



Cisco DNA Center リリース 1.3.1.0 ユーザガイド

初版：2019年9月4日

最終更新：2019年10月22日

シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先：シスココンタクトセンター

0120-092-255（フリーコール、携帯・PHS含む）

電話受付時間：平日 10:00～12:00、13:00～17:00

<http://www.cisco.com/jp/go/contactcenter/>

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

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

© 2019 Cisco Systems, Inc. All rights reserved.



目次

第 1 章	新機能および変更された機能に関する情報 1
	新機能および変更された機能に関する情報 1

第 2 章	Cisco DNA Center について 3
	Cisco DNA Center の概要について 3
	ログイン 3
	ネットワーク管理者として初回ログイン 4
	デフォルト ホームページ 5
	グローバル検索の使用 10
	ローカリゼーションの有効化 11
	開始位置 12

第 3 章	ネットワークの検出 13
	ディスカバリについて 13
	検出ダッシュボード 14
	ディスカバリの前提条件 14
	ディスカバリ クレデンシャル 15
	クレデンシャルと Cisco ISE のディスカバリ 16
	ディスカバリ クレデンシャルのガイドラインと制約事項 16
	ディスカバリ クレデンシャルの例 17
	優先管理 IP アドレス 18
	設定のガイドラインと制限事項のディスカバリ 18
	ディスカバリの実行 19
	CDP を使用したネットワークの検出 19

Discover Your Network Using an IP Address Range	25
LLDP を使用したネットワークの検出	30
検出ジョブの管理	36
ディスカバリ ジョブの停止および開始	36
ディスカバリ ジョブの編集	36
ディスカバリ ジョブでクレデンシャルを変更	37
ディスカバリ ジョブの複製	40
ディスカバリ ジョブの削除	40
ディスカバリ ジョブ情報の表示	41

第 4 章

インベントリの管理	43
インベントリについて	43
インベントリと Cisco ISE の認証	44
インベントリに関する情報の表示	45
インベントリからのトポロジマップの起動	49
Cisco DNA Center インベントリ内のデバイスのタイプ	49
ネットワーク デバイスの管理	50
ネットワーク デバイスを追加	50
ネットワーク デバイス クレデンシャルの更新	53
計算デバイスの管理	57
計算デバイスの追加	57
計算デバイス クレデンシャルの更新	60
Meraki ダッシュボードの管理	61
Meraki ダッシュボードの統合	61
Meraki ダッシュボード クレデンシャルの更新	61
デバイスのフィルタ	62
デバイスのロールの変更 (インベントリ)	63
デバイスの管理 IP アドレスの更新	64
デバイスの再同期間隔の更新	65
デバイス情報の再同期	66
ネットワーク デバイスの削除	66

コマンドランナーを起動 (インベントリ)	67
CSV ファイルを使用してデバイス設定をインポート/エクスポートします。	67
CSV ファイルからのデバイス設定のインポート	69
デバイス設定のエクスポート	69
Export Device Credentials	70
故障したデバイスの交換	71
Cisco DNA Center での RMA ワークフローの制限事項 Cisco DNA Center	72

第 5 章

ソフトウェア イメージの管理	75
イメージリポジトリについて	75
ソフトウェア イメージの整合性検証	76
ソフトウェア イメージの表示	76
推奨されるソフトウェア イメージの使用	77
ソフトウェア イメージのインポート	77
デバイスファミリへのソフトウェアイメージの割り当て	78
デバイスのソフトウェア イメージをインストールモードでアップロード	79
ゴールデン ソフトウェアのイメージについて	80
ゴールデン ソフトウェア イメージの指定	80
ソフトウェア イメージのプロビジョニング	81
デバイスのアップグレードの準備の事前チェック リスト	82
Auto Flash Cleanup	83

第 6 章

ネットワーク トポロジを表示	85
トポロジについて	85
エリア、サイト、ビルディング、フロアのトポロジを表示	86
トポロジマップでデバイスをフィルタリング	87
デバイス情報の表示	88
リンク情報の表示	89
トポロジマップにデバイスをピン留めする	89
サイトへのデバイスの割り当て	90
トポロジマップ レイアウトの保存	90

トポロジマップ レイアウトを開く	91
トポロジのレイアウトをエクスポート	91

第 7 章

ネットワーク階層と設定を設計 93

新しいネットワーク インフラストラクチャの設計	94
About Network Hierarchy	94
マップ内で使用するイメージファイルに関するガイドライン	95
ネットワーク階層のサイトの作成	95
Cisco Prime Infrastructure からサイト階層をエクスポートして Cisco DNA Center にインポートする	96
既存のサイト階層をアップロード	97
Search the Network Hierarchy	99
サイトの編集	99
サイトの削除	99
ビルディングの追加	99
ビルディングの編集	100
ビルディングの削除	100
ビルディングへのフロアの追加	101
フロアの編集	102
フロア マップのモニタリング	102
フロア要素とオーバーレイの編集	103
アクセス ポイントの配置に関するガイドライン	103
AP の追加、配置、および削除	104
AP のクイック ビュー	106
センサーの追加、配置、および削除	107
カバレッジ エリアの追加	108
障害物の作成	109
ロケーション リージョンの作成	110
フロア マップ上に包含領域と除外領域を配置するためのガイドライン	110
フロア上の包含リージョンの定義	111
フロア上の除外リージョンの定義	111

ロケーションリージョンの編集	112
ロケーションリージョンの削除	112
レールの作成	112
マーカーの配置	113
フロア ビュー オプション	114
アクセスポイントの表示オプション	114
View Options for Sensors	116
オーバーレイオブジェクトの表示オプション	116
マッププロパティの設定	116
グローバルマッププロパティの設定	117
データのフィルタリング	117
アクセスポイントデータのフィルタ処理	117
センサーデータのフィルタ処理	117
ゼロデイ Ekahau 計画ワークフロー	118
Cisco DNA Center への Ekahau プロジェクトのインポート	119
インタラクティブフロアプランニングについて	120
インタラクティブフロアプランニング	120
グローバルワイヤレス設定の構成	122
エンタープライズワイヤレスネットワーク用 SSID の作成	122
事前共有キーのオーバーライド	126
ゲストワイヤレスネットワークの SSID の作成	127
ゲストポータルページの作成	131
ワイヤレスインターフェ이스の作成	133
ワイヤレス無線周波数プロファイルの作成	133
バックホール設定の管理	136
Cisco Connected Mobile Experiences の統合について	137
Cisco CMX 設定の作成	138
Flex グループのネイティブ VLAN 設定	139
ネットワークプロファイルの作成	140
NFVIS 用のネットワークプロファイルの作成	140
ルーティング用のネットワークプロファイルの作成	142

スイッチ用のネットワークプロファイルの作成	144
ワイヤレス用のネットワークプロファイルの作成	145
グローバル ネットワーク設定について	146
デバイス クレデンシヤルについて	147
CLI クレデンシヤル	147
SNMPv2c のクレデンシヤル	147
SNMPv3 のクレデンシヤル	148
HTTPS クレデンシヤル	149
グローバル デバイス クレデンシヤルについて	149
グローバル CLI クレデンシヤルの設定	150
グローバル SNMPv2c クレデンシヤルの設定	151
グローバル SNMPv3 クレデンシヤルの設定	152
グローバル HTTPS クレデンシヤルの設定	154
グローバルデバイスのログイン情報の編集に関する注意事項	155
グローバル デバイス クレデンシヤルの編集	156
デバイス クレデンシヤルのサイトへの関連付け	157
IP アドレス プールを設定する	158
IP アドレスマネージャから IP アドレスプールをインポートする	158
CSV ファイルから IP アドレスプールをインポートする	159
IP プールの予約	159
IP プールの編集	160
IP プールの複製	161
IP プールのリリース	161
サービス プロバイダー プロファイルの設定	161
グローバル ネットワーク サーバの設定	162
Cisco ISE またはその他の AAA サーバの追加	163

第 8 章	デバイスの診断コマンドを実行	165
	コマンドランナーについて	165
	デバイスの診断コマンドを実行	165

第 9 章	デバイス設定の変更を自動化するテンプレートの作成	167
	テンプレートエディタについて	167
	プロジェクトの作成	167
	テンプレートの作成	168
	標準テンプレートの作成	168
	ブラックリストに登録されたコマンド	170
	サンプルテンプレート	170
	複合テンプレートの作成	171
	テンプレートの編集	172
	テンプレートのシミュレーション	173
	テンプレートフォームエディタ	174
	変数バインド	175
	特別なキーワード	176
	ネットワークプロファイルへのテンプレートの関連付け	178

第 10 章	テレメトリ プロファイルの設定	181
	テレメトリについて	181
	テレメトリ プロファイルの設定	181
	デバイスにテレメトリ プロファイルを適用	182
	新しいクラスタ仮想 IP アドレスを使用するためのテレメトリプロファイルの更新	184

第 11 章	ネットワーク セキュリティ アドバイザリの識別	187
	セキュリティアドバイザリの概要	187
	セキュリティアドバイザリの表示	187

第 12 章	ポリシーの設定	191
	ポリシーの概要	191
	グループベースのアクセス コントロール ポリシー	191
	ポリシー作成の概要	195
	スケーラブルグループの作成	196

アクセス契約の作成	197
グループベースのアクセス コントロール ポリシーの作成	199
IP ベースのアクセス コントロール ポリシー	202
IP ベースのアクセス コントロール ポリシー設定のワークフロー	202
グローバル ネットワーク サーバの設定	203
IP ネットワーク グループの作成	204
IP ネットワーク グループの編集または削除	205
IP ベースのアクセス コントロール契約の作成	205
Edit or Delete an IP-Based Access Control Contract	206
IP ベースのアクセス コントロール ポリシーの作成	206
IP ベースのアクセス コントロール ポリシーの編集または削除	208
IP ベースのアクセス コントロール ポリシーの展開	209
アプリケーション ポリシー	209
アプリケーション ポリシーでの CVD ベースの設定	210
サイトの範囲	210
ビジネス関連のグループ	211
コンシューマとプロデューサ	212
マーキング、キューイング、ドロップिंगの処理	212
サービス プロバイダーのプロファイル	214
キューイング プロファイル	216
リソースが制限されているデバイスの処理順	218
ポリシーのドラフト	220
ポリシーのプレビュー	221
ポリシーの事前チェック	221
ポリシーのスケジューリング	222
ポリシーのバージョン管理	222
オリジナル ポリシーの復元	223
陳腐化したアプリケーション ポリシー	223
アプリケーション ポリシーのガイドラインと制限事項	224
アプリケーション ポリシーの管理	225
前提条件	225

アプリケーション ポリシーを作成します。	225
View Application Policy Information	229
アプリケーション ポリシーの編集	230
アプリケーション ポリシーのドラフトの保存	231
アプリケーション ポリシーの展開	232
ポリシー導入のキャンセル	232
アプリケーション ポリシーの削除	233
アプリケーション ポリシーの複製	233
アプリケーション ポリシーの復元	234
デフォルトの CVD アプリケーション ポリシーをリセット	235
アプリケーション ポリシーのプレビュー	235
アプリケーション ポリシーの事前チェック	236
アプリケーション ポリシー履歴の表示	236
ポリシーの以前のバージョンにロールバック	237
キューイング プロファイルの管理	237
キューイング プロファイルの作成	237
キューイング プロファイルの編集または削除	238
WAN インターフェイスのアプリケーション ポリシーの管理	239
サービス プロバイダー プロファイルの SLA 属性をカスタマイズ	239
サービス プロバイダー プロファイルの WAN インターフェイスへの割り当て	240
トラフィック コピー ポリシー	241
送信元、宛先、およびトラフィックのコピー先	241
トラフィック コピー ポリシーの注意事項と制限事項	242
トラフィック コピー ポリシー設定のワークフロー	243
トラフィック コピーの宛先の作成	243
トラフィック コピーの宛先の編集または削除	244
トラフィック コピー契約の作成	244
トラフィック コピー契約の編集または削除	244
トラフィック コピー ポリシーの作成	245
Edit or Delete a Traffic Copy Policy	245
仮想ネットワーク	245

仮想ネットワークに関する注意事項と制限事項 246

ゲスト アクセス用の複数の仮想ネットワーク 246

仮想ネットワークの作成 246

仮想ネットワークの編集または削除 247

第 13 章

ネットワークのプロビジョニング 249

プロビジョニング 249

プラグアンドプレイ プロビジョニングを使用したオンボードデバイス 250

コントローラ ディスカバリの前提条件 252

DHCP コントローラ ディスカバリ 252

DNS コントローラ ディスカバリ 254

Plug and Play Connect コントローラ ディスカバリ 254

デバイスの表示 255

デバイスの追加または編集 258

Add Devices in Bulk 259

バーチャルアカウント プロファイルの登録または編集 260

スマートアカウントからのデバイスの追加 261

プラグアンドプレイを使用したデバイスのプロビジョニング 262

スイッチまたはルータ デバイスのプロビジョニング 262

ワイヤレスまたはセンサー デバイスのプロビジョニング 267

デバイスの削除 271

デバイスのリセット 271

インベントリ内のデバイスの管理 272

デバイスをサイトに追加する 273

デバイスのタグ付け 273

ルールを使用してデバイスにタグ付けする 274

デバイスタグの編集 275

[タグの削除 (Delete Tags)] 275

デバイスのプロビジョニング 276

Cisco Wireless Controller をプロビジョニングする 276

Cisco DNA Center からのシスコ WLC 高可用性の設定 Cisco DNA Center 279

ルーティングおよびNFVプロファイルのプロビジョニング	281
VPC インベントリ収集	283
シスコ製 AP のプロビジョニング : Day 1 AP プロビジョニング	284
ブラウフィールド デバイスのプロビジョニング	285
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの設定とプロビジョニング	288
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの概要	288
Cisco DNA Center で Cisco Catalyst 9800 ワイヤレスコントローラを設定するためのワークフロー	293
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラでのソフトウェアイメージのアップグレードのサポート	297
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラで高可用性を設定する	298
N+1 高可用性	301
モビリティ設定の概要	306
N+1 ローリング AP アップグレードについて	308
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのプロビジョニング	311
Catalyst 9000 シリーズ スイッチ用 Cisco Catalyst 9800 組み込みワイヤレスコントローラの設定とプロビジョニング	314
サポートされているハードウェア プラットフォーム	314
事前設定	315
Catalyst 9000 スイッチ用 Cisco Catalyst 9800 組み込みワイヤレスコントローラを設定するためのワークフロー	316
Cisco Catalyst 9000 シリーズ スイッチでの組み込みワイヤレスのプロビジョニング	318
Cisco Catalyst 9000 シリーズスイッチに Catalyst 9800 組み込みワイヤレスを搭載したファブリックインアボックス	321
ファブリックインアボックスに関する情報	321
拡張性に関する情報	321
リリース間コントローラモビリティの概要	322
ゲスト アンカーの設定とプロビジョニング	323
IRCM : Cisco AireOS コントローラと Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ	324
LAN アンダーレイのプロビジョニング	325
LAN 自動化のピアデバイスの使用事例	329

LAN 自動化の状態を確認	330
プロビジョニング後のデバイスの削除	331
ファブリック サイトとファブリック ドメイン	331
マルチサイトファブリック ドメイン	332
トランジット サイト	332
IP のトランジット ネットワークの作成	333
SDA トランジット ネットワークの作成	333
ファブリック ドメインの設定	334
ファブリックの概要	334
ファブリック ドメインの作成	334
ファブリックの準備状況とコンプライアンスのチェック	335
ファブリック ドメインの設定	336
ファブリックへのデバイスの追加	336
ボーダーノードとしてのデバイスの追加	338
ホスト オンボーディングの設定	340
認証テンプレートを選択	341
ファブリック ドメインへの仮想ネットワークの関連付け	341
ファブリック ドメインのワイヤレス SSID の設定	343
ファブリック ドメイン内のポートの設定	343
拡張ノードの設定	343
ポートチャネルの設定	345
マルチキャスト概要	347
マルチキャスト設定の構成	347
Applications	351
アプリケーションおよびアプリケーションセット	351
単方向と双方向のアプリケーション トラフィック	351
カスタム アプリケーション	352
お気に入りのアプリケーション	352
アプリケーションおよびアプリケーションセットの設定	353
アプリケーション設定の変更	353
サーバ名に基づくカスタム アプリケーションの作成	354

IP アドレスおよびポート ベースのカスタム アプリケーションの作成	355
URL に基づくカスタム アプリケーションの作成	356
カスタム アプリケーションの編集または削除	356
アプリケーションをお気に入りにする	357
カスタム アプリケーション設定の作成	358
カスタム アプリケーション セットの編集または削除	358
アプリケーション ホスティング	359
アプリケーション ホスティングについて	359
アプリケーション ホスティングの前提条件	359
アプリケーションをホストするデバイスの準備状況の表示	359
アプリケーションの追加	360
Cisco Catalyst 9300 デバイスへのアプリケーションのインストール	360
アプリケーションの更新	361
Cisco Catalyst 9300 デバイスからのアプリケーションのアンインストール	362
アプリケーションの削除	362
アプリケーションログのダウンロード	363
デバイスのテクニカルサポートログのダウンロード	363

第 14 章
Cisco DNA アシュアランス 365

Cisco DNA アシュアランス	365
-------------------	-----

第 15 章
データプラットフォームを使用した Cisco DNA Center のトラブルシューティング 367

データプラットフォームについて	367
分析 Ops センターを使用したトラブルシューティング	368
コレクタの設定情報の表示または更新	370
データ保持設定の表示	371
パイプライン ステータスの表示	371



第 1 章


新機能および変更された機能に関する情報

- [新機能および変更された機能に関する情報 \(1 ページ\)](#)

新機能および変更された機能に関する情報

次の表に、新機能および変更された機能の要約と参照先を示します。

表 1: Cisco DNA Center、リリース 1.3.1.0 の新機能および変更された機能

機能	説明	参照先
APSP および APDP のアップグレード	AP サービスパック (APSP) と AP デバイスパック (APDP) は、ワイヤレスコントローラに関連付けられた AP をアップグレードするためのイメージです。	ソフトウェア イメージの表示 (76 ページ)
ネットワーク階層	マップ内のサイトマーカーをクリックし、[Show Floor] オプションを選択すると、任意のサイトのフロアに直接移動できます。 左側のペインのサイトの横にある  アイコンをクリックし、[View Devices] オプションを選択することで、任意のサイトに割り当てられているデバイスを表示できます。これにより、各サイトに基づいてデバイスリストがオートフィルタされている [Provision] ページが表示されます。	—
障害のあるデバイスの交換	障害のあるデバイスに交換のマークを付けて、インベントリを介して追加された交換用デバイスを選択することで、 [Provision] > [Inventory] ページで障害のあるデバイスを交換できます。返品許可 (RMA) ワークフローが開始されます。この方法で交換用デバイスを展開すると、交換用デバイスは古いデバイスのように動作します。	故障したデバイスの交換 (71 ページ)
4 バイトの ASN サポート	Cisco DNA Center Cisco DNA Center には、ASPLAIN、ASDOT、または ASDOT+ 表記で L3 ハンドオフ時にローカル自律番号を保存するオプションがあります。	ボーダーノードとしてのデバイスの追加 (338 ページ)

機能	説明	参照先
プラグアンドプレイ プロビジョニング	一括プロビジョニングでは、ワイヤレスデバイスをプロビジョニングするために必要な追加のデータフィールドがサポートされています。要求プロセス中にデバイス名を変更でき、デフォルトのデバイスホスト名として使用されます。要求ユーザインターフェイスには、プロセスを容易にするための複数の改良が加えられています。スタックブルスイッチでは、2番目のスタックケーブル配線方式がサポートされています。	プラグアンドプレイプロビジョニングを使用したオンボードデバイス (250 ページ)
セキュリティアドバイザリ	セキュリティアドバイザリ ツールは、Cisco Product Security Incident Response Team (PSIRT; プロダクトセキュリティ インシデント レスポンス チーム) によって推奨されるセキュリティアドバイザリをキャプチャして一覧表示します。このツールを使用するには、機械推論パッケージをインストールする必要があります。アドバイザリは、デバイスに現在インストールされているソフトウェアイメージに基づいて照合されます。	セキュリティアドバイザリの表示 (187 ページ)
アプリケーションの可視性サービス：アプリケーションとアプリケーションセット	アプリケーションとアプリケーションセットは、[Policy] > [Application Policy] から [Provision] > [Services] > [Application Visibility] に移動しました。	アプリケーションおよびアプリケーションセットの設定 (353 ページ)
アプリケーション ホスティング	アプリケーション ホスティングを使用すると、Cisco IOS XE ソフトウェアバージョン 16.12.1s を搭載した Catalyst 9300 シリーズ スイッチのサードパーティ製 docker アプリケーションを利用できます。	アプリケーション ホスティングについて (359 ページ)
テレメトリプロファイルの拡張機能	このリリースでは、アプリケーションの可視性プロファイルのサポートが導入されました。	テレメトリ プロファイルの設定 (181 ページ)
デバイスタグの拡張機能	新しい拡張機能を使用すると、デバイスまたはテンプレートに関連付けられていないデバイスタグまたはテンプレートタグを削除できます。	デバイスのタグ付け (273 ページ)
IP プールを複製する機能	サイトレベルで既存の IP プールを複製できます。IP プールを複製すると、DHCP サーバと DNS サーバの IP アドレスが自動的に入力されます。	IP プールの複製 (161 ページ)



第 2 章

Cisco DNA Center について

- [Cisco DNA Center の概要について \(3 ページ\)](#)
- [ログイン \(3 ページ\)](#)
- [ネットワーク管理者として初回ログイン \(4 ページ\)](#)
- [デフォルト ホームページ \(5 ページ\)](#)
- [グローバル検索の使用 \(10 ページ\)](#)
- [ローカリゼーションの有効化 \(11 ページ\)](#)
- [開始位置 \(12 ページ\)](#)

Cisco DNA Center の概要について

Cisco Digital Network Architecture は、設計、プロビジョニング、ネットワーク環境全体へのポリシーの適用を迅速かつ容易にする一元化された使いやすい管理機能を提供します。Cisco DNA Center GUI は、エンドツーエンドネットワークの可視性を提供するとともに、ネットワークの情報を使用してネットワークのパフォーマンスを最適化し、最善のユーザおよびアプリケーションエクスペリエンスを実現します。

ログイン

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

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

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

`https://server-ip`

例 : `https://192.0.2.1`

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

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

使用しているユーザ ID に NETWORK-ADMIN-ROLE が割り当てられていて、同じ権限を持つ他のユーザが先にログインしていない場合、ホームページではなく初回セットアップウィザードが表示されます。詳細については、[ネットワーク管理者として初回ログイン \(4 ページ\)](#) を参照してください。

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

ネットワーク管理者として初回ログイン

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

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

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

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

始める前に

ウィザードを完了するには、以下の情報が必要です。

- SYSLOG サーバと SNMP サーバの IP アドレス
- Netflow サーバの IP アドレスとポート
- ディスカバリ : 開始する IP アドレス (CDP ディスカバリを選択している場合) または開始と終了の IP アドレス (範囲ディスカバリを選択している場合)

- オプション：優先される管理 IP アドレス
- デバイス CLI クレデンシヤル（イネーブル パスワードなど）
- SNMP v2c クレデンシヤル（read コミュニティ ストリングなど）

ステップ 1 ログイン (3 ページ) の説明に従って、通常の手順で Cisco DNA Center にログインします（まだログインしていない場合）。

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

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

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

前の画面に戻るには、[Back] をクリックします。

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

[Device Controllability] はデフォルトで有効になっています。[Disable] をクリックして、デバイスの制御性を無効にできます。

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

デフォルト ホームページ

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

[Summary]アシュアランス エリアには次の内容が含まれます。

- [Health]：ネットワークデバイス、有線クライアント、ワイヤレスクライアントを含む、企業全体の正常性スコアが提供されます。[View Details] をクリックすると、[Overall Health] ウィンドウが表示されます。
- [Critical Issues]：P1 と P2 の問題の数が表示されます。[View Details] をクリックすると、[Open Issues] ウィンドウが表示されます。
 - [P1]：ネットワーク運用に幅広い影響を与える可能性がある、早急な対応を必要とする重大な問題。
 - [P2]：複数のデバイスまたはクライアントに影響を与える可能性がある主要な問題。
- [Trends and Insights]：ネットワークのパフォーマンスに関するインサイトが提供されます。[View Details] をクリックすると、[Network Insights] ウィンドウが表示されます。

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

- [サイト (Sites)] : ネットワーク上で検出されたサイトの数と、DNS サーバおよび NTP サーバの数が示されます。[Add Sites] をクリックすると、[Add Site] ウィンドウが表示されます。
- [ネットワークデバイス (Network Devices)] : ネットワーク上で検出されたネットワークデバイスの数と、要求されていないデバイス、プロビジョニングされていないデバイス、および到達不能なデバイスの数が示されます。[Find New Devices] をクリックすると、[New Discovery] ウィンドウが表示されます。
- [アプリケーションポリシー (Application policies)] : ネットワーク上で検出されたアプリケーションポリシーの数と、成功およびエラーになった展開の数を表示します。[Add New Policy] をクリックすると、[Application Policies] ウィンドウが表示されます。
- [ネットワークプロファイル (Network Profiles)] : ネットワーク上で検出されたプロファイルの数を示します。[Manage Profiles] をクリックすると、[Network Profiles] ウィンドウが表示されます。
- [イメージ (Images)] : ネットワーク上で検出されたイメージの数と、タグなしイメージおよび未検証イメージの数が示されます。[Import Images/SMUs] をクリックすると、[Image Repository] ウィンドウが表示されます。
- [Licensed Devices] : Cisco DNA Center ライセンスを持つデバイスの数と、スイッチ、ルータ、およびアクセスポイントの数が示されます。[Manage Licenses] をクリックすると、[License Management] ウィンドウが表示されます。

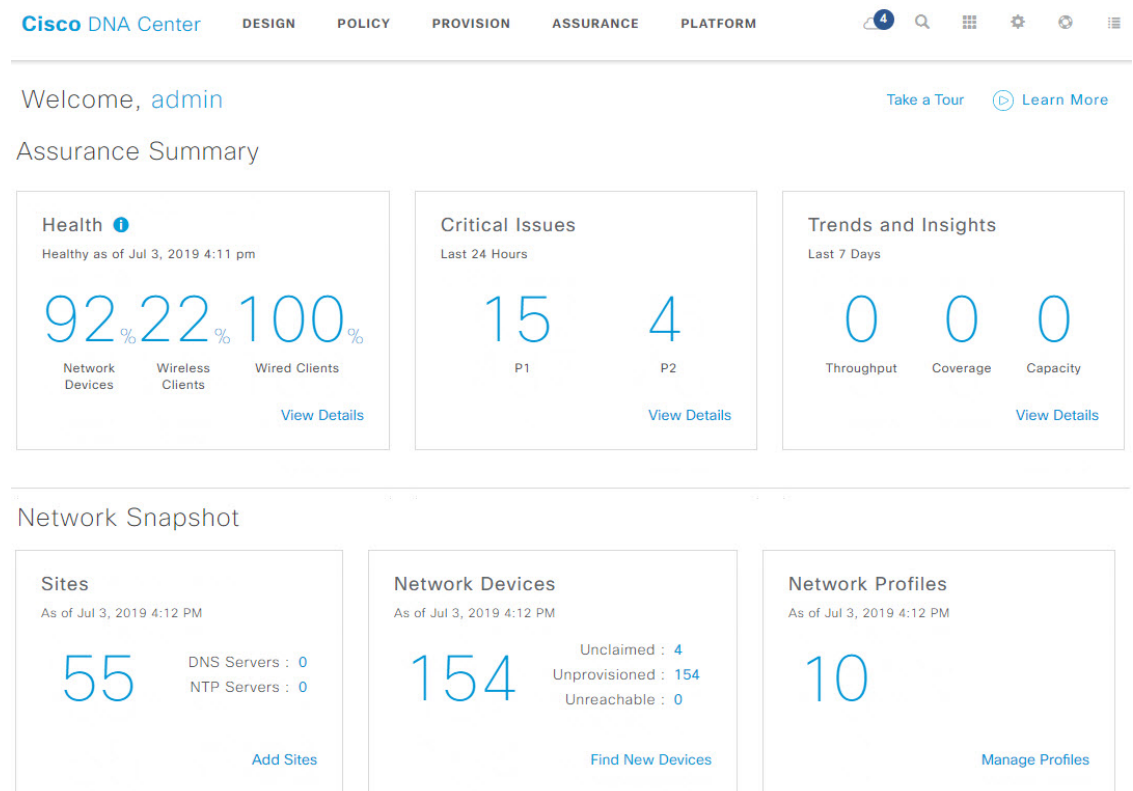
[Network Configuration] エリアには次の内容が含まれます。

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

- **[Platform]** : インテント API を使用してネットワークにプログラムでアクセスできます。最適な IT システムと統合してエンドツーエンドのソリューションを作成し、マルチベンダーデバイスのサポートを追加できます。

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

図 1: Cisco DNA Center ホームページ



ホームページのさまざまなビュー :

使用する前に

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

In a few simple steps, discover your devices to begin your Cisco DNA Center journey!

Get Started

初めてオペザバーとして Cisco DNA Center にログインすると、次のメッセージが表示されます。

Ask your Network Administrator to add Network Devices to gather Assurance data.

0 日目のホームページ

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

Welcome, admin Get Started Take a Tour Learn More

In order to gather Assurance data and calculate your network health, we'll need to discover or import your network devices.

Network Snapshot

Add Sites

[+](#)

Network Devices
As of December 19, 2018 4:31 PM

0

Unclaimed : 0
Unprovisioned : 0
Unreachable : 0

[Find New Devices](#)

Network Profiles
As of Dec 19, 2018 4:31 PM

0

[Manage Profiles](#)

Import Images/SMUs

[+](#)

DNA Licensed Devices
As of Dec 19, 2018 4:31 pm

0

Switches : 0
Routers : 0
Access Points : 0

[Manage Licenses](#)




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

We've discovered 10 devices in your network. [View Discovery](#)

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

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

アイコン	説明
	[Software Updates] : 利用可能なソフトウェアアップデートのリストが表示されます。 [Go to Software Updates] リンクをクリックすると、システムとアプリケーションのアップデートを表示できます。
	[Search] : デバイス、ユーザ、ホスト、およびその他の項目が保存されている Cisco DNA Center データベース内の任意の場所で、それらを検索します。を参照してください。検索の使用に関するヒントについては、 グローバル検索の使用 (10ページ) を参照してください。
	[Tools] : 使用可能なツールにアクセスします。

アイコン	説明
	[Settings] : システム設定の構成、監査ログの表示、ログインしたユーザ名の表示、およびログアウトを行います。
	<p>ヘルプ :</p> <ul style="list-style-type: none"> • [About] : 現在の Cisco DNA Center のソフトウェアバージョンを表示します。 [Release Notes] をクリックして、別のブラウザタブでリリースノートを開始します。 [Packages] をクリックして、システムおよびアプリケーションパッケージのバージョンを表示します。 [Serial number] をクリックして、Cisco DNA Center アプライアンスのシリアル番号を表示します。 • [API Reference] : Cisco DevNet で Cisco DNA Center プラットフォーム API ドキュメンテーションを開きます。 • [Developer Resources] : Cisco DevNet を開くと、開発者ツールにアクセスできます。 • [Help] : 状況依存オンラインヘルプをブラウザの別のタブに表示します。 • [Contact Support] : Cisco Technical Assistance Center (TAC) でサポートケースを開きます。 • [Make a Wish] : コメントや提案を Cisco DNA Center 製品チームに送信します。
	<p>[Notifications] : 最近スケジュールされたタスクやその他の通知を表示します。</p> <p>(注) 通知アイコンの横に色のバッジが表示される場合があります。バッジは、タスクまたは通知の変更を示します。青色のバッジは、新しい通知、新しいタスク、または成功したタスクを示します。赤色のバッジは、失敗したタスクを示します。</p>

Cisco DNA Center を初めて使用する場合は、[開始位置 \(12 ページ\)](#) で使い方のヒントや提案を参照してください。



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

グローバル検索の使用

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

- [アクティビティ (Activities)] : Cisco DNA Center のメニュー項目、ワークフロー、および機能を名前で検索します。
- アプリケーション : 名前で検索します。
- アプリケーショングループ : 名前で検索します。
- ホストおよびエンドポイント : 名前、IP アドレスまたは MAC アドレスで検索します。
- IP プール : 名前または IP アドレスでそれらを検索します。
- ネットワーク デバイス : 名前、IP アドレス、シリアル番号、ソフトウェア バージョン、プラットフォーム、製品ファミリー、または MAC アドレスで検索します。
- サイト : 名前で検索します。
- [ユーザ (Users)] : ユーザ名で検索します。大文字と小文字は区別されません。ユーザ名のサブストリング検索はサポートされていません。
- 新しいバージョンの Cisco DNA Center として別のアイテムがリリースされます。

グローバル検索を開始するには、Cisco DNA Center ページの右上隅にある 🔍 アイコンをクリックします。Cisco DNA Center にポップアップグローバル検索ウィンドウが表示されます。[Search] フィールドに、検索する項目に関する識別情報を入力します。

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

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

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

検索文字列にさらに多くの文字を追加すると、グローバル検索で表示されるカテゴリおよび項目の表示リストが自動的に絞り込まれます。

概要パネルには、詳細へのリンクが表示されます。リンクはカテゴリおよび項目ごとに必要に応じて変わります。例：アクティビティの場合、概要パネルには Cisco DNA Center システム以

外のメニュー項目およびワークフローへのリンクが表示されます。アプリケーションの場合、[アプリケーション360 (Application 360)]ビューが表示されます。ホスト/エンドポイントの場合は[クライアント360 (Client 360)]ビューと[トポロジ (Topology)]ビューへのリンクが表示され、ネットワーク デバイスの場合は[デバイス360 (Device 360)]ビューと[トポロジ (Topology)]ビューへのリンクが表示されます。リンクをクリックすると、適切なメニュー項目、ワークフロー、または詳細ビューが表示されます。

完了したら、✖ をクリックしてウィンドウを閉じます。

グローバル検索では、一度に最大 500 の結果を表示できます。

ローカリゼーションの有効化

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



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

デフォルトの言語を変更するには、次のタスクを実行します。

- ステップ 1 ブラウザで、サポートされている言語 (中国語、日本語、または韓国語) のいずれかにロケールを変更します。
- ステップ 2 Cisco DNA Center にログインします。
GUI 画面は、選択した言語で表示されます。

図 2: ローカライズされたログイン画面の例



開始位置

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

設定後、現在の環境で Cisco DNA Center の使用を開始する方法を決定します。

- 既存のインフラストラクチャ：既存のインフラストラクチャ（ブラウнフィールド導入）があれば、ディスカバリを実行して開始します。ディスカバリを実行すると、すべてのデバイスが **[インベントリ (Inventory)]** ウィンドウに表示されます。ディスカバリの実行の詳細については、[ネットワークの検出 \(13 ページ\)](#) を参照してください。
- 新規または存在しないインフラストラクチャ：既存のインフラストラクチャがなく、ゼロから開始（新規導入）する場合は、ネットワーク階層を作成します。



第 3 章

ネットワークの検出

- ディスカバリについて (13 ページ)
- 検出ダッシュボード (14 ページ)
- ディスカバリの前提条件 (14 ページ)
- ディスカバリ クレデンシャル (15 ページ)
- 優先管理 IP アドレス (18 ページ)
- 設定のガイドラインと制限事項のディスカバリ (18 ページ)
- ディスカバリの実行 (19 ページ)
- 検出ジョブの管理 (36 ページ)

ディスカバリについて

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

ディスカバリ機能デバイスの可制御性機能と連携して、デバイスに必要なネットワーク設定を行うこともできます (これらの設定がまだデバイスに存在しない場合)。デバイスの制御性については、[Cisco Digital Network Architecture Center 管理者ガイド](#)を参照してください。

デバイスは次の 3 つの方法で検出できます。

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

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

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

- [Subnet Filters] : IP アドレスの範囲を使用する場合は、特定の IP サブネット内のデバイスをディスカバリで無視するように指定できます。
- [Preferred Management IP] : CDP、LLDP、または IP アドレスの範囲のいずれを使用する場合でも、Cisco DNA Center がデバイスの任意の IP アドレスを追加するか、デバイスのループバックアドレスのみを追加するかを指定できます。



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

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



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

検出ダッシュボード

Cisco DNA Center のホームページで、[Tools] > [Discovery] を選択して、[Discovery Dashboard] を表示します。[Discovery Dashboard] には、インベントリの概要、最新のディスカバリ、ディスカバリタイプ、ディスカバリステータス、最近のディスカバリが表示されます。

ディスカバリの前提条件

ディスカバリを実行する前に、次の最小要件を満たしてください。

- Cisco DNA Center によって検出されるデバイスを把握するには、Supported Devices List <https://www.cisco.com/c/en/us/support/cloud-systems-management/dna-center/products-device-support-tables-list.html> を参照してください。
- Cisco DNA Center とデバイス間の最大ネットワーク遅延は 100 ミリ秒であることに注意してください。（最大遅延は 200 ミリ秒です）。

- Cisco DNA Center が使用できるように 1 つ以上の SNMP クレデンシャルがデバイス上で設定されていることを確認してください。少なくとも、これには SNMP v2C 読み取りクレデンシャルを使用できます。詳細については、[ディスカバリ クレデンシャル \(15 ページ\)](#) を参照してください。
- Cisco DNA Center に検出させ、管理委させるデバイスの SSH クレデンシャルを設定します。以下の 2 つの基準のうち、少なくとも 1 つが満たされる場合、Cisco DNA Center はデバイスを検出し、そのインベントリに追加します。
 - デバイスへの SSH アクセスのために Cisco DNA Center が使用するアカウントが、特権 EXEC モード (レベル 15) である。
 - ディスカバリ ジョブで設定される CLI クレデンシャルの一部としてデバイスのインネーブルパスワードを設定している。詳細については、[設定のガイドラインと制限事項のディスカバリ \(18 ページ\)](#) を参照してください。
 - 匿名化を設定します。匿名化は、ホスト名とユーザ ID フィールドのスクランブルを実行します。詳細については、「[コレクタの設定情報の表示または更新 \(370 ページ\)](#)」を参照してください。



重要 ディスカバリを実行した後にデータを匿名化した場合、システムに投入される新しいデータは匿名になりますが、既存のデータは匿名にはなりません。

ディスカバリ クレデンシャル

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

- 標準シスコ デバイス : CLI および SNMP クレデンシャル。
- NFVIS デバイス : HTTP (HTTPS) クレデンシャル。
- 標準デバイスと NFVIS デバイスの両方 : CLI、SNMP、および HTTP (HTTPS) クレデンシャル。

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

ネットワーク内の大半のデバイスに同じクレデンシャル値を使用する場合は、それらを設定して保存し、複数のディスカバリ ジョブで再利用できます。固有のクレデンシャルを使用するデバイスを検出するために、ディスカバリ ジョブの実行時にジョブ固有のディスカバリ クレデ

ンシャルを追加できます。クレデンシャルタイプごとに最大5つの保存済みクレデンシャルと1つのジョブ固有クレデンシャルを定義できます。

クレデンシャルと Cisco ISE のディスカバリ

Cisco ISE を認証サーバとして使用する場合、ディスカバリ機能では、Cisco ISE をディスカバリプロセスの一部として使用してデバイスが認証されます。デバイスが正しく検出されるように、次の注意事項に従ってください。

- 英数字4文字未満のディスカバリ クレデンシャルを使用しないでください。デバイスは英数字4文字未満のクレデンシャルを持つことができますが、Cisco ISE で許容される最短のユーザ名とパスワードは英数字4文字です。デバイス クレデンシャルが4文字未満の場合、Cisco DNA Center はデバイスのインベントリ データを収集できず、デバイスは不完全な収集状態になります。
- 同じユーザ名を持つが、異なるパスワードをもつクレデンシャルを使用しないでください (cisco/cisco123 と cisco/pw123)。Cisco DNA Center ではユーザ名が同じでありながらパスワードの異なるデバイスのディスカバリが可能ですが、Cisco ISE では許容されません。重複したユーザ名が使用されている場合、Cisco DNA Center はデバイスを認証してインベントリ データを収集することができず、デバイスは不完全な収集状態になります。

Cisco ISE を AAA サーバとして定義する方法については、[Cisco ISE またはその他の AAA サーバの追加 \(163 ページ\)](#) を参照してください。

ディスカバリ クレデンシャルのガイドラインと制約事項

Cisco DNA Center のディスカバリ クレデンシャルに関するガイドラインと制約事項は、次のとおりです。

- ディスカバリ ジョブで使用されるデバイス クレデンシャルを変更するには、ディスカバリ ジョブを編集し、使用しなくなったクレデンシャルの選択を解除する必要があります。その後、新しいクレデンシャルを追加してディスカバリを開始する必要があります。詳細については、「[ディスカバリ ジョブでクレデンシャルを変更 \(37 ページ\)](#)」を参照してください。
- デバイスが正常に検出された後にデバイスのクレデンシャルを変更すると、そのデバイスのその後のポーリングサイクルは失敗します。この状況を修正するには、次のいずれかのオプションを使用します。
 - ディスカバリ ツールを使用します：
 - デバイスの新しいクレデンシャルと一致する、ジョブ固有のクレデンシャルを使用して、新しいディスカバリ ジョブを実行します。
 - 既存のディスカバリ ジョブを編集し、ディスカバリを再実行します。
 - 設計ツールを使用します：

- 新しいグローバル クレデンシャルを作成し、適切なグローバル クレデンシャルを使用して新しいディスカバリ ジョブを実行します。
 - 既存のグローバル クレデンシャルを編集し、ディスカバリ ジョブを再実行します。
- デバイス認証に失敗するために進行中のディスカバリ ポーリング サイクルが失敗する場合は、次のいずれかのオプションを使用して状況を修正できます。
- ディスカバリ ツールを使用します：
 - 現在のディスカバリ ジョブを停止または削除し、デバイスのクレデンシャルと一致する、ジョブ固有のクレデンシャルを使用して、新しいディスカバリ ジョブを実行します。
 - 現在のディスカバリ ジョブを停止または削除し、既存のディスカバリ ジョブを編集して、ディスカバリを再実行します。
 - 設計ツールを使用します：
 - 新しいグローバル クレデンシャルを作成し、適切なグローバル クレデンシャルを使用して新しいディスカバリ ジョブを実行します。
 - 既存のグローバル クレデンシャルを編集し、ディスカバリ ジョブを再実行します。
- グローバル クレデンシャルを削除しても、以前に検出されたデバイスは影響を受けません。以前に検出されたデバイスのステータスは、認証の失敗を示しません。ただし、削除されたクレデンシャルの使用を試みる次のディスカバリは失敗します。ディスカバリは、いずれかのデバイスへの接続を試みる前に失敗します。

ディスカバリ クレデンシャルの例

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

このネットワーク内のすべてのデバイスを検出するために、Cisco DNA Center は次のタスクを実行します。

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

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

- ステップ 3** 190 台のデバイスの IP アドレス（グローバル クレデンシャルを共有する 190 台のデバイス）の 1 つとグローバル クレデンシャル 0 を使用してディスカバリ ジョブを実行します。
- ステップ 4** 該当するジョブ固有のクレデンシャル（クレデンシャル 1、クレデンシャル 2、クレデンシャル 3 など）を使用して、残りの 10 台のデバイスごとに 10 個の別個のディスカバリ ジョブを実行します。
- ステップ 5** [インベントリ (Inventory)] ウィンドウで結果を確認します。

優先管理 IP アドレス

Cisco DNA Center は、デバイスを検出すると、そのデバイスのいずれかの IP アドレスをそのデバイスの優先管理 IP アドレスとしてログに記録します。IP アドレスは、デバイスの組み込み管理インターフェイス、または別の物理インターフェイス、または Loopback0 のような論理インターフェイスの IP アドレスにすることができます。デバイスのループバック IP アドレスを優先管理 IP アドレスとして記録するように Cisco DNA Center を設定できます（その IP アドレスが Cisco DNA Center から到達可能である場合）。

デバイスのループバック IP アドレスを優先管理 IP アドレスとして使用する場合、Cisco DNA Center は、優先管理 IP アドレスを次のように決定します。

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

デバイスが検出された後に、[インベントリ (Inventory)] ウィンドウから管理 IP アドレスを更新できます。詳細については、「[デバイスの管理 IP アドレスの更新 \(64 ページ\)](#)」を参照してください。

設定のガイドラインと制限事項のディスカバリ

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

- CLI ユーザ名およびパスワードは特権 EXEC モード（レベル 15）で設定してください。これは、ディスカバリ機能のために Cisco DNA Center で設定する CLI ユーザ名およびパスワードと同じです。Cisco DNA Center にはデバイスへの最高レベルのアクセス権が必要です。

- 着信接続と発信接続の両方に関して、個々のインターフェイスで許可されるトランスポートプロトコルを明示的に指定してください。この設定には、**transport input** と **transport output** コマンドを使用してください。これらのコマンドについては、各デバイスタイプ用のコマンドリファレンス ドキュメントを参照してください。
- デバイスのコンソールポートと VTY 回線のデフォルトのログイン方式を変更しないでください。デバイスがすでに AAA (TACACS) ログインで設定されている場合は、Cisco DNA Center で定義されている CLI ログイン情報が、TACACS サーバで定義されている TACACS ログイン情報と同じであることを確認してください。
- Cisco ワイヤレス コントローラは、サービス ポート IP アドレスではなく、管理 IP アドレスを使用して検出する必要があります。それ以外の場合は、関連するワイヤレス コントローラ 360 および AP 360 のページでは、データが表示されません。

ディスカバリの実行

CDP を使用したネットワークの検出

Cisco Discovery Protocol (CDP) IP アドレス範囲、または LLDP を使用してデバイスを検出できます。この手順では、CDP を使用してデバイスとホストを検出する方法を示します。ディスカバリ メソッドの詳細については、[Discover Your Network Using an IP Address Range \(25 ページ\)](#) および [LLDP を使用したネットワークの検出 \(30 ページ\)](#) を参照してください。



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

始める前に

- ネットワーク デバイスで CDP を有効にします。
- [ディスカバリの前提条件 \(14 ページ\)](#) で説明されているように、ネットワーク デバイスを設定します。
- クライアント IP アドレスとしてネットワーク デバイスのホストの IP アドレスを設定します。(A host is an end-user device, such as a laptop computer or mobile device.)


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

ステップ 2 [ディスカバリ名 (Discovery Name)] フィールドに、名前を入力します。

ステップ 3 まだ表示されていない場合は [IP アドレス/範囲 (IP Address/Range)] エリアを展開し、次のフィールドを設定します。

- a) [ディスカバリ タイプ (Discovery Type)] で、[CDP] をクリックします。
- b) [IP アドレス (IP Address)] フィールドでシード IP アドレスを入力し、Cisco DNA Center でディスカバリ スキャンを開始します。
- c) (任意) [サブネットフィルタ (Subnet Filter)] フィールドで、ディスカバリ スキャンから除外する IP アドレスまたはサブネットを入力します。

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

- d)  をクリックします。

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

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

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

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

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

(注) [ループバック IP を使用 (Use Loopback IP)] の使用を選択し、デバイスにループバック インターフェイスがない場合、Cisco DNA Center は [優先管理 IP アドレス \(18 ページ\)](#) で説明されているロジックを使用して、管理 IP アドレスを選択します。

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

ステップ 4 [クレデンシャル (Credentials)] エリアを展開し、ディスカバリ ジョブで使用するクレデンシャルを設定します。

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

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

表 2: CLI クレデンシヤル

フィールド	説明
Name/Description	CLI クレデンシヤルを説明する名前または語句。
Username	ネットワーク内のデバイスの CLI にログインするために使用する名前。
Password	ネットワーク内のデバイスの CLI にログインするために使用されるパスワード。 セキュリティ上の理由から、確認のためにパスワードをもう一度入力します。 (注) パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。
Enable Password	CLI で高い権限レベルに移るために使用するパスワード。ネットワークデバイスで必要な場合にのみ、このパスワードを設定します。 セキュリティ上の理由から、有効なパスワードをもう一度入力します。 (注) パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。

d) [SNMP v2c] をクリックして、次のフィールドを設定します。

表 3: SNMPv2c のクレデンシヤル

フィールド	説明
Read	<ul style="list-style-type: none"> • Name/Description : 追加する SNMP v2c 設定の名前または説明。 • Read コミュニティ : デバイス上の SNMP 情報を表示するためにのみ使用される read-only コミュニティ ストリング パスワード。 (注) パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。
Write	<ul style="list-style-type: none"> • Name/Description : 追加する SNMP v2c 設定の名前または説明。 • Write コミュニティ : デバイス上の SNMP 情報を変更するために使用される write コミュニティ ストリング。 (注) パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。

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

表 4: SNMPv3 のクレデンシャル

フィールド	説明
Name/Description	追加した SNMPv3 設定の名前または説明。
Username	SNMPv3 設定に関連付けられている名前。
Mode	SNMP メッセージを必要とするセキュリティレベル。次のいずれかのモードを選択します。 <ul style="list-style-type: none"> • noAuthNoPriv : 認証または暗号化を提供しません。 • AuthNoPriv : 認証は提供しますが、暗号化は提供しません。 • AuthPriv : 認証と暗号化の両方を提供します。
Auth Type	使用する認証タイプ（認証モードとして [AuthPriv] または [AuthNoPriv] を選択した場合に有効になります）。次のいずれかの認証タイプを選択します。 <ul style="list-style-type: none"> • SHA : HMAC-SHA に基づく認証。 • MD5 : HMAC-MD5 に基づく認証。
Auth Password	SNMPv3 を使用するデバイスから情報にアクセスする際に使用する SNMPv3 パスワード。これらのパスワード（またはパスフレーズ）は、8 文字以上にする必要があります。 <p>(注)</p> <ul style="list-style-type: none"> •一部のシスコワイヤレスコントローラでは、パスワード（あるいはパスフレーズ）は少なくとも12文字以上である必要があります。ワイヤレスコントローラのパスワードの最小要件を必ず確認してください。パスワードに必要な最低限の文字数が守られないと、デバイスではCisco DNA Centerによる検出、監視、管理が行われなくなります。 •パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。
Privacy Type	プライバシータイプ。（認証モードとして [AuthPriv] を選択すると有効になります）。次のいずれかのプライバシータイプを選択します。 <ul style="list-style-type: none"> • DES : CBC DES-56 規格に基づく認証に DES 56-bit (DES-56) 暗号化を追加。 • AES128 : 暗号化の CBC モード AES。 • None : プライバシー設定なし。

フィールド	説明
Privacy Password	<p>DES または AES128 暗号化をサポートしているデバイスで交換されるメッセージを暗号化するための秘密鍵を生成するために使用される SNMPv3 プライバシーパスワード。パスワード（またはパスフレーズ）は、8 文字以上にする必要があります。</p> <p>(注)</p> <ul style="list-style-type: none"> 一部のシスコ ワイヤレス コントローラでは、パスワード（あるいはパスフレーズ）は少なくとも 12 文字以上である必要があります。ワイヤレス コントローラのパスワードの最小要件を必ず確認してください。パスワードに必要な最低限の文字数が守られないと、デバイスでは Cisco DNA Center による検出、監視、管理が行われなくなります。 パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。

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

表 5: *SNMP Properties*

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

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

表 6: *HTTPS クレデンシャル*

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

フィールド	説明
Read	<p>最大 5 つの HTTPS 読み取りクレデンシャルを設定できます。</p> <ul style="list-style-type: none"> • Name/Description : 追加している HTTPS ログイン情報の名前または説明。 • Username : HTTPS 接続の認証に使用される名前。 • Password : HTTPS 接続の認証に使用されるパスワード。 • Port : HTTPS トラフィックに使用される TCP/UDP ポートの番号。デフォルトはポート番号 443 (HTTPS の既知のポート) です。 <p>(注) パスワードには、少なくとも1つの小文字、1つの大文字、1つの数字、1つの特殊文字が必要で、<>@',:;!およびスペースは使用できません。セキュリティ上の理由から、確認のためにパスワードをもう一度入力します。パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。</p>
Write	<p>最大 5 つの HTTPS 書き込みクレデンシャルを設定できます。</p> <ul style="list-style-type: none"> • Name/Description : 追加している HTTPS ログイン情報の名前または説明。 • Username : HTTPS 接続の認証に使用される名前。 • Password : HTTPS 接続の認証に使用されるパスワード。 • Port : HTTPS トラフィックに使用される TCP/UDP ポートの番号。デフォルトはポート番号 443 (HTTPS の既知のポート) です。 <p>(注) パスワードには、少なくとも1つの小文字、1つの大文字、1つの数字、1つの特殊文字が必要で、<>@',:;!およびスペースは使用できません。セキュリティ上の理由から、確認のためにパスワードをもう一度入力します。パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。</p>

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

(注) Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ デバイスを検出するには、NETCONF を有効にし、ポートを 830 に設定する必要があります。NETCONF は、ネットワークデバイスの設定をインストール、操作、削除するためのメカニズムです。[Advanced] 領域で Telnet を選択すると、NETCONF は無効になります。

ステップ 5 デバイスとの接続に使用されるプロトコルを設定するには、[詳細 (Advanced)] エリアを展開し、次のタスクを実行します。

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

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

b) 使用する順序でプロトコルをドラッグアンドドロップします。

ステップ 6 [Start] をクリックします。[Discover] をクリックして、すぐにディスカバリを実行するか、または後で実行するためにディスカバリをスケジュールするかを選択します。

- 今すぐディスカバリを実行するには、[Now] オプションボタンをクリックし、[Start] をクリックします。
- 後でディスカバリをスケジュールするには、[Later] オプションボタンをクリックして日時を定義し、[Start] をクリックします。

通知アイコンをクリックして、スケジュールされたディスカバリタスクを表示します。ディスカバリを開始する前にディスカバリタスクを編集するには、[Edit] をクリックします。スケジュールされたディスカバリジョブを開始する前にキャンセルする場合は、[Cancel] をクリックします。

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

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

Discover Your Network Using an IP Address Range

IP アドレス範囲、CDP、または LLDP を使用してデバイスを検出できます。この手順では、IP アドレス範囲を使用してデバイスとホストを検出する方法を示します。ディスカバリメソッドの詳細については、[CDP を使用したネットワークの検出 \(19 ページ\)](#) および [LLDP を使用したネットワークの検出 \(30 ページ\)](#) を参照してください。


始める前に

[ディスカバリの前提条件 \(14 ページ\)](#) で説明されているように、デバイスには必須のデバイス設定が存在する必要があります。

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

ステップ 2 [ディスカバリ名 (Discovery Name)] フィールドに、名前を入力します。

ステップ 3 まだ表示されていない場合は [IP アドレス/範囲 (IP Address/Ranges)] エリアを展開し、次のフィールドを設定します。

- a) [ディスカバリ タイプ (Discovery Type)] で、[範囲 (Range)] をクリックします。
- b) [IP アドレス (IP Address)] フィールドに、Cisco DNA Center の最初と最後の IP アドレス (IP 範囲) を入力し、[追加 (Add)]  をクリックします。

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

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

- c) (任意) ステップ b を繰り返して、追加の IP アドレス範囲を入力します。
 d) [Preferred Management IP] で、次のいずれかのオプションを選択します。

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

(注) [ループバック IP を使用 (Use Loopback IP)] の使用を選択し、デバイスにループバック インターフェイスがない場合、Cisco DNA Centerは優先管理 IP アドレス (18 ページ) で説明されているロジックを使用して、管理 IP アドレスを選択します。

ステップ 4 [クレデンシヤル (Credentials)] エリアを展開し、ディスカバリ ジョブで使用するクレデンシヤルを設定します。

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

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

表 7: CLI クレデンシヤル

フィールド	説明
Name/Description	CLI クレデンシヤルを説明する名前または語句。
Username	ネットワーク内のデバイスの CLI にログインするために使用する名前。
Password	ネットワーク内のデバイスの CLI にログインするために使用されるパスワード。 セキュリティ上の理由から、確認のためにパスワードをもう一度入力します。 (注) パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。

フィールド	説明
Enable Password	<p>CLI で高い権限レベルに移るために使用するパスワード。ネットワークデバイスで必要な場合にのみ、このパスワードを設定します。</p> <p>セキュリティ上の理由から、有効なパスワードをもう一度入力します。</p> <p>(注) パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。</p>

d) [SNMP v2c] をクリックして、次のフィールドを設定します。

表 8: SNMPv2c のクレデンシャル

フィールド	説明
Read	<ul style="list-style-type: none"> • Name/Description : 追加する SNMP v2c 設定の名前または説明。 • Read コミュニティ : デバイス上の SNMP 情報を表示するためにのみ使用される read-only コミュニティ スtring パスワード。 <p>(注) パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。</p>
Write	<ul style="list-style-type: none"> • Name/Description : 追加する SNMP v2c 設定の名前または説明。 • Write コミュニティ : デバイス上の SNMP 情報を変更するために使用される write コミュニティ スtring。 <p>(注) パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。</p>

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

表 9: SNMPv3 のクレデンシャル

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

フィールド	説明
Auth Type	<p>使用する認証タイプ（認証モードとして [AuthPriv] または [AuthNoPriv] を選択した場合に有効になります）。次のいずれかの認証タイプを選択します。</p> <ul style="list-style-type: none"> • SHA : HMAC-SHA に基づく認証。 • MD5 : HMAC-MD5 に基づく認証。
Auth Password	<p>SNMPv3 を使用するデバイスから情報にアクセスする際に使用する SNMPv3 パスワード。これらのパスワード（またはパスフレーズ）は、8 文字以上にする必要があります。</p> <p>(注)</p> <ul style="list-style-type: none"> •一部のシスコ ワイヤレス コントローラでは、パスワード（あるいはパスフレーズ）は少なくとも12文字以上である必要があります。ワイヤレス コントローラのパスワードの最小要件を必ず確認してください。パスワードに必要な最低限の文字数が守られないと、デバイスではCisco DNA Centerによる検出、監視、管理が行われなくなります。 •パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。
Privacy Type	<p>プライバシータイプ。（認証モードとして [AuthPriv] を選択すると有効になります）。次のいずれかのプライバシー タイプを選択します。</p> <ul style="list-style-type: none"> • DES : CBC DES-56 規格に基づく認証に DES 56-bit (DES-56) 暗号化を追加。 • AES128 : 暗号化の CBC モード AES。 • None : プライバシー設定なし。
Privacy Password	<p>DES または AES128 暗号化をサポートしているデバイスで交換されるメッセージを暗号化するための秘密鍵を生成するために使用される SNMPv3 プライバシーパスワード。パスワード（またはパスフレーズ）は、8 文字以上にする必要があります。</p> <p>(注)</p> <ul style="list-style-type: none"> •一部のシスコ ワイヤレス コントローラでは、パスワード（あるいはパスフレーズ）は少なくとも12文字以上である必要があります。ワイヤレス コントローラのパスワードの最小要件を必ず確認してください。パスワードに必要な最低限の文字数が守られないと、デバイスではCisco DNA Centerによる検出、監視、管理が行われなくなります。 •パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。

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

表 10: SNMP Properties

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

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

表 11: HTTPS クレデンシャル

フィールド	説明
Type	設定している HTTPS クレデンシャルのタイプを指定します。有効なタイプは、[読み取り (Read)] または [書き込み (Write)] です。
Read	<p>最大 5 つの HTTPS 読み取りクレデンシャルを設定できます。</p> <ul style="list-style-type: none"> • Name/Description : 追加している HTTPS ログイン情報の名前または説明。 • Username : HTTPS 接続の認証に使用される名前。 • Password : HTTPS 接続の認証に使用されるパスワード。 • Port : HTTPS トラフィックに使用される TCP/UDP ポートの番号。デフォルトはポート番号 443 (HTTPS の既知のポート) です。 <p>(注) パスワードには、少なくとも1つの小文字、1つの大文字、1つの数字、1つの特殊文字が必要で、<>@',:;! およびスペースは使用できません。セキュリティ上の理由から、確認のためにパスワードをもう一度入力します。パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。</p>
Write	<p>最大 5 つの HTTPS 書き込みクレデンシャルを設定できます。</p> <ul style="list-style-type: none"> • Name/Description : 追加している HTTPS ログイン情報の名前または説明。 • Username : HTTPS 接続の認証に使用される名前。 • Password : HTTPS 接続の認証に使用されるパスワード。 • Port : HTTPS トラフィックに使用される TCP/UDP ポートの番号。デフォルトはポート番号 443 (HTTPS の既知のポート) です。 <p>(注) パスワードには、少なくとも1つの小文字、1つの大文字、1つの数字、1つの特殊文字が必要で、<>@',:;! およびスペースは使用できません。セキュリティ上の理由から、確認のためにパスワードをもう一度入力します。パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。</p>

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

(注) Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ デバイスを検出するには、NETCONF を有効にし、ポートを 830 に設定する必要があります。NETCONF は、ネットワークデバイスの設定をインストール、操作、削除するためのメカニズムです。

ステップ 5 (任意) デバイスとの接続に使用されるプロトコルを設定するには、[詳細 (Advanced)] エリアを展開し、次のタスクを実行します。

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

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

- b) 使用する順序でプロトコルをドラッグアンドドロップします。

ステップ 6 [Start] をクリックします。[Discover] をクリックして、すぐにディスカバリを実行するか、または後で実行するためにディスカバリをスケジュールするかを選択します。

- 今すぐディスカバリを実行するには、[Now] オプションボタンをクリックし、[Start] をクリックします。
- 後でディスカバリをスケジュールするには、[Later] オプションボタンをクリックして日時を定義し、[Start] をクリックします。

通知アイコンをクリックして、スケジュールされたディスカバリタスクを表示します。ディスカバリを開始する前にディスカバリタスクを編集するには、[Edit] をクリックします。スケジュールされたディスカバリジョブを開始する前にキャンセルする場合は、[Cancel] をクリックします。

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

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

LLDP を使用したネットワークの検出

Link Layer Discovery Protocol (LLDP)、CDP、または IP アドレス範囲を使用してデバイスを検出できます。この手順では、LLDP を使用してデバイスとホストを検出する方法を示します。ディスカバリ メソッドの詳細については、[CDP を使用したネットワークの検出 \(19 ページ\)](#) および [Discover Your Network Using an IP Address Range \(25 ページ\)](#) を参照してください。



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

始める前に

- ネットワーク デバイスで LLDP を有効にします。
- [ディスカバリの前提条件 \(14 ページ\)](#) で説明されているように、ネットワーク デバイスを設定します。
- クライアント IP アドレスとしてネットワーク デバイスのホストの IP アドレスを設定します。(A host is an end-user device, such as a laptop computer or mobile device.)


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

ステップ 2 [ディスカバリ名 (Discovery Name)] フィールドに、名前を入力します。

ステップ 3 まだ表示されていない場合は [IP アドレス/範囲 (IP Address/Range)] エリアを展開し、次のフィールドを設定します。

- [ディスカバリ タイプ (Discovery Type)] で、[LLDP] をクリックします。
- [IP アドレス (IP Address)] フィールドでシード IP アドレスを入力し、Cisco DNA Center でディスカバリ スキャンを開始します。
- (任意) [サブネットフィルタ (Subnet Filter)] フィールドで、ディスカバリ スキャンから除外する IP アドレスまたはサブネットを入力します。

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

-  をクリックします。

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

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

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

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

- [None] : デバイスはそのすべての IP アドレスを使用できます。

- [Use Loopback IP] : デバイスのループバック インターフェイスの IP アドレスを指定します。
 - (注) このオプションを選択し、デバイスにループバック インターフェイスがない場合、Cisco DNA Center は [優先管理 IP アドレス \(18 ページ\)](#) で説明されているロジックを使用して、管理 IP アドレスを選択します。
 - (注) ループバック インターフェイスの IP アドレスを優先管理 IP アドレスとして使用するには、LLDP ネイバーの IP アドレスが Cisco DNA Center から到達可能であることを確認します。

ステップ 4 [クレデンシヤル (Credentials)] エリアを展開し、ディスカバリ ジョブで使用するクレデンシヤルを設定します。

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

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

表 12: CLI クレデンシヤル

フィールド	説明
Name/Description	CLI クレデンシヤルを説明する名前または語句。
Username	ネットワーク内のデバイスの CLI にログインするために使用する名前。
Password	ネットワーク内のデバイスの CLI にログインするために使用されるパスワード。 セキュリティ上の理由から、確認のためにパスワードをもう一度入力します。 (注) パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。
Enable Password	CLI で高い権限レベルに移るために使用するパスワード。ネットワークデバイスが必要な場合にのみ、このパスワードを設定します。 セキュリティ上の理由から、有効なパスワードをもう一度入力します。 (注) パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。

- d) [SNMP v2c] をクリックして、次のフィールドを設定します。

表 13: SNMPv2c のクレデンシャル

フィールド	説明
Read	<ul style="list-style-type: none"> • Name/Description : 追加する SNMP v2c 設定の名前または説明。 • Read コミュニティ : デバイス上の SNMP 情報を表示するためにのみ使用される read-only コミュニティ スtring パスワード。 <p>(注) パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。</p>
Write	<ul style="list-style-type: none"> • Name/Description : 追加する SNMP v2c 設定の名前または説明。 • Write コミュニティ : デバイス上の SNMP 情報を変更するために使用される write コミュニティ スtring。 <p>(注) パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。</p>

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

表 14: SNMPv3 のクレデンシャル

フィールド	説明
Name/Description	追加した SNMPv3 設定の名前または説明。
Username	SNMPv3 設定に関連付けられている名前。
Mode	SNMP メッセージを必要とするセキュリティ レベル。次のいずれかのモードを選択します。 <ul style="list-style-type: none"> • noAuthNoPriv : 認証または暗号化を提供しません。 • AuthNoPriv : 認証は提供しますが、暗号化は提供しません。 • AuthPriv : 認証と暗号化の両方を提供します。
Auth Type	使用する認証タイプ (認証モードとして [AuthPriv] または [AuthNoPriv] を選択した場合に有効になります)。次のいずれかの認証タイプを選択します。 <ul style="list-style-type: none"> • SHA : HMAC-SHA に基づく認証。 • MD5 : HMAC-MD5 に基づく認証。

フィールド	説明
Auth Password	<p>SNMPv3を使用するデバイスから情報にアクセスする際に使用するSNMPv3パスワード。これらのパスワード（またはパスフレーズ）は、8文字以上にする必要があります。</p> <p>(注)</p> <ul style="list-style-type: none"> 一部のシスコワイヤレスコントローラでは、パスワード（あるいはパスフレーズ）は少なくとも12文字以上である必要があります。ワイヤレスコントローラのパスワードの最小要件を必ず確認してください。パスワードに必要な最低限の文字数が守られないと、デバイスではCisco DNA Centerによる検出、監視、管理が行われなくなります。 パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。
Privacy Type	<p>プライバシータイプ。（認証モードとして[AuthPriv]を選択すると有効になります）。次のいずれかのプライバシータイプを選択します。</p> <ul style="list-style-type: none"> DES：CBC DES-56規格に基づく認証にDES 56-bit（DES-56）暗号化を追加。 AES128：暗号化のCBCモードAES。 None：プライバシー設定なし。
Privacy Password	<p>DESまたはAES128暗号化をサポートしているデバイスで交換されるメッセージを暗号化するための秘密鍵を生成するために使用されるSNMPv3プライバシーパスワード。パスワード（またはパスフレーズ）は、8文字以上にする必要があります。</p> <p>(注)</p> <ul style="list-style-type: none"> 一部のシスコワイヤレスコントローラでは、パスワード（あるいはパスフレーズ）は少なくとも12文字以上である必要があります。ワイヤレスコントローラのパスワードの最小要件を必ず確認してください。パスワードに必要な最低限の文字数が守られないと、デバイスではCisco DNA Centerによる検出、監視、管理が行われなくなります。 パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。

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

表 15: *SNMP Properties*

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

フィールド	説明
Timeout	再試行間隔を表す秒数。

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

表 16: HTTPS クレデンシャル

フィールド	説明
Type	設定している HTTPS クレデンシャルのタイプを指定します。有効なタイプは、[読み取り (Read)] または [書き込み (Write)] です。
Read	<p>最大 5 つの HTTPS 読み取りクレデンシャルを設定できます。</p> <ul style="list-style-type: none"> • Name/Description : 追加している HTTPS ログイン情報の名前または説明。 • Username : HTTPS 接続の認証に使用される名前。 • Password : HTTPS 接続の認証に使用されるパスワード。 • Port : HTTPS トラフィックに使用される TCP/UDP ポートの番号。デフォルトはポート番号 443 (HTTPS の既知のポート) です。 <p>(注) パスワードには、少なくとも1つの小文字、1つの大文字、1つの数字、1つの特殊文字が必要で、<>@',:;! およびスペースは使用できません。セキュリティ上の理由から、確認のためにパスワードをもう一度入力します。パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。</p>
Write	<p>最大 5 つの HTTPS 書き込みクレデンシャルを設定できます。</p> <ul style="list-style-type: none"> • Name/Description : 追加している HTTPS ログイン情報の名前または説明。 • Username : HTTPS 接続の認証に使用される名前。 • Password : HTTPS 接続の認証に使用されるパスワード。 • Port : HTTPS トラフィックに使用される TCP/UDP ポートの番号。デフォルトはポート番号 443 (HTTPS の既知のポート) です。 <p>(注) パスワードには、少なくとも1つの小文字、1つの大文字、1つの数字、1つの特殊文字が必要で、<>@',:;! およびスペースは使用できません。セキュリティ上の理由から、確認のためにパスワードをもう一度入力します。パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。</p>

ステップ 5 (任意) デバイスとの接続に使用されるプロトコルを設定するには、[詳細 (Advanced)] エリアを展開し、次のタスクを実行します。

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

ステップ 6 [Start] をクリックします。[Discover] をクリックして、すぐにディスカバリを実行するか、または後で実行するためにディスカバリをスケジュールするかを選択します。

- 今すぐディスカバリを実行するには、[Now] オプションボタンをクリックし、[Start] をクリックします。
- 後でディスカバリをスケジュールするには、[Later] オプションボタンをクリックして日時を定義し、[Start] をクリックします。

通知アイコンをクリックして、スケジュールされたディスカバリタスクを表示します。ディスカバリを開始する前にディスカバリタスクを編集するには、[Edit] をクリックします。スケジュールされたディスカバリジョブを開始する前にキャンセルする場合は、[Cancel] をクリックします。

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

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

検出ジョブの管理

ディスカバリ ジョブの停止および開始

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

ステップ 2 アクティブなディスカバリ ジョブを停止するには、次の手順を実行します。

- a) [ディスカバリ (Discoveries)] ペインで、関連するディスカバリ ジョブを選択します。
- b) [Stop] をクリックします。

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

- a) [ディスカバリ (Discoveries)] ペインで、関連するディスカバリ ジョブを選択します。
- b) [Re-discover] をクリックして、選択した検出ジョブを再起動します。

ディスカバリ ジョブの編集

ディスカバリ ジョブを編集して、ジョブを再実行できます。

始める前に

少なくとも1つのディスカバリ ジョブが必要です。

-
- ステップ1** Cisco DNA Center のホームページで、**[ディスカバリ (Discovery)]** をクリックします。
- ステップ2** **[ディスカバリ (Discovery)]** ペインで、検出ジョブを選択します。
- ステップ3** **[Edit]** をクリックします。
- ステップ4** 次のフィールドを除き、ディスカバリのタイプに応じてディスカバリ ジョブのタイプを変更できます。
- **CDP** : ディスカバリ名、ディスカバリ タイプ、IP アドレス。変更可能なフィールドの詳細については、[CDP を使用したネットワークの検出 \(19 ページ\)](#) を参照してください。
 - **IP 範囲 (IP Range)** : ディスカバリ名、ディスカバリ タイプ、IP アドレス範囲 (ただし別の IP アドレス範囲を追加できます)。変更可能なフィールドの詳細については、[Discover Your Network Using an IP Address Range \(25 ページ\)](#) を参照してください。
 - **LLDP** : ディスカバリ名、ディスカバリ タイプ、IP アドレス。変更可能なフィールドの詳細については、[LLDP を使用したネットワークの検出 \(30 ページ\)](#) を参照してください。
- ステップ5** **[Start]** をクリックします。
-

ディスカバリ ジョブでクレデンシャルを変更

ディスカバリ ジョブで使用されるクレデンシャルを変更し、そのジョブを再実行できます。

始める前に

少なくとも1つのディスカバリ ジョブが必要です。

-
- ステップ1** Cisco DNA Center のホームページで、**[ディスカバリ (Discovery)]** をクリックします。
- ステップ2** **[ディスカバリ (Discovery)]** ペインで、検出ジョブを選択します。
- ステップ3** **[Edit]** をクリックします。
- ステップ4** **[クレデンシャル (Credentials)]** エリアを展開します。
- ステップ5** 使わないクレデンシャルを非選択状態にします。
- ステップ6** 使用するクレデンシャルを設定します。
- [クレデンシャルの追加 (Add Credentials)]** をクリックします。
 - CLI クレデンシャルを設定するには、次のフィールドを設定します。

表 17: CLI クレデンシャル

フィールド	説明
Name/Description	CLI クレデンシャルを説明する名前または語句。

フィールド	説明
Username	ネットワーク内のデバイスの CLI にログインするために使用する名前。
Password	ネットワーク内のデバイスの CLI にログインするために使用されるパスワード。 セキュリティ上の理由から、確認のためにパスワードをもう一度入力します。 (注) パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。
Enable Password	CLI で高い権限レベルに移るために使用するパスワード。ネットワークデバイスで必要な場合にのみ、このパスワードを設定します。 セキュリティ上の理由から、有効なパスワードをもう一度入力します。 (注) パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。

- c) [SNMP v2c] をクリックして、次のフィールドを設定します。

表 18: *SNMPv2c* のクレデンシャル

フィールド	説明
Read	<ul style="list-style-type: none"> • Name/Description : 追加する SNMP v2c 設定の名前または説明。 • Read コミュニティ : デバイス上の SNMP 情報を表示するためにのみ使用される read-only コミュニティ ストリング パスワード。 (注) パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。
Write	<ul style="list-style-type: none"> • Name/Description : 追加する SNMP v2c 設定の名前または説明。 • Write コミュニティ : デバイス上の SNMP 情報を変更するために使用される write コミュニティ ストリング。 (注) パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。

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

表 19: *SNMPv3* のクレデンシャル

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

フィールド	説明
Username	SNMPv3 設定に関連付けられている名前。
Mode	SNMP メッセージを必要とするセキュリティレベル。次のいずれかのモードを選択します。 <ul style="list-style-type: none"> • noAuthNoPriv : 認証または暗号化を提供しません。 • AuthNoPriv : 認証は提供しますが、暗号化は提供しません。 • AuthPriv : 認証と暗号化の両方を提供します。
Auth Type	使用する認証タイプ（認証モードとして [AuthPriv] または [AuthNoPriv] を選択した場合に有効になります）。次のいずれかの認証タイプを選択します。 <ul style="list-style-type: none"> • SHA : HMAC-SHA に基づく認証。 • MD5 : HMAC-MD5 に基づく認証。
Auth Password	SNMPv3 を使用するデバイスから情報にアクセスする際に使用する SNMPv3 パスワード。これらのパスワード（またはパスフレーズ）は、8 文字以上にする必要があります。 <p>(注)</p> <ul style="list-style-type: none"> •一部のシスコワイヤレスコントローラでは、パスワード（あるいはパスフレーズ）は少なくとも12文字以上である必要があります。ワイヤレスコントローラのパスワードの最小要件を必ず確認してください。パスワードに必要な最低限の文字数が守られないと、デバイスではCisco DNA Centerによる検出、監視、管理が行われなくなります。 •パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。
Privacy Type	プライバシータイプ。（認証モードとして [AuthPriv] を選択すると有効になります）。次のいずれかのプライバシータイプを選択します。 <ul style="list-style-type: none"> • DES : CBC DES-56 規格に基づく認証に DES 56-bit (DES-56) 暗号化を追加。 • AES128 : 暗号化の CBC モード AES。 • None : プライバシー設定なし。

フィールド	説明
Privacy Password	<p>DES または AES128 暗号化をサポートしているデバイスで交換されるメッセージを暗号化するための秘密鍵を生成するために使用される SNMPv3 プライバシーパスワード。パスワード（またはパスフレーズ）は、8 文字以上にする必要があります。</p> <p>(注)</p> <ul style="list-style-type: none"> 一部のシスコ ワイヤレス コントローラでは、パスワード（あるいはパスフレーズ）は少なくとも 12 文字以上である必要があります。ワイヤレス コントローラのパスワードの最小要件を必ず確認してください。パスワードに必要な最低限の文字数が守られないと、デバイスでは Cisco DNA Center による検出、監視、管理が行われなくなります。 パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。

ステップ 7 [Start] をクリックします。

ディスカバリ ジョブの複製

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

始める前に

少なくとも 1 つのディスカバリ ジョブを実行する必要があります。

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

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

ステップ 3 [Clone & Edit] をクリックします。

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

ステップ 4 (任意) 検出ジョブの名前を変更します。

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

ディスカバリ ジョブの削除

アクティブまたは非アクティブに関係なく、検出ジョブを削除できます。

始める前に

少なくとも1つのディスカバリ ジョブを実行する必要があります。

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

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

ステップ3 [削除 (Delete)] をクリックします。

ステップ4 [OK] をクリックして確定します。

ディスカバリ ジョブ情報の表示

使用された設定やクレデンシヤルなどの、ディスカバリ ジョブに関する情報を表示できます。検出された、または検出に失敗した特定のデバイスに関する情報を含め、実行された各ディスカバリ ジョブに関する履歴情報も表示できます。

始める前に

少なくとも1つのディスカバリジョブを実行します。

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

ステップ2 [**ディスカバリ (Discovery)**] ペインで、検出ジョブを選択します。もしくは、[**検索 (Search)**] 機能を使用して、デバイス IP アドレスまたは名前によって、ディスカバリ ジョブを検索できます。

ステップ3 詳細については、次の領域のひとつの隣にある下矢印をクリックします。

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

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

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



第 4 章

インベントリの管理

- [インベントリについて \(43 ページ\)](#)
- [インベントリと Cisco ISE の認証 \(44 ページ\)](#)
- [インベントリに関する情報の表示 \(45 ページ\)](#)
- [インベントリからのトポロジマップの起動 \(49 ページ\)](#)
- [Cisco DNA Center インベントリ内のデバイスのタイプ \(49 ページ\)](#)
- [デバイスのフィルタ \(62 ページ\)](#)
- [デバイスのロールの変更 \(インベントリ\) \(63 ページ\)](#)
- [デバイスの管理 IP アドレスの更新 \(64 ページ\)](#)
- [デバイスの再同期間隔の更新 \(65 ページ\)](#)
- [デバイス情報の再同期 \(66 ページ\)](#)
- [ネットワーク デバイスの削除 \(66 ページ\)](#)
- [コマンドランナーを起動 \(インベントリ\) \(67 ページ\)](#)
- [CSV ファイルを使用してデバイス設定をインポート/エクスポートします。 \(67 ページ\)](#)
- [故障したデバイスの交換 \(71 ページ\)](#)
- [Cisco DNA Center での RMA ワークフローの制限事項 Cisco DNA Center \(72 ページ\)](#)

インベントリについて

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

インベントリ機能デバイスの可制御性機能と連携して、デバイスに必要なネットワーク設定を行うこともできます (これらの設定がまだデバイスに存在しない場合)。デバイスの制御性については、[Cisco Digital Network Architecture Center 管理者ガイド](#)を参照してください。

インベントリは、必要に応じて次のプロトコルを使用します。

- リンク層検出プロトコル (LLDP)
- IP デバイス トラッキング (IPDT) またはスイッチ統合セキュリティ機能 (SISF) (IPDT または SISF をデバイス上で有効にする必要があります)。

- LLDP Media Endpoint Discovery（このプロトコルは IP フォンや一部のサーバの検出に使用されます）。
- ネットワーク設定プロトコル（NETCONF）デバイスのリストについては、[ディスカバリの前提条件（14 ページ）](#) を参照してください。

初期検出後、Cisco DNA Center は定期的にデバイスをポーリングすることでインベントリを維持します。デフォルトの間隔は6時間です。ただし、この間隔は、ネットワーク環境の必要性に応じて、最大 24 時間まで変更できます。詳細については、「[デバイスの再同期間隔の更新（65 ページ）](#)」を参照してください。また、デバイスの設定変更によって SNMP トラップがトリガーされ、その後、デバイスの再同期がトリガーされます。ポーリングはデバイス、リンク、ホスト、およびインターフェイスごとに実行されます。アクティブだった期間が1日未満のデバイスのみ表示されます。これによって、古いデバイスデータが表示されないようにします。平均すると、500 台のデバイスのポーリングには約 20 分かかります。

インベントリと Cisco ISE の認証

Cisco ISE には、Cisco DNA Center で次の 2 つの異なる使用例があります。

- ネットワークでデバイス認証に Cisco ISE を使用する場合、Cisco DNA Center で Cisco ISE を設定する必要があります。このように、デバイスをプロビジョニングする場合、Cisco DNA Center はユーザが定義した Cisco ISE サーバ情報を使用してデバイスを設定します。また、Cisco DNA Center は Cisco ISE サーバでデバイスを設定し、後に続くデバイスの更新プログラムについても伝えます。Cisco DNA Center での Cisco ISE の設定については、[グローバル ネットワーク サーバの設定（162 ページ）](#) を参照してください。



(注) Cisco ISE を使用して Cisco Catalyst 9800 シリーズ デバイスを認証する場合は、netconf ユーザの権限を提供するように Cisco ISE を設定する必要があります。

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

Cisco DNA Center が Cisco ISE サーバでデバイスを設定および更新する場合、トランザクションは Cisco DNA Center の監査ログでキャプチャされます。監査ログを使用して、Cisco DNA Center や Cisco ISE インベントリに関する問題のトラブルシューティングを実行できます。Cisco DNA Center の監査ログの詳細については、『[Cisco Digital Network Architecture Center 管理者ガイド](#)』を参照してください。

デバイスのプロビジョニング後、Cisco DNA Center は Cisco ISE でデバイスを認証します。Cisco ISE に到達できない（RADIUS 応答がない）場合、デバイスはローカルのログインクレデンシャルを使用します。Cisco ISE に到達できるが Cisco ISE にデバイスが存在しない場合や、そのクレデンシャルが Cisco DNA Center で設定されたクレデンシャルと一致し

ない場合、デバイスはローカルのログインクレデンシャルを使用するためにフォールバックしません。代わりに、部分的な収集状態になります。

この状態を回避するには、Cisco DNA Center を使用してデバイスをプロビジョニングする前に、必ず Cisco DNA Center で使用しているのと同じデバイス クレデンシャルで Cisco ISE のデバイスを設定します。また、有効なディスカバリ クレデンシャルを設定したことも確認してください。詳細については、「[ディスカバリ クレデンシャル \(15 ページ\)](#)」を参照してください。

- 必要に応じて、Cisco ISE を使用してデバイス グループにアクセス制御を実行できます。この使用例については、『[Cisco Digital Network Architecture Center 管理者ガイド](#)』を参照してください。

インベントリに関する情報の表示

[インベントリ (Inventory)] テーブルには、検出された各デバイスの情報が表示されます。[Config] カラムを除く、すべてのカラムではソートをサポートします。列ヘッダーをクリックすると、行が昇順にソートされます。列ヘッダーをもう一度クリックすると、行が降順にソートされます。

始める前に

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

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

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

表 20: Inventory

カラム	説明
Device Name	<p>デバイスの名前。</p> <p>名前をクリックすると、ダイアログボックスが開き、次の情報が表示されます。</p> <ul style="list-style-type: none"> • [Details] : デバイス名、デバイスタイプ、IP アドレス、シリアル番号、ソフトウェアイメージなどの詳細が表示されます。 • [Configuration] : show running-config コマンドの出力で表示される内容に似た詳細な設定情報が表示されます。 <p>(注) この機能は、アクセスポイント (AP) とワイヤレス コントローラにはサポートされていません。したがって、これらのデバイスタイプの場合は設定データは返されません。</p> <ul style="list-style-type: none"> • [Interface] : デバイスのインターフェイスの [Interface Name]、[MAC Address]、および [Status] が表示されます。 • [Stack] : MAC アドレス、ロール、状態、プライオリティが表示されます。 • [Run Commands] : デバイスで CLI コマンドを実行するためのコマンドランナーを開きます。 • [View 360] : 360 ウィンドウが表示されます。360 を開くには、アシュアランス アプリケーションをインストールしている必要があります。 <p>(注) 赤で表示されているデバイス名は、インベントリがデバイスをポーリングしておらず、30分を超える期間にわたってその情報を更新していないことを意味しています。</p>
IP Address	デバイスの IP アドレス

コラム	説明
<p>Support Type</p>	<p>以下に示すデバイスのサポートレベルが表示されます。</p> <ul style="list-style-type: none"> • [Supported] : Cisco DNA Center のすべてのアプリケーションに対してデバイスバックがテスト済みです。これらのデバイスのいずれかの Cisco DNA Center 機能が動作しない場合は、サービスリクエストを開くことができます。 • [Unsupported] : Cisco DNA Center でテストおよび認定されていない他のすべての Cisco デバイスとサードパーティ製デバイス。これらのデバイスについて、Cisco DNA Center でさまざまな機能をベストエフォートとして試すことができます。ただし、Cisco DNA Center の機能が期待どおりに動作しない場合、サービスリクエストまたはバグを発生させることは求められていません。 • [Third Party] : デバイスバックは、顧客/ビジネスパートナーによって構築され、認定プロセスを通過しています。サードパーティ製デバイスは、検出、インベントリ、トポロジなどの基本自動化機能をサポートします。Cisco TAC は、これらのデバイスの初期レベルのサポートを提供します。ただし、デバイスバックに問題がある場合は、ビジネスパートナーに連絡して修正を依頼する必要があります。
<p>Reachability</p>	<p>以下は、さまざまなステータスのリストです。</p> <ul style="list-style-type: none"> • [Connecting] : Cisco DNA Center がデバイスに接続しています。 • [Reachable] : Cisco DNA Center がデバイスに接続されており、CLI を使用して Cisco コマンドを実行できます。 <p>(注) 失敗は、Cisco DNA Center がデバイスに接続されていますが、CLI を使用して Cisco コマンドを実行できなかったことを示します。この状態は通常、デバイスがシスコデバイスではないことを示します。</p> <ul style="list-style-type: none"> • [Authentication Failed] : Cisco DNA Center がデバイスに接続されていますが、デバイスのタイプを判別できません。 • [Unreachable] : Cisco DNA Center がデバイスに接続できません。 <p>(注) デバイスに接続できないのは、ディスカバリ ジョブにクレデンシャルが存在しないか、ディスカバリ ジョブに誤ったクレデンシャルが存在するためである場合があります。これに該当する疑いがある場合は、新しいディスカバリ ジョブを実行し、デバイスの正しいクレデンシャルを指定します。</p>
<p>MAC Address</p>	<p>デバイスの MAC アドレス</p>
<p>Image Version</p>	<p>デバイスで現在実行されている Cisco IOS ソフトウェア。</p>


カラム	説明
Platform	シスコ製品の部品番号
Serial Number	シスコデバイスのシリアル番号。
Uptime	デバイスが起動してから、稼働している期間。
Device Role	<p>スキャンプロセス中に、検出された各デバイスに割り当てられているロール。デバイスロールは、ネットワーク内での役目と配置に従って、デバイスを識別およびグループ分けするために使用されます。Cisco DNA Center でデバイスロールを特定できない場合、デバイスロールは不明に設定されます。</p> <p>(注) デバイスロールを手動で変更すると、割り当ては静的のままになります。Cisco DNA Center は、後続のデバイスの再同期中に変更が検知されたとしても、デバイスロールは更新されません。</p> <p>必要に応じて、このカラムのドロップダウンリストを使用して、割り当てられたデバイスロールを変更することができます。次のデバイスロールを使用できます。</p> <ul style="list-style-type: none"> • 不明 • アクセス • [Core] • [Distribution] • [Border Router]
Site	デバイスに割り当てられているサイト。デバイスがどのサイトにも割り当てられていない場合は、[Assign] をクリックします。[Choose a Site] をクリックし、階層からサイトを選択して [Save] をクリックします。詳細については、 About Network Hierarchy (94 ページ) を参照してください。
Last Updated	Cisco DNA Center がデバイスをスキャンし、デバイスに関する新しい情報でデータベースを更新した最新の日付と時刻。
Device Family	ルータ、スイッチ、ハブ、またはワイヤレスコントローラなどの関連するデバイスのグループ。
Device Series	デバイスのシリーズ番号 (Cisco Catalyst 4500 シリーズ スイッチなど)。
Resync Interval	デバイスのポーリング間隔。この間隔は、[設定 (Settings)] でグローバルに設定するか、またはインベントリ内の特定のデバイスに対して設定できます。詳細については、「 Cisco Digital Network Architecture Center 管理者ガイド 」を参照してください。

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

インベントリからのトポロジマップの起動

[Inventory] ウィンドウから、検出されたデバイスのトポロジマップを起動できます。

ステップ 1 Cisco DNA Center のホームページで、[Provisioning] > [Inventory] をクリックします。

ステップ 2 トグルボタン  を使用して、トポロジマップビューとインベントリビューを切り替えます。トポロジマップビューには、デバイスのトポロジとプロビジョニングステータスが表示されます。各ノードをクリックすると、デバイスの詳細が表示されます。トポロジマップの詳細については、「[トポロジについて](#)」を参照してください。

(注) トポロジマップビューを折りたたむには [Collapse all] を、展開するには [Expand All] をクリックします。

Cisco DNA Center インベントリ内のデバイスのタイプ

デバイスは、2つの方法（検出されるか手動で追加される）のいずれかでインベントリに表示されます。Cisco DNA Center インベントリは、次のタイプのデバイスをサポートしています。



(注) サポート対象デバイスの完全なリストについては、[Cisco Digital Network Architecture Center のサポート対象デバイス](#)ドキュメントを参照してください。

- **ネットワーク デバイス**：サポート対象のネットワーク デバイスには、シスコルータ、スイッチ、およびワイヤレスコントローラ（WLC）やアクセスポイント（AP）などのワイヤレスデバイスが含まれます。
- **計算デバイス**：サポート対象の計算デバイスには、Cisco Unified Computing System（UCS）、シスコ エンタープライズ ネットワーク機能仮想化インフラストラクチャ ソフトウェア（NFVIS）を実行しているデバイス、その他のデータセンター デバイスが含まれます。
- **Meraki ダッシュボード**：Cisco Meraki 製品を管理するためのシスコ クラウド管理プラットフォームのダッシュボード。

ネットワーク デバイスの管理

ネットワーク デバイスを追加

ネットワーク デバイスは、インベントリに手動で追加できます。

始める前に

ネットワークデバイスを設定していることを確認します。詳細については、「[ディスカバリの前提条件（14 ページ）](#)」を参照してください。

- ステップ 1** Cisco DNA Center ホームページで、**[プロビジョニング (Provision)]** をクリックします。
インベントリのページには、ディスカバリ プロセス中に収集されたデバイス情報が表示されます。
- ステップ 2** **[Add Device]** をクリックします。
- ステップ 3** **[タイプ (Type)]** ドロップダウンリストから、**[ネットワークデバイス (Network Device)]** を選択します。
- ステップ 4** **[デバイスの IP/名前 (Device IP / Name)]** フィールドで、デバイスの IP アドレスまたは名前を入力します。
- (注) デバイスで HSRP プロトコルを使用している場合は、仮想 IP アドレスではなく、プライマリ IP アドレスを入力する必要があります。
- ステップ 5** 表示されていない場合は、**[SNMP]** エリアを展開します。
- ステップ 6** **[Version]** ドロップダウンリストから、**[V2C]** (SNMP バージョン 2c) または **[V3]** (SNMP バージョン 3) を選択します。
- [V2C]** を選択した場合、次のフィールドを設定します。

表 21: SNMPv2c のクレデンシャル

フィールド	説明
Read	<ul style="list-style-type: none"> • Name/Description : 追加する SNMP v2c 設定の名前または説明。 • Read コミュニティ : デバイス上の SNMP 情報を表示するためにのみ使用される read-only コミュニティ スtring パスワード。 <p>(注) パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。</p>
Write	<ul style="list-style-type: none"> • Name/Description : 追加する SNMP v2c 設定の名前または説明。 • Write コミュニティ : デバイス上の SNMP 情報を変更するために使用される write コミュニティ スtring。 <p>(注) パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。</p>

[V3] を選択した場合、次のフィールドを設定します。

表 22: SNMPv3 のクレデンシャル

フィールド	説明
Name/Description	追加した SNMPv3 設定の名前または説明。
Username	SNMPv3 設定に関連付けられている名前。
Mode	SNMP メッセージを必要とするセキュリティ レベル。次のいずれかのモードを選択します。 <ul style="list-style-type: none"> • noAuthNoPriv : 認証または暗号化を提供しません。 • AuthNoPriv : 認証は提供しますが、暗号化は提供しません。 • AuthPriv : 認証と暗号化の両方を提供します。
Auth Type	使用する認証タイプ (認証モードとして [AuthPriv] または [AuthNoPriv] を選択した場合に有効になります)。次のいずれかの認証タイプを選択します。 <ul style="list-style-type: none"> • SHA : HMAC-SHA に基づく認証。 • MD5 : HMAC-MD5 に基づく認証。

フィールド	説明
Auth Password	<p>SNMPv3 を使用するデバイスから情報にアクセスする際に使用する SNMPv3 パスワード。これらのパスワード（またはパスフレーズ）は、8文字以上にする必要があります。</p> <p>(注)</p> <ul style="list-style-type: none"> 一部のシスコワイヤレスコントローラでは、パスワード（あるいはパスフレーズ）は少なくとも12文字以上である必要があります。ワイヤレスコントローラのパスワードの最小要件を必ず確認してください。パスワードに必要な最低限の文字数が守られないと、デバイスではCisco DNA Centerによる検出、監視、管理が行われなくなります。 パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。
Privacy Type	<p>プライバシータイプ。（認証モードとして [AuthPriv] を選択すると有効になります）。次のいずれかのプライバシータイプを選択します。</p> <ul style="list-style-type: none"> DES : CBC DES-56 規格に基づく認証に DES 56-bit (DES-56) 暗号化を追加。 AES128 : 暗号化の CBC モード AES。 None : プライバシー設定なし。
Privacy Password	<p>DES または AES128 暗号化をサポートしているデバイスで交換されるメッセージを暗号化するための秘密鍵を生成するために使用される SNMPv3 プライバシーパスワード。パスワード（またはパスフレーズ）は、8文字以上にする必要があります。</p> <p>(注)</p> <ul style="list-style-type: none"> 一部のシスコワイヤレスコントローラでは、パスワード（あるいはパスフレーズ）は少なくとも12文字以上である必要があります。ワイヤレスコントローラのパスワードの最小要件を必ず確認してください。パスワードに必要な最低限の文字数が守られないと、デバイスではCisco DNA Centerによる検出、監視、管理が行われなくなります。 パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。

ステップ 7 まだ展開されていない場合は [SNMPの再試行回数とタイムアウト (SNMP RETRIES AND TIMEOUT)] エリアを展開し、次のフィールドを設定します。

表 23: *SNMP Properties*

フィールド	説明
Retries	デバイスへ接続可能な試行回数。有効な値は 1 ~ 3 です。デフォルトは 3 です。

フィールド	説明
Timeout	タイムアウトになるまでにデバイスとの接続の確立を試みる際に、Cisco DNA Center が待機する秒数。有効な値は、5 秒間隔で 1 ~ 300 秒です。デフォルトは 5 秒です。

ステップ 8 まだ展開されていない場合は [CLI] エリアを展開し、次のフィールドを設定します。

表 24: CLI クレデンシャル

フィールド	説明
Protocol	Cisco DNA Center とリモート デバイスとの通信を有効にするネットワーク プロトコル。有効な値は SSH2 または Telnet です。 NETCONF ポートを設定する場合は（次の手順を参照）、ネットワーク プロトコルとして SSH2 を選択する必要があります。
Username	ネットワーク内のデバイスの CLI にログインするために使用する名前。
Password	ネットワーク内のデバイスの CLI にログインするために使用されるパスワード。 セキュリティ上の理由から、確認のためにパスワードをもう一度入力します。 (注) パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。
Enable Password	CLI で高い権限レベルに移るために使用するパスワード。 セキュリティ上の理由から、有効なパスワードをもう一度入力します。 (注) パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。

ステップ 9 まだ展開されていない場合は **NETCONF** 領域を展開し、**ポート** フィールドを設定します。

NETCONF では、CLI プロトコルとして SSH を設定し、SSH クレデンシャルを定義することが必要です。

ステップ 10 [追加 (Add)] をクリックします。

ネットワーク デバイス クレデンシャルの更新

選択したネットワーク デバイスのディスカバリ クレデンシャルを更新することができます。選択したデバイスに対しては、この更新された設定が、グローバル設定やジョブ固有の設定よりも優先されます。

始める前に

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

この手順を実行するには、管理者 (ROLE_ADMIN) またはポリシー管理者 (ROLE_POLICY_ADMIN) 権限、および適切な RBAC スコープが必要です。

- ステップ 1** Cisco DNA Center ホームページで、**[プロビジョニング (Provision)]** をクリックします。
インベントリのページには、ディスカバリ プロセス中に収集されたデバイス情報が表示されます。
- ステップ 2** 更新するネットワーク デバイスを選択します。
- ステップ 3** [Actions] ドロップダウンリストから **[Inventory] > [Edit Device]** の順に選択します。
- ステップ 4** [Edit Device] ダイアログボックスで、[Type] ドロップダウンフィールドから **[Network Device]** を選択します (まだ選択していない場合)。
- ステップ 5** まだ展開されていない場合は、[SNMP] エリアを展開します。
- ステップ 6** [バージョン (Version)] フィールドから、SNMP バージョン ([V2C] または [V3]) を選択します。
- (注) SNMP 資格情報と CLI クレデンシャルの両方が一緒に更新されるため、両方のクレデンシャルを提供することをお勧めします。SNMP 資格情報のみが提供された場合、Cisco DNA Center は SNMP 資格情報のみを保存し、CLI クレデンシャルは更新されません。
- ステップ 7** [V2C] または [V3] のいずれかを選択したかに応じて、次の表に説明されているように、その他のフィールドに情報を入力します。

表 25: SNMPv2c のクレデンシャル

フィールド	説明
Read	<ul style="list-style-type: none"> • Name/Description : 追加する SNMP v2c 設定の名前または説明。 • Read コミュニティ : デバイス上の SNMP 情報を表示するためにのみ使用される read-only コミュニティ ストリング パスワード。 <p>(注) パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。</p>
Write	<ul style="list-style-type: none"> • Name/Description : 追加する SNMP v2c 設定の名前または説明。 • Write コミュニティ : デバイス上の SNMP 情報を変更するために使用される write コミュニティ ストリング。 <p>(注) パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。</p>

表 26: SNMPv3 のクレデンシャル

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

フィールド	説明
Username	SNMPv3 設定に関連付けられている名前。
Mode	SNMP メッセージを必要とするセキュリティ レベル。次のいずれかのモードを選択します。 <ul style="list-style-type: none"> • noAuthNoPriv : 認証または暗号化を提供しません。 • AuthNoPriv : 認証は提供しますが、暗号化は提供しません。 • AuthPriv : 認証と暗号化の両方を提供します。
Auth Type	使用する認証タイプ（認証モードとして [AuthPriv] または [AuthNoPriv] を選択した場合に有効になります）。次のいずれかの認証タイプを選択します。 <ul style="list-style-type: none"> • SHA : HMAC-SHA に基づく認証。 • MD5 : HMAC-MD5 に基づく認証。
Auth Password	SNMPv3 を使用するデバイスから情報にアクセスする際に使用する SNMPv3 パスワード。これらのパスワード（またはパスフレーズ）は、8 文字以上にする必要があります。 <p>(注)</p> <ul style="list-style-type: none"> • 一部のシスコワイヤレスコントローラでは、パスワード（あるいはパスフレーズ）は少なくとも 12 文字以上である必要があります。ワイヤレスコントローラのパスワードの最小要件を必ず確認してください。パスワードに必要な最低限の文字数が守られないと、デバイスでは Cisco DNA Center による検出、監視、管理が行われなくなります。 • パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。
Privacy Type	プライバシータイプ。（認証モードとして [AuthPriv] を選択すると有効になります）。次のいずれかのプライバシータイプを選択します。 <ul style="list-style-type: none"> • DES : CBC DES-56 規格に基づく認証に DES 56-bit (DES-56) 暗号化を追加。 • AES128 : 暗号化の CBC モード AES。 • None : プライバシー設定なし。

フィールド	説明
Privacy Password	DES または AES128 暗号化をサポートしているデバイスで交換されるメッセージを暗号化するための秘密鍵を生成するために使用される SNMPv3 プライバシー パスワード。パスワード (または パスフレーズ) は、8 文字以上にする必要があります。 (注) <ul style="list-style-type: none"> 一部のシスコワイヤレスコントローラでは、パスワード (あるいは パスフレーズ) は少なくとも 12 文字以上である必要があります。ワイヤレス コントローラのパスワードの最小要件を必ず確認してください。パスワードに必要な最低限の文字数が守られないと、デバイスでは Cisco DNA Center による検出、監視、管理が行われなくなります。 パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。

ステップ 8 [SNMP Retries and Timeout] エリアがまだ展開されていなければ展開し、次のフィールドに入力します。

表 27: SNMP Properties

フィールド	説明
Retries	デバイスへ接続可能な試行回数。有効な値は 1 ~ 3 です。デフォルトは 3 です。
Timeout	タイムアウトになるまでにデバイスとの接続の確立を試みる際に、Cisco DNA Center が待機する秒数。有効な値は、5 秒間隔で 1 ~ 300 秒です。デフォルトは 5 秒です。

ステップ 9 CLI エリアがまだ展開されていなければ展開し、次のフィールドに入力します。

(注) SNMP と CLI の両方のクレデンシャルと一緒に更新されるため、どちらのクレデンシャルも提供する必要があります。SNMP 資格情報のみが提供された場合、Cisco DNA Center は SNMP 資格情報のみを保存します。CLI クレデンシャルは更新されません。

表 28: CLI クレデンシャル

フィールド	説明
Protocol	Cisco DNA Center とリモート デバイスとの通信を有効にするネットワーク プロトコル。有効な値は SSH2 または Telnet です。 NETCONF ポートを設定する場合は (次の手順を参照)、ネットワーク プロトコルとして SSH2 を選択する必要があります。
Username	ネットワーク内のデバイスの CLI にログインするために使用する名前。

フィールド	説明
Password	ネットワーク内のデバイスの CLI にログインするために使用されるパスワード。 セキュリティ上の理由から、確認のためにパスワードをもう一度入力します。 (注) パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。
Enable Password	CLI で高い権限レベルに移るために使用するパスワード。 セキュリティ上の理由から、有効なパスワードをもう一度入力します。 (注) パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。

ステップ 10 まだ展開されていない場合は **NETCONF** 領域を展開し、**ポート** フィールドを設定します。
NETCONF では、CLI プロトコルとして SSH を設定し、SSH クレデンシャルを定義することが必要です。

ステップ 11 [HTTP(S)] エリアを展開して（まだ展開されていない場合）、次のフィールドを入力します。

- **ユーザ名**：HTTPS 接続の認証に使用される名前。
- **パスワード**：HTTPS 接続の認証に使用されるパスワード。
- **ポート**：HTTPS トラフィックで使用される TCP/UDP ポートの数。デフォルトはポート番号 443（HTTPS の既知のポート）です。

ステップ 12 [更新 (Update)] をクリックします。

計算デバイスの管理

計算デバイスの追加

計算デバイスは、インベントリに手動で追加できます。計算デバイスには、Cisco Unified Computing System (UCS) などのデバイス、Cisco Enterprise ネットワーク機能の仮想化インフラストラクチャソフトウェア (NFVIS) を実行しているデバイス、およびその他のデータセンター デバイスが含まれます。

ステップ 1 Cisco DNA Center ホームページで、[プロビジョニング (Provision)] をクリックします。
インベントリのページには、ディスカバリ プロセス中に収集されたデバイス情報が表示されます。

ステップ 2 [Add Device] をクリックします。

ステップ 3 [タイプ (Type)] ドロップダウン リストから、[計算デバイス (Compute Device)] を選択します。

ステップ 4 [デバイスの IP/名前 (Device IP/Name)] フィールドで、デバイスの IP アドレスまたは名前を入力します。

ステップ 5 表示されていない場合は [HTTP(S)] エリアを展開し、次のフィールドを設定します。

- **ユーザ名** : HTTPS 接続の認証に使用される名前。
- **パスワード** : HTTPS 接続の認証に使用されるパスワード。
- **ポート** : HTTPS トラフィックで使用される TCP/UDP ポートの数。デフォルトはポート番号 443 (HTTPS の既知のポート) です。

ステップ 6 表示されていない場合は、[SNMP] エリアを展開します。

ステップ 7 [Version] ドロップダウンリストから、[V2C] (SNMP バージョン 2c) または [V3] (SNMP バージョン 3) を選択します。

[V2C] を選択した場合、次のフィールドを設定します。

表 29: SNMPv2c のクレデンシャル

フィールド	説明
Read	<ul style="list-style-type: none"> • Name/Description : 追加する SNMP v2c 設定の名前または説明。 • Read コミュニティ : デバイス上の SNMP 情報を表示するためにのみ使用される read-only コミュニティストリングパスワード。 <p>(注) パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。</p>
Write	<ul style="list-style-type: none"> • Name/Description : 追加する SNMP v2c 設定の名前または説明。 • Write コミュニティ : デバイス上の SNMP 情報を変更するために使用される write コミュニティストリング。 <p>(注) パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。</p>

[V3] を選択した場合、次のフィールドを設定します。

表 30: SNMPv3 のクレデンシャル

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

フィールド	説明
Mode	SNMP メッセージを必要とするセキュリティ レベル。次のいずれかのモードを選択します。 <ul style="list-style-type: none"> • noAuthNoPriv : 認証または暗号化を提供しません。 • AuthNoPriv : 認証は提供しますが、暗号化は提供しません。 • AuthPriv : 認証と暗号化の両方を提供します。
Auth Type	使用する認証タイプ（認証モードとして [AuthPriv] または [AuthNoPriv] を選択した場合に有効になります）。次のいずれかの認証タイプを選択します。 <ul style="list-style-type: none"> • SHA : HMAC-SHA に基づく認証。 • MD5 : HMAC-MD5 に基づく認証。
Auth Password	SNMPv3 を使用するデバイスから情報にアクセスする際に使用する SNMPv3 パスワード。これらのパスワード（またはパスフレーズ）は、8 文字以上にする必要があります。 <p>(注)</p> <ul style="list-style-type: none"> •一部のシスコ ワイヤレス コントローラでは、パスワード（あるいはパスフレーズ）は少なくとも 12 文字以上である必要があります。ワイヤレス コントローラのパスワードの最小要件を必ず確認してください。パスワードに必要な最低限の文字数が守られないと、デバイスでは Cisco DNA Center による検出、監視、管理が行われなくなります。 •パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。
Privacy Type	プライバシー タイプ。（認証モードとして [AuthPriv] を選択すると有効になります）。次のいずれかのプライバシー タイプを選択します。 <ul style="list-style-type: none"> • DES : CBC DES-56 規格に基づく認証に DES 56-bit (DES-56) 暗号化を追加。 • AES128 : 暗号化の CBC モード AES。 • None : プライバシー設定なし。

フィールド	説明
Privacy Password	DES または AES128 暗号化をサポートしているデバイスで交換されるメッセージを暗号化するための秘密鍵を生成するために使用される SNMPv3 プライバシーパスワード。パスワード (またはパスフレーズ) は、8 文字以上にする必要があります。 (注) <ul style="list-style-type: none"> 一部のシスコ ワイヤレス コントローラでは、パスワード (あるいはパスフレーズ) は少なくとも 12 文字以上である必要があります。ワイヤレスコントローラのパスワードの最小要件を必ず確認してください。パスワードに必要な最低限の文字数が守られないと、デバイスでは Cisco DNA Center による検出、監視、管理が行われなくなります。 パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。

ステップ 8 まだ展開されていない場合は [CLI] エリアを展開し、次のフィールドを設定します。

表 31: CLI クレデンシャル

フィールド	説明
Protocol	Cisco DNA Center とリモート デバイスとの通信を有効にするネットワーク プロトコル。デフォルトでは、[SSH2] が選択され、変更することはできません。
Username	ネットワーク内のデバイスの CLI にログインするために使用する名前。
Password	ネットワーク内のデバイスの CLI にログインするために使用されるパスワード。 セキュリティ上の理由から、確認のためにパスワードをもう一度入力します。 (注) パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。
Enable Password	CLI で高い権限レベルに移るために使用するパスワード。 セキュリティ上の理由から、有効なパスワードをもう一度入力します。 (注) パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。

ステップ 9 [追加 (Add)] をクリックします。

計算デバイス クレデンシャルの更新

選択した計算デバイスのディスカバリ クレデンシャルを更新することができます。選択したデバイスに対しては、この更新された設定が、グローバル設定やジョブ固有の設定よりも優先されます。

始める前に

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

-
- ステップ 1 Cisco DNA Center ホームページで、**[プロビジョニング (Provision)]** をクリックします。
インベントリのページには、ディスカバリ プロセス中に収集されたデバイス情報が表示されます。
 - ステップ 2 更新するデバイスを選択します。
 - ステップ 3 **[Actions]** ドロップダウンリストから **[Inventory] > [Edit Device]** の順に選択します。
 - ステップ 4 **[Edit Device]** ダイアログ ボックスの **[Type]** ドロップダウンリストで、**[Compute Device]** を選択します。
 - ステップ 5 まだ展開されていない場合は、**[HTTP (S)]** エリアを展開します。
 - ステップ 6 **[ユーザ名 (Username)]** および **[パスワード (Password)]** フィールドに、ユーザ名とパスワードを入力します。
 - ステップ 7 **[ポート (Port)]** フィールドにポート番号を入力します。
 - ステップ 8 **[更新 (Update)]** をクリックします。
-

Meraki ダッシュボードの管理

Meraki ダッシュボードの統合

Meraki ダッシュボードと Cisco DNA Center を統合できます。

-
- ステップ 1 Cisco DNA Center ホームページで、**[プロビジョニング (Provision)]** をクリックします。
インベントリのページには、ディスカバリ プロセス中に収集されたデバイス情報が表示されます。
 - ステップ 2 **[Add Device]** をクリックします。
 - ステップ 3 **[Add Device]** ダイアログボックスの **[Type]** ドロップダウンリストで、**[Meraki Dashboard]** を選択します。
 - ステップ 4 まだ展開されていない場合は、**[HTTP (S)]** エリアを展開します。
 - ステップ 5 **[API キー/パスワード (API Key/Password)]** フィールドで、Meraki ダッシュボードへのアクセスに使用する API キーとパスワードのクレデンシアルを入力します。

Cisco DNA Center Cisco DNA Center は、Meraki ダッシュボードからインベントリデータを収集して、情報を表示します。
-

Meraki ダッシュボード クレデンシアルの更新

選択したデバイスの Meraki ダッシュボードのログイン情報を更新できます。選択したデバイスに対しては、この更新された設定が、グローバル設定やジョブ固有の設定よりも優先されず。

始める前に

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

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

インベントリのページには、ディスカバリ プロセス中に収集されたデバイス情報が表示されます。

ステップ 2 更新するデバイスを選択します。

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

ステップ 4 [Edit Device] ダイアログボックスの [Type] ドロップダウンリストで、**[Meraki Dashboard]** を選択します。

ステップ 5 まだ展開されていない場合は、**[HTTP (S)]** エリアを展開します。

ステップ 6 [API キー/パスワード (API Key / Password)] フィールドで、Meraki ダッシュボードへのアクセスに使用する API キーとパスワードのクレデンシャルを入力します。

ステップ 7 [ポート (Port)] フィールドにポート番号を入力します。

ステップ 8 **[更新 (Update)]** をクリックします。

デバイスのフィルタ



(注) フィルタを削除または変更するには、**[リセット (Reset)]** をクリックします。

始める前に

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

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

インベントリのページには、ディスカバリ プロセス中に収集されたデバイス情報が表示されます。

ステップ 2 **[Filter]** をクリックします。

次のフィルタが表示されます。

- **Tag**
- **Device Name**
- **IP Address**
- **Device Family**
- **Site**

- **MAC Address**
- **Reachability**
- **Device Role**
- **Image Version**
- **Up Time**
- **Last Sync Status**
- **Resync Interval**
- **Serial Number**
- **Device Series**
- **Platform**

ステップ3 選択したフィルタフィールドに適切な値を入力します。たとえば、[デバイス名 (Device Name)] フィルタには、デバイスの名前を入力します。

Cisco DNA Center では、その他のフィールドに値を入力すると、オートコンプリート値が提示されます。推奨されるいずれかの値を選択するか、または値の入力を終了します。

また、これらのフィルタではワイルドカード（アスタリスク）を使用することもできます。たとえば、文字列値の先頭、末尾、または中間にアスタリスクを含む値を入力できます。

ステップ4 [Apply] をクリックして情報をフィルタ処理します。

[Device Type] と [Reachability] のクイックフィルタを使用して、デバイスをフィルタ処理することもできます。さらに、左側のペインに表示されている任意のサイトをクリックして、デバイスに割り当てられているサイトに基づいてデバイスをフィルタ処理できます。

[デバイス (Devices)] テーブルに表示されるデータは、選択したフィルタに従って自動で更新されます。

(注) フィルタごとに複数のフィルタタイプと複数の値を使用できます。

ステップ5 (オプション) 必要に応じて、フィルタを追加します。

フィルタを削除するには、対応するフィルタ値の横にある **x** アイコンをクリックします。

デバイスのロールの変更（インベントリ）

ディスカバリ プロセスに、Cisco DNA Center は検出された各デバイスにロールを割り当てます。デバイスのロールは、デバイスを特定してグループ化するためと、トポロジツールでネットワーク トポロジマップのデバイスの配置を決定するために使用されます。最上位の層は、インターネットです。最下層のデバイスは、次のロールのいずれかに割り当てられます。

表 32: デバイスのロールとトポロジの位置

トポロジの位置	デバイス ロール
階層 1	インターネット (構成不可)
階層 2	ボーダー ルータ
階層 3	コア
階層 4	配信
階層 5	アクセス
階層 6	不明

始める前に

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

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

インベントリのページには、ディスカバリ プロセス中に収集されたデバイス情報が表示されます。

ステップ 2 ロールを変更するデバイスを見つけて、[Device Role] 列の鉛筆アイコンをクリックし、[Update Device Role] ダイアログボックスからロールを選択します。有効な選択肢は、[Unknown]、[Access]、[Core]、[Distribution]、または [Border Router] です。

デバイスロールは次の手順で、[Edit Device] ダイアログボックスでも更新できます。

- ロールを変更するデバイスを選択します。
- [Actions] > [Inventory] > [Edit Device] の順に選択します。
- [Role] タブをクリックし、[Device Role] ドロップダウンリストから適切なロールを選択します。

(注) デバイス ロールを手動で変更すると、割り当ては静的のままになります。Cisco DNA Center は、後続のデバイスの再同期中に変更が検知されたとしても、デバイス ロールは更新されません。

デバイスの管理 IP アドレスの更新

デバイスの管理 IP アドレスを更新できます。



(注) 複数のデバイスを同時に更新することはできません。また、Meraki デバイスの管理 IP アドレスは更新できません。

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

インベントリのページには、ディスカバリ プロセス中に収集されたデバイス情報が表示されます。

ステップ 2 更新するデバイスを選択します。

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

[Edit Device] ダイアログボックスが表示されます。

ステップ 4 [Management IP] タブをクリックし、[Device IP/DNS Name] フィールドに新しい管理 IP アドレスを入力します。

(注) 新しい管理 IP アドレスが Cisco DNA Center から到達可能であり、デバイス クレデンシャルが正しいことを確認します。そうでない場合、デバイスが管理対象外状態になる可能性があります。

次のタスク

デバイスを再プロビジョニングして、送信元インターフェイスの設定を更新します。

デバイスの再同期間隔の更新

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

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

始める前に

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

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

インベントリのページには、ディスカバリ プロセス中に収集されたデバイス情報が表示されます。

ステップ 2 更新するデバイスを選択します。

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

[Edit Device] ダイアログボックスが表示されます。

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

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

ステップ 6 [更新 (Update)]をクリックします。

デバイス情報の再同期

選択したデバイスのデバイス情報は、再同期間隔の設定に関わらず、直ちに再同期できます。同時に最大 40 台のデバイスを再同期することができます。

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

インベントリのページには、ディスカバリ プロセス中に収集されたデバイス情報が表示されます。

ステップ 2 情報を収集するデバイスを選択します。

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

ステップ 4 [OK] をクリックして、アクションを確認します。

ネットワーク デバイスの削除

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

始める前に

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

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

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

インベントリのページには、ディスカバリ プロセス中に収集されたデバイス情報が表示されます。

ステップ 2 削除するデバイスの横にあるチェックボックスをオンにします。

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

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

ステップ 4 [OK] をクリックして、アクションを確認します。

コマンドランナーを起動（インベントリ）

[インベントリ (Inventory)] ウィンドウで選択したデバイスのコマンドランナー アプリケーションを起動することができます。

始める前に

コマンドランナー アプリケーションをインストールします。詳細については、[Cisco Digital Network Architecture Center 管理者ガイド](#)を参照してください。

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

インベントリのページには、ディスカバリ プロセス中に収集されたデバイス情報が表示されます。

ステップ 2 コマンドを実行するデバイスを選択します。

ステップ 3 [Actions] ドロップダウンリストから、[Others] > [Launch Command Runner] を選択します。

実行可能なコマンドの詳細、およびこれらのコマンドの実行方法については、[デバイスの診断コマンドを実行 \(165 ページ\)](#) を参照してください。

CSVファイルを使用してデバイス設定をインポート/エクスポートします。

CSV ファイルのインポート

CSV ファイルを使用して、別のソースから Cisco DNA Center にデバイスの設定やサイトをインポートできます。サンプルテンプレートをダウンロードする場合は、[Provision Devices] ページに移動し、[Actions] > [Inventory] > [Import Inventory] を選択します。[Download Template] をクリックして、サンプル CSV ファイルテンプレートをダウンロードします。

CSV ファイルを使用してデバイス設定をインポート/エクスポートします。

CSV ファイルを使用してデバイスまたはサイト設定をインポートする場合、Cisco DNA Center がデバイスをどれだけ管理できるのかは CSV ファイルに指定する情報に依存します。CLI ユーザ名、パスワード、およびイネーブルパスワードの値を指定しない場合、Cisco DNA Center の機能が制限され、デバイス設定の変更、デバイス ソフトウェア イメージの更新、および他の重要な機能の実行を行うことができません。

CSV ファイルでクレデンシアル プロファイルを指定し、対応するクレデンシアルをデバイスのセットに適用できます。クレデンシアル プロファイルを指定して、CSV ファイルに手動で値も入力する場合、手動入力されたクレデンシアルが優先され、デバイスは手動入力されたクレデンシアルとクレデンシアル プロファイルの組み合わせに基づいて管理されます。たとえば、手動で入力した SNMP ログイン情報に加えて、SNMP および SSH または Telnet のログイン情報を含むログイン情報プロファイルが CSV ファイルに含まれている場合、デバイスは手動で入力された SNMP ログイン情報とログイン情報プロファイル内の SSH または Telnet ログイン情報に基づいて管理されます。Telnet は非推奨です。



- (注) また、指定したプロトコルに対応するフィールドにも値を入力する必要があります。たとえば、SNMPv3 を指定した場合、SNMPv3 のユーザ名や認証パスワードなど、サンプルの CSV ファイルの SNMPV3 フィールドに値を指定する必要があります。

Cisco DNA Center の部分的なインベントリ収集の場合は、CSV ファイルに次の値を指定する必要があります。

- デバイスの IP アドレス
- SNMP バージョン
- SNMP 読み取り専用コミュニティ ストリング
- SNMP 書き込みコミュニティ ストリング
- SNMP 再試行値
- SNMP タイムアウト値

Cisco DNA Center の完全なインベントリ収集では、CSV ファイルに以下の値を提供する必要があります。

- デバイスの IP アドレス
- SNMP バージョン
- SNMP 読み取り専用コミュニティ ストリング
- SNMP 書き込みコミュニティ ストリング
- SNMP 再試行値
- SNMP タイムアウト値
- プロトコル

- CLI ユーザ名
- CLI パスワード
- CLI イネーブルパスワード
- CLI タイムアウト値

CSV ファイル エクスポート

Cisco DNA Center では、すべてまたは選択したデバイスを含む CSV ファイルをインベントリに作成できます。このファイルを作成するには、ファイルに含まれる設定データを保護するパスワードを入力する必要があります。

CSV ファイルからのデバイス設定のインポート

CSV ファイルからデバイス設定をインポートできます。

-
- ステップ 1** Cisco DNA Center ホームページで、**[プロビジョニング (Provision)]** をクリックします。
インベントリのページには、ディスカバリ プロセス中に収集されたデバイス情報が表示されます。
- ステップ 2** [Actions] ドロップダウンリストから、**[Inventory] > [Import Inventory]** を選択してデバイスのログイン情報をインポートします。
- ステップ 3** [一括インポート (Bulk Import)] ダイアログボックスのボックスエリアに CSV ファイルをドラッグアンドドロップするか、点線のボックスエリアをクリックして CSV ファイルを参照します。
- ステップ 4** [Import] をクリックします。
-

デバイス設定のエクスポート

選択したデバイスに関する特定のデータを CSV ファイルにエクスポートできます。CSV ファイルは圧縮されます。



注意 CSV ファイルにはエクスポートされたデバイスに関する機密情報が含まれているため、取り扱いには注意してください。特別な権限を持つユーザーのみがデバイスのエクスポートを行うことを確認します。

-
- ステップ 1** Cisco DNA Center ホームページで、**[プロビジョニング (Provision)]** をクリックします。
インベントリのページには、ディスカバリ プロセス中に収集されたデバイス情報が表示されます。

ステップ 2 特定のデバイスのみを設定情報をエクスポートするには、含めるデバイスの横にあるチェックボックスをオンにします。すべてのデバイスを含めるには、デバイスリストの最上部にあるチェックボックスをオンにします。

ステップ 3 [Actions] ドロップダウンリストから、[Inventory] > [Export Inventory] を選択してデバイス設定をエクスポートします。

[エクスポート] ダイアログボックスが表示されます。

ステップ 4 [Select Export Type] で、[Data] オプションボタンをクリックします。

ステップ 5 CSV ファイルに含めるデータの横にあるチェックボックスをオンにします。

ステップ 6 [エクスポート (Export)] をクリックします。

(注) ブラウザの設定によっては、圧縮したファイルを保存したり、開くことができます。

Export Device Credentials

デバイスのクレデンシャル CSV ファイルにエクスポートできます。不要なアクセスからファイルを保護するために、パスワードを設定する必要があります。ファイルを開くことができるように、受信者にパスワードを提供する必要があります。



注意 CSV ファイルにはエクスポートされたデバイスのすべてのクレデンシャルがリストされているため、取り扱いには注意してください。特別な権限を持つユーザーのみがデバイスのエクスポートを行うことを確認します。

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

インベントリのページには、ディスカバリ プロセス中に収集されたデバイス情報が表示されます。

ステップ 2 CSV ファイルに含めるデバイスの横にあるチェックボックスをオンにします。すべてのデバイスを含めるには、リストの最上部にあるチェックボックスをオンにします。

ステップ 3 [Actions] ドロップダウンリストから、[Inventory] > [Export Inventory] を選択してデバイスのログイン情報をエクスポートします。

[エクスポート] ダイアログボックスが表示されます。

ステップ 4 [エクスポートタイプの選択 (Select Export Type)] で、[クレデンシャル (Credentials)] オプション ボタンをクリックします。

ステップ 5 [Include SSH key information] チェックボックスをオンにして、エクスポートした CSV ファイルに、最初の SSH キー、最初の SSH キーアルゴリズム、現在の SSH キー、現在の SSH キーアルゴリズムなどの情報を含めます。

ステップ 6 [パスワード (Password)] フィールドに、エクスポートされた CSV ファイルを暗号化するために使用するパスワードを入力します。

(注) エクスポートしたファイルを開くには、パスワードが必要です。

ステップ7 暗号化パスワードを確認し、[エクスポート (Export)] をクリックします。

(注) ブラウザの設定によっては、圧縮したファイルを保存したり、開くことができます。

故障したデバイスの交換

障害のあるデバイスを、デバイスインベントリにある交換用デバイスと交換できます。

始める前に

- 故障したデバイスのソフトウェア イメージバージョンをイメージリポジトリにインポートしてから、交換するデバイスにマークを付ける必要があります。
- 故障したデバイスは到達不能な状態になっている必要があります。
- 交換用デバイスがプラグアンドプレイ (PnP) で Cisco DNA Center をオンボードしている場合は、障害のあるデバイスをユーザ定義のサイトに割り当てる必要があります。
- 返品許可 (RMA) ワークフローのトリガー中は、交換用デバイスがプロビジョニング状態であってはなりません。

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

[Inventory] ページには、ディスカバリプロセス中に収集されたデバイス情報が表示されます。

ステップ2 交換する故障したデバイスを選択します。

ステップ3 [Actions] ドロップダウンリストから、[Inventory] > [Device Replacement] > [Mark Device for Replacement] を選択します。

ステップ4 [Mark For Replacement] ウィンドウで、[Mark] をクリックします。

ステップ5 [Inventory] ドロップダウンリストから、[Marked for Replacement] を選択します。

交換用としてマークされたデバイスのリストが表示されます。

ステップ6 (オプション) デバイスを交換しない場合は、デバイスを選択して、[Actions] > [Unmark for Replacement] を選択します。

ステップ7 交換するデバイスを選択し、[Actions] > [Replace Device] を選択します。

ステップ8 [Replace Device] ウィンドウで、[Start] をクリックします。

ステップ9 [Replace Device] ページで、[Available Replacement Devices] エリアの下にあるデバイスを選択します。

ステップ10 [次へ (Next)] をクリックします。

ステップ11 [Replacement Summary] を確認し、[Next] をクリックします。

ステップ 12 デバイスを今すぐ交換するか、後で交換を行うようスケジュールするかを選択し、[Submit] をクリックします。

RMA ワークフローが開始されます。

ステップ 13 [Monitor Replacement Status] をクリックして、[Provision] ページに移動します。

ステップ 14 交換用デバイスの [Replace Status] をクリックすると、次のように RMA ワークフローの進捗状況が表示されます。

- 交換用デバイスにソフトウェアイメージを配布しています。
- デバイスのソフトウェアイメージをアクティブ化しています。
(注) 交換用デバイスの上位デバイスが故障したデバイスの上位デバイスと異なる場合、交換用デバイスにプッシュされたソフトウェアイメージには互換性がないことがあります。その場合、交換用デバイスのイメージのアクティブ化は ROM モニタ (ROMmon) モードになります。
- ライセンスの展開
- VLAN とスタートアップ コンフィギュレーションのプロビジョニング
- デバイスをリロードする
- 到達可能性のチェック
- Cisco ISE を使用した認証 Cisco ISE
- PKI 証明書の取り消し
- 故障したデバイスの削除
- 交換用デバイスの同期

Cisco DNA Center での RMA ワークフローの制限事項 Cisco DNA Center

- RMA は、類似デバイスの交換のみサポートしています。たとえば Cisco Catalyst 3650 スイッチは、別の Cisco Catalyst 3650 スイッチとのみ交換できます。また、障害のあるデバイスと交換用デバイスのプラットフォーム ID も同じである必要があります。
- 交換用デバイスのスーパーバイザエンジンが障害のあるデバイスと異なる場合、交換用デバイスにプッシュされたソフトウェアイメージは互換性がない可能性があります。その場合、交換用デバイスのイメージのアクティブ化は ROM モニタ (ROMmon) モードになります。

- RMA は、LAN の自動化によってプロビジョニングされたすべてのスイッチ、ルータ、SDA デバイス、およびデバイスの交換をサポートします（スタック構成のスイッチ、Nexus スイッチ、アクセスポイント、デュアル スーパーバイザ エンジン を備えたデバイス、ワイヤレスコントローラを除く）。



(注) SDA デバイスの場合、SDA ネットワークには DHCP サーバがなく、PnP を介してデバイスを追加できないため、交換用デバイスを Cisco DNA Center に手動で追加する必要があります。

- RMA ワークフローでは、次の場合にのみデバイスの交換が可能です。
 - 障害のあるデバイスと交換用デバイスの両方に同じ拡張カードが搭載されている。
 - 両方のデバイスのポート数が拡張カードによって変わらない。
- 交換用デバイスが、障害のあるデバイスが接続されていたポートと同じポートに接続されていることを確認してください。
- Cisco DNA Center レガシーライセンスの導入はサポートされていません。また、RMA ワークフローでは、障害のあるデバイスを CSSM に登録したり、問題のあるデバイスライセンスを CSSM から削除したりはされません。
 - 障害のあるデバイスにインストールされているソフトウェアイメージが Cisco IOS XE 16.8 よりも前のバージョンの場合、[License Details] ウィンドウにはネットワークと機能のライセンスの詳細が表示されず、警告メッセージも表示されません。そのため、障害のあるデバイスに設定されているレガシー ネットワーク ライセンスを確認し、交換用デバイスに同じレガシー ネットワーク ライセンスを手動で適用する必要があります。
 - 障害のあるデバイスにインストールされているソフトウェアイメージが Cisco IOS XE 16.8 以降の場合は、[License Details] ウィンドウにネットワークライセンスの詳細（たとえば、レガシーまたはネットワーク）と機能ライセンス（IP Base、IP Service、LAN Base など）が表示されます。障害のあるデバイスを交換対象としてマークしている際に、次の警告メッセージが表示されます。

「故障した一部のデバイスに DNA ライセンスがありません。（*Some of the faulty devices don't have a DNA license.*） 交換用デバイスに、障害のあるデバイスで有効になっていたのと同じレガシーライセンスがあることを確認してください。（*Please ensure your replacement device has the same Legacy license of the faulty device enabled.*）」
- 交換用デバイスと障害のあるデバイスのレガシー ネットワーク ライセンスが一致しない場合は、ライセンスの展開中に次のエラーメッセージが表示されます。

「Cisco DNA Center はレガシーライセンスの展開をサポートしていません。（*Cisco DNA Center doesn't support legacy license deployment.*） そのため、交換用デバイスで障害のあるデバイスのライセンスを手動で更新し、再同期してから続行してください。（*So manually update the faulty device license on the replacement device and resync before proceeding.*）」

- Cisco DNA Center 障害のあるデバイスのアーカイブに保存されている実行中コンフィギュレーションと VLAN 設定を交換用デバイスにプロビジョニングします。最新のアーカイブ後に古いデバイスに何らかの設定変更が加えられた場合、交換用デバイスの設定が最新ではない可能性があります。
- 交換用デバイスが PnP DHCP 機能によってオンボードされる場合は、リロードのたびにデバイスが同じ IP アドレスを取得し、DHCP のリースタイムアウトが 2 時間を超えていることを確認してください。



第 5 章

ソフトウェア イメージの管理

- [イメージリポジトリについて \(75 ページ\)](#)
- [ソフトウェア イメージの整合性検証 \(76 ページ\)](#)
- [ソフトウェア イメージの表示 \(76 ページ\)](#)
- [推奨されるソフトウェア イメージの使用 \(77 ページ\)](#)
- [ソフトウェア イメージのインポート \(77 ページ\)](#)
- [デバイスファミリへのソフトウェア イメージの割り当て \(78 ページ\)](#)
- [デバイスのソフトウェア イメージをインストール モードでアップロード \(79 ページ\)](#)
- [ゴールデン ソフトウェアのイメージについて \(80 ページ\)](#)
- [ゴールデン ソフトウェア イメージの指定 \(80 ページ\)](#)
- [ソフトウェア イメージのプロビジョニング \(81 ページ\)](#)

イメージ リポジトリについて

Cisco DNA Center Cisco DNA Center は、ネットワークにあるデバイスのすべてのソフトウェア イメージ、Software Maintenance Update (SMU)、サブパッケージ、ROMMON イメージなどを保存します。イメージリポジトリには次の機能があります。

- **イメージリポジトリ**：Cisco DNA Center はイメージタイプとバージョンに従い、固有のソフトウェア イメージをすべて保存します。ユーザはソフトウェア イメージの表示、インポート、および削除ができます。
- **プロビジョニング**：ソフトウェア イメージをネットワーク内のデバイスにプッシュできます。

イメージリポジトリ機能を使用する前に、Catalyst 3K、4K、および 6K などの古いデバイスで Transport Layer Security (TLS) プロトコルを有効にする必要があります。システムアップグレード後は、TLS を再度有効にする必要があります。詳細については、[Cisco Digital Network Architecture Center 管理者ガイド \[英語\]](#) の「Configure Security for Cisco DNA Center」を参照してください。

ソフトウェアイメージの整合性検証

整合性検証アプリケーションでは、デバイスの感染を示す予期しない変更や無効な値がないか、Cisco DNA Centerに格納されたソフトウェアイメージをモニタします。システムは、インポートプロセス中に、インポートしているイメージのソフトウェアおよびハードウェアプラットフォームのチェックサム値と、Known Good Values (KGV) ファイルのプラットフォームで識別されたチェックサム値を比較して、2つの値の一致を確認することで、イメージの整合性を決定します。

整合性検証アプリケーションで現在の KGV ファイルを使用して選択したソフトウェアイメージを検証できない場合は、[Image Repository] ウィンドウにメッセージが表示されます。整合性検証アプリケーションおよび KGV ファイルのインポートの詳細については、[Cisco Digital Network Architecture Center 管理者ガイド \[英語\]](#) を参照してください。

ソフトウェアイメージの表示

ディスカバリを実行するか、手動でデバイスを追加した後、Cisco DNA Center は、デバイスのソフトウェアイメージ、SMU、およびサブパッケージに関する情報を自動的に保存します。

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

ソフトウェアイメージは、デバイスタイプに基づいて編成され、表示されます。デフォルトでは、物理デバイス用のソフトウェアイメージが表示されます。仮想デバイスのソフトウェアイメージを表示するには、[Virtual] タブに切り替えます。

ステップ 2 [Image Name] 列で、下向き矢印をクリックすると、指定されたデバイスタイプファミリーのすべてのソフトウェアイメージを表示できます。[イメージを使用 (Using Image)] 列は、[イメージ名 (Image Name)] フィールドで示された特定のイメージを使用しているデバイス数を示します。番号のリンクをクリックすると、イメージを使用しているデバイスを表示できます。

ステップ 3 [Version] 列で、[Add On] リンクをクリックすると、適用可能な [SMUs]、[Subpackages]、[ROMMON]、[APSP]、および基本イメージの [APDP] アップグレードが表示されます。

サブパッケージは、既存の基本イメージに追加できる追加の機能です。ここには、イメージファミリーと基本イメージのバージョンに一致するサブパッケージバージョンが表示されます。

AP サービスパック (APSP) と AP デバイスパック (APDP) は、ワイヤレスコントローラに関連付けられた AP をアップグレードするためのイメージです。

- 新しい AP ハードウェアモデルが導入されると、既存のワイヤレスネットワークへの接続に APDP が使用されます。
- 関連付けられた AP の場合、重要な AP バグ修正が APSP によって適用されます。

(注) いずれかの SMU をゴールデンとしてタグ付けすると、基本イメージがインストールされたときに、それが自動的に有効化されます。


サブパッケージはゴールデンとしてタグ付けすることはできません。

ROMMON のアップグレードでは、[cisco.com](https://www.cisco.com) の設定が必須です。デバイスが追加されると、該当するデバイスの最新の ROMMON の詳細が [cisco.com](https://www.cisco.com) から取得されます。また、基本イメージのインポートまたは基本イメージのタグ付けがある場合、ROMMON イメージが [cisco.com](https://www.cisco.com) から自動的にダウンロードされます。

ステップ 4 [Device Role] 列で、これが「ゴールデン」ソフトウェアイメージであることを示すデバイスロールを選択します。詳細については、[ゴールデンソフトウェアのイメージについて \(80 ページ\)](#) および [ゴールデンソフトウェアイメージの指定 \(80 ページ\)](#) を参照してください。

推奨されるソフトウェアイメージの使用

Cisco DNA Center は、管理しているデバイスの Cisco 推奨のソフトウェアイメージを表示します。ユーザーはそこから選択できます。

ステップ 1 Cisco DNA Center のホーム ページで、 > [システム設定 (System Settings)] > [設定 (Settings)] > [Cisco クレデンシャル (Cisco Credentials)] の順に選択し、Cisco.com へ接続するための正しいクレデンシャルが入力されていることを確認します。

ステップ 2 [Design] > [Image Repository] を選択します。

Cisco DNA Center は、デバイス タイプに従って Cisco 推奨のソフトウェアイメージを表示します。

ステップ 3 推奨のイメージをゴールデンとして指定します。詳細については、「[ゴールデンソフトウェアイメージの指定 \(80 ページ\)](#)」を参照してください。

Cisco 推奨のイメージをゴールデンとして指定すると、Cisco DNA Center はそのイメージを [cisco.com](https://www.cisco.com) から自動的にダウンロードします。

ステップ 4 推奨のソフトウェアイメージをネットワーク内のデバイスにプッシュします。詳細については、「[ソフトウェアイメージのプロビジョニング \(81 ページ\)](#)」を参照してください。

ソフトウェアイメージのインポート

ローカルコンピュータまたは URL から、ソフトウェアイメージおよびソフトウェアイメージ更新プログラムをインポートできます。

-
- ステップ 1** Cisco DNA Center のホーム ページで、[設計 (Design)] > [イメージリポジトリ (Image Repository)] を選択します。
- ステップ 2** [Import] をクリックします。
- ステップ 3** [ファイルの選択 (Choose File)] をクリックして、ローカルに保存されているソフトウェア イメージまたはソフトウェア イメージ更新プログラムに移動するか、[イメージの URL を入力 (Enter image URL)] をクリックしてソフトウェア イメージまたはソフトウェア イメージ更新プログラムのインポート元となる HTTP または FTP ソースを指定します。
- ステップ 4** インポートするイメージがサードパーティ (シスコ以外) ベンダー向けの場合、[ソース (Source)] で [サードパーティ (Third Party)] を選択します。次に [アプリケーションタイプ (Application Type)] を選択して、デバイスの [ファミリ (Family)] を示し、[ベンダー (Vendor)] を特定します。
- ステップ 5** [Import] をクリックします。
ウィンドウにインポートの進行が表示されます。
- ステップ 6** [タスクの表示 (Show Tasks)] をクリックして、イメージが正常にインポートされたことを確認します。
SMU をインポートした場合、Cisco DNA Center は自動的に SMU を適切なソフトウェア イメージに適用し、対応するソフトウェア イメージの下に [アドオン (Add-On)] リンクが表示されます。
- ステップ 7** [アドオン (Add-On)] リンクをクリックすると、SMU が表示されます。
- ステップ 8** [デバイスのロール (Device Role)] フィールドで、この SMU をゴールデンとしてマークするロールを選択します。詳細については、「[ゴールデンソフトウェア イメージの指定 \(80 ページ\)](#)」を参照してください。
- (注) SMU をゴールデンとしてマークするには、事前に対応するソフトウェア イメージをゴールデンとしてマークしている必要があります。
-

デバイスファミリへのソフトウェアイメージの割り当て

ソフトウェアイメージをインポートしたら、使用可能なデバイスファミリに割り当てることができます。インポートしたイメージは、いつでも複数のデバイスに割り当てることができます。

インポートしたソフトウェアイメージをデバイスファミリに割り当てするには、次の手順を実行します。

-
- ステップ 1** Cisco DNA Center のホームページで、[Design] > [Image Repository] を選択します。
- ステップ 2** [Imported Images] をクリックします。
- ステップ 3** [Assign] リンクをクリックします。
- ステップ 4** [Assign Device Family] ウィンドウで、このイメージを割り当てるデバイスファミリを選択します。
- ステップ 5** [Assign] をクリックします。

ソフトウェアイメージがデバイスファミリに割り当てられ、そのイメージを使用しているデバイスの数が [Using Image] 列に表示されます。イメージを割り当てたら、そのイメージをゴールデンイメージとしてマークできます。「[ゴールデンソフトウェアイメージの指定](#)」を参照してください。

(注) PnP デバイスでは、デバイスが使用可能になる前に、ソフトウェアイメージをインポートしてデバイスファミリに割り当てることができます。また、イメージをゴールデンイメージとしてマークすることもできます。デバイスがインベントリで使用可能になると、そのデバイスファミリに割り当てられたイメージが、そのデバイスファミリの新しく追加されたデバイスに自動的に割り当てられます。

イメージがインポートされ、Cisco DNA Center に cisco.com ログイン情報が追加されると、Cisco DNA Center はイメージに適用可能なデバイスファミリのリストを提供します。リストから、必要なデバイスファミリを選択できます。

イメージが cisco.com で使用できない場合、またはログイン情報が Cisco DNA Center に追加されていない場合は、そのイメージに適したデバイスファミリを設計する必要があります。

デバイスのソフトウェアイメージをインストールモードでアップロード

[イメージリポジトリ (Image Repository)] ページでは、ソフトウェアイメージがインストールモードの状態として表示されることがあります。デバイスがインストールモードの場合、Cisco DNA Center は、ソフトウェアイメージをデバイスから直接アップロードできません。デバイスがインストールモードのときは、次の手順で示すように、最初に手動でソフトウェアイメージを Cisco DNA Center リポジトリへアップロードしてから、イメージをゴールデンとしてマーキングします。

-
- ステップ 1** Cisco DNA Center のホーム ページで、[設計 (Design)] > [イメージリポジトリ (Image Repository)] を選択します。
 - ステップ 2** [Image Name] 列で、[Install Mode] で実行中のデバイスのソフトウェアイメージを検索します。
 - ステップ 3** [インポート (Import)] をクリックして、インストールモードであるイメージのバイナリソフトウェアイメージファイルをアップロードします。
 - ステップ 4** [ファイルの選択 (Choose File)] をクリックしてローカルに保存されているソフトウェアイメージへ移動するか、または [イメージの URL を入力 (Enter image URL)] でソフトウェアイメージのインポート元となる HTTP または FTP を指定します。
 - ステップ 5** [Import] をクリックします。
ウィンドウにインポートの進行が表示されます。
 - ステップ 6** [タスクの表示 (Show Tasks)] をクリックして、インポートしたソフトウェアイメージが、正常にインポートされ、Cisco DNA Center リポジトリに追加されたことを示す緑色であることを確認します。

ステップ7 [Refresh] をクリックします。

[イメージリポジトリ (Image Repository)] ウィンドウを更新します。Cisco DNA Center にソフトウェアイメージが表示され、[ゴールデンイメージ (Golden Image)] および [デバイスロール (Device Role)] 列がグレー表示ではなくなります。

ゴールデンソフトウェアのイメージについて

Cisco DNA Center では、ソフトウェアイメージと SMU をゴールデンとして指定できます。ゴールデンソフトウェアイメージや SMU は、特定のデバイスタイプのコンプライアンス要件を満たす検証済みのイメージです。ソフトウェアイメージや SMU をゴールデンとして指定すると、反復的な設定変更の必要がなくなることで時間を節約でき、デバイス間の一貫性を確保できます。標準化されたイメージを作成するために、イメージと対応する SMU をゴールデンとして指定できます。特定のデバイスロールのゴールデンイメージを指定することもできます。たとえば、Cisco 4431 統合サービスルータ デバイス ファミリのイメージがある場合、アクセスロールだけを持つ Cisco 4431 デバイスに対するゴールデンイメージを追加で指定できます。

対応するイメージもゴールデンとしてマークされていない限り、SMU をゴールデンとしてマークすることはできません。

ゴールデンソフトウェアイメージの指定

デバイスファミリまたは特定のデバイスロールに対するゴールデンソフトウェアイメージを指定することができます。デバイスロールは、ネットワークにおける役目と配置に従って、デバイスを識別およびグループ分けするために使用されます。

ステップ1 Cisco DNA Center のホーム ページで、[設計 (Design)] > [イメージリポジトリ (Image Repository)] を選択します。

デバイスタイプに従ってソフトウェアイメージが表示されます。

ステップ2 [ファミリ (Family)] 列で、ゴールデンイメージを指定するデバイスファミリを選択します。

ステップ3 [イメージ名 (Image Name)] 列で、ゴールデンイメージとして指定するソフトウェアイメージを選択します。

ステップ4 [デバイスロール (Device Role)] 列で、ゴールデンイメージを指定するデバイスロールを選択します。同じデバイスファミリのデバイスを所有していたとしても、各デバイスロールに異なるゴールデンイメージを指定することができます。物理イメージのデバイスロールのみ選択できます。仮想イメージは選択できないことに注意してください。

ゴールデンイメージとして指定したソフトウェアイメージが Cisco DNA Center リポジトリにアップロードされていない場合は、このプロセスには多少時間がかかります。[イメージリポジトリ (Image Repository)]

ページの **[アクション (Action)]** 列で、ゴミ箱アイコンがグレー表示されている場合、イメージはまだ Cisco DNA Center リポジトリにアップロードされていません。Cisco DNA Center では最初にソフトウェアイメージをリポジトリにアップロードする必要があります。その後、イメージをゴールデンとしてマークすることができます。ソフトウェアイメージが **[アクション (Action)]** 列のアクティブなゴミ箱アイコンで示された Cisco DNA Center リポジトリに既にアップロードされている場合、ゴールデンイメージを特定するプロセスはより速く完了します。

ソフトウェアイメージのプロビジョニング

ソフトウェアイメージをネットワーク内のデバイスにプッシュできます。ソフトウェアイメージをデバイスにプッシュする前に、Cisco DNA Center はデバイス管理ステータスの確認、ディスク容量の確認など、デバイスのアップグレード準備の事前チェックを実行します。事前チェックに失敗した場合は、ソフトウェアイメージの更新を実行できません。デバイスのソフトウェアイメージをアップグレード後、Cisco DNA Center は CPU 使用率、ルートサマリなどを確認し、イメージのアップグレード後にネットワークの状態が変更されていないことを保証します。



(注) 複数のデバイスで事前チェックを実行できます。

Cisco DNA Center は、各デバイスのソフトウェアイメージを、その固有のデバイスタイプに対してゴールデンと指定したイメージと比較します。デバイスのソフトウェアイメージとゴールデンイメージに違いがある場合、Cisco DNA Center はデバイスのソフトウェアイメージを無効とします。これらのデバイスに対するアップグレード準備の事前チェックがトリガーされません。すべての事前チェックをクリアしたら、新しいイメージをデバイスに配信（コピー）し、有効化できます（つまり、新しいイメージを実行中のイメージにできます）。新しいイメージの有効化には、デバイスの再起動が必要です。再起動によって現在のネットワークアクティビティが中断される可能性があるため、後でプロセスをスケジュールできます。

そのデバイスタイプにゴールデンイメージを指定していない場合、そのデバイスのイメージは更新できません。[ゴールデンソフトウェアイメージの指定 \(80 ページ\)](#) を参照してください。

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

ステップ 2 [Focus] ドロップダウンリストから **[Software Images]** を選択します。イメージをアップグレードするデバイスを選択します。

- (注) デバイスの事前チェックに成功したら、OS イメージ列の [Outdated] リンクに緑色のチェックマークが付きます。デバイスのアップグレードを準備するための事前チェックでいずれかに失敗した場合、[Outdated] リンクのマークが赤色に変わり、そのデバイスの OS イメージを更新できなくなります。先に進む前に、[Outdated] リンクをクリックし、エラーを修正します。

デバイスのアップグレードの準備の事前チェック リスト (82 ページ) を参照してください。

ステップ 3 [Actions] ドロップダウンリストから、[Software Images] > [Update Image] を選択し、以下を実行します。

- a) [Distribute] : [Now] をクリックしてすぐに配信を開始するか、[Later] をクリックして特定の時間に配信をスケジュールします。

(注) 選択したデバイスにすでにイメージが配信されている場合、配信プロセスはスキップされ、イメージの有効化のみ可能になります。

- b) [次へ (Next)] をクリックします。

- c) [Activate] : [Now] をクリックしてすぐに有効化を開始するか、[Later] をクリックして特定の時間に有効化をスケジュールします。

(注) とりあえず配信プロセスのみを実行する場合、この手順をスキップすることができます。

- d) (オプション) [Schedule Activation after Distribution is completed] チェックボックスをオンにします。

- e) [確認 (Confirm)] : [確認 (Confirm)] をクリックして、更新を確認します。

更新のステータスは、[OS の更新ステータス (OS Update Status)] 列で確認できます。この列が表示されない場合は、 をクリックして [OS Update Status] を選択します。

ステップ 4 (オプション) イメージのアップグレードの進行状況を表示するには、[アップグレードステータス (Upgrade Status)] をクリックします。

- (注) Cisco DNA Center と別のファブリック デバイス間にエッジルータなどのデバイスがある場合、ソフトウェアイメージが他のデバイスにプロビジョニングされている間に、この間にあるデバイスがリロードすると、ソフトウェア更新プロセスが失敗する可能性があります。

デバイスのアップグレードの準備の事前チェック リスト

事前チェック	説明
ファイル転送のチェック	デバイスが SCP および HTTPS を介して到達可能かどうかチェックします。
NTP クロックのチェック	デバイスの時間と Cisco DNA Center の時間を比較して、Cisco DNA Center 証明書が正常にインストールされていることを確認します。

事前チェック	説明
フラッシュのチェック	更新に十分なディスク容量があるかどうか確認します。十分なディスク容量がない場合、警告またはエラーメッセージが返されます。自動フラッシュクリーンアップでサポートされるデバイスとファイルの削除方法については、 Auto Flash Cleanup を参照してください。
設定レジスタのチェック	設定レジスタの値を確認します。
暗号化 RSA チェック	RSA 証明書がインストールされているかどうかチェックします。
暗号化 TLS のチェック	デバイスが TLS 1.2 をサポートしているかどうかチェックします。
IP ドメイン名のチェック	ドメイン名が設定されているかどうかチェックします。
スタートアップ設定のチェック	このデバイス用のスタートアップ設定があるかどうかを確認します。
NFVIS Flash チェック	NFVIS デバイスでゴールデンイメージをアップグレードする準備ができているかどうかを確認します。
サービス契約のチェック	デバイスに有効なライセンスがあるかどうかを確認します。

Auto Flash Cleanup

デバイスのアップグレード準備の事前チェックの間、フラッシュのチェックにより、新しいイメージをコピーするための十分なスペースがデバイスにあるかどうかを確認されます。スペースが十分でない場合：

- 自動フラッシュクリーンアップをサポートしているデバイスの場合：**フラッシュのチェックが失敗し、警告メッセージが表示されます。このようなデバイスの場合、十分なスペースを作成するために、イメージの配信プロセス中に自動クリーンアッププロセスが試行されます。自動フラッシュクリーンアップの一環として、Cisco DNA Center は未使用の .bin、.pkg、および .conf ファイルを特定し、デバイス上に十分な空き領域が確保されるまでそれらのファイルを繰り返し削除します。イメージの配信はフラッシュクリーンアップ後に試行されます。削除されたファイルは **[システム (System)] > [監査ログ (Audit Logs)]** で確認できます。



(注) 自動フラッシュクリーンアップは、Nexus スイッチとワイヤレスコントローラを除くすべてのデバイスでサポートされています。

- 自動フラッシュクリーンアップをサポートしていないデバイスの場合：**フラッシュのチェックが失敗し、エラーメッセージが表示されます。イメージのアップグレードを開始する前に、デバイスのフラッシュからファイルを削除して、必要なスペースを作成できます。



第 6 章

ネットワーク トポロジを表示

- [トポロジについて \(85 ページ\)](#)
- [エリア、サイト、ビルディング、フロアのトポロジを表示 \(86 ページ\)](#)
- [トポロジマップでデバイスをフィルタリング \(87 ページ\)](#)
- [デバイス情報の表示 \(88 ページ\)](#)
- [リンク情報の表示 \(89 ページ\)](#)
- [トポロジマップにデバイスをピン留めする \(89 ページ\)](#)
- [サイトへのデバイスの割り当て \(90 ページ\)](#)
- [トポロジマップ レイアウトの保存 \(90 ページ\)](#)
- [トポロジマップ レイアウトを開く \(91 ページ\)](#)
- [トポロジのレイアウトをエクスポート \(91 ページ\)](#)

トポロジについて

[Topology] ウィンドウはネットワークのグラフィック ビューを表示します。Cisco DNA Center は、ユーザが設定したディスカバリ設定を使用してネットワーク内のデバイスを検出して、デバイス ロールを割り当てます。検出中に割り当てられた（またはデバイス インベントリ内で変更された）デバイス ロールに基づいて、Cisco DNA Center は詳細なデバイス レベルのデータを使用して物理トポロジマップを作成します。

トポロジマップを使用すると、次のことができます。

- 選択したエリア、サイト、ビルディング、またはフロアのトポロジを表示する。
- 詳細なデバイス情報を表示する。
- 詳細なリンク情報を表示する。
- 特定のレイヤ 2 VLAN に基づいてデバイスをフィルタ処理する。
- レイヤ 3 プロトコル（Intermediate System-to-Intermediate System (IS-IS)、Open Shortest Path First (OSPF)、Enhanced Interior Gateway Routing Protocol (EIGRP)、スタティックルーティング）に基づいてデバイスをフィルタ処理する。
- Virtual Routing and Forwarding (VRF) 機能を使用してデバイスをフィルタ処理する。

- トポロジ マップにデバイスをピン留めする
- トポロジ マップ レイアウトの保存
- トポロジ マップ レイアウトを開く
- トポロジ レイアウト全体のスクリーンショットを PNG 形式でエクスポートする。

エリア、サイト、ビルディング、フロアのトポロジを表示

エリア、サイト、ビルディングまたはフロアのトポロジを表示できます。

始める前に

- インベントリにデバイスがあることを確認します。デバイスがない場合は、ディスカバリ機能を使用して検出します。
- ネットワーク階層を定義し、ビルディングまたはその内部のフロアにデバイスをプロビジョニングしている必要があります。

ステップ 1 Cisco DNA Centerのホームページで、[トポロジ (Topology)]をクリックします。

ステップ 2 [Tree View] メニューで、興味のあるエリア、サイト、ビルディング、またはフロアを選択します。




ステップ 3 トグルボタン  を使用して、地理的マップビューとレイヤ2マップビューを切り替えます。

地理的マップビューにサイトが表示されます。近いサイトがグループ化され、グループ内のサイト数とともに示されます。デバイスの正常性は異なる色で示されます。サイトの上にカーソルを移動すると、デバイスの正常性の詳細が表示されます。

右上隅の [Search] フィールドを使用して、地理的マップビューのビルディング、およびレイヤ2 マップビューのデバイスを検索できます。

(注)

- 右下隅にあるアイコン  をクリックすると凡例が開き、トポロジマップで利用可能なショートカットキーが表示されます。
- [Toggle Annotate] アイコンをクリックして、レイヤ2 マップに注釈を描画します。[export] アイコンをクリックして、トポロジマップを注釈とともにエクスポートできます。

ステップ 4 [Take a Tour] をクリックすると、[Topology] ページで使用できるさまざまなオプションの詳細を確認できます。

トポロジ マップでデバイスをフィルタリング

次のいずれかの属性に基づいてデバイスをフィルタ処理できます。

- VLAN
- Routing
- VRF
- Tagging

始める前に

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

ステップ 1 Cisco DNA Centerのホームページで、[トポロジ (Topology)] をクリックします。

ステップ 2 [Filter] をクリックします。

(注) [Filter] を表示できない場合は、左側のツリービューメニューでサイトをクリックします。

ステップ 3 次のいずれかを実行します。

- [VLAN] ドロップダウンリストから表示する VLAN を選択します。
- [ルーティング (Routing)] ドロップダウンリストから目的のプロトコルを選択します。
- [VRF] ドロップダウンリストから表示する VRF を選択します。
- [View All Tags] をクリックして、表示するタグを選択します。選択したタグに関連付けられているデバイスが強調表示されます。新しいタグを作成するには、次の手順を実行します。

- a) [Create New Tag] をクリックします。
- b) [Tag Name] にタグ名を入力します。
- c) [保存 (Save)] をクリックします。

また、次の手順を実行して、デバイスをタグに関連付けることもできます。

- a) デバイスをクリックします。
 - b) [Tag Device] をクリックします。
 - c) デバイスを関連付けるタグを選択します。
 - d) [Apply] をクリックします。
-

デバイス情報の表示

デバイス名、IP アドレス、およびデバイスのソフトウェア バージョンを表示することができます。



- (注) [トポロジ (Topology)] ウィンドウでアクセス可能なデバイス情報には、[デバイス インベントリ (Device Inventory)] ウィンドウでもアクセス可能です。

始める前に

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

ステップ 1 Cisco DNA Center のホームページで、[トポロジ (Topology)] をクリックします。

ステップ 2 [ツリー ビュー (Tree View)] メニューで、興味のあるエリア、サイト、ビルディング、またはフロアを選択します。

ステップ 3 トポロジ エリアで、興味のあるデバイスまたはデバイス グループにマウス オーバーします。

- (注) デバイス グループには、含まれているデバイスの数と種類がラベル付けされています。スイッチにホストがある場合、青い矢印がスイッチの下に表示されます。青い矢印をクリックすると、ホストが表示されます。

ステップ 4 [Display] をクリックして以下の項目を有効にすると、デバイスの詳細が表示されます。項目の横にある ⓘ アイコンにカーソルを合わせると、詳細情報を確認できます。

- [Device Health] : デバイスの正常性が表示されます。
- [Link Health] : デバイス間のリンクの正常性が表示されます。
- [License status] : デバイスのライセンスステータスが表示されます。デバイスのライセンスが期限切れに近づくと、強調表示され、デバイスの横に警告アイコンが表示されます。強調表示されたデバイスをクリックすると、そのライセンスの詳細が表示されます。
- [Device IP] : デバイスラベルの下にデバイスの IP アドレスが表示されます。
- [Device Suffixes] : デバイスのフルネームが、サフィックスと一緒に表示されます。

リンク情報の表示

トポロジマップ内のリンクに関する情報を表示できます。単純なリンクの場合は、1つのリンクの情報が表示されます。集約されたリンクの場合は、基本となるすべてのリンクのリストが表示されます。情報には、インターフェイス名、その速度、およびその IP アドレスが含まれます。

始める前に

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

ステップ 1 Cisco DNA Centerのホームページで、[トポロジ (Topology)] をクリックします。

ステップ 2 [ツリー ビュー (Tree View)] メニューで、興味のあるエリア、サイト、ビルディング、またはフロアを選択します。

ステップ 3 興味のあるリンクにカーソルを合わせます。

ステップ 4 [Display] をクリックして、[Link Health] を有効にします。

ダウンリンクは赤色で表示されます。リンクを削除する場合は、削除するリンクを選択して [Delete] をクリックします。次の手順を実行して、リンクをアップさせることができます。

- a) デバイスにログインします。
- b) インターフェイスをイネーブルにします。
- c) [Inventory] ページでデバイスを再同期します。

トポロジマップにデバイスをピン留めする

デバイスをグループ化または集約して、マップ上に表示するスペースを削減できます。ただし、グループからデバイスを区別する必要がある場合があります。これは、デバイスをマップにピン留めすることで可能になります。

始める前に

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

ステップ 1 Cisco DNA Centerのホームページで、[トポロジ (Topology)] をクリックします。

ステップ 2 次のいずれかを実行します。

- デバイスをピン留めするには、デバイス グループをクリックして、デバイス名の左にあるピンのアイコンをクリックします。

- すべてのデバイスをピン留めするには、デバイスグループをクリックして、ダイアログボックスで、[すべてピン留め (Pin All)] をクリックします。

(注) グループをダブルクリックすると、グループ内のデバイスのピン留めが解除されます。

サイトへのデバイスの割り当て

デバイスは、トポロジマップを使用して、特定のサイトに割り当てることができます。

始める前に

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

ステップ 1 Cisco DNA Centerのホームページで、[トポロジ (Topology)] をクリックします。

ステップ 2 左側のペインの[未割り当てのデバイス (Unassigned Devices)] をクリックします。未割り当てのデバイスはすべて、トポロジ領域に表示されます。

ステップ 3 サイトの割り当て先となるデバイスをクリックします。デバイスの詳細がポップアップに表示されます。[デバイスの割り当て先: (Assign devices to:)] セクションで、[場所の選択 (choose the location)] ドロップダウンリストをクリックして場所を選択します。

ステップ 4 (オプション) サイトを選択したデバイスにのみ割り当てを行い、接続済みの (ダウンストリーム) デバイスには割り当てない場合、[自動割り当て要求元不明のダウンストリームデバイス (Auto-assign unclaimed downstream devices)] チェック ボックスのチェックを外します。

ステップ 5 [Assign] をクリックします。

トポロジマップ レイアウトの保存

Cisco DNA Center には Cisco 推奨のトポロジレイアウトがあり、トポロジツールを開いたときにこれがデフォルトで表示されます。複数のレイアウトをカスタマイズし、後で確認するために保存できます。またレイアウトの1つを、トポロジマップを開いたときに表示されるデフォルトとして設定することもできます。

始める前に

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

ステップ 1 Cisco DNA Centerのホームページで、[トポロジ (Topology)] をクリックします。

ステップ2 [Custom View] をクリックします。

ステップ3 [表示タイトルの入力 (Enter View Title)] フィールドに、カスタマイズしたマップの名前を入力します。

ステップ4 [保存 (Save)] をクリックします。

ステップ5 (任意) カスタマイズしたマップをデフォルトとして設定するには、[デフォルトにする (MakeDefault)] をクリックします。

トポロジ マップ レイアウトを開く

以前に保存したトポロジ マップを開くことができます。

始める前に

トポロジ マップ レイアウトが保存済みである必要があります。

ステップ1 Cisco DNA Centerのホームページで、[トポロジ (Topology)] をクリックします。

ステップ2 [Custom View] をクリックします。

ステップ3 表示するマップの名前をクリックします。

トポロジのレイアウトをエクスポート

完全なトポロジレイアウトのスナップショットをエクスポートできます。スナップショットは、SVG、PDF、PNG ファイルとしてローカルマシンにダウンロードされます。

始める前に

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

ステップ1 Cisco DNA Centerのホームページで、[トポロジ (Topology)] をクリックします。

ステップ2  (このアイコンは [トポロジのエクスポート (Export Topology)]) をクリックします。

ステップ3 ファイル形式を選択し、[エクスポート (Export)] をクリックします。



第 7 章

ネットワーク階層と設定を設計

- [新しいネットワーク インフラストラクチャの設計 \(94 ページ\)](#)
- [About Network Hierarchy \(94 ページ\)](#)
- [フロア マップのモニタリング \(102 ページ\)](#)
- [フロア要素とオーバーレイの編集 \(103 ページ\)](#)
- [フロア ビュー オプション \(114 ページ\)](#)
- [データのフィルタリング \(117 ページ\)](#)
- [ゼロデイ Ekahau 計画ワークフロー \(118 ページ\)](#)
- [インタラクティブフロアプランニングについて \(120 ページ\)](#)
- [グローバルワイヤレス設定の構成 \(122 ページ\)](#)
- [ネットワークプロファイルの作成 \(140 ページ\)](#)
- [グローバルネットワーク設定について \(146 ページ\)](#)
- [デバイス クレデンシアルについて \(147 ページ\)](#)
- [グローバルデバイス クレデンシアルについて \(149 ページ\)](#)
- [グローバルデバイスのログイン情報の編集に関する注意事項 \(155 ページ\)](#)
- [グローバルデバイス クレデンシアルの編集 \(156 ページ\)](#)
- [デバイス クレデンシアルのサイトへの関連付け \(157 ページ\)](#)
- [IP アドレス プールを設定する \(158 ページ\)](#)
- [IP アドレスマネージャから IP アドレスプールをインポートする \(158 ページ\)](#)
- [CSV ファイルから IP アドレスプールをインポートする \(159 ページ\)](#)
- [IP プールの予約 \(159 ページ\)](#)
- [IP プールの編集 \(160 ページ\)](#)
- [IP プールの複製 \(161 ページ\)](#)
- [IP プールのリリース \(161 ページ\)](#)
- [サービス プロバイダー プロファイルの設定 \(161 ページ\)](#)
- [グローバルネットワーク サーバの設定 \(162 ページ\)](#)
- [Cisco ISE またはその他の AAA サーバの追加 \(163 ページ\)](#)

新しいネットワーク インフラストラクチャの設計

[設計 (Design)] 領域では、ネットワーク全体のデバイスに適用可能な物理トポロジ、ネットワーク設定、デバイスのタイプやプロファイルなど、ネットワークの構造とフレームワークを作成します。既存のインフラストラクチャがない場合は、設計ワークフローを使用します。既存のインフラストラクチャがある場合は、**ディスカバリ機能**を使用します。詳細については、「[ディスカバリについて \(13 ページ\)](#)」を参照してください。

これらのタスクは、[設計 (Design)] 領域で実行します。

-
- ステップ 1** ネットワーク階層を作成します。詳細については、[ネットワーク階層のサイトの作成 \(95 ページ\)](#) を参照してください。
- ステップ 2** グローバル ネットワーク設定を定義します。詳細については、[グローバル ネットワーク設定について \(146 ページ\)](#) を参照してください。
- ステップ 3** ネットワーク プロファイルを定義します。
-

About Network Hierarchy

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

ネットワーク階層は、次の事前設定された階層をもちます。

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

実行できるタスクのリストを以下に示します。

- 新しいネットワーク階層を作成する。詳細については、「[ネットワーク階層のサイトの作成 \(95 ページ\)](#)」を参照してください。

- Cisco Prime Infrastructure から既存のネットワーク階層をアップロードする。詳細については、「[既存のサイト階層をアップロード \(97 ページ\)](#)」を参照してください。

マップ内で使用するイメージファイルに関するガイドライン


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

ネットワーク階層のサイトの作成

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

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

世界のマップが表示されます。

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

ステップ 3 既存の階層をアップロードすることもできます。詳細については、[既存のサイト階層をアップロード \(97 ページ\)](#) を参照してください。

ステップ 4 サイトの名前を入力し、親ノードを選択します。デフォルトでは、**[グローバル (Global)]** が親ノードです。

ステップ 5 **[Add]** をクリックします。

左側のメニューの親ノードの下にサイトが作成されます。

Cisco Prime Infrastructure からサイト階層をエクスポートして Cisco DNA Center にインポートする

ネットワーク階層はネットワークの地理的な場所を表します。サイト ID とビルディング ID を作成すると、後で、設計の設定や構成を適用する場所を簡単に特定できます。Cisco Prime Infrastructure に既存のネットワーク階層がある場合は、Cisco DNA Center にインポートして、新しいネットワーク階層の作成に費やす時間と労力を節減できます。

これは、ロケーショングループまたはサイト情報を含む CSV ファイルと、ネットワーク階層内のさまざまなフロアマップを含むマップアーカイブファイルとして、Cisco Prime Infrastructure から 2 つのファイルをエクスポートするために必要な単純なプロセスです。

この手順では、Cisco Prime Infrastructure から Cisco DNA Center に既存のサイト階層をエクスポートする方法について説明します。Cisco Prime Infrastructure リリース 3.2 以降のバージョンからサイト階層をエクスポートできます。

始める前に

- シスコ ワイヤレス コントローラとアクセスポイントを検出し、Cisco DNA Center の [Inventory] ページに一覧表示します。
- フロアマップ上に AP を追加して配置します。
- Cisco Prime Infrastructure にあるサイトを Cisco DNA Center で手動作成した場合は、Cisco DNA Center にインポートする前にそれらのサイトを手動で削除する必要があります。

ステップ 1 最初のステップとして、Cisco Prime Infrastructure からワークステーションに CSV ファイルとしてロケーショングループをエクスポートする必要があります。

ステップ 2 ロケーショングループをエクスポートするには、Cisco Prime Infrastructure で、[Inventory] > [Group Management] > [Network Device Groups] を選択します。

ステップ 3 [Device Groups] ウィンドウで、[Export Groups] をクリックします。

ステップ 4 [Export Groups] ダイアログボックスで、[APIC-EM] オプションボタンをクリックして CSV ファイルをダウンロードし、[OK] をクリックします。

CSV ファイルがワークステーションにダウンロードされるまで待ちます。CSV ファイルには、さまざまなサイト、ビルディング、およびフロアの地理的場所と、ネットワーク内の階層に関する情報が含まれています。

ステップ 5 次に、Cisco Prime Infrastructure からマップをエクスポートします。これにより、Cisco Prime Infrastructure の各フロアに適用されている RF 減衰モデルなどのフロア寸法やキャリブレーション情報などのマップ情報がダウンロードされます。

ステップ 6 マップをエクスポートするには、[Maps] > [Wireless Maps] > [Site Maps (New)] を選択します。

ステップ 7 [エクスポート (Export)] ドロップダウンリストから [マップアーカイブ (Map Archive)] を選択します。

[Export Map Archive] ウィンドウが表示され、デフォルトで [Select Sites] ウィンドウが表示されます。

- ステップ 8** 特定のサイト、キャンパス、ビルディング、またはフロアのチェックボックスをオンにするか、[Select All] チェックボックスをオンにしてすべてのマップをエクスポートします。
- ステップ 9** [Map Information] と [Calibration Information] が選択されているか確認します。必ず 1 つのオプションを選択する必要があります。選択されていない場合は、[Map Information] および [Calibration Information] に対して [On] ボタンをクリックします。
- ステップ 10** [Map Information] を選択すると、長さ、幅、高さなどのフロアの寸法がエクスポートされます。また、フロアマップ上に配置された AP に関する詳細、および Cisco Prime Infrastructure 内のフロアマップ上にオーバーレイされた障害物とエリアもエクスポートされます。
- ステップ 11** [Calibration Information] を選択すると、Cisco Prime Infrastructure の各フロアに適用されている無線周波数減衰モデルがエクスポートされます。既存のキャリブレーションデータを Cisco Prime Infrastructure からエクスポートすることをお勧めします。それ以外の場合は、Cisco DNA Center でキャリブレーションの詳細を手動で入力する必要があります。
- ステップ 12** [Generate Map Archive] をクリックして、マップアーカイブを生成します。
ネットワーク階層内のさまざまなフロアマップを含む tar ファイルが作成され、お使いのワークステーションに保存されます。
- ステップ 13** サイト階層を Cisco DNA Center にインポートするには、Cisco DNA Center のホームページで、[Design] > [Network Hierarchy] の順に選択し、[Import] > [Import Sites] をクリックします。
- ステップ 14** [Import Sites] ウィンドウで、Prime Infrastructure のロケーショングループの CSV ファイルをドラッグアンドドロップするか、[Select a file from your computer] をクリックしてファイルがある場所へ移動し、[Import] をクリックして、Prime Infrastructure のロケーショングループの CSV ファイルをインポートします。
- ステップ 15** 次に、フロアマップと関連するマップ情報を含むマップアーカイブファイルをインポートします。
- ステップ 16** マップアーカイブファイルをインポートするには、[Design] > [Network Hierarchy] の順に選択し、[Import] > [Import Maps] をクリックします。
- ステップ 17** [Import Maps Archive] ウィンドウで、マップアーカイブファイルをドラッグアンドドロップするか、お使いのワークステーションからファイルを選択します。
- ステップ 18** [保存 (Save)] をクリックします。

既存のサイト階層をアップロード

既存のネットワーク階層を含んでいる CSV ファイルまたはマップアーカイブ ファイルをアップロードすることができます。たとえば、Cisco Prime Infrastructure からエクスポートしたロケーション情報を含む CSV ファイルをアップロードできます。詳細については、Prime Infrastructure からマップをエクスポートする方法に関する [マップアーカイブのエクスポート \(98 ページ\)](#) を参照してください。



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

-
- ステップ 1** Cisco DNA Center のホームページから、**[設計 (Design)]** > **[ネットワーク階層 (Network Hierarchy)]** をクリックし、**[インポート (Import)]** > **[サイトのインポート (Import Site)]** を選択します。
- ステップ 2** CSV ファイルをドラッグしてドロップするか、または、CSV ファイルがある場所に移動し、**[インポート (Import)]** をクリックして、Cisco Prime Infrastructure グループ CSV ファイルをインポートします。
- 既存の CSV ファイルがない場合は、**[テンプレートをダウンロード (Download Template)]** をクリックして、編集可能な CSV ファイルをダウンロードして、その後、アップロードすることができます。
- ステップ 3** Cisco Prime Infrastructure マップ tar.gz アーカイブファイルをインポートするには、**[インポート (Import)]** > **[マップのインポート (Map Import)]** をクリックします。
- ステップ 4** **[サイト階層アーカイブのインポート (Import Site Hierarchy Archive)]** ダイアログボックスのボックスエリアにマップアーカイブファイルをドラッグしてドロップするか、または、**[クリックして選択 (click to select)]** リンクをクリックして、アーカイブファイルを参照します。
- ステップ 5** **[Save (保存)]** を選択してファイルをアップロードします。
- [インポートプレビュー (Import Preview)]** ウィンドウが表示され、インポートされたファイルが示されます。
-

マップアーカイブのエクスポート

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

- ステップ 1** Cisco Prime Infrastructure のユーザーインターフェイスから、**[マップ (Map)]** > **[ワイヤレスマップ (Wireless Maps)]** > **[サイトマップ (新規) (Site Maps (New))]** を選択します。
- ステップ 2** **[エクスポート (Export)]** ドロップダウンリストから **[マップアーカイブ (Map Archive)]** を選択します。
- ステップ 3** **[サイトの選択 (Select Sites)]** ウィンドウで、次のように設定します。マップアーカイブに含めるマップ情報またはキャリブレーション情報を選択できます。
- **マップ情報 (Map Information)** : アーカイブにマップ情報を含めるには、**オン**または**オフ** ボタンをクリックします。
 - **キャリブレーション情報 (Calibration Information)** : キャリブレーション情報をエクスポートするには、**オン**または**オフ** ボタンをクリックします。**[選択したマップのキャリブレーション情報 (Calibration Information for selected maps)]** オプションボタンか、または**[すべてのキャリブレーション情報 (All Calibration Information)]** オプションボタンをクリックします。**[選択したマップのキャリブレーション情報 (Calibration Information for selected maps)]** を選択すると、選択したサイトマップのキャリブレーション情報がエクスポートされます。**[すべてのキャリブレーション情報 (All Calibration Information)]** を選択すると、選択したマップとともに、システムで使用可能なその他のキャリブレーション情報もエクスポートされます。
 - 左側のペインの**[サイト (Sites)]** で、エクスポートするサイト、キャンパス、ビルディングフロア、または屋外領域の1つ以上のチェックボックスをオンにします。すべてのマップをエクスポートするには、**[すべて選択 (Select All)]** チェックボックスをオンにします。

ステップ4 [マップアーカイブを生成 (Generate Map Archive)] をクリックします。「データをエクスポートしています (Exporting data is in progress) というメッセージが表示されます。
tar ファイルが作成され、ローカルマシンに保存されます。

ステップ5 [Done] をクリックします。

Search the Network Hierarchy


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

ツリー階層を検索するには、左ペインの **[階層の検索 (Find Hierarchy)]** で、検索するサイト、ビルディング、フロア名の名称の一部または正式名称をのどちらかを入力します。ツリー階層は、検索フィールドに入力したテキストに基づきフィルタリングされます。

サイトの編集

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

ステップ2 左側のツリーペインで、編集するサイトに移動します。


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

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

サイトの削除

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

ステップ2 左側のペインで、削除するサイトに移動します。



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

ステップ4 削除を確認します。


ビルディングの追加

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


世界のマップが表示されます。

- ステップ 2** [ネットワーク階層 (Network Hierarchy)] ウィンドウで、[+サイトの追加 (Add Site)] をクリックするか、または左側のツリー ペインの親サイトの隣にある歯車アイコン  をクリックして、[ビルディングの追加 (Add Building)] を選択します。
- ステップ 3** 既存の階層をアップロードすることもできます。 [既存のサイト階層をアップロード \(97 ページ\)](#) を参照してください。
- ステップ 4** ビルディングの名前を入力します。
- ステップ 5** [アドレス (Address)] テキストフィールドに、アドレスを入力します。インターネットに接続している場合、アドレスを入力すると同時に、設計アプリケーションが、入力されたアドレスを既知のアドレスを絞り込みます。適切なアドレスがウィンドウに表示されたことを確認したら、それを選択します。既知の所在地を選択すると、[経度 (Longitude)] および [緯度 (Latitude)] の座標フィールドが自動的に設定されます。
- ステップ 6** [Add] をクリックします。
- 左側のメニューの親サイトの下に、作成したビルディングが追加されます。
- ステップ 7** 別のエリアまたはビルディングを追加するには、階層フレームで、既存のエリアまたは親ノードにしたいビルディングの隣にある歯車アイコン  をクリックします。

ビルディングの編集

- ステップ 1** [設計 (Design)] > [ネットワーク階層 (Network Hierarchy)] を選択します。
- ステップ 2** 左側のツリー ペインで、編集するビルディングに移動します。
- ステップ 3** ビルディングの横にある歯車アイコン  をクリックし、[ビルディングの編集 (Edit Building)] を選択します。
- ステップ 4** [ビルディングの編集 (Edit Building)] ウィンドウで必要な変更を加え、[更新 (Update)] をクリックします。

ビルディングの削除

- ステップ 1** Cisco DNA Center のホームページで、[Design] > [Network Hierarchy] の順に選択します。
- ステップ 2** 左側のペインで、削除するビルディングに移動します。
- ステップ 3** ビルディングの隣にある歯車アイコン  をクリックし、[ビルディングの削除 (Delete Building)] を選択します。
- ステップ 4** 削除を確認します。
- (注) ビルディングを削除すると、そのテナントマップもすべて削除されます。AP は、削除されたマップから未割り当ての状態に移動します。

ビルディングへのフロアの追加

ビルディングを追加したら、フロアを作成し、フロア マップをアップロードします。


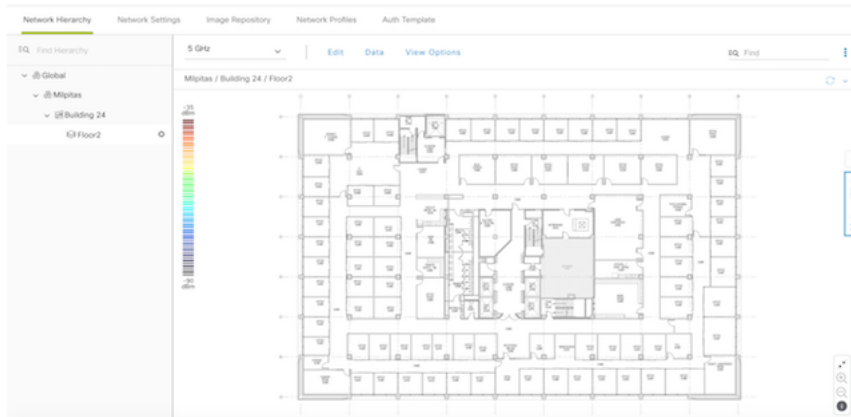
-
- ステップ 1** Cisco DNA Center のホームページで、[Design] > [Network Hierarchy] を選択します。
- ステップ 2** [グローバル (Global)] サイトと以前に作成した領域を展開し、以前に作成したすべてのビルディングを確認します。
- ステップ 3** フロアを追加するビルディングの横にある歯車アイコン  をクリックし、次に [フロアを追加 (AddFloor)] をクリックします。
- ステップ 4** フロアの名前を入力します。フロア名には21文字の制限があります。フロア名は文字またはハイフン (-) で始める必要があり、最初の文字に続く文字列は、次の1つ以上を含めることができます。
- 大文字または小文字、またはその両方
 - 数字
 - アンダースコア (_)
 - ハイフン (-)
 - ピリオド(.)
 - スペース ()
- ステップ 5** [タイプ (RFモデル) (Type (RF Model))] ドロップダウン リストから無線周波数 (RF) モデルを選択して、フロアのタイプを定義します ([屋内天井高 (Indoor High Ceiling)], [屋外オープンスペース (Outdoor Open Space)], [乾式壁オフィスのみ (Drywall Office Only)], および [キューブと壁で囲まれたオフィス (Cubes And Walled Offices)])。これにより、フロアがオープンスペースであるか、乾式壁のオフィスであるかなどを定義します。選択した RF モデルに基づいて、ワイヤレス信号強度、ヒートマップの分布が計算されます。
- ステップ 6** フロア プランをマップにドラッグしたり、ファイルをアップロードしたりできます。Cisco DNA Center は、.jpg、.gif、.png、.dxf、および .dwg の各ファイルタイプをサポートしています。
- マップをインポートした後は、必ず [オーバーレイの可視性 (Overlay Visibility)] を [ON] にしてください ([フロア (Floor)] > [表示オプション (View Option)] > [オーバーレイ (Overlays)])。デフォルトでは、マップをインポートした後にオーバーレイは表示されません。

図 3: フロアプランの例



ステップ7 [追加 (Add)] をクリックします。

フロアの編集

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


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




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

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

フロアマップのモニタリング

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

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

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

フロア要素とオーバーレイの編集

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

- 次のフロア要素を追加、配置、および削除します。
 - アクセス ポイント
 - センサー
- 次のオーバーレイ オブジェクトを追加、編集、および削除します。
 - カバレッジ エリア
 - 障害物
 - ロケーション リージョン
 - レール
 - マーカー

アクセス ポイントの配置に関するガイドライン

フロア マップに AP を配置する際は、次の注意事項を考慮してください。

- 部屋や建物の屋外の近くにデバイスが置かれるように、カバレッジ領域の境界に沿ってアクセス ポイントを設置します。このようなカバレッジ領域の中心に設置されたアクセス ポイントからは、場合によっては他の全 AP から等距離に見えてしまうデバイスに関して有益なデータが得られます。
- AP 全体の密度を高め、AP をカバレッジ エリアの周辺部に近づけることにより、位置精度を向上させることができます。

- 細長いカバレッジ領域では、直線的に AP を配置しないようにします。各 AP でデバイスロケーションのスナップショットが他と異なるように、それらを交互にずらします。
- 設計では高帯域幅アプリケーションにも十分に対応できる AP 密度が提供されますが、位置に関しては、単一デバイスの各 AP ビューが似ているという弱点があります。そのことが位置の判別を困難にしています。AP をカバレッジ領域の周辺に移動して、それらを交互にずらします。それぞれにおいてデバイスの見え方が明確に異なる可能性が高くなり、結果としてより位置精度が高まります。

AP の追加、配置、および削除

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

インベントリにシスコの AP があることを確認してください。デバイスがない場合は、ディスカバリ機能を使用して AP を検出します。[ディスカバリについて \(13 ページ\)](#) を参照してください。

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

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

-
- ステップ 1** Cisco DNA Center のホームページで、**[Design] > [Network Hierarchy]** の順に選択します。
- ステップ 2** 左ペインで、フロアを選択します。
- ステップ 3** 中央のペインのフロアプランの上にある **[編集 (Edit)]** をクリックします。
- ステップ 4** **[アクセスポイント (Access Points)]** の横にある **[フロア要素 (Floor Elements)]** パネルで、**[追加 (Add)]** をクリックします。
- フロアに割り当てられていないアクセスポイントが一覧に表示されます。
- ステップ 5** **[AP の追加 (Add Aps)]** ウィンドウで、アクセスポイントのチェックボックスをオンにして AP を一括で選択し、**[選択項目の追加 (Add Selected)]** をクリックします。または、アクセスポイントに隣接する **[追加 (Add)]** をクリックします。

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

ステップ6 フロア領域に AP を割り当てたら、[APの追加 (Add APs)] ウィンドウを閉じます。

ステップ7 新しく追加した AP はフロア マップの右上隅に表示されます。

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

- AP を配置するには、AP をクリックして、フロア マップ上の適切な場所にドラッグアンドドロップします。または、[選択したAPの詳細 (Selected AP Details)] ウィンドウで x 座標と y 座標および AP の高さを更新することもできます。マップ上のアクセスポイントをドラッグすると、その水平 (x) と垂直 (y) の位置が、テキストフィールドに表示されます。選択すると、右ペインにアクセスポイントの詳細が表示されます。[選択したAPの詳細 (Selected AP Details)] ウィンドウには、次の情報が表示されます。
 - [3点による位置決め (Position by 3 points)] : フロア マップに 3 つの点を記入し、その点を使用して AP の位置決めができます。手順は次のとおりです。
 1. [3ポイントによる位置付け (Position by 3 points)] をクリックします。
 2. ポイントを定義するには、フロア マップの任意の場所をクリックして最初のポイントの描画を開始します。ポイントの描画を終了するには、再度をクリックします。最初の点までの距離を設定するためにダイアログボックスが表示されます。距離をメートル単位で入力し、[距離の設定 (Set Distance)] をクリックします。
 3. 2 番目と 3 番目の点を同様の方法で定義し、[保存 (Save)] をクリックします。
 - [2つの壁による位置決め (Position by 2 Walls)] : フロア マップに 2 つの壁を定義し、定義した壁の間に AP の位置決めができます。これによって、2 つの壁の間の AP の位置を把握できるようになります。これは、壁の間の AP の位置を把握するのに役立ちます。
 1. [2つの壁による位置付け (Position by 2 Walls)] をクリックします。
 2. 最初の壁を定義するには、フロア マップの任意の場所をクリックして線の描画を開始します。線の描画を終了するには、再度をクリックします。最初の壁までの距離を設定するためにダイアログボックスが表示されます。距離をメートル単位で入力し、[距離の設定 (Set Distance)] をクリックします。
 3. 2 番目の壁を同様の方法で定義し、[保存 (Save)] をクリックします。

AP が、壁の間の定義された距離に従って自動的に配置されます。
 - [AP名 (AP Name)] : AP 名を表示します。
 - [APモデル (AP Model)] : 選択したアクセスポイントの AP モデルを示します。
 - [MACアドレス (MAC Address)] : MAC アドレスが表示されます。
 - [X] : マップの水平の距離をフィートで入力します。
 - [Y] : マップの垂直の距離をフィートで入力します。
 - [AP高さ (AP Height)] : アクセスポイントの高さを入力します。

- [プロトコル (Protocol)] : このアクセス ポイントのプロトコル : [802.11a/n/ac]、[802.11b/g/n] (ハイパー ロケーション AP の場合)、または [802.11a/b/g/n]。
- [アンテナ (Antenna)] : このアクセス ポイントのアンテナ タイプ。
(注) 外部の AP の場合は、アンテナを選択する必要があります。選択しなければ、AP はマップに存在しません。
- [アンテナ画像 (Antenna Image)] : AP イメージが表示されます。
- [アンテナの方向 (Antenna Orientation)] : [方位角 (Azimuth)] と [仰角 (Elevation)] の方向を度数で入力します。
- [方位角 (Azimuth)] : 全方向アンテナのパターンでは方位角が存在しなくなるため、このオプションは表示されません。

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

ヒート マップは、AP の新しい位置に基づいて生成されます。

Cisco Connected Mobile Experiences (CMX) が Cisco DNA Center と同期されている場合は、ヒートマップ上のクライアントの場所を表示できます。[Cisco CMX 設定の作成 \(138 ページ\)](#) を参照してください。

ステップ 10 [アクセス ポイント (Access Points)] の横にある [フロア要素 (Floor Elements)] パネルで、[削除 (Delete)] をクリックします。

[AP の削除 (Delete APs)] ウィンドウには、割り当てられて、配置されたアクセス ポイントすべてを一覧表示します。

ステップ 11 削除するアクセス ポイントの横にあるチェック ボックスをオンにし、[選択済みの削除 (Delete Selected)] をクリックします。

- すべてのアクセス ポイントを削除するには、[すべて選択 (Select All)] をクリックし、[選択済みの削除 (Delete Selected)] をクリックします。
- フロアからアクセス ポイントを削除するには、[削除 (Delete)] アイコンをクリックします。
- **クイック フィルタ**を使用して、AP 名、MAC アドレス、モデル、またはコントローラにより検索します。検索では大文字と小文字は区別されません。検索結果が表に表示されます。[削除 (Delete)] アイコンをクリックしてフロア領域から AP を削除します。

AP のクイック ビュー

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

- [情報 (Info)] をクリックすると、次の AP の詳細が表示されます。
 - [Associated] : AP が関連付けられているかどうかを示します。
 - [Name] : AP 名。

- [MAC Address] : AP の MAC アドレス。
 - [Model] : AP モデル番号。
 - [Admin/Mode] : AP モードの管理ステータス。
 - [Type] : 無線タイプ。
 - [OP/Admin] : 動作ステータスおよび AP モード。
 - [Channel] : AP のチャンネル番号。
 - [Antenna] : アンテナ名。
 - [Azimuth] : アンテナの方向。
- [Rxネイバー (Rx Neighbors)] ラジオ ボタンをオンにすると、マップ上に選択した AP に隣接する Rx ネイバーが接続回線とともに表示されます。また、フロア マップには AP が関連付けられているかどうか AP 名とともに表示されます。
- [Device 360] をクリックすると、特定のネットワーク要素 (ルータ、スイッチ、AP、またはシスコワイヤレスコントローラ) の 360 度ビューが表示されます。 [Cisco DNA Assurance ユーザガイド](#) の「*Monitor and Troubleshoot the Health of a Device*」トピックを参照してください。



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

センサーの追加、配置、および削除



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

センサーデバイスは AP 1800S センサー専用です。AP 1800S センサーは、PnP を使用してブートストラップされます。アシュアランスサーバに到達可能かどうかの詳細情報を取得してからアシュアランスサーバと直接通信します。

- ステップ 1 Cisco DNA Center のホームページから、**[Design] > [Network Hierarchy]** を選択します。
- ステップ 2 左ペインで、フロアを選択します。
- ステップ 3 フロアプランの上にある **[編集 (Edit)]** をクリックします。

- ステップ 4** [センサー (Sensors)] の横にある [フロア要素 (Floor Elements)] パネルで、[追加 (Add)] をクリックします。
- ステップ 5** [Add Sensors] ウィンドウで、追加するセンサーのチェックボックスをオンにするか、またはセンサー行の横にある [Add] をクリックしてセンサーを追加します。
- (注) 検索オプションを使用して、特定のセンサーを検索できます。[Filter] フィールドを使用し、センサーの名前、MACアドレス、モデルのいずれかで検索します。検索では大文字と小文字は区別されません。検索結果がテーブルに表示されます。[追加 (Add)] をクリックして、フロア領域に 1 つ以上のセンサーを追加します。
- ステップ 6** フロア マップへセンサーを割り当てたら、[センサーの追加 (Add Sensors)] ウィンドウを閉じます。新しく追加したセンサーはフロア マップの右上隅に表示されます。
- ステップ 7** センサーを正しく設定するには、[センサー (Sensors)] の横にある [フロア要素 (Floor Elements)] ペインで、[位置 (Position)] をクリックして、マップに正しくセットします。
- ステップ 8** センサーの設定と調整が完了したら、[保存 (Save)] をクリックします。
- ステップ 9** センサーを削除するには、[センサー (Sensors)] の横にある [フロア要素 (Floor Elements)] ペインで、[削除 (Delete)] をクリックします。
[Delete Sensors] ウィンドウには、割り当てられて設定されたすべてのセンサーが一覧表示されます。
- ステップ 10** 削除するセンサーのチェックボックスをオンにし、[Delete Selected] をクリックします。
- すべてのセンサーを削除するには、[すべて選択 (Select All)] をクリックし、[選択済みの削除 (Delete Selected)] をクリックします。
 - フロアからセンサーを削除するには、そのセンサーの横にある [削除 (Delete)] アイコンをクリックします。
 - [Quick Filter] を使用して、名前、MAC アドレス、モデルのいずれかで検索します。検索では大文字と小文字は区別されません。検索結果がテーブルに表示されます。[削除 (Delete)] アイコンをクリックして、フロア領域から 1 つ以上のセンサーを削除します。

カバレッジエリアの追加

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

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

- ステップ 1** Cisco DNA Center のホームページで、[Design] > [Network Hierarchy] の順に選択します。
- ステップ 2** 左ペインで、フロアを選択します。
- ステップ 3** 中央のペインのフロア プランの上にある [編集 (Edit)] をクリックします。

- ステップ 4** [オーバーレイ (Overlays)]パネルで、[カバレッジエリア (Coverage Areas)]の横にある[追加 (Add)]をクリックします。
[カバレッジの作成 (Coverage creation)]ダイアログボックスが表示されます。
- ステップ 5** カバレッジ領域を描画するには、[タイプ (Type)]ドロップダウンリストから、[カバレッジエリア (Coverage Area)]を選択します。
1. 定義するエリアの名前を入力し、[カバレッジを追加 (Add Coverage)]をクリックします。カバレッジエリアは、頂点が3つ以上の多角形でなければなりません。
 2. 輪郭を描く領域に描画ツールを移動します。
 3. このツールをクリックして、描線を開始および停止します。
 4. エリアの輪郭を描いてからダブルクリックすると、そのエリアが強調表示されます。
(注) マップ上で輪郭を描いた領域を強調表示するには、閉じたオブジェクトである必要があります。
- ステップ 6** 多角形領域を描画するには、[タイプ (Type)]ドロップダウンリストから、[周辺 (Perimeter)]を選択します。
1. 定義する領域の名前を入力し、[Ok] をクリックします。
 2. 輪郭を描く領域に描画ツールを移動します。
 - このツールをクリックして、描線を開始および停止します。
 - エリアの輪郭を描いてからダブルクリックすると、そのエリアがページ上で強調表示されます。
- ステップ 7** カバレッジ領域を編集するには、[オーバーレイ (Overlays)]パネルで、[カバレッジエリア (Coverage Areas)]の横にある[編集 (Edit)]をクリックします。
使用可能なカバレッジ領域がマップ上で強調表示されます。
- ステップ 8** 変更を加え、変更後に[保存 (Save)]をクリックします。
- ステップ 9** カバレッジ領域を削除するには、[オーバーレイ (Overlays)]パネルで、[カバレッジエリア (Coverage Areas)]の横にある[削除 (Delete)]をクリックします。
使用可能なカバレッジ領域がマップ上で強調表示されます。
- ステップ 10** カバレッジエリアにマウスカーソルを合わせ、クリックして削除します。
- ステップ 11** 削除後に[保存 (Save)]をクリックします。

障害物の作成

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

-
- ステップ 1** Cisco DNA Center のホームページで、**[Design] > [Network Hierarchy]** の順に選択します。
- ステップ 2** 左ペインで、フロアを選択します。
- ステップ 3** 中央のペインのフロアプランの上にある **[編集 (Edit)]** をクリックします。
- ステップ 4** **[障害 (Obstacles)]** の横にある **[オーバーレイ (Overlays)]** パネルで、**[追加 (Add)]** をクリックします。
- ステップ 5** **[障害を作成 (Obstacle Creation)]** ダイアログボックスで、**[障害のタイプ (Obstacle Type)]** ドロップダウンリストから障害のタイプを選択します。作成可能な障害のタイプは、**[厚い壁 (Thick Wall)]**、**[薄い壁 (Light Wall)]**、**[重い扉 (Heavy Door)]**、**[軽い扉 (Light Door)]**、**[キュービクル (Cubicle)]**、および **[ガラス (Glass)]** です。
選択した障害のタイプの予測信号損失が自動的に取り込まれます。信号損失は、これらのオブジェクトの周辺の RF 信号強度を計算するために使用されます。
- ステップ 6** **[障害物の追加 (Add Obstacle)]** をクリックします。
- ステップ 7** 障害物を作成する領域に描画ツールを移動します。
- ステップ 8** 描画ツールをクリックして、描線を開始および停止します。
- ステップ 9** エリアの輪郭を描いてからダブルクリックすると、そのエリアが強調表示されます。
- ステップ 10** 表示される **[障害物の作成 (Obstacle Creation)]** ウィンドウで **[完了 (Done)]** をクリックします。
- ステップ 11** **[保存 (Save)]** をクリックして、障害をフロアマップに保存します。
- ステップ 12** 障害を編集するには、**[障害 (Obstacles)]** の隣にある **[オーバーレイ (Overlays)]** パネルで、**[編集 (Edit)]** をクリックします。
すべての使用可能な障害物がマップ上で強調表示されます。
- ステップ 13** 変更が完了したら、**[保存 (Save)]** をクリックします。
- ステップ 14** 障害を削除するには、**[障害 (Obstacles)]** の隣にある **[オーバーレイ (Overlays)]** パネルで、**[削除 (Delete)]** をクリックします。
すべての使用可能な障害物がマップ上で強調表示されます。
- ステップ 15** 障害にマウスカーソルを合わせ、クリックして削除します。
- ステップ 16** **[保存 (Save)]** をクリックします。
-

ロケーションリージョンの作成

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

フロアマップ上に包含領域と除外領域を配置するためのガイドライン

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

- フロア上の包含リージョンを1つだけ定義できます。デフォルトでは、各フロア領域が作成されるたびに、各フロア領域に対して包含領域が定義されます。包含領域は、水色の実線で示され、通常はフロア領域全体の輪郭を描きます。
- フロア領域に複数の除外領域を定義することができます。

フロア上の包含リージョンの定義

- ステップ 1** Cisco DNA Center のホームページで、**[Design] > [Network Hierarchy]** の順に選択します。
- ステップ 2** 左ペインで、フロアを選択します。
- ステップ 3** **[オーバーレイ (Overlays)]** パネルで、**[ロケーションリージョン (Location Regions)]** の横にある **[追加 (Add)]** をクリックします。
- ステップ 4** **[ロケーションリージョンの作成 (Location Region Creation)]** ダイアログ ウィンドウで、**[包含タイプ (Inclusion Type)]** ドロップダウン リストからオプションを選択します。
- ステップ 5** **[位置領域の追加 (Add Location Region)]** をクリックします。
包含領域の輪郭を描画するための描画アイコンが表示されます。
- ステップ 6** 包含領域の定義を開始するには、描画ツールをマップ上の開始ポイントに移動して、1回クリックします。
- ステップ 7** 含める領域の境界に沿ってカーソルを移動させ、クリックして境界線を終了します。
再びクリックすると、次の境界線を定義できます。
- ステップ 8** 領域の輪郭が描画されるまでステップ 7 を繰り返したら、描画アイコンをダブルクリックします。
水色の実線によって包含領域が定義されます。
- ステップ 9** **[保存 (Save)]** をクリックします。

フロア上の除外リージョンの定義

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

- ステップ 1** Cisco DNA Center のホームページで、**[Design] > [Network Hierarchy]** の順に選択します。
- ステップ 2** 左ペインで、フロアを選択します。
- ステップ 3** 中央のペインのフロアプランの上にある **[編集 (Edit)]** をクリックします。
- ステップ 4** **[オーバーレイ (Overlays)]** パネルで、**[ロケーションリージョン (Location Regions)]** の横にある **[追加 (Add)]** をクリックします。
- ステップ 5** **[ロケーションリージョンの作成 (Location Region Creation)]** ウィンドウで、**[除外タイプ (Exclusion Type)]** ドロップダウン リストから値を選択します。
- ステップ 6** **[ロケーションリージョン (Location Region)]** をクリックします。

除外領域の輪郭を描画するための描画アイコンが表示されます。

- ステップ 7** 除外領域の定義を開始するには、描画アイコンをマップ上の開始ポイントに移動して、1回クリックします。
- ステップ 8** 除外するエリアの境界に沿って描画アイコンを移動させます。
1回クリックして境界線を開始し、再びクリックして境界線を終了します。
- ステップ 9** エリアの輪郭が描画されるまで前の手順を繰り返したら、描画アイコンをダブルクリックします。定義された除外領域は、領域が完全に定義されると紫色で網掛けされます。
- ステップ 10** さらに除外領域を定義するには、手順 5 から手順 9 を繰り返します。
- ステップ 11** すべての除外領域が定義されている場合は、**[保存 (Save)]** をクリックします。

ロケーションリージョンの編集

- ステップ 1** **[オーバーレイ (Overlays)]** パネルで、**[ロケーションリージョン (Location Regions)]** の横にある **[編集 (Edit)]** をクリックします。
使用可能なロケーションリージョンがマップ上で強調表示されます。
- ステップ 2** 必要な変更を行って、**[保存 (Save)]** をクリックします。

ロケーションリージョンの削除

- ステップ 1** **[オーバーレイ (Overlays)]** パネルで、**[ロケーションリージョン (Location Regions)]** の横にある **[削除 (Delete)]** をクリックします。
使用可能なロケーションリージョンがマップ上で強調表示されます。
- ステップ 2** 削除する領域の上にマウスのカーソルを合わせ、**[削除 (Delete)]** をクリックします。
- ステップ 3** **[保存 (Save)]** をクリックします。

レールの作成

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

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

-
- ステップ 1 Cisco DNA Center のホームページで、**[Design]** > **[Network Hierarchy]** の順に選択します。
 - ステップ 2 左ペインで、フロアを選択します。
 - ステップ 3 中央のペインのフロアプランの上にある **[編集 (Edit)]** をクリックします。
 - ステップ 4 **[レール (Rails)]** の横にある **[オーバーレイ (Overlays)]** パネルで、**[追加 (Add)]** をクリックします。
 - ステップ 5 レールのスナップ幅（フィートまたはメートル）を入力して **[レールの追加 (Add Rail)]** をクリックします。
描画アイコンが表示されます。
 - ステップ 6 レールラインの開始ポイントで描画アイコンをクリックします。ラインの描画を停止するときやラインの方向を変える際は、再びクリックします。
 - ステップ 7 フロアマップ上にレールラインを描画したら、描画アイコンを 2 回クリックします。レールラインはマップ上に表示され、片側は定義されたスナップ幅リージョンに接します。
 - ステップ 8 **[保存 (Save)]** をクリックします。
 - ステップ 9 **[オーバーレイ (Overlays)]** パネルで、**[レール (Rails)]** の横にある **[編集 (Edit)]** をクリックします。
使用可能なレールがマップ上で強調表示されます。
 - ステップ 10 変更を加えて、**[保存 (Save)]** をクリックします。
 - ステップ 11 **[オーバーレイ (Overlays)]** パネルで、**[レール (Rails)]** の横にある **[削除 (Delete)]** をクリックします。
使用可能なすべてのレールラインがマップ上で強調表示されます。
 - ステップ 12 削除するレールラインの上にマウスのカーソルを合わせ、クリックして削除します。
 - ステップ 13 **[保存 (Save)]** をクリックします。
-

マーカーの配置

- ステップ 1 Cisco DNA Center のホームページで、**[Design]** > **[Network Hierarchy]** の順に選択します。
- ステップ 2 左ペインで、フロアを選択します。
- ステップ 3 中央のペインのフロアプランの上にある **[編集 (Edit)]** をクリックします。
- ステップ 4 **[オーバーレイ (Overlays)]** パネルで、**[マーカー (Markers)]** の横にある **[追加 (Add)]** をクリックします。
描画アイコンが表示されます。
- ステップ 5 マーカーの名前を入力し、**[マーカーの追加 (Add Marker)]** をクリックします。
- ステップ 6 描画アイコンをクリックし、マーカーをマップ上に配置します。
- ステップ 7 **[Save (保存)]** をクリックします。

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

使用可能なマーカーがマップ上で強調表示されます。

ステップ 9 変更を加えて、[保存 (Save)] をクリックします。

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

使用可能なすべてのマーカーがマップ上で強調表示されます。

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

ステップ 12 [保存 (Save)] をクリックします。

フロアビューオプション

中央のペインのフロアプランの上にある [オプションを表示 (View Options)] をクリックします。フロアマップと [アクセスポイント (Access Points)]、[センサー (Sensor)]、[オーバーレイオブジェクト (Overlay Objects)]、[マッププロパティ (Map Properties)]、および [グローバルマッププロパティ (Global Map Properties)] の各パネルが右側のペインに表示されます。

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

アクセスポイントの表示オプション

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

- [表示ラベル (Display Label)]: ドロップダウンリストから、AP に関してフロアマップに表示するテキストラベルを選択します。使用可能な表示ラベルは次のとおりです。
 - [なし (None)]: 選択したアクセスポイントに関してラベルが表示されません。
 - [名前 (Name)]: AP 名。
 - [AP MAC アドレス (AP MAC Address)]: AP の MAC アドレス。
 - [コントローラ IP (Controller IP)]: アクセスポイントが接続されているシスコワイヤレスコントローラの IP アドレス。
 - [無線 MAC アドレス (Radio MAC Address)]: 無線 MAC アドレス。
 - [IP Address]

- [チャンネル (Channel)] : Cisco Radio のチャンネル番号または [使用不可 (Unavailable)] (アクセス ポイントが接続されていない場合) 。
- [カバレッジホール (Coverage Holes)] : クライアントが接続を失うまで信号が弱まったクライアントのパーセンテージ。接続されていないアクセス ポイントについては [使用不可 (Unavailable)]、monitor-only モードのアクセス ポイントについては [MonitorOnly] と表示されます。
- [送信電力 (TX Power)] : 現在の Cisco Radio の送信電力レベル (1 が高い) または [使用不可 (Unavailable)] (アクセス ポイントが接続されていない場合) 。無線帯域を変更すると、マップ上の情報もそれに応じて変更されます。
電力レベルはアクセスポイントのタイプによって異なります。1000 シリーズの AP では 1 ~ 5 の値、1230 アクセス ポイントでは 1 ~ 7 の値、1240 および 1100 シリーズのアクセス ポイントでは 1 ~ 8 の値をとります。
- [チャンネルおよび送信電力 (Channel and Tx Power)] : チャンネルと送信電力レベルまたは [使用不可 (Unavailable)] (アクセス ポイントが接続されていない場合) 。
- [使用率 (Utilization)] : 関連付けられたクライアントデバイスで使用されている帯域幅のパーセンテージ (受信、送信、およびチャンネル使用率を含む) 。アソシエーションを解除されたアクセス ポイントでは [Unavailable]、monitor-only モードのアクセス ポイントでは [MonitorOnly] が表示されます。
- [送信使用率 (Tx Utilization)] : 指定されたインターフェイスの送信 (Tx) 使用率。
- [受信使用率 (Rx Utilization)] : 指定されたインターフェイスの受信 (Rx) 使用率。
- [チャンネル使用率 (Ch Utilization)] : 指定されたアクセス ポイントのチャンネル使用率。
- [関連付けられた Clients]] : 関連付けられたクライアントの総数。
- [デュアルバンド無線 (Dual-Band Radios)] : Cisco Aironet 2800 および 3800 シリーズ アクセス ポイント上の XOR デュアルバンド無線を識別してマークします。
- [ヘルス スコア (Health Score)] : AP のヘルス スコア。
- **問題数**
- **カバレッジの問題**
- **APダウンの問題**
- [ヒートマップ タイプ (Heatmap Type)] : ヒートマップは、変数から取得した値をマップに色として表した、無線周波数 (RF) ワイヤレス データのグラフィック表示です。現在のヒートマップは、RSSI 予測モデル、アンテナの方向、および AP 送信電力に基づいて計算されます。[ヒートマップ タイプ (Heatmap Type)] ドロップダウンリストから、ヒートマップのタイプ ([なし (None)] または [カバレッジ (Coverage)]) を選択してください。
- **None**

- [カバレッジ (Coverage)]: フロア プランにモニタ モードアクセス ポイントがある場合は、カバレッジ ヒートマップを選択できます。カバレッジ ヒートマップでは、モニタ モードアクセス ポイントは除外されます。
- [ヒートマップの不透明度 (%) (Heatmap Opacity(%))]: スライダを 0 ~ 100 の範囲でドラッグして、ヒートマップの不透明度を設定します。
- [RSSIカットオフ (dBm) (RSSI Cut off (dBm))]: スライダをドラッグして RSSI カットオフ レベルを設定します。RSSI Cutoff の範囲は -60 dBm ~ -90 dBm です。
- [マップの不透明度 (%) (Map Opacity (%))]: スライダをドラッグしてマップの不透明度を設定します。

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

View Options for Sensors

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

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

オーバーレイ オブジェクトの表示オプション

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

- カバレッジエリア
- ロケーション リージョン
- 障害物
- レール
- マーカー

マップ プロパティの設定

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

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

グローバル マップ プロパティの設定

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

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

データのフィルタリング

アクセスポイントデータのフィルタ処理

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

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

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

センサーデータのフィルタ処理

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

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

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

ゼロデイ Ekahau 計画ワークフロー

始める前に

Ekahau Pro ツールを使用すると、フロアレイアウト、AP の場所、障害物など、企業の完全なネットワーク計画を作成できます。フロアレイアウトを作成した後、シミュレートされたネットワーク計画と実際のサイト調査データを、Cisco DNA Center が使用可能な形式にエクスポートできます。Ekahau プロジェクトファイルを Cisco DNA Center にインポートして、さらに計画を立てることができます。

ステップ 1 Ekahau Pro ツールでフロアレイアウトを計画します。

- ビルディングとフロアを作成します。

Ekahau Pro ツールでのビルディングの作成は必須ではありません。

- フロアプランをインポートします。
- 計画された AP または仮想的な AP を追加します。

ここで指定した AP 名は、ワイヤレス コントローラ の設定中に、シスコ ワイヤレス コントローラ の AP 名を更新するために使用されます。

- 障害物を追加します。
- プロジェクトを PDF としてエクスポートします。

ステップ 2 フロアレイアウトで設計された場所に計画された AP を展開します。

- 物理 AP は、フロアレイアウトで指定された設計済みの場所に取り付けられます。計画された AP の MAC アドレスが、物理 AP の MAC アドレスで更新されます。
- 物理 AP は、目的 ワイヤレス コントローラ の VLAN に接続されています。

ステップ 3 シスコ ワイヤレス コントローラを設定します。

- 検出された ワイヤレス コントローラ と AP が [Inventory] ウィンドウにリストされるように、**検出** ジョブを実行して、ネットワーク内のシスコ ワイヤレス コントローラ とアクセスポイントを検出します。
- フロアプランニング中に Ekahau Pro プロジェクトで指定された AP 名を使用して、ワイヤレス コントローラ の AP 名を更新します。

ステップ 4 Ekahau プロジェクトを Cisco DNA Center にインポートします。

ステップ 5 計画された AP を Cisco DNA Center の実際の AP にマッピングします。


Cisco DNA Center への Ekahau プロジェクトのインポート

ステップ 1 サイト、ビルディング、フロアなどのネットワーク階層を設計します。

詳細については、[ネットワーク階層のサイトの作成 \(95 ページ\)](#)、[ビルディングの追加 \(99 ページ\)](#)、および[ビルディングへのフロアの追加 \(101 ページ\)](#)を参照してください。

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

ステップ 2 左側のペインで、Ekahau プロジェクトをインポートするサイトに移動します。

ステップ 3 サイトの横にある歯車アイコン  をクリックし、[Import Ekahau Project] を選択します。

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

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

インポートが成功すると、計画された各 AP は、AP 名を使用してインベントリ内の既存の実際の AP にマッピングされます。計画された AP は、フロアマップ上にアイコン [P] とともに表示されます。たとえば、計画された AP の名前が SJC01-02-AP-B-1 の場合、インポートプロセスでは同じ名前の実際の AP が検索されます。

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

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

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

- 新たに検出された AP が計画された AP と一致する場合、計画された AP は検出された実際の AP で置き換えられます。
- 計画された AP のマッピングが解除されたままの場合、計画された AP を実際の AP で手動で置き換えて、失敗の原因を示すことができます。

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

[Assign Planned APs] パネルが表示されます。

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

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

ステップ 9 [保存 (Save)] をクリックします。

インタラクティブフロアプランニングについて


インタラクティブプランニングでは、ラスターイメージまたは CAD フロアプランを背景として計画された AP や仮想 AP および障害物を描くことで、フロアレイアウトを計画できます。フロアマップを PDF としてエクスポートして、AP を設置している技術者と共有できます。フロアの描画は、技術者がフロアのレイアウトと正確な AP の設置場所を可視化するのに役に立ちます。

インタラクティブフロアプランニングでは、次のことができます。

- キャンバスとしてラスターまたは CAD フロアプランを使用してフロアレイアウトを作成する。
- 信号カバレッジ要件に基づいて、計画された AP または仮想 AP をフロアマップに配置する。これらの仮想 AP または計画された AP は、Cisco DNA Center によってまだインストールまたは検出されていません。
- アンテナのタイプと方向を割り当てる。
- フロアに障害物を描画する。
- すべての AP を順番に計画する。
- フロアマップを PDF としてエクスポートする。

インタラクティブフロアプランニング

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

- ステップ 2** サイト、ビルディング、フロアなどのネットワーク階層を設計します。
- ステップ 3** 左側のメニューで、フロアを選択します。
- 選択したフロアに計画された AP と障害物を描画できます。
- ステップ 4** 中央のペインのフロアプランの上にある **[編集 (Edit)]** をクリックします。
- ステップ 5** [Floor Elements] パネルで、[Planned Access Points] の横にある [Add] をクリックします。
- [Add Planned AP] ウィンドウが表示されます。
- ステップ 6** [AP Name] テキストボックスに、計画された AP の名前を入力します。
- ステップ 7** (オプション) [MAC Address] テキストボックスに、計画された AP の MAC アドレスを入力します。
- ステップ 8** [AP Model] ドロップダウンリストから、AP モデルを選択します。
- ステップ 9** [x] および [y] テキストボックスには、マップの水平方向スパンと垂直方向スパンをフィート単位で入力します。
- ステップ 10** [Ap Height] テキストボックスに、AP の高さを入力します。
- ステップ 11** [radio band] タブをクリックして、アンテナタイプ、方位角、および垂直面の方向を設定します。
- ステップ 12** [Antenna] ドロップダウンリストから、この AP の適切なアンテナタイプを選択します。
- アンテナイメージは、選択されたアンテナを反映しています。
- ステップ 13** アンテナタイプに応じて、[Azimuth] と [Elevation] の方向を度数で入力します。
- ステップ 14** **[保存 (Save)]** をクリックします。
- 新しく追加された計画された AP がフロアマップに表示されます。
- ステップ 15** 水平方向と垂直方向のスパン（つまり、x と y 座標）を指定していない場合、計画された AP はフロアマップの右上隅に表示されます。
- ステップ 16** マップ上の適切な場所にドラッグアンドドロップして、計画された AP をマップに正しく配置します。
- ステップ 17** **[保存 (Save)]** をクリックします。
- ステップ 18** 計画可能な次の AP は、フロアマップの右上隅に表示されます。
- ステップ 19** 次の AP を計画するには、ステップ 6 ~ 14 を繰り返します。
- ステップ 20** 障害物を描画するには、[Overlays] パネルで [Obstacles] の横にある [Add] をクリックします。
- 詳細については、「[障害物の作成 \(109 ページ\)](#)」を参照してください。
- ステップ 21** フロアプランを PDF としてエクスポートするには、[Network Hierarchy] ウィンドウの右上隅にある  アイコンをクリックし、[Export] を選択します。
- ステップ 22** [Export] ウィンドウで、[PDF] チェックボックスをオンにして PDF としてエクスポートします。
- ステップ 23** [エクスポート (Export)] をクリックします。
- PDF が作成され、ローカルマシンにダウンロードされます。PDF には、設定した計画された AP の詳細とともにフロアマップが含まれています。計画された AP は、AP モデルに基づいて表示されます。

グローバルワイヤレス設定の構成

グローバルワイヤレスネットワーク設定には、サービスセット識別子（SSID）、ワイヤレスインターフェイス、ワイヤレス無線周波数（RF）、およびセンサーの設定が含まれます。



(注) ワイヤレスセンサーデバイスプロファイルの作成は、AP 1800S センサーデバイスにのみ適用されます。

エンタープライズワイヤレスネットワーク用 SSID の作成

次の手順では、エンタープライズワイヤレスネットワークに SSID を設定する方法を説明しています。



(注) すべての SSID は、グローバルレベルで作成されます。サイト、ビルディング、フロアは、グローバルレベルから設定が継承されます。

- ステップ 1** Cisco DNA Center のホームページで、[Design] を選択します。
- ステップ 2** [Network Settings] ドロップダウンリストから、[Wireless] を選択します。
- ステップ 3** [エンタープライズワイヤレス (Enterprise Wireless)] の下で、[+ Add] をクリックします。
[Create an Enterprise Wireless Network] ウィンドウが表示されます。
- ステップ 4** [Wireless Network Name (SSID)] テキストボックスに、作成するワイヤレスネットワークまたは SSID の一意の名前を入力します。
名前には、1 つのスペースを含めて、最大 32 文字の英数字を使用できます。<および / を除くすべての特殊文字を使用できます。
. および * のサブストリングの組み合わせは使用できません。
- ステップ 5** [エンタープライズネットワークのタイプ (type Of Enterprise network)] ドロップダウンリストから、エンタープライズネットワークのタイプ (**音声とデータ**、または**データのみ**) を選択します。選択タイプは、ワイヤレスネットワークでプロビジョニングされる quality of service を定義します。
[Voice and Data] を選択すると、Quality of Service (QoS) が音声またはデータトラフィックのいずれかのアクセスに対して最適化されます。
[Data Only] オプションを選択した場合、Quality of Service (QoS) はワイヤレスデータトラフィックに対してのみ最適化されます。
- ステップ 6** [Fast Lane] チェックボックスをオンにして、このネットワークで fastlane 機能を有効にします。

[Fast Lane] を選択すると、最適化されたレベルのワイヤレス接続と高度な Quality of Service (QoS) を受けるように IOS デバイスを設定できます。

ステップ 7 範囲内のすべてのワイヤレスクライアントに SSID を表示しない場合は、[Broadcast SSID] ボタンをオフにします。

[Broadcast SSID] をオフにすると、この SSID に接続しようとしているクライアントで SSID が非表示になり、ワイヤレス インフラストラクチャの不要な負荷が軽減されます。

ステップ 8 次のいずれかのワイヤレスオプションを選択して、ワイヤレスバンドの設定を行います。

- **デュアルバンド動作 (2.4 ghz および 5 ghz):** WLAN は 2.4 と 5 ghz の両方に対して作成されます。バンドセレクトはデフォルトで無効です。
- **バンドセレクトによるデュアルバンド動作:** WLAN は 2.4 ghz および 5 GHz 用に作成され、バンドセレクトは有効になっています。
- **5 ghz のみ:** WLAN は 5 ghz に対して作成され、バンドセレクトは無効になります。
- **[2.4 GHz only] :** WLAN が 2.4 GHz 用に作成され、バンドセレクトが無効になります。

ステップ 9 [セキュリティのレベル (Level of Security)] の下で、このネットワークの暗号化および認証のタイプをセットします。セキュリティのオプションは次のとおりです。

- **[WPA2 エンタープライズ (WPA2 Enterprise)] :** 拡張可能認証プロトコル (EAP) (802.1x) を使用してより高レベルのセキュリティを実現し、リモート RADIUS サーバでネットワーク ユーザを認証および承認します。

- **[WPA2 パーソナル (WPA2 Personal)] :** パスフレーズまたは事前共有キー (PSK) を使用して、良好なセキュリティを実現します。ワイヤレス ネットワークにアクセスするパスキーがあれば誰でも使用できます。[WPA2 パーソナル (WPA2 Personal)] を選択した場合は、[パスフレーズ (Passphrase)] テキストボックスにパスフレーズを入力します。

(注) サイト、ビルディング、またはフロア レベルで、事前共有キー (PSK) をオーバーライドできます。ビルディングレベルで PSK をオーバーライドすると、後続のフロアは新しい設定を継承します。詳細については、「事前共有キーのオーバーライド (126 ページ)」を参照してください。

- **開く :** セキュリティは提供されません。すべてのデバイスが認証なしでワイヤレス ネットワークにアクセスできます。

ステップ 10 次の内容を設定するには、[Show Advanced Settings] をクリックします。

ステップ 11 [Fast Transition (802.11r)] を、[有効化 (Enable)]、[アダプティブ (Adaptive)]、または[無効化 (Disable)] モードに設定します。

デフォルトでは、[Fast Transition (802.11r)] が [Adaptive] モードに設定されています。

802.r を使用すると、ワイヤレスクライアントが AP から別の AP にすばやくローミングできます。Fast Transition によって、ワイヤレスクライアントが AP から別の AP にローミングするときの接続の中断が軽減されます。

- ステップ 12** [Over the DS] チェックボックスをオンにして、分散システム経由の Fast Transition を有効にします。このオプションは、[Fast Transition] を [Adaptive] モードに設定した場合にのみ指定できます。
- デフォルトでは、[Over the DS] が有効になっています。
- ステップ 13** [MAC フィルタリング (MAC Filtering)] チェックボックスをオンにし、SSID での MAC ベースのアクセス制御を有効にします。
- MAC フィルタリングを有効にすると、ワイヤレス LAN に追加した MAC アドレスにのみ WLAN への接続が許可されます。
- ステップ 14** [Session Timeout] チェックボックスをオンにして、値 (秒) を入力します。
- セッションタイムアウトとは、クライアントセッションがアクティブである最大時間を指します。この時間が経過すると再認証を受ける必要があります。デフォルトでは、[Session Timeout] が 1800 秒のタイムアウト付きで有効になります。値の範囲は 300 ~ 86400 秒です。
- ステップ 15** [Client Exclusion] チェックボックスをオンにして、クライアント除外タイマーの設定値を入力します。
- ユーザが認証に失敗すると、ワイヤレスコントローラはクライアントを接続対象から除外するため、除外タイマーが期限切れになるまで、クライアントはネットワークに接続できません。デフォルトでは、[Client Exclusion] が 180 秒のタイムアウト付きで有効になります。指定できる範囲は 0 ~ 2147483647 秒です。
- ステップ 16** [MFP Client Protection] で、[Optional]、[Required]、および [Disabled] オプションボタンのいずれかをクリックします。
- 管理フレーム保護 (MFP) により、管理フレームのセキュリティが強化されます。これによって、アクセスポイントとクライアントとの間で送受信される、保護および暗号化されていない 802.11 管理メッセージのセキュリティが確保されます。MFP は、インフラストラクチャとクライアントサポートの両方を実現します。
- デフォルトでは [Optional] が選択されています。[Required] を選択すると、MFP がネゴシエートされている場合 (つまり、WPA2 がワイヤレスコントローラ上で設定されており、クライアントが CCXv5 MFP をサポートしていて WPA2 にも設定されている場合) のみ、クライアントはアソシエーションを許可されます。
- ステップ 17** [11k] で [Neighbor List] チェックボックスをオンにすると、その 11k 対応クライアントは、ローミングの候補となる既知のネイバー AP に関するネイバーレポートを要求できます。
- ローミングを容易にするため、AP にアソシエートした 11k 対応クライアントは、ネイバー AP のリストに対する要求を送信します。この要求は、アクションフレームと呼ばれる 802.11 管理フレームの形式で送信されます。同じ WLAN にあるネイバー AP の Wi-Fi チャネル番号が付いたリストを使用して、AP は応答します。この応答もアクションフレームです。クライアントは応答フレームに基づき、次のローミング先の AP 候補を識別します。
- ステップ 18** [11v BSS Transition Support] で、次のように設定します。
- ステップ 19** [BSS Max Idle Service] チェックボックスをオンにして、アイドル期間タイマー値を設定します。アイドル期間タイマー値は、AP からクライアントへのアソシエーションおよび再アソシエーション応答フレームを使用して送信されます。

BSS 最大アイドル期間は、接続先のクライアントからフレームが送信されないという理由で AP がこのクライアントをアソシエート解除しないタイムフレームです。

ステップ 20 [Client User Idle Timeout] チェックボックスをオンにして値を入力し、WLAN のユーザアイドルタイムアウトを設定します。

クライアントが送信するデータがユーザアイドルタイムアウト内で指定されたしきい値のクォータを超える場合、クライアントはアクティブであると見なされ、ワイヤレス コントローラは次のタイムアウト期間中に更新されます。

デフォルトでは、[Client User Idle Timeout] が 300 秒のユーザアイドルタイムアウト付きで有効になります。

ステップ 21 [Directed Multicast Service] チェックボックスをオンにして、Directed Multicast Service を有効にします。

デフォルトでは、[Directed Multicast Service] が有効になっています。クライアントは Directed Multicast Service (DMS) を使用して、必要なマルチキャストパケットをユニキャストフレームとして送信するように AP に要求します。これにより、クライアントは長時間スリープ状態になり、バッテリーの電力が節約されます。

ステップ 22 [Next] をクリックします。

[ワイヤレス プロファイル (Wireless Profiles)] ウィンドウが表示されます。この SSID をワイヤレス プロファイルと関連付けることができます。

ステップ 23 [ワイヤレス プロファイル (Wireless Profiles)] ウィンドウで [+ 追加 (+Add)] をクリックして、新しいワイヤレス プロファイルを作成します。

ステップ 24 [ワイヤレス プロファイルの作成 (Create a Wireless Profile)] ウィンドウで、次を設定します。

ステップ 25 [ワイヤレス プロファイル名 (Wireless Profile Name)] テキスト ボックスに、ワイヤレス プロファイルの名前を入力します。

ステップ 26 [Yes] または [No] を選択して、SSID がファブリックであるか、非ファブリックであるかを指定します。

ファブリック SSID は、ソフトウェア定義型アクセス (SD アクセス) の一部であるワイヤレスネットワークです。ファブリック SSID を使用する場合は、SD アクセスが必須です。非ファブリックは、SD アクセスを必要としない従来のワイヤレスネットワークです。

ステップ 27 非ファブリック SSID を作成する場合は、[No] を選択して次のパラメータを設定します。

ステップ 28 [Interface Name] ドロップダウンリストから、SSID のインターフェイス名を選択するか、または [+ create a new wireless interface] をクリックして新しいワイヤレスインターフェイスを作成します。

これは、ワイヤレス インターフェイスに関連付けられている VLAN ID です。

ステップ 29 [Select Interface] ドロップダウンリストから、SSID のインターフェイス名を選択するか、または [+ Create a Wireless Interface] をクリックして新しいワイヤレスインターフェイスを作成します。

これは、ワイヤレス インターフェイスに関連付けられている VLAN ID です。

ステップ 30 [Flex Connect Local Switching] チェックボックスをオンにして、WLAN のローカルスイッチングを有効にします。ローカルスイッチングを有効化すると、この WLAN をアドバタイズするすべての FlexConnect アクセスポイントがデータパケットをローカルにスイッチできます。

事前共有キーのオーバーライド

- ステップ 31** ワイヤレスインターフェイスに関連付けられている VLANID は、選択したインターフェイス名に基づいて自動的に入力されます。
- VLAN ID を変更する場合は、[Local to VLAN] テキストボックスに VLAN ID の新しい値を入力します。
- ステップ 32** このプロファイルをサイトに割り当てるには、[Sites] をクリックします。
- ステップ 33** [Sites] ウィンドウで、サイトの横にあるチェックボックスをオンにしてこのプロファイルに関連付けます。
- 親サイトまたは個々のサイトのいずれかを選択できます。親サイトを選択すると、すべての子が親サイトの設定を継承します。チェックボックスをオフにして、サイトの選択を解除できます。
- ステップ 34** [OK] をクリックします。
- ステップ 35** テンプレートをネットワークプロファイルに関連付けるには、[Attach Template(s)] 領域の下にある [+Add] をクリックします。
- ステップ 36** [Device Type]、[Tag Name]、および [Template] ドロップダウンリストから、デバイスのタイプ、タグ、テンプレートを選択します。
- ステップ 37** [Add] をクリックします。
- [Wireless Profiles] ウィンドウに、作成したプロファイルが表示されます。
- ステップ 38** SSID をワイヤレスプロファイルに関連付けるには、[Wireless Profile] ウィンドウで、[Profile Name] チェックボックスをオンにします。
- ステップ 39** [完了 (Finish)] をクリックします。

事前共有キーのオーバーライド

SSID はグローバル階層に作成されます。サイト、ビルディング、およびフロアは、グローバル階層からの設定を継承します。サイト、ビルディング、またはフロア レベルで、事前共有キー (PSK) をオーバーライドできます。ビルディング レベルで PSK をオーバーライドすると、後続のフロアは新しい設定を継承します。

- ステップ 1** [設計 (Design)] [ネットワーク設定 (Network Settings)] > [ワイヤレス (Wireless)] > を選択します。
- ステップ 2** ツリーメニューで、PSK を編集するサイト、ビルディング、フロアを選択します。
- ステップ 3** [エンタープライズワイヤレス (Enterprise Wireless)] 配下の [パスフレーズ (Passphrase)] テキストボックスをクリックし、PSK SSID の新しいパスフレーズを入力します。
- ステップ 4** [保存 (Save)] をクリックします。
- 「SSID のパスフレーズが正常に更新されました」という成功メッセージが表示されます。
- SSID の横にある [継承 (inherit)] アイコンをクリックすると、元の設定が表示されます。

- ステップ 5** PSK オーバーライドをリセットするには、サイト、ビルディング、またはフロアの PSK SSID のチェックボックスをオンにして、[削除(Delete)]をクリックします。PSK はグローバルパスフレーズ値にリセットされます。

ゲストワイヤレス ネットワークの SSID の作成

この手順では、ゲストワイヤレスネットワークの SSID を作成する方法について説明します。

- ステップ 1** Cisco DNA Center のホーム ページから、[設計 (Design)] > [ネットワーク設定 (Network Settings)] > [ワイヤレス (Wireless)] を選択します。
- ステップ 2** [ゲストワイヤレス (Guest Wireless)] の下で、[+ 追加 (+Add)] をクリックして、新しい SSID を作成します。
- [ゲストワイヤレス ネットワークの作成 (Create a Guest Wireless Network)] ウィンドウが表示されます。
- ステップ 3** [ワイヤレス ネットワーク名 (SSID) (Wireless Network Name (SSID))] テキストボックスに、作成するゲスト SSID の一意の名前を入力します。名前には、1 つのスペースを含めて、最大 32 文字の英数字を使用できます。<および / を除くすべての特殊文字を使用できます。>
- . および * のサブストリングの組み合わせは使用できません。
- ステップ 4** [Level of Security] の下で、このゲストネットワークの暗号化および認証のタイプを [Web Policy] と [Open] から選択します。
- 外部 Web 認証 (EWA) では、[Level of Security] として [Web Policy] を選択し、[Authentication Server] として [External Authentication] を選択します。
- 中央 Web 認証 (CWA) では、[Level of Security] として [Web Policy] を選択し、[Authentication Server] として [ISE Authentication] を選択します。
- [Web Policy] の暗号化と認証タイプは、レイヤ 3 のセキュリティを強化します。
- [オープン (Open)] 暗号化と認証タイプは、セキュリティを提供しません。すべてのデバイスが認証なしでワイヤレスネットワークに接続できます。
- ステップ 5** [Web Policy] を選択した場合、認証サーバを [ISE Authentication]、[Web Authentication]、または [Web Passthrough] として設定する必要があります。
- ステップ 6** [ISE 認証 (ISE Authentication)] を選択した場合は、ドロップダウンリストから、作成するポータルタイプを選択します。
- [SelfRegistered] : ゲストは自己登録ゲストポータルにリダイレクトされ、情報を提供して登録して、自動的にアカウントを作成します。
 - [HotSpot] : ゲストはログイン情報なしでネットワークにアクセスできます。
- 認証が成功した後にゲストをリダイレクトするには、ドロップダウンリストから以下を選択します。

- [成功ページ (Success page)] : ゲストは [認証成功 (Authentication Success)] ウィンドウにリダイレクトされます。
- [元のページ (Original URL)] : ゲストは最初にリクエストした URL にリダイレクトされます。
- [カスタム URL (Custom URL)] : ゲストはここで特定されたカスタム URL にリダイレクトされます。 [リダイレクト URL (Redirect URL)] テキスト ボックスにリダイレクト URL を入力します。

SSID を作成したので、それをワイヤレスプロファイルに関連付ける必要があります。このプロファイルは、サイトにデバイスを展開するために使用されるトポロジを構築するのに役に立ちます。

ステップ 7 [Web Authentication] または [Web Passthrough] を選択した場合は、認証タイプとして [Internal] または [External] を設定します。

レイヤ 3 セキュリティ方式である Web 認証 (Web Auth) を使用すると、クライアントは、何らかの認証方式に合格するまでの間、Dynamic Host Configuration Protocol (DHCP) およびドメインネームシステム (DNS) のトラフィックを通過させることができます。

Web パススルーは、ゲストアクセスに使用されるソリューションであり、認証ログイン情報は必要ありません。Web パススルーでは、ワイヤレスユーザがインターネットを初めて使用するときに、使用ポリシーページにリダイレクトされます。ポリシーを承認すると、ユーザはインターネットを参照できます。

- [Internal] を選択すると、ページが シスコ ワイヤレス コントローラ によって再構築されます。
- [External] を選択した場合、クライアントは指定された URL にリダイレクトされます。 [Web Auth URL] テキストボックスにリダイレクト URL を入力します。

ステップ 8 [TIMEOUT SETTINGS FOR SLEEPING CLIENTS] の下で、スリープ状態のクライアントの認証を設定します。 [Always authenticate] または [Authenticate after] を選択できます。

Web 認証に成功したゲストアクセスを持つクライアントは、ログインページから別の認証プロセスを実行せずにスリープおよび復帰することを許可されています。再認証が必要になるまでスリープ状態にあるクライアントが記録される期間を設定できます。有効範囲は 10 ~ 43200 分、デフォルトは 720 分です。WLAN にマッピングされるユーザ グループ ポリシーと WLAN に、期間を設定できます。スリープタイマーは、アイドルタイムアウト後に有効になります。クライアントタイムアウトが WLAN のスリープタイマーに設定された時間より短い場合、クライアントのライフタイムがスリープ時間として使用されます。

- スリープ状態のクライアントの認証を有効にするには、 [Always authenticate] オプションボタンを選択します。
- [Authenticate after] オプションボタンを選択し、再認証が必要になるまでスリープ状態にあるクライアントが記憶される期間を入力します。有効な範囲は 10 ~ 43200 分、デフォルト期間は 720 分です。

ステップ 9 次の内容を設定するには、 [Show Advanced Settings] をクリックします。

ステップ 10 [Client Exclusion] チェックボックスをオンにして、クライアント除外タイマーの設定値を入力します。

ユーザが認証に失敗すると、ワイヤレスコントローラはクライアントを接続対象から除外するため、除外タイマーが期限切れになるまで、クライアントはネットワークに接続できません。デフォルトでは、

[Client Exclusion] が 180 秒のタイムアウト付きで有効になります。指定できる範囲は 0 ～ 2147483647 秒です。

ステップ 11 [Session Timeout] チェックボックスをオンにして、値（秒）を入力します。

セッションタイムアウトとは、クライアントセッションがアクティブである最大時間を指します。この時間が経過すると再認証を受ける必要があります。デフォルトでは、[Session Timeout] が 1800 秒のタイムアウト付きで有効になります。値の範囲は 300 ～ 86400 秒です。

ステップ 12 [MFP Client Protection] で、[Optional]、[Required]、および [Disabled] オプションボタンのいずれかをクリックします。

管理フレーム保護（MFP）により、管理フレームのセキュリティが強化されます。これによって、アクセスポイントとクライアントとの間で送受信される、保護および暗号化されていない 802.11 管理メッセージのセキュリティが確保されます。MFP は、インフラストラクチャとクライアントサポートの両方を実現します。

デフォルトでは [Optional] が選択されています。[Required] を選択すると、MFP がネゴシエートされている場合（つまり、WPA2 がワイヤレス コントローラ 上で設定されていて、クライアントが CCXv5 MFP をサポートしていて WPA2 にも設定されている場合）のみ、クライアントはアソシエーションを許可されます。

ステップ 13 [11v BSS Transition Support] で、次のように設定します。

ステップ 14 [BSS Max Idle Service] チェックボックスをオンにして、アイドル期間タイマー値を設定します。アイドル期間タイマー値は、AP からクライアントへのアソシエーションおよび再アソシエーション応答フレームを使用して送信されます。

BSS 最大アイドル期間は、接続先のクライアントからフレームが送信されないという理由で AP がこのクライアントをアソシエート解除しないタイムフレームです。

ステップ 15 [Client User Idle Timeout] チェックボックスをオンにして値を入力し、WLAN のユーザアイドルタイムアウトを設定します。

クライアントが送信するデータがユーザアイドルタイムアウト内で指定されたしきい値のクォータを超える場合、クライアントはアクティブであると見なされ、ワイヤレス コントローラは別のタイムアウト期間中に更新します。

デフォルトでは、[Client User Idle Timeout] が 300 秒のユーザアイドルタイムアウト付きで有効になります。

ステップ 16 [Directed Multicast Service] チェックボックスをオンにして、Directed Multicast Service を有効にします。

デフォルトでは、[Directed Multicast Service] が有効になっています。クライアントは Directed Multicast Service（DMS）を使用して、必要なマルチキャストパケットをユニキャストフレームとして送信するように AP に要求します。これにより、クライアントは長時間スリープ状態になり、バッテリーの電力が節約されます。

ステップ 17 [Next] をクリックします。

[ワイヤレス プロファイル（Wireless Profiles）] ウィンドウが表示されます。

- ステップ 18** 既存のワイヤレスプロファイルがない場合は、[ワイヤレスプロファイル (Wireless Profiles)] ウィンドウで [+ 追加 (+ Add)] をクリックして、新しいワイヤレスプロファイルを作成します。
- ステップ 19** [ワイヤレス プロファイル名 (Wireless Profile Name)] テキスト ボックスにプロファイル名を入力します。
- ステップ 20** [ファブリック (Fabric)] の隣にある [はい (Yes)] または [いいえ (No)] ラジオ ボタンを選択して、SSID がファブリックであるか、そうでないかを指定します。
- ファブリック SSID は、ソフトウェア定義型アクセス (SD アクセス) の一部であるワイヤレスネットワークです。SD アクセスは、有線およびワイヤレスネットワークの設定、ポリシー、およびトラブルシューティングを自動化し、簡素化するソリューションです。ファブリック SSID を使用する場合は、SDA を使用することが必須です。非ファブリックは、SD アクセスを必要としない従来のワイヤレスネットワークです。
- ステップ 21** ゲスト SSID をゲスト アンカーにする場合、[このゲスト SSID にゲスト アンカーが必要ですか (Do you need a Guest Anchor for this guest SSID)] の隣にある [はい (Yes)] または [いいえ (No)] ラジオ ボタンをクリックします。
- ゲストの SSID をゲストアンカーにするには、[はい (Yes)] を選択します。
- [No] を選択した場合は、[Flex Connect Local Switching] チェックボックスをオンにして、FlexConnect モードを有効にします。FlexConnect を選択すると、トラフィックがローカルに切り替わります。設定に基づき、プロファイルはサイトおよび内部的に作成された Flex グループに適用されます。
- ステップ 22** [インターフェイスを選択 (Select Interface)] ドロップダウンリストからインターフェイスを選択するか、[+] をクリックして新しいワイヤレス インターフェイスを作成します。
- これは、ワイヤレス インターフェイスに関連付けられている VLAN ID です。
- ステップ 23** サイトにこのプロファイルを割り当てるには、[サイトセクタ (Site Selector)] テキスト ボックスに、完全なサイト名またはサイト名の一部を入力します。
- 使用可能なサイトが自動入力され、ドロップダウンリストから目的のサイトを選択することができます。
- ステップ 24** [保存 (Save)] をクリックします。
- [ワイヤレス プロファイル (Wireless Profiles)] ウィンドウに、作成したプロファイルが表示されます。
- ステップ 25** SSID をワイヤレスプロファイルに関連付けるには、[Wireless Profiles] ウィンドウで、[Profile Name] チェックボックスをオンにして SSID を関連付けてから、[Next] をクリックします。
- [ポータルのカスタマイズ (Portal Customization)] ウィンドウが表示され、ゲスト ポータルに SSID を割り当てることができます。
- ステップ 26** [ポータルのカスタマイズ (Portal Customization)] ウィンドウで [+ 追加 (+ Add)] をクリックして、ゲスト ポータルを作成します。
- [ポータルビルダー (Portal Builder)] ウィンドウが表示されます。
- ステップ 27** 左側のメニューで [ページ コンテンツ (Page Content)] を展開し、さまざまな変数を組み込みます。
- ステップ 28** ポータルテンプレート ウィンドウに変数をドラッグアンドドロップし、それらを編集します。
- [Login] ページの変数は、[Access Code]、[Header Text]、[AUP]、および [Text Fields] です。

- [Registration] ページの変数は、[First Name]、[Last Name]、[Phone Number]、[Company]、[Sms Provider]、[Person being visited]、[Reason for a visit]、[Header text]、[User Name]、[Email Address]、および [AUP] です。
- [Registration Success] ページの変数は、[Account Created] および [Header texts] です。
- [成功 (Success)] ページの変数：テキストフィールドです。

- ステップ 29** ポータルのデフォルト カラー スキームをカスタマイズするには、左側のメニューで [色 (Color)] を展開し、色を変更します。
- ステップ 30** フォントをカスタマイズするには、左側のメニューで [フォント (Font)] を展開し、フォントを変更します。
- ステップ 31** [保存 (Save)] をクリックします。
[ポータルのカスタマイズ (Portal Customization)] ページに作成したポータルが表示されます。
- ステップ 32** [ポータル (Portals)] の下で、[ポータル名 (Portal Name)] の隣にあるラジオ ボタンをクリックし、ゲストポータルに SSID を割り当てます。
- ステップ 33** [完了 (Finish)] をクリックします。

ゲストポータルページの作成

次のゲストポータルページを作成できます。

- ログイン ページ
- 登録 ページ
- 登録成功
- 成功 ページ

- ステップ 1** Cisco DNA Center のホームページで、[Design] > [Network Settings] > [Wireless] > [Guest Wireless] を選択します。
- ステップ 2** 作成しているポータルページに移動します。
- ステップ 3** [Portal Name] テキストボックスにポータル名を入力します。
- ステップ 4** 左側のメニューで [Page Content] を展開し、ポータルページの作成中にさまざまな変数を組み込みます。
- ログインページの変数のリスト：
 - アクセスコード：
 - ヘッダー テキスト (Header Text)
 - AUP
 - テキストフィールド (Text Fields)

- 登録ページのリスト変数 :
 - First Name
 - Last Name
 - Phone Number
 - Company
 - Sms Provider
 - Person being visited
 - Reason for a visit
 - Header text
 - User Name
 - Email Address
 - AUP
- 登録ページの変数のリスト :
 - Account Created
 - Header texts
- 成功ページの変数 :
 - Text fields

ステップ5 ポータルテンプレートページに変数をドラッグアンドドロップし、それらを編集します。

ステップ6 ポータルのデフォルトカレースキームをカスタマイズするには、左側のメニューで[Color]を展開し、次のページ要素の色を変更します。

- 本文テキスト境界線
- リンクテキストページ
- Background
- 境界線の色
- ヘッダーの背景

ステップ7 フォントをカスタマイズするには、左側のメニューで [Font] を展開し、次を変更します。

- 書体
- ヘッダー
- タイトルテキスト
- 本文

- フォームラベル

ステップ 8 [Save] をクリックしてポータルを保存します。

ワイヤレスインターフェイスの作成

非ファブリック展開でのみワイヤレスインターフェイスを作成できます。

ステップ 1 Cisco DNA Center のホーム ページから、[設計 (Design)] > [ネットワーク設定 (Network Settings)] > [ワイヤレス (Wireless)] を選択します。

ステップ 2 [ワイヤレス インターフェイス (Wireless Interfaces)] の下で、[+ 追加 (+Add)] をクリックします。
[新しいインターフェイス (New Interfaces)] ウィンドウが表示されます。

ステップ 3 [インターフェイス名 (Interfaces Name)] テキスト ボックスで、動的なインターフェイスの名前を入力します。

ステップ 4 (オプション) [VLAN ID] テキスト ボックスで、インターフェイスの VLAN ID を入力します。有効な範囲は 0 ~ 4094 です。

ステップ 5 [OK] をクリックします。

ワイヤレス インターフェイスの下に、作成したインターフェイスが表示されます。

ワイヤレス無線周波数プロファイルの作成

デフォルトの無線周波数プロファイル (低、標準、高) を使用するか、またはカスタムの無線周波数プロファイルを作成できます。

ステップ 1 Cisco DNA Center のホーム ページから、[設計 (Design)] > [ネットワーク設定 (Network Settings)] > [ワイヤレス (Wireless)] を選択します。

ステップ 2 [ワイヤレス無線周波数プロファイル (Wireless Radio Frequency Profile)] の下で、[+RF を追加 (+Add RF)] をクリックします。

[ワイヤレス無線周波数 (Wireless Radio Frequency)] ウィンドウが表示されます。

ステップ 3 [プロファイル名 (Profile Name)] テキスト ボックスに、RF プロファイル名を入力します。

ステップ 4 [オン (On)]/[オフ (Off)] ボタンを使用して、[2.4 GHz] または [5 GHz] のいずれかの無線バンドを選択します。無線のうちの1つを無効にした場合、この AP プロファイルを設定しようとしている AP の基本の無線が無効になります。

ステップ 5 [2.4 GHz] 無線タイプでは、次を設定します。

- [Parent Profile] で、[High]、[Medium (Typical)]、[Low]、または [Custom] を選択します。（[データレート (Data Rate)] および [Tx設定 (Tx Configuration)] フィールドは、選択された親プロファイルによって変更されます。たとえば、[高 (High)] を選択した場合、2.4 GHz のデバイスで使用可能なプロファイル設定が追加されます。保存された [データレート (Data Rate)] および [Tx設定 (Tx Configuration)] で設定を変更すると、[親プロファイル (Parent Profile)] は自動的に [カスタム (Custom)] に変更されます。）選択したカスタムプロファイルに対してのみ、新しい RF プロファイルが作成されることに注意してください。

(注) [低 (Low)]、[中 (標準) (Medium (Typical))]、および [高 (High)] は、事前に定義された RF プロファイルです。事前に定義された RF プロファイルのいずれかを選択した場合、デバイスにあるそれぞれの RF プロファイルが使用され、新しい RF プロファイルは Cisco DNA Center で作成されません。

- [DCA] は RF グループへのチャンネルの割り当てを動的に管理し、AP 無線ごとに割り当てを評価します。
 - [すべて選択 (Select All)] チェック ボックスをオンにして、DCA チャンネル [1]、[6]、および [11] を選択します。または、チャンネル番号の隣にある個々のチェック ボックスをオンにします。
 - [Advanced Options] の下で [Show Advanced] をクリックし、チャンネル番号を選択します。[すべてを選択 (Select All)] チェック ボックスをオンにして、[詳細オプション (Advanced Options)] の下にある DCA チャンネルを選択するか、個々のチャンネル番号の隣にあるチェック ボックスをオンにします。B プロファイルで使用可能なチャンネル番号は、[2]、[3]、[4]、[5]、[7]、[8]、[9]、[10]、[12]、[13]、[14] です。

(注) シスコワイヤレスコントローラでこれらのチャンネルをグローバルに設定する必要があります。

- アクセスポイントとクライアント間でデータを転送できるレートを設定するには、[Supported Data Rate] スライダを使用します。使用可能なデータレートは、[1]、[2]、[5.5]、[6]、[9]、[11]、[12]、[18]、[24]、[36]、[48]、[54] です。
- [Tx電力構成 (Tx Power Configuration)] で、AP の電力レベルと電力しきい値を設定できます。

- **電力レベル**：AP の電力を削減する必要があるかどうかを判断します。AP の電力を削減すると、同一チャンネルまたは近接するチャンネル上の別の AP との同一チャンネル干渉を軽減するのに役立ちます。[電力レベル (Power Level)] スライダを使用して、電力レベルの最小または最大値を設定します。指定できる範囲は -10 ～ 30 dBm で、デフォルトは -10 dBm です。
- **電力しきい値**：無線リソース管理 (RRM) を使用したカットオフ信号レベルで、AP の電力を削減するかどうかを判断します。[電力しきい値 (Power Threshold)] スライダを使用して電力値を増減させ、AP をより高い、またはより低い送信電力レートで動作させるようにします。指定できる範囲は -50 dBm ～ 80 dBm で、デフォルトのしきい値は -70 dBm です。
- **RX SOP**：レシーバのパケット検出開始しきい値 (RX SOP) は、AP の無線がパケットを復調してデコードする dBm 単位の Wi-Fi 信号レベルを決定します。[RX SOP] ドロップダウンリストから、各 802.11 バンドのしきい値を、[高 (High)]、[中 (Medium)]、[低 (Low)]、および [自動 (Auto)] から選択します。

ステップ 6 [5 GHz] 無線タイプでは、次を設定します。

- [親プロファイル (Parent Profile)] ドロップダウンリストから、[高 (High)]、[中 (標準) (Medium (Typical))]、[低 (Low)]、または[カスタム (Custom)]を選択します。([データレート (Data Rate)] および[Tx設定 (Tx Configuration)] フィールドは、選択された親プロファイルによって変更されます。たとえば、[高 (High)]を選択した場合、2.4 GHzのデバイスで使用可能な設定が追加されます。保存された[データレート (Data Rate)] および[Tx設定 (Tx Configuration)] フィールドで設定を変更すると、[親プロファイル (Parent Profile)] は自動的に[カスタム (Custom)]に変更されます。) 選択したカスタム プロファイルに対してのみ、新しい RF プロファイルが作成されます。

(注) [低 (Low)]、[中 (標準) (Medium (Typical))]、および[高 (High)]は、事前に定義された RF プロファイルです。事前に定義された RF プロファイルのいずれかを選択した場合、すでにデバイスにあるそれぞれの RF プロファイルが使用され、新しい RF プロファイルは Cisco DNA Center で作成されません。

- [チャンネル幅 (Channel Width)] ドロップダウンリストから、チャンネル帯域幅オプションを1つ選択します：[最適 (Best)]、[20 MHz]、[40 MHz]、[80 MHz]、[160 MHz]、または[最適 (Best)]。
- [DCA チャンネル (DCA Channel)] を設定して、チャンネルの割り当てを管理します。

(注) シスコ ワイヤレス コントローラでこれらのチャンネルをグローバルに設定する必要があります。

- [UNII-1 36-48] : UNII-1 バンドで使用可能なチャンネルは、[36]、[40]、[44]、[48] です。[UNII-1 36-48] チェック ボックスをオンにしてすべてのチャンネルを含めるか、チャンネルのチェック ボックスをオンにして、個別に選択します。
 - [UNII-2 52-144] : UNII-2 バンドで使用可能なチャンネルは、[52]、[56]、[60]、[64]、[100]、[104]、[108]、[112]、[116]、[120]、[124]、[128]、[132]、[136]、[140]、[144] です。[UNII-2 52-144] チェック ボックスをオンにしてすべてのチャンネルを含めるか、1つまたは複数のチャンネルのチェック ボックスをオンにして、個別に選択します。
 - [UNII-3 149-165] : UNII-3 バンドで使用可能なチャンネルは、[149]、[153]、[157]、[161]、[165] です。[UNII-3 149-165] チェック ボックスをオンにしてすべてのチャンネルを含めるか、1つまたは複数のチャンネルのチェック ボックスをオンにして、個別に選択します。
- アクセスポイントとクライアント間でデータを送信できるレートを設定するには、[データレート (Data Rate)] スライダを使用します。使用可能なデータ レートは、[6]、[9]、[12]、[18]、[24]、[36]、[48]、[54] です。
 - [Tx電力構成 (Tx Power Configuration)] で、AP の電力レベルと電力しきい値を設定できます。
 - **電力レベル** : AP の電力を削減する必要があるかどうかを判断します。AP の電力を削減すると、同一チャンネルまたは近接するチャンネル上の別の AP との同一チャンネル干渉を軽減するのに役立ちます。[電力レベル (Power Level)] スライダを使用して、電力レベルの最小または最大値を設定します。指定できる範囲は-10 ~ 30 dBm で、デフォルトは -10 dBm です。
 - **電力しきい値** : 無線リソース管理 (RRM) を使用したカットオフ信号レベルで、AP の電力を削減するかどうかを判断します。[電力しきい値 (Power Threshold)] スライダを使用して電力値を

増減させ、APをより高い、またはより低い送信電力レートを動作させるようにします。指定できる範囲は -50 dBm ~ 80 dBm で、デフォルトのしきい値は -70 dBm です。

- **RX SOP** : レシーバのパケット検出開始しきい値 (RX SOP) は、APの無線がパケットを復調してデコードする dBm 単位の Wi-Fi 信号レベルを決定します。[RX SOP] ドロップダウンリストから、各 802.11 バンドのしきい値を、[高 (High)]、[中 (Medium)]、[低 (Low)]、および [自動 (Auto)] から選択します。

ステップ 7 [保存 (Save)] をクリックします。

ステップ 8 プロファイルをデフォルトの RF プロファイルとしてマークするには、[プロファイル名 (Profile Name)] チェック ボックスをオンにし、[デフォルトとしてマーク (Mark Default)] をクリックします。

ステップ 9 [Warning] ウィンドウで [OK] をクリックします。


バックホール設定の管理


センサーのバックホール設定を表示、作成、および管理するには、次の手順を実行します。センサーには、Cisco DNA Center と通信するためのバックホール SSID が必要です。

ステップ 1 Cisco DNA Center のホームページで、**アシュアランス** タブをクリックします。
[Overall Health] ダッシュボードが表示されます。

ステップ 2 [Manage] > [Sensors] > [Backhaul Settings] の順に選択します。
[Backhaul Settings] ウィンドウが表示されます。

ステップ 3 バックホール SSID を追加および管理するには、次の手順を実行します。

- a)  **Add Backhaul** をクリックします。
[Create Sensor Backhaul SSID Assignment] ウィンドウが開きます。
- b) [Create Sensor Backhaul SSID Assignment] ウィンドウで、次の設定を行います。
 - [Settings Name] : バックホール SSID の名前を入力します。
 - [Wireless Network Name (SSID)] : このバックホール SSID に使用するワイヤレスネットワーク (SSID) を選択します。
 - [Level of Security] : 選択した SSID で使用されている暗号化と認証タイプが表示されます。使用可能なセキュリティのオプションは次のとおりです。

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

c) [保存 (Save)] をクリックします。

ステップ 4 既存のバックホール設定を編集するには、次の手順を実行します。

- バックホール設定のチェックボックスをオンにします。
- [Actions] ドロップダウンリストにカーソルを合わせて、[Edit] を選択します。

ステップ 5 バックホール設定を削除するには、次の手順を実行します。

- バックホール設定のチェックボックスをオンにします。
- [Actions] ドロップダウンリストにカーソルを合わせて、[Delete] を選択します。

Cisco Connected Mobile Experiences の統合について


Cisco DNA Center は、ワイヤレス マップのためのオンプレミス Connected Mobile Experiences (CMX) の統合をサポートしています。CMX を統合すると、Cisco DNA Center ユーザ インターフェイス内で、フロア マップ上でのクライアントの正確な場所を把握できます。

CMX の設定は、ユーザの要件に応じて、グローバルレベルで、あるいはサイト、ビルディング、またはフロアレベルで作成できます。小企業の場合はグローバルレベル (親ノード) で CMX を割り当てることができます。すべての子が親ノードから設定を継承します。中企業の場合はビルディング レベルで CMX を割り当てることができ、小企業の場合はフロア レベルで CMX を割り当てることができます。



(注) セキュリティ上の理由から、CMX は匿名にする必要があります。

Cisco CMX 設定の作成

- ステップ 1** CMX サーバを Cisco DNA Center に追加するには、Cisco DNA Center のホームページで、歯車アイコン (⚙) をクリックし、**[System Settings] > [Settings] > [CMX Servers]** を選択します。
- [CMX Servers] ウィンドウが表示されます。
- ステップ 2**  **[Add]** をクリックします。
- [Add CMX Servers] ウィンドウが表示されます。
- ステップ 3** [IP Address] フィールドに、CMX Web GUI の有効な IP アドレスを入力します。
- ステップ 4** [User Name] および [Password] フィールドに、CMX Web GUI のユーザ名とパスワードのログイン情報を入力します。
- ステップ 5** [SSH User Name] および [SSH Password] フィールドに、CMX 管理者のユーザ名とパスワードのログイン情報を入力します。
- (注) CMX が到達可能であることを確認してください。
- ステップ 6** [Add] をクリックします。
- CMX サーバが正常に追加されました。
- ステップ 7** サイト、ビル、またはフロアに CMX サーバを割り当てるには、次の手順を実行します。
- ステップ 8** [設計 (Design)] **[ネットワーク設定 (Network Settings)] > [ワイヤレス (Wireless)] >** を選択します。
- ステップ 9** 左側の [Tree View] メニューで、[Global] か、興味のあるエリア、ビルディング、フロアを選択します。
- ステップ 10** [CMX Servers] の下で、[CMX Servers] ドロップダウンリストから CMX サーバを選択します。
- ステップ 11** **[保存 (Save)]** をクリックします。
- [Create CMX Settings] ページが表示されます。
- CMX の追加後に [Network Hierarchy] ページのフロアに変更を加えた場合、その変更は自動的に CMX と同期されます。
- CMX が同期されると、Cisco DNA Center はクライアントロケーションを CMX に照会し、その場所がフロアマップに表示されます。
- フロア マップでは、次のことを実行できます。
- クライアントの場所を表示します。これは青色のドットとして表示されます。
 - AP 上にカーソルを移動します。ダイアログボックスは、[Info]、[Rx Neighbor]、[Clients] のタブで表示されます。詳細については、各タブをクリックしてください。[デバイス 360 (Device 360)] をクリックして、デバイス 360 ウィンドウを開き、問題を表示します。問題をクリックして、問題の場所とクライアントデバイスの場所を表示します。
 - AP をクリックして、AP に関する詳細を含むサイドバーを開きます。
 - Intelligent Capture と CMX を統合するときにリアルタイムでクライアント トラッキングを実行します。

- ステップ 12** 変更を加えたときに CMX がダウンした場合は、手動で同期する必要があります。手動で同期するには、[Network Hierarchy] ページで、左側のツリーペインで変更を加えたビルディングやフロアの隣にある歯車アイコンをクリックし、[Sync with CMX] を選択して、変更を手動でプッシュします。
- ステップ 13** CMX サーバの詳細を編集するには、Cisco DNA Center で歯車アイコン (⚙️) をクリックし、[System Settings] > [Settings] > [CMX Servers] を選択します。
- ステップ 14** 編集する CMX サーバを選択して変更を加え、[Update] をクリックします。
- ステップ 15**
- ステップ 16** CMX サーバを削除するには、Cisco DNA Center で歯車アイコン (⚙️) をクリックし、[System Settings] > [Settings] > [CMX Servers] を選択します。
- ステップ 17** 削除する CMX サーバを選択し、[Delete] をクリックします。
- ステップ 18** [OK] をクリックして削除を実行します。

CMX 認証に失敗した場合

- Cisco DNA Center で CMX 設定の作成時に指定したログイン情報で、CMX Web GUI にログインできるか確認します。
- SSH を使用して CMX コンソールにログインできるかどうかを確認します。
- CMX UI の API ドキュメンテーション リンクを使用して CMX REST API を使用できるかどうかを確認します。

クライアントが Cisco DNA Center フロアマップに表示されない場合

- 特定のフロアのシスコ ワイヤレス コントローラが CMX で設定されており、アクティブになっているか確認します。
- CMX GUI でフロアマップにクライアントが表示されるか確認します。
- Cisco DNA Center マップ API を使用して、フロアにクライアントをリスト表示します。

```
curl -k -u <user>:<password> -X GET
/api/v1/dna-maps-service/domains/<floor group
id>/clients?associated=true
```


Flex グループのネイティブ VLAN 設定

ネイティブ VLAN は、AP と シスコ ワイヤレス コントローラ 間の管理トラフィックを伝送します。この機能を使用すると、Cisco DNA Center ユーザ インターフェイスを介してサイトの VLAN を設定できます。グローバル レベルでネイティブ VLAN を設定し、サイト、ビルディング、またはフロア レベルでオーバーライドできます。

- ステップ 1** Cisco DNA Center のホーム ページから、[設計 (Design)] > [ネットワーク設定 (Network Settings)] > [ワイヤレス (Wireless)] を選択します。
- ステップ 2** グローバル レベルでネイティブ VLAN を設定する場合、左ペインで [グローバル (Global)] を選択します。

- ステップ 3** [ネイティブVLAN (Native VLAN)] の下の [VLAN] テキスト ボックスに、VLAN ID の値を入力します。有効な範囲は 1 ~ 4094 です。
- ステップ 4** [保存 (Save)] をクリックします。
- ステップ 5** SSID を設定し、ワイヤレス ネットワーク プロファイルを作成します。[設計 (Design)] > [ネットワークの設定 (Network Settings)] > [ワイヤレス (Wireless)] ページの [FlexConnect ローカルスイッチング (FlexConnect Local Switching)] チェック ボックスがオンになっていることを確認します。詳細については、[エンタープライズワイヤレスネットワーク用 SSID の作成 \(122 ページ\)](#) および [ゲストワイヤレスネットワークの SSID の作成 \(127 ページ\)](#) を参照してください。
- ステップ 6** 保存済みの VLAN ID をワイヤレス コントローラ で設定するには、ワイヤレス コントローラ を [プロビジョニング (Provision)] ページでプロビジョニングする必要があります。詳細については、「[Cisco Wireless Controller をプロビジョニングする \(276 ページ\)](#)」を参照してください。
- ステップ 7** ワイヤレス コントローラ のプロビジョニング後に、コントローラに関連付けられている AP をプロビジョニングする必要があります。詳細については、「[シスコ製 AP のプロビジョニング : Day 1 AP プロビジョニング \(284 ページ\)](#)」を参照してください。
- ステップ 8** サイト、ビルディング、またはフロアレベルでネイティブ VLAN をオーバーライドするには、左側のツリー ビュー メニューでサイト、ビルディングまたはフロアを選択します。
- ステップ 9** [ネイティブVLAN (Native VLAN)] の下で、VLAN ID の値を入力します。
- ステップ 10** ワイヤレス コントローラ および関連付けられているアクセス ポイントを再プロビジョニングします。

ネットワーク プロファイルの作成

Cisco DNA Center のホームページから、[設計 (Design)] > [ネットワークプロファイル (Network Profiles)] を選択します。[プロファイルの追加 (Add Profile)]  をクリックして、次の項目に関するネットワーク プロファイルを作成します。

- ルーティングと NFV
- スイッチング
- ワイヤレス

NFVIS 用のネットワークプロファイルの作成

このワークフローでは、次を実行する方法を示します。

1. ルータ WAN を設定します。
2. ENCS 統合スイッチを設定します。



(注) このオプションは、ENCS 5400 デバイスでのみ使用できます。

3. カスタム構成を作成します。
4. プロファイルの概要を表示します。

ステップ 1 [設計 (Design)] > [ネットワークプロファイル (Network Profiles)] を選択します。

ステップ 2 [+Add Profiles] をクリックし、[NFVIS] を選択します。

ステップ 3 [ルータWAN構成 (Router WAN Configuration)] ウィンドウが表示されます。

- [名前 (Name)] テキスト ボックスにプロファイル名を入力します。
- ドロップダウンリストから、[Service Providers] および [Devices] の数を選択します。プロファイルあたり最大 3 つのサービスプロバイダーと 2 つのデバイスがサポートされています。
- ドロップダウンリストから [Service Provider Profile] を選択します。詳細については、「[サービス プロバイダープロファイルの設定 \(161 ページ\)](#)」を参照してください。
- ドロップダウンリストから [Device Type] を選択します。
- [Device Tag] に一意の文字列を入力して異なるデバイスを識別するか、ドロップダウンリストから既存のタグを選択します。選択内容は、ネットワークプロファイルに適用される Day-0 および Day-N テンプレートの一致基準の一部として使用されるため、適切なタグを選択してください。
- デバイスごとに 1 つ以上の回線リンクを有効にするには、[O] をクリックし、[Connect] の横のチェックボックスをオンにします。ドロップダウンリストから、[Line Type] を選択します。[OK] をクリックします。
- [+サービスの追加 (+Add Services)] をクリックして、プロファイルにサービスを追加します。[サービスの追加 (Add Services)] ウィンドウが表示されます。[ISRV vEdge]、[WAN最適化装置 (WAN Optimizer)]、または[ファイアウォール (Firewall)] の横のチェック ボックスをオンにします。または、[+サービスまたはネットワークの追加 (+Add Service or Network)] を選択して、プロファイルにカスタム サービスまたはネットワークを追加することもできます。

ISRV ルータを構成するには、ドロップダウンリストから [Profile] を選択します。詳細については、[ソフトウェアイメージのインポート \(77 ページ\)](#) を参照してください。[保存 (Save)] をクリックします。

vEdge を構成するには、ドロップダウンリストから [Profile] を選択します。

WAN 最適化装置を構成するには、ドロップダウンリストから [Services] と [Profile] を選択します。

ファイアウォールを構成するには、ドロップダウンリストから [Services]、[Profile]、および [Mode] を選択します。

ダイレクトインターネットアクセス (DIA) を有効にするには、[ファイアウォール (Firewall)] を選択し、[DIA] の横のチェック ボックスをオンにします。

カスタムネットワークを構成するには、[+Add Custom Service or network] を選択し、[Networks] を選択します。[ネットワーク名 (Network Name)] にネットワークの名前を入力します。[接続の種類 (Connection Type)] と [ネットワークモード (Network Mode)] を選択します。[VLAN] に VLAN ID を入力し、接続するサービスを選択します。[保存 (Save)] をクリックします。

カスタムサービスを構成するには、[+Add Custom Service or network] を選択し、[Service] を選択します。[Add a Custom Service] ウィンドウで、Linux または Windows Server などのサービス名を入力します。[保存 (Save)] をクリックします。

- [次へ (Next)] をクリックします。

ステップ 4 ENCS デバイスを選択した場合は、[ENCS Integrated Switch Configuration] ページが表示されます。

- [+行の追加 (+Add Row)] をクリックします。ドロップダウンリストから、[Type] を選択し、[VLAN ID/Allowed VLAN] および [Description] を入力します。

- [次へ (Next)] をクリックします。

ステップ 5 [カスタム構成 (Custom Configuration)] ページが表示されます。

カスタム構成はオプションです。この手順をスキップしても、[Network Profiles] ページでいつでも構成を適用できます。

カスタム構成の追加を選択した場合：

- 必要に応じて、[Onboarding Template(s)] または [Day-N Templates] タブを選択します。
- ドロップダウンリストからテンプレートを選択します。テンプレートは、[Device Type] と [Tag Name] でフィルタ処理されます。
- [次へ (Next)] をクリックします。

ステップ 6 [概要 (Summary)] ページが表示されます。

このページには、ルータ設定の概要が表示されます。選択されたデバイスとサービスに基づいて、ハードウェアの推奨事項がこのページで提供されます。

- [保存 (Save)] をクリックします。

ステップ 7 [ネットワークプロファイル (Network Profiles)] ページが表示されます。

[サイトの割り当て (Assign Sites)] をクリックして、ネットワークプロファイルにサイトを割り当てます。詳細については、「[ネットワーク階層のサイトの作成 \(95 ページ\)](#)」を参照してください。

ルーティング用のネットワークプロファイルの作成

このワークフローでは、次を実行する方法を示します。

1. ルータ WAN を設定します。
2. ルータ LAN を設定します。
3. カスタム構成を作成します。
4. プロファイルの概要を表示します。

ステップ 1 [設計 (Design)] > [ネットワークプロファイル (Network Profiles)] を選択します。

ステップ 2 [+Add Profiles] をクリックし、[Routing] を選択します。

ステップ 3 [ルータWAN構成 (Router WAN Configuration)] ウィンドウが表示されます。

- [名前 (Name)] テキスト ボックスにプロファイル名を入力します。
- ドロップダウンリストから、[Service Providers] および [Devices] の数を選択します。プロファイルあたり最大 3 つのサービスプロバイダーと 10 のデバイスがサポートされています。
- ドロップダウンリストから [Service Provider Profile] を選択します。詳細については、「[サービス プロバイダー プロファイルの設定 \(161 ページ\)](#)」を参照してください。
- ドロップダウンリストから [Device Type] を選択します。
- [Device Tag] に一意の文字列を入力して異なるデバイスを識別するか、ドロップダウンリストから既存のタグを選択します。2 つ以上のデバイスが同じタイプの場合は、デバイスタグを使用します。すべてのデバイスが異なるタイプの場合、デバイスタグはオプションです。選択内容は、ネットワークプロファイルに適用される Day-0 および Day-N テンプレートの一致基準の一部として使用されるため、適切なタグを選択してください。
- デバイスごとに 1 つ以上の回線リンクを有効にするには、[O] をクリックし、[Connect] の横のチェックボックスをオンにします。ドロップダウンリストから、[Line Type] を選択します。[OK] をクリックします。

複数のサービスプロバイダーを選択した場合は、プライマリインターフェイスをギガビットイーサネットとして、セカンダリをセルラーとして、または両方のインターフェイスをギガビットイーサネットとして選択できます。また、プライマリインターフェイスをセルラーとして、セカンダリインターフェイスをギガビットイーサネットとして選択することもできます。

(注) Cisco 1100 シリーズ サービス統合型ルータ、Cisco 4200 シリーズ サービス統合型ルータ、Cisco 4300 シリーズ サービス統合型ルータ、および Cisco 4400 シリーズ サービス統合型ルータのみが、セルラーインターフェイスをサポートしています。

- [次へ (Next)] をクリックします。

ステップ 4 [ルータWAN構成 (Router WAN Configuration)] ページが表示されます。

- [L2]、[L3] または [Skip] サービスを選択します。
- [L2] を選択した場合は、ドロップダウンリストから [Type] を選択し、[VLAN ID/Allowed VLAN] および [Description] を入力します。
- [L3] を選択した場合は、ドロップダウンリストから [Protocol Routing] を選択し、[Protocol Qualifier] を入力します。
- [次へ (Next)] をクリックします。

ステップ 5 [カスタム構成 (Custom Configuration)] ページが表示されます。

カスタム構成はオプションです。この手順をスキップしても、[Network Profiles] ページでいつでも構成を適用できます。

カスタム構成の追加を選択した場合：

- 必要に応じて、[Onboarding Template(s)] または [Day-N Templates] タブを選択します。
- ドロップダウンリストからテンプレートを選択します。テンプレートは、[Device Type] と [Tag Name] でフィルタ処理されます。
- [次へ (Next)] をクリックします。

ステップ 6 [概要 (Summary)] ページが表示されます。

このページには、ルータ設定の概要が表示されます。選択されたデバイスとサービスに基づいて、ハードウェアの推奨事項がこのページで提供されます。

- [保存 (Save)] をクリックします。

ステップ 7 [ネットワークプロファイル (Network Profiles)] ページが表示されます。

[サイトの割り当て (Assign Sites)] をクリックして、ネットワークプロファイルにサイトを割り当てます。詳細については、「[ネットワーク階層のサイトの作成 \(95 ページ\)](#)」を参照してください。

スイッチ用のネットワークプロファイルの作成

スイッチングプロファイルには、2つのタイプの設定テンプレートを適用できます：

- オンボーディングテンプレート
- Day N テンプレート

始める前に

デバイスに適用する [Onboarding Configuration] テンプレートを定義します。このようなテンプレートには、ネットワーク上で管理できるようにデバイスをオンボードするための基本的なネットワーク設定コマンドが含まれています。[デバイス設定の変更を自動化するテンプレートの作成 \(167 ページ\)](#) を参照してください。

ステップ 1 [設計 (Design)] > [ネットワークプロファイル (Network Profiles)] を選択します。

ステップ 2 [+Add Profiles] をクリックし、[Switching] を選択します。

ステップ 3 [Switching Configuration] ウィンドウが表示されます。

作成するテンプレートのタイプに応じて、[OnBoarding Template(s)] または [Day-N Template(s)] をクリックします。

- [追加 (Add)] をクリックします。

- [Device Type] ドロップダウンリストから、[Switches and Hubs] を選択します。
- ドロップダウンリストから [Tag Name] を選択します。この手順は任意です。選択したタグがすでにテンプレートに関連付けられている場合は、そのテンプレートのみが [Template] ドロップダウンリストで使用できます。
- ドロップダウンリストから [Device Type] を選択します。
- ドロップダウンリストから [Template] を選択します。すでに作成済みの [Onboarding Configuration] テンプレートを選択できます。

ステップ 4 [保存 (Save)] をクリックします。

スイッチに設定されているプロファイルは、スイッチのプロビジョニング時に適用されます。サイトを有効にするには、サイトにネットワークプロファイルを追加する必要があります。

ワイヤレス用のネットワークプロファイルの作成

ステップ 1 [設計 (Design)] > [ネットワークプロファイル (Network Profiles)] を選択します。

ステップ 2 [+Add Profiles] をクリックし、[Wireless] を選択します。

ワイヤレス ネットワーク プロファイルを割り当てる前に、[Design] > [Network Settings] > [Wireless] タブにワイヤレス SSID が含まれていることを確認します。

ステップ 3 [Add a Network Profile] ウィンドウで、[Profile Name] テキストボックスに有効なプロファイル名を入力します。

ステップ 4 [+ SSIDの追加 (+ Add SSID)] をクリックします。

[Network Settings] > [Wireless] タブの下で作成された SSID が追加されます。

ステップ 5 [SSID] ドロップダウンリストで、[SSID] を選択します。

SSID タイプが表示されます。

ステップ 6 [Yes] または [No] を選択して、SSID がファブリックであるか、非ファブリックであるかを指定します。

ステップ 7 非ファブリック SSID を作成する場合は、[No] を選択して次のパラメータを設定します。

ステップ 8 [Interface Name] ドロップダウンリストから、SSID のインターフェイス名を選択するか、または [+ create a new wireless interface] をクリックして新しいワイヤレスインターフェイスを作成します。

ステップ 9 [Flex Connect Local Switching] チェックボックスをオンにして、WLAN のローカルスイッチングを有効にします。

ローカルスイッチングを有効化すると、この WLAN をアダプタイズするすべての FlexConnect アクセスポイントがデータパケットをローカルにスイッチできます。

ステップ 10 ワイヤレスインターフェイスに関連付けられている VLAN ID は、選択したインターフェイス名に基づいて自動的に入力されます。

VLAN ID を変更する場合は、[Local to VLAN] テキストボックスに VLAN ID の新しい値を入力します。

ステップ 11 [Save] をクリックして、ネットワークプロファイルを追加します。

新しく追加されたネットワーク プロファイルが、[Design] > [Network Profiles] ページに表示されます。

ステップ 12 このプロファイルをサイトに割り当てるには、[Assign Sites] をクリックします。

ステップ 13 [Add Sites To Profile] ウィンドウで、サイトの横にあるチェックボックスをオンにしてこのプロファイルに関連付けます。

親ノードまたは個々のサイトを選択できます。親サイトを選択すると、その親ノードの下にある子もすべて選択されます。チェックボックスをオフにして、サイトの選択を解除できます。

ステップ 14 [Select] をクリックします。

グローバル ネットワーク設定について

ネットワーク全体のデフォルトになるネットワーク設定を作成できます。ネットワーク内の設定を定義可能な主なエリアは次の 2 つです。

- [Global settings] : ここで定義されている設定は、ネットワーク全体、および NTP、Syslog、SNMP トラップ、NetFlow コレクタなどのサーバ、IP アドレスプール、デバイスのログイン情報プロファイルの設定などに影響を与えます。
- [Site settings] : ここで定義されている設定はグローバル設定をオーバーライドします。また、サーバ、IP アドレスプール、デバイスのログイン情報プロファイルの設定を含めることができます。



(注) アクティブなファブリックで使用されているネットワーク設定の変更はサポートされていません。それらのネットワーク設定には、サイト階層、IP プールの名前変更など複数の機能が含まれます。



(注) 一部のネットワーク設定は、デバイスの可制御性機能を使用してデバイスに自動的に設定できます。Cisco DNA Center によるデバイスの設定または更新時に、トランザクションが Cisco DNA Center の監査ログにキャプチャされます。監査ログを使用すると、変更を追跡し、問題をトラブルシューティングするのに役立ちます。デバイスの可制御性と監査ログの詳細については、[the Cisco Digital Network Architecture Center 管理者ガイド](#)を参照してください。

[Design] > [Network Settings] を選択し、[Network]、[Device Credentials]、[IP Address Pools]、[SP Profiles]、または [Wireless] などの適切なタブを選択して、次のグローバルネットワーク設定を定義できます。

- AAA、DHCP、DNS サーバなどのネットワーク サーバ：詳細については、[グローバル ネットワーク サーバの設定（162 ページ）](#)を参照してください。
- CLI、SNMP、HTTP (S) などのデバイス クレデンシャル：詳細については、[グローバル CLI クレデンシャルの設定（150 ページ）](#)、[グローバル SNMPv2c クレデンシャルの設定（151 ページ）](#)、[グローバル SNMPv3 クレデンシャルの設定（152 ページ）](#)、および[グローバル HTTPS クレデンシャルの設定（154 ページ）](#)を参照してください。
- IP アドレス プール：詳細については、[IP アドレス プールを設定する（158 ページ）](#)を参照してください。
- SSID、ワイヤレス インターフェイス、および無線周波数プロファイルなどのワイヤレス 設定：詳細については、[グローバルワイヤレス設定の構成（122 ページ）](#)を参照してください。

デバイス クレデンシャルについて

デバイス クレデンシャルとは、ネットワーク デバイスに設定されている CLI、SNMP、HTTPS クレデンシャルを指します。Cisco DNA Center では、これらのクレデンシャルを使用してネットワーク内のデバイスに関する情報を検出および収集します。Cisco DNA Center では、ほとんどのデバイスが使用するクレデンシャルを指定できるため、ディスカバリ ジョブを実行するたびにクレデンシャルを入力する必要はありません。設定したクレデンシャルは、[ディスカバリ (Discovery)] ツールで使用可能になります。

CLI クレデンシャル

ディスカバリ ジョブを実行するには、Cisco DNA Center でネットワーク デバイスの CLI クレデンシャルを設定する必要があります。

これらのクレデンシャルは、ネットワーク デバイスの CLI にログインするために Cisco DNA Center によって使用されます。Cisco DNA Center は、これらのクレデンシャルを使用して、ネットワーク デバイスに関する情報を検出し、収集します。ディスカバリ プロセスの実行時に、Cisco DNA Center は CLI ユーザ名とパスワードを使用してネットワーク デバイスにログインし、**show** コマンドを実行してデバイスのステータスや設定情報を収集します。また、**clear** コマンドやその他のコマンドを実行して、デバイスの設定に保存されていないアクションを実行することもあります。



(注) Cisco DNA Center の実装では、ユーザ名だけがクリアテキストで提供されます。

SNMPv2c のクレデンシャル

簡易ネットワーク管理プロトコル (SNMP) は、アプリケーション層プロトコルであり、SNMP マネージャと SNMP エージェントとの通信に使用されるメッセージフォーマットを提供しま

す。SNMP は、ネットワーク デバイスをモニタおよび管理するために標準化されたフレームワークと共通言語を提供しています。

SNMPv2c は SNMPv2 に代わるコミュニティ スtring ベースの管理フレームワークです。SNMPv2c では、認証および暗号化が行われません (noAuthNoPriv セキュリティ レベル)。代わりに、クリアテキストで通常提供されるパスワードタイプとして、コミュニティ スtring を使用します。



(注) Cisco DNA Center の実装では、セキュリティの理由から SNMP コミュニティ スtring はクリアテキストで提供されません。

ディスカバリ機能を使用してネットワーク デバイスを検出する前に、SNMPv2c コミュニティ スtring 値を設定する必要があります。設定する SNMPv2c コミュニティ スtring 値は、ネットワーク デバイスで設定された SNMPv2c 値と一致している必要があります。Cisco DNA Center では、最大 5 つの read コミュニティ スtring と 5 つの write コミュニティ スtring を設定できます。

ネットワークで SNMPv2 を使用している場合、最善の結果を実現するには Read Only (RO) コミュニティ スtring 値と Read/Write (RW) コミュニティ スtring 値の両方を指定します。両方を指定できない場合は、RO 値を指定することを推奨します。RO 値を指定しなければ、Cisco DNA Center はデフォルトの RO コミュニティ スtring の *public* を使用してデバイスを検出しようとします。RW 値のみを指定すると、ディスカバリで RW 値が RO 値として使用されます。

SNMPv3 のクレデンシャル

ディスカバリを使用するために設定する SNMPv3 値は、ネットワーク デバイスで設定された SNMPv3 値と一致している必要があります。最大 5 つの SNMPv3 値を設定できます。

SNMPv3 が提供するセキュリティ機能は、次のとおりです。

- メッセージの完全性：パケットが伝送中に改ざんされていないことを保証します。
- 認証：メッセージが有効な送信元からのものかどうかを判別します。
- 暗号化：パケットコンテンツのスクランブルによって、不正な送信元から認識できないようにします。

SNMPv3 では、セキュリティモデルとセキュリティレベルの両方が提供されています。セキュリティ モデルは、ユーザおよびユーザ ロール向けに設定される認証方式です。セキュリティ レベルとは、セキュリティ モデル内で許可されるセキュリティのレベルです。セキュリティ モデルとセキュリティ レベルの組み合わせにより、SNMP パケット処理中に採用されるセキュリティ メカニズムが決まります。

セキュリティ レベルは、SNMP メッセージを開示から保護する必要があるかどうか、およびメッセージを認証するかどうか判断します。セキュリティ モデル内のさまざまなセキュリティ レベルは、次のとおりです。

- noAuthNoPriv : 認証または暗号化を実行しないセキュリティ レベル
- authNoPriv : 認証は実行するが、暗号化を実行しないセキュリティ レベル。
- AuthPriv : 認証と暗号化両方を実行するセキュリティ レベル

次の表に、セキュリティ モデルとセキュリティ レベルの組み合わせを示します。

表 33: *SNMPv3* セキュリティ モデルおよびセキュリティ レベル

レベル	認証	暗号化	結果
noAuthNoPriv	ユーザ名	未対応	ユーザ名の照合を使用して認証します。
AuthNoPriv	次のいずれかを行います。 • HMAC-MD5 • HMAC-SHA	なし	ハッシュメッセージ認証コード - セキュア ハッシュ アルゴリズム (HMAC-SHA) に基づく認証を提供します。
AuthPriv	次のいずれかを行います。 • HMAC-MD5 • HMAC-SHA	次のいずれかを行います。 • CBC-DES • CBC-AES-128	HMAC-MD5 または HMAC-SHA に基づく認証を提供します。 暗号ブロック連鎖 (CBC) DES (DES-56) 標準または CBC モードの AES 暗号化に基づいた認証に加え、データ暗号規格 (DES) の 56 ビット暗号化を提供します。

HTTPS クレデンシャル

HTTPS は、特殊な PKI 証明書ストアに基づく HTTP のセキュアバージョンです。Cisco DNA Center では、シスコ エンタープライズ ネットワーク機能仮想化インフラストラクチャ ソフトウェア (NFVIS) デバイスの検出にのみ HTTPS が使用されます。

グローバル デバイス クレデンシャルについて

「グローバル デバイス クレデンシャル」とは、ネットワーク内のデバイスに関する情報を検出して収集するために Cisco DNA Center で使用される共通の CLI、SNMP、および HTTPS クレデンシャルを指します。Cisco DNA Center は、グローバル クレデンシャルを使用して設定済み デバイス クレデンシャルを共有するネットワーク内のデバイスを認証し、アクセスします。グローバル デバイス クレデンシャルの追加、編集、および削除することができます。また、グローバル サイトまたは特定のサイトに クレデンシャルを関連付けることもできます。

グローバル CLI クレデンシャルの設定

最大 5 つのグローバル CLI クレデンシャルを設定して保存できます。

- ステップ 1** Cisco DNA Center のホームページで、[設計 (Design)] > [ネットワーク設定 (Network Settings)] > [デバイス クレデンシャル (Device Credentials)] の順に選択します。
- ステップ 2** グローバル サイトを選択した状態で、[CLI クレデンシャル (CLI Credentials)] エリアで [追加 (Add)] をクリックします。
- ステップ 3** 次のフィールドに情報を入力します。

表 34: CLI クレデンシャル

フィールド	説明
Name/Description	CLI クレデンシャルを説明する名前または語句。
Username	ネットワーク内のデバイスの CLI にログインするために使用する名前。
Password	ネットワーク内のデバイスの CLI にログインするために使用されるパスワード。 セキュリティ上の理由から、確認のためにパスワードをもう一度入力します。 (注) パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。
Enable Password	CLI で高い権限レベルに移るために使用するパスワード。ネットワーク デバイスが必要な場合にのみ、このパスワードを設定します。 セキュリティ上の理由から、有効なパスワードをもう一度入力します。 (注) パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。

- ステップ 4** [保存 (Save)] をクリックします。

サイトにクレデンシャルを適用するには、左側の階層にあるサイトをクリックし、クレデンシャルの横にあるボタンを選択して、[保存 (Save)] をクリックします。

- ステップ 5** 既存のクレデンシャルを変更する場合は、デバイスで新しいクレデンシャルを今すぐ更新するか、後で更新をスケジュールすることが求められます。
- 新しいクレデンシャルを今すぐ更新するには、[今すぐ実行 (Now)] ラジオボタンをクリックし、[適用 (Apply)] をクリックします。
 - 後で更新をスケジュールするには、[後で実行 (Later)] ラジオボタンをクリックして更新の日時を定義し、[適用 (Apply)] をクリックします。

(注) [タイムゾーン (Time Zone)] チェック ボックスを使用して、サイトのタイムゾーンに従って更新を行うか、特定のタイムゾーンに従って更新を行うかを指示します。

グローバル SNMPv2c クレデンシャルの設定

ネットワーク デバイスをモニタおよび管理するために、グローバル SNMPv2c クレデンシャルを設定できます。

始める前に

ネットワークの SNMP 情報は必須です。

- ステップ 1** Cisco DNA Centerのホームページで、[設計 (Design)] > [ネットワーク設定 (Network Settings)] > [デバイス クレデンシャル (Device Credentials)] の順に選択します。
- ステップ 2** グローバルサイトを選択した状態で、[SNMP クレデンシャル (SNMP Credentials)] エリアで [追加 (Add)] をクリックします。
- ステップ 3** [タイプ (Type)] で、[SNMP v2c] をクリックし、次の情報を入力します。

表 35: SNMPv2c のクレデンシャル

フィールド	説明
Read	<ul style="list-style-type: none"> • Name/Description : 追加する SNMP v2c 設定の名前または説明。 • Read コミュニティ : デバイス上の SNMP 情報を表示するためにのみ使用される read-only コミュニティ ストリング パスワード。 <p>(注) パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。</p>
Write	<ul style="list-style-type: none"> • Name/Description : 追加する SNMP v2c 設定の名前または説明。 • Write コミュニティ : デバイス上の SNMP 情報を変更するために使用される write コミュニティ ストリング。 <p>(注) パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。</p>

- ステップ 4** [保存 (Save)] をクリックします。
- ステップ 5** 既存のクレデンシャルを変更する場合は、デバイスで新しいクレデンシャルを今すぐ更新するか、後で更新をスケジュールすることが求められます。

- 新しいクレデンシャルを今すぐ更新するには、[今すぐ実行 (Now)] ラジオボタンをクリックし、[適用 (Apply)] をクリックします。
- 後で更新をスケジュールするには、[後で実行 (Later)] ラジオ ボタンをクリックして更新の日時を定義し、[適用 (Apply)] をクリックします。

(注) [タイムゾーン (Time Zone)] チェック ボックスを使用して、サイトのタイムゾーンに従って更新を行うか、特定のタイムゾーンに従って更新を行うかを指示します。

グローバル SNMPv3 クレデンシャルの設定

ネットワーク デバイスをモニタおよび管理するために、グローバル SNMPv3 クレデンシャルを設定できます。

始める前に

ネットワークの SNMP 情報は必須です。

ステップ 1 Cisco DNA Center のホームページで、[設計 (Design)] > [ネットワーク設定 (Network Settings)] > [デバイス クレデンシャル (Device Credentials)] の順に選択します。

ステップ 2 グローバルサイトを選択した状態で、[SNMP クレデンシャル (SNMP Credentials)] エリアで [追加 (Add)] をクリックします。

ステップ 3 [タイプ (Type)] で、[SNMP v3] をクリックし、次の情報を入力します。

表 36: SNMPv3 のクレデンシャル

フィールド	説明
Name/Description	追加した SNMPv3 設定の名前または説明。
Username	SNMPv3 設定に関連付けられている名前。
Mode	SNMP メッセージを必要とするセキュリティ レベル。次のいずれかのモードを選択します。 <ul style="list-style-type: none"> • noAuthNoPriv : 認証または暗号化を提供しません。 • AuthNoPriv : 認証は提供しますが、暗号化は提供しません。 • AuthPriv : 認証と暗号化の両方を提供します。
Auth Type	使用する認証タイプ (認証モードとして [AuthPriv] または [AuthNoPriv] を選択した場合に有効になります)。次のいずれかの認証タイプを選択します。 <ul style="list-style-type: none"> • SHA : HMAC-SHA に基づく認証。 • MD5 : HMAC-MD5 に基づく認証。

フィールド	説明
Auth Password	<p>SNMPv3 を使用するデバイスから情報にアクセスする際に使用する SNMPv3 パスワード。これらのパスワード（またはパスフレーズ）は、8 文字以上にする必要があります。</p> <p>(注)</p> <ul style="list-style-type: none"> 一部のシスコ ワイヤレス コントローラでは、パスワード（あるいはパスフレーズ）は少なくとも 12 文字以上である必要があります。ワイヤレス コントローラのパスワードの最小要件を必ず確認してください。パスワードに必要な最低限の文字数が守られないと、デバイスでは Cisco DNA Center による検出、監視、管理が行われなくなります。 パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。
Privacy Type	<p>プライバシー タイプ。（認証モードとして [AuthPriv] を選択すると有効になります）。次のいずれかのプライバシー タイプを選択します。</p> <ul style="list-style-type: none"> DES : CBC DES-56 規格に基づく認証に DES 56-bit (DES-56) 暗号化を追加。 AES128 : 暗号化の CBC モード AES。 None : プライバシー設定なし。
Privacy Password	<p>DES または AES128 暗号化をサポートしているデバイスで交換されるメッセージを暗号化するための秘密鍵を生成するために使用される SNMPv3 プライバシーパスワード。パスワード（またはパスフレーズ）は、8 文字以上にする必要があります。</p> <p>(注)</p> <ul style="list-style-type: none"> 一部のシスコ ワイヤレス コントローラでは、パスワード（あるいはパスフレーズ）は少なくとも 12 文字以上である必要があります。ワイヤレス コントローラのパスワードの最小要件を必ず確認してください。パスワードに必要な最低限の文字数が守られないと、デバイスでは Cisco DNA Center による検出、監視、管理が行われなくなります。 パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。

ステップ 4 [保存 (Save)] をクリックします。

ステップ 5 既存のクレデンシャルを変更する場合は、デバイスで新しいクレデンシャルを今すぐ更新するか、後で更新をスケジュールすることが求められます。

- 新しいクレデンシャルを今すぐ更新するには、[今すぐ実行 (Now)] ラジオ ボタンをクリックし、[適用 (Apply)] をクリックします。
- 後で更新をスケジュールするには、[後で実行 (Later)] ラジオ ボタンをクリックして更新の日時を定義し、[適用 (Apply)] をクリックします。

(注) [タイムゾーン (Time Zone)] チェックボックスを使用して、サイトのタイムゾーンに従って更新を行うか、特定のタイムゾーンに従って更新を行うかを指示します。

グローバル HTTPS クレデンシャルの設定

- ステップ 1** Cisco DNA Center のホームページで、[Design] > [Network Settings] > [Device Credentials] の順に選択します。
- ステップ 2** グローバルサイトを選択した状態で、[HTTPS クレデンシャル (HTTPS Credentials)] エリアで [追加 (Add)] をクリックします。
- ステップ 3** 次の情報を入力します。

表 37: HTTPS クレデンシャル

フィールド	説明
Type	設定している HTTPS クレデンシャルのタイプを指定します。有効なタイプは、[読み取り (Read)] または [書き込み (Write)] です。
Read	<p>最大 5 つの HTTPS 読み取りクレデンシャルを設定できます。</p> <ul style="list-style-type: none"> • Name/Description : 追加している HTTPS ログイン情報の名前または説明。 • Username : HTTPS 接続の認証に使用される名前。 • Password : HTTPS 接続の認証に使用されるパスワード。 • Port : HTTPS トラフィックに使用される TCP/UDP ポートの番号。デフォルトはポート番号 443 (HTTPS の既知のポート) です。 <p>(注) パスワードには、少なくとも1つの小文字、1つの大文字、1つの数字、1つの特殊文字が必要で、<>@',;:!およびスペースは使用できません。セキュリティ上の理由から、確認のためにパスワードをもう一度入力します。パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。</p>

フィールド	説明
Write	<p>最大 5 つの HTTPS 書き込みクレデンシャルを設定できます。</p> <ul style="list-style-type: none"> • Name/Description : 追加している HTTPS ログイン情報の名前または説明。 • Username : HTTPS 接続の認証に使用される名前。 • Password : HTTPS 接続の認証に使用されるパスワード。 • Port : HTTPS トラフィックに使用される TCP/UDP ポートの番号。デフォルトはポート番号 443 (HTTPS の既知のポート) です。 <p>(注) パスワードには、少なくとも1つの小文字、1つの大文字、1つの数字、1つの特殊文字が必要で、<>@',:;!およびスペースは使用できません。セキュリティ上の理由から、確認のためにパスワードをもう一度入力します。パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。</p>

ステップ 4 [保存 (Save)] をクリックします。

ステップ 5 既存のクレデンシャルを変更する場合は、デバイスで新しいクレデンシャルを今すぐ更新するか、後で更新をスケジュールすることが求められます。

- 新しいクレデンシャルを今すぐ更新するには、[今すぐ実行 (Now)] ラジオ ボタンをクリックし、[適用 (Apply)] をクリックします。
- 後で更新をスケジュールするには、[後で実行 (Later)] ラジオ ボタンをクリックして更新の日時を定義し、[適用 (Apply)] をクリックします。

(注) [タイムゾーン (Time Zone)] チェック ボックスを使用して、サイトのタイムゾーンに従って更新を行うか、特定のタイムゾーンに従って更新を行うかを指示します。

グローバルデバイスのログイン情報の編集に関する注意事項

既存のグローバル デバイス クレデンシャルの編集に関する注意事項と制約事項は、次のとおりです。

- Cisco DNA Center グローバル デバイス クレデンシャルを編集、保存、および適用する際は、次のプロセスが使用されます。
 1. Cisco DNA Center クレデンシャルをデバイスにプッシュします。
 2. クレデンシャルがデバイスに正常にプッシュされると、Cisco DNA Center は新しいクレデンシャルを使用してデバイスに到達できることを確認します。



(注) この手順に失敗すると、Cisco DNA Center が新しいクレデンシャルをデバイスにプッシュしていても、インベントリでは古いクレデンシャルを使用してデバイスが管理されます。この場合、既存のクレデンシャルを更新すると、[プロビジョニング (Provision)] > [デバイス (Devices)] > [インベントリ (Inventory)] 画面でデバイスが管理対象外であると示される可能性があります。

3. 新しいクレデンシャルを使用してデバイスに正常に到達すると、Cisco DNA Center のインベントリは、新しいクレデンシャルを使用してデバイスの管理を開始します。
 - サイトには、SNMPv2c クレデンシャルと SNMPv3 クレデンシャルを使用するデバイスを含めることができます。SNMPv2c または SNMPv3 のグローバルクレデンシャルを編集して保存すると、Cisco DNA Center はその変更をデバイスにプッシュし、そのクレデンシャルを有効にします。たとえば、SNMPv2c を使用するデバイスがあるのに、SNMPv3 のグローバルクレデンシャルを編集して保存すると、Cisco DNA Center は関連付けられたサイトのすべてのデバイスに新しいSNMPv3のクレデンシャルをプッシュして、そのクレデンシャルを有効にします。つまり、以前はSNMPv2cが有効になっていたデバイスを含め、すべてのデバイスがSNMPv3を使用して管理されるようになります。
 - 混乱が生じないようにするために、CLI ログイン情報を編集する際は [User Name] を変更してください。これにより、新しいCLIクレデンシャルが作成され、既存のCLIクレデンシャルは変更されません。

グローバル デバイス クレデンシャルの編集

グローバル デバイス クレデンシャルを編集する場合、変更はグローバル サイトの下のサイトに関連付けられているすべてのデバイスに影響します。グローバル デバイス クレデンシャルを編集および保存した後に、Cisco DNA Center は、変更したデバイス クレデンシャルを参照するすべてのサイトを検索し、すべてのデバイスに変更をプッシュします。

新しいグローバル デバイス クレデンシャルを更新または作成できますが、Cisco DNA Center はデバイスからクレデンシャルを削除することはありません。

- ステップ 1 Cisco DNA Center のホームページで、[Design] > [Network Settings] > [Device Credentials] の順に選択します。
- ステップ 2 グローバルサイトを選択した状態で、変更するデバイスログイン情報を選択し、右側の [Actions] 列の下にある [Edit] をクリックします。
- ステップ 3 [EDIT CLI Credentials] ダイアログボックスで、[Save] をクリックします。
- ステップ 4 [Apply CLI Credentials] ダイアログボックスで、[Cancel] をクリックします。
- ステップ 5 [Device Credentials] ページの下部で、[Save] をクリックします。

次のメッセージが表示されます。

```
Created Common Settings successfully.
```

ステップ 6 [Device Credentials] ページに戻り、目的のデバイスのログイン情報の [Edit] をクリックします。

ステップ 7 [Edit CLI Credentials] ダイアログボックスで、変更を加えて、[Save] をクリックします。

ステップ 8 デバイスで新しいクレデンシャルを今すぐ更新するか、後で更新をスケジュールするかを選択します。

- 新しいクレデンシャルを今すぐ更新するには、[今すぐ実行 (Now)] ラジオボタンをクリックし、[適用 (Apply)] をクリックします。
- 後で更新をスケジュールするには、[後で実行 (Later)] ラジオ ボタンをクリックして更新の日時を定義し、[適用 (Apply)] をクリックします。

(注) [タイムゾーン (Time Zone)] チェック ボックスを使用して、サイトのタイムゾーンに従って更新を行うか、特定のタイムゾーンに従って更新を行うかを指示します。

ステータスメッセージに、デバイスログイン情報の変更が成功したか、失敗したかが示されます。

ステップ 9 ログイン情報の変更のステータスを表示するには、Cisco DNA Center のホームページで、[Provision] > [Devices] > [Inventory] の順に選択します。

[クレデンシャル ステータス (Credential Status)] 列に、次のいずれかのステータスが表示されます。

- [Success] : Cisco DNA Center はログイン情報の変更を正常に適用しました。
- [Failed] : Cisco DNA Center はログイン情報の変更を適用できませんでした。失敗したログイン情報の変更とその理由に関する追加情報を表示するには、アイコンの上にカーソルを重ねます。
- [Not Applicable] : ログイン情報はデバイスタイプに適用できません。

複数のクレデンシャル (CLI、SNMP、HTTPS など) を編集して保存した場合、がいずれかのクレデンシャルを適用できなかったときには、[クレデンシャルステータス (Credential Status)] 列に [失敗 (Failed)] と表示されます。Cisco DNA Center 失敗したログイン情報の変更に関する追加情報を表示するには、アイコンの上にカーソルを重ねます。

デバイス クレデンシャルのサイトへの関連付け

グローバルサイトを作成するサイトは、グローバルなデバイスのクレデンシャルを継承できません。または特定サイトの別のデバイスのクレデンシャルを作成することができます。

ステップ 1 Cisco DNA Center のホームページで、[設計 (Design)] > [ネットワーク設定 (Network Settings)] > [デバイス クレデンシャル (Device Credentials)] の順に選択します。

ステップ 2 左側のペインの階層からサイトを選択します。

ステップ 3 選択したサイトに関連付けるクレデンシャルを選択し、次に [保存 (Save)] をクリックします。

デバイスのクレデンシャルとサイトとの関連付けが正常に成功したことを示すメッセージが、画面の下部に表示されます。

ステップ 4 [リセット (Reset)] をクリックして、画面上のエントリをクリアします。

IP アドレス プールを設定する

Cisco DNA Center IPv4 と IPv6 のデュアルスタック IP プールがサポートされています。

IPv4 および IPv6 アドレスプールは手動で設定できます。

Cisco DNA Center を外部 IP アドレス マネージャと通信するように設定することもできます。詳細については、[Cisco Digital Network Architecture Center 管理者ガイド](#)を参照してください。

ステップ 1 Cisco DNA Center のホームページで、[設計 (Design)] > [ネットワーク設定 (Network Settings)] > [IP アドレス プール (IP Address Pools)] の順に選択します。

ステップ 2 [Add] をクリックし、[Add IP Pool] ウィンドウの必須入力フィールドをすべて入力します。

Cisco DNA Center が外部の IP アドレス マネージャと通信するように設定した場合、外部 IP アドレス マネージャの既存の IP アドレス プールと重複する IP プールを作成することはできません。

ステップ 3 [保存 (Save)] をクリックします。

新しく追加されたプールが IP アドレスプールテーブルに表示されます。IPv4 または IPv6 のアドレスプールのみを表示する場合は、[SUBNET TYPE] 領域で [IPv4] または [IPv6] オプションをクリックします。

(注) IP アドレス プールを編集して、DHCP を変更すると、その IP アドレス プールを使用してデバイスを再設定する必要はありません。

IP アドレス マネージャから IP アドレス プールをインポートする

Bluecat または Infoblox から IP アドレス プールをインポートできます。



(注) IP アドレス プールはサブプールを持つことができず、IP アドレス プールから割り当てられた IP アドレスを持つことはできません。

外部 IP アドレス マネージャ (IPAM) と通信するには Cisco DNA Center を設定する必要があります。詳細については、[Cisco Digital Network Architecture Center 管理者ガイド](#)を参照してください。

-
- ステップ 1 Cisco DNA Center のホームページで、**[設計 (Design)]** > **[ネットワーク設定 (Network Settings)]** > **[IP アドレス プール (IP Address Pools)]** の順に選択します。
 - ステップ 2 **[Actions]** ドロップダウンリストから、**[Import from IPAM Server]** を選択し、必須フィールドに値を入力します。
 - ステップ 3 CIDR を入力し、**[取得 (Retrieve)]** をクリックして、インポートできる IP プールのリストを取得します。
 - ステップ 4 **[Select All]** をクリックするか、またはインポートする IP アドレスプールを選択して **[Import]** をクリックします。
-

CSV ファイルから IP アドレスプールをインポートする

CSV ファイルから IP アドレスプールをインポートできます。

-
- ステップ 1 Cisco DNA Center のホームページで、**[設計 (Design)]** > **[ネットワーク設定 (Network Settings)]** > **[IP アドレス プール (IP Address Pools)]** の順に選択します。
 - ステップ 2 **[Actions]** ドロップダウンリストから、**[Import from CSV File]** を選択します。
 - ステップ 3 **[Download Template]** をクリックしてサンプルファイルをダウンロードします。
 - ステップ 4 ファイルに IP アドレスプールを追加して、ファイルを保存します。
 - ステップ 5 次のアクションのいずれかを実行して、CSV ファイルをアップロードします。
 - a) ドラッグアンドドロップエリアにファイルをドラッグアンドドロップします。
 - b) **[クリックして選択 (click to select)]** が表示される場所をクリックしてファイルを選択します。
 - ステップ 6 **[Import]** をクリックします。
-

IP プールの予約

始める前に

1 つまたは複数の IP アドレスプールが作成されていることを確認します。

-
- ステップ 1 Cisco DNA Center のホームページで、**[設計 (Design)]** > **[ネットワーク設定 (Network Settings)]** > **[IP アドレス プール (IP Address Pools)]** の順に選択します。
 - ステップ 2 **[hierarchy]** ペインを展開し、サイトを選択します。
 - ステップ 3 **[Reserve]** をクリックして以下のフィールドに入力し、使用可能なグローバル IP アドレスプールのすべてまたは一部を特定のサイト用に予約します。

- **[IP Address Pool Name]** : 予約済み IP アドレスプールの一意の名前。

- [タイプ (Type)] : IP アドレス プールのタイプ。LAN 自動化のバイアは、**LAN** を選択します。次のオプションがあります。
 - [LAN] : 該当する VNF とアンダーレイの LAN インターフェイスに IP アドレスを割り当てます。
 - [Management] : IP アドレスを管理インターフェイスに割り当てます。管理ネットワークは、VNF 管理用に VNF に接続される専用ネットワークです。
 - [Service] : IP アドレスをサービスインターフェイスに割り当てます。サービスネットワークは、VNF 内の通信に使用されます。
 - [WAN] : UCS-E プロビジョニングの場合は NFVIS に IP アドレスを割り当てます。
 - [Generic] : 他のすべてのネットワークタイプで使用されます。
- [IP Address Space] : すべてまたは一部の IP アドレスを予約する IPv4 および IPv6 アドレスプール。
- [CIDR Prefix/No. of IP Addresses] : グローバル IP アドレスプールのすべてまたは一部を予約するために使用する IP サブネットとマスクアドレス、または予約する IP アドレスの数。IPv6 IP プールの [CIDR Prefix] として \64 を選択すると、[SLAAC] オプションがオンになります。 ([SLAAC] が選択されている場合、デバイスは DHCP サーバを必要とせずに、自動的に IP アドレスを獲得します)。
- [Gateway] : ゲートウェイ IP アドレス。
- [DHCP Servers] : DHCP サーバの IP アドレス。
- [DNS Servers] : DNS サーバのアドレス。

ステップ 4 [予約 (Reserve)] をクリックします。

IPv4 と IPv6 の両方のアドレスプールを予約している場合（ファブリックがデュアルスタック IP プールでプロビジョニングされている場合）で、IPv6 プールがすでに VN に接続されているときは、シングルスタック IP プールに戻すことはできません。

ただし、IPv6 プールが VN に接続されていない場合は、デュアルスタック IPv6 プールからシングルスタック IPv4 プールにダウングレードできます。シングルスタックにダウングレードするには、[IP Address Pools] ウィンドウで、デュアルスタック IP プールの [Edit] をクリックします。[Edit IP Pool] ウィンドウで、[IPv6] チェックボックスをオフにして、[Save] をクリックします。

IP プールの編集

ステップ 1 Cisco DNA Center のホームページで、[設計 (Design)] > [ネットワーク設定 (Network Settings)] > [IP アドレス プール (IP Address Pools)] の順に選択します。

ステップ 2 階層ツリーを展開し、サイトを選択します。

ステップ 3 目的の IP プールを見つけ、[Actions] エリアで [Edit] をクリックします。

ステップ4 [Edit IP Pool] ウィンドウで、必要な変更を行い、[Save] をクリックします。

IP プールの複製

サイトレベルで既存の IP プールを複製できます。IP プールを複製すると、DHCP サーバと DNS サーバの IP アドレスが自動的に入力されます。

ステップ1 Cisco DNA Center のホームページで、[Design] > [Network Settings] > [IP Address Pools] の順にクリックします。

ステップ2 階層ツリーを展開し、サイトを選択します。

ステップ3 目的の IP プールを見つけ、[Actions] 領域で [Clone] をクリックします。

ステップ4 [Clone IP Pool] ウィンドウで、次の手順を実行します。

- 必要に応じて、プール名を編集します（タイプ、IP アドレス空間、またはグローバルプール値は、複製元のプールから継承されるため編集できません）。
- 必要に応じて、CIRD プレフィックス値を編集します。
- [Clone] をクリックします。

IP プールのリリース

サイトレベルで予約されているシングルスタックおよびデュアルスタックプールをリリースできます。

ステップ1 Cisco DNA Center のホームページで、[設計 (Design)] > [ネットワーク設定 (Network Settings)] > [IP アドレス プール (IP Address Pools)] の順に選択します。

ステップ2 階層ツリーを展開し、サイトを選択します。

ステップ3 目的の IP プールを見つけ、[Actions] エリアで [Release] をクリックします。

ステップ4 プロンプトで [Release] をクリックします。

サービス プロバイダー プロファイルの設定

特定の WAN プロバイダーのサービスクラスを定義するサービスプロバイダー (SP) プロファイルを作成することができます。サービスモデルには、4クラス、5クラス、6クラス、および8クラスを定義できます。SP プロファイルの作成後、アプリケーションポリシーの範囲内 (必

要に応じてインターフェイスのサブラインレート設定を含む) のアプリケーションポリシーと WAN インターフェイスにそのプロファイルを割り当てることができます。

-
- ステップ 1** Cisco DNA Center のホームページから、**[Design] > [Network Settings] > [SP Profiles]** を選択します。
- ステップ 2** **[Qos]** 領域で、**[追加 (Add)]** をクリックします。
- ステップ 3** **[プロファイル名 (Profile Name)]** フィールドに、SP プロファイルの名前を入力します。
- ステップ 4** **[WAN Provider]** ドロップダウンリストから、新しいサービスプロバイダーを入力するか、既存のプロバイダーを選択します。
- ステップ 5** **[Model]** ドロップダウンリストから、クラスモデル (**[4 class]**、**[5 class]**、**[6 class]**、および **[8 class]**) のいずれかを選択します。
- これらのクラスの詳細については、[サービスプロバイダーのプロファイル \(214 ページ\)](#) を参照してください。
-

グローバル ネットワーク サーバの設定

ネットワーク全体のデフォルトになるグローバル ネットワーク サーバを定義することができます。



-
- (注) サイト固有の設定を定義することで、サイトのグローバル ネットワーク設定を上書きできます。
-

- ステップ 1** Cisco DNA Center のホームページで、**[Design] > [Network Settings] > [Network]** の順に選択します。
- ステップ 2** **[DHCP サーバ (DHCP Server)]** フィールドに、DHCP サーバの IP アドレスを入力します。
- (注) プラスアイコンをクリックすると、IPv4 アドレスと IPv6 アドレスの両方を入力できます。
- IP アドレスプールを作成するには、少なくとも 1 つの DHCP サーバを定義する必要があります。
- ステップ 3** **[DNS サーバ (DNS Server)]** フィールドに、DNS サーバのドメイン名を入力します。
- (注) プラスアイコンをクリックすると、IPv4 アドレスと IPv6 アドレスの両方を入力できます。
- IP アドレスプールを作成するために、少なくとも 1 つの DNS サーバを定義する必要があります。
- ステップ 4** (任意) Syslog、SNMP トラップ、および NetFlow コレクタ サーバ情報を入力できます。**[サーバの追加 (Add Servers)]** をクリックして NTP サーバを追加します。
- (注) ファブリック コンプライアンス チェックをトリガするには、Cisco DNA Center の IP アドレスを使用して SNMP サーバを設定します。詳細については、[ファブリックへのデバイスの追加](#)を参照してください。

ステップ 5 [保存 (Save)] をクリックします。

Cisco ISE またはその他の AAA サーバの追加

Cisco Identity Services Engine (ISE) サーバまたはその他の同様の AAA サーバを、ネットワーク、クライアント、およびエンドポイント認証のためにサイトまたはグローバルレベルで定義することができます。ネットワーク認証では、RADIUS および TACACS プロトコルがサポートされています。クライアントとエンドポイント認証では、RADIUS のみがサポートされます。Cisco DNA Center ごとに 1 つの ISE のみがサポートされます。

マルチ ISE 設定をサポートするために、RADIUS または TACACS サーバグループの下に送信元インターフェイスを設定できます。各 ISE クラスタには独自のサーバグループがあります。RADIUS サーバと TACACS サーバに使用される送信元インターフェイスは、次のように決定されます。

- デバイスに Loopback0 インターフェイスが設定されている場合、Loopback0 は送信元インターフェイスとして設定されます。
- それ以外の場合は、Cisco DNA Center を管理 IP として使用するインターフェイスが送信元インターフェイスとして設定されます。

あるサイトに Cisco ISE サーバを設定すると、サイトに割り当てられているデバイスは、対応する Cisco ISE サーバで自動的に更新されます。その後、Cisco ISE でこれらのデバイスに変更が行われると、Cisco DNA Center に自動的に送信されます。

- ステップ 1 Cisco DNA Center のホームページで、[設計 (Design)] > [ネットワーク設定 (Network Settings)] > [ネットワーク (Network)] の順に選択します。
- ステップ 2 [サーバの追加 (Add Servers)] をクリックして AAA サーバを追加します。
- ステップ 3 [サーバの追加 (Add Servers)] ウィンドウで、[AAA] チェックボックスをオンにし、[OK] をクリックします。
- ステップ 4 AAA サーバをネットワークユーザ、クライアント/エンドポイントユーザ、またはその両方に設定します。
- ステップ 5 [Network] または [Client/Endpoint] チェックボックスをオンにし、AAA サーバのサーバとプロトコルを設定します。
- ステップ 6 認証と認可のための [Servers] を選択します ([ISE] または [AAA]) 。
- [ISE] を選択した場合は、次のように設定します。
 - [Network] ドロップダウンリストから、ISE サーバの IP アドレスを選択します。[Network] ドロップダウンリストには、Cisco DNA Center のホームページの [System Settings] に登録されている Cisco ISE サーバのすべての IP アドレスが含まれています。ISE の IP を選択すると、選択した ISE のポリシーサービスノード (PSN) の IP アドレスを持つプライマリおよび追加 IP アドレスのドロップダウンリストが表示されます。AAA サーバの IP アドレスを入力することも、[IP Address (Primary)] と [IP Address (Additional)] ドロップダウンリストから PSN IP アドレスを選択することもできます。

- [Protocol] を選択します ([RADIUS] または [TACACS]) 。

(注) 特定の WLC の物理サイトと管理サイトの AAA 設定が一致する必要があります。一致しない場合、プロビジョニングは失敗します。

- [AAA] を選択した場合は、次のように設定します。
 - AAA サーバの IP アドレスを入力することも、[IP Address (Primary)] および [IP Address (Additional)] ドロップダウンリストから IP アドレスを選択することもできます。これらのドロップダウンリストには、[System Settings] で登録されている ISE 以外の AAA サーバが含まれています。

ステップ 7 [保存 (Save)] をクリックします。



第 8 章

デバイスの診断コマンドを実行

- [コマンドランナーについて \(165 ページ\)](#)
- [デバイスの診断コマンドを実行 \(165 ページ\)](#)

コマンドランナーについて

コマンドランナーツールでは、選択したデバイスに診断 CLI コマンドを送信できます。現在、**show** とその他の読み取り専用コマンドが許可されています。

デバイスの診断コマンドを実行

コマンドランナーを使用すると、選択したデバイスで診断 CLI コマンドを実行し、結果のコマンド出力を表示できます。

始める前に

コマンドランナーの使用を開始する前に、次の手順を実行します。

1. まず、コマンドランナー アプリケーションをインストールします。Cisco DNA Center のホームページで、歯車のアイコン (⚙️) をクリックし、[System Settings]>[Software Updates]>[Installed Apps] を選択します。[Command Runner] アプリケーションを検索し、[Install] をクリックします。
2. インストール後、ディスカバリ ジョブを実行し、デバイスに Cisco DNA Center を入力します。これらデバイスの一覧が表示され、ここから診断 CLI コマンドを実行します。

ステップ 1 Cisco DNA Center ホームページで、[ツール (Tools)]の[コマンドランナー (Command Runner)]をクリックします。

[コマンドランナー (Command Runner)]ウィンドウが表示されます。

ステップ 2 [Search] フィールドで、ドロップダウン矢印をクリックして、[Device IP] または [Device Name] で検索します。

ステップ3 診断 CLI コマンドを実行するデバイス（複数可）を選択します。

選択した [デバイス一覧 (Device List)] が表示されます。

ステップ4 (オプション) 一覧に追加する別のデバイスを選択します。到達可能なデバイスを 20 台まで選択できません。

(注) デバイス一覧にはインベントリで利用可能なデバイスがすべて表示されますが、コマンドランナーはワイヤレス アクセス ポイント デバイスおよび Cisco Meraki デバイスではサポートされていません。アクセス ポイント デバイスまたは Cisco Meraki デバイスを選択すると、コマンドが実行されないという警告メッセージが表示されます。

ステップ5 [Select/Enter commands] フィールドに CLI コマンドを入力し、[Add] をクリックします。

コマンドランナーでは、先行入力がサポートされています。入力を開始すると、選択可能なコマンドがコマンドランナーによって表示されます。新しい有効なコマンドを入力することもできます。

ステップ6 [コマンドの実行 (Run Command(s))] をクリックします。

成功すると、「コマンドは正常に実行されました」というメッセージが表示されます。

ステップ7 コマンド出力を表示するには、デバイスの下に表示されているコマンドをクリックします。

[Command Runner] ウィンドウにすべてのコマンド出力が表示されます。

ステップ8 [Export CLI Output] をクリックすると、コマンド出力をテキストファイルにエクスポートしてローカルに保存できます。

ステップ9 [Go Back] をクリックすると前のウィンドウに戻ります。

(注) 必要に応じて、デバイス名の横にある [x] をクリックすると、デバイス一覧からデバイスが削除されます。同様に、コマンドの横にある [x] をクリックすると、コマンド一覧からコマンドが削除されます。



第 9 章

デバイス設定の変更を自動化するテンプレートの作成

- [テンプレートエディタについて \(167 ページ\)](#)
- [プロジェクトの作成 \(167 ページ\)](#)
- [テンプレートの作成 \(168 ページ\)](#)
- [テンプレートフォームエディタ \(174 ページ\)](#)
- [ネットワークプロファイルへのテンプレートの関連付け \(178 ページ\)](#)


テンプレートエディタについて

Cisco DNA Center Cisco DNA Center には、CLI テンプレートを作成するためのテンプレートエディタと呼ばれるインタラクティブなエディタがあります。テンプレートエディタは一元化された CLI 管理ツールで、ブランチにデバイスを構築するために必要な一連のデバイス設定の設計に役立ちます。一連の同様のデバイスや設定を使用するサイト、オフィス、またはブランチがある場合、テンプレートエディタを使用して汎用設定を作成し、ブランチ内の 1 台以上のデバイスに適用できます。テンプレートエディタを使用すると、次のことができます。

- テンプレートを作成、編集、および削除します。
- インタラクティブ コマンドの追加
- テンプレート内のエラーの検証
- 追跡のためのテンプレートのバージョン管理
- テンプレートのシミュレーション

プロジェクトの作成





プロジェクトは、一連のテンプレートに対する論理的なグルーピングです。

- ステップ1 Cisco DNA Center ホームページで、[ツール (Tools)] > [テンプレート エディタ (Template Editor)] を選択します。
- ステップ2 左側のペインで、 > [プロジェクトの作成 (Create Project)] の順にクリックします。
- ステップ3 [Add New Project] ウィンドウで、プロジェクトの名前、説明、およびタグを入力します。
- ステップ4 [Add] をクリックします。
- 左側のペインに作成したプロジェクトが表示されます。

テンプレートの作成

Cisco DNA Center Cisco DNA Center は、通常の設定テンプレートと複合設定テンプレートを提供します。CLI テンプレートを使用すると、設定の要素を選択できます。Cisco DNA Center には、実際の値や論理ステートメントと置き換えることができる変数が用意されています。

標準テンプレートの作成

- ステップ1 Cisco DNA Center ホームページで、[ツール (Tools)] > [テンプレート エディタ (Template Editor)] を選択します。デフォルトでは、[Onboarding Configuration] プロジェクトは、day-0 テンプレートの作成に使用できます。独自のカスタムプロジェクトを作成できます。カスタムプロジェクトで作成されたテンプレートは、day-N テンプレートとして分類されます。
- ステップ2 ツリーペインで、テンプレートを作成しているプロジェクトを選択し、歯車アイコンをクリックして [Add Templates]  > を選択します。または、[Add Templates]  > をクリックします。
- (注) day 0 用に作成したテンプレートは、day N にも適用できます。
- ステップ3 [Add New Template] ウィンドウで、[Regular Template] をクリックします。
- ステップ4 [名前 (Name)] テキストボックスに、テンプレートの一意の名前を入力します。
- ステップ5 [Project Name] ドロップダウンリストで、プロジェクトを選択します。
- [Add Templates] パスから移動してきた場合、ドロップダウンリストが有効になっています。  > プロジェクトを選択し、歯車アイコンをクリックしてからツリーペインの [Add Templates] を選択した場合、ドロップダウンリストは無効になります。  >
- ステップ6 [説明(Description)] テキストボックスに、テンプレートの説明を入力します。
- ステップ7 [Tags] テキストボックスに、テンプレートにタグ付けするわかりやすい名前を入力します。設定テンプレートにタグ付けすることで、次のことが可能になります。
- 検索フィールドでタグ名を使用したテンプレートの検索
 - 追加のデバイスを設定するための、参照としてのタグ付けされたテンプレートの使用

(注) タグを使用してテンプレートをフィルタ処理する場合は、テンプレートを適用するデバイスに同じタグを適用する必要があります。適用しないと、プロビジョニング中に次のエラーが表示されます。「デバイスを選択できません。テンプレートとの互換性がありません (Cannot select the device. Not compatible with template.)」。

ステップ 8 [Edit] をクリックして選択したデバイスタイプを表示し、テンプレートに適用するデバイスタイプを選択します。

選択したデバイスを表示するには、[Show] ドロップダウンリストから [Selected] を選択します。デフォルトでは、すべてのデバイスタイプが表示されます。

階層構造から選択するデバイスタイプには、さまざまな細かいレベルがあります。展開時にデバイスタイプを使用して、指定したデバイスタイプの条件に一致するデバイスをテンプレートが確実に展開できるようにします。これにより、特定のデバイスモデルに対して専用のテンプレートを作成できます。

テンプレートエディタには、デバイスの製品 ID (PID) は表示されません。代わりに、デバイスのシリーズとモデルの説明が表示されます。Cisco.com を使用すると、PID に基づいたデバイスデータシートの検索、デバイスシリーズとモデルの説明の検索、適切なデバイスタイプの選択を実行できます。

ステップ 9 デバイスタイプを選択したら、[Back to Add New Template] をクリックします。

ステップ 10 [Software Type] ドロップダウンリストから、ソフトウェアタイプとして、[IOS]、[IOS XE]、[IOS XR]、[NX-OS]、[Cisco Controller]、[Wide Area Application Services]、[Adaptive Security Appliance]、[NFV-OS]、[Others] を選択します。

シスコワイヤレスコントローラサポート対象ソフトウェアバージョンおよびサポート対象最小バージョンの詳細については、[Cisco DNA Center サポート対象デバイス \[英語\]](#) を参照してください。

たとえば、ソフトウェアタイプに IOS を選択すると、IOS XE や IOS XR など、すべてのソフトウェアタイプにコマンドを適用できます。この値は、プロビジョニング時に、選択したデバイスがテンプレートの選択に準拠しているかどうかを確認するために使用されます。

ステップ 11 [Software Version] テキストボックスに、ソフトウェアのバージョンを入力します。プロビジョニングの間、Cisco DNA Center は、選択したデバイスにテンプレートに記載されているのと同じソフトウェアバージョンがあるか確認します。不一致がある場合、プロビジョニングはテンプレートをスキップします。

ステップ 12 [Add] をクリックします。テンプレートが作成され、選択したプロジェクトの下のツリービューに表示されます。

ステップ 13 左側のメニューで作成したテンプレートを選択して、テンプレートの内容を編集することができます。テンプレートの内容を編集するには、[テンプレートの編集 \(172 ページ\)](#) を参照してください。

ステップ 14 [Template Editor] ウィンドウに、テンプレートの内容を入力します。Velocity Template Language (VTL) を使用して、テンプレートの内容を書き込むことができます。VTL の使用に関する詳細については、<http://velocity.apache.org/engine/devel/vtl-reference.html> を参照してください。

テンプレートを保存後、Cisco DNA Center がテンプレート内のすべてのエラーをチェックします。Velocity 構文エラーがある場合、テンプレートの内容は保存されず、テンプレートで定義されているすべての入力変数が保存プロセス中に自動的に識別されます。ローカル変数 (**for** ループ内で使用され、セットを通じて割り当てられる変数など) は無視されます。

ステップ 15 テンプレートを検証するには、[アクション (Actions)] ドロップダウンリストから [エラーのチェック] を選択します。

ブラックリストに登録されたコマンド

Cisco DNA Center Cisco DNA Center は、次のエラーをチェックし、報告します。

- Velocity 構文エラー。
- ブラックリストコマンドと競合しています。 [ブラックリストに登録されたコマンド \(170 ページ\)](#) を参照してください。

ステップ 16 テンプレートの内容を保存するには、[アクション (Actions)] ドロップダウンリストから、[保存 (Save)] を選択します。

ステップ 17 テンプレートをコミットするには、[アクション (Actions)] ドロップダウンリストから、[コミット (Commit)] を選択します。ネットワーク プロファイルセクションでコミットされたテンプレートのみを表示できます。

(注) ネットワーク プロファイルにコミットされたテンプレートのみを関連付けることができます。

次のタスク

1. テンプレートに変数の追加情報を入力します。詳細については、「[テンプレートフォームエディタ \(174 ページ\)](#)」を参照してください。
2. テンプレートを編集します。詳細については、「[テンプレートの編集 \(172 ページ\)](#)」を参照してください。
3. プロファイルにテンプレートを割り当てます。詳細については、「[ネットワークプロファイルへのテンプレートの関連付け \(178 ページ\)](#)」を参照してください。

ブラックリストに登録されたコマンド

ブラックリストコマンドは、ブラックリストカテゴリに追加されているコマンドです。これらのコマンドは、Cisco DNA Center アプリケーションを介してのみ使用できます。テンプレートでブラックリストコマンドを使用すると、テンプレートに警告が表示されます。この場合、一部の Cisco DNA Center プロビジョニングアプリケーションと競合している可能性があります。

このリリースには、次のブラックリストコマンドがあります。

- ルータ LISP : Cisco Catalyst 3K、Catalyst 4K、Catalyst 6K、および Catalyst K デバイス用。
- [Hostname] : Cisco サービス統合型仮想ルータ (ISRv) および Cisco 適応型セキュリティ仮想アライアンス (ASAv) の場合。

サンプル テンプレート

ホスト名を設定します

```
hostname $name
```

インターフェイスの設定

```
interface $interfaceName
description $description
```

シスコワイヤレスコントローラでの NTP の設定

```
config time ntp interval $interval
```

複合テンプレートの作成

2つ以上の標準テンプレートは、連続した複合テンプレートにまとめられます。一連のテンプレートに対し、デバイスに集合的に適用される連続的な複合テンプレートを作成できます。たとえば、ブランチを展開するときに、ブランチルータの最小設定を指定する必要があります。作成したすべてのテンプレートは、単一の複合テンプレートに追加できます。これは、ブランチルータに必要なすべての個々のテンプレートを集約したものです。複合テンプレートに含まれるテンプレートが、デバイスに展開される順序を指定してください。



(注) 複合テンプレートには、コミットされたテンプレートのみを追加できます。

- ステップ 1 Cisco DNA Center ホームページで、[ツール (Tools)] > [テンプレート エディタ (Template Editor)] を選択します。
- ステップ 2 左側のペインで、テンプレートを作成するプロジェクトを選択します。[Add Templates] を選択するか、[Add Templates] をクリックします。* > + >
- ステップ 3 [Add New Template] ウィンドウで、[Composite Template] オプションボタンをクリックし、連続した複合テンプレートを作成します。
- ステップ 4 [名前 (Name)] テキストボックスに、テンプレートの一意の名前を入力します。
- ステップ 5 [プロジェクト名 (Project Name)] テキストボックスに、プロジェクトの一意の名前を入力します。
[テンプレートの追加 (Add Templates)] + > パスから移動してきた場合、テキストボックスは有効です。ツリーペインでプロジェクトを選択し、[Add Templates] を選択した場合、テキストボックスは無効です。* >
- ステップ 6 [説明(Description)] テキストボックスに、テンプレートの説明を入力します。
- ステップ 7 [Tags] テキストボックスに、テンプレートにタグ付けするわかりやすい名前を入力します。設定テンプレートにタグ付けすることで、次のことが可能になります。

- 検索フィールドでタグ名を使用したテンプレートの検索
- 追加のデバイスを設定するための、参照としてのタグ付けされたテンプレートの使用

(注) タグを使用してテンプレートをフィルタ処理する場合は、テンプレートを適用するデバイスに同じタグを適用する必要があります。適用しないと、プロビジョニング中に次のエラーが表示されます。「デバイスを選択できません。テンプレートとの互換性がありません (Cannot select the device. Not compatible with template.)」。

- ステップ 8** [Edit] をクリックして選択したデバイスタイプを表示し、テンプレートに適用するデバイスタイプを選択します。
- 選択したデバイスを表示するには、[Show] ドロップダウンリストから [Selected] を選択します。デフォルトでは、すべてのデバイスタイプが表示されます。
- ステップ 9** [Back to Add New Template] をクリックします。
- ステップ 10** [ソフトウェアのタイプ (Software Type)] ドロップダウンリストから、ソフトウェアのタイプを選択します。ソフトウェアタイプに固有のコマンドがある場合は、特定のソフトウェアタイプ (IOS XE や IOS XR など) を選択できます。ソフトウェアタイプに IOS を選択すると、IOS XE や IOS XR など、すべてのソフトウェアタイプにコマンドを適用できます。この値は、プロビジョニング時に、選択したデバイスがテンプレートの選択に準拠しているかどうかを確認するために使用されます。
- ステップ 11** [Software Version] テキストボックスに、ソフトウェアのバージョンを入力します。プロビジョニングの間、Cisco DNA Center は、選択したデバイスにテンプレートに記載されていると同様のソフトウェアバージョンがあるか確認します。不一致がある場合、プロビジョニングはテンプレートをスキップします。
- ステップ 12** [Add] をクリックします。複合テンプレートが作成され、選択したプロジェクトの下の左側のメニューに表示されます。
- ステップ 13** ツリー ビュー ペインで作成した複合テンプレートをクリックします。
- ステップ 14** [Template Editor] ウィンドウで、ツリービューペインからテンプレートをドラッグアンドドロップして、順序を作成できます。テンプレートは順序付けされた順序に基づいて導入されます。[テンプレート エディタ (Template Editor)] ウィンドウでテンプレートの順序を変更できます。
- (注) デフォルトでは、[View] フィルタで [Applicable] オプションが選択され、複合テンプレートに追加できる適用可能なテンプレートのみが [Template Editor] ウィンドウに表示されます。[View] フィルタで [All] オプションを選択すると、[Template Editor] ウィンドウにすべてのテンプレートを表示できます。[All] オプションビューでは、選択したデバイスタイプとソフトウェアバージョンに一致するテンプレートがプラスアイコンでマークされます。
- 複合テンプレートと同じデバイスタイプ、ソフトウェアタイプ、およびソフトウェアバージョンを持つテンプレートをドラッグアンドドロップできます。
- ステップ 15** 最初のテンプレートの障害発生時に導入プロセスを中止するには、[Template Editor] ウィンドウで最初のテンプレートを選択し、[Abort sequence on targets if deployment fails] チェックボックスをオンにします。
- ステップ 16** [アクション (Actions)] ドロップダウンリストで、[コミット (Commit)] を選択してテンプレートのコンテンツをコミットします。

テンプレートの編集

テンプレートを作成したら、テンプレートを編集してコンテンツを含めることができます。

- ステップ 1** Cisco DNA Center ホームページで、[ツール (Tools)] > [テンプレート エディタ (Template Editor)] を選択します。
- ステップ 2** 左側のツリー ペインで、編集するテンプレートを選択します。

右側ペインに [テンプレート エディタ (Template Editor)] ウィンドウが表示されます。

ステップ 3 [テンプレート エディタ (Template Editor)] ウィンドウで、テンプレートのコンテンツを入力します。単一行設定または複数選択設定を含むテンプレートを使用できます。

(注) 速度テンプレートフレームワークでは、数値で始まる変数の使用が制限されます。したがって、変数名が数値ではなく文字で開始することを確認する必要があります。

ステップ 4 テンプレートを検証するには、[アクション (Actions)] ドロップダウンリストで [エラーのチェック (Check for errors)] を選択します。

Cisco DNA Center 次のエラーをチェックし、報告します。

- Velocity 構文エラー
- ブラック リストに登録されたコマンドと競合しています

ステップ 5 [アクション (Actions)] アクション ドロップダウンリスト、[保存 (Save)] を選択してテンプレートのコンテンツを保存します。

ステップ 6 [アクション (Actions)] ドロップダウンリストで、[コミット (Commit)] を選択してテンプレートのコンテンツをコミットします。

次のタスク

1. テンプレートをプロファイルに割り当て、テンプレートをプロビジョニングします。「[ネットワークプロファイルへのテンプレートの関連付け \(178ページ\)](#)」を参照してください。

テンプレートのシミュレーション

インタラクティブ テンプレート シミュレーションを使用すると、変数をデバイスに送信する前に、変数にテストデータを指定することで、テンプレートの CLI 生成をシミュレーションできます。テストシミュレーションの結果を保存し、必要に応じてそれらを後で使用できます。

ステップ 1 [Tools] > [Template Editor] を選択します。

ステップ 2 左側のメニューから、編集するテンプレートを選択します。

右側ペインに [テンプレート エディタ (Template Editor)] ウィンドウが表示されます。

ステップ 3 右上隅にある [Simulator] アイコンをクリックし、コマンドのシミュレーションを実行します。

- [アクション (Actions)] ドロップダウンリストから、[新規シミュレーション (New Simulation)] を選択します。[New Simulation] ウィンドウで、シミュレーションの名前を入力し、[Submit] をクリックします。
- [シミュレーション入力 (Simulation Input)] フォームの必須フィールドを入力し、[実行 (Run)] をクリックします。結果は、[テンプレートプレビュー (Template Preview)] ウィンドウに表示されます。

テンプレートフォームエディタ

- ステップ 1** 左側のツリーペインでテンプレートを選択します。[テンプレート (Template)] ウィンドウが表示されます。
- ステップ 2** [Form Editor] アイコンをクリックして、テンプレート変数にメタデータを追加します。テンプレートで識別されたすべての変数が表示されます。以下のメタデータを設定できます。
- これがプロビジョニング中に必要な変数の場合、[必須 (Required)] チェックボックスにチェックを付けます。デフォルトでは、すべての変数に [必須 (Required)] マークが付いています。これはつまり、プロビジョニング時にこの変数の値を入力する必要があることを意味します。パラメータに [Required] マークがなく、このパラメータに何も値を渡さない場合は、実行時に空の文字列に置換されます。変数の不足は、コマンドの失敗につながります。また、構文上正しくない可能性があります。[Required] マークが付いていない変数に基づいてコマンド全体をオプションにしたい場合は、テンプレートで **if-else** ブロックを使用します。
 - 文字列を変数として考慮しない場合は、変数を選択し、[Not a Variable] チェックボックスをオンにします。
 - [フィールド名 (FieldName)] テキストボックスに、フィールド名を入力します。これは、プロビジョニング中に各変数の UI ウィジェットに使用されるラベルです。
 - [ツールチップ (Tooltip)] テキストボックスに、各変数に表示されるツールチップのテキストを入力します。
 - [デフォルト値 (Default Value)] テキストボックスに、デフォルト値を入力します。この値は、プロビジョニング中にデフォルト値として表示されます。
 - [説明文 (Instructional Text)] テキストボックスに、任意の説明文を入力します。説明文は UI ウィジェット内に表示されます (たとえば、「ここにホスト名を入力してください」など)。ユーザがテキストを入力するためにウィジェットをクリックすると、ウィジェット内のテキストは消去されます。
 - [データタイプ (Data Type)] ドロップダウンリストから、データタイプ: [文字列 (String)]、[整数 (Integer)]、[IP アドレス (IP Address)]、または [MAC アドレス (Mac Address)] を選択します。
 - [表示タイプ (Display Type)] ドロップダウンリストから、プロビジョニング時に作成する UI ウィジェットのタイプ: [テキストフィールド (Text Field)]、[単一選択 (Single Select)]、または [複数選択 (Multi Select)] を選択します。
 - [最大文字数 (Maximum Characters)] テキストボックスに、入力できる最大文字数を入力します。これは文字列データタイプの場合にのみ適用可能です。
- ステップ 3** メタデータ情報を設定したら、[Actions] ドロップダウンリストから [Save] を選択します。
- ステップ 4** テンプレートを保存したら、バージョンを付ける必要があります。テンプレートは、変更を加えるたびにバージョンを付ける必要があります。[Actions] ドロップダウンリストから、[Commit] を選択します。[コミット (Commit)] ウィンドウが表示されます。[コミットメモ (Commit Note)] テキストボックスに、コミットのメモを入力することができます。バージョン番号はシステムによって自動的に生成されます。
- ステップ 5** 履歴を表示するには、[アクション (Actions)] ドロップダウンリストから、[履歴の表示 (Show History)] を選択します。以前作成してバージョンを付けたテンプレートが表示されます。ポップアップウィンドウが表示されます。

- 古いバージョンのコンテンツを表示するには、ポップアップウィンドウの[表示 (View)]をクリックします。
- テンプレートを編集するには、ポップアップウィンドウの[編集 (Edit)]をクリックします。

変数バインド

テンプレートを作成する場合、コンテキストに合わせて置き換わる変数を指定できます。それらの変数の多くは、[Template Editor] ドロップダウンリストで使用できます。Cisco DNA Center リリース 1.1 では、テンプレートで定義されるすべての変数に値を手動で入力する必要がありました。

リリース 1.2 以降では、テンプレートエディタに、編集または入力フォーム機能拡張 (DHCP サーバ、DNS サーバ、Syslog サーバなど) から、ソースオブジェクト値を使用してテンプレートで変数をバインドまたは使用するオプションがあります。

事前定義済みのオブジェクト値は、次のいずれかにすることができます。

- Inventory
 - デバイス オブジェクト
 - インターフェイス オブジェクト
- [Common Settings] : [Design] > [Network Settings] > [Network] で利用可能な設定。共通設定の変数バインドによって、デバイスが属するサイトに基づいた値が解決されます。

- ステップ 1** Cisco DNA Center ホームページで、[ツール (Tools)] > [テンプレート エディタ (Template Editor)] を選択します。
- ステップ 2** テンプレートを選択し、[Input Form] アイコンをクリックして、テンプレート内の変数をネットワーク設定にバインドします。
- ステップ 3** 変数をネットワーク設定にバインドするには、[Input Form] ペインで変数を選択し、[Required] チェックボックスをオンにします。
- ステップ 4** [Display] ドロップダウンリストから、プロビジョニング時に作成する UI ウィジェットのタイプを選択します。[Text Field]、[Single Select]、または [Multi Select]。
- ステップ 5** 変数をネットワーク設定にバインドするには、[Input Form] で各変数を選択し、[Content] の下の [Bind to Source] チェックボックスをオンにします。
 - それぞれのドロップダウンリストで、[ソース (Source)]、[エンティティ (Entity)]、および [属性 (Attributes)] を選択します。
 - ソースタイプが [Common Settings] の場合は、次のエンティティのいずれかを選択します。[dhcp.server]、[syslog.server]、[snmp.trap.receiver]、[ntp.server]、[timezone.site]、[device.banner]、[dns.server]、[netflow.collector]。

- ソースタイプが [NetworkProfile] の場合、エンティティタイプとして [SSID] を選択します。入力される SSID エンティティは、[Design] > [Network Profile] で定義されます。バインドにより、SSID 名、サイト、および SSID カテゴリの組み合わせであるわかりやすい SSID 名が生成されます。[Attributes] ドロップダウンリストから、[wlanid] を選択します。この属性は、テンプレートのプロビジョニング時の高度な CLI 設定中に使用されます。
- ソースタイプが [Inventory] の場合、次のいずれかのエンティティを選択します。[Device]、[Interface]、[AP Group]、[Flex Group]、[Wlan]、[Policy Profile]、[Flex Profile]。エンティティタイプ [Device] および [Interface] の場合、[Attribute] ドロップダウンリストにデバイスまたはインターフェイスの属性が表示されます。変数は、テンプレートを適用するデバイスで設定されている AP グループと Flex グループの名前を解決します。

変数を共通設定にバインドしたら、テンプレートをワイヤレスプロファイルに割り当て、テンプレートをプロビジョニングするときに、[Network Settings] > [Network] の下で定義したすべてのネットワーク設定がドロップダウンリストに表示されます。これらの属性は、ネットワークの設計時に[ネットワーク設定 (Network Settings)] > [ネットワーク (Network)] の下で定義する必要があります。

特別なキーワード

テンプレートを通じて実行されるすべてのコマンドは、常に **config t** モードになります。そのため、テンプレートで明示的に **enable or config t** コマンドを指定する必要はありません。

イネーブルモードコマンド

config t コマンドの他に任意のコマンドを実行する場合は、**#MODE_ENABLE** コマンドを指定します。

次の構文を使用して、CLI テンプレートに **enable mode** コマンドを追加します。

```
#MODE_ENABLE
<<commands>>
#MODE_END_ENABLE
```

インタラクティブコマンド

ユーザ入力が必要なコマンドを実行する場合は、**#INTERACTIVE** を指定します。

インタラクティブコマンドには、コマンドの実行後に入力する必要がある入力が含まれています。[CLIContent] 領域にインタラクティブコマンドを入力するには、次の構文を使用します。

```
CLI Command<IQ>interactive question 1 <R> command response 1 <IQ>interactive question 2<R>command response 2
```

ここで、**<IQ>** タグおよび **<R>** タグは大文字と小文字を区別し、大文字で入力する必要があります。

```
#INTERACTIVE
crypto key generate rsa general-keys <IQ>yes/no<R> no
#ENDS_INTERACTIVE
```




- (注) 応答後にインタラクティブ コマンドの質問に対応するとき、改行文字が必要ない場合は **<SF>** タグを入力する必要があります。 **<SF>** タグの前にスペースを1つ含めます。 **<SF>** タグを入力すると、 **</SF>** タグが自動的にポップアップ表示されます。 **</SF>** タグは不要なため削除できます。

次に例を示します。

```
#INTERACTIVE
config advanced timers ap-fast-heartbeat local enable 20 <SF><IQ>Apply(y/n)?<R>y
#ENDS_INTERACTIVE
```

インタラクティブイネーブルモードコマンドの組み合わせ

次の構文を使用して、インタラクティブな **Enable Mode** コマンドを結合します。

```
#MODE_ENABLE
#INTERACTIVE
commands<IQ>interactive question<R> response
#ENDS_INTERACTIVE
#ENDS_END_ENABLE
```

```
#MODE_ENABLE
#INTERACTIVE
mkdir <IQ>Create directory<R>xyz
#ENDS_INTERACTIVE
#MODE_END_ENABLE
```

複数行コマンド

CLI テンプレートで複数行をラップする場合は、**MLTCMD** タグを使用します。そうしなければ、コマンドは1行ずつデバイスに送信されます。[CLI Content] 領域にマルチライン コマンドを入力するには、次の構文を使用します。

```
<MLTCMD>first line of multiline command
second line of multiline command
...
...
last line of multiline command</MLTCMD>
```

- ここで、**<MLTCMD>** および **</MLTCMD>** は大文字と小文字を区別し、大文字で入力する必要があります。
- 複数行のコマンドは、**<MLTCMD>** タグと **</MLTCMD>** タグの間に挿入する必要があります。
- タグをスペースで開始することはできません。
- 1行に **<MLTCMD>** タグと **</MLTCMD>** タグを使用することはできません。

ネットワークプロファイルへのテンプレートの関連付け

始める前に

テンプレートをプロビジョニングする前に、テンプレートがネットワークプロファイルに関連付けられており、そのプロファイルがサイトに割り当てられていることを確認してください。

プロビジョニング中にデバイスが特定のサイトに割り当てられると、ネットワークプロファイルを介してサイトに関連付けられたテンプレートが詳細設定に表示されます。

ステップ 1 [設計 (Design)] > [ネットワーク プロファイル (Network Profiles)] の順に選択し、[プロファイルの追加 (Add Profile)] をクリックします。

プロファイルには次の 3 つのタイプがあります。

- [ルーティングと NFV (Routing & NFV)] : ルーティングと NFV プロファイルの作成時にこれを選択します。詳細については、「ルーティングと NFC」を参照してください。
- [スイッチング (Switching)] : スwitching プロファイルの作成時にこれを選択します。
 - 必要に応じて、[Onboarding Templates] または [Day-N Templates] をクリックします。
 - プロファイル名を入力します。
 - [+Add] をクリックして、[Device Type]、[Tag Name]、および [Template] ドロップダウンリストから、デバイスのタイプ、タグ、およびテンプレートを選択します。

(注) 必要なテンプレートが見つからない場合は、[標準テンプレートの作成 \(168 ページ\)](#) の説明に従ってテンプレート エディタで新しいテンプレートを作成できます。
 - [保存 (Save)] をクリックします。
- [ワイヤレス (Wireless)] : ワイヤレス プロファイルの作成時にこれを選択します。ワイヤレス ネットワーク プロファイルを割り当てる前に、ワイヤレス SSID が作成されていることを確認してください。
 - プロファイル名を入力します。
 - [+ SSID の追加 (+ Add SSID)] をクリックします。[ネットワーク設定 (Network Settings)] > [ワイヤレス (Wireless)] の下で作成されたこれらの SSID が追加されます。
 - [テンプレートの添付 (Attach Template(s))] エリアで、[テンプレート (Template)] ドロップダウンリストからプロビジョニングするテンプレートを選択します。
 - [保存 (Save)] をクリックしてプロファイルを保存します。

ステップ 2 [ネットワーク プロファイル (Network Profiles)] ページには、次のリストが表示されます。

- プロファイル名
- Type

- **Version**
- **作成者**
- [サイト (Sites)]: [サイトの割り当て (Assign Site)] をクリックして、選択したプロファイルにサイトを追加します。

ステップ 3 Day-N プロビジョニングの場合は、**[Provision] > [Devices]** を選択します。[デバイス インベントリ (Device Inventory)] ウィンドウが表示されます。

- プロビジョニングするデバイス名の隣にあるチェックボックスを 1 つ以上オンにします。
- [アクション (Actions)] ドロップダウンリストから、[プロビジョニング (Provision)] を選択します。
- [サイトの割り当て (Assign Site)] ウィンドウで、プロファイルが添付されたサイトを割り当てます。[サイトを選択 (Choose a Site)] フィールドで、コントローラと関連付けるサイトの名前を入力するか、[サイトを選択 (Choose a Site)] ドロップダウンリストから選択します。
- [Next] をクリックします。

[設定 (Configuration)] ウィンドウが表示されます。[管理 AP の場所 (Managed AP Locations)] フィールドで、コントローラで管理する AP の場所を入力します。これで、サイトの変更、削除、または再割り当てができるようになります。これはワイヤレス プロファイルにのみ適用可能です。

- [Next] をクリックします。
- **[Advanced Configuration (詳細設定)]** ウィンドウが表示されます。ネットワーク プロファイルを介してサイトに関連付けられているテンプレートが [詳細設定 (Advanced Configuration)] に表示されます。

- [Find] 機能を使用し、デバイス名を入力して素早くデバイスを検索するか、左側のペインでテンプレートフォルダを展開してテンプレートを選択します。右側のペインで、ドロップダウンリストから送信元にバインドされている属性の値を選択します。

- テンプレートを導入する間にテンプレートの変数を CSV ファイルにエクスポートするには、右側のペインで [エクスポート (Export)] をクリックします。CSV ファイルを使用して変数設定に必要な変更を加え、右側のペインで [Import] をクリックすると、後でそれを Cisco DNA Center にインポートできます。

- [次へ (Next)] をクリックしてテンプレートを導入します。テンプレートを今すぐ導入するか、または後でスケジュールするかどうかを求められます。
- テンプレートをすぐに導入するには、[今すぐ実行 (Now)] ラジオ ボタンをクリックし、次に [適用 (Apply)] をクリックします。将来の日付と時刻でテンプレートの導入をスケジュールするには、[後で実行 (Later)] ラジオ ボタンをクリックし、導入する日時を定義します。

導入が成功すると、[デバイスインベントリ (Device Inventory)] ウィンドウの [ステータス (Status)] 列に、「成功 (SUCCESS) 」と表示されます。

ステップ 4 Day-0 プロビジョニングの場合は、**[Provision] > [Devices] > [Plug and Play]** を選択します。[Plug and Play] ウィンドウが表示されます。

- デバイスを選択し、[Actions] ドロップダウンリストから [Claim] をクリックします。
- [Next] をクリックし、[Site Assignment] ウィンドウで、[Site] ドロップダウンリストからサイトを選択します。

- [Next] をクリックし、[Configuration] ウィンドウで、イメージと Day-0 テンプレートを選択します。
 - [Next] をクリックし、[Advanced Configuration] ウィンドウで場所を入力します。
 - [Next] をクリックして、[Device Details]、[Image Details]、[Day-0 Configuration Preview]、および [Template CLI Preview] を表示します。
-



第 10 章

テレメトリ プロファイルの設定

- [テレメトリについて \(181 ページ\)](#)
- [テレメトリ プロファイルの設定 \(181 ページ\)](#)
- [デバイスにテレメトリ プロファイルを適用 \(182 ページ\)](#)
- [新しいクラスタ仮想 IP アドレスを使用するためのテレメトリプロファイルの更新 \(184 ページ\)](#)

テレメトリについて

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

テレメトリ プロファイルの設定

テレメトリ ツールを使用して、ネットワーク デバイスにテレメトリ アセスメント プロファイルを作成できます。



- (注) デフォルトでは、[Disable-Telemetry] プロファイルが、ネットワーク データ プラットフォーム (NDP) によってすべての有効なデバイスのすべてのインターフェイス上に設定されています。
-

始める前に

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

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

[テレメトリ (Telemetry)] ウィンドウが表示されます。

ステップ 2 [Site View] タブをクリックし、ネットワークデバイスがこのウィンドウに表示されているか確認します。

(注) テレメトリプロファイルを設定した後、このウィンドウに戻り、テレメトリプロファイルをデバイスに適用する必要があります。

ステップ 3 [プロファイルの表示 (Profile View)] タブをクリックします。

[プロファイルの表示 (Profile View)] タブには以下の情報を表示します。

- [Profile Name] : Cisco DNA Center が事前設定したプロファイルとユーザが設定するプロファイルの名前。Cisco DNA Center には、次の事前設定されたプロファイルが用意されています。
- [Maximal Visibility] : 考えられるすべてのテレメトリをすべての有効なデバイス上のすべてのインターフェイスで有効にするために、NDP によって生成されるテレメトリプロファイル。このプロファイルは、Syslog およびアプリケーションの可視性プロファイルを組み合わせたものです。
- [Optimal Visibility] : ネットワークトポロジ、デバイスの機能、PIN、有効な アシユアランス 機能を分析した後、NDP によって生成されたテレメトリプロファイル。このプロファイルは、ネットワークデバイスに Syslog プロファイルを適用する際に使用できます。
- [Disable Telemetry] : NDP によってすべての有効なデバイス上のすべてのインターフェイス上に設定されたテレメトリプロファイルを無効化します。
- [Customized] : プロファイルが、Cisco DNA Center 事前設定のプロファイルか、ユーザ設定のプロファイルかどうかに関する情報。
- [Profile Usage] : テレメトリプロファイルが適用されるデバイスの数。

ステップ 4 [プロファイルを追加 (Add Profile)] をクリックします。

ステップ 5 [Name] フィールドに、プロファイルの名前を入力します。

ステップ 6 (オプション) [Syslog] チェックボックスをオンにして、ドロップダウンリストから [Severity Level] を選択します。

ステップ 7 [保存 (Save)] をクリックして、プロファイル設定を保存するか、[キャンセル (Cancel)] をクリックして、プロファイル設定をキャンセルします。

デバイスにテレメトリ プロファイルを適用

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

始める前に

次の予備タスクを実行します。

- Cisco DNA Center を使用して、ネットワーク内のデバイスを検出します。
- [Telemetry] [Profile View] オプションとフィールドを使用して、使用可能なテレメトリプロファイルを確認および設定します。

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

[テレメトリ (Telemetry)] ウィンドウが表示されます。

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

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

次の情報が表示されます。

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

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

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

ステップ 6 [Show] ドロップダウンメニューから、先ほど適用したテレメトリプロファイルを選択します。

デバイスは、同じテレメトリ プロファイルで設定された他のデバイスとともに、フィルタリングされたリストに表示されます。

次のタスク

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

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

新しいクラスタ仮想 IP アドレスを使用するためのテレメトリプロファイルの更新

Cisco DNA Center テレメトリツールを使用してデバイスデータを監視しており、Cisco DNA Center クラスタ仮想 IP アドレス (VIP) を変更する必要がある場合は、次の手順を完了して VIP を変更し、ノードテレメトリデータが新しい VIP に送信されることを確認します。

始める前に

- 使用している Cisco DNA Center のバージョンを確認します。確認するには、Cisco DNA Center Web インターフェイスにログインし、[About] オプションを選択して Cisco DNA Center のバージョン番号を表示します。たとえば、使用しているバージョンが 1.1 で始まる場合は、1.1.x リリーストレインに含まれます。
- SSH クライアントソフトウェアを入手します。
- Cisco DNA Center マスターノード上のエンタープライズネットワーク側の 10 GB インターフェイスに設定された VIP アドレスを特定します。ポート 2222 上のこのアドレスを使用してアプライアンスにログインします。このポートを特定するには、[Cisco Digital Network Architecture Center 設置ガイド \[英語\]](#) の「Front and Rear Panels」セクションにある背面パネルの図を参照してください。
- マスターノードに設定されている Linux ユーザ名 (**maglev**) とパスワードを取得します。
- 割り当てるクラスタ VIP を特定します。クラスタ VIP は、[Cisco Digital Network Architecture Center 設置ガイド \[英語\]](#) の「Required IP Addresses and Subnets」セクションで説明されている要件に準拠している必要があります。

ステップ 1 以下の手順を実行して Cisco DNA Center GUI にアクセスし、テレメトリツールを使用して、[Disable Telemetry] プロファイルをすべてのノードにプッシュします。

- a) Cisco DNA Center のホームページで、[Tools] エリアまで下にスクロールし、[Telemetry] をクリックします。
- b) [サイトの表示 (Site View)] タブをクリックします。
- c) [Site View] テーブルで、現在監視されているすべてのサイトとデバイスを選択します。
- d) [Actions] ボタンをクリックして、ドロップダウンリストから [Disable Telemetry] プロファイルを選択します。
- e) [Site View] テーブルに、サイトとデバイスに対してテレメトリが無効になったことが表示されるまで待ちます。

ステップ 2 アプライアンス構成ウィザードを使用して、次のようにクラスタ VIP を変更します。

- a) SSH クライアントを使用して、Cisco DNA Center マスターノード上のエンタープライズネットワーク側の 10 GB インターフェイスに設定された VIP アドレスにログインします。ポート 2222 にログインしていることを確認します。

- b) プロンプトが表示されたら、Linux のユーザ名とパスワードを入力します。
- c) 次のコマンドを入力すると、マスターノード上で構成ウィザードにアクセスできます。

```

$ sudo maglev-config update
    
```

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

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

Cisco DNA Center 1.2.5 以降では、設定したインターフェイスごとに 1 つの仮想 IP を設定する必要があります。 `sudo maglev-config update` コマンドを入力して、設定したインターフェイスごとに 1 つの VIP を入力するよう指示されるようにウィザードを設定することを推奨します。

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

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

設定プロセスの最後に成功メッセージが表示され、SSH プロンプトが再表示されます。

ステップ 3 SSH プロンプトで次の一連のコマンドを入力して、必要な Cisco DNA Center サービスを再起動します。使用している Cisco DNA Center バージョンに適したリリーストレインのコマンドを使用します。

1.1.x リリーストレイン（バージョン 1.1.1 以降、1.2.0 未満）に属する Cisco DNA Center のバージョンの場合は、次のコマンドを入力します。

```

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

1.2.x リリーストレイン（バージョン 1.2.0 以降）に属する Cisco DNA Center のバージョンの場合は、次のコマンドを入力します。

```

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

ステップ 4 すべてのサービスが再起動するまで待ちます。次のコマンドを入力して、再起動の進行状況をモニタリングできます。必要に応じて、使用している Cisco DNA Center のバージョンが属するリリーストレインに適したサービス名に置き換えてください。たとえば、1.2.x リリーストレインに属する Cisco DNA Center のバージョンを使用している場合は、次のコマンドを入力します。

```

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

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

```

assurance-backend wirelesscollector-123-bc99s 1/1 Running 0 25d <IP> <IP>
ndp collector-netflow-456-lxv1x 1/1 Running 0 1d <IP> <IP>
ndp collector-syslog-789-r0rr1 1/1 Running 0 25d <IP> <IP>
ndp collector-trap-101112-3ppl1m 1/1 Running 0 25d <IP> <IP>
    
```

ステップ 5 手順 1 と同じように、Cisco DNA Center の GUI にアクセスし、テレメトリツールを使用して、すべてのノードに [Optimal Visibility] プロファイルをプッシュします。



第 11 章

ネットワーク セキュリティ アドバイザリの の識別

- [セキュリティアドバイザリの概要](#) (187 ページ)
- [セキュリティアドバイザリの表示](#) (187 ページ)

セキュリティアドバイザリの概要


Cisco Product Security Incident Response Team (PSIRT; プロダクトセキュリティインシデントレスポンスチーム) は、シスコ製品のセキュリティインシデントに対応し、セキュリティ脆弱性ポリシーを規制し、[シスコのセキュリティアドバイザリとアラート](#)を推奨します。

セキュリティアドバイザリ ツールは、これらの推奨されるアドバイザリを使用して、Cisco DNA Center内のインベントリをスキャンし、既知の脆弱性を持つデバイスを検出します。

セキュリティアドバイザリの表示


始める前に

- セキュリティアドバイザリ ツールを使用するには、[機械推論パッケージ](#)をインストールする必要があります。Cisco *Digital Network Architecture Center* 管理者ガイド [英語] の「[Download and Install Packages and Updates](#)」を参照してください。
- オブザーバとして Cisco DNA Center にログインすると、ホームページで [Security Advisories] ツールを表示できません。

ステップ 1 Cisco DNA Center のホームページで、[Tools] エリアまで下にスクロールし、[Security Advisories] をクリックします。右上隅の  アイコンをクリックし、[Security Advisories] を選択することもできます。

ステップ 2 [Security Advisories] ページを初めて起動する場合は、[Scan] をクリックします。

Cisco DNA Center Cisco DNA Center は、セキュリティの問題を特定して自動分析を改善するために、ナレッジベースを使用します。最新のセキュリティアドバイザリを表示するには、定期的にナレッジベースを更新することをお勧めします。

- a)  > [System Settings] > [Settings] > [Machine Reasoning] をクリックします。
- b) [Import Latest from Cisco] をクリックするか、[ここ](#)をクリックして最新の使用可能なナレッジベースをダウンロードし、[Import from local] をクリックします。
- c) 自動更新に登録するには、[AUTO UPDATE] トグルボタンをクリックします。

- (注)
- セキュリティアドバイザリ ダッシュボードにはシスコが公開しているセキュリティアドバイザリが表示されます。アドバイザリは現行のソフトウェアイメージに基づいており、ネットワーク上のデバイスに影響する場合があります。脆弱性が実際に存在するかどうかを判断するには、設定、プラットフォームの詳細、またはその他の基準をさらに詳しく分析する必要があります。
 - セキュリティアドバイザリ スキャンのサポートは、サポートされている最小ソフトウェアバージョンに準拠しているルータおよびスイッチでのみ使用できます。サポートされている最小のソフトウェアバージョンの詳細については、「[Cisco DNA Centerサポート対象デバイス](#)」を参照してください。
 - 表示されるセキュリティアドバイザリは、[シスコのセキュリティ脆弱性ポリシー](#)に基づいています。

次の表に、使用できる情報を記載します。

カラム	説明
アドバイザリ ID	ネットワークで検出されたセキュリティアドバイザリの ID。
アドバイザリタイトル	ネットワークデバイスに適用されるセキュリティ脆弱性アドバイザリの名前。アドバイザリをクリックして、それぞれのアドバイザリ Web ページに移動します。
CVSS スコア	共通脆弱性評価システム (CVSS) モデルに基づいて評価されたスコア。
Impact	ネットワークへの脆弱性の影響 (Critical、High、Medium、Low など)。
CVE	脆弱性の Common Vulnerabilities and Exposures (CVE) 識別子。
デバイス	脆弱性の影響を受けるデバイスの数。この特定のアドバイザリに基づいて脆弱性が存在する可能性のあるデバイスを表示するには、番号をクリックし、必要に応じてデバイスをアップグレードします。
検出以降の期間 (日数)	脆弱性が検出されてからの経過日数。
Last Updated	アドバイザリが最後に更新された日付。

ステップ 3 各デバイスに適用可能なアドバイザリの数を表示するには、[Devices] タブをクリックします。

- a) デバイスに一致するものをすべて表示するには、アドバイザリの数をクリックします。

- b) デバイストポロジを表示するには、右上隅にあるトポロジアイコンをクリックします。トポロジ内のデバイスをクリックすると、そのデバイスに一致するすべてのアドバイザリが表示されます。
- デバイスの横にあるロックアイコンは、デバイスに適用可能な1つ以上のアドバイザリがあることを示します。

ステップ 4 いつでも [Scan] をクリックすれば、表示された結果を更新できます。



第 12 章

ポリシーの設定

- [ポリシーの概要 \(191 ページ\)](#)
- [グループベースのアクセス コントロール ポリシー \(191 ページ\)](#)
- [IP ベースのアクセス コントロール ポリシー \(202 ページ\)](#)
- [アプリケーションポリシー \(209 ページ\)](#)
- [トラフィック コピー ポリシー \(241 ページ\)](#)
- [仮想ネットワーク \(245 ページ\)](#)

ポリシーの概要

Cisco DNA Center を使用すると、ネットワークの特定の側面（ネットワークアクセスなど）に対する組織のビジネス目標を反映したポリシーを作成できます。Cisco DNA Center は、ポリシー内で収集された情報を取得し、お使いのネットワークデバイスのさまざまなタイプ、メーカー、モデル、オペレーティングシステム、ロール、およびリソースの制約によって必要とされる、ネットワーク固有およびデバイス固有の設定に変換します。

Cisco DNA Center を使用して、仮想ネットワーク、アクセス コントロール ポリシー、トラフィック コピー ポリシー、およびアプリケーション ポリシーを作成できます。

グループベースのアクセス コントロール ポリシー

Cisco DNA Center Cisco DNA Center は、次の 2 つの方法で Software-Defined Access を実装します。

- 仮想ネットワーク (VN) は、マクロレベルのセグメンテーションを提供します。たとえば、企業のネットワークから IoT デバイスを分離します。
- グループベースのポリシーは、マイクロレベルのセグメンテーションを提供します。たとえば、エンジニアリンググループと HR グループの間で許可または拒否するネットワークトラフィックのタイプを制御します。

グループベースのアクセスコントロールポリシーメニューを使用すると、スケーラブルグループアクセスポリシーを監視および管理できます。それらのポリシーには、次の利点があります。

- ネットワークの自動化とアシュアランスの利点を備えた、豊富なアイデンティティベースのアクセスコントロール機能。
- きめ細かいアクセス制御。
- スケーラブルグループは、すべての仮想ネットワークに適用されるため、ポリシー管理が簡素化されます。
- ポリシービューは、全体的なポリシー構造を理解し、必要なアクセスコントロールポリシーを作成または更新するのに役立ちます。
- さまざまなアプリケーションを切り替えてスケーラブルグループを管理し、保護される資産を定義する必要がなくなります。
- エンタープライズ全体のアクセスコントロールポリシーを展開するための拡張機能を提供します。
- アイデンティティまたはネットワーク アドミッション コントロール (NAC) アプリケーションが配置される前に、ランサムウェアなどの脅威のラテラルムーブメントを制限します。
- サードパーティのアイデンティティ アプリケーションを使用しているが Cisco ISE 移動する必要があるユーザに対して、Cisco Identity Services Engine (Cisco ISE) への簡単な移行パスを提供します。

Cisco DNA Center での IP プール、サイト、および仮想ネットワークの作成方法については、[Cisco Digital Network Architecture Center ユーザガイド \[英語\]](#) を参照してください。

Cisco DNA Center for Cisco ISE のインストールと設定の詳細については [Cisco Digital Network Architecture Center 設置ガイド \[英語\]](#) を参照してください。

Cisco ISE for Cisco DNA Center の設定の詳細については、[Cisco Identity Services Engine 管理者ガイド \[英語\]](#) を参照してください。

まず、スケーラブルグループと契約を定義してから、アクセスコントロールポリシーを作成します。アクセスコントロールポリシーでは、送信元スケーラブルグループから宛先スケーラブルグループに渡すことができるネットワークトラフィックを定義します。

- **スケーラブルグループ**：ユーザ、ネットワークデバイス、またはリソースを割り当てることができる分類カテゴリ。スケーラブルグループは、アクセスコントロールポリシーで使用されます。組織のネットワーク設定、アクセス要件、および制限に基づいて、スケーラブルグループを仮想ネットワークに関連付けることができます。
- **契約**：アクセス契約は、送信元と宛先のスケーラブルグループ間の通過を許可されるネットワークトラフィックのタイプを制御する一連のルールです。つまり、契約はトラフィックフィルタの定義です。アクセス契約は、トラフィックがネットワークアプリケーション、プロトコル、およびポートに一致したときに実行されるアクション（許可または拒

否)を定義します。他のルールが一致しない場合、デフォルトアクションでは Catch All ルールが使用されます。

- **グループベースのアクセスコントロールポリシー**：グループベースのアクセスコントロールポリシーは、特定の送信元と宛先グループのペアを識別し、アクセス契約を関連付けます。アクセス契約では、送信元グループと宛先グループの間で許可または拒否されるトラフィックのタイプを指定します。これらのポリシーは一方方向だけに作用します。

スケーラブルグループおよびアクセス契約は、アクセスコントロールポリシーの基本的な構成要素です。アクセスコントロールポリシーを作成する際には、前に作成したスケーラブルグループと契約を使用したり、ポリシーの作成時に新しいスケーラブルグループと契約を作成したりできます。特定の送信元グループからアクセスできるネットワークリソースを指定する場合は、1つの送信元グループと複数の宛先グループを含むアクセスコントロールポリシーを作成できます。一方、特定のネットワークリソースへのアクセスが許可されている送信元グループを指定する場合は、1つの宛先グループと複数の送信元グループを含むアクセスコントロールポリシーを作成できます。たとえば、「請負業者」送信元スケーラブルグループに関連付けられたユーザがアクセスできるネットワークリソースを指定する場合は、1つの送信元グループと複数の宛先グループを含むアクセスコントロールポリシーを作成できます。「財務サーバ」宛先スケーラブルグループへのアクセスが許可されている送信元グループを指定する場合は、1つの宛先グループと複数の送信元グループを含むアクセスコントロールポリシーを作成できます。

送信元と宛先のスケーラブルグループの組み合わせに契約が指定されていない場合に使用するデフォルトポリシーを指定できます。デフォルトポリシーは [Permit] です。必要に応じて、このポリシーを [Deny]、[Permit_IP_Log]、または [Deny_IP_Log] に変更できます。ネットワークタイプ、オープンネットワーク、またはクローズネットワークに基づいて、デフォルトポリシーを設定できます。



- (注) すべてのネットワークインフラストラクチャデバイスに必要なネットワークトラフィックを許可する明示的なポリシーを作成した場合のみ、デフォルトポリシーを [Permit] から [Deny] に変更することをお勧めします。それ以外の場合に変更すると、すべてのネットワーク接続が失われる可能性があります。

リストビュー

[Group-Based Access Control] ウィンドウの右上にある [List] アイコンをクリックして、[List] ビューを起動します。

- [Source View]：このビューには、送信元グループに基づいて編成された既存のポリシーのリストが表示されます。各行を展開して、特定の送信元と宛先のポリシーの詳細を表示できます。
- [Destination View]：このビューには、宛先グループに基づいて編成された既存のポリシーのリストが表示されます。各行を展開して、特定の送信元と宛先のポリシーの詳細を表示できます。

特定の送信元グループから使用可能な宛先グループを確認するには、[Source] ビューを使用します。特定の宛先グループへのアクセスが許可されている送信元グループを確認するには、[Destination] ビューを使用します。たとえば、「請負業者」送信元スケーラブルグループの一部であるユーザが使用できる宛先グループを確認するには、[Source] ビューを使用します。「財務サーバ」宛先スケーラブルグループにアクセスできる送信元グループを確認するには、[Destination] ビューを使用します。

[Deploy] をクリックして、更新されたポリシーをネットワークデバイスに展開します。[Deploy] をクリックすると、Cisco DNA Center は Cisco Identity Services Engine (Cisco ISE) に、ポリシーの変更に関する通知をネットワークデバイスに送信するように要求します。

マトリクス ビュー

[Group-Based Access Control] ウィンドウの右上にある [Grid] アイコンをクリックして、[Matrix] ビューを起動します。[Matrix] ビューはコアポリシービューであり、すべてのスケーラブルグループ（明示的またはデフォルトのいずれか）のすべてのポリシーの概要を提供します。[Matrix] ビューを使用して、すべての送信元と宛先のポリシーを表示し、全体的なポリシー構造を理解できます。[Matrix] ビューからアクセスコントロールポリシーを表示、作成、および更新できます。

[Matrix] ビューには、次の 2 つの軸があります。

- 送信元軸：垂直軸にはすべての送信元スケーラブルグループがリストされます。
- 宛先軸：水平軸にはすべての宛先スケーラブルグループがリストされます。

特定の送信元スケーラブルグループと宛先スケーラブルグループのポリシーを表示するには、セルにカーソルを置きます。セルの色は、そのセルに適用されるポリシーに基づいています。次の色は、各セルに適用されるポリシーを示しています。

- [Permit]：緑色
- [Deny]：赤色
- [Custom]：金色
- [Default]：灰色

マトリクスの上部に表示される [Permit]、[Deny]、[Custom]、または [Default] アイコンにカーソルを置くと、そのポリシーが適用されているセルが表示されます。

セルをクリックすると、[Create Policy] または [Edit Policy] スライドインペインが開き、選択したセルのポリシーを作成または編集できます。[Create Policy] スライドインペインには、送信元と宛先のスケーラブルグループが読み取り専用フィールドとして表示されます。ポリシーのステータスとアクセス契約を更新できます。

[Filter] オプションを使用して、選択した一連の送信元および宛先グループのポリシーマトリクスのサブセットを表示できます。フィルタを作成して、関心のあるポリシーだけに絞り込むことができます。フィルタを作成するには、含める送信元および宛先グループを選択します。

カーソルでマトリックスコンテンツ領域をドラッグするか、または水平および垂直スクロールバーを使用して、マトリックス内を移動できます。ミニマップを使用して、マトリックス内を移動することもできます。ミニマップを使用すると、マトリックスのサイズが大きく、画面サイズを超えている場合に、マトリックス内を簡単に移動できます。ミニマップは、画面上の任意の場所に動かして配置できます。ミニマップにはマトリックスビュー全体が表示されます。ミニマップの薄い灰色の部分は、画面に現在表示されているマトリックスの部分を表します。この領域をドラッグして、マトリックスをスクロールできます。



(注) ミニマップはデフォルトでは閉じられています。[Expand] アイコンをクリックして、ミニマップを展開して表示します。

セルを選択すると、[Matrix] ビューによってそのセルと対応する行（送信元スケーラブルグループ）と列（宛先スケーラブルグループ）が強調表示されます。選択したセルの座標（送信元および宛先スケーラブルグループ）がマトリックスコンテンツ領域の近くに表示されます。

[Deploy] をクリックして、更新されたポリシーをネットワークデバイスに展開します。[Deploy] をクリックすると、Cisco DNA Center は Cisco ISE に、ポリシーの変更に関する通知をネットワークデバイスに送信するように要求します。

Cisco DNA Center と Cisco ISE を統合します。Cisco ISE は、Cisco DNA Center の代わりにネットワークデバイスにポリシーをダウンロードするためのランタイム ポリシー プラットフォームを提供します。ポリシーの同期の問題を防ぐために、セキュリティグループ、セキュリティグループ アクセス コントロール リスト (SGACL)、およびイーグレスポリシーの [TrustSec Work Center] ユーザインターフェイス画面が Cisco ISE に読み取り専用モードで表示されます。

ポリシー作成の概要

1. 組織の分類を定義するか、または最初に使用する組織の部分を定義します。
2. 特定した分類のスケーラブルグループを作成します。
3. 制御するネットワークトラフィックのタイプに対するアクセス契約を作成します。すべてのトラフィックを許可または拒否するためのサンプルアクセス契約が事前に定義されています。また、一部の契約例では、より具体的なトラフィックフィルタリングが示されています。特定のアプリケーション定義に基づいて、さらにきめ細かいアクセス契約を作成できます。
4. アプリケーションサーバや他のネットワークへの接続など、特定のネットワークリソースへのアクセスを必要とするネットワークユーザのカテゴリを決定します。
5. アクセスポリシーを作成し、送信元グループ、宛先グループ、およびアクセス契約を関連付け、送信元から宛先へのトラフィックフローを許可する方法を定義します。

スケーラブルグループの作成

始める前に

次のタスクを実行するには、スーパー管理者またはネットワーク管理者である必要があります。

ステップ 1 [Policy] > [Group-Based Access Control] > [Scalable Groups] の順に選択します。

ステップ 2 [Create Scalable Group] をクリックします。

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

ステップ 3 [Create Scalable Group] スライドインペインで、スケーラブルグループの名前と説明（任意）を入力します。

（注） [Name] フィールドでサポートされる文字は次のとおりです：

- 英数字
- アンダースコア (_)

スケーラブルグループ名は英字で開始する必要があります。

Cisco DNA Center タグ値を生成します。必要に応じて、この値を更新できます。指定した値が既存のスケーラブルグループによってすでに使用されている場合は、エラーメッセージが表示されます。有効な範囲は 2 ～ 65519 です。

ステップ 4 このスケーラブルグループに関連付ける**仮想ネットワーク**をドロップダウンリストから選択します。デフォルトでは、デフォルトの仮想ネットワーク (DEFAULT_VN) が選択されています。

ステップ 5 スケーラブルグループを Cisco Application Centric Infrastructure (ACI) に伝播する場合は、[Propagate to ACI] チェックボックスをオンにします。

ステップ 6 [保存 (Save)] をクリックします。

[Scalable Groups] ウィンドウには、スケーラブルグループ名、タグ値、割り当てられた仮想ネットワーク、および関連付けられたポリシーが表示されます。このウィンドウでは、スケーラブルグループのサンプルを表示することもできます。それらのスケーラブルグループは、使用または削除できます。

スケーラブルグループの [Policies] 列のリンクをクリックすると、そのスケーラブルグループとそのグループが属するポリシーを使用するアクセス制御ルールが表示されます。

Cisco ISE との同期が完了していない場合は、スケーラブルグループの横にオレンジ色の三角形のアイコンが表示されます。

スケーラブルグループは、[Scalable Groups] ウィンドウから編集または削除できます。ACI から学習したスケーラブルグループを編集または削除することはできません。スケーラブルグループがいずれかのアクセスポリシーで使用されている場合、そのスケーラブルグループは削除できません。

Cisco ISE は、内部エンドポイントグループ (IEPG) を同期し、Cisco ISE に関連付けられている読み取り専用スケーラブルグループを作成することで、ACI から TrustSec ドメインへのパケットをサポートします。それらのスケーラブルグループは、[Learned From] フィールドに ACI という値を持つ [Scalable Groups] ウィンドウに表示されます。ACI から学習したスケーラブルグループは編集も削除もできませんが、ポリシーで使用することはできます。

IEPG が ACI で更新されると、対応するスケーラブルグループ設定が Cisco ISE で更新されます。Cisco ISE でスケーラブルグループが作成されると、新しい EEPG が ACI に作成されます。

スケーラブルグループの詳細を表示するには、[Scalable Group Name] のリンクをクリックします。スケーラブルグループの詳細を更新するには、[View Scalable Group] ウィンドウで [Edit] をクリックします。[Deploy] をクリックすると、Cisco DNA Center は Cisco ISE に、ネットワークデバイスへの変更に関する通知を送信するように要求します。[Deploy] 列の展開ステータスを確認できます。



(注) 名前が「ANY」またはタグ値が 0xFFFF/65535 のスケーラブルグループは作成できません。スケーラブルグループ ANY/65535 は、Cisco DNA Center デフォルトポリシーに使用される予約済みの内部スケーラブルグループです。

Cisco DNA Center でスケーラブルグループを Cisco ISE と同期する場合、次のようになります。

- スケーラブルグループが Cisco DNA Center に存在し、Cisco ISE に存在しない場合は、Cisco ISE に作成されます。
- スケーラブルグループが Cisco ISE に存在し、Cisco DNA Center に存在しない場合は、Cisco DNA Center に作成されます。
- スケーラブルグループ名が Cisco DNA Center と Cisco ISE の両方で同じで、説明と ACI データが異なっている場合、Cisco DNA Center は Cisco ISE で指定されたデータを使用して更新されます。
- Cisco DNA Center と Cisco ISE でスケーラブルグループ名が同じで、タグ値が異なっている場合、Cisco ISE で指定されたタグ値を持つ新しいスケーラブルグループが Cisco DNA Center に作成されます。Cisco DNA Center にある既存のスケーラブルグループの名前は、サフィックス _DNAC 付きで更新されます。
- タグ値が同じで、スケーラブルグループ名が異なっている場合、Cisco DNA Center のスケーラブルグループ名が Cisco ISE で指定された名前更新されます。

アクセス契約の作成

アクセス契約は、送信元と宛先のスケーラブルグループ間の通過を許可されるネットワークトラフィックのタイプを制御する一連のルールです。アクセス契約は、トラフィックがネットワークアプリケーション、プロトコル、およびポートに一致したときに実行されるアクション（許可または拒否）を定義します。



(注) Cisco ISE のセキュリティ グループ アクセス コントロール リスト (SGACL) は、Cisco DNA Center のアクセス契約と呼ばれます。

始める前に

次のタスクを実行するには、スーパー管理者またはネットワーク管理者である必要があります。

ステップ 1 [Policy] > [Group-Based Access Control] > [Access Contracts] の順に選択します。

ステップ 2 [Create Access Contract] をクリックします。

ステップ 3 [Create Access Contract] スライドインペインで、契約の名前と説明を入力します。

ステップ 4 トラフィックフィルタルールを作成します。

- [Action] ドロップダウンリストで、[Deny] または [Permit] を選択します。
- [Application] ドロップダウンリストで、このアクションに割り当てるアプリケーションを選択します。ポートとプロトコルは、選択したアプリケーションに基づいて自動的に選択されます。
トランスポートプロトコル、送信元ポート、および宛先ポートを指定する場合は、[Application] ドロップダウンリストから [Advanced] オプションを選択します。

複数のルールを作成できます。1つの契約に複数のルールを作成するには、[Plus] 記号をクリックし、[Action] 列と [Application] 列の設定を選択します。ルールは、契約に記載されている順序でチェックされます。ルールの左端にあるハンドルアイコンを使用して、ルールをドラッグして順序を変更します。

[Logging] トグルを使用して、任意のトラフィックフィルタルール（デフォルトアクションを含む）のロギングを有効化または無効化できます。ロギングはデフォルトではディセーブルになっています。ロギングが有効になっている場合、トラフィックフィルタルールにヒットすると、ネットワークデバイスは syslog メッセージを送信します。これは、ポリシーのトラブルシューティングと初期テストに役立つ場合があります。ただし、ネットワークデバイスのリソースとパフォーマンスに影響を与える可能性があるため、このオプションは慎重に使用することを推奨します。

ステップ 5 [Default Action] ドロップダウンリストで、[Deny] または [Permit] を選択します。

必要に応じて、デフォルトアクションのロギングを有効にできます。

ステップ 6 [保存 (Save)] をクリックします。

[Access Contracts] リストウィンドウで、契約の表示、作成、複製、更新、および削除ができます。

また、[Access Contracts] ウィンドウでサンプル契約を表示することもできます。それらのサンプル契約は使用または削除できます。ただし、デフォルトの契約 (Permit IP、Deny IP、Permit_IP_Log、Deny_IP_Log) は削除できません。

[Filter] オプションを使用して、探している契約を検索できます。

Cisco ISE との同期が完了していない場合は、契約の横にオレンジ色の三角形のアイコンが表示されます。

[Access Contracts] ウィンドウの [Contract Name] リンクをクリックして、契約の詳細を表示します。契約の詳細を編集するには、[View Contract] ウィンドウで [Edit] をクリックします。

[Rules Count] 列で、各契約で使用されているルールを確認できます。

スケーラブルグループ、契約、またはポリシーを更新する場合は、ネットワークデバイスに変更を展開する必要があります。ポリシーを更新し、更新されたポリシーを展開しない場合、ポリシーの変更に関する通知はネットワークデバイスに送信されず、ネットワークで現在アクティブになっているポリシーは、Cisco DNA Center に表示されているポリシー情報と一致していない可能性があります。この状況を解決するには、ネットワークデバイスに更新されたポリシーを展開する必要があります。展開ステータスが [Deployed] 列に表示されます。

契約を使用するポリシーを表示するには、その契約の [Policies] 列のリンクをクリックします。

ポリシーで使用されている契約は削除できません。契約を削除する前に、ポリシーからその契約を削除する必要があります。

既存の契約を複製し、必要な詳細情報を編集して新しい契約を作成できます。契約を複製すると、既存の契約にあるすべての情報がコピーされ、コピーされた契約には、末尾に文字列「Copy」が付加された既存の契約名が含まれます。

Cisco DNA Center のアクセス契約を Cisco ISE と同期している間：

- 契約が Cisco DNA Center に存在し、Cisco ISE に存在しない場合は、Cisco ISE に作成されます。
- 契約が Cisco ISE に存在し、Cisco DNA Center に存在しない場合は、Cisco DNA Center に作成されます。
- 契約名が Cisco DNA Center と Cisco ISE で同じであるが、説明とトラフィックルールの内容が異なっている場合、Cisco DNA Center は Cisco ISE で指定されたデータを使用して更新されます。
- 契約名とルールが同じで、説明が異なっている場合、Cisco DNA Center は Cisco ISE で指定された説明を使用して更新されます。
- Cisco ISE の Text SGACL コマンドラインは、非解析コンテンツとして移行されます。それらの契約は編集できますが、Cisco DNA Center では解析や構文チェックは実行されません。Cisco DNA Center で加えた変更は、同様に Cisco ISE にも反映されます。
- Cisco ISE でポリシーに複数の SGACL がある場合、それらの契約は Cisco DNA Center のデフォルトポリシーとして移行されます。

グループベースのアクセスコントロールポリシーの作成

スケーラブルグループおよびアクセス契約は、アクセスコントロールポリシーの基本的な構成要素です。アクセスコントロールポリシーを作成する際には、前に作成したスケーラブルグループと契約を使用したり、ポリシーの作成時に新しいスケーラブルグループと契約を作成

したりできます。特定の送信元グループからアクセスできるネットワークリソースを指定する場合は、1つの送信元グループと複数の宛先グループを含むアクセスコントロールポリシーを作成できます。一方、特定のネットワークリソースへのアクセスが許可されている送信元グループを指定する場合は、1つの宛先グループと複数の送信元グループを含むアクセスコントロールポリシーを作成できます。たとえば、「請負業者」送信元スケーラブルグループに関連付けられたユーザがアクセスできるネットワークリソースを指定する場合は、1つの送信元グループと複数の宛先グループを含むアクセスコントロールポリシーを作成できます。「財務サーバ」宛先スケーラブルグループへのアクセスが許可されている送信元グループを指定する場合は、1つの宛先グループと複数の送信元グループを含むアクセスコントロールポリシーを作成できます。

グループベースのアクセスコントロールポリシーの作成

ステップ 1 [Policy List] または [Matrix] ビューで、[Create Policies] をクリックします。

ステップ 2 [Source To Destination(s)] をクリックして、単一の送信元と複数の宛先グループを含むアクセスコントロールポリシーを作成します。

- a) 選択する送信元スケーラブルグループの横にあるオプションボタンをクリックします。必要なスケーラブルグループが存在しない場合は、[Create Scalable Group] をクリックして、新しいスケーラブルグループを作成します。詳細については、「[スケーラブルグループの作成 \(196 ページ\)](#)」を参照してください。
- b) [Next] をクリックします。
- c) 選択した送信元スケーラブルグループをマッピングする必要がある、宛先のスケーラブルグループを選択します。

必要に応じて、スケーラブルグループの詳細を表示したり、スケーラブルグループを編集したりできます。

送信元と宛先の間にはポリシーがすでに存在する場合は、スケーラブルグループの近くにオレンジ色の三角形のアイコンが表示されます。

- d) [次へ (Next)] をクリックします。
- e) 選択する契約の横にあるオプションボタンをクリックします。必要な契約が存在しない場合は、[Create Contract] をクリックして新しい契約を作成します。詳細については、「[アクセス契約の作成 \(197 ページ\)](#)」を参照してください。

必要に応じて、契約の詳細を表示および編集できます。

(注) 1つのポリシーに対して1つの契約のみを選択できます。

- f) [次へ (Next)] をクリックします。

[Summary] ウィンドウには、選択したスケーラブルグループと契約に基づいて作成されたポリシーが一覧表示されます。

- g) [保存 (Save)] をクリックします。

ステップ 3 [Destination to Source(s)] をクリックして、1つの宛先と複数の送信元グループを含むアクセスコントロールポリシーを作成します。

- a) 選択する宛先スケーラブルグループの横にあるオプションボタンをクリックします。必要なスケーラブルグループが存在しない場合は、[Create Scalable Group] をクリックして、新しいスケーラブルグループを作成します。詳細については、「[スケーラブルグループの作成 \(196ページ\)](#)」を参照してください。
- b) [Next] をクリックします。
- c) 選択した宛先スケーラブルグループをマッピングする必要がある送信元スケーラブルグループを選択します。

必要に応じて、スケーラブルグループの詳細を表示したり、スケーラブルグループを編集したりできます。

送信元と宛先の間にはポリシーがすでに存在する場合は、スケーラブルグループの近くにオレンジ色の三角形のアイコンが表示されます。

- d) [次へ (Next)] をクリックします。
- e) 選択する契約の横にあるオプションボタンをクリックします。必要な契約が存在しない場合は、[Create Contract] をクリックして新しい契約を作成します。詳細については、「[アクセス契約の作成 \(197ページ\)](#)」を参照してください。

必要に応じて、契約の詳細を表示および編集できます。

(注) 1つのポリシーに対して1つの契約のみを選択できます。

- f) [次へ (Next)] をクリックします。

[Summary] ウィンドウには、選択したスケーラブルグループと契約に基づいて作成されたポリシーが一覧表示されます。

- g) [保存 (Save)] をクリックします。

(注) 拡張可能グループリスト領域の右上隅に表示される [Toggle] ボタンを使用して、[List] ビューと [Drag and Drop] ビューを切り替えることができます。[Drag and Drop] ビューを使用すると、アクセスコントロールポリシーの作成時に、スケーラブルグループを [Source] フィールドと [Destination] フィールドにドラッグアンドドロップできます。ただし、[Drag and Drop] ビューには、最初の 50 のスケーラブルグループのみが表示されます。スケーラブルグループの数が少ない場合 (最大 50) は、[Drag and Drop] ビューを使用できます。スケーラブルグループの数が多 (50 より多) い場合は、[List] ビューを使用して、すべてのスケーラブルグループを表示する必要があります。

Cisco DNA Center でポリシーを Cisco ISE と同期する場合、次のようになります。

- ポリシーが Cisco DNA Center に存在し、Cisco ISE に存在しない場合は、Cisco ISE に作成されます。
- 契約が Cisco ISE に存在し、Cisco DNA Center に存在しない場合は、Cisco DNA Center に作成されます。
- Cisco ISE のポリシー契約が異なる場合、Cisco DNA Center は Cisco ISE で指定された契約で更新されます。

- ポリシーモード情報（有効、無効、またはモニタ）も Cisco ISE からインポートされます。

Cisco ISE には、単一のポリシーに対して複数の SGACL を許可するオプションがあります（このオプションは ISE ではデフォルトでは無効になっています）。Cisco DNA Center では、単一のポリシーに対する複数のアクセス契約の使用はサポートされていません。ポリシーの同期中に、Cisco ISE のポリシーに複数の SGACL がある場合、Cisco DNA Center 管理者には、そのポリシーを変更して契約を選択しないようにするオプションが表示されます（デフォルトポリシーを使用する場合）。管理者は、ポリシーの同期が完了した後に、そのポリシーに対して新規または既存のアクセス契約を選択できます。

IP ベースのアクセスコントロールポリシー

IP ベースのアクセスコントロールポリシーは、アクセスコントロールリスト（ACL）と同じ方法でシスコデバイスに出入りするトラフィックを制御します。ACL と同様に、IP ベースのアクセスコントロールポリシーにはプロトコルタイプ、送信元 IP アドレス、宛先 IP アドレス、宛先ポート番号などのさまざまな条件に基づいてトラフィックフローに適用される許可条件および拒否条件のリストが含まれています。

IP ベースのアクセスコントロールポリシーを使用して、セキュリティ、モニタリング、ルート選択、ネットワークアドレス変換などのさまざまな目的のためにトラフィックをフィルタ処理できます。

IP ベースのアクセスコントロールポリシーには、次の2つの主要コンポーネントがあります。

- **[IP Network Groups]** : IP ネットワークグループは、同じアクセス制御要件を共有する IP サブネットで構成されています。これらのグループは Cisco DNA Center でのみ定義できます。IP ネットワークグループに含めることができる IP サブネットは1つだけです。
- **[Access Contract]** : アクセス契約は、IP ベースのアクセスコントロールポリシーとグループベースのアクセスコントロールポリシーの両方で使用される共通の構成要素です。これはアクセス制御ポリシーを構成するルールを定義します。これらのルールでは、トラフィックが特定のポートまたはプロトコルに一致したときに実行されるアクション（許可または拒否）や他のルールが一致しないときに実行される暗黙のアクション（許可または拒否）を指定します。

IP ベースのアクセスコントロールポリシー設定のワークフロー

始める前に

- **[Policy] > [IP Based Access Control] > [IP Network Groups]** ウィンドウから IP ネットワークグループを作成するには、Cisco ISE と Cisco DNA Center が統合されていることを確認します。ただし、新しい IP ベースのアクセスコントロールポリシーを作成中に、**[Policy] > [IP Based Access Control] > [IP Network Groups]** ウィンドウでグループを追加する場合は、Cisco ISE は必須ではありません。



(注) Cisco ISE なしでも、**[Policy] > [IP Based Access Control]** ウィンドウで IP ネットワークグループを編集できます。ただし、**[IP Based Access Control]** ウィンドウからの IP ネットワークグループの作成には、Cisco ISE が必要です。

- 次のグローバルネットワーク設定が定義されていることを確認し、デバイスをプロビジョニングします。
 - AAA、DHCP、DNS サーバなどのネットワークサーバ：[グローバルネットワークサーバの設定 \(162 ページ\)](#) を参照。
 - CLI、SNMP、HTTP、HTTPS などのデバイスのログイン情報：[グローバルデバイス クレデンシャルについて \(149 ページ\)](#) を参照。
 - IP アドレスプール：[IP アドレス プールを設定する \(158 ページ\)](#) を参照。
 - SSID、ワイヤレスインターフェイス、ワイヤレス無線周波数プロファイルなどのワイヤレス設定：[グローバル ワイヤレス設定の構成 \(122 ページ\)](#) を参照。
 - デバイスのプロビジョニング：[プロビジョニング \(249 ページ\)](#) を参照。

ステップ 1 IP ネットワーク グループを作成します。

詳細については、「[IP ネットワーク グループの作成 \(204 ページ\)](#)」を参照してください。

ステップ 2 IP ベースのアクセス制御契約を作成します。

IP ベースのアクセス制御契約は、送信元と宛先の間の一連のルールを定義します。これらのルールは、ネットワーク デバイスが、指定されたプロトコルまたはポートに一致するトラフィックに基づいて実行するアクション（許可または拒否）を指定します。詳細については、「[IP ベースのアクセスコントロール契約の作成 \(205 ページ\)](#)」を参照してください。

ステップ 3 IP ベースのアクセス コントロール ポリシーの作成アクセス コントロール ポリシーは、送信元と宛先の IP ネットワーク グループ間のトラフィックを制御するアクセス制御契約を定義します。

詳細については、「[IP ベースのアクセスコントロールポリシーの作成 \(206 ページ\)](#)」を参照してください。

グローバル ネットワーク サーバの設定

ネットワーク全体のデフォルトになるグローバル ネットワーク サーバを定義することができます。



(注) サイト固有の設定を定義することで、サイトのグローバル ネットワーク設定を上書きできます。

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

ステップ2 **[DHCP サーバ (DHCP Server)]** フィールドに、DHCP サーバの IP アドレスを入力します。

(注) プラスアイコンをクリックすると、IPv4 アドレスと IPv6 アドレスの両方を入力できます。

IP アドレス プールを作成するには、少なくとも 1 つの DHCP サーバを定義する必要があります。

ステップ3 **[DNS サーバ (DNS Server)]** フィールドに、DNS サーバのドメイン名を入力します。

(注) プラスアイコンをクリックすると、IPv4 アドレスと IPv6 アドレスの両方を入力できます。

IP アドレス プールを作成するために、少なくとも 1 つの DNS サーバを定義する必要があります。

ステップ4 (任意) Syslog、SNMP トラップ、および NetFlow コレクタ サーバ情報を入力できます。**[サーバの追加 (Add Servers)]** をクリックして NTP サーバを追加します。

(注) ファブリック コンプライアンス チェックをトリガするには、Cisco DNA Center の IP アドレスを使用して SNMP サーバを設定します。詳細については、[ファブリックへのデバイスの追加](#)を参照してください。

ステップ5 **[保存 (Save)]** をクリックします。

IP ネットワーク グループの作成

ステップ1 Cisco DNA Center ホームページで、**[ポリシー (Policy)] >> [IP ベースのアクセスコントロール (IP Based Access Control)] >> [IP ネットワーク グループ (IP Network Groups)]** の順に選択します。

ステップ2 **[グループの追加 (Add Group)]** をクリックします。

ステップ3 **[名前 (Name)]** フィールドに、IP ネットワーク グループの名前を入力します。

ステップ4 **[説明 (Description)]** フィールドに、IP ネットワーク グループを説明する単語またはフレーズを入力します。

ステップ5 **[IP アドレスまたは IP/CIDR (IP Address or IP/CIDR)]** フィールドに、IP ネットワーク グループを構成する IP アドレスを入力します。

ステップ6 **[保存 (Save)]** をクリックします。

IP ネットワーク グループの編集または削除

- ステップ 1** Cisco DNA Center ホームページで、[ポリシー (Policy)] > > [IP ベースのアクセスコントロール (IP Based Access Control)] > > [IP ネットワーク グループ (IP Network Groups)] の順に選択します。
- ステップ 2** [IP ネットワーク グループ (IP Network Groups)] テーブルで、編集または削除するグループの横にあるチェックボックスをオンにします。
- ステップ 3** 次のいずれか 1 つのタスクを実行します。
- グループを変更するには、[編集 (Edit)] をクリックします。フィールドの定義については、[IP ネットワーク グループの作成 \(204 ページ\)](#) を参照してください。
 - グループを削除するには、[削除 (Delete)] をクリックし、次に [はい (Yes)] をクリックして確定します。

IP ベースのアクセスコントロール契約の作成

- ステップ 1** Cisco DNA Center のホームページで、[Policy] > [IP Based Access Control] > [Access Contract] の順に選択します。
- ステップ 2** [コントラクトの追加 (Add Contract)] をクリックします。
- ステップ 3** ダイアログボックスに、契約の名前と説明を入力します。
- ステップ 4** [暗黙的アクション (Implicit Action)] ドロップダウンリストから、[拒否 (Deny)] または [許可 (Permit)] を選択します。
- ステップ 5** テーブルの [アクション (Action)] ドロップダウンリストから、[拒否 (Deny)] または [許可 (Permit)] を選択します。
- ステップ 6** [ポート/プロトコル (Port/Protocol)] ドロップダウンリストから、ポートまたはプロトコルを選択します。
- a) Cisco DNA Center に必要なポートまたはプロトコルがない場合は、[ポート/プロトコルの追加 (Add Port/Protocol)] をクリックして、自分で作成します。
 - b) [名前 (Name)] フィールドで、ポートまたはプロトコルの名前を入力します。
 - c) [プロトコル (Protocol)] ドロップダウンリストで、[UDP]、[TDP]、または [TCP/UDP] を、プロトコルとして選択します。
 - d) [ポート範囲 (Port Range)] フィールドにポート範囲を入力します。
 - e) Cisco DNA Center で定義したとおりにポートまたはプロトコルを設定し、競合をレポートしないようにするには、[競合を無視する (Ignore Conflict)] チェックボックスをオンにします。
- ステップ 7** (任意) 契約にさらにルールを含めるには、[追加 (Add)] をクリックして、手順 5 および 6 を繰り返します。
- ステップ 8** [保存 (Save)] をクリックします。

Edit or Delete an IP-Based Access Control Contract

ポリシーで使用されている契約を編集すると、**[IP ベースのアクセスコントロール ポリシー (IP Based Access Control Policies)]** ウィンドウのポリシーの状態が **[変更 (MODIFIED)]** に変わります。変更されたポリシーは、ネットワークに導入されたポリシーと一致しないため、古いと見なされます。この問題を解決するには、ネットワークにポリシーを再展開する必要があります。

ステップ 1 Cisco DNA Center のホームページで、**[ポリシー (Policy)] > [IP ベースのアクセスコントロール (IP Based Access Control)] > [契約へのアクセス (Access Contract)]** の順に選択します。

ステップ 2 編集または削除する契約の横にあるチェックボックスをオンにして、次のいずれかのタスクを実行します。

- 契約を変更するには、**[編集 (Edit)]** をクリックして変更を行い、**[保存 (Save)]** をクリックします。フィールドの定義については、**IP ベースのアクセスコントロール契約の作成 (205 ページ)** を参照してください。

(注) ポリシーで使用されている契約を変更した場合は、**[ポリシー (Policy)] > [IP ベースのアクセスコントロール (IP-Based Access Control)] > [IP ベースのアクセスコントロール ポリシー (IP-Based Access Control Policies)]** の順に選択し、ポリシー名の横にあるチェックボックスをオンにして、**[展開 (Deploy)]** をクリックすることによって、変更したポリシーを展開する必要があります。

- 契約を削除するには、**[削除 (Delete)]** をクリックします。

IP ベースのアクセスコントロールポリシーの作成

IP ネットワーク グループ間のトラフィックを制限する、IP ベースのアクセスコントロールポリシーを作成します。

- 1 つのポリシーに異なる設定で複数のルールを追加することができます。
- IP グループと契約の分類子の特定の組み合わせでルールが作成され、デバイスにプッシュされます。この数は、Cisco WLC が ACL でのルールを最大 64 に制限しているため、64 個のルールを超えることはできません。
- **展開された** ポリシー内で使用されるカスタム契約または IP グループが変更された場合、そのポリシーは古いものであり、デバイスにプッシュする新しい設定のために再展開される必要があることを示す **[変更済み (Modified)]** というステータスでフラグが付けられます。

ステップ 1 Cisco DNA Center のホームページで、**[ポリシー (Policy)] > [IP ベースのアクセスコントロール (IP Based Access Control)] > [IP ベースのアクセスコントロールポリシー (IP Based Access Control Policy)]** の順に選択します。

ステップ2 [ポリシーの追加 (Add Policy)] をクリックします。

ステップ3 次のフィールドに入力します。

フィールド	説明
Policy Name	ポリシーの名前。
Description	ポリシーを表す単語またはフレーズ。
SSID	<p>SSID の設計中に作成された FlexConnect SSID および 非 FlexConnect SSID をリストします。選択した SSID が FlexConnect モードで設定されている場合、アクセスポリシーも FlexConnect モードで設定されます。そうでない場合は、通常の方法で設定されます。</p> <p>(注) SSID が 1 つのポリシーの一部である場合は、その SSID は別のポリシーで使用できません。</p> <p>ポリシーの展開には有効なサイト SSID の組み合わせが必要です。選択した SSID がデバイスの下でプロビジョニングされていない場合、ポリシーを展開することはできません。</p>
Site Scope	<p>サイトのポリシーが適用される範囲。有線ポリシーを設定すると、ポリシーは、サイト範囲内のすべての有線デバイスに適用されます。同様に、選択したサービスセット識別子 (SSID) のワイヤレス ポリシーを設定すると、範囲内で SSID が定義されているすべてのワイヤレス デバイスにポリシーが適用されます。詳細については、サイトの範囲 (210 ページ) を参照してください。</p>
Source	<p>契約の影響を受けるトラフィックの送信元。[送信元の検索 (SearchSource)] ドロップダウンリストから、IP ネットワーク グループを選択します。使用したい IP ネットワークがない場合は、[+グループの追加 (+Group)] をクリックして作成します。</p>
Contract	<p>ACL 内で送信元と宛先間のネットワーク連携を管理するルール。[契約の追加 (Add Contract)] をクリックして、ポリシーの契約を定義します。ダイアログボックスで、使用する契約の横にあるラジオ ボタンをクリックします。または、契約の [許可 (permit)] (すべてのトラフィックを許可) または [拒否 (deny)] (すべてのトラフィックを拒否) を選択することもできます。</p>
Destination	<p>契約の影響を受けるトラフィックの宛先。[宛先 (Destination)] ドロップダウンリストをクリックして、IP ネットワーク グループを選択します。使用したい IP ネットワークがない場合は、[+IP ネットワーク グループの作成 (+Create IP Network Group)] をクリックして作成します。</p>
Direction	<p>送信元と宛先間のトラフィックフローの関係を設定します。送信元から宛先へのトラフィックフローの契約を有効にするには、[一方向 (One-Way)] を選択します。両方向 (送信元から宛先へ、および宛先から送信元へ) でのトラフィックフローの契約を有効にするには、[双方向 (Bi-directional)] を選択します。</p>

ステップ4 (任意) IP ネットワーク グループを作成するには、[IP ネットワーク グループの作成 (Create IP Network Group)] をクリックします。

ステップ5 (任意) 別のルールを追加するには、プラス記号をクリックします。

(注) ルールを削除するには、[x] をクリックします。

ステップ6 (任意) ルールの順序を変更するには、変更したい順序でルールをドラッグアンドドロップします。

ステップ7 [展開 (Deploy)] をクリックします。

「IP ベースのアクセス コントロール ポリシーが作成され、正常に展開されました (IP-Based Access Control Policy has been created and deployed successfully)」という成功メッセージが表示されます。選択した SSID によっては、FlexConnect ポリシーまたは標準ポリシーが異なるマッピング情報レベルで作成され、展開されます。ポリシーの[ステータス (Status)] は、[展開済み (DEPLOYED)] として表示されます。[ポリシー名 (Policy Name)] の横にあるワイヤレスアイコンは、展開されたアクセス ポリシーがワイヤレス ポリシーであることを示しています。

IP ベースのアクセスコントロールポリシーの編集または削除

必要な場合は、IP ベースのアクセスコントロールポリシーを変更または削除できます。



- (注) ポリシーを編集すると、[IPベースのアクセスコントロールポリシー (IP-Based Access Control Policies)] ウィンドウのポリシーの状態が[変更 (MODIFIED)] に変わります。変更されたポリシーは、ネットワークに導入されたポリシーと一致しないため、古いと見なされます。この問題を解決するには、ネットワークにポリシーを再展開する必要があります。

ステップ1 Cisco DNA Center のホームページで、[Policy] > [IP Based Access Control] > [IP Based Access Control Policies] の順に選択します。

ステップ2 編集または削除するポリシーの横にあるチェックボックスをオンにして、次のいずれかのタスクを実行します。

- 変更するには、[編集 (Edit)] をクリックします。完了したら、[Save] をクリックします。フィールドの定義については、[IP ベースのアクセスコントロールポリシーの作成 \(206 ページ\)](#) を参照してください。
- ポリシーを削除するには、[削除 (Delete)] をクリックします。

ステップ3 ポリシーを変更した場合は、ポリシー名の横にあるチェックボックスをオンにして[展開 (Deploy)] をクリックすることによって、変更したポリシーを展開します。

IP ベースのアクセスコントロールポリシーの展開

ポリシーの設定に影響する変更を加えた場合は、これらの変更を実装するポリシーを再度展開する必要があります。

ステップ 1 Cisco DNA Center のホームページで、**[Policy] > [IP Based Access Control] > [IP Based Access Control Policies]** の順に選択します。

ステップ 2 展開するポリシーを探します。

ステップ 3 ポリシーの横にあるチェック ボックスをオンにします。

ステップ 4 **[展開 (Deploy)]** をクリックします。

ポリシーを今すぐ展開するか、または後でスケジュールするかどうかを求められます。

ステップ 5 次のいずれかを実行します。

- ポリシーをすぐに展開するには、**[今すぐ実行 (Run Now)]** ラジオ ボタンをクリックし、**[適用 (Apply)]** をクリックします。
- 将来の日付と時刻でポリシー展開をスケジュールするには、**[後でスケジュール (Schedule Later)]** ラジオ ボタンをクリックし、展開する日時を定義します。

(注) アプリケーションポリシーの展開のスケジュール設定では、サイトのタイムゾーンの設定はサポートされていません。

アプリケーションポリシー

Quality of Service (QoS) とは、選択したネットワーク トラフィックに、優先的なサービスやニーズに合ったサービスを提供するネットワーク機能を意味します。QoS を設定することで、ビジネスの目標（音声品質が会社の標準規格を満たしていることの保証、ビデオの高い Quality of Experience (QoE) の確保など）を引き続き順守しながら、ネットワーク リソースを最も効率的に使用する方法でネットワーク トラフィックを処理することができます。

QoS は、Cisco DNA Center のアプリケーションポリシーを使用してネットワークに設定できます。アプリケーションポリシーは、次の基本的なパラメータで構成されています。

- **[アプリケーションセット (Application Sets)]** : 同様のネットワーク トラフィックを必要とする一連のアプリケーション。各アプリケーションセットには、トラフィックの優先順位を定義するビジネスとの関連性グループ（ビジネス関連、デフォルト、またはビジネスと無関係）が割り当てられます。QoS パラメータは、Cisco Validated Design (CVD) に基づいて3つのグループごとに定義されます。一部のパラメータは、それぞれの目的に合わせて変更できます。詳細については、「[アプリケーションおよびアプリケーションセット \(351 ページ\)](#)」を参照してください。
- **[サイトの範囲 (Site Scope)]** : アプリケーションポリシーが適用されているサイト。有線ポリシーを設定すると、ポリシーは、サイト範囲内のすべての有線デバイスに適用されま

す。同様に、選択したサービスセット識別子（SSID）のワイヤレスポリシーを設定すると、範囲内で SSID が定義されているすべてのワイヤレスデバイスにポリシーが適用されます。詳細については、[サイトの範囲（210 ページ）](#) を参照してください。

Cisco DNA Center はこれらのパラメータをすべて受け取り、適切なデバイスの CLI コマンドに変換します。Cisco DNA Center はポリシーの展開時に、サイトの範囲で定義されているデバイスに各コマンドを設定します。



(注) Cisco DNA Center はデバイスで使用可能な QoS 機能セットに基づいて、各デバイスに QoS ポリシーを設定します。デバイスの QoS 実装の詳細については、対応するデバイスの製品マニュアルを参照してください。

アプリケーションポリシーでの CVD ベースの設定

アプリケーションポリシーのデフォルトの QoS 信頼およびキューイング設定は、Enterprise Medianet の QoS デザイン向けの Cisco Validated Design (CVD) に基づいています。CVD は、一般的な使用例や現行のシステム設計上の優先事項に基づき、システム設計の基盤を提示しています。CVD には、お客様のニーズに応じるための幅広いテクノロジー、機能、アプリケーションが組み込まれています。それぞれのソリューションには、エンジニアによる包括的なテストと文書化が実施されており、迅速で、信頼性が高く、予測可能な導入が確保されています。

QoS に関連する最新の検証済み設計は、Cisco Press の書籍『*End-to-End QoS Network Design: Quality of Service for Rich-Media & Cloud Networks, 2nd Edition*』

(<http://www.ciscopress.com/store/end-to-end-qos-network-design-quality-of-service-for-9781587143694>) で公開されています。追加情報については、次のシスコのドキュメントを参照してください。

- [シスコ検証済みデザイン \(CVD\)](#)
- [Enterprise Medianet Quality of Service Design 4.0](#)
- [Medianet Campus QoS Design 4.0](#)
- [Medianet WAN Aggregation QoS Design 4.0](#)

サイトの範囲

サイト範囲は、アプリケーションポリシーが適用されるサイトを定義します。ポリシーを定義するときに、ポリシーが有線デバイス用かワイヤレスデバイス用かを設定します。また、サイト範囲も設定します。有線ポリシーを設定すると、ポリシーは、サイト範囲内のすべての有線デバイスに適用されます。同様に、選択したサービスセット識別子（SSID）のワイヤレスポリシーを設定すると、サイト範囲内で SSID が定義されている、サイト範囲内のすべてのワイヤレスデバイスにポリシーが適用されます。

これにより、有線ネットワーク セグメントとワイヤレス ネットワークセグメントの動作の相違を補うために、必要に応じてトレードオフを実施できます。たとえば、ワイヤレス ネットワークでは通常、有線ネットワークと比較した場合に低帯域幅、低速、パケット損失増加の特徴があります。個々のワイヤレスセグメントは、ローカルのRF干渉、輻輳、ネットワーク デバイスの機能の違いなどの要因によってさらに変動が見られます。個々のワイヤレスセグメントにセグメントごとのポリシーを適用できるすることで、優先順位の高いトラフィックが受ける、ワイヤレスネットワークの劣化による影響が小さくなるように、トラフィック処理ルールを調整できます。

ビジネス関連のグループ

ビジネス関連グループは、ビジネスや事業への関連性に応じて、指定されたアプリケーション セットを分類します。

ビジネス関連グループ（ビジネス関連、デフォルト、ビジネスと無関係）は、基本的に3種類のトラフィック（高優先順位、ニュートラル、低優先順位）にマッピングされます。

- **[Business Relevant]**：（高優先トラフィック）このグループのアプリケーションは組織の目的に直接関与するもので、たとえば、音声、ビデオ、ストリーミングやコラボレーション型マルチメディア アプリケーション、データベース アプリケーション、エンタープライズリソース アプリケーション、電子メール、ファイル転送、コンテンツ配布などの様々なアプリケーションが含まれます。ビジネス関連として指定されているアプリケーションは、Internet Engineering Task Force (IETF) RFC 4594 の規定に従い、業界推奨のベストプラクティスに従って処理されます。
- **[Default]**：（ニュートラルトラフィック）このグループは、ビジネスに関連していてもいなくてもよいアプリケーションを対象としています。たとえば、一般的なHTTPまたはHTTPS トラフィックは、組織の目的に寄与する場合もしない場合もあります。たとえば、レガシーアプリケーションや新しく導入されたアプリケーションなどでも、一部のアプリケーションの目的については分析していない場合があります。したがって、これらのアプリケーションのトラフィック フローは、IETF RFC 2747 および 4594 で説明されているように、デフォルトの転送サービスで処理する必要があります。
- **[Business Irrelevant]**：（低優先順位トラフィック）このグループは、組織の目的達成に関与しないと識別されたアプリケーションを対象としています。主にコンシューマ向けかエンターテインメント向け、あるいは本質的にその両方に該当するアプリケーションです。この種類のトラフィックは、IETF RFC 3662 および 4594 で説明されている「スカベンジャ」サービスとして処理することをお勧めします。

アプリケーションはアプリケーションセットに分類されて、ビジネス関連グループにソートされます。アプリケーションセットはポリシーに現状のまま含めることができます。または、ビジネス目標やネットワーク構成のニーズを満たすように変更することができます。

たとえば、YouTube はコンシューマ メディア アプリケーションセットのメンバーです。一般的に、ほとんどのお客様がこのアプリケーションをこのように分類しているため、（デフォルトでは）YouTubeはビジネスと無関係です。ただし、この分類がすべての企業に当てはまるわけではありません。たとえば、いくつかのビジネスでは YouTube をトレーニング目的で使用

することがあります。このような場合、管理者は、デフォルトでビジネス関連であるストリーミングビデオアプリケーションセットに YouTube アプリケーションを移動できます。

コンシューマとプロデューサ

あるアプリケーションから別のアプリケーションにトラフィックが送られた（特定の a から b へのトラフィックフローが作成された）ときにトラフィックが特定の方法で処理されるように、アプリケーション間の関係を設定することができます。このような関係のアプリケーションをプロデューサとコンシューマと呼び、次のように定義しています。

- **プロデューサ**：アプリケーショントラフィックの送信元。たとえば、クライアント/サーバアーキテクチャでは、トラフィックフローは主にサーバからクライアントの方向であるため、アプリケーションサーバがプロデューサと見なされます。ピアツーピアアプリケーションの場合は、リモートピアがプロデューサと見なされます。
- **コンシューマ**：アプリケーショントラフィックの受信者。コンシューマに該当するのは、クライアント/サーバアーキテクチャの場合はクライアントエンドポイント、ピアツーピアアプリケーションの場合はローカルデバイスなどです。コンシューマはエンドポイントデバイスであることがありますが、場合によっては、そのようなデバイスの特定のユーザであることもあります（通常、IP アドレスまたは特定のサブネットによって識別される）。また、あるアプリケーションが別のアプリケーショントラフィックフローのコンシューマになる場合もあります。

このような関係を設定することにより、このシナリオに一致するトラフィックに特定のサービスレベルを設定することが可能になります。

マーキング、キューイング、ドロップिंगの処理

Cisco DNA Center は、IETF RFC 4594 およびアプリケーションに割り当てられたビジネス関連のカテゴリでの処理のマーキング、キューイング、およびドロップングをベースとしています。Cisco DNA Center は、デフォルトカテゴリのすべてのアプリケーションをデフォルトの転送アプリケーションクラスに割り当て、無関係なビジネスカテゴリのすべてのアプリケーションをスカベンジャアプリケーションクラスに割り当てます。関連するビジネスカテゴリのアプリケーションについては、Cisco DNA Center はアプリケーションのタイプに基づいてトラフィッククラスをアプリケーションに割り当てます。次の表に、アプリケーションクラスとそれぞれの処理を示します。

表 38: マーキング、キューイング、ドロップングの処理

ビジネス関連性	アプリケーションクラス	ホップ毎の挙動	キューイングとドロップング	アプリケーションの説明
該当する	VoIP ¹	Expedited Forwarding (EF)	プライオリティキューイング (PQ)	VoIP テレフォニー (ベアラのみ) トラフィック。たとえば、Cisco IP 電話。
	ブロードキャストビデオ	クラス セレクタ (CS) 5	PQ	ブロードキャスト TV、ライブイベント、ビデオ監視フロー、同様の非弾性ストリーミングメディアフロー (Cisco IP Video Surveillance や Cisco Enterprise TV など)。(非弾性フローとは、非常にドロップされやすく、再送信またはフロー制御機能のいずれか、または両方がないフローを意味します。)
	リアルタイムインタラクティブ	CS4	PQ	非弾性の高解像度インタラクティブ ビデオアプリケーションおよびそれらのアプリケーションのオーディオおよびビデオコンポーネント (Cisco TelePresence など)。
	マルチメディア会議	相対的優先転送 (AF) 41	帯域幅 (BW) キューと Differentiated Services Code Point (DSCP) Weighted Random Early Detect (WRED)	デスクトップソフトウェアのマルチメディアコラボレーションアプリケーションおよびそれらのアプリケーションのオーディオおよびビデオコンポーネント (Cisco Jabber や Cisco Webex など)。
	マルチメディアストリーミング	AF31	BW キューと DSCP WRED	ビデオオンデマンド (VoD) ストリーミングビデオフローおよび仮想デスクトップアプリケーション。例えば、Cisco Digital Media System。
	ネットワーク制御	CS6	BW キューのみ ²	EIGRP、OSPF、BGP、HSRP、IKE などのエンタープライズネットワークの信頼性の高い運用のために必要とされるネットワークコントロールプレーントラフィック。
	シグナリング	CS3	BW キューと DSCP	IP 音声およびビデオテレフォニー インフラストラクチャのコントロールプレーントラフィック。
	Operations, Administration, and Management (OAM)	CS2	BW キューと DSCP ³	SSH、SNMP、syslog などのネットワーク運用、管理、管理トラフィック
	AF21			

ビジネス関連性	アプリケーションクラス	ホップ毎の挙動	キューイングとドロッピング	アプリケーションの説明
	トランザクションデータ (低遅延データ)		BW キューと DSCP WRED	エンタープライズ リソース プランニング (ERP)、顧客関係管理 (CRM)、およびその他のデータベースアプリケーションなどのインタラクティブ (フォアグラウンド) データアプリケーション。
	バルクデータ (高スループットデータ)	AF11	BW キューと DSCP WRED	電子メール、File Transfer Protocol (FTP)、バックアップアプリケーションなどの非インタラクティブ (バックグラウンド) データアプリケーション。
デフォルト	デフォルトの転送 (ベストエフォート)	DF	デフォルトキューと RED	デフォルトのアプリケーション、およびデフォルトのビジネス関連グループに割り当てられるアプリケーション。プライオリティ、保証された帯域幅、または差分サービスクラスに割り当てられるのはごく少数のアプリケーションであるため、大部分のアプリケーションは引き続きデフォルトでベストエフォート型サービスになります。
非関連	スカベンジャー	CS1	最小 BW キュー (ディファレンシャル) と DSCP	非ビジネス関連のトラフィックフロー、およびビジネス関連でないグループに割り当てられているアプリケーション (エンターテイメント向けのデータやメディア アプリケーションなど)。たとえば、YouTube、Netflix、iTunes、Xbox Live。

¹ VoIP シグナリングトラフィックは、コールシグナリングクラスに割り当てられます。

² ネットワーク制御トラフィックはドロップされるべきではないため、このクラスでは WRED が有効になりません。

³ OAM トラフィックはドロップされるべきではないため、このクラスでは WRED が有効になりません。

サービス プロバイダーのプロファイル

サービス プロバイダー (SP) プロファイルは、特定の WAN プロバイダーのサービス クラスを定義します。4 クラス、5 クラス、6 クラス、8 クラスのモデルを定義できます。

アプリケーションポリシーがデバイスに展開されると、各 SP プロファイルには、各 SP クラスを DSCP 値と帯域幅割当てのパーセンテージにマップする特定のサービス レベル契約 (SLA) が割り当てられます。

アプリケーションポリシーを設定するときに SP プロファイルの DSCP 値と帯域幅割当てのパーセンテージをカスタマイズできます。

SP プロファイルを作成したら、そのプロファイルを WAN インターフェイスで設定する必要があります。

表 39: 4クラスでの SP プロファイルのデフォルト SLA 属性

クラス名	DSCP	プライオリティ クラス	SLA	
			帯域幅 (%)	Remaining Bandwidth (%)
音声	EF	はい	10	—
クラス 1 データ	AF31	—	—	44
クラス 2 データ	AF21	—	—	25
デフォルト	0	—	—	31

表 40: 5クラスでの SP プロファイルのデフォルト SLA 属性

クラス名	DSCP	プライオリティ クラス	SLA	
			帯域幅 (%)	Remaining Bandwidth (%)
音声	EF	はい	10	—
クラス 1 データ	AF31	—	—	44
クラス 2 データ	AF21	—	—	25
クラス 3 データ	AF11	—	—	1
デフォルト	ベスト エフォート	—	—	30

表 41: 6クラスでの SP プロファイルのデフォルト SLA 属性

クラス名	DSCP	プライオリティ クラス	SLA	
			帯域幅 (%)	Remaining Bandwidth (%)
クラス 1 データ	AF31	—	—	10
クラス 3 データ	AF11	—	—	1
ビデオ	AF41	—	—	34
音声	EF	はい	10	—
デフォルト	0	—	—	30

クラス名	DSCP	プライオリティ クラス	SLA	
			帯域幅 (%)	Remaining Bandwidth (%)
クラス 2 データ	AF21	—	—	25

表 42: 8 クラスでの SP プロファイルのデフォルト SLA 属性

クラス名	DSCP	プライオリティ クラス	SLA	
			帯域幅 (%)	Remaining Bandwidth (%)
ネットワーク-コ ントロール管理	CS6	—	—	5
ストリーミング ビデオ	AF31	—	—	10
コール シグナリ ング	CS3	—	—	4
スカベンジャー	CS1	—	—	1
インタラクティブ ビデオ	AF41	—	—	30
音声	EF	はい	10	—
デフォルト	0	—	—	25
重要なデータ	AF21	—	—	25

キューイング プロファイル

キューイング プロファイルでは、インターフェイス速度とトラフィック クラスに基づいたインターフェイスの帯域幅割り当てを定義することができます。



(注) キューイング プロファイルは、サービス プロバイダー プロファイルに接続されている WAN 側インターフェイスには適用されません。

次のインターフェイス速度がサポートされます。

- 100 Gbps
- 10/40 Gbps
- 1 Gbps

- 100 Mbps
- 10 Mbps
- 1 Mbps

インターフェイスの速度が 2 つのインターフェイス速度の間である場合、Cisco DNA Center は、より低いインターフェイス速度でインターフェイスを取り扱います。



(注) Cisco DNA Center は、正しいポリシーを適用するためにインターフェイスの動作速度の検出を試みます。ただし、スイッチポートが管理上ダウンしている場合、Cisco DNA Center は速度を検出できません。この場合、Cisco DNA Center は、インターフェイスのサポートされた速度を使用します。

キューイング ポリシーは、アプリケーション ポリシーの一部として定義します。アプリケーションポリシーを展開すると、サイト範囲内の選択されたサイトのデバイスが、割り当てられた LAN キューイング ポリシーで設定されます。LAN キューイング ポリシーが割り当てられていない場合、アプリケーションポリシーはデフォルトの CVD キューイング ポリシーを使用します。

すでに展開されているアプリケーションポリシーのキューイングポリシーを変更すると、ポリシーは失効し、変更をデバイスに適用するにはポリシーを展開しなおす必要があります。

キューイングポリシーに関する次の追加の注意事項および制約事項に注意してください。

- LAN キューイングプロファイルは、ポリシーで使用されている場合には削除できません。
- ポリシーに関連付けられているキューイングプロファイルを更新すると、ポリシーは期限切れとしてマーキングされます。最新の変更をプロビジョニングするには、ポリシーを展開しなおす必要があります。
- トラフィッククラスキューイングをカスタマイズしても、シスコのサービスプロバイダースイッチおよびルータのインターフェイスは影響を受けません。これらのインターフェイスの設定は、引き続き Cisco DNA Center を使用することなく実施します。

表 43: デフォルト CVD LAN キューイング ポリシー

トラフィック クラス	デフォルトの帯域幅 (合計= 100%) ⁴
音声	10 %
ブロードキャスト ビデオ	10 %
リアルタイム インタラクティブ	13 %
マルチメディア会議	10 %
マルチメディア ストリーミング	10 %
ネットワーク制御	3 %

トラフィック クラス	デフォルトの帯域幅 (合計= 100%) ⁴
シグナリング	2 %
OAM	2 %
トランザクション データ	10 %
バルク データ	4 %
スカベンジャー	1 %
ベスト エフォート	25 %

⁴ 音声、ブロードキャストビデオ、およびリアルタイムインタラクティブトラフィッククラスの合計帯域幅を 33% 以下にすることを推奨します。

リソースが制限されているデバイスの処理順

ネットワーク デバイスの中には、ネットワーク アクセス コントロール リスト (ACL) および ACE を格納するためのメモリ (TCAM と呼ばれる) が制限されているものがあります。このため、アプリケーション用の ACL と ACE がこれらのデバイス上に設定されている場合は、利用可能な TCAM 領域が使用されます。When the TCAM space is depleted, QoS settings for additional applications cannot be configured on that device.

そのようなデバイスで最も重要なアプリケーションの QoS ポリシーが確実に設定されるように、Cisco DNA Center は次の順序で TCAM スペースを割り当てます。

1. [Rank] : カスタムアプリケーションおよびお気に入りのアプリケーションに割り当てられた番号 (ただし既存のデフォルト NBAR アプリケーションは除く)。ランクの番号が小さくなるほど、優先順位が高くなります。たとえば、ランク 1 のアプリケーションはランク 2 のアプリケーションよりも優先順位が高くなります。ランクがない場合は、優先順位が最も低くなります。



- (注)
- カスタム アプリケーションには、デフォルトでランク 1 が割り当てられています。
 - NBAR アプリケーションをお気に入りとしてマークすると、ランクは 1000 に設定されます。
2. [Traffic Class] : 優先順位は次の順序に基づいています。シグナリング、バルクデータ、ネットワーク制御、Operations Administration Management (Ops Admin Mgmt)、トランザクションデータ、スカベンジャー、マルチメディアストリーミング、マルチメディア会議、リアルタイムインタラクティブ、ブロードキャストビデオ、VoIP テレフォニー。
 3. [Popularity] : CVD の基準に基づいて割り当てられた番号 (1 ~ 10)。ポピュラリティの番号は変更できません。ポピュラリティが 10 のアプリケーションは、ポピュラリティが 9 のアプリケーションよりも優先順位が高くなります。



- (注)
- カスタムアプリケーションには、ポピュラリティ 0 が割り当てられます。
 - デフォルト NBAR アプリケーションには、CVD の基準に基づいてポピュラリティ番号 (1 ~ 10) が割り当てられます。アプリケーションをお気に入りとしてマークしても、ポピュラリティ番号は変わりません (ランクのみ変更されます)。
-
4. [Alphabetization] : 2 つ以上のアプリケーションのランクとポピュラリティ番号が同一の場合、それらのアプリケーションはアプリケーション名のアルファベット順にソートされ、ソート順に従い優先順位が割り当てられます。

たとえば、次のアプリケーションを指定したポリシーを定義する場合を想定しましょう。

- カスタム アプリケーション `custom_realtime`。デフォルトでランク 1 とポピュラリティ 10 が割り当てられています。
- カスタム アプリケーション `custom_salesforce`。デフォルトでランク 1 とポピュラリティ 10 が割り当てられています。
- `corba-iiop` という名前のトランザクション データ トラフィック クラスのアプリケーション。お気に入りとして指定されており、ランク 10,000、および (CVD に基づいて) ポピュラリティ 9 が付与されています。
- `gss-http` という名前の Ops Admin Mgmt トラフィック クラスのアプリケーション。お気に入りとして指定されており、ランク 10,000、および (CVD に基づいて) ポピュラリティ 10 が付与されています。
- 他のすべてのデフォルト NBAR アプリケーションにはランクはありませんが、トラフィック クラスと (CVD に基づいて) デフォルト ポピュラリティに従って処理されます。

優先順位付けのルールに従って、アプリケーションはデバイスにおいて次の順序で設定されます。

アプリケーションの設定順	理由
1. カスタム アプリケーション <code>custom_realtime</code>	カスタム アプリケーションには最も高い優先順位が付与されます。 <code>custom_salesforce</code> アプリケーションと <code>custom_realtime</code> アプリケーションのランクおよびポピュラリティが同じであるとする、これらのアプリケーションはアルファベット順にソートされ、 <code>custom_realtime</code> が <code>custom_salesforce</code> より前になります。
2. カスタム アプリケーション <code>custom_salesforce</code>	

アプリケーションの設定順	理由
3. お気に入りのアプリケーション gss-http	これら両方のアプリケーションはお気に入りとして指定されているため、同じアプリケーション ランクになります。そのため、Cisco DNA Center は各アプリケーションをトラフィック クラスに基づいて評価します。gss-http は、Ops Admin Mgmt トラフィック クラスであるため、先に処理され、その後にトランザクションデータ トラフィック クラスの corba-iiop アプリケーションが処理されます。トラフィック クラスによって処理順が決まっているため、ポピュラリティは考慮されません。
4. お気に入りのアプリケーション corba-iiop	
5. 他のすべてのデフォルト NBAR アプリケーション	他のすべてのアプリケーションは、トラフィック クラスとポピュラリティに従って次に優先され、ポピュラリティが同じアプリケーションは、アプリケーション名のアルファベット順にソートされます。

ポリシーのドラフト

ポリシーを作成するときに、ポリシーを展開せずにドラフトとして保存できます。ドラフトとして保存すると、後でポリシーを開いて変更できます。また、展開したポリシーを変更して、ドラフトとして保存することもできます。



(注) ポリシーを保存または展開した後に、名前を変更することはできません。

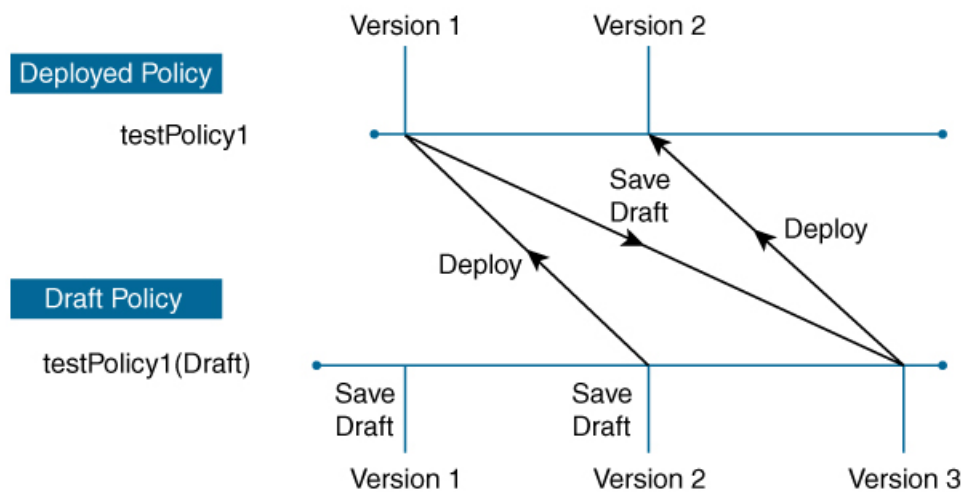
ドラフト ポリシーと展開したポリシーは相互に関連付けられますが、次のように独自にバージョン管理されます。

ポリシーをドラフトとして保存すると、Cisco DNA Center はポリシー名に (Draft) を追加してバージョン番号を 1 つ上げます。ポリシーを展開すると、Cisco DNA Center が展開したポリシーのバージョン番号を 1 つ上げます。

たとえば、次の図に示すように、testPolicy1 という名前のポリシーを作成してドラフトとして保存します。ポリシーは testPolicy1 (Draft)、バージョン番号 1 として保存されます。ドラフトを変更して、再度保存します。ポリシーの名前は同じ testPolicy1 (Draft) のままですが、バージョン番号は 2 に上がります。

ポリシーが気に入ったのでネットワークに展開します。ポリシーは testPolicy1 という名前で展開され、バージョン番号は 1 です。展開したポリシーを変更して、ドラフトとして保存します。ドラフト ポリシー testPolicy1 (Draft) は、バージョン番号 3 に上がります。最終的にそのバージョンを展開するとき、testPolicy1 はバージョン 2 になります。

図 4: 展開したポリシーとドラフトポリシーのバージョン管理



ドラフトポリシーまたは展開したポリシーのいずれかを変更および保存するときは、ドラフトポリシーのバージョン番号が上がります。同様に、ドラフトポリシーまたは変更した展開済みポリシーのいずれかを展開するときは、展開したポリシーのバージョンが上がります。

展開したポリシーと同様に、ドラフトポリシーの履歴を表示し、以前のバージョンにロールバックすることができます。

ポリシーバージョンの履歴表示と以前のバージョンへのロールバックについては、[ポリシーのバージョン管理](#) (222 ページ) を参照してください。

ポリシーのプレビュー

ポリシーを展開する前に、デバイスに適用される CLI を生成できます。

プレビュー操作では、ポリシーの CLI コマンドが生成され、デバイスの実行コンフィギュレーションの CLI コマンドと比較され、デバイスでポリシーを設定するのに必要な残りの CLI だけが返されます。

プレビュー出力の確認後、範囲内の全デバイスにポリシーを展開するか、ポリシーの変更を続行することができます。

ポリシーの事前チェック

アプリケーションポリシーを作成するとき、ポリシーを展開する前に、サイト範囲のデバイスでサポートされるかどうかを確認できます。事前チェック機能では、デバイスタイプ、モデル、ラインカード、およびソフトウェアイメージが作成したアプリケーションポリシーをサポートするかどうかをチェックします。これらのコンポーネントのいずれかがサポートされず Cisco DNA Center されていない場合、はデバイスの障害を報告します。Cisco DNA Center また、障害を修正する方法についても説明します。これらの対応で障害が修正されない場合、サイト範囲からデバイスを削除できます。

アプリケーションポリシーをそのまま展開すると、事前チェックプロセス中に障害が報告されたデバイスでポリシー展開が失敗します。失敗を回避するには、サイト範囲からデバイスを削除するか、デバイスコンポーネントをアプリケーションポリシーがサポートするレベルに更新します。サポート対象デバイスのリストについては、[Cisco Digital Network Architecture Centerのサポート対象デバイスドキュメント](#)を参照してください。

ポリシーのスケジューリング

ポリシーを作成または変更した後に、そのポリシーを、ポリシーに関連付けられたデバイスに展開または再展開できます。このポリシーの展開/再展開は、すぐに行うことも、特定の日時（たとえば、週末のオフピーク時）に行うこともできます。ポリシー導入のスケジューリングは有線またはワイヤレスのデバイスに対して実施できます。

展開するポリシーのスケジュールを設定すると、そのポリシーとサイト範囲がロックされます。ポリシーの表示は可能ですが、編集することはできません。ポリシーを展開する予定が変更された場合は、その展開をキャンセルできます。



- (注) スケジュールイベントが発生すると、ポリシーは、さまざまなポリシーコンポーネント（アプリケーション、アプリケーションセット、およびキューイングプロファイルなど）に対して検証されます。この検証に失敗すると、ポリシーの変更は行われません。

ポリシーのバージョン管理

このポリシーのバージョン管理により、次のタスクが可能になります。

- 以前のバージョンと現在（最新）のバージョンを比較して相違点を確認する。
- ポリシーの以前のバージョンを表示し、サイト範囲内のデバイスに再適用するバージョンを選択する。

あるバージョンのポリシーを編集しても、そのポリシーの別のバージョンやポリシーのコンポーネント（そのポリシーによって管理されるアプリケーションセットなど）は影響を受けません。たとえば、ポリシーからアプリケーションセットを削除しても、そのアプリケーションセットはCisco DNA Center、そのポリシーの別のバージョン、または他のポリシーからは削除されません。ポリシーとアプリケーションセットは互いに独立して存在するため、存在しなくなったアプリケーションセットを含むバージョンのポリシーを保持できます。存在しなくなったアプリケーションセットを参照するポリシーを展開しようとしたり、それらのポリシーを古いバージョンにロールバックしようとしたりすると、エラーが発生します。



- (注) ポリシーのバージョン管理では、アプリケーション（ランク、ポート、プロトコルなど）、アプリケーションセットメンバー、LANキューイングプロファイル、およびサイトの変更は取得されません。

オリジナルポリシーの復元

初めてデバイスにポリシーを展開する際、Cisco DNA Center は、デバイスの元の Cisco Modular QoS CLI ポリシー設定をデタッチしますが、それらはデバイス上に残ります。Cisco DNA Center は、デバイスの元の NBAR 設定を Cisco DNA Center に保存します。このアクションにより、必要に応じてオリジナルのモジュラー式 QoS CLI ポリシーと NBAR 設定を後でデバイスに復元することが可能になります。



(注) このようにモジュラー式 QoS CLI ポリシーはデバイスから削除されませんが、ユーザがこれらのポリシーを削除すると、元のポリシー復元する Cisco DNA Center の機能を使用してそれらを復元することができなくなります。

元のポリシー設定をデバイスに復元する際、Cisco DNA Center は、展開されている既存のポリシー設定を削除し、デバイス上にあった元の設定に戻します。

アプリケーションポリシーを展開する前に存在していたモジュラー式 QoS CLI ポリシー設定はすべて、インターフェイスに再アタッチされます。ただし、マルチレイヤスイッチング (MLS) 設定などのキューイングポリシーは復元されません。代わりに、デバイスは、Cisco DNA Center によって最後に適用された MLS 設定を維持します。

元のポリシー設定をデバイスに復元すると、Cisco DNA Center に保存されているポリシーが削除されます。

この機能には、次のような追加のガイドラインと制限事項があるので、注意してください。

- 初めてポリシーをデバイスに展開する試みが失敗すると、Cisco DNA Center は、元のポリシー設定をデバイスに復元することを自動的に試みます。
- そのポリシーがデバイスに適用された後にデバイスがアプリケーションポリシーから削除された場合、そのポリシーはデバイス上に残ります。Cisco DNA Center は、ポリシーを自動的に削除したり、デバイスの QoS 設定を元の (事前 Cisco DNA Center) 設定に復元したりしません。

陳腐化したアプリケーションポリシー

ポリシーで参照されているものの設定を変更すると、アプリケーションポリシーが陳腐化する可能性があります。アプリケーションポリシーが陳腐化した場合、変更を有効化するためにアプリケーションポリシーを再展開する必要があります。

アプリケーションポリシーは、次の理由で陳腐化する可能性があります。

- アプリケーション設定で参照されているアプリケーションの変更。
- SP プロファイルの割り当て、WAN サブ回線のレート、WAN または LAN マーキングなどのインターフェイスの変更。
- キューイングプロファイルの変更。

- ポリシーの親サイト下への新規サイトの追加。
- ポリシーによって参照されるサイトへのデバイスの追加。
- ポリシーが同じサイト間でのデバイスの移動。
- インターフェイス除外/包含の変更。
- デバイスコントローラベースのアプリケーション認識 (CBAR) ステータスの変更

アプリケーションポリシーのガイドラインと制限事項

- Cisco DNA Center Cisco DNA Center は、ワイヤレスコントローラ (WLC) 上で同じ SSID 名を使用して複数のワイヤレス LAN (WLAN) を学習することはできません。WLC には、名前は同じで WLAN プロファイル名が異なる複数のエントリを含めることもできますが、Cisco DNA Center はどの時点においても、一意の名前を持つ WLAN に対するエントリを 1 つだけ持ちます。

WLC ごとに重複する SSID 名を意図的に持つことも、Cisco DNA Center を使用して重複する SSID 名を持つ WLC を誤って追加してしまうこともあります。いずれの場合も、WLC ごとに重複する SSID 名を持つことは一部の機能にとって問題になります。

- [Learn Config] : Cisco DNA Center は WLC ごとにランダムに選択された 1 つの SSID 名のみ学習し、残りの重複する SSID 名はすべて破棄します。([設定の学習 (Learn Config)] は、通常はブラウフィールドシナリオで使用されます)。
- [Application Policy] : Cisco DNA Center は、アプリケーションポリシーの展開時に、重複するいずれかの SSID 名にのみポリシーをランダムに適用して、他には適用しません。さらに、ポリシーの復元、CLI プレビュー、EasyQoS ファーストトレイン、および PSK オーバーライド機能が失敗するか、予期しない結果が生じることになります。
- [Multiscale Network] : MULTISCALE ネットワークでは、複数のデバイスの複数の重複する SSID 名が原因で問題が発生することもあります。たとえば、1 台のデバイスには非ファブリック SSID として WLAN が設定されていて、2 台目のデバイスには同じ WLAN がファブリック SSID として設定されている場合、[設定の学習 (Learn Config)] を実行すると、1 つの SSID 名のみ学習されます。その他のデバイスの他の SSID 名は破棄されます。この動作により、特に、2 台目のデバイスがファブリック SSID 名のみサポートしていて、Cisco DNA Center が非ファブリック SSID 名を持つデバイスに対して操作を実行しようとする場合に競合が生じることがあります。
- [IPACL Policy] : Cisco DNA Center は、IPACL ポリシーの展開時に、重複するいずれかの SSID にのみポリシーをランダムに適用します。また、Flex Connect が関係するシナリオも影響を受けます。
- Cisco DNA Center では、デバイス設定に対するアウト オブ バンド (OOB) の変更は推奨されません。OOB に変更を加えると、Cisco DNA Center のポリシーとデバイスに設定されているポリシーは一貫性のない状態になります。2 つのポリシーは、Cisco DNA Center のポリシーをデバイスに再度展開するまで一貫性のない状態のままになります。

- QoS trust 機能は変更できません。

アプリケーションポリシーの管理

ここでは、アプリケーションポリシーの管理の方法に関する情報について説明します。

前提条件

アプリケーションポリシーを設定する場合は、次の要件を満たしていることを確認してください。

- Cisco DNA Center は、ほとんどの Cisco LAN、WAN、WLAN デバイスをサポートします。お使いのネットワーク内でデバイスとソフトウェアバージョンがサポートされているかどうかを確認するには、[Cisco Digital Network Architecture Center のサポート対象デバイス](#)を参照してください。
- ISR-G2、ASR 1000、ワイヤレス LAN コントローラなど、シスコのネットワーク デバイスに AVC (Application Visibility and Control) 機能のライセンスがインストールされていることを確認します。詳細については、「[NBAR2 \(Next Generation NBAR\) Protocol Pack FAQ](#)」を参照してください。
- AVC サポートは、スイッチで自動 QoS が設定されていない場合にのみ、IOS XE バージョン 16.9 を実行しているスイッチで使用できます。AVC サポートを利用するには、自動 QoS 設定のスイッチを IOS XE バージョン 16.11 以降にアップグレードする必要があります。
- ポリシーが必要な WAN インターフェイスを Cisco DNA Center で特定するには、インターフェイス タイプ (WAN) および (必要に応じて) 副回線レートとサービス プロバイダーのサービス クラス モデルを指定する必要があります。詳細については、「[サービス プロバイダープロファイルの WAN インターフェイスへの割り当て \(240 ページ\)](#)」を参照してください。
- ディスカバリ プロセス中にデバイスに割り当てられたデバイス ロールが、ネットワークに適切であることを確認します。必要に応じて、不適切なデバイス ロールを変更します。詳細については、「[デバイスのロールの変更 \(インベントリ\) \(63 ページ\)](#)」を参照してください。

アプリケーションポリシーを作成します。


ここでは、アプリケーションポリシーの作成方法について説明します。

始める前に

- ビジネス目標を定義します。例えば、ネットワーク応答時間を最短化させたり、非ビジネスアプリケーションを特定して優先度を下げたりすることで、ユーザの生産性を向上させるようなものです。これらの目標に基づいて、どのビジネスとの関連性カテゴリがアプリケーションに分類されるかを決定します。

アプリケーションポリシーを作成します。

- インベントリにデバイスがあることを確認します。デバイスがない場合は、ディスカバリ機能を使用して検出します。
- ディスカバリ プロセス中にデバイスに割り当てられたデバイス ロールが、ネットワークに適切であることを確認します。必要に応じて、不適切なデバイスロールを変更します。詳細については、「[デバイスのロールの変更 \(インベントリ\) \(63 ページ\)](#)」を参照してください。
- サイトへのデバイスの追加詳細については、「[デバイスをサイトに追加する \(273 ページ\)](#)」を参照してください。
- Cisco DNA Center で定義されていないアプリケーションがある場合、それらを追加し、QoS 属性を定義することができます。詳細については、「[カスタム アプリケーション \(352 ページ\)](#)」を参照してください。
- SP 向けのトラフィック用に対してこのポリシーを SP プロファイルで設定する場合は、SP プロファイルが設定されていることを確認してください。アプリケーションポリシーの作成後に SP プロファイルに戻り、SLA 属性をカスタマイズして SP プロファイルを WAN インターフェイスに割り当てます。詳細については、「[サービス プロバイダー プロファイルの設定 \(161 ページ\)](#)」を参照してください。
- デバイス上にあるアプリケーションより先に一部のアプリケーションを設定する場合は、それらのアプリケーションをお気に入りとしてマークします。詳細については、「[アプリケーションをお気に入りにする \(357 ページ\)](#)」を参照してください。


-
- ステップ 1** Cisco DNA Center のホームページで、**[Policy] > [Application] > [Application Policies]** の順に選択します。
- ステップ 2** [ポリシーの追加 (Add Policy)] をクリックします。
- ステップ 3** [アプリケーション ポリシー名 (Application Policy Name)] フィールドに、ポリシーの名前を入力します。
- ステップ 4** [有線 (Wired)] または [ワイヤレス (Wireless)] ラジオ ボタンのいずれかを選択します。
- ステップ 5** ワイヤレスネットワークの場合は、[SSID] ドロップダウンリストからプロビジョニングされた SSID を選択します。
- ステップ 6** [サイトの範囲 (Site Scope)] をクリックし、展開するポリシーの横にあるチェック ボックスをオンにします。
- (注) 有線デバイスのポリシーでは、別のポリシーに割り当て済みのサイトは選択することができません。ワイヤレス デバイスのポリシーでは、同じ SSID で別のポリシーに割り当て済みのサイトを選択することができません。
- ステップ 7** 有線デバイスのポリシーでは、デバイスまたは特定のインターフェイスがポリシーで設定されないようにすることができます。
- a) [サイトの範囲 (Site Scope)] ペインで、興味のあるサイトの横にある  をクリックします。
- 選択した範囲内のデバイスのリストが表示されます。

- b) 除外するデバイスを見つけ、関連する [ポリシーの除外 (Policy Exclusions)] 列にあるトグル ボタンをクリックします。
- c) 特定のインターフェイスを除外するには、[Exclude Interfaces] をクリックします。
- d) [Applicable Interfaces] のリストから、除外するインターフェイスの横にあるトグルボタンをクリックします。

デフォルトでは、[Applicable Interfaces] のみが表示されます。すべてのインターフェイスを表示するには、[Show] ドロップダウンリストから [All] を選択します。

- e) [< サイト名のデバイスへ戻る] をクリックします。
- f) [< サイト範囲へ戻る (< Back to Site Scope)] をクリックします。

ステップ 8 WAN デバイスでは、特定のインターフェイスを設定できます。

- a) [サイトの範囲 (Site Scope)] ペインで、興味のあるサイトの横にある  をクリックします。
- b) サイト内のデバイスのリストで、興味のあるデバイスの横にある [SP プロファイルの設定 (SP Profile Settings)] 列の [設定 (Configure)] をクリックします。

(注) このオプションは、ルータの場合にのみ使用可能です。

- c) [WAN インターフェイス (WAN Interface)] 列で、[インターフェイスの選択 (Select Interface)] ドロップダウン リストからインターフェイスを選択します。
- d) [ロール (Role)] 列で [ロールの選択 (Select Role)] ドロップダウン リストから設定するインターフェイスのタイプに従ってロールを選択します。

- **物理インターフェイス** : WAN を選択します。このロールは、物理インターフェイスに対してのみ有効なロールです。

- **トンネル インターフェイス** : [DMVPN ブランチ (DMVPN Branch)] または のいずれかを選択します。[DMVPN ハブ (DMVPN Hub)] を選択した場合、関連するブランチに帯域幅を定義することもできます。

(注) これらのポリシー設定を展開する前に、デバイスにトンネル インターフェイスが作成されていることを確認します。

- e) [サービスプロバイダープロファイル (Service Provider Profile)] 列で、[プロファイルの選択 (Select Profile)] ドロップダウン リストから SP プロファイルを選択します。
- f) (任意) 必要に応じて、[サブ回線のレート (Mbps) (Sub-Line Rate (Mbps))] 列で、インターフェイスに必要なアップストリーム帯域幅を入力します。
- g) (任意) 追加の WAN インターフェイスを設定するには、[+] をクリックし、手順 c ~ f を繰り返します。
- h) [Save (保存)] をクリックします。
- i) [< サイト範囲へ戻る (< Back to Site Scope)] をクリックします。

ステップ 9 [サイトの範囲 (Site Scope)] ペインで、[OK] をクリックします。

ステップ 10 (任意) Cisco Validated Design (CVD) キューイング プロファイルがニーズを満たしていない場合は、カスタム キューイング プロファイルを作成することができます。

- a) [キューイング プロファイル (Queuing Profiles)] をクリックします。

アプリケーションポリシーを作成します。

- b) 左ペインのリストから、キューイングプロファイルを選択します。
- c) [Select] をクリックします。

ステップ 11 (任意) このポリシーが SP 向けトラフィックである場合は、SP プロファイルの SLA 属性をカスタマイズします。


- a) [SP プロファイル (SP Profile)] をクリックします。
- b) SP プロファイルを選択します。
- c) SLA 属性をカスタマイズします ([DSCP]、[SP 帯域幅 (%) (SP Bandwidth %)]、および [キューイング帯域幅 (%) (Queuing Bandwidth %)])。

ステップ 12 (任意) ネットワークで使用されるアプリケーションセットのビジネスとの関連性を設定します。

Cisco DNA Center には、ビジネス関連性グループに事前設定されたアプリケーションセットが付属しています。あるビジネス関連性グループから別のグループにアプリケーションセットをドラッグアンドドロップして、この設定を維持したり、変更したりすることができます。

お気に入りとしてマークされたアプリケーションは、アプリケーションセットの上部に表示されます。お気に入りを変更するには、[Applications registry] に移動します。詳細については、[アプリケーションをお気に入りにする \(357 ページ\)](#) を参照してください。

ステップ 13 (任意) コンシューマを作成してアプリケーションに割り当てるか、アプリケーションを双方向としてマークすることにより、アプリケーションをカスタマイズします。

- a) アプリケーショングループを展開します。
- b) 興味のあるアプリケーションの横にある歯車のアイコン  をクリックします。
- c) [トラフィックの方向 (Traffic Direction)] エリアで、[単方向 (Unidirectional)] または [双方向 (Bi-directional)] ラジオ ボタンを選択します。
- d) 既存のコンシューマを選択するには、[コンシューマ (Consumer)] ドロップダウン リストから設定するコンシューマを選択します。新しいコンシューマを作成するには、[+ コンシューマの追加 (+ Add Consumer)] をクリックして、[コンシューマ名 (Consumer Name)]、[IP/サブネット (IP/Subnet)]、[プロトコル (Protocol)]、および [ポート/範囲 (Port/Range)] を定義します。
- e) [OK] をクリックします。

ステップ 14 ホスト トラッキングを設定します。[ホスト トラッキング (Host Tracking)] トグル ボタンをクリックして、ホスト トラッキングのオンとオフを切り替えます。

アプリケーションポリシーを展開する際に、Cisco DNA Center では、コラボレーションエンドポイント (テレプレゼンス ユニットやシスコ電話など) が接続されているスイッチに、ACL のエントリを自動的に適用します。

ACE は、コラボレーションエンドポイントによって生成された音声およびビデオトラフィックと一致し、音声およびビデオトラフィックが正しくマークされるようにします。

ホスト トラッキングが開始されると、Cisco DNA Center はサイトの範囲内でコラボレーションエンドポイントの接続をトラッキングし、コラボレーションエンドポイントがネットワークに接続されるか、1 つのインターフェイスから別のインターフェイスに移動したときに、ACL エントリを自動的に再設定します。

ホスト トラッキングが終了すると、Cisco DNA Center は、コラボレーションエンドポイントが新しいインターフェイスに移動または接続したときに、デバイスにポリシーを自動的に展開しません。代わりに、

コラボレーションエンドポイントで正しく設定されるように、ACLのポリシーを再展開する必要があります。

ステップ 15 (任意) デバイスに送信される CLI コマンドをプレビューします。詳細については、「[アプリケーションポリシーのプレビュー \(235 ページ\)](#)」を参照してください。

ステップ 16 (任意) ポリシーを展開するデバイスを事前にチェックします。詳細については、「[アプリケーションポリシーの事前チェック \(236 ページ\)](#)」を参照してください。

ステップ 17 次のいずれか 1 つのタスクを実行します。

- [ドラフトの保存 (Save Draft)] をクリックして、ポリシーをドラフトとして保存します。詳細については、「[ポリシーのドラフト \(220 ページ\)](#)」を参照してください。
- [展開 (Deploy)] をクリックしてポリシーを展開します。ポリシーを今すぐ展開するか、または後でスケジュールできます。

ポリシーをすぐに展開するには、[今すぐ実行 (Now)] ラジオボタンをクリックし、[適用 (Apply)] をクリックします。

将来の日付と時刻でポリシー展開をスケジュールするには、[後で実行 (Later)] ラジオ ボタンをクリックし、展開する日時を定義します。詳細については、[ポリシーのスケジュールリング \(222 ページ\)](#) を参照してください。

(注) アプリケーションポリシーの展開のスケジュール設定では、サイトのタイムゾーンの設定はサポートされていません。

View Application Policy Information

作成および展開したアプリケーション ポリシーに関するさまざまな情報を表示できます。

始める前に

少なくとも 1 つの展開されたアプリケーション ポリシーがなければなりません。

ステップ 1 Cisco DNA Center のホームページで、[ポリシー (Policy)] > [アプリケーション (Application)] > [アプリケーション ポリシー (Application Policies)] の順に選択します。

ステップ 2 ポリシーを名前ですべて替えたり、名前、ステータス、キューイングプロファイルによってフィルタ処理したりします。

ステップ 3 ポリシーのリストと、それぞれに関する次の情報が表示されます。

- [ポリシー名 (Policy Name)] : ポリシーの名前。
- バージョン (Version) : ポリシーのバージョン。ポリシーが展開されるか、または、ドラフトとして保存されるたびに、バージョンが 1 ずつ増分されます。たとえば、ポリシーを作成して展開すると、ポリシーはバージョン 1 になります。ポリシーを変更して、再度展開すると、ポリシーのバージョンはバージョン 2 に増分されます。詳細については、[ポリシーのドラフト \(220 ページ\)](#) および [ポリシーのバージョン管理 \(222 ページ\)](#) を参照してください。

- ポリシーのステータス (Policy Status) : ポリシーの状態。Cisco Catalyst 3850、Catalyst 4500、および Catalyst 9K デバイスに適用されたポリシーがポートチャネルの更新 (作成/変更/削除) によって影響を受ける場合は、アラートがポリシーステータスに表示されます。
- 導入ステータス (Deployment Status) : 最新の導入の状態 (デバイスごと)。次の概要を示します。
 - 正常にプロビジョニングされたデバイス
 - プロビジョニングに失敗したデバイス
 - 導入が中止されたために、プロビジョニングされなかったデバイス

最新の導入の状態をクリックすると、[ポリシーの展開 (Policy Deployment)] ウィンドウが表示され、ポリシーが展開されたデバイスのフィルタ処理可能なリストが示されます。デバイスごとに、次の情報が表示されます。

- デバイスの詳細 (名前、サイト、タイプ、ロール、および IP アドレス)
 - 成功した導入のステータス。ステータスの横にある歯車アイコンをクリックすると、デバイスに展開された有効なマーキングポリシーの詳細が表示されます。TCAM リソースまたは古い NBAR プロトコルパックに限定されているデバイスの場合は、ポリシーに含まれるアプリケーションのサブセットのみをプロビジョニングでき、それらがビューで表示されます。
 - 障害ステータスには、障害の理由が示されます。
- スコープ (Scope) : ポリシーに割り当てられているサイト (デバイスではなく) の数。ワイヤレスデバイスのポリシーの場合は、ポリシーの適用先の SSID の名前が含まれます。
 - LAN キューイングプロファイル (LAN Queuing Profile) : ポリシーに割り当てられている LAN キューイングプロファイルの名前。

アプリケーションポリシーの編集

アプリケーションポリシーを編集できます。

始める前に

少なくとも 1 つのポリシーを作成しておく必要があります。

-
- ステップ 1** Cisco DNA Center のホームページで、[ポリシー (Policy)] > [アプリケーション (Application)] > [アプリケーションポリシー (Application Policies)] の順に選択します。
 - ステップ 2** 編集するポリシーを見つけるには、[フィルタ (Filter)] フィールドを使用します。
 - ステップ 3** 対応するポリシーの横にあるラジオ ボタンをクリックします。
 - ステップ 4** [アクション (Actions)] ドロップダウンリストから、[編集 (Edit)] を選択します。
 - ステップ 5** 必要に応じて、アプリケーションポリシーを変更します。

ステップ6 アプリケーションのビジネスとの関連性を変更するには、ビジネス関連、ビジネスと無関係、およびデフォルトグループの間でアプリケーションセットを移動します。

アプリケーションポリシーの設定については、[アプリケーションポリシーを作成します。](#) (225 ページ) を参照してください。

ステップ7 キューイングプロファイルを更新するには、[Queuing Profiles] をクリックし、左ペインのリストからキューイングプロファイルを選択します。

ステップ8 [Select] をクリックします。

ステップ9 次のいずれか1つのタスクを実行します。

- [ドラフトの保存 (Save Draft)] をクリックして、ポリシーをドラフトとして保存します。詳細については、「[ポリシーのドラフト](#) (220 ページ) 」を参照してください。
- [展開 (Deploy)] をクリックしてポリシーを展開します。ポリシーを今すぐ展開するか、または後でスケジュールできます。

ポリシーをすぐに導入するには、[今すぐ実行 (Run Now)] ラジオボタンをクリックし、[適用 (Apply)] をクリックします。

将来の日付と時刻でポリシー導入をスケジュールするには、[後でスケジュール (Schedule Later)] ラジオボタンをクリックし、導入する日時を定義します。詳細については、[ポリシーのスケジュールリング](#) (222 ページ) を参照してください。

(注) アプリケーションポリシーの展開のスケジュール設定では、サイトのタイムゾーンの設定はサポートされていません。

アプリケーションポリシーのドラフトの保存

ポリシーを作成、編集、または複製する際、ドラフトとして保存し、後で変更を続けることができます。また、展開したポリシーを変更して、ドラフトとして保存することもできます。

ステップ1 Cisco DNA Centerのホームページで、[ポリシー (Policy)] > [アプリケーション (Application)] > [アプリケーションポリシー (Application Policies)] の順に選択します。

ステップ2 ポリシーを[アプリケーションポリシーを作成します。](#)、[アプリケーションポリシーの編集](#)、または[アプリケーションポリシーの複製](#)します。

ステップ3 [ドラフトの保存 (Save Draft)] をクリックします。

詳細については、「[ポリシーのドラフト](#) (220 ページ) 」を参照してください。

アプリケーションポリシーの展開

新しいアプリケーションの追加や、アプリケーションをお気に入りとしてマークするなど、ポリシーの設定に影響する変更を加えた場合は、これらの変更を実装するポリシーを再展開する必要があります。



(注) Cisco Catalyst 3850、Catalyst 3650、および IOS バージョン 16.x 以降がインストールされた Catalyst 9K デバイスでは、ポリシーを展開する前に、自動 QoS 設定が自動的に削除されます。

ステップ 1 Cisco DNA Center のホームページで、[ポリシー (Policy)] > [アプリケーション (Application)] > [アプリケーションポリシー (Application Policies)] の順に選択します。

ステップ 2 導入するポリシーを見つけるには、[フィルタ (Filter)] フィールドを使用します。

ステップ 3 導入するポリシーの横のラジオ ボタンをクリックします。

ステップ 4 [アクション (Actions)] ドロップダウンリストから、[導入 (Deploy)] を選択します。

a) ポリシーを再展開すると、ポリシーの範囲から削除されたデバイスに対して適切なアクションを実行するように求められます。次のいずれかの適切なアクションを選択します。

- デバイスからポリシーを削除する (推奨)
- ポリシーの範囲からデバイスを削除する
- ポリシーの範囲からデバイスを削除し、デバイスをブラウンフィールド設定に復元する

b) [Apply] をクリックします。

ステップ 5 ポリシーを今すぐ導入するか、または後でスケジュールするかどうかを求められます。次のいずれかを実行します。

- ポリシーをすぐに導入するには、[今すぐ実行 (Run Now)] ラジオ ボタンをクリックし、[適用 (Apply)] をクリックします。
- 将来の日付と時刻でポリシー導入をスケジュールするには、[後でスケジュール (Schedule Later)] ラジオ ボタンをクリックし、導入する日時を定義します。

(注) アプリケーションポリシーの展開のスケジュール設定では、サイトのタイムゾーンの設定はサポートされていません。

ポリシー導入のキャンセル

[導入 (Deploy)] をクリックすると、Cisco DNA Center は、サイト範囲内のデバイスに関するポリシーの設定を開始します。間違いがあることに気付いた場合は、ポリシーの導入をキャンセルできます。

ポリシー設定プロセスはバッチ処理として実行され、一度に40台のデバイスが設定されます。したがって、デバイスが40台以下の場合にポリシーの導入をキャンセルしても、デバイスの最初のバッチへの導入がすでに行われているため、デバイスが設定されている可能性があります。ただし、何百台ものデバイスがある場合は、必要に応じてポリシー導入のキャンセルを活用できます。

[中止 (Abort)] をクリックすると、Cisco DNA Centerによって設定がまだ開始されていないデバイスの設定プロセスがキャンセルされ、デバイスのステータスが [ポリシーの中止 (Policy Aborted)] に変更されます。Cisco DNA Center では、完了している、または完了する予定の処理での導入はキャンセルされません。これらのデバイスでは、更新されたポリシー設定が維持され、ポリシー設定の状態 (設定中、成功、または失敗) が反映されます。

手順

ポリシー導入中に [中止 (Abort)] をクリックしてポリシー設定プロセスをキャンセルします。

アプリケーションポリシーの削除

不要になったアプリケーションポリシーを削除できます。

ポリシーを削除すると、クラスマップ、ポリシーマップ、およびポリシーマップとワイヤレスポリシープロファイルの関連付けが削除されます。

- ステップ1 Cisco DNA Centerのホームページで、[ポリシー (Policy)] > [アプリケーション (Application)] > [アプリケーションポリシー (Application Policies)] の順に選択します。
- ステップ2 削除するポリシーを見つけるには、[フィルタ (Filter)] フィールドを使用します。
- ステップ3 削除するポリシーの横にあるラジオ ボタンを選択します。
- ステップ4 [Actions] ドロップダウンリストから、[Undeploy Policy] を選択します。
- ステップ5 [Undeploy Policy] ウィンドウで、[Delete policy from devices] オプションボタンをクリックし、[Apply] をクリックします。
- ステップ6 削除を確定する場合は、[OK] をクリックします。それ以外の場合は、[キャンセル (Cancel)] をクリックします。
- ステップ7 削除を確認するメッセージが表示されたら、[OK] を再度クリックします。

[Application Policies] ページで、ポリシーの削除ステータスを確認できます。ステータスに [deletion failed] と表示された場合は、次の手順を実行します。

- a) [Application Policies] ページの [Deployment Status] の下にある失敗状態リンクをクリックします。
- b) [Undeployment Status] ウィンドウで、[Retry] をクリックしてポリシーを削除します。

アプリケーションポリシーの複製

既存のアプリケーションポリシーに、新しいポリシーに必要な設定のほとんどが含まれている場合は、既存のポリシーの複製し、変更してから異なる範囲に展開することで時間を節約できます。

始める前に

少なくとも1つのポリシーを作成しておく必要があります。

- ステップ1 Cisco DNA Centerのホームページで、[ポリシー (Policy)] > [アプリケーション (Application)] > [アプリケーションポリシー (Application Policies)] の順に選択します。
- ステップ2 複製するポリシーを見つけるには、[フィルタ (Filter)] フィールドを使用します。
- ステップ3 複製するポリシーの横にあるラジオ ボタンを選択します。
- ステップ4 [アクション (Actions)] ドロップダウンリストから、[複製 (Clone)] を選択します。
- ステップ5 必要に応じてアプリケーションポリシーを設定します。アプリケーションポリシーの設定については、[アプリケーションポリシーを作成します。\(225 ページ\)](#) を参照してください。
- ステップ6 次のいずれか1つのタスクを実行します。

- [ドラフトの保存 (Save Draft)] をクリックして、ポリシーをドラフトとして保存します。詳細については、「[ポリシーのドラフト \(220 ページ\)](#)」を参照してください。
- [展開 (Deploy)] をクリックしてポリシーを展開します。ポリシーを今すぐ展開するか、または後でスケジュールできます。

ポリシーをすぐに展開するには、[今すぐ実行 (Run Now)] ラジオボタンをクリックし、[適用 (Apply)] をクリックします。

将来の日付と時刻でポリシー展開をスケジュールするには、[後でスケジュール (Schedule Later)] ラジオボタンをクリックし、展開する日時を定義します。詳細については、[ポリシーのスケジュールリング \(222 ページ\)](#) を参照してください。

(注) アプリケーションポリシーの展開のスケジュール設定では、サイトのタイムゾーンの設定はサポートされていません。

アプリケーションポリシーの復元

ポリシーを作成または変更してから、最初からやり直すことを決定した場合、Cisco DNA Center を使ってこれを設定する前に、デバイスにあった元の QoS 設定を復元することができます。

- ステップ1 Cisco DNA Centerのホームページで、[ポリシー (Policy)] > [アプリケーション (Application)] > [アプリケーションポリシー (Application Policies)] の順に選択します。
- ステップ2 リセットするポリシーを見つけるには、[フィルタ (Filter)] フィールドを使用します。
- ステップ3 ポリシーの横にあるラジオ ボタンをクリックします。
- ステップ4 [Actions] ドロップダウンリストから、[Undeploy Policy] を選択します。
- ステップ5 [Undeploy Policy] ウィンドウで、[Restore devices to original configurations] オプションボタンをクリックし、[Apply] をクリックします。
- ステップ6 [OK] をクリックして変更を確認するか、[キャンセル (Cancel)] をクリックして中止します。

[Application Policies] ページで、ポリシーの復元ステータスを確認できます。ステータスに [restoration failed] と表示された場合は、次の手順を実行します。

- a) [Application Policies] ページの [Deployment Status] の下にある失敗状態リンクをクリックします。
- b) [Undeployment Status] ウィンドウで、[Retry] をクリックしてポリシーを復元します。

デフォルトの CVD アプリケーション ポリシーをリセット

CVD 設定は、アプリケーションのデフォルト設定です。ポリシーの作成または変更を行った後で最初からやり直す必要が生じた場合は、アプリケーションを CVD 設定にリセットすることができます。CVD 設定の詳細については、[アプリケーション ポリシー \(209 ページ\)](#) を参照してください。

-
- ステップ 1** Cisco DNA Center のホームページで、[ポリシー (Policy)] > [アプリケーション (Application)] > [アプリケーション ポリシー (Application Policies)] の順に選択します。
 - ステップ 2** リセットするポリシーを見つけるには、[フィルタ (Filter)] フィールドを使用します。
 - ステップ 3** ポリシーの横にあるラジオ ボタンをクリックします。
 - ステップ 4** [アクション (Actions)] ドロップダウンリストから、[編集 (Edit)] を選択します。
 - ステップ 5** [シスコ検証済みデザインのリセット (Reset to Cisco Validated Design)] をクリックします。
 - ステップ 6** [OK] をクリックして変更を確認するか、[キャンセル (Cancel)] をクリックして中止します。
 - ステップ 7** 次のいずれか 1 つのタスクを実行します。
 - ポリシーのドラフトを保存するには、[ドラフトの保存 (Save Draft)] をクリックします。
 - ポリシーを展開するには、[展開 (Deploy)] をクリックします。

アプリケーション ポリシーのプレビュー

ポリシーを展開する前に、デバイスに適用する CLI を生成して設定をプレビューできます。

-
- ステップ 1** Cisco DNA Center のホームページで、[ポリシー (Policy)] > [アプリケーション (Application)] > [アプリケーション ポリシー (Application Policies)] の順に選択します。
 - ステップ 2** [アプリケーション ポリシーを作成します。 \(225 ページ\)](#) または [アプリケーション ポリシーの編集 \(230 ページ\)](#) の説明に従って、ポリシーを作成または編集します。
 - ステップ 3** ポリシーを展開する前に、[プレビュー (Preview)] をクリックします。
範囲内のデバイスのリストが表示されます。
 - ステップ 4** 対象のデバイスの横にある [生成 (Generate)] をクリックします。
Cisco DNA Center により、ポリシーの CLI が生成されます。

ステップ5 [表示 (View)] をクリックして CLI を表示するか、CLI をクリップボードにコピーします。

アプリケーションポリシーの事前チェック

アプリケーションポリシーを展開する前に、サイト範囲内のデバイスがサポート対象であるかどうかをチェックできます。事前チェックプロセスには、デバイスのモデル、ラインカード、およびソフトウェアイメージの検証が含まれます。

ステップ1 Cisco DNA Centerのホームページで、[ポリシー (Policy)] > [アプリケーション (Application)] > [アプリケーションポリシー (Application Policies)] の順に選択します。

ステップ2 [アプリケーションポリシーを作成します。\(225 ページ\)](#) または [アプリケーションポリシーの編集\(230 ページ\)](#) の説明に従って、ポリシーを作成または編集します。

ステップ3 [事前チェック (Pre-check)] をクリックします。

Cisco DNA Center は、デバイスをチェックして、問題があれば [事前チェック結果 (Pre-Check Result)] 列に内容を報告します。[Errors] タブには、このポリシーをサポートしていないデバイスが表示されます。[Warnings] タブには、デバイスにこのポリシーを展開することを選択した場合に、サポートされていない制限や機能が表示されます。[Warnings] タブに一覧表示されているデバイスのポリシーを展開することもできます。問題を解決するには、[Cisco Digital Network Architecture Center のサポート対象デバイス](#)に記載されている仕様にデバイスを準拠させます。

アプリケーションポリシー履歴の表示

アプリケーションポリシーのバージョン履歴を表示できます。バージョン履歴には、ポリシーのシリーズ番号 (反復) と、バージョンが保存された日付と時刻が含まれています。

ステップ1 Cisco DNA Centerのホームページで、[ポリシー (Policy)] > [アプリケーション (Application)] > [アプリケーションポリシー (Application Policies)] の順に選択します。

ステップ2 表示したいポリシーの横にあるラジオ ボタンをクリックします。

ステップ3 [アクション (Actions)] ドロップダウン リストから、[履歴 (History)] を選択します。

ステップ4 [ポリシー履歴 (Policy History)] ダイアログボックスでは、次のことを実行できます。

- 現在のバージョンとバージョンを比較するには、関心のあるバージョンの横にある [差異 (Difference)] をクリックします。
- ポリシーの前のバージョンにロールバックするには、ロールバック先となるバージョンの横にある [ロールバック (Rollback)] をクリックします。

ポリシーの以前のバージョンにロールバック

ポリシー設定を変更し、その後その設定が不適切だと判明した場合、またはネットワークで目的の効果が得られなかった場合、最大で5バージョン前のポリシーに戻すことができます。

始める前に

以前のポリシーバージョンにロールバックするには、少なくとも2つのポリシーバージョンを作成しておく必要があります。

-
- ステップ 1** Cisco DNA Centerのホームページで、[ポリシー (Policy)] > [アプリケーション (Application)] > [アプリケーションポリシー (Application Policies)] の順に選択します。
- ステップ 2** 表示したいポリシーの横にあるラジオ ボタンをクリックします。
- ステップ 3** [アクション (Actions)] ドロップダウンリストから、[履歴の表示 (Show History)] を選択します。
- 選択したポリシーの以前のバージョンは降順に表示され、最も新しいバージョン (最も大きい番号) が一覧の最上部に表示され、最も古いバージョン (最も小さい番号) が最下部に表示されます。
- ステップ 4** (任意) 選択したバージョンと最新バージョンの間の差異を表示するには、[View] 列で [Difference] をクリックします。
- ステップ 5** ロールバックする先のポリシーバージョンを決定した場合、そのポリシーバージョンに対して [Rollback] をクリックします。
- (注) 選択したサイトの範囲がポリシーバージョン間で変更された場合、ロールバックは選択されている現在 (最新) のサイトでは行われません。ポリシーのコンテンツのみがロールバックされます。
- ステップ 6** [OK] をクリックして、ロールバック手順を確定します。
- ロールバック先のバージョンが最新バージョンになります。
-

キューイング プロファイルの管理

次のセクションでは、キューイングプロファイルを管理するために実行できるさまざまなタスクについて詳しく説明します。

キューイング プロファイルの作成

Cisco DNA Center では、デフォルトの CVD キューイング プロファイル (CVD_QUEUEING_PROFILE) を提供します。このキューイングプロファイルがニーズを満たしていない場合は、カスタム キューイング プロファイルを作成することができます。

-
- ステップ 1** Cisco DNA Centerのホームページで、[ポリシー (Policy)] > [アプリケーション (Application)] > [キューイング プロファイル (Queuing Profile)] の順に選択します。
- ステップ 2** [プロファイルを追加 (Add Profile)] をクリックします。

ステップ 3 [Profile Name] フィールドに、プロファイルの名前を入力します。

ステップ 4 スライダーを使用して各トラフィック クラスに帯域幅を設定します。プラス記号 (+) またはマイナス (-) 記号をクリックするか、フィールドに特定の数値を入力します。

数値は、選択したアプリケーションクラスに確保されるインターフェイス帯域幅の合計に対しての割合を示します。帯域幅の合計は 100 なので、1つのアプリケーションクラスに帯域幅を追加すると、別のアプリケーションクラスから帯域幅が差し引かれます。

開いた錠のアイコンは、そのアプリケーションクラスの帯域幅を編集できることを示します。閉じた錠のアイコンは、編集できないことを示します。

間違えた場合は、[シスコ検証済みデザインのリセット (Reset to Cisco Validated Design)] をクリックして CVD 設定に戻ることができます。

中央のグラフは、各アプリケーションクラスを設定している帯域幅の量の視覚化に役立ちます。

ステップ 5 (高度なユーザ向け) Cisco DNA Center が各トラフィック クラスで使用する DSCP コードポイントをカスタマイズするには、[表示 (Show)] ドロップダウンリストで、[DSCP値 (DSCP Values)] を選択し、フィールドに特定の数値を入力して、各アプリケーションクラスの値を設定します。

SP のクラウド内で必要な DSCP コードポイントをカスタマイズするには、SP のプロファイルを設定します。

ステップ 6 [保存 (Save)] をクリックします。

キューイング プロファイルの編集または削除

ステップ 1 Cisco DNA Center のホームページで、[ポリシー (Policy)] > [アプリケーション (Application)] > [キューイング プロファイル (Queuing Profile)] の順に選択します。

ステップ 2 [キューイング プロファイル (Queuing Profile)] ペインで、編集または削除するキューイング プロファイルの横にあるラジオ ボタンをクリックします。

ステップ 3 次のいずれか 1 つのタスクを実行します。

- プロファイルを編集するには、プロファイル名を除くフィールドの値を変更し、[保存 (Save)] をクリックします。フィールドの詳細については、[キューイング プロファイルの作成 \(237 ページ\)](#) を参照してください。
- プロファイルを削除するには、[削除 (Delete)] をクリックします。

(注) アプリケーションポリシーによって参照されている場合は、キューイングプロファイルを削除できません。

WAN インターフェイスのアプリケーション ポリシーの管理

次のセクションでは、WAN インターフェイスのアプリケーション プロファイルを管理するために実行できるさまざまなタスクについて詳しく説明します。

サービス プロバイダー プロファイルの SLA 属性をカスタマイズ

自身のクラスモデルによって SP プロファイルに割り当てられたデフォルトの SLA 属性を使用しない場合は、要件に合わせて SP プロファイルの SLA 属性をカスタマイズすることができます。SP プロファイルの SLA 属性の詳細については、[サービスプロバイダーのプロファイル \(214 ページ\)](#) を参照してください。

始める前に

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

ステップ 1 Cisco DNA Center のホームページで、[ポリシー (Policy)] > [アプリケーション (Application)] > [アプリケーション ポリシー (Application Policies)] の順に選択します。

ステップ 2 変更するポリシーを見つけるには、[フィルタ (Filter)] フィールドを使用します。

ステップ 3 ポリシーの横にあるラジオ ボタンを選択します。

ステップ 4 [アクション (Actions)] ドロップダウンリストから、[編集 (Edit)] を選択します。

ステップ 5 [SP プロファイル (SP Profiles)] をクリックし、SP プロファイルを選択します。

ステップ 6 次のフィールドの情報を変更できます。

- [DSCP] : Differentiated Services Code Point (DSCP) 値。有効値は 0 ~ 63 です。
 - Expedited Forwarding (EF)
 - [Class Selector (CS)] : CS1、CS2、CS3、CS4、CS5、CS6
 - [Assured Forwarding] : AF11、AF21、AF41
 - [Default Forwarding (DF)]

これらの DSCP 値の詳細については、[マーキング、キューイング、ドロップの処理 \(212 ページ\)](#) を参照してください。

- [SP 帯域幅の割合 (SP Bandwidth %)] : 特定のサービス クラスに割り当てられた帯域幅の割合。
- [キューイング帯域幅の割合 (Queuing Bandwidth %)] : 各トラフィック クラスに割り当てられた帯域幅の割合。次のうちいずれかの変更を行うことができます。
 - キューイング帯域幅をカスタマイズするには、鍵アイコンをクリックして、帯域幅の設定をアンロックし、帯域幅の割合を調整します。
 - SP 帯域幅から自動的にキューイング帯域幅を計算するには、鍵アイコンをクリックしてキューイング帯域幅の設定をロックし、次に [OK] をクリックして確認します。デフォルトでは、Cisco

DNA Center は、SP クラスのすべてのトラフィック クラスのキューイング帯域幅の合計がそのクラスの SP 帯域幅の割合と一致するように、キューイング帯域幅の割合を自動的に配信します。


ステップ7 [OK] をクリックします。

サービス プロバイダー プロファイルの WAN インターフェイスへの割り当て

アプリケーション ポリシーがすでに作成済みで、SP プロファイルを WAN インターフェイスに割り当てる場合は、ポリシーを編集してこの設定を実行し、必要に応じてインターフェイスに Subline Rate の設定を含めます。

始める前に

ポリシーを作成していない場合は、ポリシーを作成し、同時に SP プロファイルを WAN インターフェイスに割り当てることができます。詳細については、「[アプリケーションポリシーを作成します。](#) (225 ページ)」を参照してください。

- ステップ1 Cisco DNA Centerのホームページで、[ポリシー (Policy)] > [アプリケーション (Application)] > [アプリケーション ポリシー (Application Policies)] の順に選択します。
- ステップ2 編集するポリシーを見つけるには、[フィルタ (Filter)] フィールドを使用します。
- ステップ3 ポリシーの横にあるラジオ ボタンをクリックします。
- ステップ4 [アクション (Actions)] ドロップダウンリストから、[編集 (Edit)] を選択します。
- ステップ5 [サイトの範囲 (Site Scope)] ペインで、対象のサイトの横にある歯車アイコン  をクリックします。
- ステップ6 対象のデバイスの [SPプロファイル設定 (SP Profile Settings)] 列にある [設定 (Configure)] をクリックします。
- ステップ7 [WAN インターフェイス (WAN Interface)] 列で、[インターフェイスの選択 (Select Interface)] ドロップダウンリストからインターフェイスを選択します。
- ステップ8 [ロール (Role)] 列で [ロールの選択 (Select Role)] ドロップダウンリストから設定するインターフェイスのタイプに従ってロールを選択します。
- **物理インターフェイス** : WAN を選択します。このロールは、物理インターフェイスに対してのみ有効なロールです。
 - **トンネル インターフェイス** : [DMVPN ブランチ (DMVPN Branch)] または のいずれかを選択します。[DMVPN ハブ (DMVPN Hub)] を選択した場合、関連するブランチに帯域幅を定義することもできます。
- (注) これらのポリシー設定を展開する前に、デバイスにトンネル インターフェイスが作成されていることを確認します。
- ステップ9 [サービス プロバイダー プロファイル (Service Provider Profile)] 列で、[プロファイルの選択 (Select Profile)] ドロップダウン フィールドをクリックし、SP プロファイルを選択します。

- ステップ 10** 必要に応じて、[サブ回線のレート (Mbps) (Sub-Line Rate (Mbps))] 列で、インターフェイスに必要なアップストリーム帯域幅を入力します。
- ステップ 11** 追加の WAN インターフェイスを設定するには [+] をクリックし、ステップ 7 ~ 10 を繰り返します。
- ステップ 12** [Save (保存)] をクリックします。
- ステップ 13** [< サイト範囲へ戻る (< Back to Site Scope)] をクリックします。
- ステップ 14** [OK] をクリックします。
- ステップ 15** [展開 (Deploy)] をクリックします。

ポリシーを今すぐ導入するか、または後でスケジュールするかどうかを求められます。

- ステップ 16** 次のいずれかを実行します。
- ポリシーをすぐに導入するには、[今すぐ実行 (Run Now)] ラジオ ボタンをクリックし、[適用 (Apply)] をクリックします。
 - 将来の日付と時刻でポリシー導入をスケジュールするには、[後でスケジュール (Schedule Later)] ラジオ ボタンをクリックし、導入する日時を定義します。
- (注) アプリケーションポリシーの展開のスケジュール設定では、サイトのタイムゾーンの設定はサポートされていません。

トラフィック コピー ポリシー

Cisco DNA Center を使用して、2つのエンティティ間の IP トラフィック フローがモニタリングまたはトラブルシューティングのために指定された宛先にコピーされるように Encapsulated Remote Switched Port Analyzer (ERSPAN) を設定できます。

Cisco DNA Center を使用して ERSPAN を設定するには、コピーするトラフィック フローの送信元と宛先を定義するトラフィック コピー ポリシーを作成します。トラフィックのコピーを送信するデバイスおよびインターフェイスを指定するトラフィック コピー契約も定義できます。



- (注) トラフィック コピー ポリシーにはスケーラブル グループまたは IP ネットワーク グループのいずれかを含めることができるため、このガイド全体を通して、グループという用語を使用する場合は他に指定がなければスケーラブル グループおよび IP ネットワーク グループの両方を指します。

送信元、宛先、およびトラフィックのコピー先

Cisco DNA Center Cisco DNA Center はトラフィックのモニタリングプロセスを簡素化します。物理ネットワーク トポロジを知っている必要はありません。必要なのは、トラフィック フロー

の送信元および宛先とコピーされたトラフィックの宛先となるトラフィック コピーの宛先を定義することだけです。

- [送信元 (Source)] : モニタするトラフィックが通過する 1 つまたは複数のネットワーク デバイス インターフェイス。このインターフェイスは、エンドポイント デバイス、これらのデバイスの特定ユーザ、またはアプリケーションに接続することがあります。送信元グループを構成できるのは、イーサネット、ファストイーサネット、ギガビットイーサネット、10 ギガビットイーサネット、またはポート チャネル インターフェイスのみです。
- [宛先 (Destination)] : モニタするトラフィックが流れる IP サブネットです。IP サブネットはサーバ、リモートピア、またはアプリケーションに接続することがあります。
- [トラフィックコピーの宛先 (Traffic Copy Destination)] : ERSPAN データを受信、処理、および分析するデバイス上にあるレイヤ 2 またはレイヤ 3 の LAN インターフェイス。このデバイスは、通常、分析用にトラフィックのコピーを受信するパケットキャプチャツールまたはネットワーク分析ツールになります。



(注) 宛先では、スイッチプロンプデバイスなどのネットワークアナライザやその他のリモートモニタリング (RMON) プロンプを使用してトラフィック分析を実行することを推奨します。

使用可能なインターフェイスタイプは、イーサネット、ファストイーサネット、ギガビットイーサネット、または 10 ギガビットイーサネットのみです。宛先として設定されると、そのインターフェイスはコピーされたトラフィックのみを受信するために使用されます。このインターフェイスは今後その他のタイプのトラフィックを受信できなくなり、トラフィック コピー機能が必要とする以外のトラフィックを転送できません。トランク インターフェイスを宛先として設定できます。この設定により、インターフェイスはカプセル化されたトラフィックを送信できるようになります。



(注) 1 つのトラフィック コピー契約で使用できるトラフィック コピーの宛先は 1 つのみです。

トラフィック コピー ポリシーの注意事項と制限事項

トラフィック コピー ポリシー機能には次の制約事項があります。

- 最大 8 つのトラフィック コピー ポリシー、16 のコピー契約、および 16 のコピーの宛先を作成できます。
- 同じインターフェイスを複数のトラフィック コピーの宛先に使用することはできません。
- Cisco DNA Center は、トラフィック コピー ポリシーが変更され、ネットワークに展開されているポリシーとの整合性が失われていることを示すステータスメッセージを表示しま

せん。ただし、トラフィック コピー ポリシーが展開された後に変更されたことが分かった場合は、そのポリシーを展開しなおすことができます。

- 管理インターフェイスを送信元グループまたはトラフィック コピーの宛先として設定することはできません。

トラフィック コピー ポリシー設定のワークフロー

始める前に

- モニタ対象にする、トラフィック コピー ポリシーで使用されている送信元スケラブルグループが、スイッチとそれらのインターフェイスに静的にマッピングされている必要があります。
- トラフィック コピー ポリシー宛先グループは、IP ネットワーク グループとして設定されている必要があります。詳細については、「[IP ネットワーク グループの作成 \(204 ページ\)](#)」を参照してください。

ステップ 1

トラフィック コピーの宛先を作成します。

これは、さらに分析するためにトラフィック フローがコピーされる、デバイス上のインターフェイスです。詳細については、[トラフィック コピーの宛先の作成 \(243 ページ\)](#) を参照してください。

ステップ 2

トラフィック コピーの契約を作成します。

契約はコピーの宛先を定義します。詳細については、[トラフィック コピー契約の作成 \(244 ページ\)](#) を参照してください。

ステップ 3

トラフィック コピー ポリシーを作成します。

ポリシーは、トラフィック フローの送信元と宛先、およびコピーされたトラフィックが送信される宛先を指定するトラフィック コピーの契約を定義します。詳細については、[トラフィック コピーポリシーの作成 \(245 ページ\)](#) を参照してください。

トラフィック コピーの宛先の作成

ステップ 1 Cisco DNA Center のホームページで、[ポリシー (Policy)] > [トラフィック コピー (Traffic Copy)] > [トラフィック コピーの宛先 (Traffic Copy Destination)] の順に選択します。

ステップ 2 トラフィック コピーの宛先の名前と説明を入力します。

ステップ 3 デバイスと 1 つまたは複数のポートを選択します。

ステップ 4 [保存 (Save)] をクリックします。

トラフィック コピーの宛先の編集または削除

- ステップ1 Cisco DNA Center のホームページで、[ポリシー (Policy)] > [トラフィック コピー (Traffic Copy)] > [トラフィック コピーの宛先 (Traffic Copy Destination)] の順に選択します。
- ステップ2 編集または削除する宛先の横にあるチェックボックスをオンにします。
- ステップ3 次のいずれかを実行します。
 - 変更を行うには、[編集 (Edit)] をクリックして必要な変更を行い、[保存 (Save)] をクリックします。
 - 宛先を削除するには、[削除 (Delete)] をクリックします。

トラフィック コピー契約の作成

- ステップ1 Cisco DNA Center ホームページで、[ポリシー (Policy)] > [トラフィック コピー (Traffic Copy)] > [トラフィック コピー契約 (Traffic Copy Contracts)] の順に選択します。
- ステップ2 [Add] をクリックします。
- ステップ3 ダイアログボックスに、契約の名前と説明を入力します。
- ステップ4 [コピー先 (Copy Destination)] ドロップダウン リストから、コピー先を選択します。

(注) コピー先は、1つのトラフィック コピー契約に対し1つだけ指定できます。

選択可能なコピー先がない場合は、1つ作成できます。詳細については、[トラフィック コピーの宛先の作成 \(243 ページ\)](#) を参照してください。
- ステップ5 [保存 (Save)] をクリックします。

トラフィック コピー契約の編集または削除

- ステップ1 Cisco DNA Center ホームページで、[ポリシー (Policy)] > [トラフィック コピー (Traffic Copy)] > [トラフィック コピー契約 (Traffic Copy Contracts)] の順に選択します。
- ステップ2 編集または削除する契約の横にあるチェックボックスをオンにします。
- ステップ3 次のいずれかを実行します。
 - 変更を行うには、[編集 (Edit)] をクリックして必要な変更を行い、[保存 (Save)] をクリックします。
 - 契約を削除するには、[削除 (Delete)] をクリックします。

トラフィック コピー ポリシーの作成

- ステップ 1 Cisco DNA Center のホームページで、[ポリシー (Policy)] > [トラフィック コピー (Traffic Copy)] > [トラフィック コピー ポリシー (Traffic Copy Policies)] の順に選択します。
- ステップ 2 [ポリシーの追加 (Add Policy)] をクリックします。
- ステップ 3 [ポリシー名 (Policy Name)] フィールドに名前を入力します。
- ステップ 4 [説明 (Description)] フィールドにポリシーを表す単語またはフレーズを入力します。
- ステップ 5 [契約 (Contract)] フィールドで、[契約の追加 (Add Contract)] をクリックします。
- ステップ 6 使用する契約の隣にあるラジオ ボタンをクリックし、次に [保存 (Save)] をクリックします。
- ステップ 7 [使用可能なグループ (Available Groups)] エリアから、[送信元 (Source)] エリアにグループをドラッグアンドドロップします。
- ステップ 8 [使用可能なグループ (Available Groups)] エリアから、[宛先 (Destination)] エリアにグループをドラッグアンドドロップします。
- ステップ 9 [保存 (Save)] をクリックします。

Edit or Delete a Traffic Copy Policy

- ステップ 1 Cisco DNA Center のホームページで、[ポリシー (Policy)] > [トラフィック コピー (Traffic Copy)] > [トラフィック コピー ポリシー (Traffic Copy Policies)] の順に選択します。
- ステップ 2 編集または削除したいポリシーの横のチェック ボックスをオンにします。
- ステップ 3 次のいずれかを実行します。
 - 変更を行うには、[編集 (Edit)] をクリックして必要な変更を行い、[保存 (Save)] をクリックします。
 - ポリシーを削除するには、[削除 (Delete)] をクリックします。

仮想ネットワーク

仮想ネットワークは、独立したルーティングおよびスイッチング環境です。仮想ネットワークを使用して、物理ネットワークを複数の論理ネットワークにセグメント化できます。

仮想ネットワークに入れることができるのは、割り当てられたユーザグループのみです。仮想ネットワーク内で、ユーザとデバイスは、アクセスポリシーによって明示的にブロックされていなければ相互に通信できます。異なる仮想ネットワークにまたがるユーザは、相互に通信できません。ただし、例外ポリシーを作成して、一部のユーザに異なる仮想ネットワークをまたぐ通信を許可することができます。

一般的な使用例はビルディング管理です。照明、冷暖房空調（HVAC）システム、セキュリティシステムなどのビルディングシステムからユーザコミュニティをセグメント化する必要があります。このケースでは、ユーザコミュニティとビルディングシステムを2つ以上の仮想ネットワークにセグメント化して、ビルディングシステムの不正アクセスをブロックします。

仮想ネットワークは、複数のサイトロケーションやネットワークドメイン（ワイヤレス、キャンパス、およびWAN）にまたがる場合があります。

デフォルトでは、Cisco DNA Centerには単一の仮想ネットワークがあり、すべてのユーザおよびエンドポイントがこの仮想ネットワークに属しています。Cisco DNA CenterがCisco Identity Services Engine（ISE）と統合されると、デフォルトの仮想ネットワークにCisco ISEのユーザグループおよびエンドポイントが移入されます。

Cisco DNA Centerでは、仮想ネットワークの概念はワイヤレス、キャンパス、およびWANネットワークで共通です。仮想ネットワークが作成されたら、ワイヤレス、有線、またはWAN導入が組み合わされているサイトと関連付けることができます。たとえば、ワイヤレスデバイスと有線デバイスが含まれるキャンパスファブリックがサイトで展開されている場合、仮想ネットワークの作成プロセスによってキャンパスファブリックでサービスセット識別子（SSID）とVirtual Routing and Forwarding（VRF）の作成がトリガーされます。また、サイトにWANファブリックも展開されている場合、VRFがキャンパスからWANに同様に拡張します。

サイトの設計および初期設定時に、ワイヤレスデバイス、有線スイッチ、およびWANルータをサイトに追加できます。Cisco DNA Centerは、仮想ネットワークと関連付けられたポリシーがサイトに対して作成されたことを検出し、それらを異なるデバイスに適用します。

仮想ネットワークに関する注意事項と制限事項

仮想ネットワークには次の注意事項と制約事項があります。


- VRFはすべてのドメインで共通です。VRFの最大数は、ドメイン内のVRFが最も少ないデバイスに基づきます。

ゲストアクセス用の複数の仮想ネットワーク

ゲストアクセス用に複数の仮想ネットワークを作成できます。この機能を使用すると、企業のトラフィックが存在しない場所で、ゲストトラフィック用に異なる仮想ネットワークを使用できます。ワイヤレスゲストSSIDを異なる仮想ネットワークのIPプールに制限なしでマッピングできるようになりました。

仮想ネットワークの作成

仮想ネットワークを作成し、物理ネットワークを複数の論理ネットワークにセグメント化することができます。

- ステップ 1** Cisco DNA Center のホームページで、[ポリシー (Policy)] > [仮想ネットワーク (Virtual Network)] の順に選択します。
- ステップ 2**  をクリックして、新しい仮想ネットワークを作成します。
- ステップ 3** [ネットワーク名 (Network Name)] フィールドに、仮想ネットワークの名前を入力します。
- ステップ 4** 仮想ネットワークをゲストネットワークとして設定するには、[Guest Virtual Network] チェックボックスをオンにします。
- ゲストに制限されたアクセスを許可する、特別なルールが設定されているデバイス。
- ステップ 5** [使用可能なスケーラブル グループ (Available Scalable Groups)] エリアから、[仮想ネットワーク内のグループ (Groups in the Virtual Network)] エリアにドラッグアンドドロップします。
- ステップ 6** [保存 (Save)] をクリックします。
- ステップ 7** 複数のゲスト仮想ネットワークを作成するには、ステップ 2～6 を繰り返します。

仮想ネットワークの編集または削除

あるカスタム仮想ネットワークから別のカスタム仮想ネットワークにスケーラブルなグループを移動すると、スケーラブルなグループのマッピングが変更されます。この変更によって、グループ内のユーザまたはデバイスに影響が及ぶ可能性があることに注意してください。

- ステップ 1** Cisco DNA Center のホームページで、[ポリシー (Policy)] > [仮想ネットワーク (Virtual Network)] の順に選択します。
- ステップ 2** 次のいずれか 1 つのタスクを実行します。
- 仮想ネットワークを編集するには、左側のナビゲーション ウィンドウから仮想ネットワークの名前をクリックし、次の表に示す任意のフィールドの情報を変更します (仮想ネットワーク名を除きます)。

表 44: 仮想ネットワーク フィールド

フィールド	説明
Network Name	仮想ネットワークの名前。(変更できません)。
Guest Virtual Network	ゲストに制限されたアクセスを許可する、特別なルールが設定されているデバイス。ゲスト ネットワークとして仮想ネットワークを設定するには、このチェックボックスをオンにします。ゲスト仮想ネットワークを 1 つだけ作成することができます。
Available Groups	仮想ネットワークに含めることができるスケーラブルなグループ。[使用可能なグループ (Available Groups)] エリアから、[仮想ネットワーク内のグループ (Groups in the Virtual Network)] エリアにドラッグアンドドロップします。

フィールド	説明
Groups in the Virtual Network	仮想ネットワーク内にあるスケーラブルなグループ。[使用可能なグループ (Available Groups)]エリアから、[仮想ネットワーク内のグループ (Groups in the Virtual Network)]エリアにドラッグアンドドロップします。

- 仮想ネットワークを削除するには、 をクリックし、削除を確定します。
-



第 13 章

ネットワークのプロビジョニング

- [プロビジョニング \(249 ページ\)](#)
- [プラグ アンド プレイ プロビジョニングを使用したオンボードデバイス \(250 ページ\)](#)
- [インベントリ内のデバイスの管理 \(272 ページ\)](#)
- [デバイスのプロビジョニング \(276 ページ\)](#)
- [LAN 自動化の状態を確認 \(330 ページ\)](#)
- [プロビジョニング後のデバイスの削除 \(331 ページ\)](#)
- [ファブリック サイトとファブリック ドメイン \(331 ページ\)](#)
- [マルチサイトファブリック ドメイン \(332 ページ\)](#)
- [トランジット サイト \(332 ページ\)](#)
- [ファブリック ドメインの設定 \(334 ページ\)](#)
- [Applications \(351 ページ\)](#)
- [アプリケーションホスティング \(359 ページ\)](#)

プロビジョニング

Cisco DNA Center でネットワークのポリシーを設定した後に、デバイスをプロビジョニングできます。この段階で、デバイスにオンボードし、デバイス間にポリシーを導入します。

プロビジョニングデバイスには、次の側面が含まれます。

- プラグ アンド プレイでのデバイスのオンボーディングと、デバイスのインベントリへの追加。
- 必要な設定とポリシーのインベントリ内デバイスへの展開。
- デバイスのサイトへの追加。
- ファブリック ドメインの作成とデバイスのファブリックへの追加。

Cisco DNA Center プロビジョニングでは IBNS 2.0 のみをサポートしています。これにより AAA 設定が変更され、関連するすべての認証コマンドがクラスベースのポリシー言語 (CPL) 制御ポリシーの対応するコマンドに変換されます。CPL 変換では、変換 CLI **authentication display [legacy|new-style]** が無効になるため、現在の設定をバックアップしておくことを推奨します。

また、IBNS 2.0 に合わせた AAA 設定の更新をサポートするように変更管理期間を設定してください。

プラグアンドプレイ プロビジョニングを使用したオンボードデバイス

プラグアンドプレイ プロビジョニングは、最小限のネットワーク管理者およびフィールド担当者の関与で、新しいネットワークデバイスを自動的にかつリモートにプロビジョニングおよびオンボードする方法を提供します。

プラグアンドプレイ プロビジョニングを使用すると、次の操作を実行できます。

- サイトの割り当て、サイト設定の展開、デバイスソフトウェアイメージのインストール、およびカスタムオンボード設定の適用によって、デバイスをプロビジョニングする。
- インストールの前に、デバイス情報を入力し、プロビジョニング操作を選択してデバイスを計画します。デバイスはオンラインになると Cisco DNA Center に接続します。次に、デバイスのプロビジョニングとオンボーディングが自動で実行されます。
- 事前の計画なしにネットワーク上に表示される新しいデバイスである、要求されていないネットワーク デバイスをプロビジョニングします。
- Cisco スマートアカウントの Cisco Plug and Play Connect クラウドポータルから、デバイスインベントリをプラグアンドプレイに同期して、すべてのデバイスが Cisco DNA Center に表示されるようにします。
- ネットワーク デバイスの詳細なオンボーディング ステータスを表示します。

前提条件

プラグアンドプレイ プロビジョニングを使用する前に、次の操作を実行します。

- メインの Cisco DNA Center の設定で、[System Settings] > [Settings] > [Cisco Credentials] を使用して、シスコのログイン情報を設定します。詳細については、「[Cisco Digital Network Architecture Center 管理者ガイド](#)」の「Cisco クレデンシャルの設定」を参照してください。
- [System Settings] > [Settings] > [Device EULA Acceptance] を使用して、メインの Cisco DNA Center の設定でエンドユーザライセンス契約 (EULA) に同意します。詳細については、[Cisco Digital Network Architecture Center 管理者ガイド \[英語\]](#) の「[Accept the License Agreement](#)」を参照してください。
- プロビジョニングするシスコネットワークデバイスについて、サポートされているソフトウェアリリースがあり、工場出荷時のデフォルト状態になっていることを確認します。以前に設定されたネットワークデバイス、または不明な状態になっているネットワークデバイスを使用している場合は、[Cisco Digital Network Architecture Center](#) のネットワーク プラ

[プラグアンドプレイのトラブルシューティング ガイド \[英語\]](#) のデバイスのクリーンアップとリセットの詳細を参照してください。

ここでは、プラグアンドプレイプロビジョニングの一般的な使用例とワークフローについて説明します。

計画されたプロビジョニング

管理者は、次のように新しいサイトまたはその他のネットワーク デバイス グループのプロビジョニングを計画できます。

1. ネットワーク階層内のサイトを定義します。 [About Network Hierarchy \(94 ページ\)](#) を参照してください。
2. 必要に応じて、デバイスに適用する [Onboarding Configuration] テンプレートを定義します。このようなテンプレートには、ネットワーク上で管理できるようにデバイスをオンボードするための基本的なネットワーク設定コマンドが含まれています。多くの場合、Day 0 設定をカスタマイズする必要がない限り、このようなテンプレートは必要ありません。 [デバイス設定の変更を自動化するテンプレートの作成 \(167 ページ\)](#) を参照してください。
3. 展開するデバイスのタイプについて、ネットワーク プロファイルを定義します。 [ネットワーク プロファイルの作成 \(140 ページ\)](#) を参照してください。
4. 展開するデバイスのデバイスのログイン情報 (CLI および SNMP) を定義します。 [デバイス スクレデンシャルについて \(147 ページ\)](#) を参照してください。
5. 必要に応じて、プロビジョニングするデバイスのソフトウェアイメージがアップロードされ、イメージリポジトリ内でゴールデンとしてマークされていることを確認します。 [ソフトウェア イメージのインポート \(77 ページ\)](#) を参照してください。
6. CSV ファイルを使用して一度にまたは一括で、計画したデバイスに関する詳細を追加します。 [デバイスの追加または編集 \(258 ページ\)](#) または [Add Devices in Bulk \(259 ページ\)](#) を参照してください。
7. デバイスが起動し、自動的にプロビジョニングされます。

要求されていないプロビジョニング。

計画前に新しいネットワーク デバイスをネットワークに追加すると、このネットワーク デバイスは要求のないデバイスとしてラベル付けされます。要求のないデバイスは、管理者が手動で追加することも、[コントローラ ディスカバリの前提条件 \(252 ページ\)](#) で説明されているいずれかの検出方法を使用して自動的に追加することもできます。管理者は、次の方法でデバイスをプロビジョニングできます。

1. 要求のないデバイスでフィルタリングするか、名前を検索して、デバイスリストのデバイスを検索します。 [デバイスの表示 \(255 ページ\)](#) を参照してください。
2. サイト、イメージ、設定テンプレート、またはプロファイルを割り当てて、デバイスを要求します。 [プラグアンドプレイを使用したデバイスのプロビジョニング \(262 ページ\)](#) を参照してください。

Cisco スマート アカウントの同期およびプロビジョニング

ネットワーク デバイスは、シスコのプラグアンドプレイ接続クラウドサービスによって Cisco スマート アカウントを通じて自動的に登録されます。管理者は Cisco Plug and Play Connect から Cisco DNA Center プラグ アンド プレイにデバイス インベントリを同期することができます。これにより、すべてのデバイスが Cisco DNA Center に表示されます。次に、これらのデバイスを要求してプロビジョニングすることができます。

1. スマートアカウントとバーチャルアカウントを登録して同期します。[バーチャルアカウント プロファイルの登録または編集 \(260 ページ\)](#) を参照してください。
2. スマート アカウントからデバイス インベントリを同期します。[スマート アカウントからのデバイスの追加 \(261 ページ\)](#) を参照してください。
3. 要求のないデバイスでフィルタリングするか、名前を検索して、デバイスリストのデバイスを検索します。[デバイスの表示 \(255 ページ\)](#) を参照してください。
4. サイト、イメージ、設定テンプレート、またはプロファイルを割り当てて、デバイスを要求します。[プラグアンドプレイを使用したデバイスのプロビジョニング \(262 ページ\)](#) を参照してください。
5. デバイスが起動し、自動的にプロビジョニングされます。

コントローラ ディスカバリの前提条件

プラグ アンド プレイによってデバイスのオンボーディングが自動化されます。デバイスは、Cisco DNA Center コントローラを検出して接続できるようにする必要があります。デバイスは、次のいずれかの方法でコントローラを自動的に検出できるようにする必要があります。

- DHCP : [DHCP コントローラ ディスカバリ \(252 ページ\)](#) を参照してください。
- DNS : [DNS コントローラ ディスカバリ \(254 ページ\)](#) を参照してください。
- Cisco Plug and Play Connect クラウドサービス : [Plug and Play Connect コントローラ ディスカバリ \(254 ページ\)](#) を参照してください。

DHCP コントローラ ディスカバリ

Cisco ネットワーク デバイスは、初回起動時にスタートアップコンフィギュレーションを使用しないと、DHCP オプション 43 を使用して Cisco DNA Center コントローラの検出を試行します。

DHCP による検出方法の前提条件は次のとおりです。

- 新しいデバイスが DHCP サーバにアクセスできる。
- DHCP サーバが Cisco Plug and Play のオプション 43 を使用して設定されている。このオプションにより、Cisco DNA Center コントローラの IP アドレスを持つネットワーク デバイスが通知されます。

DHCP サーバが文字列「ciscopnp」を含むオプション 60 を使用してデバイスから DHCP の検出メッセージを受信すると、オプション 43 の情報を含む応答をデバイスに返します。デバイスの Cisco Plug and Play IOS エージェントは、応答から Cisco DNA Center コントローラの IP アドレスを抽出し、このアドレスを使用してコントローラと通信します。

DHCP オプション 43 は、DHCP サーバとして機能する Cisco ルータ CLI で、次のように設定された文字列の値で構成されます。

```
ip dhcp pool pnp_device_pool          <-- Name of DHCP pool
network 192.168.1.0 255.255.255.0    <-- Range of IP addresses assigned to clients
default-router 192.168.1.1          <-- Gateway address
option 43 ascii "5A1N;B2;K4;I172.19.45.222;J80" <-- Option 43 string
```

このオプション 43 の文字列には、セミコロンで区切られた次のコンポーネントが含まれています。

- 5A1N; (プラグ アンド プレイ用の DHCP サブオプション、アクティブ動作、バージョン 1、デバッグ情報なし)。文字列のこの部分は変更する必要がありません。
- B2; (IP アドレスのタイプ) :
 - B1 = ホスト名
 - B2 = IPv4 (デフォルト)
- Ixxx.xxx.xxx.xxx; : Cisco DNA Center コントローラの IP アドレスまたはホスト名 (大文字の i の後)。この例では、IP アドレスは 172.19.45.222 です。
- Jxxxx : Cisco DNA Center コントローラへの接続に使用するポート番号。この例では、ポート番号は 80 です。HTTP のデフォルトはポート 80、HTTPS のデフォルトはポート 443 です。
- K4; : デバイスとコントローラの間で使用されるトランスポート プロトコル。
 - K4 = HTTP (デフォルト)
 - K5 = HTTPS
- TtrustpoolBundleURL : デフォルト (Cisco DNA Center コントローラ) 以外の別の場所から trustpool バンドルを取得する場合は、このオプションパラメータを使用して trustpool バンドルの外部 URL を指定します。APIC-EM コントローラは、Cisco InfoSec Cloud (<http://www.cisco.com/security/pki/>) からバンドルを取得します。たとえば、10.30.30.10 の TFTP サーバからバンドルをダウンロードするには、パラメータを「Ttftp://10.30.30.10/ios.p7b」と指定します。

trustpool セキュリティを使用していて、T パラメータを指定しない場合、デバイスは Cisco DNA Center コントローラから trustpool バンドルを取得します。
- Zxxx.xxx.xxx.xxx; (NTP サーバの IP アドレス)。trustpool セキュリティを使用してすべてのデバイスを同期させる場合、このパラメータは必須です。

DHCP の設定の詳細については、『*Cisco IOS Command Reference*』を参照してください。

DHCP オプション 43 が設定されていない場合、デバイスが DHCP サーバに接続できない場合、またはこの方法が別の理由で失敗する場合は、ネットワークデバイスで DNS を使用して検出を試行します。詳細については、「[DNS コントローラ ディスカバリ \(254 ページ\)](#)」を参照してください。

DNS コントローラ ディスカバリ

DHCP ディスカバリが Cisco DNA Center コントローラの IP アドレスを取得できない場合、ネットワークデバイスは DNS ルックアップ方式にフォールバックします。DHCP サーバから返されたネットワークドメイン名に基づき、事前設定されたホスト名「pnpserver」を使用して、コントローラの完全修飾ドメイン名 (FQDN) を作成します。NTP のサーバ名は、事前設定されたホスト名 pnpserver に基づいています。

たとえば、DHCP サーバからドメイン名「customer.com」が返された場合、ネットワーク デバイスは「pnpserver.customer.com」というコントローラの FQDN を作成します。次に、この FQDN の IP アドレスを解決するために、ローカルネームサーバを使用します。NTP サーバ名の FQDN は pnpntpserver.customer.com です。

DNS による検出方法の前提条件は次のとおりです。

- 新しいデバイスが DHCP サーバにアクセスできる。
- Cisco DNA Center コントローラがホスト名「pnpserver」を使用して展開されている。
- NTP のサーバ名はホスト名「pnpserver」で展開される。

Plug and Play Connect コントローラ ディスカバリ

DHCP または DNS による検出方法の使用がオプションでない場合は、Cisco Plug and Play Connect クラウドサービスによって、デバイスが Cisco DNA Center コントローラの IP アドレスを検出できます。ネットワーク デバイスが起動すると、DHCP または DNS を介してコントローラを特定できない場合に、devicehelper.cisco.com に接続して Plug and Play Connect を試行し、組織に定義されている適切なコントローラの IP アドレスを取得します。通信を保護するために、デバイスは Plug and Play Connect に接続するときに、最初に Cisco trustpool バンドルをダウンロードしてインストールします。

次の手順では、検出に Plug and Play Connect を使用して、Cisco Plug and Play でシスコのネットワーク デバイスを展開する方法についての概要を説明します。

始める前に

シスコのネットワーク デバイスは、Cisco Plug and Play をサポートし、Cisco Plug and Play Connect クラウドサービスに接続している Cisco IOS イメージを実行しています。

ステップ 1 ネットワーク管理者は、Cisco スマートアカウントの Web ポータルにある Plug and Play Connect を使用して、組織に適した Cisco DNA Center コントローラのコントローラ プロファイルを設定します。詳細については、web ポータルのスマートアカウントのマニュアルを参照してください。

ステップ 2 Cisco Commerce Workspace (CCW) を介してプラグアンドプレイ ネットワーク デバイスを注文した場合、Cisco スマート アカウントが注文に割り当てられていれば、Plug and Play Connect を使用してネットワーク デバイスが自動的に登録されます。Cisco Plug and Play で使用する各デバイスに、NETWORK-PNP-LIC オプションを追加します。

このオプションにより、デバイスのシリアル番号と PID がプラグアンドプレイ用にスマートアカウントで自動登録されます。デフォルト コントローラを指定済みの場合、注文の処理時にデバイスがそのコントローラに自動的に割り当てられます。

ステップ 3 または、Plug and Play Connect の Web ポータルからデバイスを手動で追加することもできます。

ステップ 4 Cisco DNA Center を、Cisco Plug and Play Connect のコントローラとして、リダイレクト サービス用に Cisco スマートアカウントに登録します。 [バーチャルアカウントプロファイルの登録または編集 \(260 ページ\)](#) を参照してください。

CCW を通してプラグアンドプレイ ネットワーク デバイスを注文し、これらのネットワーク デバイスがスマートアカウント経由で Plug and Play Connect に自動登録される場合には、この手順が必須です。

ステップ 5 Cisco Plug and Play Connect クラウドポータルのスマートアカウントから、デバイス インベントリを Cisco DNA Center プラグアンドプレイに同期します。

Plug and Play Connect の Web ポータルに登録されたデバイスがコントローラに同期され、SmartAccount のソースとともにプラグアンドプレイのデバイス リストに表示されます。

ステップ 6 新しく同期されたデバイスを要求します。 [プラグアンドプレイを使用したデバイスのプロビジョニング \(262 ページ\)](#) を参照してください。

ステップ 7 デバイス インストーラによって、シスコ ネットワーク デバイスがインストールされ、電源が投入されません。

ステップ 8 デバイスは、Plug and Play Connect サービスをクエリして Cisco DNA Center コントローラを検出し、Cisco DNA Center でプラグアンドプレイのシリアル番号によってコントローラを識別します。次に、要求プロセス中に計画された内容に従ってプロビジョニングされます。



(注) デバイスが定義済みの NTP サーバ **time-pnp.cisco.com** または **pool.ntp.org** と同期できない場合、デバイスは Plug and Play Connect のコンタクトに失敗します。この問題を解決するには、これらの 2 つのホスト名への NTP トラフィックをブロック解除するか、これら 2 つの NTP ホスト名を DNS サーバのローカル NTP サーバアドレスにマップします。

デバイスの表示

この手順では、プラグアンドプレイデバイスを表示する方法、デバイスでアクションを実行する方法、および新しいデバイスを追加する方法について説明します。

ステップ 1 Cisco DNA Center のホームページで、**[Provision] > [Devices] > [Plug and Play]** の順に選択します。

ステップ 2 テーブル内のデバイスを表示します。

[Filter] オプションを使用して、特定のデバイスを検索します。[Refresh] をクリックして、デバイスリストを更新します。

ステップ 3 デバイスの名前をクリックします。

デバイスの詳細を示すウィンドウが表示されます。

ステップ 4 [Details]、[History]、[Configuration]、または [Stack] タブをクリックして、デバイスに関するさまざまな種類の情報を表示します。一部のタブには、クリックして詳細を表示できる追加のリンクがあります。

[スタック (Stack)] タブは、スイッチ スタック デバイスの場合にのみ表示されます。

ステップ 5 デバイスで特定のタスクを実行するには、ダイアログボックスの上部にある次のアクションをクリックします。使用可能なアクションは、デバイスの状態によって異なります。

- [Refresh] : デバイス状態情報を更新します。
- [Claim] : デバイスを要求しプロビジョニングします。 [プラグアンドプレイを使用したデバイスのプロビジョニング \(262 ページ\)](#) を参照してください。
- [Edit] : デバイスを編集します。 [デバイスの追加または編集 \(258 ページ\)](#) を参照してください。
- [Reset] : デバイスがエラー状態になっている場合に、デバイスをリセットします。 [デバイスのリセット \(271 ページ\)](#) を参照してください。
- [Delete] : デバイスを削除します。 [デバイスの削除 \(271 ページ\)](#) を参照してください。

ステップ 6 複数のデバイスに対してアクションを実行するには、テーブルビューで各デバイスの横にあるチェックボックスをオンにし、[Actions] ドロップダウンメニューからアクションを選択します。

ステップ 7 [Add Device] をクリックして、新しいデバイスを追加します。

デバイスを追加する各種方法についての詳細は、次を参照してください。 [デバイスの追加または編集 \(258 ページ\)](#)、 [Add Devices in Bulk \(259 ページ\)](#)、 [スマートアカウントからのデバイスの追加 \(261 ページ\)](#)

デバイステーブルには、各デバイスについて、以下の表に示した情報が表示されます。すべての列はソートに対応しています。列ヘッダーをクリックすると、行が昇順にソートされます。列ヘッダーをもう一度クリックすると、行が降順にソートされます。



(注) デフォルトの列表示設定では一部の列が非表示になっています。これは、列の見出しの右端にある 3 つの点 (⋮) をクリックするとカスタマイズできます。

表 45: デバイス情報

カラム	説明
#	行番号。

カラム	説明
Device Name	デバイスのホスト名。このリンクをクリックすると、デバイスの詳細ウィンドウが開きます。スタックアイコンはスイッチスタックを示します。
シリアル番号 (Serial Number)	デバイスのシリアル番号。
製品 ID	デバイスの製品 ID。
Source	デバイスエントリの送信元： <ul style="list-style-type: none"> • [User]：ユーザが GUI または API を介してデバイスを追加しました。 • [Network]：コントローラに接続されたデバイスが要求解除されました。 • [SmartAccount]：デバイスはスマートアカウントから同期されました。
State	<ul style="list-style-type: none"> • [Unclaimed]：デバイスはプロビジョニングされていません。 • [Planned]：デバイスはすでに要求されていますが、まだサーバと接続していません。 • [Onboarding]：デバイスオンボーディングが進行中です。 • [Provisioned]：デバイスは正常にオンボーディングされ、インベントリに追加されています。 • [Error]：デバイスにエラーがあり、プロビジョニングできませんでした。
Onboarding State	デバイスのオンボーディング状態。
Site	デバイスが関連付けられているサイト。
Last Contact	デバイスが最後にプラグアンドプレイに接続した日時。
Smart Acct	デバイスが関連付けられている Cisco スマート アカウント。
Virtual Acct	デバイスが関連付けられている (Cisco スマート アカウント内の) バーチャルアカウント。
Created	デバイスがプラグアンドプレイに追加された日時。

デバイスの追加または編集

この手順では、[Plug and Play Devices] リストのデバイスを追加または編集する方法について説明します。代わりに、[編集 (Edit)] をクリックしてデバイスの詳細ウィンドウからデバイスを編集することもできます。

表 46: [デバイス (Device)] フィールド

フィールド	説明
Serial Number	デバイス シリアル番号 (デバイスを編集している場合は読み取り専用)。
Product ID	デバイス製品 ID (デバイスを編集している場合は読み取り専用)。
Device Name	デバイス名
Enable SUDI Authorization	セキュアな固有デバイス識別子 (SUDI) 認証をサポートするデバイスで有効にします。
SUDI Serial Numbers	SUDI をサポートするデバイスには、シャーシのシリアル番号と SUDI シリアル番号 (デバイス ラベルのライセンス SN と呼ばれる) の 2 つのシリアル番号があります。SUDI 認証を使用するデバイスを追加するときは、このフィールドに 1 つまたは複数の SUDI シリアル番号をカンマで区切って入力します。このフィールドは、[SUDI 認証の有効化 (Enable SUDI Authorization)] がチェックされている場合のみ表示されます。
This Device Represents a Stack	デバイスがスタックを表します (デバイスを編集している場合、この項目は読み取り専用です)。サポート対象のスタックブルスイッチにのみ適用されます。

始める前に

デバイスにクレデンシャルが必要な場合は、グローバル デバイス クレデンシャルが [設計 (Design)] > [ネットワーク設定 (Network Settings)] > [デバイス クレデンシャル (Device Credentials)] ページで設定されていることを確認します。詳細については、[グローバル CLI クレデンシャルの設定 \(150 ページ\)](#) を参照してください。

ステップ 1 Cisco DNA Center のホームページで、[Provision] > [Devices] > [Plug and Play] の順に選択します。

ステップ 2 テーブル内のデバイスを表示します。

[Filter] オプションを使用して、特定のデバイスを検索します。[Refresh] をクリックして、デバイスリストを更新します。

ステップ 3 次のようにデバイスを追加または編集します。

- デバイスを追加するには、[Add Device] をクリックします。[Add Devices] ダイアログが表示されます。
- デバイスを編集するには、編集するデバイス名の横にあるチェックボックスをオンにして、デバイステーブルの上部にあるメニューバーから[アクション (Actions)] > [編集 (Edit)] をクリックします。
[デバイスの編集 (Edit Device)] ダイアログが表示されます。

ステップ 4 必要に応じてフィールドを設定します。詳細については上記の表を参照してください。

ステップ 5 次のいずれかの操作を実行して、設定を保存します。

- デバイスを追加し、後で要求するには、[デバイスの追加 (Add Device)] をクリックします。
- デバイスを追加し、すぐに要求するには、[追加 + 要求 (Add + Claim)] をクリックします。デバイスの要求の詳細については [プラグアンドプレイを使用したデバイスのプロビジョニング \(262 ページ\)](#)、を参照してください。
- デバイスを編集する場合は、[デバイスの編集 (Edit Device)] をクリックします。

Add Devices in Bulk

この手順では、CSV ファイルからデバイスを一括で追加する方法を示します。



- (注) プラグアンドプレイにすでに存在するデバイスを追加する場合、既存のデバイスに対する変更はありません。

ステップ 1 Cisco DNA Center のホームページで、[Provision] > [Devices] > [Plug and Play] の順に選択します。

ステップ 2 [Add Device] をクリックします。

[デバイスの追加 (Add Device)] ダイアログが表示されます。

ステップ 3 [一括デバイス (Bulk Devices)] タブをクリックします。

ステップ 4 [ファイル テンプレートのダウンロード (Download File Template)] をクリックしてサンプル ファイルをダウンロードします。

ステップ 5 各デバイスの情報をファイルに追加し、ファイルを保存します。デバイスタイプによっては、特定のフィールドが必須になることに注意してください。

ステップ 6 次のアクションのいずれかを実行して、CSV ファイルをアップロードします。

- ドラッグアンドドロップエリアにファイルをドラッグアンドドロップします。
- [クリックして選択 (click to select)] が表示される場所をクリックしてファイルを選択します。

ステップ 7 [デバイスのインポート (Import Devices)] をクリックします。

CSV ファイル内のデバイスがテーブルにリストされます。

ステップ 8 インポートする各デバイスの横にあるチェックボックスをオンにするか、上部にあるチェックボックスをオンにしてすべてのデバイスを選択します。

ステップ 9 次のいずれかの操作を実行して、デバイスを追加します。

- デバイスを追加し、それらを後で要求するには、[デバイスの追加 (Add Devices)] をクリックします。
- デバイスを追加し、それらをすぐに要求するには、[追加 + 要求 (Add + Claim)] をクリックします。デバイスの要求の詳細については [プラグアンドプレイを使用したデバイスのプロビジョニング \(262 ページ\)](#)、を参照してください。

バーチャルアカウント プロファイルの登録または編集

この手順により、Cisco DNA Center コントローラを、リダイレクション サービス向けの Cisco スマートアカウントに、Cisco Plug and Play Connect のデフォルトのコントローラとして登録できます。また、これによって Cisco Plug and Play Connect クラウドポータルから Cisco DNA Center プラグアンドプレイにデバイスインベントリを同期することができます。

表 47: バーチャルアカウント フィールド

フィールド	説明
Select Smart Account	Cisco スマートアカウント名
Select Virtual Account	バーチャルアカウント名バーチャルアカウントは、Cisco スマートアカウント内のサブアカウントです。
Use as Default Controller Profile	Cisco DNA Center コントローラを Cisco プラグアンドプレイ接続のクラウドポータルにデフォルトコントローラとして登録するには、このボックスにチェックを付けます。
Controller IP or FQDN	この Cisco DNA Center コントローラの IP アドレスまたは完全修飾ドメイン名。
Profile Name	コントローラのプロファイル名

始める前に

メインの Cisco DNA Center の設定で、[システム設定 (System Settings)] > [設定 (Configurations)] > [Cisco クレデンシヤル (Cisco Credentials)] を使って、Cisco スマートアカウントのクレデンシヤルを設定します。詳細については、「[Cisco Digital Network Architecture Center 管理者ガイド](#)」の「Cisco クレデンシヤルの設定」を参照してください。

ステップ 1 Cisco DNA Center のホームページで、[システム設定 (System Settings)] > [設定 (Settings)] > [シスコクレデンシヤル (Cisco Credentials)] の順にクリックします。

ステップ 2 [PnP Connect] タブをクリックします。

このテーブルには、登録されている Plug and Play Connect のバーチャルアカウントプロファイルがすべて一覧表示されます。

ステップ3 次のように、バーチャルアカウントプロファイルを追加または編集します。

- バーチャルアカウントを登録するには、[Add] をクリックします。[register virtual account] ダイアログが表示されます。
- 登録済みのバーチャルアカウントプロファイルを編集するには、編集したいプロファイル名の横にあるラジオボタンをクリックし、テーブルの上にあるメニューバーの[プロファイルの編集 (EditProfile)] をクリックします。[バーチャルアカウントの編集 (edit virtual account)] ダイアログが表示されます。

ステップ4 上掲の「バーチャルアカウントフィールド」表を参照して、必要に応じてフィールドを設定します。

ステップ5 次のいずれかの操作を実行して、設定を保存します。

- 新しいバーチャルアカウントプロファイルを登録する場合は、[登録 (Register)] をクリックします。
- バーチャルアカウントプロファイルを編集する場合は、[変更 (Change)] をクリックします。

次のタスク

Cisco Plug and Play Connect クラウドポータルから、デバイスインベントリを Cisco DNA Center プラグアンドプレイに同期します。詳細については、「[スマートアカウントからのデバイスの追加 \(261 ページ\)](#)」を参照してください。

スマートアカウントからのデバイスの追加

このタスクにより、Cisco Plug and Play Connect クラウドポータルのスマートアカウントから Cisco DNA Center プラグアンドプレイにデバイスインベントリを同期することができます。

バーチャルアカウントテーブルには、プロファイルごとに以下の情報が表示されます。

表 48: バーチャルアカウント情報

カラム	説明
バーチャルアカウント	バーチャルアカウント名
スマートアカウント	バーチャルアカウントが関連付けられているスマートアカウント
同期ステータス	直近の同期プロセスのステータス

始める前に

Cisco プラグアンドプレイ接続クラウドポータルからデバイスインベントリを同期する前に、バーチャルアカウントを登録する必要があります。[バーチャルアカウントプロファイルの登録または編集 \(260 ページ\)](#) を参照してください。

ステップ 1 Cisco DNA Center のホームページで、**[Provision] > [Devices] > [Plug and Play]** の順に選択します。

ステップ 2 **[Add Device]** をクリックします。

[デバイスの追加 (Add Device)] ダイアログが表示されます。

ステップ 3 **[スマートアカウントデバイス (Smart Account Devices)]** タブをクリックします。

ステップ 4 デバイスを追加する **Plug and Play Connect** バーチャルアカウントプロファイルの名前の横にあるラジオボタンをクリックします。

ステップ 5 **[同期 (Sync)]** をクリックして、このバーチャルアカウントの **Cisco Plug and Play Connect** から **Cisco DNA Center** プラグアンドプレイに、デバイスインベントリを同期させます。

追加されたデバイスは、**SmartAccount** に設定されたソースとともに **[プラグアンドプレイデバイス (Plug and Play Devices)]** テーブルに表示されます。

次のタスク

新しく同期されたデバイスを要求します。デバイスの要求の詳細については [プラグアンドプレイを使用したデバイスのプロビジョニング \(262 ページ\)](#) 、を参照してください。

プラグアンドプレイを使用したデバイスのプロビジョニング

デバイスのプロビジョニングまたは要求では、イメージとオンボーディングの設定をデバイスに展開するか、ワイヤレスデバイスのネットワークプロファイルを展開して、それをインベントリに追加してプロビジョニングします。まだ起動していないデバイスを初めて要求する場合は、起動時に自動的にプロビジョニングされるようにデバイスを計画します。

デバイスをプロビジョニングするためのワークフローは、デバイスのタイプによって次のように異なります。

- スイッチとルータの参照資料：[スイッチまたはルータデバイスのプロビジョニング \(262 ページ\)](#)
- ワイヤレスアクセスポイントおよびセンサーの参照資料：[ワイヤレスまたはセンサーデバイスのプロビジョニング \(267 ページ\)](#)

スイッチまたはルータ デバイスのプロビジョニング

デバイスを要求すると、それをサイトに割り当て、イメージをインストールし、サイト設定とオンボーディングの設定を展開して、インベントリに追加することでプロビジョニングされます。まだ起動していないデバイスを初めて要求する場合は、起動時に自動的にプロビジョニングされるようにデバイスを計画します。

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

され、システム設定を上書きします。システムによってプッシュされる CLI コマンドには、次のものがあります。

- デバイスのログイン情報 (CLI および SNMP)
- SSH v2 と SCP サーバの有効化
- HTTP と HTTPS サーバの無効化
- スイッチの場合、VTP トランスペアレントモードが有効になっている



(注) デバイスの制御性が有効 (デフォルト設定) になっている場合、デバイスがインベントリに追加されるときに次の設定が追加されます。

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

この手順では、[Plug and Play] デバイスリストからデバイスを要求する方法について説明します。代わりに、[要求 (Claim)] をクリックしてデバイスの詳細ウィンドウからデバイスを要求することもできます。

始める前に

- プロビジョニングするシスコネットワークデバイスについて、サポートされているソフトウェアリリースがあり、工場出荷時のデフォルト状態になっていることを確認します。以前に設定されたネットワークデバイス、または不明な状態になっているネットワークデバイスを使用している場合は、[Cisco Digital Network Architecture Center のネットワーク プラグアンドプレイのトラブルシューティング ガイド \[英語\]](#) のデバイスのクリーンアップとリセットの詳細を参照してください。
- プロビジョニングされているデバイスで Cisco DNA Center を検出して接続できることを確認します。詳細については、「[コントローラ ディスカバリの前提条件 \(252 ページ\)](#)」を参照してください。
- ネットワーク階層内のサイトを定義します。[About Network Hierarchy \(94 ページ\)](#) を参照してください。
- デバイスの CLI および SNMP ログイン情報を定義します。[デバイス クレデンシャルについて \(147 ページ\)](#) を参照してください。

- (オプション) イメージを展開する場合は、プロビジョニングされるデバイスのソフトウェアイメージをアップロードし、イメージリポジトリ内でゴールデンとしてマークされるようにします。 [ソフトウェアイメージのインポート \(77 ページ\)](#) を参照してください。



(注) Day-0 プロビジョニング中にプラグアンドプレイで 사용되는イメージ導入プロセスは、後でデバイスイメージの更新時に使用されるプロセスと同じではありません。これは [ソフトウェアイメージのプロビジョニング \(81 ページ\)](#) で説明されています。プラグアンドプレイ プロビジョニングでは、デバイスが工場出荷時のデフォルト状態にあると想定されているため、デバイスの事前チェック、自動フラッシュクリーンアップ、事後チェックは行われません。

- 必要に応じて、デバイスに適用する [Onboarding Configuration] テンプレートを定義します。このようなテンプレートには、ネットワーク上で管理できるようにデバイスをオンボードするための基本的なネットワーク設定コマンドが含まれています。ほとんどの場合、Day-0 設定をカスタマイズする必要がない限り、このようなテンプレートは必要ありません。 [デバイス設定の変更を自動化するテンプレートの作成 \(167 ページ\)](#) を参照してください。



(注) Onboarding Configuration テンプレートで `ip http client source-interface` CLI コマンドを使用すると、Cisco DNA Center は、IP や VRF が複数あるケースなどを筆頭に、IP アドレスをデバイスの管理用 IP アドレスとして利用できます。

- デバイスのネットワーク プロファイルを定義します。 [ネットワーク プロファイルの作成 \(140 ページ\)](#) を参照してください。

ステップ 1 Cisco DNA Center のホームページで、[Provision] > [Devices] > [Plug and Play] の順に選択します。

ステップ 2 テーブル内のデバイスを表示します。

[フィルタ (Filter)] または [検索 (Find)] オプションを使用して、特定のデバイスを見つけることができます。

ステップ 3 要求する 1 つ以上のデバイスの横にあるチェックボックスをオンにします。

ステップ 4 デバイステーブルの上にあるメニューバーで、[アクション (Actions)] > [要求 (Claim)] をクリックします。

[デバイスの要求 (Claim Devices)] ウィンドウが開き、最初の手順「サイトの割り当て」が表示されます。

ステップ5 (オプション) 必要に応じて、最初の列のデバイスのホスト名を変更します。

ステップ6 [Select a Site] ドロップダウンリストから、各デバイスに割り当てるサイトを選択します。

最初のデバイスと同じサイトをすべてのデバイスに適用するには、[Apply Site to All] チェックボックスをオンにします。あるデバイスのサイトを別のデバイスに割り当てるには、[Assign this Site to Other Devices] をクリックし、デバイスを選択して [Assign] をクリックします。

ステップ7 [Next] をクリックします。

[設定 (Configuration)] ウィンドウが表示されます。

ステップ8 (オプション) 次のように、デバイステーブルに対するグローバルな変更を行います。

- テーブルに表示される列を変更するには、表の見出しの右端にある3つの点をクリックし、目的の列を選択します。[Apply] をクリックして、変更内容を保存します。
- [Clear Images] をクリックして、デバイス用に設定されたデフォルトイメージをクリアします。イメージをクリアする各デバイスのチェックボックスをオンにして、[Clear] をクリックします。
- [Clear Templates] をクリックして、デバイス用に設定されたデフォルトテンプレートをクリアします。テンプレートをクリアする各デバイスのチェックボックスをオンにして、[Clear] をクリックします。
- デバイスに設定されているライセンスレベルをクリアするには、[Clear License Levels] をクリックします。ライセンスレベルをクリアする各デバイスのチェックボックスをオンにして、[Clear] をクリックします。
- デバイスの横にある [Actions] 列の3つの点をクリックし、[Apply Image to Other Devices] または [Apply Template to Other Devices] を選択することで、あるデバイスのイメージまたはテンプレートを他のデバイスに適用できます。スタック構成のデバイスの場合は、[Apply License Level to Other Devices] をクリックして、デバイスのライセンスレベルを他のデバイスに適用できます。

ステップ9 設定するデバイスの名前をクリックし、次の手順を実行します。

- デバイス設定の概要を表示し、変更が不要な場合は [Cancel] をクリックします。
- (オプション) 必要に応じて [Device Name] フィールドでデバイスのホスト名を変更します。
- (オプション) [イメージ (Image)] ドロップダウンリストで、デバイスに適用するゴールデンソフトウェア イメージを選択します。イメージリポジトリにこのデバイスタイプのゴールデンイメージが1つしかない場合は、そのイメージがデフォルトで選択されます。
- (オプション) [テンプレート (Template)] ドロップダウンリストで、デバイスに適用する [オンボーディングの設定 (onboarding configuration)] テンプレートを selects します。このデバイスタイプに対して定義されているオンボーディング設定テンプレートが1つしかない場合は、そのテンプレートがデフォルトで選択されます。

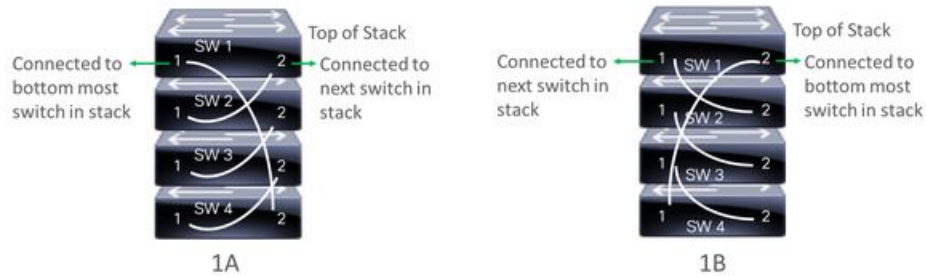
選択したテンプレートの横にある [Preview] をクリックすると、テンプレートが表示されます。

- (オプション) スタックの番号を付け直す場合は、[Select a Cabling Scheme] ドロップダウンリストで、スタックのケーブル配線方式を選択します。

この項目は、スタック構成をサポートしているスイッチが次のいずれかのケーブル配線方式に従って接続されている場合にのみ表示されます。

図 5: ケーブル配線方式

Supported Stack Switch Wiring Schemes:



- f) (オプション) スタックの番号を付け直す場合は、[Select a Top of Stack serial Number] ドロップダウンリストで、スタックスイッチの先頭のシリアル番号を選択します。

この項目は、スタック構成をサポートしているスイッチが図のように接続されている場合にのみ表示されます。

- g) (オプション) [ライセンスレベルの選択 (Select a License Level)] ドロップダウンリストで、スタックのライセンスレベルを選択します。

この項目は、スタック構成をサポートしているスイッチにのみ表示されます。

- h) 変更した場合は、[Save] をクリックします。それ以外の場合は、[Cancel] をクリックしてリストに戻り、他のデバイスを設定します。

ステップ 10 複数のデバイスを選択してプロビジョニングした場合は、リストで次のデバイスをクリックし、この設定手順を繰り返します。これを、すべてのデバイスに対して実行します。

ステップ 11 [次へ (Next)] をクリックします。

[Advanced Configuration] ウィンドウが表示されます。ここでは、テンプレートに定義されたパラメータの値を指定できます。

ステップ 12 設定するデバイスの名前をクリックし、次の手順を実行します。

- a) デバイスに設定テンプレートが割り当てられている場合は、テンプレートで定義されたパラメータの値を指定します。

各デバイスのフィールドに各パラメータの値を入力します。赤のアスタリスクは、必須フィールドを示します。

- b) 複数のデバイスを選択してプロビジョニングした場合は、ウィンドウの左側にあるリストで次のデバイスをクリックし、パラメータ値を入力します。これを、すべてのデバイスに対して実行します。

- c) 以前に展開されていた場合でも、リストされているすべてのデバイスに設定をプッシュするには、[Push these templates even if its deployed before] チェックボックスをオンにします。

ステップ 13 すべてのデバイスのパラメータ値を一括で指定するには、次の手順を実行します。

- a) [エクスポート (Export)] をクリックして、CSV テンプレートファイルを保存します。
 b) 各パラメータの値をファイルに追加して、ファイルを保存します。
 c) [Import] をクリックします。

- d) ドラッグアンドドロップエリアにファイルをドラッグアンドドロップするか、[クリックして選択 (click to select)] と表示されている場所をクリックしてファイルを選択します。
- e) [Import] をクリックします。

ステップ 14 [次へ (Next)] をクリックします。

[Summary] ウィンドウが表示されます。ここで、デバイスに関する詳細や設定プレビューステータスを確認できます。

ステップ 15 設定プレビューが成功したかどうかを確認するには、各デバイスの [Day-0 Config Preview Status] 列をチェックします。

プレビューでエラーが表示された場合は、デバイスを要求する前に問題を解決してプロビジョニングエラーを回避する必要があります。「詳細設定」手順に戻ってパラメータ値やテンプレートを変更したり、[設計 (Design)] エリアに再度アクセスしてネットワーク設計の設定を更新したり、ネットワーク接続の問題を解決したりすることが必要になる場合があります。

ステップ 16 デバイス名をクリックすると、デバイス、デバイスの設定、および設定プレビューエラーに関する詳細情報が表示されます。

ステップ 17 [要求 (Claim)] をクリックします。

確認のダイアログボックスが表示されます。

ステップ 18 [Yes] をクリックしてデバイスを要求します。

次のタスク

プロビジョニングプロセスを完了するには、デバイスがインベントリに追加された後、[Inventory] タブに移動し、デバイスを選択し、[Actions] > [Provision] > [Provision Device] をクリックします。すべての手順を実行し、[Summary] ステップで [Deploy] をクリックします。デバイスにプッシュされる残りのネットワーク設定が [Summary] に表示されます。詳細については、「[デバイスのプロビジョニング \(276 ページ\)](#)」を参照してください。このプロセスは、[Design] 領域で設定した可能性のあるネットワーク設定をプッシュする場合に必要です。プラグアンドプレイのプロビジョニング中に、デバイスのログイン情報とオンボーディング設定のみがデバイスにプッシュされます。[Inventory] からのプロビジョニングが完了するまで、他のネットワーク設定はプッシュされません。さらに、デバイスは、RADIUS および TACACS の AAA クライアントとして Cisco DNA Center によって ISE に追加されます (そのように設定されている場合)。

ワイヤレスまたはセンサー デバイスのプロビジョニング

デバイスを要求すると、デバイスにネットワークプロファイルを割り当て、それをインベントリに追加することでプロビジョニングされます。まだ起動していないデバイスを初めて要求する場合は、起動時に自動的にプロビジョニングされるようにデバイスを計画します。

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

され、システム設定を上書きします。システムによってプッシュされる CLI コマンドには、次のものがあります。

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



(注) デバイスの制御性が有効 (デフォルト設定) になっている場合、デバイスがインベントリに追加されるときの次の設定が追加されます。

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

この手順では、メインの [Plug and Play] タブからデバイスを要求する方法について説明します。代わりに、[要求 (Claim)] をクリックしてデバイスの詳細ウィンドウからデバイスを要求することもできます。

始める前に

- プロビジョニングするシスコネットワークデバイスについて、サポートされているソフトウェアリリースがあり、工場出荷時のデフォルト状態になっていることを確認します。以前に設定されたネットワークデバイス、または不明な状態になっているネットワークデバイスを使用している場合は、[Cisco Digital Network Architecture Center のネットワーク プラグアンドプレイのトラブルシューティング ガイド \[英語\]](#) のデバイスのクリーンアップとリセットの詳細を参照してください。
- プロビジョニングされているデバイスで Cisco DNA Center を検出して接続できることを確認します。詳細については、「[コントローラ ディスカバリの前提条件 \(252 ページ\)](#)」を参照してください。
- ネットワーク階層内のサイトを定義します。[About Network Hierarchy \(94 ページ\)](#) を参照してください。
- デバイスの CLI および SNMP ログイン情報を定義します。[デバイス クレデンシャルについて \(147 ページ\)](#) を参照してください。

- ワイヤレス アクセス ポイント デバイスをプロビジョニングするには、ワイヤレス アクセス ポイントを管理しているワイヤレス LAN コントローラがインベントリに追加され、ワイヤレス デバイスが割り当てられているサイトに割り当てられていることを確認します。この手順は **Mobility Express** アクセスポイントには必要ありません。
- センサー デバイスをプロビジョニングするには、センサーが **Cisco DNA Center** エンタープライズ IP アドレス (`private/enp9s0`) を介して到達可能であることを確認します。DHCP オプション 43 の文字列を使用すると、デバイスが **Cisco DNA Center** の未要求モードで到達可能になります。ただし、デバイスを要求するには、インターフェイス `enp9s0` IP アドレスから到達可能である必要があります。DHCP サーバで ASCII 値「5A1D;B2;K4;I172.16.x.x;J80」を使用して、NTP サーバ (DHCP オプション 42) とベンダー固有の DHCP オプション 43 を設定します。ここで、172.16.x.x は `enp9s0` インターフェイスに関連付けられた **Cisco DNA Center** の仮想 IP アドレスです。
- ワイヤレス アクセス ポイント デバイスのワイヤレス無線周波数プロファイルを定義し、**Mobility Express** アクセスポイントを除く。 [ワイヤレス無線周波数プロファイルの作成 \(133 ページ\)](#) を参照してください。
- ワイヤレスセンサーデバイスのバックホール設定を行います。 [バックホール設定の管理 \(136 ページ\)](#) を参照してください。
- **Mobility Express** アクセスポイントの場合は、IP アドレスプールと管理インターフェイスを定義します。 [IP アドレスプールを設定する \(158 ページ\)](#) を参照してください。

ステップ 1 Cisco DNA Center のホームページで、**[Provision] > [Devices] > [Plug and Play]** の順に選択します。

ステップ 2 テーブル内のデバイスを表示します。

[フィルタ (Filter)] または **[検索 (Find)]** オプションを使用して、特定のデバイスを見つけることができます。

ステップ 3 要求する 1 つ以上のワイヤレスデバイスの横にあるチェックボックスをオンにします。

ステップ 4 デバイス表の上にあるメニューバーで、**[Actions] > [Claim]** の順に選択します。

[デバイスの要求 (Claim Devices)] ウィンドウが開き、最初の手順「サイトの割り当て」が表示されます。

ステップ 5 (任意) 必要に応じて、最初の列のデバイス名を変更します。

ステップ 6 (任意) 必要に応じて、2 番目の列のデバイスタイプを変更します。デバイスが使用しているモードに応じて、AP (アクセスポイント) または ME (**Mobility Express**) を選択できます。

誤ったモードを選択すると、デバイスのプロビジョニングエラーにつながります。この項目は、センサーデバイスには表示されません。

ステップ 7 **[Select a Site]** ドロップダウンリストから、各デバイスに割り当てるサイトとフロアを選択します。アクセスポイントデバイスは、ワイヤレスコントローラを備えたフロアに割り当てる必要があります。

最初のデバイスと同じサイトをすべてのデバイスに適用するには、**[Apply Site to All]** チェックボックスをオンにします。あるデバイスのサイトを別のデバイスに割り当てるには、**[Assign this Site to Other Devices]**

をクリックし、デバイスを選択して [Assign] をクリックします。ワイヤレスデバイスは、ビルディング自体ではなくビルディング内のフロアにのみ割り当てることができます。

ステップ 8 [Next] をクリックします。

[設定 (Configuration)] ウィンドウが表示されます。

ステップ 9 (任意) テーブルに表示される列を変更するには、表の見出しの右端にある 3 つの点をクリックし、目的の列を選択します。[Apply] をクリックして、変更内容を保存します。

ステップ 10 設定するデバイスの名前をクリックし、次の手順を実行します。

- a) デバイス設定の概要を表示し、変更が不要な場合は [Cancel] をクリックします。
- b) (任意) [Device Name] フィールドで、必要に応じてデバイス名を変更します。
- c) アクセスポイントデバイスの場合、[RF Profile] ドロップダウンリストで、デバイスに適用する RF プロファイルを選択します。これは、1 つのプロファイルをデフォルトとして指定した場合に設定できます。
- d) Mobility Express デバイスの場合は、[Management IP]、[Subnet Mask]、および [Gateway] の各フィールドに値を入力します。
- e) ワイヤレスセンサーデバイスの場合、[Sensor Settings] ドロップダウンリストで、デバイスに適用するセンサー デバイス プロファイルを選択します。
- f) 変更した場合は、[Save] をクリックします。それ以外の場合は、[Cancel] をクリックしてリストに戻り、他のデバイスを設定します。
- g) [Actions] 列の [Apply ... to Other Devices] をクリックして、あるデバイスに割り当てた設定を同じタイプの他のデバイスに適用できます。

ステップ 11 複数のデバイスを選択してプロビジョニングした場合は、リストで次のデバイスをクリックし、この設定手順を繰り返します。これを、すべてのデバイスに対して実行します。

ステップ 12 [次へ (Next)] をクリックします。

[Summary] ウィンドウが表示されます。ここで、デバイスや設定に関する詳細を確認できます。

ステップ 13 設定プレビューが成功したかどうかを確認するには、各デバイスの [Day-0 Config Preview Status] 列をチェックします。

プレビューでエラーが表示された場合は、デバイスを要求する前に問題を解決してプロビジョニングエラーを回避する必要があります。[Configuration] 手順に戻って設定を変更したり、[Design] エリアに再度アクセスしてネットワーク設計の設定を更新したり、ネットワーク接続の問題を解決したりすることが必要になる場合があります。デバイスを管理しているワイヤレス LAN コントローラがインベントリに追加され、ワイヤレスデバイスが割り当てられているサイトに割り当てられていることを確認します。

ステップ 14 [要求 (Claim)] をクリックします。

確認のダイアログボックスが表示されます。

ステップ 15 [Yes] をクリックしてデバイスを要求し、プロビジョニングプロセスを開始します。

次のタスク

プロビジョニングプロセスを完了するには、デバイスがインベントリに追加された後、[Inventory] タブに移動し、デバイスを選択し、[Actions] > [Provision] > [Provision Device] をクリックします。すべての手順を実行し、[Summary] ステップで [Deploy] をクリックします。デバイスに

プッシュされる残りのネットワーク設定が [Summary] に表示されます。詳細については、[デバイスのプロビジョニング \(276 ページ\)](#) を参照してください。このプロセスは、[Design] 領域で設定した可能性のあるネットワーク設定をプッシュする場合に必要です。プラグアンドプレイのプロビジョニング中に、デバイスのログイン情報とオンボーディング設定のみがデバイスにプッシュされます。[Inventory] からのプロビジョニングが完了するまで、他のネットワーク設定はプッシュされません。さらに、デバイスは、RADIUS および TACACS の AAA クライアントとして Cisco DNA Center によって ISE に追加されます (そのように設定されている場合)。

デバイスの削除

デバイスを削除すると、デバイスはプラグアンドプレイのデータベースから削除されますが、リセットはされません。エラー状態のデバイスをリセットする場合は、[Reset] を使用します。

この手順では、[プラグアンドプレイ (Plug and Play)] タブからデバイスを削除する方法について説明します。代わりに、[削除 (Delete)] をクリックしてデバイスの詳細ウィンドウからデバイスを削除することもできます。



(注) デバイスがプロビジョニングの状態の場合は、[Inventory] タブからのみ削除できます。

ステップ 1 Cisco DNA Center のホームページで、[Provision] > [Devices] > [Plug and Play] の順に選択します。

ステップ 2 テーブル内のデバイスを表示します。

[Filter] オプションを使用して、特定のデバイスを検索します。[Refresh] をクリックしてデバイスリストを更新します。

ステップ 3 削除する 1 つ以上のデバイスの横にあるチェックボックスをオンにします。

ステップ 4 デバイス テーブルの上にあるメニューバーで、[アクション (Actions)] > [削除 (Delete)] をクリックします。

確認のダイアログボックスが表示されます。

ステップ 5 [Yes] をクリックして、このデバイスを削除することを確認します。

デバイスのリセット

デバイスのリセットはエラー状態のデバイスにのみ適用され、状態が [Unclaimed] にリセットされデバイスがリロードされますが、プラグアンドプレイ データベースからは削除されません。デバイスを削除する場合は、[削除 (Delete)] を使用します。



(注) デバイスで保存された設定が工場出荷時のデフォルトまたは同様の最小限の設定である場合、このオプションを選択すると、デバイスはプロビジョニングプロセスを再起動します。ただし、デバイスに以前に保存されたスタートアップコンフィギュレーションがある場合は、これによってデバイスのプロビジョニングプロセスの再起動を回避できますが、工場出荷時のデフォルトにリセットする必要があります。ワイヤレスデバイスおよびセンサーデバイスでは、デバイスの状態だけがリセットされ、デバイスはリロードされません。

この手順では、**[プラグアンドプレイ (Plug And Play)]** タブからデバイスをリセットする方法について説明します。代わりに、**[Reset]** をクリックしてデバイスの詳細ウィンドウからリセットすることもできます。

ステップ 1 Cisco DNA Center のホームページで、**[Provision] > [Devices] > [Plug and Play]** の順に選択します。

ステップ 2 テーブル内のデバイスを表示します。

[Filter] オプションを使用して、特定のデバイスを検索します。[Refresh] をクリックしてデバイスリストを更新します。

ステップ 3 リセットする 1 個以上のデバイスの横にあるチェック ボックスをオンにします。

ステップ 4 デバイス テーブルの上にあるメニュー バーで、**[Actions (アクション)] > [Reset (リセット)]** をクリックします。

確認のダイアログボックスが表示されます。

ステップ 5 次のいずれかのオプションを選択します。

- **[Reset and keep current claim parameters]** : 現在の請求パラメータが維持され、デバイスは **[Planned]** 状態になります。
- **[Reset and remove all claim parameters]** : 現在の請求パラメータを削除し、デバイスが **[Unclaimed]** 状態になります。


ステップ 6 **[リセット (Reset)]** をクリックします。

インベントリ内のデバイスの管理

ここでは、**[Device Inventory]** ウィンドウを使用して、サイトにデバイスを割り当て、デバイス タグを管理する方法について説明します。

[Device Inventory] ページを使用してデバイスを管理する方法の詳細については、[インベントリの管理 \(43 ページ\)](#) を参照してください。

デバイスをサイトに追加する

- ステップ 1 Cisco DNA Center ホームページで、**[プロビジョニング (Provision)]** をクリックします。
[Inventory] ウィンドウには、ディスカバリプロセス中に収集されたデバイス情報が表示されます。
- ステップ 2 サイトに割り当てるデバイスのチェックボックスをオンにします。
- ステップ 3 [Actions] メニューから、**[Provision] > [Assign Device to Site]** を選択します。
[Assign Device to Site] スライドインペインが表示されます。
- ステップ 4 [Assign Device To Site] スライドインペインで、デバイスの  アイコンの横にあるリンクをクリックします。
[Choose a floor] スライドインペインが表示されます。
- ステップ 5 [Choose a floor] スライドインペインで、デバイスに割り当てるフロアを選択します。
- ステップ 6 **[保存 (Save)]** をクリックします。
- ステップ 7 (任意) 複数のデバイスを選択して同じ場所に追加した場合は、最初のデバイスで **[Apply to All]** チェックボックスをオンにすると、残りのデバイスに同じ場所を割り当てることができます。
- ステップ 8 **[Assign]** をクリックします。

デバイスのタグ付け

デバイスタグは属性またはルールに基づいてデバイスをグループ化することができます。単一のデバイスに複数のタグを設定できます。同様に、複数のデバイスに適用できる単一のタグもあります。

[プロビジョン (Provision)] ウィンドウのデバイスに対してタグを追加したり、削除できます。

- ステップ 1 Cisco DNA Center ホームページで、**[プロビジョニング (Provision)]** をクリックします。デバイスインベントリのページには、ディスカバリ プロセス中に収集されたデバイス情報が表示されます。
- ステップ 2 タグを適用するデバイスの横にあるチェックボックスをオンにして、**[Tag Device]** をクリックします。
- ステップ 3 **[タグ名 (Tag Name)]** フィールドにタグ名を入力します。
 - 新しいタグを作成している場合は、**[新規タグの作成 (Create New Tag)]** をクリックします。ルールを使用して新規タグを作成することもできます。詳細については、「[ルールを使用してデバイスにタグ付けする \(274 ページ\)](#)」を参照してください。
 - 既存のタグを使用している場合は、リストからタグを選択して、**[Apply]** をクリックします。タグを適用するデバイス名の下に、タグアイコンとタグ名が表示されます。
- ステップ 4 デバイスからタグを削除するには、以下のいずれか 1 つを行います。
 - **[Create New Tag]** をクリックしてすべてのタグの選択を解除し、**[Apply]** をクリックします。

- タグアイコンまたはタグ名にカーソルを合わせて、[X]をクリックし、デバイスからタグの関連付けを解除します。

ルールを使用してデバイスにタグ付けする

ルールを定義するタグに基づいてデバイスをグループ化することができます。ルールを定義するとき、Cisco DNA Center は指定したルールと一致するすべてのデバイスにタグを適用します。ルールはデバイス名、デバイスファミリー、デバイスシリーズ、IP アドレス、ロケーション、またはバージョンに基づくことができます。

ステップ 1 Cisco DNA Center ホームページで、[プロビジョニング (Provision)] をクリックします。デバイスインベントリのページには、ディスカバリ プロセス中に収集されたデバイス情報が表示されます。

ステップ 2 タグを適用するデバイスの隣のチェックボックスをオンにして、[**デバイスのタグ付け (Tag Device)**] をクリックします。

ステップ 3 [**タグ名 (Tag Name)**] フィールドにタグ名を入力し、[**ルールによる新規タグの作成 (Create New Tag with Rule)**] をクリックします。

[**新規 VRF の作成 (Create New VRF)**] ウィンドウが表示されます。

[**タグ付きデバイスの合計数 (Total Devices Tagged Count)**] の下の [**手動で追加 (Manually Added)**] フィールドは、ステップ 2 で選択されたデバイスの合計数を示します。

ステップ 4 [**条件の追加 (Add Condition)**] をクリックして、ルールに必要なフィールドに記入します。

[**一致するデバイス (Matching Devices)**] の数は、この条件に一致するデバイスの数に応じて、自動的に変更されます。

追加条件を作成するためには、次の 2 つのオプションがあります。

- **And** 条件— [**条件の追加 (Add Condition)**] リンクをクリックします。 **And** が条件の上に表示されます。
- **Or** 条件—既存の条件の隣の追加アイコン (+) をクリックします。 **Or** は条件の隣に表示されます。

必要に応じていくつでも条件を追加できます。ルールを変更すると、指定したルールに一致するインベントリのデバイス数を反映して一致するデバイス数を変更されます。デバイス数でクリックして、ルールと一致するデバイスを表示できます。

ステップ 5 [**保存 (Save)**] をクリックして、定義されたルールと共にタグを保存します。

タグを適用するデバイス名の下に、タグアイコンとタグ名が表示されます。

デバイスがインベントリに追加されると、定義した rule と一致する場合、タグは自動的にデバイスに適用されます。

デバイスタグの編集

以前に作成したデバイスタグを編集できます。

-
- ステップ 1** Cisco DNA Center ホームページで、[プロビジョニング (Provision)] をクリックします。デバイスインベントリのページには、ディスカバリ プロセス中に収集されたデバイス情報が表示されます。
- [デバイス名 (Device Name)] 列のデバイス名の下に以前に作成したデバイスタグがありある場合はそれがリスト表示されます。
- ステップ 2** デバイスを選択しないで、[デバイスのタグ付け (Tag Device)] をクリックします。
- 以前に作成されたタグがリストされます。
- ステップ 3** 編集するタグをマウスオーバーして、タグ名の隣の鉛筆アイコンをクリックします。
- 代わりに、[デバイスのタグ付け (Tag Device)] > [すべてのタグの表示 (View All Tags)] を選択し、編集するタグの隣の鉛筆アイコンをクリックします。
- ステップ 4** タグを変更し、[保存 (Save)] をクリックして変更を保存します。
-

[タグの削除 (Delete Tags)]

デバイスタグまたはテンプレートタグは、デバイスまたはテンプレートに関連付けられていない場合にのみ削除できます。

始める前に

デバイスに (ルールを使用して) 静的または動的に関連付けられているタグを削除します。

テンプレートに関連付けられているタグを削除します。

-
- ステップ 1** Cisco DNA Center ホームページで、[プロビジョニング (Provision)] をクリックします。
- デバイスインベントリのページには、ディスカバリ プロセス中に収集されたデバイス情報が表示されます。
- ステップ 2** デバイスを選択しないで、[Tag Device] > [Manage Tags] をクリックします。
- ステップ 3** 削除するタグにマウスカーソルを合わせてから、タグ名の横にある削除アイコンをクリックします。
- ステップ 4** タグの削除の警告メッセージで [Yes] をクリックします。
- タグがデバイスまたはテンプレートに関連付けられている場合は、エラーメッセージがスローされます。デバイスまたはテンプレートに関連付けられているタグを除去し、タグを削除します。
-

デバイスのプロビジョニング

次の項では、さまざまなシスコ デバイスをプロビジョニングする方法について説明します。

Cisco Wireless Controller をプロビジョニングする

始める前に

- シスコ ワイヤレス コントローラ をプロビジョニングする前に、次のグローバル ネットワーク設定を定義したことを確認します。
 - AAA、DHCP、および DNS などのネットワーク サーバ。詳細については、[グローバル ネットワーク サーバの設定 \(162 ページ\)](#) を参照してください。
 - CLI、SNMP、HTTP、HTTPS などのデバイス クレデンシアル。詳細については、[グローバル CLI クレデンシアルの設定 \(150 ページ\)](#)、[グローバル SNMPv2c クレデンシアルの設定 \(151 ページ\)](#)、[グローバル SNMPv3 クレデンシアルの設定 \(152 ページ\)](#)、および[グローバル HTTPS クレデンシアルの設定 \(154 ページ\)](#) を参照してください。
 - IP アドレス プール 詳細については、「[IP アドレス プールを設定する \(158 ページ\)](#)」を参照してください。
 - SSID、ワイヤレス インターフェイス、およびワイヤレス無線周波数プロファイルなどのワイヤレス設定です。詳細については、「[グローバル ワイヤレス設定の構成 \(122 ページ\)](#)」を参照してください。
- インベントリにシスコ ワイヤレス コントローラ があることを確認します。ない場合は、[Discovery] 機能を使用して ワイヤレス コントローラ を検出します。
- サイトにシスコ ワイヤレス コントローラ が追加されたことを確認します。詳細については、「[デバイスをサイトに追加する \(273 ページ\)](#)」を参照してください。

Cisco DNA Center によって管理されている ワイヤレス コントローラ の設定に手動で変更を加えることはできません。設定はすべて Cisco DNA Center ユーザインターフェイスから実行する必要があります。

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

[Devices] > [Inventory] ウィンドウが表示され、検出されたすべてのデバイスがこのウィンドウに一覧表示されます。

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

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

- ステップ 3** [Device Type] リストから [WLCs] タブをクリックし、[Reachability] リストから [Reachable] タブをクリックして、検出済みで到達可能なワイヤレス コントローラのリストを取得します。
- ステップ 4** プロビジョニングするコントローラ デバイス名の隣にあるチェック ボックスをオンにします。
- ステップ 5** [Actions] ドロップダウンリストから、[Provision] > [Provision Device] を選択します。
[サイトの割り当て (Assign Site)] ウィンドウが表示されます。
- ステップ 6** [Choose a Site] をクリックしてサイトを割り当てます。
- ステップ 7** [Choose a site] ウィンドウで、サイトを選択して [Save] をクリックします。
- ステップ 8** [Next] をクリックします。
[設定 (Configuration)] ウィンドウが表示されます。
- ステップ 9** ワイヤレス コントローラのロールを選択します ([Active Main WLC] または [Guest Anchor WLC]) 。
- ステップ 10** [Select Primary Managed AP Locations] をクリックして、ワイヤレス コントローラ の管理 AP の場所を選択します。
- ステップ 11** [Managed AP Location] ウィンドウで、サイト名の横にあるチェックボックスをオンにします。親サイトまたは個々のサイトのいずれかを選択できます。親サイトを選択すると、親サイトの下にある子は自動的に選択されます。

(注) 管理 AP の場所を継承することで、サイトをその下のビルディングやフロアとともに自動で選択できます。1 つの ワイヤレス コントローラ で管理できるのは 1 つのサイトのみです。
- ステップ 12** [保存 (Save)] をクリックします。
- ステップ 13** [Interface and VLAN Configuration] で [+ Add] をクリックして、アクティブメイン ワイヤレス コントローラ のインターフェイスと VLAN の詳細を設定します。

インターフェイスおよび VLAN の設定は、非ファブリックの ワイヤレス コントローラ プロビジョニングにのみ適用できます。

[インターフェイスと VLAN の設定 (Configure Interface and VLAN)] ウィンドウが表示されます。
- ステップ 14** [インターフェイス名 (Interface Name)] ドロップダウン リストからインターフェイス名を選択します。
- ステップ 15** [VLAN ID] フィールドに、VLAN の値を入力します。
- ステップ 16** [Interface IP Address] フィールドに、インターフェイス IP アドレスの値を入力します。
- ステップ 17** [Interface Net Mask (in bits)] フィールドに、インターフェイスのサブネットマスクを入力します。
- ステップ 18** [Gateway IP Address] フィールドにゲートウェイ IP アドレスを入力します。
- ステップ 19** [LAG/Port Number] ドロップダウンリストから、リンク集約またはポート番号を選択します。
- ステップ 20** [OK] をクリックします。
- ステップ 21** ゲスト アンカー ワイヤレス コントローラ の場合、[ゲスト SSID を DMZ サイトに割り当てる (Assign Guest SSIDs to DMZ site)] で [VLAN ID] を変更して、VLAN ID 設定を変更できます。
- ステップ 22** [Mobility Group] で [Configure] をクリックして、ワイヤレス コントローラ をモビリティピアとして設定します。

詳細については、「[モビリティ設定の概要 \(306 ページ\)](#)」を参照してください。

[Configure Mobility Group] サイドパネルが表示されます。

ステップ 23 [Mobility Group Name] ドロップダウンリストで、**+** をクリックして新しいモビリティグループを追加するか、既存のモビリティグループの中から選択します。

既存のモビリティピア情報は、Cisco DNA Center で使用可能なインテントからロードされます。

ステップ 24 [RF Group Name] テキストボックスに RF グループの名前を入力します。

ステップ 25 [Mobility Peers] で [Add]**+** をクリックして、ワイヤレスコントローラをモビリティピアとして設定します。

ステップ 26 [Device Name] ドロップダウンリストからコントローラを選択します。

デバイスがプロビジョニングされると、Cisco DNA Center はデバイスにモビリティグループを作成し、RF グループを割り当て、ピアのすべての終端を設定します。モビリティグループの設定は、選択したすべてのピアデバイスに自動的に展開されます。

ステップ 27 [保存 (Save)] をクリックします。

ステップ 28 モビリティグループ名と RF グループ名をリセットするには、次のいずれかを実行します。

- [Configure Mobility Group] サイドパネルで、[Mobility Group Name] ドロップダウンリストから [default] を選択します。
- [Provision] > [Configuration] ページの [Mobility Group] で、[Reset] をクリックします。

これにより、[RF Group Name] が自動的に [default] に設定され、すべてのピアが削除されます。プロビジョニングが完了すると、デバイスのモビリティが設定され、そのデバイスは他のすべてのピアから削除されます。

ステップ 29 [次へ (Next)] をクリックします。

[Advanced Configuration] ウィンドウが表示されます。ここでは、事前定義されたテンプレート変数の値を入力できます。

ステップ 30 [Devices] パネルでデバイスまたはテンプレートを検索できます。

ステップ 31 [wlanid] フィールドに、事前定義されたテンプレート変数の値を入力します。

ステップ 32 [Next] をクリックします。

[Summary (サマリー)] ウィンドウには、次の情報が表示されます。

- デバイスの詳細
- ネットワーク設定
- SSID
- 管理サイト
- インターフェイス
- **Advanced Configuration**

ステップ 33 [展開 (Deploy)] をクリックして、コントローラをプロビジョニングします。

- すぐにデバイスを展開するには、[Now] オプションボタンをクリックし、[Apply] をクリックします。
- 将来の日付と時刻でデバイスの展開をスケジュールするには、[Later] オプションボタンをクリックし、展開する日時を定義します。

ステップ 34 セカンダリコントローラをプロビジョニングします。

詳細については、「[Cisco DNA Center からの N+1 高可用性の設定 \(303 ページ\)](#)」を参照してください。

ステップ 35 展開が正常に完了すると、[デバイスインベントリ (Device Inventory)] ウィンドウの [ステータス (Status)] 列に「成功 (SUCCESS)」と表示されます。

プロビジョニング後に何らかの変更を行う場合は、[Design] をクリックしてサイトのプロファイルを変更し、もう一度ワイヤレスコントローラをプロビジョニングします。

ステップ 36 デバイスが正常に展開されると、[Provision Status] が [Configuring] から [Success] に変わります。

ステップ 37 [Device Inventory] ウィンドウで、[Provision Status] 列の [See Details] をクリックし、ネットワークインテントの詳細情報を取得するか、さらに実行する必要があるアクションのリストを表示します。

ステップ 38 [Device Provisioning] の下の [See Details] をクリックします。

ステップ 39 [Deployment of network intent] の下の [View Details] をクリックし、デバイス名をクリックします。

ステップ 40 [Configuration Summary] エリアを展開して、操作の詳細、機能名、および管理機能を表示します。

また、[Configuration Summary] には、デバイスのプロビジョニング中に発生したエラーも表示されます。

ステップ 41 デバイスに送信される正確な設定の詳細を表示するには、[Provision Summary] エリアを展開します。

Cisco DNA Center からのシスコ WLC 高可用性の設定 Cisco DNA Center

シスコ ワイヤレス コントローラ高可用性 (HA) を Cisco DNA Center から設定できます。現在、ワイヤレスコントローラ HA の形成がサポートされています。HA およびスイッチオーバーオプションの中断はサポートされていません。

ハイ アベイラビリティ用 Cisco ワイヤレス コントローラ設定の前提条件

- ワイヤレスコントローラ 1 とワイヤレスコントローラ 2 の検出機能とインベントリ機能が正常である必要があります。デバイスが [Managed] 状態になっている必要があります。
- ワイヤレスコントローラ 1 とワイヤレスコントローラ 2 のサービスポートと管理ポートが設定されている必要があります。
- ワイヤレスコントローラ 1 とワイヤレスコントローラ 2 の冗長ポートが物理的に接続されている必要があります。
- ワイヤレスコントローラ 1 とワイヤレスコントローラ 2 の管理アドレスが同じサブネット内にある必要があります。ワイヤレスコントローラ 1 とワイヤレスコントローラ 2 の冗長管理アドレスも同じサブネット内にある必要があります。
- ワイヤレスコントローラで次のブート変数を手動で設定します。

```

config t
boot system bootflash:<device_iosxe_image_filename>
config-register 0x2102

show boot. (IOSXE cli)

BOOT variable = bootflash:<device_iosxe_image_filename>,12;
Configuration register is 0x2102

```

シスコワイヤレスコントローラ HA の設定

ステップ 1 Cisco DNA Center のホームページから、[Provision] > [Devices] を選択します。

[Devices] > [Inventory] ページが表示され、検出されたすべてのデバイスがこのページに一覧表示されます。

ステップ 2 プライマリコントローラとして設定するコントローラ名の隣にあるチェックボックスをオンにします。

ステップ 3 [Actions] ドロップダウンリストから、[Provision] > [Configure WLC HA] を選択します。

[High Availability] ページが表示されます。

ステップ 4 [Redundancy Management IP] と [Peer Redundancy Management IP] のアドレスをそれぞれテキストボックスに入力します。

冗長性管理 IP およびピア冗長管理 IP に使用される IP アドレスは、シスコワイヤレスコントローラの管理インターフェイスと同じサブネットに設定する必要があります。これらの IP アドレスがこのサブネット範囲内で未使用の IP アドレスであることを確認します。

ステップ 5 [Select Secondary WLC] ドロップダウンリストから、セカンダリコントローラを選択します。

ステップ 6 [HA の設定 (Configure HA)] をクリックします。

HA 設定は、CLI コマンドを使用してバックグラウンドで開始されます。最初に、プライマリ ワイヤレスコントローラが設定されます。成功したら、セカンダリ ワイヤレスコントローラが設定されます。設定が完了したら、両方のワイヤレスコントローラが再起動します。このプロセスは、完了するまで最大 2.5 分かかります。

ステップ 7 HA 設定を確認するには、[Devices] > [Inventory] ページで、HA デバイスとして設定したデバイスをクリックします。

ステップ 8 [Wireless Info] タブをクリックします。

[Redundancy Summary] には、[Sync Status] が [In Progress] として表示されます。Cisco DNA Center で HA のペアリングが成功したことが検出されると、[Sync Status] が [Complete] に変わります。

これは、インベントリ ポーラーまたは手動による再同期によってトリガーされます。これで、セカンダリ ワイヤレス コントローラ (ワイヤレスコントローラ 2) は、Cisco DNA Center から削除されます。このフローは、ワイヤレスコントローラでの正常な HA 設定を示しています。

高可用性プロセス中および完了後に起こること

1. Cisco WLC-1 および WLC-2 は、冗長管理、冗長ユニット、および SSO とともに設定されます。ワイヤレスコントローラはロールをアクティブまたはスタンバイとしてネゴシエートするために再起動します。設定は、アクティブからスタンバイに同期されます。

2. [冗長性の概要の表示 (Show Redundancy Summary)] ページで、次の設定を確認できます。
 - SSO が有効になっています
 - ワイヤレス コントローラがアクティブ状態になっています
 - ワイヤレス コントローラがホット スタンバイ状態になっています
3. アクティブ ワイヤレス コントローラの管理ポートは、両方のコントローラによって共有され、アクティブ コントローラを指します。スタンバイ ワイヤレス コントローラのユーザーインターフェイス、Telnet、および SSH は機能しません。コンソールとサービスポート インターフェイスを使用して、スタンバイ ワイヤレス コントローラを制御できます。

高可用性を設定および確認するためのコマンド

シスコ ワイヤレス コントローラ HA を設定するには、Cisco DNA Center で次のコマンドを送信します。

Cisco DNA Center で次のコマンドを ワイヤレス コントローラ 1 に送信します。

- **config interface address redundancy-management 198.51.100.xx peer-redundancy-management 198.51.100.yy**
- **config redundancy unit primary**
- **config redundancy mode sso**

Cisco DNA Center で次のコマンドを ワイヤレス コントローラ 2 に送信します。

- **config interface address redundancy-management 198.51.100.yy peer-redundancy-management 198.51.100.xx**
- **config redundancy unit secondary**
- **config port adminmode all enable**
- **config redundancy mode sso**

ワイヤレス コントローラ から HA 設定を検証するには、次のコマンドを入力します。

- HA 関連の詳細情報を確認する場合：**config redundancy mode sso**
- 設定済みのインターフェイスを確認する場合：**show redundancy summary**

ルーティングおよび NFV プロファイルのプロビジョニング

始める前に

ルーティングと NFV プロファイルをプロビジョニングする前に、次のグローバルネットワーク設定を定義したことを確認します。

- AAA、DHCP、および DNS などのネットワーク サーバ。詳細については、[グローバル ネットワーク サーバの設定 \(162 ページ\)](#) を参照してください。

- CLI、SNMP、HTTP、HTTPS などのデバイス クレデンシャル。詳細については、[グローバル CLI クレデンシャルの設定 \(150 ページ\)](#)、[グローバル SNMPv2c クレデンシャルの設定 \(151 ページ\)](#)、[グローバル SNMPv3 クレデンシャルの設定 \(152 ページ\)](#)、および [グローバル HTTPS クレデンシャルの設定 \(154 ページ\)](#) を参照してください。
- IP アドレス プール詳細については、「[IP アドレス プールを設定する \(158 ページ\)](#)」を参照してください。
- SP プロファイル。詳細については、「[サービス プロバイダー プロファイルの設定 \(161 ページ\)](#)」を参照してください。



(注) Cisco Firepower Threat Defense Virtual を NFV プロビジョニング フローを通じてプロビジョニングする場合、デフォルトのクレデンシャルユーザ名が保持され、パスワードはネットワーク設定でサイトに割り当てられたクレデンシャル プロファイルの設定に基づいて更新されます。

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

[Devices] > [Inventory] ウィンドウが表示され、検出されたすべてのデバイスがこのウィンドウに一覧表示されます。

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

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

ステップ 3 [Device Type] リストから [Routers] タブをクリックし、[Reachability] リストから [Reachable] タブをクリックして、検出され到達可能なデバイスのリストを取得します。

ステップ 4 プロビジョニングするデバイス名の横にあるチェックボックスをオンにします。

ステップ 5 サイトで [Assign] をクリックすると、[Assign Device to Site] ウィンドウが表示されます。[Choose a Site] をクリックしてサイトを割り当てます。

ステップ 6 [Actions] ドロップダウンリストから、[Provision] > [Provision] を選択します。

NFVIS デバイスをプロビジョニングするには、次の手順を実行します。

- [Confirm Profile] ウィンドウで詳細を確認し、[Next] をクリックします。
- [Router WAN Configuration] ウィンドウで詳細を確認します。[O] をクリックして WAN の IP アドレスを入力します。[+Edit Services] ウィンドウで詳細を確認します。**[次へ (Next)]** をクリックします。

(注) vEDGE 関連サービスをプロビジョニングする前に、[system setting] ページで vManage 設定を構成する必要があります。詳細については、[Cisco Digital Network Architecture Center 管理者ガイド \[英語\]](#) の「Configure vManage Properties」セクションを参照してください。
- [ENCS Integrated Switch Configuration] ウィンドウで詳細を確認し、[Next] をクリックします。
- [Custom Configuration] ウィンドウで詳細を確認し、[Next] をクリックします。

- [Summary] ページで詳細を確認します。

ルータをプロビジョニングするには、次の手順を実行します。

- [Confirm Profile] ウィンドウで詳細を確認し、[Next] をクリックします。
- [Router WAN Configuration] ウィンドウで詳細を確認します。
 - 回線インターフェイスとしてギガビットイーサネットを選択した場合は、[O] をクリックし、静的 IP アドレスを選択した場合は WAN IP アドレスを入力します。[DHCP] を選択した場合は、DHCP サーバの IP アドレスを入力します。プライマリ WAN がすでに PnP を使用して設定されている場合は、[Do Not Change] を選択して、ドロップダウンリストからプライマリ WAN として設定されているインターフェイスを選択します。
 - 回線インターフェイスとしてセルラーを選択した場合は、[O] をクリックして、[IP Negotiated] を選択し、ドロップダウンリストから [Interface Name] を選択して [Access Point Name (APN)] を入力します。サービスプロバイダーに応じて、[PAP] または [CHAP] の横にあるチェックボックスをオンにします。
 - 複数のサービスプロバイダーを利用している場合は、バックアップ WAN インターフェイスの [IP SLA Address] を入力します。

仮想ルータをプロビジョニングしている場合、このウィンドウは表示されません。

- [Router LAN Configuration] ウィンドウで詳細を確認し、[Next] をクリックします。

[Interface(s)] ドロップダウンリストから、1つの L3 インターフェイスまたは1つまたは複数の L2 インターフェイスを選択できるようになりました。

(注) switchport インターフェイスでは、Cisco 1100 シリーズ サービス統合型ルータのみがサポートされています。
- [Custom Configuration] ウィンドウで詳細を確認し、[Next] をクリックします。このウィンドウは、ルーティングプロファイルに Day-0 および Day-N テンプレートが設定されている場合にのみ表示されます。
- [Summary] ページで詳細を確認します。

ステップ7 [展開 (Deploy)] をクリックして、デバイスをプロビジョニングします。

展開が正常に完了すると、[デバイス インベントリ (Device Inventory)] ウィンドウの [プロビジョニング ステータス (Provision Status)] 列に「成功 (SUCCESS)」と表示されます。[SUCCESS] をクリックして詳細なプロビジョニング ログ ステータスを確認します。

VPC インベントリ収集

クラウドインベントリ収集が正常に完了すると、[Provision] セクションの [Cloud] タブに、収集した AWS VPC インベントリのビューが表示されます。左側のナビゲーションを展開して、クラウドプロファイルまたはアクセスキーのクラウド領域を表示できます。左側のナビゲーター

ション項目をキーワードでフィルタ処理してクリックすると、選択した領域またはアクセスキーに対してのみ VPC が表示されます。

[VPC Inventory] ビューでは、VPC をクリックして、その VPC のサブネットや仮想インスタンスなどの詳細を確認することもできます。AWS VPC インベントリ収集は、すべてのインベントリ収集のデフォルト間隔で行われるようにスケジュールされており、クラウドアクセスキーの歯車メニューの [Sync] アクションを使用して、オンデマンドでトリガーすることもできます。インベントリ収集のステータスを表示するには、[VPC Inventory] ビューで [Show Sync Status] をクリックします。

シスコ製 AP のプロビジョニング : Day 1 AP プロビジョニング

始める前に

インベントリにシスコの AP があることを確認してください。ない場合は、ディスカバリ機能を使用して AP を検出します。詳細については、「[ネットワークの検出 \(13 ページ\)](#)」を参照してください。

-
- ステップ 1** Cisco DNA Center のホームページで、[Provision] を選択します。
- [Devices] > [Inventory] ウィンドウが表示され、検出されたすべてのデバイスがこのウィンドウに一覧表示されます。
- ステップ 2** 特定のサイトで使用可能なデバイスを表示するには、左側のペインで [Global] サイトを展開し、関心のあるサイト、ビルディング、またはフロアを選択します。
- 選択したサイトで使用可能なすべてのデバイスが [Inventory] ウィンドウに表示されます。
- ステップ 3** [Device Type] リストから [AP] タブをクリックし、[Reachability] リストから [Reachable] タブをクリックして、検出され到達可能な AP のリストを取得します。
- ステップ 4** プロビジョニングする AP デバイス名の横にあるチェックボックスをオンにします。
- ステップ 5** [Actions] ドロップダウンリストから、[Provision] > [Provision] を選択します。
- [サイトの割り当て (Assign Site)] ウィンドウが表示されます。
- ステップ 6** [Choose a floor] をクリックし、サイトに AP を割り当てます。
- ステップ 7** [Choose a floor] ウィンドウで AP を関連付けるフロアを選択し、[Save] をクリックします。
- ステップ 8** [Next] をクリックします。
- [設定 (Configuration)] ウィンドウが表示されます。
- ステップ 9** デフォルトでは、[Network Settings] > [Wireless] > [Wireless Radio Frequency Profile] でデフォルトとマークしたカスタム RF プロファイルが、[RF Profile] ドロップダウンリストで選択されています。
- [RF プロファイル (RF Profile)] ドロップダウンリストから値を選択して、AP のデフォルト RF プロファイル値を変更できます。オプションは、[High]、[Typical]、[Low] です。
- 選択した RF プロファイルに基づいて AP グループが作成されます。

ステップ 10 [次へ (Next)] をクリックします。

ステップ 11 [Summary] ウィンドウでデバイスの詳細を確認し、[Deploy] をクリックして AP をプロビジョニングします。

- すぐに AP を展開するには、[Now] オプションボタンをクリックし、[Apply] をクリックします。
- 将来の日付と時刻で AP の展開をスケジュールするには、[Later] オプションボタンをクリックし、展開する日時を定義します。

ステップ 12 AP グループの作成または変更が進行中であることを示すメッセージが表示されます。

「プロビジョニング後に AP が再起動します。続行しますか? (After provisioning AP(s) will reboot. Do you want to continue?) 」というメッセージが表示されます。

ステップ 13 [OK] をクリックします。

展開が正常に完了した場合、[Device Inventory] ウィンドウの [Last Sync Status] 列に、「SUCCESS」と表示されます。

ブラウフィールド デバイスのプロビジョニング

始める前に



(注) ブラウフィールドのサポートは、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ デバイスではなく Cisco AireOS ワイヤレス コントローラ デバイスに対応しています。

Cisco DNA Center を使用すると、シスコ ワイヤレス コントローラ などのブラウフィールド デバイスをネットワークに追加してプロビジョニングできます。ブラウフィールドは、既存サイトの以前から存在しているインフラストラクチャに属しているデバイスを指します。

- 初めに、デバイスについてディスカバリを実行します。すべてのデバイスが [インベントリ (Inventory)] ウィンドウに表示されます。詳細については、[ネットワークの検出 \(13 ページ\)](#) および [インベントリについて \(43 ページ\)](#) を参照してください。
- ワイヤレス コントローラ は到達可能で、[インベントリ (Inventory)] ウィンドウで管理状態でなければなりません。詳細については、[インベントリについて \(43 ページ\)](#) を参照してください。

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

[Device] > [Inventory] ウィンドウが表示されます。このウィンドウには、ネットワークで使用可能な検出済みのデバイスが一覧表示されます。

- ステップ 2** [フィルタ (Filter)] をクリックして、選択したフィルタ フィールドに適切な値を入力します。たとえば、[デバイス名 (Device Name)] フィルタの場合、デバイスの名前を入力します。
[デバイス (Devices)] テーブルに表示されるデータは、選択したフィルタに従って自動で更新されます。
- ステップ 3** プロビジョニングする ワイヤレス コントローラ デバイス名の横にあるチェックボックスをオンにします。
- ステップ 4** [Actions] ドロップダウンリストから、[Provision] > [Learn Device Config] を選択します。 >
[サイトの割り当て (Assign Site)] ウィンドウが表示されます。
- ステップ 5** [Choose a site] をクリックして、コントローラにサイトを割り当てます。
- ステップ 6** [Choose a site] ウィンドウで、ワイヤレス コントローラ を関連付けるサイトを選択し、[Save] をクリックします。
- ステップ 7** [次へ (Next)] をクリックします。
- ステップ 8** [Resolve Conflict] ウィンドウに、解決する必要がある Cisco DNA Center の競合する設定が表示されます。
- ステップ 9** [次へ (Next)] をクリックします。
[Design Object] ウィンドウに、学習したすべての設定が一覧表示されます。
- ステップ 10** 左ペインで [ネットワーク (Network)] をクリックします。
右側のペインに、デバイス設定学習の一部として学習されたネットワーク設定と、次の情報が表示されます。
- [AAA サーバ (AAA Server)] の詳細。
 - システム設定。AAA サーバの IP アドレスとプロトコルについての詳細情報を含みます。
 - [DHCP Server] の詳細。
- ステップ 11** AAA サーバの共有秘密を入力します。
- ステップ 12** 左ペインで [ワイヤレス (Wireless)] をクリックします。
右側のペインには、企業 SSID、ゲスト SSID、およびワイヤレスインターフェイスの詳細が一覧表示されます。
- ステップ 13** 事前共有キー (PSK) を使用する SSID の場合、事前共有キーを入力します。
- ステップ 14** 左ペインで [破棄された設定 (Discarded Config)] をクリックします。
右ペインに、Cisco DNA Center 上で競合する設定、または既に存在する設定が一覧表示されます。破棄された設定エントリは、次のように分類されます。
- 設計エンティティの重複
 - 無線ポリシーの不明なデバイス設定
- ステップ 15** [次へ (Next)] をクリックします。
[ネットワーク プロファイル (Network Profile)] ウィンドウに、AP と WLAN の組み合わせに基づいて作成されたネットワーク プロファイルまたはサイト プロファイルが一覧表示されます。

- ステップ 16** [保存 (Save)] をクリックします。
- 「ブラウフィールド設定に成功しました (Brownfield Configuration is Successful)」というメッセージが表示されます。
- ステップ 17** [設計 (Design)] > [ネットワーク プロファイル (Network Profile)] を選択して、サイトをネットワーク プロファイルに割り当てます。
- ステップ 18** [ネットワーク プロファイル (Network Profile)] ページで [サイトの割り当て (Assign Site)] をクリックして、選択したプロファイルにサイトを追加します。
- ステップ 19** [サイトをプロファイルに追加 (Add Sites to Profile)] ウィンドウでドロップダウンリストからサイトを選択して、[保存 (Save)] をクリックします。
- ステップ 20** [プロビジョニング (Provision)] タブをクリックします。
- ステップ 21** [フィルタ (Filter)] をクリックして、選択したフィルタ フィールドに適切な値を入力します。
- [デバイス (Devices)] テーブルに表示されるデータは、選択したフィルタに従って自動で更新されます。
- ステップ 22** プロビジョニングするコントローラ デバイス名の横にあるチェック ボックスをオンにします。
- ステップ 23** [アクション (Actions)] ドロップダウン リストから、[プロビジョニング (Provision)] を選択します。
- ステップ 24** [サイトの割り当て (Assign Site)] ウィンドウで詳細を確認して、[次へ (Next)] をクリックします。
- [設定 (Configurations)] ウィンドウが表示されます。
- ステップ 25** [インターフェイスと VLAN の設定 (Interface and VLAN Configuration)] で、[+ 追加 (+ Add)] をクリックしてインターフェイスと VLAN の詳細を設定します。
- ステップ 26** [インターフェイスと VLAN の設定 (Configure Interface and VLAN)] ウィンドウで必要なフィールドを設定して、[OK] をクリックします。
- ステップ 27** [Next] をクリックします。
- ステップ 28** [Summary (サマリ)] ウィンドウには、次の情報が表示されます。
- デバイスの詳細
 - ネットワーク設定
 - SSID
 - 管理サイト
 - インターフェイス
- ステップ 29** [展開 (Deploy)] をクリックして、デバイスをプロビジョニングします。
- 展開が正常に完了すると、[デバイスインベントリ (Device Inventory)] ウィンドウの [プロビジョニング ステータス (Provision Status)] 列に「成功 (SUCCESS)」と表示されます。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの設定とプロビジョニング

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの概要

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラは、インテントベース ネットワーク用に構築された次世代のワイヤレスコントローラです。Cisco Catalyst 9800 シリーズ ワイヤレス コントローラは Cisco IOS XE ベースであり、Aironet の優れた RF 性能と Cisco IOS XE のインテントベース ネットワーク機能を統合して、組織にクラス最高水準のワイヤレスエクスペリエンスを提供します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラはモジュール型オペレーティングシステムに基づいて構築され、オープンでプログラマブルな API 機能が搭載されていて、0 日目から N 日目のネットワーク運用を自動化できます。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラは、次のような複数のフォームファクタで使用できます。

- Catalyst 9800-40 ワイヤレス コントローラ
- Catalyst 9800-80 ワイヤレス コントローラ
- Catalyst 9800-CL Cloud ワイヤレスコントローラ：プライベートクラウド（ESXi、KVM、Cisco ENCS）に展開可能、Cisco DNA Center で管理可能 Cisco DNA Center
- Catalyst 9300 シリーズ スイッチ、Catalyst 9400 シリーズ スイッチ、および Catalyst 9500H シリーズ スイッチ用 Catalyst 9800 組み込みワイヤレスコントローラ
- Cisco Catalyst 9800-L ワイヤレスコントローラ：中小企業向けにシームレスなソフトウェアアップデートを提供します。Cisco Catalyst 9800-L ワイヤレスコントローラは 2 つのバリエーションで使用できます。銅線と光ファイバアップリンクのいずれかを選択でき、ネットワークの柔軟性が向上します。

次の表に、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラでサポートされている仮想プラットフォームおよびハードウェア プラットフォームを示します。

プラットフォーム	説明
Cisco Catalyst 9800-80 ワイヤレス コントローラ	<p>最大 6000 アクセスポイントと 64,000 クライアントをサポートします。</p> <p>最大 80 Gbps のスループットをサポートし、2 ラックユニットスペースを使用します。</p> <p>最大 100-GE のアップリンクおよびシームレスなソフトウェア アップデートを搭載したモジュール型ワイヤレス コントローラ。</p>

プラットフォーム	説明
Cisco Catalyst 9800-40 ワイヤレス コントローラ	<p>シームレスなソフトウェアアップデートを備えた、中小企業やキャンパスでの導入向けの固定ワイヤレスコントローラ。</p> <p>最大2000アクセスポイントと32,000クライアントをサポートします。</p> <p>最大40 Gbpsのスループットをサポートし、1ラックユニットスペースを使用します。</p> <p>4つの1-GEまたは10-GEアップリンクポートを提供します。</p>
Cisco Catalyst 9800-CL Cloud ワイヤレスコントローラ：プライベートクラウド用 Cisco Catalyst 9800-CL をサポート	<p>Cisco Catalyst 9800-CL Cloud ワイヤレスコントローラは、高可用性とセキュリティを実現するために構築された次世代のエンタープライズクラスの仮想ワイヤレスコントローラです。</p> <p>Cisco Catalyst 9800-CL Cloud ワイヤレスコントローラの仮想フォームファクタは、プライベートクラウド（ESXi、KVM、およびCisco ENCSをサポート）に展開できます。</p>
Catalyst 9k シリーズ スイッチ用 Cisco Catalyst 9800 組み込みワイヤレスコントローラ	<p>Catalyst 9k シリーズ スイッチ用 Cisco Catalyst 9800 組み込みワイヤレスコントローラは、有線およびワイヤレス インフラストラクチャを一貫性のあるポリシーと管理とともに提供します。</p> <p>この導入モデルは、小規模キャンパスや分散型ブランチ向けの安全性に優れたソリューションである Cisco SD-Access でのみサポートされます。組み込みコントローラは、ファブリックモードでのみアクセスポイント（AP）をサポートします。</p>

プラットフォーム	説明
Cisco Catalyst 9800-L ワイヤレス コントローラ	<p>Cisco Catalyst 9800-L ワイヤレスコントローラは、中小企業向けにシームレスなソフトウェアアップデートを提供します。Cisco Catalyst 9800-L ワイヤレスコントローラは2つのバリエーションで使用できます。銅線と光ファイバアップリンクのいずれかを選択でき、ネットワークの柔軟性が向上します。</p> <ul style="list-style-type: none"> • Cisco Catalyst 9800-L Copper シリーズ ワイヤレス コントローラ (9800-L-C RJ45) • Cisco Catalyst 9800-L ファイバシリーズ ワイヤレス コントローラ (9800-L-F SFP)

次の表に、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラでサポートされているホスト環境を示します。

ホスト環境	ソフトウェアバージョン
VMware ESXi	<ul style="list-style-type: none"> • VMware ESXi vSphere 6.0 • VMware ESXi vSphere 6.5⁵ • VMware ESXi vCenter 6.0 • VMware ESXi VCenter 6.5
KVM	<ul style="list-style-type: none"> • Red Hat Enterprise Linux 7.1 および 7.2 をベースとした Linux KVM • Ubuntu 14.04.5 LTS、Ubuntu 16.04.5 LTS
NFVIS	Cisco ENCS 3.8.1 および 3.9.1

⁵ ESXi vSphere を使用した C9800-CL の .ova ファイルのインストールは機能しません。これは C9800 ova に限定されませんが、他の製品に影響します。シスコと VMware は、問題解決に向けて積極的に取り組んでいます。問題が修正されたかどうかを確認するには、シスコのアカウント担当者にお問い合わせください。VMware 6.5 および C9800-CL OVA ファイルの展開に固有の問題があります。「必要なディスクイメージがありません。(A required disk image was missing)」という警告が表示され、「VMの展開に失敗しました：postNFCData に失敗しました：ディスク以外のファイルに POST できません。(Failed to deploy VM: postNFCData failed: Cannot POST to non-disk files.)」というエラーで展開が失敗します。VMware ESXi 6.5 に C9800-CL をインストールするには、次のいずれかを実行します。1) ESXi 組み込み GUI を使用して C9800-CL の .iso ファイルをインストールする (ESXi 6.5 クライアントバージョン 1.29.0 はテスト済みで必須)。2) OVF ツールを使用して C9800-CL の .ova ファイルをインストールする。

次の表に、Cisco DNA Centerでサポートされている Cisco Enterprise Network Function Virtualization Infrastructure Software (NFVIS) のバージョンを示します。



-
- (注) Cisco Enterprise NFVIS デバイスは、N-1 から N へのアップグレードパスのみをサポートします。たとえば、Cisco Enterprise NFVIS Release 3.8.x から Cisco Enterprise NFVIS 3.9.x へのアップグレードのみがサポートされています。Cisco Enterprise NFVIS リリース 3.8.x から Cisco Enterprise NFVIS リリース 3.10.x へのアップグレードはサポートされていません。
-

Cisco Enterprise NFVIS バージョン	エンタープライズ ネットワーク コンピューティング システム (ENCS) デバイス プラットフォーム	注
<ul style="list-style-type: none"> • 3.8.1 • 3.9.1 • 3.9.2 • 3.10.1 • 3.10.2 • 3.10.3 • 3.11.1 • 3.11.2 • 3.12.2 	<ul style="list-style-type: none"> • ENCS 5400 • UCS-E • UCS-C 	<p>Cisco Enterprise NFVIS リリース 3.12.1 は、Cisco DNA Center のいずれのバージョンでもサポートされていません。</p> <ul style="list-style-type: none"> • Cisco Enterprise NFVIS リリース 3.12.1 は、Cisco DNA Center のいずれのバージョンでもサポートされていません。これは、Cisco Enterprise NFVIS リリース 3.12.1 では、警告 CSCvq66963 の修正を利用できないためです。 • Cisco DNA Center リリース 1.3.1 を使用した Cisco Enterprise NFVIS リリース 3.11.x から Cisco Enterprise NFVIS リリース 3.12.1 へのアップグレードはサポートされていません。 • Cisco DNA Center リリース 1.3.1 を使用した Cisco Enterprise NFVIS リリース 3.12.1 から Cisco Enterprise NFVIS リリース 3.12.2 へのアップグレードはサポートされていません。 <p>Cisco Enterprise NFVIS リリース 3.12.2 は、Cisco DNA Center リリース 1.3.1 でサポートされています。</p> <ul style="list-style-type: none"> • Cisco DNA Center リリース 1.3.1 を使用した Cisco Enterprise NFVIS リリース 3.11.2 からリリース 3.12.2 へのアップグレードはサポートされています。 • Cisco Enterprise NFVIS リリース 3.12.2 は、Cisco DNA Center リリース 1.3.1 でサポートされています。

Cisco Enterprise NFVIS バージョン	エンタープライズ ネットワークコンピューティングシステム (ENCS) デバイスプラットフォーム	注
<ul style="list-style-type: none"> • 3.8.1 • 3.9.1 • 3.9.2 	ENCS 5100	Cisco 5100 エンタープライズ ネットワーク コンピューティング システム (ENCS) は、Cisco Enterprise NFVIS 3.10.x をサポートしていません。

Cisco DNA Center で Cisco Catalyst 9800 ワイヤレスコントローラを設定するためのワークフロー

1. Cisco DNA Center をインストールします。
詳細については、[Cisco Digital Network Architecture Center 設置ガイド \[英語\]](#) を参照してください。
2. ソフトウェアイメージのアップグレードに関する詳細については、[Cisco Catalyst 9800 シリーズワイヤレスコントローラでのソフトウェアイメージのアップグレードのサポート \(297 ページ\)](#) を参照してください。
3. Cisco DNA Center GUI にログインし、必要なアプリケーションが [Running] 状態であることを確認します。
確認するには、Cisco DNA Center のホームページで、歯車アイコン  をクリックし、**[System Settings] > [Software Updates] > [Installed Apps]** を選択します。
4. Cisco Identity Services Engine と Cisco DNA Center を連動させます。統合後、関連する設定やデータとともに Cisco DNA Center が検出されたデバイスは、Cisco ISEにプッシュされます。
5. Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ を検出します。
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラを検出するには、NETCONF を有効にしてポートを 830 に設定する必要があります。NETCONF は、ネットワークデバイスの設定をインストール、操作、削除するメカニズムです。
詳細については、[CDPを使用したネットワークの検出 \(19 ページ\)](#) または[Discover Your Network Using an IP Address Range \(25 ページ\)](#) を参照してください。
ワイヤレス管理 IP アドレスを手動で追加する必要があります。
[Discovery] ウィンドウで Cisco Discovery Protocol (CDP) または IP アドレス範囲を使用して検出を実行する場合は、[Preferred Management IP] ドロップダウンリストから [Use Loopback] を選択してデバイスのループバック インターフェイス IP アドレスを指定します。
6. 検出されたデバイスが [Device Inventory] ページに [Managed] 状態で表示されていることを確認します。

詳細については、[インベントリについて \(43 ページ\)](#) および [インベントリに関する情報の表示 \(45 ページ\)](#) を参照してください。

デバイスが [Managed] 状態になるまで待機する必要があります。

7. Cisco Catalyst 9800 シリーズ ワイヤレス コントローラでアシュアランス接続を確認するには、次のコマンドを使用します。

- **#show crypto pki trustpoints | sec DNAC-CA**

```
Trustpoint DNAC-CA
  Subject Name:
    cn=kube-ca
    Serial Number (hex): 00E*****
  Certificate configured.
```

- **#show crypto pki trustpoints | sec sdn-network**

```
Trustpoint sdn-network-infra-iwan:
  Subject Name:
    cn=sdn-network-infra-ca
    Serial Number (hex): 378*****
  Certificate configured.
```

- **#show telemetry ietf subscription all**

```
Telemetry subscription brief

  ID           Type           State           Filter type
  -----
  1011          Configured     Valid           tdl-uri
  1012          Configured     Valid           tdl-uri
  1013          Configured     Valid           tdl-uri
```

- **#show telemetry internal connection**

```
Telemetry connection

Address Port Transport State Profile
-----
IP address 25103 tls-native Active sdn-network-infra-iwan
```

- **#show network-assurance summary**

```
Network-Assurance           : True
Server Url                   : https://10.***.***.***
ICap Server Port Number     : 3***
Sensor Backhaul SSID        :
Authentication                : Unknown
```

8. 認証サーバとポリシーサーバの設定時に TACACS サーバを設定します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラでユーザ名をローカルに設定している場合、TACACS の設定は必須ではありません。

9. サイト、ビルディング、フロアを追加してネットワーク階層を設計すると、後で設計の設定や構成を適用する場所を簡単に特定できるようになります。

新しいネットワーク階層を作成します。または Cisco Prime Infrastructure に既存のネットワーク階層がある場合は、それを Cisco DNA Center にインポートできます。

既存のネットワーク階層をインポートしてアップロードするには、[既存のサイト階層をアップロード \(97 ページ\)](#) を参照してください。

新しいネットワーク階層を作成するには、[ネットワーク階層のサイトの作成 \(95 ページ\)](#)、[ビルディングの追加 \(99 ページ\)](#)、および[ビルディングへのフロアの追加 \(101 ページ\)](#) を参照してください。

10. AP の位置情報を追加し、フロアマップに配置して、ヒートマップカバレッジを可視化します。

詳細については、「[AP の追加、配置、および削除 \(104 ページ\)](#)」を参照してください。

11. AAA (Cisco ISE がネットワークおよびクライアントエンドポイント用に設定されている)、NetFlow コレクタ、NTP、DHCP、DNS、syslog、および SNMP トラップなどのネットワーク設定を定義します。これらのネットワークサーバが、ネットワーク全体のデフォルトになります。AAA サーバを追加するときに、TACACS サーバを追加できます。

詳細については、[グローバル ネットワーク設定について \(146 ページ\)](#)、[グローバル ネットワーク サーバの設定 \(162 ページ\)](#)、および「[Cisco ISE またはその他の AAA サーバの追加](#)」を参照してください。

12. カスタムとして、親プロファイルでワイヤレス無線周波数プロファイルを作成します。

詳細については、「[ワイヤレス無線周波数プロファイルの作成 \(133 ページ\)](#)」を参照してください。

13. IP アドレスプールをグローバルレベルで作成します。

Cisco DNA Center Cisco DNA Center は、IP アドレスプールを使用して、SD-Access ネットワークの設定と展開を自動化します。

IP アドレスプールを作成するには、[IP アドレスプールを設定する \(158 ページ\)](#) を参照してください。

プロビジョニングするビルディング用に IP アドレスプールを予約する必要があります。詳細については、「[LAN アンダーレイのプロビジョニング](#)」を参照してください。

14. エンタープライズおよびゲストワイヤレスネットワークを作成します。グローバルワイヤレス設定を 1 回定義します。次に、Cisco DNA Center は地理的な場所全体でさまざまなデバイスに設定をプッシュします。

ワイヤレスネットワークの設計は、2 段階のプロセスです。まず SSID を作成し、次に作成した SSID をワイヤレス ネットワーク プロファイルに関連付ける必要があります。このプロファイルは、サイトにデバイスを展開するために使用されるトポロジを構築するのに役に立ちます。

詳細については、[エンタープライズワイヤレス ネットワーク用 SSID の作成 \(122 ページ\)](#) および[ゲストワイヤレス ネットワークの SSID の作成 \(127 ページ\)](#) を参照してください。

15. バックホールの設定を行います。詳細については、「[バックホール設定の管理 \(136 ページ\)](#)」を参照してください。
16. Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの [Policy] ウィンドウで、次のように設定します。
 - 仮想ネットワークを作成します。仮想ネットワークを使用して、物理ネットワークを複数の論理ネットワークにセグメント化できます。詳細については、[仮想ネットワーク \(245 ページ\)](#) および [仮想ネットワークの作成 \(246 ページ\)](#) を参照してください。
 - グループベースのアクセスコントロールポリシーを作成し、契約を追加する。詳細については、「[グループベースのアクセスコントロールポリシーの作成 \(199 ページ\)](#)」を参照してください。
17. 高可用性を設定します。

詳細については、「[Cisco Catalyst 9800 シリーズ ワイヤレス コントローラで高可用性を設定する \(298 ページ\)](#)」を参照してください。
18. 設計フェーズ中に追加された設定を使用して、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラをプロビジョニングします。

詳細については、「[Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのプロビジョニング \(311 ページ\)](#)」を参照してください。
19. Cisco Catalyst 9800 シリーズ ワイヤレス コントローラでアプリケーションポリシーを設定および展開します。

詳細については、[アプリケーションポリシーを作成します。 \(225 ページ\)](#)、[アプリケーションポリシーの展開 \(232 ページ\)](#)、および [アプリケーションポリシーの編集 \(230 ページ\)](#) を参照してください。



(注) アプリケーションポリシーを展開する前に、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラデバイスをプロビジョニングする必要があります。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ デバイスの場合、2 つの異なる SSID で異なるビジネスとの関連性を持つ 2 つの異なるポリシーは機能しません。関連性を設定するときは、最後に展開したポリシーが常に優先されます。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ デバイスの場合、アプリケーションのデフォルトのビジネスとの関連性を変更しても、FlexConnect モードでは機能しません。

非ファブリック SSID にのみアプリケーションポリシーを適用できます。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラでのソフトウェアイメージのアップグレードのサポート

始める前に

- Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ を検出します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ を検出するには、NETCONF を有効にしてポートを 830 に設定します。NETCONF は、ネットワークデバイスの設定をインストール、操作、削除するためのメカニズムです。これにより、コントローラでワイヤレスサービスが有効になります。

詳細については、[CDP を使用したネットワークの検出 \(19 ページ\)](#) または [Discover Your Network Using an IP Address Range \(25 ページ\)](#) を参照してください。

- デバイスが [Device Inventory] に [Managed] 状態で表示されていることを確認します。

詳細については、[インベントリについて \(43 ページ\)](#) および [インベントリに関する情報の表示 \(45 ページ\)](#) を参照してください。

ステップ 1 Cisco DNA Center のホームページで、**[Design] > [Image Repository]** を選択するか、Cisco DNA Center のホームページで **[Image Repository]** をクリックします。

ステップ 2 ローカルコンピュータまたは URL から、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ ソフトウェアイメージをインポートします。

詳細については、「[ソフトウェア イメージのインポート \(77 ページ\)](#)」を参照してください。

ステップ 3 ソフトウェアイメージをデバイスファミリに割り当てます。

詳細については、「[デバイスファミリへのソフトウェアイメージの割り当て \(78 ページ\)](#)」を参照してください。

ステップ 4 デバイスファミリまたは特定のデバイスロールの星印をクリックして、ソフトウェアイメージをゴールデンとしてマークできます。

詳細については、「[ゴールデン ソフトウェア イメージの指定 \(80 ページ\)](#)」を参照してください。

ステップ 5 ソフトウェアイメージをプロビジョニングするには、Cisco DNA Center のホームページで **[Provision]** をクリックします。

[Devices] > [Inventory] ウィンドウが表示されます。

ステップ 6 **[Inventory]** ウィンドウで、アップグレードするイメージ Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の横にあるチェックボックスをオンにします。

ステップ 7 **[Actions]** ドロップダウンから、**[Software Image] > [Update Image]** を選択します。

詳細については、[ソフトウェア イメージのプロビジョニング \(81 ページ\)](#) を参照してください。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラで高可用性を設定する

始める前に

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラで高可用性 (HA) を設定するための前提条件となるタスクを次に示します。

- 両方の Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ デバイスが同じソフトウェアバージョンを実行していて、プライマリ Catalyst 9800 シリーズ ワイヤレス コントローラ上にアクティブなソフトウェアイメージがあります。
- Catalyst 9800 シリーズ ワイヤレス コントローラ 1 と Catalyst 9800 シリーズ ワイヤレス コントローラ 2 のサービスポートおよび管理ポートが設定されています。
- Catalyst 9800 シリーズ ワイヤレス コントローラ 1 および Catalyst 9800 シリーズ ワイヤレス コントローラ 2 の冗長ポートが物理的に接続されています。
- インターフェイス設定、ルート追加、SSH回線設定、NETCONF-YANG設定などの事前設定は、Catalyst 9800 シリーズ ワイヤレス コントローラアプライアンスで完了します。
- Catalyst 9800 シリーズ ワイヤレス コントローラ 1 と Catalyst 9800 シリーズ ワイヤレス コントローラ 2 の管理インターフェイスは同じサブネット内にあります。
- Catalyst 9800 シリーズ ワイヤレス コントローラ 1 デバイスおよび Catalyst 9800 シリーズ ワイヤレス コントローラ 2 デバイスのディスカバリとインベントリは、Cisco DNA Center から正常に実行されます。
- デバイスは到達可能で、[Managed] 状態になっています。

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

ステップ 2 [Devices] > [Inventory] ウィンドウが表示され、検出されたすべてのデバイスがこのウィンドウに一覧表示されます。

ステップ 3 特定のサイトで使用可能なデバイスを表示するには、左側のペインで [Global] サイトを展開し、関心のあるサイト、ビルディング、またはフロアを選択します。

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

ステップ 4 [Device Type] リストから [WLCs] タブをクリックし、[Reachability] リストから [Reachable] タブをクリックして、検出済みで到達可能なワイヤレス コントローラのリストを取得します。

ステップ 5 [Inventory] ウィンドウで目的の Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ名をクリックし、プライマリコントローラとして設定します。

ステップ 6 [High Availability] タブをクリックします

デフォルトで選択された Catalyst 9800 シリーズ ワイヤレス コントローラがプライマリコントローラになり、[Primary C9800] フィールドはグレー表示されます。

ステップ 7 [Select Primary Interface] および [Secondary Interface] ドロップダウンリストから、HA 接続に使用するインターフェイスを選択します。

HA インターフェイスは次の目的で使用されます。

- IOSd が起動する前に、コントローラペア間の通信を有効にする。
- すべてのコントローラペアに IPC のトランスポートを提供する。
- コントローラペア間で交換される制御メッセージ全体の冗長性を有効にする。制御メッセージには、HA ロールの解決、キープアライブ、通知、HA 統計情報などがあります。

ステップ 8 [Select Secondary C9800] ドロップダウンリストから、HA ペアを作成するセカンダリコントローラを選択します。

ステップ 9 各フィールドに [Redundancy Management IP] と [Peer Redundancy Management IP] のアドレスを入力します。

(注) 冗長性管理 IP およびピア冗長性管理 IP に使用される IP アドレスは、Catalyst 9800 シリーズ ワイヤレス コントローラの管理インターフェイスと同じサブネットに設定する必要があります。これらの IP アドレスがそのサブネット範囲内で未使用の IP アドレスであることを確認します。

ステップ 10 [Netmask] フィールドに、ネットマスクアドレスを入力します。

ステップ 11 [HA の設定 (Configure HA)] をクリックします。

HA 設定は、CLI コマンドを使用してバックグラウンドで開始されます。最初に、プライマリコントローラが設定されます。成功すると、セカンダリコントローラが設定されます。HA が有効になると、両方のデバイスが再起動します。このプロセスは、完了するまで最大 2.5 分かかります。

ステップ 12 HA が開始されたら、[High Availability] タブの [Redundancy Summary] に、[Sync Status] が [HA Pairing is in Progress] と表示されます。HA ペアリングが成功したことを Cisco DNA Center が検出すると、[Sync Status] が [Complete] になります。

これは、インベントリ ポーラーまたは手動による再同期によってトリガーされます。これで、セカンダリコントローラ (Catalyst 9800 シリーズ ワイヤレス コントローラ 2) が Cisco DNA Center から削除されます。このフローは、Catalyst 9800 シリーズ ワイヤレス コントローラでの正常な HA 設定を示しています。

ステップ 13 手動でコントローラを再同期するには、[Provision] > [Inventory] ウィンドウで、手動で同期するコントローラを選択します。

ステップ 14 [アクション (Actions)] ドロップダウンリストから、[再同期 (Resync)] を選択します。

ステップ 15 プロセスが完了した後に発生するアクションのリストを次に示します。

- Catalyst 9800 シリーズ ワイヤレス コントローラ 1 および Catalyst 9800 シリーズ ワイヤレス コントローラ 2 は、冗長性管理、冗長性単位、およびシングルサインオン (SSO) を使用して設定されます。デバイスは、ロールをアクティブコントローラまたはスタンバイコントローラとしてネゴシエートするために再起動します。設定はアクティブからスタンバイへと同期されます。
- [冗長性の概要の表示 (Show Redundancy Summary)] ウィンドウで、次の設定を確認できます。
 - SSO は有効
 - Catalyst 9800 シリーズ ワイヤレス コントローラ 1 がアクティブ状態である

- Catalyst 9800 シリーズ ワイヤレス コントローラ 2 がスタンバイ状態である

ハイアベイラビリティについて

高可用性 (HA) によって、コントローラのフェールオーバーが原因で生じるワイヤレスネットワークのダウンタイムを短縮できます。Cisco DNA Center を使用して Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の高可用性を設定できます。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラで高可用性を設定するためのコマンド

ステップ 1 次のコマンドを使用して、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのプライマリで HA を設定します。

- **chassis ha-interface GigabitEthernet <redundancy interface num> local-ip <redundancy ip> <netmask> remote-ip <peer redundancy ip>** コマンドを実行して、HA シャーシインターフェイスを設定します。

次に、HA シャーシインターフェイスの設定例を示します。

```
chassis ha-interface GigabitEthernet 3 local-ip 1.1.1.2 255.255.255.0 remote-ip 1.1.1.3
```

- **reload** コマンドを実行して、変更が有効になるようにデバイスをリロードします。

ステップ 2 次のコマンドを使用して、Catalyst 9800 シリーズ ワイヤレス コントローラのセカンダリで HA を設定します。

- **chassis ha-interface GigabitEthernet <redundancy interface num> local-ip <redundancy ip> <netmask> remote-ip <peer redundancy ip>** コマンドを実行して、HA シャーシインターフェイスを設定します。

次に、HA シャーシインターフェイスの設定例を示します。

```
chassis ha-interface GigabitEthernet 2 local-ip 1.1.1.3 255.255.255.0 remote-ip 1.1.1.2
```

ステップ 3 **chassis clear** コマンドを実行して、すべての HA 関連のパラメータ（ローカル IP、リモート IP、HA インターフェイス、マスク、タイムアウト、プライオリティなど）をクリアまたは削除します。

(注) **reload** コマンドを実行して、変更を反映するためにデバイスをリロードします。

ステップ 4 Cisco Catalyst 9800-40 ワイヤレスコントローラおよび Cisco Catalyst 9800-80 ワイヤレス コントローラ デバイスのプライマリに HA を設定するには、次のコマンドを使用します。

- HA シャーシインターフェイスを設定するには、**chassis ha-interface local-ip <redundancy ip> <netmask> remote-ip <peer redundancy ip>** コマンドを実行します。

次に、HA シャーシインターフェイスの設定例を示します。

```
chassis ha-interface local-ip 1.1.1.2 255.255.255.0 remote-ip 1.1.1.3
```

- **reload** コマンドを実行して、変更が有効になるようにデバイスをリロードします。

ステップ 5 次のコマンドを使用して、Cisco Catalyst 9800-40 ワイヤレス コントローラおよび Cisco Catalyst 9800-80 ワイヤレス コントローラ デバイスのセカンダリに HA を設定します。

- HA シャーシインターフェイスを設定するには、**chassis ha-interface local-ip <redundancy ip> <netmask> remote-ip <peer redundancy ip>** コマンドを実行します。

次に、HA シャーシインターフェイスの設定例を示します。

```
chassis ha-interface local-ip 1.1.1.3 255.255.255.0 remote-ip 1.1.1.2
```

ステップ 6 **chassis clear** コマンドを実行して、すべての HA 関連のパラメータ（ローカル IP、リモート IP、HA インターフェイス、マスク、タイムアウト、プライオリティなど）をクリアまたは削除します。

(注) **reload** コマンドを実行して、変更を反映するためにデバイスをリロードします。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの高可用性を確認するためのコマンド

次のコマンドを使用して、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの高可用性設定を確認します。

- **config redundancy mode sso** コマンドを実行して、HA 関連の詳細情報を確認します。
- **show chassis** コマンドを実行して HA ペアのシャーシ設定を表示します。これには、MAC アドレス、ロール、スイッチプライオリティ、および冗長 HA ペア内の各コントローラ デバイスの現在の状態が含まれています。
- **show ip interface brief** コマンドを実行して、プラットフォームで設定されている設定モードではなく、デバイスで実行されている実際に稼働中の冗長モードを表示します。
- **show redundancy states** コマンドを実行して、アクティブコントローラとスタンバイコントローラの冗長性状態を表示します。
- **show redundancy summary** コマンドを実行して、設定されているインターフェイスを確認します。
- 高可用性設定の詳細を確認するには、**show romvar** コマンドを実行します。

N+1 高可用性

N+1 高可用性の概要

Cisco DNA Center では、シスコ ワイヤレス コントローラおよび Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ プラットフォームでの N+1 高可用性 (HA) がサポートされています。

HA-SKU を使用した N+1 HA は、Cisco 2504、5500、7500、および 8500 シリーズのスタンドアロン ワイヤレス コントローラ および WiSM2 コントローラ でサポートされています。

N+1 HA アーキテクチャは、低い導入コストで、地理的に離れたデータセンター間のコントローラに冗長性をもたらします。

N+1 HA では、単一のシスコワイヤレスコントローラを複数のプライマリコントローラのバックアップコントローラとして使用できます。これらのワイヤレスコントローラは互いに独立して、インターフェイスの設定や IP アドレスを共有しません。

Cisco DNA Center Cisco DNA Center は、N+1 HA のプライマリおよびセカンダリコントローラの設定をサポートします。

N+1 HA 設定は、グローバルレベルではなく AP レベルで行われます。設定は AP に直接ブッシュされます。

AP フォールバックオプションが有効の場合、プライマリ ワイヤレス コントローラが動作を再開すると、AP はバックアップワイヤレスコントローラからプライマリ ワイヤレス コントローラに自動的にフォールバックします。



(注) プライマリコントローラとセカンダリコントローラは、同じデバイスタイプである必要があります。たとえば、プライマリデバイスが Catalyst 9800 シリーズ ワイヤレス コントローラの場合は、セカンダリデバイスも Catalyst 9800 シリーズ ワイヤレス コントローラにする必要があります。

プライマリコントローラで高い優先順位が設定されている AP は、優先順位の低い AP が排除されることになっても、常に最初にバックアップコントローラに接続されます。

N+1 HA 設定には次の制限があります。

- N+1 HA 設定は、非ファブリック展開でのみサポートされます。
- VLAN ID の設定が原因で、セカンダリコントローラの自動プロビジョニングはサポートされていません。
- プライマリコントローラに変更を加えた場合、最新の設計の設定を使用してセカンダリコントローラを手動で再プロビジョニングする必要があります。
- Cisco DNA Center Cisco DNA Center では耐障害性はサポートされていません。
- アクセスポイントのステートフル スイッチオーバー (AP SSO) 機能は、N+1 HA ではサポートされていません。AP Control and Provisioning of Wireless Access Points (CAPWAP) ステートマシンは、プライマリコントローラに障害が発生したときに再起動されます。

Cisco DNA Center から N+1 高可用性を設定するための前提条件

- [Discovery] 機能を実行して、プライマリコントローラとセカンダリコントローラを検出します。

詳細については、[CDP を使用したネットワークの検出 \(19 ページ\)](#) または [Discover Your Network Using an IP Address Range \(25 ページ\)](#) を参照してください。

- ワイヤレス コントローラが到達可能で、[Managed] 状態である必要があります。

詳細については、[インベントリについて \(43 ページ\)](#) および [インベントリに関する情報の表示 \(45 ページ\)](#) を参照してください。

- デバイス間のネットワーク接続を確認します。プライマリコントローラがダウンした場合は、AP が N+1 の設定に従ってセカンダリコントローラに接続できる必要があります。
- 2つのビルディングを作成して、両方のデバイスのプライマリおよびセカンダリの場所を管理します。たとえば、ビルディング A とビルディング B のような2つのビルディングを作成し、ビルディング A をコントローラ1のプライマリ管理場所かつコントローラ2のセカンダリ管理場所に設定し、ビルディング B をコントローラ2のプライマリ管理場所としてのみ設定できます。

詳細については、[ネットワーク階層のサイトの作成 \(95 ページ\)](#)、[ビルディングの追加 \(99 ページ\)](#)、および[ビルディングへのフロアの追加 \(101 ページ\)](#)を参照してください。

- 設計フェーズ中にカバレッジヒートマップが可視化されるようにするには、フロアマップに AP を追加して配置します。

詳細については、「[APの追加、配置、および削除 \(104 ページ\)](#)」を参照してください。

- 2つの SSID を作成し、バックホール SSID として関連付けます。

詳細については、[エンタープライズワイヤレス ネットワーク用 SSID の作成 \(122 ページ\)](#)、[ゲストワイヤレス ネットワークの SSID の作成 \(127 ページ\)](#)、および[バックホール設定の管理 \(136 ページ\)](#)を参照してください。

Cisco DNA Center からの N+1 高可用性の設定

この手順では、非ファブリック展開環境において、シスコ ワイヤレス コントローラおよび Cisco Catalyst 9800 シリーズワイヤレス コントローラ プラットフォームに N+1 高可用性 (HA) を設定する方法について説明します。

-
- ステップ 1** Cisco DNA Center のホームページで、**[Provision]** を選択します。
- [Devices] > [Inventory]** ウィンドウが表示され、検出されたすべてのデバイスがこのウィンドウに一覧表示されます。
- ステップ 2** プライマリコントローラとしてプロビジョニングするには、目的のコントローラの隣にあるチェックボックスをオンにします。
- ステップ 3** **[Actions]** ドロップダウンリストから、**[Provision] > [Provision]** を選択します。
- [サイトの割り当て (Assign Site)]** ウィンドウが表示されます。
- ステップ 4** プライマリコントローラのプライマリ管理 AP 場所を割り当てるには、**[Choose a site]** をクリックします。
- ステップ 5** **[Choose a site]** ウィンドウで、サイトを選択して **[Save]** をクリックします。
- ステップ 6** **[次へ (Next)]** をクリックします。
- [Configuration]** ウィンドウが表示され、プライマリデバイスのプライマリ管理対象 AP の場所が表示されます。
- ステップ 7** **[Select Primary Managed AP Locations]** をクリックして、プライマリコントローラの管理対象 AP の場所を追加または更新できます。

- ステップ 8** [Managed AP Location] ウィンドウで、サイト名の隣にあるチェックボックスをオンにして、[Save] をクリックします。
- 親サイトまたは個々のサイトのいずれかを選択できます。
- ステップ 9** インターフェイスと VLAN の詳細を設定します。
- ステップ 10** [Configure Interface and VLAN] 領域で、IP アドレスとサブネットマスクの詳細を設定し、[Next] をクリックします。
- ステップ 11** [Advanced Configuration] ウィンドウで、事前定義されたテンプレート変数の値を設定し、[Next] をクリックします。
- ステップ 12** [Summary] ウィンドウでプライマリコントローラの管理対象 AP の場所およびその他の設定の詳細を確認し、[Deploy] をクリックします。
- デバイスをすぐに展開するには、[Now] オプションボタンをクリックし、[Apply] をクリックします。
 - 将来の日付と時刻でデバイスの展開をスケジュールするには、[Later] オプションボタンをクリックし、展開する日時を定義します。
- ステップ 13** 次に、セカンダリコントローラをプロビジョニングします。
- ステップ 14** [Inventory] ウィンドウで目的のコントローラの隣にあるチェックボックスをオンにし、セカンダリコントローラとしてプロビジョニングします。
- ステップ 15** [Actions] ドロップダウンリストから、[Provision] > [Provision] を選択します。
- [サイトの割り当て (Assign Site)] ウィンドウが表示されます。
- ステップ 16** セカンダリコントローラの管理対象 AP の場所を割り当てるには、[Choose a site] をクリックします。
- セカンダリコントローラの管理対象 AP の場所は、プライマリコントローラの管理対象 AP の場所と同じにする必要があります。
- ステップ 17** [Choose a site] ウィンドウで、セカンダリコントローラを関連付けるサイト名の隣にあるチェックボックスをオンにして、[Save] をクリックします。
- ステップ 18** [次へ (Next)] をクリックします。
- [Configuration] ウィンドウが表示され、セカンダリデバイスのプライマリ管理対象 AP の場所とセカンダリ管理対象 AP の場所が表示されます。
- ステップ 19** [Select Secondary Managed AP Locations] をクリックして、セカンダリコントローラの管理対象 AP の場所を追加または更新できます。
- ステップ 20** [Managed AP Location] ウィンドウで、サイト名の隣にあるチェックボックスをオンにして、[Save] をクリックします。
- 親サイトまたは個々のサイトのいずれかを選択できます。
- ステップ 21** セカンダリコントローラのインターフェイスと VLAN の詳細を設定します。
- ステップ 22** [Configure Interface and VLAN] 領域で、セカンダリコントローラの IP アドレスとサブネットマスクの詳細を設定し、[Next] をクリックします。

- ステップ 23** [Advanced Configuration] ウィンドウで、事前定義されたテンプレート変数の値を設定し、[Next] をクリックします。
- ステップ 24** [Summary] ウィンドウで、セカンダリコントローラの管理対象 AP の場所やその他の設定の詳細を確認し、[Deploy] をクリックします。
- デバイスをすぐに展開するには、[Now] オプションボタンをクリックし、[Apply] をクリックします。
 - 将来の日付と時刻でデバイスの展開をスケジュールするには、[Later] オプションボタンをクリックし、展開する日時を定義します。
- ステップ 25** プライマリおよびセカンダリコントローラの管理対象場所を確認するには、[Provision] > [Device] > [Inventory] ウィンドウでプロビジョニングしたコントローラのデバイス名をクリックします。
- ステップ 26** [Device details] ウィンドウで、[Managed ap locations] タブをクリックして、プライマリおよびセカンダリの管理場所の詳細を表示します。
- ステップ 27** プライマリコントローラの AP をプロビジョニングします。
- ステップ 28** [Devices] > [Inventory] ウィンドウで、プロビジョニングする AP の隣にあるチェックボックスをオンにします。
- ステップ 29** [Actions] ドロップダウンリストから、[Provision] > [Provision] を選択します。
- ステップ 30** [Assign Site] ウィンドウで、[Choose a Floor] をクリックして、プライマリ管理場所からフロアを選択します。
- ステップ 31** [Next] をクリックします。
- [設定 (Configuration)] ウィンドウが表示されます。
- ステップ 32** デフォルトでは、[Network Settings] > [Wireless] > [Wireless Radio Frequency Profile] でデフォルトとマークしたカスタム RF プロファイルが、[RF Profile] ドロップダウンリストで選択されています。
- [RF プロファイル (RF Profile)] ドロップダウンリストから値を選択して、AP のデフォルト RF プロファイル値を変更できます。
- ステップ 33** [次へ (Next)] をクリックします。
- ステップ 34** [Summary] ウィンドウで、詳細を確認します。
- ステップ 35** [Deploy] をクリックして、プライマリ AP をプロビジョニングします。
- ステップ 36** AP グループの作成または変更が進行中であることを示すメッセージが表示されます。
- 「プロビジョニング後に AP が再起動します。続行しますか? (After provisioning AP(s) will reboot. Do you want to continue?) 」というメッセージが表示されます。
- ステップ 37** [OK] をクリックします。
- 展開が成功すると、[Device Inventory] ウィンドウの [Last Sync Status] 列に、[SUCCESS] と表示されます。

モビリティ設定の概要

Cisco DNA Center のモビリティ設定では、一連のシスコワイヤレスコントローラをモビリティグループにグループ化して、ワイヤレスクライアントのシームレスなローミング体験を実現できます。

モビリティグループを作成すると、ネットワーク内で複数のワイヤレスコントローラを有効にして、コントローラ間またはサブネット間のローミングが発生した際に、動的に情報を共有してデータトラフィックを転送できます。異なるモビリティグループ名を同じ無線ネットワーク内の異なるワイヤレスコントローラに割り当てると、モビリティグループによって、1つの企業内の異なるフロア、ビルディング、キャンパス間でのローミングを制限できます。

Cisco DNA Center では、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラおよび Cisco AireOS コントローラなどのさまざまなプラットフォーム間でモビリティグループを作成できます。

モビリティ設定の注意事項と制約事項：

- [Provision] ページでは、モビリティを設定するために複数のコントローラを選択することはできません。
- デフォルトとしてグループ名を使用してモビリティグループを作成することはできません。これにより、モビリティおよび RF グループ名がデフォルトとしてリセットされ、すべてのピアが削除されます。
- アンカーコントローラでモビリティグループ名を設定することはできません。
- Cisco AireOS コントローラでモビリティグループを設定しているときに仮想 IP アドレスが変更された場合は、ワイヤレス コントローラを手動で再起動する必要があります。
- 同じモビリティグループ名を持つワイヤレスコントローラは、自動的に1つのモビリティグループにグループ化され、互いにピアとして追加されます。
- Cisco AireOS コントローラでモビリティグループを設定するときに、ワイヤレス コントローラに IP アドレス 192.0.2.1 がない場合、Cisco DNA Center は仮想 IP アドレス (192.0.2.1) をすべてのワイヤレス コントローラにプッシュします。
- ゲストアンカーコントローラをモビリティグループに明示的に追加しないでください。プロビジョニングされたゲストアンカーコントローラは、[Mobility Configuration] ページでピアを追加している間、ドロップダウンリストに表示されません。
- ワイヤレスコントローラをゲストアンカーとしてプロビジョニングする場合は、そのワイヤレスコントローラがモビリティグループに追加されていないことを確認します。

モビリティ設定ワークフロー

次に、シスコワイヤレスコントローラでモビリティを設定するために使用できるワークフローを示します。

- モビリティ設定は、[Provision] ページの [Configuration] ウィンドウにあります。

- モビリティを設定するには、モビリティグループ名、RFグループ名、およびモビリティピアを指定してワイヤレスコントローラをプロビジョニングする必要があります。
- ワイヤレスコントローラのプロビジョニング中に適用される設定は、そのグループに設定されているすべてのモビリティピアに自動的に複製されます。
- ワイヤレスコントローラを再同期して、最新のトンネルステータスを取得します。

モビリティ設定の使用例

次の使用例では、コントローラ間のモビリティの設定手順について説明します。

使用例 1

シスコワイヤレスコントローラ1、ワイヤレスコントローラ2、およびワイヤレスコントローラ3は、モビリティグループ名 (Default) を使用して Cisco DNA Center 新たに追加されていて、まだプロビジョニングされていません。

1. モビリティグループ名、RFグループ名を設定してワイヤレスコントローラ1をプロビジョニングし、ピアとしてワイヤレスコントローラ2およびワイヤレスコントローラ3を追加します。
2. ワイヤレスコントローラ2をプロビジョニングします。
[Provision] ウィンドウでは、ワイヤレスコントローラ2のモビリティ設定がグループ名とピアとともに自動的に入力されます。
3. ワイヤレスコントローラ3をプロビジョニングします。
4. すべてのワイヤレスコントローラをプロビジョニング後、ワイヤレスコントローラを再同期して、最新のトンネルステータスを受信します。

使用例 2

異なるモビリティグループ名を持つシスコワイヤレスコントローラ1、ワイヤレスコントローラ2、およびワイヤレスコントローラ3はすでに Cisco DNA Center に追加されていて、プロビジョニングされています。

1. モビリティグループ名、RFグループ名を設定してワイヤレスコントローラ1をプロビジョニングし、ピアとしてワイヤレスコントローラ2およびワイヤレスコントローラ3を追加します。
2. モビリティ設定は、ワイヤレスコントローラ2、ワイヤレスコントローラ3などの他のピア間で自動的に複製されます。
 - ワイヤレスコントローラ1のプロビジョニングが成功すると、ワイヤレスコントローラ2とワイヤレスコントローラ3がピアとしてワイヤレスコントローラ1に追加されます。
 - ワイヤレスコントローラ1とワイヤレスコントローラ3は、ワイヤレスコントローラ2のピアとして追加されます。

- ワイヤレス コントローラ 1 とワイヤレス コントローラ 2 は、ワイヤレス コントローラ 3 のピアとして追加されます。

N+1 ローリング AP アップグレードについて

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのローリング AP アップグレード機能では、ダウンタイムを最小限に抑えるために、シスコ ワイヤレス コントローラと AP をアップグレードする方法が提供されています。ゼロダウンタイムを実現するために、N+1 ローリング AP アップグレード機能を使用して、段階的に AP をアップグレードできます。

ローリング AP アップグレードは、N+1 コントローラの詳細と一度に再起動可能な AP の割合を指定することによって、プライマリコントローラで開始されます。設定された割合に基づいて、プライマリコントローラは RRM ネイバー情報に基づくアルゴリズムを使用して、内部的に AP を複数回の反復に分割します。1 回の反復分の AP が再起動している間は常に、他の AP によってネットワークカバレッジが提供されます。

プライマリコントローラは、反復処理の一部として AP のセットを選択し、そのプライマリコントローラが N+1 コントローラをポイントするように設定し、AP の交換と再起動を行います。N+1 コントローラ上で AP が使用可能になると、プライマリコントローラにメッセージが送信され、次の回の反復に進みます。すべての AP がアップグレードされて N+1 コントローラに移動すると、プライマリコントローラが再起動され、新しいイメージがアクティブになります。プライマリコントローラが新しいイメージでアップグレードされると、N+1 コントローラからの AP は、AP を再起動することなく、交互にプライマリコントローラに戻されます。

次に、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのローリング AP アップグレードを設定するための前提条件を示します。

- N+1 コントローラではすでにゴールデンイメージが実行されているため、ローリング AP アップグレードはダウンタイムなしで動作します。
- N+1 コントローラはに到達可能であり、Cisco DNA Center で [Managed] 状態になっています。
- プライマリコントローラと N+1 コントローラ間のモビリティトンネルを確立します。プライマリコントローラと N+1 コントローラ間のアップグレード情報は、モビリティトンネルを介して交換されます。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのローリング AP アップグレードを設定するためのワークフロー


始める前に



- (注) N+1 ローリング AP アップグレードは、ファブリック以外の導入でのみサポートされています。

ステップ 1 Cisco DNA Center を設置します。

詳細については、[Cisco Digital Network Architecture Center 設置ガイド \[英語\]](#) を参照してください。

- ステップ 2** Cisco DNA Center GUI にログインし、必要なアプリケーションが [Running] 状態であることを確認します。
- 確認するには、Cisco DNA Center のホームページで、歯車アイコン  をクリックし、[System Settings] > [Software Updates] > [Installed Apps] を選択します。
- ステップ 3** ディスカバリ機能を使用して Cisco Catalyst 9800 シリーズ ワイヤレス コントローラを検出します。
- Catalyst 9800 シリーズ ワイヤレス コントローラを検出するには、NETCONF を有効にしてポートを 830 に設定する必要があります。NETCONF は、ネットワークデバイスの設定をインストール、操作、削除するためのメカニズムです。
- 詳細については、[CDP を使用したネットワークの検出 \(19 ページ\)](#) または [Discover Your Network Using an IP Address Range \(25 ページ\)](#) を参照してください。
- ステップ 4** 検出されたデバイスが [Device Inventory] ウィンドウに [Managed] 状態で表示されていることを確認します。
- 詳細については、[インベントリについて \(43 ページ\)](#) および [インベントリに関する情報の表示 \(45 ページ\)](#) を参照してください。
- デバイスが [Managed] になるまで待機する必要があります。
- ステップ 5** サイト、ビルディング、フロアを追加してネットワーク階層を設計すると、後で設計の設定や構成を適用する場所を簡単に特定できるようになります。
- 新しいネットワーク階層を作成します。または Cisco Prime Infrastructure に既存のネットワーク階層がある場合は、それを Cisco DNA Center にインポートできます。
- 既存のネットワーク階層をインポートしてアップロードするには、[既存のサイト階層をアップロード \(97 ページ\)](#) を参照してください。
- 新しいネットワーク階層を作成するには、[ネットワーク階層のサイトの作成 \(95 ページ\)](#)、[ビルディングの追加 \(99 ページ\)](#)、および [ビルディングへのフロアの追加 \(101 ページ\)](#) を参照してください。
- ステップ 6** AP の位置情報を追加し、フロアマップに配置して、ヒートマップカバレッジを可視化します。
- 詳細については、「[AP の追加、配置、および削除 \(104 ページ\)](#)」を参照してください。
- ステップ 7** プライマリ管理対象 AP の場所、およびローリング AP アップグレードが有効になっており、モビリティグループがセカンダリコントローラをピアとして設定されている状態で、プライマリコントローラをプロビジョニングします。
- これを行うには、[Provision] > [Devices] > [Inventory] を選択し、プライマリコントローラ名の隣にあるチェックボックスをオンにします。
- ステップ 8** モビリティグループ設定で、モビリティピアとして N+1 コントローラを設定します。
- 詳細については、「[モビリティ設定の概要 \(306 ページ\)](#)」を参照してください。

ステップ 9 プライマリコントローラのプライマリ管理対象 AP の場所を N+1 コントローラのセカンダリ管理対象 AP の場所として設定することで、N+1 HA コントローラをプロビジョニングします。これにより、セカンダリコントローラが N+1 コントローラとして設定されます。

詳細については、「[Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのプロビジョニング \(311 ページ\)](#)」を参照してください。

ステップ 10 プライマリコントローラに関連付けられている AP をプロビジョニングします。

詳細については、「[シスコ製 AP のプロビジョニング : Day 1 AP プロビジョニング \(284 ページ\)](#)」を参照してください。

ステップ 11 ソフトウェアイメージをリポジトリにインポートします。

詳細については、「[ソフトウェア イメージのインポート \(77 ページ\)](#)」を参照してください。

ステップ 12 ソフトウェアイメージをデバイスファミリに割り当てます。

詳細については、「[デバイスファミリへのソフトウェアイメージの割り当て \(78 ページ\)](#)」を参照してください。

ステップ 13 デバイスファミリまたはデバイスロールの星印をクリックして、ソフトウェアイメージをゴールデンとしてマークします。

詳細については、「[ゴールデン ソフトウェア イメージの指定 \(80 ページ\)](#)」を参照してください。

ステップ 14 イメージをアップグレードする前に、両方のデバイスでイメージの準備状況チェックが成功していることを確認してください。

また、[N+1 Device Check] と [Mobility Tunnel Check] のステータスに緑色のチェックマークが付いていることも確認してください。

- イメージ更新の準備状況チェックを実行するには、[Provision] > [Devices] > [Software Images] を選択します。
- イメージをアップグレードするデバイスを選択します。
- デバイスの事前チェックが成功すると、[Image Precheck Status] 列の [Status] リンクに緑色のチェックマークが付きます。デバイスのアップグレード準備状況の事前チェックのいずれかが失敗した場合、[Image Precheck Status] リンクのマークが赤色に変わり、そのデバイスの OS イメージは更新できません。先に進む前に [Status] リンクをクリックし、エラーを修正します。

ステップ 15 プライマリコントローラでアップグレードを開始します。

ステップ 16 [Provision] > [Devices] > [Software Images] ページで、プライマリコントローラの隣にあるチェックボックスをオンにします。

ステップ 17 [Actions] ドロップダウンリストから、[Software Image] > [Update Image] を選択します。

詳細については、「[ソフトウェア イメージのプロビジョニング \(81 ページ\)](#)」を参照してください。

ステップ 18 イメージのアップグレードの進行状況をモニタするには、[Software Image] 列で [In Progress] をクリックします。

[Device Status] ページには、次の情報が表示されます。

- [Distribution Operation] : イメージ配信プロセスに関する情報が表示されます。イメージは Cisco DNA Center からプライマリデバイスにコピーされます。アクティブ化操作は、配信プロセスが完了すると開始されます。
- [Activate Operation] : アクティブ化操作の詳細が表示されます。このプロセス中に、ローリング AP アップグレードが開始されます。
- [Rolling AP Upgrade Operation] : ローリング AP アップグレードタスクが完了したかどうか、保留中の AP の数、再起動中の AP の数、N+1 コントローラに接続している AP の数など、ローリング AP アップグレードの概要が表示されます。


[View AP Status] をクリックすると、プライマリコントローラ、N+1 コントローラ、デバイス名、現在のステータス、および反復に関する詳細が表示されます。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのプロビジョニング

始める前に

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのプロビジョニングを行う前に、[Cisco DNA Center](#) で [Cisco Catalyst 9800 ワイヤレスコントローラを設定するためのワークフロー](#) (293 ページ) の手順を完了したことを確認します。

-
- ステップ 1** Cisco DNA Center のホームページで、[Provision] を選択します。
- [Devices] > [Inventory] ウィンドウに、検出されたデバイスのリストが表示されます。
- ステップ 2** サイトに関連付ける Catalyst 9800 シリーズ ワイヤレス コントローラ名の横にあるチェックボックスをオンにします。
- ステップ 3** [Actions] ドロップダウンリストから、[Provision] > [Assign Device to Site] を選択します。
- ステップ 4** [Assign Device to Site] ウィンドウで、[Choose a Site] をクリックして Catalyst 9800 シリーズ ワイヤレス コントローラ デバイスのサイトを割り当てます。
- ステップ 5** [Add Sites] ウィンドウで、サイト名の横にあるチェックボックスをオンにして Catalyst 9800 シリーズ ワイヤレス コントローラ を関連付けます。
- 親サイトまたは個々のサイトのいずれかを選択できます。親サイトを選択すると、その下にあるすべての子も選択されます。このチェックボックスをオフにすると、個々のサイトの選択を解除できます。
- ステップ 6** [Save (保存)] をクリックします。
- ステップ 7** [Apply] をクリックします。
- ステップ 8** 設計フェーズ中に追加された設定を使用して、デバイスをプロビジョニングします。
- ステップ 9** [Provision] > [Devices] > [Inventory] の順に選択します。
- ステップ 10** プロビジョニングする Catalyst 9800 シリーズ ワイヤレス コントローラ 名の横にあるチェックボックスをオンにします。

- ステップ 11** [Actions] ドロップダウンリストから、**[Provision] > [Provision]** を選択します。
- ステップ 12** [Assign Site] ウィンドウで、[Next] をクリックします。
[設定 (Configuration)] ウィンドウが表示されます。
- ステップ 13** Catalyst 9800 シリーズ ワイヤレス コントローラ デバイスでワイヤレス コントローラのロールを [Active Main WLC] として選択します。
- ステップ 14** プライマリ コントローラの管理 AP の場所を設定するには、[Select Primary Managed AP Locations] をクリックします。
- ステップ 15** [Select Secondary Managed AP Locations] をクリックして、セカンダリ管理 AP の場所のセカンダリコントローラをプライマリ管理 AP の場所のプライマリコントローラとして設定します。
- ステップ 16** 親サイトまたは個々のサイトのいずれかを選択できます。親サイトを選択すると、その下にあるすべての子も選択されます。チェックボックスをオフにして、特定のサイトの選択を解除することができます。
(注) 管理対象 AP の場所を継承することで、サイトおよび特定のサイトのビルディングとフロアを自動的に選択できます。1つのサイトは1つの ワイヤレス コントローラ によってのみ管理されます。
- ステップ 17** [Rolling AP Upgrade] エリアで、[Enable] チェックボックスをオンにして、ローリング AP アップグレード ステータスを有効にします。
ローリング AP アップグレードの詳細については、[Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのローリング AP アップグレードを設定するためのワークフロー \(308 ページ\)](#) を参照してください。
(注) ローリング AP アップグレード操作は、ファブリック対応のゲストアンカーデバイスではサポートされていません。
- ステップ 18** [AP Reboot Percentage] ドロップダウンリストから、反復 1 回で再起動できる AP の割合を選択します。
- ステップ 19** [Mobility Group] で [Configure] をクリックして、モビリティピアを設定します。
[Configure Mobility Group] サイドパネルが表示されます。
詳細については、「[モビリティ設定の概要 \(306 ページ\)](#)」を参照してください。
- ステップ 20** [Mobility Group Name] ドロップダウンリストで、**+** をクリックして新しいモビリティグループを追加するか、既存のモビリティグループから選択します。
既存のモビリティピア情報は、Cisco DNA Center で使用可能なインテントからロードされます。
- ステップ 21** [RF Group Name] テキストボックスに RF グループの名前を入力します。
- ステップ 22** [Mobility Peers] で [Add] をクリックして、モビリティピアを設定します。 
- ステップ 23** [Device Name] ドロップダウンリストからコントローラを選択します。
デバイスがプロビジョニングされると、Cisco DNA Center はデバイスにモビリティグループを作成し、RF グループを割り当て、ピアのすべての終端を設定します。モビリティグループの設定は、選択したすべてのピアデバイスに自動的に展開されます。
- ステップ 24** [保存 (Save)] をクリックします。

- ステップ 25** モビリティグループ名と RF グループ名をリセットするには、次のいずれかを実行します。
- [Configure Mobility Group] サイドパネルで、[Mobility Group Name] ドロップダウンリストから [default] を選択します。
 - [Provision] > [Configuration] ページの [Mobility Group] で、[Reset] をクリックします。
- これにより、[RF Group Name] が自動的に [default] に設定され、すべてのピアが削除されます。プロビジョニングが完了すると、デバイスのモビリティが設定され、そのデバイスは他のすべてのピアから削除されます。
- ステップ 26** アクティブなメイン ワイヤレス コントローラ では、インターフェイスと VLAN の詳細を設定する必要があります。
- ステップ 27** [Assign Interface] エリアで、次の操作を実行します。
- [VLAN ID] : VLAN ID の値を入力します。
 - [IP Address] : インターフェイス IP アドレスを入力します。
 - [Gateway IP Address] : ゲートウェイ IP アドレスを入力します。
 - [Subnet Mask (in bits)] : インターフェイスのネットマスクの詳細を入力します。
- (注) Catalyst 9800 シリーズ ワイヤレス コントローラ では、IP アドレス、ゲートウェイ IP アドレス、およびサブネットマスクを割り当てる必要はありません。
- ステップ 28** [次へ (Next)] をクリックします。
- [Advanced Configuration] ウィンドウが表示されます。ここでは、事前定義されたテンプレート変数の値を入力できます。
- ステップ 29** [Devices] パネルでデバイスまたはテンプレートを検索します。
- ステップ 30** [wlanid] フィールドに、事前定義されたテンプレート変数の値を入力します。
- ステップ 31** [次へ (Next)] をクリックします。
- ステップ 32** [Summary] ウィンドウで、次の設定を確認します。
- デバイスの詳細
 - ネットワークの設定
 - SSID
 - 管理サイト
 - インターフェイス
 - 詳細設定
- ステップ 33** [Deploy] をクリックして、Catalyst 9800 シリーズ ワイヤレス コントローラ をプロビジョニングします。
- デバイスをすぐに展開するには、[Now] オプションボタンをクリックし、[Apply] をクリックします。

- 将来の日付と時刻でデバイスの展開をスケジュールするには、[Later] オプションボタンをクリックし、展開する日時を定義します。

ステップ 34 Cisco DNA Center からデバイスにプッシュされる設定を確認するには、Catalyst 9800 シリーズ ワイヤレスコントローラ デバイスで次のコマンドを使用します。

- `#show wlan summary`
- `#show run | sec line`
- `#show running-configuration`

ステップ 35 デバイスが正常に展開されると、[Provision Status] が [Configuring] から [Success] に変わります。

ステップ 36 [Inventory] ウィンドウで、デバイスの [Provision Status] カラムの [See Details] をクリックし、ネットワークインテントの詳細情報を取得するか、アクションのリストを表示します。

ステップ 37 [Device Provisioning] の下の [See Details] をクリックします。

ステップ 38 [Deployment of network intent] の下の [View Details] をクリックし、デバイス名をクリックします。

ステップ 39 デバイス名をクリックして展開します。

ステップ 40 [Configuration Summary] エリアを展開して、操作の詳細、機能名、および管理機能を表示します。また、[Configuration Summary] には、デバイスのプロビジョニング中に発生したエラーも理由とともに表示されます。

ステップ 41 デバイスに送信される正確な設定の詳細を表示するには、[Provision Summary] エリアを展開します。

ステップ 42 AP をプロビジョニングします。

詳細については、「[シスコ製APのプロビジョニング : Day 1 APプロビジョニング \(284 ページ\)](#)」を参照してください。

Catalyst 9000 シリーズ スイッチ用 Cisco Catalyst 9800 組み込みワイヤレスコントローラの設定とプロビジョニング

サポートされているハードウェア プラットフォーム

デバイス ロール	プラットフォーム
組み込みワイヤレスコントローラ	Cisco Catalyst 9300 シリーズ スイッチ Cisco Catalyst 9400 シリーズ スイッチ Cisco Catalyst 9500-H シリーズ スイッチ
ファブリック エッジ	Cisco Catalyst 9300 シリーズ スイッチ Cisco Catalyst 9400 シリーズ スイッチ Cisco Catalyst 9500-H シリーズ スイッチ

デバイス ロール	プラットフォーム
	Cisco Catalyst 3600 シリーズ スイッチ Cisco Catalyst 3850 シリーズ スイッチ
AP	Cisco 802.11ac Wave 2 AP : <ul style="list-style-type: none"> • Cisco Aironet 1810 シリーズ OfficeExtend アクセス ポイント • Cisco Aironet 1810W シリーズ アクセス ポイント • Cisco Aironet 1815i Access Point • Cisco Aironet 1815w アクセスポイント • Cisco Aironet 1815m アクセス ポイント • Cisco 1830 Aironet シリーズ アクセスポイント • Cisco Aironet 1850 シリーズ アクセス ポイント • Cisco Aironet 2800 シリーズ アクセス ポイント • Cisco Aironet 3800 シリーズ アクセス ポイント • Cisco Aironet 4800 シリーズ アクセス ポイント Cisco 802.11ac Wave 1 AP <ul style="list-style-type: none"> • Cisco Aironet 1700 シリーズ アクセス ポイント • Cisco Aironet 2700 シリーズ アクセス ポイント • Cisco Aironet 3700 シリーズ アクセス ポイント


事前設定

Catalyst 9300 シリーズスイッチ用 Cisco Catalyst 9800 組み込みワイヤレスコントローラで、スイッチが **aaa new-model** を使用してすでに設定されている場合は、次のコマンドが存在することを確認してください。

```
aaa new-model
aaa authentication login default local
aaa authorization exec default local
aaa session-id common
```

これは、NETCONF の設定では必須です。プロビジョニングに自動アンダーレイを使用している場合、これらの設定は必要ありません。

Catalyst 9000 スイッチ用 Cisco Catalyst 9800 組み込みワイヤレスコントローラを設定するためのワークフロー

1. Cisco DNA Center を設置します。
詳細については、[Cisco Digital Network Architecture Center 設置ガイド \[英語\]](#) を参照してください。
2. Cisco DNA Center GUI にログインし、必要なアプリケーションが [Running] 状態であることを確認します。
確認するには、Cisco DNA Center のホームページで、歯車アイコン  をクリックし、**[System Settings] > [Software Updates] > [Installed Apps]** を選択します。
3. Cisco Identity Services Engine と Cisco DNA Center を連動させます。Cisco ISE が Cisco DNA Center に登録されると、Cisco DNA Center が検出するすべてのデバイスが、関連する設定データやその他のデータとともに Cisco ISE にプッシュされます。
4. Cisco Catalyst 9000 シリーズ スイッチおよびエッジスイッチを検出します。
Catalyst 9000 シリーズ スイッチの Cisco Catalyst 9800 組み込みワイヤレスコントローラを検出するには、NETCONF を有効にし、ポートを 830 に設定する必要があります。
エッジスイッチを検出するために NETCONF を有効にする必要はありません。
詳細については、[CDP を使用したネットワークの検出 \(19 ページ\)](#) および [Discover Your Network Using an IP Address Range \(25 ページ\)](#) を参照してください。
[Preferred Management IP] を [Use Loopback] に変更します。
5. デバイスが [Device Inventory] に [Managed] 状態で表示されていることを確認します。
詳細については、[インベントリについて \(43 ページ\)](#) および [インベントリに関する情報の表示 \(45 ページ\)](#) を参照してください。
デバイスが [Managed] 状態になっていることを確認します。
6. ネットワークの地理的な場所を表すネットワーク階層を設計します。サイト、ビルディング、フロアを作成すると、後で設計の設定や構成を適用する場所を簡単に特定できるようになります。
新しいネットワーク階層を作成します。または Cisco Prime Infrastructure に既存のネットワーク階層がある場合は、それを Cisco DNA Center にインポートできます。
既存のネットワーク階層をインポートしてアップロードするには、[既存のサイト階層をアップロード \(97 ページ\)](#) を参照してください。
新しいネットワーク階層を作成するには、[ネットワーク階層のサイトの作成 \(95 ページ\)](#)、[ビルディングの追加 \(99 ページ\)](#)、および [ビルディングへのフロアの追加 \(101 ページ\)](#) を参照してください。
7. 非ファブリックネットワークで設計フェーズ中にヒートマップの可視化を取得するには、フロアマップに AP を追加して配置します。

ファブリックネットワークの場合、設計時にフロアマップに AP を配置することはできません。AP は、ファブリックネットワークにデバイスを追加した後にオンボードされます。

詳細については、「[AP の追加、配置、および削除 \(104 ページ\)](#)」を参照してください。

8. AAA (Cisco Identity Services Engine がネットワークおよびクライアントエンドポイント用に設定されている)、NetFlow コレクタ、NTP、DHCP、DNS、syslog、および SNMP トラップなどのネットワーク設定を定義します。これらのネットワークサーバが、ネットワーク全体のデフォルトになります。

詳細については、[グローバル ネットワーク設定について \(146 ページ\)](#)、[グローバル ネットワーク サーバの設定 \(162 ページ\)](#)、および「[Cisco ISE またはその他の AAA サーバの追加](#)」を参照してください。

9. CLI、SNMP、HTTP などのデバイスのログイン情報を設定します。

詳細については、[グローバル デバイス クレデンシヤルについて \(149 ページ\)](#)、[グローバル CLI クレデンシヤルの設定 \(150 ページ\)](#)、[グローバル SNMPv2c クレデンシヤルの設定 \(151 ページ\)](#)、[グローバル SNMPv3 クレデンシヤルの設定 \(152 ページ\)](#)、[グローバル HTTPS クレデンシヤルの設定 \(154 ページ\)](#) を参照してください。

10. IP アドレスプールをグローバルレベルで設定します。

IP アドレスプールを設定するには、[IP アドレスプールを設定する \(158 ページ\)](#) を参照してください。

プロビジョニングするビルディングの IP アドレスプールを予約するには、「[LAN アンダーレイのプロビジョニング](#)」を参照してください。

11. エンタープライズおよびゲストワイヤレスネットワークを作成します。グローバルワイヤレス設定を 1 回定義します。次に、Cisco DNA Center は地理的な場所全体でさまざまなデバイスに設定をプッシュします。

ワイヤレスネットワークの設計は、2 段階のプロセスです。まず、[Wireless] ページで SSID を作成する必要があります。次に、作成した SSID をワイヤレス ネットワーク プロファイルに関連付けます。このプロファイルは、サイトにデバイスを展開するために使用されるトポロジを構築するのに役に立ちます。

詳細については、[エンタープライズ ワイヤレス ネットワーク用 SSID の作成 \(122 ページ\)](#) および [ゲスト ワイヤレス ネットワークの SSID の作成 \(127 ページ\)](#) を参照してください。

12. バックホールの設定を行います。詳細については、「[バックホール設定の管理 \(136 ページ\)](#)」を参照してください。

13. [Policy] ページで、次のように設定します。

- 仮想ネットワークを作成します。仮想ネットワークを使用して、物理ネットワークを複数の論理ネットワークにセグメント化できます。詳細については、[仮想ネット](#)

ワーク (245 ページ) および仮想ネットワークの作成 (246 ページ) を参照してください。

- グループベースのアクセスコントロールポリシーを作成し、契約を追加します。詳細については、「[グループベースのアクセスコントロールポリシーの作成 \(199 ページ\)](#)」を参照してください。

14. 設計フェーズ中に追加された設定を使用して、Cisco Catalyst 9000 シリーズ スイッチとエッジノードスイッチをプロビジョニングします。

- ファブリックドメインを作成します。
- CP+ボーダー+エッジまたはCP+ボーダーを作成して、デバイスをファブリックネットワークに追加します。
- Catalyst 9000 シリーズ スイッチの Cisco Catalyst 9800 組み込みワイヤレスコントローラで、組み込みワイヤレス機能を有効にします。
- ファブリックドメイン内のオンボード AP。

デバイスが正常に展開されると、展開ステータスが [Configuring] から [Success] に変わります。

詳細については、「[Cisco Catalyst 9000 シリーズ スイッチでの組み込みワイヤレスのプロビジョニング \(318 ページ\)](#)」を参照してください。

Cisco Catalyst 9000 シリーズ スイッチでの組み込みワイヤレスのプロビジョニング

始める前に

Catalyst 9000 シリーズ スイッチの Cisco Catalyst 9800 組み込みワイヤレスコントローラをプロビジョニングする前に、[Catalyst 9000 スイッチ用 Cisco Catalyst 9800 組み込みワイヤレスコントローラを設定するためのワークフロー \(316 ページ\)](#) の手順を完了していることを確認します。

この手順では、Cisco Catalyst 9300 シリーズ スイッチ、Cisco Catalyst 9400 シリーズ スイッチ、および Cisco Catalyst 9500H シリーズ スイッチに組み込みワイヤレスをプロビジョニングする方法について説明します。

-
- ステップ 1** Cisco DNA Center のホームページで、[Provision] を選択します。
[Devices] > [Inventory] ウィンドウに、検出されたデバイスのリストが表示されます。
- ステップ 2** Catalyst 9000 シリーズ スイッチデバイスと、サイトに関連付けるエッジスイッチの横にあるチェックボックスをオンにします。
- ステップ 3** [Actions] ドロップダウンリストから、[Provision] > [Assign Device to Site] を選択します。
- ステップ 4** [Assign Device to Site] ウィンドウで、[Choose a Site] をクリックします。

- ステップ 5** [Choose a site] ウィンドウで、サイトの横にあるチェックボックスをオンにして、デバイスを関連付けます。
- ステップ 6** [Save (保存)] をクリックします。
- ステップ 7** [Apply] をクリックします。
次の手順では、設計フェーズ中に追加された設定を使用して、Catalyst 9000 シリーズ スイッチとエッジノードをプロビジョニングします。
- ステップ 8** [Devices] > [Inventory] ウィンドウで、プロビジョニングするデバイス名の横にあるチェックボックスをオンにします。
- ステップ 9** [Actions] ドロップダウンリストから、[Provision] を選択します。
- ステップ 10** [次へ (Next)] をクリックします。
- ステップ 11** [Summary] ウィンドウで設定を確認し、[Deploy] をクリックします。
- ステップ 12** エッジスイッチをプロビジョニングするには、プロビジョニングするエッジスイッチの横にあるチェックボックスをオンにします。
- ステップ 13** [Actions] ドロップダウンリストから、[Provision] を選択します。
- ステップ 14** [次へ (Next)] をクリックします。
- ステップ 15** [Summary] ウィンドウで設定を確認し、[Deploy] をクリックします。
デバイスが正常に展開されると、[Provision Status] が [Configuring] から [Success] に変わります。
- ステップ 16** ファブリックドメインにデバイスを追加するには、Cisco DNA Center のホームページで [Provision] > [Fabric] を選択します。
- ステップ 17** ファブリック LAN を作成します。詳細については、「[ファブリックドメインの作成 \(334 ページ\)](#)」を参照してください。
- ステップ 18** IP トランジットネットワークを追加します。
IP トランジットネットワークは通常の IP ネットワークで使用され、外部に接続したり、2 つ以上のファブリックサイトを接続したりします。詳細については、「[IP のトランジットネットワークの作成 \(333 ページ\)](#)」を参照してください。
- ステップ 19** デバイスを追加して、ファブリックドメインへ仮想ネットワークを関連付けます。詳細については、「[ファブリックへのデバイスの追加 \(336 ページ\)](#)」を参照してください。
- ステップ 20** Cisco Catalyst 9000 シリーズ スイッチをコントロールプレーン、ボーダーノード、およびエッジノードか、またはコントロールプレーンとボーダーノードとして追加します。
デバイスをクリックし、[Add as CP+Border+Edge] または [Add as CP+Border] を選択します。
詳細については、「[ボーダーノードとしてのデバイスの追加 \(338 ページ\)](#)」を参照してください。
- ステップ 21** エッジノードをクリックして、[Add to Fabric] を選択します。
- ステップ 22** [保存 (Save)] をクリックします。
- ステップ 23** ワイヤレス機能を有効にする前に Cisco Catalyst 9000 シリーズ スイッチにワイヤレスパッケージをインストールしなかった場合は、Cisco DNA Center に「9800-SW イメージは機能を有効にするために必要です。[OK] をクリックして、9800-SW イメージを手動でインポートしてください。(9800-SW image is necessary for turning on the capability. Click "OK" to import the 9800-SW image manually)」という警告メッセージが表示されます。

- ステップ 24** [OK] をクリックして、イメージを手動でインストールします。
- ステップ 25** [Download Image] ウィンドウで、[Choose File] をクリックしてローカルに保存されているソフトウェアイメージへ移動するか、または [Enter image URL] でソフトウェアイメージのインポート元となる HTTP または FTP を指定します。
- ステップ 26** [Import] をクリックします。
インポートの進捗状況が表示されます。
- ステップ 27** [Activate image on device] をクリックします。
「デバイスでイメージが有効化されると、デバイスがリブートします。デバイスをリブートしてもよろしいですか。(Activate image on device will reboot the device. Are you sure you want to reboot the device?) 」という警告メッセージが表示されます。
- ステップ 28** [Yes] をクリックします。
デバイスパッケージのアップグレードが完了すると、デバイスがリブートし、オンラインになります。
- ステップ 29** 表示されるダイアログボックスに、コントローラで管理されている AP の場所が表示されます。ここからサイトの変更、削除、または再割り当てができます。
- ステップ 30** [次へ (Next)] をクリックします。
- ステップ 31** [Summary] ウィンドウで詳細を確認し、[Save] をクリックします。
- ステップ 32** [Modify Fabric Domain] ウィンドウで、[Now] をクリックして変更を確定し、[Apply] をクリックして設定を適用します。
次の手順では、ファブリックドメインで AP をオンボードします。
- ステップ 33** Cisco DNA Center ホームページで、[プロビジョニング (Provision)] をクリックします。
- ステップ 34** [ファブリック (Fabric)] タブをクリックします。
ファブリックドメインのリストが表示されます。
- ステップ 35** 作成したファブリックドメインを選択し、[Host Onboarding] タブをクリックして、AP の IP プールを有効にします。
- ステップ 36** ファブリックドメイン内のデバイスに適用される認証テンプレートを選択します。これらのテンプレートは、Cisco ISE から取得される事前定義済みの設定です。認証テンプレートを選択したら、[保存 (Save)] をクリックします。
- ステップ 37** [Virtual Networks] の下で、[INFRA_VN] をクリックして、選択した仮想ネットワークに 1 つ以上の IP プールを関連付けます。
- ステップ 38** [Virtual Network] の下で、ゲスト仮想ネットワークをクリックして、選択したゲスト仮想ネットワークの IP プールを関連付けます。
- ステップ 39** 設計フェーズ中に AP 用に作成された [IP Pool Name] チェックボックスをオンにします。
- ステップ 40** [Update] をクリックして設定を保存します。
AP は、指定したプールから IP アドレスを取得します。このプールは、AP VLAN に関連付けられていて、いずれかの検出方法を通じてシスコ ワイヤレス コントローラに登録されます。

- ステップ 41** ホストがアクセスできるネットワーク内のワイヤレス SSID を指定します。[Wireless SSID] セクションで、ゲスト SSID または企業 SSID を選択してアドレスプールを割り当ててから、[Save] をクリックします。
- ステップ 42** [Inventory]>[Resync] を実行して手動で再同期をトリガーし、組み込みのワイヤレス用の Cisco DNA Center で AP を確認します。
検出された AP が [Provision] ページの [Inventory] に表示され、[Status] は [Not Provisioned] として表示されます。
- ステップ 43** AP をプロビジョニングします。
詳細については、「[シスコ製 AP のプロビジョニング : Day 1 AP プロビジョニング \(284 ページ\)](#)」を参照してください。
- ステップ 44** アプリケーションポリシーを設定および展開します。詳細については、[アプリケーションポリシーを作成します。\(225 ページ\)](#)、[アプリケーションポリシーの展開 \(232 ページ\)](#)、および [アプリケーションポリシーの編集 \(230 ページ\)](#) を参照してください。
アプリケーションポリシーを展開する前に、Catalyst 9300 シリーズ スイッチおよび Cisco Catalyst 9500H シリーズ スイッチをプロビジョニングします。
2つの異なる SSID で異なるビジネスとの関連性を持つ2つの異なるポリシーは機能しません。関連性を設定するときは、最後に展開したポリシーが常に優先されます。
アプリケーションのデフォルトのビジネスとの関連性を変更しても、FlexConnect モードでは動作しません。
非ファブリック SSID にのみアプリケーションポリシーを適用できます。

Cisco Catalyst 9000 シリーズスイッチに Catalyst 9800 組み込みワイヤレスを搭載したファブリックインアボックス

ファブリックインアボックスに関する情報

Cisco Catalyst 9000 シリーズ スイッチには、Cisco DNA Center を使用して設定できる、単一のスイッチでファブリックエッジ、コントロールプレーン、ボーダー、および組み込みのワイヤレス機能をホストする機能があります。

この機能を使用すると、小規模サイトの場所での設定が簡素化され、Cisco SD-Access の導入コストが削減されます。

Cisco Catalyst 9000 シリーズ スイッチに CP+ボーダー+エッジノードを追加する方法については、[Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのプロビジョニング \(311 ページ\)](#) を参照してください。

拡張性に関する情報

次の表に、デバイスの拡張性に関する情報を示します。

ファブリックの構造	Cisco Catalyst 9300 シリーズ スイッチ	Cisco Catalyst 9400 シリーズ スイッチ	Cisco Catalyst 9500 シリーズ スイッチ	Cisco Catalyst 9500-H シリーズ スイッチ
仮想ネットワーク	256	256	256	256
ローカルエンドポイント/ホスト	4 K	4 K	4 K	4 K
SGT/DGT テーブル	8 K	8 K	8 K	8 K
SGACL (セキュリティ ACE)	5K	18K	18K	18K

リリース間コントローラモビリティの概要

リリース間コントローラモビリティ (IRCM) は、異なるソフトウェアバージョンのさまざまなシスコ ワイヤレス コントローラで実行されるシームレスなモビリティとワイヤレスサービスをサポートします。

Cisco DNA Center Cisco DNA Center は、次のデバイスの組み合わせでゲストアンカー機能をサポートしています。

- アンカーコントローラとしての Cisco AireOS コントローラとフォーリンコントローラとしての Cisco AireOS コントローラの設定。
- フォーリンコントローラとしての Cisco Catalyst 9800 シリーズ ワイヤレス コントローラとゲストアンカーコントローラとしての Cisco AireOS コントローラの設定。
- アンカーコントローラとしての Cisco Catalyst 9800 シリーズ ワイヤレス コントローラとフォーリンコントローラとしての Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの設定。

このリリースのコントローラデバイスで IRCM を設定する際の制限事項を次に示します。

- フォーリンコントローラとしての Cisco AireOS コントローラの設定、およびアンカーコントローラとしての Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの設定はサポートされていません。
- ファブリックゲストアンカーの設定はサポートされていません。
- 複数のアンカーコントローラの設定、および 1 つのフォーリン コントローラ シナリオの設定はサポートされていません。
- ゲスト SSID のみがサポートされています。

- ゲストアンカーノードでの非ゲストアンカー SSID のブロードキャストはサポートされていません。
- モビリティトンネルは暗号化されません。

ゲストアンカーの設定とプロビジョニング



(注) リリース間コントローラモビリティ (IRCM) の使用中は、Cisco AireOS コントローラをフォーリンコントローラとして、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラをゲストアンカーコントローラとして設定することはできません。

ゲストアンカー シスコ ワイヤレス コントローラ を設定するには、次の手順に従います。

- ステップ 1** サイト、ビルディング、フロアなどのネットワーク階層を設計します。詳細については、[ネットワーク階層のサイトの作成 \(95 ページ\)](#)、[ビルディングの追加 \(99 ページ\)](#)、および[ビルディングへのフロアの追加 \(101 ページ\)](#) を参照してください。
- ステップ 2** AAA、DHCP、DNS サーバなどのネットワーク サーバを設定します。詳細については、[グローバルネットワークサーバの設定 \(162 ページ\)](#) および[Cisco ISE またはその他の AAA サーバの追加 \(163 ページ\)](#) を参照してください。
- ステップ 3** Cisco Identity Services Engine を設定し、外部 Web 認証と中央 Web 認証を使用してゲスト ワイヤレス ネットワークの SSID を作成します。詳細については、「[ゲスト ワイヤレス ネットワークの SSID の作成 \(127 ページ\)](#)」を参照してください。
- ステップ 4** Cisco Discovery Protocol (CDP) または IP アドレス範囲を使用してワイヤレス コントローラ を検出します。デバイスは [Inventory] ウィンドウに示され、[Managed] 状態になっています。詳細については、「[ディスカバリについて \(13 ページ\)](#)」を参照してください。
- ステップ 5** アクティブなメインワイヤレス コントローラ として外部ワイヤレス コントローラ をプロビジョニングします。[Cisco Wireless Controller をプロビジョニングする \(276 ページ\)](#) を参照してください。
- ステップ 6** ゲストアンカーとしてワイヤレス コントローラ のロールを選択し、ゲストアンカーコントローラをプロビジョニングします。詳細については、「[Cisco Wireless Controller をプロビジョニングする \(276 ページ\)](#)」を参照してください。
- ステップ 7** CLI、SNMP、HTTP、HTTPS などのデバイスクレデンシャルを設定します。詳細については、[グローバル CLI クレデンシャルの設定 \(150 ページ\)](#)、[グローバル SNMPv2c クレデンシャルの設定 \(151 ページ\)](#)、[グローバル SNMPv3 クレデンシャルの設定 \(152 ページ\)](#)、および[グローバル HTTPS クレデンシャルの設定 \(154 ページ\)](#) を参照してください。

IRCM : Cisco AireOS コントローラと Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ

始める前に

- Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ および Cisco AireOS コントローラを検出します。

Catalyst 9800 シリーズ ワイヤレス コントローラを検出するには、NETCONF を有効にしてポートを 830 に設定する必要があります。NETCONF は、ネットワークデバイスの設定をインストール、操作、削除するためのメカニズムです。

詳細については、[CDP を使用したネットワークの検出 \(19 ページ\)](#) または [Discover Your Network Using an IP Address Range \(25 ページ\)](#) を参照してください。

- サイト、ビルディング、フロアを追加してネットワーク階層を設計すると、後で設計の設定や構成を適用する場所を簡単に特定できるようになります。

新しいネットワーク階層を作成するには、[ネットワーク階層のサイトの作成 \(95 ページ\)](#)、[ビルディングの追加 \(99 ページ\)](#)、および [ビルディングへのフロアの追加 \(101 ページ\)](#) を参照してください。

- AP の位置情報を追加し、フロアマップに配置して、ヒートマップカバレッジを可視化します。

詳細については、「[AP の追加、配置、および削除 \(104 ページ\)](#)」を参照してください。

- AAA (Cisco ISE がネットワークとクライアントエンドポイント向けに設定されている)、NetFlow コレクタ、NTP、DHCP、DNS、syslog、SNMP トラップなどのネットワーク設定を定義します。これらのネットワークサーバが、ネットワーク全体のデフォルトになります。AAA サーバを追加するときに、TACACS サーバを追加できます。

詳細については、[グローバルネットワーク設定について \(146 ページ\)](#)、[グローバルネットワークサーバの設定 \(162 ページ\)](#)、および「[Cisco ISE またはその他の AAA サーバの追加](#)」を参照してください。

- ゲスト ワイヤレス ネットワークの SSID を作成します。

詳細については、「[ゲスト ワイヤレス ネットワークの SSID の作成 \(127 ページ\)](#)」を参照してください。

- フォーリンコントローラとアンカーコントローラの WLAN プロファイル名は、モビリティに対して同じにする必要があります。

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

[Devices] > [Inventory] ウィンドウに、検出されたデバイスのリストが表示されます。

ステップ 2 フォーリンコントローラとしてプロビジョニングする Catalyst 9800 シリーズ ワイヤレス コントローラの横にあるチェックボックスをオンにします。

- ステップ 3** [Actions] ドロップダウンリストから、**[Provision] > [Provision]** を選択します。
- ステップ 4** [Assign Site] ウィンドウで、**[Choose a Site]** をクリックして Catalyst 9800 シリーズ ワイヤレス コントローラ デバイスにサイトを割り当てます。
- ステップ 5** [Add Sites] ウィンドウで、サイト名の横にあるチェックボックスをオンにして Catalyst 9800 シリーズ ワイヤレス コントローラ を関連付けます。
- ステップ 6** **[Save (保存)]** をクリックします。
- ステップ 7** **[Apply]** をクリックします。
- ステップ 8** **[次へ (Next)]** をクリックします。
- ステップ 9** Catalyst 9800 シリーズ ワイヤレス コントローラ のロールを **[Active Main WLC]** として選択します。
- ステップ 10** アクティブなメイン ワイヤレス コントローラ では、インターフェイスと VLAN の詳細を設定する必要があります。
- ステップ 11** [Assign Interface] エリアで、次の操作を実行します。
- **[VLAN ID]** : VLAN ID の値を入力します。
 - **[IP Address]** : インターフェイス IP アドレスを入力します。
 - **[Gateway IP Address]** : ゲートウェイ IP アドレスを入力します。
 - **[Subnet Mask (in bits)]** : インターフェイスのネットマスクの詳細を入力します。
- (注) Catalyst 9800 シリーズ ワイヤレス コントローラ では、IP アドレス、ゲートウェイ IP アドレス、およびサブネットマスクを割り当てる必要はありません。
- ステップ 12** **[次へ (Next)]** をクリックします。
- ステップ 13** [Summary] ウィンドウで、設定の詳細を確認します。
- ステップ 14** **[Deploy]** をクリックし、Catalyst 9800 シリーズ ワイヤレス コントローラ をフォーリンコントローラとしてプロビジョニングします。
- ステップ 15** **[Devices] > [Inventory]** ウィンドウで、ゲストアンカーコントローラとしてプロビジョニングする Cisco AireOS コントローラの横にあるチェックボックスをオンにします。
- ステップ 16** 手順 3 ~ 8 を繰り返します。
- ステップ 17** Cisco AireOS コントローラのロールを **[Guest Anchor]** として選択します。
- ステップ 18** ゲストアンカー ワイヤレス コントローラ の場合は、インターフェイスと VLAN の詳細を設定する必要があります。
- ステップ 19** 手順 11 ~ 14 を繰り返します。

LAN アンダーレイのプロビジョニング

LAN 自動化を使用して、LAN アンダーレイをプロビジョニングします。

始める前に

- ネットワーク階層を設定します。(デバイスサイトを追加する (273 ページ) を参照)。
- 以下のグローバル ネットワーク設定が定義済みであることを確認します。
 - AAA、DHCP、DNS サーバなどのネットワーク サーバ。(グローバル ネットワーク サーバの設定 (162 ページ) を参照)。
 - CLI、SNMP、HTTP、HTTPS などのデバイスのクレデンシャル。(グローバル CLI クレデンシャルの設定 (150 ページ)、グローバル SNMPv2c クレデンシャルの設定 (151 ページ)、グローバル SNMPv3 クレデンシャルの設定 (152 ページ)、グローバル HTTPS クレデンシャルの設定 (154 ページ) を参照。)
 - IP アドレス プール。(IP アドレス プールを設定する (158 ページ) を参照)。
- インベントリに少なくとも1つのデバイスがあることを確認してください。デバイスがない場合は、ディスカバリ機能を使用して検出します。



(注) 検出されたサイトがユーザ名「cisco」の CLI ログイン情報を使用して設定されている場合、LAN 自動化はブロックされます。

- ネットワークに Cisco Catalyst 9400 スイッチが設定されている場合は、LAN 自動化で 40G ポートが自動的に有効になるように設定されたスイッチで次の操作が実行されていることを確認します。
 - Day-0 設定はスイッチで実行されます。
 - 40G Quad Small Form-Factor Pluggable (QSFP) トランシーバはスーパーバイザのポート 9 またはポート 10 のいずれかに挿入されます。スーパーバイザ上の 1～8 のポートには、10G または 1G Small Form-Factor Pluggable (SFP) トランシーバは挿入されません。デュアルスーパーバイザエンジンがある場合は、40G QSFP がポート 9 に挿入されていることを確認します。
- Catalyst 9400 シリーズ スーパーバイザの詳細については、Cisco Catalyst 9400 シリーズ スーパーバイザの設置時の注意事項 [英語] を参照してください。

ステップ1 プロビジョニングするサイト用に IP アドレス プールを予約します。

(注) LAN 自動化 IP アドレス プールのサイズは、最小 25 ビット以上のサイズのネットマスクでなければなりません。

- Cisco DNA Center のホームページで、[設計 (Design)] > [ネットワーク設定 (Network Settings)] > [IP アドレス プール (IP Address Pools)] の順に選択します。
- [ネットワーク階層 (Network Hierarchy)] ペインで、サイトを選択します。

- c) [IP プールの予約 (Reserve IP Pool)] をクリックして以下のフィールドに入力し、使用可能なグローバル IP アドレス プールのすべてまたは一部を特定のサイト用に予約します。
- [IP プール名 (IP Pool Name)] : 予約済み IP アドレスのプールの一意の名前。
 - [タイプ (Type)] : IP アドレス プールのタイプ。LAN 自動化のバイアは、**LAN** を選択します。
 - [Global IP Pool] : IP アドレスのすべてまたは一部を予約する IPv4 アドレスプール。
(注) LAN 自動化では、IPv4 サブネットのみが使用されます。
 - [CIDR Prefix/No. of IP Addresses] : グローバル IP アドレスプールのすべてまたは一部を予約するための IP サブネットとマスクアドレス、または予約する IP アドレス数。
 - ゲートウェイ IP アドレス (Gateway IP Address) : ゲートウェイ IP アドレス。
 - **DHCP Servers**: DHCP サーバの IP アドレス。
- d) [予約 (Reserve)] をクリックします。

ステップ 2 デバイスを検出してプロビジョニングします。

- a) Cisco DNA Center のホームページから、[**プロビジョニング (Provision)**] > [**デバイス (Devices)**] > [**インベントリ (Inventory)**] を選択します。
すべての検出されたデバイスが表示されます。
- b) [LAN 自動化 (LAN Automation)] ドロップダウン リストから、[LAN 自動化 (LAN Automation)] を選択します。
- c) スライドして表示される [LAN 自動化 (LAN Automation)] ダイアログ ボックスで、以下のフィールドに入力します。
- [Primary Site] : このサイトからプライマリデバイスを選択します。
 - [Peer Site] : このサイトがピアデバイスの選択に使用されます。このサイトは、プライマリサイトとは異なる場合がありますので注意してください。
 - [Primary Device] : Cisco DNA Center が新しいデバイスを検出しプロビジョニングする起点として使用するプライマリデバイスを選択します。
 - [Peer Device] : ピアデバイスを選択します。
 - プライマリ検出ポート (Primary Discover Ports) : 新規デバイスの検出とプロビジョニングに使用するポート。
 - [Discovered Device Site] : 新たに検出されたすべてのデバイスがこのサイトに割り当てられます。このサイトは、プライマリサイトおよびピアサイトとは異なる場合があります。
 - IP プール (LAN Pool) : LAN 自動化用に予約された IP アドレスプール。(ステップ 1 を参照)。
 - [ISIS ドメイン パスポート (ISIS Domain Password)] : LAN 自動化が開始するときにユーザが指定する IS-IS パスワード。パスワードがすでにシードデバイスに存在する場合は、再使用され、上書きされることはありません。ユーザが指定するパスワードが入力され、既存の IS-IS パスワード

がデバイスにない場合、ドメインパスワードがしつ用されます。プライマリとセコンダリ シードの両方がドメインパスワードをもつ場合、それらが一致することを確認してください。

- [マルチキャストの有効化 (Enable Multicast)] : LAN 自動化は RP としてシードデバイスから、サブスクリバとして検出されたデバイスからマルチキャストツリーを作成します。
- [Device Name Prefix] : プロビジョニングしているデバイスの名前プレフィックス。Cisco DNA Center で各デバイスをプロビジョニングするときに、ここで指定したテキストでデバイスにプレフィックスを付与し、末尾に一意の番号を追加します。たとえば、名前プレフィックスとして **Access** を入力した場合、各デバイスがプロビジョニングされると、Access-1、Access-2、Access-3 のように名前が付けられます。
- [Hostname Map File] : シリアル番号とホスト名のマッピングを含む CSV ファイルを使用して、検出されたデバイスのユーザ指定の名前を設定します。検出されたデバイスがスタックの場合、スタックのすべてのシリアル番号が CSV ファイルで指定されます。

CSV ファイルの例を次に示します。

```
standalone-switch,FCW2212L0NF
stack-switch,"FCW2212E00Y,FCW2212L0GV"
```

- d) [開始 (Start)] をクリックします。

Cisco DNA Center は、新規デバイスの検出とプロビジョニングを開始します。

LAN 自動化では、VLAN 1 のシードデバイスで IP アドレスを設定します。シードデバイスのこの VLAN 1 IP アドレスが Cisco DNA Center から到達できない場合は、[LAN Automation Status] ウィンドウにエラーメッセージが表示されます。エラーの詳細および可能な修復アクションを表示するには、このウィンドウの [See Details] リンクにマウスカーソルを合わせます。

ステップ 3 プロビジョニングしているデバイスの進行状況をモニタして確認します。

- a) [プロビジョニング (Provisioning)] > [デバイス (Device)] > [インベントリ (Inventory)] タブから、[LAN 自動化 (LAN Automation)] > [LAN 自動化ステータス (LAN Status)] をクリックします。

[LAN 自動化のステータス (LAN Automation Status)] ダイアログボックスに、プロビジョニングしているデバイスの進捗状況が表示されます。

(注) 新規デバイスをプロビジョニングするプロセスは、数分かかる場合があります。

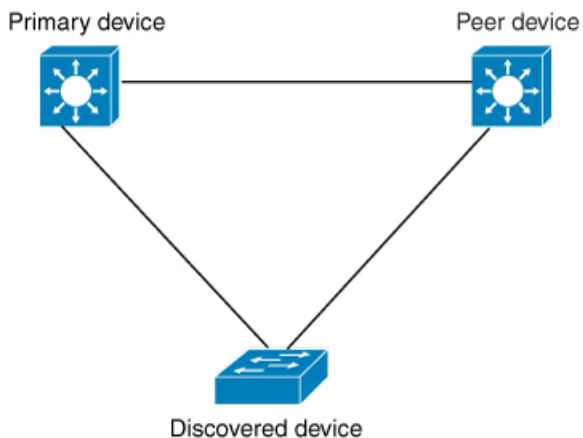
- b) すべてのデバイスが検出され、管理状態にある場合、[LAN 自動化ステータス (LAN Automation Status)] ダイアログボックスの [LAN 自動化ステータス (LAN Automation Status)] ダイアログボックスをクリックします。

LAN 自動化プロセスが完了し、新規デバイスがインベントリに追加されます。

LAN 自動化のピアデバイスの使用事例

デュアルホームのスイッチのプロビジョニング

デュアルホームのスイッチのプロビジョニングのために、常にピアデバイスを選択する必要があります。

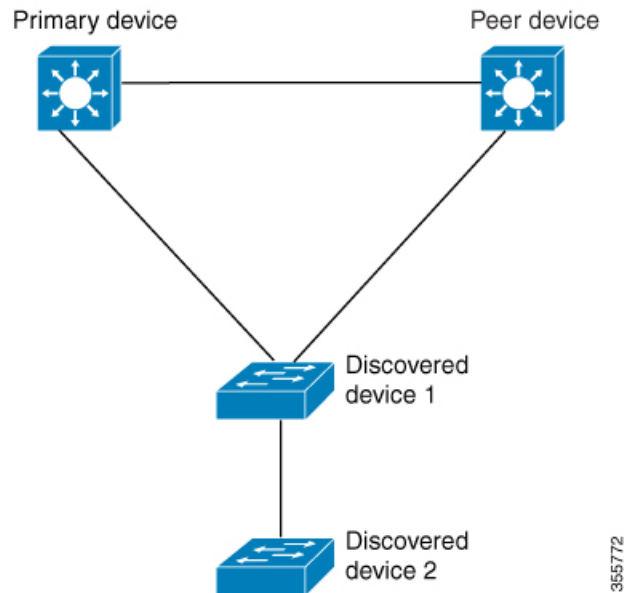


Cisco DNA Center プライマリ デバイスで DHCP サーバを設定します。Cisco DNA Center が検出されたデバイスがプライマリ デバイスとピア デバイスの両方に接続されていることを理解しているため、LAN 自動化タスクが停止されると、2つのレイヤー3 ポイントツーポイント接続を設定します。1つの接続は、検出されたデバイスとプライマリ デバイスの間で確立されます。もう1つの接続は検出されたデバイスとピア デバイスの間で確立されます。



- (注) LAN 自動化ジョブが実行される前に、プライマリ デバイスとピア デバイスの間のリンクが設定される場合、ピア デバイスを Cisco DNA Center のLAN 自動化設定の一部としてピア デバイスに接続するプライマリ デバイスのインターフェイスを選択する必要があります。

LAN 自動化の 2 段階制限



前述のトポロジの場合、Cisco DNA Center は次のリンクを設定します。

- ポイントツーポイントのレイヤ 3 は 検出されたデバイス 1 から プライマリ デバイス に接続するためにルートする
- ポイントツーポイントのレイヤ 3 は 検出されたデバイス 1 から ピア デバイス に接続するためにルートする
- ポイントツーポイントのレイヤ 3 は 検出されたデバイス 1 から 検出されたデバイス 2 に接続するためにルートする

検出されたデバイス 3 という名前のデバイスが以下の検出されたデバイス 2 に直接接続されるシナリオを考えてください。検出されたデバイス 2 と 検出されたデバイス 3 の間の接続は、LAN 自動化ジョブの一部として設定されません。プライマリ デバイスから 2 段階以上離れているためです。

LAN 自動化の状態を確認

実行中の LAN 自動化ジョブのステータスを確認できます。

始める前に

LAN 自動化ジョブを作成し、開始する必要があります。

ステップ 1 Cisco DNA Center のホームページから、[プロビジョニング (Provision)] > [デバイス (Devices)] を選択します。

- ステップ 2** [Inventory] タブをクリックします。
すべての検出されたデバイスが表示されます。
- ステップ 3** [LAN 自動ステータス (LAN Auto Status)] をクリックします。
LAN 自動化ジョブ実行中または完了のステータスが表示されます。

プロビジョニング後のデバイスの削除

- 既にファブリック ドメインに追加されているデバイスを削除する場合、ファブリック ドメインからそのデバイスを削除し、次に[プロビジョニング (Provision)] メニューから削除します。
- [インベントリ (Inventory)] ウィンドウからデバイスを削除することはできません。代わりに、[プロビジョニング (Provision)] メニューからプロビジョニングしたデバイスを削除する必要があります。

-
- ステップ 1** Cisco DNA Center のホームページから、[プロビジョニング (Provision)] > [デバイス (Devices)] を選択します。
[デバイス インベントリ (Device Inventory)] ウィンドウが表示されます。
- ステップ 2** 検出され、プロビジョニングされたすべてのデバイスが表示される [インベントリ (Inventory)] タブをクリックします。
- ステップ 3** 削除するデバイスの横にあるチェックボックスをオンにします。
(注) APは、接続していたコントローラが削除された場合にのみ削除されます。
- ステップ 4** [アクション (Actions)] ドロップダウンリストから、[デバイスの削除 (Delete Device)] を選択します。
- ステップ 5** 確認プロンプトで、[OK (OK)] をクリックします。

ファブリック サイトとファブリック ドメイン

ファブリック サイトは、コントロールプレーン、ボーダー ノード、エッジ ノード、ワイヤレスコントローラ、ISE/PNEのネットワークデバイスの固有のセットをもつ独立したファブリック領域です。異なるレベルの冗長性とスケールは、DHCP、AAA、DNS、インターネットなどのローカル リソースを含むことにより、サイトごとに設計することができます。

ファブリック サイトは、単一の物理的ロケーション、複数のロケーション、またはロケーションのサブセットのみをカバーすることができます。

- 単一の場所: ブランチ、キャンパスまたはメトロ キャンパス

- 複数の場所: メトロ キャンパス + 複数ブランチ
- ロケーションのサブセット: キャンパス内での構築または領域

ファブリックドメインは、1つ以上のファブリックサイトとトランジットサイトで構成できます。複数のファブリックサイトは、トランジットサイトを使用して互いに接続されます。¥ トランジットサイトには2つのタイプがあります。

- SD-Access トランジット: サイト間通信のためのドメイン全体のコントロールプレーンノードでネイティブ SD-Access (LISP、VXLAN、CTS) ファブリックを有効にします。
- IP ベース トランジット: 従来型の IP ベース (VRF-LITE、MPLS) ネットワークを利用します。これは、サイト間で VRF と SGT のマッピングを必要とします。

マルチサイト ファブリック ドメイン

マルチサイトファブリックドメインは、トランジットサイト経由で相互接続されたファブリックサイトの集合体です。ファブリックサイトは、コントロールプレーンノード、ボーダーノード、およびエッジノードの独自のセットを持つファブリックの一部です。指定されたファブリックサイトもまた、ファブリック WLC と AP、および関連するサイト指定の ISE PSN も含みます。単一のファブリックドメインに含まれる複数のファブリックサイトは、トランジットサイトを使用して相互接続されます。

Software-Defined Access (SDA) ファブリックは、複数のサイトで構成されることがあります。各サイトは、優れた拡張性、復元力、生存性、およびモビリティを備えます。サイトの全体的な集約（すなわち、ファブリックドメイン）には、非常に多くのエンドポイントに対応できることや、各サイト内に含まれるサイトを集約することによってモジュール方式で（または水平方向に）拡張できることも要求されます。

トランジット サイト

トランジットサイトとは、2つ以上のファブリックサイトを相互に接続したり、ファブリックサイトと外部ネットワーク（インターネット、データセンターなど）を接続するサイトです。トランジットネットワークには2つのタイプがあります。

- IP トランジット: 通常の IP ネットワークを使用して、外部ネットワークに接続するか2つ以上のファブリックサイトを接続します。
- SDA トランジット: LISP/VxLAN のカプセル化を使用して2つのファブリックサイトを接続します。SDA トランジットエリアは、独自のコントロールプレーンノードを持つがエッジノードやボーダーノードはないファブリックの一部として定義できます。ただし、外部ボーダーを持つファブリックを使用することもできます。SDA トランジットを使用すると、エンドツーエンドポリシープレーンはSGT グループタグを使用して維持されます。

IP のトランジット ネットワークの作成

新しい IP トランジット ネットワークを追加するには、次の手順に従います。

- ステップ 1 Cisco DNA Center ホームページで、**[プロビジョニング (Provision)]** をクリックします。
- ステップ 2 **[ファブリック (Fabric)]** タブをクリックします。
- ステップ 3 **[ファブリック ドメインまたはトランジットを追加 (Add Fabric Domain or Transit)]** タブをクリックします。
- ステップ 4 ポップアップから、**[トランジットを追加 (Add Transit)]** を選択します。
- ステップ 5 ネットワークのトランジットの名前を入力します。
- ステップ 6 トランジット タイプとして、**IP ベース** を選択します。
ルーティング プロトコルが BGP にデフォルトとして設定されます。
- ステップ 7 トランジットネットワークの自律システム番号 (ASN) を、3 つのオプションボタン (**[ASPLAIN]**、**[ASDOT]**、**[ASDOT+]**) から選択した正しい ASN 形式で入力します。
- ステップ 8 **[保存 (Save)]** をクリックします。

SDA トランジット ネットワークの作成

新しい SDA トランジット ネットワークを追加するには、次の手順に従います。

- ステップ 1 Cisco DNA Center ホームページで、**[プロビジョニング (Provision)]** をクリックします。
- ステップ 2 **[ファブリック (Fabric)]** タブをクリックします。
- ステップ 3 **[ファブリック ドメインまたはトランジットを追加 (Add Fabric Domain or Transit)]** タブをクリックします。
- ステップ 4 ポップアップから、**[トランジットを追加 (Add Transit)]** を選択します。
- ステップ 5 ネットワークのトランジットの名前を入力します。
- ステップ 6 トランジット タイプとして **[SD-Access]** を選択します。
- ステップ 7 このトランジットネットワークのトランジット **コントロール プレーン**のサイトを入力します。少なくとも 1 つのトランジット マップ サーバを選択します。
- ステップ 8 このトランジット ネットワークのトランジット **コントロール プレーン**を入力します。
- ステップ 9 追加するすべてのマップ サーバに対し、手順 7 および 8 を繰り返します。
- ステップ 10 **[保存 (Save)]** をクリックします。

次のタスク

SDA トランジットの作成後、ファブリック サイトに移動し、SDA トランジットを接続するサイトに接続します。**[プロビジョニング (Provision)]** > **[ファブリック (Fabric)]** > **[ファブリック**

クサイト (Fabric Site)]の順に移動します。作成したファブリックサイトを選択します。[ファブリックサイト (Fabric Site)]>[ボーダー (Border)]>[ボーダーの編集 (Edit Border)]>[トランジット (Transit)]の順にクリックします。ドロップダウンリストで SDA トランジットサイトをポイントし、[追加 (Add)]をクリックします。

ファブリックドメインの設定

ファブリックの概要

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

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

はじめる前に

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

ファブリックドメインの作成

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

-
- ステップ 1 Cisco DNA Center ホームページで、[プロビジョニング (Provision)] をクリックします。
 - ステップ 2 [ファブリック (Fabric)] タブをクリックします。
 - ステップ 3 [ファブリックドメインまたはトランジットを追加 (Add Fabric Domain or Transit)] タブをクリックします。
 - ステップ 4 ポップアップから、[トランジットを追加 (Add Transit)] を選択します。
 - ステップ 5 ファブリック名を入力します。
 - ステップ 6 ファブリックサイトの 1 つを選択します。
 - ステップ 7 [追加 (Add)] をクリックします。
-

ファブリックの準備状況とコンプライアンスのチェック

ファブリックの準備状況チェック

ファブリックの準備状況チェックは、デバイスがファブリックに追加される準備が整っていることを確認するために、デバイス上で実行される一連の事前プロビジョニングチェックです。ファブリックの準備状況チェックは、デバイスのプロビジョニング時に自動的に実行されるようになります。インターフェイス VLAN とマルチ VRF の設定チェックは、ファブリックの準備状況チェックの一環としては行われません。

ファブリックの準備状況チェックには、次の項目が含まれます。

- ソフトウェアバージョン：デバイスが適切なソフトウェアイメージを使用して実行されているかどうかを確認します。
- ソフトウェアライセンス：デバイスが適切なソフトウェアライセンスを使用して実行されているかどうかを確認します。
- ハードウェアバージョン：デバイスのハードウェアバージョンがサポートされているかどうかを確認します。
- イメージタイプ：デバイスがサポートされているイメージタイプ（IOSXE、IOS、NXOS、シスココントローラ）を使用して実行されているかどうかを確認します。
- ループバック インターフェイス：デバイス上のループバック インターフェイスの設定を確認します。SDA アプリケーションを使用するには、デバイスにループバック インターフェイスが設定されている必要があります。
- 接続チェック：エッジノードからマップサーバへの接続、エッジノードからボーダーへの接続など、デバイス間で必要な接続を確認します。
- 既存の設定チェック（ブラウフィールドチェック）：SD-Access を介してプッシュされ、後でエラーになる可能性がある設定と競合するデバイス上の設定を確認します。

サポートされているソフトウェアバージョンの詳細については、[Cisco SD-Access ハードウェアおよびソフトウェアの互換性マトリックス \[英語\]](#) を参照してください。

ファブリックの準備状況チェックの実行中にエラーが検出された場合、エラー通知が [topology] エリアに表示されます。問題を修正し、デバイスのプロビジョニングワークフローを続行できます。

ファブリック コンプライアンス チェック

ファブリック コンプライアンスとは、ファブリック プロビジョニング中に設定されたユーザ インテントに従って動作するデバイスの状態です。ファブリック コンプライアンス チェックは、次の条件に基づいてトリガーされます。

- 有線デバイスの場合は 24 時間ごと、ワイヤレス デバイスの場合は 6 時間ごと。
- 有線デバイスで設定が変更された場合。

有線デバイスの設定変更によってSNMPトラップがトリガーされ、次にコンプライアンスチェックがトリガーされます。Cisco DNA Center サーバがSNMPサーバとして設定されていることを確認します。

次のコンプライアンスチェックを実行し、デバイスがファブリックに準拠していることを確認します。

- 仮想ネットワーク：Cisco DNA Center 上の仮想ネットワークのユーザインテントの現在の状態に準拠するように、必要なVRFがデバイスに設定されているかどうかを確認します。
- ファブリックロール：デバイスの設定が、Cisco DNA Center のファブリックロールのユーザインテントに準拠しているか確認します。
- セグメント：セグメントのVLAN設定とSVI設定を確認します。
- ポートの割り当て：VLAN および認証プロファイルのインターフェイス設定を確認します。

ファブリックドメインの設定

デバイスをサイトに追加し、それらのデバイス（ボーダー、コントロールプレーン、またはエッジ）にロールを割り当てることができます。また、IPアドレスプールを設定してホスト間の通信を有効にできます。

ファブリックへのデバイスの追加

ファブリックドメインを作成した後にファブリックサイトを追加してから、このファブリックサイトにデバイスを追加できます。また、デバイスがコントロールプレーンノード、エッジノード、またはボーダーノードとして機能する必要があるかどうかを指定することもできます。



-
- (注) ファブリックドメイン内のデバイスをコントロールプレーンノードまたはボーダーノードとして指定する手順はオプションです。デバイスによってはこれらのロールを実行しない場合があります。ただし、各ファブリックドメインには、少なくとも1つのコントロールプレーンノードデバイスと1つのボーダーノードデバイスが存在する必要があります。有線ファブリックの現在のリリースでは、冗長性を確保するために最大6つのコントロールプレーンノードを追加できます。
-



-
- (注) 現在、シスコワイヤレスコントローラは2つのコントロールプレーンノードとのみ通信しません。
-

始める前に

デバイスをプロビジョニングします。デバイスをプロビジョニングするには、[プロビジョニング (Provision)] タブをクリックし、[デバイス (Devices)] を選択します。ファブリックの準備状況チェックに合格し、プロビジョニングする準備が整ったら、トポロジにデバイスがグレー色で表示されます。

ファブリックの準備状況チェックの実行中にエラーが検出された場合、エラー通知が[**topology**] エリアに表示されます。[**See more details**] をクリックして、結果のウィンドウに一覧表示された問題領域を確認します。問題を修正し、[**Re-check**] をクリックして問題が解決されていることを確認します。問題解決の一環としてデバイスの設定を更新する場合は、デバイスで [**Inventory**] > [**Resync**] を実行して、デバイス情報を再同期してください。



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

ステップ 1 Cisco DNA Center のホームページで、[**Provision**] > [**Fabric**] の順に選択します。すべてのプロビジョニングされたファブリック ドメインがウィンドウに表示されます。

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

ステップ 3 サイトを選択します。

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

ステップ 4 デバイスをクリックします。[**Device Details**] ウィンドウに、次のオプションが表示されます。

オプション	説明
エッジ ノード	選択したデバイスをエッジノードとして有効にするには、このオプションの横にあるトグルボタンをクリックします。
ボーダー ノード	選択したデバイスをボーダーノードとして有効にするには、このオプションの横にあるトグルボタンをクリックします。詳細については、「 ボーダーノードとしてのデバイスの追加 」を参照してください。
コントロール プレーン	選択したデバイスをコントロールプレーンノードとして有効にするには、このオプションの横にあるトグルボタンをクリックします。
ゲスト境界/コントロールプレーン	次のオプションを使用できます。 <ul style="list-style-type: none"> [Control Plane] : デバイスをコントロールプレーンとして使用する場合はこのチェックボックスをオンにします。 [Border] : デバイスをボーダーノードとして使用する場合はこのチェックボックスをオンにします。

オプション	説明
	<ul style="list-style-type: none"> • [Select One Guest Virtual Network] : 作成済みのゲスト仮想ネットワークがすべて一覧表示されます。ゲスト仮想ネットワークのチェックボックスをオンにして、[有効化 (Enable)] をクリックします。 <p>(注) [ポリシー (Policy)] アプリケーションでゲスト仮想ネットワークを作成したことを確認してください。 仮想ネットワークの作成 (246 ページ) を参照してください。</p>
ランデブーポイント	<p>デバイスでランデブーポイントを設定するには、このトグルボタンをクリックします。</p> <p>詳細については、「ランデブーポイントとしてのデバイスの追加」を参照してください。</p>

デバイスをファブリックインボックスとして設定するには、[Control Plane]、[Border Node]、および [Edge Node] オプションを選択します。

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

ステップ 5 [保存 (Save)] をクリックします。

次のタスク

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

ボーダーノードとしてのデバイスの追加

ファブリックにデバイスを追加する場合、[ファブリックへのデバイスの追加 \(336 ページ\)](#) で説明したように、コントロールプレーン、ボーダーノード、またはエッジノードとして動作するようにさまざまな組み合わせで追加できます。

ボーダーノードとしてデバイスを追加するには、次の手順を実行します。

- ステップ 1** Cisco DNA Center のホームページで、[Provision] > [Fabric] をクリックします。プロビジョニングされたすべてのファブリック ドメインのリストが表示されます。
- ステップ 2** ファブリック ドメインのリストから、ファブリックを選択します。すべてのファブリック対応サイトのリストが表示されます。

ステップ3 ファブリックサイトのリストから、サイトを選択します。インベントリされたネットワーク内のすべてのデバイスが結果のトポロジビューに表示されます。トポロジ表示では、ファブリックに追加されるすべてのデバイスは青です。

ステップ4 デバイスをクリックして、[Border Node] を選択します。

ステップ5 スライドインウィンドウが、追加するデバイスの名前と一緒に表示されます。

- a) [Layer 3 Handoff] を展開します。
- b) 次のいずれかのオプションボタンをクリックします。
 - [ASPLAIN] : 自律システム番号 (ASN) を ASPLAIN 形式で受け入れます。
 - [ASDOT] : ASN を ASDOT 形式で受け入れます。
 - [ASDOT+] : ASN を ASDOT+ 形式で受け入れます。
- c) デバイスの [ローカル自律番号 (Local Autonomous Number)] を入力します。
- d) [IPアドレスプールの選択 (Select IP Address Pools)] ドロップダウン リストから、IP アドレス プールを選択します。
- e) ボーダーデバイスで有効になっているトランジットネットワークを選択します。
 - ボーダーで SDA トランジットを有効にするには、[トランジットを選択 (Select Transit)] ドロップダウンリストからユーザが作成した SDA トランジット ドメインを選択します。[Add] をクリックします。
 - ボーダーで IP トランジットを有効にするには、[トランジットを選択 (Select Transit)] ドロップダウンリストからユーザが作成した IP トランジット ドメインを選択します。[Add] をクリックします。

デザイン階層から IP プールを選択します。選択したプールは、ボーダー ノードと IP ピア間で IP ルーティングを自動化するために使用されます。[インターフェイスの追加 (Add Interface)] をクリックして、次の画面でインターフェイスの詳細を入力します。

ドロップダウン リストから [外部インターフェイス (External Interface)] を選択します。[リモートAS番号 (Remote AS Number)] を入力します。リストで [仮想ネットワーク (Virtual Network)] をチェックします。この仮想ネットワークは、ボーダーによってリモートピアにアダプタイズされなければなりません。1つ、複数、またはすべての仮想ネットワークを選択できます。[保存 (Save)] をクリックします。
- f) デフォルトでは、ボーダーノードは内部ボーダーとして指定されています。ボーダーノードを外部、または内部および外部のいずれかにするには、次の手順を実行します。
 - **内部および外部ボーダー** : このボーダーノードを内部および外部ボーダーとして指定するには、[Default To all Virtual Networks] チェックボックスをオンにします。これは、エッジノードから送信されたすべての不明なトラフィックへのゲートウェイとして機能します。 ([Do Not Import External Routes] チェックボックスはオンにしないでください) 。
 - **外部ボーダー** : [Default to all Virtual Networks] および [Do not Import External Routes] チェックボックスの両方をオンにして、ボーダーノードを外部ボーダーとして指定します。

- **内部ボーダー** : [Default to all Virtual Networks] および [Do not Import External Routes] チェックボックスをオンにしないでください。

ステップ 6 (オプション) ファブリックネットワークに非ファブリックネットワークを接続している場合、または従来のネットワークから **Software-Defined Access** ネットワークに移行する場合にのみ、この手順を実行します。[Layer 2 Handoff] をクリックします。仮想ネットワークの 1 つをクリックします。

すべての仮想ネットワークと、各仮想ネットワークのプールの数が表示されます。

仮想ネットワークリストのチェックボックスをクリックできない場合、仮想ネットワークの下にあるセグメントが外部 VLAN にハンドオフされたことを示します。

仮想ネットワークを選択すると、仮想ネットワークに存在する IP アドレス プールのリストが表示されます。非ファブリックデバイスを接続できるインターフェイスのリストが表示されます。

ファブリックを拡張する必要がある [External VLAN] 番号を入力します。仮想ネットワークは、1 つのインターフェイスでのみハンドオフできます。複数のインターフェイス経由で同じ仮想ネットワークをハンドオフすることはできません。

[保存 (Save)] をクリックします。

ステップ 7 [追加 (Add)] をクリックします。

ホストオンボーディングの設定

[ホストのオンボーディング (Host Onboarding)] タブでは、ファブリック ドメインにアクセスできる各種デバイスまたはホストの設定を指定することができます。

このタブでは次の操作を実行できます。

- ファブリックに適用する認証テンプレートを選択します。これらのテンプレートは、Cisco ISE から取得される定義済みの設定です。認証テンプレートを選択したら、[保存 (Save)] をクリックします。
- IP アドレス プールを仮想ネットワーク (デフォルト、ゲスト、またはユーザ定義) に関連付け、[更新 (Update)] をクリックします。表示される IP アドレス プールは、サイト固有のプールのみです。
- ホストがアクセスできるネットワーク内のワイヤレス SSID を指定します。ゲスト SSID またはエンタープライズ SSID を選択してアドレス プールを割り当て、[保存 (Save)] をクリックできます。
- ファブリックドメインに接続している特定のタイプのデバイスについて、各ポート固有の設定を適用します。これを行うには、固有の割り当てが必要なポートを選択し、[Assign] をクリックして、ドロップダウンリストからポートタイプを選択します。

次の制約事項に注意してください。

- Cisco SD-Access 展開環境では、AP、拡張ノード、ユーザデバイス（単一のコンピュータまたは単一のコンピュータと電話機など）、および単一サーバのみがサポートされます。
- 各ポートは最大 10 個の MAC アドレスを学習できます。
- 内部スイッチまたは仮想スイッチを備えたサーバはサポートされていません。
- その他のネットワーキング機器（ハブ、ルータ、スイッチなど）はサポートされていません。

認証テンプレートを選択

ファブリック ドメイン内のすべてのデバイスに適用される認証テンプレートを選択できます。

ステップ 1 [認証テンプレート (Auth Template)] セクションから認証テンプレートを選択します。

- **クローズ認証 (Closed Authentication)** : 認証前のすべてのトラフィック (DHCP、DNS、ARP を含む) は廃棄されます。
- **簡単接続 (Easy Connect)** : スイッチポートに ACL を適用することでセキュリティを追加して、認証前に非常に制限されたネットワーク アクセスを許可します。ホストが正常に認証されると、追加のネットワーク アクセスが許可されます。
- **認証なし**
- **オープン認証 (Open Authentication)** : ホストには、802.1X 認証を受ける必要なくネットワーク アクセスが許可されます。

ステップ 2 [保存 (Save)] をクリックします。

ファブリック ドメインへの仮想ネットワークの関連付け

IP アドレス プールにより、ホストデバイスはファブリック ドメイン内で通信できるようになります。

IP アドレス プールを設定すると、Cisco DNA Center はすぐに各ノードに接続し、ホストが通信できるように適切なスイッチ仮想インターフェイス (SVI) を作成します。

IP アドレス プールを追加することはできませんが、リストされているものからプールを設定できます。ここにリストされている IP アドレスプールは、ネットワークの設計時に作成されたものです。

ステップ 1 [Host Onboarding] タブの [Virtual Networks] セクションで、仮想ネットワーク (VN) をクリックします。

ステップ 2 [Edit Virtual Network] ウィンドウの次のフィールドを確認します。

フィールド	説明
IP Pool Name	IP アドレスプールが表示されます。

フィールド	説明
	IP アドレスプールのリストから、仮想ネットワークの一部にする必要があるものを選択します。
Authentication policy	仮想ネットワークの認証ポリシーが表示されます。
Traffic Type	仮想ネットワーク上で有効になっているトラフィックのタイプが表示されます。 仮想ネットワークを介した音声トラフィックまたはデータトラフィックの送信を選択します。
Group	IP プールが属しているグループが表示されます。
Wireless Pool	Cisco DNA Center Cisco DNA Center リリース 1.3.1.4 では、選択した IP プールをワイヤレスプールとして有効にする機能が導入されています。このトグルボタンを使用すると、ワイヤレスプールを有効化または無効化できます。 有効にすると、ファブリックのワイヤレス SSID を設定するときに、定義済みのワイヤレスプールから選択できます。
Layer-2 Extension	レイヤ2フラッディングが有効になっているか、無効になっているかが表示されます。 IP プールおよびレイヤ2 VNI のレイヤ2 MAC アドレス登録を有効にします。レイヤ2拡張機能はデフォルトで有効になっており、無効にすることはできません。
Layer-2 Flooding	レイヤ2フラッディングが有効になっているか、無効になっているかが表示されます。 レイヤ2フラッディングはデフォルトで無効になっています。

ステップ 3 [Add] をクリックして、選択した仮想ネットワークに 1 つ以上の IP アドレスプールを関連付けます。

結果のウィンドウの必須フィールドに入力します。

- 対応するドロップダウンリストから、[IP] プール、[Traffic] タイプ、および [Groups] を選択します。
- レイヤ2フラッディングを有効にするには、[Layer-2 Flooding] チェックボックスをオンにします。
- [Critical Pool] チェックボックスをオンにして、この IP プールをクリティカル IP アドレスプールに含めます。

ステップ 4 [更新 (Update)] をクリックして設定を保存します。ここで指定した設定は、仮想ネットワーク上のすべてのデバイスに展開されます。

ステップ 5 すべての仮想ネットワークに IP プールを関連付けた後、[Save] をクリックします。

ファブリック ドメインのワイヤレス SSID の設定

- ステップ 1** [Wireless SSID] セクションで、ホストがアクセス可能なネットワーク内のワイヤレス SSID を指定します。
- ステップ 2** [Choose Pool] をクリックし、SSID の IP プール予約を選択します。
- ステップ 3** [Assign SGT] ドロップダウンリストから、SSID のスケラブルグループを選択します。
- ステップ 4** SSID でワイヤレスマルチキャストを有効にするには、[Enable Wireless Multicast] チェックボックスをオンにします。

ファブリック ドメイン内のポートの設定

[ポート割り当ての選択 (Select Port Assignment)] セクションでは、ファブリック ドメイン上の各アクセスデバイスを設定できます。各デバイスでは、各ポートのネットワークの動作設定を指定できます。



- (注) ここで行うポートの設定は、[仮想ネットワーク (Virtual Networks)] セクションで行ったデバイスの一般設定をオーバーライドします。

- ステップ 1** [ファブリック デバイスの選択 (Select Fabric Device)] セクションで、設定するアクセス デバイスを選択します。
デバイスで利用可能なポートが表示されます。
- ステップ 2** デバイス上のポートを選択し、許可された IP アドレスプール、プロビジョニングされているグループ、音声またはデータ プール、およびポートの認証タイプを指定します。
- ステップ 3** [保存 (Save)] をクリックします。

拡張ノードの設定

拡張ノードはレイヤ 2 スイッチモードで動作するデバイスで、ファブリックテクノロジーをネイティブにはサポートしていません。拡張ノードは、自動化されたワークフローによって設定されます。設定後、拡張ノードデバイスがファブリックトポロジビューに表示されます。拡張ノードのポート割り当ては、[Host Onboarding] ウィンドウで実行できます。

実際のパケット転送、認証、およびポリシーの適用は、拡張ノードの上にあるファブリックエッジレイヤで行われます。拡張ノードに入るパケットはすべて残りのファブリック宛てで、ファブリックエッジに転送されて、パケットの処理方法が決まります。ポリシーのセグメンテーションとファブリックの自動化による利点は、拡張スイッチポートでも利用できます。

拡張ノードの設定手順

Cisco Catalyst 9300、Cisco Catalyst 9400、および Cisco Catalyst 9500 シリーズ スイッチは、ファブリックエッジとして設定されたときに拡張ノードをサポートします。

拡張ノードをサポートするエッジノードでサポートされている最小ソフトウェアバージョンは IOS XE 17.1.1s です。



(注) ファブリックエッジノードとして設定されている Cisco Catalyst 9200 シリーズ スイッチは、拡張ノードデバイスをサポートしていません。

以下に、拡張ノードでサポートされている最小ソフトウェアバージョンを示します。

- Cisco Industrial Ethernet 4000、4010、5000 シリーズ スイッチ : 15.2(7)E0s
- Cisco Catalyst IE 3300、3400、3400 Heavy Duty (X-coded) シリーズ スイッチ : IOS XE 17.1.1s
- Cisco Catalyst IE 3400 Heavy Duty (D-coded) シリーズ スイッチ : IOS XE 16.12.1s
- Cisco Digital Building シリーズ スイッチ、Cisco Catalyst 3560-CX スイッチ : 15.2(7)E0s

ステップ 1 拡張ノードのネットワーク範囲を設定します。IP アドレスプールの設定手順については、[IP アドレスプールを設定する \(158 ページ\)](#) を参照してください。この手順では、IP アドレスプールを追加し、サイトレベルで IP プールを予約します。CLI および SNMP ログイン情報が設定されていることを確認します。

ステップ 2 拡張 IP アドレスプールを、[Fabric] > [Host Onboarding] タブの下にある INFRA_VN に割り当てます。プールタイプとして **拡張ノード** を選択します。

Cisco DNA Center は、サポートされているファブリックエッジデバイスで拡張 IP アドレスプールと VLAN を設定します。これにより、拡張ノードのオンボーディングが有効になります。

ステップ 3 拡張 IP アドレスプールとオプション 43 を使用して DHCP サーバを設定します。拡張 IP アドレスプールが Cisco DNA Center から到達可能であることを確認します。

(注) オプション 43 の詳細については、[DHCP コントローラ ディスカバリ \(252 ページ\)](#) を参照してください。

ステップ 4 ファブリックエッジデバイスに拡張ノードデバイスを接続します。拡張ノードデバイスからファブリックエッジへ複数のリンクを設定できます。

ステップ 5 (オプション) ポートチャネルを作成します。

この手順は、ファブリックのグローバル認証モードが [No Authentication] ではない場合にのみ実行します。認証モードは、**Open**、**Easy Connect**、または **Closed** 認証のいずれかになります。

拡張ノードに接続されているファブリックエッジノードでポートチャネルを作成します。ポートチャネルを作成するには、次の手順を実行します。

- a) [Provision] > [Fabric] > [Fabric Infrastructure] タブに移動し、ファブリックエッジノードを選択します。タイトルにデバイス名の付いたウィンドウがスライド表示されます。
- b) [ポートチャネルの作成 (Create Port Channel)] をクリックします。
- c) 結果のウィンドウのすべてのフィールドに入力します。拡張ノードのオンボーディングでは LACP は機能しないことに注意してください。

- [LACP] は選択しないでください。
- すべてのデバイスに対して [PAGP] を選択します。

Cisco IOS XE リリース 17.1.1s 以降、IE 3300 および IE 3400 デバイスは PAGP をサポートしていません。

- Cisco IOS XE 17.1.1s よりも前のバージョンを実行している場合は、IE 3300 および IE 3400 デバイスの [Static mode] を選択します。

- d) [Provision] > [Fabric] > [Host Onboarding] ページに移動します。作成されたポートチャネルを選択します。結果のウィンドウで、[Connected Device] タイプとして [Extended Node] を選択します。

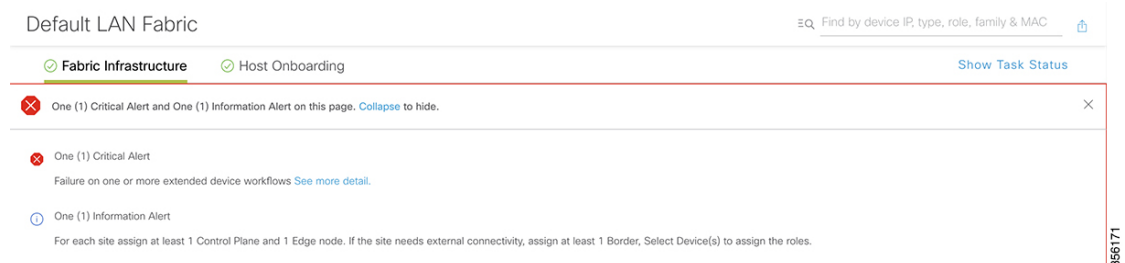
これで、ファブリックエッジノードにポートチャネルが作成されて、拡張デバイスがオンボードされます。

ステップ 6 以前の設定がない場合は、拡張ノードデバイスの電源をオンにします。拡張ノードデバイスに設定がある場合は、以前の設定の書き込み消去を実行して、拡張ノードデバイスをリロードします。

Cisco DNA Center Cisco DNA Center では、拡張ノードデバイスをインベントリに追加し、同じサイトをファブリックエッジとして割り当てます。次に、拡張ノードデバイスがファブリックに追加されます。これで、拡張ノードデバイスがオンボードされ、管理できるようになりました。

設定が完了すると、拡張ノードがファブリックトポロジに、拡張ノードであることを示すタグ (X) とともに表示されます。

拡張ノードの設定中にワークフローでエラーが発生した場合は、[Topology] ウィンドウにバナーでエラー通知が表示されます。



[See more details] をクリックしてエラーを確認します。

[Task Monitor] ウィンドウがスライド表示され、拡張ノード設定タスクのステータスが表示されます。

[See Details] をクリックして、エラーの原因と考えられるソリューションを確認します。

ポートチャネルの設定

単一のエンティティとして機能するようにバンドルされたポートのグループは、ポートチャネルと呼ばれます。ファブリックエッジと、拡張ノードやサーバなどリモート接続されたデバイスとの間のポートチャネルでは、接続の復元力と帯域幅が増加します。

ポートチャネルの作成

認証がクロズド認証の場合にのみ、次の手順を実行します。他の認証モードでは、次の手順が自動化されていることに注意してください。

ステップ 1 [Provision] > [Fabric] > [Fabric Infrastructure] タブに移動し、ファブリックエッジノードを選択します。

タイトルにデバイス名の付いたウィンドウがスライド表示されます。

ステップ 2 [Port Channel] タブを選択し、[Create Port Channel] をクリックします。

ステップ 3 表示されたポートの一覧から、バンドルするポートと適切なプロトコルを選択します。

IE 3300 または IE 3400 拡張ノードの場合は、プロトコルとして [On] を選択します。

他の拡張ノードの場合は、プロトコルとして [PAGP] を選択します。

ステップ 4 [完了 (Done)] をクリックします。

新しいポートチャネルが作成され、ウィンドウに表示されます。

ステップ 5 [Provision] > [Fabric] > [Host Onboarding] ページに移動します。作成されたポートチャネルを選択します。

結果のウィンドウで、ファブリックエッジノードと拡張ノードの間にポートチャネルを作成する場合は、[Connected Device] タイプとして [Extended Node] を選択します。

ファブリックエッジノードとサーバの間にポートチャネルを作成する場合は、[Connected Device] として [Server] を選択します。

ステップ 6 [更新 (Update)] をクリックします。

ポートチャネルの更新

始める前に

ポートチャネルを更新する前に、少なくとも1つのメンバーインターフェイスが存在することを確認します。

ステップ 1 [Provision] > [Fabric] > [Fabric Infrastructure] タブに移動し、ファブリックエッジノードを選択します。

タイトルにデバイス名の付いたウィンドウがスライド表示されます。

ステップ 2 [Port Channel] タブを選択します。

ステップ 3 表示されるポートチャネルのリストから、更新するポートチャネルを選択します。

結果のウィンドウに、選択したポートチャネルのすべてのインターフェイスとステータスが表示されます。

ステップ 4 ポートチャネルでインターフェイスを追加したり、既存のインターフェイスを削除したりできます。ポートチャネルに必要な更新を実行します。

ステップ5 [Done] をクリックします。

ポートチャネルの削除

ステップ1 ホームページから、[Provision] > [Fabric] > [Fabric Infrastructure] トポロジビューに移動します。

ステップ2 ポートチャネルを削除するデバイスをクリックします。

デバイス名の付いたウィンドウがスライド表示されます。

ステップ3 [Port Channel] タブを選択します。

結果の [Port Channel] ビューには、既存のポートチャネルがすべて表示されます。

ステップ4 削除するポートチャネルを選択して、[Delete] をクリックします。

ステップ5 表示された削除の確認メッセージで [Yes] をクリックします。

これにより、ポートチャネルが削除されます。

マルチキャスト概要

マルチキャストトラフィックは、次のような異なる方法で転送されます。

- ランデブーポイントを使用した共有ツリー経由。この場合、PIM SM が使用されます。
- 最短パスツリー (SPT) 経由。PIM Source Specific Multicast (SSM) では SPT だけが使用されます。PIM SM は、受信側が接続しているエッジルータで送信元が認識されると SPT に切り替わります。

『[IP マルチキャストルーティングテクノロジーの概要 \(IP Multicast Technology Overview\)](#)』を参照してください。

マルチキャスト設定の構成

ファブリックドメインにデバイスを追加したら、マルチキャスト IP アドレスプールとランデブーポイント (RP) を作成できます。適用可能なマルチキャスト設定は、そのファブリックドメインで動作しているすべてのファブリックデバイスで自動化されます。

RP は、マルチキャストネットワークドメイン内にあるルータで、マルチキャスト共有ツリーの共有ルートとして動作します。

マルチキャスト IP アドレスプールの作成

始める前に

マルチキャスト IP アドレスプールは、ファブリックドメイン内の内部 PIM 通信に使用されます。必要に応じて、複数のマルチキャストプールを定義し、それぞれを別個の仮想ネットワー

クに関連付けることができます。各仮想ネットワークには、別個のマルチキャスト IP アドレスプールが作成され、関連付けられている必要があります。

ステップ 1 Cisco DNA Center のホームページで、**[設計 (Design)] > [ネットワーク設定 (Network Settings)] > [IP アドレスプール (IP Address Pools)]** の順に選択します。
すべての IP アドレスプールのリストが表示されます。

ステップ 2 **[追加 (Add)]** をクリックして、プールから形成するマルチキャストアドレスを指定します。

- **[IP プール名 (IP Pool name)]** : マルチキャスト IP アドレスプールの名前を入力します。
- **[サブネット/マスク (Subnet/Mask)]** : マルチキャストプールのサブネット IP アドレスとサブネットマスクを入力します。
- **[ゲートウェイ IP アドレス (Gateway IP Address)]** : ゲートウェイの IP アドレスを入力します。

ステップ 3 **[保存 (Save)]** をクリックします。

ステップ 4 複数の仮想ネットワークでマルチキャストを有効化する場合は、仮想ネットワークごとに別個の IP マルチキャストプールを作成します。(手順 2 および 3 を繰り返します。)

ネイティブファブリックマルチキャスト



(注) ネイティブマルチキャストの既存の展開の場合は、アンダーレイマルチキャストコマンドを手動で設定します。LAN 自動化を使用してマルチキャストを有効にすると、デバイスの検出中にマルチキャストコマンドが設定されます。

ファブリックサイトでネイティブファブリックマルチキャストを有効または無効にするには、次のようにします。

ステップ 1 Cisco DNA Center ホームページで、**[プロビジョニング (Provision)]** をクリックします。すべてのプロビジョニングされたファブリックドメインが画面に表示されます。

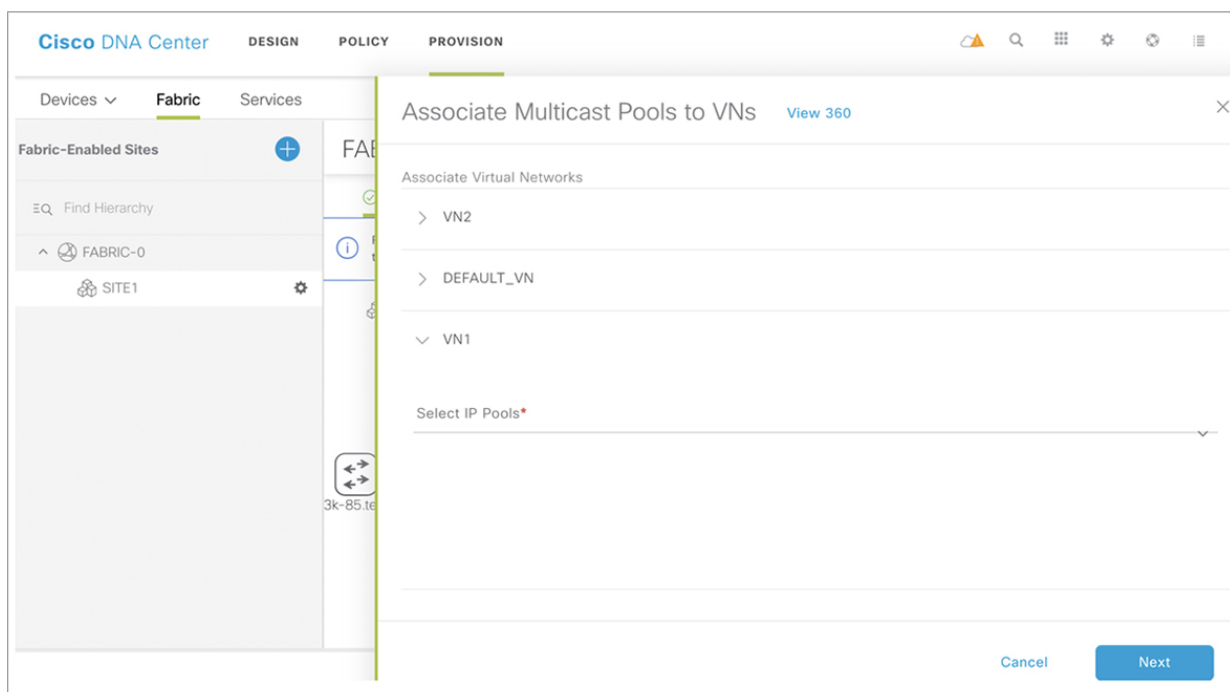
ステップ 2 ファブリックドメインのリストから、ファブリックを選択します。インベントリされたネットワーク内のすべてのデバイスが画面に表示されます。トポロジ表示またはリスト表示でデバイスを表示することができます。トポロジ表示では、ファブリックに追加されるすべてのデバイスは青です。

ステップ 3 デフォルトでは、ネイティブマルチキャストはサイトに対して無効になっています。サイトのネイティブマルチキャストを有効にするには、リストされているファブリックの横にある歯車ボックスをクリックし、**[IPv4 のネイティブマルチキャストを有効にする (Enable Native multicast For IPv4)]** を選択します。ファブリックを保存します。

ステップ 4 ファブリックサイトのネイティブマルチキャストを無効にするには、リストされているファブリックの横にある歯車ボックスをクリックし、**[IPv4 のネイティブマルチキャストを無効にする (Disable Native multicast For IPv4)]** を選択します。ファブリックを保存します。

ランデブーポイントとしてのデバイスの追加

- ステップ 1** Cisco DNA Center のホームページで、[Provision] > [Fabric] をクリックします。
プロビジョニングされたすべてのファブリック ドメインのリストが表示されます。
- ステップ 2** ファブリック ドメインのリストから、ファブリックを選択します。
すべてのファブリック対応サイトのリストが表示されます。
- ステップ 3** ファブリックサイトのリストから、サイトを選択します。インベントリされたネットワーク内のすべてのデバイスが結果のトポロジビューに表示されます。トポロジ表示では、ファブリックに追加されるすべてのデバイスは青です。
- ステップ 4** ランデブーポイントとして追加するファブリックデバイスをクリックします。
スライドインウィンドウに、仮想ネットワークのリストが表示されます。
- ステップ 5** [Rendezvous Point] オプションの横にあるトグルボタンをクリックします。
- ステップ 6** Cisco DNA Center は、仮想ネットワークのリストをポップアップ ウィンドウに表示します。[仮想ネットワーク (Virtual Networks)] を展開し、[プラス (Plus)] ボタンをクリックして、[IP マルチキャストプール (IP multicast pool)] を選択します。[次へ (Next)] をクリックします。



(注) マルチキャストでは各仮想ネットワークに対して単一IPアドレスプールのみが現在サポートされています。

複数の仮想ネットワークでマルチキャストを有効にするには、複数のマルチキャストIPアドレスプールを作成する必要があります。

- ステップ 7** 対応する仮想ネットワークを関連付け、[有効化 (Enable)] をクリックします。

ステップ 8 メイン画面で [保存 (Save)] をクリックします。変更を [適用 (Apply)] します。

ランデブーポイントの確認

ステップ 1 Cisco DNA Center ホームページで、[プロビジョニング (Provision)] をクリックします。
デフォルトでは、[デバイス (Devices)] ウィンドウが表示されます。

ステップ 2 [ファブリック (Fabric)] タブをクリックします。
ファブリックドメインのリストが表示されます。

ステップ 3 ファブリックを選択します。ネットワークに設定されているすべてのデバイスを表示する [ファブリック デバイス (Fabric - Devices)] ウィンドウが表示されます。
IP マルチキャストが有効になっている仮想ネットワークは、**M** でマークされます。

冗長ランデブーポイントとしてのデバイスの追加



(注) デュアル RP は、外部または内部のボーダー ノードでのみサポートされます。

冗長 RP がネットワークに追加されると、MSDP セッションが有効化されます。RP をホストする各ファブリック デバイスは、VRF ごとに 2 つのループバック (RP 用のループバックと MSDP セッションを確立するためのループバック) を作成します。

ステップ 1 Cisco DNA Center のホームページで、[Provision] > [Fabric] をクリックします。
プロビジョニングされたすべてのファブリック ドメインのリストが表示されます。

ステップ 2 ファブリック ドメインのリストから、ファブリックを選択します。
すべてのファブリック対応サイトのリストが表示されます。

ステップ 3 ファブリックサイトのリストから、サイトを選択します。インベントリされたネットワーク内のすべてのデバイスが結果のトポロジビューに表示されます。トポロジ表示では、ファブリックに追加されるすべてのデバイスは青です。

ステップ 4 冗長 RP として追加するファブリック デバイスをクリックします。
スライドインウィンドウに、仮想ネットワークのリストが表示されます。

ステップ 5 冗長 RP を追加する仮想ネットワークを展開します。マルチキャスト IP アドレスプールが事前に設定されている必要があります。[次へ (Next)] をクリックします。

ステップ 6 仮想ネットワークを関連付け、[有効化 (Enable)] をクリックします。

ステップ 7 メイン画面で [保存 (Save)] をクリックします。変更を [適用 (Apply)] します。

Applications

アプリケーションおよびアプリケーションセット

アプリケーションは、ネットワーク内で使用されているソフトウェアプログラムまたはネットワーク シグナリング プロトコルです。Cisco DNA Center は、約 1400 の異なるアプリケーションから成る Cisco Next Generation Network-Based Application Recognition (NBAR2) ライブラリの全アプリケーションをサポートしています。

アプリケーションは、アプリケーションセットと呼ばれる論理グループに分類されています。アプリケーションセットには、ポリシー内でのビジネスとの関連性を割り当てることができます。

アプリケーションは、同様のトラフィック処理要件が規定されている RFC 4594 の定義に従い、業界標準ベースのトラフィック クラスにもマッピングされています。トラフィッククラスでは、割り当てられているビジネスとの関連性グループに基づいて、アプリケーショントラフィックに適用される処理 (Differentiated Services Code Point (DSCP) マーキング、キューイング、破棄など) を定義します。

Cisco DNA Center に含まれていない追加のアプリケーションがある場合は、カスタム アプリケーションとして追加して、アプリケーションセットに割り当てることができます。詳細については、[カスタムアプリケーション \(352 ページ\)](#) を参照してください。必要なすべてのアプリケーションを含むカスタム アプリケーションセットを作成することもできます。

NBAR2 の詳細については、<https://www.cisco.com/c/en/us/products/ios-nx-os-software/network-based-application-recognition-nbar/index.html> を参照してください。

単方向と双方向のアプリケーショントラフィック

一部のアプリケーションは、完全な左右対称であり、接続の両端に同一の帯域幅プロビジョニングを必要とします。このようなアプリケーションのトラフィックを、双方向のトラフィックと呼びます。たとえば、100 kbps の低遅延キューイング (LLQ) が一方の音声トラフィックに割り当てられている場合、逆方向の音声トラフィックにも 100 kbps の LLQ をプロビジョニングする必要があります。このシナリオは、同じ Voice over IP (VoIP) コーダ/デコーダ (コーデック) が両方の方向で使用されており、マルチキャスト保留音 (MOH) のプロビジョニングが考慮されていないことが前提となっています。しかし、Streaming-Video やマルチキャスト MoH などの特定のアプリケーションは、ほとんどの場合単方向です。したがって、ブランチからキャンパスに向かう方向のトラフィックフローでは、ブランチルータでこのようなトラフィック向けの帯域幅保証をプロビジョニングするのは、不要であるばかりか非効率的となる可能性があります。

Cisco DNA Center では、アプリケーションが特定のポリシーに関して単方向か双方向かを指定できます。

スイッチおよびワイヤレスコントローラでは、NBAR2やカスタムアプリケーションがデフォルトで単方向となっています。ただし、ルータでは、NBAR2アプリケーションはデフォルトで双方向です。

カスタムアプリケーション

カスタムアプリケーションは、Cisco DNA Centerに追加するアプリケーションです。カスタムアプリケーションの横にはオレンジ色のバーが表示され、標準NBAR2アプリケーションおよびアプリケーションセットと区別されます。有線デバイスについては、サーバ名、IPアドレスとポート、またはURLに基づいてアプリケーションを定義できます。ワイヤレスデバイスについてはカスタムアプリケーションを定義できません。

IPアドレスとポートに従ってアプリケーションを定義する場合は、DSCP値とポート分類を定義することもできます。

設定プロセスを簡素化するために、類似のトラフィックおよびサービスレベル要件を持つ別のアプリケーションに基づいてアプリケーションを定義できます。Cisco DNA Centerは、他のアプリケーションのトラフィッククラス設定を、定義しているアプリケーションにコピーします。

Cisco DNA Center カスタムアプリケーションの一部として定義される場合でも、ポート番号80、443、および8080のACLを設定しません。カスタムアプリケーションでトランスポートIPが定義されている場合、Cisco DNA Centerはデバイス上のアプリケーションを設定します。



(注) ポリシーが展開されているときにデバイス上のカスタムアプリケーションをプログラムする場合は、そのカスタムアプリケーションを、ポリシーで定義されているいずれかのアプリケーションセットに割り当てる必要があります。

お気に入りのアプリケーション

Cisco DNA Centerでは、他のすべてのアプリケーションの前に設定したいアプリケーションにフラグを付けることができます（カスタムアプリケーションを除く）。お気に入りとしてアプリケーションにフラグを付けることで、デバイス上のお気に入りのアプリケーションに対してQoSポリシーが設定されていることを確認できるようにします。詳細については、[リソースが制限されているデバイスの処理順（218ページ）](#)を参照してください。

お気に入りとしてマークできるアプリケーションの数に制限はありませんが、少数のお気に入りのアプリケーション（たとえば、25未満）だけを指定すると、TCAM（Ternary Content Addressable Memory）が限られているネットワークデバイスによる展開において、それらのアプリケーションがビジネス関連の観点から正しく処理されるのに役立ちます。

お気に入りのアプリケーションは、ビジネス関連のグループまたはトラフィッククラスに属させることが可能で、ポリシー単位ではなくシステム全体で設定されます。たとえば、お気に入りとしてcisco-jabber-videoアプリケーションにフラグを付けた場合、そのアプリケーションはすべてのポリシーでお気に入りのフラグが付きます。

ビジネス関連のアプリケーションだけでなく、ビジネスに関係のないアプリケーションにもお気に入りのフラグを付けられることに注意してください。たとえば、管理者がネットワーク上に大量の望ましくない NetFlix トラフィックがあることに気づいた場合、NetFlix にお気に入りのアプリケーションとしてフラグを付けることができます (NetFlix がビジネスに関係ないアプリケーションとして割り当てられている場合でも可能)。この場合、Netflix は、その他のビジネスに関係のないアプリケーションより先にデバイスポリシーに組み込まれるようになり、このアプリケーションを制御するビジネス上の目的が確実に実現されます。

アプリケーションおよびアプリケーションセットの設定

次のサブセクションでは、アプリケーションとアプリケーションセットのコンテキストで実行できるさまざまなタスクについて説明します。

アプリケーション設定の変更

アプリケーションの設定、あるいは既存の NBAR アプリケーションまたはカスタムアプリケーションのトラフィッククラスを変更できます。

ステップ 1 Cisco DNA Center のホームページで、[Provision] > [Services] > [Application Visibility] > [Application] を選択します。

ステップ 2 [検索 (Search)]、[表示 (Show)]、または [表示方法 (View By)] フィールドを使用して、変更するアプリケーションを見つけます。

ステップ 3 [アプリケーション名 (Application Name)] をクリックします。

ステップ 4 ダイアログボックスで、1 つまたは両方の設定を変更します。

- [Traffic Class] : ドロップダウンリストからトラフィッククラスを選択します。有効なトラフィッククラスは、BROADCAST_VIDEO、BULK_DATA、MULTIMEDIA_CONFERENCING、MULTIMEDIA_STREAMING、NETWORK_CONTROL、OPS_ADMIN_MGMT、REAL_TIME_INTERACTIVE、SIGNALING、TRANSACTIONAL_DATA、VOIP_TELEPHONY です。
- [Application Set] : ドロップダウンリストからアプリケーションの設定を選択します。有効なアプリケーションの設定は、認証サービス、バックアップおよびストレージ、コラボレーションアプリケーション、コンシューマブラウジング、コンシューマファイルシェアリング、コンシューマゲーミング、コンシューマメディア、コンシューマ misc、コンシューマソーシャルネットワーキング、データベースアプリケーション、デスクトップ仮想化、電子メール、企業 ipc、ファイル共有、一般的なブラウジング、一般的なメディア、一般的な misc、トンネリング、ローカルサービス、ネーミングサービス、ネットワーク制御、ネットワーク管理、リモートアクセス、saas アプリケーション、シグナリング、ソフトウェア開発ツール、ソフトウェアアップデート、ストリーミングメディアです。

ステップ 5 [保存 (Save)] をクリックします。

サーバ名に基づくカスタムアプリケーションの作成

Cisco DNA Centerに存在しないアプリケーションがある場合、カスタムアプリケーションとして追加することができます。

ステップ 1 Cisco DNA Center のホームページで、[Provision] > [Services] > [Application Visibility] の順にクリックします。

ステップ 2 [Application] タブをクリックします。

ステップ 3 [アプリケーションの追加 (Add Application)] をクリックします。

ステップ 4 ダイアログボックスで、次のフィールドに必要な情報を入力します。

フィールド	説明
Application name	カスタムアプリケーションの名前。名前には、下線とハイフンも含めて最大 24 文字の英数字を指定できます。アプリケーション名で使用できる特殊文字は、下線とハイフンのみです。
Type	ユーザがアプリケーションにアクセスする方法。サーバ経由でアクセス可能なアプリケーションの [サーバ名 (Server Name)] を選択します。
Server name	アプリケーションをホストするサーバの名前。
Similar to	類似するトラフィック処理要件を持つアプリケーション。オプションボタンをクリックしてこのオプションを選択し、ドロップダウンリストからアプリケーションを選択します。Cisco DNA Center は他のアプリケーションのトラフィッククラスを、定義しているアプリケーションにコピーします。
Traffic class	アプリケーションが属するトラフィック クラス。有効な値は BULK_DATA、TRANSACTIONAL_DATA、OPS_ADMIN_MGMT、NETWORK_CONTROL、VOIP_TELEPHONY、MULTIMEDIA_CONFERENCING、MULTIMEDIA_STREAMING、BROADCAST_VIDEO、REAL_TIME_INTERACTIVE、および SIGNALING です。
Application set	アプリケーションを配置するアプリケーションセット。有効なアプリケーションの設定は、認証サービス、バックアップおよびストレージ、コラボレーションアプリケーション、コンシューマブラウジング、コンシューマファイルシェアリング、コンシューマゲーミング、コンシューマメディア、コンシューマ misc、コンシューマ ソーシャル ネットワーキング、データベースアプリケーション、デスクトップ仮想化、電子メール、企業 ipc、ファイル共有、一般的なブラウジング、一般的なメディア、一般的な misc、トンネリング、ローカルサービス、ネーミングサービス、ネットワーク制御、ネットワーク管理、リモートアクセス、saas アプリケーション、シグナリング、ソフトウェア開発ツール、ソフトウェアアップデート、ストリーミングメディアです。

ステップ 5 [OK] をクリックします。

IP アドレスおよびポートベースのカスタム アプリケーションの作成

Cisco DNA Centerに存在しないアプリケーションがある場合、カスタム アプリケーションとして追加することができます。

- ステップ 1 Cisco DNA Center のホームページで、[Provision] > [Services] > [Application Visibility] の順にクリックします。
- ステップ 2 [Application] タブをクリックします。
- ステップ 3 [アプリケーションの追加 (Add Application)] をクリックします。
- ステップ 4 [Application Name] フィールドに、アプリケーションの名前を入力します。名前には、下線とハイフンも含めて最大 24 文字の英数字を指定できます。アプリケーション名で使用できる特殊文字は、下線とハイフンのみです。
- ステップ 5 [種類 (Type)] エリアで、[サーバ IP/ポート (Server IP/Port)] ラジオボタンをクリックして、アプリケーションが IP アドレスとポートを通じてアクセスできます。
- ステップ 6 [DSCP] チェックボックスをオンにして、DSCP 値を定義します。値を定義しない場合のデフォルト値は [Best Effort] です。ベストエフォート サービスとは原則的に、いずれの QoS も適用されないネットワーク デバイスのデフォルト動作です。
- ステップ 7 [IP/Port Classifiers] チェックボックスをオンにして、アプリケーションの IP アドレスとサブネット、プロトコル、およびポートまたはポート範囲を選択します。有効なプロトコルは、[IP]、[TCP]、[UDP]、[TCP/UDP] です。[IP] プロトコルを選択した場合は、ポート番号または範囲は定義しません。+ をクリックして、さらに分類子を追加します。
- ステップ 8 次のいずれかの方法を使用して、アプリケーショントラフィック処理要件を定義します。
 - [Similar To] : お使いのアプリケーションに既存のアプリケーションと同様のトラフィック処理要件がある場合は、[Similar To] オプションボタンをクリックし、ドロップダウンリストからアプリケーションを選択します。Cisco DNA Center は、他のアプリケーションのトラフィッククラスを、定義しているアプリケーションにコピーします。
 - [Traffic Class] : アプリケーションに定義するトラフィッククラスがわかっている場合は、[Traffic Class] オプションボタンをクリックし、ドロップダウンリストからトラフィッククラスを選択します。有効な値は BULK_DATA、TRANSACTIONAL_DATA、OPS_ADMIN_MGMT、NETWORK_CONTROL、VOIP_TELEPHONY、MULTIMEDIA_CONFERENCING、MULTIMEDIA_STREAMING、BROADCAST_VIDEO、REAL_TIME_INTERACTIVE、および SIGNALING です。
- ステップ 9 [Application Set] ドロップダウンリストから、アプリケーションが属するアプリケーションセットを選択します。有効なアプリケーションの設定は、認証サービス、バックアップおよびストレージ、コラボレーションアプリケーション、コンシューマブラウジング、コンシューマファイルシェアリング、コンシューマゲーミング、コンシューマメディア、コンシューマ misc、コンシューマ ソーシャル ネットワーキング、データベースアプリケーション、デスクトップ仮想化、電子メール、企業 ipc、ファイル共有、一般的なブラウジング、一般的なメディア、一般的な misc、トンネリング、ローカルサービス、ネーミング サービス、ネットワーク制御、ネットワーク管理、リモートアクセス、saas アプリケーション、シグナリング、ソフトウェア開発ツール、ソフトウェアアップデート、ストリーミングメディアです。

ステップ10 [OK] をクリックします。

URLに基づくカスタムアプリケーションの作成

Cisco DNA Centerに存在しないアプリケーションがある場合、カスタムアプリケーションとして追加することができます。

ステップ1 Cisco DNA Center のホームページで、[Provision] > [Services] > [Application Visibility] の順にクリックします。

ステップ2 [Application] タブをクリックします。

ステップ3 [アプリケーションの追加 (Add Application)] をクリックします。

[アプリケーションの追加 (Add Application)] ダイアログボックスが表示されます。

ステップ4 [アプリケーション名 (Application Name)] フィールドに、アプリケーションの名前を入力します。名前には、下線とハイフンも含めて最大24文字の英数字を指定できます。アプリケーション名で使用できる特殊文字は、下線とハイフンのみです。

ステップ5 タイプについては、[URL] オプションボタンをクリックします。

ステップ6 [Url] フィールドに、アプリケーションに到達するために使用する url を入力します。

ステップ7 トラフィック クラスの設定:

- 同様のトラフィック処理要件を持つ別のアプリケーションと同じトラフィッククラスを使用するには、オプションボタンをクリックして、ドロップダウンリストからアプリケーションを選択します。
- トラフィッククラスを指定するには、[**トラフィッククラス (Traffic class)**] オプションボタンをクリックし、ドロップダウンリストからトラフィッククラスを選択します。有効な値は BULK_DATA、TRANSACTIONAL_DATA、OPS_ADMIN_MGMT、NETWORK_CONTROL、VOIP_TELEPHONY、MULTIMEDIA_CONFERENCING、MULTIMEDIA_STREAMING、BROADCAST_VIDEO、REAL_TIME_INTERACTIVE、および SIGNALING です。

ステップ8 [アプリケーションセット (Application set)] ドロップダウンリストから、アプリケーションを配置するアプリケーションセットを選択します。


ステップ9 [OK] をクリックします。

カスタムアプリケーションの編集または削除

必要な場合は、カスタムアプリケーションを変更または削除できます。



- (注) アプリケーション ポリシーによって直接参照されているカスタム アプリケーションを削除することはできません。通常、アプリケーションポリシーはアプリケーションセットを参照し、個々のアプリケーションを参照しません。ただし、ポリシーにアプリケーションの特別な定義（コンシューマまたはプロデューサの割り当てや双方向の帯域幅プロビジョニングなど）が設定されている場合、ポリシーはそのアプリケーションを直接参照します。そのため、アプリケーションを削除する前に、特別な定義を削除するか、またはアプリケーションへの参照を削除する必要があります。

- ステップ 1** Cisco DNA Center のホームページで、[Provision] > [Services] > [Application Visibility] の順にクリックします。
- ステップ 2** [Application] タブをクリックします。
- ステップ 3** [検索 (Search)]、[表示 (Show)]、または [表示方法 (View By)] フィールドを使用して、変更するアプリケーションを見つけます。
- ステップ 4** アプリケーションを編集するには、次の手順を実行します。
- アプリケーション名をクリックして、必要な変更を行います。フィールドの詳細については、[サーバ名に基づくカスタムアプリケーションの作成 \(354 ページ\)](#)、[IP アドレスおよびポートベースのカスタムアプリケーションの作成 \(355 ページ\)](#)、または[URL に基づくカスタムアプリケーションの作成 \(356 ページ\)](#) を参照してください。
 - [OK] をクリックします。
- ステップ 5** アプリケーションを削除するには、アプリケーションボックスで  をクリックし、[OK] をクリックして確定します。

アプリケーションをお気に入りにする

アプリケーションをお気に入りにしてマークして、アプリケーションの QoS 設定を、他のアプリケーションの QoS 設定の前にデバイスに展開する必要があることを指定できます。お気に入りにしてマークされたアプリケーションには、その横に黄色の星が付いています。

ポリシーを追加または編集すると、お気に入りにしてマークされたアプリケーションがアプリケーションセットの上部に表示されます。

アプリケーションは、個々のポリシーベースではなくシステム全体で設定されます。詳細については、「[お気に入りのアプリケーション \(352 ページ\)](#)」を参照してください。

- ステップ 1** Cisco DNA Center のホームページで、[Provision] > [Services] > [Application Visibility] の順にクリックします。
- ステップ 2** [Application] タブをクリックします。
- ステップ 3** お気に入りにしてマークするアプリケーションを特定します。

ステップ4 ★ をクリックします。

カスタムアプリケーション設定の作成

使用したいアプリケーション設定がない場合、カスタムアプリケーション設定を作成できません。

ステップ1 Cisco DNA Center のホームページで、[Provision] > [Services] > [Application Visibility] の順にクリックします。

ステップ2 [Application Sets] タブをクリックします。

ステップ3 [アプリケーション設定の追加 (Add Application Set)] をクリックします。

ステップ4 ダイアログ ボックスに、新しいアプリケーション設定の名前を入力します。

Cisco DNA Center で新しいアプリケーション設定が作成されますが、その中にアプリケーションは存在しません。

ステップ5 [OK] をクリックします。

ステップ6 [検索 (Search)] を使用して [表示 (Show)] または [表示方法 (View By)] フィールドを使用して、アプリケーション設定を見つけます。

ステップ7 新しいアプリケーション設定に移動させるアプリケーションを見つけます。

ステップ8 移動させるアプリケーションの横にあるチェック ボックスをオンにします。

ステップ9 新しいアプリケーション設定にアプリケーションをドラッグアンドドロップします。

カスタムアプリケーションセットの編集または削除

必要な場合は、カスタムアプリケーションを変更または削除できます。



(注) アプリケーションポリシーによって参照されているカスタムアプリケーションセットを削除することはできません。アプリケーションセットを削除する前に、ポリシーからアプリケーションセットを削除する必要があります。


ステップ1 [Home]Cisco DNA Center ページで、[Provision] > [Services] > [Application Visibility] の順にクリックします。

ステップ2 [Application Sets] タブをクリックします。

ステップ3 [検索 (Search)]、[表示 (Show)]、または [表示方法 (View By)] フィールドを使用して、変更するアプリケーションセットを見つけます。

ステップ4 次のいずれかを実行します。

- アプリケーション設定するには、アプリケーション設定に、またはアプリケーション設定からアプリケーションをドラッグアンドドロップします。[OK] をクリックして、それぞれの変更を確定します。

- アプリケーション設定を削除するには、アプリケーション設定ボックスにある  をクリックし、次に [OK] をクリックして確定します。

アプリケーションホスティング

アプリケーションホスティングについて

アプリケーションホスティングを使用すると、Cisco DNA Centerによって管理されているデバイス上のサードパーティ製アプリケーションのライフサイクルを管理できます。このリリースでは、Cisco IOS XE ソフトウェアバージョン 16.12.1s を搭載した Catalyst 9300 シリーズスイッチのサードパーティ製 Docker アプリケーションを利用できます。

アプリケーションホスティングの前提条件

デバイスでアプリケーションをホストするには、次の前提条件を満たしている必要があります。

- デバイスの HTTPS ログイン情報を設定します。デバイスを手動で Cisco DNA Center に追加するときに HTTPS ログイン情報を設定するか、デバイスのログイン情報を編集できます。詳細については、「[ネットワーク デバイス クレデンシャルの更新 \(53 ページ\)](#)」を参照してください。
- ユーザ認証用にローカルの認証サーバまたは AAA サーバを設定します。ユーザ名およびパスワードは特権 EXEC モード (レベル 15) で設定する必要があります。詳細については、[Cisco Digital Network Architecture Center 管理者ガイド \[英語\]](#) の「Configure Authentication and Policy Servers」を参照してください。
- デバイスで、着脱可能な USB SSD 外部ストレージがサポートされていることを確認します。

アプリケーションをホストするデバイスの準備状況の表示

スイッチにアプリケーションをインストールする前に、Cisco Catalyst 9300 シリーズスイッチのアプリケーションをホスティングするための準備状況を確認する必要があります。

ステップ 1 Cisco DNA Center のホームページで、[Provision] > [Services] > [App Hosting] の順に選択します。

ステップ 2 [All Devices] をクリックします。

ステップ3 アプリケーションをホストできるデバイスのリストが表示されます。[App Hosting Status] は、デバイスがアプリケーションをホストするための準備状況を示します。ステータスに[Not Ready]と表示されている場合は、ステータスをクリックして理由を確認できます。

アプリケーションの追加

Cisco Package または Docker アプリケーションを追加できます。

始める前に

- [Cisco Package] アプリケーション：IOS SDK ツールを使用してアプリケーションをパッケージ化し、アプリケーションが IOS XE オペレーティングシステムと互換性を持つようにする必要があります。
- [Docker] アプリケーション：Docker イメージを tar ファイルとして保存する必要があります。Docker イメージを tar ファイルとして保存するには、次のコマンドを使用します。

```
docker save -o <path for generated tar file> <image name:tag>
```

```
Example: docker save -o alpine-tcpdump.tar itsthenetwork/alpine-tcpdump:latest
```

ステップ1 Cisco DNA Center のホームページで、[Provision] > [Services] > [App Hosting] の順に選択します。

ステップ2 [New Application] をクリックします。

ステップ3 ドロップダウンリストからアプリケーションの [Type] と [Category] を選択します。

ステップ4 [Select] をクリックして、アップロードするアプリケーションを選択します。

ステップ5 [Upload] をクリックします。

新しく追加されたアプリケーションは、[App Hosting] ページで確認できます。

Cisco Catalyst 9300 デバイスへのアプリケーションのインストール

Cisco DNA Center Cisco DNA Center では、Cisco Catalyst 9300 シリーズ スイッチにアプリケーションをインストールできます。

始める前に

- 前提条件を満たします。詳細については、「[アプリケーション ホスティングの前提条件 \(359 ページ\)](#)」を参照してください。
- アプリケーションを Cisco DNA Center に追加します。詳細については、「[アプリケーションの追加 \(360 ページ\)](#)」を参照してください。
- アプリケーションをホストするためのスイッチの準備状況を確認します。詳細については、「[アプリケーションをホストするデバイスの準備状況の表示 \(359 ページ\)](#)」を参照してください。

ステップ 1 Cisco DNA Center のホームページで、**[Provision] > [Services] > [App Hosting]** の順に選択します。

ステップ 2 アプリケーションを選択し、**[Install]** をクリックします。

ステップ 3 アプリケーションのインストール先デバイスを選択し、**[Next]** をクリックします。

ステップ 4 **[Configuration App]** タブで次の設定を行います。

- **アプリケーションネットワーキング**

- **[Device Network] : [Select Network]** ドロップダウンリストをクリックして、アプリケーションを設定する VLAN を選択します。

- **[App IP address] : [Address Type]** ドロップダウンリストから、**[Static]** または **[Dynamic]** を選択します。**[Static]** を選択した場合は、サムネイルアイコンをクリックして、アプリケーションの **[IP Address]**、**[Gateway]**、**[Prefix/Mask]**、および **[DNS]** を入力します。

- **[Resource Allocation] : [Allocate all resources available on a device]** または **[Customize resource allocation]** チェックボックスをオンにします。**[Customize resource allocation]** チェックボックスをオンにすると、**[CPU]**、**[Memory]**、および **[Persistent Storage]** の最大値を低い値に変更できます。

- (オプション) **[Custom Settings]** : シスコパッケージアプリケーションにのみ適用可能です。アプリケーションによって指定された属性の設定の詳細を入力します。

- (オプション) **[App Data]** : アプリケーション固有のファイルを参照し、アップロードします。必要なアプリケーション固有のファイルを特定するには、関連するアプリケーションのドキュメントを参照してください。

- **[Docker Runtime Options]** : アプリケーションに必要な Docker ランタイムオプションを入力します。

ステップ 5 **[Next]** をクリックして、**[Confirm]** 画面でアプリケーション設定を確認します。

ステップ 6 **[完了 (Finish)]** をクリックします。

ステップ 7 インストールの **[Confirmation]** ウィンドウで **[Yes]** をクリックして、選択した Cisco Catalyst 9300 デバイスでのアプリケーションのインストールを完了します。

次のタスク

アプリケーションをインストールすると、デバイスの **IOS XE** 設定も変更されます。実行コンフィギュレーションのこの変更は、ルータのリロード後にアプリケーションが予期したとおりに機能するように、スタートアップコンフィギュレーションにコピーする必要があります。アプリケーションのインストールが正常に完了したら、**テンプレートエディタ**を使用して実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

アプリケーションの更新

Cisco DNA Center で追加されたアプリケーションを更新できます。

-
- ステップ 1** Cisco DNA Center のホームページで、**[Provision] > [Services] > [App Hosting]** の順に選択します。
使用可能なアプリケーションは、**[App Hosting]** ページで確認できます。
- ステップ 2** 更新するアプリケーションを選択します。
- ステップ 3** **[Update Application]** をクリックします。
- ステップ 4** ドロップダウンリストからアプリケーションの **[Type]** と **[Category]** を選択します。
- ステップ 5** **[Select]** をクリックして、アップロードするアプリケーションの新しいバージョンを選択します。
- ステップ 6** **[Upload]** をクリックします。
-

Cisco Catalyst 9300 デバイスからのアプリケーションのアンインストール

Cisco Catalyst 9300 シリーズ スイッチからアプリケーションをアンインストールできます。

- ステップ 1** Cisco DNA Center のホームページで、**[Provision] > [Services] > [App Hosting]** の順に選択します。
- ステップ 2** アプリケーションを選択し、**[Manage]** をクリックして、アプリケーションを使用するデバイスを表示します。
- ステップ 3** アプリケーションをアンインストールするデバイスを選択します。
- ステップ 4** **[Actions]** ドロップダウンリストから **[Uninstall App]** を選択します。
-

アプリケーションの削除

Cisco DNA Center からアプリケーションを削除できます。

始める前に

アプリケーションを使用しているすべてのデバイスからアプリケーションをアンインストールする必要があります。詳細については、[Cisco Catalyst 9300 デバイスからのアプリケーションのアンインストール \(362 ページ\)](#) を参照してください。

- ステップ 1** Cisco DNA Center のホームページで、**[Provision] > [Services] > [App Hosting]** の順に選択します。
[App Hosting] ページで使用可能なホストされたアプリケーションを表示できます。
- ステップ 2** 削除するアプリケーションを選択します。
- ステップ 3** **[Delete Application]** をクリックします。
- ステップ 4** 確認ダイアログボックスで **[OK]** をクリックします。

アプリケーションは、Cisco DNA Center によって管理されているいずれのデバイスでも使用されていない場合にのみ削除されます。それ以外の場合、エラーメッセージに、アプリケーションを使用しているデバイスの数が表示されます。

確認ダイアログボックスで [Cancel] をクリックし、アプリケーションをアンインストールします。詳細については、[Cisco Catalyst 9300 デバイスからのアプリケーションのアンインストール \(362 ページ\)](#) を参照してください。

アプリケーションログのダウンロード

Cisco DNA Center からアプリケーションログをダウンロードできます。

ステップ 1 Cisco DNA Center のホームページで、[Provision] > [Services] > [App Hosting] の順に選択します。

ステップ 2 [All Devices] をクリックします。

アプリケーションをホストできるデバイスのリストが表示されます。

ステップ 3 [App logs] をクリックして、Cisco DNA Center からアプリケーションログをダウンロードします。

ステップ 4 [App Logs] ポップアップウィンドウで、ダウンロードするアプリケーションログファイルをドロップダウンリストから選択し、[Download] をクリックします。

デバイスのテクニカルサポートログのダウンロード

トラブルシューティングを行うために、Cisco DNA Center からデバイスのテクニカルサポートログをダウンロードできます。

ステップ 1 Cisco DNA Center のホームページで、[Provision] > [Services] > [App Hosting] の順に選択します。

ステップ 2 [All Devices] をクリックします。

アプリケーションをホストできるデバイスのリストが表示されます。

ステップ 3 [Tech Support logs] をクリックして、デバイスのテクニカルサポートログを Cisco DNA Center からダウンロードします。



第 14 章

Cisco DNA アシユアランス

- [Cisco DNA アシユアランス \(365 ページ\)](#)

Cisco DNA アシユアランス

Cisco DNA アシユアランスは、Cisco DNA Center から入手可能なアプリケーションです。Cisco DNA Center は、リリース 1.2.5 から、Cisco DNA アシユアランス のみを扱うユーザガイドを提供しています。

ネットワークの正常性、クライアントの正常性、およびアプリケーションの正常性をモニタおよびトラブルシューティングする方法、およびNetFlowの収集を有効にする方法など、アシユアランスアプリケーションの詳細については、[Cisco DNA Assurance ユーザガイド](#)を参照してください。



第 15 章

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

- [データプラットフォームについて \(367 ページ\)](#)
- [分析 Ops センターを使用したトラブルシューティング \(368 ページ\)](#)
- [コレクタの設定情報の表示または更新 \(370 ページ\)](#)
- [データ保持設定の表示 \(371 ページ\)](#)
- [パイプラインステータスの表示 \(371 ページ\)](#)

データプラットフォームについて

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

- [Analytics Ops Center] : データがコレクタとパイプラインを経由してどのように流れているかをグラフィカルに表示します。また、ネットワーク内のパターン、傾向、および問題領域を特定できる Grafana ダッシュボードも用意されています。[分析 Ops センターを使用したトラブルシューティング \(368 ページ\)](#) を参照してください。
- [Collectors] : さまざまなネットワークテレメトリとコンテキストデータをリアルタイムで収集します。データが取り込まれると、Cisco DNA Center はデータを関連付けて分析します。コレクタのステータスを表示し、問題領域をすばやく見分けることができます。[コレクタの設定情報の表示または更新 \(370 ページ\)](#) を参照してください。
- [Store Settings] : アプリケーションデータの保存期間を指定できます。[データ保持設定の表示 \(371 ページ\)](#) を参照してください。
- [Pipelines] : Cisco DNA Center アプリケーションが、ストリーミングデータを処理できるようにします。データパイプラインでは、外部ソースからの入力データを受け入れ、有用な

情報を提供するためにそのデータを変換し、出力データを生成する一連の計算をカプセル化します。パイプラインのステータスを表示し、問題領域をすばやく見分けることができます。「[パイプラインステータスの表示 \(371 ページ\)](#)」を参照してください。

分析 Ops センターを使用したトラブルシューティング

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

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

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

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

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

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

各コンポーネントの現在のヘルス ステータスは、色によって示されます。

- 赤色：エラー
- 黄色：警告
- 灰色：通常動作

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

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

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

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

スライドインペインに次のタブが表示されます。

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

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

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

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

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

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

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

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

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


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

ステップ 10 特定のフローのメトリックを表示するには、次を実行します。

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

コレクタの設定情報の表示または更新

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

-
- ステップ 1** Cisco DNA Center のホームページで、歯車のアイコン  をクリックして、[システムの設定 (System Settings)] > [データ プラットフォーム (Data Platform)] の順に選択します。
- ステップ 2** [コレクタ (Collectors)] をクリックします。各コレクタの横にある色付きの点は、全体的なステータスを示しています。
- ステップ 3** 追加の詳細を表示するには、コレクタ名をクリックします。
- 適切な [Collector] ページが表示されます。デフォルトでは、Cisco DNA Center に [Configuration] タブが表示され、現在の設定リストを確認できます。
- ステップ 4** 構成を表示、更新、または削除するには、特定の構成名をクリックします。
- ステップ 5** 新規の設定を追加するには、[Configuration] タブで [+ Add] をクリックします。
- スライドインペインが表示されます。
- (注) [COLLECTOR-ISE] の設定については、[Cisco DNA Assurance ユーザガイド \[英語\]](#) の「Configure Assurance for Cisco ISE Integration」セクションを参照してください。
- ステップ 6** スライドインペインで、設定に必要な情報を入力します。
- ステップ 7** (任意) [Anonymize] チェックボックスをオンにすると、[WIRELESSCOLLECTOR] などの一部のコレクタのデータを匿名化できます。
- (注) [Anonymize] チェックボックスをオンにすると、[Client Health] ウィンドウのホスト名とユーザ ID は、復号化できない一方ハッシュを用いてスクランブル処理されます。
- 重要** データを匿名化する場合は、[Discovery] ツールを使用してデバイスを検出する前に、[Anonymize] チェックボックスをオンにしてください。デバイスを検出した後にデータを匿名化した場合、システムに入ってくる新しいデータは匿名化されますが、既存のデータは匿名化されません。
- ステップ 8** [Save Configuration] をクリックします。
- ステップ 9** 設定されているインスタンスを表示するには、[インスタンス (Instances)] タブをクリックします。
- ステップ 10** 概要情報とメトリックを表示するには、リストからインスタンスを選択します。
- ステップ 11** (任意) Cisco DNA Center を Cisco Connected Mobile Experience (CMX) と統合する場合は、CMX 側でデータの匿名化を選択できます。次の手順を実行します。
- SSH クライアントを使用して、cmxadmin CLI ユーザとして Cisco CMX にログインします。
 - ルートユーザに変更します。
 - /opt/cmx/etc/node.conf に移動し、[location] の下に **user_options** を追加します。次に例を示します。


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

- d) Cisco CMX CLI で、次のコマンドを入力します。

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


データ保持設定の表示

アプリケーションのデータの保存期間を表示できます。

- ステップ 1** Cisco DNA Center のホームページで、歯車のアイコン  をクリックして、[システムの設定 (System Settings)] > [データ プラットフォーム (Data Platform)] の順に選択します。
- ステップ 2** [ストア設定 (Store Settings)] をクリックします。
- ステップ 3** 完了した履歴消去ジョブのリストを表示するには、[データ消去スケジュール (Data Purge Schedule)] をクリックします。
- [HISTORY] テーブルには、消去ジョブの名前、結果、時刻、その他のデータが表示されます。テーブル内のデータをソート、フィルタリング、エクスポートすることができます。
- ステップ 4** 現在のデータの保持または消去の設定を表示するには、[Data Retention & Purge Configuration] をクリックします。次の出力が表示されます。
- [Document Store] : 最大サイズ、ウォーターマークの下限および上限しきい値など、すべての時間ベースのデータの設定。
 - [Metric Graph Store] : 最大サイズ、下限および上限しきい値など、すべての時間ベースのグラフィカルデータの設定。

パイプラインステータスの表示

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

- ステップ 1** Cisco DNA Center のホームページで、歯車のアイコン  をクリックして、[システムの設定 (System Settings)] > [データ プラットフォーム (Data Platform)] の順に選択します。
- ステップ 2** [パイプライン (Pipelines)] をクリックします。

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

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

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

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