[接続（Connect）] をクリックします。
c) アクセス方法に設定されたログイン情報を入力します。

API キーの生成

API キーを生成するには、次の手順を完了します。

始める前に

Cisco IoT ダッシュボードへのログイン （1399 ページ）。

手順

ステップ 1 Cisco IoT ダッシュボードの右上隅にあるログイン名を表示するドロップダウンリストをクリックしてから、[アクセス制御（Access Control）] をクリックします。

ステップ 2 [アクセス制御（Access Control）] ウィンドウで、[APIキー（Access Control）] タブをクリックします。

ステップ 3 [APIキーの生成（Generate API Key）] リンクをクリックします。

ステップ 4 次の情報を入力し、[生成（Generate）] をクリックします。

- [名前（Name）]：API キーの名前を入力します。
- [ロール（Role）]：適切なユーザーロールを入力します。
- [有効期限（Expiration）]：この API キーを有効にする期間を選択します。

ステップ 5 [APIキーの生成（Generate API Key）] ウィンドウの下部にあるコピーアイコンをクリックし、生成された API キーをコピーします。

Cisco Cyber Vision Center と Catalyst Center の統合

Catalyst Center は、ネットワーク セキュリティ ソリューションである Cisco Cyber Vision との統合をサポートしています。ブラウザベースのマネージャは、Cisco Cyber Vision Center と呼ばれます。Cyber Vision Center は、ネットワークデバイスの監視と管理に役立ちます。

Cisco Cyber Vision 機能は、Catalyst Center で**産業用アプリケーション オーケストレータ** パッケージをインストールすると、Catalyst Center UI の **[プロビジョニング（Provision）]** > **[サービス（Services）]** メニューに表示されます。詳細については、『Cisco Catalyst Center Administrator Guide』の「Download and install applications」を参照してください。

アクティブ検出をサポートする Cyber Vision アプリケーション（CiscoCyberVision-IOx-Active-Discovery-aarch64-5.2.0.tar など）は、Catalyst Center にデフォルトでバンドルされています。簡素化された Cyber Vision アプリケーション展開ワークフローは、このアプリケーションをサポートしています。アクティブ検出をサポートしていない Cyber Vision アプリケーション（CiscoCyberVision-IOx-aarch64-5.2.0.tar など）は、Catalyst Center のアプリケーションホスティングにアップロードできます。このアプリケーションは、アプリケーション名とアプリケーション ID が異なり、Cyber Vision 展開トークンが必要です。そのため、簡素化された Cyber Vision アプリケーション展開ワークフローはサポートされていません。このアプリケーションを IE デバイスに展開するには、標準のアプリケーション展開ワークフローを使用し、必要なすべての展開パラメータを手動で指定します。

Cyber Vision アプリケーションの展開は、IE3300、IE3400、IE3400H、IE3500、IE3500H、IE9300 高耐久性シリーズ スイッチでサポートされています。

Cyber Vision Center の管理

Catalyst Center の Cyber Vision Center を追加、編集、および削除できます。

手順

ステップ 1 メインメニューから次を選択します。**[プロビジョニング（Provision）] > [サービス（Services）] > [Cisco Cyber Vision]**の順に選択します。

ステップ 2 「Cyber Vision Center のトークンを取得するための手順」を読み、展開トークンを生成します。

詳細については、『Cisco Cyber Vision GUI アドミニストレーション ガイド』を参照してください。

Cyber Vision Center の追加

ステップ 3 [センターの管理（Manage Centers）] ドロップダウンリストから [追加（Add）] を選択します。

ステップ 4 [Cyber Vision Centerの追加（Add Cyber Vision Centers）] ウィンドウで、Cyber Vision Center の [名前（Name）]、[ホスト名/IPアドレス（Hostname/IP Address）]、および [トークン（Token）] を入力します。[Add] をクリックします。

[行の追加（Add Row）] をクリックすると、最大 20 の Cyber Vision Center を追加できます。

Cyber Vision Center の編集

ステップ 5 [センターの管理（Manage Centers）] ドロップダウンリストから [編集（Edit）] を選択します。

ステップ 6 必要に応じて [名前（Name）] および [ホスト名/IPアドレス（Hostname/IP Address）] を編集し、[保存（Save）] をクリックします。

Cyber Vision Center に関連付けられたセンサーがない場合にのみ、[ホスト名/IPアドレス（Hostname/IP Address）] を編集できます。

ステップ 7 変更の保存に関する警告メッセージが表示されたら、[保存（Save）] をクリックします。

Cyber Vision Center の削除

ステップ 8 [アクション（Actions）] ドロップダウンリストから、[削除（Remove）] を選択します。

ステップ 9 Cyber Vision Center を選択し、[削除（Remove）] をクリックします。

Cyber Vision Center は、関連付けられているセンサーがない場合にのみ削除できます。

Cyber Vision Center のセンサーの展開

Catalyst Center によって管理されるスイッチに Cyber Vision センサーアプリケーションを展開できます。

Before you begin

次の前提条件が満たされていることを確認してください。

- スイッチでサポートされているハードウェアおよびソフトウェアのバージョンを確認します。
- スイッチにある SD カードをフォーマットまたはパーティションします。
- Cyber Vision Center に到達可能になるように、スイッチでアップリンクインターフェイスとルートを設定します。
- スイッチの NTP サーバーの日付および時刻を Cyber Vision Center と同期します。
- スイッチで HTTPS、SSH、またはその両方のプロトコルを有効にします。
- キャプチャ VLAN は、AppGigabitEthernet1/1 インターフェイス以外の物理インターフェイスまたはトランクに含まれていません。
- 展開する前に、CLI テンプレートを使用してスイッチに前提条件設定をプッシュします。詳細については、『Cisco Cyber Vision Sensor Application for Cisco Switches Installation Guide』の「Initial Configuration」を参照してください。
- Catalyst Center で追加された Cyber Vision Center 展開トークンが現在有効であり、期限切れや使用回数に達していないことを確認してください。

手順

ステップ 1 メインメニューから次を選択します。**[プロビジョニング（Provision）] > [サービス（Services）] > [Cisco Cyber Vision]**の順に選択します。

ステップ 2 センサーアプリケーションを展開する Cyber Vision Center に対応する [センサーアプリケーションの展開（Deploy Sensor Apps）] をクリックします。

ステップ 3 [前提条件の確認（Review Prerequisites）] ウィンドウに示されている前提条件を満たし、[次へ（Next）]をクリックします。

ステップ 4 [サイトの選択（Select Site）] ウィンドウで、アプリケーションを有効にするサイトを選択し、[次へ（Next）] をクリックします。

ステップ 5 [スイッチの選択（Select Switches）] ウィンドウで、Cyber Vision センサーアプリケーションを展開するスイッチを選択し、[次へ（Next）] をクリックします。

一度に最大 10 個のスイッチを選択できます。

ステップ 6 [ネットワークの設定（Configure Network）] ウィンドウで、[コレクションインターフェイス（Collection Interface）] と [キャプチャインターフェイス（Capture Interface）] の設定を完了します。[Next] をクリックします。

コレクションインターフェイスはセンサー通信を処理します。キャプチャインターフェイスはトラフィックを監視します。

ステップ 7 [概要（Summary）] ウィンドウで構成を確認し、[展開（Deploy）] をクリックします。

展開ステータスは、[アプリケーションホスティング（Application Hosting）] ページに表示されます。詳細については、デバイスでホストされているアプリケーションの表示（1361 ページ）を参照してください。



第 VI 部

ポリシーの設定

- グループベースのアクセス コントロール ポリシーおよび分析の設定 （1409 ページ）
- IP ベースおよび URL ベースのアクセス コントロール ポリシーの設定 （1443 ページ）
- アプリケーションポリシーの設定 （1453 ページ）
- トラフィックコピーポリシーの設定 （1487 ページ）
- ルールベースのコンプライアンスポリシーの設定 （1493 ページ）
- トラフィック ステアリング ポリシーの設定 （1509 ページ）



第 24 章

グループベースのアクセス コントロール ポリシーおよび分析の設定

- グループベースのアクセスコントロール （1409 ページ）
- シスコのグループベースポリシー分析 （1427 ページ）

グループベースのアクセスコントロール

Catalyst Center は、次の 2 つの方法で Software-Defined Access（SD-Access）を実装します。

- 仮想ネットワーク（VN）は、たとえば、企業のネットワークから IoT デバイスを分離するといった、マクロレベルのセグメンテーションを提供します。
- グループベースのポリシーは、たとえば、エンジニアリンググループと HR グループの間で許可または拒否するネットワークトラフィックのタイプを制御するといった、マイクロレベルのセグメンテーションを提供します。

グループベースのアクセス コントロール ポリシーには、次の利点があります。

- ネットワークの自動化とアシュアランスの利点を備えた、豊富なアイデンティティベースのアクセス制御機能。
- きめ細かいアクセス制御。
- セキュリティグループは、すべての仮想ネットワークに適用されるため、ポリシー管理が簡素化されます。
- ポリシービューは、全体的なポリシー構造を理解し、必要なアクセス コントロール ポリシーを作成または更新するのに役立ちます。
- さまざまなアプリケーションを切り替えてセキュリティグループを管理し、保護される資産を定義する必要がなくなります。
- エンタープライズ全体のアクセス コントロール ポリシーを展開するための拡張機能を提供します。

- アイデンティティまたはネットワーク アドミッション コントロール（NAC）アプリケーションが配置される前に、ランサムウェアなどの脅威のラテラルムーブメントを制限します。
- サードパーティのアイデンティティ アプリケーションを使用しているが、Cisco ISE に移行したいユーザーに対して、Cisco Identity Services Engine（Cisco ISE）への簡単な移行パスを提供します。

Catalyst Center での IP プール、サイト、および仮想ネットワークの作成方法については、*Catalyst Center* 管理者ガイド [英語] を参照してください。

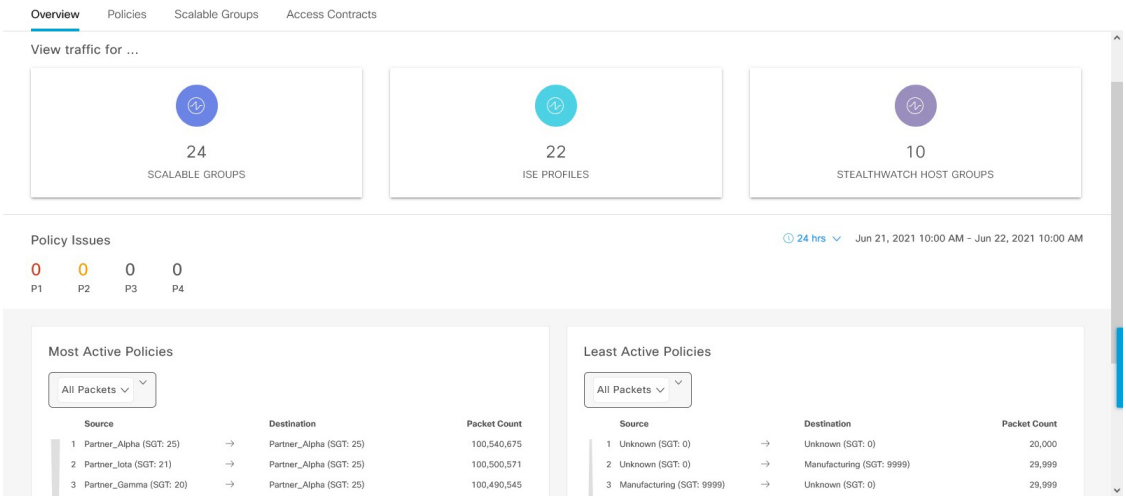
Cisco ISE 向け Catalyst Center の設定の詳細については、*Catalyst Center* 設置ガイド [英語] を参照してください。

Cisco ISE for Catalyst Center の設定の詳細については、Cisco Identity Services Engine 管理者ガイド [英語] を参照してください。

グループベースのアクセス コントロール ポリシー ダッシュボード

グループベースのアクセスコントロールポリシーダッシュボードでは、ネットワークアクティビティ、ポリシー関連の問題、およびトラフィックトレンドの概要が提供されます。このダッシュボードを表示するには、メインメニューから次を選択します。**[Policy]** > **[Group-Based Access Control]** > **[Overview]** の順に選択します。

図 *29* : グループベースのアクセス コントロール ポリシー ダッシュボード



このダッシュボードでは、次の詳細を表示できます。

- [View Traffic]：セキュリティグループ、Cisco ISE プロファイル、および Stealthwatch ホストグループのトラフィックを表示できます。このデータを表示するには、グループベースポリシー分析パッケージをインストールする必要があります。グループベースポリシー分析で提供される分析情報により、新しいアクセスコントロールの導入による影響を評価するために、資産間の通信を可視化してグループベースポリシーを作成したり、そのポリシーで許可する必要があるプロトコルを正確に特定することができます。シスコのグルー

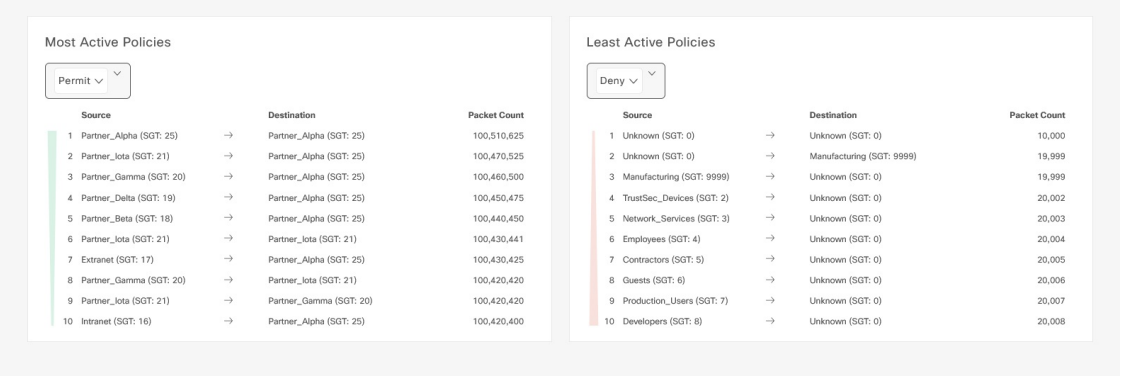
プベースポリシー分析では、ネットワーク上のアセットのグループとそれらの通信に関する情報が集約されます。詳細については、シスコのグループベースポリシー分析（1427ページ）を参照してください。

- [View Policy-Related Issues]：ポリシー関連の問題の数が表示されます。数をクリックすると詳細情報が表示されます。新しいブラウザタブで [Assurance Issues] ダッシュボードが開きます。ここで、詳細情報を確認できます。

（注） このポリシー関連の問題のビューは、現在選択されている期間のものとなります。必要に応じて、時間セレクタを使用して時間枠を調整します。

- [View Most Active and Least Active Policies]：最もアクティブなポリシーと最もアクティブでないポリシーの詳細情報が提供されます。デフォルトでは、このビューは、各ポリシー（各送信元/宛先グループペア）に関してネットワークで確認されたパケットの総数に基づいています。ドロップダウンリストを使用して、許可されたパケットまたはドロップされたパケットのみを選択することができます。ドロップされたパケットのオプションを使用すると、ポリシーベースのドロップが最もアクティブに実行されているポリシーを確認することができます。

図 *30*：最もアクティブなポリシーのダッシュレットと最もアクティブでないポリシーのダッシュレット



（注） このポリシーアクティビティのビューは、現在選択されている期間のものとなります。必要に応じて、時間セレクタを使用して時間枠を調整します。

グループベースのアクセス コントロール ポリシー

アクセス コントロール ポリシーでは、送信元セキュリティグループから宛先セキュリティグループに渡すことができるネットワークトラフィックを定義します。

- [Security Group]：ユーザー、ネットワークデバイス、またはリソースを割り当てることができる分類カテゴリ。セキュリティグループは、アクセス コントロール ポリシーで使用されます。組織のネットワーク設定、アクセス要件、および制限に基づいて、セキュリティグループを仮想ネットワークに関連付けることができます。

- [Contract]：アクセス契約は、送信元と宛先のセキュリティグループ間の通過を許可されるネットワークトラフィックのタイプを制御する一連のルールです。つまり、契約はトラフィックフィルタの定義です。アクセス契約は、トラフィックがネットワーク アプリケーション、プロトコル、およびポートに一致したときに実行されるアクション（許可または拒否）を定義します。他のルールが一致しない場合、デフォルトアクションでは catch all ルールが使用されます。

- **グループベースのアクセス コントロール ポリシー**：グループベースのアクセス コントロール ポリシーは、特定の送信元と宛先グループのペアを識別し、アクセス契約を関連付けます。アクセス契約は、送信元グループと宛先グループの間で許可または拒否されるトラフィックのタイプを指定します。これらのポリシーは単方向です。

  セキュリティグループおよびアクセス契約は、アクセス コントロール ポリシーの基本的な構成要素です。アクセスコントロールポリシーを作成する際には、前に作成したセキュリティグループと契約を使用したり、ポリシーの作成時に新しいセキュリティグループと契約を作成したりできます。特定の送信元グループからアクセスできるネットワークリソースを指定する場合は、1つの送信元グループと複数の宛先グループを含むアクセス コントロールポリシーを作成できます。一方、特定のネットワークリソースへのアクセスが許可されている送信元グループを指定する場合は、1 つの宛先グループと複数の送信元グループを含むアクセス コントロール ポリシーを作成できます。たとえば、請負業者送信元セキュリティグループに関連付けられたユーザーがアクセスできるネットワークリソースを指定する場合は、1 つの送信元グループと複数の宛先グループを含むアクセス コントロールポリシーを作成できます。財務サーバー宛先セキュリティグループへのアクセスが許可されている送信元グループを指定する場合は、1 つの宛先グループと複数の送信元グループを含むアクセス コントロール ポリシーを作成できます。

  送信元と宛先のセキュリティグループの組み合わせに契約が指定されていない場合に使用されるデフォルトポリシーを指定できます。デフォルトポリシーは [Permit] です。必要に応じて、このポリシーを [Deny]、[Permit_IP_Log]、または [Deny_IP_Log] に変更できます。ネットワークタイプ（オープンネットワークまたはクローズドネットワーク）に基づいて、デフォルトポリシーを設定できます。

（注） すべてのネットワーク インフラストラクチャ デバイスに必要なネットワークトラフィックを許可する明示的なポリシーを作成した場合のみ、デフォルトポリシーを [Permit] から [Deny] に変更することをお勧めします。そのようにしない場合、すべてのネットワーク接続が失われる可能性があります。

リストビュー

[Group-Based Access Control] ウィンドウの右上隅にある [List] アイコンをクリックして、[List] ビューを起動します。

- [Source View]：送信元グループに基づいて編成された既存のポリシーのリストが表示されます。各行を展開して、特定の送信元と宛先のポリシーの詳細を表示できます。
- [Destination View]：宛先グループに基づいて編成された既存のポリシーのリストが表示されます。各行を展開して、特定の送信元と宛先のポリシーの詳細を表示できます。

特定の送信元グループから使用可能な宛先グループを確認するには、[Source] ビューを使用します。特定の宛先グループへのアクセスが許可されている送信元グループを確認するには、[Destination] ビューを使用します。たとえば、請負業者送信元セキュリティグループの一部であるユーザーが使用できる宛先グループを確認するには、[Source] ビューを使用します。財務サーバー宛先セキュリティグループにアクセスできる送信元グループを確認するには、[Destination] ビューを使用します。

ポリシー適用統計データをポリシーリストテーブルで表示することもできます。選択した期間内のポリシーの許可と拒否の総数が表示されます。

ポリシー適用統計は、グループベースのポリシーおよびテレメトリデータ言語（TDL）サブスクリプション用にプロビジョニングされたネットワークデバイスから収集されます。これらの設定は、通常、ファブリックの一部であるネットワークデバイスに関して自動的にプロビジョニングされます。非ファブリック ネットワーク デバイスに関しては手動設定を実行できます。

ポリシー適用統計データを使用する場合は、次の点を考慮してください。

- ポリシー適用統計データは、グループベースポリシー分析パッケージが展開されている場合にのみ使用できます。
- テレメトリ サブスクリプションは、ファブリック ネットワーク デバイスと非ファブリック ネットワーク デバイスの両方に関する基本プロビジョニングの一部として追加されます。新しいネットワークデバイスが Catalyst Center に追加され、サイトに割り当てられると、TrustSec 適用アクションが呼び出されます。
- Software-Defined Access（SD-Access）は、ファブリックに追加されたネットワークデバイスに TrustSec 適用を追加します。TrustSec テレメトリデータは、ネットワークデバイスでこの適用が有効になっている場合にのみ収集されます。有効になっていない場合は、ポリシーモニターリングに使用されるテレメトリ サブスクリプションが TrustSec の TDL データの収集に使用されます。
- Cisco IOS XE 16.12 以降では、TDL ストリーミングデータがサポートされています。
- ネットワークデバイスで NETCONF を有効にする必要があります。
- 非ファブリック ネットワーク デバイスについては、次の設定を手動で追加する必要があります。

```
cts role-based enforcement vlan-list <VLAN of the endpoints>
```

- アップグレード後、[プロビジョニング（Provision）] > [ネットワークデバイス（Network Devices）] > [インベントリ（Inventory）] ウィンドウに次のメッセージが表示されます。

  IOS-XE デバイスがネットワークで検出されました。これには、保証データの新しいテレメトリ サブスクリプションを有効にし、既存のサブスクリプションの一部をパフォーマンスのために最適化する必要があります。netconf を有効にし、これらのデバイスのインベントリクレデンシャルで netconf ポートを設定する必要があることに注意してください。また、これらのデバイスは、グループベースのポリシー モニターリング テレメトリの新しいサブスクリプションを受信することに注意してください。これらのサブスクリプションをプロビジョニングするためのアクションを実行しますか?

  [Apply Fix] をクリックして、サイトが割り当てられているすべてのネットワークデバイスに設定をプッシュします。

マトリックスビュー

[Group-Based Access Control] ウィンドウの右上隅にある [Grid] アイコンをクリックして、[Matrix] ビューを起動します。[Matrix] ビューは中核となるポリシービューであり、すべてのセキュリティグループのすべてのポリシー（明示的とデフォルトの両方）の概要を提供します。[Matrix] ビューを使用して、すべての送信元と宛先のポリシーを表示し、全体的なポリシー構造を理解できます。[Matrix] ビューからアクセス コントロール ポリシーを表示、作成、および更新できます。

[Matrix] ビューには、次の 2 つの軸があります。

- 送信元軸：垂直軸にはすべての送信元セキュリティグループがリストされます。
- 宛先軸：水平軸にはすべての宛先セキュリティグループがリストされます。

特定の送信元セキュリティグループと宛先セキュリティグループのポリシーを表示するには、セルにカーソルを置きます。セルの色は、そのセルに適用されるポリシーに基づいています。色は、次のとおり各セルに適用されるポリシーを示しています。

- [Permit]：緑色
- [Deny]：赤色
- [Custom]：金色
- [Default]：灰色

マトリックスの上部に表示される [許可（Permit）]、[拒否（Deny）]、[カスタム（Custom）]、または [デフォルト（Default）] アイコンにカーソルを置くと、そのポリシーが適用されているセルが表示されます。

[Matrix] ビューでは、セルを選択すると、そのセルと対応する行（送信元セキュリティグループ）と列（宛先セキュリティグループ）が強調表示されます。選択したセルの座標（送信元および接続先セキュリティグループ）がマトリックス コンテンツ エリアの近くに表示されます。

セルをクリックして、そのセルの [Create Policy] または [Edit Policy] スライドインペインを開きます。[Create Policy] スライドインペイン には、送信元と宛先のセキュリティグループが読み取り専用フィールドとして表示されます。そのセルのポリシーのステータスとアクセス契約の更新のみ実行できます。

ポリシーマトリックスのカスタムビューを作成して、関心のあるポリシーだけに絞り込むことができます。これを実行するには、[View] ドロップダウンリストから [Create View] を選択します。カスタムビューを作成するときに、カスタムビューに含めるセキュリティグループのサブセットを指定できます。必要に応じて、カスタムビューを保存し、後で編集することができます。[View] ドロップダウンリストから、[Manage Views] を選択して、カスタムビューを作成、編集、複製、または削除します。[Default View] には、すべての送信元および宛先セキュリティグループが表示されます。

カーソルをマトリックスコンテンツ領域でドラッグするか、または水平および垂直スクロールバーを使用して、マトリックス内を移動できます。ミニマップを使用して、マトリックス内を移動することもできます。ミニマップを使用すると、マトリックスのサイズが大きく、画面サイズを超えている場合に、マトリックス内を簡単に移動できます。ミニマップは、画面上の任意の場所に移動して配置できます。ミニマップにはマトリックスビュー全体が表示されます。ミニマップの薄い灰色の部分は、画面に現在表示されているマトリックスの部分を表します。カーソルをこの領域でドラッグして、マトリックスをスクロールできます。



（注） ミニマップはデフォルトで閉じられています。[Expand]アイコンをクリックして、ミニマップを展開して表示します。

[Filter]オプションを使用して、選択した一連の送信元および宛先グループのポリシーマトリックスのサブセットを表示します。関心のあるポリシーのみに焦点を当てるフィルタを作成できます。フィルタを作成するには、含める送信元および宛先グループを選択します。

ポリシー作成の概要

1. 組織の分類を定義するか、または最初に使用する組織の一部を定義します。
2. 特定した分類のセキュリティグループを作成します。
3. 制御するネットワークトラフィックのタイプのアクセス契約を作成します。すべてのトラフィックを許可または拒否するためのサンプルアクセス契約が事前に定義されています。また、一部の契約例では、より具体的なトラフィックフィルタリングが示されています。特定のアプリケーション定義に基づいて、さらにきめ細かいアクセス契約を作成できます。
4. アプリケーションサーバーや他のネットワークへの接続など、特定のネットワークリソースへのアクセスを必要とするネットワークユーザーのカテゴリを決定します。
5. アクセスポリシーを作成し、送信元グループ、宛先グループ、およびアクセス契約を関連付け、送信元から宛先へのトラフィックのフローを許可する方法を定義します。

セキュリティグループの作成

始める前に

このタスクを実行するには、スーパー管理者またはネットワーク管理者である必要があります。

手順

ステップ 1 メインメニューから次を選択します。**[Policy]** > **[Group-Based Access Control]** > **[Security Groups]** の順に選択します。

ステップ 2 [セキュリティグループの作成（Create Security Group）] をクリックします。

ステップ 3 [Create Security Group] スライドインペインで、セキュリティグループの名前と説明（任意）を入力します。



（注） [名前（Name）] フィールドでサポートされる文字は次のとおりです。

- 英数字
- アンダースコア (_)

セキュリティグループ名は英字で開始する必要があります。

Catalyst Center タグ値を生成します。必要に応じて、この値を更新できます。指定した値が既存のセキュリティグループによってすでに使用されている場合は、エラーメッセージが表示されます。有効な範囲は 2 ～ 65519 です。

ステップ 4 [Virtual Networks] ドロップダウンリストから、このセキュリティグループに関連付ける仮想ネットワークを選択します。デフォルトでは、デフォルトの仮想ネットワークが選択されています。



（注） Catalyst Center 2.3.3 以降が Cisco ISE 3.2 以降と統合されている場合、セキュリティグループは仮想ネットワークに関連付けられず、これらのリリースでは [仮想ネットワーク（Virtual Networks）] フィールドは表示されません。ただし、Cisco ISE 3.1 以前を使用している場合は、セキュリティグループと仮想ネットワークの関連付けの詳細が表示されます。

ステップ 5 セキュリティグループを Cisco Application-Centric Infrastructure（ACI）に伝播する場合は、[Propagate to ACI] チェックボックスをオンにします。

ステップ 6 セキュリティグループを今すぐ作成するか、後でスケジュールするかを選択します。

[Automation Events for ITSM (ServiceNow)] バンドルが有効になっている場合、[Save Now] オプションは無効になり、グループベースのポリシー変更に対する [Schedule Later] オプションのみが有効になります。スケジュールされたタスクは、スケジュールされた時刻の前に IT サービス管理（ITSM）で承認される必要が

あります。スケジュールされた時刻までにタスクが承認されない場合、タスクは失敗します。ITSM と Catalyst Center の統合方法の詳細については、『*Cisco Catalyst Center ITSM Integration Guide*』を参照してください。

[Security Groups] ウィンドウの右上隅で、今後のタスク、進行中のタスク、および失敗したタスクの合計数を確認できます。**[Activities] [Tasks]** でタスクのステータスリンクをクリックすると、タスクの詳細が表示されます。タスクは、実行前に編集またはキャンセルできます。

（注） 名前が「ANY」またはタグ値が 0xFFFF/65535 のセキュリティグループは作成できません。セキュリティグループ ANY/65535 は、Catalyst Center デフォルトポリシーに使用される予約済みの内部セキュリティグループです。

セキュリティグループの編集

始める前に

このタスクを実行するには、スーパー管理者またはネットワーク管理者である必要があります。

手順

ステップ 1 メインメニューから次を選択します。**[Policy]** > **[Group-Based Access Control]** > **[Security Groups]** の順に選択します。

ステップ 2 [Security Groups] ウィンドウで、編集するセキュリティグループの横にあるチェックボックスをオンにし、[Edit] をクリックします。

ステップ 3 [Edit Security Group] スライドインペインで、必要な変更を加えた後、次の操作を実行します。

- 変更をすぐに保存するには、[Save Now] をクリックします。
- 特定の時間に更新をスケジュールするには、[Schedule Later] をクリックします。[Scheduler] スライドインペインで、開始時刻、日付、およびタイムゾーンを指定し、[Apply] をクリックします。

セキュリティグループを更新する場合は、ネットワークデバイスに変更を展開する必要があります。[Deploy Now] をクリックして変更をすぐに展開するか、[Deploy Later] をクリックして変更を後で展開します。

セキュリティグループの削除

始める前に

このタスクを実行するには、スーパー管理者またはネットワーク管理者である必要があります。

手順

ステップ 1 メインメニューから次を選択します。**[Policy]** > **[Group-Based Access Control]** > **[Security Groups]** の順に選択します。

ステップ 2 削除するセキュリティグループの横にあるチェックボックスをオンにします。

ステップ 3 次のオプションのいずれかを選択します。

- セキュリティグループをすぐに削除するには、[Delete Now] をクリックします。
- 後でセキュリティグループを削除するには、[Delete Later] をクリックします。[Schedule Delete] スライドインペインで、開始時刻、日付、およびタイムゾーンを指定し、[Apply] をクリックします。



（注） セキュリティグループの [Policies] 列のリンクをクリックすると、そのセキュリティグループとそのグループが属するポリシーを使用するアクセスコントロールルールが表示されます。セキュリティグループがいずれかのアクセスポリシーで使用されている場合、そのセキュリティグループは削除できません。

Catalyst Center と Cisco ISE 間のセキュリティグループの同期

Catalyst Center 内のセキュリティグループを Cisco ISE と同期しているときは、次のように動作します。

- セキュリティグループが Catalyst Center に存在し、Cisco ISE に存在しない場合は、Cisco ISE に作成されます。
- セキュリティグループが Cisco ISE に存在し、Catalyst Center に存在しない場合は、Catalyst Center に作成されます。
- セキュリティグループ名が Catalyst Center と Cisco ISE の両方で同じで、説明と ACI データが異なっている場合、Catalyst Center は Cisco ISE で指定されたデータを使用して更新されます。
- Catalyst Center と Cisco ISE でセキュリティグループ名が同じで、タグ値が異なっている場合、Cisco ISE で指定されたタグ値を持つ新しいセキュリティグループが Catalyst Center に

作成されます。Catalyst Center にすでにあるセキュリティグループの名前は、サフィックス **_DNAC** で更新されます。

- タグの値が同じでセキュリティグループ名が異なる場合、Catalyst Center のセキュリティグループ名が Cisco ISE で指定された名前で更新されます。

Cisco ISE との同期が完了していない場合は、セキュリティグループの横にオレンジ色の三角形のアイコンが表示されます。

Cisco ISE は、内部エンドポイントグループ（IEPG）を同期し、Cisco ISE に関連付けられている読み取り専用セキュリティグループを作成することで、ACI から TrustSec ドメインへのパケットをサポートします。これらのセキュリティグループは、[Created In] 列の値が **ACI** となって [Security Groups] ウィンドウに表示されます。ACI から学習したセキュリティグループは編集も削除もできませんが、ポリシーで使用することはできます。

[Associated Contracts] 列には、ACI から学習したセキュリティグループに関連付けられている契約が表示されます。[Associated Contracts] 列に表示されるリンクをクリックすると、関連付けられた契約に関する詳細が表示されます。

IEPG が ACI で更新されると、対応するセキュリティグループ設定が Cisco ISE で更新されます。Cisco ISE でセキュリティグループが作成されると、新しい EEPG が ACI に作成されます。

アクセス契約の作成

アクセス契約は、送信元と宛先のセキュリティグループ間の通過を許可されるネットワークトラフィックのタイプを制御する一連のルールです。アクセス契約は、トラフィックがネットワークアプリケーション、プロトコル、およびポートに一致したときに実行されるアクション（許可または拒否）を定義します。

始める前に

このタスクを実行するには、スーパー管理者またはネットワーク管理者である必要があります。

手順

ステップ 1 メインメニューから次を選択します。**[Policy]** > **[Group-Based Access Control]** > **[Access Contracts]** の順に選択します。

ステップ 2 [Create Access Contract] をクリックします。

ステップ 3 [Create Access Contract] スライドインペインで、必要な詳細を入力します。

[Modeled Access Contract] チェックボックスはデフォルトで有効になっています。これにより、Catalyst Center が基盤となるセキュリティグループ ACL（SGACL）の有効なコマンドを生成します。このオプションを有効にすると、アクセス契約は、基盤となるコマンドラインシンタックスを知らなくても作成および編集できるモデルに基づくようになります。

SGACL コマンドラインを直接入力し、アクセス契約をテキストとして保存する場合は、[Modeled Access Contract] チェックボックスをオフにします。 入力したコマンドラインのテキストに対してシンタックスチェックは行われません。コマンドシンタックスが有効であることを確認する必要があります。



（注）
- このオプションは、アクセス契約の作成時にのみ有効または無効にできます。既存のアクセス契約では、このオプションを更新できません。
- SGACL コマンドが高度なものは、Cisco ネットワーク デバイスでサポートされていない場合もあります。

ステップ 4 トラフィックフィルタルールを作成します。

- [Action] ドロップダウンリストで、[Deny] または [Permit] を選択します。
- [Application] ドロップダウンリストから、アクションを適用するアプリケーションを選択します。ポートとプロトコルは、選択したアプリケーションに基づいて自動的に選択されます。

  トランスポートプロトコル、送信元ポート、および宛先ポートを指定する場合は、[Application] ドロップダウンリストから [Advanced] オプションを選択します。

複数のルールを作成できます。1 つの契約に複数のルールを作成するには、[+] 記号をクリックし、[Action] 列と [Application] 列の設定を選択します。ルールは、契約に記載されている順序でチェックされます。ルールの左端にあるハンドルアイコンを使用してドラッグして、ルールの順序を変更します。

[Logging] トグルを使用して、任意のトラフィックフィルタルール（デフォルトアクションを含む）のロギングを有効化または無効化できます。ロギングはデフォルトではディセーブルになっています。ロギングが有効になっている場合、トラフィックフィルタルールにヒットすると、ネットワークデバイスは syslog メッセージを送信します。これは、ポリシーのトラブルシューティングと初期化テストに役立つ場合があります。ただし、ネットワークデバイスのリソースとパフォーマンスに影響を与える可能性があるため、このオプションは慎重に使用することを推奨します。

ステップ 5 [Default Action] ドロップダウンリストで、[Deny] または [Permit] を選択します。

必要に応じて、デフォルトアクションのロギングを有効にできます。

ステップ 6 アクセス契約を今作成するか、後でスケジュールするかを選択します。

[Automation Events for ITSM (ServiceNow)] バンドルが有効になっている場合、[Save Now] オプションは無効になり、グループベースのポリシー変更に対する [Schedule Later] オプションのみが有効になります。スケジュールされたタスクは、スケジュールされた時刻の前に IT サービス管理（ITSM）で承認される必要があります。スケジュールされた時刻までにタスクが承認されない場合、タスクは失敗します。ITSM と Catalyst Center の統合方法の詳細については、『Cisco Catalyst Center ITSM Integration Guide』を参照してください。

[Access Contract] ウィンドウの右上隅で、今後のタスク、進行中のタスク、および失敗したタスクの合計数を表示できます。[Activities] > [Tasks] でタスクのステータスリンクをクリックすると、タスクの詳細が表示されます。タスクは、実行前に編集またはキャンセルできます。

アクセス契約の編集

始める前に

このタスクを実行するには、スーパー管理者またはネットワーク管理者である必要があります。

手順

ステップ 1 メインメニューから次を選択します。**[Policy]** > **[Group-Based Access Control]** > **[Access Contracts]** の順に選択します。

ステップ 2 [Access Contracts] ウィンドウで、編集するアクセス契約の横にあるチェックボックスをオンにします。

ステップ 3 [Actions] > [Edit] の順に選択します。

ステップ 4 [Edit Access Contract] ウィンドウで、必要な変更を行った後、アクセス契約を今すぐ更新するか、後で更新するようスケジュールするかを選択します。

[Filter] オプションを使用して、契約を検索できます。

既存のアクセス契約を複製し、必要な詳細情報を編集して新しいアクセス契約を作成できます。アクセス契約を複製すると、既存のアクセス契約に含まれるすべての情報がコピーされ、コピーされた契約は、既存の契約名の末尾に文字列**Copy**が付加された名前になります。[Save Now] をクリックして複製契約をすぐに作成するか、[Schedule Later] をクリックして複製契約を後で作成します。

セキュリティグループ、契約、またはポリシーを更新する場合は、ネットワークデバイスに変更を展開する必要があります。ポリシーを更新し、更新したポリシーを展開しない場合、ポリシーの変更に関する通知はネットワークデバイスに送信されず、ネットワークで現在アクティブになっているポリシーは、Catalyst Center に表示されるポリシー情報と一致しない可能性があります。この状況を解決するには、ネットワークデバイスに、更新したポリシーを展開する必要があります。[Deploy Now] をクリックして変更をすぐに展開するか、[Deploy Later] をクリックして変更を後で展開します。

Cisco ISE は、Catalyst Center の代わりにネットワークデバイスにポリシーをダウンロードするためのランタイム ポリシー プラットフォームを提供します。ポリシーの同期の問題を防ぐために、セキュリティグループ、セキュリティ グループ アクセス コントロール リスト（SGACL）、およびイーグレスポリシーの [TrustSec Workcenter] ユーザーインターフェイス画面が Cisco ISE に読み取り専用モードで表示されます。

アクセス契約の削除

始める前に

このタスクを実行するには、スーパー管理者またはネットワーク管理者である必要があります。

手順

ステップ 1 メインメニューから次を選択します。**[Policy]** > **[Group-Based Access Control]** > **[Access Contracts]** の順に選択します。

ステップ 2 [Access Contracts] ウィンドウで、削除するアクセス契約の横にあるチェックボックスをオンにして、アクセス契約を今すぐ削除するか、後で削除するようスケジュールするかを選択します。

[Access Contracts] ウィンドウではサンプル契約を表示できます。それらのサンプル契約は使用または削除できます。ただし、デフォルトの契約（Permit IP、Deny IP、Permit_IP_Log、Deny_IP_Log）は削除できません。

アクセス契約を使用するポリシーを表示するには、そのアクセス契約の [Policies] 列のリンクをクリックします。ポリシーで使用されている場合、契約を削除することはできません。契約を削除する前に、そのポリシーから契約を削除する必要があります。

Catalyst Center と Cisco ISE 間のアクセス契約の同期

Catalyst Center のアクセス契約を Cisco ISE と同期している間：

- 契約が Catalyst Center に存在し、Cisco ISE に存在しない場合は、Cisco ISE に作成されます。
- 契約が Cisco ISE に存在し、Catalyst Center に存在しない場合は、Catalyst Center に作成されます。
- 契約名が Catalyst Center と Cisco ISE で同じであるが、説明とトラフィックルールの内容が異なっている場合、Catalyst Center は Cisco ISE で指定されたデータを使用して更新されます。
- 契約名とルールが同じで、説明が異なっている場合、Catalyst Center は Cisco ISE で指定された説明を使用して更新されます。
- Cisco ISE の Text SGACL コマンドラインは、解析できないコンテンツとして移行されます。これらの契約は編集できますが、Catalyst Center ではその解析やシンタックスチェックは行われません。Catalyst Center で加えた変更は、Cisco ISE に反映されます。
- Cisco ISE でポリシーに複数の SGACL がある場合、それらの契約は Catalyst Center のデフォルトポリシーとして移行されます。

Cisco ISE との同期が完了していない場合、アクセス契約の横にオレンジ色の三角形のアイコンが表示されます。

ACI から学習した契約は [Access Contracts] ウィンドウに表示され、[Created In] 列の値が [ACI] になります。ACI から学習したアクセス契約を編集したり削除したりすることはできませんが、ACIから学習したセキュリティグループの使用中にポリシーで使用することはできます。マトリックスビューからポリシーを作成または更新する場合に、ACI から学習したセキュリティグループを接続先グループとして選択すると、関連するアクセス契約が [Preferred Contracts] タブに表示されます。[All Contracts] タブですべてのアクセス契約を確認できます。

グループベースのアクセス コントロール ポリシーの作成

セキュリティグループおよびアクセス契約は、アクセス コントロール ポリシーの基本的な構成要素です。アクセス コントロール ポリシーを作成する際には、前に作成したセキュリティグループと契約を使用したり、ポリシーの作成時に新しいセキュリティグループと契約を作成したりできます。

特定の送信元グループからアクセスできるネットワークリソースを指定する場合は、1 つの送信元グループと複数の宛先グループを含むアクセス コントロール ポリシーを作成できます。一方、特定のネットワークリソースへのアクセスが許可されている送信元グループを指定する場合は、1つの宛先グループと複数の送信元グループを含むアクセス コントロール ポリシーを作成できます。

たとえば、「請負業者」送信元セキュリティグループに関連付けられたユーザーがアクセスできるネットワークリソースを指定する場合は、1 つの送信元グループと複数の宛先グループを含むアクセス コントロール ポリシーを作成できます。「財務サーバー」宛先セキュリティグループへのアクセスが許可されている送信元グループを指定する場合は、1 つの宛先グループと複数の送信元グループを含むアクセス コントロール ポリシーを作成できます。

グループベースのアクセス コントロール ポリシーは、送信元グループと宛先グループの特定ペアのトラフィックフローに基づいて作成または更新することもできます。

手順

ステップ 1 [Policy List] または [Matrix] ビューで、[Create Policies] をクリックします。

ステップ 2 1つの送信元グループと複数の宛先グループを含むアクセス コントロール ポリシーを作成するには、[Source To Destination(s)] をクリックし、次の手順を実行します。

a) 選択する送信元セキュリティグループの横にあるオプションボタンをクリックします。

必要なセキュリティグループが存在しない場合は、[Create Security Group] をクリックして新しいセキュリティグループを作成します。このオプションは、[Automation Events for ITSM (ServiceNow)] バンドルが有効になっている場合は使用できません。

b) [Next] をクリックします。

c) 選択した送信元セキュリティグループにマッピングする宛先セキュリティグループを選択します。

必要に応じて、セキュリティグループの詳細を表示したり、セキュリティグループを編集したりできます。



（注） 送信元と宛先の間にポリシーがすでに存在する場合、セキュリティグループの近くにはオレンジ色の三角形のアイコンが表示されます。

d) **[次へ (Next)]** をクリックします。

e) 選択する契約の横にあるオプションボタンをクリックします。必要に応じて、契約の詳細を表示および編集できます。

必要な契約が存在しない場合は、[Create Contract] をクリックして新しい契約を作成します。このオプションは、[Automation Events for ITSM (ServiceNow)] バンドルが有効になっている場合は使用できません。



（注） 1 つのポリシーに対して 1 つの契約のみを選択できます。

f) **[次へ (Next)]** をクリックします。

[Summary] ウィンドウには、選択したセキュリティグループと契約に基づいて作成されたポリシーが一覧表示されます。

g) ポリシーを今すぐ作成するか、後でスケジュールするかを選択します。

ステップ 3 1 つの宛先グループと複数の送信元グループを含むアクセス コントロール ポリシーを作成するには、[Destination to Source(s)] をクリックし、次の手順を実行します。

a) 選択する宛先セキュリティグループの横にあるオプションボタンをクリックします。

必要なセキュリティグループが存在しない場合は、[Create Security Group] をクリックして新しいセキュリティグループを作成します。このオプションは、[Automation Events for ITSM (ServiceNow)] バンドルが有効になっている場合は使用できません。

b) [Next] をクリックします。

c) 選択した宛先セキュリティグループにマッピングする送信元セキュリティグループを選択します。

必要に応じて、セキュリティグループの詳細を表示したり、セキュリティグループを編集したりできます。



（注） 送信元と宛先の間にポリシーがすでに存在する場合、セキュリティグループの近くにはオレンジ色の三角形のアイコンが表示されます。

d) **[次へ (Next)]** をクリックします。

e) 選択する契約の横にあるオプションボタンをクリックします。

必要な契約が存在しない場合は、[Create Contract] をクリックして新しい契約を作成します。このオプションは、[Automation Events for ITSM (ServiceNow)] バンドルが有効になっている場合は使用できません。

（注） 1 つのポリシーに対して 1 つの契約のみを選択できます。

f) **[次へ (Next)]** をクリックします。

[Summary] ウィンドウには、選択したセキュリティグループと契約に基づいて作成されたポリシーが一覧表示されます。

g) ポリシーを今すぐ作成するか、後でスケジュールするかを選択します。

[Automation Events for ITSM (ServiceNow)] バンドルが有効になっている場合、[Save Now] オプションは無効になり、グループベースのポリシー変更に対する [Schedule Later] オプションのみが有効になります。スケジュールされたタスクは、スケジュールされた時刻の前に IT サービス管理（ITSM）で承認される必要があります。スケジュールされた時刻までにタスクが承認されない場合、タスクは失敗します。ITSM と Catalyst Center の統合方法の詳細については、『Cisco Catalyst Center ITSM Integration Guide』を参照してください。

[Policies] ウィンドウの右上隅で、今後のタスク、進行中のタスク、および失敗したタスクの合計数を表示できます。[Activities] > [Tasks] でタスクのステータスリンクをクリックすると、タスクの詳細が表示されます。タスクは、実行前に編集またはキャンセルできます。

トラフィックフローに基づくグループベースのアクセスコントロールポリシーの更新

手順

ステップ 1 ポリシーマトリックスビューで、グループベースのアクセス コントロール ポリシーを更新するセルをクリックします。

ステップ 2 [Policy Details] スライドインペインで、[View Traffic Flows] をクリックします。

[View Traffic Flows] スライドインペインの左側のペインでは、選択した契約のルールまたはデフォルトのポリシーを確認できます。右側のペインでは、選択したルールに一致するトラフィックフローを確認できます。

ステップ 3 [Default Action] ルールの [View Traffic] をクリックして、そのルールに一致するフローのリストを表示します。追加のルールを持つアクセス契約を使用して既存のポリシーを変更する際、任意のルールの [View Traffic] オプションを使用して、そのルールに一致するフローのリストを表示します。

[Default Action] ルール（明示的に選択されたアクセス契約がない）を使用しているポリシーの場合、アクセス契約を選択するか、そのポリシーで使用される新しいアクセス契約を作成することができます。

アクセス契約の PERMIT または DENY を使用したポリシーの場合、アクセス契約を選択するか、そのポリシーで使用される新しいアクセス契約を作成することができます。

カスタムアクセス契約を使用したポリシーの場合、選択したアクセス契約を編集できます。

ステップ 4 必要な変更を行った後、次のオプションのいずれかを選択します。

- **変更を既存の契約に保存します。変更は、その契約を参照するすべてのポリシーに影響します。**
- **変更を新しい契約として保存します。変更は現在のポリシーにのみ適用されます。**
- **変更を新しい契約として保存します。変更はどのポリシーにも適用されません。**

Catalyst Center と Cisco ISE の間のポリシーの同期

Catalyst Center でポリシーを Cisco ISE と同期する場合、次のようになります。

- ポリシーが Catalyst Center に存在し、Cisco ISE に存在しない場合は、Cisco ISE に作成されます。
- 契約が Cisco ISE に存在し、Catalyst Center に存在しない場合は、Catalyst Center に作成されます。
- Cisco ISE でポリシー契約が異なる場合、 Catalyst Center は Cisco ISE で指定された契約で更新されます。
- ポリシーモード情報（有効、無効、またはモニター）も Cisco ISE からインポートされます。

Cisco ISE には、単一のポリシーに対して複数の SGACL を許可するオプションがあります（このオプションは Cisco ISE ではデフォルトで有効になっていません）。Catalyst Center では、単一のポリシーに対して複数のアクセス契約を使用することはサポートされていません。ポリシーの同期中に、Cisco ISE のポリシーに複数の SGACL がある場合、Catalyst Center 管理者には、そのポリシーを変更して契約を選択しないようにするオプションがあります（デフォルトポリシーを使用する場合）。管理者は、ポリシーの同期が完了した後に、そのポリシーに対して新規または既存のアクセス契約を選択できます。

シスコのグループベースポリシー分析

シスコのグループベースポリシー分析について

グループベースポリシー分析で提供される情報を使用することで、資産間の通信を可視化してグループベースポリシーを作成したり、新しいアクセスコントロールの導入による影響を評価したり、ポリシーで許可する必要があるプロトコルを正確に特定したりできます。

シスコのグループベースポリシー分析では、ネットワーク上の資産のグループとそれらの通信に関する次のような情報が集約されます。

- 相互に通信しているグループ
- 通信の種類
- 特定の資産が属するグループ

購入できる Catalyst Center のライセンスの種類は次のとおりです。

- Essentials
- Advantage
- Premier

Advantage と Premier ライセンスには、グループベースポリシー分析パッケージが含まれています。このパッケージは、次のアーカイブ（.tar.gz ファイル）で構成されています。

- バックエンド
- ユーザー インターフェイス
- サマライザパイプライン
- 集約の定義

グループベースポリシー分析のインストール

シスコのグループベースポリシー分析は Catalyst Center の一部ですが、デフォルトではインストールされません。

グループベースポリシー分析をインストールするには、次の手順を実行します。

手順

ステップ 1 メインメニューから次を選択します。**[System]** > **[Software Management]** の順に選択します。

ステップ 2 [Available Applications for 2.3.xx-xxxxx] エリアまで下にスクロールし、[Group-Based Policy Analytics] を選択します。

ステップ 3 [Install] をクリックしてアプリケーションをインストールします。

ハードウェアとソフトウェアの互換性

プラットフォームのサポート

シスコのグループベースポリシー分析は、次のハードウェアプラットフォームでサポートされています。

- 44 コアのシングルノードクラスタと 3 ノードクラスタ
- 56 コアのシングルノードクラスタと 3 ノードクラスタ
- 112 コアのシングルノードクラスタと 3 ノードクラスタ

これらのプラットフォームは、ここで説明するパフォーマンスと拡張性の要件を満たしている必要があります。

サポートされているハードウェアの詳細については、「Cisco UCS M4 appliances」または「Cisco UCS M5 appliances」を参照してください。

次の表に、Catalyst Center およびシスコのグループベースポリシー分析でサポートされるパフォーマンスメトリックをコアプラットフォームごとに示します。NetFlow メトリックは、シスコのグループベースポリシー分析で導入されています。

（注） 次の表に、スタンドアロン展開のパフォーマンスメトリックを示します。これらの値は、クラスタ内のノードの数とインストールされているパッケージの数によって異なる場合があります。

表 *58 :* 評価指標

メトリック	44 コア、3 ノード	56 コア	112 コア
デバイス（NAD）	5000 スイッチが 1000、ルータが 1000、またはその両方の組み合わせ、AP が 4000	8000 スイッチが 2000、ルータが 2000、またはその両方の組み合わせ、AP が 6000	18,000 スイッチが 5000、ルータが 5000、またはその両方の組み合わせ、AP が 13,000
クライアント（エンドポイント）	25,000 ワイヤレスが 20,000、有線が 5,000	40,000 ワイヤレスが 30,000、有線が 10,000	100,000 ワイヤレスが 60,000、有線が 40,000

メトリック	44 コア、3 ノード	56 コア	112 コア
NetFlow/秒	30,000	48,000	120,000

デバイス サポート

シスコのグループベースポリシー分析を使用するには、NetFlowを有効にする必要があります。次の表に、さまざまなネットワークデバイスで NetFlow を有効にする方法を示します。

表 *59 :* デバイス サポート

ネットワーク デバイス	シリーズ	Catalyst Center UI の [ネットワーク設定（Network Settings）] の [テレメトリ（Telemetry）] セクションで設定可能な NetFlow（Flexible NetFlow または Application Visibility and Control ベースの NetFlow）	Catalyst Center UI の CLI テンプレートツールを使用して設定可能な NetFlow（Flexible NetFlow または Application Visibility and Control ベースの NetFlow）	ファブリック展開での NetFlow の収集	非ファブリック展開での NetFlow の収集
ルータ	Cisco 1000 シリーズ サービス統合型ルータ（ISR1K）	対応	対応	対応	対応
	Cisco 4000 シリーズ サービス統合型ルータ（ISR4K）	対応	対応	対応	対応
	Cisco 1000v シリーズ クラウド サービス ルータ（CSR 1000v）	対応	対応	対応	対応
	Cisco 1000 シリーズ アグリゲーション サービス ルータ（ASR1K）	対応	対応	対応	対応

ネットワークデバイス	シリーズ	**Catalyst Center UI** の [ネットワーク設定（**Network Settings**）] の [テレメトリ（**Telemetry**）] セクションで設定可能な **NetFlow**（**Flexible NetFlow** または **Application Visibility and Control** ベースの **NetFlow**）	**Catalyst Center UI** の **CLI** テンプレートツールを使用して設定可能な **NetFlow**（**Flexible NetFlow** または **Application Visibility and Control** ベースの **NetFlow**）	ファブリック展開での **NetFlow** の収集	非ファブリック展開での **NetFlow** の収集
スイッチ	Cisco Catalyst 9200 シリーズ	対応	対応	対応	対応
	Cisco Catalyst 9300 シリーズ	対応	対応	対応	対応
	Cisco Catalyst 9400 シリーズ	対応	対応	対応	対応
	Cisco Catalyst 9500 シリーズ	非対応	対応	対応	対応
	Cisco Catalyst 9600 シリーズ	非対応	対応	対応	対応
	Cisco Catalyst 2k シリーズ	非対応	はい	該当なし	対応
	Cisco Catalyst 3560 シリーズ	非対応	はい	該当なし	対応
	Cisco Catalyst 3650 シリーズ	非対応	対応	対応	対応
	Cisco Catalyst 3850 シリーズ	非対応	対応	対応	対応
	Cisco Catalyst 4k シリーズ	非対応	対応	対応	対応
	Cisco Catalyst 6500 シリーズ スイッチ	非対応	対応	対応	対応
	Cisco Catalyst 6800 シリーズ スイッチ	非対応	対応	対応	対応
ワイヤレスコントローラ	Cisco 3504 ワイヤレスコントローラ（AireOS ベース）	対応	対応	非対応	対応、中央スイッチング SSID のみ
	Cisco 5520 ワイヤレスコントローラ（AireOS ベース）	対応	対応	非対応	対応、中央スイッチング SSID のみ
	Cisco 8540 ワイヤレスコントローラ（AireOS ベース）	対応	対応	非対応	対応、中央スイッチング SSID のみ
	Cisco Catalyst 9800 ベースのコントローラ	対応	対応	対応	対応

Cisco ISE

Catalyst Center は、Cisco ISE 2.4 パッチ 7 以降、Cisco ISE 2.6 パッチ 1 以降、Cisco ISE 2.7 以降をサポートしています。

Cisco StealthWatch

Catalyst Center は、Cisco Stealthwatch 7.x 以降をサポートしています。

コネクタについて

Cisco グループベースポリシー分析は、コネクタとも呼ばれるさまざまなソースからテレメトリを収集します。シスコのグループベースポリシー分析の初期設定 （1432 ページ） ワークフローに従うか、**[Policy]** > **[Group-Based Access Control]** > **[Analytics]** > **[Configurations]** > **[Analytics Settings]** の順に選択して、コネクタを設定できます。

グループデータコネクタ

グループデータコネクタは、資産が分類されるグループに関する情報を収集します。Cisco ISE と Cisco Stealthwatch はグループデータコネクタです。

- **Cisco ISE**

  Cisco ISE は次世代のアイデンティティおよびアクセス コントロール ポリシー プラットフォームであり、企業がコンプライアンスを適用し、インフラストラクチャのセキュリティを強化し、サービス運用を合理化できるようにします。 Cisco ISE は、仮想マシン、物理マシン、または両マシンの組み合わせにインストールされます。 Cisco ISE は、セッションディレクトリ、セキュリティグループ、およびその他の情報を共有するためのパブリッシャ/サブスクライバモジュールとして Cisco Platform Exchange Grid（pxGrid）サービスを使用します。PxGrid は、クエリインターフェイスを使用し、一括ダウンロードをサポートしています。ネットワークのユーザーの認証、許可、アカウンティングが行われ、セッションディレクトリが維持されます。ユーザーイベントは、Session Directory サービスに登録されているコネクタにパブリッシュされます。セキュリティグループ通知などの他のサービスにも登録できます。

  ネットワークに入ってきたパケットは、認証で取得したユーザーアイデンティティとデバイスの情報を使用して分類されます。このパケット分類は、パケットがネットワークに入ってきたときに、そのパケットにタグ付けすることによって維持されます。これにより、パケットはデータパス全体で正しく識別され、セキュリティおよびその他のポリシー基準が適用されるようになります。このタグは、セキュリティグループタグ（SGT）と呼ばれることもあり、SGT に応じてネットワークデバイスによるトラフィックのフィルタ処理を可能にすることで、Cisco ISE がアクセス コントロール ポリシーを適用できるようにします。

  さらに、Cisco ISE は、ネットワークに接続されているエンドポイントに関する情報を収集します。情報には、デバイスのタイプ、OS、OS バージョン、IP アドレスなどの属性が含まれます。これらは ISE プロファイルと呼ばれます。

  Cisco ISE コネクタは、Cisco ISE の SGT 定義とプロファイルをシスコのグループベースポリシー分析に提供します。

- **Cisco StealthWatch**

  Cisco Stealthwatch は、高度な脅威検出、脅威への迅速な対応、およびネットワークトラフィックのセキュリティ分析を可能にするネットワークベースの異常検出システムです。Cisco Stealthwatch コネクタは、Cisco Stealthwatch で設定されているホストグループを取得します。ホストグループは基本的に、場所、機能、トポロジなどの類似の属性を持つ複数のホスト IP アドレスまたは IP アドレス範囲の仮想コンテナです。

通信コネクタ

通信コネクタは、グループベースのポリシーの決定に役立つグループ間のトラフィックに関する情報を収集します。これは、Catalyst Center で管理しているネットワークデバイスからの NetFlow を使用して実行されます。Catalyst Center では、NetFlow がネイティブで収集および集約されます。

シスコのグループベースポリシー分析の初期設定

このワークフローでは、ネットワークアクティビティやエンドポイントに関連するテレメトリデータを Cisco ISE、Cisco Stealthwatch、NetFlow などの特定のソースから収集するために必要なデータコネクタを設定できます。このタスクは、初めてデータコネクタを設定するときに便利です。

始める前に

Catalyst Center にシスコのグループベースポリシー分析がインストールされている必要があります。

手順

ステップ 1 メインメニューから次を選択します。**[Policy]** > **[Group-Based Access Control]** > **[Overview]** の順に選択します。[確実なポリシーの作成（Create policies with more confidence）] ウィンドウが表示されます。

ステップ 2 [Get Started] をクリックします。
[データコネクタの設定（Configure your data connectors）] ウィンドウが表示されます。

ステップ 3 [Let's Do it] をクリックします。

[グループデータコネクタの設定（Configure Group Data Connectors）] ウィンドウが表示されます。

（注） Cisco ISE のバージョンがシスコのグループベースポリシー分析を実行するために必要なバージョンよりも前のバージョンの場合は、次のエラーメッセージが表示されます。

ステップ 4 設定するコネクタの下部にある [Configure] をクリックします。

新しいウィンドウが開き、Catalyst Center の [Settings] ウィンドウにリダイレクトされます。ここで必要なコネクタを設定できます。Cisco ISE コネクタを設定する必要があります。Cisco Stealthwatch コネクタの設定は任意です

ステップ 5 [Settings] ウィンドウを閉じます。[グループデータコネクタの設定（Configure Group Data connectors）] ウィンドウで、正常に設定されたコネクタの [設定（Configure）] オプションの横に緑色のドットが表示されます。

ステップ 6 [Next] をクリックします。
[通信コネクタの設定（Configure Communication Connectors）] ウィンドウが表示されます。

ステップ 7 次のいずれかのオプションを使用して、通信コネクタ（NetFlow）を設定します。

- Catalyst Center のデバイスインターフェイスで NetFlow を手動でプロビジョニングします。
- [CLI Templates] をクリックし、Catalyst Center の [CLI Templates] ツールを使用して NetFlow を設定します。
- [Telemetry in Network Settings] をクリックし、ネットワーク設定のテレメトリのセクションで NetFlow を設定します。

ステップ 8 [Next] をクリックします。
[Summary] ウィンドウにコネクタの設定の詳細情報が表示されます。

ステップ 9 グループとエンドポイントの検出を開始するには、[Done] をクリックします。

グループとエンドポイントの確認

このセクションは、各種グループ間のトラフィックを可視化するさまざまな方法について説明します。

複数のグループから複数のグループ

[概要（Overview）] ウィンドウの [セキュリティグループ（Security Groups）] ボックスに表示されている数をクリックすると、**[セキュリティグループの詳細（Explore Security Groups）]** ウィンドウが表示されます。このウィンドウでは、セキュリティグループのグループ間通信すべての概要を確認できます。デフォルトでは、過去 24 時間の時間範囲のデータが表示されます。

（注） これは、過去 14 日間に設定された [概要（Overview）] ウィンドウの時間範囲とは異なります。チャートには、特定の期間に一意のフロー数が多い送信元セキュリティグループなど、上位 25 の送信元セキュリティグループとその対応するやり取りが表示されます。

 アイコンをクリックするとチャートビューが表示され、 をクリックするとテーブルビューが表示されます。

テーブルビューで、特定の行の [See destinations] リンクをクリックすると、選択した送信元セキュリティグループに対応するすべての宛先セキュリティグループが表示されたウィンドウが開き、各宛先セキュリティグループの一意のフロー数が表示されます。

送信元グループをクリックすると、**単一のグループから複数のグループ**のウィンドウが表示されます。

リンクにカーソルを合わせると強調表示され、ツールチップに一意のトラフィックフローの数が表示されます。リンクをクリックすると、**単一のグループから単一のグループ**のウィンドウに切り替わります。

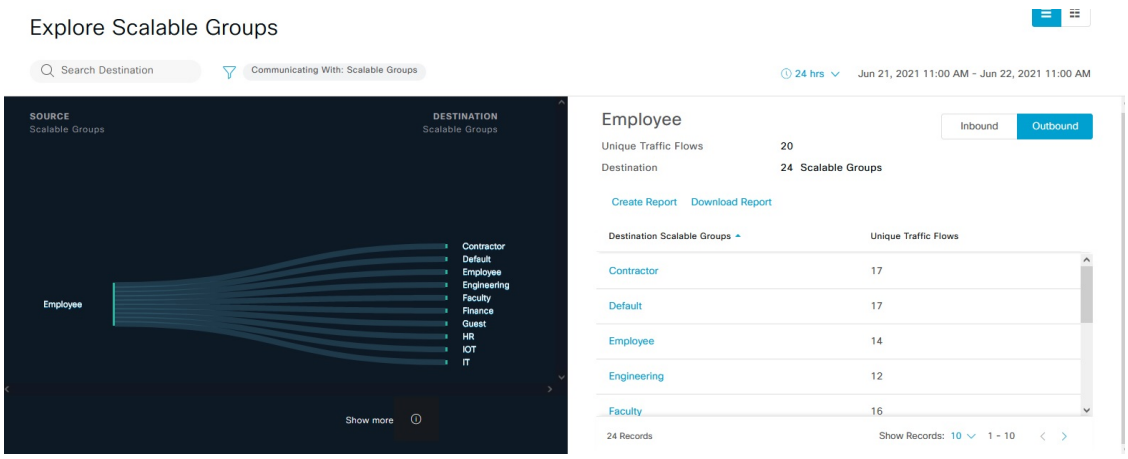
[概要（Overview）] ウィンドウの [ISEプロファイル（ISE Profiles）] ボックスに表示されている数をクリックすると、**[ISEプロファイルの詳細（Explore ISE Profiles）]** ウィンドウが表示されます。このウィンドウでは、送信元がISEプロファイルで宛先がセキュリティグループであるすべての通信の概要を確認できます。グループベースポリシーを決定することが目的の場合は、このビューで送信元または宛先のいずれかのカテゴリをセキュリティグループにする必要があります。

[概要（Overview）] ウィンドウの [Stealthwatchホストグループ（Stealthwatch Host Groups）] ボックスに表示されている数をクリックすると、**[Stealthwatchホストグループの詳細（Explore Stealthwatch Host Groups）]** ウィンドウが表示されます。このウィンドウでは、送信元がStealthwatch ホストグループで宛先がセキュリティグループであるすべての通信の概要を確認できます。グループベースポリシーを決定することが目的の場合は、このビューで送信元または宛先のいずれかのカテゴリをセキュリティグループにする必要があります。

単一のグループから複数のグループ

単一のグループから複数のグループ：アウトバウンド

このウィンドウには、単一の送信元グループと複数の宛先グループの間のアクティビティが表示されます。送信元と宛先の少なくとも一方がセキュリティグループである必要があります。デフォルトでは過去 24 時間の時間範囲のデータが表示され、表示されるリンクまたはレコードのデフォルト数は 10 です。



アイコンをクリックするとチャートビューが表示され、 をクリックするとテーブルビューが表示されます。

[Outbound] をクリックすると、選択したセキュリティグループから開始された接続が表示されます。[Inbound] をクリックすると、このセキュリティグループに対して別のグループから開始された接続が表示されます。

任意の列をクリックして、昇順または降順で並べ替えることができます。

グループをクリックすると、選択したグループを宛先とする**単一のグループから単一のグループ**のウィンドウが表示されます。送信元グループは変わりません。

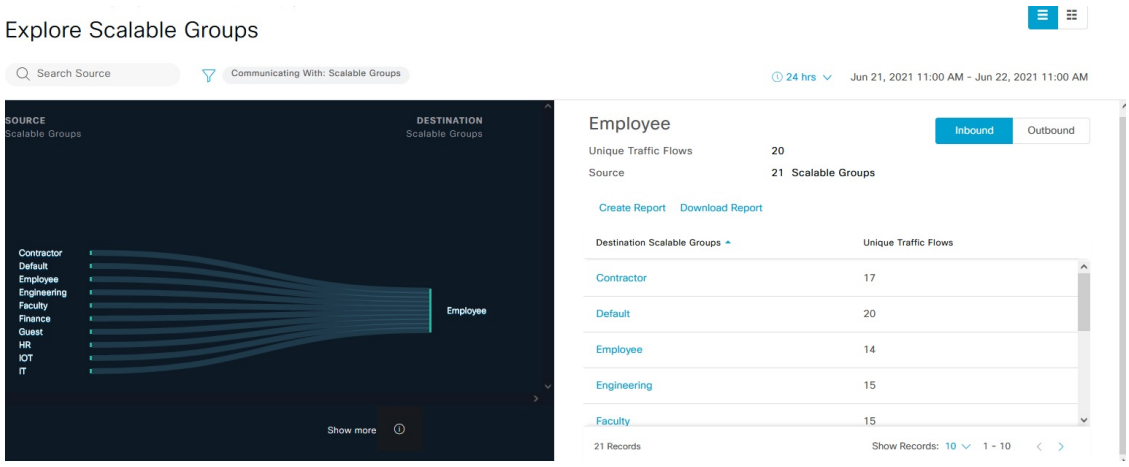
リンクにカーソルを合わせると強調表示され、ツールチップに一意のトラフィックフローの数が表示されます。リンクをクリックすると、**単一のグループから単一のグループ**のウィンドウに切り替わります。

[Create Report] をクリックすると、このビューの情報から CSV 形式の新しいレポートが生成されます。表示される [Reports] ウィンドウで、生成されたレポートを確認できます。このウィンドウから、以前生成されたレポートにアクセスし、レポートをダウンロードすることもできます。

[Download Report] をクリックして、生成されたレポートを表示します。表示される [Reports] ウィンドウで、[Last Run] 列のダウンロードアイコンをクリックするとレポートをダウンロードできます。

単一のグループから複数のグループ：インバウンド

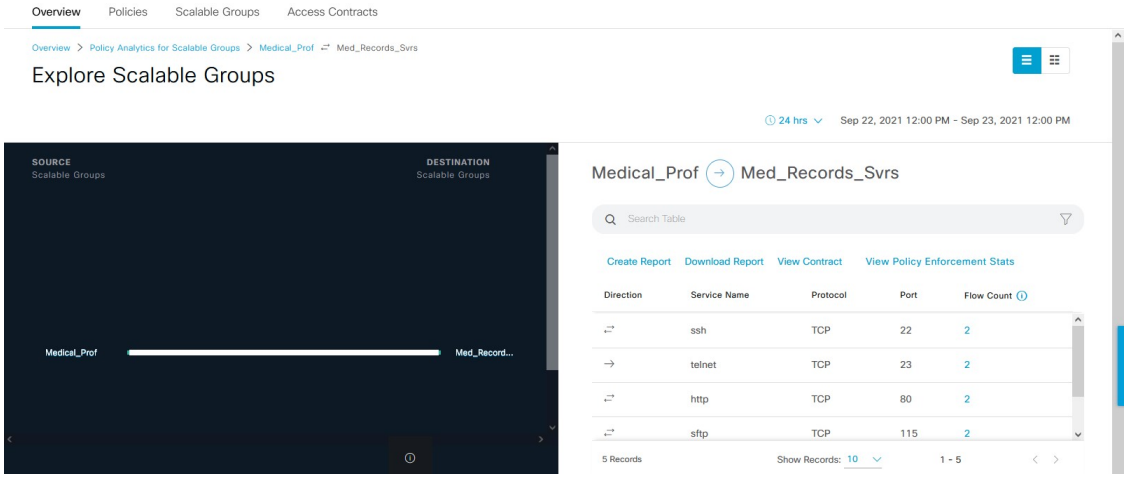
[Inbound] をクリックすると、選択したセキュリティグループを宛先としていずれかのグループから開始されたすべての接続が表示されます。



単一のグループから単一のグループ

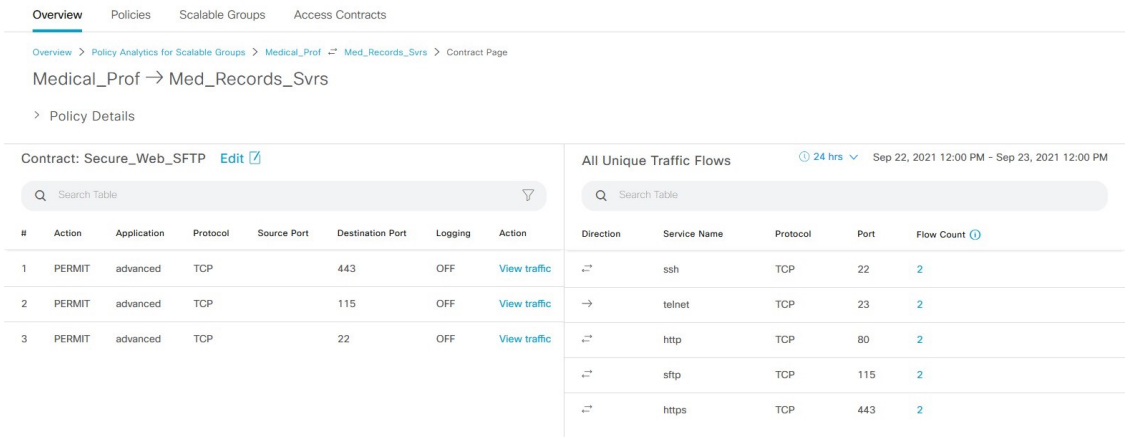
このウィンドウには、1 つの送信元グループと 1 つの宛先グループの間のアクティビティが表示されます。送信元グループと宛先グループの少なくとも一方がセキュリティグループである

必要があります。デフォルトでは過去 24 時間の時間範囲のデータが表示され、表示されるリンクまたはレコードのデフォルト数は 10 です。

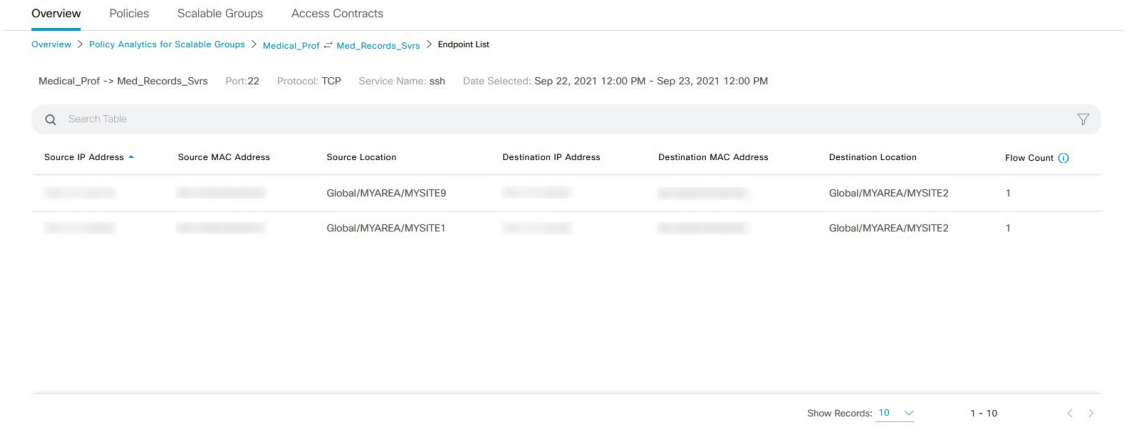


送信元グループと宛先グループの間に表示されている方向矢印をクリックすると、このビューの送信元グループと宛先グループが入れ替わります。

[View Contract] をクリックして、トラフィックフローと、この送信元と宛先グループのペアに有効なアクセス契約のルールを 1 対 1 で比較します。

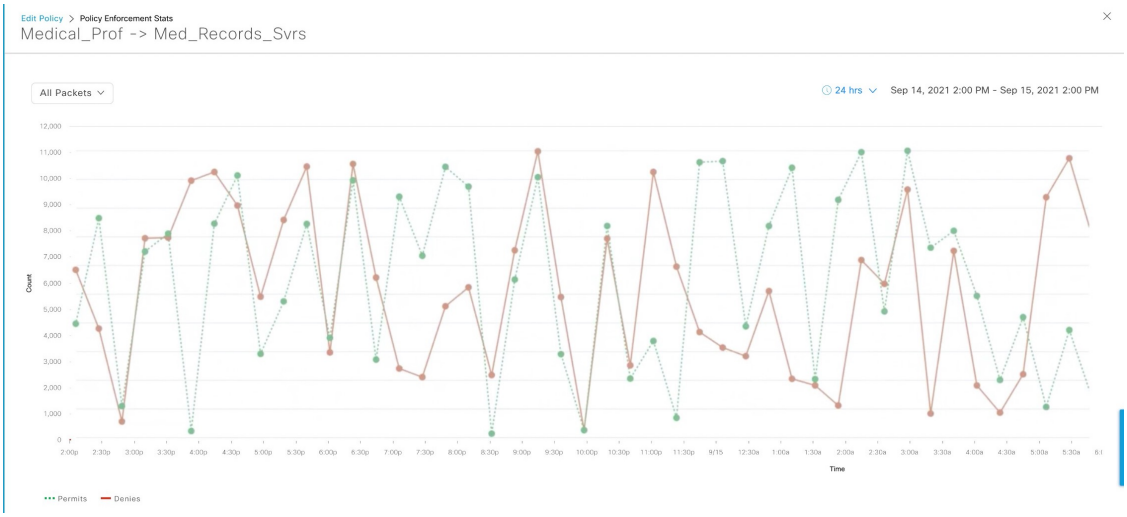


[View Contract] ウィンドウの左側のペインに、送信元グループと宛先グループ間で許可および拒否されるトラフィックのルールが表示されます。右側のペインでは、選択したルールに一致するトラフィックフローを確認できます。右側のペインで、フローの方向、サービス名、フロー数、ポート、およびプロトコルの詳細を表示できます。[Flow Count] 列には、選択した期間に特定のサービス、ポート、およびプロトコルの組み合わせで検出されたフローの数が表示されます。フロー数のリンクをクリックして、各エンドポイントのフローの詳細を表示できます。



（注） フロー数に基づいて [トラフィックフロー（Traffic Flows）] テーブルを並べ替えると、1000 レコードのみが表示されます。

[View Policy Enforcement Stats] をクリックして、任意の送信元および宛先グループペアの許可カウントと拒否カウントの時系列グラフを表示します。これにより、ポリシーごとの適用統計情報が可視化されます。[All Packets] ドロップダウンリストを使用して、許可されたパケットまたはドロップされたパケットのみを選択することができます。グラフデータポイントは、15 分のデータ収集期間ごとに表示されます。データポイントにカーソルを合わせると、許可と拒否の数が表示されます。データポイントまたは期間をクリックして、選択した期間の契約とトラフィックフローの詳細を表示できます。



（注） フローデータの集計は 60 分ごとに実行されるため、選択した期間は、選択したデータポイントに対応する 15 分間隔を含む時間です。

ポリシーの作成または編集中に、[Policy Details] スライドインペインから [Traffic Flows] テーブルにアクセスすることもできます。

 アイコンをクリックするとチャートビューが表示され、 をクリックするとテーブルビューが表示されます。

日時セレクタを使用して日付と時刻を設定できます。

[Create Report] をクリックすると、このビューの情報から CSV 形式の新しいレポートが生成されます。表示される [Reports] ウィンドウで、生成されたレポートを確認できます。このウィンドウから、以前生成されたレポートにアクセスし、レポートをダウンロードすることもできます。

[Download Report] をクリックして、生成されたレポートを表示します。表示される [Reports] ウィンドウで、[Last Run] 列のダウンロードアイコンをクリックするとレポートをダウンロードできます。

アクセス契約数

アクセス契約は分析ワークフローで直接作成および変更できるようになりました。

契約の表示

[View Contract] ウィンドウを起動するには、[Explore Security Groups] ウィンドウで [View Contract] をクリックします。[View Contract] ウィンドウの左側のペインに、送信元グループと宛先グループ間で許可および拒否されるトラフィックのルールが表示されます。右側のペインでは、選択したルールに一致するトラフィックフローを確認できます。

この表には [Policies] ウィンドウからもアクセスできます。メインメニューから次を選択します。**[Policy]** > **[Group-Based Access Control]** > **[Policies]** の順に選択します。

ポリシーマトリックスビューで、契約を作成または変更するセルをクリックします。[Policy Details] スライドインペインで、[View Traffic Flows] をクリックします。

現在、送信元グループと宛先グループの間に契約が割り当てられていない場合、データは表示されません。[Change Contract] または [Create Access Contract] オプションを使用して、契約を作成または変更することができます。

[Action] 列の [View traffic] をクリックして、そのルールに一致するフローのリストを表示します。

アクセス契約の作成

[Contract Content] ウィンドウを起動するには、[Policy Details] ペインで [Create Access Contract] をクリックします。トラフィックフィルタルールを作成するには、次の手順を実行します。

1. [Action] ドロップダウンリストで、[Deny] または [Permit] を選択します。

2. [Application] ドロップダウンリストから、アクションを適用するアプリケーションを選択します。ポートとプロトコルは、選択したアプリケーションに基づいて自動的に選択されます。

   トランスポートプロトコル、送信元ポート、および宛先ポートを指定する場合は、[Application] ドロップダウンリストから [Advanced] オプションを選択します。

複数のルールを作成できます。1 つの契約に複数のルールを作成するには、**[+]** アイコンをクリックし、[アクション（Action）] 列と [アプリケーション（Application）] 列の設定を選択します。ルールは、契約に記載されている順序でチェックされます。ルールの左端にあるハンドルのアイコンを使用して、ルールをドラッグして順序を変更します。

[All Unique Traffic Flows] ペインの [Add to Contract] オプションを使用して契約にエントリを追加することができます。

新たに作成または編集した契約を保存するときに使用できるオプションは、次のとおりです。

- [Update current policy only]：契約の複製が作成され、現在のポリシーに適用されます。この契約を参照する他のポリシーは影響を受けません。
- [参照されているすべてのポリシーの契約を更新（Update contract for all referenced policies）]：契約が更新され、現在のポリシーとこの契約を参照する他のポリシーに適用されます。
- [Create a new contract with no policies affected]：契約の複製が作成されますが、どのポリシーにも適用されません。

契約の変更

[Change Contract] ウィンドウを起動するには、[Policy Details] ペインで [Change Contract] をクリックします。使用可能なすべての契約が表示されます。必要な契約を選択し、[Change] をクリックすると、その契約をポリシーに追加できます。

契約の編集

[編集（Edit）] オプションは、契約がすでにポリシーに追加されている場合にのみ表示されます。契約の詳細を編集する場合は、契約の名前の横に表示される [編集（Edit）] をクリックします。

契約を更新したら、[Save] をクリックします。次のオプションを使用できます。

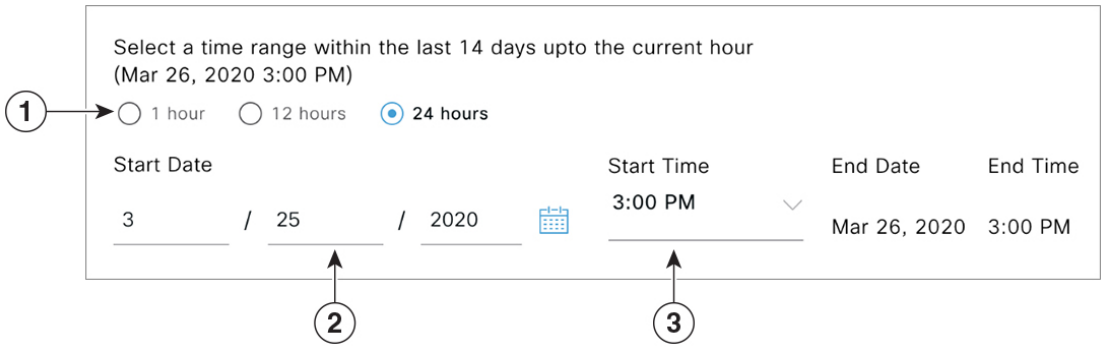
- [Update current policy only]：契約の複製が作成され、現在のポリシーに適用されます。この契約を参照する他のポリシーは影響を受けません。
- [参照されているすべてのポリシーの契約を更新（Update contract for all referenced policies）]：契約が更新され、現在のポリシーとこの契約を参照する他のポリシーに適用されます。
- [Create a new contract with no policies affected]：契約の複製が作成されますが、どのポリシーにも適用されません。

適切なオプションを選択した後に、名前と説明を入力し（1 つ目または 3 つ目のオプションを選択した場合）、[Confirm] をクリックします。

日時セレクタ

接続の概要のデータを指定するために、期間を選択できます。過去 14 日から現在の 1 時間までの時間範囲を選択できます。

図 *31* : 日時セレクタ



1. 次のいずれかのオプションを選択します。[End Time] は自動的に調整されます。
2. 月、日、年を手動で入力するかカレンダーアイコンを使用して [Start Date] を指定します。
3. [Start Time] をドロップダウンメニューから選択します。

検索の使用

[Overview] ウィンドウには、セキュリティグループ、ISE プロファイル、Stealthwatch ホストグループ、IP アドレス、または MAC アドレスのデータ全体を検索するための [Search] フィールドが用意されています。

検索フィールドへの文字入力を開始すると、セキュリティグループ、ISE プロファイル、および Stealthwatch ホストグループの自動検索が実行され、グループタイプごとに最大 3 件の結果が表示されます。MAC アドレスの場合、関連文字は 16 進数とコロンです。

Cisco グループベースポリシー分析は、エンドポイントに対し IPv4 アドレスと IPv6 アドレスの両方をサポートしています。IPv4 または IPv6 アドレスを使用してエンドポイントを検索およびフィルタリングできます。

- 次の文字を使用して、IPv4 アドレスを検索およびフィルタリングできます。
  - 数字（0 ～ 9）
  - ドット（.）

  フィルタフィールドには、最大 15 文字入力できます。
- 次の文字を使用して、IPv6 アドレスを検索およびフィルタリングできます。
  - 数字（0 ～ 9）
  - 小文字と大文字の英字（a～f、A～F）

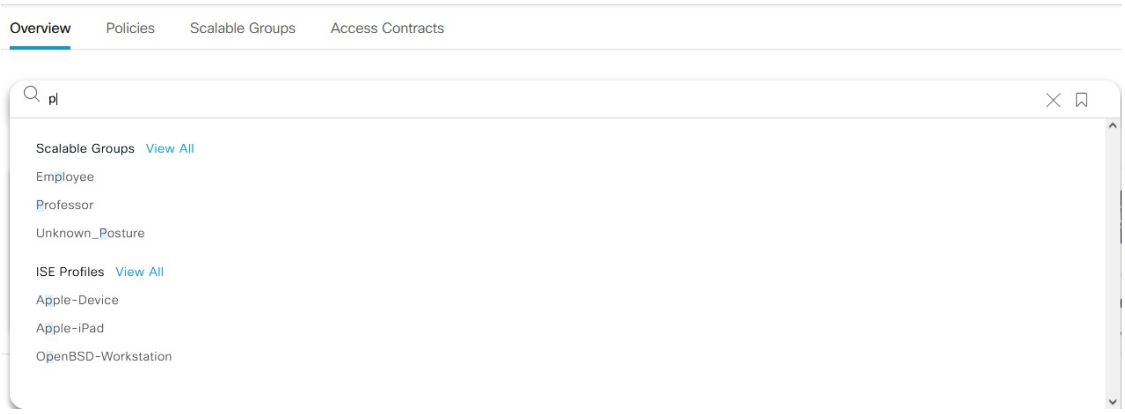
- コロン（:）

フィルタフィールドには、最大 39 文字入力できます。

（注）

- [Search Results] ウィンドウは、[View All] リンクをクリックするまで開きません。
- 読み取り専用ユーザーは、IP アドレスや MAC アドレスは検索できません。詳細については、ロールベース アクセス コントロール （1441 ページ）を参照してください。

図 *32 : [*検索（*Search***）*]* ウィンドウ**



[Focus] ドロップダウンリストから、検索条件を変更するために必要なオプションを選択します。

フィルタのアイコンは高度なフィルタ処理に使用され、MAC アドレスまたは IP アドレスを検索する場合にのみ使用できます。フィルタのアイコンをクリックすると、各列の列名の上に検索フィールドが表示されます。

列ごとの検索条件は、最大 3 つまで入力できます。列ごとの条件を複数入力する場合は、OR 演算または AND 演算を指定できます。このように作成したクエリでは、複数の列を対象に AND 演算が実行されます。

ブックマークのアイコンをクリックして [Save Current Search] オプションを使用すると、現在表示されている検索を保存できます。

保存した検索を削除するには、ブックマークのアイコンをクリックします。保存した検索の名前にカーソルを合わせ、十字アイコンをクリックします。[Delete Saved Filter] ダイアログボックスで [Yes] をクリックすると、フィルタが完全に削除されます。

ロールベース アクセス コントロール

シスコのグループベースポリシー分析は、ロールベースアクセス制御をサポートしています。読み取り/書き込みユーザーと読み取り専用ユーザーが区別されます。ただし、シスコのグルー

プベースポリシー分析は可視化を主としたもので、システムに変更は加えられないため、読み取り専用ユーザーに対する制限は限られたものになります。

- 読み取り専用ユーザーは検索クエリを保存できません。
- 読み取り専用ユーザーはデータコネクタを構成できません。
- データのエクスポートはHTTPS POST操作であるため、読み取り専用ユーザーはデータをエクスポートできません。
- 読み取り専用ユーザーはグループによる検索のみを実行でき、HTTPS POST操作を伴う他の検索機能は実行できません。



第 25 章

IP ベースおよび URL ベースのアクセス コントロール ポリシーの設定

- IP ベースのアクセス コントロール ポリシー （1443 ページ）
- IP ベースのアクセス コントロール ポリシー設定のワークフロー （1444 ページ）
- グローバル ネットワーク サーバーの設定 （1445 ページ）
- IP ネットワーク グループの作成 （1446 ページ）
- IP ネットワーク グループの編集または削除 （1447 ページ）
- IP ベースのアクセスコントロール契約の作成 （1447 ページ）
- IP ベースのアクセス コントロール コントラクトの編集または削除 （1448 ページ）
- IP ベースおよび URL ベースのアクセス コントロール ポリシーの作成 （1449 ページ）
- IP ベースおよび URL ベースのアクセス コントロール ポリシーの編集または削除 （1451 ページ）

IP ベースのアクセス コントロール ポリシー

IP ベースのアクセス コントロール ポリシーは、アクセス コントロール リスト（ACL）と同じ方法でシスコ デバイスに出入りするトラフィックを制御します。ACL と同様に、IP ベースのアクセス コントロール ポリシーにはプロトコルタイプ、送信元 IP アドレス、宛先 IP アドレス、宛先ポート番号などのさまざまな条件に基づいてトラフィックフローに適用される許可条件および拒否条件のリストが含まれています。

IP ベースのアクセス コントロール ポリシーを使用して、セキュリティ、モニターリング、ルート選択、ネットワーク アドレス変換などのさまざまな目的のためにトラフィックをフィルタ処理できます。

IP ベースのアクセス コントロール ポリシーには、次の 2 つの主要コンポーネントがあります。

- [IP Network Groups]：IP ネットワーク グループは、同じアクセス制御要件を共有する IP サブネットで構成されています。これらのグループは Catalyst Center でのみ定義できます。IP ネットワーク グループに含めることができる IP サブネットは 1 つだけです。
- [Access Contract]：アクセスコントラクトは、IP ベースのアクセス コントロール ポリシーとグループベースのアクセス コントロール ポリシーの両方で使用される共通の構成要素

です。これはアクセス制御ポリシーを構成するルールを定義します。これらのルールでは、トラフィックが特定のポートまたはプロトコルに一致したときに行われるアクション（許可または拒否）や他のルールが一致しないときに行われる暗黙のアクション（許可または拒否）を指定します。

IP ベースのアクセス コントロール ポリシー設定のワークフロー

始める前に

- 新しい IP ベースのアクセス コントロール ポリシーを作成中に、**[Policy]** > **[IP & URL Based Access Control]** > **[IP Network Groups]** ウィンドウでグループを追加する場合は、Cisco ISE は必須ではありません。
- ブラウザまたはネットワークでプロキシ設定が構成されている場合は、IP アクセス コントロール ポリシーにプロキシサブネットを含めます。
- 次のグローバルネットワーク設定が定義されていることを確認し、デバイスをプロビジョニングします。
  - AAA、DHCP、DNS サーバーなどのネットワークサーバー詳細については、グローバル ネットワーク サーバーの設定 （377 ページ）を参照してください。
  - CLI、SNMP、HTTP、HTTPS などのデバイス クレデンシャル。詳細については、グローバル デバイス クレデンシャルの設定 （379 ページ）を参照してください。
  - IP アドレス プール詳細については、「IP アドレスプールを設定する （397 ページ）」を参照してください。
  - SSID、ワイヤレス インターフェイス、およびワイヤレス無線周波数プロファイルなどのワイヤレス設定です。詳細については、「グローバルワイヤレス設定の構成 （414 ページ）」を参照してください。

手順

ステップ 1 IP ネットワーク グループを作成します。

詳細については、「IP ネットワーク グループの作成 （1446 ページ）」を参照してください。

ステップ 2 IP ベースのアクセス制御契約を作成します。

IP ベースのアクセス制御契約は、送信元と宛先の間の一連のルールを定義します。これらのルールは、ネットワーク デバイスが、指定されたプロトコルまたはポートに一致するトラフィックに基づいて実行するア

クション（許可または拒否）を指定します。詳細については、「IP ベースのアクセスコントロール契約の作成 （1447 ページ）」を参照してください。

ステップ 3 IP ベースのアクセス コントロール ポリシーの作成アクセス コントロール ポリシーは、送信元と宛先の IP ネットワーク グループ間のトラフィックを制御するアクセス制御契約を定義します。

詳細については、IP ベースおよび URL ベースのアクセス コントロール ポリシーの作成 （1449 ページ）を参照してください。

グローバル ネットワーク サーバーの設定

ネットワーク全体のデフォルトになるグローバル ネットワーク サーバーを定義することができます。

（注） サイト固有の設定を定義することで、サイトのグローバル ネットワーク設定をオーバーライドできます。

手順

ステップ 1 メインメニューから次を選択します。**[Design]** > **[Network settings]**。

ステップ 2 [Servers] タブをクリックします。

ステップ 3 [DHCP]エリアを展開します。クライアントデバイスのネットワーキング設定を管理するための 1 つまたは複数の専用 Dynamic Host Configuration Protocol（DHCP）サーバーを指定します。

ステップ 4 [Add DHCP servers] チェックボックスをオンにして、フィールドを表示します。

ステップ 5 [IP Address] フィールドに DHCP サーバーの IP アドレスを入力します。アイコンをクリックして、IP アドレスを追加します。

（注） + アイコンをクリックすると、IPv4 アドレスと IPv6 アドレスの両方を入力できます。IP アドレスを削除するには、 アイコンをクリックします。

IP アドレス プールを作成するには、少なくとも 1 つの DHCP サーバーを定義する必要があります。

ステップ 6 [DNS]エリアを展開してネットワークのドメイン名を設定し、ホスト名解決用のDomain Name System（DNS）サーバーを指定します。

ステップ 7 [Set a domain name] チェックボックスをオンにして、DNS サーバーのドメイン名を入力します。

ステップ 8 [Add DNS servers] チェックボックスをオンにして、IP アドレスを入力します。

（注）
- アイコンをクリックすると、IPv4 アドレスと IPv6 アドレスの両方を入力できます。IP アドレスを削除するには、 アイコンをクリックします。

IP アドレス プールを作成するために、少なくとも 1 つの DNS サーバーを定義する必要があります。

ステップ 9 ネットワークのシステムクロックの同期を容易にするために、1 つ以上の Network Time Protocol（NTP）サーバーを指定するには、[NTP] エリアを展開します。

ステップ 10 [Add NTP servers] チェックボックスをオンにして、フィールドを表示します。

ステップ 11 [IP Address] フィールドに、NTP サーバーの IP アドレスを入力します。アイコンをクリックして、IP アドレスを追加します。

（注）
- アイコンをクリックすると、IPv4 アドレスと IPv6 アドレスの両方を入力できます。IP アドレスを削除するには、 アイコンをクリックします。

ステップ 12 [Save] をクリックします。

IP ネットワーク グループの作成

手順

ステップ 1 メインメニューから次を選択します。 **[Policy]** > **[IP & URL Based Access Control]** > **[IP Network Groups]** の順に選択します。

ステップ 2 **[グループの追加（Add Group）]** をクリックします。

ステップ 3 **[名前（Name）]** フィールドに、IP ネットワーク グループの名前を入力します。

ステップ 4 **[説明（Description）]** フィールドに、IP ネットワーク グループを説明する単語またはフレーズを入力します。

ステップ 5 **[IP アドレスまたは IP/CIDR（IP Address or IP/CIDR）]** フィールドに、IP ネットワーク グループを構成する IP アドレスを入力します。

ステップ 6 [Save] をクリックします。

IP ネットワーク グループの編集または削除

手順

ステップ 1 メインメニューから次を選択します。 **[Policy]** > **[IP & URL Based Access Control]** > **[IP Network Groups]** の順に選択します。

ステップ 2 **[IP ネットワーク グループ（IP Network Groups）]** テーブルで、編集または削除するグループの横にあるチェックボックスをオンにします。

ステップ 3 次のいずれか 1 つのタスクを実行します。

- グループを編集するには、[編集（Edit）] をクリックします。フィールド定義の詳細については、IP ネットワーク グループの作成 （1446 ページ）を参照してください。変更を加えたら、[保存（Save）] をクリックします。
- グループを削除するには、**[削除（Delete）]** をクリックし、次に **[はい（Yes）]** をクリックして確定します。

IP ベースのアクセスコントロール契約の作成

IP ベースのアクセス契約を作成するには、次の手順を実行します。

手順

ステップ 1 メインメニューから次を選択します。**[Policy]** > **[IP & URL Based Access Control]** > **[Access Contract]** の順に選択します。

ステップ 2 [コントラクトの追加（Add Contract）] をクリックします。

ステップ 3 [Add Contract] スライドインペインの [Name] フィールドに、アクセス契約の名前を入力します。

ステップ 4 （任意） [Description] フィールドに、アクセス契約の説明を入力します。

ステップ 5 **[暗黙的アクション（Implicit Action）]** ドロップダウン リストから、**[拒否（Deny）]** または **[許可（Permit）]** を選択します。

ステップ 6 [Add] をクリックして、ポートまたはプロトコルを追加します。

ステップ 7 [ポート/プロトコルの追加（Add Port/Protocol）] ダイアログボックスで、次の手順を実行します。

a) [Action] ドロップダウンリストで、[Deny] または [Permit] を選択します。

b) **[ポート/プロトコル（Port/Protocol）]** ドロップダウン リストから、ポートまたはプロトコルを選択します。

c) [Save] をクリックします。

ステップ 8 Catalyst Center に必要なポートまたはプロトコルがない場合は、[ポート/プロトコルの作成（Create Port/Protocol）] をクリックしてポートとプロトコルを作成し、[ポート/プロトコルの作成（Create Port/Protocol）] ダイアログボックスで次の手順を実行します。

a) **[名前（Name）]** フィールドで、ポートまたはプロトコルの名前を入力します。
b) プロトコル ドロップダウン リストから、プロトコルを選択します。
c) **[ポート範囲（Port Range）]** フィールドにポート範囲を入力します。
d) Catalyst Centerで定義したとおりにポートまたはプロトコルを設定し、競合をレポートしないようにするには、[Ignore Conflict] チェックボックスをオンにします。
e) [Save] をクリックします。

ステップ 9 （任意）アクセス契約にさらにルールを含めるには、[Add] をクリックして、ステップ 7（1447 ページ）を繰り返します。

ステップ 10 [Save] をクリックします。

IP ベースのアクセス コントロール コントラクトの編集または削除

ポリシーで使用されている契約を編集すると、**[IP ベースのアクセス コントロール ポリシー（IP Based Access Control Policies）]** ウィンドウのポリシーの状態が **[変更（MODIFIED）]** に変わります。変更されたポリシーは、ネットワークに導入されたポリシーと一致しないため、古いと見なされます。この問題を解決するには、ネットワークにポリシーを再展開する必要があります。

手順

ステップ 1 メインメニューから次を選択します。**[Policy]** > **[IP & URL Based Access Control]** > **[Access Contract]** の順に選択します。

ステップ 2 編集または削除するコントラクトの横にあるチェックボックスをオンにして、次のいずれかのタスクを実行します。

- 契約を変更するには、[Edit] をクリックして変更を行い、[Save] をクリックします。フィールド定義の詳細については、IP ベースのアクセスコントロール契約の作成（1447 ページ）を参照してください。

（注） ポリシーで使用されている契約を変更した場合は、**[Policy]** > **[IP & URL Based Access Control]** > **[IP & URL Access Control Policies]** の順に選択し、ポリシー名の横にあるチェックボックスをオンにして、[Deploy] をクリックすることによって、変更したポリシーを展開する必要があります。

• 契約を削除するには、[削除（Delete）] をクリックします。

IP ベースおよび URL ベースのアクセス コントロール ポリシーの作成

ネットワークの認証後アクセス制御リスト（ACL）を作成できます。ACL は、IP、URL、またはその両方に基づくことができます。

始める前に

IP ベースのアクセス コントロール ポリシー設定のワークフロー（1444 ページ）を参照してください。

手順

ステップ 1 メインメニューから次を選択します。**[Policy]** > **[IP & URL Based Access Control]** > **[IP & URL Access Control Policies]** の順に選択します。

ステップ 2 [ポリシーの追加（Add Policy）] をクリックします。

または、最初の 2 つの手順の代わりに、メニューアイコンをクリックして、**[Workflows]** > **[Create IP & URL-Based Access Control Policy]** を選択できます。 [Overview] ウィンドウが開いたら、[Let's Do it] をクリックしてワークフローを開始します。

ステップ 3 [Policy Name and Details] ウィンドウで、次の手順を実行します。

a) ポリシーの名前と説明を入力します。

b) [Select ACL Type] で、必要なチェックボックスをオンにします。

- [IPv4] **または [IPv6]**：IP ベースのアクセス コントロール ポリシーを設定します。
- [URL]：URL ベースのアクセス コントロール ポリシーを設定します。
- [IPv4] と [URL]：IPv4 ベースおよび URL ベースのアクセス コントロール ポリシーを設定します。
- [IPv6] と [URL]：IPv6 ベースおよび URLベースのアクセス コントロール ポリシーを設定します。

ステップ 4 **[サイトとSSIDの選択（Select Sites and SSID）]** ウィンドウで、ポリシーを適用するサイトを選択し、SSID を選択します。

サイトが SSID で既にプロビジョニングされていることを確認してください。

Flex またはファブリック SSID の場合は、AP がサイトでプロビジョニングされていることを確認します。

URL ACL を選択した場合、Flex またはファブリック SSID と併せてローカル SSID を選択することはできません。

ステップ 5 IP ACL を選択した場合、**[IPアクセス制御リスト（IP Access Control List）]** ウィンドウで IP ACL のカスタムルールを設定します。

実行する操作	結果
ルールの追加	**1.** [Add New Rule] をクリックします。 **2.** [新規ルールの追加（Add New Rule）] ダイアログボックスで、対応するドロップダウンリストから送信元、宛先、契約、および方向を選択します。 （注） 双方向ルールの場合は、送信元と宛先が異なることを確認してください。送信元と宛先が [任意（Any）] に設定されている場合は、カスタム契約のみを使用します。 **3.** [Add] をクリックします。
ルールの編集	**1.** 編集するルールの鉛筆アイコンをクリックします。 **2.** 必要な設定を編集します。 **3.** [Save] をクリックします。 （注） デフォルトルールは編集できません。
ルールの削除	削除したいルールの [削除（delete）] アイコンをクリックします。 （注） デフォルトルールは削除できません。
ルールのシーケンスの更新	ルールの アイコンをクリックし、必要な位置にルールをドラッグアンドドロップします。 （注） デフォルトルールのシーケンスは更新できません。

ステップ 6 URL ACL を選択した場合は、**[URLアクセス制御リスト（URL Access Control List）]** ウィンドウで次の手順を実行します。

1. URL を入力します。

（注） 最大 20 個の URL を含めることができます。

2. [アクション（Action）] ドロップダウンリストから、[許可（Permit）] または [拒否（Deny）] を選択します。

ステップ 7 [Summary] ウィンドウで、設定を確認します。変更するには、[Edit] をクリックします。

ステップ 8 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

ステップ 9 [Tasks] ウィンドウで、タスクの展開を監視します。

IP ベースおよび URL ベースのアクセス コントロール ポリシーの編集または削除

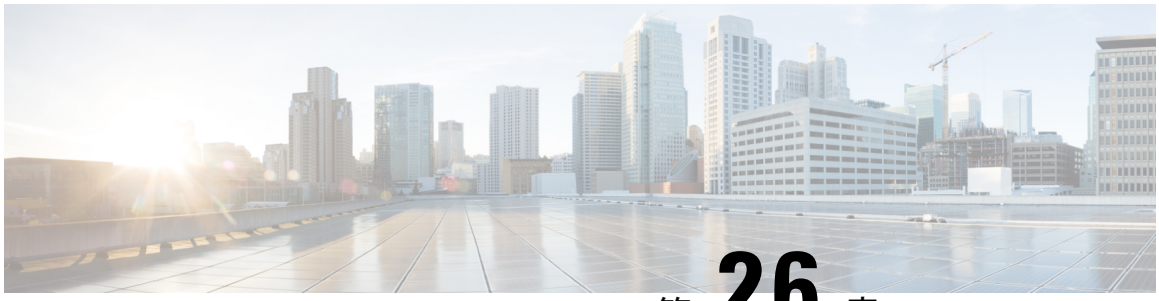
必要な場合は、IP ベースおよび URL ベースのアクセス コントロール ポリシーを変更または削除できます。

手順

ステップ 1 メインメニューから次を選択します。**[Policy] > [IP & URL Based Access Control] > [IP & URL Access Control Policies]** の順に選択します。

ステップ 2 ポリシーを編集するには、編集するポリシーの名前をクリックし、必要な変更を加えて、[Save & Schedule] をクリックします。詳細については、IP ベースおよび URL ベースのアクセス コントロール ポリシーの作成 （1449 ページ）を参照してください。

ステップ 3 ポリシーを削除するには、削除するポリシーの横にあるチェックボックスをオンにして [Delete] をクリックします。



第 26 章

アプリケーションポリシーの設定

- アプリケーションポリシーの概要 （1453 ページ）
- アプリケーションポリシーの管理 （1469 ページ）
- キューイングプロファイルの管理 （1482 ページ）
- WAN インターフェイスのアプリケーションポリシーの管理 （1483 ページ）

アプリケーションポリシーの概要

Quality of Service（QoS）とは、選択したネットワーク トラフィックに、優先的なサービスやニーズに合ったサービスを提供するネットワーク機能を意味します。QoS を設定することで、ビジネスの目標（音声品質が会社の標準規格を満たしていることの保証、ビデオの高い Quality of Experience（QoE）の確保など）を引き続き順守しながら、ネットワーク リソースを最も効率的に使用する方法でネットワーク トラフィックを処理することができます。

QoS は、Catalyst Center のアプリケーション ポリシーを使用してネットワークに設定できます。アプリケーション ポリシーは、次の基本的なパラメータで構成されています。

- [Application Sets]：同様のネットワークトラフィックを必要とする一連のアプリケーション。各アプリケーションセットには、トラフィックの優先順位を定義するビジネスとの関連性グループ（ビジネス関連、デフォルト、またはビジネスと無関係）が割り当てられます。QoS パラメータは、Cisco Validated Design（CVD）に基づいて 3 つのグループごとに定義されます。一部のパラメータは、それぞれの目的に合わせてより詳細に調整できます。

- [Site Scope]：アプリケーションポリシーが適用されているサイト。有線ポリシーを設定すると、ポリシーは、サイト範囲内のすべての有線デバイスに適用されます。同様に、選択したサービス セット識別子（SSID）のワイヤレス ポリシーを設定すると、範囲内で SSID が定義されているすべてのワイヤレス デバイスにポリシーが適用されます。

（注） プラグアンドプレイでオンボードされた有線デバイスの場合、サイトで QoS ポリシーを設定すると、その QoS ポリシーはサイトに追加されたデバイスにおいてデフォルトで有効になります。

Catalyst Center はこれらのパラメータをすべて受け取り、適切なデバイスの CLI コマンドに変換します。Catalyst Center はポリシーの展開時に、サイトの範囲で定義されているデバイスに各コマンドを設定します。

（注） Catalyst Center はデバイスで使用可能な QoS 機能セットに基づいて、各デバイスに QoS ポリシーを設定します。デバイスの QoS 実装の詳細については、対応するデバイスの製品マニュアルを参照してください。

アプリケーションポリシーでの CVD ベースの設定

アプリケーション ポリシーのデフォルトの QoS 信頼およびキューイング設定は、Enterprise Medianet の QoS デザイン向けの Cisco Validated Design（CVD）に基づいています。CVD は、一般的な使用例や現行のシステム設計上の優先事項に基づき、システム設計の基盤を提示しています。CVD には、お客様のニーズに応じるための幅広いテクノロジー、機能、アプリケーションが組み込まれています。それぞれのソリューションには、エンジニアによる包括的なテストと文書化が実施されており、迅速で、信頼性が高く、予測可能な導入が確保されています。

QoS に関連する最新の検証済み設計は、Cisco Press の書籍『*End-to-End QoS Network Design: Quality of Service for Rich-Media & Cloud Networks*, 2nd Edition』（http://www.ciscopress.com/store/end-to-end-qos-network-design-quality-of-service-for-9781587143694）で公開されています。追加情報については、次のシスコのドキュメントを参照してください。

- シスコ検証済みデザイン（CVD）
- Enterprise Medianet Quality of Service Design 4.0
- Medianet Campus QoS Design 4.0
- Medianet WAN Aggregation QoS Design 4.0

サイトの範囲

サイト範囲は、アプリケーションポリシーが適用されるサイトを定義します。ポリシーを定義するときに、ポリシーが有線デバイス用かワイヤレスデバイス用かを設定します。また、サイト範囲も設定します。有線ポリシーを設定すると、ポリシーは、サイト範囲内のすべての有線デバイスに適用されます。同様に、選択したサービス セット識別子（SSID）のワイヤレス ポリシーを設定すると、サイト範囲内で SSID が定義されている、サイト範囲内のすべてのワイヤレス デバイスにポリシーが適用されます。

これにより、有線ネットワーク セグメントとワイヤレス ネットワークセグメントの動作の相違を補うために、必要に応じてトレードオフを実施できます。たとえば、ワイヤレス ネットワークでは通常、有線ネットワークと比較した場合に低帯域幅、低速、パケット損失増加の特徴があります。個々のワイヤレスセグメントは、ローカルの RF 干渉、輻輳、ネットワークデバイスの機能の違いなどの要因によってさらに変動が見られます。個々のワイヤレスセグメン

トにセグメントごとのポリシーを適用することで、優先順位の高いトラフィックが受ける、ワイヤレスネットワークの劣化による影響が小さくなるように、トラフィック処理ルールを調整できます。

ビジネス関連グループ

ビジネス関連グループは、ビジネスや事業への関連性に応じて、指定されたアプリケーションセットを分類します。

ビジネス関連グループは、高優先、中立、低優先の3つのタイプのトラフィックにマッピングされます。これらのグループには、次のものがあります。

- **ビジネス関連（Business Relevant）**：（高優先トラフィック）このグループのアプリケーションは組織の目的に直接関与し、音声、ビデオ、ストリーミング、コラボレーション型マルチメディア アプリケーション、データベース アプリケーション、エンタープライズ リソース アプリケーション、電子メール、ファイル転送、コンテンツ配布など、さまざまな種類があります。ビジネス関連として指定されているアプリケーションは、Internet Engineering Task Force（IETF）RFC 4594 の規定に従い、業界推奨のベスト プラクティスに従って処理されます。
- **デフォルト（Default）**：（平均的優先度のトラフィック）このグループは、ビジネスに関連している場合もあればしていない場合もあるアプリケーションを対象としています。たとえば一般的な HTTP または HTTPS トラフィックは、組織の目的に寄与する場合もしない場合もあります。たとえば、レガシーアプリケーションや新しく導入されたアプリケーションなどでも、一部のアプリケーションの目的については分析していない場合があります。したがって、これらのアプリケーションのトラフィック フローは、IETF RFC 2747 および 4594 で説明されているように、デフォルトの転送サービスで処理する必要があります。
- **ビジネスと無関係（Business Irrelevant）**：（低優先トラフィック）このグループは、組織の目的達成に寄与しないと識別されたアプリケーションを対象としています。主にコンシューマ向けかエンターテイメント向け、あるいは本質的にその両方に該当するアプリケーションです。この種類のトラフィックは、IETF RFC 3662 および 4594 で説明されている「スカベンジャ」サービスとして処理することをお勧めします。

アプリケーションはアプリケーションセットに分類されて、ビジネス関連グループにソートされます。アプリケーションセットはポリシーに現状のまま含めることができます。または、ビジネス目標やネットワーク構成のニーズを満たすように変更することができます。

たとえば、YouTube はコンシューマ メディア アプリケーション セットのメンバーです。一般的に、ほとんどのお客様がこのアプリケーションをこのように分類しているため、（デフォルトでは）YouTube はビジネスと無関係です。ただし、この分類がすべての企業に当てはまるわけではありません。たとえば、いくつかのビジネスでは YouTube をトレーニング目的で使用することがあります。このような場合、管理者は、デフォルトでビジネス関連であるストリーミング ビデオ アプリケーション セットに YouTube アプリケーションを移動できます。

コンシューマとプロデューサ

あるアプリケーションから別のアプリケーションにトラフィックが送られた（特定の a から b へのトラフィック フローが作成された）ときにトラフィックが特定の方法で処理されるように、アプリケーション間の関係を設定することができます。このような関係のアプリケーションをプロデューサとコンシューマと呼び、次のように定義しています。

- **プロデューサ**：アプリケーション トラフィックの送信元。たとえば、クライアント/サーバー アーキテクチャでは、トラフィック フローは主にサーバーからクライアントの方向であるため、アプリケーション サーバーがプロデューサと見なされます。ピアツーピア アプリケーションの場合は、リモート ピアがプロデューサと見なされます。
- **コンシューマ**：アプリケーション トラフィックの受信者。コンシューマに該当するのは、クライアント/サーバ アーキテクチャの場合はクライアント エンドポイント、ピアツーピア アプリケーションの場合はローカル デバイスなどです。コンシューマはエンドポイントデバイスの場合がありますが、そのようなデバイスの特定のユーザーの場合もあります（通常、IP アドレスまたは特定のサブネットによって識別される）。また、あるアプリケーションが別のアプリケーション トラフィック フローのコンシューマになる場合もあります。

この関係を設定することにより、このシナリオに一致するトラフィックに関して特定のサービスレベルを設定できます。

マーキング、キューイング、ドロッピングの処理

Catalyst Center は、IETF RFC 4594 およびアプリケーションに割り当てられたビジネス関連のカテゴリでの処理のマーキング、キューイング、およびドロッピングをベースとしています。Catalyst Center は、デフォルト カテゴリのすべてのアプリケーションをデフォルトの転送アプリケーション クラスに割り当て、無関係なビジネス カテゴリのすべてのアプリケーションをスカベンジャ アプリケーション クラスに割り当てます。関連するビジネス カテゴリのアプリケーションについては、Catalyst Center はアプリケーションのタイプに基づいてトラフィック クラスをアプリケーションに割り当てます。次の表に、アプリケーションクラスとそれぞれの処理を示します。

表 *60 :* マーキング、キューイング、ドロッピングの処理

ビジネス関連性	アプリケーションクラス	ホップ単位動作	キューイングとドロッピング	アプリケーションの説明
該当する	VoIP[5]	Expedited Forwarding（EF）	プライオリティキューイング（PQ）	VoIP テレフォニー（ベアラのみ）トラフィック。たとえば、Cisco IP 電話。
	ブロードキャストビデオ	クラス セレクタ（CS）5	PQ	ブロードキャスト TV、ライブイベント、ビデオ監視フロー、同様の非弾性ストリーミング メディア フロー（Cisco IP Video Surveillance や Cisco Enterprise TV など）。（非弾性フローとは、非常にドロップされやすく、再送信またはフロー制御機能のいずれか、または両方がないフローです。）
	リアルタイムインタラクティブ	CS4	PQ	非弾性の高解像度インタラクティブ ビデオ アプリケーションおよびそれらのアプリケーションのオーディオおよびビデオコンポーネント（Cisco TelePresence など）。
	マルチメディア会議	相対的優先転送（AF）41	帯域幅（BW）キューと Differentiated Services Code Point（DSCP）Weighted Random Early Detect（WRED）	デスクトップソフトウェアのマルチメディア コラボレーション アプリケーションおよびそれらのアプリケーションのオーディオおよびビデオコンポーネント（Cisco Jabber や Cisco Webex など）。
	マルチメディアストリーミング	AF31	BW キューと DSCP WRED	ビデオオンデマンド（VoD）ストリーミング ビデオフローおよび仮想デスクトップアプリケーション。たとえば、Cisco Digital Media System。
	ネットワーク制御	CS6	BW キューのみ[6]	EIGRP、OSPF、BGP、HSRP、IKE などのエンタープライズ ネットワークの信頼性の高い運用のために必要とされるネットワーク コントロール プレーン トラフィック。
	シグナリング	CS3	BW キューと DSCP	IP 音声およびビデオ テレフォニー インフラストラクチャのコントロールプレーン トラフィック。
	Operations, Administration, and Management（OAM）	CS2	BW キューと DSCP[7]	SSH、SNMP、syslog などのネットワーク運用、管理、管理トラフィック
		AF21		

ビジネス関連性	アプリケーションクラス	ホップ単位動作	キューイングとドロッピング	アプリケーションの説明
	トランザクションデータ（低遅延データ）		BW キューと DSCP WRED	エンタープライズ リソース プランニング（ERP）、顧客関係管理（CRM）、およびその他のデータベース アプリケーションなどのインタラクティブ（フォアグラウンド）データ アプリケーション。
	バルクデータ（高スループットデータ）	AF11	BW キューと DSCP WRED	電子メール、File Transfer Protocol（FTP）、バックアップ アプリケーションなどの非インタラクティブ（バックグラウンド）データ アプリケーション。
デフォルト	デフォルトの転送（ベストエフォート）	DF	デフォルト キューと RED	デフォルトのアプリケーション、およびデフォルトのビジネス関連グループに割り当てられるアプリケーション。プライオリティ、保証された帯域幅、または差分サービス クラスに割り当てられるのはごく少数のアプリケーションであるため、大部分のアプリケーションは引き続きデフォルトでベストエフォート型サービスになります。
非関連	スカベンジャー	CS1	最小 BW キュー（ディファレンシャル）と DSCP	非ビジネス関連のトラフィック フロー、およびビジネス関連でないグループに割り当てられているアプリケーション（エンターテイメント向けのデータやメディア アプリケーションなど）。たとえば、YouTube、Netflix、iTunes、Xbox Live。

[5] VoIP シグナリング トラフィックは、コール シグナリング クラスに割り当てられます。
[6] ネットワーク制御トラフィックはドロップされるべきではないため、このクラスでは WRED が有効になりません。
[7] OAM トラフィックはドロップされるべきではないため、このクラスでは WRED が有効になりません。

サービスプロバイダーのプロファイル

サービス プロバイダー プロファイルでは、特定の WAN プロバイダーのサービスクラスを定義します。4 クラス、5 クラス、6 クラス、8 クラスのモデルを定義できます。

アプリケーションポリシーがデバイスに展開されると、各サービス プロバイダー プロファイルには、各サービスプロバイダークラスを DSCP 値と帯域幅割り当てのパーセンテージにマップする特定のサービスレベル契約（SLA）が割り当てられます。

アプリケーションポリシーを設定するときにサービス プロバイダー プロファイルの DSCP 値と帯域幅割り当てのパーセンテージをカスタマイズできます。

サービス プロバイダー プロファイルを作成したら、そのプロファイルを WAN インターフェイスで設定する必要があります。

表 *61 : 4* クラスでのサービス プロバイダー プロファイルのデフォルト *SLA* 属性

クラス名	DSCP	プライオリティクラス	SLA	
			帯域幅（%）	残りの帯域幅（%）
音声	EF	はい	10	—
クラス 1 データ	AF31	—	—	44
クラス 2 データ	AF21	—	—	25
デフォルト	0	—	—	31

表 *62 : 5* クラスでのサービス プロバイダー プロファイルのデフォルト *SLA* 属性

クラス名	DSCP	プライオリティクラス	SLA	
			帯域幅（%）	残りの帯域幅（%）
音声	EF	はい	10	—
クラス 1 データ	AF31	—	—	44
クラス 2 データ	AF21	—	—	25
クラス 3 データ	AF11	—	—	1
デフォルト	ベスト エフォート	—	—	30

表 *63 : 6* クラスでのサービス プロバイダー プロファイルのデフォルト *SLA* 属性

クラス名	DSCP	プライオリティクラス	SLA	
			帯域幅（%）	残りの帯域幅（%）
クラス 1 データ	AF31	—	—	10
クラス 3 データ	AF11	—	—	1
ビデオ	AF41	—	—	34
音声	EF	はい	10	—
デフォルト	0	—	—	30

クラス名	DSCP	プライオリティクラス	SLA	
			帯域幅（%）	残りの帯域幅（%）
クラス 2 データ	AF21	—	—	25

表 *64 : 8* クラスでのサービス プロバイダー プロファイルのデフォルト *SLA* 属性

クラス名	DSCP	プライオリティクラス	SLA	
			帯域幅（%）	残りの帯域幅（%）
ネットワーク-コントロール管理	CS6	—	—	5
ストリーミングビデオ	AF31	—	—	10
コール シグナリング	CS3	—	—	4
スカベンジャー	CS1	—	—	1
インタラクティブビデオ	AF41	—	—	30
音声	EF	はい	10	—
デフォルト	0	—	—	25
重要なデータ	AF21	—	—	25

キューイングプロファイル

キューイング プロファイルでは、インターフェイス速度とトラフィック クラスに基づいたインターフェイスの帯域幅割り当てを定義することができます。

（注） キューイングプロファイルは、サービス プロバイダ プロファイルに接続されている WAN 側インターフェイスには適用されません。

次のインターフェイス速度がサポートされます。

- 100 Gbps
- 10/40 Gbps
- 1 Gbps

- 100 Mbps
- 10 Mbps
- 1 Mbps

インターフェイスの速度が 2 つのインターフェイス速度の間である場合、Catalyst Center は、より低いインターフェイス速度でインターフェイスを取り扱います。

（注） Catalyst Center は、正しいポリシーを適用するためにインターフェイスの動作速度の検出を試みます。ただし、スイッチ ポートが管理上ダウンしている場合、Catalyst Center は速度を検出できません。この場合、Catalyst Center は、インターフェイスのサポートされた速度を使用します。

キューイング ポリシーは、アプリケーション ポリシーの一部として定義します。アプリケーションポリシーを展開すると、サイト範囲内の選択されたサイトのデバイスが、割り当てられた LAN キューイング ポリシーで設定されます。LAN キューイング ポリシーが割り当てられていない場合、アプリケーション ポリシーはデフォルトの CVD キューイング ポリシーを使用します。

すでに展開されているアプリケーション ポリシーのキューイング ポリシーを変更すると、ポリシーは失効し、変更をデバイスに適用するにはポリシーを展開しなおす必要があります。

（注） キューイングポリシーに関するその他のガイドラインと制限事項は、次のとおりです。

- LANキューイングプロファイルは、ポリシーで使用されている場合には削除できません。
- ポリシーに関連付けられているキューイングプロファイルを更新すると、ポリシーは期限切れとしてマーキングされます。最新の変更をプロビジョニングするには、ポリシーを展開しなおす必要があります。
- トラフィック クラス キューイングをカスタマイズしても、シスコのサービス プロバイダ スイッチおよびルータのインターフェイスは影響を受けません。これらのインターフェイスの設定は、引き続き Catalyst Center を使用することなく実施します。

表 *65* : デフォルト *CVD LAN* キューイングポリシー

トラフィッククラス	デフォルトの帯域幅（合計 = 100%）[8]
ビジネス関連の音声	10%
ビジネス関連のブロードキャストビデオ	10%
ビジネス関連のリアルタイム インタラクティブ	13%

トラフィッククラス	デフォルトの帯域幅（合計 = 100%）[8]
ビジネス関連のマルチメディア会議	10%
ビジネス関連のマルチメディア ストリーミング	10%
ビジネス関連のネットワーク制御	3%
ビジネス関連のシグナリング	2%
ビジネス関連の OAM	2%
ビジネス関連のトランザクションデータ	10%
ビジネス関連のバルクデータ	4%
ビジネス関連のスカベンジャ	1%
ビジネス関連のベストエフォート	25%

[8] 音声、ブロードキャストビデオ、およびリアルタイムインタラクティブ トラフィック クラスの合計帯域幅を 33% 以下にすることを推奨します。

リソースが制限されているデバイスの処理順

ネットワーク デバイスの中には、ネットワーク アクセス コントロール リスト（ACL）および ACE を格納するためのメモリ（TCAM と呼ばれる）が制限されているものがあります。このため、アプリケーション用の ACL と ACE がこれらのデバイス上に設定されている場合は、利用可能な TCAM 領域が使用されます。TCAM スペースを使い果たすと、そのデバイスには追加アプリケーション用の QoS 設定を設定できません。

そのようなデバイスで最も重要なアプリケーションの QoS ポリシーが確実に設定されるように、Catalyst Center は次の順序で TCAM スペースを割り当てます。

1. [Rank]：カスタムアプリケーションおよびお気に入りのアプリケーションに割り当てられた番号（ただし既存のデフォルト NBAR アプリケーションは除く）。ランクの番号が小さくなるほど、優先順位が高くなります。たとえば、ランク 1 のアプリケーションはランク 2 のアプリケーションよりも優先順位が高くなります。ランクがない場合は、優先順位が最も低くなります。

（注）
- カスタム アプリケーションには、デフォルトでランク 1 が割り当てられています。
- NBAR アプリケーションをお気に入りとしてマークすると、ランクは 1000 に設定されます。

2. [トラフィッククラス（Traffic Class）]：優先順位は次の順序に基づいています。シグナリング、バルク データ、Operations Administration Management（Ops Admin Mgmt）、トランザクション データ、スカベンジャ、マルチメディア ストリーミング、マルチメディア会議、リアルタイム インタラクティブ、ブロードキャスト ビデオ、VoIP テレフォニー。
3. [Popularity]：CVD の基準に基づいて割り当てられた番号（1 ～ 10）。ポピュラリティの番号は変更できません。ポピュラリティが 10 のアプリケーションは、ポピュラリティが 9 のアプリケーションよりも優先順位が高くなります。

（注）
- カスタムアプリケーションには、ポピュラリティ 0 が割り当てられます。
- デフォルトNBARアプリケーションには、CVDの基準に基づいてポピュラリティ番号（1 ～10）が割り当てられます。アプリケーションをお気に入りとしてマークしても、ポピュラリティ番号は変わりません（ランクのみ変更されます）。

4. [Alphabetization]：2 つ以上のアプリケーションのランクとポピュラリティ番号が同一の場合、それらのアプリケーションはアプリケーション名のアルファベット順にソートされ、ソート順に従い優先順位が割り当てられます。

たとえば、次のアプリケーションを含むポリシーを定義すると仮定します。

- カスタム アプリケーション custom_realtime。デフォルトでランク 1 とポピュラリティ 10 が割り当てられています。
- カスタム アプリケーション custom_salesforce。デフォルトでランク 1 とポピュラリティ 10 が割り当てられています。
- corba-iiop という名前のトランザクション データ トラフィック クラスのアプリケーション。お気に入りとして指定されており、ランク 10,000、および（CVD に基づいて）ポピュラリティ 9 が付与されています。
- gss-http という名前の Ops Admin Mgmt トラフィック クラスのアプリケーション。お気に入りとして指定されており、ランク 10,000、および（CVD に基づいて）ポピュラリティ 10 が付与されています。
- 他のすべてのデフォルトNBARアプリケーションにはランクはありませんが、トラフィック クラスと（CVD に基づいて）デフォルト ポピュラリティに従って処理されます。

優先順位付けのルールに従って、アプリケーションはデバイスにおいて次の順序で設定されます。

アプリケーションの設定順	理由
1. カスタム アプリケーション custom_realtime	カスタム アプリケーションには最も高い優先順位が付与されます。custom_salesforce アプリケーションと custom_realtime アプリケーションのランクおよびポピュラリティが同じであるとすると、これらのアプリケーションはアルファベット順にソートされ、custom_realtime が custom_salesforce より前になります。
2. カスタム アプリケーション custom_salesforce	
3. お気に入りのアプリケーション gss-http	これら両方のアプリケーションはお気に入りとして指定されているため、同じアプリケーション ランクになります。そのため、Catalyst Center は各アプリケーションをトラフィック クラスに基づいて評価します。gss-http は Ops Admin Mgmt トラフィック クラスに属しているため最初に処理され、その後、トランザクション データ トラフィック クラスに属している corba-iiop アプリケーションが処理されます。トラフィック クラスによって処理順が決まっているため、ポピュラリティは考慮されません。
4. お気に入りのアプリケーション corba-iiop	
5. 他のすべてのデフォルト NBAR アプリケーション	他のすべてのアプリケーションは、トラフィック クラスとポピュラリティに従って次に優先され、ポピュラリティが同じアプリケーションは、アプリケーション名のアルファベット順にソートされます。

ポリシーのドラフト

ポリシーを作成するときに、ポリシーを展開せずにドラフトとして保存できます。ドラフトとして保存すると、後でポリシーを開いて変更できます。また、展開したポリシーを変更して、ドラフトとして保存することもできます。

（注） ポリシーを保存または展開した後に、名前を変更することはできません。

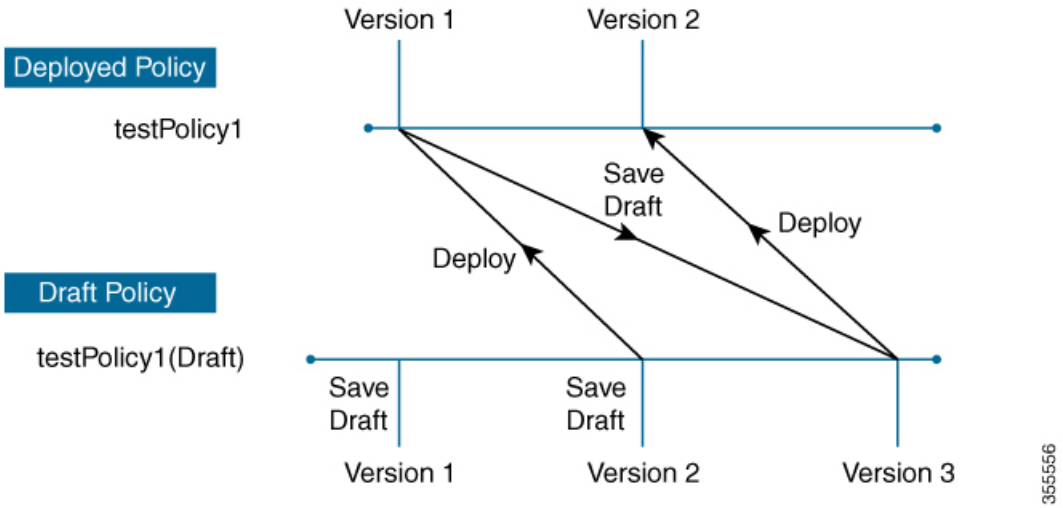
ドラフトポリシーと展開したポリシーは相互に関連付けられますが、それぞれ独自にバージョン管理されます。

ポリシーをドラフトとして保存すると、Catalyst Center はポリシー名に (Draft) を追加してバージョン番号を 1 つ上げます。ポリシーを展開すると、Catalyst Center が展開したポリシーのバージョン番号を 1 つ上げます。

たとえば、図に示すように、testPolicy1 という名前のポリシーを作成してドラフトとして保存します。ポリシーは testPolicy1 (Draft)、バージョン番号 1 として保存されます。ドラフトを変更して、再度保存します。ポリシーの名前は同じ testPolicy1 (Draft) のままですが、バージョン番号は 2 に上がります。

ポリシーが気に入ったのでネットワークに展開します。ポリシーは testPolicy1 という名前で展開され、バージョン番号は 1 です。展開したポリシーを変更して、ドラフトとして保存します。ドラフトポリシー testPolicy1 (Draft) は、バージョン番号 3 に上がります。最終的にそのバージョンを展開するとき、testPolicy1 はバージョン 2 になります。

図 *33* : 展開したポリシーとドラフトポリシーのバージョン管理



ドラフトポリシーまたは展開したポリシーのいずれかを変更および保存するときは、ドラフトポリシーのバージョン番号が上がります。同様に、ドラフトポリシーまたは変更した展開済みポリシーのいずれかを展開するときは、展開したポリシーのバージョンが上がります。

展開したポリシーと同様に、ドラフト ポリシーの履歴を表示し、以前のバージョンにロールバックすることができます。

ポリシー バージョンの履歴表示と以前のバージョンへのロール バックについては、ポリシーのバージョン管理 （1466 ページ）を参照してください。

ポリシーのスケジューリング

ポリシーを作成または変更した後に、そのポリシーを、ポリシーに関連付けられたデバイスに展開または再展開できます。このポリシーの展開/再展開は、すぐに行うことも、特定の日時（たとえば、週末のオフピーク時）に行うこともできます。ポリシー導入のスケジューリングは有線またはワイヤレスのデバイスに対して実施できます。

展開するポリシーのスケジュールを設定すると、そのポリシーとサイト範囲がロックされます。ポリシーの表示は可能ですが、編集することはできません。ポリシーを展開する予定が変更された場合は、その展開をキャンセルできます。

（注） スケジュール イベントが発生すると、ポリシーは、さまざまなポリシー コンポーネント（アプリケーション、アプリケーションセット、およびキューイング プロファイルなど）に対して検証されます。この検証に失敗すると、ポリシーの変更は行われません。

ポリシーのバージョン管理

このポリシーのバージョン管理により、次のタスクが可能になります。

- 以前のバージョンと現在（最新）のバージョンを比較して相違点を確認する。
- ポリシーの以前のバージョンを表示し、サイト範囲内のデバイスに再適用するバージョンを選択する。

あるバージョンのポリシーを編集しても、そのポリシーの別のバージョンやポリシーのコンポーネント（そのポリシーによって管理されるアプリケーションセットなど）は影響を受けません。たとえば、ポリシーからアプリケーションセットを削除しても、そのアプリケーションセットは Catalyst Center、そのポリシーの別のバージョン、または他のポリシーからは削除されません。ポリシーとアプリケーション セットは互いに独立して存在するため、存在しなくなったアプリケーションセットを含むバージョンのポリシーを保持できます。存在しなくなったアプリケーションセットを参照するポリシーを展開しようとしたり、それらのポリシーを古いバージョンにロールバックしようとしたりすると、エラーが発生します。

（注） ポリシーのバージョン管理では、アプリケーション（ランク、ポート、プロトコルなど）、アプリケーション セット メンバー、LAN キューイング プロファイル、およびサイトの変更は取得されません。

オリジナルポリシーの復元

初めてデバイスにポリシーを展開する際、Catalyst Center は、デバイスの元の Cisco Modular QoS CLI ポリシー設定をデタッチしますが、それらはデバイス上に残ります。Catalyst Center は、デバイスの元の NBAR 設定を Catalyst Center に保存します。このアクションにより、必要に応じてオリジナルのモジュラー式 QoS CLI ポリシーと NBAR 設定を後でデバイスに復元することが可能になります。

（注） このようにモジュラー式QoS CLIポリシーはデバイスから削除されませんが、ユーザーがこれらのポリシーを削除すると、元のポリシー復元する Catalyst Center の機能を使用してそれらを復元することができなくなります。

元のポリシー設定をデバイスに復元する際、Catalyst Centerは、展開されている既存のポリシー設定を削除し、デバイス上にあった元の設定に戻します。

アプリケーション ポリシーを展開する前に存在していたモジュラー式 QoS CLI ポリシー設定はすべて、インターフェイスに再アタッチされます。ただし、マルチレイヤ スイッチング（MLS）設定などのキューイングポリシーは復元されません。代わりに、デバイスは、Catalyst Center によって最後に適用された MLS 設定を維持します。

元のポリシー設定をデバイスに復元すると、Catalyst Center に保存されているポリシーが削除されます。

（注） この機能には、次のような追加のガイドラインと制限事項があります。

- 初めてポリシーをデバイスに展開する試みが失敗すると、Catalyst Centerは、元のポリシー設定をデバイスに復元することを自動的に試みます。
- そのポリシーがデバイスに適用された後にデバイスがアプリケーションポリシーから削除された場合、そのポリシーはデバイス上に残ります。Catalyst Centerは、ポリシーを自動的に削除したり、デバイスの QoS 設定を元の (事前Catalyst Center) 設定に復元したりしません。

陳腐化したアプリケーションポリシー

ポリシーで参照されているものの設定を変更すると、アプリケーションポリシーが陳腐化する可能性があります。アプリケーションポリシーが陳腐化した場合、変更を有効化するためにアプリケーション ポリシーを再展開する必要があります。

アプリケーション ポリシーは、次の理由で陳腐化する可能性があります。

- アプリケーション設定で参照されているアプリケーションの変更。
- サービス プロバイダー プロファイルの割り当て、WAN サブラインレート、WAN または LAN マーキングなどのインターフェイスの変更。
- キューイング プロファイルの変更。
- ポリシーの親サイト下への新規サイトの追加。
- ポリシーによって参照されるサイトへのデバイスの追加。
- ポリシーが同じサイト間でのデバイスの移動。
- インターフェイス除外/包含の変更。
- デバイスコントローラベースのアプリケーション認識（CBAR）ステータスの変更。

アプリケーションポリシーのガイドラインと制限事項

- Catalyst Center は、ワイヤレスコントローラ 上で同じ SSID 名を使用して複数の WLAN を学習できません。シスコ ワイヤレス コントローラ には、名前は同じで WLAN プロファイル名が異なる複数のエントリを含めることもできますが、Catalyst Center はどの時点においても、一意の名前を持つ WLAN に対するエントリを 1 つだけ持ちます。

  ワイヤレスコントローラ ごとに重複する SSID 名を意図的に持つことも、Catalyst Center を使用して重複する SSID 名を持つ ワイヤレスコントローラ を誤って追加してしまうこともあります。いずれの場合も、ワイヤレスコントローラ ごとに重複する SSID 名を持つことは一部の機能にとって問題になります。

  - **設定の学習**：Catalyst Center は ワイヤレスコントローラ ごとにランダムに選択された 1 つの SSID 名のみ学習し、残りの重複する SSID 名はすべて破棄します。（**設定の学習**は、通常は既存の展開シナリオで使用されます。）
  - **アプリケーションポリシー**：Catalyst Center は、アプリケーションポリシーの展開時に、重複するいずれかの SSID 名にのみポリシーをランダムに適用して、他には適用しません。さらに、ポリシーの復元、CLI プレビュー、EasyQoS ファーストレーン、および PSK オーバーライド機能が失敗するか、予期しない結果が生じることになります。
  - **マルチスケールネットワーク**：マルチスケールネットワークでは、複数のデバイスの複数の重複 SSID 名が原因で問題が発生することがあります。たとえば、1 台のデバイスには非ファブリック SSID として WLAN が設定されていて、2 台目のデバイスには同じ WLAN がファブリック SSID として設定されている場合、**[設定の学習（Learn Config）]** を実行すると、1 つの SSID 名のみ学習されます。その他のデバイスの他の SSID 名は破棄されます。この動作により、特に、2 台目のデバイスがファブリック SSID 名のみサポートしていて、Catalyst Center が非ファブリック SSID 名を持つデバイスに対して操作しようとする場合に競合が生じることがあります。
  - **IPACL ポリシー**：IPACL ポリシーの展開時に、Catalyst Center は重複する SSID のいずれか 1 つにのみランダムにポリシーを適用します。また、Flex Connect が関係するシナリオも影響を受けます。

- Catalyst Center では、デバイス設定に対するアウト オブ バンド（OOB）の変更は推奨されません。OOB に変更を加えると、Catalyst Center のポリシーとデバイスに設定されているポリシーは一貫性のない状態になります。2 つのポリシーは、Catalyst Center のポリシーをデバイスに再度展開するまで一貫性のない状態のままになります。
- QoS trust 機能は変更できません。
- 設計から SSID を削除して ワイヤレスコントローラ を再プロビジョニングする前に、対応するワイヤレス アプリケーション ポリシーを必ず削除してください。
- Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のワイヤレスアプリケーションは、学習された設定からプロビジョニングされた SSID ではサポートされません。

- Catalyst Center は、Cisco Catalyst IE 3300 高耐久性シリーズ スイッチおよび Cisco Catalyst IE 3400 Heavy Duty シリーズ スイッチに対する ACL ベースのアプリケーションポリシーのサポートを提供します。最大 8 つのポートベースのカスタムアプリケーションを展開できます。ただし、DSCP ベースのアプリケーションには制限はありません。
- ワイヤレスの場合、一度に 1 つの SSID のみを選択して、QoS ポリシーを展開できます。複数の SSID で QoS を展開する場合は、SSID にポリシーを順番に展開します。
- ワイヤレスの場合、Catalyst Center はマーキングポリシーのみをプッシュします。
- ワイヤレスでアプリケーションポリシーを使用する前に、ワイヤレスコントローラ と AP が Catalyst Center を使用してプロビジョニングされていることを確認してください。

（注） Catalyst Center では、AireOS および Catalyst 9800 シリーズ ワイヤレス コントローラ プラットフォームの FlexConnect ローカルスイッチングモードはサポートされていません。

アプリケーションポリシーの管理

以降のセクションでは、アプリケーションポリシーの管理方法に関する情報を提供します。

前提条件

アプリケーションポリシーを設定する場合は、次の要件に対応する必要があります。

- Catalyst Center は、ほとんどの Cisco LAN、WAN、WLAN デバイスをサポートしています。お使いのネットワークでデバイスおよびソフトウェアバージョンがサポートされているかどうかを確認するには、*Cisco Catalyst Center Compatibility Matrix*を参照してください。
- ISR-G2、ASR 1000、ワイヤレスコントローラなど、シスコのネットワーク デバイスに Application Visibility and Control（AVC）機能ライセンスがインストールされていることを確認します。詳細については、「*NBAR2 (Next Generation NBAR) Protocol Pack FAQ*」を参照してください。
- AVC サポートは、スイッチで自動 QoS が設定されていない場合にのみ、Cisco IOS-XE 16.9 を実行しているスイッチで使用できます。AVC サポートを利用するには、自動 QoS のスイッチを Cisco IOS-XE 16.11 以降にアップグレードする必要があります。
- ポリシーが必要な WAN インターフェイスを Catalyst Center で特定するには、インターフェイス タイプ（WAN）および（必要に応じて）副回線レートとサービス プロバイダのサービス クラス モデルを指定する必要があります。詳細については、サービス プロバイダー プロファイルの WAN インターフェイスへの割り当て（1485 ページ）を参照してください。
- ディスカバリプロセス中にデバイスに割り当てられたデバイスロールが、ネットワークに適切であることを確認します。必要に応じて、不適切なデバイスロールを変更します。詳細については、デバイスロールを手動で変更する （215 ページ）を参照してください。

アプリケーションポリシーの作成

ここでは、アプリケーションポリシーの作成方法について説明します。

始める前に

- ビジネス目標を定義します。例えば、ネットワーク応答時間を最短化させたり、非ビジネスアプリケーションを特定して優先度を下げたりすることで、ユーザの生産性を向上させるようなものです。これらの目標に基づいて、どのビジネスとの関連性カテゴリがアプリケーションに分類されるかを決定します。
- インベントリにデバイスがあることを確認します。デバイスがない場合は、ディスカバリ機能を使用して検出します。
- ディスカバリプロセス中にデバイスに割り当てられたデバイスロールが、ネットワークに適切であることを確認します。必要に応じて、不適切なデバイスロールを変更します。詳細については、デバイスロールを手動で変更する （215 ページ）を参照してください。
- サイトへのデバイスの追加詳細については、「プロビジョニングされていないデバイスのサイトへの割り当て （189 ページ）」を参照してください。
- サービスプロバイダー向けのトラフィックに対してこのポリシーをサービスプロバイダープロファイルで設定する場合は、サービス プロバイダー プロファイルが設定されていることを確認してください。アプリケーションポリシーの作成後にサービス プロバイダープロファイルに戻り、SLA 属性をカスタマイズしてサービス プロバイダー プロファイルを WAN インターフェイスに割り当てます。詳細については、サービス プロバイダ プロファイルの設定 （413 ページ）を参照してください。

手順

ステップ 1 メインメニューから次を選択します。**[Policy]** > **[Application QoS]** > **[Application Policies]** の順に選択します。

ステップ 2 [Add Policy] をクリックします。

ステップ 3 [Application QoS Policy Name] フィールドに、ポリシーの名前を入力します。

ステップ 4 [有線（Wired）] または [ワイヤレス（Wireless）] ラジオ ボタンのいずれかを選択します。

ステップ 5 ワイヤレスネットワークの場合は、[SSID] ドロップダウンリストからプロビジョニングされた SSID を選択します。

ステップ 6 [サイトの範囲（Site Scope）] をクリックします。

ステップ 7 [サイトの範囲の編集（Edit Site Scope）] をクリックし、展開するポリシーの横にあるチェックボックスをオンにします。

（注） 有線デバイスのポリシーでは、別のポリシーに割り当て済みのサイトは選択することができません。ワイヤレス デバイスのポリシーでは、同じ SSID で別のポリシーに割り当て済みのサイトを選択することができません。

プラグアンドプレイでオンボードされた有線デバイスの場合、QoS ポリシーがサイトで設定されていると、その QoS ポリシーはサイトに追加されたデバイスにおいてデフォルトで有効になります。

ステップ 8 有線デバイスのポリシーでは、デバイスまたは特定のインターフェイスがポリシーで設定されないようにすることができます。

a) [Site Scope] ペインで、対象のサイトの横にある省略記号アイコン（ *** ）をクリックします。

選択した範囲内のデバイスのリストが表示されます。

b) 除外するデバイスを見つけ、関連する [ポリシーの除外（Policy Exclusions）] 列にあるトグル ボタンをクリックします。
c) 特定のインターフェイスを除外するには、[Exclude Interfaces] をクリックします。
d) [Applicable Interfaces] のリストから、除外するインターフェイスの横にあるトグルボタンをクリックします。

デフォルトでは、[Applicable Interfaces] のみが表示されます。すべてのインターフェイスを表示するには、[Show] ドロップダウンリストから [All] を選択します。

e) [< Back to Devices in *Site-Name*] をクリックします。
f) [< サイト範囲へ戻る（< Back to Site Scope）] をクリックします。

ステップ 9 WAN デバイスでは、特定のインターフェイスを設定できます。

a) [Site Scope] ペインで、目的のサイトの横にある省略記号アイコン *** をクリックします。
b) サイトのデバイスのリストで、目的のデバイスの横にある [SP Profile Settings] 列の [Configure] をクリックします。

（注） このオプションは、ルータの場合にのみ使用可能です。

c) [WAN インターフェイス（WAN Interface）] 列で、[インターフェイスの選択（Select Interface）] ドロップダウン リストからインターフェイスを選択します。
d) [ロール（Role）] 列で[ロールの選択（Select Role）] ドロップダウン リストから設定するインターフェイスのタイプに従ってロールを選択します。

- 物理インターフェイス：[WAN] を選択します。このロールは、物理インターフェイスに対してのみ有効なロールです。

- トンネルインターフェイス：[DMVPN Branch] または [DMVPN Hub] のいずれかを選択します。[DMVPN ハブ（DMVPN Hub）] を選択した場合、関連するブランチに帯域幅を定義することもできます。



（注） これらのポリシー設定を展開する前に、デバイスにトンネルインターフェイスが作成されていることを確認します。

e) [Service Provider Profile] 列で、[Select Profile] ドロップダウンリストから サービス プロバイダー プロファイルを選択します。

f) （任意） 必要に応じて、[サブ回線のレート（Mbps）（Sub-Line Rate（Mbps））] 列で、インターフェイスに必要なアップストリーム帯域幅を入力します。

g) （任意） 追加の WAN インターフェイスを設定するには、[+] をクリックし、手順 c ～ f を繰り返します。

h) [Save] をクリックします。

i) [< サイト範囲へ戻る（< Back to Site Scope）] をクリックします。

ステップ 10 [サイトの範囲（Site Scope）] ペインで、[OK] をクリックします。

ステップ 11 （任意） Cisco Validated Design（CVD）キューイング プロファイルがニーズを満たしていない場合は、カスタム キューイング プロファイルを作成することができます。

a) [キューイング プロファイル（Queuing Profiles）] をクリックします。

b) 左ペインのリストから、キューイング プロファイルを選択します。

c) [Select] をクリックします。

ステップ 12 （任意） このポリシーがサービスプロバイダー向けトラフィックである場合は、サービス プロバイダー プロファイルの SLA 属性をカスタマイズします。

a) [SP プロファイル（SP Profile）] をクリックします。

b) サービスプロバイダー プロファイルを選択します。

c) SLA 属性をカスタマイズします（[DSCP]、[SP 帯域幅（%）（SP Bandwidth %）]、および [キューイング帯域幅（%）（Queuing Bandwidth %）]）。

ステップ 13 （任意） ネットワークで使用されるアプリケーション セットのビジネスとの関連性を設定します。

Catalyst Center には、ビジネス関連性グループに事前設定されたアプリケーション セットが付属しています。あるビジネス関連性グループから別のグループにアプリケーション セットをドラッグ アンド ドロップして、この設定を維持したり、変更したりすることができます。

お気に入りとしてマークされたアプリケーションは、アプリケーションセットの上部に表示されます。お気に入りを変更するには、[Applications registry] に移動します。

ステップ 14 （任意） コンシューマを作成してアプリケーションに割り当てるか、アプリケーションを双方向としてマークすることにより、アプリケーションをカスタマイズします。

a) アプリケーション グループを展開します。

b) 目的のアプリケーションの横にある歯車アイコン ⚙ をクリックします。

c) [トラフィックの方向（Traffic Direction）] エリアで、[単方向（Unidirectional）] または [双方向（Bi-directional）] ラジオ ボタンを選択します。

d) 既存のコンシューマを選択するには、[コンシューマ（Consumer）] ドロップダウン リストから設定するコンシューマを選択します。新しいコンシューマを作成するには、[+ コンシューマの追加（+ Add Consumer）] をクリックして、[コンシューマ名（Consumer Name）]、[IP/サブネット（IP/Subnet）]、[プロトコル（Protocol）]、および [ポート/範囲（Port/Range）] を定義します。

e) [OK] をクリックします。

ステップ 15 ホスト トラッキングを設定します。[ホスト トラッキング（Host Tracking）] トグル ボタンをクリックして、ホスト トラッキングのオンとオフを切り替えます。

アプリケーションポリシーを展開する際に、Catalyst Center では、コラボレーション エンドポイント（テレプレゼンスユニットやシスコ電話など）が接続されているスイッチに、ACL のエントリを自動的に適用します。

ACE は、コラボレーション エンドポイントによって生成された音声およびビデオトラフィックを照合し、音声およびビデオトラフィックが正しくマークされるようにします。

ホストトラッキングがオンの場合、Catalyst Center はサイトの範囲内でコラボレーション エンドポイントの接続をトラッキングし、コラボレーション エンドポイントがネットワークに接続されるか、1 つのインターフェイスから別のインターフェイスに移動したときに、ACL エントリを自動的に再設定します。

ホストトラッキングが終了すると、Catalyst Center は、コラボレーション エンドポイントが新しいインターフェイスに移動または接続したときに、デバイスにポリシーを自動的に展開しません。代わりに、コラボレーション エンドポイントで正しく設定されるように、ACL のポリシーを再展開する必要があります。

ステップ 16 次のいずれか 1 つのタスクを実行します。

- [ドラフトの保存（Save Draft）] をクリックして、ポリシーをドラフトとして保存します。詳細については、「ポリシーのドラフト （1464 ページ）」を参照してください。
- [展開（Deploy）] をクリックしてポリシーを展開します。

  [Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

  - デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
  - デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

アプリケーションポリシー情報の表示

作成および展開したアプリケーション ポリシーに関するさまざまな情報を表示できます。

始める前に

少なくとも 1 つの展開されたアプリケーション ポリシーがなければなりません。

手順

ステップ 1 メインメニューから次を選択します。**[Policy]** > **[Application QoS]** > **[Application Policies]** の順に選択します。

ステップ 2 ポリシーを名前で並べ替えたり、名前、ステータス、キューイング プロファイルによってフィルタ処理したりします。

ステップ 3 ポリシーのリストと、各ポリシーに関する次の情報が表示されます。

- [Policy Name]：ポリシーの名前。
- [Version]：ポリシーの反復。ポリシーが展開されるか、または、ドラフトとして保存されるたびに、バージョンが 1 ずつ増分されます。たとえば、ポリシーを作成して展開すると、ポリシーはバージョン 1 になります。ポリシーを変更して、再度展開すると、ポリシーのバージョンはバージョン 2 に増分されます。詳細については、ポリシーのドラフト（1464 ページ）およびポリシーのバージョン管理（1466 ページ）を参照してください。
- [Policy Status]：ポリシーの状態。Cisco Catalyst 3850、Catalyst 4500、および Catalyst 9000 デバイスに適用されたポリシーがポートチャネルの更新（作成/変更/削除）によって影響を受ける場合は、アラートがポリシーステータスに表示されます。
- [Deployment Status]：最新の展開の状態（デバイスごと）。次の情報を含む概要を表示します。
  - 正常にプロビジョニングされたデバイス
  - プロビジョニングに失敗したデバイス
  - 展開が終了したためにプロビジョニングされなかったデバイス

  最新の導入の状態をクリックすると、[ポリシーの展開（Policy Deployment）] ウィンドウが表示され、ポリシーが展開されたデバイスのフィルタ処理可能なリストが示されます。各デバイスについて、次の情報が表示されます。
  - デバイスの詳細（名前、サイト、タイプ、ロール、および IP アドレス）
  - 成功した導入のステータス。ステータスの横にある歯車のアイコンをクリックすると、[Effective Marking Policy] ウィンドウが開き、[Business Relevant] および [Business Irrelevant] アプリケーションと、それらが最終的に渡されるトラフィッククラスキューが表示されます。TCAM リソースまたは古い NBAR プロトコルパックに限定されているデバイスの場合は、ポリシーに含まれるアプリケーションのサブセットのみをプロビジョニングでき、それらがビューで表示されます。
  - 障害ステータスには、障害の理由が示されます。
- [Scope]：ポリシーに割り当てられているサイト（デバイスではなく）の数。ワイヤレスデバイスのポリシーの場合は、ポリシーの適用先の SSID の名前が含まれます。

- [LAN Queuing Profile]：ポリシーに割り当てられている LAN キューイングプロファイルの名前。

アプリケーションポリシーの編集

アプリケーション ポリシーを編集できます。

始める前に

少なくとも 1 つのポリシーを作成しておく必要があります。

手順

ステップ 1 メインメニューから次を選択します。**[Policy]** > **[Application QoS]** > **[Application Policies]** の順に選択します。

ステップ 2 編集するポリシーを見つけるには、[フィルタ（Filter）] フィールドを使用します。

ステップ 3 対応するポリシーの横にあるラジオ ボタンをクリックします。

ステップ 4 [Actions] ドロップダウン リストから、[Edit] を選択します。

ステップ 5 必要に応じて、アプリケーション ポリシーを変更します。

ステップ 6 アプリケーションのビジネスとの関連性を変更するには、ビジネス関連、ビジネスと無関係、およびデフォルトグループの間でアプリケーションセットを移動します。

アプリケーションポリシーの設定については、アプリケーションポリシーの作成（1470ページ）を参照してください。

ステップ 7 キューイングプロファイルを更新するには、[Queuing Profiles] をクリックし、左ペインのリストからキューイングプロファイルを選択します。

ステップ 8 [Select] をクリックします。

ステップ 9 次のいずれか 1 つのタスクを実行します。

- [ドラフトの保存（Save Draft）] をクリックして、ポリシーをドラフトとして保存します。詳細については、「ポリシーのドラフト （1464 ページ）」を参照してください。
- [展開（Deploy）] をクリックしてポリシーを展開します。ポリシーを今すぐ展開するか、または後でスケジュールできます。

  ポリシーをすぐに導入するには、[今すぐ実行（Run Now）] ラジオボタンをクリックし、[適用（Apply）] をクリックします。

  将来の日付と時刻でポリシー導入をスケジュールするには、[後でスケジュール（Schedule Later）] ラジオ ボタンをクリックし、導入する日時を定義します。詳細については、ポリシーのスケジューリング （1465 ページ）を参照してください。

（注） アプリケーション ポリシーの展開のスケジュール設定では、サイトのタイム ゾーンの設定はサポートされていません。

アプリケーションポリシーのドラフトの保存

ポリシーを作成、編集、または複製する際、ドラフトとして保存し、後で変更を続けることができます。また、展開したポリシーを変更して、ドラフトとして保存することもできます。

手順

ステップ 1 メインメニューから次を選択します。**[Policy]** > **[Application QoS]** > **[Application Policies]** の順に選択します。

ステップ 2 ポリシーを作成、編集、または複製します。

ステップ 3 [ドラフトの保存（Save Draft）] をクリックします。

詳細については、ポリシーのドラフト （1464 ページ）を参照してください。

アプリケーションポリシーの展開

新しいアプリケーションの追加や、アプリケーションをお気に入りとしてマークするなど、ポリシーの設定に影響する変更を加えた場合は、ポリシーを再展開してこれらの変更を実装する必要があります。

（注） Cisco IOS 16.x 以降を搭載した Cisco Catalyst 3650、Catalyst 3850、および Catalyst 9000 デバイスでは、ポリシーを展開する前に、自動 QoS 設定が自動的に削除されます。

カスタムアプリケーションの作成後、デバイスに関して CBAR が有効になっている場合、そのデバイスでカスタムアプリケーションが自動的に設定されます。デバイスにアプリケーションポリシーを展開する前に、最新のアプリケーションレジストリへの同期の完了を待つ必要があります。**Provision** > **Services** > **Service Catalog** > **Application Visibility** で同期ステータスを確認することができます。

デバイスに関して CBAR が有効になっている場合、カスタムアプリケーションは CBAR を介して設定されるため、アプリケーションポリシーの展開時には属性セットおよびマップだけがデバイスで設定されます。

手順

ステップ 1 メインメニューから次を選択します。**[Policy]** > **[Application QoS]** > **[Application Policies]** の順に選択します。

ステップ 2 導入するポリシーを見つけるには、[フィルタ（Filter）] フィールドを使用します。

ステップ 3 導入するポリシーの横のラジオ ボタンをクリックします。

ステップ 4 [アクション（Actions）] ドロップダウンリストから、[導入（Deploy）] を選択します。

a) ポリシーを再展開すると、ポリシーの範囲から削除されたデバイスに対して適切なアクションを実行するように求められます。次のアクションのいずれかを選択します。

- デバイスからポリシーを削除する（推奨）
- ポリシーの範囲からデバイスを削除する
- ポリシーの範囲からデバイスを削除し、デバイスを既存の設定に復元する

b) [Apply] をクリックします。

ステップ 5 ポリシーを今すぐ展開するか、後で展開するようにスケジュールするかを求められます。次のいずれか 1 つのタスクを実行します。

- ポリシーをすぐに導入するには、[今すぐ実行（RunNow）] ラジオボタンをクリックし、[適用（Apply）] をクリックします。
- 将来の日付と時刻でポリシー導入をスケジュールするには、[後でスケジュール（Schedule Later）] ラジオ ボタンをクリックし、導入する日時を定義します。

（注） アプリケーション ポリシーの展開のスケジュール設定では、サイトのタイム ゾーンの設定はサポートされていません。

ポリシー展開のキャンセル

[導入（Deploy）] をクリックすると、Catalyst Center は、サイト範囲内のデバイスに関するポリシーの設定を開始します。間違いが見つかった場合は、ポリシーの展開をキャンセルできます。

ポリシー設定プロセスはバッチ処理として実行され、一度に 40 台のデバイスが設定されます。デバイスが 40 台以下の場合にポリシーの展開をキャンセルしても、デバイスの最初のバッチへの展開がすでに行われているため、デバイスが設定されている可能性があります。ただし、何百台ものデバイスがある場合は、必要に応じてポリシーの展開をキャンセルできます。

[中止（Abort）] をクリックすると、Catalyst Center によって設定がまだ開始されていないデバイスの設定プロセスがキャンセルされ、デバイスのステータスが [ポリシーの中止（Policy Aborted）] に変更されます。Catalyst Center では、完了している、または完了する予定の処理での導入はキャンセルされません。これらのデバイスでは、更新されたポリシー設定が維持され、ポリシー設定の状態（設定中、成功、または失敗）が反映されます。

ポリシー導入中に [中止（Abort）] をクリックしてポリシー設定プロセスをキャンセルします。

アプリケーション ポリシーの削除

不要になったアプリケーション ポリシーを削除できます。

ポリシーを削除すると、クラスマップ、ポリシーマップ、およびポリシーマップとワイヤレス ポリシー プロファイルの関連付けが削除されます。

手順

ステップ 1 メインメニューから次を選択します。**[Policy]** > **[Application QoS]** > **[Application Policies]** の順に選択します。

ステップ 2 削除するポリシーを見つけるには、[フィルタ（Filter）] フィールドを使用します。

ステップ 3 削除するポリシーの横にあるラジオ ボタンを選択します。

ステップ 4 [Actions] ドロップダウンリストから、[Undeploy Policy] を選択します。

ステップ 5 [Undeploy Policy] ウィンドウで、[Delete policy from devices] オプションボタンをクリックし、[Apply] をクリックします。

ステップ 6 削除を確定する場合は、[OK] をクリックします。それ以外の場合は、[Cancel] をクリックします。

ステップ 7 削除を確認するメッセージが表示されたら、[OK] を再度クリックします。

[アプリケーションQoSポリシー（Application QoS Policies）] ページで、ポリシーの削除ステータスを確認できます。ステータスに [削除失敗（deletion failed）] が表示された場合は、次の手順を実行します。

a) [Application QoS Policies] ウィンドウの [Deployment Status] の下にある失敗状態リンクをクリックします。

b) [Undeployment Status] ウィンドウで、[Retry] をクリックしてポリシーを削除します。

アプリケーションポリシーの複製

既存のアプリケーションポリシーに、新しいポリシーで必要な設定のほとんどが含まれている場合は、既存のポリシーの複製し、変更してから異なる範囲に展開することで時間を節約できます。

始める前に

少なくとも 1 つのポリシーを作成しておく必要があります。

手順

ステップ 1 メインメニューから次を選択します。**[Policy]** > **[Application QoS]** > **[Application Policies]** の順に選択します。

ステップ 2 複製するポリシーを見つけるには、[フィルタ（Filter）] フィールドを使用します。

ステップ 3 複製するポリシーの横にあるラジオ ボタンを選択します。

ステップ 4 [アクション（Actions）] ドロップダウンリストから、[複製（Clone）] を選択します。

ステップ 5 必要に応じてアプリケーション ポリシーを設定します。アプリケーション ポリシーの設定については、アプリケーションポリシーの作成 （1470 ページ）を参照してください。

ステップ 6 次のいずれか 1 つのタスクを実行します。

- [ドラフトの保存（Save Draft）] をクリックして、ポリシーをドラフトとして保存します。詳細については、「ポリシーのドラフト （1464 ページ）」を参照してください。
- [展開（Deploy）] をクリックしてポリシーを展開します。ポリシーを今すぐ展開するか、または後でスケジュールできます。

  ポリシーをすぐに導入するには、[今すぐ実行（Run Now）] ラジオボタンをクリックし、[適用（Apply）] をクリックします。

  将来の日付と時刻でポリシー展開をスケジュールするには、**[後でスケジュール（Schedule Later）]** ラジオ ボタンをクリックし、展開する日時を定義します。詳細については、ポリシーのスケジューリング （1465 ページ）を参照してください。

（注） アプリケーション ポリシーの展開のスケジュール設定では、サイトのタイム ゾーンの設定はサポートされていません。

アプリケーションポリシーの復元

ポリシーを作成または変更してから、最初からやり直すことを決定した場合、Catalyst Center を使ってこれを設定する前に、デバイスにあった元の QoS 設定を復元することができます。

手順

ステップ 1 メインメニューから次を選択します。**[Policy]** > **[Application QoS]** > **[Application Policies]** の順に選択します。

ステップ 2 リセットするポリシーを見つけるには、[フィルタ（Filter）] フィールドを使用します。

ステップ 3 ポリシーの横にあるラジオ ボタンをクリックします。

ステップ 4 [Actions] ドロップダウンリストから、[Undeploy Policy] を選択します。

ステップ 5 [Undeploy Policy] ウィンドウで、[Restore devices to original configurations] オプションボタンをクリックし、[Apply] をクリックします。

ステップ 6 [OK] をクリックして変更を確定するか、[Cancel] をクリックして変更をキャンセルします。

[Application QoS Policies] ウィンドウで、ポリシーの復元ステータスを確認できます。ステータスに [復元に失敗（restoration failed）] と表示された場合は、次の手順を実行します。

a) [Application QoS Policies] ウィンドウの [Deployment Status] の下にある失敗状態リンクをクリックします。

b) [Undeployment Status] ウィンドウで、[Retry] をクリックしてポリシーを復元します。

デフォルトの CVD アプリケーションポリシーのリセット

CVD 設定は、アプリケーションのデフォルト設定です。ポリシーの作成または変更を行った後で最初からやり直す必要が生じた場合は、アプリケーションを CVD 設定にリセットすることができます。CVD設定の詳細については、アプリケーションポリシーの概要（1453 ページ）を参照してください。

手順

ステップ 1 メインメニューから次を選択します。**[Policy]** > **[Application QoS]** > **[Application Policies]** の順に選択します。

ステップ 2 リセットするポリシーを見つけるには、[フィルタ（Filter）] フィールドを使用します。

ステップ 3 ポリシーの横にあるラジオ ボタンをクリックします。

ステップ 4 [Actions] ドロップダウン リストから、[Edit] を選択します。

ステップ 5 [シスコ検証済みデザインのリセット（Reset to Cisco Validated Design）] をクリックします。

ステップ 6 [OK] をクリックして変更を確定するか、[Cancel] をクリックして変更をキャンセルします。

ステップ 7 次のいずれか 1 つのタスクを実行します。

- ポリシーのドラフトを保存するには、[ドラフトの保存（Save Draft）] をクリックします。
- ポリシーを展開するには、[展開（Deploy）] をクリックします。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する（238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

アプリケーション ポリシー履歴の表示

アプリケーションポリシーのバージョン履歴を表示できます。バージョン履歴には、ポリシーのシリーズ番号（反復）と、バージョンが保存された日付と時刻が含まれています。

手順

ステップ 1 メインメニューから次を選択します。**[Policy]** > **[Application QoS]** > **[Application Policies]** の順に選択します。

ステップ 2 表示したいポリシーの横にあるラジオ ボタンをクリックします。

ステップ 3 [アクション（Actions）] ドロップダウン リストから、[履歴（History）] を選択します。

ステップ 4 **[ポリシー履歴（Policy History）]** ダイアログボックスでは、次のタスクを実行できます。

- 現在のバージョンとバージョンを比較するには、関心のあるバージョンの横にある [差異（Difference）] をクリックします。
- ポリシーの前のバージョンにロールバックするには、ロールバック先となるバージョンの横にある [ロールバック（Rollback）] をクリックします。

以前のポリシーバージョンへのロールバック

ポリシー設定を変更し、その後その設定が不適切だと判明した場合、またはネットワークで目的の効果が得られなかった場合、最大で 5 バージョン前のポリシーに戻すことができます。

始める前に

以前のポリシーバージョンにロールバックするには、少なくとも 2 つのポリシーバージョンを作成しておく必要があります。

手順

ステップ 1 メインメニューから次を選択します。**[Policy]** > **[Application QoS]** > **[Application Policies]** の順に選択します。

ステップ 2 表示したいポリシーの横にあるラジオ ボタンをクリックします。

ステップ 3 [アクション（Actions）] ドロップダウンリストから、[履歴の表示（Show History）] を選択します。

選択したポリシーの以前のバージョンは降順に表示され、最も新しいバージョン（最も大きい番号）が一覧の最上部に表示され、最も古いバージョン（最も小さい番号）が最下部に表示されます。

ステップ 4 （任意） 選択したバージョンと最新バージョンの間の差異を表示するには、[View] 列で [Difference] をクリックします。

ステップ 5 ロールバックする先のポリシー バージョンを決定した場合、そのポリシー バージョンに対して [Rollback] をクリックします。

（注） 選択したサイトの範囲がポリシーバージョン間で変更された場合、ロールバックは選択されている現在（最新）のサイトでは行われません。ポリシーのコンテンツのみがロールバックされます。

ステップ 6 [OK] をクリックして、ロールバック手順を確定します。

ロールバック先のバージョンが最新バージョンになります。

キューイングプロファイルの管理

次のセクションでは、キューイングプロファイルを管理するために実行できるさまざまなタスクについて詳しく説明します。

キューイングプロファイルの作成

Catalyst Center では、デフォルトの CVD キューイング プロファイル（CVD_QUEUING_PROFILE）を提供します。このキューイング プロファイルがニーズを満たしていない場合は、カスタム キューイング プロファイルを作成することができます。

手順

ステップ 1 メインメニューから次を選択します。**[Policy]** > **[Application QoS]** > **[Queuing Profiles]** の順に選択します。

ステップ 2 [Add Profile] をクリックします。

ステップ 3 [Profile Name] フィールドに、プロファイルの名前を入力します。

ステップ 4 スライダを使用して各トラフィック クラスに帯域幅を設定します。プラス記号（+）またはマイナス（-）記号をクリックするか、フィールドに特定の数値を入力します。

数値は、選択したアプリケーション クラスに確保されるインターフェイス帯域幅の合計に対しての割合を示します。帯域幅の合計は 100 なので、1 つのアプリケーション クラスに帯域幅を追加すると、別のアプリケーション クラスから帯域幅が差し引かれます。

開いた錠のアイコンは、そのアプリケーション クラスの帯域幅を編集できることを示します。閉じた錠のアイコンは、編集できないことを示します。

間違えた場合は、[シスコ検証済みデザインのリセット（Reset to Cisco Validated Design）] をクリックして CVD 設定に戻ることができます。

中央のグラフは、各アプリケーション クラスを設定している帯域幅の量の視覚化に役立ちます。

ステップ 5 （高度なユーザー向け）Catalyst Center が各トラフィック クラスで使用する DSCP コード ポイントをカスタマイズするには、[表示（Show）] ドロップダウン リストで、[DSCP値（DSCP Values）] を選択し、フィールドに特定の数値を入力して、各アプリケーション クラスの値を設定します。

サービスプロバイダーのクラウド内で必要な DSCP コードポイントをカスタマイズするには、サービスプロバイダーのプロファイルを設定します。

ステップ 6 [Save] をクリックします。

キューイングプロファイルの編集または削除

手順

ステップ 1 メインメニューから次を選択します。**[Policy]** > **[Application QoS]** > **[Queuing Profiles]** の順に選択します。

ステップ 2 [キューイング プロファイル（Queuing Profile）] ペインで、編集または削除するキューイング プロファイルの横にあるラジオ ボタンをクリックします。

ステップ 3 次のいずれか 1 つのタスクを実行します。

- プロファイルを編集するには、プロファイル名を除くフィールドの値を変更し、[保存（Save）] をクリックします。フィールドの詳細については、キューイングプロファイルの作成 （1482 ページ）を参照してください。
- プロファイルを削除するには、[削除（Delete）] をクリックします。

  アプリケーション ポリシーによって参照されている場合は、キューイング プロファイルを削除できません。

WANインターフェイスのアプリケーションポリシーの管理

これらのセクションでは、WAN インターフェイスのアプリケーション プロファイルを管理するために実行できるさまざまなタスクについて詳しく説明します。

サービス プロバイダー プロファイルの SLA 属性のカスタマイズ

自身のクラスモデルによってサービス プロバイダー プロファイルに割り当てられたデフォルトの SLA 属性を使用しない場合は、要件に合わせてサービス プロバイダー プロファイルの SLA 属性をカスタマイズできます。サービス プロバイダー プロファイルのデフォルトの SLA

属性の詳細については、「サービスプロバイダーのプロファイル（1458ページ）」を参照してください。

始める前に

インベントリにデバイスがあることを確認します。デバイスがない場合は、ディスカバリ機能を使用して検出します。

手順

ステップ 1 メインメニューから次を選択します。**[Policy]** > **[Application QoS]** > **[Application Policies]** の順に選択します。

ステップ 2 変更するポリシーを見つけるには、[フィルタ（Filter）] フィールドを使用します。

ステップ 3 ポリシーの横にあるラジオ ボタンを選択します。

ステップ 4 [Actions] ドロップダウン リストから、[Edit] を選択します。

ステップ 5 [SP Profiles] をクリックして、サービス プロバイダー プロファイルを選択します。

ステップ 6 次のフィールドの情報を変更できます。

- [DSCP]：Differentiated Services Code Point（DSCP）値。有効値は 0 ～ 63 です。
  - Expedited Forwarding（EF）
  - クラスセレクタ（CS）：CS1、CS2、CS3、CS4、CS5、CS6
  - 相対的優先転送：AF11、AF21、AF41
  - [Default Forwarding (DF)]

  これらのDSCP値の詳細については、マーキング、キューイング、ドロッピングの処理（1456ページ）を参照してください。
- [SP Bandwidth %]：特定のサービスクラスに割り当てられた帯域幅の割合。
- [Queuing Bandwidth %]：各トラフィッククラスに割り当てられた帯域幅の割合。次のいずれかの変更を加えられます。
  - キューイング帯域幅をカスタマイズするには、鍵アイコンをクリックして、帯域幅の設定をアンロックし、帯域幅の割合を調整します。
  - サービスプロバイダー帯域幅からキューイング帯域幅を自動的に計算するには、ロックアイコンをクリックしてキューイング帯域幅の設定をロックし、[OK] をクリックして確認します。デフォルトでは、Catalyst Centerは、サービスプロバイダークラスのすべてのトラフィッククラスのキューイング帯域幅の合計がそのクラスのサービスプロバイダー帯域幅の割合と一致するように、キューイング帯域幅の割合を自動的に分配します。

ステップ 7 [OK] をクリックします。

サービス プロバイダー プロファイルの WAN インターフェイスへの割り当て

アプリケーションポリシーをすでに作成していて、サービス プロバイダー プロファイルを WAN インターフェイスに割り当てる場合は、ポリシーを編集してこの設定を実行し、必要に応じてインターフェイスにサブラインレートの設定を含めます。

始める前に

ポリシーを作成していない場合は、ポリシーを作成し、同時にサービスプロバイダープロファイルを WAN インターフェイスに割り当てます。詳細については、「アプリケーションポリシーの作成 （1470 ページ）」を参照してください。

手順

ステップ 1 メインメニューから次を選択します。**[Policy]** > **[Application QoS]** > **[Application Policies]** の順に選択します。

ステップ 2 編集するポリシーを見つけるには、[フィルタ（Filter）] フィールドを使用します。

ステップ 3 ポリシーの横にあるラジオ ボタンをクリックします。

ステップ 4 [Actions] ドロップダウン リストから、[Edit] を選択します。

ステップ 5 [Site Scope] ペインで、対象のサイトの横にある歯車アイコンをクリックします。

ステップ 6 対象のデバイスの [SPプロファイル設定（SP Profile Settings）] 列にある [設定（Configure）] をクリックします。

ステップ 7 [WAN インターフェイス（WAN Interface）] 列で、[インターフェイスの選択（Select Interface）] ドロップダウン リストからインターフェイスを選択します。

ステップ 8 [ロール（Role）] 列で[ロールの選択（Select Role）] ドロップダウン リストから設定するインターフェイスのタイプに従ってロールを選択します。

- **物理インターフェイス**：[WAN] を選択します。このロールは、物理インターフェイスに対してのみ有効なロールです。
- **トンネルインターフェイス**：[DMVPN Branch] または [DMVPN Hub] のいずれかを選択します。[DMVPN ハブ（DMVPN Hub）] を選択した場合、関連するブランチに帯域幅を定義することもできます。

（注） これらのポリシー設定を展開する前に、デバイスにトンネル インターフェイスが作成されていることを確認します。

ステップ 9 [Service Provider Profile] 列で、[Select Profile] ドロップダウンフィールドをクリックし、サービス プロバイダー プロファイルを選択します。

ステップ 10 必要に応じて、[サブ回線のレート（Mbps）（Sub-Line Rate（Mbps））] 列で、インターフェイスに必要なアップストリーム帯域幅を入力します。

ステップ 11 追加の WAN インターフェイスを設定するには [+] をクリックし、ステップ 7 ～ 10 を繰り返します。

ステップ 12 [Save] をクリックします。

ステップ 13 [< サイト範囲へ戻る（< Back to Site Scope）] をクリックします。

ステップ 14 [OK] をクリックします。

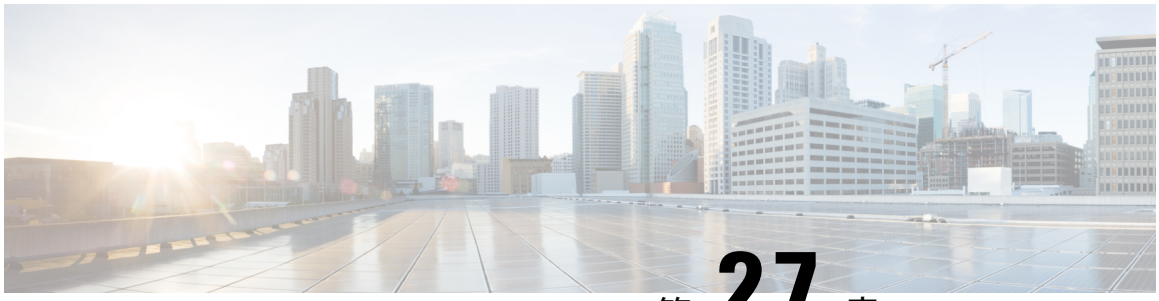
ステップ 15 [Deploy] をクリックします。

ポリシーを今すぐ導入するか、または後でスケジュールするかどうかを求められます。

ステップ 16 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。



第 27 章

トラフィックコピーポリシーの設定

- トラフィックコピーポリシー （1487 ページ）
- 送信元、宛先、トラフィックのコピー先 （1488 ページ）
- トラフィックコピーポリシーのガイドラインと制限事項 （1489 ページ）
- トラフィックコピーポリシーの設定のワークフロー （1489 ページ）
- トラフィックのコピー先の作成 （1490 ページ）
- トラフィックのコピー先の編集または削除 （1490 ページ）
- トラフィックコピー契約の作成 （1491 ページ）
- トラフィックコピー契約の編集または削除 （1491 ページ）
- トラフィックコピーポリシーの作成 （1492 ページ）
- トラフィックコピーポリシーの編集または削除 （1492 ページ）

トラフィックコピーポリシー

Catalyst Center を使用して、2 つのエンティティ間の IP トラフィック フローがモニターリングまたはトラブルシューティングのために指定された宛先にコピーされるように Encapsulated Remote Switched Port Analyzer（ERSPAN）を設定できます。

Catalyst Center を使用して ERSPAN を設定するには、コピーするトラフィック フローの送信元と宛先を定義するトラフィック コピー ポリシーを作成します。トラフィックのコピーを送信するデバイスおよびインターフェイスを指定するトラフィック コピー契約も定義できます。

（注） トラフィックコピーポリシーにはセキュリティグループまたは IP ネットワークグループのいずれかを含めることができるため、このガイド全体を通して、他に指定がなければ「グループ」という用語はセキュリティグループおよび IP ネットワークグループの両方に対して使用します。

送信元、宛先、トラフィックのコピー先

Catalyst Center トラフィックのモニターリングプロセスを簡素化します。物理ネットワーク トポロジを知っている必要はありません。必要なのは、トラフィック フローの送信元および宛先とコピーされたトラフィックの宛先となるトラフィック コピーの宛先を定義することだけです。

- [送信元（Source）]：モニターするトラフィックが通過する 1 つまたは複数のネットワーク デバイス インターフェイス。このインターフェイスは、エンドポイント デバイス、これらのデバイスの特定ユーザー、またはアプリケーションに接続することがあります。送信元グループを構成できるのは、イーサネット、ファストイーサネット、ギガビットイーサネット、10 ギガビット イーサネット、またはポート チャネル インターフェイスのみです。
- [宛先（Destination）]：モニターするトラフィックが流れる IP サブネットです。IP サブネットはサーバー、リモート ピア、またはアプリケーションに接続することがあります。
- [トラフィックコピーの宛先（Traffic Copy Destination）]：ERSPAN データを受信、処理、および分析するデバイス上にあるレイヤ 2 またはレイヤ 3 の LAN インターフェイス。このデバイスは、通常、分析用にトラフィックのコピーを受信するパケットキャプチャ ツールまたはネットワーク分析ツールになります。

（注） 宛先では、スイッチ プローブ デバイスなどのネットワーク アナライザやその他のリモートモニターリング（RMON）プローブを使用してトラフィック分析を実行することを推奨します。

使用可能なインターフェイス タイプは、イーサネット、ファストイーサネット、ギガビット イーサネット、または 10 ギガビット イーサネットのみです。宛先として設定されると、そのインターフェイスはコピーされたトラフィックのみを受信するために使用されます。このインターフェイスは今後その他のタイプのトラフィックを受信できなくなり、トラフィック コピー機能が必要とする以外のトラフィックを転送できません。トランク インターフェイスを宛先として設定できます。この設定により、インターフェイスはカプセル化されたトラフィックを送信できるようになります。

（注） 1 つのトラフィック コピー契約で使用できるトラフィック コピーの宛先は 1 つのみです。

Catalyst Center は、次のデバイスのトラフィックコピーポリシーをサポートしています。

- 送信元：Cisco Catalyst 3000、Catalyst 4000、Catalyst 9000
- 宛先：Cisco Nexus 7000、ASR 1000、Catalyst 6000、ISR 4000

トラフィックコピーポリシーのガイドラインと制限事項

トラフィックコピーポリシー機能には、次の制限事項があります。

- 最大 8 つのトラフィック コピー ポリシー、16 のコピー契約、および 16 のコピーの宛先を作成できます。
- 同じインターフェイスを複数のトラフィック コピーの宛先に使用することはできません。
- Catalyst Center は、トラフィック コピー ポリシーが変更され、ネットワークに展開されているポリシーとの整合性が失われていることを示すステータス メッセージを表示しません。ただし、トラフィック コピー ポリシーが展開された後に変更されたことが分かった場合は、そのポリシーを展開しなおすことができます。
- 管理インターフェイスを送信元グループまたはトラフィック コピーの宛先として設定することはできません。

トラフィックコピーポリシーの設定のワークフロー

始める前に

- モニター対象にするには、トラフィックコピーポリシーで使用されている送信元セキュリティグループが、スイッチとそれらのインターフェイスに静的にマッピングされている必要があります。

  セキュリティグループの作成と送信元ポートへのセキュリティグループの割り当ての詳細については、セキュリティグループの作成（1416ページ）およびファブリックサイト内のポートの設定 （1252 ページ）を参照してください。
- トラフィック コピー ポリシー宛先グループは、IP ネットワーク グループとして設定されている必要があります。詳細については、「IP ネットワーク グループの作成 （1446 ページ）」を参照してください。

手順

ステップ 1 トラフィック コピーの宛先を作成します。

これは、さらに分析するためにトラフィック フローがコピーされる、デバイス上のインターフェイスです。詳細については、トラフィックのコピー先の作成 （1490 ページ）を参照してください。

ステップ 2 トラフィック コピーの契約を作成します。

契約はコピーの宛先を定義します。詳細については、トラフィックコピー契約の作成 （1491 ページ）を参照してください。

ステップ 3 トラフィック コピー ポリシーを作成します。

ポリシーは、トラフィック フローの送信元と宛先、およびコピーされたトラフィックが送信される宛先を指定するトラフィック コピーの契約を定義します。詳細については、トラフィックコピーポリシーの作成（1492 ページ）を参照してください。

トラフィックのコピー先の作成

手順

ステップ 1 メインメニューから次を選択します。、**[ポリシー（Policy）]** > **[トラフィックコピー（Traffic Copy）]** > **[トラフィックコピー（Traffic Copy）]** > **[トラフィックコピーの宛先（Traffic Copy Destination）]** の順に選択します。

ステップ 2 トラフィック コピーの宛先の名前と説明を入力します。

ステップ 3 デバイスと 1 つまたは複数のポートを選択します。

ステップ 4 [Save] をクリックします。

トラフィックのコピー先の編集または削除

手順

ステップ 1 メインメニューから次を選択します。、**[ポリシー（Policy）]** > **[トラフィックコピー（Traffic Copy）]** > **[トラフィックコピーの宛先（Traffic Copy Destination）]**の順に選択します。

ステップ 2 編集または削除する宛先の横にあるチェックボックスをオンにします。

ステップ 3 次のいずれか 1 つのタスクを実行します。

- 変更を行うには、**[編集（Edit）]** をクリックして必要な変更を行い、**[保存（Save）]** をクリックします。
- 宛先を削除するには、**[削除（Delete）]** をクリックします。

トラフィックコピー契約の作成

手順

ステップ 1 メインメニューから次を選択します。、**[ポリシー（Policy）]** > **[トラフィックコピー（Traffic Copy）]** > **[トラフィックコピーの契約（Traffic Copy Contract）]**の順に選択します。

ステップ 2 [Add]をクリックします。

ステップ 3 ダイアログボックスに、契約の名前と説明を入力します。

ステップ 4 **[コピー先（Copy Destination）]** ドロップダウン リストから、コピー先を選択します。

（注） コピー先は、1 つのトラフィック コピー契約に対し 1 つだけ指定できます。

選択可能なコピー先がない場合は、1 つ作成できます。詳細については、トラフィックのコピー先の作成（1490 ページ）を参照してください。

ステップ 5 [Save] をクリックします。

トラフィックコピー契約の編集または削除

手順

ステップ 1 メインメニューから次を選択します。、**[ポリシー（Policy）]** > **[トラフィックコピー（Traffic Copy）]** > **[トラフィックコピーの契約（Traffic Copy Contract）]**の順に選択します。

ステップ 2 編集または削除する契約の横にあるチェックボックスをオンにします。

ステップ 3 次のいずれかの手順を実行します。

- 変更を行うには、**[編集（Edit）]** をクリックして必要な変更を行い、**[保存（Save）]** をクリックします。
- 契約を削除するには、[削除（Delete）] をクリックします。

トラフィックコピーポリシーの作成

手順

ステップ 1 メインメニューから次を選択します。**[ポリシー（Policy）]** > **[トラフィックコピー（Traffic Copy）]** > **[トラフィックコピーポリシー（Traffic Copy Policies）]** の順に選択します。

ステップ 2 [Add Policy] をクリックします。

ステップ 3 [ポリシー名（Policy Name）] フィールドに名前を入力します。

ステップ 4 [説明（Description）] フィールドにポリシーを表す単語またはフレーズを入力します。

ステップ 5 [契約（Contract）] フィールドで、[契約の追加（Add Contract）] をクリックします。

ステップ 6 使用する契約の隣にあるラジオ ボタンをクリックし、次に [保存（Save）] をクリックします。

ステップ 7 [使用可能なグループ（Available Groups）] エリアから、[送信元（Source）]エリアにグループをドラッグ アンド ドロップします。

ステップ 8 [使用可能なグループ（Available Groups）]エリアから、[宛先（Destination）]エリアにグループをドラッグ アンド ドロップします。

ステップ 9 [Save] をクリックします。

トラフィックコピーポリシーの編集または削除

手順

ステップ 1 メインメニューから次を選択します。 **[ポリシー（Policy）]** > **[トラフィックコピー（Traffic Copy）]** > **[トラフィックコピーポリシー（Traffic Copy Policies）]** の順に選択します。

ステップ 2 編集または削除したいポリシーの横のチェック ボックスをオンにします。

ステップ 3 次のいずれか 1 つのタスクを実行します。

- 変更を行うには、**[編集（Edit）]** をクリックして必要な変更を行い、**[保存（Save）]** をクリックします。
- ポリシーを削除するには、**[削除（Delete）]** をクリックします。



第 28 章

ルールベースのコンプライアンスポリシーの設定

- ルールベースのコンプライアンスポリシー （1493 ページ）
- ルールベースのコンプライアンスポリシーの作成 （1494 ページ）
- Cisco Prime Infrastructure からコンプライアンスポリシーを XML としてエクスポートして Catalyst Center にインポートする （1506 ページ）
- Catalyst Centerからルールベースのコンプライアンスポリシーをエクスポートし、別の Catalyst Center にインポートします。 （1507 ページ）

ルールベースのコンプライアンスポリシー

ルールベースのコンプライアンスでは、Catalyst Center がネットワーク全体で定期的に評価して違反を検出するカスタム設定ルールおよびポリシーを作成できます。プラットフォーム固有のコンプライアンス ポリシー ルールでは、文字列の比較、正規表現、式の評価を使用することが可能です。これらは、設定、CLI show コマンド、デバイスプロパティに適用されます。各ルールには、変数、複数の条件、設定可能な違反メッセージとともに違反のシビラティレベルを含めることができます。

たとえば、次のようなポリシーを設定できます。

- ACL ロギングがオフであることを確認する。
- ネットワークで Telnet が無効になっていることを確認する。
- ログイン認証で外部 AAA サーバーが使用されていることを確認する。
- RADIUS サーバーの最小数を設定する。
- DHCP リース時間を特定の日数で設定する。
- コンソール接続が許可されていることを確認する。
- 失敗したログイン試行のトラッキングを有効にする。
- パスワードポリシーを確認する。

スケールの考慮事項

ルールベースのコンプライアンスでは、ポリシー、ルール、条件を柔軟に定義できる必要があります。ただし、過負荷を防ぐための制限も必要です。

これらの制限は、システムレベルとデバイスごとのレベルの両方で推奨されます。

カテゴリ（**Category**）	システム制限	個別の制限
ポリシー	500	
ルール	5000	1 ポリシー：最大 20 個のルール
変数	12,500（ルールの 50% で変数を使用（ルールあたり平均 5 個））	1 ルール：最大 10 個の変数
条件	25,000（ルールあたり平均 5 個）	1 ルール：最大 10 個の条件

ルールベースのコンプライアンスポリシーの作成

ルールベースのコンプライアンスポリシーを作成するには、次の手順を実行します。

手順

ステップ 1 メインメニューから次を選択します。、**[ポリシー（Policy）]**>**[ルールベースのコンプライアンスポリシー（Rule-Based Compliance Policies）]** の順に選択します。

ステップ 2 [Create Policy] をクリックします。

1. [コンプライアンスポリシーの作成（Create compliance policy）] スライドインペインで、[ポリシー名（Policy Name）] フィールドにポリシー名を入力します。
2. [説明（Description）] フィールドに任意の説明を入力します。
3. [Save] をクリックします。

ルールベースのコンプライアンス ポリシー ルールの作成

ルールベースのコンプライアンスポリシーの新しいルールを作成するには、次の手順を実行します。

手順

ステップ 1 メインメニューから次を選択します。**[ポリシー（Policy）]** > **[ルールベースのコンプライアンスポリシー（Rule-Based Compliance Policies）]** の順に選択します。

ステップ 2 [ルールベースのコンプライアンスポリシー（Rule -Based Compliance Policies）] テーブルで、ポリシー名をクリックしてポリシーダッシュボードを開きます。

ステップ 3 （任意）[ルール（Rule）] ペインで、[ルールの追加（Add rule）] をクリックして新しいルールを追加し、次の設定を完了します。

a) [ルール名（Rule Name）] フィールドに、ルールの名前を入力します。

b) [説明（Description）] フィールドに、ルールの説明を入力します。

c) （オプション）[影響と推奨される修正の追加（Add impact and suggested fix）] を展開し、次の値を設定します。

- [影響（Impact）] - ルールが生成する違反の影響に関する簡単なメモを入力します。
- [推奨される修正（Suggested fix）] - ルールが生成する違反の推奨される修正に関するメモを入力します。

（注） ルールは、選択した条件に一致するデバイスでのみ実行されます。デバイスファミリまたはデバイスシリーズのみを選択した場合、ルールはデバイスファミリまたはデバイスシリーズのすべてのデバイスに適用されます。

ステップ 4 [ソフトウェアタイプ（Software type）] ドロップダウンリストから、ソフトウェアタイプを [IOX]、[IOS-XE]、または [シスココントローラ（Cisco Controllers）] として選択します。

ステップ 5 [デバイスファミリ（Device family）] ドロップダウンリストから、デバイスファミリを [ルータ（Routers）]、[スイッチとハブ（Switches and Hubs）]、または [ワイヤレスコントローラ（Wireless Controllers）] として選択します。

ステップ 6 [デバイスシリーズ（Device series）] または [デバイスモデル（Device models）] のいずれかのトグルボタンをクリックします。

ステップ 7 ルールを適用するデバイスシリーズまたはデバイスモデルのチェックボックスをオンにします。

ステップ 8 [保存（Save）] をクリックしてルールを作成します。

コンプライアンス ポリシー ルールへの条件の追加

ルールベースのコンプライアンス ポリシー ルールに条件を追加するには、次の手順を実行します。

手順

ステップ 1 メインメニューから次を選択します。 **[ポリシー（Policy）]** > **[ルールベースのコンプライアンスポリシー（Rule-Based Compliance Policies）]** の順に選択します。

ステップ 2 [ルールベースのコンプライアンスポリシー（Rule -Based Compliance Policies）] テーブルで、ポリシー名をクリックしてポリシーダッシュボードを開きます。

ステップ 3 [ルール（Rules）] ペインで、ルールの名前をクリックします。

ステップ 4 [条件（Conditions）] ペインを展開します。[条件を追加（Add Condition）] をクリックします。

ステップ 5 [条件の追加（Add Conditions）] ペインで、ルールに条件を追加します。

a) 基本設定を構成するのか、詳細設定を構成するのかに基づいて条件を設定します。

b) 基本設定を構成する場合は、[条件（Conditions）] ペインを展開します。

c) [範囲（Scope）] ドロップダウンリストから、条件の範囲を選択し、基本設定の次の設定を完了します。

表 *66* : 基本設定

選択内容	結果
設定	[演算子（Operator）] ドロップダウンリストから、選択した範囲に必要な演算子を選択します。 • 文字列を含む • 文字列を含まない • 表現に一致 • 表現に一致しない • 式の評価 [Value] フィールドに値を入力します。 [正規表現のテスト（Test regular expression）] をクリックし、正規表現演算子のテストデータを使用して入力した正規表現の値をテストします。

選択内容	結果
デバイスのコマンド出力	[Showコマンド（Show command）] フィールドで、show コマンドを選択するか、カスタム show コマンドを入力してリストに追加します。 [演算子（Operator）] ドロップダウンリストから、選択した範囲に必要な演算子を選択します。 • 文字列を含む • 文字列を含まない • 表現に一致 • 表現に一致しない • 式の評価 [Value] フィールドに値を入力します。 [正規表現のテスト（Test regular expression）] をクリックし、正規表現演算子のテストデータを使用して入力した正規表現の値をテストします。

[アクション（Actions）] ペインを展開し、基本設定の次の設定を完了します。

選択内容	結果
続行	違反を発生させずに続行します。
違反を発生して続行	条件の範囲に基づいて違反のシビラティを設定します。 • [違反のシビラティ（Violation severity）] ドロップダウンリストから、違反のシビラティを選択します。 • [カスタム違反メッセージ（Custom violation message）] フィールドに、任意のユーザー定義違反メッセージを入力します。

d) 詳細条件を設定する場合は、[条件の追加（Add condition）] ペインで [詳細設定（Advance settings）] を有効にし、設定を解析してアクションを実行するための追加オプションにアクセスします。
e) [条件（Conditions）] ペインを展開します。[範囲（Scope）] ドロップダウンリストから、条件の範囲を選択し、詳細設定の次の設定を完了します。

表 *67 :* 詳細設定

選択内容	結果
設定	

選択内容	結果
	[ブロックとして解析（Parse as Blocks）] チェックボックスをオンにして、実行コンフィギュレーション全体をブロックに分割し、各ブロック内の条件一致基準値を検索します。 [ブロック開始式（Block start expression）] と [ブロック終了式（Block end expression）] を入力します。ブロックは、開始表現と終了表現に基づいて分割されます。 （オプション）[詳細ブロックオプション（Advance block options）] をクリックして、違反オプションを選択します。 • [いずれかのブロックに違反がある場合に違反が発生（Raise violation if ANY block has a violation）]：1 つまたは複数の違反が発生する可能性があります。 • [複数の違反（違反ブロックごとに1つの違反）が発生（Raise multiple violations - one violation per violating block）]：すべてのブロックに対して実行が継続され、多くの違反が発生します。 • [すべての違反ブロックに対して1つの違反が発生（Raise a single violation for all violating blocks）]：違反のあるブロックが検出されると、実行が停止します。 • [すべてのブロックに違反がある場合にのみ違反が発生（Raise violation only if ALL blocks have a violation）]：ルールに対して 1 つの違反のみ発生します。 [演算子（Operator）] ドロップダウンリストから、選択した範囲に必要な演算子を選択します。 • 文字列を含む • 文字列を含まない • 表現に一致 • 表現に一致しない • 式の評価 [値（Value）] フィールドに値を入力します。

選択内容	結果
	[正規表現のテスト（Test regular expression）] をクリックし、正規表現演算子のテストデータを使用して入力した正規表現の値をテストします。
デバイスのコマンド出力	[Showコマンド（Show command）] フィールドで、show コマンドを選択するか、カスタム show コマンドを入力してリストに追加します。 [演算子（Operator）] ドロップダウンリストから、選択した範囲に必要な演算子を選択します。 • 文字列を含む • 文字列を含まない • 表現に一致 • 表現に一致しない • 式の評価 [値（Value）] フィールドに値を入力します。 [正規表現のテスト（Test regular expression）] をクリックし、正規表現演算子のテストデータを使用して入力した正規表現の値をテストします。

[アクション（Actions）] ペインを展開し、次の設定を完了します。

選択内容	結果
[続行（Continue）] としてアクションを照合	違反を発生させずに、次の条件のチェックに進みます（存在する場合）。
不一致時のアクションとして [違反を発生させて続行（Raise a violation and continue）] を選択	違反と違反メッセージのシビラティを設定することによって違反を引き起こします。 • [違反のシビラティ（Violation severity）] ドロップダウンリストから、違反のシビラティを選択します。 • [カスタム違反メッセージ（Custom violation message）] フィールドに、任意のユーザー定義違反メッセージを入力します。

例：ブロック オプション

このコンプライアンスポリシーでは、ある特定のブロック内に定義されている不正または未承認のSNMPコミュニティ文字列があるかどうかを確認します。ブロック内で検出された場合、ポリシーは「承認されていないコミュニティ文字列<1.1>を検出しました（Detected unauthorized community string <1.1>）」というメッセージで違反を報告し、すべての非準拠 SNMP 文字列をブロックから削除します。

ペイン	ペインエリア	フィールド	値
ルール情報（**Rule Information**）		ルールタイトル（Rule Title）	snmp-server community having non-standard entries
プラットフォームの選択（**Platform Selection**）			Cisco IOS デバイス、Cisco IOS-XE デバイス
Condition 1			
[条件の詳細（Condition Details）]	**[条件範囲の詳細（Condition Scope Details）]**	条件の範囲（Condition Scope）	設定（Configuration）
	ブロック オプション（**Block Options**）	ブロック開始表現（Block Start Expression） （このフィールドは、[ブロックとして解析（Parse as Blocks）] チェックボックスがオンになっている場合にのみ有効になります）	^snmp-server community .*
	Condition Match Criteria	演算子	Matches the expression
		値	snmp-server community (.*)
アクションの詳細（**Action Details**）	一致アクションの選択（**Select Match Action**）	アクションの選択（Select Action）	続行（Continue）
	不一致アクションの選択（**Select Does Not Match Action**）	アクションの選択（Select Action）	違反を発生させません（Does Not Raise a Violation）
Condition 2			

ペイン	ペインエリア	フィールド	値
[条件の詳細（Condition Details）]	**[条件範囲の詳細（Condition Scope Details）]**	条件の範囲（Condition Scope）	以前に一致したブロック（Previously Matched Blocks）
	ブロック オプション（Block Options）	ブロック開始表現（Block Start Expression） （このフィールドは、[ブロックとして解析（Parse as Blocks）] チェックボックスがオンになっている場合にのみ有効になります）	^snmp-server community .*
	Condition Match Criteria	演算子	Matches the expression
		値	snmp-server community ((public RO)|(private RW))
アクションの詳細（Action Details）	**一致アクションの選択（Select Match Action）**	アクションの選択（Select Action）	続行（Continue）
	不一致アクションの選択（Select Does Not Match Action）	アクションの選択（Select Action）	違反を発生させます。
		違反メッセージタイプ（Violation Message Type）	ユーザー定義の違反メッセージ
		違反テキスト（Violation Text）	承認されていないコミュニティ文字列 <1.1> を検出しました。（Detected unauthorized community string <1.1>.）

（注） 上記の例では、最初の条件での一致基準は 1.1、1.2 などと呼びます。2 番目の条件での一致基準は 2.1、2.2 などと呼びます。

条件およびアクションの例：NTP サーバーの冗長性

このコンプライアンス ポリシーは、デバイスでコマンド **ntp server** が少なくとも 2 回表示されるかどうかを確認します。表示されない場合、ポリシーは、「少なくとも2つのNTPサーバーを構成する必要があります（At least two NTP servers must be configured）」というメッセージで違反を発生させます。

ペイン	ペインエリア	フィールド	値
[条件の詳細（Condition Details）]	**[条件範囲の詳細（Condition Scope Details）]**	条件の範囲（Condition Scope）	設定（Configuration）
	Condition Match Criteria	演算子	Matches the expression
		値	(ntp server.*\n){2,}
アクションの詳細（Action Details）	**一致アクションの選択（Select Match Action）**	アクションの選択（Select Action）	続行（Continue）
	不一致アクションの選択（Select Does Not Match Action）	アクションの選択（Select Action）	違反を発生させる
		違反メッセージタイプ（Violation Message Type）	ユーザー定義の違反メッセージ
		違反テキスト（Violation Text）	At least two NTP servers must be configured.

ポリシールールへの変数の追加

ルールベースのコンプライアンスポリシー規則に新しい変数を追加するには、次の手順を実行します。

手順

ステップ 1 メインメニューから次を選択します。 **[ポリシー（Policy）]** > **[ルールベースのコンプライアンスポリシー（Rule-Based Compliance Policies）]** の順に選択します。

ステップ 2 [ルールベースのコンプライアンスポリシー（Rule -Based Compliance Policies）] テーブルで、ポリシー名をクリックしてポリシーダッシュボードを開きます。

ステップ 3 [ルール（Rules）] ペインで、ルールの名前をクリックします。

ステップ 4 （任意） [変数（Variables）] ペインを展開します。**[変数の追加（Add Variable）]** をクリックして、ルールに変数を追加します。

a) 変数名、識別子、および説明を対応するフィールドに入力します。
b) [データタイプ（Data type）] ペインを展開し、データタイプを選択します。

選択内容	結果
文字列	**1.** （オプション）[入力必須（Input required）] チェックボックスをオンにして、入力必須条件を定義します。 **2.** （オプション）ルール変数の値のリストを提供するには、[値のリスト（Is list of values）] チェックボックスをオンにします。 **3.** [追加（Add）] をクリックします。次に、対応するフィールドに名前と値を追加します。[Save] をクリックします。 **4.** （オプション）ルール変数の準拠チェック時に複数の値を指定するには、[複数の値を受け入れる（Accept multiple values）] チェックボックスをオンにします。 （オプション）[デフォルト値（Default value）] : デフォルト値を入力します。整数データ型には整数を使用します。 [最大長（Maximum Length）] : 文字列の最大長を入力します。 [有効な正規表現（Valid regex）] : 文字列入力を検証するための有効な正規表現を入力します。
整数	**1.** （オプション）[入力必須（Input required）] チェックボックスをオンにして、入力必須条件を定義します。 **2.** （オプション）ルール変数の値のリストを提供するには、[値のリスト（Is list of values）] チェックボックスをオンにします。 **3.** [追加（Add）] をクリックします。次に、対応するフィールドに名前と値を追加します。[Save] をクリックします。 **4.** （オプション）ルール変数の準拠チェック時に複数の値を指定するには、[複数の値を受け入れる（Accept multiple values）] チェックボックスをオンにします。 （オプション）[デフォルト値（Default value）] : デフォルト値を入力します。整数データ型には整数を使用します。 [最小値（Minimum value）] : 整数の最小値を入力します。 [最大値（Maximum value）] : 整数の最大値を入力します。

選択内容	結果
ブール	**1.** （オプション）[入力必須（Input required）] チェックボックスをオンにして、入力必須条件を定義します。 **2.** （オプション）ルール変数の値のリストを提供するには、[値のリスト（Is list of values）] チェックボックスをオンにします。 **3.** [追加（Add）] をクリックします。次に、対応するフィールドに名前と値を追加します。[Save] をクリックします。 （オプション）[デフォルト値（Default value）] : [true] または [false] を選択します。
IP address	**1.** （オプション）[入力必須（Input required）] チェックボックスをオンにして、入力必須条件を定義します。 **2.** （オプション）ルール変数の準拠チェック時に複数の値を指定するには、[複数の値を受け入れる（Accept multiple values）] チェックボックスをオンにします。 （オプション）[デフォルト値（Default value）] : デフォルト値を入力します。
Interface	**1.** （オプション）[入力必須（Input required）] チェックボックスをオンにして、入力必須条件を定義します。 **2.** （オプション）ルール変数の準拠チェック時に複数の値を指定するには、[複数の値を受け入れる（Accept multiple values）] チェックボックスをオンにします。 （オプション）[デフォルト値（Default value）] : デフォルト値を入力します。
IPマスク	**1.** （オプション）[入力必須（Input required）] チェックボックスをオンにして、入力必須条件を定義します。 **2.** （オプション）ルール変数の値を指定するには、[複数の値を受け入れる（Accept multiple values）] チェックボックスをオンにし、準拠チェック中に複数の値を指定します。 （オプション）[デフォルト値（Default value）] : デフォルト値を入力します。

c) [プレビュー（Preview）] セクションには、設定された変数のプレビューが表示されます。[Save] をクリックします。

サイトへのポリシーの割り当て

次の手順を実行して、ルールベースのコンプライアンスポリシーをサイトに割り当てます。

手順

ステップ 1 メインメニューから次を選択します。 **[ポリシー（Policy）] > [ルールベースのコンプライアンスポリシー（Rule-Based Compliance Policies）]** の順に選択します。

ステップ 2 [ルールベースのコンプライアンスポリシー（Rule -Based Compliance Policies）] テーブルで、ポリシー名をクリックしてポリシーダッシュボードを開きます。

ステップ 3 [サイト（Sites）] ペインで、右上隅にある [サイトへの割り当て（Assign to sites）] をクリックします。

または、ポリシーテーブルから割り当てるには、対応するチェックボックスをオンにして、[サイト（Sites）] 列で [割り当て（Assign）] をクリックします。

ステップ 4 **[サイトへの割り当て（Assign to sites）]** スライドインペインで、サイト階層内のサイトの横にあるチェックボックスをオンにして選択し、[割り当て（Assign）] をクリックします。

ポリシーは、選択したサイトの対象デバイスに適用されます。

Cisco Prime Infrastructure からコンプライアンスポリシーを XML としてエクスポートして Catalyst Center にインポートする

Cisco Prime Infrastructure からコンプライアンスポリシーを XML としてエクスポートし、Catalyst Center にインポートするには、次の手順を実行します。

- 必要に応じて、個別のコンプライアンスポリシーをエクスポートし、別のサーバーにインポートできます。

手順

ステップ 1 Cisco Prime Infrastructure の GUI で、[設定（Configuration）] > [コンプライアンス（Compliance）] > [ポリシー（Policies）] の順に選択します。

ステップ 2 コンプライアンスポリシーをエクスポートするには、次の手順を実行します。

a) [コンプライアンスポリシー（Compliance Policies）] ナビゲーションエリアから、ポリシーの横にある [i] アイコンにカーソルを合わせます。

b) ポップアップウィンドウで、[XMLとしてポリシーをエクスポート（Export Policy as XML）] ハイパーリンクをクリックし、ファイルを保存します。

ステップ 3 コンプライアンスポリシーを Catalyst Center にインポートするには、次の手順を実行します。

a) 左上隅にあるメニューアイコンをクリックし、**[ポリシー（Policy）]>[ルールベースのコンプライアンスポリシー（Rule-Based Compliance Policies）]** の順に選択します。
b) [ポリシーのインポート（Import policies）] をクリックすると、[コンプライアンスポリシーのインポート（Import compliance policy）] スライドインペインが開きます。
c) [コンプライアンスポリシーのインポート（Import compliance policy）] スライドインペインで、XML ファイルをアップロードエリアにドラッグアンドドロップします。または、[ファイルをクリックするかこのエリアにドラッグしてアップロード（Click or drag files to this area to upload）] をクリックし、XML ファイルを見つけて [インポート（Import）] をクリックします。

Catalyst Centerからルールベースのコンプライアンスポリシーをエクスポートし、別の Catalyst Center にインポートします。

この手順を使用して、Catalyst Center からコンプライアンスポリシーをエクスポートし、別の Catalyst Center インスタンスにインポートします。

- 主に Catalyst Center インスタンス間のポリシーのエクスポートに使用される JSON ファイルをインポートできます。
- 個別のコンプライアンスポリシーをインポートし、必要に応じて、それらのポリシーを別のサーバーに転送することができます。
- アクティビティ センター ページには、成功したインポートと失敗したインポートの両方に関する詳細が表示されるため、ポリシーの監視とトラブルシュートが容易になります。

手順

ステップ 1 左上隅にあるメニューアイコンをクリックし、[ポリシー（Policy）]>[ルールベースのコンプライアンスポリシー（Rule-Based Compliance Policies）] の順に選択します。

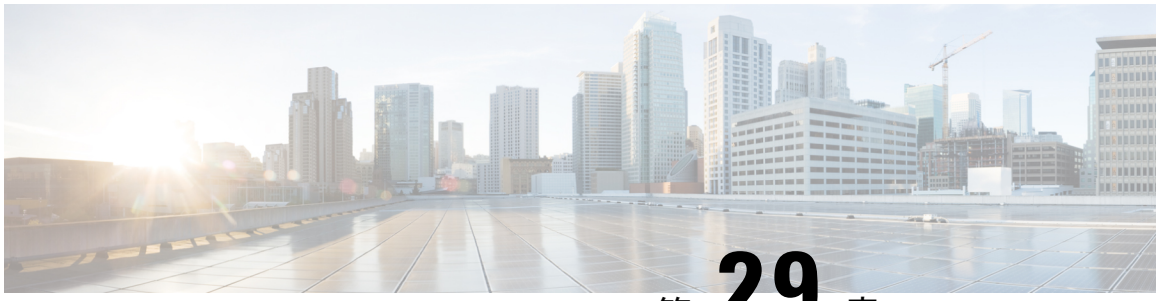
ステップ 2 コンプライアンスポリシーをエクスポートするには、次の手順を実行します。

a) ポリシーテーブルで、目的のポリシーの横にあるチェックボックスをオンにします。
b) [エクスポート（Export）] をクリックします。ZIP ファイルから JSON ファイルを抽出し、ローカルデスクトップに保存します。

ステップ 3 コンプライアンスポリシーを Catalyst Center にインポートするには、次の手順を実行します。

a) [ポリシーのインポート（Import policies）] をクリックすると、[コンプライアンスポリシーのインポート（Import compliance policy）] スライドインペインが開きます。
b) [コンプライアンスポリシーのインポート（Import compliance policy）] スライドインペインで、XML ファイルをアップロードエリアにドラッグアンドドロップします。または、[ファイルをクリックする

かこのエリアにドラッグしてアップロード（Click or drag files to this area to upload）] をクリックし、XML ファイルを見つけて [インポート（Import）] をクリックします。



第 29 章

トラフィック ステアリング ポリシーの設定

- トラフィックス テアリング ポリシーの概要 （1509 ページ）
- トラフィック ステアリング ポリシー （1510 ページ）
- トラフィック ステアリング コントラクト （1515 ページ）

トラフィックス テアリング ポリシーの概要

トラフィック ステアリング ポリシーは、セキュリティサービスの挿入（SSI）のためにネットワーク内のファイアウォールに送信されるトラフィックを決定します。

これらのポリシーには、次のものが含まれます。

- セキュリティグループ（送信元および宛先セキュリティグループ）
- ファイアウォール
- トラフィック ステアリング コントラクト

概要ウィンドウ

トラフィック ステアリング ポリシー の **[概要（Overview）]** ウィンドウには、セキュリティサービスの挿入設定の概要が表示されます。

メインメニューから次を選択します。 **[概要（Overview）]** ウィンドウを表示するには、**[ポリシー（Policy）]** > **[トラフィック ステアリング ポリシー（Traffic Steering Policy）]**を選択します。

次の表に、セキュリティサービスの挿入ステータスに基づいて、このウィンドウのコンポーネントに関する情報を示します。

セキュリティサービスの挿入のステータス	結果
無効	このウィンドウには、セキュリティサービスの挿入を有効にするための [サービスの挿入の有効化（Enable Service Insertion）] オプションが表示されます。 詳細については、サービス挿入サイトの有効化（1389ページ）を参照してください。

enabled	このウィンドウには、次のエリアが表示されます。
	• [概要（Summary）]：次の項目の総数を表示します。
	  • サービス挿入サイト
	  • ポリシー
	  • トラフィック ステアリング コントラクト
	• [設定別の統計（Statistics by configuration）]：次の情報を表示します。
	  • 上位 5 つのファイアウォール IP アドレス
	  • 上位 5 つのトラフィック ステアリング コントラクト
	  • 上位 5 つのノード

トラフィック ステアリング ポリシー

サービス挿入サイトの場合、[トラフィックステアリングポリシー（Traffic steering policies）] タブには、ステアリングポリシーの詳細がマトリックスビューとリストビューで表示されます。

マトリックスビュー

右上隅にある アイコンをクリックすると、マトリックスビューが開きます。マトリックスビューには、すべてのセキュリティグループのポリシーすべてに関する概要が表示されます。

マトリックスビューには、次の 2 つの軸があります。

- 送信元軸：垂直軸にはすべての送信元セキュリティグループがリストされます。
- 宛先軸：水平軸にはすべての宛先セキュリティグループがリストされます。

マトリックスの各セルには、対応する送信元および宛先セキュリティグループに設定されているポリシーのタイプに基づいた色が表示されます。

- トラフィック ステアリング ポリシー

- グループベースポリシー
- トラフィック ステアリング ポリシーとグループベースポリシーの両方
- ポリシーなし
- 適用されないポリシー

アイコンをクリックすると、凡例が表示されます。

トラフィック ステアリング ポリシーが設定されている送信元と宛先のセキュリティグループのペアについては、対応するセルをクリックしてトラフィック ステアリング ポリシーの詳細を表示し、編集できます。トラフィック ステアリング ポリシーが設定されていない送信元と宛先のセキュリティグループのペアについては、対応するセルをクリックしてポリシーを作成できます。

このビューでは、トラフィック ステアリング ポリシーを作成して展開することもできます。

リストビュー

右上隅にある アイコンをクリックすると、リストビューが開きます。リストビューには、使用可能なすべてのトラフィック ステアリング ポリシーのリストが表示されます。

このビューでは、トラフィック ステアリング ポリシーの作成、編集、表示、削除、展開が可能です。

Day 0 におけるトラフィック ステアリング ポリシーの作成

この手順を使用して、デイゼロでトラフィック ステアリング ポリシーを作成します。

手順

ステップ 1 メインメニューから次を選択します。**[ポリシー（Policy）]>[トラフィック ステアリング ポリシー（Traffic Steering Policy）]**の順に選択します。

ステップ 2 [トラフィック ステアリング ポリシー（Traffic steering policies）] タブをクリックします。

ステップ 3 [サービスの挿入の有効化（Enable Service Insertion）] をクリックして、サービスの挿入を有効にし、ワークフローの中でトラフィック ステアリング ポリシーを作成します。

サービスの挿入の有効化については、「サービス挿入サイトの有効化（1389 ページ）」を参照してください。

Day N におけるトラフィック ステアリング ポリシーの作成

次の手順を使用して、Day n にトラフィック ステアリング ポリシーを作成します。

トラフィック ステアリング ポリシーを作成すると、Catalyst Center は対応するミラーポリシーを自動的に作成してトラフィックを反転します。

始める前に

- 前提条件を満たしていることを確認します。詳細については、デイゼロでサービス挿入サイトを有効にするための事前チェック （1388 ページ）を参照してください。
- Catalyst Center におけるセキュリティサービスの挿入の有効化詳細については、サービス挿入サイトの有効化 （1389 ページ）を参照してください。

（注） セキュリティサービスの挿入が有効になっていない場合、Catalyst Centerではトラフィック ステアリング ポリシーを作成できません。

- トラフィック ステアリング コントラクトを作成します。詳細については、トラフィック ステアリング コントラクトの作成 （1515 ページ）を参照してください。
- レイヤ 3 仮想ネットワークを作成します。詳細については、レイヤ 3 仮想ネットワークの作成 （1257 ページ）を参照してください。

手順

ステップ 1 メインメニューから次を選択します。**[ポリシー（Policy）]>[トラフィック ステアリング ポリシー（Traffic Steering Policy）]**の順に選択します。

ステップ 2 [トラフィック ステアリング ポリシー（Traffic steering policies）] タブをクリックします。

ステップ 3 [ファブリックサイト（Fabric site）] ドロップダウンリストからファブリックサイトを選択します。

ステップ 4 [ポリシーの作成（Create Policy）] をクリックします。

ステップ 5 ドロップダウンリストから、 を選択します。

- 送信元セキュリティグループ
- 宛先セキュリティグループ
- トラフィック ステアリング コントラクト

（注） 送信元と宛先のセキュリティグループは異なる必要があります。

ステップ 6 [VNの選択（Select a VN）] ドロップダウンリストから、仮想ネットワークを選択します。

仮想ネットワークを選択すると、Catalyst Center は対応するファイアウォール名を表示します。

ステップ 7 （任意）[+] アイコンをクリックして、別の仮想ネットワークとファイアウォールを追加します。

ステップ 8 [プロビジョニングのスケジュール（Schedule provisioning）] で、スケジュールを選択します。

a) [タスク名（Task Name）] フィールドにプロビジョニングタスクの名前を入力します。

b) [プロビジョニングのスケジュール（Schedule provisioning）] で、ポリシーを Cisco ISE にプッシュするスケジュールを選択します。

クリックする対象	目的
[Now]	設定をすぐに展開します。
後で追加	展開する日付と時刻をスケジュールし、タイムゾーンを定義します。

ステップ 9 [Save] をクリックします。

次のタスク

デバイスにポリシーを展開します。詳細については、トラフィック ステアリング ポリシーの展開 （1515 ページ）を参照してください。

トラフィック ステアリング ポリシーの編集

次の手順を実行して、トラフィック ステアリング ポリシーを編集します。

トラフィック ステアリング ポリシーを編集すると、Catalyst Center は対応するミラーポリシーを自動的に更新します。Catalyst Center はミラーポリシーを使用してトラフィックをリバースします。

手順

ステップ 1 メインメニューから次を選択します。**[ポリシー（Policy）]>[トラフィック ステアリング ポリシー（Traffic Steering Policy）]**の順に選択します。

ステップ 2 [トラフィック ステアリング ポリシー（Traffic steering policies）] タブをクリックします。

ステップ 3 [ファブリックサイト（Fabric site）] ドロップダウンリストからファブリックサイトを選択します。

ステップ 4 リストビュー（☰）で、編集するトラフィック ステアリングポリシーの横にあるチェックボックスをオンにします。

ステップ 5 [Actions] にカーソルを合わせて [Edit] を選択します。

ステップ 6 [ポリシーの編集（Edit policy）] スライドインペイン で、必要な設定を編集します。

詳細については、DayN におけるトラフィック ステアリング ポリシーの作成（1511 ページ）を参照してください。

ステップ 7 [プロビジョニングのスケジュール（Schedule provisioning）] で、スケジュールを選択します。

a) [タスク名（Task Name）] フィールドにプロビジョニングタスクの名前を入力します。
b) [プロビジョニングのスケジュール（Schedule provisioning）] で、ポリシーを Cisco ISE にプッシュするスケジュールを選択します。

クリックする対象	目的
[Now]	設定をすぐに展開します。
後で追加	展開する日付と時刻をスケジュールし、タイムゾーンを定義します。

ステップ 8 [Save] をクリックします。

次のタスク

デバイスにポリシーを展開します。詳細については、トラフィック ステアリング ポリシーの展開 （1515 ページ）を参照してください。

トラフィック ステアリング ポリシーの削除

トラフィック ステアリング ポリシーを削除するには、次の手順を実行します。

トラフィック ステアリング ポリシーを削除すると、Catalyst Center は対応するミラーポリシーを自動的に削除します。

手順

ステップ 1 メインメニューから次を選択します。**[ポリシー（Policy）]>[トラフィック ステアリング ポリシー（Traffic Steering Policy）]**の順に選択します。
ステップ 2 [トラフィック ステアリング ポリシー（Traffic steering policies）] タブをクリックします。
ステップ 3 [ファブリックサイト（Fabric site）] ドロップダウンリストからファブリックサイトを選択します。
ステップ 4 リストビュー （☰）で、削除するトラフィック ステアリング ポリシーの横にあるチェックボックスをオンにします。
ステップ 5 [Actions] にカーソルを合わせて [Delete] を選択します。
ステップ 6 ダイアログボックスで、[削除（Delete）] をクリックします。

次のタスク

デバイスに更新を展開します。詳細については、トラフィック ステアリング ポリシーの展開（1515 ページ）を参照してください。

トラフィック ステアリング ポリシーの展開

トラフィック ステアリング ポリシーを作成、編集、または削除した後、サービス挿入サイトに関連付けられたデバイスにトラフィック ステアリング ポリシーを展開するには、この手順を使用します。

手順

ステップ 1 メインメニューから次を選択します。**[ポリシー（Policy）]**>**[トラフィック ステアリング ポリシー（Traffic Steering Policy）]**の順に選択します。

ステップ 2 [トラフィック ステアリング ポリシー（Traffic steering policies）] タブをクリックします。

ステップ 3 [ファブリックサイト（Fabric site）] ドロップダウンリストからファブリックサイトを選択します。

ステップ 4 [Deploy] をクリックします。

ステップ 5 [展開のスケジュール（Schedule deployment）] スライドインペイン で、展開をスケジュールします。

a) [タスク名（Task Name）] フィールドにタスクの名前を入力します。

b) 展開をスケジュールするために必要なオプションを選択します。

オプション	説明
[Now]	設定をすぐに展開します。
後で追加	日時をスケジュールし、設定を展開するタイムゾーンを定義します。

c) [Deploy] をクリックします。

トラフィック ステアリング コントラクト

トラフィック ステアリング コントラクトは、特定のネットワークトラフィックが次のものと一致する場合、そのトラフィックを送信元セキュリティグループから接続先セキュリティグループにリダイレクトする一連のルールを定義します。

- ネットワーク アプリケーション
- トランスポートプロトコル
- 送信元および宛先ポート

トラフィック ステアリング コントラクトの作成

この手順を使用して、トラフィック ステアリング コントラクトを作成し、トラフィックをリダイレクトします。

Catalyst Center は、グローバルレベルで契約を作成し、どのサイトにも割り当てません。

手順

ステップ 1 メインメニューから次を選択します。**[ポリシー（Policy）]**>**[トラフィック ステアリング ポリシー（Traffic Steering Policy）]**の順に選択します。

ステップ 2 [トラフィック ステアリング コントラクト（Traffic steering contracts）] タブをクリックします。

ステップ 3 [ステアリングコントラクトの作成（Create steering contract）] をクリックします。

ステップ 4 [ステアリングコントラクトの作成（Create a steering contract）] スライドインペイン の [ステアリングコントラクト名（Steering contract name）] フィールドに、ステアリングコントラクトの名前を入力します。

ステップ 5 （任意） [Description] フィールドに、説明を入力します

ステップ 6 [ルールの追加（Add Rule）] をクリックしてルールを追加し、次の設定を完了します。

a) [**Application**] で、ルールを適用するアプリケーションを選択します。

1. 鉛筆アイコンをクリックします。
2. [**Choose Application**] ダイアログボックスで、必要なアプリケーションを選択します。
3. [確認（Confirm）] をクリックします。

選択内容	結果
advanced	• [トランスポートプロトコル（Transport Protocol）] で、ドロップダウンリストからルールのトランスポートプロトコルを選択します。 • [送信元ポート（Source port）] と [接続先ポート（Destination port）] で、ルールに対応するポート番号を入力します。 値の範囲は 1 ～ 65535 です。
その他のアプリケーション	選択したアプリケーションに基づいて、Catalyst Center には対応するポートとトランスポートプロトコルが自動的に表示されます。

b) [ログの有効化（Enable logs）] トグルを使用して、任意の通信フィルタルール（デフォルトアクションを含む）のロギングを有効または無効にします。

ロギングはデフォルトでは無効になっています。ロギングが有効になっている場合、ルールがトリガーされると、デバイスは syslog メッセージを送信します。

ロギングは、ポリシーの障害対応と初期化テストに役立ちます。ただし、デバイスのリソースとパフォーマンスに影響を与える可能性があるため、慎重に使用することを推奨します。

ステップ 7 （任意） 次の設定を完了します。

実行する操作	結果
別のルールの作成	次のいずれかのオプションを使用します。 • ステップ 6 （1516 ページ） を繰り返す、または • [アクション（Actions）] で、対応する [+] アイコンをクリックし、6.a （1516 ページ） と 6.b （1516 ページ） を繰り返します。
ルールのシーケンスの更新。	ルールは、[ルール（Rules）] テーブルにリストされている順にチェックされます。シーケンスを更新するには、次の手順を実行します。 1. 対応する ⠿ アイコンをクリックします。 2. 必要な位置にルールをドラッグアンドドロップします。
複数のルールのログの有効化。	1. 必要なルールの横にあるチェックボックスをオンにします。 2. [ログを有効化（Enable Logs）] をクリックします。
ルールの削除	1. 削除するルールの横にあるチェックボックスをオンにし、[削除（Delete）] をクリックします。 2. [**Actions**] で、削除するルールに対応する削除アイコン（🗑）をクリックします。

ステップ 8 [Save] をクリックします。

Catalyst Center は、トラフィック ステアリング コントラクトを保存しているときに、重複するルールを検出し、自動的に統合します。

トラフィック ステアリング コントラクトの編集または複製

次の手順を実行して、トラフィック ステアリング コントラクトを編集または複製します。

手順

ステップ 1 メインメニューから次を選択します。**[ポリシー（Policy）]>[トラフィック ステアリング ポリシー（Traffic Steering Policy）]**の順に選択します。

ステップ 2 [トラフィック ステアリング コントラクト（Traffic steering contracts）] タブをクリックします。

ステップ 3 編集または複製する契約の横にあるチェックボックスをオンにします。

ステップ 4 必要なオプションを選択します。

実行する操作	結果
ステアリング契約の編集	[その他のアクション（More Actions）] にカーソルを合わせて [編集（Edit）] を選択します。
ステアリング契約の複製	[その他のアクション（More Actions）] にカーソルを合わせ、[複製（Duplicate）]を選択します。

ステップ 5 必要な設定を編集します。

詳細については、トラフィック ステアリング コントラクトの作成 （1515 ページ）を参照してください。

ステップ 6 [Save] をクリックします。

トラフィック ステアリング コントラクトの削除

トラフィック ステアリング コントラクトを削除するには、次の手順を実行します。

手順

ステップ 1 メインメニューから次を選択します。**[ポリシー（Policy）]>[トラフィック ステアリング ポリシー（Traffic Steering Policy）]**の順に選択します。

ステップ 2 [トラフィック ステアリング コントラクト（Traffic steering contracts）] タブをクリックします。

ステップ 3 削除する契約の横にあるチェックボックスをオンにします。

ステップ 4 [その他の操作（More Actions）] にカーソルを合わせて [削除（Delete）] を選択します。

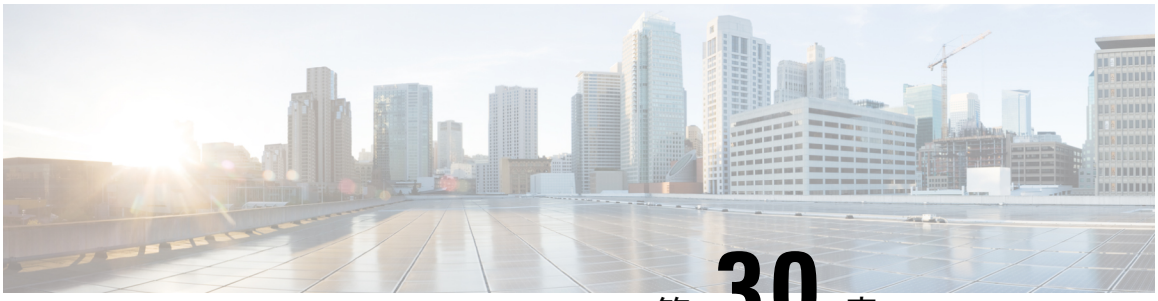
ステップ 5 警告ダイアログボックスで、[Yes] をクリックします。



第 VII 部

ネットワークのモニタリングとトラブルシューティング

- 高度な機能のトライアルの有効化 （1521 ページ）
- Cisco AI Endpoint Analytics （1525 ページ）
- ネットワーク推論機能を使用したネットワークデバイスのトラブルシューティング （1585 ページ）
- ネットワークバグの特定 （1601 ページ）
- ネットワーク セキュリティ アドバイザリの識別 （1605 ページ）
- ネットワークの Field Notice の特定 （1619 ページ）
- Catalyst Center からの根本原因分析ファイルの生成 （1623 ページ）



第 30 章

高度な機能のトライアルの有効化

- 高度な機能のトライアルの概要 （1521 ページ）
- ネットワークバグ ID トライアルの有効化 （1521 ページ）
- セキュリティ アドバイザリ トライアルの有効化 （1522 ページ）
- Field Notice トライアルの有効化 （1523 ページ）

高度な機能のトライアルの概要

高度な機能のトライアルは、期間限定で無料です。これらの機能は CX Cloud と連携し、運用データとネットワーク設定に基づいてカスタマイズされたインサイトを提供します。Catalyst Center ダッシュボードから「CX Cloud の接続への同意」（CX Cloud Consent to Connect）契約を承認することにより、高度な機能へのアクセスを有効にできます。

これらの高度な機能は、ネットワークを保護し、最新の状態に保つために役立ちます。シスコは高度な機械学習アルゴリズムを使用して、ハードウェア、ソフトウェア、およびデバイス構成をスキャンして分析し、現在の環境に固有のカスタマイズされた実用的なインサイトを生成します。

（注）

- これらの高度な機能を有効にした場合、Catalyst Center は、米国でホストされている CX Cloud にのみデータを送信し、他の地域には送信しません。
- EoX（サポート終了マイルストーン）機能は、高度な機能のトライアルとは別に提供されています。EoX 機能へのアクセスを有効にするには、Catalyst Center ダッシュボードから「CX Cloud の接続への同意」（CX Cloud Consent to Connect）契約を承認します。EoX 機能の詳細については、コンプライアンスカテゴリ （666 ページ）を参照してください。

ネットワークバグ ID トライアルの有効化

90 日間のトライアル用に CX ライセンスを有効にすることで、この機能を試すことができます。

始める前に

- CX Cloud に到達するには、Catalyst Center のファイアウォールに正しい URL とポートを入力する必要があります。

手順

ステップ 1 メインメニューから次を選択します。**[Tools]** > **[Network Bug Identifier]** の順に選択します。

機能のトライアルがまだ開始されていない場合、Catalyst Center にはトライアルオファーのバナーが表示されます。機能のトライアルがすでに開始されている場合は、トライアルの残り日数が表示されます。

ステップ 2 トライアルを開始するには、トライアルの利用規約に同意する必要があります。

- 別の機能のトライアルや機能に関するトライアル利用規約にすでに同意している場合は、次のステップに進みます。
- まだ同意していない場合は、同意するように求められます。バナーで、[Consent to Connect] リンクをクリックしてトライアル利用規約を表示し、内容を読了したことを確認して同意します。

ステップ 3 トライアルを有効にすることを確認します。

セキュリティ アドバイザリ トライアルの有効化

90 日間のトライアル用に CX ライセンスを有効にすることで、この機能を試すことができます。

始める前に

- CX Cloud に到達するには、Catalyst Center のファイアウォールに正しい URL とポートを入力する必要があります。

手順

ステップ 1 メインメニューから次を選択します。**[Tools]** > **[Security Advisories]** の順に選択します。

機能のトライアルがまだ開始されていない場合、Catalyst Center にはトライアルオファーのバナーが表示されます。機能のトライアルがすでに開始されている場合は、トライアルの残り日数が表示されます。

ステップ 2 トライアルを開始するには、トライアルの利用規約に同意する必要があります。

- 別の機能のトライアルや機能に関するトライアル利用規約にすでに同意している場合は、次のステップに進みます。

- まだ同意していない場合は、同意するように求められます。バナーで、[Consent to Connect] リンクをクリックしてトライアル利用規約を表示し、内容を読了したことを確認して同意します。

ステップ 3 トライアルを有効にすることを確認します。

Field Notice トライアルの有効化

90 日間のトライアル用に CX ライセンスを有効にすることで、この機能を試すことができます。

始める前に

- CX Cloud に到達するには、Catalyst Center のファイアウォールに正しい URL とポートを入力する必要があります。

手順

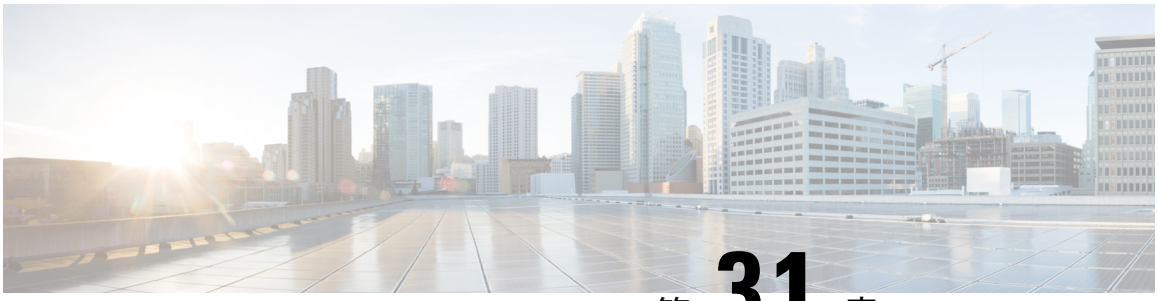
ステップ 1 メインメニューから次を選択します。**[Tools]** > **[Field Notices]** の順に選択します。

機能のトライアルがまだ開始されていない場合、Catalyst Center にはトライアルオファーのバナーが表示されます。機能のトライアルがすでに開始されている場合は、トライアルの残り日数が表示されます。

ステップ 2 トライアルを開始するには、トライアルの利用規約に同意する必要があります。

- 別の機能のトライアルや機能に関するトライアル利用規約にすでに同意している場合は、次のステップに進みます。
- まだ同意していない場合は、同意するように求められます。バナーで、[Consent to Connect] リンクをクリックしてトライアル利用規約を表示し、内容を読了したことを確認して同意します。

ステップ 3 トライアルを有効にすることを確認します。



第 31 章

Cisco AI Endpoint Analytics

- Cisco AI エンドポイント分析 の概要 （1525 ページ）
- Cisco AI エンドポイント分析の主な機能 （1526 ページ）
- FIPS の準拠性 （1527 ページ）
- Catalyst Center での Cisco AI エンドポイント分析のセットアップ （1528 ページ）
- Cisco AI エンドポイント分析の概要ウィンドウ （1533 ページ）
- エンドポイント インベントリ （1545 ページ）
- 信頼得点 （1551 ページ）
- プロファイリングルール （1570 ページ）
- スマートグループ化のための Cisco AI ルール （1577 ページ）
- 階層 （1581 ページ）

Cisco AI エンドポイント分析 の概要

可視性は、エンドポイントを保護するための最初のステップです。Cisco AI エンドポイント分析は、エンドポイントと Internet of Things（IoT）デバイスの識別とプロファイリングに役立つエンドポイント可視性ソリューションです。Cisco AI エンドポイント分析エンジンを使用すると、さまざまなソースからネットワーク経由で受信したテレメトリ情報を使用して、エンドポイントにラベルを割り当てることができます。

Cisco AI エンドポイント分析で使用できるプロファイリングラベルは、エンドポイントタイプ、ハードウェアモデル、製造元、およびオペレーティング システム タイプです。これは多要素分類と呼ばれます。

Cisco AI エンドポイント分析は、潜在的に危険なエンドポイントやデバイスを特定して対処することを可能にする信頼スコアなどの機能により、ネットワークにおける繊細な可視化と処置を実現します。Cisco AI エンドポイント分析の GUI から Cisco ISE を介して ANC ポリシーを適用することにより、潜在的なリスクを管理することもできます。Cisco AI エンドポイント分析でエンドポイントのランダムおよび変更 MAC アドレスの問題をモニターして回避し、MAC アドレスの代わりに「DUID」と呼ばれる一意の属性を使用してエンドポイントを正確に識別することができます。

Cisco AI エンドポイント分析は、さまざまなソースからエンドポイントテレメトリを収集するのに役立ちます。主要なソースは、Network-Based Application Recognition（NBAR）メカニズム

です。NBAR メカニズムは、Cisco Catalyst 9000 シリーズ スイッチ（アクセスデバイス）に組み込まれていて、ディープ パケット インスペクション（DPI）を実行します。Cisco AI エンドポイント分析は、Catalyst Center トラフィック テレメトリ アプライアンスからもテレメトリを受信できます。

Cisco ISE、自己登録型ポータル、ServiceNow のような構成管理データベース（CMDB）ソフトウェアなど、さまざまなソースからエンドポイントコンテキスト情報を収集できます。

Cisco AI エンドポイント分析を使用すると、さまざまなネットワークデバイスからのデータインフローが可能になり、エンドポイントをより高い精度で容易に識別してプロファイリングし、異常に対処する機能が拡張されます。Cisco AI エンドポイント分析では、さまざまなエンドポイント情報を集約し、そのデータを使用してエンドポイントをプロファイリングできます。エンドポイントのプロファイリング後、AI と機械学習アルゴリズムを使用して、さまざまな方法を直感的に活用することで不明なエンドポイントの数を減らすこともできます。

Cisco AI エンドポイント分析の主な機能

- **Cisco AI エンドポイント分析ダッシュボード**

  Cisco AI エンドポイント分析ダッシュボードでは、ネットワークに接続されているエンドポイントの全体像を確認できます。既知のエンドポイント、不明なエンドポイント、プロファイリングされたエンドポイント、プロファイリングされていないエンドポイント、信頼スコアが低いエンドポイント、およびランダム MAC アドレスを使用するエンドポイントの数を表示できます。[AI Proposals] ダッシュレットには、エンドポイントのプロファイリングと管理を強化するためのインテリジェントなプロファイリングの提案が表示されます。

- **潜在的に危険なエンドポイントにフラグを付ける信頼スコア**

  Cisco AI エンドポイント分析は、エンドポイントに信頼スコアを割り当てます。これにより、ネットワーク内の潜在的に危険なエンドポイントを簡単にモニタして対処することができます。異常な動作がモニタおよび追跡され、追跡された異常の数と頻度に基づいて信頼スコアが割り当てられます。エンドポイントの信頼スコア （1552 ページ）を参照してください。

- **ランダム MAC アドレスを使用するエンドポイントの検出**

  Cisco AI エンドポイント分析を使用すると、Cisco ISE から「DUID」と呼ばれる（Cisco ISE では「GUID」とも呼ばれます）一意のエンドポイント識別子を受信することにより、ランダムおよび変更 MAC アドレスの問題を処理できます。Cisco AI エンドポイント分析は、MAC アドレスの代わりに、エンドポイントの識別子として DUID を使用します。

- **機械学習機能を使用したネット内の不明なエンドポイントの削減**

  Cisco AI エンドポイント分析では、エンドポイントのグループ化で学習した情報に基づいてプロファイリング提案が提供されます。このような提案を使用して、ネットワーク内の不明なエンドポイントやプロファイリングされていないエンドポイントの数を減らすことができます。

- **システムルールおよびカスタム プロファイリング ルールによるエンドポイントの管理**

  ネットワークに接続されたエンドポイントを確実にプロファイリングおよび管理するには、シスコが提供するシステムルールと自分で設計したカスタムルールを使用します。

- **Cisco AI エンドポイント分析によるエンドポイントの登録**

  Cisco AI エンドポイント分析を使用して、エンドポイントをオンボードおよびプロファイリングできます。この登録プロセスでエンドポイント属性データが収集されて、エンドポイントのプロファイリングに使用されます。

- **外部ソースを使用したエンドポイントの登録**

  構成管理データベース（CMDB）などエンドポイントデータの外部ソースの中には、Cisco AI エンドポイント分析に接続できるものがあります。これにより、ネットワーク内のエンドポイントを簡単に登録、管理、およびプロファイリングできます。

- **定義された非アクティブ期間後のエンドポイントのパージ**

  定義された時間にわたって非アクティブだったエンドポイントをネットワークから削除するには、エンドポイント パージ ポリシーを定義します。エンドポイントを削除する必要があるまでの非アクティブ期間を定義できます。また、プロファイリング属性に基づいて特定のエンドポイントのセットに作用するようにパージポリシーをカスタマイズすることもできます。

FIPS の準拠性

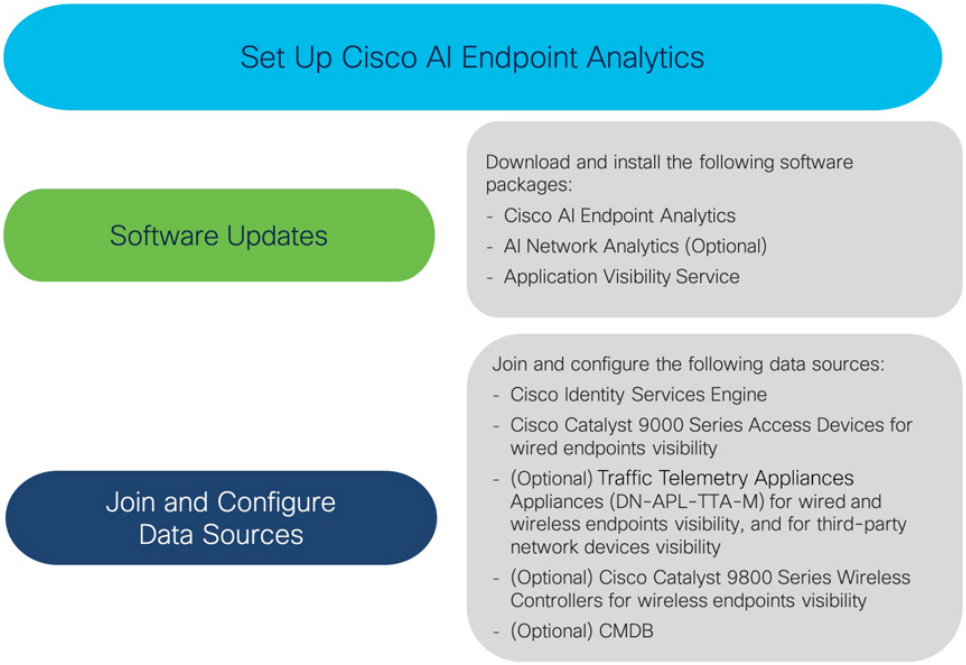
Catalyst Center は米国の連邦情報処理標準（FIPS）をサポートしています。FIPS は、Catalyst Centerイメージのインストール時に有効にできるオプションのモードです。デフォルトでは、FIPS モードはディセーブルです。

Catalyst Center で FIPS モードが有効になっている場合、Catalyst Center GUI の次の機能は使用できません。

- [AI Endpoint Analytics Setup] の [Optional Configurations] セクションにある [Enable AI Network Analytics] ダッシュレット。
- **[Policy]** > **[AI Endpoint Analytics]** > **[Overview]**の [AI Proposals] ダッシュレット。
- **[Policy]** > **[AI Endpoint Analytics]** > **[Overview]** > **[Configuration]** の [Profile Rule Settings] タブ。
- **[Policy]** > **[AI Endpoint Analytics]** > **[Overview]** > **[Configuration]** > **[Trust Analytics]** の [AI Spoofing Detection] セクション。
- **[ポリシー（Policy）]** > **[AIエンドポイント分析（AI Endpoint Analytics）]** > **[エンドポイントインベントリ（Endpoint Inventory）]**の特定のエンドポイントの [信頼スコア（Trust Score）] の詳細の下にある [エンドポイントの異常検出（Endpoint Anomaly Detection）] の [AIスプーフィング検出（AI Spoofing Detection）] セクション。

- **[Policy]** > **[AI Endpoint Analytics]** > **[Endpoint Inventory]** > **[Focus as Trust Score]** の [AI Spoofing Detection] 列。
- **[ポリシー（Policy）]** > **[AIエンドポイント分析（AI Endpoint Analytics）]** > **[概要（Overview）]** > **[設定（Configuration）]** > **[信頼スコアソース（Trust Score Sources）]** にある [TalosのIPレピュテーション（Talos IP Reputation）] セクション。

Catalyst Center での Cisco AI エンドポイント分析のセットアップ



ソフトウェアアップデートのインストール

次の手順で説明するように、Catalyst Center にソフトウェアアップデートをインストールして Cisco AI エンドポイント分析 を使用します。

手順

ステップ 1 Catalyst Center にログインします。

ステップ 2 メインメニューから次を選択します。**[System]** > **[Software Management]** の順に選択します。

ステップ 3 [Updates] タブで、[Cisco AI Endpoint Analytics]、[AI Network Analytics]、および [Application Visibility Service] が [Application Updates] セクションにリストされているかどうかを確認してください。これらのアプリケーション更新が表示されている場合は、[Install All] をクリックします。

- Catalyst Center でエンドポイント プロファイリング ソリューションにアクセスするには、[Cisco AI Endpoint Analytics] 更新をインストールします。
- 機械学習と AI の機能を使用してインテリジェントなプロファイリング提案を受け取るには、[AI Network Analytics] 更新をインストールします。
- NBAR およびコントローラベースのアプリケーション認識（CBAR）の技術を使用してエンドポイント プロファイリングを通知するには、[Application Visibility Service] 更新をインストールします。

ステップ 4 これらの更新が [Updates] タブにリストされていない場合は、[Installed Apps] タブをクリックして、更新がすでにインストールされ、使用可能であるかどうかを確認してください。[Currently Installed Applications] タブでは、ソフトウェアインストールが正常に完了しているかどうかも確認できます。

データソースの接続と有効化

Cisco AI エンドポイント分析が使用するデータソースは、すでに Catalyst Center に接続されている可能性があります。データソースが接続されている場合は、次の手順に従って、Cisco AI エンドポイント分析 でデータソースを使用できることを確認します。

Cisco AI エンドポイント分析が結果を提供できるようにするには、Cisco ISE または Catalyst 9000 シリーズ アクセスデバイスを Catalyst Center に追加する必要があります。

手順

ステップ 1 Cisco ISE を Catalyst Center に接続します。

Cisco Catalyst Center 設置ガイド [英語] の「Complete First-Time Setup」にある「Integrate Cisco ISE with Catalyst Center」セクションを参照してください。

以下の Cisco ISE リリースでは Cisco AI エンドポイント分析 がサポートされています。

- 2.4 パッチ 11 以降
- 2.6 パッチ 5 以降
- 2.7 パッチ 1 以降
- 3.0 以降

Cisco ISE 3.1 以降の場合、Cisco ISE 管理ポータルで次の手順を実行します。

a) **[Work Centers]** > **[Profiler]** > **[Settings]** の順に選択します。
b) [エンドポイント分析設定（Endpoint Analytics Settings）] エリアで、次のチェックボックスをオンにします。

- [Publish Endpoint Attributes to AI Endpoint Analytics]
- [Consume Endpoint Profiles from AI Endpoint Analytics]

Cisco ISE が 802.1X または MAB 認証方式でエンドポイントを認証すると、収集されたエンドポイント属性が Cisco AI エンドポイント分析で使用可能になります。Cisco ISE はまた Cisco AI エンドポイント分析とテレメトリデータを共有します。

Cisco ISE 2.4、2.6、および 3.0 の場合、Cisco ISE 管理ポータルで次の手順を実行します。

a) **[Work Centers]** > **[Profiler]** > **[Settings]** の順に選択します。
b) [Enable Probe Data Publisher] オプションを選択します。
c) [Save] をクリックします。

ステップ 2 有線エンドポイントが表示されるように、Cisco 9000 シリーズ アクセスデバイスを Catalyst Center に接続します。

Cisco Catalyst Center ユーザーガイド [英語] の「Discover Your Network」を参照してください。

Cisco AI エンドポイント分析機能を有効にするには、Cisco 9000 シリーズアクセスデバイスを Cisco IOS-XE リリース 17.6 以降にアップグレードします。

必要なアクセスデバイスの CBAR を有効にするには、

a) Catalyst Center GUI でメニューアイコンをクリックして、**[Provision]** > **[Services]** > **[Application Visibility]** の順に選択します。
b) データが必要な Cisco Catalyst 9000 アクセスデバイスを選択します。[Site Devices] セクションのデバイス名の横にあるチェックボックスをオンにします。
c) [Enable CBAR] をクリックします。
d) 表示される確認ウィンドウで、[Yes] をクリックします。
e) [Enable CBAR] スライドインペインで、サポートされている SSID タイプの横にあるチェックボックスをオンにします。
f) [Enable] をクリックします。

ステップ 3 （任意）ワイヤレスエンドポイントを可視化するには、Cisco Catalyst 9800 シリーズ ワイヤレスコントローラを Catalyst Center に接続します。

次の Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ モデルは Cisco AI エンドポイント分析 によりサポートされます。

- 9800-CL
- 9800-40
- 9800-80
- 9800-L

Catalyst Center は、Cisco IOS XE リリース 17.7.1 以降を搭載した Cisco Catalyst 9800 シリーズ ワイヤレス コントローラで FlexConnect をサポートします。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの概要 （754 ページ） で Cisco Catalyst 9800 シリーズ ワイヤレス コントローラを設定およびプロビジョニングするには、Catalyst Centerを参照してください。

ステップ 4 （オプション）Cisco Catalyst IE9300 高耐久性シリーズ スイッチを Catalyst Center に接続します。

Cisco Catalyst IE9300 高耐久性シリーズ スイッチは Cisco AI エンドポイント分析でサポートされます。

Cisco Catalyst Center ユーザーガイド [英語] の「Discover Your Network」を参照してください。

ステップ 5 （任意）有線およびワイヤレスエンドポイントを可視化し、サードパーティ製のネットワークデバイスを可視化するには、Catalyst Center トラフィック テレメトリ アプライアンス を Catalyst Center に接続します。

Catalyst Center トラフィック テレメトリ アプライアンス（DN-APL-TTA-M）エンドポイント分析のためにミラーリングされたネットワークトラフィックからテレメトリを生成します。このアプライアンスでは、Network-Based Application Recognition ベース（NBAR ベース）のプロトコル検査、およびエンドポイント属性の抽出が可能です。

テレメトリアプライアンスで収集されたエンドポイント属性を Cisco AI エンドポイント分析で受信するには、Cisco ISE と Catalyst Center を統合する必要があります。

Catalyst Center でのアプライアンスのインストール、接続の構成、およびアプライアンスの管理については、「Traffic Telemetry Appliances」を参照してください。

Catalyst Center トラフィック テレメトリ アプライアンス に接続されたアクセススイッチの Switched Port Analyzer（SPAN; スイッチドポートアナライザ）受信ポートで CBAR を有効にするには、次のコマンドを使用します。

```
ip nbar protocol-discovery
```

テレメトリアプライアンスに接続されているすべてのエンドポイントが Cisco AI エンドポイント分析に表示されるわけではありません。Cisco Catalyst Assurance で管理されるネットワーク アクセスデバイス（NAD）にも接続されているエンドポイントのみが、Cisco AI エンドポイント分析 に表示されます。

ステップ 6 （任意）Catalyst Center で ServiceNow を有効にします。

a) ServiceNow を Catalyst Center に接続した後に、メニューアイコンをクリックして次を選択します。**[Platform]** > **[Manage]** > **[Bundles]** の順に選択します。

b) バンドル [Endpoint Attribute Retrieval with ITSM (ServiceNow)] の [Status] が [New] の場合は、バンドルの [Enable] をクリックします。

ステップ 7 （任意）Catalyst Center で Cisco AI 分析を有効にします。

AI ベースのエンドポイントグループ化、カスタム プロファイリング ルール自動化、およびエンドポイントラベルに関する提案を受け取るには、また、ネットワーク内のスプーフィングされている可能性のあるデバイスを検出するには、[Cisco AI Analytics] ウィンドウで、必要な設定を有効にする必要があります。

これらの AI ベースの提案を受け取るには、AI ネットワーク分析ソフトウェアをインストールする必要があります。

a) メインメニューから次を選択します。 **[System]** > **[Settings]** > **[External Services]** > **[Cisco AI Analytics]** の順に選択します。

b) 有効にする各サービスのトグルボタンをクリックします。

- **AI エンドポイント分析**：AI ネットワーク分析は、機械学習を利用してネットワークのインテリジェンスを推進し、ネットワークパフォーマンスを効果的に改善して問題解決を加速できるようにします。AI ネットワーク分析は、ネットワークの動作を分析し、ネットワーク環境に適応することで、ノイズや誤検出を大幅に削減します。

- **エンドポイント スマートグループ化**：エンドポイントスマートグループ化は、AIと機械学習を使用して、AIベースのエンドポイントグループ化、自動化されたカスタム プロファイリング ルール、クラウドソーシングされたエンドポイントラベルを提供することにより、ネットワーク内の不明なエンドポイントの数を減らします。
- **AI スプーフィング検出**：AI スプーフィング検出は、事前トレーニング動作モデルに基づいてスプーフィングされているエンドポイントを識別します。 [Enable AI Spoofing Detection] トグルボタンを有効にすると、Catalyst Center はこれらの動作モデルとネットワークデバイスによって提供されるフロー情報を使用して、スプーフィングされたエンドポイントを検出できます。参加しているお客様から収集されたフロー情報を使用して、いくつかの行動モデルが構築され、集中的にトレーニングされます。
  - スプーフィングの検出はクラウドで行われ、Catalyst Center からクラウドへの匿名化データのエクスポートが必要となります。その後、Catalyst Center はクラウドにスプーフィング検出の有無をポーリングします。
  - 中断のないインターネット接続が必要です。
  - 最新リリースへのアップグレード中に、以前のリリースでデータエクスポートが無効になっていた場合、アップグレードのときにデータエクスポートが無効になっていることを示す警告が表示されます。スプーフィング検出を再度有効にする必要があります。

エンドポイント テレメトリ ソース

Cisco AI エンドポイント分析は、次の方法でテレメトリデータを受信します。

- **ディープ パケット インスペクション**

  ディープ パケット インスペクションは、Cisco Catalyst 9000 シリーズ アクセス デバイスによって実行される高度なパケット分析方法です。これらのアクセスデバイスは、NBAR を実行します。NBAR は、アプリケーション トラフィックを検査し、プロトコル分析を実行して、精度の高いエンドポイントを検出および識別し、プロファイリングします。

  ディープ パケット インスペクションのプロファイリングは、ネットワークへのエンドポイントトラフィックから収集されたさまざまな属性に基づいています。これらの属性は、パケットヘッダーレイヤ 4 ～ 7 から複数のプロトコルにわたって収集されます。

- **構成管理データベース接続**

  Cisco AI エンドポイント分析は、エンドポイント プロファイリングの精度を高めるために、構成管理データベース（CMDB）接続からエンドポイントデータを受信します。ServiceNow との接続により、CMDB から Cisco AI エンドポイント分析への情報を受信できます。

- **機械学習機能**

  プロファイリング用に収集されたデータは、匿名化されて、Cisco Cloud でデバイスデータレイクとして機能する場所に送信されます。ここでは、機械学習アルゴリズムで使用可能

なデータを分析し、必要に応じて評価して適用できるプロファイリングルールを作成します。エンドポイント プロファイリングと管理を簡素化かつ効率化できるように、Cisco AI エンドポイント分析によってスマート プロファイリング ルールが提案されます。既存のルールも評価され、この継続学習に基づいて改善提案が提供されます。

Cisco AI エンドポイント分析の概要ウィンドウ

メインメニューから次を選択します。**[Policy]** > **[AI Endpoint Analytics]**の順に選択します。

[概要（Overview）] ウィンドウに次のダッシュレットが表示されます。

- **合計エンドポイント数**

  このダッシュレットでは、ネットワーク内のエンドポイントの合計数が [Fully Profiled] と [Partially Profiled] の 2 つのグループに分かれて表示されます。Cisco AI Endpoint Analytics は、次の 4 つの要因に基づいてエンドポイントをプロファイリングします。

  - エンドポイントタイプ
  - OS タイプ
  - ハードウェアのモデル
  - ハードウェアメーカー

  エンドポイントにこれらの要因の 1 つ以上が欠落している場合は、[Partially Profiled] グループにプロファイリングされます。

  [Partially Profiled Labels] をクリックすると、ネットワーク内のプロファイルが欠落しているエンドポイントの数が、プロファイルラベルタイプで分類されて表示されます。特定のプロファイルラベルが欠落しているエンドポイントを確認するには、プロファイルラベルの横にある数字をクリックします。[エンドポイントインベントリ（Endpoint Inventory）] タブが、対応するエンドポイントのリストとともに表示されます。

- **AI 提案**

  Cisco AI エンドポイント分析は、スマートグループ化アルゴリズムを使用して、ネットワーク内で類似するプロファイリングデータを持つ不明なエンドポイントをグループ化します。AI エンドポイント分析を有効にした場合、次のタイプのルール提案が表示されます。これらのルール提案は、次のようにエンドポイントクラスタから学習した内容に基づいています。

  - 類似している可能性があるエンドポイントをプロファイリングするための新しいルール。
  - 以前に受け入れられていたルールの変更提案。
  - 不要になったプロファイリングルールの確認。

詳細については、スマートグループ化のための Cisco AI ルール （1577 ページ）を参照してください。

- **信頼スコア**

  [Trust Scores] ダッシュレットには、ネットワーク内のエンドポイントに割り当てられている信頼スコアの全体像が示されます。エンドポイントの信頼スコア （1552 ページ）を参照してください。

- **設定**

  [概要（Overview）] エリアの右上隅にある [設定（Configuration）] リンクをクリックすると、次の設定にアクセスできます。

  - [Profile Rule Settings]：システムプロファイルルールの自動更新をスケジュールします。エンドポイントプロファイリング用の自動システムルール更新 （1572 ページ）を参照してください。
  - [ISE Integration]：Cisco ISE への承認属性の公開 （1538 ページ）を参照してください。
  - [**Trust Analytics**]：信頼スコアのソースを有効または無効にするには、このトグルボタンをクリックします。[Authentication Method] ソースを無効にすることはできません。アクティブな Cisco ISE 統合が設定されている場合、エンドポイントが使用する認証方式およびそのポスチャステータスによって、エンドポイントの信頼スコアが通知されます。[AIスプーフィング検出（AI Spoofing Detection）]、[エンドポイント属性の競合（Endpoint Attribute Conflict）]、[NATモード検出（NAT Mode Detection）]、[同時MACアドレス（Concurrent MAC Addresses）]、[セキュリティセンサー（Security Sensor）] など、信頼スコアデータのその他のソースは、有効または無効にできます。

    「エンドポイントの信頼スコア （1552 ページ）」を参照してください。
  - [Endpoint Purge Policy]：エンドポイント パージ ポリシー （1543 ページ）を参照してください。
  - [Endpoint Subnet Inspection]：エンドポイントサブネット検査の設定 （1544 ページ）を参照してください。

- **エンドポイント MAC ランダム化**

  [Endpoint MAC Randomization] には、ネットワーク内の静的 MAC アドレスとランダムおよび変更 MAC アドレスの数が表示されます。ランダムおよび変更 MAC アドレスを持つエンドポイントの信頼スコア （1560 ページ）を参照してください。

Cisco Talos インテリジェンス

Cisco Talos インテリジェンスは、包括的な脅威検出ネットワークです。Talos インテリジェンスは、脅威検出アナリストと、Web リクエスト、電子メール、マルウェアサンプル、オープンソースデータセット、エンドポイントインテリジェンス、ネットワーク侵入に及ぶリアルタイムの自動検出システムで構成されています。Talos IP レピュテーション機能を使用して Cisco AI エンドポイント分析 と Talos を統合することにより、信頼できない IP アドレスに到達する

ネットワーク接続にフラグを立て、それらを隔離し、最も一般的なサイバー脅威からネットワークを保護できます。

Catalyst Center - Cloud は Talos インテリジェンス クラウド サービスと通信し、更新された IP レピュテーションデータを 30 分ごとに取得します。これらの更新は、登録されているすべての Catalyst Center デバイスにプッシュされます。

Catalyst Center での Cisco Talos インテリジェンスの設定は、2 つの手順で行うことができます。

アプリケーションの有効化による Cisco AI エンドポイント分析 と Cisco Talos インテリジェンスの統合

始める前に

Talos IP レピュテーション機能がスムーズに動作するには、アプリケーションテレメトリを有効にして、NetFlow コレクタとして Catalyst Center を選択します。NetFlow コレクタの詳細については、「テレメトリの設定」を参照してください。

推奨される手順は、次のとおりです。

手順

ステップ 1 Catalyst Center GUI でメニューアイコンをクリックして、**[System]** > **[Settings]** > **[External Services]** > **[Cisco Catalyst - Cloud]** の順に選択します。

ステップ 2 [Region] ドロップダウンリストから、適切なリージョンを選択します。

ステップ 3 [Talos Threat Intelligence] アプリまでスクロールします。

ステップ 4 [Talos Threat Intelligence] アプリで [Activate] をクリックします。Cisco Cloud Services のホームページが表示されます。

ステップ 5 Cisco Cloud Services GUI でメニューアイコンをクリックして、[Applications] をクリックします。

ステップ 6 [Region] ドロップダウンリストから、適切なリージョンを選択します。

ステップ 7 [Talos Threat Intelligence] アプリで [Activate] をクリックします。

[アプリケーション（Applications）] ウィンドウでリージョンが選択されていない場合は、[リージョンの選択（Select Region）] ダイアログボックスが表示されます。必要なリージョンを選択してから、[Activate] をクリックします。

ステップ 8 チェックボックスをオンにして利用規約に同意し、[Subscribe] をクリックします。

ステップ 9 [Choose Your Product] ウィンドウで Catalyst Center をクリックし、Talos 脅威インテリジェンスのアクティベーション用に選択します。

ステップ 10 [Activate Talos Threat Intelligence Application for your Product] ウィンドウでは、[Host Name/IP]、[Name]、[Description]（ある場合）などです。**[Type]** ドロップダウンリストから、Catalyst Center などの登録する製品の適切なタイプを選択します。

ステップ 11 [登録（Register）] をクリックします。

ステップ 12 [Choose Your Product] ウィンドウで Catalyst Center をクリックして再度選択し、[Select Product] をクリックします。

ステップ 13 [Authenticate your Product] ウィンドウで [Auto Redeem] をクリックし、OTP を自動的に引き換えて製品を認証します。Catalyst Center が新しいウィンドウで開きます。

ワンタイムパスコード（OTP）をコピーしてウィンドウを閉じ、製品を手動で登録することもできます。

ステップ 14 表示される Catalyst Center ウィンドウで、Catalyst Center のログイン情報を使用してログインします。

（注）
- 登録が成功したら、ウィンドウを閉じてから Cisco Cloud Services に進み、ワークフローを続行します。
- Catalyst Center を Cisco Cloud Services に登録したら、3 分待ってからステップ 15 に進みます。
- Cisco Cloud Services GUI（**[Menu]** > **[Applications]**）で、登録した製品と登録ステータスを確認できます。

ステップ 15 [Scope Selection] ウィンドウで Catalyst Center に必要な範囲を選択し、[Next] をクリックします。

Catalyst Center 用に選択されたアプリケーション、製品、および範囲が要約されている **[概要（Summary）]** ウィンドウが表示されます。

ステップ 16 [Activate] をクリックし、Catalyst Center を Talos 脅威インテリジェンスに接続します。

有効化のステータスが表示されます。

ステップ 17 次のいずれか 1 つのタスクを実行します。

- （Catalyst Center デバイスを初めて登録し、Cisco Cloud Services で Talos をアクティブ化した場合）[Exit] をクリックしてウィンドウを閉じます。
- （Cisco Cloud Services で事前登録済みの Catalyst Center デバイスの Talos をアクティブ化した場合）[Exit] をクリックし、Cisco Cloud Services の [Applications] ウィンドウに戻ります。**[アプリケーション（Applications）]** ウィンドウに接続されたアプリケーションが表示されます。

クラウド認証を使用した Cisco AI エンドポイント分析 と Cisco Talos インテリジェンスの統合

手順

ステップ 1 Catalyst Center GUI でメニューアイコンをクリックして、**[System]** > **[Settings]** > **[External Services]** > **[Cloud Authentication]** の順に選択します。

ステップ 2 [dna.cisco.com] リンクをクリックし、Catalyst Center - Cloud アカウントを作成します。

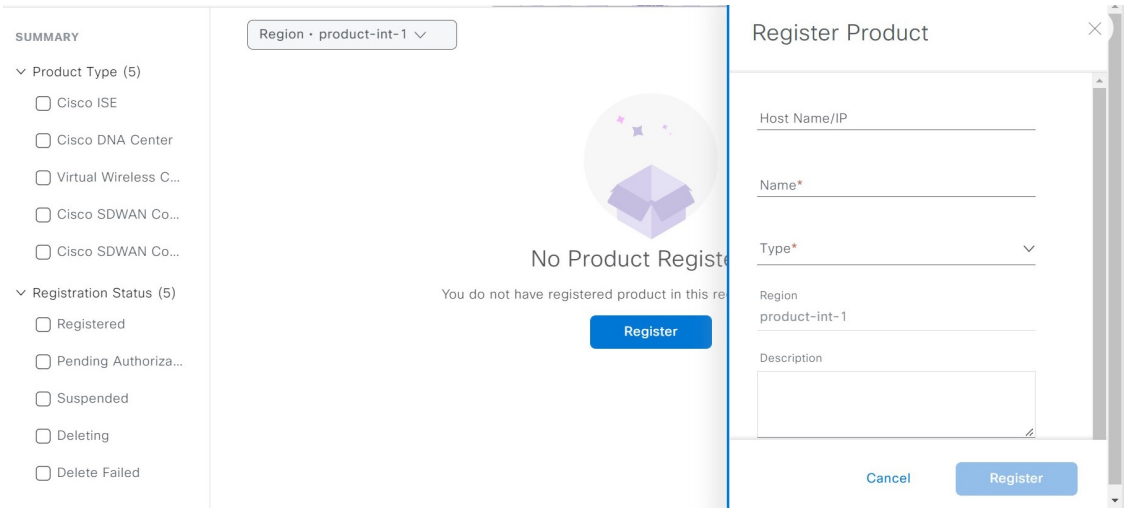
ステップ 3 Catalyst Center - Cloud の GUI で、[Menu] アイコンをクリックしてから [Applications] をクリックし、[Products] を選択します。

ステップ 4 [Region] ドロップダウンリストから、適切なリージョンを選択します。

ステップ 5 [登録（Register）] をクリックします。

ステップ 6 [Register Product] ペインで、[Host Name/IP]、[Name]、[Description]（ある場合）などの必要な詳細を入力します。**[Type]** ドロップダウンリストから、Catalyst Center などの登録する製品の適切なタイプを選択します。[登録（Register）] をクリックします。

図 *34 : Catalyst Center - Cloud* への製品の登録



（注） [Enable Cloud Access Login] チェックボックスをオンにして、Catalyst Center - Cloud から Catalyst Center への自動ログインを有効にします。

OTP の交換が自動的に行われ、Catalyst Center が新しいウィンドウで開きます。

ステップ 7 Catalyst Center ウィンドウで、Catalyst Center のログイン情報を使用してログインします。

- 登録が成功したら、ウィンドウを閉じて Catalyst Center - Cloud に進み、ワークフローを続行します。
- Catalyst Center デバイスを Catalyst Center - Cloud に登録したら、3 分待ってからステップ 8 に進みます。

ステップ 8 Catalyst Center - Cloud の GUI（**[Menu]** > **[Applications]**）で、登録した製品と登録ステータスを確認できます。

ステップ 9 Catalyst Center の GUI で、Cisco AI エンドポイント分析 ウィンドウ（**[AI Endpoint Analytics]** > **[Configurations]** > **[Trust Analytics]**）に移動し、[Talos IP Reputation] トグルボタンをクリックして有効にします。[Trust Score Sources] ウィンドウまたは **[System]** > **[Settings]** ウィンドウから [Talos IP Reputation] を有効にできます。

[Talos IP Reputation] を有効にすると、Catalyst Center は更新された IP のレピュテーションデータが利用可能になるたびにそのデータを受信します。ネットワーク内のエンドポイントが信頼できない IP アドレスにアクセスしようとすると、フラグが設定され、エンドポイントの [Trust Score] ビューの Talos IP レピュテーションに対して、「Detected」という警告メッセージが表示されます。この警告により、エンドポイントの全体的な信頼スコアが低下します。Talos IP レピュテーション機能により、アクセスされた信頼できない IP アドレスと、エンドポイントによるアクセス試行回数に関する情報が保存されます。この情報は、ネットワークのセキュリティを強化することを決定するときに役立ちます。

[Talos Reputation] ウィンドウ（**[System]** > **[Settings]** > **[Talos IP Reputation]**）には、Talos から受信したさまざまなファイルの最新バージョンが表示されます。これらのファイルを受信した時刻も表示されます。IPv4 および IPv6 ファイルは Talos IP レピュテーション データ ファイルであり、通常 1 日に 1 回更新されます。ただし、Threat Level ファイルはメタデータであり、このファイルが変更されることはほとんどありません。

Cisco ISE への承認属性の公開

ネットワークへのエンドポイントアクセスを承認し、エンドポイントを制御するために、Cisco ISE へ AI エンドポイント分析プロファイルデータを公開します。Cisco AI エンドポイント分析によって共有される属性情報には、AI エンドポイント分析ディクショナリを介して Cisco ISE 管理者が簡単にアクセスできるようになります。Cisco ISE 管理者は、Cisco ISE で許可ポリシーを簡単に作成できます。Cisco ISE と共有される属性には、次のものが含まれます。

1. 全体的な信頼スコアと、記録された各異常スコア。
2. CMDB 属性。
3. 次の多要素プロファイリング属性。
   - ハードウェアメーカー
   - ハードウェアのモデル
   - オペレーティングシステム
   - エンドポイントタイプ

もし Catalyst Center が Cisco ISE リリース 3.1 以降とアクティブに統合されており、承認属性を Cisco ISE に公開する必要がある場合は、次のタスクを実行します。

手順

ステップ 1 Catalyst Center で属性の共有を有効にするには、次の手順を実行します。

a) Cisco AI エンドポイント分析の [Overview] ウィンドウで、[Configurations] をクリックします。
b) 左側のパネルから [ISE Integration] をクリックします。
c) [Enable Profile Publishing to ISE] トグルボタンをクリックしてこの機能を有効にします。

d) 属性情報をCisco ISEに公開するために使用するトピックのタイプに応じて、[Asset Topic Based Integration] チェックボックスと [Enhanced Authorization Integration] チェックボックスのいずれかまたは両方をオンにします。

e) **[Save]** をクリックします。

ステップ 2 Cisco ISE で pxGrid サブスクリプションを有効にするには、次の手順を行います。

a) Cisco ISE GUI でメニューアイコンをクリックし、**[Work Center]** > **[Profiler]** > **[Settings]** の順に選択します。

b) Cisco ISE Release 3.1 に接続している場合、**[エンドポイント分析の設定（Endpoint Analytics Settings）]** エリアで、次のチェックボックスをオンにします。

- [Publish Endpoint Attributes to AI Endpoint Analytics]
- [Consume Endpoint Profiles from AI Endpoint Analytics]

次のタスク

サブスクリプションを確認するには、Cisco ISE メインメニューから次の手順を実行します。

- Cisco ISE 3.1 の場合、**[管理（Administration）]** > **[pxGridサービス（pxGrid Services）]** > **[診断（Diagnostics）]** > **[WebSocket]** > **[クライアント（Clients）]**を選択します。
- Cisco ISE 3.1 より後のリリースの場合、**[管理（Administration）]** > **[pxGridサービス（pxGrid Services）]** > **[診断（Diagnostics）]** > **[接続（Connections）]** > **[クライアント（Clients）]**を選択します。

新しく作成された「`com.cisco.ea.data.ise-<Cisco ISE node>`」を含むサブスクリプションが、PSN ノードの [サブスクリプション（Subscription）] 列に表示されます。

Cisco ISE の **[Policy]** > **[Policy Sets]** ウィンドウで、[Conditions Studio] に「**Endpoint-Analytics**」という名前の新しいディクショナリが表示されます。

Cisco ISE の **[Context Visibility]** > **[Endpoints]** ウィンドウで、エンドポイントの詳細情報の [MAC Address] をクリックします。その詳細情報の属性エリアに、Cisco AI エンドポイント分析から受信された属性の「EA-」というプレフィックスを含む属性が表示されます。

Trust Analytics

[Trust Analytics] ウィンドウでは、さまざまな信頼スコアソースが表示されます。また、一定期間非アクティブになった後にこれらのソースで発生したアラートを手動または自動でリセットしたり、エンドポイントの全体的な信頼スコアを正確に測定するために各信頼スコアソースの影響度を設定したりすることもできます。

信頼スコアは、Zero Trust の成果を達成できるように、ネットワーク上の特定のエンドポイントの信頼性を評価します。値は、1（低信頼度）から 10（高信頼度）の範囲で、複数のソースを使用して計算されます。

- [Endpoint Context]：このカテゴリのソースは、エンドポイントで使用される認証方法とエンドポイントのポスチャステータスに基づいて、エンドポイントの信頼性に関する情報を提供します。
- [Threat and vulnerability Context]：このカテゴリのソースは、エンドポイントに関連する各種の脅威に基づいて、エンドポイントがどの程度脆弱であるかに関する情報を提供します。
- [Network Context]：このカテゴリのソースは、エンドポイントからネットワークへのアクセス方法に関する情報を提供します。

信頼スコアの影響度により、異常が発生した場合のエンドポイントの信頼スコアを制御できます。次の影響度を使用できます。

- [Low]：ネットワークでの異常の重要度が低いとわかっている場合は、その影響度を [Low] に設定して、信頼スコアへの影響を小さくすることができます。影響度をこのように設定した後で同様の異常が再度検出されると、異常が検出されたエンドポイントの信頼スコアはゆっくりと 1 に低下します（システム生成の影響度が合計信頼スコアの 50% 上がります）。
- [Critical]：ネットワークでの異常の重要度が高いとわかっている場合は、その影響レベルを [Critical] に設定して、信頼スコアに非常に大きな影響を与えるようにすることができます。影響度をこのように設定した後で同様の異常が再度検出されると、異常が検出されたエンドポイントの信頼スコアはすぐに 1 に低下します（システム生成の影響度が合計信頼スコアの 50% 下がります）。
- [No Impact]：異常が検出されますが、全体的な信頼スコアには影響しません。このオプションを使用すると、全体的な信頼スコアを変更せずに異常をテストして表示できます。
- [System Default]：デフォルトのシステム生成の信頼スコア。

ソースの影響度をカスタマイズする方法については、「影響度のカスタマイズ」を参照してください。

異常や脆弱性が原因で逸脱が発生した場合、またはエンドポイント接続やインターフェイスに弱点が見つかった場合にアラートが表示されます。アラートは、対処後に手動でリセットできます。対処する必要がないアラートを手動でリセットすることもできます。または、リセットタイマーを設定して、アラートを自動的にリセットすることもできます。一定期間非アクティブになった後、このアラートはエンドポイントで検出されません。

ソースのアラートをリセットする方法については、「アラートのリセット」を参照してください。

影響度のカスタマイズ

エンドポイントについて把握している影響度を設定することにより、エンドポイントの信頼スコアをカスタマイズできるようになりました。ソースに対して設定した影響度に基づいて、エンドポイントの全体的な信頼スコアが再計算されます。これにより、ある異常について、システム生成の信頼スコアに関係なく、ユーザーがその信頼度を決定できます。

（注） 認証方式 EAT-TLS およびポスチャ非準拠エンドポイントの場合、影響度を変更しても、信頼度は同じままです。信頼度は、MAB 認証の場合にのみ変更されます。

（注） 使用する認証方式によって得られる高い信頼スコアは、その認証方式の影響度を変更しても低下しません。認証方式の影響度が増大した場合、エンドポイントでは、その新しいセッションが受信されない限り、現在の信頼スコアを保持し続けます。

手順

ステップ 1 メインメニューから次を選択します。**[Policy]** > **[AI Endpoint Analytics]** > **[Overview]** > **[Manage Sources]** の順に選択します。
[Trust Analytics] ウィンドウが開きます。

ステップ 2 [Customize Impact Level] をクリックします。

ステップ 3 [Let's Do It] をクリックします。
[Customize Trust Score Sources] ワークフローが開始されます。ワークフローウィンドウの下部にある [Exit] オプションをクリックすると、いつでもワークフローを終了できます。

ステップ 4 影響度を変更するソースの横にあるチェックボックスをオンにします。

ステップ 5 [More Actions] ドロップダウンリストから [New Impact Level] を選択します。

ステップ 6 [Next] をクリックします。

次のウィンドウでは、個々のエンドポイントに対する信頼スコアのカスタマイズの影響を示す、以前の信頼スコアと新しい信頼スコアの比較調査が提供されます。この円グラフには、ソースの影響レベルの変化による影響を受けたかどうかに関係なく、ネットワーク内のすべてのエンドポイントが含まれています。下の [Endpoints (After)] テーブルには、影響度構成の変更の結果として影響を受けた各エンドポイントの新しい信頼スコアが表示されます。

ステップ 7 [Next] をクリックします。

各ソースの新しい影響度を示す概要が表示されます。結果に満足できない場合は、[Edit] をクリックしてワークフローに戻り、信頼スコアの影響度を編集します。

ステップ 8 [Next] をクリックします。

エンドポイントの信頼スコアが更新され、Cisco ISE にも送信されます。これにより、Cisco ISE が信頼スコアベースの認証ポリシーを使用している場合、該当するエンドポイントの認可変更が生じる可能性があります。

次のタスク

[ポリシー（Policy）] > **[AIエンドポイント分析（AI Endpoint Analytics）]** > **[信頼スコア（Trust Score）]**で、エンドポイントの新しい信頼スコアを確認します。

アラートのリセットの設定

一定期間非アクティブになった後にアラートを手動または自動でリセットできます。デフォルトでは、サポートされているすべてのソースのリセットアクションは手動に設定されています。ここで説明されているグローバル構成ワークフローを使用して、アラートをリセットするように構成できます。

手順

ステップ 1 メインメニューから次を選択します。**[Policy]** > **[AI Endpoint Analytics]** > **[Manage Sources]** の順に選択します。

[Trust Analytics] ウィンドウが開きます。

ステップ 2 [Alert Configuration] をクリックします。

ステップ 3 [Choose Reset Alert Type] ウィンドウで、[Let's Do It] をクリックします。

ワークフローウィンドウの下部にある [Exit] オプションをクリックすると、いつでもワークフローを終了できます。

ステップ 4 [Reset Alert Type] ドロップダウンリストから、[Manual] または [Customize reset timer after alert inactivity] を選択します。

ステップ 5 [Customize reset timer after alert inactivity] を選択した場合は、非アクティブなときにアラートをリセットするまでの日数（0 ～ 365 日）または時間数（0 ～ 24 時間）を入力します。

ANC ポリシーを削除するか、保持するかを選択できます。複数の信頼スコアソースからの信頼値がエンドポイントにある場合、[Remove ANC Policy] チェックボックスがオンになっていても、ANC ポリシーは削除されません。

ステップ 6 [Next] をクリックします。

ステップ 7 手順 4 で選択した設定を適用するすべてのソースの横にあるチェックボックスをオンにします。

ステップ 8 [Apply] をクリックします。

[Trust Analytics] ウィンドウからローカルでアラートをリセットするように構成することもできます。アラートのリセットを構成するソースを選択します。右側のスライドインウィンドウで、適切な設定を選択し、[Save] をクリックします。

（注） アラートのリセット設定オプションは、すべてのソースで使用できるわけではありません。アラートがリセットされると、同じ情報が Cisco ISE に伝達されます。

アラートは、更新のために 30 分ごとにチェックされます。また、チェック中に、アラートのリセット構成で設定された期間が経過した場合、その異常について信頼スコアがリセットされます。アラートのリセットのステータスは、監査ログに表示されます。

エンドポイント パージ ポリシー

定義された時間にわたって非アクティブだったエンドポイントをネットワークから削除するには、エンドポイント パージ ポリシーを定義します。エンドポイントを削除する必要があるまでの非アクティブ期間を定義できます。また、プロファイリング属性に基づいて特定のエンドポイントのセットに作用するようにパージポリシーをカスタマイズすることもできます。パージポリシーは毎日午前2時（サーバー時間）に実行され、定義されたパージ要件を満たすエンドポイントがネットワークから削除されます。

Cisco AI エンドポイント分析にインポートされた登録済みエンドポイントおよび静的エンドポイントは、エンドポイント パージ ポリシーの影響を受けません。

Catalyst Centerのバックアップ/復元操作、およびエンドポイント パージアクティビティを同時に実行することはできません。バックアップ/復元操作が午前 2 時に進行中の場合、パージアクティビティは開始されません。エンドポイント アクティビティの進行中にバックアップ/復元操作が開始されると、エンドポイントパージの実行は停止され、パージアクティビティは未完了のままになります。残りのエンドポイントは、次のパージが翌日の午前2時（サーバー時間）に実行されるまで処理されません。

エンドポイント パージ ポリシーを表示、編集、または追加するには、メニューアイコンをクリックして次を選択します。 **[Policy]** > **[AI Endpoint Analytics]** > **[Configurations]** > **[Endpoint Purge Policy]**の順に選択します。デフォルトでは、次のポリシーを使用できます。

- **Default**
- **Random MAC Default**

これらのデフォルトポリシーは編集できません。有効または無効にすることだけが可能です。

[Purge Now] オプションを使用すると、午前 2 時まで待つのではなく、すぐにパージポリシーを実行できます。[Purge Now] オプションを使用するには、次の 2 つの方法があります。

- すぐに実行する必要があるパージポリシーを選択し、[More Actions] ドロップダウンリストから [Purge Now] を選択します。
- すぐに実行する必要があるパージポリシーの [Actions] 列の下にあるアイコンをクリックし、[Purge Now] を選択します。

パージポリシーの作成

手順

ステップ 1 メインメニューから次を選択します。**[Policy]** > **[AI Endpoint Analytics]** > **[Configurations]** > **[Endpoint Purge Policy]**の順に選択します。

ステップ 2 [Add Endpoint Purge Policy] をクリックします。

ステップ 3 [Add Endpoint Purge Policy] ダイアログボックスで、[Let's Do It] をクリックしてワークフローに直接移動します。

ステップ 4 [ポリシーの詳細の定義（Define Policy Details）] ウィンドウで、次の手順を実行します。

1. ポリシーの名前を [Rule Name] フィールドに入力します。
2. [Select Status] ドロップダウンリストで [Enabled] または [Disabled] を選択します。
3. エンドポイントがパージされるまでの非アクティブ時間を定義します。[Elapsed Greater than or Equal to] フィールドに値（日単位）を入力してください。有効な値の範囲は 5 ー 180 日です。

ステップ 5 （オプション）[Define Additional Policy Conditions] ウィンドウで、このパージポリシーの影響を受けるエンドポイントをフィルタ処理するためのプロファイリング属性を選択します。選択する属性の横にあるチェックボックスをオンにして、その属性に関して表示されるドロップダウンリストで必要な値を選択してください。

ステップ 6 [Summary] ウィンドウに、パージポリシーの設定が表示されます。表示される詳細情報を確認し、[Done] をクリックしてポリシーを作成します。

次のタスク

エンドポイント パージ アクティビティの監査ログ

エンドポイント パージ ポリシーを有効にして、パージアクティビティが実行された後に、監査ログを確認することができます。詳細については、Cisco Catalyst Center 管理者ガイド [英語] の「**View Audit Logs**」を参照してください。

エンドポイントサブネット検査の設定

展開内では、アクセスレイヤにあるデバイスとアクセスレイヤよりも上にあるデバイスの IP サブネットが異なります。シスコの TTA デバイスの場合、エンドポイント プロファイリングの精度は、Cisco AI エンドポイント分析によってサウスバウンドトラフィックのみが分析される場合に最大になります。エンドポイントプロファイリングを向上させるには、Cisco AI エンドポイント分析 で分析する必要がある特定の IP サブネットまたはサブネット範囲を設定します。

その後、このフィルタ処理されたサブネットに関する設定は、Cisco SD-AVC サーバーと共有されます。この設定は、Cisco SD-AVC サーバーを介して Cisco TTA デバイスに適用されます。

手順

ステップ 1 メインメニューから次を選択します。**[Policy]** > **[AI Endpoint Analytics]** > **[Configurations]** > **[Endpoint Subnet Inspection]**の順に選択します。

ステップ 2 [IP Subnet] フィールドに必要な値を入力します。

ステップ 3 [+] をクリックして IP サブネットを追加します。このウィンドウでは、複数のサブネットまたはサブネット範囲を追加できます。

エンドポイント インベントリ

[Endpoint Inventory] タブには、設定されたデータソースを介して Cisco AI エンドポイント分析に接続されているエンドポイントの詳細が表示されます。このビューには、接続されているすべてのエンドポイントのプロファイリング情報が表示されます。

表示するエンドポイントのプロファイリング情報を選択するには、テーブルの右上隅にある垂直省略記号アイコンをクリックします。次のプロファイリング情報セットのいずれかを選択し、[適用（Apply）] をクリックします。

- [All]：使用可能なすべてのプロファイリング情報が表示されます。このセットは編集できません。
- [General]：これを選択すると、エンドポイントの全体図を確認できるプロファイリング情報が表示されます。これは、デフォルトで表示される列のセットです。このセットは編集できません。
- [Detailed]：これを選択すると、エンドポイントを深く洞察できるプロファイリング情報が表示されます。このセットは編集できません。
- [Custom]：これは編集可能な唯一のセットです。[Endpoint Inventory] ウィンドウに表示するプロファイリング情報をオンまたはオフにします。

必要な [View Known Profiles] ボタンをクリックして、[All Endpoints] ビューに表示されるエンドポイントのリストをフィルタ処理することもできます。**エンドポイントタイプ**、**ハードウェア製造元**、**ハードウェアモデル**、および **OS タイプ**でエンドポイントのリストをフィルタ処理できます。

表示されるエンドポイント インベントリ テーブルを編集またはカスタマイズするには、テーブルの上部の右隅にある歯車アイコンをクリックします。表示されるペインには、[テーブルの外観（Table Appearance）]、[テーブルの列の編集（Edit Table Columns）]、および [カスタムビューの編集（Edit Custom Views）] メニューが含まれており、テーブルビューや、テーブルに表示する情報を選択したり、カスタムビューを作成したりできます。

[Apply] をクリックして変更を保存するか、[Reset All Settings] をクリックしてエンドポイント インベントリ テーブルのデフォルト設定を適用します。

要件に基づいて一連のエンドポイントを簡単にフィルタ処理できます。テーブルの上部にある検索バーを使用すると、フィルタパラメータを簡単に見つけることができます。入力して検索支援機能を使用するか、表示されるドロップダウンをスクロールして必要なパラメータを見つけて選択することができます。

ほとんどの列にはクイックフィルタが含まれています。一部のフィルタでは値を選択できるドロップダウンメニューが表示され、一部のフィルタは入力可能なテキストフィールドです。

エンドポイントを登録したり、登録済みのエンドポイントを編集、削除、およびプロファイリングしたりできます。単一または複数のエンドポイントを選択するには、MAC アドレスの横にあるチェックボックスをオンにします。これにより、選択したエンドポイントに対して、[Actions] ドロップダウンリストから特定のアクションをフィルタリングして実行することができます。

登録済みのエンドポイント、未登録のエンドポイント、および他のソースから学習したエンドポイントを削除できます。エンドポイントを選択すると、テーブル内のすべての行を選択できるバナー行が表示されます。バナーをクリックすると、バナー行でテーブル内のすべての行をクリアできるようになりました。すべてのエンドポイントを削除するには、バナーをクリックするか、[その他の操作（More Actions）] ドロップダウンリストから [削除（Delete）] オプションを選択します。

エンドポイントのプロファイリングの完全な詳細を表示するには、エンドポイントの [MAC Address] をクリックします。表示されるスライドイン ダイアログボックスには、ユーザーの詳細、エンドポイントの詳細、およびエンドポイントの属性の詳細が含まれます。

[詳細（Details）] タブに次のフィールドが表示され、Cisco ISEから受信した詳細が示されます。

- [Authentication Status]：このフィールドには、エンドポイントが Cisco ISE で認証された場合は [Started]、そうでない場合は [Disconnected] と表示されます。
- [Authorization Profile]：Cisco ISE のエンドポイントに設定されている認証ポリシーがここに表示されます。
- [Security Group Tag]：Cisco ISE でエンドポイントに設定されたセキュリティグループタグがここに表示されます。

これらの属性の詳細については、使用する Cisco ISE リリースの Cisco ISE 管理者ガイド [英語] を参照してください。

エンドポイントの詳細を示すスライドイン ダイアログボックスに [Trust Score] タブがあります。このタブには、エンドポイントの信頼スコアを示すさまざまな要因の詳細が表示されます。エンドポイントの信頼スコア （1552 ページ）を参照してください。

[Details] タブに [Previous MAC Addresses] エリアがあり、MAC ランダム化機能が有効になっているエンドポイントで使用された MAC アドレスが表示されます。ランダムおよび変更 MAC アドレスを持つエンドポイントの信頼スコア （1560 ページ）を参照してください。

Cisco AI エンドポイント分析データのエクスポート

このウィンドウからエンドポイントとエンドポイントの詳細のリストをエクスポートするには、[Export] をクリックします。[Endpoint Inventory] ウィンドウでフィルタを適用すると、フィルタ処理されたエンドポイントのみがエクスポート用に処理されます。すべてのエンドポイントの詳細をエクスポートするには、フィルタが適用されていないことを確認して、[エクスポート（Export）] をクリックします。

[Export] をクリックすると、[Reports] ウィンドウで新しいタブが開きます。[Generated Reports] ウィンドウには、開始されたエクスポートのリストが表示され、リストの一番上に最新のエクスポート要求が表示されます。[エンドポイントインベントリ（Endpoint Inventory）] ウィンドウから生成されたレポートの [テンプレートカテゴリ（Template Category）] 列に [AIエンドポイント分析（AI Endpoint Analytics）] が含まれています。レポートの生成には数分かかります。レポートのダウンロード準備ができると、[Last Run] 列の値が [Not Initiated] から、その横にダウンロードアイコンがあるタイムスタンプに変わります。タイムスタンプは、エクスポートリストが生成された時刻を示します。ダウンロードアイコンをクリックして、エンドポイントのリストの CSV ファイルをシステムにダウンロードします。

次の手順で、[レポート（Reports）] ウィンドウから Cisco AI エンドポイント分析データをエクスポートすることもできます。

（注） エンドポイントの AI エンドポイント分析データの最初のエクスポートは [Endpoint Inventory] ウィンドウから実行する必要があります。その後、[Reports] ウィンドウから直接 AI エンドポイント分析レポートを生成できます。

手順

ステップ 1 メインメニューから次を選択します。**[Reports]** > **[Report Templates]** > **[AI Endpoint Analytics]** の順に選択します。

ステップ 2 タスクの概要ウィンドウが表示されたら、[Let's Do It] をクリックして、ワークフローに直接移動します。

（注） 今後この画面をスキップするには、[Don't show this to me again] チェックボックスをオンにします。

ステップ 3 **[レポートテンプレートの選択（Select Report Template）]** ウィンドウでは、[エンドポイントプロファイリング（Endpoint Profiling）] テンプレートがデフォルトで適用されます。

ステップ 4 **[レポート範囲の設定（Setup Report Scope）]** ウィンドウで、次の手順を実行します。

a) [Report Name] フィールドに名前を入力します。

b) [Endpoint Inventory] ウィンドウからエクスポートするエンドポイントのリストに適用するフィルタを定義します。

c) すべてのエンドポイントの詳細をエクスポートするには、[Scope]エリアで値を選択しないでください。

ステップ 5 [Select File Type] ウィンドウの [Client Details] エリアで、選択したパラメータを確認できます。関連するフィールドの横にあるチェックボックスをオンまたはオフにして、エクスポートする情報を編集します。

ステップ 6 [Schedule Report] ウィンドウで、[Run Now]、[Run Later]（[One-Time] または [Run Recurring]）オプションボタンをクリックします。

（注） [Run Later] の [One-Time] および [Run Recurring] オプションには、エクスポートの時間を定義するスケジューリングフィールドが表示されます。

ステップ 7 [Delivery and Notification] ウィンドウでは、[Email Report] チェックボックスをオンにしないでください。

ステップ 8 [Summary] ウィンドウで、すべての設定を確認します。変更するには、[Edit] をクリックします。

ステップ 9 生成されたレポートのリストを表示するには、このウィンドウの [View Reports] リンクをクリックします。レポートが生成され、このウィンドウに表示されるまで数分かかります。

エンドポイントのフィルタ処理

次の手順を使用して、プロファイリングデータ、プライマリ プロファイリング ラベル、既知のプロファイル、および正常性ステータスに基づいてエンドポイントをフィルタ処理します。

手順

ステップ 1 [Endpoint Inventory] ウィンドウで、[Filter] をクリックします。

ステップ 2 必要に応じて、対応するドロップダウンリストから値を選択するか、必要な値のオプションボタンをクリックするか、特定のフィールドの必要な値の横にあるチェックボックスをオンにして、次のフィルタを定義します。

- **Profile Status Condition**
- **Mac Address**
- **Is Random Mac**
- **Trust Score**
- [IP Address]
- **Last Seen**
- **Host Name**
- **Endpoint Type**
- **OS Type**
- **Hardware Model**

- **Hardware Manufacturer**
- **Registered**

ステップ 3 [Apply] をクリックします。

また、4 つのプライマリ プロファイリング ラベルで表示されるプロファイリング済みのエンドポイントをフィルタ処理することもできます。[View Known Profiles] セクションで 1 つ以上のラベルをクリックします。

エンドポイントの正常性ステータスは 5 分ごとに更新されます。

属性用語集

属性用語集は、Cisco ISE プローブデータから使用可能なすべてのプロファイリング属性のリストです。

すべてのプロファイリング属性を表示するには、次の手順を実行します。

手順

ステップ 1 [Endpoint Inventory] ウィンドウで、エンドポイントの MAC アドレスをクリックします。

ステップ 2 右側に表示される新しい領域で、[View Attribute Glossary] をクリックします。

[属性用語集（Attribute Glossary）] ウィンドウに、属性ごとに次の情報が表示されます。

- キープロファイリング属性
- 説明
- 関連付けられたプロファイルラベル
- ソース
- ディクショナリ
- ディスカバリの方法

用語集では、すべてのプロファイリング属性の詳細ビューが表示されます。プロファイリング属性がプロファイルラベルの作成に頻繁に使用される場合は、そのラベルが [Associated Profile Labels] 列に一覧表示されます。

また、ルールの論理条件の作成中に、[Choose Attribute Condition] ウィンドウに属性用語集を表示することもできます。詳細については、「カスタムルールの作成」を参照してください。

エンドポイントの登録

新しいエンドポイントをオンボードおよびプロファイリングするには、そのエンドポイントを Cisco AI エンドポイント分析に登録します。エンドポイントのプロファイリング情報は、分類のための信頼できる情報源です。また、[Register Endpoint] オプションを使用して、登録済みのエンドポイントの新しいプロファイル情報を更新することもできます。

手順

ステップ 1 **[Actions]** > **[Register Endpoints]** の順に選択します。

ステップ 2 [単一（Single）] または [一括（Bulk）] のいずれかのオプションボタンをクリックして、単一のエンドポイントまたは複数のエンドポイントを登録するかどうかを選択します。

a) [Single] オプションボタンをクリックしたら、エンドポイントの [MAC Address]、[Endpoint Type]、[Hardware Model]、および [Hardware Manufacturer] を入力します。

b) [一括（Bulk）] オプションボタンをクリックしたら、次の手順を実行します。

1. [Download .csv Template] オプションをクリックして、.csv テンプレートをダウンロードします。
2. ダウンロードした .csv ファイルに、登録する必要がある各エンドポイントの詳細を入力します。具体的には、MAC アドレス、エンドポイントタイプ、ハードウェアモデル、およびハードウェア製造元です。このファイルを保存します。
3. [Choose a File] オプションを使用して .csv ファイルをアップロードします。

[Bulk] オプションを使用すると、一度に最大 500 個のエンドポイントを登録できます。

ステップ 3 [Review Endpoint] ウィンドウでエンドポイントの詳細を確認します。変更するには、[Edit] をクリックします。

（注） 既存のエンドポイントの登録中は、エンドポイントのプロファイルラベルの変更が紫色で反映され、編集できます。

ステップ 4 [Next] をクリックして、登録プロセスを続行します。

ステップ 5 [登録（Register）] をクリックします。

登録済みエンドポイントの編集

登録済みのエンドポイントのプロファイリング情報は、[Endpoint Inventory] ウィンドウから更新できます。

手順

ステップ 1 編集するエンドポイントの MAC アドレスの横にあるチェックボックスをオンにします。
ステップ 2 [Actions] をクリックします。
ステップ 3 [Edit Endpoint] をクリックします。
ステップ 4 [Endpoint Type]、[Hardware Model]、[Hardware Manufacturer] に詳細を入力します。
ステップ 5 [Save] をクリックします。

登録済みエンドポイントの削除

登録済みのエンドポイントがネットワークの一部ではなくなった場合は、Cisco AI エンドポイント分析から削除できます。

手順

ステップ 1 削除するエンドポイントの MAC アドレスの横にあるチェックボックスをオンにします。
ステップ 2 [Actions] をクリックします。
ステップ 3 [Delete Endpoint] をクリックします。

次のメッセージが表示されます。

「Do you really want to delete the selected endpoint(s)?」

ステップ 4 [Yes] をクリックして、Cisco AI エンドポイント分析からエンドポイントを完全に削除します。

信頼得点

[信頼スコア（Trust Score）] ウィンドウは、次の 2 つの表形式セクションで構成されています。

[Alerts]：

異常や脆弱性が原因で逸脱が発生した場合、またはエンドポイント接続やインターフェイスに弱点が見つかった場合にアラートが表示されます。これらのアラートは、信頼スコアに悪影響を与える検出（MAC アドレスの同時検出、NAT モード、またはその他の信頼できない変更など）があったことを表しています。アラートを監視することで、ネットワーク内の最も緊急のリスクに迅速に対処できます。

[Alerts] タブには、ネットワーク内のエンドポイントが受信したさまざまなアラートが表示されます。以前は、エンドポイントが受信したアラートのタイプを確認するために各エンドポイ

ントの詳細を個別に確認する必要があり、他のどのエンドポイントが同じアラートを受信したかを知る方法はありませんでした。今では、特定のタイプのアラートを受信したすべてのエンドポイントがわかるようになりました。アラートをクリックすると、このアラートを受信したエンドポイントのリストを表示できます。さらに各エンドポイントをクリックすれば、詳細を表示できます。アラートは、次に示す 3 つの状態のいずれかになります。

- [Open]：エンドポイントで最初に検出されたアラートはオープン状態であり、解決または後で対処するためのユーザーによるアクションが必要になります。
- [Disabled]：オープンアラートに対してアクションを実行しない場合は、アラートを無効状態に移行できます。アラートを任意の期間、さらには無期限に無効にすることができます。この期間中は、このアラートで新しいエンドポイントが検出されても、アラートは無効状態のままです。
- [Reset]：アラートに対してすぐにアクションを実行しない場合は、アラートをリセット状態に移行できます。リセット後に別のエンドポイントでこのアラートが検出されると、アラートはオープン状態に戻ります。

[Endpoint]：

このビューには、エンドポイントの全体的な信頼スコアを示すさまざまな要因の列が表示されます。信頼スコアは、動作異常が検出されたエンドポイントを特定するために役立ちます。これにより、エンドポイントの詳細情報を調べて、必要な修復アクションを実行することができます。低い信頼スコアを管理するためにエンドポイントに ANC ポリシーを適用する場合、[Trust Score] ビューには、適用された ANC ポリシーの名前とポリシーが適用された日時も表示されます。エンドポイントの信頼スコア （1552 ページ）を参照してください。

オプションの [Reset Trust Score] を使用すると、一度に複数のエンドポイントをリセットできるようになりました。ただし、パフォーマンスの問題を避けるために、最大 10 個のエンドポイントまでという上限があります。エンドポイントのリセット時には、監査目的で、アクションの正当化が必要になります。エンドポイントがリセットされると、そのエンドポイントの信頼スコアとそのエンドポイントに適用されていた ANC ポリシーがクリアされます。

エンドポイントの信頼スコア

Cisco AI エンドポイント分析は、エンドポイントに信頼スコアを割り当てます。これにより、ネットワーク内の潜在的に危険なエンドポイントを簡単にモニターして対処することができます。異常な動作がモニタおよび追跡され、追跡された異常の数と頻度に基づいて信頼スコアが割り当てられます。

信頼スコアの計算に含める必要があるソースを選択するには、Cisco AI エンドポイント分析の **[概要（Overview）]** ウィンドウで、**[設定（Configuration）]** > **[信頼分析（Trust Analytics）]** の順に選択します。ソースをクリックすると、スライドイン構成ウィンドウが右側に表示されます。トグルボタンをクリックしてソースを有効にします。

Cisco AI エンドポイント分析は、次の要因に基づいて履歴信頼スコアを生成します。

- エンドポイントに関連付けられた異常の履歴（このエンドポイントに関して検出された異常の数）。

- エンドポイントで検出された各異常の重大度。

エンドポイントの全体的な信頼スコア計算に次の異常が考慮され、検出された異常ごとにスコアが表示されます（対応するソースが有効になっている場合）。

- **AI スプーフィング検出**

  Cisco AI エンドポイント分析 は、NetFlow テレメトリデータ、および Cisco ISE デバイスと SD-AVC デバイスからのネットワークプローブデータを分析して、スプーフィングされたエンドポイントを検出します。NetFlow コレクタサーバーの構成方法の詳細については、テレメトリを使用した syslog、SNMP トラップ、NetFlow コレクタサーバー、および有線クライアントデータ収集の設定 （59 ページ）を参照してください。Catalyst Center トラフィック テレメトリ アプライアンスからのプローブおよび NetFlow データ（DN-APL-TTA-M）も分析されます。Catalyst Center トラフィック テレメトリ アプライアンスへのトラフィックの受信スパンを構成して、Cisco AI エンドポイント分析でエンドポイント トラフィック データを スプーフィング検出に使用できるようにします。

  各エンドポイントタイプには、機械学習アルゴリズムを使用して開発された動作モデルがあります。エンドポイントに対して受信されたデータに基づき、エンドポイントの動作がエンドポイント タイプ プロファイルで予期されていない動作の場合、エンドポイントには [AI Spoofing Detection] 領域で低い信頼スコアが割り当てられます。エンドポイントで使用されるアプリケーションおよびサーバーポートは、このスプーフィング検出プロセスで分析されます。たとえば、プリンタとしてプロファイリングされたエンドポイントがビデオ通話アプリケーションを使用する場合、スプーフィングされたエンドポイントとして識別され、信頼スコアが割り当てられます。

  エンドポイントは、Catalyst Center の管理対象スイッチの MAC アドレスによって識別されます。NAT の使用、仮想マシンまたはコンテナの実行など、単一の MAC アドレスを使用する複数のエンドポイントは、Cisco AI エンドポイント分析でサポートされている構成ではありません。

  AI スプーフィング検出は、次のデバイスタイプをカバーしています。

  - IP 電話
  - プリンタ
  - カメラ
  - 次のハードウェアモデル属性を持つビルディング オートメーション デバイス：
    - Automated-Logic-Device
    - Honeywell-Device
    - Johnson-Controls-Device
    - Rockwell-Automation-Device
    - Schneider-Electric-Device
    - Siemens-Automation-Device
    - Siemens-Building-Device

- Trane-Device

- TelePresence：
  - 次のいずれかのハードウェアモデルを持つエンドポイント：
    - Cisco-Tandberg-Device
    - Cisco-TelePresence
    - Cisco TelePresence SX80
    - Cisco Telepresence SX20
    - Cisco-Collaboration-Room-Endpoint
    - Poly-Device
  - デバイスタイプがビデオ会議のエンドポイント

- **エンドポイント属性の競合**

  デバイスがネットワークに参加し、デバイスがアクティブであるときに定期的にプローブを実行すると、エンドポイントのプロファイリングデータが継続的にモニタされ、更新されます。エンドポイントから受信したプロファイリングデータにおける特定の変化は、Cisco AI エンドポイント分析 で異常としてフラグが付けられます。たとえば、エンドポイントが最初に Linux デバイスとしてプロファイルされ、その後で macOS デバイスとしてプロファイルされた場合、これは重大度の高い異常としてフラグが付けられます。エンドポイントの [Endpoint Attribute Conflict] 列にスコアが割り当てられ、エンドポイントの全体的な信頼スコアもこの変化を反映して更新されます。

  ただし、macOS のバージョンに変化があり、エンドポイントが新しいリリースから古いリリースにダウングレードされたように見える場合、そのような変化は優先順位の低い異常としてフラグが付けられ、対応するスコアがそれに応じて更新されます。

- **NAT モード検出**

  ネットワーク内に NAT 対応ルータがある場合、NAT ルータに接続されたエンドポイントは、特定のエンドポイントの IP アドレスまたは MAC アドレスではなくルータの IP アドレスまたは MAC アドレスによって認識されます。NAT 対応ルータに関する情報は、接続先の Cisco Catalyst 9000 シリーズ デバイスから収集されます。

- **同時 MAC アドレス**

  同じ MAC アドレスを共有し、Cisco Catalyst 9000シリーズ デバイスに接続されているエンドポイントを特定してください。共有 MAC アドレスを持つエンドポイントには、同時 MAC アドレススコアが割り当てられます。これにより、容易に、それらのエンドポイントを識別して詳細情報を調べることができます。

- **セキュリティ センサー**

  セキュリティ センサー スキャン機能を使用すると、特定の Cisco Catalyst 9000 シリーズ スイッチにアクティブプローブをインストールし、開いていると想定されていないのに開

いているポート、クレデンシャルの脆弱性、またはその両方についてエンドポイントをスキャンするように Cisco AI エンドポイント分析 を設定できます。

エンドポイントの信頼スコアは、Cisco ISEから収集されるイベントによっても通知されます。Cisco ISE を介して認証するすべてのエンドポイントは、次のイベントに基づいて初期信頼スコアを受け取ります。

- **認証方式**
- **ポスチャ**

（注） Cisco Catalyst 9000 シリーズ デバイスからデータを受信する信頼スコアソースの場合、デバイスで CBAR を有効にし、デバイスを Cisco IOS-XE リリース 17.6 以降にアップグレードする必要があります。

[エンドポイントインベントリ（Endpoint Inventory）] ウィンドウに表示される信頼スコアは、エンドポイントの異常の履歴とシビラティを考慮した全体的な信頼スコアです。[MAC Address] をクリックすると、エンドポイントに割り当てられた信頼スコアの原因の詳細情報が表示されます。たとえば、エンドポイントに関して低レベルの異常が検出され、これが異常の唯一のインスタンスである場合、エンドポイントの全体的な信頼スコアは 9 になります。

複数の低レベルの異常が検出された場合は、異常の数を考慮して全体的な信頼スコアがさらに低下します。

割り当てられる信頼スコアの範囲は 1 ー 10 で、次の表のように分類されます。

信頼スコアカテゴリ	範囲	エンドポイントの脅威レベル
低	1 〜 3	高
中規模	4 〜 6	中程度
高	7 〜 10	低

その後、Cisco ISE から適応型ネットワーク制御（ANC）ポリシーを適用して、エンドポイントで適切な修復アクションを実施することができます。*Cisco ISE* の管理者ガイドで「Maintain and Monitor」の章にある「Adaptive Network Control」を参照してください。

ANC ポリシーは、Cisco ISE で定義され、選択したエンドポイントに修復アクションを適用することを可能にします。ANC ポリシーを適用して、エンドポイントを隔離またはシャットダウンしたり、エンドポイントのポートをバウンスしたり、エンドポイントの再認証を強制的に実行することができます。Cisco AI エンドポイント分析で望ましくない信頼スコアを持つエンドポイントに ANC ポリシーを適用すると、認可変更（CoA）が Cisco ISE からそのエンドポイントに送信されます。

エンドポイントは、MAC アドレスによって識別されます。Cisco ISE は、ANC 適用時点で識別された MAC アドレスに関してアクティブセッションを保持しているエンドポイントに CoA を送信します。その時点で Cisco ISE においてアクティブセッションを持たない、同じ MAC ア

ドレスのエンドポイントは、新しいセッションが開始されたときに、または設定された再認証タイマーの終了時に再認証する必要がある場合に、ANC ポリシーと照合されます。

ANC ポリシーが適用されているエンドポイントを確認するには、Cisco ISE 管理ポータルにログインします。メインメニューから、**[Operations]** > **[RADIUS]** > **[Live Sessions]** の順に選択します。[Endpoint ID] 列に、スプーフィングされたエンドポイントの MAC アドレスを入力します。これにより、同じ MAC アドレスを共有し、現在 Cisco ISE でライブセッションを持つエンドポイントがフィルタ処理されます。これらが、ANC ポリシーの影響を受けるエンドポイントです。

Cisco ISE で RADIUS セッションの履歴ログを表示するには、メインメニューから、**[Operations]** > **[Reports]** > **[Reports]** > **[Endpoints and Users]** > **[RADIUS Authentications]** の順に選択します。

Cisco ISE でエンドポイントへの ANC ポリシーの適用を表示または変更するには、メインメニューから、**[Context Visibility]** > **[Endpoints]** の順に選択します。必要に応じて、エンドポイントの MAC アドレスの横にあるチェックボックスをオンにして、リストの上部に表示されるオプションをクリックしてください。

前提条件

エンドポイントの信頼スコアを受信するための前提条件：

- Cisco ISE がオンプレミス Catalyst Center に接続されている。
- ネットワーク アクセス デバイスが、Cisco Catalyst Assurance と Cisco ISE の両方によって管理されている。

（注） Cisco Catalyst Assurance では 500 台の NetFlow エクスポータのみサポートされるため、エンドポイント スプーフィング検出機能は、NetFlow エクスポートフローで最大 500 台のネットワーク アクセス デバイスをサポートします。

- ネットワーク アクセス デバイスに接続されているエンドポイントが、Cisco ISE を介して認証されている。
- [Trust Score Sources] ウィンドウ（**[Policy]** > **[AI Endpoint Analytics]** > **[Configurations]** > **[Trust Analytics]**）で、信頼スコアの計算に必要なソースが有効になっている。

エンドポイント属性の競合

Cisco AI エンドポイント分析では、エンドポイントの正確なプロファイルラベルを取得するために、さまざまなソースから複数のプローブのデータが継続的に収集されます。Cisco AI エンドポイント分析では、次のソースから、次のデータが収集されます。

Cisco ISE から：

- RADIUS プローブ

- ディレクトリからのユーザーの詳細情報
- VPN の詳細情報（AnyConnect の可用性などの）
- オプションで、ポートフォワーディングが設定されている場合のその他のデータ（DHCP の詳細情報など）

スイッチから：

- デバイス接続メッセージ（DHCP メッセージや NetBIOS メッセージなど）
- ディープ パケット インスペクション
- スイッチテレメトリ

Cisco AI エンドポイント分析では、これらのソースから受信した情報に基づいてシステムルールが作成されます。デバイスがネットワークに参加し、デバイスがアクティブであるときに定期的にプローブを実行すると、エンドポイントのプロファイリングデータが継続的にモニタされ、更新されます。

エンドポイントから受信したプロファイリングデータにおける特定の変化は、Cisco AI エンドポイント分析で異常としてフラグが付けられます。たとえば、エンドポイントが最初に Linux デバイスとしてプロファイルされ、その後で macOS デバイスとしてプロファイルされた場合、これは重大度の高い異常としてフラグが付けられます。エンドポイントの [Endpoint Attribute Conflict] 列にスコアが割り当てられ、エンドポイントの全体的な信頼スコアもこの変化を反映して更新されます。

ただし、macOS のサブバージョンに変化があり、エンドポイントが新しいリリースから古いリリースにダウングレードされたように見える場合、そのような変化は優先順位の低い異常としてフラグが付けられ、対応するスコアがそれに応じて更新されます。

[Endpoint Inventory] ウィンドウで、**[Endpoint Attribute Conflict]** スコアを持つエンドポイントの MAC アドレスをクリックすると、記録されたプロファイリングデータの変化を確認できます。ここにはエンドポイントの新旧のプロファイルが表示されます。プロファイリングの変化が何らかの理由で問題ないと判断できる場合、または検出されたプロファイリングの変化に誤りがあると思われる場合は、エンドポイントの詳細情報の **[Endpoint Attribute Conflict]** エリアで対応するボタンをクリックしてスコアをリセットします。

エンドポイントの詳細情報の [Endpoint Attribute Conflict] エリアにあるトグルボタンをクリックすることにより、特定のエンドポイントに関してエンドポイント属性の競合の検出を無効にすることもできます。

影響を受けるエンドポイントが Cisco ISE に接続されている場合は、この異常に関するデータが Cisco ISE に送信されます。このデータは、Cisco ISE 管理者がポリシーを定義するために簡単に使用できるエンドポイント分析ディクショナリ属性として使用できます。

エンドポイント属性の競合の検出は、カスタムルールが適用されているエンドポイントには使用できません。

NAT モード検出

ネットワークアドレス変換（NAT）は、登録されていないIPアドレスを使用してインターネットへ接続するプライベート IP インターネットワークを可能にします。NAT は、ネットワーク全体で1つだけのアドレスを外部にアドバタイズするように設定できます。ネットワーク内に NAT 対応ルータがある場合、NAT ルータに接続されたエンドポイントは、特定のエンドポイントの IP アドレスまたは MAC アドレスではなくルータの IP アドレスまたは MAC アドレスによって認識されます。NAT 対応ルータに関する情報は、接続先の Cisco Catalyst 9000 シリーズ デバイスから収集されます。

NAC 対応ルータとして機能するデバイスは、不正なエンドポイントをネットワークに接続させる可能性があるため、NAT 検出が信頼スコアの計算に含まれます。NAT モード検出スコアが割り当てられているエンドポイントの場合は、[Endpoint Inventory] タブで MAC アドレスをクリックすると、スライドインウィンドウにエンドポイントの詳細情報が表示されます。エンドポイントのアイデンティティがネットワーク内の NAT 対応ルータに対応していることが確実な場合は、次の手順を実行します。

1. 詳細情報のスライドインウィンドウの [信頼スコア（Trust Score）] タブで、[NATモード検出（NAT Mode Detection）] をクリックします。
2. トグルボタンをクリックして、この特定エンドポイントの NAT 検出を無効にします。

Cisco Catalyst 9000 シリーズ デバイスに接続された同時 MAC アドレスを持つエンドポイント

同じ MAC アドレスを共有し、Cisco Catalyst 9000 シリーズ デバイスに接続されているエンドポイントを特定してください。同時 MAC アドレスを持つエンドポイントの問題は、有線環境と、有線展開およびワイヤレス展開を含むハイブリッド環境で発生します。ワイヤレス環境では、常時、特定の MAC アドレスを持つエンドポイントは 1 つしかネットワークにアクセスできないため、同時 MAC アドレスは発生しません。

Cisco AI エンドポイント分析では、同時 MAC アドレススコアをエンドポイントに割り当てることにより、同時 MAC アドレスを持つエンドポイントを特定することができます。ネットワーク内で共有 MAC アドレスを持つエンドポイントを検出するには、接続されている Cisco Catalyst 9000 シリーズ デバイスで CBAR を有効にする必要があります。

同じ MAC アドレスを持つデバイスが Cisco Catalyst 9000 シリーズ デバイスに接続すると、それらのエンドポイントは同時エンドポイントとして認識され、その MAC アドレスに低いスコアが割り当てられます。同時 MAC アドレスを持つエンドポイントは、次のデバイスに接続できます。

- 異なる VLAN から同じ Cisco Catalyst 9000 シリーズ デバイス
- 異なる Cisco Catalyst 9000 シリーズ デバイス

表 *68 :* 同時 *MAC* アドレスの問題が発生する環境

展開 1	展開 2	ネットワークで同時 MAC アドレスが発生するか	この環境での同時 MAC アドレス検出のサポート
有線	有線	対応	対応
有線	ワイヤレス	対応	対応
ワイヤレス	有線	対応	対応
ワイヤレス	ワイヤレス	非対応	非対応

[Endpoint Inventory] タブの [Trust Scores] ビューに [Concurrent MAC Address] 列があります。共有 MAC アドレスは異常として検出され、[Concurrent MAC Address] 列に低いスコアが割り当てられます。[MAC Address] をクリックすると、スライドインウィンドウが表示され、その MAC アドレスの詳細情報が示されます。[Concurrent MAC Address] をクリックすると、フィールドが展開され、MAC アドレスのさまざまな送信元に関する情報が表示されます。

[Concurrent MAC Address] エリアの [Network Device Name] 列には、エンドポイントが接続されている Cisco Catalyst 9000 シリーズ デバイスの名前が表示されます。[Interface] 列と [VLAN] 列には対応する値が表示され、エンドポイントがネットワークにどのように接続されているのかを特定するために役立ちます。

Cisco ISE からのポスチャおよび認証値を使用した初期信頼スコアアセスメント

エンドポイントが Cisco ISE を介して認証されると、認証およびポスチャの詳細情報に基づいて、エンドポイントに信頼スコアがただちに割り当てられます。認証方式スコアはデフォルトで割り当てられ、このスコアを無効にすることも、このスコアに対処することもできません。[Configurations] ウィンドウからグローバルレベルで、または [Endpoint Inventory] タブで特定のエンドポイントについて、ポスチャベースのスコアを有効または無効にすることができます。認証方式およびポスチャ値に基づいて割り当てられた信頼スコアが、エンドポイントの初期信頼スコアになります。

その後、このエンドポイントで検出されたその他の異常な動作は、この初期信頼スコアに影響を与え、異常の重大度と数に基づいて信頼スコアを低下させます。

[Endpoint Inventory] タブのエンドポイントの詳細情報に表示される**認証方式**スコアは、使用される認証方式の認識されたセキュリティレベルに基づいています。たとえば、「HTTPS を介した Web 認証」、「証明書ベースの認証」、「セキュアトンネルを使用した認証」などは、高い信頼スコアを得ます。

ポスチャスコアは、接続エンドポイントがポスチャに準拠しているかどうかに基づきます。

エンドポイントの信頼スコアが認証方式スコアのみで構成されている場合、[Reset Trust Score] ボタンは非アクティブになります。認証方式以外の信頼スコアソースにスコアが表示されている場合は、リセットオプションを使用できます。

ランダムおよび変更 MAC アドレスを持つエンドポイントの信頼スコア

プライバシー対策として、モバイルデバイスでは接続先の SSID ごとにランダムおよび変更 MAC アドレスを使用することが増えています。一部のデスクトップ オペレーティング システムは、ユーザーが定期的に MAC アドレスをランダム化する機能も提供しています。つまり、エンドポイントは、異なる SSID に接続するたびに異なる MAC アドレスを提示します。

Cisco AI エンドポイント分析を使用すると、Cisco ISE から「DUID」と呼ばれる（Cisco ISE では「GUID」とも呼ばれます）一意のエンドポイント識別子を受信することにより、ランダムおよび変更 MAC アドレスの問題を処理できます。Cisco AI エンドポイント分析は、MAC アドレスの代わりに、エンドポイントの識別子として DUID を使用します。

Cisco AI エンドポイント分析の [Overview] ウィンドウの [Endpoint MAC Randomization] ダッシュレットには、ネットワーク内のランダムおよび変更 MAC アドレスを使用しているエンドポイントの数がグラフィカルに表示されます。

Cisco ISE に接続され、DUID 情報を使用可能なエンドポイントの場合、この情報は Cisco AI エンドポイント分析にも表示されます。次の列には、Cisco AI エンドポイント分析の [エンドポイントインベントリ（Endpoint Inventory）] ウィンドウで必要になる情報が表示されます。

- [DUID]：エンドポイントの DUID 値。
- [Previous MAC Addresses]：エンドポイントが以前にネットワークへの接続に使用していたランダムおよび変更 MAC アドレス。

DUID 値を使用することで、Cisco AI エンドポイント分析では、エンドポイントを確実に識別し、エンドポイントが以前に使用していたさまざまな MAC アドレスを追跡することが可能になっています。これは、ランダムおよび変更 MAC アドレスを持つエンドポイントの信頼スコアも高精度であることを意味します。以前の MAC アドレスでのエンドポイントの信頼スコアは、エンドポイントが提示している現在の MAC アドレスに引き継がれ、同じエンドポイントに関して受信されたプローブデータの影響を受け続けます。

デバイスで [Private Address] 設定が有効になっている場合、このデバイスの [Is MAC Random] 列に [Yes] という値が表示されます。つまり、このデバイスは、ランダムおよび変更 MAC アドレスとして認識されます。ただし、このデバイスに関して DUID 値を使用できるかどうかは、エンドポイントが Cisco ISE を介して認証されているかどうかと、Cisco ISE でこのエンドポイントの GUID が生成されているかどうかに依存します。

オープンポートとログイン情報の脆弱性を確認するためのセンサースキャン

アクティブなプローブコンテナをインストールして、ネットワーク内のエンドポイントに関する詳細情報を取得します。セキュリティ センサー スキャンを有効にすると、エンドポイントに割り当てられるトラストスコアは、開いているポートとエンドポイントのログイン情報の異常を考慮します。

センサースキャン機能は、次のスイッチでサポートされています。

- Cisco Catalyst 9300 シリーズ スイッチ
- Cisco Catalyst 9400 シリーズ スイッチ

（注） Cisco Catalyst 9800 シリーズ ワイヤレスコントローラは、センサースキャン機能をサポートしていません。

Cisco AI エンドポイント分析は、スイッチで利用可能なアプリケーション ホスティング機能を使用して、開いているポートと弱いログイン情報のスキャンを有効にします。

センサースキャンの有効化と監視

始める前に

- スキャン結果に基づいてエンドポイントポリシーを適用する場合は、Cisco ISE リリース 3.1 以降のリリースに接続します。
- Cisco Catalyst 9300 または 9400 シリーズ デバイスに接続します。
- スイッチが Cisco IOS XE リリース 17.7.1 以降のリリースにアップグレードされていることを確認します。

手順

ステップ 1 Catalyst Center にログインします。

ステップ 2 メインメニューから **[ポリシー（Policy）]** > **[AI エンドポイント分析（AI Endpoint Analytics）]** を選択します。

ステップ 3 表示される **[概要（Overview）]** ウィンドウで、[設定（Configurations）] をクリックします。

ステップ 4 左ペインから、[**Trust Analytics**] を選択します。

ステップ 5 [セキュリティセンサー（Security Sensor）] エリアには、センサースキャン機能を使用して、開いているポートと脆弱なエンドポイントの資格情報を識別するための前提条件が表示されます。このエリアで対応するリンクをクリックして、次のタスクを実行します。

1. Cisco Catalyst 9000 シリーズ デバイスのリリースノートで、サポートされている Catalyst Center および Cisco IOS-XE リリースを確認します。関連する Cisco Catalyst 9000 シリーズ デバイスのセキュリティ センサー コンテナを software.cisco.com からダウンロードします。.tar ファイルがシステムにダウンロードされます。
2. Catalyst Center にアプリケーション ホスティングをインストールします。手順については、アプリケーション ホスティング （1352 ページ）を参照してください。
3. Catalyst Center **[アプリケーションホスティング（App Hosting）]** ウィンドウに .tar ファイルをアップロードします。[セキュリティセンサー（Security Sensor）] エリアに **[アプリケーションホスティング（App Hosting）]** ウィンドウへのリンクが表示されます。
4. センサースキャンを有効にする Cisco Catalyst 9000 シリーズデバイスごとに、.tar ファイルをインストールして有効にします。

Catalyst Center の **[アプリケーション ホスティング（App Hosting）]** ウィンドウで、.tar ファイルを有効にしている Cisco Catalyst 9000 シリーズ デバイスの少なくとも 1 つの [アプリケーションのホスティングステータス（App Hosting Status）] がアクティブであることを確認します。

ステップ 6 前の手順で説明したようにアクティブプローブコンテナをインストールして有効にした後、[Security Sensor] 領域で、Cisco AI エンドポイント分析の信頼スコア設定を構成して、Cisco ISE に接続されているエンドポイントと、アクティブなプローブアプリケーションが有効になっている Cisco Catalyst デバイスで、開いているポートと、脆弱なクレデンシャルをスキャンできます。

- [Open Port Scan] トグルボタンをクリックして、Cisco AI エンドポイント分析がポートスキャンをプロアクティブに実行して、ネットワーク上の定義済みエンドポイントで考えられる脆弱性を検出して解決できるようにします。
- [Credential Vulnerability Scan] トグルボタンをクリックして、ネットワーク上のエンドポイントが脆弱なクレデンシャルを使用している場合に、Cisco AI エンドポイント分析がプロアクティブに検出できるようにして、悪意のあるアクティビティを防止します。

ステップ 7 （任意） 開いているポートのスキャンを有効にすることを選択した場合は、[Open Port Scan] 領域の [Scan Configuration] をクリックしてスキャンを定義できます。

a) [Scan Configuration] ウィンドウの [Defined Scans] タブで、[Define Scan] ボタンをクリックします。
b) ポートのスキャンの範囲を定義できるダイアログボックスが表示されます。
   - エンドポイントの登録時に各エンドポイントをスキャンするには、[On enrollment, scan all endpoints] オプションボタンを選択します。
   - サブネット、プロファイル属性などにより、開いているポートのスキャンの範囲を定義するには、[Create a Custom Scan] オプションボタンを選択します。

   どちらのタイプのポートのスキャンでも、許可されていないポートのリストを定義して、常に閉じておく必要があるポートを指定します。このリストにより、Cisco AI エンドポイント分析はエンドポイントの異常なポートアクティビティを認識し、低い信頼スコアを割り当てることができます。どちらのタイプのポートのスキャンでも、設定できるスキャンの最小頻度は 12 時間です。
c) [Scan Configuration] ウィンドウの [Open Ports List] タブで、スキャンする必要があるポートのタイプと範囲、または個々のポートを指定します。
d) [Scan Configuration] ウィンドウの [Unauthorized Ports] タブで、ネットワーク内の許可されていないポートをポート番号とポートタイプで定義します。Cisco AI エンドポイント分析がこれらのポートをアクティブとして検出した場合、エンドポイントには、許可されていないポートがアクティブである異常に対して低い信頼スコアが与えられます。

ステップ 8 （任意） 脆弱なクレデンシャルの検出を有効にすることを選択した場合は、[Credential Vulnerability Scan] 領域の [Scan Configuration] をクリックしてスキャンを定義できます。この機能では、SSH および TELNET プロトコルがサポートされています。

a) [Credential Vulnerability Scan] ウィンドウの [Scan] タブで、脆弱なクレデンシャルとして識別するクレデンシャルのリストを定義します。企業の要件に従って、脆弱であると見なされるユーザー名とパスワードのリストを定義します。

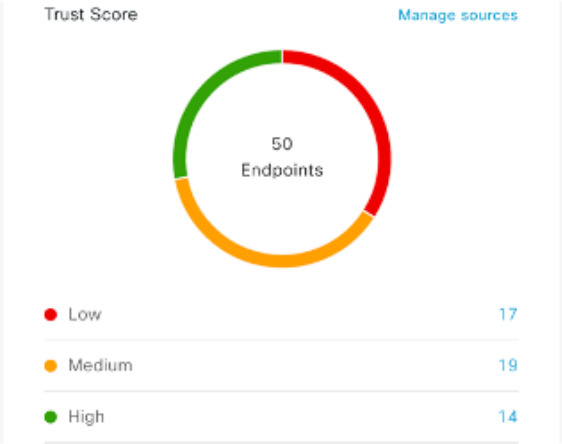
b) [Credentials] タブでは、デフォルトで、3500 を超える脆弱なクレデンシャルのデフォルトリストが利用可能です。このデフォルトリストを使用して、クレデンシャルの脆弱性スキャンを作成できます。脆弱なクレデンシャルの新しいリストを追加するには、[Create New List] をクリックします。

クレデンシャル脆弱性スキャンの設定可能な最小頻度は 12 時間です。

ステップ 9 [Security Sensor] で有効にしたスキャンでは、関連するエンドポイントがスキャンされ、開いているポートまたはクレデンシャルの確認で異常が検出された場合、これらのエンドポイントの信頼スコアがそれに応じて調整されます。[Endpoint Inventory] タブ（該当する場合）では、エンドポイントの [Trust Score] タブに、エンドポイントで開いている許可されていないポート、脆弱なユーザー名、またはその両方のリストが表示されます。

エンドポイントの信頼スコアの表示と管理

図 35 : [Cisco AI Endpoint Analytics Overview] タブの [Trust Score] ダッシュレット



Catalyst Center をアップグレードし、必要な信頼スコアのソースを有効にすると、Cisco AI エンドポイント分析の [Overview] タブ（メインメニュー > **[Policy]** > **[AI Endpoint Analytics]**）に [Trust Scores] ダッシュレットが表示されます。このダッシュレットには、次の情報が含まれます。

- 信頼スコアが割り当てられているエンドポイントの総数。
- 信頼スコアが低、中、および高のエンドポイントの数に関するドーナツグラフおよびリスト。

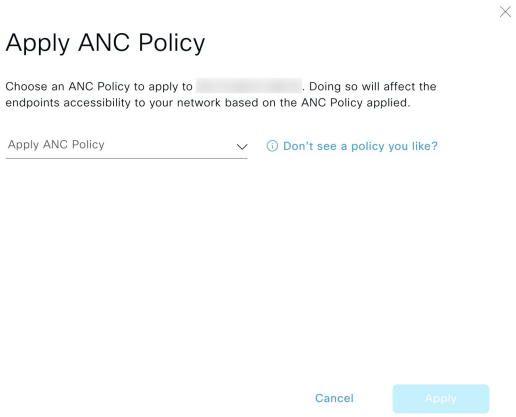
信頼スコアカテゴリのエンドポイントの詳細を表示するには、[Trust Scores] ダッシュレットでエンドポイント数をクリックします。**[エンドポイントインベントリ（Endpoint Inventory）]** タブの [信頼スコア（Trust Score）] ビューが、適切なフィルタが適用されて表示されます。

次の 2 つの方法で信頼スコアを持つエンドポイントを表示できます。

- [Trust Score] タブで、[Endpoints] タブを選択して、信頼スコアが割り当てられているすべてのエンドポイントを表示します。
- [Endpoint Inventory] タブで、表示される警告メッセージの [View endpoints in Trust Score View] をクリックすると、低スコアと中スコアのエンドポイントが表示されます。

信頼スコアのあるエンドポイントでは、次のアクションを実行できます。

- **ANC ポリシーの適用**



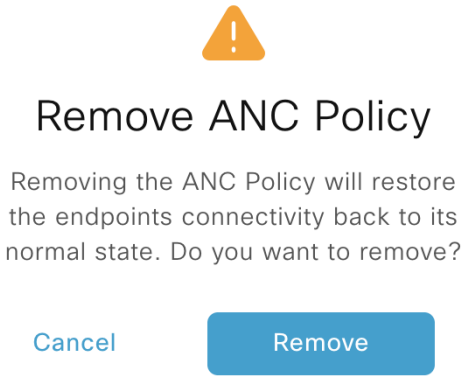
[Apply ANC Policy] ボタンをクリックして、エンドポイントに適用する ANC ポリシーを選択します。ネットワークへのエンドポイントのアクセスは、ポリシーに応じて変更されます。ANC ポリシーは Cisco ISE からインポートされ、表示されるポップアップウィンドウのドロップダウンリストに表示されます。

- **ANC ポリシーの置換**



[Change ANC Policy] ボタンをクリックして、エンドポイントの既存の ANC ポリシーを別の ANC ポリシーに置き換えます。表示されるポップアップウィンドウで、[Change ANC Policy] ドロップダウンリストから適用する新しいポリシーを選択します。

- **ANC ポリシーの削除**



適用された ANC ポリシーをエンドポイントから削除するには、[Remove ANC Policy] ボタンをクリックします。表示されるポップアップウィンドウで、[Remove] をクリックします。これにより、エンドポイントに適用された修復ポリシーが削除され、エンドポイントがネットワークに正常に接続できるようになります。

- **信頼スコアのリセット**

図 *36 : ANC* ポリシーを使用しないエンドポイントの信頼スコアのリセット

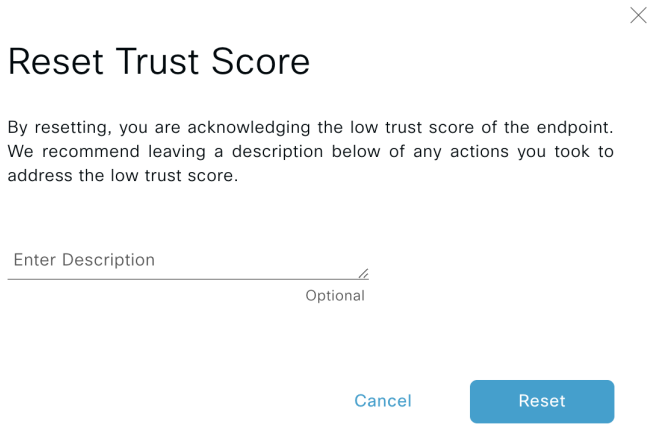
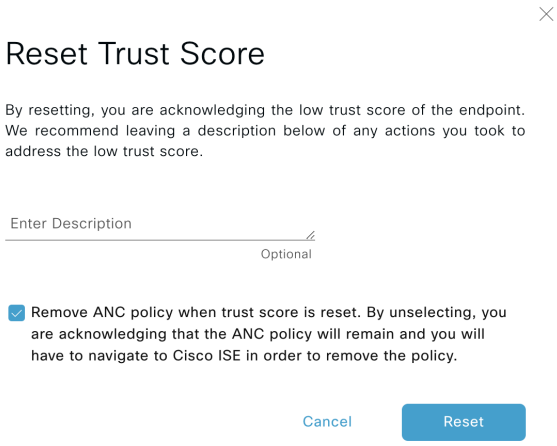


図 *37* : *ANC* ポリシーを使用したエンドポイントの信頼スコアのリセット



信頼スコアインベントリからエンドポイントを削除するには、[Reset Trust Score] ボタンをクリックします。表示されるポップアップウィンドウで、[Reset] をクリックします。

ANC ポリシーの適用後にエンドポイントに対してこのオプションを選択した場合、このエンドポイントは信頼スコアインベントリに再度表示されません。この場合、このようなエンドポイントの ANC ポリシーを変更するには、Cisco ISE からポリシーを削除する必要があります。

ANCポリシーを適用せずにエンドポイントのスコアをリセットした場合、信頼スコアデータの次回の自動更新時に、エンドポイントが信頼スコアインベントリに再度表示されることがあります。

各アクションのボタンは、[エンドポイントインベントリ（Endpoint Inventory）] タブの 2 つの場所に表示されます。アクションは、単一のエンドポイントまたは複数のエンドポイントで実行できます。

- **単一エンドポイントの信頼スコアの管理**

図 *38 : ANC* ポリシーを使用しないエンドポイントの信頼スコアオプション

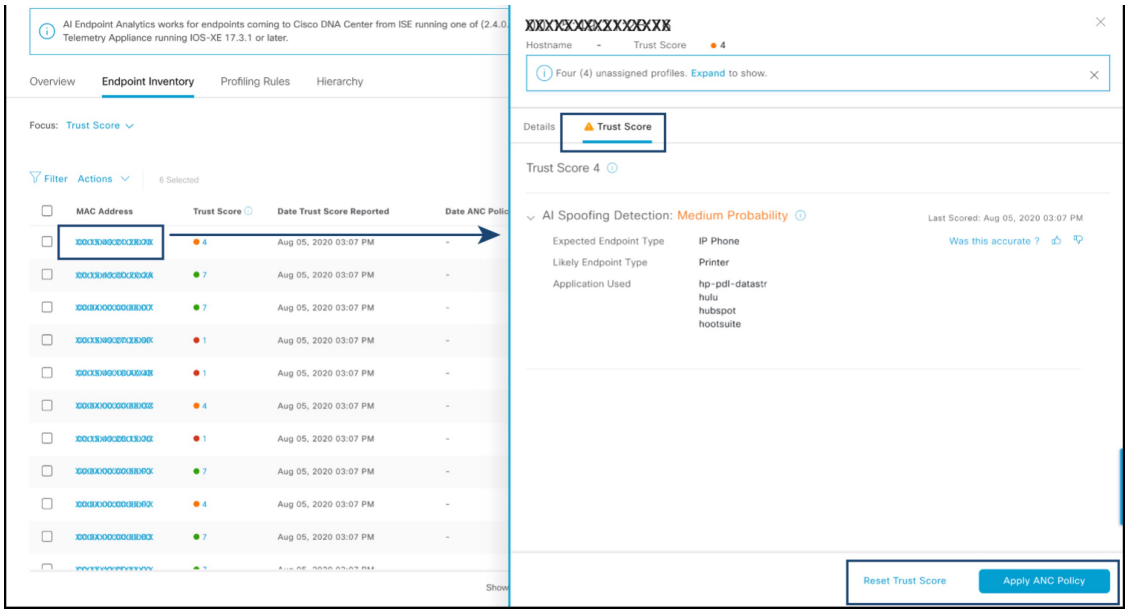
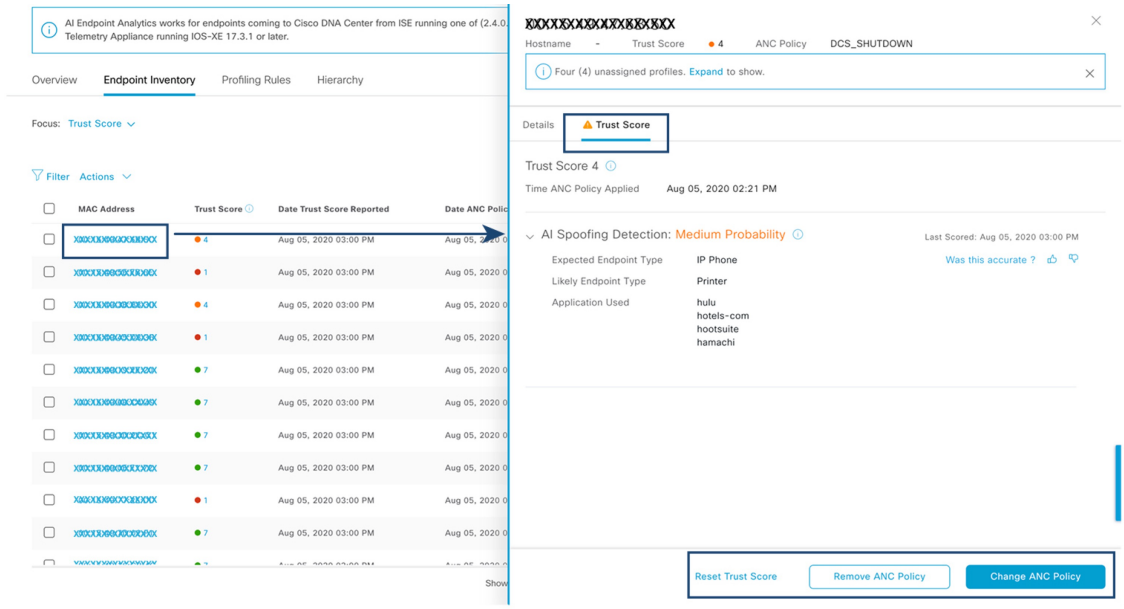


図 *39 : ANC* ポリシーを使用したエンドポイントの信頼スコアオプション



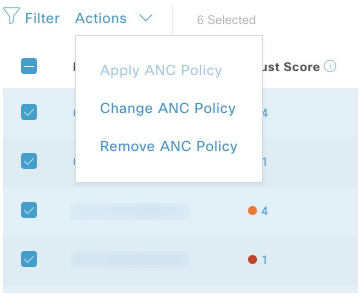
信頼スコアのあるエンドポイントのリストから、管理するエンドポイントの MAC アドレスをクリックします。表示されるエンドポイントの詳細ペインで、[信頼スコア（Trust Score）] タブをクリックします。

ここには、[予想されるエンドポイントタイプ（Expected Endpoint Type）] の値が表示されます。[Applications Used] フィールドには、エンドポイントで使用されるアプリケーションが一覧表示されます。

このペインには、ANC ポリシーの受け入れと削除のワークフローを開始し、信頼スコアをリセットするためのボタンがあります。目的のタスクのボタンをクリックします。

または、[Endpoint Inventory] ウィンドウで個々のエンドポイントのチェックボックスをオンにし、[Actions] をクリックして、ドロップダウンリストから必要なオプションを選択します。

- **複数のエンドポイントの信頼スコアの管理**



[エンドポイントインベントリ（Endpoint Inventory）] タブで、特定のアクションを実行する必要があるすべてのエンドポイントのチェックボックスをオンにします。[Actions] をクリックし、ドロップダウンリストから必要なアクションを選択します。

エンドポイント スプーフィングの制御

同時 MAC アドレス検出とは、同じ MAC アドレスを持つ 2 つのエンドポイントがネットワークにアクセスしてトラフィックを生成していることが検出されることを意味します。次に、実際のエンドポイントとスプーフィングされたエンドポイントを区別し、スプーフィングされたエンドポイントに対して必要な修復アクションを実行することが不可欠になります。

コントロール エンドポイント スプーフィング機能は、エンドポイントの MAC アドレス以外のネットワーク情報を提供することにより、詳細なポリシーコントロールを提供します。ネットワーク情報には、サイト情報、ネットワークデバイスの IP アドレス、ネットワークデバイスポート、最初に承認されたタイムスタンプ、最後に承認されたタイムスタンプ、およびエンドポイントがネットワークで使用可能であった期間が含まれます。従来のように MAC アドレスでエントリを区別するか、MAC アドレスと提供されたネットワーク情報の両方を使用してエントリを区別するかを選択できます。MAC アドレスと接続（ネットワーク情報）で区別することを選択した場合、スプーフィングされたエンドポイントを検出するための選択が自動的に行われます。自動選択を使用するか、スプーフィングされたエンドポイントであると思われるものを選択して、そのエンドポイントに適切な修復アクションを適用することができます。使用可能な修復アクションは、Cisco ISE で設定された適応型ネットワーク制御（ANC）ポリシーです。

これはポリシーを適用する詳細な方法であるため、**[Operations] > [Adaptive Network Control] > [Endpoint Assignment]** にこのポリシーのリストは表示されません。

同時MACアドレス検出がなく、NATモード検出のみのエンドポイントの場合、ANCポリシーは「エンドポイントの信頼スコアの表示と管理（1563ページ）」で説明されているように適用

されます。このようなシナリオでは、エンドポイントは Cisco ISE の [Endpoint Assignment] の下にリストされます。

同時 MAC アドレスと NAT モードの両方の検出があるエンドポイントの場合、詳細なポリシー制御が優先されます。したがって、[Apply ANC Policy] をクリックすると、エントリを区別する 2 つのオプションがある新しい [Apply ANC Policy] ウィンドウが表示されます。

また、いつでもエンドポイントの ANC ポリシーを変更することを選択できます。ANC ポリシーの変更中に、ANC ポリシーを適用できる複数のエントリを選択するオプションがあります。

（注） 修復アクションとして [Shutdown] を選択し、アクションを変更する場合、エンドポイントはアクションの変更後に自動的に再起動されません。エンドポイントが接続されているスイッチのインターフェイスを手動でオンにする必要があります。

ANC ポリシーはいつでも削除できます。

始める前に

ダイナミック認証を、ネットワークデバイスで設定する必要があります。Catalyst Center から AAA 設定を使用してネットワークデバイスをプロビジョニングすることをお勧めします。

手順

ステップ 1 Catalyst Center の GUI から、**[Policy]** > **[AI Endpoint Analytics]** > **[Endpoint Inventory]** > **[View endpoints in trust score view]** の順に選択します。

ステップ 2 確認するエンドポイントをクリックして、ANC ポリシーを適用します。

ステップ 3 [Trust Score] > [Concurrent MAC Address] を選択します。

ステップ 4 [Apply ANC Policy] をクリックします。

ステップ 5 [Apply ANC Policy] ウィンドウで、[Based on MAC address] または [Based on MAC address and connectivity] を選択します。

ステップ 6 [Apply ANC Policy] ドロップダウンリストから適切な修復アクションを選択します。

ステップ 7 [Apply ANC Policy] をクリックします。

このタスクを完了した後、そのエンドポイントの [Trust Score] ビューに戻ると、ANC ポリシー名と、ポリシーが適用されたネットワークデバイスの IP アドレスと、ANC ポリシーが適用された時刻を確認できます。

設定を確認するには、Cisco ISE の GUI で、**[Operation]** > **[RADIUS]** > **[Live logs]** の順に選択します。[Identity] 列をエンドポイントの MAC アドレスでフィルタリングできます。

このエンドポイントの Cisco ISE から開始された CoA アクションのエントリが一覧表示されます。詳細を確認すると、エンドポイントに適用した ANC ポリシーが [CoA Reason] に表示されます。

プロファイリングルール

Cisco AI エンドポイント分析のプロファイリングルールを使用すると、共通の属性を組み合わせてエンドポイントをグループ化できます。これらの属性により、エンドポイントタイプ、OS タイプ、ハードウェアモデル、およびハードウェア製造元でエンドポイントを識別できます。プロファイリングルールを使用すると、多くのエンドポイントを簡単に管理できます。

Cisco AI エンドポイント分析は、DPI、メディアプロトコル、医療業界のプロトコルなどを介してネットワークデバイスからプロファイリングデータを受信します。Cisco ISE からのプロファイリングデータは、pxGrid を介して通信されます。これらのプロファイリング属性をデバイスディクショナリで使用してプロファイルルールを作成できます。

プロファイリングルールは、Cisco AI エンドポイント分析の [Profiling Rules] タブで確認できます。このタブの下に表示されるテーブルで、[ルール名（Rule Name）] エントリをクリックすると、割り当てられたプロファイルと使用される属性が表示されます。

Cisco AI エンドポイント分析でエンドポイントをプロファイリングするために使用されるプロファイリングルールは次のとおりです。

- システムルール
- シスコの規則
- Cisco AI ルール

ルールの優先順位付け

Cisco AI エンドポイント分析のプロファイリングルールには優先順位があります。プロファイリングルールの実行は、このルールの優先順位に従って、精度の高いエンドポイントをプロファイリングします。

Cisco AI エンドポイント分析ではユーザー入力がプライマリであるため、プロファイリングルールの優先順位は次のようになります。

- 管理者が作成した静的プロファイル（たとえば、[Register Endpoints] オプションを使用して追加したプロファイル）。
- 管理者が作成したカスタムルール。
- デフォルトで使用可能なシスコ提供のシステムルール。
- 機械学習対応のスマートグループ化ワークフローによって自動生成されたルール。

ルールに設定された優先順位を表示するには、[Profiling Rules] ウィンドウで [Rule priorityitization] をクリックします。

登録済みのエンドポイントは、さまざまなプロファイリングラベルの複数の Cisco AI エンドポイント分析ルールによってプロファイリングできます。次の表に、2 つのエンドポイントに対するプロファイリングルールの設計を示します。

エンドポイント 1	エンドポイント 2
システムルールによってプロファイリングされたハードウェアモデル Cisco AI ルールによってプロファイリングされた OS タイプ カスタムルールによってプロファイリングされたハードウェア製造元	システムルールによってプロファイリングされたハードウェアモデル カスタムルールによってプロファイリングされたハードウェアモデル Cisco AI ルールによってプロファイリングされたハードウェアモデル

エンドポイント 2 のルール優先順位では、カスタムルールが他のルールよりも優先されます。エンドポイント 2 のハードウェアモデルラベルは、カスタムルールによってプロファイリングされます。

エンドポイント 1 の場合、ルールごとに異なるプロファイルラベルが定義され、それに応じて各ラベルがプロファイリングされます。

プロファイリングルールのフィルタ処理

手順

ステップ 1 [Profiling Rules] ウィンドウで、[Filter] をクリックします。

ステップ 2 [Rule Name] フィールドに、名前を入力します。

ステップ 3 対応するドロップダウンリストからエンドポイント属性の値を選択して、一連のエンドポイントをフィルタ処理します。

ステップ 4 [Apply] をクリックします。

更新されたプロファイリングルールの表示

手順

ステップ 1 [Endpoint Inventory] ウィンドウに移動します。

ステップ 2 エンドポイントのMACアドレスの横にあるチェックボックスをクリックして、エンドポイントのプロファイリングの詳細を表示します。

ステップ 3 プロファイルラベルの横にある情報アイコンをクリックし、ルール名をクリックして、割り当てられたプロファイルと属性の詳細を表示します。

システムルール

Cisco AI エンドポイント分析には、エンドポイントをプロファイリングするためのシステムルールと呼ばれる事前定義済みのルールが用意されています。Cisco AI エンドポイント分析を導入すると、特定のルールを設定することなく、エンドポイントのゼロデイ可視性を実現できます。

新しくオンボーディングされたエンドポイントは、デフォルトでシステムルールを使用してプロファイリングされます。

ネットワークデバイスは、**[Provision]** > **[Network Devices]** > **[Inventory]** ウィンドウの Catalyst Center で管理されます。

これらのネットワークデバイスは、システムルールによってプロファイリングされ、Cisco AI エンドポイント分析の [Endpoint Inventory] ウィンドウには表示されません。ただし、カスタムルールは、ネットワークデバイスを**[デバイスタイプ（Device Type）]**として作成されるため、カスタムルールによってプロファイリングされたエンドポイントを表示できます。

エンドポイント プロファイリング用の自動システムルール更新

Cisco AIエンドポイント分析でエンドポイントプロファイリングに使用されるシステムルールは、プロファイリングの精度を高めるために定期的に更新されます。シスコからのエンドポイント プロファイリング システム ルールの更新を受信するように自動更新をスケジュールします。Catalyst Center が設定された時間に更新を受信し、変更内容が Cisco AI エンドポイント分析に適用されます。[Profiling Rules] ウィンドウ（**[Policy]** > **[AI Endpoint Analytics]** > **[Profiling Rules]**）で、エンドポイントプロファイルの変更の詳細を確認し、システムルールの更新を承認または拒否します。

承認されたシステムルールの更新によってエンドポイントのハードウェアモデルの値が変更された場合、[Endpoint Inventory] タブでエンドポイントの詳細を表示すると、[Hardware Model] フィールドにシステムルールの更新の名前があります。

始める前に

NBARクラウドを設定し、有効にします。「CBARクラウドの設定（1332ページ）」を参照してください。

NBAR クラウドのステータスを確認するには、**[Policy]** > **[AI Endpoint Analytics]** > **[Overview]** の順に選択し、[Configuration] をクリックします。

手順

ステップ 1 メインメニューから、**[System]** > **[Settings]** > **[Cisco Accounts]** > **[Profile Rule Settings]** の順に選択します。

[Schedule Automatic Updates] エリアの [Enabled] トグルボタンは、デフォルトでアクティブに設定されています。

ステップ 2 更新をスケジュールする曜日のボタンをクリックします。複数の曜日を選択できます。次に、[Time Slot] テキストフィールドを使用して、更新の時間を選択します。Catalyst Centerによって更新が受信されるまでに 30 分かかります。2 番目のタイムスロット領域は編集できず、スケジュールされた更新が完了すると予想される時間が表示されます。

ステップ 3 Catalyst Center がシステムルールの更新を受信すると、[Profiling Rules] ウィンドウ（**[Policy]** > **[AI Endpoint Analytics]** > **[Profiling Rules]**）に通知が表示されます。ダイアログボックスで [展開（Expand）] をクリックすると、次の通知が表示されます。

最新バージョン（最新バージョンの名前）に更新され、最近のシスコプロファイリングルールによって一部のエンドポイントのプロファイルが変更されています。

[更新の確認（Review Update）] をクリックします。

ステップ 4 [エンドポイントプロファイルの更新の確認（Endpoint Profile Update Review）] ダイアログボックスが表示されます。このダイアログボックスには、現在適用されている安定版の更新、受信した最新の更新などの情報が表示されます。また、クリックして関連するエンドポイントプロファイルの更新を表示できる次のセクションも含まれています。

1. [Major Updates]：Linux エンドポイントとして現在記録されている Windows エンドポイントなど、プロファイルに大きな変更があったエンドポイントが一覧表示されます。
2. [Minor Updates]：Windows OS の更新バージョンなど、プロファイルにマイナーな変更があったエンドポイントが一覧表示されます。
3. [Newly Profiled]：以前にプロファイル解除され、現在プロファイル情報が割り当てられているエンドポイントが一覧表示されます。

ステップ 5 エンドポイントプロファイルの変更を確認した後、プロファイルの更新を受け入れるには、[Endpoint Profile Update Review] ダイアログボックスで [Mark As Approved Version] をクリックします。エンドポイントプロファイルの変更に同意しない場合は、[Rollback] をクリックします。

ロールバックを選択する場合、対応するオプションをクリックして、最後の実行バージョンにロールバックするのか、最後に承認されたバージョンにロールバックするのかを選択する必要があります。

また、**[AIエンドポイント分析（AI Endpoint Analytics）]** > **[概要（Overview）]** > **[設定（Configuration）]** ウィンドウから、承認およびロールバックアクションを実行することもできます。

ステップ 6 [x] をクリックして、ダイアログボックスを閉じます。

カスタムルール

システムルールのほかに、エンドポイント属性を組み合わせて、エンドポイントをプロファイリングするためのカスタムルールを作成することもできます。カスタムルールは、Cisco AI エンドポイント分析の他のエンドポイント プロファイリング ルールよりも優先されます。

プロファイリングルールの論理と条件

[Endpoint Inventory] ウィンドウでカスタムプロファイリング ルールを作成できます。カスタムプロファイリングルールを作成するには、エンドポイントの属性と値に基づいて論理条件を作成する必要があります。これらの属性は、ネットワークプローブデータから収集され、[Attribute Glossary] ウィンドウで使用できる分類属性とは異なります。

値は、エンドポイントグループを一意に識別するユーザー入力です。次の表の演算子を使用して、属性と値から正規表現が作成されます。

演算子	説明
Contains	属性は、選択した値を持ちます。
Equals	属性は、選択した値に厳密にマッピングされます。
Matches	属性は、選択した値の正規表現パターンと一致する必要があります。
Starts With	属性は、選択した値で始まる必要があります。

（注） Contains、Equals、および Starts With は、大文字と小文字を区別する演算子です。大文字と小文字を区別しない値の場合は、Matches 演算子を使用します。

論理（[AND] および [OR]）によってこれらの条件をさらに組み合わせて、ネストされたルールを作成できます。

論理条件の作成と編集

論理条件を作成するには、次の手順に従います。

手順

ステップ 1 [Choose Attribute Conditions] ウィンドウで、更新する [Attribute] の横にあるチェックボックスをオンにします。

ステップ 2 [Operator] ドロップダウンリストからオプションを選択します。

ステップ 3 [Value] フィールドに値を入力します。

ステップ 4 [Next] をクリックします。

ステップ 5 表示される [Add Logic to Conditions] ウィンドウで、条件間の [AND] ロジックまたは [OR] ロジックをドラッグアンドドロップして、カスタムルールの条件の論理シーケンスを作成します。

（注） 条件の横にある垂直省略記号を使用して、[Add Logical Conditions] ウィンドウで属性条件を追加または編集することもできます。

ステップ 6 [Next] をクリックします。

カスタムルールの作成

手順

ステップ 1 [Endpoint Inventory] ウィンドウで、プロファイリングするエンドポイントの MAC アドレスの横にあるチェックボックスをオンにします。

ステップ 2 [Actions] をクリックし、[Profile with Custom Rules] を選択します。

ステップ 3 表示される **[ルール名とタイプ（Name Rule and Type）]** ウィンドウの [ルール名（Rule Name）] フィールドにルールの名前を入力し、[プロファイルラベル（Profile Label）] ドロップダウンリストからラベルを選択します。

[Profile Label] ドロップダウンリストから選択した内容に応じて、対応するフィールドが表示され、その名前は動的に更新されます。たとえば、[Endpoint Type] を選択すると、[Endpoint Type] フィールドが表示されます。

ステップ 4 表示される新しいフィールドに値を入力します。情報の入力を開始すると、一致するオプションが表示されます。要件に一致するオプションがあれば、そのオプションを選択します。なければ、タイプ名全体を入力します。

ステップ 5 [Next] をクリックします。

ステップ 6 表示される **[属性条件の選択（Choose Attribute Conditions）]** ウィンドウで、論理条件を作成します。

詳細については、「論理条件」を参照してください。

ステップ 7 [Review Rule] ウィンドウで、このカスタムルールでプロファイリングされるエンドポイントのリストを確認します。

ステップ 8 [Next] をクリックします。

ステップ 9 [Profiles] をクリックします。

カスタムルールの編集

手順

ステップ 1 [Profiling Rules] ウィンドウで、編集する管理ルールの横にあるチェックボックスをオンにします。

ステップ 2 [Actions] をクリックし、[Edit] を選択します。

ステップ 3 表示される **[編集（Edit）]** ウィンドウの [ルール名（Rule Name）] フィールドにルールの名前を入力し、ルールの作成時に選択したプロファイルラベル（[Profile Label）] に基づいてプロファイルの詳細を選択または入力します。

ステップ 4 [Logic and Conditions] セクションで、垂直省略記号をクリックし、[Edit] を選択して、プロファイリングルールの論理と条件を更新します。詳細については、「論理条件」を参照してください。

ステップ 5 **[次へ (Next)]** をクリックします。

ステップ 6 **[適用 (Apply)]** をクリックします。
既存のルールが新しいプロファイリングの詳細で更新されると、そのルールでプロファイリングされたエンドポイントが新しいプロファイリングの詳細で更新されます。

カスタムルールの削除

手順

ステップ 1 [Profiling Rules] ウィンドウで、削除するルールの横にあるチェックボックスをオンにします。

ステップ 2 [Actions] をクリックし、[Delete] を選択します。

次のメッセージが表示されます。

「Do you really want to delete the selected Rule(s)?」

ステップ 3 [Yes] をクリックして、Cisco AI エンドポイント分析からルールを完全に削除します。
カスタムルールが削除されると、このルールでプロファイリングされたエンドポイントがシステムルールで更新されます。

展開間での API を使用したカスタム プロファイリング ルールのエクスポートとインポート

Catalyst Center には、カスタム プロファイリング ルールのインポート、エクスポート、編集、および削除に使用できる Cisco AI エンドポイント分析 API が含まれています。

Cisco AI エンドポイント分析 API バンドルを有効にするには、次の手順を実行します。

1. メインメニューから次を選択します。**[Platform]** > **[Manage]** > **[Bundles]** の順に選択します。

2. [AI Endpoint Analytics] という名前のバンドルを見つけ、[Enable] をクリックします。
3. [ステータス（Status）] 列の値が [無効（Disabled）] から [アクティブ（Active）] に更新され、API のリストが表示されます。各 API の予期される要求および応答ペイロードを確認することもできます。
4. API バンドルを有効にすると、Cisco AI エンドポイント分析 API が Catalyst Center 開発者用ツールキットに追加されます。その後、[Developer Toolkit] ウィンドウ（**[Platform]** > **[Developer Toolkit]**）から API にアクセスできます。

[Bundles] ウィンドウと [Developer Toolkit] ウィンドウの両方から、次の操作を実行できます。

- コードプレビューを生成して、API を実行する別のツールで使用できる API コードを表示します。
- [Try It] をクリックして、Catalyst Center GUI から API を実行します。JSON 応答を受信し、それを任意のテキストエディタにコピーアンドペーストして作業を続行できます。

スマートグループ化のための Cisco AI ルール

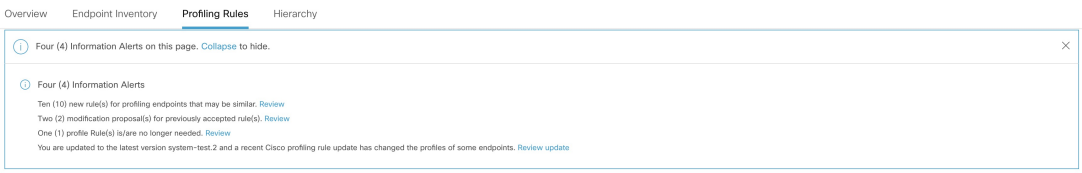
Cisco AI エンドポイント分析の AI アルゴリズムは、展開全体のエンドポイント プロファイリング ラベルとグループに関するデータを分析し、スマートなプロファイリングルールの提案を提供します。

Cisco AI エンドポイント分析の [概要（Overview）] タブの [AI提案（AI Proposal）] ダッシュレットには、エンドポイントクラスタからの学習に基づいた次のルールの提案が表示されます。

- ネットワーク内のプロファイルされていない、またはラベル付けされていないエンドポイントの新しいプロファイリングルール。詳細については、ネットワーク内の類似のエンドポイントに対する新しいプロファイリングの提案 （1578 ページ）を参照してください。

また、ワークフローを開始して、Cisco AI エンドポイント分析の [Profiling Rules] タブから、エンドポイントプロファイリングルールへの変更の提案を確認および適用することもできます。[Profiling Rules] は、情報アラートを含むダイアログボックスを表示します。情報アラートのダイアログボックスで、[Expand] をクリックして、エンドポイント プロファイリング ルールの変更に関する利用可能な提案を表示します。調査する情報アラートの横にある [Review] をクリックして、対応するワークフローを開始します。

図 *40 : [プロファイリングルール（Profiling Rules）] タブの情報アラート*



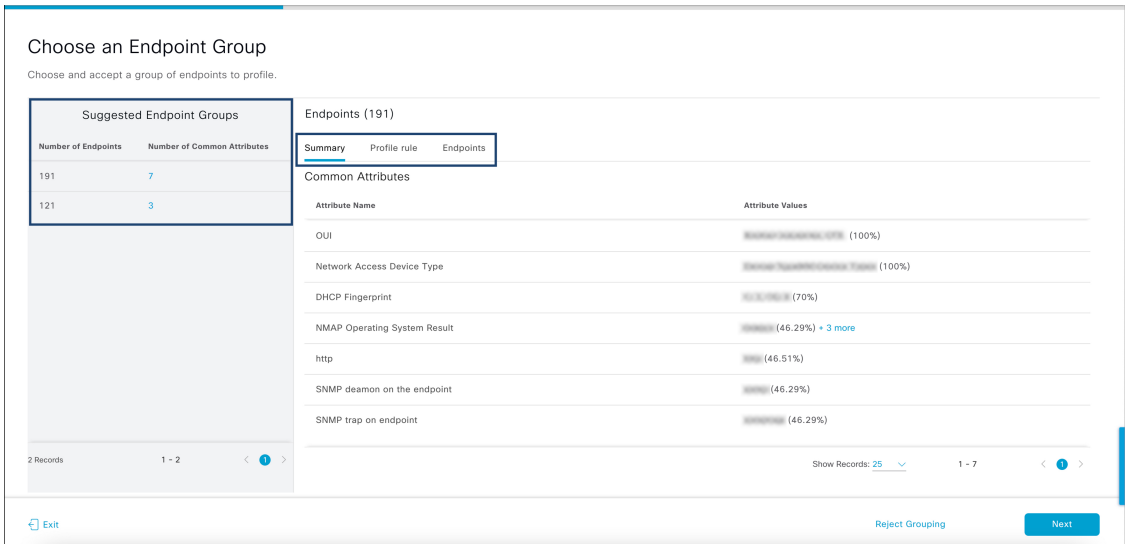
ネットワーク内の類似のエンドポイントに対する新しいプロファイリングの提案

手順

ステップ 1 [AI Proposals] ダッシュレットで、[New rule(s) for profiling endpoints that may be similar] の横にある [Review] ボタンをクリックします。
[Smart Group Profile] ワークフローが起動されます。

ステップ 2 表示される **[エンドポイントグループの選択（Choose an Endpoint Group）]** ウィンドウには、左側のペインに新しいプロファイリングルールの提案のリストが含まれています。リスト内のエントリをクリックして、右側のペインにプロファイリングルールの詳細を表示します。

図 *41* : スマート グループ プロファイル ワークフローの *[エンドポイントグループの選択（Choose an Endpoint Group）]* ウィンドウ

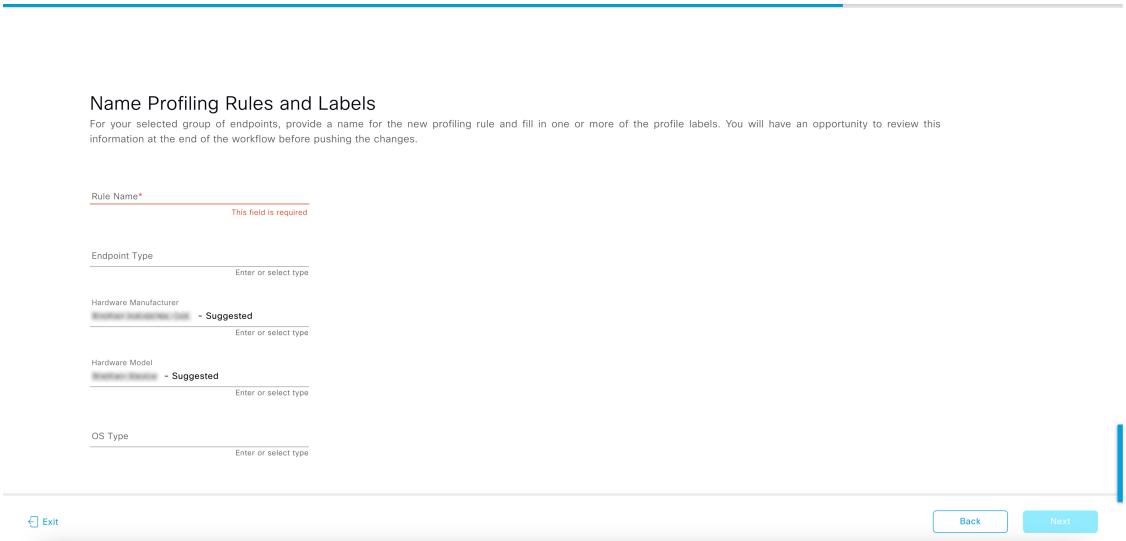


右側のペインには、[Summary]、[Profile Rule]、および [Endpoints] タブが含まれており、提案されたプロファイリングルールの詳細を簡単に表示できます。

ステップ 3 [Next] をクリックして、推奨されるプロファイリングルールを作成します。

ステップ 4 表示される [Name Profiling Rules and Labels] ウィンドウの [Rule Name] フィールドにルールの名前を入力します。

図 *42:* スマート グループ プロファイル ワークフローの *[*名前プロファイリングルールとラベル（***Name Profiling Rules and Labels***）*]* ウィンドウ



ステップ 5 次の 1 つ以上のフィールドに、必要な値を入力します。

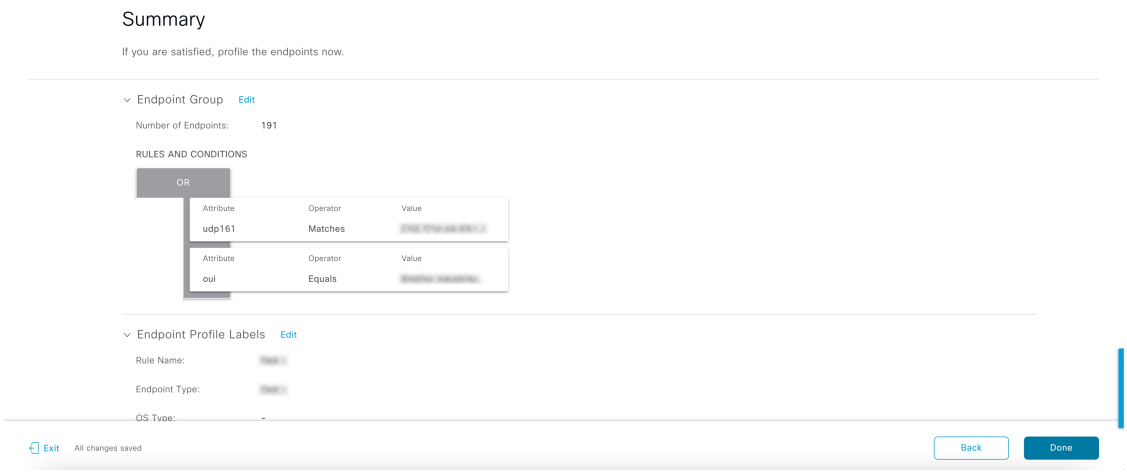
- **エンドポイント タイプ**
- **ハードウェア製造元**
- **ハードウェア モデル**
- **OS タイプ**

AIアルゴリズムがエンドポイントのプロファイリングラベルを識別した場合、そのラベルは対応するフィールドに提案として表示されます。提案されたラベルで続行するか、別のラベルを選択するかを選択できます。

ステップ 6 [次へ（**Next**）] をクリックして続行します。

ステップ 7 [Summary] ウィンドウで、プロファイリングルールの詳細を確認します。変更するには、[Edit] をクリックします。

図 *43* : スマート グループ プロファイル ワークフローの *[*概要（***Summary***）*]* ウィンドウ



ステップ 8 プロファイリングルールを作成するには、[Done] をクリックします。

プロファイリングルールのインポート

カスタムプロファイリングルールと Cisco AI ルールを移行するには、.json ファイルをインポートします。

手順

ステップ 1 [Profiling Rule] ウィンドウで、[Actions] をクリックします。
ステップ 2 [Import Profiling Rules] を選択します。
ステップ 3 [Choose a file] をクリックし、システムの .json ファイルを参照します。
ステップ 4 [OK] をクリックします。

プロファイリングルールのエクスポート

Cisco AI エンドポイント分析からカスタムルールおよび Cisco AI プロファイリングルールをエクスポートしてバックアップできます。[Export Profiling Rules] オプションは、使用可能なすべてのカスタムルールと Cisco AI プロファイリングルールをエクスポートします。ルールを選択してエクスポートすることはできません。

手順

ステップ 1 [Profiling Rules] ウィンドウで、[Actions] をクリックします。

ステップ 2 [Export Profiling Rules] を選択します。

ステップ 3 [Yes] をクリックして、すべてのカスタムルールと ML プロファイリングルールをエクスポートします。終了するには、[No] をクリックします。

（注） 同じファイルを Cisco AI エンドポイント分析に再度インポートできます。

階層

Cisco AI エンドポイント分析階層は、エンドポイントタイプに基づいてエンドポイントの論理グループを作成するのに役立ちます。エンドポイントのカテゴリとサブカテゴリを作成すると、エンドポイントの可視性に焦点が当てられ、許可プロセスが簡素化されます。

デフォルトの [All Endpoints] 親カテゴリからカテゴリを作成できます。エンドポイントの総数、エンドポイントタイプ、サブカテゴリなどのカテゴリの詳細が [Hierarchy] ウィンドウの個々のボックス内に表示されます。

カテゴリを作成、編集、および削除して、階層を並べ替えることができます。

カテゴリとサブカテゴリの作成

手順

ステップ 1 [Hierarchy] ウィンドウで、親カテゴリの水平省略記号をクリックします。

ステップ 2 [Create Category] をクリックします。

ステップ 3 カテゴリ名を入力します。

ステップ 4 Enter キーを押します。

次のタスク

カテゴリを作成したら、[Endpoint Type] ウィンドウからエンドポイントタイプをドラッグアンドドロップするか、カテゴリを編集してエンドポイントを追加できます。

カテゴリまたはサブカテゴリの編集

手順

ステップ 1 [Hierarchy] ウィンドウで、カテゴリの水平省略記号をクリックします。
ステップ 2 [Edit] をクリックします。
ステップ 3 表示される **[編集（Edit）]** ウィンドウで、[カテゴリ名（Category Name）] に値を入力します。
ステップ 4 カテゴリを再割り当てする場合は、ドロップダウンメニューから [Parent Category] を入力します。
ステップ 5 [Endpoint Type] タブをクリックします。
ステップ 6 [Actions] をクリックし、[Add Endpoint Type] を選択します。
ステップ 7 [Search Dropdown] リストからエンドポイントタイプを選択します。
ステップ 8 **[保存（Save）]** をクリックします。

次のタスク

[Endpoint Type] ウィンドウで、[All]、[Available]、および [Assigned] でエンドポイントタイプをフィルタ処理できます。

カテゴリからのエンドポイントタイプの削除

手順

ステップ 1 [Hierarchy] ウィンドウで、削除するカテゴリの水平省略記号をクリックします。
ステップ 2 [Edit] をクリックします。
ステップ 3 [Edit] ウィンドウで、[Endpoint Type] タブをクリックします。
ステップ 4 削除するエンドポイントタイプの横にあるチェックボックスをオンにします。
ステップ 5 [Actions] をクリックし、[Remove From Category] を選択します。

次のメッセージが表示されます。

「Are you sure you want to delete this category?」

ステップ 6 カテゴリからエンドポイントを削除するには、[Yes] をクリックします。終了するには、[No] をクリックします。

カテゴリからのエンドポイントタイプの再割り当て

手順

ステップ 1 [Hierarchy] ウィンドウで、カテゴリの水平省略記号をクリックします。

ステップ 2 [Edit] をクリックします。

ステップ 3 [Edit] ウィンドウで、[Endpoint Type] タブをクリックします。

ステップ 4 再割り当てするエンドポイントタイプの横にあるチェックボックスをオンにします。

ステップ 5 [Actions] をクリックし、[Re-assign to existing category] または [Re-assign to a new category] を選択します。

オプション	手順
既存のカテゴリへの再割り当て	1. [再割り当て（Reassign）] ウィンドウで、[カテゴリ（Category）] ドロップダウンリストから既存のカテゴリを選択します。 2. **[保存（Save）]** をクリックします。
新しいカテゴリへの再割り当て	1. [再割り当て（Reassign）] ウィンドウで、[カテゴリ（Category）] ドロップダウンリストから [新しいカテゴリ（New Category）] を選択します。 2. [親カテゴリ（Parent Category）] ドロップダウンリストから親カテゴリを選択します。 3. [New Category] フィールドにカテゴリ名を入力します。 4. [Save] をクリックします。

カテゴリの削除

始める前に

親カテゴリを削除する前に、そのサブカテゴリを確認します。サブカテゴリを別の既存のカテゴリまたは新しいカテゴリに再割り当てできます。そうしないと、すべてのサブカテゴリが親カテゴリとともに削除されます。カテゴリの削除中にサブカテゴリを再割り当てすることもできます。

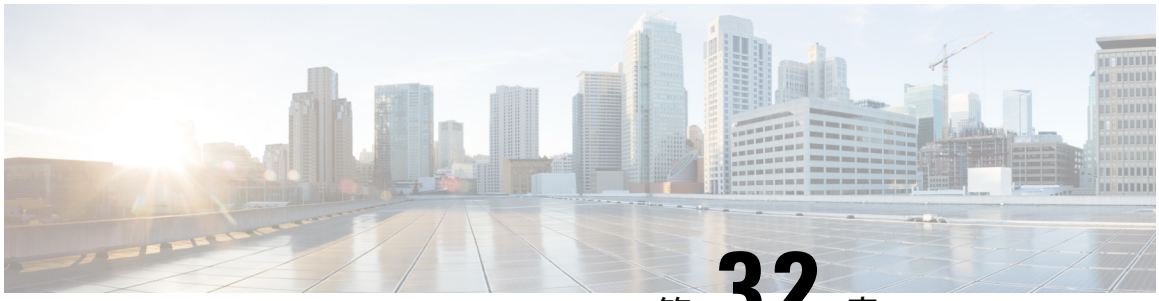
手順

ステップ 1 [Hierarchy] ウィンドウで、カテゴリの水平省略記号をクリックします。

ステップ 2 [削除（Delete）] をクリックします。

サブカテゴリが割り当てられているカテゴリを削除する場合には、[関係の再割り当て（Reassign Relationships）] ダイアログボックスが表示されます。次のオプションのいずれかを選択します。

オプション	条件	手順
既存のカテゴリへの再割り当て	既存のカテゴリにサブカテゴリを再割り当てします。	**1.** [Category] ドロップダウンリストからカテゴリを選択します。 **2.** [Reassign] をクリックします。 親カテゴリが削除され、選択したカテゴリにサブカテゴリが再割り当てされます。
新しいカテゴリへの再割り当て	既存のカテゴリにサブカテゴリを再割り当てします。	**1.** [Parent Category] ドロップダウンリストからカテゴリを選択します。 **2.** [New Category] フィールドにカテゴリ名を入力します。 **3.** [Reassign] をクリックします。 親カテゴリが削除され、新しいカテゴリにサブカテゴリが再割り当てされます。
カテゴリからの削除	親カテゴリとともにサブカテゴリを削除します。	[Reassign] をクリックします。 親カテゴリとそのサブカテゴリが削除されます。



第 32 章

ネットワーク推論機能を使用したネットワークデバイスのトラブルシューティング

- ネットワーク推論機能の概要 （1585 ページ）
- MRE ワークフローを使用した Cisco SD-Access への移行の検証 （1586 ページ）
- CPU 使用率が高い場合のトラブルシューティング （1588 ページ）
- 電源障害のトラブルシューティング （1590 ページ）
- インターフェイスが停止した場合のトラブルシューティング （1591 ページ）
- ネットワーク接続のトラブルシューティング （1593 ページ）
- デバイスの IP 接続のトラブルシューティング （1594 ページ）
- MRE ワークフローを使用したワイヤレスクライアントの障害対応 （1594 ページ）
- MRE ワークフローを使用したワイヤレス AP のトラブルシューティング （1596 ページ）
- MRE ワークフローを使用した監視対象外のデバイスのトラブルシューティング （1597 ページ）
- MRE ワークフローを使用した シスコ ワイヤレス コントローラの HA のトラブルシューティング （1598 ページ）

ネットワーク推論機能の概要

ネットワーク推論機能ツールを使用すると、ネットワークのさまざまな問題を迅速にトラブルシューティングできます。メインメニューから次を選択します。**[Tools]** > **[Network Reasoner]** の順に選択すると、ネットワーク推論機能ダッシュボードが起動します。ネットワーク推論機能ダッシュボードには、ネットワークの問題を事前にトラブルシューティングできる個別のワークフローが用意されています。ダッシュボードには、ワークフローに関する簡単な説明、過去 24 時間に影響を受けたデバイスの数、およびワークフローをネットワークで実行した場合の影響が表示されます。

（注） ネットワーク推論機能を使用するには機械推論パッケージをインストールする必要があり、インストールされていないと [Tools] メニューに表示されません。詳細については、*Cisco Catalyst Center Administrator Guide*を参照してください。

MRE ワークフローを使用した Cisco SD-Access への移行の検証

次の機械推論エンジン（MRE）ワークフローは、Cisco SD-Access への移行を計画する際に役立ちます。

- SDA ハードウェアの準備状況チェック
- SDA ソフトウェアの準備状況チェック
- 冗長リンクチェック
- L3 アクセスチェック
- MTU リンクチェック
- SDA 正常性チェック
- SDA スケール制限チェック

手順

ステップ 1 メインメニューから次を選択します。**[Tools]** > **[Network Reasoner]** の順に選択します。

ステップ 2 [ネットワーク推論機能（Network Reasoner）] ダッシュボードで、必要に応じて次のワークフローをクリックします。

ワークフロー	説明	操作
SDA ハードウェアの準備状況チェック	ハードウェアが Cisco SD-Access の移行準備ができているかどうかを確認します。	1. [SDA Hardware Readiness Check] をクリックします。 2. [Run Machine Reasoning] をクリックします。
SDA ソフトウェアの準備状況チェック	ソフトウェアが Cisco SD-Access の移行準備ができているかどうかを確認します。	1. [SDA Software Readiness Check] をクリックします。 2. [Run Machine Reasoning] をクリックします。
冗長リンクチェック	デバイスに冗長アップリンクが存在するかどうか、およびアクセススイッチで冗長アップリンクを設定して可用性を向上させる方法があるかどうかを確認します。	1. [Redundant Link Check] をクリックします。 2. 適切なデバイスを選択します。 3. [Troubleshoot] をクリックします。

ワークフロー	説明	操作
L3 アクセスチェック	最小限の設計変更で Cisco SD-Access に移行するレイヤ 3 ルーティングプロトコルを実行しているアクセススイッチがネットワークにあるかどうかを確認します。	**1.** [L3 Access Check] をクリックします。 **2.** 適切なデバイスを選択します。 **3.** [Troubleshoot] をクリックします。
MTU リンクチェック	メインのネットワークデバイスとアクセス、コア、およびその他のスイッチ間のリンクが正しい MTU で設定されているかどうかを確認します。	**1.** [MTU Link Check] をクリックします。 **2.** 適切なデバイスを選択します。 **3.** [Troubleshoot] をクリックします。
SDA 正常性チェック：ファブリック数	Catalyst Center クラスタの正常性をチェックし、ファブリックの管理が原因でスケール制限のいずれかのしきい値に達しているかどうかを確認します。	**1.** [Fabric Count] をクリックします。 **2.** [Run Machine Reasoning] をクリックします。
SDA 正常性チェック：ファブリックデータ収集	ネットワークデバイスから show コマンドの出力を収集して、ファブリックネットワークの問題のトラブルシューティングを行います。	**1.** [Fabric Data Collection] をクリックします。 **2.** デバイスを選択し、[Troubleshoot] をクリックします。 **3.** 機械推論が完了したら、[View Details] をクリックします。 **4.** [Consultions] タブで、リンクをクリックして出力ファイルをダウンロードします。出力ファイルは、選択したデバイスで実行されたすべてのコマンドを含むテキストファイルのバンドルです。
SDA 正常性チェック：SDA スケール制限チェック	Catalyst Center に設定されているクライアントエンドポイント、ネットワークデバイス、およびファブリックの数が、公開されている SDA の制限内であるかどうかを確認します。	**1.** [SDA Scale Limits Check] をクリックします。 **2.** [Run Machine Reasoning] をクリックします。
SDA 正常性チェック：クライアント数	Catalyst Center クラスタの正常性をチェックし、クライアントの管理が原因でスケール制限のいずれかのしきい値に達しているかどうかを確認します。	**1.** [Client Count] をクリックします。 **2.** [Run Machine Reasoning] をクリックします。

ワークフロー	説明	操作
SDA 正常性チェック：デバイス数	Catalyst Center クラスタの正常性をチェックし、ネットワークデバイスの管理が原因でスケール制限のいずれかのしきい値に達しているかどうかを確認します。	1. [Device Count] をクリックします。 2. [Run Machine Reasoning] をクリックします。
SDA 正常性チェック：LISP PubSub セッションチェック	ファブリック ボーダーデバイスで LISP PubSub の正常性を確認します。PubSub セッションがダウンしている場合は、トラブルシューティングを行って根本原因を特定します。	1. [LISP PubSub Session Check] をクリックします。 2. デバイスを選択し、[Troubleshoot] をクリックします。 3. 機械推論が完了したら、[View Details] をクリックします。
SDA 正常性チェック：LISP セッションチェック	選択したデバイスでのすべての LISP セッションのステータスを確認します。セッションがダウンしている場合は、トラブルシューティングを行って根本原因を特定します。	1. [LISP Session Check] をクリックします。 2. デバイスを選択し、[Troubleshoot] をクリックします。 3. 機械推論が完了したら、[View Details] をクリックします。

CPU 使用率が高い場合のトラブルシューティング

CPU 使用率のトラブルシューティングは、ソフトウェアバージョン 16.9.3 以降の次のネットワークデバイスでのみサポートされます。

- Cisco Catalyst 9400 シリーズ スイッチ
- Cisco Catalyst 9300 シリーズ スイッチ
- Cisco Catalyst 3850 シリーズ スイッチ
- Cisco Catalyst 3650 シリーズ スイッチ

始める前に

- 機械推論パッケージをインストールします。詳細については、Cisco Catalyst Center 管理者ガイド [英語] の「Download and Install Packages and Updates」を参照してください。
- [System] 機能で機械推論に対する書き込み権限を持つユーザーロールを作成します。詳細については、『Cisco Catalyst Center Administrator Guide』の「Configure Role-Based Access Control」を参照してください。

手順

ステップ 1 メインメニューから次を選択します。**[Tools]** > **[Network Reasoner]** の順に選択します。

ステップ 2 [CPU Utilization] タブをクリックします。

[CPU使用率（CPU Utilization）] ウィンドウには、過去 24 時間の CPU 使用率が高いデバイスのフィルタ処理されたリストが表示されます。

[All] をクリックするとインベントリの全デバイスのリストが表示され、ワークフローを実行するデバイスを選択できます。

ステップ 3 トラブルシューティングするデバイスを選択します。

[Filter] をクリックし、[Tag]、[Device Name]、[IP Address]、[Device Type]、[Site]、または [Reachability] にデバイスの情報を入力します。

ステップ 4 [Troubleshoot] をクリックします。

ステップ 5 [Reasoner Input] ウィンドウで、[CPU Utilization Threshold] にチェックする使用率を入力します。

ステップ 6 [Run Machine Reasoning] をクリックします。

（注） 次のプロセスが確認されると、詳細な分析の対象となります。

- [MATM Process Group]：MATM RP Shim、NGWC Learning、VMATM Callback
- [IOSXE Process Group]：IP Input、ARP Input、IOSXE-RP Punt Se、SISF Main Thread、DAI Packet、ARP Snoop

[CPU使用率（CPU Utilization）] ウィンドウでは、選択したデバイスの CPU 使用率が高い原因に関する情報が [根本原因分析（Root Cause Analysis）] に表示されます。

[Reasoning Activity] タブには、トラブルシューティング プロセスで確認されるさまざまなパラメータが表示されます。

ステップ 7 （オプション）進行中の推論アクティビティを停止するには、[Stop] をクリックします。

ステップ 8 [結論（Conclusion）] タブをクリックして、CPU の消費が多いプロセスとその使用率を確認します。

ステップ 9 それぞれのプロセスについて、[View Relevant Activities] をクリックし、右側のペインで [Activity Details] を確認します。

ステップ 10 （オプション）同じデバイスについてトラブルシューティングプロセスをもう一度実行する場合は、[Run Again] をクリックします。

（注） 機械推論エンジン（MRE）では、しきい値が指定のレベルを超えた場合や非アクティブのタイムアウト要求からイベントを受信しなかった場合にネットワーク推論機能ワークフローを検出して終了するシステム終了アルゴリズムを実装しています。

電源障害のトラブルシューティング

電源トラブルシューティング ワークフローは、ソフトウェアバージョン 16.6.1 以降の次のネットワークデバイスでのみサポートされます。

- Cisco Catalyst 3650 シリーズ スイッチ
- Cisco Catalyst 3850 シリーズ スイッチ
- Cisco Catalyst 9300 シリーズ スイッチ
- Cisco Catalyst 9400 シリーズ スイッチ
- Cisco Catalyst 9500 シリーズ スイッチ

始める前に

- 機械推論パッケージをインストールします。詳細については、Cisco Catalyst Center 管理者ガイド [英語] の「Download and Install Packages and Updates」を参照してください。
- [System] 機能で機械推論に対する書き込み権限を持つユーザーロールを作成します。詳細については、『Cisco Catalyst Center Administrator Guide』の「Configure Role-Based Access Control」を参照してください。

手順

ステップ 1 メインメニューから次を選択します。**[Tools]** > **[Network Reasoner]** の順に選択します。

ステップ 2 [Power Supply] タブをクリックします。

[Power Supply] ウィンドウに、過去 24 時間に電源障害が発生したデバイスのフィルタ処理されたリストが表示されます。

インベントリ内のすべてのデバイスのリストを表示するには、[All] をクリックします。ワークフローを実行する任意のデバイスを選択できます。

ステップ 3 トラブルシューティングするデバイスを選択します。

[Filter] をクリックし、[Tag]、[Device Name]、[IP Address]、[Device Type]、[Site]、または [Reachability] にデバイスの情報を入力してデバイスをフィルタ処理します。

ステップ 4 [Troubleshoot] をクリックします。

[Power Supply] ウィンドウで、選択したデバイスの電源障害の原因に関する情報が [Root Cause Analysis] に表示されます。

[推論アクティビティ（Reasoning Activity）] タブには、トラブルシューティング プロセスで確認されるさまざまなパラメータが表示されます。

ステップ 5 （オプション）進行中の推論アクティビティを停止するには、[Stop] をクリックします。

ステップ 6 [Conclusion] タブをクリックして、選択したデバイスの電源の [Stack Identifier]、[Product ID]、[Serial Number]、および [Status] の情報と推奨されるアクションを確認します。

ステップ 7 それぞれのスタック識別子について、[View Relevant Activities] をクリックし、右側のペインで [Activity Details] を確認します。

ステップ 8 （オプション）同じデバイスについてトラブルシューティング プロセスをもう一度実行する場合は、[Run Again] をクリックします。

（注） 機械推論エンジン（MRE）では、しきい値が指定のレベルを超えた場合や非アクティブのタイムアウト要求からイベントを受信しなかった場合にネットワーク推論機能ワークフローを検出して終了するシステム終了アルゴリズムを実装しています。

インターフェイスが停止した場合のトラブルシューティング

インターフェイス ダウン トラブルシューティング ワークフローは、ソフトウェアバージョン 16.9.3 以降の次のネットワークデバイスでのみサポートされます。

- Cisco Catalyst 3650 シリーズ スイッチ
- Cisco Catalyst 3850 シリーズ スイッチ
- Cisco Catalyst 9300 シリーズ スイッチ
- Cisco Catalyst 9400 シリーズ スイッチ
- Cisco Catalyst 9500 シリーズ スイッチ

始める前に

- 機械推論パッケージをインストールします。詳細については、Cisco Catalyst Center 管理者ガイド [英語] の「Download and Install Packages and Updates」を参照してください。
- [System] 機能で機械推論に対する書き込み権限を持つユーザーロールを作成します。詳細については、『Cisco Catalyst Center Administrator Guide』の「Configure Role-Based Access Control」を参照してください。

手順

ステップ 1 メインメニューから次を選択します。**[Tools]** > **[Network Reasoner]** の順に選択します。

ステップ 2 [Interface Down] タブをクリックします。

[Interface Down] ウィンドウには、過去 24 時間にインターフェイスが停止したデバイスのフィルタ処理されたリストが表示されます。

[All] をクリックするとインベントリの全デバイスのリストが表示され、ワークフローを実行するデバイスを選択できます。

ステップ 3 トラブルシューティングするデバイスを選択します。

[Filter] をクリックし、[Tag]、[Device Name]、[IP Address]、[Device Type]、[Site]、または [Reachability] にデバイスの情報を入力します。

ステップ 4 [Troubleshoot] をクリックします。

ステップ 5 [Reasoner Input] ウィンドウで、問題が疑われるインターフェイスの名前を入力します。

ステップ 6 [Run Machine Reasoning] をクリックします。

[Interface Down] ウィンドウには、選択したデバイスのインターフェイスが停止する原因に関する情報が [Root Cause Analysis] に表示されます。

[Reasoning Activity] タブには、トラブルシューティング プロセスで確認されるさまざまなパラメータが表示されます。

ステップ 7 （オプション）進行中の推論アクティビティを停止するには、[Stop] をクリックします。

ステップ 8 [Conclusion] タブをクリックして、インターフェイスが停止する問題についての考えられる根本原因と推奨されるアクションを確認します。

ステップ 9 それぞれの根本原因分析について、[View Relevant Activities] をクリックし、右側のペインで [Activity Details] を確認します。

ステップ 10 （オプション）同じデバイスについてトラブルシューティング プロセスをもう一度実行する場合は、[Run Again] をクリックします。

（注） 機械推論エンジン（MRE）では、しきい値が指定のレベルを超えた場合や非アクティブのタイムアウト要求からイベントを受信しなかった場合にネットワーク推論機能ワークフローを検出して終了するシステム終了アルゴリズムを実装しています。

ネットワーク接続のトラブルシューティング

Cisco IOS-XE ソフトウェアバージョン 16.9.3 以降を実行している次のネットワークデバイスでのみ、ネットワーク接続のトラブルシューティングがサポートされています。

- Cisco Catalyst 9200 シリーズ スイッチ
- Cisco Catalyst 9300 シリーズ スイッチ
- Cisco Catalyst 9400 シリーズ スイッチ
- Cisco Catalyst 9500 シリーズ スイッチ
- Cisco Catalyst 9600 シリーズ スイッチ

IP アドレスを使用してデバイスからエンドポイントの到達可能性を確認するには、次の手順を実行します。

始める前に

- 機械推論パッケージをインストールします。詳細については、Cisco Catalyst Center 管理者ガイド [英語] の「Download and Install Packages and Updates」を参照してください。
- [System] 機能で機械推論に対する書き込み権限を持つユーザーロールを作成します。詳細については、『Cisco Catalyst Center Administrator Guide』の「Configure Role-Based Access Control」を参照してください。

手順

ステップ 1 メインメニューから次を選択します。**[Tools]** > **[Network Reasoner]** の順に選択します。

ステップ 2 [Network Connectivity] タブをクリックします。

ステップ 3 **デバイス名**、**IP アドレス**、**デバイスタイプ**、**サイト**、**到達可能性**、**ロール**、**プラットフォーム**などの詳細情報を含むデバイステーブルを表示できます。

ステップ 4 デバイスを選択して、[Troubleshoot] を選択します。

ステップ 5 [Reasoner Inputs] ウィンドウの [Destination IP address] フィールドに有効な IP アドレスを入力し、[Run Machine Reasoning] をクリックします。

（注） Virtual Routing and Forwarding（VRF）の名前を入力します（該当する場合）。

ステップ 6 [Root Cause Analysis] ウィンドウの [Reasoning Activity] で、トラブルシューティング プロセスの一環として検証されるさまざまなワークフローを確認できます。

ステップ 7 [Conclusions] タブで、検証チェックのステータスと推奨アクションを確認できます。

デバイスの IP 接続のトラブルシューティング

ping はシンプルなコマンドであるため、すべてのネットワークデバイスで IP 接続のトラブルシューティングをサポートできます。

始める前に

- 機械推論パッケージをインストールします。詳細については、Cisco Catalyst Center 管理者ガイド [英語] の「Download and Install Packages and Updates」を参照してください。
- [System] 機能で機械推論に対する書き込み権限を持つユーザーロールを作成します。詳細については、『Cisco Catalyst Center Administrator Guide』の「Configure Role-Based Access Control」を参照してください。

手順

ステップ 1 メインメニューから次を選択します。**[Tools]** > **[Network Reasoner]** の順に選択します。

ステップ 2 [Network Reasoner] ダッシュボードで、[Ping Device] をクリックします。

ステップ 3 [Devices] ウィンドウで、デバイスを選択し、[Troubleshoot] をクリックします。

ステップ 4 [Reasoner Inputs] ウィンドウで、[Target IP Address] に値を入力し、[Run Machine Reasoning] をクリックします。

ステップ 5 [View Details] をクリックして、ping ステータスを確認します。

MRE ワークフローを使用したワイヤレスクライアントの障害対応

この手順を使用して、MRE ワークフローを使用してワイヤレスクライアントの問題をトラブルシューティングします。

（注）
- ワイヤレスクライアントのトラブルシューティング ワークフローのサポートは、Cisco IOS-XE ソフトウェアバージョン 17.3.4 以降のネットワークデバイスでのみ使用できます。
- MRE ワークフローは HA をサポートしていません。つまり、ワークフロー中に切り替えが発生した場合は、ワークフローをやり直す必要があります。

始める前に

機械推論エンジン（MRE）ナレッジベースが最新のナレッジパックで更新されていることを確認します。詳細については、『*Cisco Catalyst Center Administrator Guide*』の「Update the Machine Reasoning Knowledge Base」[英語] のトピックを参照してください。

手順

ステップ 1 メインメニューから次を選択します。**[Tools]** > **[Network Reasoner]** の順に選択します。

ステップ 2 [Wireless Client Data Collection] タイルをクリックします。
[Devices] ウィンドウに、フィルタリングされたワイヤレス コントローラ デバイスが表示されます。

ステップ 3 トラブルシューティングするワイヤレスコントローラを選択し、[Troubleshoot] をクリックします。

ステップ 4 [Reasoner Inputs] ウィンドウで、次のフィールドに値を入力します。
- [Troubleshoot Duration]
- [Client MAC Address]
- [PCAP Interface]：ドロップダウン矢印をクリックし、リストからインターフェイスを選択します。パケットキャプチャが必要な場合は、このオプションを使用します。

ステップ 5 [Run Machine Reasoning] をクリックします。
[Wireless Client Data Collection] スライドインペインが表示されます。

ステップ 6 [Root Cause Analysis] エリアの [Reasoning Activity] タブには、トラブルシューティング プロセスで確認されるさまざまなパラメータが表示されます。必要に応じて、[Stop] をクリックして進行中の推論アクティビティを停止します。

ステップ 7 トラブルシューティング処理が完了するまで待ちます。完了したら、[Conclusions] タブでトラブルシューティング ファイルを表示できます。

ステップ 8 （任意）同じデバイスについてトラブルシューティング プロセスをもう一度実行する場合は、[Run Again] をクリックします。

ステップ 9 （任意）ワイヤレスクライアントの障害対応ワークフローを開始すると、[ワイヤレスクライアントのデータ収集（Wireless Client Data Collection）] スライドインペインで最新の障害対応ファイルを表示できます。

MRE ワークフローを使用したワイヤレス AP のトラブルシューティング

この手順により、MRE ワークフローを使用して無線クライアントの問題をトラブルシュートします。

（注）
- 無線 AP のトラブルシューティングをするワークフローは、Cisco IOS-XE 17.3.4 以降を搭載したネットワークデバイスでのみ使用できます。
- MRE ワークフローは HA をサポートしていません。つまり、ワークフロー中に切り替えが発生した場合は、ワークフローをやり直す必要があります。

始める前に

MRE ナレッジベースが最新のナレッジパックで更新されていることを確認します。詳細については、『Cisco Catalyst Center Administrator Guide』の「Update the Machine Reasoning Knowledge Base」を参照してください。

手順

ステップ 1 メインメニューから次を選択します。**[Tools]** > **[Network Reasoner]** の順に選択します。

ステップ 2 [Wireless Client Data Collection] タイルをクリックします。

ステップ 3 [Devices] ウィンドウに、フィルタリングされたワイヤレス コントローラ デバイスが表示されます。AP についてトラブルシュートするワイヤレス コントローラ デバイスを選択し、[Troubleshoot] をクリックします。

ステップ 4 [Reasoner Inputs] ウィンドウで、次のフィールドに値を入力します。

- [Troubleshoot Duration]
- [Two AP MAC Address]：AP の MAC アドレス（イーサネットと無線）を入力します。
- パケットキャプチャが必要な場合は、次のオプションを使用します。
  - [PCAP Interface]：ドロップダウンリストをクリックし、インターフェイスを選択します。
  - [AP IP Address]：AP の IP アドレスを入力します。
- [AP Name]

ステップ 5 [Run Machine Reasoning] をクリックします。
[Wireless AP Data Collection] スライドインペインが表示されます。

ステップ 6 [Root Cause Analysis] エリアの [Reasoning Activity] タブには、トラブルシューティング プロセスで確認されるさまざまなパラメータが表示されます。必要に応じて、[Stop] をクリックして進行中の推論アクティビティを停止します。

ステップ 7 トラブルシューティング処理が完了するまで待ちます。完了したら、[Conclusions] タブでトラブルシューティング ファイルを表示できます。

ステップ 8 （任意） 同じデバイスについてトラブルシューティング プロセスをもう一度実行する場合は、[Run Again] をクリックします。

ステップ 9 （任意） 無線 AP トラブルシューティング ワークフローを開始すると、[ワイヤレスAPデータ収集（Wireless AP Data Collection）] スライドインペインに最新のトラブルシューティング ファイルが表示されます。

MRE ワークフローを使用した監視対象外のデバイスのトラブルシューティング

この手順を使用して、監視されていないデバイスまたは Assurance データが表示されないデバイスのトラブルシューティングを行います。監視されていないデバイスのトラブルシューティング ワークフローは、スイッチ、Cisco AireOS ワイヤレスコントローラ、および Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のみをサポートします。

始める前に

機械推論エンジン（MRE）ナレッジベースが最新のナレッジパックで更新されていることを確認します。詳細については、『*Cisco Catalyst Center Administrator Guide*』の「Update the Machine Reasoning Knowledge Base」[英語] のトピックを参照してください。

手順

ステップ 1 メインメニューから次を選択します。**[Tools]** > **[Network Reasoner]** の順に選択します。

ステップ 2 [Assurance Telemetry Analysis] タイルをクリックします。

ステップ 3 [Devices] ウィンドウには、監視されていないデバイスがフィルタリングされて表示されます。トラブルシューティングするデバイスを選択し、[Troubleshoot] をクリックします。

[Assurance Telemetry Analysis] スライドインペイン が表示されます。[Root Cause Analysis] エリアの [Reasoning Activity] タブには、トラブルシューティング プロセスで確認されるさまざまなパラメータが表示されます。

ステップ 4 進行中の推論アクティビティを停止するには、[Stop] をクリックします。

障害対応が完了すると、[機械推論完了（Machine Reasoning Completed）] ダイアログボックスが表示されます。

ステップ 5 **[Show Details]** をクリックします。

ステップ 6 [Conclusions] タブでトラブルシューティング ファイルを表示できます。問題はアイコン（⚠）で強調表示され、問題の下に [推奨されるアクション（Suggested Action）] が表示されます。

提示された推奨案を使用して、監視されていないデバイスのトラブルシューティングを行うことができます。

ステップ 7 同じデバイスについてトラブルシューティング プロセスをもう一度実行する場合は、[Run Again] をクリックします。

ステップ 8 [Inventory] タブからデバイスのトラブルシューティングを行うこともできます。下にスクロールして [Health Score] 列を表示します。[Health Score] 列の下の [No Health] をクリックし、[View Assurance Telemetry Analysis] をクリックして、トラブルシューティング プロセスを実行します。

MRE ワークフローを使用した シスコ ワイヤレス コントローラの HA のトラブルシューティング

MRE ワークフローは、コマンド出力を処理することにより、シスコ ワイヤレス コントローラの HA の正常性を分析します。このワークフローは、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラと、Cisco IOS XE リリース 17.1 以降を実行しているクラウド向け Cisco Catalyst 9800-CL ワイヤレスコントローラでサポートされています。この手順により、MRE ワークフローを使用して ワイヤレスコントローラ の HA の問題をトラブルシューティングできます。

始める前に

機械推論エンジン（MRE）ナレッジベースが最新のナレッジパックで更新されていることを確認します。詳細については、『*Cisco Catalyst Center Administrator Guide*』の「Update the Machine Reasoning Knowledge Base」[英語] のトピックを参照してください。

手順

ステップ 1 メインメニューから次を選択します。**[Tools]** > **[Network Reasoner]** の順に選択します。

また、**[Provision]** > **[Inventory]**ウィンドウから、ワイヤレスコントローラ の HA の問題をトラブルシューティングすることもできます。 ワイヤレスコントローラに HA の問題がある場合は、ワイヤレスコントローラの横に赤色のリンクアイコン（🔗）が表示されます。HA の問題をトラブルシューティングするには、赤色のリンクアイコンをクリックし、[HA SSO Analysis] をクリックします。ステップ 5 （1599 ページ）にスキップします。

ステップ 2 [Catalyst 9800 Wireless Controller HA SSO Analysis] タイルをクリックします。
[Devices] ウィンドウに ワイヤレスコントローラ が表示されます。ワイヤレスコントローラ で HA が設定されている場合、Catalyst Center ではデバイス名の横にリンクアイコン（🔗）が表示されます。赤色のリンクアイコン（🔗）は、ワイヤレスコントローラ の HA に問題があることを示しています。

ステップ 3 左側の階層ツリーから目的のサイトを選択します。

ステップ 4 トラブルシュートするデバイス名の横にあるオプションボタンをクリックしてから、[Troubleshoot] をクリックします。

必要に応じて、進行中の推論アクティビティを停止するには、[Stop] をクリックします。

ステップ 5 トラブルシューティングが完了すると、[Machine Reasoning Completed] ダイアログボックスが表示されます。**[Show Details]** をクリックします。

ステップ 6 [Root Cause Analysis] エリアの [Reasoning Activity] タブには、トラブルシューティング プロセスで確認されるパラメータが表示されます。アクティビティの詳細を表示するには、対応するアクティビティのタイルをクリックします。

分析では、次のパラメータが記載されている順序で使用されます。

番号	MRE 分析パラメータ	説明
1	[Check Controller Manageability]	• ワイヤレスコントローラで Cisco IOS XE リリース 17.1 以降が実行されているかどうかを確認します。 • ワイヤレスコントローラの IP アドレスが到達可能状態であるかどうかを確認します。 • SNMP、CLI ログイン情報、および NETCONF を確認します。 • ワイヤレスコントローラが Cisco Catalyst 9800 シリーズ ワイヤレス コントローラまたはクラウド向け Cisco Catalyst 9800-CL ワイヤレスコントローラであるかどうかを確認します。
2	[Evaluate Catalyst Center platform]	プラットフォーム内のすべてのサービスが Catalyst Center ISO の一部であるかどうかを確認します。
3	[Check HA is configured in Controller]	アクティブおよびスタンバイ ワイヤレスコントローラ のセンサーが正常なしきい値範囲内で動作しているかどうかを確認します。
4	[Check Primary device and Secondary device status in HA Pair]	ワイヤレスコントローラで HA 設定が完了しているかどうかを確認します。
5	[Show RP and RMI status]	Cisco IOS XE リリース 17.6 以降を実行しているアクティブ ワイヤレス コントローラとスタンバイ ワイヤレスコントローラの間にある冗長ポート（RP）リンクおよび冗長管理インターフェイス（RMI）リンクの接続を確認します。

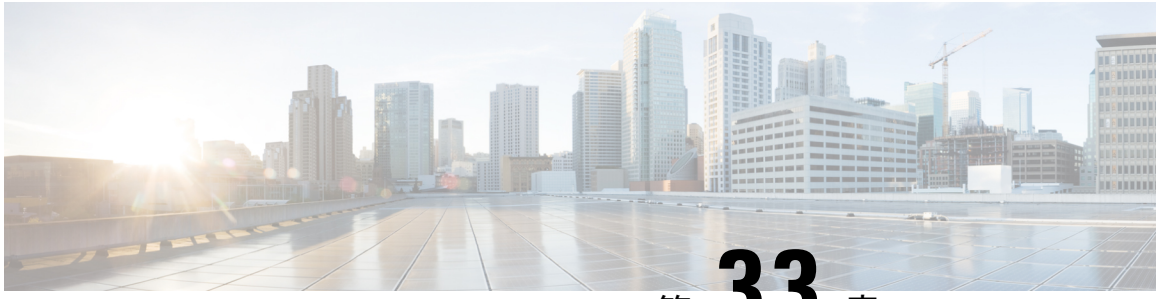
番号	MRE 分析パラメータ	説明
6	[Check the HA Status]	• スタンバイ ワイヤレスコントローラが HA 削除状態であるかどうかを確認します。 • スタンバイ ワイヤレスコントローラ同期が進行中かどうかを確認します。 • スタンバイ ワイヤレスコントローラの電源と RP ネットワーク接続が予期どおりに動作しているかどうかを確認します。 • アクティブとスタンバイの両方の ワイヤレスコントローラが同じイメージバージョンを実行しているかどうかを確認します。
7	[Secondary device deletion check]	• HA が正常に設定されているかどうかを確認します。 • スタンバイ ワイヤレスコントローラが削除状態であるかどうかを確認します。

ステップ 7 [Conclusions] タブには、トラブルシューティングの情報が表示されます。Catalyst Center では、⚠アイコンによって問題が強調表示されます。問題の下の [Suggested Action] エリアに、問題を解決するための推奨アクションが表示されます。

ステップ 8 （任意） デバイスのトラブルシューティング プロセスをもう一度実行する場合は、[Run Again] をクリックします。

次のタスク

HA の問題が根本原因のリストにない場合、または追加の支援が必要な場合は、Cisco Technical Assistance Center（TAC）にお問い合わせください。



第 33 章

ネットワークバグの特定

- ネットワークバグ識別ツールの概要 （1601 ページ）
- ネットワークのバグのスキャン （1602 ページ）
- Catalyst Center のバグのスキャン （1604 ページ）

ネットワークバグ識別ツールの概要

Catalyst Center のネットワークバグ ID ツールを使用すると、ネットワークをスキャンして、以前に識別され、シスコが認識している、選択された一連の障害またはバグを検出することができます。

Catalyst Center のネットワークバグ ID は、デバイス設定またはデバイスの動作データ内の特定パターンを識別するために役立ちます。それらのパターンに基づいて、既知の障害と照合することができます。このツールは、バグに焦点を合わせたビューとデバイスに焦点を合わせたビューの両方を提供します。

Catalyst Center は、ネットワークデバイスで CLI コマンドを実行してネットワークデバイスの構成と運用データを収集し、その情報を CX Cloud に送信して、潜在的なセキュリティアドバイザリやバグの公開に使用されます。Catalyst Center はネットワークバグ識別ツールのために次の CLI コマンドを呼び出します。

- **show buffers summary**
- **show cef interfaces**
- **show clock**
- **show crypto eli all**
- **show crypto isakmp sa detail**
- **show eigrp service-family ipv4 neighbors**
- **show environment all**
- **show interfaces counters error**
- **show interfaces summary**

- **show inventory**
- **show ip interface brief**
- **show ip nat translations verbose**
- **show ip nbar protocol-discovery**
- **show ip nbar resources flow**
- **show ip nhrp**
- **show ip nhrp summary**
- **show ip route**
- **show ip ssh**
- **show ip vrf**
- **show logging**
- **show performance monitor cache detail**
- **show platform software route-map fp active map**
- **show pnp profile**
- **show redundancy**
- **show redundancy application group**
- **show running-config all**
- **show scp status**
- **show stackwise-virtual**
- **show startup-config**
- **show terminal**
- **show version**

ネットワークのバグのスキャン

次の手順を実行して、ネットワークバグ識別ツールを使用してバグを識別します。

始める前に

- Catalyst Center のコアパッケージをインストールします。詳細については、『*Cisco Catalyst Center Administrator Guide*』の「Download and Install Packages and Updates」を参照してください。
- 機械推論パッケージをインストールします。詳細については、『*Cisco Catalyst Center Administrator Guide*』の「Download and Install Packages and Updates」を参照してください。

手順

ステップ 1 メインメニューから次を選択します。**[Tools]** > **[Network Bug Identifier]** の順に選択します。

ステップ 2 [Scan Network] をクリックします。

ステップ 3 **[ネットワークスキャン（Scan Network）]** ウィンドウで、システムのバグを今すぐスキャンする（[今すぐ（Now）]）か、後で実行するようにスケジュールする（[後で（Later）]）を選択します。

ダッシュボードの進捗状況インジケータには、スキャンされたデバイスのリスト（10 台ずつ）が表示されます。スキャンが完了すると、[Network Bug Identifier] ウィンドウが表示されます。

ステップ 4 次の表で説明されているとおり、上部のペインを使用して、スキャンの結果に関する情報を表示したり、ネットワークを再スキャンしたり、スキャン設定を変更したりできます。

アイテム	説明
Bug Summary	ネットワーク内の [Catastrophic]、[Severe]、および [Moderate] のバグの数。
Affected Devices	スキャンされたデバイスタイプの数。 • ルータ • スイッチとハブ
Scan Mode	スキャンの実行に使用された方法： • **Essential**：Cisco Network Reasoner Engine（NRE）を使用して実行されるスキャン。 • **CX Cloud**：CX Cloud を使用して実行されるスキャン。
Re-scan Network	このボタンをクリックして、ネットワークを再度スキャンします。
Settings	[設定（Settings）] アイコンをクリックして、次のタスクを実行します。 • 毎週のスキャンを有効または無効にします。 • CX Cloud によるネットワークのスキャンを有効または無効にします。

ステップ 5 [Bugs on Devices] タブをクリックして、バグに関する情報を表示します（[Bug ID]、[Name]、[Affected Devices]、[Severity]、[Affected Versions]、[Workaround] など）。

ハイパーリンクされた値をクリックすると、その値に関する詳細が表示されます。

ステップ 6 [Devices] タブをクリックして、デバイスに関する情報を表示します（[Device Name]、[Image Version]、[IP Address]、[Device Type]、[Bugs]、[Scan Status]、[Scan Mode]、[Site]、[Reachability] など）。

ハイパーリンクされた値をクリックすると、その値に関する詳細が表示されます。

ステップ 7 [Devices] タブで、[Tag Device] をクリックして、デバイスのタグを作成、編集、または削除します。

Catalyst Center のバグのスキャン

システムバグ ID ツールには、Catalyst Center のバグを識別するためのオプションがあります。この手順では、システムバグ識別ツールを有効にする方法について説明します。

始める前に

- Catalyst Center のコアパッケージをインストールします。詳細については、『*Cisco Catalyst Center Administrator Guide*』の「Download and Install Packages and Updates」を参照してください。
- 機械推論パッケージをインストールします。詳細については、『*Cisco Catalyst Center Administrator Guide*』の「Download and Install Packages and Updates」を参照してください。

手順

ステップ 1 メインメニューから次を選択します。**[Tools]** > **[Network Reasoner]** の順に選択します。

ステップ 2 [System Bug Identifier] を選択します。

ステップ 3 [Scan System] をクリックします。

ステップ 4 **[Scan System]** ウィンドウで、システムのバグを今すぐスキャンする（**[Now]**）か、後でスキャンするようにスケジュールするか（**[Later]**）を選択します。

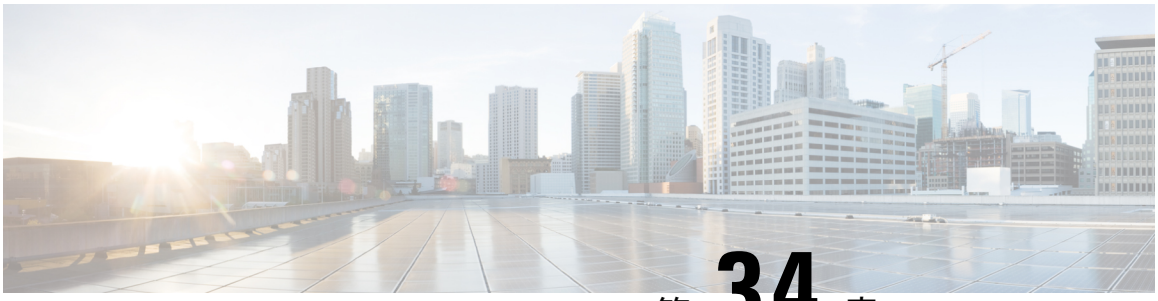
（注） ウィンドウの上部に表示されるバナーの [here] リンクをクリックして、デバイス設定に基づいてカスタマイズされたバグ情報へのアクセスを提供する新しいトライアルを作成します。

ステップ 5 [System Bug Identifier] ウィンドウには、[BUG SUMMARY] と [Bugs Identified on Your System] テーブルが表示されます。

このウィンドウには、基本的なバグ情報に加えて、バグが最初に特定された時期と最後に特定された時期、特定された頻度、影響を受けるバージョンなどの情報が表示されます。

ステップ 6 [Bug ID] をクリックします。
[Bug Details] ダイアログボックスに、バグの詳細情報が表示されます。

ステップ 7 [Bug ID] の横にある矢印をクリックし、[Bug Search Tools] ウィンドウに移動して、バグの詳細情報を確認します。



第 34 章

ネットワーク セキュリティ アドバイザリの識別

- セキュリティアドバイザリの概要 （1605 ページ）
- 前提条件 （1606 ページ）
- セキュリティアドバイザリの表示 （1606 ページ）
- セキュリティ アドバイザリ スキャンのスケジュール設定 （1608 ページ）
- セキュリティアドバイザリのために呼び出される CLI コマンド （1610 ページ）
- ネットワークを再スキャンしてセキュリティアドバイザリを特定 （1611 ページ）
- アドバイザリからのデバイスの表示/非表示 （1611 ページ）
- デバイスからのアドバイザリの表示/非表示 （1612 ページ）
- セキュリティ アドバイザリ ナレッジ バンドルの通知の追加 （1613 ページ）
- インベントリでのセキュリティアドバイザリの表示 （1614 ページ）
- 一致パターンの追加 （1615 ページ）
- 一致パターンの AND/OR の定義 （1616 ページ）
- 一致パターンの編集 （1616 ページ）
- 一致パターンの削除 （1617 ページ）

セキュリティアドバイザリの概要

Cisco Product Security Incident Response Team（PSIRTT; プロダクト セキュリティ インシデント レスポンス チーム）は、シスコ製品セキュリティインシデントに対応し、セキュリティ脆弱性ポリシーを規制し、シスコのセキュリティアドバイザリとアラートを推奨します。

セキュリティ アドバイザリ ツールは、これらの推奨されるアドバイザリを使用して、Catalyst Center 内のインベントリをスキャンし、既知の脆弱性を持つデバイスを検出します。

前提条件

セキュリティ アドバイザリ ツールを使用するには、機械推論パッケージをインストールする必要があります。『Cisco Catalyst Center 管理者ガイド』の「Download and Install Packages and Updates」を参照してください。

オブザーバとして Catalyst Center にログインすると、ホームページで [セキュリティアドバイザリ（Security Advisories）] ツールを表示できません。

セキュリティアドバイザリの表示

手順

ステップ 1 メインメニューから次を選択します。**[Tools]** > **[Security Advisories]** の順に選択します。

ステップ 2 [Security Advisories] ページを初めて起動する場合は、[Scan Network] をクリックします。

Catalyst Center では、セキュリティの問題を特定して自動分析を改善するためにナレッジベースを使用します。最新のセキュリティアドバイザリを表示するには、定期的にナレッジベースを更新することをお勧めします。

a) メインメニューから次を選択します。**System** > **Settings** > **Machine Reasoning Engine** の順に選択します。

b) [Import] をクリックするか、[Download Latest] をクリックして最新の使用可能なナレッジベースをダウンロードします。ダウンロードが完了したら、[Import] をクリックしてください。

c) 自動更新に登録するには、[AUTO UPDATE] トグルボタンをクリックします。

（注） 上部のバナーの **[here]** リンクをクリックして、デバイス設定に基づいてカスタマイズされた Field Notice へのアクセスを提供する新しいトライアルを作成します。

ステップ 3 [アドバイザリ（ADVISORIES）] エリアには、[重大（Critical）] や [高（High）] など、ネットワークに対するそれぞれの影響の割合が表示されます。

（注） [中（Medium）]、[低（Low）]、または [情報（Informational）] アドバイザリは、[セキュリティアドバイザリ（Security Advisories）] ページに表示されなくなりました。

ステップ 4 スキャンは、各デバイスに関連付けられているライセンスに基づいてデバイスで実行されます。[スキャン基準（SCAN CRITERIA）] エリアで、次の順序に従ってアドバイザリをデバイスと一致させます。

- [Software Version]：スキャンは、**Essentials** ライセンスを持つデバイスでソフトウェアバージョンに基づいて実行されます。
- [Custom]：スキャンは、**Advantage** ライセンスを持つデバイスで、ソフトウェアバージョンと、デバイスの実行コンフィギュレーションに対するアドバイザリ（ある場合）に関して入力されたカスタム設定に基づいて実行されます。
- [Advanced]：スキャンは、**Cisco CX Cloud Success Track** の利用資格を持つデバイスで、ソフトウェアバージョン、設定、および運用データに基づいて実行されます。

  トライアル期間中はソフトウェア利用資格が適用されず、すべてのデバイスが [Advanced] レベルでスキャンされます。

（注）
- セキュリティ アドバイザリ ダッシュボードにはシスコが公開しているセキュリティアドバイザリが表示されます。セキュリティアドバイザリは、インストールされているソフトウェアイメージに基づいて、ネットワーク上のデバイスに影響を及ぼす場合があります。脆弱性が実際に存在するかどうかを判断するには、設定、プラットフォームの詳細、またはその他の基準をさらに詳しく分析する必要があります。
- セキュリティ アドバイザリ スキャンは、サポートされている最小ソフトウェアバージョン以上を実行しているルータ、スイッチ、ハブ、ワイヤレスコントローラでのみ使用できます。詳細については、『Catalyst Center Compatibility Matrix』を参照してください。
- 表示されるセキュリティアドバイザリは、「シスコのセキュリティ脆弱性ポリシー」に基づいています。

次の表に、参照できる情報を記載します。

カラム	説明
Advisory ID	ネットワークで検出されたセキュリティアドバイザリの ID。ID をクリックして、それぞれのアドバイザリ Web ページに移動します。
Advisory title	ネットワークデバイスに適用可能なセキュリティ脆弱性アドバイザリの名前。
CVSS score	共通脆弱性評価システム（CVSS）モデルに基づいて評価されたスコア。
Impact	脆弱性がネットワークに及ぼす影響。
CVE	脆弱性の Common Vulnerabilities and Exposures（CVE）識別子。
Devices	脆弱性の影響を受けるデバイスの数。この特定のアドバイザリに基づいて脆弱性が存在する可能性のあるデバイスを表示するには、番号をクリックし、必要に応じてデバイスをアップグレードします。
Match Type	検出された脆弱性が [Image Version] の一致と [Configuration] の一致のどちらに基づくかを示します。

カラム	説明
Known since (days)	脆弱性が検出されてからの経過日数。
Last updated	アドバイザリが最後に更新された日付。

ステップ 5 [FAILED DEVICES] エリアには、将来の日時にスケジュールされたデバイススキャンに関する情報が表示されます。

（注） [FAILED DEVICES] エリアは、スキャンに失敗したデバイスがあり、スキャンが自動的にスケジュールされる場合にのみ表示されます。

ステップ 6 [Advisories] テーブルで [All] タブをクリックして、すべてのアドバイザリを一覧表示します。

ステップ 7 [Advisories] テーブルで [Affecting Devices] タブをクリックして、影響するデバイスに基づいたアドバイザリを表示します。

ステップ 8 各デバイスに適用可能なアドバイザリの数を表示するには、[Devices] タブをクリックします。

a) デバイスに一致するものをすべて表示するには、アドバイザリの数をクリックします。

b) デバイストポロジを表示するには、右上隅にあるトポロジアイコンをクリックします。トポロジ内のデバイスをクリックすると、デバイスに一致するすべてのアドバイザリが表示されます。

デバイスの横にあるロックアイコンは、デバイスに適用可能な 1 つ以上のアドバイザリがあることを示します。

[Fixed Version] 列には、アドバイザリが適用されたバージョンが表示されます。この列に示されているバージョンにアップグレードすることで、デバイス上のアドバイザリを削除できます。

ステップ 9 [Re-scan Network] をクリックして、ネットワークのスキャンを再度実行します。

自動設定スキャンの詳細については、ネットワークを再スキャンしてセキュリティアドバイザリを特定（1611 ページ）を参照してください。

セキュリティアドバイザリスキャンのスケジュール設定

手順

ステップ 1 メインメニューから次を選択します。**[Tools]** > **[Security Advisories]** の順に選択します。

ステップ 2 [Scan Network] をクリックします。

[Scan Network] ウィンドウが表示されます。

ステップ 3 セキュリティアドバイザリをすぐにスキャンするには、[Now] オプションボタンをクリックし、[Start] をクリックします。

ステップ 4 スキャンを後で実行するようにスケジュールするには、[Later] オプションボタンをクリックし、日付と時刻を指定します。

ステップ 5 [Time Zone] ドロップダウンリストを使用して、スキャンのスケジュール設定に使用するタイムゾーンを選択します。

ステップ 6 繰り返しオプションとして [None]（デフォルト）、[Daily]、[Weekly] のいずれかを選択します。

ステップ 7 [Run at Interval] フィールドに、スキャンの繰り返しの間隔（日または週の数）を入力します。

ステップ 8 （オプション）スケジュールの終了日や終了までの回数を指定する場合は、[Set Schedule End] チェックボックスをオンにします。

a) スキャン終了日をスケジュールするには、[End Date] オプションボタンをクリックし、日付と時刻を定義します。

b) スキャンの繰り返し回数を定義するには、[End After] オプションボタンをクリックします。

ステップ 9 [Schedule] をクリックします。

ステップ 10 メインメニューから次を選択します。**[Activities]** > **[Tasks]** の順に選択して、スキャンのスケジュールと繰り返しを確認します。

（注） Catalyst Center リリース 2.1.1.x 以降では、シスコによるテレメトリの収集を許可するかどうかを選択できます。収集を許可すると、cisco.com ID、システムテレメトリ、機能使用状況テレメトリ、ネットワーク デバイス インベントリ、およびソフトウェア利用資格の情報が収集されます。テレメトリは、アプリケーションごとや機能ごとではなく、Catalyst Center 全体について開示されます。Catalyst Center 2.1.1.x 以降では、テレメトリの収集は必須です。収集されたテレメトリは、ユーザーが使用している機能の開発に役立てられます。収集されるデータの詳しいリストについては、*Cisco DNA Center* データシート [英語] を参照してください。

セキュリティ アドバイザリ スキャンの実行時に収集されるテレメトリデータは次のとおりです。

- ナレッジパッケージの自動更新が設定されているかどうか。
- 繰り返しのスキャンおよび繰り返しのレポートが設定されているかどうか。
- 実行されたレポートの数。
- ソフトウェアのバージョンと設定に基づいて一致するセキュリティアドバイザリがあるデバイスの数。
- 各スキャンの受理と拒否の数。
- 検索で入力された手動設定とそれに関連するアドバイザリ。
- ソフトウェアのバージョンと設定（製品ファミリを含む）が一致するアドバイザリの数。
- 他のカテゴリ（アドバイザリなし、不明、サポート対象外）に基づくデバイスの数。
- 成功したスキャン、失敗したスキャン、終了したスキャンの数。
- 平均スキャン時間。

セキュリティアドバイザリのために呼び出される CLI コマンド

Catalyst Center は、ネットワークデバイスで CLI コマンドを実行してネットワークデバイスの構成と運用データを収集し、その情報を CX Cloud に送信して処理され、可能性があるセキュリティアドバイザリやバグのリスクを可視化します。Catalyst Center はセキュリティアドバイザリのための次の CLI コマンドを呼び出します。

- **show inventory**
- **show running-config**
- **show version**

ネットワークを再スキャンしてセキュリティアドバイザリを特定

ネットワークを再スキャンし、自動構成スキャンに基づいてセキュリティアドバイザリを特定するには、次の手順を実行します。

始める前に

Cisco CX Cloud サービスを有効にする必要があります。詳細については、*Cisco Catalyst Center Administrator Guide*の「**Update the Machine Reasoning Knowledge Base**」を参照してください。

手順

ステップ 1 メインメニューから次を選択します。**[Tools]** > **[Security Advisories]** > **[Advisories]** の順に選択します。

ステップ 2 [Re-Scan Network] をクリックして、ネットワークスキャンを再度開始します。

ステップ 3 セキュリティアドバイザリをすぐに再スキャンするには、[Now] オプションボタンをクリックし、[Start] をクリックします。

ステップ 4 再スキャンを後で実行するようにスケジュールするには、[Later] オプションボタンをクリックし、詳細を指定します。詳細については、セキュリティアドバイザリ スキャンのスケジュール設定（1608 ページ）を参照してください。

[Device] テーブルで、[Advisories] 列がアドバイザリの数で更新されます。

- Catalyst Center ネットワークの再スキャンは、プラットフォームの詳細や CX Cloud ソフトウェアのバージョンなどの他の詳細とともに、デバイスの実行コンフィギュレーションを送信します。情報は処理され、Catalyst Center に返送されます。Catalyst Center 上で実行されている Machine Reasoning Engine（MRE）は、Cisco CX Cloud によって提供されるデバイスに対してアドバイザリをマッピングします。
- Catalyst Center で特定のデバイスの正しいライセンスレベルを判断できない場合、セキュリティ アドバイザリ スキャンはソフトウェアバージョンごとのスキャンにフォールバックします。

アドバイザリからのデバイスの表示/非表示

手順

ステップ 1 メインメニューから次を選択します。**[Tools]** > **[Security Advisories]** の順に選択します。

ステップ 2 [Security Advisories] ウィンドウを初めて起動する場合は、[Scan Network] をクリックします。

ステップ 3 [Scan Network] ウィンドウで、[Now] を選択し、[Start] をクリックします。

ステップ 4 アドバイザリからのデバイスを非表示にするには、次の手順を実行します。

a) [Focus] ドロップダウンリストから、[Advisories] を選択します。

b) [Devices] 列で、デバイスを非表示にするアドバイザリに対応するデバイス数をクリックします。

[Active] タブには、これらのアドバイザリが発行されたデバイスの数が表示されます。

c) 非表示にするデバイスを選択し、[Suppress Device] をクリックします。

非表示にしたデバイスは、[Suppressed] タブで確認できます。

d) アドバイザリウィンドウを閉じ、このアドバイザリのデバイス数の変化を確認します。

ステップ 5 アドバイザリからのデバイスを復元するには、次の手順を実行します。

a) [Focus] ドロップダウンリストから、[Advisories] を選択します。

b) [Devices] 列で、デバイスを再表示するアドバイザリに対応するデバイス数をクリックします。

c) [Suppressed] タブをクリックして、非表示のデバイスを表示します。

d) 再表示するデバイスを選択し、[Mark as Active] をクリックします。

復元されたデバイスは、[Active] タブで確認できます。

e) アドバイザリウィンドウを閉じ、このアドバイザリのデバイス数の変化を確認します。

デバイスからのアドバイザリの表示/非表示

手順

ステップ 1 メインメニューから次を選択します。**[Tools]** > **[Security Advisories]** の順に選択します。

ステップ 2 [Security Advisories] ページを初めて起動する場合は、[Scan Network] をクリックします。

ステップ 3 [Scan Network] ウィンドウで、[Now] を選択し、[Start] をクリックします。

ステップ 4 デバイスのアドバイザリを非表示にするには、次の手順を実行します。

a) [Focus] ドロップダウンリストから、[Devices] を選択します。

b) [Advisories] 列で、アドバイザリを非表示にするデバイスに対応するアドバイザリカウントをクリックします。

[Active] タブには、このデバイスに対して発行されたアドバイザリの数が表示されます。

c) 非表示にするアドバイザリを選択し、[Suppress Advisory] をクリックします。

非表示のアドバイザリは、[Suppressed] タブで確認できます。

d) デバイスウィンドウを閉じ、このデバイスのアドバイザリカウントの変化を確認します。

ステップ 5 デバイスのアドバイザリを復元するには、次の手順を実行します。

a) [Focus] ドロップダウンリストから、[Devices] を選択します。
b) [Advisories] 列で、アドバイザリを再表示するデバイスに対応するアドバイザリカウントをクリックします。
c) [Suppressed] タブをクリックして、非表示のアドバイザリを表示します。
d) 再表示するアドバイザリを選択し、[Mark as Active] をクリックします。

   復元されたアドバイザリは、[Active] タブで確認できます。

e) デバイスウィンドウを閉じ、このデバイスのアドバイザリカウントの変化を確認します。

セキュリティ アドバイザリ ナレッジ バンドルの通知の追加

セキュリティ アドバイザリ ナレッジ バンドル（KB）は、機械推論エンジン（MRE）を使用してネットワークをスキャンします。新しいセキュリティアドバイザリの KB が利用可能になったときに通知するように Catalyst Center を設定できます。通知を有効にすると、新しいセキュリティアドバイザリの KB が利用可能になるたびに、Catalyst Center から視覚的な通知と実用的なアラートが表示されます。

新しいセキュリティアドバイザリ KB の通知を追加するには、次の手順を実行します。

始める前に

- Catalyst Center のコアパッケージをインストールする必要があります。『*Cisco Catalyst Center Administrator Guide*』の「Download and Install Packages and Updates」を参照してください。
- 機械推論（MRE）パッケージをインストールする必要があります。『*Cisco Catalyst Center Administrator Guide*』の「Download and Install Packages and Updates」を参照してください。
- 次のコンテナがシステムに存在している必要があります。
  - cnsr-reasoner
  - cloud connectivity/download

手順

ステップ 1 Catalyst Center GUI の右上隅にある通知アイコンをクリックします。ドロップダウンメニューから、歯車のアイコンを選択して通知設定を表示します。

ステップ 2 [My Profile and Settings] ウィンドウで、[Security Advisories] オプションを選択してセキュリティアドバイザリ通知を有効にします。

ステップ 3 [保存（**Save**）] をクリックします。

ステップ 4 [Machine Reasoning Engine] ウィンドウで、[Download Latest] リンクをクリックして最新のナレッジバンドルをダウンロードします。

ステップ 5 ナレッジベースの設定を確認して更新します。

ステップ 6 [Security Advisory Settings] セクションで、繰り返しオプションとして [None]（デフォルト）、[Daily]、または [Weekly] を選択します。

ステップ 7 **[通知センター（Notification Center）]** > **[セキュリティアドバイザリに移動（Go to Security Advisories）]** の順に選択し、[セキュリティアドバイザリ（Security Advisories）] ツールウィンドウを直接表示します。

ステップ 8 新しくダウンロードしたセキュリティアドバイザリでネットワークを再スキャンします。詳細については、セキュリティ アドバイザリ スキャンのスケジュール設定 （1608 ページ）を参照してください。

インベントリでのセキュリティアドバイザリの表示

Catalyst Center のセキュリティ フォーカス ビューでは、前回のセキュリティスキャンで取得したデータに基づいて、デバイスのセキュリティアドバイザリのリストを表示します。[Security Advisories] ツールから取得したデバイスデータは [Inventory] ウィンドウに表示されます。

セキュリティアドバイザリを表示するには、次の手順を実行します。

始める前に

- Catalyst Center のコアパッケージをインストールする必要があります。『*Cisco Catalyst Center Administrator Guide*』の「Download and Install Packages and Updates」を参照してください。
- 機械推論パッケージをインストールする必要があります。『*Cisco Catalyst Center Administrator Guide*』の「Download and Install Packages and Updates」を参照してください。

手順

ステップ 1 メインメニューから次を選択します。**[Tools]** > **[Security Advisories]** の順に選択します。

ステップ 2 [Scan Network] をクリックします。

ステップ 3 セキュリティアドバイザリをすぐにスキャンするには、[Now] オプションボタンをクリックし、[Start] をクリックします。

ステップ 4 メインメニューから次を選択します。**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。

ステップ 5 [FOCUS: Inventory] ドロップダウンメニューから [Security] を選択します。
[アドバイザリ（Advisories）] 列が [インベントリ（Inventory）] テーブルに表示されます。

ステップ 6 [Device Details] ウィンドウで、デバイスを選択し、アドバイザリデータを確認します。

ステップ 7 [Manage All] をクリックして**セキュリティアドバイザリ** ツールに移動します。

一致パターンの追加

特定のデバイス条件でアドバイザリの影響を受けるデバイスと影響を受けないデバイスを確認するには、ネットワークスキャンを実行する前にアドバイザリに一致パターンを追加しておきます。

新しいネットワークスキャンを実行する場合、Catalyst Centerは最初に、デバイスのソフトウェアバージョンがアドバイザリに記載されているソフトウェアバージョンと一致するかどうかを確認します。バージョンが一致しない場合、アドバイザリの一致パターンは無視されます。バージョンが一致する場合、Catalyst Center はデバイス設定と一致パターンの一致をチェックします。一致がある場合、影響を受けるアドバイザリが影響を受けるデバイスにアタッチされます。一致しない場合、影響を受けるアドバイザリは影響を受けるデバイスからデタッチされます。

（注） この機能は、基本スキャン基準のみを使用したネットワークスキャンに適用されます。

手順

ステップ 1 メインメニューから次を選択します。**[Tools]** > **[Security Advisories]** の順に選択します。

ステップ 2 [Security Advisories] ウィンドウを初めて起動する場合は、[Scan Network] をクリックします。

ステップ 3 [Scan Network] ウィンドウで、[Now] を選択し、[Start] をクリックします。

ステップ 4 アドバイザリを選択し、[Match Type] 列で [Add match pattern] をクリックします。

ステップ 5 [Add Configuration Match Pattern] ウィンドウで、[CONDITIONS] テキストボックスにデバイスと一致する条件を入力します。

ステップ 6 **[保存（Save）]** をクリックします。

一致パターンがアドバイザリに追加されます。

ステップ 7 [Scan Network] をクリックします。

[スキャン済み（Scanned）] フィルタを選択すると、[デバイス（Devices）] テーブルにスキャンされたデバイスの結果が表示されます。

一致パターンの AND/OR の定義

手順

ステップ 1 メインメニューから次を選択します。**[Tools]** > **[Security Advisories]** の順に選択します。

ステップ 2 [Security Advisories] ページを初めて起動する場合は、[Scan Network] をクリックします。

ステップ 3 [Scan Network] ウィンドウで、[Now] を選択し、[Start] をクリックします。

ステップ 4 アドバイザリを選択し、[Match Type] 列で [Add match pattern] をクリックします。

ステップ 5 **[設定一致パターンの追加（Add Configuration Match Pattern）]** ウィンドウで、次の手順を実行します。

a) [CONDITIONS] テキストボックスに条件を入力し、[Add] アイコンをクリックします。
b) ドロップダウンリストから、[AND] または [OR] を選択し、次の条件を入力します。
c) 条件を削除する場合は、[Remove] アイコンをクリックします。
d) **[保存（Save）]** をクリックします。
一致パターンがアドバイザリに追加されます。

ステップ 6 [Scan Network] をクリックして、一致パターンに一致するデバイスの数を確認します。

一致パターンの編集

手順

ステップ 1 メインメニューから次を選択します。**[Tools]** > **[Security Advisories]** の順に選択します。

ステップ 2 [Security Advisories] ページを初めて起動する場合は、[Scan Network] をクリックします。

ステップ 3 [Scan Network] ウィンドウで、[Now] を選択し、[Start] をクリックします。

ステップ 4 すでに一致パターンがあるアドバイザリを選択し、[Match Type] 列で [Edit match pattern] をクリックします。

ステップ 5 [Edit Configuration Match Pattern] ウィンドウで、[CONDITIONS] テキストボックスにデバイスと一致する条件を入力します。

ステップ 6 **[保存（Save）]** をクリックします。

一致パターンが変更されます。

ステップ 7 [Scan Network] をクリックして、一致パターンに一致するデバイスの数を確認します。

一致パターンの削除

手順

ステップ 1 メインメニューから次を選択します。**[Tools]** > **[Security Advisories]** の順に選択します。

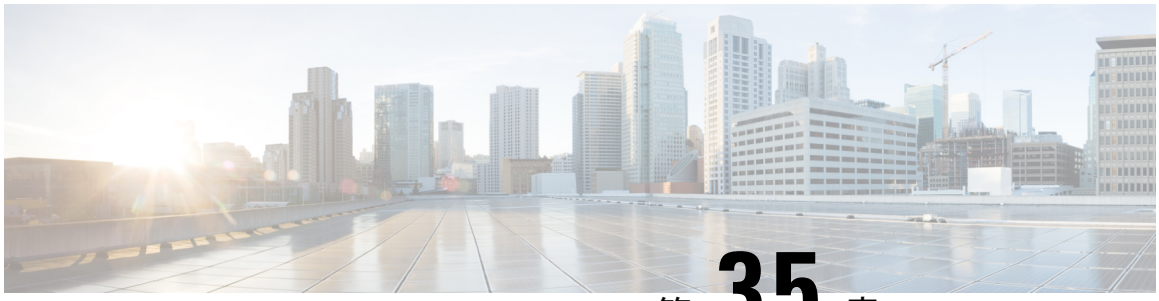
ステップ 2 [Security Advisories] ページを初めて起動する場合は、[Scan Network] をクリックします。

ステップ 3 [Scan Network] ウィンドウで、[Now] を選択し、[Start] をクリックします。

ステップ 4 すでに一致パターンがあるアドバイザリを選択し、[Match Type] 列で [Edit match pattern] をクリックします。

ステップ 5 [Edit Configuration Match Pattern] ウィンドウで、[Delete] をクリックします。

一致パターンが削除されます。



第 35 章

ネットワークの Field Notice の特定

- Field Notice ID ツールの概要 （1619 ページ）
- Field Notice の表示 （1619 ページ）

Field Notice ID ツールの概要

Field Notice とは、セキュリティ脆弱性の問題以外でシスコ製品に直接関係する重要な問題に関する通知です。通常、アップグレード、回避策、またはその他の対策が必要となります。

Field Notice ツールはこれらの通知を使用して、Catalyst Center 内のインベントリをスキャンして、既知の問題があるデバイスを検出します。

Field Notice の表示

手順

ステップ 1 メインメニューから次を選択します。**[Tools]** > **[Field Notices]** の順に選択します。

ステップ 2 [Field Notices] ウィンドウを初めて起動する場合は、[Scan Network] をクリックします。

ステップ 3 [ネットワークのスキャン（Scan Network）] ウィンドウで、次の手順を実行します。

a) 必要に応じて、デフォルトの [タスク名（Task Name）] を編集します。

b) ネットワークをすぐにスキャンする場合は **[Now]** をクリックし、後でスキャンする場合は **[Later]** をクリックします。

（注） 上部のバナーの **[here]** リンクをクリックして、デバイス設定に基づいてカスタマイズされた Field Notice へのアクセスを提供する新しいトライアルを作成します。

ステップ 4 スキャンが完了すると、[FIELD NOTICES] エリアに、ハードウェアおよびソフトウェアの問題に関する Field Notice が表示されます。デバイスとそのデバイスで特定された問題のリストを表示するには、[デバイス（Devices）] タブをクリックし、次の手順を実行します。

a) **[SUMMARY]** エリアで **[Devices Family]** を展開し、そのデバイスファミリ（**[Routers]**、**[Switches and Hubs]**、**[Unified AP]**、または **[Wireless Controller]**）をフィルタ処理します。

b) **[Scan Status]** を展開し、**[Success]**、**[Failed]**、または **[Not Scanned]** に基づいてデバイスをフィルタ処理します。

[Devices] テーブルには、デバイス名（[Device Name]）、IP アドレス（[IP Address]）、デバイスファミリ（[Device Family]）、サイト（[Site]）、Field Notice（[Field Notice]）、潜在的な Field Notice（[Potential Field Notices]）、スキャンステータス（[Scan Status]）、最後のスキャン（[Last Scanned]）、サイト（[Site]）、および到達可能性（[Reachability]）に基づいてデバイスのリストが表示されます。

[Field Notices] 列と [Potential Field Notices] 列には、デバイスの Field Notice と潜在的な Field Notice の数が表示されます。

c) それぞれの列の番号をクリックすると、スライドインペインが開き、追加の詳細情報が表示されます。

d) スライドインペイン で、[Field Notices] または [Potential Field Notices] タブをクリックして、追加情報を含むテーブルを表示します。

（注） [Reason] 列は、潜在的な Field Notice についてのみ表示されます。

e) （オプション）[Details] タブをクリックして、ハードウェア、ソフトウェアの詳細、および動作の概要を表示します。

ステップ 5 [Field Notices] タブをクリックし、次の手順を実行します。

a) [SUMMARY] エリアで、[Field Notice Type] を展開します。

b) タイプとして「ハードウェア」（[Hardware]）または「ソフトウェア」（[Software]）を選択します。

[Field Notices] テーブルが表示され、追加情報が示されます。

c) [Affected Devices] 列に、影響を受けるデバイスの数が表示されます。番号をクリックすると、スライドインペイン が開き、追加の詳細情報が表示されます。

影響を受けるデバイスは、Field Notice について自動的に確認できるすべての基準を満たしています。デバイスが影響を受けていることを確認するために、追加の手動検証は必要ありません。

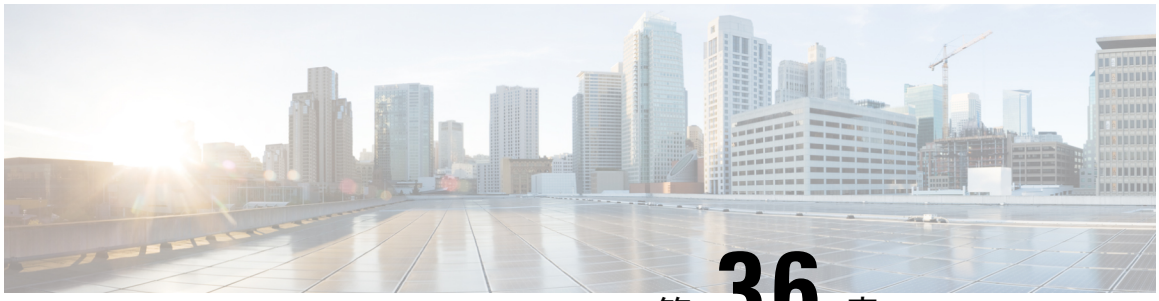
d) [Potentially Affected Devices] 列に、影響を受ける可能性のあるデバイスの数が表示されます。番号をクリックすると、スライドインペイン が開き、追加の詳細情報が表示されます。

影響を受ける可能性のあるデバイスは、Field Noticeについて自動的に確認できるすべての基準を満たしていますが、デバイスが影響を受けることを確認するために追加の手動検証が必要です。

ステップ 6 （オプション）[Re-scan Network] をクリックして、ネットワークのスキャンを再度実行します。

a) [Scan Network] スライドインペインで、システムの Field Notice を今すぐスキャンする（[Now]）か後でスキャンする（[Later]）かを選択し、[Submit] をクリックします。

b) 進捗状況を確認するには、メニューアイコンをクリックして次を選択します。**[Activities]** > **[Tasks]** の順に選択して、スキャンのスケジュールと繰り返しを確認します。



第 36 章

Catalyst Center からの根本原因分析ファイルの生成

- サポートバンドルの概要 （1623 ページ）
- プロビジョニング失敗の根本原因分析データの収集とアップロード （1623 ページ）

サポートバンドルの概要

サポートバンドルを使用すると、さまざまなサービスについて、よりモジュール化された詳細な根本原因分析（RCA）データを収集できます。RCA データには、ノード情報、Catalyst Center バージョン、パッケージ、ディザスタ リカバリ ステータス、パッケージ リリース バージョンなどのクラスタのメタデータに加えて、選択したサービスに固有の関連情報が含まれます。

プロビジョニング失敗の根本原因分析データの収集とアップロード

この手順では、プロビジョニングの失敗から根本原因分析（RCA）データを収集し、その RCA データを Cisco TAC サービスリクエスト（SR）にアップロードする方法を示します。

手順

ステップ 1 右上隅にあるヘルプアイコンをクリックし、**[Support Bundle]** を選択します。

ステップ 2 [サポート バンドルの作成（Create Support Bundle）] をクリックします。

ステップ 3 **[Create Support Bundle]** スライドインペイン で、サポートバンドルの名前と説明を入力します。

ステップ 4 サポートを要求する期間を選択し、システムカテゴリを選択します。

ステップ 5 [アプリケーション（Application）] ドロップダウンリストから、適用可能なサポートバンドルを選択します。

ステップ 6 [Have Cisco Personnel Requested Any Additional Parameters?] を展開し、RCA 収集を最適化するための追加パラメータを入力します。

ステップ 7 [Submit] をクリックします。

ステップ 8 **[Actions]** 列でダウンロードアイコンをクリックし、新しく作成したサポートバンドルをダウンロードします。

サポートバンドル RCA ファイルは、.tar.gz ファイル形式でダウンロードされます。

ステップ 9 RCA ファイルを Cisco TAC サービスリクエストにアップロードするには、**[Actions]** 列でアップロードアイコンをクリックします。

ステップ 10 [RCAアップロード：CLIの生成（RCA Upload - Generate CLI）] ウィンドウで、次の手順を実行します。

- **SR 番号** を入力します。
- **ファイル アップロード トークン** を入力します。
- **[Generate CLI Commands]** をクリックします。
- **[Copy]** をクリックして、CLI コマンドをコピーします。

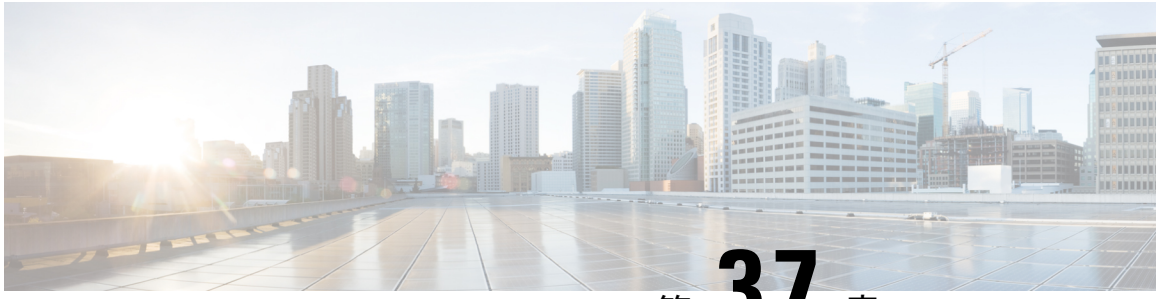
ステップ 11 Catalyst Center CLI にログインし、CLI シェルプロンプトに CLI コマンドを貼り付けます。



第 VIII 部

Catalyst Center の管理

- 構築と展開のワークフロー （1627 ページ）
- ワイヤレスネットワークの設定の使用例 （1689 ページ）
- ネットワークのエネルギーの管理 （1721 ページ）
- データプラットフォームを使用した Catalyst Center のトラブルシューティング （1733 ページ）



第 37 章

構築と展開のワークフロー

- Catalyst Center ワークフローナビゲーション （1627 ページ）
- デバイスの検出 （1628 ページ）
- AP 更新ワークフロー （1630 ページ）
- スイッチでのアプリケーション ホスティングの有効化 （1634 ページ）
- IoT サービスの有効化 （1637 ページ）
- Catalyst Center での AP 設定 （1638 ページ）
- デバイスの交換 （1664 ページ）
- スイッチの更新 （1670 ページ）
- リモートサポート許可の作成 （1673 ページ）
- イベント通知の作成 （1674 ページ）
- リモート LAN の設定 （1679 ページ）
- ファブリックサイトでの Parallel Redundancy Protocol の設定 （1684 ページ）

Catalyst Center ワークフローナビゲーション

Catalyst Center ワークフローはウィザードに似ています。ワークフローは GUI に組み込まれており、複雑すぎたり完了するには高度すぎるような多段階のタスクをガイドします。それらの多くには、さまざまなメニューオプションから、または [Workflows] メニューオプションから直接アクセスできます。

次のガイドラインを使用すると、ワークフローのナビゲートに役立ちます。

- ワークフローの手順に従い、[Next] をクリックして次のページに進みます。
- ワークフローの各ページの上部近くにカーソルを合わせると、進行状況バーが表示され、プロセスを完了するためのステップと現在実行中のステップが示されます。
- 一部のワークフローではダイアログボックスが開き、クリックすることでタスクの概要を視覚的に表示できます。タスクの概要の任意の時点で、[Let's Do it] をクリックして、ワークフローの最初に直接ジャンプできます。

  今後タスクの概要をスキップするには、[Don't show this to me again] チェックボックスをオンにします。

- 左下の隅で、[終了（Exit）] をクリックしてワークフローを終了します。次に、確認ダイアログボックスで、[終了（Exit）] をクリックします。進行状況は自動的に保存され、**[ワークフロー（Workflows）]** ウィンドウにはタスクのワークフローが進行中であるカードが表示されます。
- **[ワークフロー（Workflows）]** ウィンドウで、進行中のワークフローカードの右下の省略記号にカーソルを合わせ、[再開（Resume）] をクリックしてそのワークフローを再開します。

デバイスの検出

このワークフローは、デバイス検出からネットワークの正常性までをガイドします。

始める前に

- ディスカバリの前提条件 （75 ページ）で説明されているように、デバイスには必須のデバイス設定が存在する必要があります。
- シスコ検出プロトコル（CDP）を使用する場合は、ネットワークデバイスで CDP を有効にします。
- リンク層検出プロトコル（LLDP）を使用する場合は、ネットワークデバイスで LLDP を有効にします。
- クライアント IP アドレスとしてネットワークデバイスのホストの IP アドレスを設定します。（ホストは、ラップトップコンピュータまたはモバイルデバイスなどのエンドユーザデバイスです。）

手順

ステップ 1 メインメニューから次を選択します。**[Workflows]** > **[Discover Devices]** の順に選択します。

ステップ 2 タスクの概要ウィンドウが開いたら、[Let's Do It] をクリックして、ワークフローに直接移動します。

ステップ 3 [Discover Devices] ウィンドウで、次のフィールドに入力します。

a) 検出ジョブの名前を入力します。

b) [検出タイプ（Discovery Type）] で、デバイスの検出に使用するプロトコルを選択し、対応するフィールドに入力します。

- [CDP] ：[IP Address] 、[CDP Level] 、および [Subnet Filter] を入力します。
- [IP Address Range] ：[Starting IP Address] および [Ending IP Address] を入力します。
- [LLDP] ：[IP Address] 、[LLDP Level] 、および [Subnet Filter] を入力します。

c) [Preferred Management IP Address] を選択します。

ステップ 4 [Provide Credentials] ウィンドウで、必要に応じてディスカバリ クレデンシャルとその他の設定を行います。

少なくとも 1 つの CLI ログイン情報と 1 つの SNMP ログイン情報を入力します。このログイン情報は、Catalyst Center によって検出されたデバイスに対して構成されます。最大 5 つのグローバルログイン情報、およびタイプごとに 1 つのタスク固有のログイン情報を使用できます。詳細については、ディスカバリ クレデンシャル （76 ページ）を参照してください。

a) 左側のペインで、[CLI] をクリックして CLI ログイン情報を追加します。
b) [SNMP] を展開して、SNMP ログイン情報を追加します。
c) [Advanced Settings] を展開し、次の設定を行います。

設定	タスク
Protocol Order	[SSH] または [Telnet] を選択します。両方を選択した場合は、プロトコルを上下にドラッグして、使用する順序を指定できます。
SNMP Polling Properties	**[Network Settings]** > **[Device Credentials]** ウィンドウで定義されたグローバル SNMP ポーリングプロパティを使用するか、この検出インスタンス用に変更します。

（注） 必要に応じて、NETCONF、HTTP、HTTPS などの他のログイン情報を設定できます。

ステップ 5 [Schedule Job] ウィンドウで、次の手順を実行します。

a) [Now] をクリックしてデバイスの検出をすぐに開始するか、[Later] をクリックしてデバイスの検出を特定の時間にスケジュールします。

[Daily] または [Weekly] の繰り返しオプションを選択すると、[Discover new devices only] オプションは無効になります。

b) トグルボタンをクリックして、[Discover new devices only] オプションを有効または無効にします。
c) [Assign devices to an existing site] リンクをクリックします。

[設定の可視性と制御（Visibility and Control of Configurations）] ダイアログボックスが表示され、サイトの割り当て時にデバイスで有効になる設定に関する情報が示されます。[設定の可視性（Visibility of Configurations）] が有効であり、検出中にサイトが割り当てられている場合、設定のプレビューは生成されません。

検出ワークフローの間、デバイスは既存のサイトにのみ割り当てることができ、新しいサイトの作成はサポートされません。

ダイアログボックスで、次のオプションのいずれかを選択します。

オプション	タスク
Assign to site without Configuration Preview	[Search Hierarchy] 検索フィールドまたはフィルタアイコンを使用して、サイト、ビルディング、またはエリアを見つけます。詳細については、ネットワーク階層の検索 （284 ページ）を参照してください。
Skip site assignment for now	後でデバイスをインベントリからサイトに割り当てる場合は、このオプションを使用します。

ステップ 6 [Summary] ウィンドウで、設定を確認します。変更するには、[Edit] をクリックします。

ステップ 7 [Start Discovery] をクリックします。

[Activities] > **[Tasks]** ウィンドウでタスクのステータスを確認できます。

次のタスク

[Device Discovery] ウィンドウに、サイト割り当てに基づいて検出されたデバイスを表示するオプションが表示されます。このオプションを使用して、サイトまたはネットワークに割り当てられたデバイス、またはインベントリ内の未割り当てのデバイスを表示します。

AP 更新ワークフロー

AP リフレッシュ機能を使用すると、アクセス ポイント リフレッシュ ワークフローを使用して、プロビジョニングされた古い AP モデルとプロビジョニングされていない古い AP モデルの両方を新しい AP モデルに置き換えることができます。以下の使用例の場合、次の手順を使用して、Catalyst Center で古い AP を新しい AP に交換できます。

- 自動化のユースケース：ワイヤレスコントローラと AP が Catalyst Center のネットワークインテント設定を介してプロビジョニングされる展開。AP の更新後、新しい AP はネットワークインテント設定でプロビジョニングされます。
- アシュアランスまたはキャンパス自動化のユースケース：Catalyst Center が主にアシュアランスの目的で使用され、ワイヤレスコントローラと AP が Catalyst Center のネットワークインテント設定を介してプロビジョニングされない展開。AP の更新後に新しい AP はプロビジョニングされず、古い設定のみが新しい AP にコピーされます。

デバイスの互換性については、「*Catalyst Center Compatibility Matrix*」を参照してください。

始める前に

- 古い AP がサイトに割り当てられていることを確認します。
- 新しい AP は、どのサイトにも割り当てることはできません。

- 自動化の使用例では、古い AP サイトは、新しい AP が関連付けられる ワイヤレスコントローラ の管理対象 AP の場所としてプロビジョニングする必要があります。
- アシュアランスまたはキャンパス自動化のユースケースでは、新しい AP は、古い AP が以前に関連付けられていたのと同じワイヤレスコントローラに接続する必要があります。
- 自動化の使用例では、新しいAPをワイヤレスコントローラに接続する必要があります。新しい AP は、Catalyst Center インベントリに登録されているか、プラグアンドプレイ（PnP）を介して Catalyst Center に接続できる必要があります。また、到達可能状態である必要があります。
- アシュアランスまたはキャンパス自動化のユースケースでは、新しい AP をワイヤレスコントローラに接続する必要があります。新しいAPは、Catalyst Centerインベントリに登録されているか、プラグアンドプレイ（PnP）を介して Catalyst Center に接続できる必要があります。また、到達可能状態である必要があります。

手順

ステップ 1 メインメニューから次を選択します。**[Workflows]** > **[Access Point Refresh]** の順に選択します。

（注） [Overview] ウィンドウが開いたら、[Let's Do it] をクリックしてワークフローを開始します。

ステップ 2 [Before you begin] ウィンドウで、AP 更新ワークフローの前提条件を確認します。

ステップ 3 [Get Started] ウィンドウで、タスクの一意の名前を入力します。

ステップ 4 **[シナリオの選択（Select your scenario）]** ウィンドウで、必要なユースケース（[自動化のユースケース（Automation Use Case）] または [アシュアランス/キャンパス自動のユースケース（Assurance/Campus Automation Usecase）]）の横にあるオプションボタンをクリックします。

ステップ 5 [Select Access Points] ウィンドウで、次の手順を実行します。

1. 左側のペインで、AP を更新するフロアの横にあるチェックボックスをオンにします。
2. 右側のペインで、置き換えるデバイス名の隣にあるチェックボックスをオンにします。

ステップ 6 [Assign New APs to Old APs] ウィンドウで、次の手順を実行します。

a) （任意） デフォルトでは、スイッチポートを介した新しい AP の自動検出が有効になっています。必要に応じてトグルボタンを使用し、新しい AP の自動検出を無効化できます。

新しいAPの自動検出のために、ワイヤレスコントローラまたはAPでCisco Discovery Protocol（CDP）が有効になっていることを確認します。

（注） スイッチポートを介した新しい AP の自動検出は、プラグアンドプレイを介してオンボードされている場合はサポートされません。

新しい AP の自動検出を有効にすると、このワークフローで次の処理が実行されます：

- 古い AP が接続されているのと同じスイッチポートに新しい AP が接続されている場合、新しい AP のシリアル番号が自動的に入力されます。
- 新しい AP がまだオンボードされていない場合、新しい AP のシリアル番号は AP の検出後に検出されますが、代わりに、新しい AP のシリアル番号を入力できます。

b) 新しい AP の詳細を提供する方法を選択します。

- GUI を使用して新しい AP の詳細を追加するには、AP の編集アイコン（ ）をクリックし、[Edit details] ウィンドウで次の手順を実行します。

  1. （オプション）新しい AP 名を更新します。
  2. （オプション）[Choose Platform ID] ドロップダウンリストから、新しい AP のプラットフォームを選択します。
  3. [Choose Serial Number] ドロップダウンリストから、新しい AP のシリアル番号を選択します。

     新しい AP がすでにワイヤレスコントローラに関連付けられ、インベントリに登録されている場合、Catalyst Center ではその AP のシリアル番号は [Choose Serial Number] ドロップダウンリストに [Managed] として表示されます。

     新しい AP が PnP で Catalyst Center に接続されている場合、Catalyst Center ではその AP のシリアル番号は [Choose Serial Number] ドロップダウンリストに [Unclaimed] として表示されます。

     新しい AP のシリアル番号がインベントリに登録されていない場合、そのシリアル番号は [Serial Number] ドロップダウンリストに表示されません。インベントリに登録されていない新しいシリアル番号を追加するには、[Choose Serial Number] ドロップダウンリストでシリアル番号を入力して [+] をクリックします。

     （注） スイッチポートを使用した新しい AP の自動検出を有効にする場合、シリアル番号の選択は任意です。

  4. [Save] をクリックします。

- カンマ区切り値（CSV）ファイルを使用して新しい AP の詳細を追加するには、次の手順を実行します：

  1. [Download CSV] をクリックします。ダウンロードした CSV テンプレートファイルには、古い AP の詳細が含まれています。デバイス名を更新し、新しい AP のシリアル番号を追加します。
  2. CSV ファイルをインポートするには、[Upload CSV] をクリックします。

3. [Upload CSV] ウィンドウで、CSV ファイルをドラッグアンドドロップ領域にドラッグアンドドロップするか、[Choose a file] をクリックして CSV ファイルの場所を参照し、[Open] をクリックします。

   Catalyst Center で検証チェックが実行されます。アップロードした CSV ファイルが要件を満たしていない場合は、エラーメッセージが表示されます。[View Details] をクリックすると、エラーメッセージの詳細が表示されます。

4. [Upload] をクリックします。

ステップ 7 [Configuration Copied from Old Access Point to New] ウィンドウで、古い AP から新しい AP にコピーされる設定を表示します。

ステップ 8 [Schedule Access Point Refresh Task] ウィンドウで、[Now] をクリックします。または [Run Later] をクリックして AP 更新タスクを後の日時にスケジュールします。

ステップ 9 [Summary] ウィンドウで、設定を確認します。変更するには、[Edit] をクリックします。

ステップ 10 [Track Replacement Status] ウィンドウで AP 交換ステータスをモニターします。

- AP の交換に成功した場合、[Replacement Status] に [REPLACED] と表示されます。
- AP の交換に失敗した場合、[Replacement Status] に [Error] と表示されます。

（注） 新しい AP がインベントリでまだ検出されておらず、対応する AP 更新エントリが新しいデバイスの接続を待機している場合、または PnP 要求プロセスが進行中の場合は、シスコ ワイヤレス コントローラを再同期します。

ステップ 11 （任意） [Track Replacement Status] ウィンドウで、次のいずれかを実行します。

- 最新の AP 交換ステータスを表示するには、[Refresh Data] をクリックします。
- 交換エントリを削除するには、[削除（Delete）] をクリックします。[Warning] ダイアログボックスで、[Yes] をクリックします。
- 交換中にエラーが発生した場合は、[再試行（Retry）] をクリックして交換を再トリガーします。
- プロビジョニング ステータス レポートをダウンロードするには、[Download Report] をクリックします。

ステップ 12 [Next] をクリックして、更新の概要を表示します。

[Activities] > **[Tasks]** ウィンドウでタスクのステータスを確認できます。

交換が正常に完了すると、Cisco Catalyst Assurance で古い AP と新しい AP についての AP 更新イベントが生成されます。

ステップ 13 （任意） AP 更新イベントは、[AP View 360] ウィンドウの [Event Viewer] で確認します。

Catalyst Center では、[Network Hierarchy] ウィンドウの対応するフロアマップで、新しい AP が自動的に更新されます。

スイッチでのアプリケーション ホスティングの有効化

次の手順に従って、特定のサイトで選択したスイッチで、ThousandEyes Enterprise Agent、iPerf などの Docker アプリケーションを有効にします。

始める前に

- 前提条件を満たします。詳細については、「アプリケーションホスティングの前提条件（1354 ページ）」を参照してください。
- アプリケーションを Catalyst Center に追加します。詳細については、「アプリケーションの追加 （1358 ページ）」を参照してください。
- アプリケーションをホストするためのスイッチの準備状況を確認します。詳細については、「アプリケーションをホストするデバイスの準備状況の表示（1355 ページ）」を参照してください。

手順

ステップ 1 **[Provision]** > **[Services]** > **[Application Hosting]**メインメニューから次を選択します。。

ステップ 2 アプリケーションを選択し、ウィンドウの下部にある [Install] をクリックします。

または、**[Workflows]** > **[Enable Apps on Switches]** > **[Let's Do it]** を選択してワークフローを起動することもできます。

（注） ウィンドウの上部にある青色の進捗状況バーにカーソルを合わせると、一覧表示される前の手順に戻ることができます。

ステップ 3 [Select Site] ウィンドウで、アプリケーションを有効にするビルディングに移動します。

ステップ 4 [Select App] ウィンドウで、選択するアプリケーションをクリックします。

（注） [+ New App] リンクにアクセスして、Catalyst Center に存在しないアプリケーションを追加できます。

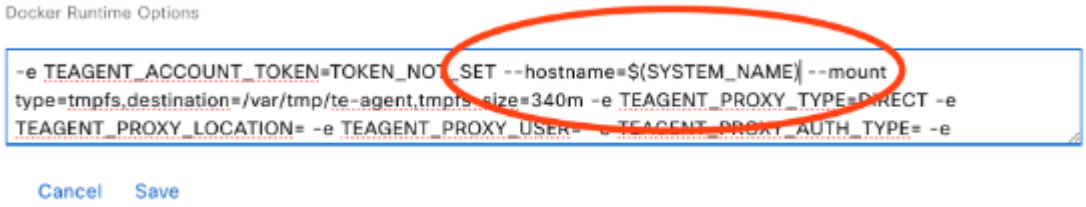
ステップ 5 [Select Switches] ウィンドウで、アプリケーションを有効にするデバイス名の横にあるチェックボックスをオンにします。

（注） [Select Switches] ダイアログボックスで指定したテンプレートに詳細を入力することにより、デバイスを一括でインポートまたはエクスポートできます。

ステップ 6 **[設定アプリ（Configuration App）]** ウィンドウで、次の設定を実行します。

- **アプリケーション ネットワーキング**
  - [Device Network]：[Select Network] ドロップダウンリストから、アプリケーションを設定する VLAN を選択します。
  - [App IP address]：[Address Type] ドロップダウンリストから [Static] または [Dynamic] を選択します。[Static] を選択した場合は、サムネイルアイコンをクリックして、アプリケーションの [IP Address]、[Gateway]、[Prefix/Mask]、および [DNS] を入力します。
- [Resource Allocation]：[Allocate resources as asked by the app] または [Allocate all resources available on a device] チェックボックスをオンにします。
- [Custom Settings]：（Cisco パッケージアプリケーションにのみ適用）アプリケーションによって指定された属性の設定の詳細を入力します。
- [App Data]：アプリケーション固有のファイルを参照してアップロードします。必要なアプリケーション固有のファイルを特定するには、関連するアプリケーションのドキュメントを参照してください。
- [Docker Runtime Options]：アプリケーションに必要な Docker ランタイムオプションを入力します。

重要 ThousandEyes アプリケーションの場合、デフォルトでは、docker ランタイムオプションはホスト名を変数 $(SYSTEM_NAME) として示します。



変数 $(SYSTEM_NAME) には、完全修飾ドメイン名（FQDN）が必要なため、ドメイン名を追加する必要があります。FQDN はホスト名およびドメイン名の 2 つのパートで構成されています。

ドメイン名は、$(SYSTEM_NAME).domain.name の形式で変数 $(SYSTEM_NAME) に手動で追加する必要があります。 変数 $(SYSTEM_NAME) は、展開後にデバイスのホスト名に自動的に置き換えられます。

たとえば、デバイスの FQDN が ise.cisco.com の場合、ホスト名は「ise」、ドメイン名は「cisco.com」です。Docker ランタイムオプションでは、変数に「cisco.com」を手動で追加して、$(SYSTEM_NAME).cisco.com のようにする必要があります。変数は、展開後に「ise」に自動的に置き換えられます。

ステップ 7 [Summary] ウィンドウで、設定を確認します。変更するには、[Edit] をクリックします。

[Provisioning Task] ウィンドウに、スイッチでのアプリケーションの展開を追跡するタスク名が表示されます。

ステップ 8 自動生成されたタスク名を確認し、[Provision] をクリックします。

ステップ 9 [Track Provisioning Status] ウィンドウで展開の進捗状況を追跡できます。

ステップ 10 [View Details] をクリックして、個々のデバイスのプロビジョニングステータスと障害を確認し（ある場合）、[Next] をクリックします。

アプリケーションが正常に有効化されました。

タスクの結果の概要と成功と失敗の回数が表示されます。

ステップ 11 [Manage App] をクリックします。ここで、アプリケーションのライフサイクル動作を管理して、*n* 日目のタスクを実行することができます。

IoT サービスの有効化

ここでは、Catalyst Center の [Workflows] を使用して、Cisco Catalyst 9100 シリーズ アクセスポイントで Bluetooth、Zigbee、ESL などの IoT テクノロジーを有効にする方法について説明します。

Cisco Catalyst 9100 シリーズ アクセス ポイントでの IoT サービスの有効化

この手順では、選択した Catalyst 9100 シリーズ アクセスポイントで、Bluetooth、Zigbee、ESL などの IoT テクノロジーを有効にする方法を説明します。

手順

ステップ 1 メインメニューから次を選択します。[Workflows] > [Enable IOT Services] の順に選択します。

ステップ 2 タスクの概要ウィンドウが開いたら、[Let's Do It] をクリックして、ワークフローに直接移動します。

ステップ 3 [Select Site] ウィンドウで、IoT サービスを有効にするフロアまで移動し、[Next] をクリックします。

ステップ 4 [Select the Application] ウィンドウで、ネットワークで IoT を有効にするための SES-imagotag ESL Connector アプリケーションを選択し、[Next] をクリックします。

（注） Catalyst Center に存在しないアプリケーションを追加するには、「アプリケーションの追加」を参照してください。

[Select Access Points] ウィンドウには、特定のフロアで使用可能なすべての AP が表示されます。

ステップ 5 [Select Access Points] ウィンドウで、IoT コネクタアプリケーションをインストールするデバイスの [Device Name] の横にあるチェックボックスをオンにして、[Next] をクリックします。

ステップ 6 [Summary] ウィンドウで、設定を確認します。変更するには、[Edit] をクリックします。

ステップ 7 **[プロビジョニングタスク（Provisioning Task）]** ウィンドウが表示され、AP への任意のアプリケーションの展開を追跡するために作成されたタスク名が表示されます。自動生成されたタスク名を確認し、[Provision] をクリックします。

ステップ 8 [Track Provisioning Status] ウィンドウで展開の進捗状況を追跡できます。[View Details] をクリックして、プロビジョニングステータスを確認し、[Next] をクリックします。

ステップ 9 タスク完了Task Completed] ウィンドウが表示されます。[IoTアプリケーションの管理（Manage IoT Application）] をクリックして、Day-N タスクを実行します。

IoT アプリケーションの管理

IoT アプリケーションを管理するには、次の手順を実行します。

始める前に

Cisco Catalyst 9000 シリーズ アクセス ポイントで IoT サービスを有効にしておく必要があります。

手順

ステップ 1 IoT サービスを有効にした後、[Done! Task Completed] ウィンドウで [Manage IoT Application] をクリックします。

ステップ 2 [ホスト名（Hostname）] の横にあるチェックボックスをオンにして、次のタスクを実行します。

- アプリケーションを起動するには、[Actions] ドロップダウンリストから [Start App] を選択します。
- アプリケーションを停止するには、[Actions] ドロップダウンリストから [Stop App] を選択します。
- アプリケーション設定を編集するには、[Actions] ドロップダウンリストから [Edit App Config] を選択します。
- アプリケーションをアップグレードするには、[Actions] ドロップダウンリストから [Upgrade App] を選択します。
- 選択した AP からアプリケーションをアンインストールするには、[Actions] ドロップダウンリストから [Uninstall App] を選択します。

ステップ 3 AP 名をクリックして、AP 名、ステータス、IP アドレス、正常性などの詳細を表示します。

ステップ 4 [Tech Support logs] をクリックして、アプリケーション ホスティング ログを収集します。

Catalyst Center での AP 設定

[アクセスポイントの設定 （Configure Access Points）] ワークフローを使用して、次のタスクを実行します。

- AP レベルおよび無線レベルのパラメータの設定および展開AP の設定 （1639 ページ）を参照してください。
- AP の定期的なイベントをスケジュールします。AP の定期的なイベントのスケジュール （1657 ページ）を参照してください。
- 既存のテンプレートを使用して AP を設定します。既存のテンプレートを使用した AP の設定 （1660 ページ）を参照してください。

AP の設定

次の手順を使用して、Catalyst Center で AP および無線パラメータを設定します。

[**Configure Access Points**] ワークフローを使用して構成された次の設定は、ワイヤレスコントローラや AP が再プロビジョニングされても上書きされません。

- 無線の管理ステータス（Cisco AireOS ワイヤレスコントローラにのみ適用）
- AP のプライマリコントローラ
- AP のセカンダリコントローラ

（注） AP 設定は、Catalyst Center インベントリで利用可能な情報から生成されます。最新の設定が生成されるようにするには、コントローラでインベントリの同期を完了します。

手順

ステップ 1 メインメニューから次を選択します。**[Workflows]** > **[Configure Access Points]** の順に選択します。

[Configure Your Access Points] ダイアログボックスが表示された場合は、[Let's Do It] をクリックしてワークフローに直接移動します。

ステップ 2 [Get Started] ウィンドウで、[Task Name] フィールドにワークフローの一意の名前を入力し、[Next] をクリックします。

ステップ 3 **[APの設定方法を指定（How do you want to configure APs?）]** ウィンドウで、AP および無線パラメータを設定します。

a) **[APおよび無線パラメータの設定（Configure AP And Radio Parameters）] [APおよび無線パラメータの設定（Configure AP and Radio Parameters）]** ラジオボタンをクリックします。

b) 実行するタスクの横にあるチェックボックスをオンにします。

- **[Modify AP Name]**
- Configure AP Geolocation Parameters
- [Configure AP Parameters]
- Configure AP LAN port parameters
- [Configure 5 GHz Radio Parameters]
- [Configure 2.4 GHz Radio Parameters]
- [Configure 6 GHz Radio Parameters]
- [Configure Dual-Band (XOR) Radio Parameters]
- [Configure Tri-Radio Parameters]

- テンプレートの作成

（注） オンにしたチェックボックスに基づいて、Catalyst Center では対応する後続の構成手順が表示されます。

c) [Next] をクリックします。

ステップ 4 [Select Access Points] ウィンドウで、設定する AP を選択します。

a) 設定する割り当て済み AP または未割り当て AP を選択します。

選択内容	結果
[Assigned APs] タブ	AP 関連の設定を適用するサイトに移動します。 右側のペインに、選択したサイトで使用可能なすべての AP が一覧表示されます。 （注） このウィンドウでは、最大2,000のサイトを選択できます。
[Unassigned APs] タブ	[Unassigned Devices] チェックボックスをオンにします。 右側のペインには、どのサイトにも割り当てられていないすべての AP が一覧表示されます。

b) 設定する AP を選択します。

（注） このウィンドウでは、サイトに割り当てられている AP と未割り当て AP の両方を含め、最大 4,000 個の AP を選択できます。

AP を選択するには、次のいずれかの方法を使用します。

- AP を個別に選択するには、AP 名の横にあるチェックボックスをオンにします。
- ページに表示されているすべてのAPを選択するには、テーブルの一番上にあるチェックボックスをオンにします。

  デフォルトでは、ページごとに 100 行が表示されます。
- 複数ページにあるすべてのAPを選択するには、テーブルの上部にあるチェックボックスをオンにして、表示される [すべてを選択（Select All）] をクリックします。

（注） このオプションは、AP の総数が 4,000 を超えない場合にのみ使用できます。

- 各列の上部にあるフィルタフィールドを使用して、必要な条件に基づいてAPをフィルタ処理します。フィルタリングした後、テーブルの上部にあるチェックボックスをオンにして、ページ上の検索条件に一致したすべての AP を選択するか、必要な AP 名の横にあるチェックボックスをオンにします。

c) （任意）[アクセスポイント（Access Points）] テーブルをカスタマイズするには、テーブルの右上隅にある歯車アイコンをクリックして、次のオプションを使用します。

- [テーブル密度（Table density）] で、希望するテーブル密度を選択します。
- [テーブル列（Table columns）] で、テーブルに表示する列名の横にあるチェックボックスをオンにします。

d) [Next] をクリックします。

ステップ 5 ライセンス要件を満たしていない AP を選択すると、Catalyst Center は詳細を示すダイアログボックスを表示します。ダイアログボックスで、必要なオプションをクリックします。

オプション	説明
ライセンス マネージャ	[License Manager] ウィンドウを開いて、対応するライセンスを有効にします。 ライセンスを有効にするには、『*Cisco Catalyst Center Administrator Guide*』の「Manage Licenses」を参照してください。
[Continue With The Workflow]	ワークフローを続行します。 （注） ライセンス要件を満たしていない AP は、ワールドワイドセーフモード（WWSM）になります。
Cancel	ダイアログボックスを閉じて、[Select Access Points] ウィンドウで別の AP を選択します。

ステップ 6 （任意） [Modify AP Name] ウィンドウで、次のいずれかのオプションを使用して 1 つ以上の AP 名を変更します。

- [Create a New Naming Convention]：このオプションボタンをクリックして、命名規則に基づいて名前を入力し、[Apply Pattern] をクリックします。[Access Points] テーブルには、入力した命名パターンに基づいて新しい AP 名が表示されます。

- [Upload a CSV file]：このオプションボタンをクリックして、サンプル CSV テンプレートファイルをダウンロードし、そのファイルに AP 名を追加します。次に、CSV ファイルをドラッグしてドロップエリアにドロップすることにより、または [Choose a file] をクリックし、CSV ファイルを参照して選択することにより、ファイルをアップロードします。

ステップ 7 （任意） [Configure AP Geolocation Parameters] ウィンドウで、対象の AP の地理位置情報パラメータを設定します。

地理位置情報パラメータは、自動周波数調整（AFC）などの機能に使用されます。これらのパラメータは、Cisco IOS XE リリース 17.12 以降を実行している AP でのみ使用できます。

（注） 標準電力で 6 GHz 帯域を使用するには、地理位置情報パラメータを設定し、RF プロファイルの [Standard Power Service] トグルボタンを有効にする必要があります。詳細については、ワイヤレス無線周波数プロファイルの作成 （451 ページ）を参照してください。

このウィンドウに、地理位置情報パラメータをサポートする到達可能な AP が一覧表示されます。

実行する操作	結果
AP をフィルタリングする	次のいずれかを実行できます。 • [**Search Table**] をクリックし、値を入力して **Enter** キーを押します。 • フィルタアイコン（▽）をクリックし、テーブルの列で利用可能なフィールドに任意の値の組み合わせを入力します。たとえば、[AP Name]、[Ethernet MAC Address]、および [Site] フィールドに値を入力できます。
標準電力設定ステータスに基づいて AP をフィルタリングする	[All]、[Enabled]、または [Disabled] トグルボタンをクリックします。

実行する操作	結果
高さを設定する	次の手順を実行します。 **1.** 必要な AP の横にあるチェックボックスをオンにします。 **2.** **[高さの設定（Configure Height）]** をクリックします。 **3.** [Height (m)] フィールドに、地上からの高さをメートル単位で入力します（最も近い整数に丸めます）。 有効な範囲は 100 ～ 1000 です。 **4.** [Height Uncertainty (m)] フィールドに、高さの不確実性をメートル単位で入力します。 有効な範囲は 1 ～ 100 です。 （注） 高さの不確実性が高いほど、AFC によって報告される電力制限の精度が低くなる可能性があります。 **5.** （オプション）AP がアンテナケーブルを介して接続されている場合は、[Cable Length (m)] フィールドに、ケーブルの長さをメートル単位で入力します。 有効な範囲は 1 ～ 100 です。 （注） APがこのデータをサポートしていない場合、このフィールドはグレー表示されます。
CSV形式でデータをダウンロードする	次の手順を実行します。 **1.** 必要な AP の横にあるチェックボックスをオンにします。 **2.** [Download CSV] をクリックします。

実行する操作	結果
複数の AP のデータを CSV 形式でアップロードする	次の手順を実行します。 **1.** 必要な AP の横にあるチェックボックスをオンにします。 **2.** [Upload CSV] をクリックします。 **3.** [Warning] ダイアログボックスで、[Yes] をクリックします。 **4.** [Upload CSV] ダイアログボックスで、CSV ファイルをドラッグアンドドロップ領域にドラッグアンドドロップするか、[Choose a file] をクリックして CSV ファイルの場所を参照します。 （注） この CSV ファイルは、ダウンロードした CSV ファイルと同じ形式である必要があります。 **5.** [Upload] をクリックします。

ステップ 8 （任意） [Configure AP Parameters] ウィンドウで、AP パラメータを設定します。

- [Admin Status]：管理ステータスを無効にするには、このチェックボックスをオンにして、[Disable] をクリックします。
- [AP LED Status]：AP LED ステータスを無効にするには、このチェックボックスをオンにして、[Disable] をクリックします。
- [VLAN Tag]：このチェックボックスをオンにして次の設定を完了すると、複数の VLAN を 1 つのポートで管理できるようになります。
  1. [Enable] をクリックします。
  2. [VLAN Tag ID] フィールドに、タグを入力します。有効な範囲は 1 ～ 4094 です。

（注）
- VLAN タグ設定は、ブリッジモードの AP には適用されません。
- VLAN タグ、AP モード、ブリッジロールを個別のワークフローで設定します。これらのパラメータを指定すると AP が再起動するためです。
- このオプションを有効にすると、ブリッジロールと RAP ダウンリンク バックホール オプションがグレー表示されます。このオプションは、AP モード、ブリッジロール、RAP ダウンリンクバックホールのオプションが有効になっている場合にグレー表示されます。

- [AP Mode]：このチェックボックスをオンにして、[Select AP Mode] ドロップダウンリストから AP モードを選択します。有効なモードは、[Local/Flexconnect]、[Monitor]、[Sniffer]、および [Bridge/Flex+Bridge] です。

  このオプションを有効にすると、VLAN タグ、ブリッジロール、RAP ダウンリンクバックホールのオプションがグレー表示されます。

  （注） AP モードを [Monitor] または [Sniffer] から [Local/Flexconnect] に変更すると、Catalyst Center では次の設定が使用されます。

  - 関連付けられた SSID で [FlexConnect Local Switching] が有効になっている場合は、Catalyst Center では AP に [FlexConnect] モードが設定されます。それ以外の場合は、AP に [Local] モードが設定されます。
  - 割り当てられていない AP または割り当てられているがプロビジョニングされていない AP の場合、Catalyst Center ではデバイスに基づいた AP に [FlexConnect] モードが設定されます。
    - Cisco AireOS ワイヤレスコントローラ：AP が存在する AP グループ内の関連付けられた SSID で [FlexConnect Local Switching] が有効になっている場合。
    - Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ：AP の現在関連付けられているサイトタグで [Local site] が無効になっている場合。
  - AP モード、VLAN タグ、およびブリッジロールを個別のワークフローで設定します。これらのパラメータを指定すると AP が再起動するためです。

  メッシュネットワークの詳細については、「ワイヤレス メッシュ ネットワークについて （531 ページ）」を参照してください。

- [LED Brightness Level]：このチェックボックスをオンにして、[LED Brightness Level] から明るさのレベルを選択します。

- [**Bridge Role**]：AP のメッシュロールを設定するには、このオプションを使用します。チェックボックスをオンにして AP でブリッジモードを有効にし、ドロップダウンリストからメッシュロール（メッシュアクセスポイントまたはルートアクセスポイント）を選択します。

  [**Applicable APs**] フィールドには、デバイスごとの設定がある（インテントベースの AP ではない）AP でのみ使用可能なメッシュロール設定をサポートする AP の数が表示されます。

  ブリッジロール、VLAN タグ、および AP モードを個別のワークフローで設定します。これらのパラメータを指定すると AP が再起動するためです。

（注） このオプションを有効にすると、VLAN タグと RAP ダウンリンク バックホールオプションがグレー表示されます。このオプションは、VLAN タグまたは RAP ダウンリンク バックホール オプションが有効になっている場合にグレー表示されます。

- [加速度計（Accelerometer）]：サポートされている AP の AP アクセラレータを有効または無効にするには、このチェックボックスをオンにして [有効化（Enable）] または [無効化（Disable）] をクリックします。加速度計は、AP の方向をモニターするための傾斜データを提供します。

  加速度計を有効にすると、Catalyst Center によりインベントリに AP 傾斜情報が表示されます。デフォルトでは、AP 加速度計は無効になっています。

  Catalyst Center により適用可能な AP の数が表示されます。適用可能な AP が使用できる場合は、番号をクリックすると AP の詳細が表示されます。

  加速度計機能は、Cisco Catalyst 9166D1 シリーズ AP、Cisco Catalyst 9176I シリーズアクセス AP、Cisco Catalyst 9176D1 シリーズ AP、および Cisco Catalyst 9178I シリーズ AP でのみ使用できます。

（注） ワイヤレスコントローラ を再同期して、インベントリにセンサーの傾斜の詳細を表示します。詳細については、デバイス情報の再同期 （217 ページ）を参照してください。

- [Domain Name System Configuration] で、静的 IP アドレスを持つ AP のドメインネームシステム（DNS）を設定します。
  - [DNS Server] チェックボックスをオンにして、サーバーの IP アドレスを入力します。

    IPv4 または IPv6 アドレスを入力できますが、AP で設定されている静的 IP アドレスから IP アドレスに到達できることを確認してください。
  - [Domain Name] チェックボックスをオンにして、ドメイン名を入力します。

- [RAPダウンリンクバックホール（RAP Downlink Backhaul）]：このチェックボックスをオンにして、ドロップダウンリストから、ブリッジロールのルートアクセスポイント（RAP）のダウンリンクバックホール無線バンドを選択します。

  Catalyst Center により適用可能な AP の数が表示されます。適用可能な AP が使用できる場合は、番号をクリックすると AP の詳細が表示されます。

（注） このオプションを有効にすると、ブリッジロールと VLAN タグのオプションがグレー表示されます。ブリッジロールまたは VLAN タグオプションが有効になっている場合、このオプションはグレー表示されます。

- [AP Failover Priority]：このチェックボックスをオンにして、[AP Failover Priority] ドロップダウンリストからフェールオーバー優先順位を選択します。
  - [Low]（デフォルト）：レベル 1 の優先順位。これは最も低い優先度レベルです。
  - [Medium]：レベル 2 の優先順位。
  - [High]：レベル 3 の優先順位。
  - [Critical]：レベル 4 の優先順位。これは最も高い優先度レベルです。
- [AP Location]：このチェックボックスをオンにすると、[Enter Location] フィールドに AP の場所の詳細を入力できます。

  現在割り当てられているサイトを AP の場所として使用するには、[Use currently assigned site location] チェックボックスをオンにします。このチェックボックスをオンにすると、[Enter Location] フィールドが無効になります。この変更をデバイスにプッシュする前に、[Click here to view location details] をクリックすると、各 AP に設定されている AP のロケーションを表示できます。

  （注） どのサイトにも割り当てられていない AP の場合、[Use currently assigned site location] チェックボックスをオンにしても、Catalyst Center に AP の場所は設定されません。
- [High Availability]：このチェックボックスをオンにして、AP のプライマリ、セカンダリ、およびターシャリコントローラの名前と IP アドレスを設定します。

  プライマリコントローラとセカンダリコントローラに対して [Inherit from site / Clear] を選択した場合：
  - プロビジョニングされた状態の AP の場合、AP が割り当てられているフロアのプライマリおよびセカンダリとして設定されたコントローラが、AP のプライマリおよびセカンダリコントローラとして設定されます。
  - プロビジョニングされた状態にない AP の場合、現在のプライマリ、セカンダリコントローラの設定が AP から消去されます。

  ターシャリコントローラの場合、[Clear] オプションのみが使用可能です。

  （注）
  - コントローラで AP フォールバックが無効になっている場合、AP は新しく設定されたプライマリ、セカンダリ、およびターシャリコントローラに参加しません。
  - AP が ROW AP の場合は、コントローラの国のリストに、運用国のサポートが追加されていることを確認してください。コントローラの管理対象 AP ロケーションとして、運用国の少なくとも 1 つのサイトを設定する必要があります。

- [CleanAir Pro / CleanAir / Spectrum Intelligence]：2.4 GHz、5 GHz、または 6 GHz 無線帯域の CleanAir スペクトルインテリジェンスを無効にするには、対応するチェックボックスをオンにして [Disable] をクリックします。

（注） CleanAir スペクトルインテリジェンスは、[Local/FlexConnect] モードまたは [Monitor] モードの CleanAir スペクトルインテリジェンス対応 AP にのみ設定できます。802.11a ネットワークで CleanAir スペクトルインテリジェンスが無効になっている場合、AP の動作ステータスはダウンです。

ステップ 9 （任意） [Configure AP LAN port parameters] ウィンドウで、該当する AP の AP LAN ポートパラメータを設定します。

- LAN1、LAN2、および LAN3 で、対応する [Port Status] チェックボックスをオンにし、[Enable] をクリックして対応するポートを有効にします。
- LAN1 ポートを有効にした場合は、[**PoE Status**] チェックボックスをオンにして、ポートの Power over Ethernet（PoE）を有効にします。

  PoE を有効にすると、デバイス上の USB モジュールは自動的に無効になります。

（注） サイトベースのネットワークプロファイルを使用して管理されるワイヤレスコントローラに関連付けられている AP を選択した場合は、AP LAN ポートのパラメータを設定できません。

ステップ 10 （任意） [Configure 5 GHz Radio Parameters] ウィンドウで、802.11 a/n/ac/ax パラメータを設定します。

- [Admin Status]：管理ステータスを無効にするには、このチェックボックスをオンにして、[Disable] をクリックします。
- [Radio Role Assignment]：無線ロールを選択するには、このチェックボックスをオンにして、[Auto]、[Client-Serving]、または [Monitor] をクリックします。

  5 GHz 無線パラメータ設定に適用可能な AP のリストを表示するには、[View Devices] をクリックします。Catalyst Center では、5 GHz 無線パラメータをサポートする AP が使用可能な場合にのみ、[View Devices] オプションが表示されます。
- [Power Assignment]：カスタム電力値を選択するには、このチェックボックスをオンにして [Custom] をクリックします。[Select Custom Power] ドロップダウンリストから電力レベルを選択します。
- [Channel Assignment]：カスタムチャネル番号を選択するには、このチェックボックスをオンにして [Custom] をクリックします。[Select Custom Channel] ドロップダウンリストからカスタムチャネル番号を選択します。
- [Channel Width]：チャネル幅を選択するには、このチェックボックスをオンにし、チャネル帯域幅を選択します。

- [Antenna Gain]：アンテナを選択するには、このチェックボックスをオンにして、[Select Antenna] ドロップダウンリストからアンテナを選択します。アンテナとして [Other] を選択した場合は、[Antenna Gain (in dBi) (for Antenna-Other)] フィールドにアンテナ利得を入力します。外部アンテナの性能を指定する数値を入力し、領域に無線エネルギーを向けたり、収束させたりします。高ゲイン アンテナの放射パターンは、特定の方向により収束したものになります。アンテナゲイン値の範囲は 0 ～ 40 です。

  （注） 選択したアンテナ名はワイヤレスマップに反映されません。

- [Antenna Cable]：アンテナケーブルを選択するには、このチェックボックスをオンにして、[Select Antenna Cable] ドロップダウンリストからアンテナケーブルを選択します。アンテナケーブルとして [Other] を選択した場合は、[Cable Loss (in dBi) (for Cable-Other)] フィールドにケーブル損失値を入力します。ケーブル損失値は 0 ～ 40 です。

- [BSS Color Configuration]：該当する AP の BSS カラーを設定するには、このチェックボックスをオンにして、次のいずれかのオプションを選択します。
  - グローバルレベルで BSS カラーを設定するには、[Global] をクリックします。
  - カスタムの BSS カラーを設定するには、[Custom] をクリックします。

  （注） Cisco AireOS ワイヤレスコントローラに関連付けられている AP の場合、この帯域の BSS カラーを有効にすると、グローバルレベルで BSS カラーが有効になり、ネットワークの中断が発生する可能性があります。

- [BSS Color Radio Admin Status]：BSS カラー設定を有効にした場合に、この無線の BSS カラーを有効にするには、このチェックボックスをオンにして [Enable] をクリックします。

  [BSS Color Code] フィールドに、BSS カラーコードを入力します。有効な範囲は 1 ～ 63 です。

  （注） [Disable] をクリックすると、このフィールドはグレー表示されます。

（注） [Configure Access Points] ワークフローでは、[Azimuth] と [Elevation] のパラメータは使用できなくなりました。これらのパラメータは、**[Design]** > **[Network Hierarchy]**ウィンドウで設定できます。詳細については、AP の編集 （318 ページ）を参照してください。

ステップ 11 （任意） [Configure 2.4 GHz Radio Parameters] ウィンドウで、2.4 GHz 無線パラメータを設定します。

a) 2.4 GHz 無線パラメータの設定に適用可能な AP のリストを表示するには、[View Devices] をクリックします。

Catalyst Center では、2.4 GHz 無線パラメータをサポートする AP が使用可能な場合にのみ、[View Devices] オプションが表示されます。

b) 必要な 802.11 b/g/n パラメータを設定します。

- [Admin Status]：管理ステータスを無効にするには、このチェックボックスをオンにして、[Disable] をクリックします。
- [Radio Role Assignment]：無線ロールを選択するには、このチェックボックスをオンにして、[Auto]、[Client-Serving]、または [Monitor] をクリックします。
- [Power Assignment]：カスタム電力値を選択するには、このチェックボックスをオンにして [Custom] をクリックします。[Select Custom Power] ドロップダウンリストから電力レベルを選択します。
- [Channel Assignment]：カスタムチャネル番号を選択するには、このチェックボックスをオンにして [Custom] をクリックします。[Select Custom Channel] ドロップダウンリストからカスタムチャネル番号を選択します。
- [Antenna Gain]：アンテナを選択するには、このチェックボックスをオンにして、[Select Antenna] ドロップダウンリストからアンテナを選択します。アンテナとして [Other] を選択した場合は、[Antenna Gain (in dBi) (for Antenna-Other)] フィールドにアンテナ利得を入力します。外部アンテナの性能を指定する数値を入力し、領域に無線エネルギーを向けたり、収束させたりします。高ゲイン アンテナの放射パターンは、特定の方向により収束したものになります。アンテナゲイン値の範囲は 0 ～ 40 です。

（注） 選択したアンテナ名はワイヤレスマップに反映されません。

- [Antenna Cable]：アンテナケーブルを選択するには、このチェックボックスをオンにして、[Select Antenna Cable] ドロップダウンリストからアンテナケーブルを選択します。アンテナケーブルとして [Other] を選択した場合は、[Cable Loss (in dBi) (for Cable-Other)] フィールドにケーブル損失値を入力します。ケーブル損失値は 0 ～ 40 です。
- [BSS Color Configuration]：該当する AP の BSS カラーを設定するには、このチェックボックスをオンにして、次のいずれかのオプションを選択します。
  - グローバルレベルで BSS カラーを設定するには、[Global] をクリックします。
  - カスタムの BSS カラーを設定するには、[Custom] をクリックします。

（注） Cisco AireOS ワイヤレスコントローラに関連付けられている AP の場合、この帯域の BSS カラーを有効にすると、グローバルレベルで BSS カラーが有効になり、ネットワークの中断が発生する可能性があります。

- [BSS Color Radio Admin Status]：BSS カラー設定を有効にした場合に、この無線の BSS カラーを有効にするには、このチェックボックスをオンにして [Enable] をクリックします。

  [BSS Color Code] フィールドに、BSS カラーコードを入力します。有効な範囲は 1 ～ 63 です。

（注） [Disable] をクリックすると、このフィールドはグレー表示されます。

（注） [Configure Access Points] ワークフローでは、[Azimuth] と [Elevation] のパラメータは使用できなくなりました。これらのパラメータは、**[Design]** > **[Network Hierarchy]** ウィンドウで設定できます。詳細については、AP の編集 （318 ページ）を参照してください。

ステップ 12 （任意） [Configure 6 GHz Radio Parameters] ウィンドウで、6 GHz 無線パラメータを設定します。

a) 6 GHz 無線パラメータの設定に適用可能な AP のリストを表示するには、[View Devices] をクリックします。

   Catalyst Center では、6 GHz 無線パラメータをサポートする AP が使用可能な場合にのみ、[View Devices] オプションが表示されます。

b) 必須パラメータを設定します。

   - [Admin Status]：管理ステータスを無効にするには、このチェックボックスをオンにして、[Disable] をクリックします。
   - [Radio Role Assignment]：無線ロールを選択するには、このチェックボックスをオンにして、[Auto]、[Client-Serving]、または [Monitor] をクリックします。
   - [Power Assignment]：カスタム電力値を選択するには、このチェックボックスをオンにして [Custom] をクリックします。[Select Custom Power] ドロップダウンリストから電力レベルを選択します。
   - [Channel Assignment]：カスタムチャネル番号を選択するには、このチェックボックスをオンにして [Custom] をクリックします。[Select Custom Channel] ドロップダウンリストからカスタムチャネル番号を選択します。
   - [Channel Width]：チャネル幅を選択するには、このチェックボックスをオンにし、チャネル帯域幅を選択します。

（注） 320 MHz のチャネル幅は Wi-Fi 7 AP（Cisco Catalyst 9172H Series Access Points, Cisco Catalyst 9172I Series Access Points、Cisco Catalyst 9176D1 シリーズ アクセスポイント、Cisco Catalyst 9176I シリーズ アクセスポイント、および Cisco Catalyst 9178I シリーズ アクセスポイント）でのみ使用できます。

- [BSS Color Configuration]：該当する AP の BSS カラーを設定するには、このチェックボックスをオンにして、次のいずれかのオプションを選択します。
  - グローバルレベルで BSS カラーを設定するには、[Global] をクリックします。
  - カスタムの BSS カラーを設定するには、[Custom] をクリックします。
- [BSS Color Radio Admin Status]：BSS カラー設定を有効にした場合に、この無線の BSS カラーを有効にするには、このチェックボックスをオンにして [Enable] をクリックします。

  [BSS Color Code] フィールドに、BSS カラーコードを入力します。有効な範囲は 1 ～ 63 です。



（注） [Disable] をクリックすると、このフィールドはグレー表示されます。



（注） [Configure Access Points] ワークフローでは、[Azimuth] と [Elevation] のパラメータは使用できなくなりました。これらのパラメータは、**[Design]** > **[Network Hierarchy]** ウィンドウで設定できます。詳細については、AP の編集 （318 ページ）を参照してください。

ステップ 13 （任意） [Configure Dual-Band (XOR) Radio Parameters] ウィンドウで、デュアルバンド（XOR）無線パラメータを設定します。

a) XOR 無線パラメータの設定に適用可能な AP のリストを表示するには、[View Devices] をクリックします。

Catalyst Center では、XOR パラメータをサポートする AP が使用可能な場合にのみ [View Devices] オプションが表示されます。

次の AP で XOR 無線パラメータを設定できます。

- Cisco Aironet 2800 シリーズ アクセス ポイント
- Cisco Aironet 3800 シリーズ アクセスポイント
- Cisco Aironet 4800 シリーズ アクセスポイント
- Cisco Catalyst 9120 シリーズ アクセスポイント
- Cisco Catalyst 9166 シリーズ アクセスポイント
- Cisco IOS XE リリース 17.18 以降を実行している Cisco Wireless 9171I シリーズ アクセスポイント
- Cisco IOS XE リリース 17.18 以降を実行している Cisco Wireless 9174I シリーズ アクセスポイント
- Cisco IOS XE リリース 17.18 以降を実行している Cisco Wireless 9174E シリーズ アクセスポイント

- Cisco IOS XE リリース 17.15 以降を実行している Cisco Catalyst 9176D1 シリーズ アクセスポイント
- Cisco IOS XE リリース 17.15 以降を実行している Cisco Catalyst 9176I シリーズ アクセスポイント
- Cisco Catalyst IW9165E アクセスポイント
- Cisco Catalyst IW9165D Heavy Duty アクセスポイント
- Cisco Catalyst IW9167E Heavy Duty アクセスポイント

（注） Cisco Catalyst 9166 シリーズ アクセスポイントおよび Cisco Wireless 9171I シリーズ アクセスポイントは、5 GHz と 6 GHz の無線モード間の XOR をサポートしています。他の AP は、2.4 GHz と 5 GHz の無線モード間の XOR をサポートしています。

b) 必須パラメータを設定します。

- [Admin Status]：管理ステータスを無効にするには、このチェックボックスをオンにして、[Disable] をクリックします。
- [Radio Role Assignment]：無線ロールを選択するには、このチェックボックスをオンにして、[Auto]、[Client-Serving]、または [Monitor] をクリックします。

  （オプション）[Client-Serving] ロールの場合、利用可能なオプションから 2.4 GHz、5 GHz、または 6 GHz 無線帯域を選択します。

（注） 外部アンテナを備えた AP モデルの場合、指向性アンテナ無線端末（DART）コネクタが接続されている場合にのみ、5 GHz 無線帯域を選択できます。

- [Power Assignment]：カスタム電力値を選択するには、このチェックボックスをオンにして [Custom] をクリックします。[Select Custom Power] ドロップダウンリストから電力レベルを選択します。
- [Channel Assignment]：カスタムチャネル番号を選択するには、このチェックボックスをオンにして [Custom] をクリックします。[Select Custom Channel] ドロップダウンリストからカスタムチャネル番号を選択します。
- [Channel Width]：チャネル幅を選択するには、このチェックボックスをオンにし、チャネル帯域幅を選択します。

（注） XOR 対応 AP でデュアル無線モードが有効になっている場合、そのスロット 2 は 160 MHz チャネル幅の [Client-Serving] 無線ロールにすることはできません。

- [Antenna Gain]：アンテナを選択するには、このチェックボックスをオンにして、[Select Antenna] ドロップダウンリストからアンテナを選択します。アンテナとして [Other] を選択した場合は、[Antenna Gain (in dBi) (for Antenna-Other)] フィールドにアンテナ利得を入力します。外部アンテナの性能を指定する数値を入力し、領域に無線エネルギーを向けたり、収束させたりします。高ゲイン アンテナの放射パターンは、特定の方向により収束したものになります。アンテナゲイン値の範囲は 0 ～ 40 です。

（注） 選択したアンテナ名はワイヤレスマップに反映されません。

- [Antenna Cable]：アンテナケーブルを選択するには、このチェックボックスをオンにして、[Select Antenna Cable] ドロップダウンリストからアンテナケーブルを選択します。アンテナケーブルとして [Other] を選択した場合は、[Cable Loss (in dBi) (for Cable-Other)] フィールドにケーブル損失値を入力します。ケーブル損失値は 0 ～ 40 です。
- [BSS Color Configuration]：該当する AP の BSS カラーを設定するには、このチェックボックスをオンにして、次のいずれかのオプションを選択します。
  - グローバルレベルで BSS カラーを設定するには、[Global] をクリックします。
  - カスタムの BSS カラーを設定するには、[Custom] をクリックします。
- [BSS Color Radio Admin Status]：BSS カラー設定を有効にした場合に、この無線の BSS カラーを有効にするには、このチェックボックスをオンにして [Enable] をクリックします。

  [BSS Color Code] フィールドに、BSS カラーコードを入力します。有効な範囲は 1 ～ 63 です。

（注） [Disable] をクリックすると、このフィールドはグレー表示されます。

（注） [Configure Access Points] ワークフローでは、[Azimuth] と [Elevation] のパラメータは使用できなくなりました。これらのパラメータは、**[Design]** > **[Network Hierarchy]** ウィンドウで設定できます。詳細については、AP の編集 （318 ページ）を参照してください。

ステップ 14 （任意） [Configure Tri-Radio Parameters] ウィンドウで、トライ無線パラメータを設定します。

a) トライ無線パラメータの設定に適用可能な AP のリストを表示するには、[View Devices] をクリックします。

（注）
- Catalyst Center では、トライ無線パラメータをサポートする AP が使用可能な場合にのみ、[View Devices] オプションが表示されます。
- Catalyst Center では、[Monitor] モードまたは [Sniffer] モードの AP のトライ無線パラメータ設定をサポートしていません。

次の AP で トライ無線パラメータを設定できます。

- Cisco Catalyst 9124AXE シリーズ アクセスポイント
- Cisco Catalyst 9130AXI シリーズ アクセスポイント
- Cisco Catalyst 9130AXE シリーズ アクセスポイント
- Cisco Catalyst 9178I シリーズ アクセスポイント
- Cisco Catalyst 9179F シリーズ アクセスポイント

b) 必須パラメータを設定します。

- [Dual Radio Mode]：デュアル無線モードを選択するには、このチェックボックスをオンにして、[Auto]、[Enable]、または [Disable] をクリックします。

（注） デュアル無線モードを有効にすると、対応するワイヤレスコントローラでグローバルトライ無線モードが有効になります。

- [Radio Role Assignment]：無線ロールを選択するには、このチェックボックスをオンにして、[Auto]、[Client-Serving]、または [Monitor] をクリックします。
- [Admin Status]：管理ステータスを無効にするには、このチェックボックスをオンにして、[Disable] をクリックします。
- [Power Assignment]：カスタム電力値を選択するには、このチェックボックスをオンにして [Custom] をクリックします。[Select Custom Power] ドロップダウンリストから電力レベルを選択します。
- [Channel Assignment]：カスタムチャネル番号を選択するには、このチェックボックスをオンにして [Custom] をクリックします。[Select Custom Channel] ドロップダウンリストからカスタムチャネル番号を選択します。
- [Channel Width]：チャネル幅を選択するには、このチェックボックスをオンにし、チャネル幅を選択します。

（注） [Channel Assignment] の [Custom] オプションを選択すると、Catalyst Center でこのパラメータが有効になります。

- [Antenna Gain]：アンテナを選択するには、このチェックボックスをオンにして、[Select Antenna] ドロップダウンリストからアンテナを選択します。アンテナとして [Other] を選択した場合は、[Antenna Gain (in dBi) (for Antenna-Other)] フィールドにアンテナ利得を入力します。外部アンテナの性能を指定する数値を入力し、領域に無線エネルギーを向けたり、収束させたりします。高ゲイン アンテナの放射パターンは、特定の方向により収束したものになります。アンテナゲイン値の範囲は 0 ～ 40 です。

（注） 選択したアンテナ名はワイヤレスマップに反映されません。

- [Antenna Cable]：アンテナケーブルを選択するには、このチェックボックスをオンにして、[Select Antenna Cable] ドロップダウンリストからアンテナケーブルを選択します。アンテナケーブルとして [Other] を選択した場合は、[Cable Loss (in dBi) (for Cable-Other)] フィールドにケーブル損失値を入力します。ケーブル損失値は 0 ～ 40 です。
- [BSS Color Configuration]：該当する AP の BSS カラーを設定するには、このチェックボックスをオンにして、次のいずれかのオプションを選択します。
  - グローバルレベルで BSS カラーを設定するには、[Global] をクリックします。
  - カスタムの BSS カラーを設定するには、[Custom] をクリックします。
- [BSS Color Radio Admin Status]：BSS カラー設定を有効にした場合に、この無線の BSS カラーを有効にするには、このチェックボックスをオンにして [Enable] をクリックします。

  [BSS Color Code] フィールドに、BSS カラーコードを入力します。有効な範囲は 1 ～ 63 です。

（注） [Disable] をクリックすると、このフィールドはグレー表示されます。

（注） [Configure Access Points] ワークフローでは、[Azimuth] と [Elevation] のパラメータは使用できなくなりました。これらのパラメータは、**[Design]** > **[Network Hierarchy]** ウィンドウで設定できます。詳細については、AP の編集 （318 ページ）を参照してください。

ステップ 15 （オプション）[Save As Reusable Template] ウィンドウで、オプションを選択します。

- 新しいテンプレートとして保存するには、[Create] をクリックし、[Template Name] フィールドにテンプレートの名前を入力します。デフォルトでは、[Template Name] フィールドにはワークフロー名が自動的に入力されています。同じ名前を使用したり、必要に応じて名前を変更したりできます。

（注） サポートされるテンプレートの最大数は 500 です。

- テンプレートの作成をスキップするには、[Do Not Save] をクリックします。

ステップ 16 [Summary] ウィンドウで、設定を確認します。変更するには、[Edit] をクリックします。

ステップ 17 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

（注） この設定済みワークフローを新しいテンプレートとして保存する場合、[Configure] をクリックすると作成されます。

ステップ 18 [Tasks] ウィンドウで、タスクの展開を監視します。

AP の定期的なイベントのスケジュール

Catalyst Center で AP および無線パラメータの定期的なイベントをスケジュールするには、次の手順を実行します。

手順

ステップ 1 メインメニューから次を選択します。**[Workflows]** > **[Configure Access Points]** の順に選択します。

[Configure Your Access Points] ダイアログボックスが表示された場合は、[Let's Do It] をクリックしてワークフローに直接移動します。

ステップ 2 [Get Started] ウィンドウで、[Task Name] フィールドにタスクの一意の名前を入力します。

ステップ 3 **[APの設定方法の指定（How do you want to configure APs?）]** ウィンドウで、**[APおよび無線パラメータの定期的なイベントのスケジュール（Schedule Recurring Events For AP And Radio Parameters）]** オプションボタンをクリックします。

ステップ 4 [Select Access Points] ウィンドウで、設定する AP を選択します。

a) 設定する割り当て済み AP または未割り当て AP を選択します。

選択内容	結果
[Assigned APs] タブ	AP 関連の設定を適用するサイトに移動します。 右側のペインに、選択したサイトで使用可能なすべての AP が一覧表示されます。 （注） このウィンドウでは、最大 2,000 のサイトを選択できます。
[Unassigned APs] タブ	[Unassigned Devices] チェックボックスをオンにします。 右側のペインには、どのサイトにも割り当てられていないすべての AP が一覧表示されます。

b) 設定する AP を選択します。

（注） このウィンドウでは、サイトに割り当てられている AP と未割り当て AP の両方を含め、最大 4,000 個の AP を選択できます。

AP を選択するには、次のいずれかの方法を使用します。

- AP を個別に選択するには、AP 名の横にあるチェックボックスをオンにします。
- ページに表示されているすべての AP を選択するには、テーブルの一番上にあるチェックボックスをオンにします。

  デフォルトでは、ページごとに 100 行が表示されます。
- 複数ページにあるすべての AP を選択するには、テーブルの上部にあるチェックボックスをオンにして、表示される [すべてを選択（Select All）] をクリックします。

  （注） このオプションは、AP の総数が 4,000 を超えない場合にのみ使用できます。
- 各列の上部にあるフィルタフィールドを使用して、必要な条件に基づいて AP をフィルタ処理します。フィルタリングした後、テーブルの上部にあるチェックボックスをオンにして、ページ上の検索条件に一致したすべての AP を選択するか、必要な AP 名の横にあるチェックボックスをオンにします。

c) （任意）[アクセスポイント（Access Points）]テーブルをカスタマイズするには、テーブルの右上隅にある歯車アイコンをクリックして、次のオプションを使用します。

- [テーブル密度（Table density）] で、希望するテーブル密度を選択します。

- [テーブル列（Table columns）] で、テーブルに表示する列名の横にあるチェックボックスをオンにします。

d) [Next] をクリックします。

ステップ 5 ライセンス要件を満たしていない AP を選択すると、Catalyst Center は詳細を示すダイアログボックスを表示します。ダイアログボックスで、必要なオプションをクリックします。

オプション	説明
ライセンス マネージャ	[License Manager] ウィンドウを開いて、対応するライセンスを有効にします。 ライセンスを有効にするには、『*Cisco Catalyst Center Administrator Guide*』の「Manage Licenses」を参照してください。
[Continue With The Workflow]	ワークフローを続行します。 （注） ライセンス要件を満たしていない AP は、ワールドワイドセーフモード（WWSM）になります。
Cancel	ダイアログボックスを閉じて、[Select Access Points] ウィンドウで別の AP を選択します。

ステップ 6 **[APおよび無線パラメータの選択（Select AP and Radio Parameters）]** ウィンドウで、設定する AP および無線パラメータを選択します。

Catalyst Center は、次のような特定の設定を 1 つの AP スロットのみに適用します。

- [5 GHz管理ステータス（5 GHz Admin Status）]：該当する AP のスロット 1 に適用されます。
- [2.4 GHz管理ステータス（2.4 GHz Admin Status）]：該当する AP のスロット 0 に適用されます。
- [6 GHz管理ステータス（6 GHz Admin Status）]：次のスロットに適用されます。
  - 6-GHz 対応 Cisco Catalyst 9136 シリーズ AP、Cisco Catalyst 9178I シリーズ AP、Cisco Catalyst 9179F シリーズ AP のスロット 3。
  - 6-GHz 対応 Cisco Catalyst 9162 シリーズ AP、Cisco Catalyst 9162 シリーズ AP、Cisco Catalyst 9164 シリーズ AP、Cisco Catalyst 9172H シリーズアクセスポイント、Cisco Catalyst 9172I シリーズアクセスポイント、Cisco Catalyst 9176D1 シリーズアクセスポイント、Cisco Catalyst 9176I シリーズアクセスポイント、Cisco Catalyst IW9167I Heavy Duty AP のスロット 2。
- [デュアルバンド（XOR）管理ステータス（Dual-Band (XOR) Admin Status）]：次のデュアルバンド（XOR）対応 AP のスロット 0 に適用されます。
  - Cisco Aironet 2800 シリーズ アクセス ポイント
  - Cisco Aironet 3800 シリーズ アクセスポイント

- Cisco Aironet 4800 シリーズ アクセスポイント
- Cisco Catalyst 9120 シリーズ アクセスポイント
- Cisco Catalyst 9176D1 シリーズ アクセスポイント
- Cisco Catalyst 9176I シリーズ アクセスポイント

デュアルバンド（XOR）対応 Cisco Wireless 9171I シリーズ AP のスロット 1 に適用されます。

次のデュアルバンド（XOR）対応 AP のスロット 2 に適用されます。

- Cisco Catalyst 9166 シリーズ AP
- Cisco Catalyst IW9165E AP
- Cisco Catalyst IW9165D Heavy Duty AP
- Cisco Catalyst IW9167E Heavy Duty AP
- Cisco Wireless 9174I シリーズ アクセスポイント
- Cisco Wireless 9174E シリーズ アクセスポイント

- [Tri-Radio Admin Status]：デュアル無線モードが有効になっているトライ無線対応 AP のスロット 2 に適用されます。

パラメータの構成を無効にするには、対応するチェックボックスをオンにして、[Disable] をクリックします。

ステップ 7 [Summary] ウィンドウで、設定を確認します。変更するには、[Edit] をクリックします。

ステップ 8 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

ステップ 9 [Tasks] ウィンドウで、タスクの展開を監視します。

既存のテンプレートを使用した AP の設定

次の手順に従って、既存のテンプレートを使用して Catalyst Center で AP および無線パラメータを設定します。

始める前に

AP 設定テンプレートが使用可能であることを確認します。新しいテンプレートを作成するには、[Configure AP And Radio Parameters] のワークフローで [Create Template] オプションを選択します。詳細については、AP の設定 （1639 ページ）を参照してください。

手順

ステップ 1 メインメニューから次を選択します。**[Workflows]** > **[Configure Access Points]** の順に選択します。

[Configure Your Access Points] ダイアログボックスが表示された場合は、[Let's Do It] をクリックしてワークフローに直接移動します。

ステップ 2 **[開始（Get Started）]** ウィンドウで、[タスク名（Task Name）] フィールドにワークフローの一意の名前を入力します。

ステップ 3 **[APの設定方法を指定（How do you want to configure APs?）]** ウィンドウで、次の設定を完了します。

a) [Configure AP Parameters Using Existing Templates] オプションボタンをクリックします。

テンプレートのリストが表示されます。

b) （任意） テンプレート名をクリックすると、設定が表示されます。

c) 必要なテンプレート名の横にあるチェックボックスをオンにします。

一度に選択できるテンプレートは 1 つだけです。

ステップ 4 [Select Access Points] ウィンドウで、設定する AP を選択します。

a) 設定する割り当て済み AP または未割り当て AP を選択します。

選択内容	結果
[Assigned APs] タブ	AP 関連の設定を適用するサイトに移動します。 右側のペインに、選択したサイトで使用可能なすべての AP が一覧表示されます。 （注） このウィンドウでは、最大2,000のサイトを選択できます。
[Unassigned APs] タブ	[Unassigned Devices] チェックボックスをオンにします。 右側のペインには、どのサイトにも割り当てられていないすべての AP が一覧表示されます。

b) 設定する AP を選択します。

（注） このウィンドウでは、サイトに割り当てられている AP と未割り当て AP の両方を含め、最大 4,000 個の AP を選択できます。

AP を選択するには、次のいずれかの方法を使用します。

- AP を個別に選択するには、AP 名の横にあるチェックボックスをオンにします。
- ページに表示されているすべての AP を選択するには、テーブルの一番上にあるチェックボックスをオンにします。

  デフォルトでは、ページごとに 100 行が表示されます。
- 複数ページにあるすべての AP を選択するには、テーブルの上部にあるチェックボックスをオンにして、表示される [すべてを選択（Select All）] をクリックします。

  （注） このオプションは、AP の総数が 4,000 を超えない場合にのみ使用できます。
- 各列の上部にあるフィルタフィールドを使用して、必要な条件に基づいて AP をフィルタ処理します。フィルタリングした後、テーブルの上部にあるチェックボックスをオンにして、ページ上の検索条件に一致したすべての AP を選択するか、必要な AP 名の横にあるチェックボックスをオンにします。

c) （任意）[アクセスポイント（Access Points）] テーブルをカスタマイズするには、テーブルの右上隅にある歯車アイコンをクリックして、次のオプションを使用します。

- [テーブル密度（Table density）] で、希望するテーブル密度を選択します。
- [テーブル列（Table columns）] で、テーブルに表示する列名の横にあるチェックボックスをオンにします。

d) [Next] をクリックします。

ステップ 5 ライセンス要件を満たしていない AP を選択すると、Catalyst Center は詳細を示すダイアログボックスを表示します。ダイアログボックスで、必要なオプションをクリックします。

オプション	説明
ライセンス マネージャ	[License Manager] ウィンドウを開いて、対応するライセンスを有効にします。 ライセンスを有効にするには、『*Cisco Catalyst Center Administrator Guide*』の「Manage Licenses」を参照してください。

オプション	説明
[Continue With The Workflow]	ワークフローを続行します。 （注） ライセンス要件を満たしていない AP は、ワールドワイドセーフモード（WWSM）になります。
Cancel	ダイアログボックスを閉じて、[Select Access Points] ウィンドウで別の AP を選択します。

ステップ 6 Catalyst Center は、選択したテンプレートの設定に基づいて対応する後続の設定ウィンドウを表示します。これらの各設定ウィンドウには、テンプレートに従って事前設定が表示されます。必要に応じて、既存の設定を使用するか再設定するかを選択できます。AP および無線パラメータの設定の詳細については、「AP の設定 （1639 ページ）」を参照してください。

（注） **[AP名の変更（Modify AP Name）]** ウィンドウに表示される AP のリストは、テンプレート設定に従っているのではなく、**[アクセスポイントの選択（Select Access Points）]** ウィンドウで前に選択した AP に基づいています。

- **[Modify AP Name]**
- Configure AP Geolocation Parameters
- [Configure AP Parameters]
- Configure AP LAN port parameters
- [Configure 5 GHz Radio Parameters]
- [Configure 2.4 GHz Radio Parameters]
- [Configure 6 GHz Radio Parameters]
- [Configure Dual-Band (XOR) Radio Parameters]
- [Configure Tri-Radio Parameters]

ステップ 7 （任意） **[再利用可能なテンプレートとして保存（Save As Reusable Template）]** ウィンドウで、次のオプションのいずれかを選択して設定の変更をテンプレートとして保存するか、この時点で変更を保存しない場合は [保存しない（Do Not Save）] をクリックします。

- 新しいテンプレートとして保存するには、[Create] をクリックし、[Template Name] フィールドに名前を入力します。
- 既存のテンプレートを更新するには、[Update] をクリックします。

ステップ 8 [Summary] ウィンドウで、設定を確認します。変更するには、[Edit] をクリックします。

ステップ 9 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 10 [Tasks] ウィンドウで、タスクの展開を監視します。

デバイスの交換

次の手順では、故障したデバイスの交換方法について説明します。

シスコスイッチスタック（ハードウェアスタッキング）内のメンバースイッチを交換する場合も、同じ手順で交換できます。アクティブスイッチは、交換用のソフトウェアイメージと設定を提供します。 Catalyst Center はスタック全体の交換を処理します。

（注） デバイスの交換ワークフローを完了する前に終了する場合は、進行中のカードに関して次のガイドラインを確認してください。

- デバイスの**[ワークフロー（Workflows）]** ウィンドウに [進行中（In progress）] カードがあり、**[インベントリ（Inventory）]** > **[交換するようにマーク済み（Marked for Replacement）]** ウィンドウから同じデバイスを交換しようとすると、[進行中（In Progress）] のシリアル番号とタスク名を含む確認メッセージが表示されます。シリアル番号で特定される各デバイスにつき 1 つのデバイス置換ワークフローしか開始できないため、このメッセージが表示されます。このデバイスの交換を続行するには、[はい（Yes）] をクリックします。続行しない場合、同じデバイスで新しいワークフローを開始するには、[キャンセル（Cancel）] をクリックし、進行中のワークフローを削除してから、新しいワークフローを開始します。
- **[ワークフロー（Workflows）]** ウィンドウで、交換対象としてマークされていないデバイスの [進行中（In progress）] カードをクリックすると、警告メッセージが表示されます。[Yes] をクリックし、障害のある別のデバイスを選択して、新しいワークフローを開始します。[Cancel] をクリックすると、ワークフローがキャンセルされます。

始める前に

- 交換するデバイスにマークを付ける前に、故障したデバイスのソフトウェアイメージバージョンをイメージリポジトリにインポートしてください。
- 故障したデバイスが到達不能であることを確認します。

- プラグアンドプレイ（PnP）で交換用デバイスが Catalyst Center にオンボードされている場合は、故障したデバイスをユーザー定義サイトに割り当ててください。
- デバイスの交換ワークフローを開始するときに、交換用のデバイスがプロビジョニング状態ではないことを確認します。
- スイッチスタックを交換する場合、故障したデバイスと交換用デバイスのスタック数は同一である必要があります。
- 交換用の ワイヤレスコントローラ がサイトに割り当てられていないこと、またはプロビジョニングされていないことを確認してください。

手順

ステップ 1 メインメニューから次を選択します。**[Workflows]** > **[Replace Device]** の順に選択します。

[インベントリ（Inventory）] ウィンドウから故障したデバイスを交換することもできます。ワークフローは **[交換用デバイスの選択（Choose Replacement Device）]** ウィンドウから開始します（「ステップ 6（1665 ページ）」を参照）。詳細については、故障したデバイスの交換（244 ページ）を参照してください。

ステップ 2 [始める（Get Started）] ウィンドウで、ワークフローの一意のタスク名を入力します。

ステップ 3 [Choose Device Type] 画面で、交換する故障したデバイスのタイプを選択します。

ステップ 4 [Choose Site] 画面で、故障したデバイスがあるサイトを選択します。

ステップ 5 [Choose Faulty Device] ウィンドウで、交換する故障したデバイスを選択します。

故障したデバイスが見つからない場合は、故障したデバイスを追加します。

1. [Add Faulty Device] をクリックします。
2. 故障したデバイスを選択し、[Next] をクリックします。
3. [Mark For Replacement] ウィンドウで、[Mark] をクリックします。

（注） 選択ウィンドウで、右下隅にある [確認（Review）] をクリックして、現在の要約された設定の詳細を表示します。

ステップ 6 **[交換用デバイスの選択（Choose Replacement Device）]** ウィンドウの [プラグアンドプレイ（Plug and Play）] タブまたは [インベントリ（Inventory）] タブから交換用デバイスを選択します。

[プラグアンドプレイ（Plug and Play）] タブには、PnP によってオンボードされたデバイスが表示されます。[インベントリ（Inventory）] タブには、インベントリまたは検出プロセスによってオンボードされたデバイスが表示されます。

交換用のデバイスが PnP を介してオンボードされていない場合は、手動または自動で追加します。

- 手動：[プラグアンドプレイ（Plug and Play）] タブで、[デバイスの追加（Add Device）] をクリックします。**[新しいデバイスの追加（Add New Device）]** ウィンドウで、デバイスのシリアル番号を入力し、[新しいデバイスの追加（Add New Device）] をクリックします。
- 自動：[プラグアンドプレイ（Plug and Play）] タブで、[スマートアカウントとの同期（Sync with Smart Account）] をクリックします。**[スマートアカウントとの同期（Sync with Smart Account）]** ウィンドウで、[同期（Sync）] をクリックします。

ステップ 7 ワイヤレスコントローラ の場合、**[交換デバイスの設定（Configure replacement device）]** ウィンドウで、交換に必要な設定の詳細を入力します。

a) 故障した ワイヤレスコントローラ にマスター暗号化キーが設定されている場合は、ワイヤレスコントローラ 交換用の [マスター暗号化設定キー（Master Encryption Configuration Key）] フィールドにキーを入力します。

（注） 暗号化されたパスワードとキーは、正しいマスター暗号化キーがないと復元できません。このキーがないと、ワイヤレスコントローラ にアクセスできなくなり、RMA プロセスが失敗します。

b) [HAの設定（Configure HA）] で、次のいずれかのオプションを選択します。

- [はい（Yes）]：故障した ワイヤレスコントローラ 高可用性（HA）ペアを新しいペアに置き換える場合。

  プライマリ交換とセカンダリ交換 ワイヤレスコントローラの両方に必要な設定を完了します。

  （注） HA ペアの ワイヤレスコントローラ の場合、ペアの両方のデバイスがダウンしている場合にのみ、デバイスの置換ワークフローを使用します。このワークフローを使用して、アクティブな HA ペア内の単一の故障した ワイヤレスコントローラ を置き換えることはできません。

- [いいえ（No）]：スタンドアロン ワイヤレスコントローラを交換する場合。

  交換用の ワイヤレスコントローラ に必要な設定を完了します。

交換用のデバイスを設定するには、IPv4 アドレスとその対応する設定、IPv6 アドレスとその対応する設定、またはその両方を使用できます。

（注） 障害のある ワイヤレスコントローラ の IP アドレスは、PnP を介して交換用 ワイヤレスコントローラ を要求するときに再利用できません。

オプション	説明
Wireless Management IPv4	ワイヤレス管理インターフェイスの有効な IPv4 アドレスを入力します。 （注） • 交換用 ワイヤレスコントローラ のワイヤレス管理 IP アドレスは、故障したワイヤレスコントローラのワイヤレス管理 IP アドレスと異なる必要があります。 • 故障した ワイヤレスコントローラ HA ペアを新しいペアに置き換えるには、プライマリおよびセカンダリ ワイヤレスコントローラのワイヤレス管理IPアドレスが異なっている必要があります。
Subnet Mask	IPv4 サブネット マスクを選択します。
Wireless Management IPv6	該当する場合は、ワイヤレス管理インターフェイスの有効な IPv6 アドレスを入力します。 （注） • 交換用 ワイヤレスコントローラ のワイヤレス管理 IP アドレスは、故障したワイヤレスコントローラのワイヤレス管理 IP アドレスと異なる必要があります。 • 故障した ワイヤレスコントローラ HA ペアを新しいペアに置き換えるには、プライマリおよびセカンダリ ワイヤレスコントローラのワイヤレス管理IPアドレスが異なっている必要があります。
Prefix Length	IPv6 プレフィックス長を選択します。
Gateway IPv4	デフォルトゲートウェイ IPv4 アドレスを入力します。
Gateway IPv6	デフォルト ゲートウェイ IPv6 アドレスを入力します。
VLAN ID	VLAN ID を入力します。 有効な範囲は 1 ～ 4094 です。 （注） 故障した ワイヤレスコントローラ と交換用の両方で VLAN ID が同じである必要があります。
Interface Name	ワイヤレス管理に使用する特定のインターフェイス名を入力します。

オプション	説明
ローカル冗長性管理 IP	該当する場合は、交換用 ワイヤレスコントローラ のローカル冗長管理 IP アドレスを入力します。 （注） • この IP アドレスとピア冗長性管理 IP アドレスが同じでないことを確認します。 • このIPアドレスが他のネットワークエンティティに割り当てられていないことを確認します。
セカンダリ WLC の選択	該当する場合は、HA のセカンダリ ワイヤレスコントローラを選択します。 （注） 障害のある ワイヤレスコントローラ HA ペアを新しいペアに置き換えるには、次のことを確認します。 • セカンダリ ワイヤレスコントローラ のワイヤレス管理 IPアドレスとサブネットマスクが、故障したワイヤレスコントローラ のワイヤレス管理 IP アドレスと同じ IP サブネット内にあることを確認してください。 • セカンダリ ワイヤレスコントローラ のワイヤレス管理 VLAN がプライマリ ワイヤレスコントローラ の VLAN と一致していることを確認してください。 • 将来のワイヤレスコントローラをプライマリまたはセカンダリ ワイヤレスコントローラとして選択することはできません。要求元不明、オンボード済みのワイヤレスコントローラ、およびプロビジョニングされていないインベントリベースのワイヤレスコントローラのみを選択できます。
ピア冗長性管理 IP	該当する場合は、セカンダリ ワイヤレスコントローラ のピア冗長管理 IP アドレスを入力します。 （注） • この IP アドレスとローカル冗長性管理 IP アドレスが同じでないことを確認します。 • このIPアドレスが他のネットワークエンティティに割り当てられていないことを確認します。

ステップ 8　**[概要（Summary）]** ウィンドウで、要約された詳細を確認します。

必要に応じて、[編集（Edit）]をクリックして、デバイスタイプまたは故障したデバイスの詳細を更新します。

（注） 設定の可視性と制御が無効になっている場合は、[交換用デバイス（Replacement Device）] の [表示（View）] をクリックして、交換用デバイスの設定を確認します。

ステップ 9 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 10 **[インベントリ（Inventory）]** ウィンドウでは、デバイスが交換されるときに、デバイス交換タスクの進行状況を表示します。

または、**[タスク（Tasks）]** ウィンドウからタスクをモニターできます。

1. **[インベントリ（Inventory）]** ウィンドウで、[フォーカス（Focus）] ドロップダウンリストから [デバイスの交換（Device Replacement）] を選択します。
2. [交換ステータス（Replace Status）] 列で交換のステータスを確認します。

   デバイスが正常に交換されると、[交換済み（Replaced）] ステータスが表示されます。

   デバイスの交換に失敗し、エラーメッセージが表示された場合は、エラーリンクをクリックします。[再試行（Retry）]をクリックして、同じ障害のあるデバイスと交換デバイスのセットを使用してワークフローを再試行します。

   （注） [Main Inventory] ウィンドウには、故障したデバイスと交換した新しいデバイスの詳細情報が表示されます。

3. [交換ステータス（Replace Status）]列で、デバイスのステータスをクリックすると、スライドインペインに詳細情報が表示されます。

   たとえば、スライドインペインには、システムがタスクを完了するために次の手順が表示されます。

   1. デバイス交換の準備状況チェックを実行します。
   2. （PnP）交換用デバイスを請求します。
   3. 交換用デバイスにソフトウェアイメージを配信してアクティブ化します。
   4. ライセンスを展開する。
   5. VLAN 構成をプロビジョニングします。

6. スタートアップ構成をプロビジョニングします。
7. 交換用デバイスをリロードします。
8. 交換用デバイスの到達可能性を確認します。
9. 交換用デバイスに SNMPv3 ログイン情報を展開します。
10. 交換用デバイスを同期します。
11. 故障したデバイスを CSSM から削除します。
12. 交換用デバイスを CSSM に追加します。
13. PKI 証明書を失効化して作成します。
14. Cisco ISE を更新します。
15. 障害のあるデバイスを削除します。

次のタスク

ワイヤレスコントローラの交換中には、次のファイルと設定は交換用のワイヤレスコントローラに転送されません。

- カスタム Web 認証バンドルおよび NBAR プロトコルパック
- IP アドレス SSH RSA キーまたはキーペア名
- カスタムトラストポイント

交換後、交換用のワイヤレスコントローラでこれらの設定をコピーして手動で再設定します。

スイッチの更新

スイッチの更新ワークフローを使用すると、サポート終了（EoX）に達した古いスイッチを新しいスイッチに交換できます。たとえば、Cisco Catalyst 3650 スイッチを Cisco Catalyst 9300 スイッチに交換できます。

（注） 現在、スイッチの更新は、Cisco IOS XE で実行されている Cisco Catalyst 3650 および Cisco Catalyst 3850 スイッチで使用できます。

この機能には次の制限があります。

- サポートされていないオペレーティングシステム： Cisco IOS イメージで実行されている古いデバイス（Cisco Catalyst 2000、3000、4000、6000 シリーズ スイッチ）はサポートさ

れていません。Cisco IOS XE（Cisco Catalyst 3650 および 3850 シリーズ スイッチ）で実行されている古いデバイスのみがサポートされています。

- 一貫性のないポートタイプまたは速度：古いデバイスとはポートタイプや速度が異なる新しいデバイスはサポートされません。たとえば、ギガビットイーサネットから10ギガビットイーサネットへの変換はサポートされていません。
- 新しいデバイスの最小ソフトウェアバージョン要件：Cisco Catalyst 3650 シリーズ、3850 シリーズ、および 9300 シリーズ スイッチの場合、必要な最小ソフトウェアバージョンは 16.9.x です。
- ファブリックネットワークでのプラグアンドプレイ（PnP）オンボーディング：ファブリックネットワーク内の新しいデバイスの PnP オンボーディングはサポートされていません。PnP を使用して新しいデバイスをオンボードするには、新しいデバイスに IP アドレスと PnP プロファイルを手動で設定する必要があります。

始める前に

次の条件が満たされていることを確認します。

- ポート数：新しいデバイスには、古いデバイスと同じ数以上のポートを設定できます。

  たとえば、24 ポートの Cisco Catalyst 3650 スイッチを 24 ポートの Cisco Catalyst 9300 スイッチや 48 ポートの Cisco Catalyst 9300 スイッチに交換できます。
- ポートタイプ：ポートタイプは、古いデバイスと新しいデバイスで同じである必要があります。
- デバイスの到達可能性：ワークフローに進む前に、古いデバイスが到達不能状態であることを確認します。
- スタックメンバー数：スタック構成スイッチの場合、新しいデバイスのスイッチメンバー数は同数以上である必要があります。
- ロールの一貫性：ワークフローで選択されるデバイスは、同じロールである必要があります。
- ポート接続：新しいデバイスのすべてのポートが古いデバイスと同じ方法で接続されていることを確認します。

手順

ステップ 1 メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。

ステップ 2 交換する古いデバイスの横にあるチェックボックスをオンにして、**[Actions]** > **[Switch Refresh]** > **[Mark for Refresh]** の順に選択します。

ステップ 3 確認ウィンドウで、[Mark] をクリックします。

[成功（Success）] メッセージが表示され、古いデバイスが交換対象として正常にマークされます。

ステップ 4 古いデバイスを選択し、次に**[アクション（Actions）]**>**[デバイスの更新（Device Refresh）]**>**[デバイスの更新（Refresh Device(s)）]**を選択します。

スイッチ更新ワークフローがトリガーされます。

または、ワークフローをトリガーするために、**[Workflows]** > **[Switch Refresh]**の順に選択します。

ステップ 5 タスクの概要ウィンドウが表示されたら、[実行する（Let's Do It）] をクリックして、ワークフローに直接移動します。

ステップ 6 [Task Name] フィールドに一意の名前を入力し、[Next] をクリックします。

ステップ 7 [Pre-requisites] ウィンドウで、ゴールデンイメージが新しいデバイスにすでにタグ付けされている場合は、[Next] をクリックします。それ以外の場合は、[Image Repository] ハイパーリンクをクリックして、新しいデバイスにゴールデンイメージをタグ付けします。

ゴールデンイメージのタグ付け方法については、ソフトウェアイメージをスタンダードとしてマークする （646 ページ）を参照してください。

タスクが完了したら、[スイッチの更新（Switch Refresh）] ワークフロータブに移動し、[次へ（Next）] をクリックします。



（注） 古いスイッチが MD5 で設定され、新しいスイッチのゴールデンイメージが 17.14.1 より後の場合、新しいスイッチは SHA で設定されます。

ステップ 8 [Select Devices] ウィンドウで、交換対象としてマークされた古いデバイスを選択し、[Next] をクリックします。

ステップ 9 [古いデバイスを新しいデバイスに置換（Replace old device with the new device）]ウィンドウで次の手順を実行します。

1. 必要に応じて、デフォルトの [New Device Name] を編集します。
2. ドロップダウンリストからデバイスの [Platform] および [Serial Number] を選択します。
3. [Next] をクリックします。

ステップ 10 [Resolve Dependencies] ウィンドウで、デバイスにゴールデンイメージが割り当てられていない場合、ワークフローを続行できません。

a) デバイスにゴールデンイメージを割り当てるには、[Image Repository] ハイパーリンクをクリックし、ソフトウェアイメージをスタンダードとしてマークする （646 ページ）に記載されている手順に従います。

b) タスクが完了したら、[スイッチの更新（Switch Refresh）] ワークフロータブに移動し、[次へ（Next）] をクリックします。

ステップ 11 [View Device Configuration] ウィンドウで、古いデバイスから新しいデバイスにプッシュされた設定を確認し、[Next] をクリックします。

ステップ 12 [Schedule Task] ウィンドウで、[Now] をクリックしてデバイスの交換をただちに開始するか、[Later] をクリックして特定時刻でのデバイスの交換をスケジュールします。[Next] をクリックします。

ステップ 13 [Summary] ウィンドウで設定を確認し、[Refresh Devices] をクリックします。

古いデバイスと新しいデバイスの交換が開始されます。

ステップ 14 [Monitor Refresh Status] をクリックして、交換用デバイスのステータスを表示します。

[Inventory] ウィンドウが表示されます。デバイス交換ステータスは、[Refresh Status] 列で確認できます。

ステップ 15 [Refresh Status] 列にあるリンクをクリックして、進行中のプロセスを表示します。

ステップ 16 [Refresh] をクリックします。この処理には、しばらく時間がかかる場合があります。

デバイスの交換が正常に完了すると、古いデバイスが新しいデバイスに置き換えられます。

リモートサポート許可の作成

リモートサポート許可を作成するには、次の手順を実行します。



（注） Catalyst Center のリモートサポート承認は、RADKit バージョン 1.2.1 以降でのみサポートされます。

手順

ステップ 1 メインメニューから次を選択します。**[Workflows]** > **[Create a Remote Support Authorization]**の順に選択します。

ステップ 2 タスクの概要ウィンドウが表示されたら、[Let's Do It] をクリックして、ワークフローに直接移動します。

ステップ 3 [アクセス許可に関する合意事項（Access Permission Agreement）] ウィンドウで、次の手順を実行します。

a) [I agree to provide access to network devices] チェックボックスをオンにして、ネットワークデバイスへのアクセスを承認します。

b) **[I agree to provide access to Catalyst Center]** チェックボックスをオンにして、シスコスペシャリストが SSH ログイン情報を使用して Catalyst Center セットアップにアクセスできるよう承認します。



（注） 承認は、期限前であればいつでも取り消すことができます。承認を取り消すには、「View the Remote Support Authorization Dashboard」を参照してください。

ステップ 4 [次のステップ（Next Step）] をクリックします。

ステップ 5 [許可の設定（Set up the Authorization）] ウィンドウで、次のフィールドに入力します。

- シスコスペシャリストの電子メールアドレス

- シスコスペシャリストのアクセスロール
- 既存のケース番号
- アクセスを許可する理由

ステップ 6 [次のステップ（Next Step）] をクリックします。

ステップ 7 [Schedule the Access] ウィンドウで、[Now] または [Later] をクリックして、シスコスペシャリストによる Catalyst Center へのアクセスをいつ許可するかを指定します。

ステップ 8 [次のステップ（Next Step）] をクリックします。

ステップ 9 [Summary] ウィンドウで、設定を確認します。変更するには、[Edit] をクリックします。

ステップ 10 [作成（Create）] をクリックします。

タスク完了許可が作成されました（Authorization is created）] ウィンドウが表示されます。

ステップ 11 [View All Authorizations] をクリックして、[Remote Support Authorization] ウィンドウに移動します。詳細は、「View the Remote Support Authorization Dashboard」を参照してください。

イベント通知の作成

Catalyst Center イベント通知を使用すると、複数のポイントで発生する選択したイベントの詳細を配信する 1 つの通知内に複数のチャネルを関連付けることができます。

手順

ステップ 1 メインメニューから次を選択します。**[Workflows]** > **[Create a New Notification]**の順に選択します。

ステップ 2 タスクの概要ウィンドウが開いたら、[Let's Do It] をクリックして、ワークフローに直接移動します。

ステップ 3 [チャネルの選択（Select Channels）] ウィンドウで、通知チャネルを選択します。

サポートされているチャネルは、[REST]、[PAGERDUTY]、[SNMP]、[SYSLOG]、[WEBEX]、[EMAIL]、およびカスタムチャネルです。Assurance イベントでは、SNMP はサポートされません。

ステップ 4 [サイトとイベントの選択（Select Site and Events）] ウィンドウで、[サイトの選択（Select a site）] ドロップダウンリストから、選択したイベントの通知を受け取る特定のサイトを選択します。

（注） 同時に複数のサイトを選択できます。

ステップ 5 イベントの横にあるプラスアイコンをクリックするか、[Add All] をクリックしてすべてのイベントをそれぞれの通知に追加します。

ステップ 6 通知からイベントを削除するには、削除するイベントの横にあるXアイコンをクリックするか、[Remove All] をクリックしてイベントリストからすべてのイベントを削除します。

（注）
- 通知チャネルを選択すると、[サイトとイベントの選択（Select Site and Events）] ウィンドウのテーブルに、選択した通知チャネルでサポートされるイベントの数が一覧表示されます。
- 複数の通知チャネルを選択すると、[サイトとイベントの選択（Select Site and Events）] ウィンドウのテーブルに、選択した通知チャネルに共通のサポートされているイベントの数が一覧表示されます。

ステップ 7 **[通知の設定（Configure Notification）]** ウィンドウで、次の値を設定します。

1. [EMAIL] 通知チャネルを選択した場合は、**[メールの設定（Email Settings）]** ウィンドウで次のように設定します。
   1. リンクをクリックして **[Email] GUI** ウィンドウにアクセスし、新しいメールサーバーを設定します。

（注）
- 通知タイプは、[REST] API エンドポイント（ウェブフック）、[PAGERDUTY]、[SNMP]、[SYSLOG]、[WEBEX]、または [EMAIL] のいずれかに設定できます。[EMAIL] を選択した場合に電子メール設定が完了していないと、該当する **[GUI]** ウィンドウにアクセスして設定作業を行うよう求められます。電子メール設定は、[Email] タブで設定します。

  （オプション）[Email] タブにアクセスするには、メニューアイコンをクリックして次を選択します。 **[System]** > **[Settings]** > **[External Services]**を選択します。

  [外部サービス（External Services）] を展開し、**[宛先（Destinations）]** を選択して、[Email] タブをクリックします。
- 電子メール通知を受信する電子メールアドレスは、エンドポイントごとに最大 20 個まで設定できます。複数の電子メールアドレスを追加するには、各電子メールアドレスを個別に追加し、追加するたびに（キーボードの）Enter を押す必要があります。Catalyst Center により電子メールアドレスが検証され、構文が正しくない場合は通知されます。
- エンドポイントごとに 20 を超える電子メールアドレスを設定する必要がある場合は、グループ電子メールエイリアスを使用できます。
- イベント サブスクリプションに電子メールの宛先を使用している場合、送信される電子メールには UTC タイムスタンプ付きのイベントが表示されます。

   2. [Select Existing Instance] をクリックして既存の電子メールインスタンスを使用するか、[Create New Instance] をクリックして新しい電子メールインスタンスを作成します。
   3. [既存のインスタンスを選択（Select Existing Instance）] をクリックした場合は、[インスタンスの選択（Select Instance）] ドロップダウンリストから電子メールインスタンスを選択します。

4. [From] および [To] フィールドに電子メールアドレスを入力し、電子メールの [Subject] ヘッダーに件名を入力します。

2. [SYSLOG] 通知を選択した場合は、**[Syslogの設定（Syslog Settings）]** ウィンドウで次の値を設定します。

   1. リンクをクリックして **[Syslog]** GUI ウィンドウにアクセスし、新しい syslog エンドポイント（Syslog サーバーのホスト名とポート番号）を設定します。

      （注） 通知タイプは、[REST] API エンドポイント（ウェブフック）、[PAGERDUTY]、[SNMP]、[SYSLOG]、[WEBEX]、または [EMAIL] のいずれかに設定できます。[SYSLOG] を選択したが、Syslog サーバーの設定を行っていない場合、GUI ウィンドウにアクセスして設定作業を行うよう求められます。Syslog サーバーの設定は、[Syslog] タブで行います。

      （オプション）[Syslog] タブにアクセスするには、メニューアイコンをクリックして次を選択します。 **[System]** > **[Settings]** > **[External Services]**を選択します。

      [外部サービス（External Services）] を展開し、**[宛先（Destinations）]** を選択して、[Syslog] タブをクリックします。

   2. [Protocol] フィールドに、TCP または UDP のいずれかを入力します。
   3. [Port] フィールドに、syslog サーバーのポート番号を入力します。
   4. [Hostname/IP] フィールドで、syslog サーバーのホスト名または IP アドレスを入力します。
   5. [インスタンスの選択（Select Instance）] ドロップダウンリストで syslog インスタンスを選択します。

3. [REST] 通知を選択した場合は、**[RESTの設定（REST Settings）]** ウィンドウで次の値を設定します。

   - リンクをクリックして **[RESTウェブフック（REST Webhook）]** GUI ウィンドウにアクセスし、新しいウェブフックエンドポイントを設定します。

（注） 通知タイプは、[REST] API エンドポイント（ウェブフック）、[PAGERDUTY]、[SNMP]、[SYSLOG]、[WEBEX]、または [EMAIL] のいずれかに設定できます。[REST] を選択したが、ウェブフックの設定を行っていない場合、 GUI ウィンドウにアクセスして設定作業を行うよう求められます。ウェブフックの設定は [Webhook] タブで行います。

（オプション）[Webhook] タブにアクセスするには、メニューアイコンをクリックして次を選択します。 **[System]** > **[Settings]** > **[External Services]**を選択します。

[外部サービス（External Services）] を展開し、**[宛先（Destinations）]** を選択して、[Webhook] タブをクリックします。

- [ウェブフックインスタンス（Webhook Instance）] ドロップダウンリストから、通知エンドポイントと URL を選択します。
- [URL] フィールドにイベント送信先の REST API エンドポイントの URL アドレスを入力します。

  [Trust certificate]：REST API エンドポイント通知に信頼できる証明書が必要かどうか。

  [Method]：PUT メソッドまたは POST メソッド。
- [Basic]：クライアントが HTTP 要求を送信することで認証を行います。認証ヘッダーには「Basic」という単語が含まれ、後にスペース、「username:password」の形式の base64 でエンコードされた文字列が続きます。GUI で [Basic] を選択すると、[Headers] フィールドに「Authorization」という値が自動的に入力されます。
- [Token]：サーバーから提供されたセキュリティトークンを使用してユーザーが認証されます。[Token] を選択すると、[Headers] フィールドに「X-Auth-Token」という値が自動的に入力されます。
- [No Authentication]：認証が不要になります。
- [Headers]：[Header Name] と [Header Value]。

（注） [Headers] フィールドは、認証の選択内容に応じて自動的に値が入力される場合があります。

4. [SNMP] 通知チャネルを選択した場合は、**[SNMPの設定（SNMP Settings）]** ウィンドウで次のように値を設定します。
   1. リンクをクリックして **[SNMP]** GUI ウィンドウにアクセスし、新しい SNMP エンドポイントを設定します。



（注） 通知タイプは、[REST] API エンドポイント（ウェブフック）、[PAGERDUTY]、[SNMP]、[SYSLOG]、[WEBEX]、または [EMAIL] のいずれかに設定できます。[SNMP] を選択した場合に SNMP 設定が完了していないと、該当する GUI ウィンドウにアクセスして設定作業を行うよう求められます。SNMP の設定は [SNMP] タブで行います。

（オプション）[SNMP] タブにアクセスするには、メニューアイコンをクリックして次を選択します。 **[System]** > **[Settings]** > **[External Services]**を選択します。

[外部サービス（External Services）] を展開し、**[宛先（Destinations）]** を選択して、[SNMP] タブをクリックします。

SNMP トラップ通知は、システム ハードウェア イベントに対してのみ使用できます。ハードウェアコンポーネントの正常性状態が変化した場合、システム ハードウェア イベントによってサブスクライバへの通知がトリガーされます。変更がモニターされるハードウェアコンポーネントには、CPU、メモリ、ディスク、NIC、ファン、電源、RAID コントローラなどがあります。

2. [SNMPインスタンス（SNMP Instance）] ドロップダウンリストから、通知エンドポイントを選択します。
3. [Create a new endpoint]：新しいエンドポイント名と説明を入力します。
4. [Hostname/IP Address] フィールドに SNMP トラップ受信機（サーバー）のホスト名または IP アドレスを入力します。
5. [Port] フィールドに SNMP トラップ受信機（サーバー）のポート番号を入力します。

5. [PAGERDUTY] 通知チャネルを選択した場合は、**[PAGERDUTYの設定（PAGERDUTY Settings）]** ウィンドウで次のように設定します。
   1. [SERVICE CONFIGURATION] エリアで、[Select Existing Instance] をクリックして既存の PagerDuty インスタンスを使用するか、[Create New Instance] をクリックして新しい PagerDuty インスタンスを作成します。
   2. [Select Instance] ドロップダウンリストで PagerDuty インスタンスを選択します。
   3. [PagerDuty Events API URL] フィールドに、PagerDuty イベント API URL を入力します。
   4. [PagerDuty Integration Key] フィールドに、PagerDuty 統合キーを入力します。
6. [WEBEX] 通知チャネルを選択した場合は、**[WEBEXの設定（WEBEX Settings）]** ウィンドウで次のように値を設定します。
   1. [インスタンスの選択（Select Instance）] ドロップダウンリストで Webex インスタンスを選択します。
   2. [Webex URL] フィールドに、Webex URL を入力します。
   3. [Webex Room ID] フィールドに、Webex ルーム ID を入力します。

4. [Webex Bot Access Token] フィールドに、Webex ボットアクセストークンを入力します。

ステップ 8 **[Save]** をクリックします。

[名前と説明（Name and Description）] ウィンドウで、次の手順を実行します。

a) [Name] フィールドに、通知の一意の名前を入力します。
b) [Description] ボックスに、通知の説明を入力します。

ステップ 9 [Summary] ウィンドウで、設定を確認します。変更するには、[Edit] をクリックします。

ステップ 10 [完了（Finish）] をクリックします。

タスク完了[Done! Your new notification is complete] ウィンドウが表示されます。

リモート LAN の設定

リモート LAN（RLAN）を使用すると、シスコ ワイヤレス コントローラ の AP に RLAN ポートを構成できます。ワイヤレスコントローラは有線クライアントを認証し、ネットワークへの接続を許可します。

Catalyst Center は Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ でのみ RLAN 構成をサポートします。Cisco IOS XE リリース 16.12 以降を実行する ワイヤレスコントローラ では非ファブリックサイトに RLAN を設定できます。Cisco IOS XE リリース 17.7 以降を実行する ワイヤレスコントローラ ではファブリックサイトに RLAN を設定できます。

ネットワーク設定またはネットワークプロファイル（APプロファイル、RFプロファイル、サイトタグなど）の変更は、RLANワークフローの一部としてプッシュされるため、接続されているクライアントのネットワークが中断される可能性があります。

（注） Catalyst Center は Cisco AireOS ワイヤレスコントローラ での RLAN 設定をサポートしていません。

RLAN ポートを設定するには、この手順を使用します。

始める前に

- RLAN ポートを設定するサイトにワイヤレスコントローラおよび 1 つ以上の AP がプロビジョニングされていることを確認します。
- 関連するネットワークプロファイルのCLIテンプレートと機能テンプレートの変更は、このワークフローでは設定されません。[Inventory] ウィンドウで、関連付けられたワイヤレスコントローラのプロビジョニングステータスが最新であることを確認します。プロビジョニングステータスの横に [Out of Sync] 通知がある場合は、RLAN を設定する前にワイヤレスコントローラを再プロビジョニングします。

ファブリックサイトに RLAN ポートを構成するには、次の手順を実行します。

- 必要なファブリックサイトがプロビジョニングされていることを確認します。
- IP プールとセキュリティグループタグ（SGT）が作成されていることを確認します。

手順

ステップ 1 メインメニューから次を選択します。 **[Workflows]** > **[Configure RLAN]** の順に選択します。

ステップ 2 タスクの概要ウィンドウが表示されたら、[実行する（Let's Do It）] をクリックして、ワークフローに直接移動します。

ステップ 3 [Get Started] ウィンドウで、タスクの一意の名前を入力します。

ステップ 4 [Select Sites] ウィンドウで、RLAN ポートを設定するサイトを選択します。

（注） 複数のサイトを選択できますが、選択したサイトは同じ Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ で管理する必要があります。

選択したサイトの AP に RLAN 設定を割り当てると、ポリシータグの割り当てに基づいて、他のサイトの AP の RLAN 設定に影響を与える可能性があります。

右側のペインには、選択したサイトの概要が表示されます。Catalyst Center は選択したサイトのフロアでプロビジョニングされたすべての AP の RLAN を設定します。

ステップ 5 [Select Policy Tags] ウィンドウで、RLAN を設定するポリシータグの横にあるチェックボックスをオンにします。

この選択は、ポリシータグの割り当てに基づいて、他のサイトの AP の RLAN 設定に影響を与える可能性があります。

- ポリシータグの影響を受けるサイトを表示するには、[Impacted Sites] で対応する番号をクリックします。サイトを検索するには、[Impacted Sites] ダイアログボックスの [Search Table] フィールドにサイトの名前の一部または完全な名前を入力し、**Enter** キーを押します。
- ポリシータグの影響を受ける AP を表示するには、[Impacted APs] で対応する番号をクリックします。[影響を受けるアクセスポイント（Impacted Access Points）] ダイアログボックスで特定の詳細に基づいて AP をフィルタ処理するには、検索アイコンをクリックし、フィルタオプション（[クイックフィルタ（Quick Filters）]、[詳細フィルタ（Advanced Filters）]、または [最近のフィルタ（Recent Filters）]）から選択します。フィルタで必要なオプションを選択し、[適用（Apply）] をクリックします。

ステップ 6 [リモートLANの設定（Remote LAN Configuration）] ウィンドウで、次の手順を実行します。

a) [ポート1（Port 1）]、[ポート2（Port 2）]、および [ポート3（Port 3）] オプションから必要な RLAN ポートを選択します。

サイトには、異なる番号の LAN ポートを持つ AP を設定できます。RLAN 設定は、対応する LAN ポート番号に適用されます。AP に単一の RLAN ポートがある場合、Catalyst Center では AP の [Port 2]、および [Port 3] の設定は無視されます。

サイトがセカンダリのワイヤレスコントローラによって管理されている場合、セカンダリのワイヤレスコントローラで RLAN クライアント用に設定される VLAN は、プライマリのワイヤレスコントローラで設定される VLAN と同じです。

b) 対応するポートの RLAN を有効または無効にするには、[AP LAN Port] トグルボタンを使用します。

c) ファブリックサイトの RLAN ポートを設定するには、[Fabric] トグルボタンを使用します。

このトグルは、デバイスがファブリックサイトにある場合にのみ使用できます。[ファブリック（Fabric）] トグルボタンを有効にする場合は、次の手順を実行します。

- [IP Address Pool] フィールドに、IP アドレスを入力します。
- （オプション）[スケーラブルグループタグ（Scalable Group Tag）] ドロップダウンリストから必要なオプションを選択します。

d) （任意） [RLANプロファイル（RLAN Profile）] タブで、[RLANプロファイル（RLAN Profile）] ドロップダウンリストから RLAN プロファイルを選択します。

RLAN プロファイルを作成するには、[新規作成（Create New）] をクリックし、次の手順を実行します。

1. [Create new RLAN Profile] ダイアログボックスの [RLAN Profile Name] フィールドに、RLAN プロファイルの名前を入力します。

   既存の RLAN プロファイルがある場合、そこから設定をコピーするには、[Copy Configuration from Existing RLAN Profile] チェックボックスをオンにします。[RLANプロファイル（RLAN Profile）] ドロップダウンリストから、既存の RLAN プロファイルを選択します。

2. [Save] をクリックします。

RLAN プロファイルを選択した場合は、次のタスクを実行します。

- RLAN プロファイルを有効または無効にするには、[Admin Status] トグルボタンを使用します。
- [Maximum End Points] フィールドに、エンドポイントの数を入力します。有効な範囲は 0 ～ 10000 です。

（注） このフィールドでは、RLAN ごとのクライアント接続数を設定します。0 は無制限のクライアント接続を示します。

- （オプション）[レイヤ2（Layer 2）] ドロップダウンリストから必要なオプション（[Dot1x] または [オープン（Open）]）を選択します
- （オプション）[レイヤ3（Layer 3）] ドロップダウンリストから必要なオプション（[オープン（Open）] または [内部Web認証（Internal Web Authentication）]）を選択します

- （オプション）[AAAサーバーグループの選択（Select a AAA Server Group）] ドロップダウンリストから、AAA サーバーグループを選択します。

  このドロップダウンには、プライマリコントローラでの WLAN プロビジョニングの一部として設定された AAA サーバーグループが一覧表示されます。AAA サーバーグループを選択しない場合、Catalyst Center では選択したセキュリティ設定の RLAN プロファイルでデフォルトの方式が設定されます。

  （注） このドロップダウンリストは、[Layer 2] が [Dot1x] であるか、[Layer 3] が [Internal Web Authentication] である場合にのみ使用できます。

- （オプション）MAC フィルタリングを有効にするには、[MAC Filtering] チェックボックスをオンにします。

- （オプション）[フォールバック認証（Fallback Authentication）] ドロップダウンリストから、必要なフォールバック認証（[なし（None）]、[MACフィルタリングの障害時はDot1x （Dot1x on MAC Filtering Failure）]、または [Dot1xの障害時はMACフィルタリング（MAC Filtering on Dot1x Failure）]）を選択します。

  （注） フォールバック認証は、[Layer 2] が [Dot1x] であり、MAC フィルタリングが有効になっている場合にのみ使用できます。

e) （任意）[RLANポリシー（RLAN Policy）] タブをクリックし、[RLANポリシー（RLAN Policy）] ドロップダウンリストから RLAN ポリシーを選択します。

RLAN ポリシーを作成するには、[新規作成（Create New）] をクリックし、次の手順を実行します。

1. [Create new RLAN Policy] ダイアログボックスの [RLAN Policy Name] フィールドに、RLAN ポリシーの名前を入力します。

   既存の RLAN ポリシーがある場合、そこから設定をコピーするには、[Copy Configuration from Existing RLAN Policy] チェックボックスをオンにします。[RLANポリシー（RLAN Policy）] ドロップダウンリストから、既存の RLAN ポリシーを選択します。

2. [Save] をクリックします。

RLAN ポリシーを選択した場合は、次のタスクを実行します。

- RLAN ポリシーを有効または無効にするには、[Admin Status] トグルボタンを使用します。

- [転送モード（Forwarding Mode）] ドロップダウンリストから、必要なオプション（[ローカルスイッチング（Local Switching）] または [中央スイッチング（Central Switching）]）を選択します

  ローカルスイッチングを選択した場合は、[VLAN] フィールドに VLAN 名を入力します。中央スイッチングを選択した場合は、[VLAN ID] フィールドに VLAN ID を入力します。VLAN ID の有効な範囲は 1 ～ 4096 です。

（注）
- Cisco Aironet 1815T アクセスポイントは、RLAN のローカルスイッチングをサポートしていません。他の AP モデルでは、AP がローカルモードの場合、Cisco IOS XE リリース 17.2 以降で RLAN のローカルスイッチングがサポートされています。
- [Fabric] トグルボタンを有効にすると、[Central Switching] オプションは使用できません。

- [Timeout Period (in seconds)] フィールドに、タイムアウト期間を秒単位で入力します。タイムアウトの有効範囲は 0 ～ 86400 です。
- Point over Ethernet（PoE）を有効または無効にするには、[PoE] トグルボタンを使用します。

（注） Catalyst Center は、PoE 対応ポートを備えた AP でのみ PoE を有効にします。

- （オプション）AAA オーバーライドを有効にするには、[AAA override] チェックボックスをオンにします。

f) [Review Impacted Sites] ダイアログボックスで、影響を受けるサイトの詳細を確認し、[Confirm] をクリックします。

ステップ 7 （任意） [Delete Unused RLAN Profiles and Policies] ウィンドウで、削除する未使用の RLAN プロファイルと RLAN ポリシーの横にあるチェックボックスをオンにします。

このウィンドウには、選択したワイヤレスコントローラの未使用の RLAN プロファイルと RLAN ポリシーが一覧表示されます。これらを削除すると、ワイヤレスコントローラのストレージが最適化されます。

ステップ 8 [Summary] ウィンドウで、設定を確認します。変更するには、[Edit] をクリックします。

ステップ 9 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 10 [Tasks] ウィンドウで、タスクの展開を監視します。

次のタスク

[Activities] > **[Tasks]** ウィンドウで RLAN 設定のステータスを表示できます。

セカンダリ ワイヤレスコントローラ をプロビジョニングした場合は、**[Provision]** > **[Inventory]** ウィンドウからセカンダリ ワイヤレスコントローラ を再プロビジョニングします。

ファブリックサイトでの Parallel Redundancy Protocol の設定

このワークフローは、Parallel Redundancy Protocol（PRP）チャネルの設定に役立ちます。PRP チャネルは、重要なネットワークシステムで高可用性とゼロパケット損失を実現するために使用されます。PRP 設定は、Cisco IOS XE リリース 17.16.x 以降を実行する Cisco Catalyst IE3400 および IE3400H 高耐久性シリーズ スイッチと互換性があります。

（注） Catalyst Center は、FIAB での PRP 設定をサポートしていません。

始める前に

- RedBox が LAN-B エッジデバイスに接続されていないことを確認します。これにより、ネットワークでループが発生し、ネットワークが輻輳する可能性があります。
- LAN-B エッジデバイスで既存の PRP 設定がクリアされていることを確認します。

手順

ステップ 1 メインメニューから次を選択します。、**[ワークフロー（Workflows）]** > **[PRPの設定（Configure PRP）]** の順に選択します。

または、ファブリック サイト トポロジ ビューに移動し、PRP を設定する拡張ノードを選択して、[PRP] タブの [PRPの有効化（Enable PRP）] をクリックします。

ステップ 2 タスクの概要ウィンドウが表示されたら、[実行する（Let's Do It）] をクリックして、ワークフローに直接移動します。

ステップ 3 [サイトの選択（Select a site）] ウィンドウで、PRP を設定する RedBox に関連付けられているファブリックサイトを選択します。

ステップ 4 [RedBoxデバイスの選択（Select a RedBox device）] ウィンドウで、RedBox デバイスを選択します。

ステップ 5 [PRPチャネルの設定（Configure PRP Channel）] ウィンドウで、冗長化を有効にするための、このスイッチのプライマリおよびセカンダリインターフェイスとして機能するインターフェイスペアを選択します。

ステップ 6 [高精度時間プロトコルの有効化（Enable Precision Time Protocol）] ウィンドウで、[次へ（Next）] をクリックします。

現時点では、高精度時間プロトコル（PTP）は設定できません。

ステップ 7 [VLANの設定（Configure VLAN）] ウィンドウで、スイッチポートと VLAN の設定を完了します。

- [スイッチポートモード（Switchport mode）] : [トランクモード（Trunk mode）] を選択します。
- [許可済みVLAN（Allowed VLANs）] : [すべて（All）] または [リスト（List）] オプションボタンをクリックします。[リスト（List）] オプションを選択した場合は、[許可済みVLAN（Allowed VLANs）] フィールドに VLAN を入力します。
- [監視フレームのタグ付け（Supervisory frame tagging）] : [監視フレームにタグを付ける（Tag Supervisory frames）] トグルボタンをクリックし、タグ付けタイプを設定します。
  - [単一のVLAN（Single VLAN）] : [VLAN ID] を入力します。
  - [VLAN対応（VLAN aware）] : VLAN を入力し、[タグなし監視フレームを拒否（Reject untagged supervisory frame）] トグルボタンをクリックして、ネットワークのセキュリティとセグメンテーションを強化します。

ステップ 8 [LANの設定（Configure LAN）] ウィンドウで、LAN-B の設定を完了します。

- [LAN-Bサイト（LAN-B site）] : ファブリックサイトを選択します。
- [LAN-Bスイッチ（LAN-B switch）] : リストされたエッジノードから、LAN-B デバイスとして使用するスイッチを選択します。
- [LAN-Bインターフェイス（LAN-B interface）] : 選択した LAN-B スイッチで使用するインターフェイスを選択します。

  ドロップダウンリストには、管理上ダウン状態のポートを含む PRP 設定に使用可能なインターフェイスが表示されます。ポートチャネルまたは PRP チャネルに参加しているポートは、ドロップダウンリストに表示されません。

ステップ 9 [概要（Summary）] ウィンドウで、PRP の設定を確認して確定します。

ステップ 10 [Deploy] をクリックします。

ステップ 11 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（238 ページ）を参照してください。

ステップ 12 [Tasks] ウィンドウで、タスクの展開を監視します。

次のタスク

RedBox インターフェイスを正しい LAN-B インターフェイスに接続します。

PRP 設定の削除

PRP 設定を変更する場合は、LAN-A エッジデバイスと LAN-B エッジデバイスから PRP 設定を削除して PRP 設定をやり直す必要があります。

始める前に

RedBox として設定されたデバイスをファブリックサイトから削除し、そのデバイスをインベントリから削除する必要があります。詳細については、ファブリックからデバイスを削除（1239 ページ）およびネットワークデバイスの削除 （218 ページ）を参照してください。

手順

ステップ 1 メインメニューから次を選択します。**[Provision]** > **[Fabric Sites]**。

ステップ 2 [SUMMARY] で、ファブリックサイトの数を示す数字をクリックします。

ステップ 3 PRP 設定を削除するファブリックサイトをクリックします。

ステップ 4 [ポートの割り当て（Port Assignment）] タブで、PRP 設定を削除する PRP LAN-A または PRP LAN-B ポートを選択します。

ステップ 5 [その他のアクション（More Actions）] にカーソルを合わせ、[PRPの削除（Delete PRP）] をクリックします。

ステップ 6 画面上のガイドラインに従って PRP 設定を削除します。

ステップ 7 [Deploy] をクリックします。

ステップ 8 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

ステップ 9 [Tasks] ウィンドウで、タスクの展開を監視します。

PRP チャネルの編集

PRP 設定で許可済み VLAN の詳細を変更します。

手順

ステップ 1 メインメニューから次を選択します。**[Provision]** > **[Fabric Sites]**。

ステップ 2 PRP チャネルを編集するファブリックサイトをクリックします。

ステップ 3 [ポート割り当て（Port Assignment）] タブをクリックし、RedBox として設定されたデバイスを選択します。

ステップ 4 [その他のアクション（More Actions）] にカーソルを合わせ、[PRPチャネルの編集（Edit PRP Channel）] をクリックします。

または、[インターフェイス（Interface）] 列の下にある [PRPチャネル（PRP-channel）] をクリックします。

ステップ 5 [PRPチャネルの編集（Edit PRP Channel）] スライドインペインで、必要に応じて許可済み VLAN の詳細を編集します。[Update] をクリックします。

ステップ 6 画面上のガイドラインに従って、PRP チャネルの設定を編集します。

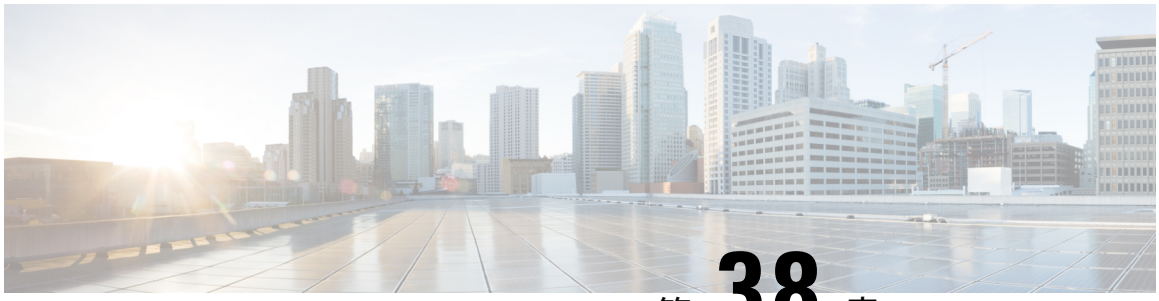
ステップ 7 [Deploy] をクリックします。

ステップ 8 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （238 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （238 ページ）を参照してください。

ステップ 9 [Tasks] ウィンドウで、タスクの展開を監視します。



第 38 章

ワイヤレスネットワークの設定の使用例

- ワイヤレスネットワーク設定のユースケース （1689 ページ）
- ワイヤレスコントローラ 管理ユースケース （1689 ページ）
- Wi-Fi 7 設定のユースケース （1693 ページ）
- 高可用性のユースケース （1696 ページ）
- ワイヤレスモビリティのユースケース （1699 ページ）
- AP 管理のユースケース （1707 ページ）
- Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのキャンパスネットワーク設定のユースケース （1716 ページ）

ワイヤレスネットワーク設定のユースケース

これらのユースケースを使用して、ワイヤレスネットワークの設定について学びます。

ワイヤレス自動化を使用した最適なネットワーク管理については、「*Leveraging Cisco Catalyst Center Wireless Automation for Optimal Network Management*」を参照してください。

ワイヤレスコントローラ 管理ユースケース

これらのトピックは、ワイヤレスネットワークの ワイヤレスコントローラ 管理ユースケースを理解するのに役立ちます。

WLAN プロファイルおよびポリシープロファイルの設定

Catalyst Center は複雑なサイト階層にまたがる SSID を管理する際に柔軟性とインテリジェンスを提供します。Catalyst Center では、設計インテントと特定のサイトコンテキストに基づいて、ネットワーク設定またはネットワークプロファイルから WLAN プロファイルとポリシープロファイル名が動的に選択されます。

SSID がグローバルサイトでオーバーライドなしで定義される

SSIDがサイト階層でのオーバーライドなしでグローバルサイトで定義されている場合、WLANプロファイルとポリシープロファイル名は、そのサイトのネットワークプロファイルに基づきます。

Catalyst Center は、同じ SSID が同じ WLAN プロファイルとポリシープロファイル名に関連付けられているが、複数のネットワークプロファイル間で異なる設定フレーバで設定されている場合、競合を自動的に検出します。たとえば、WLANプロファイルとポリシープロファイル名 `store_wifi_area1` を持つ SSID `Store_wifi` は、`Site1` に接続されるネットワークプロファイルではFlexとして定義され、`Site2`に接続されるネットワークプロファイルでは非Flexとして定義されているとします。`Site1` と `Site2` が同じ ワイヤレスコントローラ によって管理されている場合、競合設定となります。

競合を解決するには、各ネットワークプロファイルを更新して、WLAN プロファイルとポリシープロファイル名が一意になるようにします。たとえば、`Site2` のネットワークプロファイルを、`store_wifi_area1_site2` の WLAN プロファイルとポリシープロファイル名で更新します。

子サイトで SSID がオーバーライドされる

SSID が子サイトでオーバーライドされると、Catalyst Center は次の条件に基づいて、ネットワーク設定またはネットワークプロファイルに基づいて WLAN プロファイルとポリシープロファイル名を決定します。

プロファイル名の選択	基準
ネットワーク設定から	• ネットワークプロファイル内のWLANプロファイルおよびポリシープロファイル名は、グローバルネットワーク設定での名前と同じです。 • オーバーライドされたサイトの下のすべてのネットワークプロファイルで、同じWLANプロファイルまたはポリシープロファイル名が使用されます。
ネットワークプロファイルから	複数のネットワークプロファイルが存在し、それぞれに一意の WLAN プロファイルとポリシープロファイル名があります。

Catalyst Center は、同じ SSID と WLAN プロファイルまたはポリシープロファイル名が、複数のネットワークプロファイルで異なる設定で使用されている場合、競合を自動的に検出します。

たとえば、ワイヤレスコントローラ はSSID `store_wifi` と次の階層を持つネットワークを管理します。

- Area 1
  - Site1 (`store_wifi_area1`)
    - Building-01
      - Floor1

- Floor2

- Site2 (store_wifi_area1)
  - Building-02
    - Floor1
    - Floor2

次の表に、競合の設定例と解決策を示します。

例	対処法
WLAN プロファイルまたはポリシープロファイル名は store_wifi_profile です。SSID は次のように定義されています。 • Network Profile-1 に関連付けられている Site1 の Flex 設定 • Network Profile-2 に関連付けられている Site2 の非 Flex 設定 ワイヤレスコントローラ は、両方のサイトを管理するため競合を検出します。	各ネットワークプロファイルを更新して、一意の WLAN またはポリシープロファイル名を使用します（例：Site2 には store_wifi_area1_site2）。
ワイヤレスコントローラ は、（フロアごとに 1 つの）2 つのネットワークプロファイルを使用して、階層のビルディングのみを管理します。 • WLAN プロファイルとポリシープロファイル名 store_wifi_area1_np1 を使用する各ビルディングの 1 階の Network Profile-1。 • WLAN プロファイルとポリシープロファイル名 store_wifi_area1_np2 を使用する各ビルディングの 2 階の Network Profile-2。 オーバーライドは、同じ WLAN プロファイルとポリシープロファイル名 store_wifi_area1 を持つ 2 つのサイトで設定されます。 Catalyst Center は、各オーバーライドサイト（Site1 と Site2）の下の Network Profile-1 と Network Profile-2 で詳細レベルのプロファイル名を見つけます。 Site1 と Site2 で、SSID が同じ WLAN プロファイルとポリシープロファイル名 store_wifi_area1_np1 を使用して異なる設定でオーバーライドされているため、ワイヤレスコントローラ は競合を検出します。	• ネットワーク プロファイル レベルで設定の違いがない場合、すべての管理対象フロアに単一のネットワークプロファイルを使用します。 • エリアレベルのネットワーク設定で共通の設定を適用します。 • 一意の WLAN プロファイルとポリシープロファイル名を使用して、各フロアのネットワークプロファイルを作成します。

WLAN プロファイルまたはポリシープロファイル名の変更

ワイヤレスコントローラ がインテント変更なしで再プロビジョニングされると、Catalyst Center は移行された SSID を自動的に検出します。Catalyst Center は、次の条件に基づいて WLAN プロファイルとポリシープロファイル名を再利用します。

- サイトレベルのオーバーライドは移行前と同じです。
- ネットワークプロファイルまたはネットワーク設定で、WLAN プロファイルまたはポリシープロファイル名は移行前と同じです。

これらの条件は、リリース 2.3.7.7 で作成され、WLAN プロファイルまたはポリシープロファイル名の変更によって再プロビジョニングされた移行対象外の SSID にも適用されます。

サイト階層（**[ネットワーク設定（Network Settings）] > [ワイヤレス（Wireless）] > [SSID]**）かネットワークプロファイルのいずれかで SSID の WLAN プロファイル名やポリシープロファイル名を変更してから、ワイヤレスコントローラ を再プロビジョニングする場合、その SSID が、ネットワークプロファイルまたはネットワーク設定で定義された名前といずれかに一致する WLAN プロファイル名またはポリシープロファイル名を使用して、同じサイトの ワイヤレスコントローラ にすでにプロビジョニングされていると、Catalyst Center はプロビジョニングされた WLAN プロファイル名またはポリシープロファイル名をサイトに再利用しようとします。Catalyst Center は、更新されたプロファイル名を無視し、既存のプロファイル名を引き続き使用します。

たとえば、ワイヤレスコントローラ は、WLAN プロファイルまたはポリシープロファイル名 `store_wifi_profile` を使用して、グローバルレベルで作成された SSID `store_wifi` を持つネットワークを管理します。グローバルの下のネットワーク階層は次のとおりです:

- Area 1
  - Site1
    - Building-01
      - Floor1
      - Floor2
  - Site2
    - Building-02
      - Floor1
      - Floor2

- 例 1：
  - ネットワークプロファイル `Network Profile-1` は、WLAN プロファイルまたはポリシープロファイル名 `store_wifi_area1_np1` とともに `Site1/Building-01` のすべてのフロアに割り当てられます。
  - ネットワークプロファイル `Network Profile-2` は、WLAN プロファイルまたはポリシープロファイル名 `store_wifi_area1_np2` とともに `Site2/Building-02` のすべてのフロアに割り当てられます。

ワイヤレスコントローラ をプロビジョニングすると、WLAN プロファイルとポリシープロファイル store_wifi_area1_np1 および store_wifi_area1_np2 が ワイヤレスコントローラ に作成されます。

Network Profile-1 を使用するサイトに新しい WLAN プロファイルまたはポリシープロファイル名（たとえば store_wifi_area1_np1_1）を使用するには、Network Profile-1 でプロファイル名を更新してから、ワイヤレスコントローラを再プロビジョニングできます。新しいプロファイル名が使用されます。同様に、Network Profile-2 のプロファイル名を store_wifi_area1_np2_1 に変更し、ワイヤレスコントローラ を再プロビジョニングすると、更新されたプロファイル名が使用されます。

- 例 2：WLAN プロファイル名およびポリシープロファイル名として store_wifi_profile を持つ単一のネットワークプロファイル Network Profile-1 が、すべてのフロアに使用されます。

  すべてのフロアを管理する ワイヤレスコントローラ をプロビジョニングすると、WLAN プロファイルとポリシープロファイル store_wifi_profile がすべてのフロアに適用されます。

  ワイヤレスコントローラ で使用される WLAN プロファイルまたはポリシープロファイル名を更新するには、新しいプロファイル名が正しく適用されるように、Network Profile-1 の名前とグローバルネットワーク設定の SSID 設定を更新する必要があります。

Wi-Fi 7 設定のユースケース

このセクションは、ワイヤレスネットワークの Wi-Fi 7 設定のユースケースを理解するのに役立ちます。

Wi-Fi 7 設定の有効化

Catalyst Center で Wi-Fi 7 設定を有効にするには、次の手順を使用します。

始める前に

- **[Provision]** > **[Inventory]** ウィンドウで、Wi-Fi 7 AP が使用可能であることを確認します。

  Wi-Fi 7 AP には次のものが含まれます。

  - Cisco IOS XE リリース 17.18 以降を実行している Cisco Wireless 9171I シリーズ アクセスポイント、
  - Cisco Catalyst 9172H シリーズ アクセスポイント、
  - Cisco Catalyst 9172I シリーズ アクセスポイント、
  - Cisco IOS XE リリース 17.17.1 以降を実行している Cisco Catalyst 9176D1 シリーズ アクセスポイント、

- Cisco IOS XE リリース 17.17.1 以降を実行している Cisco Catalyst 9176I シリーズ アクセスポイント、および
- Cisco Catalyst 9178I シリーズ アクセスポイント。

- デバイスは、Cisco IOS XE リリース 17.15.2 以降を実行している必要があります。
- Wi-Fi 7 AP は CNS ライセンスを使用します。ライセンス要件を満たしていない AP は、ワールドワイドセーフモード（WWSM）で動作します。

  WWSM を無効にしてライセンス要件を満たするには、[License Manager] ウィンドウで CNS ライセンスを有効にします。詳細については、『*Cisco Catalyst Center Administrator Guide*』の「Manage Licenses」を参照してください。

手順

ステップ 1 **[Dot11be Status Configuration]** 機能テンプレートで、2.4 GHz、5 GHz、および 6 GHz 無線帯域の 802.11be ステータスを有効にします。

既存のデフォルトプロファイルを使用することも、無線帯域ごとにカスタムプロファイルを作成することもできます。詳細については、Dot 11be ステータス設定用の機能テンプレートの作成（618 ページ）を参照してください。

ステップ 2 必要な設定で RF プロファイルを作成し、必要な Wi-Fi 7 設定を行います。

- 5 GHz および 6 GHz 無線帯域の **[Preamble Puncturing]** トグルボタンを使用して、プリアンブル パンクチャリングを有効にします。
- **[DBS Channel Width]** スライダを使用して、6 GHz 無線帯域の最大チャネル幅を 320 MHz に設定します。
- 対応するチェックボックスをオンにして、6 GHz 無線帯域の 802.11be パラメータを有効にします。
  - ダウンリンク OFDMA
  - アップリンク OFDMA
  - ダウンリンク MU-MIMO
  - アップリンク MU-MIMO
  - OFDMA Multi-RU

（注） Cisco IOS XE リリース 17.18.2 以降、OFDMA アップリンク、OFDMA ダウンリンク、MU-MIMO アップリンク、および MU-MIMO ダウンリンクの設定は廃止され、[802.11BEパラメータ（802.11BE PARAMETERS）] では無視されます。これらの設定を構成するには、[802.11AX PARAMETERS] セクションを使用します。

詳細については、ワイヤレス無線周波数プロファイルの作成 （451 ページ）を参照してください。

ステップ 3 802.11be プロファイルを作成します。

- 2.4 GHz および 5 GHz 無線帯域用の 802.11be 設定を設定します。

（注） この 802.11be プロファイルは WLAN にマッピングされ、2.4 GHz および 5 GHz 帯域にのみ適用されます。6 GHz 無線帯域の場合、802.11be 設定は、RF プロファイルの対応する設定から使用されます。

- すべての無線帯域の MLO グループ設定を設定します。

詳細については、802.11be プロファイルの作成 （527 ページ）を参照してください。

ステップ 4 関連付けられたワイヤレス ネットワーク プロファイルで、次の手順を実行します。

- 802.11beプロファイルを、ネットワークプロファイルの対応するSSIDに関連付ける（詳細については「ネットワークプロファイルへの SSID の追加 （544 ページ）」を参照）、および
- ネットワークプロファイルに [Dot11beステータスの設定（Dot11be Status Configuration）] 機能テンプレートを追加する（詳細については、「ネットワークプロファイルへの機能テンプレートの追加 （549 ページ）」を参照してください）。

ステップ 5 （任意） 対応する SSID で、**[AP Beacon Protection]** チェックボックスをオンにして AP ビーコン保護を有効にします。

詳細については、エンタープライズ ワイヤレス ネットワーク用 SSID の作成 （415 ページ）およびゲスト ワイヤレス ネットワークの SSID の作成 （432 ページ）を参照してください。

ステップ 6 Wi-Fi 7 AP を設定します。

詳細については、AP の設定 （1639 ページ）を参照してください。

ステップ 7 関連付けられたネットワークプロファイルを使用して Wi-Fi 7 AP をプロビジョニングします。

詳細については、Day 1 の Cisco AP プロビジョニング （745 ページ）を参照してください。

高可用性のユースケース

次のトピックは、ワイヤレスネットワークの高可用性（HA）のユースケースを理解するために役立ちます。

シスコ ワイヤレス コントローラ HA の設定

シスコ ワイヤレス コントローラ HA を使用すると、ワイヤレスコントローラをプライマリ ワイヤレスコントローラのバックアップとして使用できます。アクティブ ワイヤレスコントローラは、すべてのAP、クライアントトラフィックを処理し、APおよびクライアントデータベースをスタンバイ ワイヤレスコントローラ と共有します。フェールオーバーが発生すると、スタンバイ ワイヤレスコントローラ がすぐに動作を引き継ぐため、クライアントサービスのダウンタイムがゼロになり、SSID の停止が回避されます。

始める前に

- 両方のワイヤレスコントローラが同じフォームファクタであることを確認します。
- 両方のワイヤレスコントローラが同じソフトウェアバージョンを実行していることを確認します。
- ワイヤレスコントローラ HA は、80 ミリ秒のラウンドトリップ時間（RTT）の最大冗長ポートリンク遅延、60 Mbps の最小帯域幅、および 1500 の最小最大伝送ユニット（MTU）をサポートしています。
- 両方のワイヤレスコントローラの冗長ポートが物理的に、またはレイヤ 2 仮想ネットワークを介して、接続されていることを確認します。レイヤ 2 仮想ネットワークを介して冗長ポートを接続する場合は、リンク遅延、帯域幅、および MTU の要件が満たされていることを確認します。
- ESXi、KVM、および Hyper-V で動作している Cisco Catalyst 9800-CL ワイヤレスコントローラの場合は、冗長ポートが同じ仮想スイッチに接続されていることを確認します。

手順

ステップ 1 インベントリにワイヤレスコントローラがあることを確認します。詳細については、インベントリについて （100 ページ）およびネットワークデバイスの追加 （157 ページ）を参照してください。

ワイヤレスコントローラがインベントリにない場合は、検出機能を使用して検出します。詳細については、ネットワークの検出 （73 ページ）を参照してください。

ステップ 2 両方のワイヤレスコントローラがインベントリで「管理対象」（Managed）状態であることを確認します。詳細については、インベントリに関する情報の表示 （102 ページ）を参照してください。

ステップ 3 **show redundancy** コマンドを使用して、両方のワイヤレスコントローラで動作冗長モードが「非冗長」（Non-redundant）であることを確認します。

ステップ 4 メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。

ステップ 5 必要なワイヤレスコントローラの横にあるチェックボックスをオンにして、**[Actions]** > **[Provision]** > **[Configure WLC HA]**の順にクリックします。

ステップ 6 [Redundancy Management IP] と [Peer Redundancy Management IP] にそれぞれ冗長性管理 IP アドレスとピア冗長性管理 IP アドレスを入力します。

冗長性管理 IP およびピア冗長性管理 IP に使用される IP アドレスは、ワイヤレスコントローラ の管理インターフェイスと同じサブネットに設定する必要があります。これらの IP アドレスがこのサブネット範囲内で未使用の IP アドレスであることを確認します。

ステップ 7 **ネットマスク**を入力します。

ステップ 8 [Select Secondary WLC] ドロップダウンリストから、セカンダリワイヤレスコントローラを選択します。

ステップ 9 Cisco Catalyst 9800-CL ワイヤレスコントローラには専用の冗長ポートがないため、冗長ポートに使用するインターフェイスを選択します。

（注） アプライアンスベースの Cisco Catalyst 9800 シリーズ ワイヤレス コントローラには専用の冗長ポートがあるため、これらのデバイスの場合は、冗長ポートインターフェイスを選択する必要はありません。

ステップ 10 [Configure HA] をクリックします。

次のタスク

HA のステータスを確認するには、**show redundancy** コマンドを使用します。次に、コマンドの出力例を示します。

```
  cat_9800-1 #show redundancy
Redundant System Information :
------------------------------
       Available system uptime = 5 minutes
Switchovers system experienced = 0
                Standby failures = 0
       Last switchover reason = none

                 Hardware Mode = Duplex
    Configured Redundancy Mode = sso
     Operating Redundancy Mode = sso
              Maintenance Mode = Disabled
                Communications = Up

Current Processor Information :
-------------------------------
              Active Location = slot 1
       Current Software state = ACTIVE
      Uptime in current state = 5 minutes
                Image Version = Cisco IOS Software [Bengaluru], C9800-CL Software (C9800-CL-K9_IOSXE), Version 17.6.3, RELEASE SOFTWARE (fc4)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2022 by Cisco Systems, Inc.
Compiled Wed [redacted] 23:13 by [redacted]
       Configuration register = 0x2102
                Recovery mode  = Not Applicable

Peer Processor Information :
----------------------------
              Standby Location = slot 2
       Current Software state = STANDBY HOT
      Uptime in current state = 3 minutes
                Image Version = Cisco IOS Software [Bengaluru], C9800-CL Software (C9800-CL-K9_IOSXE), Version 17.6.3, RELEASE SOFTWARE (fc4)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2022 by Cisco Systems, Inc.
Compiled Wed [redacted] 23:13 by [redacted]
                        BOOT =
                  CONFIG_FILE =
       Configuration register = 0x2102
```

プライマリ ワイヤレスコントローラの**優先順位**を確認するには、**show chassis** コマンドを使用します。プライマリ ワイヤレスコントローラの**優先順位**が 2 に変更され、そのロールが**アクティブ**である状態が確保されます。次に、コマンドの出力例を示します。

```
  cat_9800-1 #show chassis
Chassis/Stack Mac Address : 000c.2972.9b46 - Local Mac Address
Mac persistency wait time: Indefinite
                                          H/W   Current
Chassis#   Role    Mac Address     Priority Version  State                 IP
-----------------------------------------------------------------------------
*1       Active   000c.2972.9b46     2      V02     Ready               172.16.0.2
 2       Standby  0050.56ae.a54f     1      V02     Ready               172.16.0.3
```

シスコ ワイヤレス コントローラ N+1 HA の設定

シスコ ワイヤレス コントローラ N+1 HA では、ワイヤレスコントローラ を複数のプライマリ ワイヤレスコントローラ のバックアップとして使用できます。Catalyst Center は、N+1 HA のステートフル スイッチオーバーをサポートしておらず、各 ワイヤレスコントローラ を個別に管理する必要があります。

（注）

- Catalyst Center は、プライマリおよびセカンダリ ワイヤレスコントローラ の N+1 HA 設定をサポートしています。Catalyst Center は、ターシャリ ワイヤレスコントローラ 設定をサポートしていません。
- プライマリ ワイヤレスコントローラ 設定を編集する場合は、更新された設定を使用してセカンダリ ワイヤレスコントローラ を手動で再プロビジョニングします。

手順

ステップ 1 インベントリにワイヤレスコントローラがあることを確認します。詳細については、インベントリについて （100 ページ）およびネットワークデバイスの追加 （157 ページ）を参照してください。

ワイヤレスコントローラがインベントリにない場合は、検出機能を使用して検出します。詳細については、ネットワークの検出 （73 ページ）を参照してください。

ステップ 2 両方のワイヤレスコントローラがインベントリで「管理対象」（Managed）状態であることを確認します。詳細については、インベントリに関する情報の表示 （102 ページ）を参照してください。

ステップ 3 エンタープライズおよびゲストワイヤレス SSID を作成します。詳細については、エンタープライズ ワイヤレス ネットワーク用 SSID の作成 （415 ページ）およびゲスト ワイヤレス ネットワークの SSID の作成 （432 ページ）を参照してください。

ステップ 4 SSID の作成時にワイヤレス ネットワーク プロファイルを作成した場合は、それをプライマリ ワイヤレスコントローラ管理対象サイトに割り当てます。メインメニューから次を選択します。**[Design]** > **[Network**

Profiles]の順に選択し、ワイヤレス ネットワーク プロファイルに対応する [Assign Site] オプションをクリックします。

ステップ 5 プライマリ ワイヤレスコントローラをプロビジョニングします。ロールとして [Active Main WLC] を選択します。詳細については、Cisco AireOS コントローラのプロビジョニング （738 ページ）およびCisco Catalyst 9800 シリーズ ワイヤレス コントローラ のプロビジョニング （782 ページ）を参照してください。

ステップ 6 セカンダリ ワイヤレスコントローラをプロビジョニングします。ロールとして [Active Main WLC] を選択し、セカンダリ ワイヤレス コントローラの管理対象 AP の場所（プライマリ ワイヤレスコントローラの管理対象 AP の場所と同じもの）を選択します。詳細については、Cisco AireOS コントローラのプロビジョニング （738 ページ）およびCisco Catalyst 9800 シリーズ ワイヤレス コントローラ のプロビジョニング （782 ページ）を参照してください。

ステップ 7 AP をプロビジョニングします。詳細については、Day 1 の Cisco AP プロビジョニング （745 ページ）を参照してください。

ワイヤレスモビリティのユースケース

次のトピックは、ワイヤレスネットワークのモビリティ設定のユースケースを理解するのに役立ちます。

ワイヤレスモビリティの設定

Catalyst Center でのモビリティ設定により、ネットワーク内の シスコ ワイヤレス コントローラ間にトンネルを確立して、相互に通信させ、動的に情報を共有させることができます。モビリティトンネルにより、ワイヤレスネットワーク内のクライアントのシームレスなローミングが可能になります。この手順では、次のユースケースでワイヤレスコントローラ間にモビリティトンネルを設定する手順について説明します。

- 同じモビリティグループを持つ新たに追加された 2 つのワイヤレスコントローラ：2 つのワイヤレスコントローラは Catalyst Center に新たに追加されていて、まだプロビジョニングされていません。
- 同じモビリティグループを持つ既存の 2 つのワイヤレスコントローラ：ワイヤレスコントローラはすでに Catalyst Center に追加されてプロビジョニングされており、同じモビリティグループ名を持っています。
- 異なるモビリティグループを持つ既存の 2 つのワイヤレスコントローラ：ワイヤレスコントローラはすでに Catalyst Center に追加されてプロビジョニングされており、異なるモビリティグループ名を持っています。
- 2 つの既存のワイヤレスコントローラと 3 つ目のワイヤレスコントローラ：2 つのワイヤレスコントローラの間にある既存のモビリティグループに新しいワイヤレスコントローラが追加されます。

始める前に

- インベントリにシスコ ワイヤレス コントローラがあり、それらが「管理対象」（Managed）状態であることを確認します。詳細については、インベントリについて（100ページ）およびインベントリに関する情報の表示（102 ページ）を参照してください。
- ワイヤレスモビリティ設定の詳細については、モビリティ設定の概要（772ページ）を参照してください。

手順

ステップ 1 同じモビリティグループを持つ新たに追加されたワイヤレスコントローラの場合は、次の手順を実行します。

a) **show wireless mobility summary** コマンドを実行して、コントローラ間に既存のモビリティトンネルがないことを確認します。
b) いずれかのワイヤレスコントローラを選択して、モビリティグループを設定し、もう一方のワイヤレスコントローラをピアとして追加します。詳細については、モビリティグループの設定（774ページ）を参照してください。
c) プロビジョニングする前に設定を確認します。
d) ワイヤレスコントローラをプロビジョニングします。

（注） 2 つ目のワイヤレスコントローラをプロビジョニングする必要はありません。最初のワイヤレスコントローラのピアとして追加すると、同じモビリティグループ名とピア設定で自動的にプロビジョニングされます。

ステップ 2 同じモビリティグループを持つ 2 つの既存ワイヤレスコントローラの場合は、次の手順を実行します。

a) ワイヤレスコントローラに同じモビリティグループ名が設定されていることを確認します。詳細については、インベントリについて（100ページ）およびインベントリに関する情報の表示（102 ページ）を参照してください。
b) いずれかのワイヤレスコントローラを選択して、モビリティグループを設定し、もう一方のワイヤレスコントローラをピアとして追加します。詳細については、モビリティグループの設定（774ページ）を参照してください。
c) プロビジョニングする前に設定を確認します。
d) ワイヤレスコントローラをプロビジョニングします。

（注） 2 つ目のワイヤレスコントローラをプロビジョニングする必要はありません。最初のワイヤレスコントローラのピアとして追加すると、同じモビリティグループ名とピア設定で自動的にプロビジョニングされます。

ステップ 3 モビリティグループが異なる 2 つの既存ワイヤレスコントローラの場合は、次の手順を実行します。

a) ワイヤレスコントローラにモビリティグループ名が設定されていることを確認します。詳細については、インベントリについて（100 ページ）およびインベントリに関する情報の表示（102 ページ）を参照してください。

b) いずれかのワイヤレスコントローラを選択して、モビリティグループを設定し、もう一方のワイヤレスコントローラをピアとして追加します。詳細については、モビリティグループの設定（774 ページ）を参照してください。

c) プロビジョニングする前に設定を確認します。

d) ワイヤレスコントローラをプロビジョニングします。

（注） 2 つ目のワイヤレスコントローラをプロビジョニングする必要はありません。最初のワイヤレスコントローラのピアとして追加すると、同じモビリティグループ名とピア設定で自動的にプロビジョニングされます。

ステップ 4 2 つのワイヤレスコントローラの間にある既存のモビリティグループに新しいワイヤレスコントローラを追加する場合は、次の手順を実行します。

a) [Mobility] タブでモビリティグループ名とモビリティピア情報を調べることにより、既存のワイヤレスコントローラの間にモビリティトンネルが確立されていることを確認します。詳細については、インベントリについて（100 ページ）およびインベントリに関する情報の表示（102 ページ）を参照してください。

b) 新たに追加されたワイヤレスコントローラを選択して、モビリティグループを設定し、他の 2 つの既存ワイヤレスコントローラをピアとして追加します。詳細については、モビリティグループの設定（774 ページ）を参照してください。

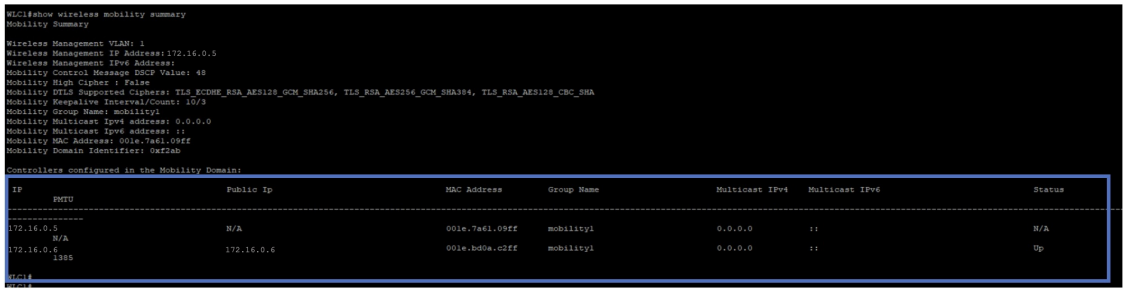
c) プロビジョニングする前に設定を確認します。

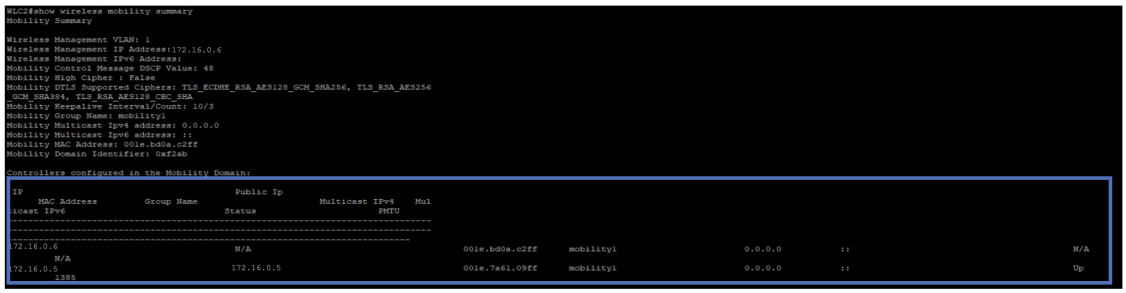
d) ワイヤレスコントローラをプロビジョニングします。

（注） 既存の 2 つのワイヤレスコントローラをプロビジョニングする必要はありません。新たに追加されたワイヤレスコントローラのピアとして追加すると、同じモビリティグループ名とピア設定で自動的にプロビジョニングされます。

次のタスク

プロビジョニング後に、各コントローラで **show wireless mobility summary** コマンドを実行して、モビリティトンネルのステータスを確認します。次に、コマンドの出力例を示します。





アンカーおよび外部ワイヤレスモビリティの設定

Catalyst Center でのアンカーおよび外部ワイヤレス設定により、異なるワイヤレスネットワーク上の シスコ ワイヤレス コントローラ間でワイヤレスモビリティを確立できます。アンカーおよび外部セットアップでは、外部ワイヤレスコントローラは、モビリティトンネル内のクライアント L3 トラフィックをカプセル化し、アンカー ワイヤレスコントローラに転送します。アンカーワイヤレスコントローラは、トンネルのカプセル化を解除し、クライアントトラフィックを切り替えます。ここでは、次のユースケースでアンカー/外部ワイヤレスモビリティを設定する手順について説明します。

- 新しく追加された 2 つのワイヤレスコントローラを設定します。1 つのアンカー ワイヤレス コントローラと 1 つの外部ワイヤレスコントローラです。
- 新しく追加された 3 つのワイヤレスコントローラを設定します。1 つのアンカー ワイヤレス コントローラと 2 つの外部ワイヤレスコントローラです。
- 新しく追加された 3 つのワイヤレスコントローラを設定します。1 つの外部ワイヤレスコントローラと 2 つのアンカー ワイヤレス コントローラです。
- アンカー/外部セットアップを削除します。

始める前に

- インベントリにシスコ ワイヤレス コントローラがあり、それらが「管理対象」（Managed）状態であることを確認します。詳細については、インベントリについて （100 ページ）およびインベントリに関する情報の表示 （102 ページ）を参照してください。
- **show wireless mobility summary** コマンドを使用して、ワイヤレスコントローラ間に既存のモビリティトンネルがないことを確認します。

手順

ステップ 1 ワイヤレスネットワークの SSID を作成し、新しいワイヤレス ネットワーク プロファイルに関連付けます。詳細については、エンタープライズ ワイヤレス ネットワーク用 SSID の作成 （415 ページ）またはゲスト ワイヤレス ネットワークの SSID の作成 （432 ページ）を参照してください。

[プロファイルへのSSIDの関連付け（Associate SSID to Profile）] ステップで、[プロファイルの追加（Add Profile）] オプションを選択して次のように設定します。

- [Profile Name]：プロファイルの名前を入力します。
- [Fabric]：[No] を選択します。
- [Do you need Anchor for this SSID?]：[Yes] を選択します。

ステップ 2 1 つのアンカー ワイヤレス コントローラと 1 つの外部ワイヤレスコントローラのシナリオでは、次の手順を実行します。

a) 新しく作成したワイヤレスプロファイルを、外部ワイヤレスコントローラによって管理されるサイトに割り当てます。

サイトを割り当てるには、次の手順を実行します。

- メインメニューから次を選択します。**[Design]** > **[Network Profiles]**の順に選択します。
- プロファイルを選択し、[Assign Site] をクリックします。サイトの作成については、サイトの作成、編集、削除 （285 ページ）を参照してください。

b) アンカー ワイヤレスコントローラをプロビジョニングします。

- ワイヤレスコントローラのロールとして [Anchor WLC] を選択し、[Managed AP location(s)] でアンカーの管理対象 AP の場所を選択します。
- インターフェイスの詳細を設定します。
- 必要に応じて、その他の詳細設定を指定し、展開します。

ワイヤレスコントローラのプロビジョニングの詳細については、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のプロビジョニング （782 ページ）またはCisco AireOS コントローラのプロビジョニング （738 ページ）を参照してください。

c) 外部ワイヤレスコントローラをプロビジョニングします。

- ワイヤレスコントローラのロールとして [Active Main WLC] を選択し、[Managed AP location(s)] で管理対象 AP の場所を選択します。
- 必要に応じて、その他の詳細設定を指定し、展開します。

ワイヤレスコントローラのプロビジョニングの詳細については、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のプロビジョニング （782 ページ）またはCisco AireOS コントローラのプロビジョニング （738 ページ）を参照してください。

d) ワイヤレスコントローラの下に AP をプロビジョニングします。

AP に正しい SSID があることを確認します。AP のプロビジョニングの詳細については、Day 1 の Cisco AP プロビジョニング （745 ページ）を参照してください。

ステップ 3 1 つのアンカー ワイヤレス コントローラと 2 つの外部ワイヤレスコントローラのシナリオでは、次の手順を実行します。

a) 新しく作成したワイヤレスプロファイルを、外部ワイヤレスコントローラによって管理されるサイトに割り当てます。

- メインメニューから次を選択します。**[Design]** > **[Network Profiles]**の順に選択します。
- プロファイルを選択し、[Assign Site] をクリックします。サイトの作成については、サイトの作成、編集、削除 （285 ページ）を参照してください。

b) アンカー ワイヤレスコントローラをプロビジョニングします。

- ワイヤレスコントローラのロールとして [Anchor WLC] を選択し、[Managed AP location(s)] で管理対象 AP の場所（両方の外部サイト）を選択します。
- インターフェイスの詳細を設定します。
- 必要に応じて、その他の詳細設定を指定し、展開します。

ワイヤレスコントローラのプロビジョニングの詳細については、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のプロビジョニング （782 ページ）またはCisco AireOS コントローラのプロビジョニング （738 ページ）を参照してください。

c) 外部ワイヤレスコントローラをプロビジョニングします。

- ワイヤレスコントローラのロールとして [Active Main WLC] を選択し、[Managed AP location(s)] で管理対象 AP の場所を選択します。
- 必要に応じて、その他の詳細設定を指定し、展開します。

ワイヤレスコントローラのプロビジョニングの詳細については、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のプロビジョニング （782 ページ）またはCisco AireOS コントローラのプロビジョニング （738 ページ）を参照してください。

d) ワイヤレスコントローラの下に AP をプロビジョニングします。

AP に正しい SSID があることを確認します。AP のプロビジョニングの詳細については、Day 1 の Cisco AP プロビジョニング （745 ページ）を参照してください。

ステップ 4 1 つの外部ワイヤレスコントローラと 2 つのアンカー ワイヤレス コントローラのシナリオでは、次の手順を実行します。

a) 新しく作成したワイヤレスプロファイルを、両方のワイヤレスコントローラ（外部とアンカー）によって管理されるサイトに割り当てます。

- メインメニューから次を選択します。**[Design]** > **[Network Profiles]**の順に選択します。

- プロファイルを選択し、[Assign Site] をクリックします。サイトの作成については、サイトの作成、編集、削除 （285 ページ）を参照してください。

b) 外部ワイヤレスコントローラをプロビジョニングします。

- ワイヤレスコントローラのロールとして [Active Main WLC] を選択し、[Managed AP location(s)] で管理対象 AP の場所（外部サイトとアンカーサイトの両方）を選択します。
- 必要に応じて、その他の詳細設定を指定し、展開します。

ワイヤレスコントローラのプロビジョニングの詳細については、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のプロビジョニング （782 ページ）またはCisco AireOS コントローラのプロビジョニング （738 ページ）を参照してください。

c) アンカー ワイヤレスコントローラをプロビジョニングします。

- ワイヤレスコントローラのロールとして [Anchor WLC] を選択し、[Managed AP location(s)] で管理対象 AP の場所を選択します。
- インターフェイスの詳細を設定します。
- 必要に応じて、その他の詳細設定を指定し、展開します。

ワイヤレスコントローラのプロビジョニングの詳細については、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のプロビジョニング （782 ページ）またはCisco AireOS コントローラのプロビジョニング （738 ページ）を参照してください。

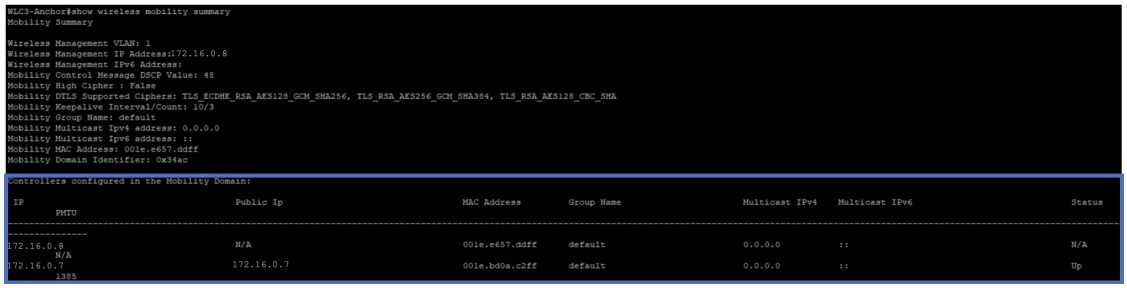
d) ワイヤレスコントローラの下に AP をプロビジョニングします。

AP に正しい SSID があることを確認します。AP のプロビジョニングの詳細については、Day 1 の Cisco AP プロビジョニング （745 ページ）を参照してください。

次のタスク

プロビジョニング後、Catalyst Center は、アンカー ワイヤレス コントローラと外部ワイヤレス コントローラの間にモビリティトンネルを自動的に作成します。モビリティトンネルのステータスを確認するには、各コントローラで **show wireless mobility summary** コマンドを使用します。次に、コマンドの出力例を示します。





ワイヤレスコントローラで次のモビリティ設定を確認します。

- 両方のワイヤレスコントローラに同じ WLAN およびポリシープロファイルがある。
- 外部ワイヤレスコントローラでポリシータグが作成され、AP にマッピングされている。
- アンカー ワイヤレスコントローラ用に VLAN インターフェイスが作成され、ポリシープロファイルにマッピングされている。

アンカー/外部セットアップの削除

アンカーおよび外部セットアップを削除するには、次の手順を実行します。

1. アンカー ワイヤレス コントローラと外部ワイヤレスコントローラの間のモビリティトンネルが「稼働」（up）状態であることを確認します。
2. ワイヤレスネットワーク用に作成された SSID を削除します。
   1. メインメニューから次を選択します。**[Design]** > **[Network Settings]** の順に選択します。
   2. [Wireless] タブをクリックします。
   3. 左側の階層ツリーから、[Global] を選択します。
   4. [SSID] テーブルで SSID を選択し、[Delete] をクリックします。
3. 外部ワイヤレスコントローラをプロビジョニングします。

   プロビジョニングの [Summary] ウィンドウで、SSID の詳細が削除されていることを確認します。

   プロビジョニング後、Catalyst Center がアンカー ワイヤレス コントローラと外部ワイヤレスコントローラの間のモビリティトンネルを自動的に削除し、WLANおよびポリシープロファイルがすべてのワイヤレスコントローラで削除されます。

AP 管理のユースケース

次のトピックは、ワイヤレスネットワークの AP 管理のユースケースを理解するために役立ちます。

AP の設定

Catalyst Center の AP に対して次のタスクを実行できます。

- AP の AP レベルのパラメータと無線レベルのパラメータを設定します。
- AP の定期的なイベントをスケジュールします。
- 既存のテンプレートを使用して AP を設定します。

詳細については、Catalyst Center での AP 設定 （1638 ページ）を参照してください。

AP 更新

Catalyst Center を使用して、古い AP モデルを新しい AP モデルに置き換えることができます。Catalyst Center でプロビジョニングされた AP とプロビジョニングされていない AP の両方を新しい AP に置き換えることができます。詳細については、AP 更新ワークフロー （1630 ページ）を参照してください。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのプロビジョニング中に AP プロビジョニングをスキップする

ワイヤレスコントローラ を初めてプロビジョニングすると、Catalyst Center は関連付けられた AP もプロビジョニングします。ワイヤレスコントローラを再プロビジョニングすると、Catalyst Center は次の AP インテント設定に変更があるかどうかを検出します。

- VLAN 設定：ローカル VLAN、ネイティブ VLAN、AAA VLAN。
- タグ設定：ポリシータグ、サイトタグ、AP プロファイル名、Flex プロファイル名、サイトタグのロード数。
- 以前のプロビジョニング試行からの失敗した AP ワイヤレス設定パラメータ。

これらの AP インテント設定に変更がない場合、Catalyst Center は関連付けられた AP のプロビジョニングをスキップします。APインテント設定に変更がある場合は、[APのプロビジョニングをスキップ（Skip AP Provision）] オプションを使用して、ワイヤレスコントローラ の再プロビジョニング中に AP のプロビジョニングをスキップできます。[APのプロビジョニングをスキップ（Skip AP Provision）] チェックボックスをオンにすると、Catalyst Center は既存の AP とワイヤレスコントローラによって管理される AP を再プロビジョニングしません。ただし、新たに追加された AP はプロビジョニングされます。

選択的 AP グループリソース向けサービス（RFS）変換機能は、変更された AP インテントのみを変換することにより、（AP タグマッピング、RF タグ、Flex または RF プロファイルなどの）AP 関連の設定に対するワイヤレスコントローラの再プロビジョニングを最適化します。アウトオブバンド AP 設定は、コンプライアンスレポートで明示的にフラグが付けられていない限り、再プロビジョニング中に自動的に修正されません。ネットワークインテントに一致するように AP 関連のアウトオブバンド設定を修正するには、ワイヤレスコントローラ再同期およびコンプライアンス実行を行います。たとえば、静的タグマッピングを手動で更新する場合は、次のようになります。

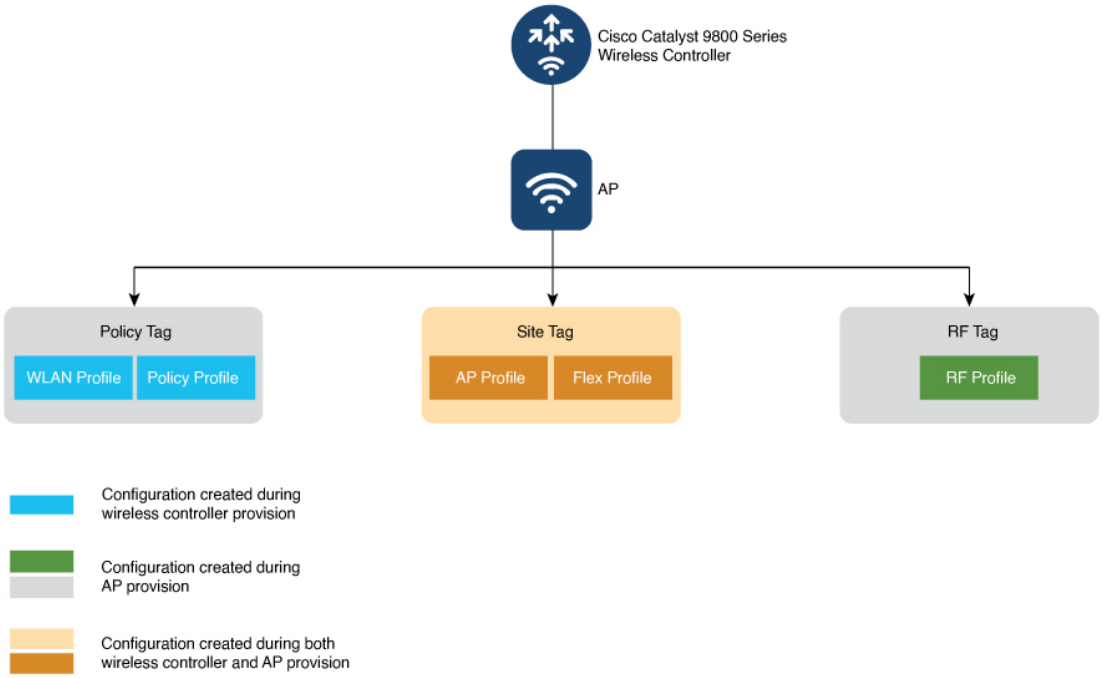
- 再同期とコンプライアンス実行を行った場合、手動での変更がインテント設定と一致するように修正されます。
- 再同期とコンプライアンス実行を行わなかった場合、手動での変更は修正されず、新しいインテントの変更のみが適用されます。

選択的 AP グループ RFS 変換機能を無効にする場合は、Cisco Technical Assistance Center （TAC）にお問い合わせください。

Catalyst Center は、ポリシータグ、サイトタグ、および RF タグを使用し、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラを介して個々の AP にワイヤレスネットワーク構成をプッシュします。

初回プロビジョニングの場合、Catalyst Center は、カスタムタグおよび Catalyst Center で生成されたサイトタグの両方、ポリシータグ、RF タグを、AP のプロビジョニング中にのみ設定します。タグおよび Flex プロファイルの設定の詳細については、AP グループ、Flex グループ、サイトタグ、およびポリシータグの概要 （550 ページ）を参照してください。

次の図は、Catalyst Center によるタグの処理方法を示しています。



ワイヤレスコントローラ のタグの詳細については、Catalyst 9800 ワイヤレスコントローラ構成モデルについて [英語] を参照してください。

次の表に、ワイヤレスコントローラおよび AP の初回プロビジョニング中のタグと関連するタグの情報を示します。

Tag	**[Design] ウィンドウ**	**ワイヤレスコントローラのプロビジョニング（[Skip AP Provision] をオフ）**	**AP のプロビジョニング**
ポリシー タグ	**[Design]** > **[Network Settings]** > **[Wireless]** > **[SSIDs]**	WLAN プロファイルとポリシープロファイルの自動生成された名前が作成されます。	必要な WLAN プロファイルを含むポリシータグが作成されます。
サイト タグ	AP プロファイル：**[Design]** > **[Network Settings]** > **[Wireless]** > **[AP Profiles]** カスタムサイトタグおよび Flex プロファイル：**[Design]** > **[Network Profiles]** > **[Add Profile]** > **[Wireless]** > **[Advanced Settings]** > **[Provision Group]**	非 Flex 設定の場合、カスタムサイトタグにマッピングされた AP プロファイルが作成されます。 （注） サイトタグは、AP のプロビジョニング中に作成され、AP プロファイルに関連付けられます。	非 Flex の場合： • サイトタグが作成されます。 • ROW AP に対してデフォルト以外の AP プロファイルが生成されます。 • メッシュおよび OEAP サイトに対してデフォルト以外の AP プロファイルが生成されます。
		Flex 設定の場合、**[IP Overlap]** が有効になっている機能テンプレートで定義されたインテント設定と、ネイティブ VLAN 設定が作成されます。	Flex の場合、デフォルト以外の Flex プロファイルが作成されます。
RF タグ	**[Design]** > **[Network Settings]** > **[Wireless]** > **[RF Profiles]**	変更なし	RF タグと RF プロファイルが作成されます。

次の表に、AP インテント設定に変更がある場合の、ワイヤレスコントローラ と AP の再プロビジョニング時のタグと、関連付けられたタグの情報を示します。

Tag	[Design] ウィンドウ	ワイヤレスコントローラのプロビジョニング（[Skip AP Provision] をオフ）	AP のプロビジョニング
ポリシー タグ	**[Design]** > **[Network Settings]** > **[Wireless]** > **[SSIDs]**	• WLAN プロファイルおよびポリシープロファイルのマッピングが設定されます。 • ポリシータグの更新は、プロビジョニングされた AP に対して設定されます。 • ポリシータグ名の更新は、プロビジョニングされた AP に対して設定されます。	• 必要なプロファイルを含むポリシータグが設定されます。 • ポリシータグ名の更新が設定されます。
サイト タグ	AP プロファイル：**[Design]** > **[Network Settings]** > **[Wireless]** > **[AP Profiles]** カスタムサイトタグおよび Flex プロファイル：**[Design]** > **[Network Profiles]** > **[Add Profile]** > **[Wireless]** > **[Advanced Settings]** > **[Provision Group]**	サイトタグの更新は、プロビジョニングされた AP に対して設定されます。	サイトタグ、Flex プロファイル、および AP プロファイルが作成または設定されます。
RF タグ	**[Design]** > **[Network Settings]** > **[Wireless]** > **[RF Profiles]**	RF プロファイルの更新が設定されます。	RF タグが設定されます。

（注） フロアにプロビジョニングされた AP がない場合、ワイヤレスコントローラ の再プロビジョニング中にフロアでタグが設定されません。

フラッピング AP の自動タグ付け

Catalyst Center は、フラッピング AP の自動タグ付けをサポートしています。AP が 6 分間に 10 回以上フラップすると、Catalyst Center は AP に AUTO_INV_EVENT_SYNC_DISABLED タグを

自動的に割り当てます。AP にこのタグが割り当てられている場合、その AP のイベントはすべて破棄されます。このタグは、不要なワイヤレスコントローラ同期によるフラッピング AP の AP 情報の更新を防ぎます。

この AP が 10 分間フラップしない場合、Catalyst Center は AUTO_INV_EVENT_SYNC_DISABLED タグを自動的に削除します。

[Audit Logs] ウィンドウで、AP のタグ付けとタグ解除のログを表示できます。

AP フラッピングの根本原因が解決されたら、最新の AP の詳細をすぐに反映させるために手動同期を実行することをお勧めします。または、次にスケジュールされた同期による AP 情報の更新を待ちます。

ROW AP の設定

その他の地域（ROW）ドメイン AP を設定するには、次の手順を実行します。

手順

ステップ 1 必要な国コードを使用して AP プロファイルを作成し、カスタムサイトタグを設定します。詳細については、Cisco IOS XE デバイスの AP プロファイルの追加設定を行う （509 ページ）およびネットワークプロファイルへの AP グループ、Flex グループ、サイトタグ、およびポリシータグの追加 （563 ページ）を参照してください。

（注） AP プロファイルを作成しない場合、Catalyst Center は、AP プロビジョニングまたは AP PnP オンボーディング時に、選択されたサイトの国コードと ROW AP のサイトタグを使用して AP プロファイルを自動生成します。

ステップ 2 運用国のサポートを、ワイヤレスコントローラの国リストに追加します。ワイヤレスコントローラの管理対象 AP ロケーションとして、運用国の少なくとも 1 つのサイトを設定する必要があります。詳細については、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のプロビジョニング （782 ページ）を参照してください。

ステップ 3 ワイヤレスコントローラがステップ 1 （1711 ページ）およびステップ 2 （1711 ページ）の設定でまだプロビジョニングされていない場合は、ワイヤレスコントローラをプロビジョニングします。詳細については、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のプロビジョニング （782 ページ）を参照してください。

ステップ 4 AP パラメータを設定します。詳細については、AP の設定 （1639 ページ）を参照してください。

ステップ 5 AP をプロビジョニングします。詳細については、Day 1 の Cisco AP プロビジョニング （745 ページ）を参照してください。

（注） 既存の AP があるサイトに ROW AP をオンボーディングすると、既存の AP のサービスが短時間中断する可能性があります。

次のタスク

AP の設定を確認するには、**show ap summary** コマンドを使用します。コマンドの出力例を次に示します。

```
C9800LC-94#show ap summary
Number of APs: 4

CC = Country Code
RD = Regulatory Domain

AP Name                          Slots AP Model           Ethernet MAC   Radio MAC      CC   RD   IP Address                                 State       Location
-------------------------------------------------------------------------------------------------------------------------------------------------------------
AP68-C9130I-0D40                 3     C9130AXI-B         3c41.[redacted] 1416.[redacted] IN   -B   [redacted]                                 Registered  Texas
C9130AXI-5A40                    3     C9130AXI-D         548a.[redacted] 488b.[redacted] IN   -D   [redacted]                                 Registered  DEFAULT
C9136I-E1F4                      4     C9136I-ROW         4891.[redacted] 6cd6.[redacted] IN   -RW  [redacted]                                 Registered  DEFAULT
C9115AXI-4AD4                    2     C9115AXI-D         6c41.[redacted] a4b4.[redacted] IN   -D   [redacted]                                 Registered  DEFAULT
```

このコマンドにより、AP の国コード（CC）と規制ドメイン（RD）が表示されます。ROW AP の場合、規制ドメインは **-RW** です。

（注） ROW AP の場合、コマンド出力の国コードが **--**のときは、その国コードが AP に関して使用不可であることを示します。国コードのない ROW AP については、すべての無線の動作ステータスが **down** になります。ROW AP の国コードを設定するには、ROW AP をプロビジョニングする必要があります。

ワイヤレス メッシュ ネットワークの設定

シスコ ワイヤレス メッシュ ネットワーク内の AP は、次のいずれかの方法で動作します。

- ルート AP（RAP）：有線ネットワークに接続されます。
- メッシュ AP（MAP）：ワイヤレス接続を使用して他の MAP および RAP と通信します。

ワイヤレス メッシュ ネットワークを設定するワークフローに含まれる主な手順は、次のとおりです。

1. ワイヤレスコントローラのプロビジョニング：メッシュプロファイルを設定し、AP 認証リストを設定して、ワイヤレスコントローラをプロビジョニングします。
2. AP の設定：AP をブリッジモードで設定し、展開します。
3. AP プロビジョニング：AP のメッシュロール（RAP または MAP）を設定し、AP をプロビジョニングします。

Before you begin

すべての AP は MAP として設定され、出荷されています。AP を RAP として使用するには、AP のプロビジョニング時にその AP を RAP として再設定する必要があります。メッシュネットワークには、少なくとも 1 つの RAP が含まれている必要があります。ワイヤレス メッシュ ネットワークの シスコ ワイヤレス コントローラ 設定および AP 設定の詳細については、ワイヤレス メッシュ ネットワークについて, on page 531を参照してください。

Procedure

ステップ 1 Catalyst Center のデバイスインベントリ（**[Provision]** > **[Inventory]**）で、ワイヤレスコントローラと AP が管理対象状態であり、それぞれのサイトに割り当てられていることを確認します。

ステップ 2 メッシュ設定を使用して AP プロファイルを作成します。詳細については、Cisco IOS XE デバイスの AP プロファイルのメッシュ設定を行う, on page 506およびCisco AireOS デバイスの AP プロファイルのメッシュ設定, on page 513を参照してください。

ステップ 3 AP のイーサネット MAC アドレスを AP 認証リストに追加します。詳細については、AP 認証リストの作成, on page 492を参照してください。

ステップ 4 シスコ ワイヤレス コントローラをプロビジョニングします。詳細については、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のプロビジョニング, on page 782およびCisco AireOS コントローラのプロビジョニング, on page 738を参照してください。

プロビジョニング設定のウィンドウで、手順 3 で定義した **AP 認証リスト**を選択し、メッシュアクセスポイントのみを許可するオプションを選択します。

ステップ 5 （オプション）**アクセスポイント設定**ワークフローで AP を選択し、AP モードが [Local/Flexconnect] モードの場合は [Bridge/Flex+Bridge] モードに変更します。詳細については、AP の設定, on page 1639を参照してください。

ステップ 6 AP をプロビジョニングします。詳細については、Day 1 の Cisco AP プロビジョニング, on page 745を参照してください。

- RAP の場合は、[Mesh Role] で [RAP (Root AP)] を選択します。
- MAP の場合は、[Mesh Role] で [MAP (Mesh AP)] を選択します。

What to do next

次のコマンドを使用して、シスコ ワイヤレス コントローラ のメッシュ設定を確認できます。

- AP のイーサネット MAC アドレス：**show run | inc username**
- プロビジョニング後の AP のメッシュロール（MAP/RAP）：**show wireless mesh ap summary**
- サイトタグの詳細：**show wireless tag site detailed <site tag name>**
- AP プロファイル：**show run | section ap profile**

- ワイヤレスメッシュ設定：
  - **show wireless profile mesh summary**
  - **show wireless profile mesh detailed <mesh profile name>**

ワイヤレスコントローラから別のワイヤレスコントローラへの AP の移行

ネットワーク階層内の同じフロアにある ワイヤレスコントローラ から別の ワイヤレスコントローラ に AP を移行できます。詳細については、ワイヤレスコントローラ から別の ワイヤレスコントローラ に AP を移行する （749 ページ）を参照してください。

RMA ワークフローを使用した AP の交換

Catalyst Center の返品許可（RMA）機能を使用して、ネットワーク内の障害のあるアクセスポイントを交換できます。RMA ワークフローにより、障害が発生したデバイスを迅速に交換できるため、生産性が向上し、運用コストが減少します。ワイヤレス AP の場合、交換用デバイスは同じサイトに割り当てられ、プライマリ ワイヤレス コントローラ、RF プロファイル、および AP グループ設定でプロビジョニングされ、障害が発生した AP と同じ Catalyst Center のフロアマップの場所に配置されます。

詳細については、障害のあるアクセスポイントの交換 （251 ページ）を参照してください。

非インテントベースの展開に PnP を使用する AP のオンボーディング

次のような条件の展開でプラグアンドプレイ（PnP）を使用して AP をオンボーディングおよびプロビジョニングする場合に、この手順を使用します。

- インテントベースの設定を使用しない、かつ
- Catalyst Center のネットワークプロファイルでプロビジョニングされていない

非インテントベースの設定には、アシュアランスのユースケースと デバイスごとの設定 が含まれます。

Before you begin

- Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ が一覧に追加されていることを確認します。
- DHCP サーバーに PnP のオプション 43 を設定します。このオプションにより、Catalyst Center コントローラの IP アドレスを持つネットワークデバイスが通知されます。
- AP が初期設定リセットの状態になっていることを確認します。
- AP、Catalyst Center、および ワイヤレスコントローラ 間のネットワーク接続を確認します。

手順

ステップ 1 PnP を使用して AP をオンボーディングするための通常の Day-0 テンプレートを作成します。

a) 次の設定を使用します。

- [Template Name]：テンプレートの名前を入力します。
- [Project Name]：[Onboarding Configuration]
- [Deployment Type]：[Day 0]
- [Template Language]：[Jinja]
- [Software Type]：[IOS-XE]
- [Device Family]：[Wireless Controller]
- [Device Model]：[Cisco Catalyst 9800 Wireless Controllers]

詳細については、標準テンプレートの作成 （576 ページ） を参照してください。

b) 次の設定をテンプレートに追加して保存し、変更を確定します。

- プライマリ ワイヤレスコントローラ IP アドレス
- プライマリ ワイヤレスコントローラ 名
- セカンダリ ワイヤレスコントローラ IP アドレス
- セカンダリ ワイヤレスコントローラ 名
- ポリシータグ名
- サイトタグ名
- RF タグ名

詳細については、テンプレートの編集 （581 ページ） を参照してください。

Catalyst Center は、PnP 要求中にこれらの設定を AP にプッシュします。

たとえば、次の設定をテンプレートに追加します。

```
{
  "primaryWlcIP": "10.0.0.1",
  "primaryWlcName": "Primary-WLC",
  "secondaryWlcIP": "10.0.0.5",
  "secondaryWlcName": "Secondary-WLC",
  "policyTagName": "default-policy-tag",
  "siteTagName": "default-site-tag",
  "RFTagName": "default-rf-tag"
}
```

ステップ 2 PnP を使用して AP を要求する。

a) AP をサイトに割り当てない。
b) AP のオンボーディング用に作成した Day-0 テンプレートを選択する。

詳細については、ワイヤレスコントローラ のプロビジョニング （722 ページ） を参照してください。

PnP 要求後、設定が AP にプッシュされ、対応する ワイヤレスコントローラ に接続します。AP が一覧に表示されます。

次のタスク

AP コンソールで、**show pnp log** を使用して、PnP 要求を検証します。コマンドの出力例を次に示します。

```
#show pnp log
722 - pnp.agent - DEBUG - Setting sid from stored value
551de96a-c719-44f0-8964-16b150f7325d
APC414.A2FB.0CB0#
PNP CONFIG - HOST NAME    : APC414.A2FB.0CB0
PNP CONFIG - PRI WLC IP   : 10.0.0.1
PNP CONFIG - SEC WLC IP   : 10.0.0.5
PNP CONFIG - PRI WLC NAME: Primary-WLC
PNP CONFIG - SEC WLC NAME: Secondary-WLC
PNP CONFIG - Policy Tag   : default-policy-tag
PNP CONFIG - Site Tag     : default-site-tag
PNP CONFIG - RF Tag       : default-rf-tag
PnP: Config Upgrade received. Start CAPWAP discovery
```

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのキャンパスネットワーク設定のユースケース

Catalyst Center は、既存のCisco Catalyst 9800 シリーズ ワイヤレス コントローラから設定を学習し、その設定を設定プロファイルとして保存できます。設定プロファイルは、デバイスごとの設定を使用してプロビジョニングされた、またはインテントベースのネットワーク設定を使用してプロビジョニングされた、またはプロビジョニングされずにインベントリに登録されている、ワイヤレスコントローラ から学習できます。設定プロファイルを使用して複数の ワイヤレスコントローラ をプロビジョニングできるため、一貫した設定と標準化された展開が保証されます。

（注） この機能はベータ版であり、機能を有効にする必要があります。有効にするには、Cisco TAC にお問い合わせください。この機能が有効になっていない場合、ワイヤレスコントローラ 関連の設定のオプションは使用できないか、グレー表示されます。

設定プロファイルはバージョン固有です。特定の Cisco IOS XE リリースを実行している ワイヤレスコントローラ から学習したプロファイルは、同じバージョンを実行している ワイヤレ

スコントローラにのみ適用できます。設定プロファイルはサイトやネットワークに関連付けられていないため、異なるネットワークで使用できます。

キャンパスネットワークの詳細については、「キャンパスネットワークのプロビジョニング（1305 ページ）」を参照してください。

前提条件

- ワイヤレスコントローラは、Cisco IOS XE リリース 17.12 以降を実行している必要があります。
- デバイスごとの設定は、キャンパスネットワークに含まれるワイヤレスコントローラで有効にする必要があります。詳細については、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の デバイスごとの設定 を有効にします。 （802 ページ） を参照してください。
- ワイヤレスコントローラと AP をインベントリに追加し、必要なサイトに割り当てる必要があります。

Day-0 における ワイヤレスコントローラ のすべての設定の標準化

既存の ワイヤレスコントローラ からデバイス設定をコピーし、セットアップを標準化することで、ネットワーク内のすべての ワイヤレスコントローラ で一貫した初期設定を実現します。

Before you begin

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのキャンパスネットワーク設定のユースケース （1716 ページ） を参照してください。

この手順を使用して、ワイヤレスコントローラから設定をコピーし、ネットワーク内の他のすべての ワイヤレスコントローラ に適用して、一貫した Day-0 設定を確保します。

手順

ステップ 1 ネットワークを作成し、ネットワークに含める必要がある ワイヤレスコントローラ を追加します。

ワイヤレスコントローラ を使用したネットワークの作成に関する情報については、「ネットワークの作成（1308 ページ）」を参照してください。

ステップ 2 既存の ワイヤレスコントローラ から 設定プロファイル を学習します。

詳細については、ワイヤレスコントローラ から 設定プロファイル を学習する （1311 ページ） を参照してください。

ステップ 3 ネットワーク内の ワイヤレスコントローラ の設定を標準化します。

a) 設定プロファイルを必要な ワイヤレスコントローラ に割り当て、プロビジョニングに影響を与える検証エラーを解決して、プロビジョニングをスケジュールします。

詳細については、設定プロファイルの ワイヤレスコントローラ への割り当て （1320 ページ） を参照してください。

（注） ワイヤレスコントローラ が、設定プロファイル の学習元となる ワイヤレスコントローラ と同じ Cisco IOS XE リリースを実行していることを確認してください。

b) （任意） ワイヤレスコントローラ の 設定プロファイル 割り当てを編集します。

詳細については、設定プロファイルの ワイヤレスコントローラ 割り当ての編集 （1321 ページ） を参照してください。

ステップ 4 設定が ワイヤレスコントローラ にプッシュされていることを確認します。

a) メインメニューから次を選択します。**[プロビジョニング（Provision）] > [キャンパスネットワーク（Campus Network）] > [ネットワークおよび設定プロファイル（Networks & Configuration Profiles）]**。

b) ネットワークの詳細を表示するには、ネットワーク名をクリックします。

c) [Devices] タブをクリックします。

d) [ワイヤレスコントローラ（wireless controllers）] をクリックします。

e) デバイス名をクリックします。

f) [同期ステータス（Sync Status）] 列で、ワイヤレスコントローラのステータスが [同期中（In Sync）] であることを確認します。

ステップ 5 ワイヤレスコントローラ に関連付けられた AP に対し、デバイスごとの設定を使用してサイトタグ、ポリシータグ、および RF タグを設定します。

詳細については、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ に関連付けられた AP の管理 （805 ページ） を参照してください。

Day-0 における ワイヤレスコントローラ の部分的な設定の標準化

設定プロファイル の一部を ワイヤレスコントローラ に適用してカスタマイズし、必要な設定のみが初回展開時にプロビジョニングされるようにします。

この手順を使用して、既存の ワイヤレスコントローラ から学習した 設定プロファイル をカスタマイズします。たとえば、学習したプロファイルに 10 個の SSID が含まれていて、サイトに必要な SSID が 2 つだけの場合、サイトの要件に一致するようにプロファイルを変更します。

Before you begin

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのキャンパスネットワーク設定のユースケース （1716 ページ） を参照してください。

手順

ステップ 1 ネットワークを作成し、ネットワークに含める必要がある ワイヤレスコントローラ を追加します。

ワイヤレスコントローラを使用したネットワークの作成に関する情報については、「ネットワークの作成（1308 ページ）」を参照してください。

ステップ 2 既存の ワイヤレスコントローラ から 設定プロファイル を学習します。

詳細については、ワイヤレスコントローラ から 設定プロファイル を学習する （1311 ページ） を参照してください。

ステップ 3 ネットワーク内の必要な ワイヤレスコントローラ の部分的な設定を標準化します。

a) ワイヤレスプロファイルの 設定プロファイル を複製します。

詳細については、設定プロファイルの管理 （1309 ページ） を参照してください。

b) （任意） 必要に応じて、重複したプロファイルの設定を編集または削除します。

ワイヤレスコントローラの設定プロファイルの編集または削除については、「設定プロファイルの管理 （1309 ページ）」を参照してください。

たとえば、設定プロファイルで 10 個の SSID のうち 2 つだけを使用する場合は、不要な 8 個の SSID を削除します。

c) 設定プロファイルを必要なワイヤレスコントローラに割り当て、プロビジョニングに影響を与える検証エラーを解決して、プロビジョニングをスケジュールします。

詳細については、設定プロファイルの ワイヤレスコントローラ への割り当て （1320ページ） を参照してください。

ステップ 4 設定が ワイヤレスコントローラ にプッシュされていることを確認します。

a) メインメニューから次を選択します。**[プロビジョニング（Provision）] > [キャンパスネットワーク（Campus Network）] > [ネットワークおよび設定プロファイル（Networks & Configuration Profiles）]**。

b) ネットワークの詳細を表示するには、ネットワーク名をクリックします。

c) [Devices] タブをクリックします。

d) [ワイヤレスコントローラ（wireless controllers）] をクリックします。

e) デバイス名をクリックします。

f) [同期ステータス（Sync Status）] 列で、ワイヤレスコントローラのステータスが [同期中（In Sync）] であることを確認します。

Day-n のワイヤレスコントローラ設定の管理

設定プロファイルを更新することによって、ワイヤレスコントローラの設定を維持、更新、または削除します。

Day-n のワイヤレスコントローラの設定プロファイルにおける設定を追加、編集、または削除するには、この手順を使用します。たとえば、次の手順を使用して、Wi-Fi 7 クライアント用の SSID を作成できます。

手順

ステップ 1 設定プロファイルで設定を管理します。

a) 必要に応じて、ワイヤレス プロファイルの設定プロファイル内の設定を編集または削除します。

ワイヤレスコントローラの設定プロファイルの編集または削除については、「設定プロファイルの管理 （1309 ページ）」を参照してください。

たとえば、[WLANプロファイル（WLAN Profiles）] テーブルの [追加（Add）] をクリックして、Wi-Fi 7 の SSID を追加できます。SSID を作成したら、その SSID をポリシータグにマッピングします。

ワイヤレスコントローラ ですでに割り当ておよびプロビジョニングされている設定プロファイルが変更されると、ワイヤレスコントローラ（ステップ 2 （1720 ページ）を参照）の [同期ステータス（Sync Status）] は [非同期（Out of sync）] に変わります。

b) 更新された設定を確認し、プロビジョニングに影響を与える検証エラーを解決して、更新された 設定プロファイルで ワイヤレスコントローラ を再プロビジョニングしてください。

[変更タイプ（Change type）] 列では、プロビジョニング中の各設定のステータスが特定されます。この列では、更新された既存の設定については [変更（Modify）]、新しく作成された設定については [追加（Add）]、すでに同期されていて更新されていない設定については [変更なし（No changes）] が表示されます。

詳細については、設定プロファイルの ワイヤレスコントローラ 割り当ての編集 （1321 ページ） を参照してください。

ステップ 2 設定が ワイヤレスコントローラ にプッシュされていることを確認します。

a) メインメニューから次を選択します。**[プロビジョニング（Provision）] > [キャンパスネットワーク（Campus Network）] > [ネットワークおよび設定プロファイル（Networks & Configuration Profiles）]**。

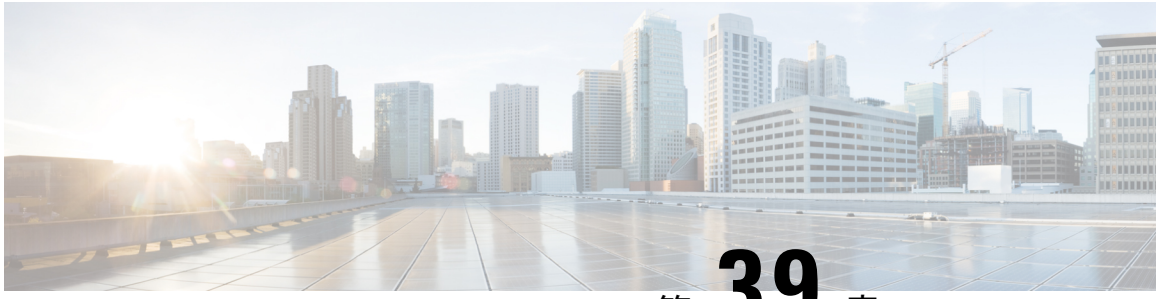
b) ネットワークの詳細を表示するには、ネットワーク名をクリックします。

c) [Devices] タブをクリックします。

d) [ワイヤレスコントローラ（wireless controllers）] をクリックします。

e) デバイス名をクリックします。

f) [同期ステータス（Sync Status）] 列で、ワイヤレスコントローラのステータスが [同期中（In Sync）] であることを確認します。



第 39 章

ネットワークのエネルギーの管理

- 概要 （1721 ページ）
- ネットワークデバイスのエネルギーの管理 （1722 ページ）
- エネルギー管理ダッシュボードの使用 （1723 ページ）
- ネットワークデバイスのエネルギー管理に関するレポートの生成 （1725 ページ）
- ネットワークデバイスのエネルギー消費量の表示 （1725 ページ）
- ネットワークデバイスの炭素排出量 （1727 ページ）
- 省エネルギーの表示 （1728 ページ）
- サイト間のエネルギー比較 （1729 ページ）

概要

Catalyst Center は、組織がエネルギー使用量を最適化し、コストを削減し、サステナビリティを向上させることを支援するために設計されたさまざまなエネルギー管理機能を提供します。Catalyst Center のエネルギー管理ソリューションは、次の主な機能を提供します。

- コスト最適化：エネルギー消費データを定期的に確認し、コスト削減に向けた戦略を調整できます。
- サステナビリティ：エネルギー管理機能は、エネルギーの効率的な使用によって二酸化炭素排出量を削減することにより、サステナビリティへの取り組みをサポートします。
- 高電力消費デバイスのアセスメント：Catalyst Center は、高電力消費デバイスとパターンを特定するためのエネルギー監査を提供します。このアセスメントは、古くなったネットワークデバイスをエネルギー効率の高いモデルに置き換えるのに役立ちます。
- レポートと分析：Catalyst Center では、エネルギー使用量に関する詳細なレポートと分析を提供します。傾向を特定し、節約量を追跡し、サステナビリティへの取り組みをサポートするためにご使用ください。

ネットワークデバイスのエネルギーの管理

エネルギー管理を活用して、ネットワークのコスト、エネルギー消費、および炭素排出量を監視します。

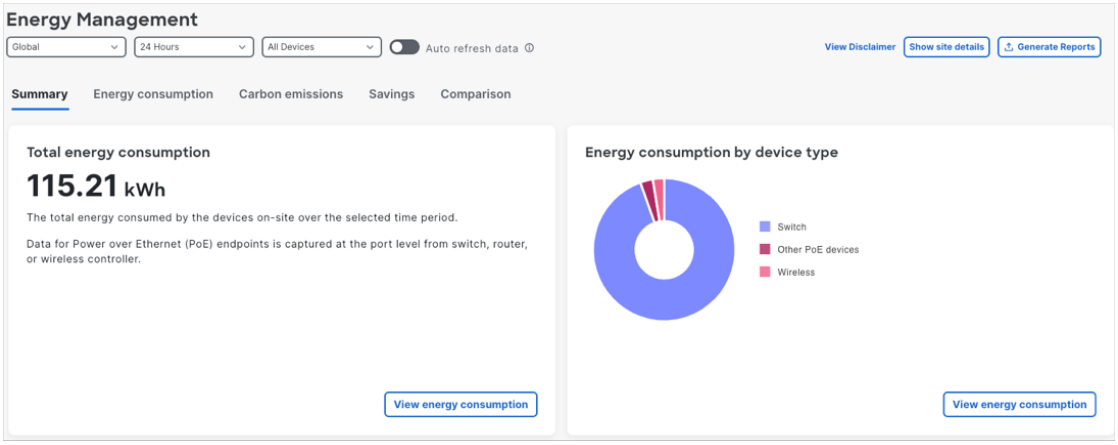
このセクションでは、**[エネルギー管理（Energy Management）]** ウィンドウで使用できるオプションについて説明します。

手順

ステップ 1 メインメニューから次を選択します。、[エネルギー管理（Energy Management）] を選択します。

デフォルトで、Catalyst Center は、過去 24 時間のすべてのネットワークデバイスのエネルギー消費量を表示します。

重要 このダッシュボードで生成されたデータおよびその他の情報は、[免責事項（Disclaimer）] スライドインペインに記載されている免責事項の対象となります。このペインを表示するには、[免責事項の表示（View Disclaimer）] リンクをクリックします。



ステップ 2 [グローバル（Global）] ドロップダウンリストからサイトを選択すると、そのサイトのエネルギー消費量を表示できます。

ステップ 3 過去 24 時間または 7 日間のエネルギー消費量を表示できます。時間範囲を変更するには、[24時間（24 Hours）] ドロップダウンリストから [7日間（7 Days）] を選択し、[適用（Apply）] をクリックします。

また、[開始時刻および終了時刻（Start Time and End Time）] エリアの日付と時刻を変更して、特定の日や週のエネルギー消費量を表示することもできます。

ステップ 4 スイッチ、ルータ、アクセスポイント、またはその他の Power over Ethernet（PoE）デバイスのエネルギー消費量を表示するには、[すべてのデバイス（All Devices）] ドロップダウンリストからデバイスタイプを選択します。

ステップ 5 [データの自動更新（Auto refresh data）] トグルボタンを有効にして、**[エネルギー管理（Energy Management）]** ウィンドウでデータを更新します。

データは 5 分ごとに更新されます。データ更新を一時的に停止するには、[一時停止（pause）] ボタンをクリックします。

ステップ 6 すべてのサイトの詳細情報を表示するには、[サイトの詳細を表示（Show site details）] ボタンをクリックします。

すべてのサイトの炭素濃度、エネルギー消費量、推定排出量、および推定コストを表示できます。

Sites (3)

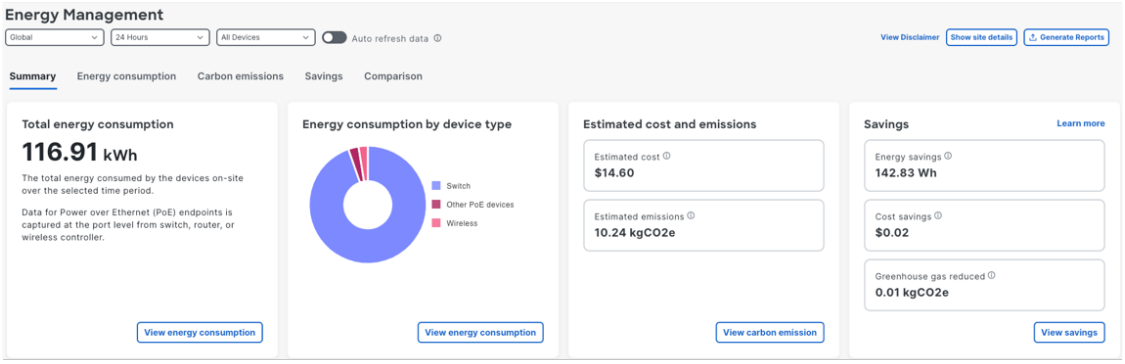
Site	Carbon Intensity (gCO2e/kWh)	Energy Consumption (kWh)	Estimated Emissions (kgCO2e)	Estimated Cost ($)
Global	150.71	37.87	5.71	5.30
San Jose	192.10	21.79	4.18	3.29
Kanata	94.67	16.09	1.52	2.01

この表で、さまざまなサイト間の値を比較できます。サイト内の建物やフロアのエネルギー消費量、炭素濃度、推定排出量、消費コストなどの詳細を表示するには、サイト名のハイパーリンクをクリックします。

マップビューアイコン（ ）をクリックして、マップ上にサイトを表示します。エネルギー消費量、炭素濃度、排出量、推定消費コストなどの詳細を表示するには、サイトにカーソルを合わせます。

エネルギー管理ダッシュボードの使用

このセクションでは、エネルギー管理ダッシュボードのコンポーネントについて説明します。



- [合計エネルギー消費量（Total energy consumption）]：このダッシュレットには、選択したサイトと時間範囲におけるデバイスのエネルギー消費量が表示されます。
- [デバイスタイプ別のエネルギー消費量（Energy consumption by device type）]：このダッシュレットには、選択したサイトと時間範囲における各デバイスタイプのエネルギー消費量が表示されます。
- [推定コストおよび排出量（Estimated cost and emissions）]：

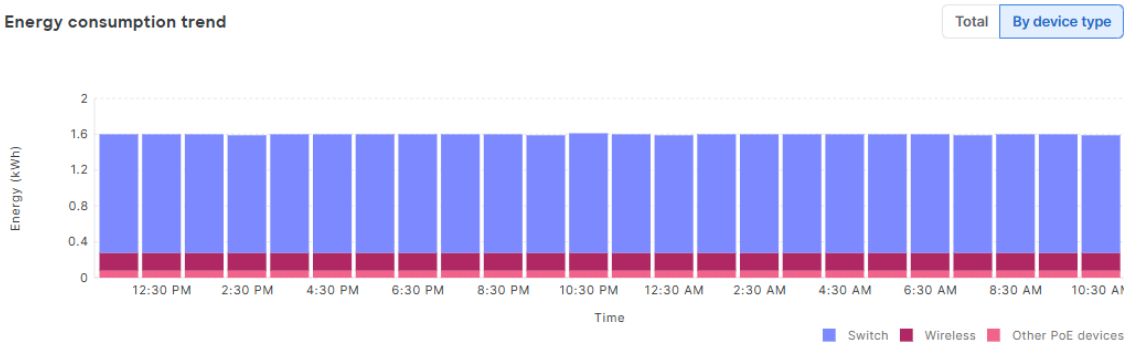
- [推定コスト（Estimated cost）]：電力マップ（使用可能な場合）または国際エネルギー機関（IEA）のデータに基づいて、消費されたエネルギーの推定コストを表示します。
- [推定排出量（Estimated emissions）]：消費されたエネルギーの炭素排出量を二酸化炭素換算キログラム（kgCO2e）で表示します。

- [削減量（Savings）]：このダッシュレットには、省エネルギー、コスト削減、削減された温室効果ガス排出量が表示されます。

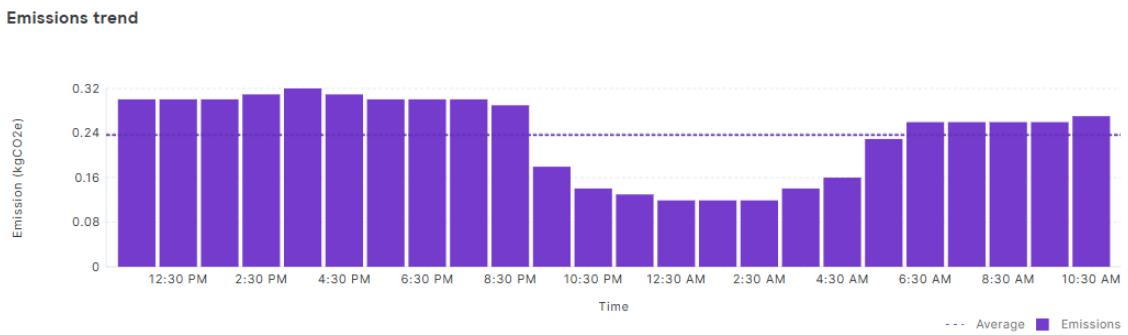
（注） 省電力モードで動作している AP を介してのみ実現された削減量を表示できます。

Catalyst Center で AP を省電力モードで設定する方法については、「AP 電力プロファイルの作成（514 ページ）」を参照してください。

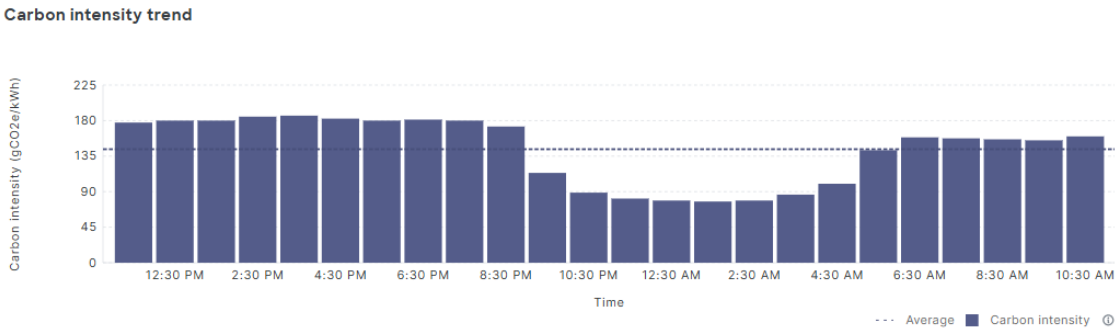
- [エネルギー消費傾向（Energy consumption trend）]：一定の時間範囲に消費されたエネルギーの傾向を表示します。トグルボタンをクリックすると、すべてのデバイスまたはデバイスタイプ別のエネルギー消費傾向が表示されます。



- [排出量傾向（Emissions trend）]：一定の時間範囲における選択したデバイスの炭素排出量の傾向を表示します。



- [炭素強度傾向（Carbon intensity trend）]：一定の時間範囲における炭素強度の傾向を表示します。炭素強度とは、エネルギー出力単位あたりの二酸化炭素（CO_2）排出量を指します。



各カテゴリの詳細情報を表示するには、[エネルギー消費量（Energy consumption）]、[炭素排出量（Carbon emissions）]、[削減量（Savings）]、[比較（Comparison）] タブをクリックします。

ネットワークデバイスのエネルギー管理に関するレポートの生成

Catalyst Center は、統合されたエネルギー管理レポートを提供します。レポートには、ネットワークデバイスのエネルギー消費量、コスト、炭素排出量、および炭素強度データが表示されます。

詳細については、『*Cisco Catalyst Center Platform User Guide*』の「Run a Network Devices Report」を参照してください。

ネットワークデバイスのエネルギー消費量の表示

Catalyst Center では、ネットワークデバイスのエネルギー消費量を評価できます。このアセスメントを使用して運用コストを管理し、環境への影響を軽減します。

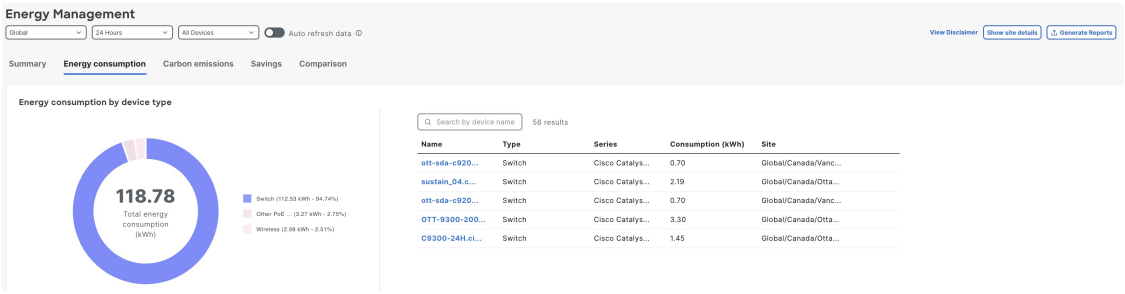
ネットワークデバイスのエネルギー消費量に影響する要因は次のとおりです。

- [デバイスタイプ（Device Type）]：それぞれエネルギー要件が異なる、スイッチ、ルータ、AP、その他の PoE デバイス。
- [使用パターン（Usage Patterns）]：フルキャパシティまたは非常に高い負荷で動作しているデバイスは通常、エネルギー消費量が多くなります。
- [環境条件（Environmental Conditions）]：動作温度と動作湿度は、エネルギー使用量に影響する可能性があります。

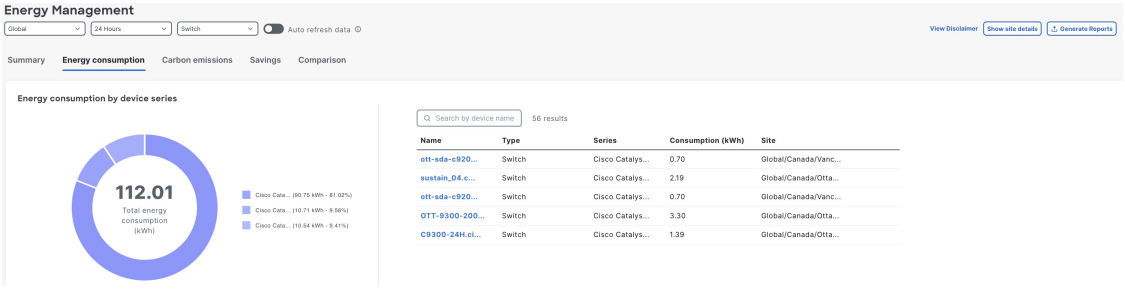
メインメニューから次を選択します。、**[エネルギー管理（Energy Management）] > [エネルギー消費量（Energy consumption）]** の順に選択します。

[エネルギー消費量（Energy Consumption）] ダッシュボードには、次のセクションが含まれます。

- [デバイスタイプ別のエネルギー消費量（Energy consumption by device type）] には、 すべてのデバイスと各デバイスタイプの合計エネルギー消費量が表示されます。



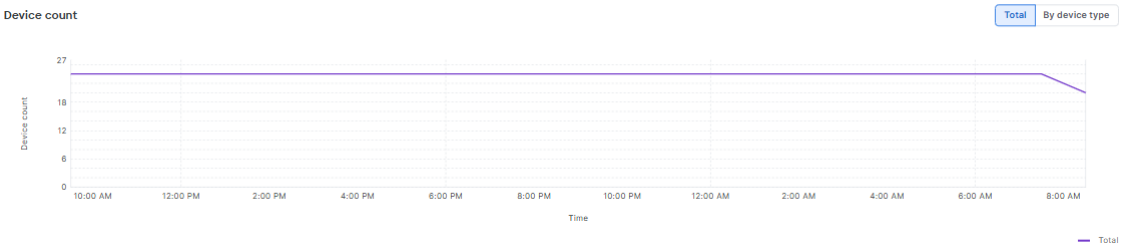
[すべてのデバイス（All Devices）] ドロップダウンリストから、デバイスシリーズのエネルギー消費量を表示するデバイスタイプを選択します。



このテーブルには、すべてのデバイスが一覧表示され、デバイスタイプ、デバイスシリーズ、サイト、デバイスで消費されたエネルギーなどの情報が示されます。

- [エネルギー消費傾向（Energy consumption trend）] には、 一定の時間範囲に消費されたエネルギーがグラフィカルに表示されます。

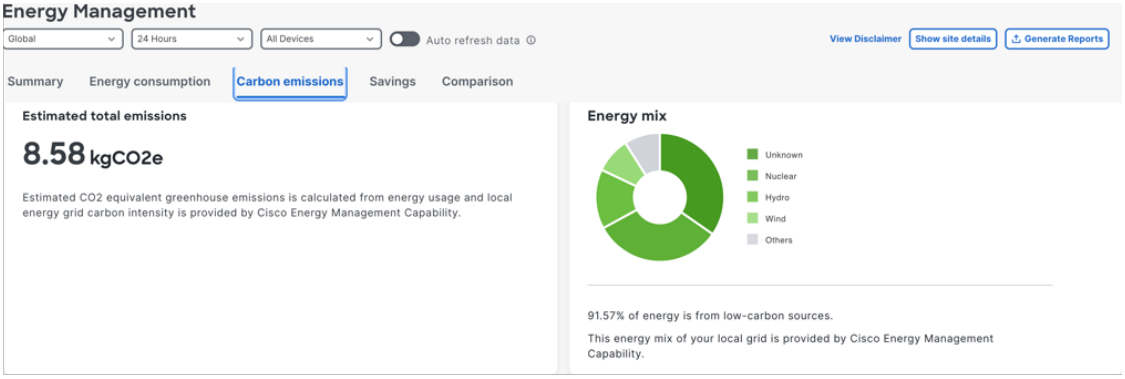
- [デバイス数（Device count）] には、一定の時間範囲におけるデバイスの総数とデバイスタイプに基づくデバイスの数が表示されます。このグラフには、エネルギーデータを報告したデバイスの数のみが表示されます。エネルギーデータを報告しないデバイスは、デバイス数から除外されます。



ネットワークデバイスの炭素排出量

炭素排出量は、大気中への炭素（特に二酸化炭素（CO_2））の放出です。これらの排出量は、温室効果の増大により気候変動の大きな一因となります。これは地球温暖化を引き起こし、環境にさまざまな影響をもたらします。

エネルギー管理機能は、ネットワークデバイスの推定炭素排出量データを提供し、選択した時間範囲の洞察を示します。

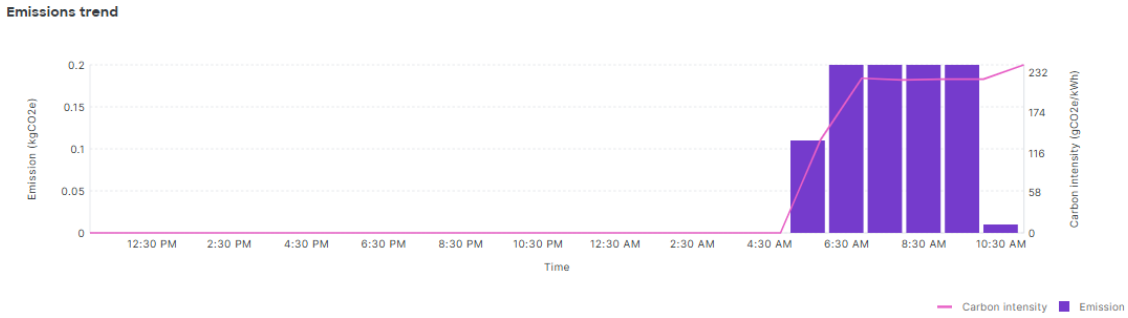


炭素排出量ダッシュボードを表示するには、左上隅にあるメニューアイコンをクリックします。次に、[エネルギー管理（Energy Management）]>[炭素排出量（Carbon emissions）]の順に選択します。このダッシュボードには、次のセクションが表示されます。

- [推定合計排出量（Estimated total emissions）]：このダッシュレットには、エネルギー消費量とローカルエネルギーグリッドの炭素強度に基づく、推定温室効果ガス排出量（特に二酸化炭素（CO_2）換算）が表示されます。
- [エネルギーミックス（Energy mix）]：このダッシュレットには、ガス発電所、原子力発電所、水力発電所、風力発電、バッテリ放電など、さまざまな発生源から生成されたエネルギーが表示されます。

  電力生成は、特に石炭や天然ガスなどの化石燃料を使用する場合、CO_2 を含む温室効果ガス排出の大きな原因になります。

  原子力発電所、水力発電所、風力タービンは、炭素排出量がゼロか無視できるレベルのクリーンな電力源です。これらの電力源は緑色で表示されます。ガス発電所からの電力は、炭素排出量が多いことを示す赤色で表示されます。灰色の電力源は、不明な電力源からの電力を示します。
- [排出量傾向（Emissions trend）]：このエリアには、一定の時間範囲における炭素排出量と炭素強度がグラフで表示されます。



省エネルギーの表示

[エネルギー管理および削減効果（Energy Management Savings）]ダッシュボードは、APに省電力モードを適用した場合の推定コストとエネルギー削減量、および推定温室効果ガス排出削減量を示します。

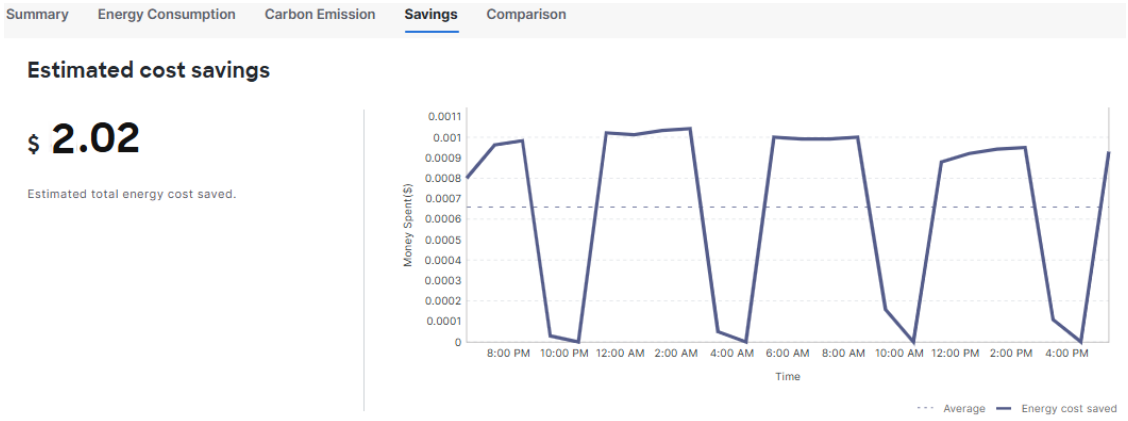
メインメニューから次を選択します。、**[エネルギー管理（Energy Management）]**>**[削減効果（Savings）]** を選択し、削減効果を監視および分析します。

（注） ダッシュボードは、AP が省電力モードで動作している場合に実現する削減効果のみをキャプチャします。

Catalyst Center で AP を省電力モードで設定する方法については、「AP 電力プロファイルの作成 （514 ページ）」を参照してください。

[削減効果（Savings）] ダッシュボードは次のセクションで構成されます。

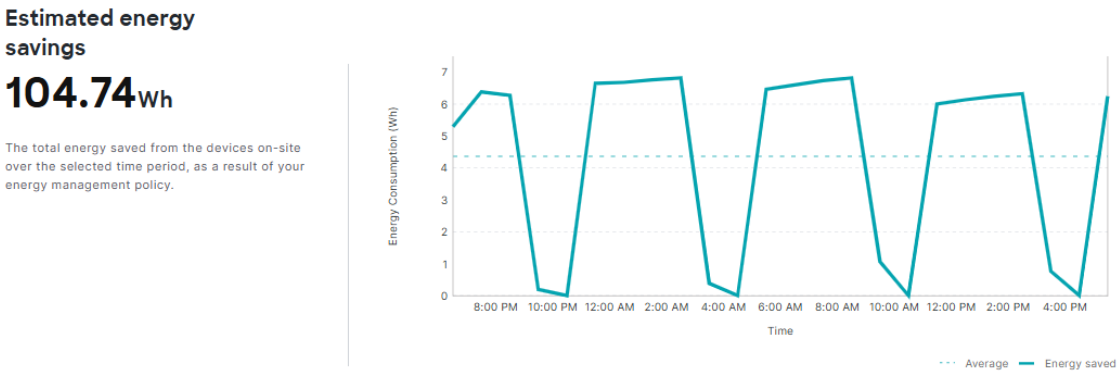
- [推定コスト削減量（Estimated cost savings）]：このエリアには、エネルギー消費量の削減により達成された推定コスト削減量が表示されます。また、一定期間における支出金額を示すグラフも表示されます。



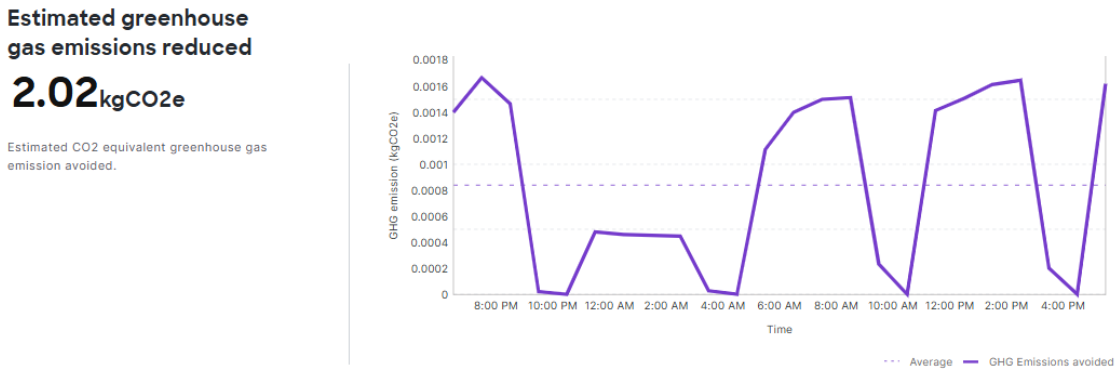
- [推定エネルギー削減量（Estimated energy savings）]：このエリアには、達成された推定エネルギー削減量がワット時間（Wh）単位で表示されます。通常モードまたは省電力モー

ドで動作するように AP を設定できます。削減値は、通常モードのエネルギー消費量から省電力モードのエネルギー消費量を差し引いて計算されます。この削減量は、スイッチによって報告されたリアルタイムのエネルギー消費量に基づいて計算されます。

このメトリックは、電力サンプルに基づく、[アシュアランス（Assurance）] > [PoE ダッシュボード（PoE dashboard）] > [推定 AP 電力削減量（Estimated AP Power Savings）] の値よりも精度が高いです。[PoE] ダッシュボードで、Assurance は毎時 1 回データをサンプリングし、これらのサンプルからエネルギー消費量を計算します。これは、[エネルギー管理（Energy Management）] ウィンドウに表示されるエネルギー削減量よりも高いレベルの概算を提供します。



- [推定温室効果ガス削減量（Estimated greenhouse gas emissions reduced）]：エネルギー消費は、多くの場合、温室効果ガス（GHG）排出量につながります。このエリアには、エネルギー消費量の減少により削減された二酸化炭素（CO_2）およびその他の温室効果ガスの量が表示されます。

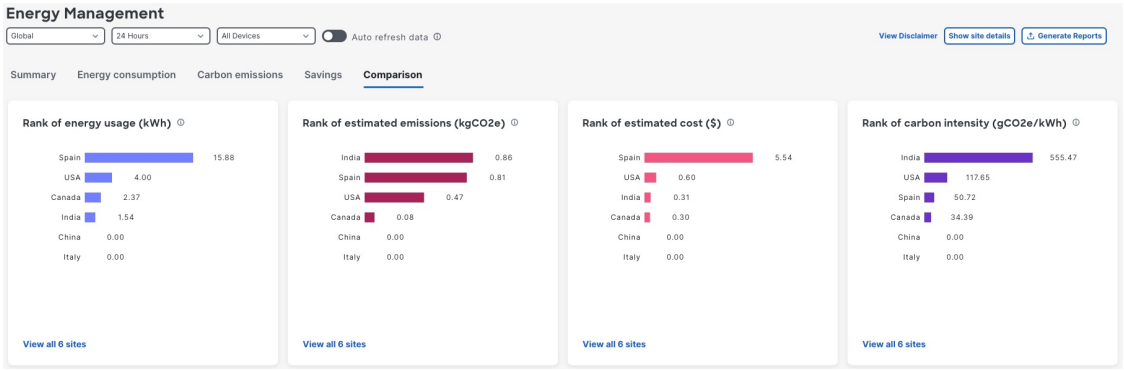


温室効果ガス排出量を削減することは、気候変動の緩和と大気質の改善に貢献します。

サイト間のエネルギー比較

ネットワーク全体のエネルギーを分析するために、Catalyst Center では、エネルギー消費、推定排出量、コスト、および炭素排出係数でサイトがランク付けされます。

メインメニューから次を選択します。**[エネルギー管理（Energy Management）] > [比較（Comparison）]**の順に選択します。。

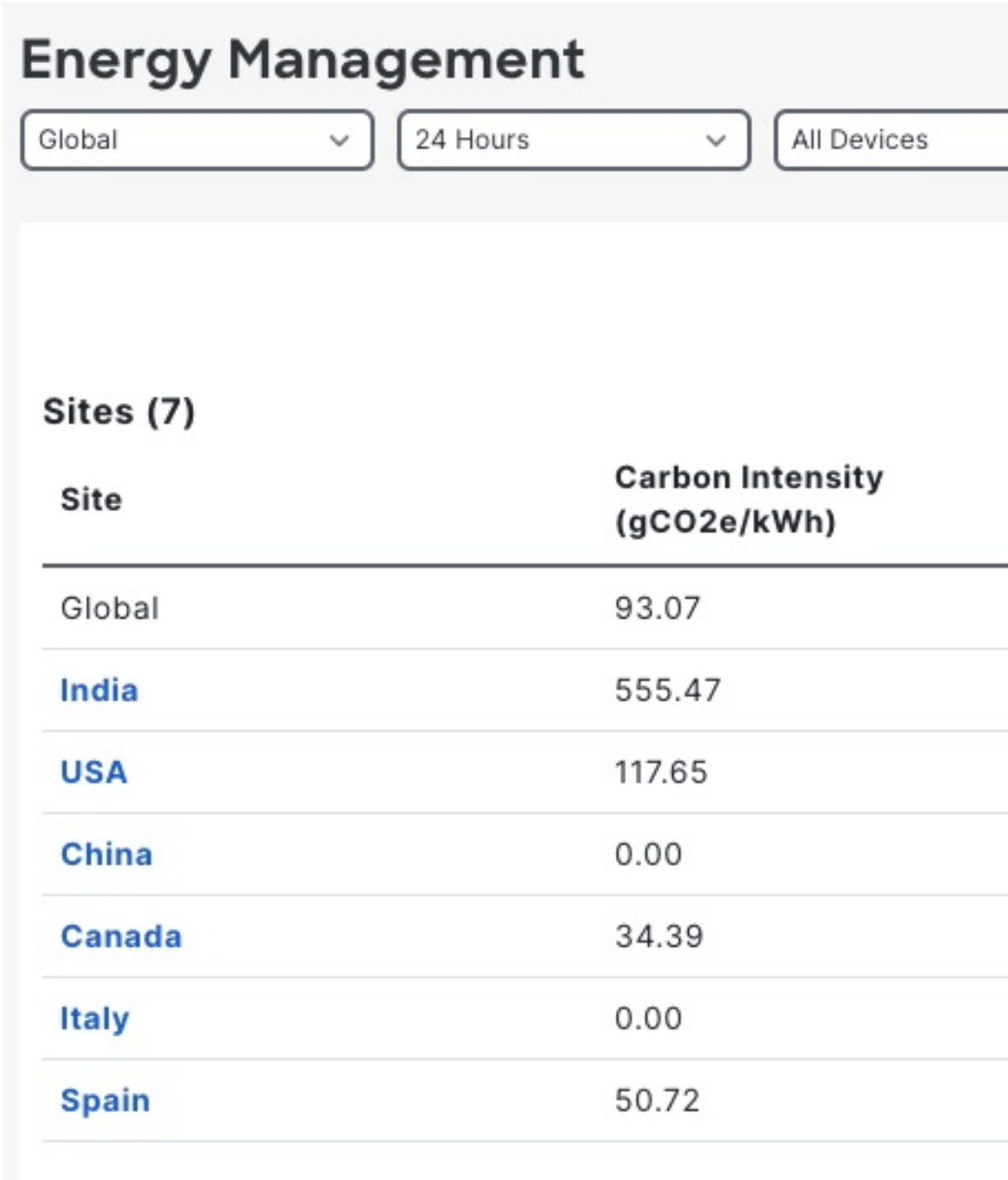


[比較（Comparison）] ダッシュボードでは、エネルギー消費量、推定排出量、コスト、および炭素排出係数でサイトがランク付けされます。特定のランクのサイトの詳細を表示するには、対応するリンクをクリックします。

Sites by kWh energy usage (6)

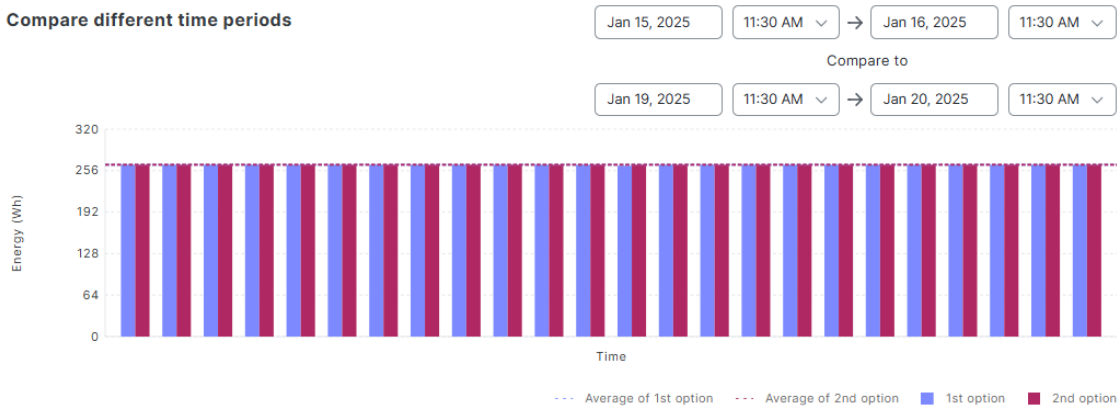
Rank	Site	Energy consumption (kWh)	Emissi (kgCO2
1	Spain	15.88	0.81
2	USA	4.00	0.47
3	Canada	2.37	0.08
4	India	1.54	0.86
5	China	0.00	0.00
5	Italy	0.00	0.00

[サイトの詳細を表示（Show site details）] をクリックして、各サイトの名前とランクを表示します。



サイト名をクリックすると、そのサイトの詳細情報が表示されます。

[異なる期間の比較（Compare different time periods）] エリアには、選択した時間範囲におけるエネルギー消費量のグラフがワット時単位で表示されます。





第 40 章

データプラットフォームを使用した Catalyst Center のトラブルシューティング

- データ プラットフォームについて （1733 ページ）
- コレクタの設定情報の表示または更新 （1734 ページ）
- データ保持設定の表示 （1735 ページ）
- パイプラインステータスの表示 （1735 ページ）

データ プラットフォームについて

データ プラットフォームには、Catalyst Center アプリケーションのモニターとトラブルシューティングに役立つツールがあります。[Data Platform] には、ネットワークのパターン、トレンド、問題領域を特定するのに役立つ、さまざまな入力から合成されたデータが表示されます。たとえば、ネットワークに問題が発生した場合、パイプラインがエラー状態になっているかどうか、特定のエリアにおけるリアルタイム トラフィック フローが何かなど、問題に対する回答を迅速に得ることができます。

管理者ユーザーには、データプラットフォーム管理セクションへの読み取りおよび書き込みアクセス権があります。オブザーバユーザーには読み取りアクセス権のみがあります。

データプラットフォームの主なエリアは次のとおりです。

- [Collectors]：さまざまなネットワークテレメトリとコンテキストデータをリアルタイムで収集します。データが取り込まれると、Catalyst Center はデータを関連付けて分析します。コレクタのステータスを表示し、問題領域をすばやく見分けることができます。コレクタの設定情報の表示または更新 （1734 ページ）を参照してください。
- [ストアの設定（Store Settings）]：アプリケーションのデータの保存期間を示します。データ保持設定の表示 （1735 ページ）を参照してください。
- [Pipelines]：Catalyst Center アプリケーションが、ストリーミングデータを処理できるようにします。データパイプラインは、一連の計算全体をカプセル化します。これらの計算は、外部ソースからの入力データを受け入れ、有用な情報を提供するためにそのデータを変換し、出力データを生成します。パイプラインのステータスを表示し、問題領域をすば

やく見分けることができます。パイプラインステータスの表示（1735 ページ）を参照してください。

- [タスクマネージャ（Task Managers）]：タスクマネージャのリストを、最後のハートビート、すべてのスロット、空きスロットなどの詳細情報とともに表示できます。この詳細情報は CSV ファイルとしてエクスポートできます。

コレクタの設定情報の表示または更新

コレクタは、さまざまなネットワークテレメトリおよびコンテクスチュアルデータをリアルタイムで収集します。データが取り込まれると、Catalyst Center はデータを関連付けて分析します。コレクタのステータスを表示し、問題領域をすばやく見分けることができます。

手順

ステップ 1 メインメニューから次を選択します。**[System]** > **[Data Platform]**。

ステップ 2 [Collectors] をクリックします。各コレクタの横にある点は、全体的なステータスを示しています。

ステップ 3 追加の詳細を表示するには、コレクタ名をクリックします。

適切な *[Collector]* ページが表示されます。デフォルトでは、Catalyst Center に [設定（Configuration）] タブが表示され、現在の設定リストを確認できます。

ステップ 4 構成を表示、更新、または削除するには、特定の構成名をクリックします。

ステップ 5 新規の設定を追加するには、**[Configuration]** タブで **[+ Add]** をクリックします。

ステップ 6 設定に必要な情報をスライドインペインに入力します。

ステップ 7 （任意） ワイヤレスコレクタなどの一部のコレクタでは、[Anonymize] チェックボックスをオンにして、[Client Health] ウィンドウに表示されるホスト名とユーザー ID を、復号化できない一方向ハッシュを用いてスクランブル処理することができます。



重要 データを匿名化する場合は、**[Discovery]** ツールを使用してデバイスを検出する前に、**[Anonymize]** チェックボックスをオンにしてください。デバイスを検出した後にデータを匿名化した場合、システムに入ってくる新しいデータは匿名化されますが、既存のデータは匿名化されません。

ステップ 8 [Save Configuration] をクリックします。

ステップ 9 設定されているインスタンスを表示するには、[Instances] タブをクリックします。

ステップ 10 概要情報とメトリックを表示するには、リストからインスタンスを選択します。

ステップ 11 （任意） Catalyst Center を Connected Mobile Experience（CMX）と統合する場合は、CMX 側でデータの匿名化を選択できます。次の手順を実行します。

a) SSH クライアントを使用して、cmxadmin CLI ユーザーとして CMX にログインします。

b) ルートユーザに変更します。

c) /opt/cmx/etc/node.conf に移動し、[location] の下に **user_options** を追加します。次に例を示します。

```
[location]
…
user_options=-Dhideusername=true
```

d) CMX CLI で、次のコマンドを入力します。

```
cmxctl agent restart
cmxctl location restart
```

データ保持設定の表示

アプリケーションのデータの保存期間を表示できます。

手順

ステップ 1 メインメニューから次を選択します。**[System]** > **[Data Platform]**。

ステップ 2 [Store Settings] をクリックします。

ステップ 3 完了した履歴消去ジョブのリストを表示するには、[Data Purge Schedule] をクリックします。

[履歴（HISTORY）] テーブルには、消去ジョブの名前、結果、時刻、などのデータが表示されます。テーブル内のデータをソート、フィルタリング、エクスポートすることができます。

ステップ 4 現在のデータの保持または消去の設定を表示するには、[Data Retention & Purge Configuration] をクリックします。

[メトリックグラフストア（Metric Graph Store）] オプションが表示されます。最大サイズ、ウォーターマークの下限および上限しきい値など、すべての時間ベースのグラフィカルデータの設定を表示します。

パイプラインステータスの表示

データ パイプラインによって、Catalyst Center アプリケーションは、ストリーミング データを処理できます。データパイプラインは、一連の計算をカプセル化します。外部ソースからの入力データを受け入れ、インテリジェンスを提供するためにそのデータを変換し、出力データを生成します。パイプラインのステータスを表示し、問題領域をすばやく見分けることができます。

手順

ステップ 1 メインメニューから次を選択します。**[System]** > **[Data Platform]**。

ステップ 2 [Pipelines] をクリックします。

ステップ 3 アプリケーションが基盤となるパイプラインからデータを受信しているかどうかを表示するには、パイプライン名をクリックします。

適切な *[*パイプライン（*Pipeline*）*]* ページが、次のタブとともに表示されます。

（注） [Exceptions] タブをクリックして、パイプラインで例外が発生していないかどうかを確認してください。通常の動作状況では、このタブは **null** を表示します。

- [メトリック（Metrics）]： 30 分ごとに更新されるメトリックを表示します。
- [サマリ（Summary）]：統計、ランタイム、マニフェストなどのサマリ情報を表示します。
- **例外**：パイプラインで発生した例外を表示します。
- **ステージ**：パイプラインのステージを表示します。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。