Cisco Prime Infrastructure 3.7 ユーザ ガイド

初版：2019 年 5 月 13 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 NONINFRINGEMENT 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. 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)

© 2012–2019 Cisco Systems, Inc. All rights reserved.

目 次

Full Cisco Trademarks with Software License ?

第 I 部 : **Prime Infrastructure の概要 51**

第 1 章 **Cisco Prime Infrastructure の概要 1**

Prime Infrastructure の構成 1

を使用する前に完了する必要のあるタスクのセットアップ Prime Infrastructure 2

ログインおよびログアウト 3

パスワードの変更 4

メイン ウィンドウ コントロールの使用 4

デフォルトのホーム ページの変更 5

ダッシュボードのセットアップと使用 6

ダッシュボードの使用方法 7

[ドック（Dock）] ウィンドウのカスタマイズ 9

ダッシュボードのタイプ 9

ネットワーク概要ダッシュボードを使用したネットワーク全体の健全性の確認 10

概要ダッシュボードを使用したすべてのデバイスまたはすべてのインターフェイスのヘルスの確認 11

ワイヤレス ダッシュボードを使用したワイヤレス ネットワークのヘルスの確認 12

[パフォーマンス（Performance）] ダッシュボードを使用して、特定のデバイスまたはインターフェイスのパフォーマンスをチェックする 13

ダッシュボードへのダッシュレットの追加 15

事前定義のダッシュレットをダッシュボードに追加する 15

[デバイス トレンド（Device Trends）] ダッシュボードへのカスタマイズ済みダッシュレットの追加 16

新しいダッシュボードの追加 18
ダッシュレット データの CSV または PDF ファイルへのエクスポート 18
ダッシュボードを使用したネットワーク ヘルスのトラブルシューティング 19
ヘルス ルールの定義 20
QoS およびインターフェイスの設定の定義 21
ネットワーク ヘルス マップ機能 21
ネットワーク ヘルス表示オプション 22
ネットワーク ヘルスの概要 23
QoS メトリック 24
トラフィック カンバセーション 25
別の仮想ドメインで作業する 27
ジョブ ダッシュボードを使用したジョブの管理 27
Cisco Prime Infrastructure 機能の拡張 29
最新のインベントリに存在をチェック マニュアル 30

第 2 章 Prime Infrastructure のユーザ設定の変更 31
ユーザ設定 31
ユーザ設定の変更 31
アイドル ユーザ タイムアウトの変更 32
リストの長さの変更 33

第 II 部： インベントリの管理 35

第 3 章 デバイスの追加と整理 37
Prime Infrastructure へのデバイスの追加 37
ディスカバリ プロセスについて 39
ディスカバリを使用したデバイスの追加 39
検出されたデバイスの管理 IP アドレス タイプ（IPv4/IPv6）の指定 41
クイック ディスカバリの実行 41
カスタマイズされたディスカバリ設定でのディスカバリの実行 42
検出の確認 43

他のソースからのデバイスのインポート 44
デバイスのインポート CSV ファイルの作成 44
手動によるデバイスの追加（新規デバイス タイプまたはデバイス シリーズ） 46
仮想デバイス コンテキストの追加 48
Prime Infrastructure への Meraki デバイスの追加 48
ワイヤレス コントローラを追加するための前提条件 50
追加されたデバイスの検証と問題のトラブルシューティング 51
デバイスの到達可能性の状態および管理ステータスの確認 52
デバイスの到達可能性状態と管理状態 53
デバイスのメンテナンス状態の切り替え 54
デバイス パラメータの編集 55
デバイスの同期化 55
スマート インベントリ 56
NAM HTTP/HTTPS クレデンシャルの追加 56
CSV ファイルへのデバイス情報のエクスポート 57
クレデンシャル プロファイルを使用したデバイス クレデンシャルの一貫した適用 58
新しいクレデンシャル プロファイルの作成 58
既存のデバイスへの新規または変更されたプロファイルの適用 59
クレデンシャル プロファイルの削除 60
簡単な管理と設定のためのデバイス グループの作成 60
グループの仕組み 61
ネットワーク デバイス グループ 61
ポート グループ 63
データセンター グループ 64
グループに要素を追加する方法：動的、手動、および混在グループ 65
グループおよび仮想ドメイン 66
ユーザ定義のデバイス グループの作成 66
デバイスが属するすべてのグループの表示 67
ロケーション グループの作成 68
CSV ファイルを使用したグループの作成 70
CSV ファイルへのグループのエクスポート 70

デバイス グループとロケーション グループへの AP の追加 70
ポート グループの作成 72
ユーザ定義データセンター グループの作成 72
ユーザ定義グループの編集 73
グループのコピーの作成 74
ユーザ定義グループおよびロケーション グループのコピー 74
メンバーがいないグループの非表示 75
グループの削除 75
コンピューティング リソース グループの作成 76

第 4 章 デバイスの表示 77
ネットワーク デバイスの表示 77
コンピューティング デバイスの表示 81
ユーザ定義の UCS グループの作成 88
ユーザ定義のホストと VM の作成 89

第 5 章 コンピューティング リソースの管理 91
VMware vCenter Server の管理 91
VMware vCenter Server の追加 91
vCenter をインポートするための CSV ファイルの要件 92
コンピューティング リソース パフォーマンスのモニタ 93
データセンター デバイスのポーリング間隔の設定 93
クラスタ モニタリングのセットアップ 94

第 6 章 デバイス コンフィギュレーション ファイルの管理 95
デバイス コンフィギュレーション ファイル管理のセットアップ 95
アーカイブのトリガー方法の制御 96
イベント トリガー アーカイブをセットアップする 97
設定ファイルの変更を確認する場合に除外する項目の指定 98
設定アーカイブ操作のタイムアウトの制御 98
アーカイブ サマリーの更新頻度の制御 98

並行してアーカイブできるファイル数の制御 99
エクスポート中に設定ファイルのコンテンツをマスクするかどうかの制御 99
コンフィギュレーション ファイルのダウンロード 99
データベースからデバイス コンフィギュレーション ファイルを消去するタイミングの制御 100
ファイルが最後にアーカイブされた時刻を確認する方法 101
デバイス コンフィギュレーション ファイルのアーカイブへのバックアップ 101
データベースにバックアップされる内容 101
コンフィギュレーション ファイルをバックアップ（アーカイブ）する 102
アーカイブに保存されているデバイス コンフィギュレーション ファイルの表示 103
すべてのアーカイブされたファイルを表示する 104
特定のデバイスのアーカイブされたファイルを表示する 104
アーカイブされた設定ファイルの raw コンテンツの表示 105
タグを使用した重要なコンフィギュレーション ファイルのラベル付け 105
実行デバイス コンフィギュレーションとスタートアップ デバイス コンフィギュレーションの同期 106
デバイスのコンフィギュレーション ファイルの比較または削除 107
デバイスへの外部コンフィギュレーション ファイルの展開 108
実行コンフィギュレーションによるスタートアップ コンフィギュレーションの上書き 109
アーカイブされたバージョンへのデバイス設定のロールバック 109
コンフィギュレーション ファイルのダウンロード 111
設定アーカイブ操作に関する変更監査の確認 112

第 7 章 デバイス ソフトウェア イメージの管理 113
ソフトウェア イメージ管理のセットアップ 113
デバイスが正しく構成されていることを確認する 114
Prime Infrastructure サーバでの FTP/TFTP/SFTP/SCP 設定の確認 115
インベントリ収集中にイメージ リポジトリに保存されたイメージの制御方法 115
ソフトウェア イメージの管理プロセスとサポートされているデバイス 115
Cisco.com のイメージ推奨事項に応じた基準の調整 124
イメージの転送および配布設定の調整 125

デバイス グループを管理するソフトウェア イメージ管理サーバの追加 127
ソフトウェア イメージ操作に関する Cisco.com クレデンシャルの変更 128
デバイスからイメージ リポジトリへのソフトウェア イメージのコピー（ベースラインの作成） 128
ネットワーク デバイスでどのイメージが使用されているかを調べる方法 129
デバイスに最新のイメージがあることを確認する方法 129
Cisco.com からソフトウェアをダウンロードする権限があるかどうかを調べる方法 130
イメージ リポジトリに保存されたイメージを表示する 130
イメージを使用しているデバイスの確認 131
Cisco.com で推奨されるイメージの表示 132
Cisco.com からのイメージのダウンロード 133
ソフトウェア イメージをリポジトリに追加（インポート）する 134
管理対象デバイスで実行されているソフトウェア イメージの追加 134
IPv4 または IPv6 サーバからソフトウェア イメージを追加する（URL） 136
FTP プロトコル サーバのソフトウェア イメージの追加（プロトコル） 136
クライアント マシンのファイル システムからのソフトウェア イメージの追加 137
仮想イメージ リポジトリへのソフトウェア イメージのインポート 138
ソフトウェア イメージをアップグレードするためのデバイス要件の変更 139
デバイスがイメージ要件を満たしていることの確認（アップグレード分析） 139
デバイスへの新しいソフトウェア イメージの配布 140
デバイスで新しいソフトウェア イメージをアクティブにする 143
ワイヤレス/DC デバイスへのソフトウェア イメージの展開 145
スタック デバイスのサポートされているイメージ形式 146
デバイスのリロード間での Cisco ISO XR イメージのコミット 147
ソフトウェア イメージ操作に関する変更監査の確認 148
ASD の例外とエラー条件 149
ローリング AP アップグレードの使用によるコントローラ ソフトウェアのアップグレード 151

第 8 章 コンプライアンスを使用した設定の監査の実行 153
コンプライアンス監査の実行方法 153

コンプライアンス監査の有効化および無効化 154
新しいコンプライアンス ポリシーの作成 155
コンプライアンス ポリシー ルールの作成 155
例：ルールの条件とアクション 157
例：ブロック オプション 157
条件およびアクションの例：コミュニティ文字列 159
条件およびアクションの例：IOS ソフトウェア バージョン 161
条件およびアクションの例：NTP サーバの冗長性 161
ポリシーとルールが含まれているコンプライアンス プロファイルの作成 162
コンプライアンス監査の実行 164
コンプライアンス監査の結果の表示 165
デバイスのコンプライアンス違反の修正 166
違反サマリーの詳細の表示 167
違反ジョブの詳細の表示 168
コンプライアンス ポリシーのインポートおよびエクスポート 169
コンプライアンス ポリシー XML ファイルのコンテンツの表示 169
PSIRT および EOX 情報の表示 170
デバイスのセキュリティ脆弱性の表示 170
デバイスのハードウェアとソフトウェアのサポート終了レポートの表示 171
モジュール ハードウェアのサポート終了レポートの表示 172
デバイスのフィールド通知の表示 172

第 III 部： ネットワークの視覚化 175

第 9 章 ネットワーク トポロジの視覚化 177
ネットワーク トポロジの概要 177
データセンター トポロジ 179
ネットワーク トポロジ マップでのアラームとリンクの詳細なテーブルの表示 179
詳細テーブルでのデータのフィルタ処理 180
トポロジ マップの表示内容の決定 181
ネットワーク トポロジ マップに表示するデバイス グループの選択 181

トポロジ マップにサブグループのコンテンツを表示する 182
トポロジ マップへのデバイスとネットワークの手動による追加 183
トポロジ マップへのリンクの手動による追加 183
ネットワーク トポロジ マップに表示するリンクとデバイス タイプの変更 184
トポロジ マップでのアラームとラベルの表示/非表示 185
大規模なトポロジ マップの特定のセクションを隔離する 186
デバイスの詳細情報の取得 186
リンクの詳細情報の取得 187
デバイスおよびリンクの障害情報の表示 187
ネットワーク トポロジ マップのレイアウトの変更 188
将来の Web GUI セッション用にネットワーク トポロジ マップのレイアウトを保存する 188
ネットワーク トポロジ マップでのクロック同期ネットワークの表示 189
イメージ ファイルとしてトポロジ マップを保存する 190

第 10 章 ワイヤレス サイト マップの使用 191
次世代ワイヤレス サイト マップの紹介 191
ワイヤレス サイト マップの構成方法 192
ワイヤレス サイト マップ内で使用するためのイメージ ファイルの準備に関するガイドライン 193
サイト マップの使用 193
サイトの追加 194
サイトの削除 195
サイトの更新 195
マップ アーカイブのインポート 196
マップ アーカイブのエクスポート 197
CSV 形式での一括 AP のインポート 197
CSV 形式での一括 AP のエクスポート 198
Geo マップのアクセス ポイントのインポート 199
Geo マップのアクセス ポイントのエクスポート 199
マップ プロパティの編集 199
屋外領域の設定 200

屋外領域の追加 201
屋外領域の編集 201
屋外領域の削除 202
ビルディングの設定 202
建物の 3D ビューの使用 202
建物の追加 203
ビルディングの編集 204
ビルディングの削除 204
フロア領域のモニタ 204
フロア領域の設定 208
ビルディングへのフロア領域の追加 209
さまざまなフロア要素の表示設定 210
アクセス ポイントの表示設定の構成 210
メッシュ アクセス ポイントの表示設定の構成 213
802.11 タグの表示の設定を構成します。 215
オーバーレイ オブジェクトの表示設定を構成します。 215
クライアントの表示設定を構成します。 216
不正アクセス ポイントの表示設定の構成 216
アドホックの悪党の表示設定を構成します。 217
不正クライアントの表示設定の構成 217
干渉源の表示設定の構成 217
wIPS 攻撃の表示設定の構成 218
MSE/CMX サイト マップ統合の表示設定の構成 218
マップ プロパティの設定 219
フロア要素の編集 219
AP の追加、配置、および削除 220
AP のクイック ビュー 223
チョーク ポイントの追加、配置、および削除 223
WiFi TDOA レシーバの追加、配置、および削除 225
カバレッジ領域の追加 227
障害物の作成 228

マーカーの配置 229
ロケーション リージョンの作成 229
フロア上の包含リージョンの定義 230
フロア上の除外リージョンの定義 231
ロケーション リージョンの編集 231
ロケーション リージョンの削除 232
レールの作成 232
GPS マーカーの配置 233
フロア ツールの使用 234
検出された不正 AP の表示 234
モニタリング ツールの使用 234
チャートの表示 234
クライアント プレイバックの使用によるクライアントの移動の追跡 235
位置の準備状態の調査 235
音声準備状況の検査 236
RF キャリブレーション方法 237
ワイヤレス マップで使用される RF キャリブレーション モデルの調整 237
新しい RF キャリブレーション モデルの作成 238
新しい RF キャリブレーション モデルの調整、コンピューティング、適用 239
新しい RF キャリブレーション モデルの収集された「ライブ」データ ポイントの計算 241
ワイヤレス サイト マップのフロアへの完全調整された RF キャリブレーション モデルの適用 242
RF キャリブレーション モデルの削除 242
RF キャリブレーション モデルのプロパティの表示 243
ワイヤレス サイト マップへの RF キャリブレーション モデルの適用 243
プランニング モードの使用 244
ワイヤレス サイト マップ エディタの機能 245
ワイヤレス サイト マップ エディタの使用に関するガイドライン 245
アクセス ポイントの配置に関するガイドライン 246
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 248
ワイヤレス サイト マップ エディタの起動と使用 248

ワイヤレス サイト マップ エディタのアイコン 249
ワイヤレス サイト マップでのカバレッジ領域の定義 250
ワイヤレス サイト マップにおける障害物のカラー コーディング 250
ワイヤレス サイト マップでの包含リージョンの定義 251
ワイヤレス サイト マップでの除外リージョンの定義 252
ワイヤレス サイト マップでのレール ラインの定義 253
ワイヤレス サイト マップの検索 254
ワイヤレス サイト マップ エディタを使用した RF アンテナの調整 255
AP ロケーション準備状況を使用した低カバレッジ領域の検索 255
RF キャリブレーション データを使用した AP カバレッジの品質評価 256
RF カバレッジが音声対応に十分かどうかの判断 257
有線デバイス情報の表示 258
干渉源通知の設定 258
表示/非表示 259
PDF へのエクスポート 259
距離の測定 259
データのフィルタリング 259
アクセス ポイント データのフィルタリング 259
クライアント データのフィルタリング 260
タグ データのフィルタリング 261
不正な ap 通信データのフィルタ リング 261
アドホックの不正なデータをフィルタ リング 261
干渉源データのフィルタリング 262
アクセス ポイント ヒートマップ データのフィルタリング 262
プランニング モードを使用したワイヤレス ワイト マップでの AP の配置 263
プランニング モードを使用したアクセス ポイント カバレッジ要件の計算 264
ワイヤレス サイト マップの更新設定の構成 265
RF ヒートマップの計算方法 266
[フロアビュー（Floor View）] ナビゲーション ウィンドウのツール 267
自動階層作成を使用したワイヤレス サイト マップの作成 268
ワイヤレス サイト マップでの Google Earth マップの表示 271

ワイヤレス サイト マップでの Google Earth マップ詳細の表示 271
地理座標を使用したワイヤレス サイト マップ上の屋外位置への AP のグループ化 272
地理座標を使用して屋外位置を作成するための前提条件 272
Google Earth を使用してワイヤレス サイト マップ上の屋外位置に地理座標をインポートする 273
ワイヤレス サイト マップで使用される KML ファイルの目印の作成 274
ワイヤレス サイト マップに地理座標をインポートするための CSV ファイルの作成 275
ワイヤレス サイト マップで屋外位置を作成するための地理座標ファイルのインポート 276
Google Earth のロケーション起動ポイントをアクセス ポイントの詳細に追加する 277
Google Earth のマップ設定 277
マップを使用したメッシュ アクセス ポイントのモニタ 278
ワイヤレス サイト マップを使用したメッシュ アクセス ポイント構成の表示 279
ワイヤレス サイト マップでのデバイス詳細の表示 279
ワイヤレス ネットワーク サイト マップとは 279
簡単なワイヤレス ネットワーク サイト マップの作成 280

第 IV 部 : ネットワークの監視 281

第 11 章 ネットワーク モニタリングのセットアップ 283
ポートおよびインターフェイス モニタリングのセットアップ 283
WAN インターフェイス モニタリングのセットアップ 284
Cisco ISE を使用した拡張ワイヤレス クライアント モニタリングのセットアップ 284
Cisco アイデンティティ サービス エンジンの追加 285
パフォーマンスのモニタリングを目的とした NAM および NetFlow データ収集のセットアップ 286
NAM データ収集の有効化 286
NAM ポーリング パラメータの定義 286
NetFlow データ収集の有効化 287
Catalyst 2000 スイッチにおける NetFlow エクスポートの設定 291
Catalyst 3000、4000、6000 スイッチ ファミリにおける NetFlow の設定 293
ISR デバイスにおける NetFlow の設定 294

第 12 章 デバイスのモニタリング 297

ネットワーク トラフィックをモニタするパケット キャプチャのセットアップ 297

ジョブ ダッシュボードを使用したジョブの管理 299

第 13 章 ワイヤレス デバイスのモニタ 303

コントローラのモニタ 303

システム パラメータのモニタ 303

スパニング ツリー プロトコルとは 306

管理フレーム保護とは 306

不正アクセス ポイント ルールとは 306

サードパーティ製コントローラに関するシステム詳細の表示 307

スイッチ コントローラに関するシステム詳細の表示とスイッチ リストの設定 307

[スイッチリスト（Switch List）] ページの設定 307

モニタ アクセス ポイント 308

アクセス ポイントの表示 308

アクセス ポイントのレポート タイプ 309

アクセス ポイントに関するシステムの詳細の表示 311

アクセス ポイント無線 Air Time Fairness 情報の表示 312

不正アクセス ポイントとは 313

Cisco Prime Infrastructure が不正アクセス ポイントを検出する仕組み 314

不正アクセス ポイント状態の判断方法 315

不正アクセス ポイントの分類方法 316

不正アクセス ポイント アラームの表示 318

不正アクセス ポイント クライアントの表示 319

アドホック不正とは 320

アドホック不正アクセス ポイント アラームの表示 320

Prime Infrastructure が不正アクセス ポイントを検索、タグ付け、および包含する方法 321

不正アクセス ポイントを検出する Lightweight アクセス ポイントの識別 322

Spectrum Expert からのアクセス ポイント干渉情報の表示 322

WiFi TDOA レシーバのモニタ 323

[無線リソース管理（Radio Resource Management Dashboard）] ダッシュボードを使用した RF パフォーマンスの表示 323
アクセス ポイントのアラームとイベントの表示 324
アクセス ポイント障害オブジェクトの表示 324
アクセス ポイントの不正アクセス ポイントの表示 324
アクセス ポイントのアドホック不正の表示 325
アクセス ポイントの適応型 wIPS イベントの表示 325
アクセス ポイントの CleanAir 電波品質イベントの表示 325
アクセス ポイントの干渉源セキュリティ リスク イベントの表示 326
アクセス ポイントのヘルス モニタ イベントの表示 326
ヘルス モニタ イベントの詳細の表示 326

第 14 章 デバイスおよびネットワークの健全性とパフォーマンスのモニタ 327
デバイスのヘルスとパフォーマンスのモニタ方法：モニタリング ポリシー 327
基本的なデバイス ヘルス モニタリングのセットアップ 329
基本的なインターフェイス モニタリングの設定 329
デフォルトのモニタリング ポリシー 330
デフォルトのモニタリング ポリシーの変更 333
ダッシュボードを使用したネットワークとデバイスの状態の確認 334
Prime Infrastructure によるモニタリング対象のチェック 334
モニタリング ポリシーによりポーリングされるパラメータとカウンタの確認 337
モニタリング ポリシーのデバイス、ポーリング、しきい値、およびアラーム設定の確認 337
モニタ対象を調整する 338
既存のポリシー ベースの新規モニタリング ポリシーの作成 339
事前設定されたポリシー タイプを使用した新規モニタリング ポリシーの作成 340
GETVPN モニタリング ポリシー 340
DMVPN モニタリング ポリシー 344
LISP モニタリング ポリシー 345
Nexus 仮想ポート チャネル（VPC）のヘルス モニタリング ポリシー 345
サポートされないパラメータとサードパーティ デバイスを対象としたモニタリング ポリシーの作成 346

例：IP SLA のモニタ 347
過去のモニタリング ポリシー データ収集のステータスの確認 348
ポリシーでモニタするデバイス セットの変更 348
モニタリング ポリシーのポーリングの変更 349
モニタリング ポリシーのしきい値およびアラーム動作の変更 349
レポートを使用したネットワーク パフォーマンスのモニタ 352

第 15 章 アラームとイベントのモニタリング 353
アラームおよびイベントとは 353
アラームおよびイベントはどのように作成および更新しますか。 354
リンク アップ/ダウン フラッピング 356
アラームの検索および表示 356
既存のアラームの抑制 358
既存のアラームの重大度の変更 359
アラームとイベント管理の設定 360
アラームとイベントの表示設定のセットアップ 360
アラーム サマリーのカスタマイズ 363
イベントとアラームのバッジと色の解釈 364
アラーム重大度アイコン 364
トラブルシューティングと詳細なアラーム情報の取得 364
アラームの詳細を表示する 364
アクティブ アラームのトラブルシューティング情報の検索 365
アラームに関連付けられているイベントの検索 365
アラームの確認とクリア 366
未確認 366
確認済み 366
クリア済み 366
アラームへの注釈の追加 367
アラームがトリガーされる方法の管理（アラームしきい値） 368
サポートされるイベント 368
イベントの表示 369

Syslog ポリシーの表示 370
新しい syslog ポリシーの作成 370
Syslog ポリシーの編集 372
syslog ポリシーの削除 372
Syslog ポリシー ランクを変更します 372
Syslog の表示 373
CSV ファイルまたは PDF ファイルへのアラーム、イベント、または syslog のエクスポート 374
アラーム、イベント、および Syslog レポートの操作 374
新しいアラームレポートを作成する 374
新しいイベントレポートを作成する 375
新しい Syslog レポートの作成 377
シスコからサポートを受ける 378
Prime Infrastructure 内の問題への対応 378
アラーム ポリシーとは 378
アラーム ポリシーのタイプ 379
アラーム ポリシーのランク 380
アラーム ポリシーの表示 381
新しいアラーム ポリシーの作成 381
既存のアラーム ポリシーの編集 383
アラーム ポリシーの削除 383
アラームおよびイベントの通知ポリシー 384

第 16 章 ネットワーク クライアントとユーザのモニタ 385
ネットワーク有線/ワイヤレス クライアントとは 385
クライアントサマリ ダッシュボードを使用したネットワーク ユーザーおよびクライアントのモニタ 387
ネットワーク クライアントとユーザを表示する方法 388
ネットワーク クライアントとユーザのリストを CSV ファイルにエクスポートする 390
ネットワーク クライアント トラブルシューティング ツールの起動 391
[クライアントのトラブルシューティング（Client Troubleshooting）] ページについて 391

クライアント トラブルシューティング ツールによるヒントの仕組み 393
ネットワーク クライアント トラブルシューティング ツールを使用する方法 396
RTTS のデバッグ コマンド 402
ネットワーク クライアントの接続時の確認 404
ネットワークに接続しているクライアントに関する通知のセットアップ 405
不明なネットワーク ユーザの識別 406
不明ネットワーク ユーザのリストのインポート 407
不明ネットワーク ユーザのリストのエクスポート 408
[コントローラクライアントとユーザ（Controller Client and Users）] ページのカスタマイズ 409
診断チャネルでの自動コントローラ クライアント トラブルシューティングのセットアップ 410
ワイヤレス ネットワーク クライアントの無線測定値の取得 410
ネットワーク クライアント無線測定結果の表示 411
ネットワーク クライアント V5 の統計情報を表示するためのテストの実行 411
ネットワーク クライアントの動作パラメータを表示するためのテストの実行 413
ネットワーク クライアントの詳細の表示 415
ネットワーク クライアントの無効化 416
Prime Infrastructure からのネットワーク クライアントの削除 417
ワイヤレス マップでのネットワーク クライアントの検索 417
レポートを使用したネットワーク クライアント ローミングの表示 418
ネットワーク クライアントを聞くことができるアクセス ポイントの特定 419
ネットワーク クライアントのロケーション履歴の表示 419

第 17 章 **PfRv3 モニタリングを使用したネットワーク パフォーマンスのモニタ 421**
PfRv3 とは 421
ユーザ グループの PfR モニタリングへのアクセス 422
[PfRモニタリング（PfR Monitoring）] ページの使用 422
PfRv3 サービス プロバイダーおよび DSCP チャートの表示 426
PfRv3 を使用したサイト間イベントに関する詳細の表示 427
PfRv3 を使用した WAN インターフェイスの使用状況の比較 430

第 18 章 ワイヤレス ネットワークのモニタ 431

無線リソース管理（RRM）とは 431

Prime Infrastructure に送信される RRM 通知 432

[RRM] ダッシュボードを使用した AP のモニタ 433

AP 干渉源の表示 434

[APが検出した干渉源（AP Detected Interferers）] ページの編集 435

RFID タグ付き AP の表示 436

RFID タグの検索 436

RFID タグの検索結果の確認 437

タグ リストの表示 437

ワイヤレス メディア ストリームのモニタ 438

非結合 AP のトラブルシューティング 438

低周波送信 AP デバイス（チョークポイント）の識別 439

Prime Infrastructure への AP チョークポイントの追加 439

Prime Infrastructure からの AP チョークポイントの削除 440

Prime Infrastructure マップからのチョークポイントの削除 440

AP チョークポイントの編集 440

WiFi TDOA レシーバによるタグ位置レポートの強化 441

MSE への WiFi TDOA レシーバの追加 442

Cisco Prime Infrastructure およびマップへの WiFi TDOA レシーバの追加 442

第 19 章 モニタリング ツールの使用 445

ワイヤレス コントローラの音声監査の実行 445

音声診断ツールを使用した AP パフォーマンスの確認 446

ワイヤレス設定の監査 447

Lightweight AP に移行できる自律 AP の決定 447

ロケーション精度ツールによる AP ロケーション精度の確保 448

AP ロケーション精度ツールのセットアップ 448

ロケーション精度テストのスケジューリング 449

オンデマンド ロケーション精度テストの実行 451

IPSLA のモニタリング 453

第 20 章 パフォーマンス グラフを使用したワイヤレスおよびデータセンターのパフォーマンスのモニタ 455

パフォーマンス グラフの作成 455

1 つのパフォーマンス グラフにおける複数のメトリックの表示 456

パフォーマンス グラフのオプション 457

第 21 章 トラブルシューティング 459

シスコ サポート コミュニティとテクニカル アシスタンス センター（TAC）から支援を受ける 459

シスコ サポート ケースの登録 459

シスコ サポート コミュニティへの参加 460

ユーザの問題に関するトラブルシューティング 461

アプリケーションとそのパフォーマンスのモニタ 465

ワイヤレス デバイスのパフォーマンスの問題のトラブルシューティング 465

物理および仮想データセンター コンポーネントの根本原因およびインパクト分析 466

UCS デバイスのハードウェアの問題のトラブルシューティング 466

UCS デバイスの帯域幅の問題のトラブルシューティング 468

第 22 章 オペレーション センターを使用した複数の Prime Infrastructure インスタンスのモニタ 469

複数の Cisco Prime Infrastructure インスタンスのモニタ方法 469

オペレーション センターの構成ダッシュボードを使用した複数の Cisco Prime Infrastructure サーバの管理 470

オペレーション センターを使用したデバイスの追加 471

1 つの Prime Infrastructure インスタンスから別の Prime Infrastructure インスタンスへのデバイスの移動 472

オペレーション センターによるすべての Cisco Prime Infrastructure サーバの管理対象デバイスの表示 472

オペレーション センターを使用したデバイスの同期 473

オペレーション センターを使用した複数の Cisco Prime Infrastructure サーバを含む展開での仮想ドメインの使用 474

Cisco Prime Infrastructure への仮想ドメインの配布 475
オペレーション センター RBAC サポートの有効化 475
オペレーション センターを使用した Prime Infrastructure サーバ間のデバイス設定テンプレートの共有 476
オペレーション センターを使用した設定テンプレートの表示 476
オペレーション センターを使用した設定テンプレートの展開 477
管理対象サーバへの設定テンプレートの配布 477
オペレーション センターを使用した Prime Infrastructure サーバの管理 478
オペレーション センターを使用した複数の Prime Infrastructure サーバのステータスの表示 479
スマート ライセンシングを使用したオペレーションのアクティベート 480
オペレーション センターで管理されている Prime Infrastructure インスタンスにソフトウェア更新を配信します 480
オペレーション センターによる複数の Cisco Prime Infrastructure サーバによって管理されるデバイスでのアラームの表示 481
オペレーション センターによる複数の Cisco Prime Infrastructure サーバの管理対象クライアントおよびユーザの表示 482
オペレーション センターを使用した複数の Cisco Prime Infrastructure サーバを含む展開でのレポートの実行 482

第 23 章 高度なモニタリング 485
サイト ダッシュレットで使用されるデータ ソースとは 485
WAN 最適化の有効化 487

第 24 章 レポートの管理 489
レポートの概要 489
新しいレポートの作成、スケジュール設定、実行 490
Prime Infrastructure でのレポートの結合 492
カスタム レポートの作成 493
レポート結果のカスタマイズ 496
Cisco Prime Infrastructure でスケジュール設定されたレポート 496
保存済みレポートのテンプレート 499

Prime Infrastructure レポートのデータ保持期間 500

第 V 部 : デバイスの設定 501

第 25 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 503

新しい設定テンプレートを作成する理由 504

Prime Infrastructure を使用して設定テンプレートを作成する方法 504

既存のテンプレートを使用した新機能およびテクノロジー テンプレートの作成 505

CLI テンプレートを作成するための前提条件 506

空白テンプレートを使用した新しい CLI 設定テンプレートの作成 506

既存のテンプレートを使用した新規 CLI 設定テンプレートの作成 507

例 : CLI テンプレートを使用したパスワードの更新 508

テンプレートへの変数の入力 509

データ型 509

CLI テンプレートのデータベース変数の管理 510

検証式の使用 511

マルチライン コマンドの追加 511

イネーブル モード コマンドの追加 512

CLI 設定テンプレートのインポートとエクスポート 513

新規複合テンプレートの作成 514

タグを使用したテンプレートへのショートカットの作成 514

デバイスへのテンプレートの展開 515

デバイスのグループにテンプレートを展開するための設定グループの作成 515

ウィザードを使用した設定グループの展開フロー 516

ウィザードを使用した CLI テンプレートの展開フロー 517

インタラクティブ コマンドの追加 520

ウィザードを使用した複合テンプレートの展開フロー 522

設定グループを使用しないデバイスへのテンプレートの展開 524

設定テンプレートを使用したコントローラの設定 524

コントローラ テンプレートの作成 525

コントローラ WLAN クライアント プロファイルの設定 528

モバイル コンシェルジュ（802.11u）を使用するようにコントローラを設定する 529
AP グループを使用した WLAN 構成と展開の管理 530
WLAN AP グループ テンプレートの作成 530
WLAN AP グループの削除 531
WLAN AP グループの追加 531
リモート LAN（RLAN）テンプレートの作成 532
AP グループへのリモート LAN（RLAN）のマッピング 533
FlexConnect AP グループでの FlexConnect ユーザの構成 533
デバイスベースおよびユーザベースのコントローラ ポリシーの設定 534
設定テンプレートを使用したコントローラでの AAA の設定 534
コントローラへのユーザ アクセスを制御するための RADIUS 認証サーバの設定 535
コントローラでの RADIUS および TACACS サーバ フォールバック設定の構成 535
ローカル EAP タイムアウト設定の構成 536
LDAP とローカル データベースを使用してコントローラへのユーザ アクセスを制御する場合の認証順序の設定 537
コントローラのユーザ認証に使用するクレデンシャルの設定（ローカル ネットワーク テンプレート） 537
ユーザが同時に実行できるログイン セッション数の制御 538
MAC アドレスでフィルタするための AP の設定 538
AP または MSE コントローラ認証の設定 539
MAC アドレスでクライアントを手動で無効化するためのコントローラの設定 540
コントローラのクライアント除外ポリシーの設定 540
MFP を使用した AP 認証の設定 541
コントローラ WLAN の Web 認証の認証タイプを設定する 542
コントローラへのカスタマイズされた Web 認証ページのダウンロード 543
コントローラの外部 Web 認証サーバの設定 545
コントローラのパスワード ポリシーの設定 545
コントローラ テンプレートの適用 546
コントローラのアクセス コントロール リストの設定 547
コントローラでのトラフィックを制御するための FlexConnect アクセス コントロール リストの設定 550
FlexConnect グループの一括更新の管理 552

FlexConnect グループの一括作成 552
一括で FlexConnect グループへのユーザーの追加 553
一括で FlexConnect グループへの AP の追加 555
コントローラ CPU と NPU 間のアクセス コントロール リスト トラフィック制御の設定 556
コントローラでの不正 AP およびクライアント セキュリティ ポリシーの設定 557
コントローラの不正 AP 分類ルールの定義 558
不正 AP ルール グループでの複数のコントローラ不正 AP ルールの組み合わせ 559
展開された不正 AP ルールの表示 559
コントローラの SIP スヌーピングの設定 560
管理テンプレートの作成 560
Cisco Prime Infrastructure で Microsoft LyncSDN を使用する 561
Microsoft LyncSDN 診断を使用するためのコントローラの設定 561
ネットワーク トラフィックの QoS をモニタする Microsoft LyncSDN ポリシーを使用するためのコントローラの設定 562
Microsoft LyncSDN WLAN プロファイルを使用するためのコントローラの設定 562
コントローラでのアプリケーション分類用 AVC プロファイルの設定 563
NetFlow を使用するためのデバイスの設定 564
コントローラでの Ethernet over GRE（EoGRE）トンネルの設定 565
テンプレートを使用した Lightweight AP の設定 566
AP テンプレート展開のための AP ソースの選択 566
テンプレートを使用した自律 AP の設定 567
テンプレートを使用したスイッチの場所情報の設定 567
AP 移行テンプレートを使用した Autonomous アクセス ポイントから Lightweight アクセス ポイントへの移行 568
自律 AP 移行の影響の分析 568
設定テンプレートの展開 569
モデルベースの設定テンプレートの展開フロー 571
グローバル変数 572
共有ポリシー オブジェクト 572
インターフェイス ロールの定義 573
ネットワーク オブジェクトの定義 573

セキュリティ ルール パラメータ マップの作成 574
セキュリティ サービス グループの作成 575
セキュリティ ゾーンの作成 575
設定グループとは 576
ユーザ定義グループを使用した NE グループへの変更の適用 576
WLAN コントローラ設定グループとは 577
コントローラ設定グループを作成し、それらに設定テンプレートを適用する 577
コントローラ設定グループでのコントローラの追加または削除 579
コントローラ設定グループへの DCA チャネルの設定 579
コントローラ設定グループへのテンプレート展開のスケジュール設定 580
コンプライアンスを確保するためのコントローラ設定グループの監査 581
設定グループのリブート 582
コントローラ設定グループへのテンプレート展開ステータスの表示 582
ワイヤレス設定テンプレートの作成 583
設定テンプレートを使用した Lightweight AP の設定 583
AP へのデバイス ベース ポリシーの設定 584

第 26 章 ワイヤレス デバイスの設定 587
Cisco Prime Infrastructure でのコントローラの表示 589
設定テンプレートの展開のためのコントローラ固有のコマンド 590
コントローラで使用されている設定テンプレートの確認と関連付けの削除 592
[ネットワークデバイス（Network Devices）]テーブルからのコントローラ クレデンシャルの変更 592
レポートでのコントローラ監査結果の表示 593
インポートした CSV ファイルを使用したコントローラ クレデンシャルの変更 594
再起動によるコントローラ変更の適用 595
コントローラへのソフトウェアのダウンロード 595
FTP/TFTP サーバへのコントローラ設定とログ ファイルのアップロード 597
コントローラへの IDS シグネチャのダウンロード 597
コントローラへの圧縮された Web 認証ログイン ページ情報のダウンロード 598
コントローラへのベンダー デバイス証明書のダウンロード 599

TFTP を介したコントローラへのベンダー デバイス証明書のダウンロード 600
コントローラへの CA 証明書のダウンロード 600
ネットワーク アシュアランスの設定 601
デバイス公開証明書のダウンロードおよびインストール 601
ネットワーク アシュアランスの自己署名付き証明書を生成 602
コントローラへの NA サーバ CA 証明書のダウンロード 604
デバイス フラッシュへのコントローラ設定の保存 605
データベースへのコントローラ設定の保存（同期） 606
コントローラの既存のテンプレートを検出 606
コントローラに適用されているテンプレートの表示 607
IP アドレスを保持したままのコントローラ交換 608
コントローラ プロパティの変更 608
[ネットワークデバイス（Network Devices）]テーブルからコントローラの一般システム プロパティを変更する 608
コントローラで障害が発生した場合の AP への優先順位の割り当て 609
コントローラでの 802.3 ブリッジングの設定 609
コントローラでの 802.3 フロー制御の設定 610
[ネットワーク デバイス（Network Devices）] テーブルからの Lightweight AP Protocol 転送モードの設定 610
アグレッシブ ロード バランシングとは 611
リンク アグリゲーションとは 612
ワイヤレス管理の前提条件 612
モビリティ アンカー キープアライブ間隔とは 612
コントローラの設定ファイルおよびログ ファイルを TFTP サーバにアップロードする 613
コントローラへのソフトウェアのダウンロード 613
単一コントローラでのインターフェイスの設定 614
コントローラでのインターフェイスの表示 615
コントローラからの動的インターフェイスの削除 615
コントローラ システム インターフェイス グループを使用したコントローラ グループへのインターフェイス変更の適用 616
コントローラ インターフェイス グループの表示と管理 616
NAC アプライアンスを使用したコントローラへのユーザ アクセスの制御 617

SNMP NAC の使用時の前提条件 618
RADIUS NAC の使用時の前提条件 619
コントローラでの SNMP NAC の設定 619
検疫 VLAN の設定（SNMP NAC） 619
WLAN またはゲスト LAN での NAC の有効化（SNMP NAC） 620
ネットワーク クライアントまたはユーザの NAC 状態の表示 621
有線コントローラへのゲスト アカウント アクセスの設定 621
有線ゲスト ユーザ アクセスの設定と有効化：ワークフロー 622
有線ゲスト ユーザ アクセス用の動的インターフェイスの設定 622
ゲスト ユーザ アクセス用の有線 LAN の設定 623
コントローラでのゲスト LAN 入力インターフェイスの設定 624
コントローラでのゲスト LAN 出力インターフェイスの設定 625
コントローラ サービス ポートでのネットワーク ルートの設定 626
既存のコントローラ ネットワーク ルートの表示 626
コントローラへのネットワーク ルートの追加 626
コントローラの STP パラメータの表示 627
モビリティとは 628
コントローラ内ローミングとは 628
コントローラ間ローミングとは 629
サブネット間ローミングとは 630
対称トンネリングとは 632
モビリティ グループとは 632
コントローラをモビリティ グループに追加するための前提条件 634
コントローラのモビリティ グループ メッセージングの仕組み 635
モビリティ グループの設定：ワークフロー 636
コントローラをモビリティ グループに追加するための前提条件 636
モビリティ グループに属しているコントローラの表示 637
[ネットワークデバイス（Network Devices）] テーブルからコントローラをモビリティ グループに追加する 637
コントローラへの NTP サーバの追加 638
メッシュ ネットワーク バック グラウンド スキャン用のコント ローラーを構成します。 638

メッシュ ネットワーク バックグラウンド スキャンのシナリオ 639
コントローラでのメッシュ ネットワーク バックグラウンド スキャンの有効化 641
コントローラ QoS プロファイルの設定 641
内部 DHCP サーバに関する情報 642
現在の DHCP スコープの表示 642
DHCP スコープの設定 643
DHCP スコープの削除 644
DHCP スコープの詳細のエクスポート 645
コントローラのユーザ認証に使用されるコントローラのローカル ネットワーク テンプレートの表示 646
コントローラのユーザ認証に使用されるコントローラのローカル ネットワーク テンプレートの設定 646
コントローラに接続する AP のコントローラ ユーザ名とパスワードの設定 647
コントローラでの CDP の設定 647
コントローラへの 802.1X 認証の設定 648
コントローラへの 802.1X 認証の設定 649
コントローラでの DHCP の設定 650
障害検出時間を短縮するコントローラの拡張タイマーの設定 651
コントローラでの WLAN の作成 652
コントローラで構成されている WLAN の表示 652
コントローラ上の WLAN へのセキュリティ ポリシーの追加 653
コントローラでのモバイル コンシェルジュ（802.11u）の設定 654
コントローラへの WLAN の追加 657
コントローラからの WLAN の削除 657
コントローラの WLAN の管理ステータスを変更する 658
コントローラ WLAN のモビリティ アンカーの表示 659
802.11r 高速移行の設定 660
Fastlane QoS の設定 662
Fastlane QoS の無効化 662
コントローラの WLAN AP グループの設定 663
コントローラの WLAN AP グループの作成 664

コントローラの WLAN AP グループの削除 666
構成の違いを特定するためのコントローラ WLAN AP グループの監査 666
キャプティブ ポータル バイパスに関する情報 667
キャプティブ ネットワーク ポータル バイパスの設定 668
WLAN ごとのキャプティブ ネットワーク ポータル バイパスの設定 668
FlexConnect を使用した AP の設定とモニタ 669
FlexConnect がサポートされるデバイス 669
FlexConnect の使用時の前提条件 670
FlexConnect が認証を実行する仕組み 671
FlexConnect 動作モード：[接続中（Connected）] および [スタンドアロン（Standalone）] 671
FlexConnect の状態 672
FlexConnect の設定方法と使用方法：ワークフロー 673
FlexConnect のリモート スイッチの設定 674
例：リモート サイトでスイッチに FlexConnect を設定する 674
FlexConnect 用の中央でスイッチングされる WLAN コントローラの設定 675
FlexConnect 用のローカルでスイッチングされる WLAN コントローラの設定 676
ゲスト アクセス用の中央でスイッチングされる WLAN コントローラの設定 676
中央でスイッチングされる WLAN へのゲストの追加（FlexConnect） 677
AP での FlexConnect の設定 678
クライアント デバイスの WLAN への接続（FlexConnect） 678
FlexConnect で使用する AP グループの作成 679
FlexConnect グループおよびバックアップ RADIUS サーバ 680
FlexConnect グループおよび CCKM 680
FlexConnect グループおよびローカル認証 681
既存の FlexConnect AP グループの表示 682
FlexConnect AP グループの設定 682
構成の違いを特定するためのコントローラ FlexConnect AP グループの監査 683
デフォルト FlexConnect グループ 683
デフォルトの FlexConnect AP グループから別の FlexConnect グループへの AP の移動 684
FlexConnect AP グループの削除 685

コントローラまたはデバイスのセキュリティ設定の構成 685
コントローラへの AAA セキュリティの設定 686
コントローラの AAA 一般パラメータの設定 686
コントローラの AAA RADIUS 認証サーバの表示 687
コントローラへの AAA 認証サーバの追加 687
コントローラの AAA RADIUS アカウンティング サーバの表示 688
コントローラへの AAA アカウンティング サーバの追加 688
コントローラからの AAA アカウンティング サーバの削除 689
コントローラでの AAA RADIUS フォールバック パラメータの設定 689
コントローラでの AAA LDAP サーバの設定 690
コントローラへの AAA LDAP サーバの追加 690
コントローラからの AAA LDAP サーバの削除 691
コントローラでの AAA TACACS サーバの設定 691
コントローラの AAA ローカル ネット ユーザの表示 692
コントローラからの AAA ローカル ネット ユーザの削除 693
コントローラでの AAA MAC フィルタリングの設定 693
コントローラでの AAA AP/MSE 認証の設定 694
コントローラでの AAA AP/MSE ポリシーの編集 695
コントローラでの AAA Web 認証の設定 695
コントローラでの AAA パスワード ポリシーの設定 696
コントローラでのローカル EAP の設定 697
コントローラでのローカル EAP 一般パラメータの設定 697
コントローラで使用されるローカル EAP プロファイルの表示 698
コントローラへのローカル EAP プロファイルの追加 699
コントローラでのローカル EAP 一般ネットワーク ユーザ優先度の設定 700
コントローラの Web 認証証明書の設定 700
コントローラのユーザ ログイン ポリシーの設定 701
デバイスの手動で無効化されるクライアントの設定 701
コントローラのアクセス コントロール リスト（ACL）の設定 702
コントローラ ACL ルールの設定 702
新しいコントローラの ACL ルールの作成 702

コントローラの FlexConnect ACL セキュリティの設定 703
コントローラでの FlexConnect ACL の追加 703
コントローラの FlexConnect ACL の削除 704
コントローラ CPU 用の ACL セキュリティの追加 704
コントローラの設定済み IDS セキュリティ センサーの表示 704
コントローラでの IP Sec CA 証明書の設定 705
コントローラへの IP Sec 証明書のインポート 705
コントローラへの IP Sec 証明書の貼り付け 705
コントローラでのネットワーク アイデンティティ（ID）証明書の設定 706
コントローラへの ID 証明書のインポート 706
コントローラへの ID 証明書の貼り付け 707
コントローラでのワイヤレス保護ポリシーの設定 707
コントローラでの不正 AP ポリシーの設定 707
コントローラでの不正 AP ポリシーの表示 709
コントローラでのクライアント除外ポリシーの設定 709
デバイスの IDS 署名の設定 710
コントローラに適用されるシスコが提供する IDS 署名の表示 711
コントローラへの IDS 署名ファイルのダウンロード 711
コントローラからの IDS 署名ファイルのアップロード 712
コントローラ上のすべての IDS 署名の有効化と無効化 713
コントローラでの単一の IDS シグニチャの有効化と無効化 714
カスタム IDS 署名の作成 715
コントローラの AP 認証と管理フレーム保護の設定 716
URL ACL の構成 717
アクセス コントロール リストの設定 718
URL ACL の削除 718
フレキシブル ラジオ アサインメント 719
フレキシブル ラジオ アサインメントの設定 719
デバイスの 802.11 パラメータの設定 720
802.11 コントローラでの複数の国コードの設定 721

どのようなときにコントローラが追加のクライアント アソシエーションを受け入れられなくなるかの指定（AP ロード バランシング） 721
AP チャネル干渉を抑えるバンド選択の有効化 723
SIP コールの優先度の制御 724
MediaStream を使用した IP マルチキャスト配信の確保 725
AP グループで使用できる RF プロファイルの作成 726
デバイスの 802.11a/n パラメータの設定 727
デバイスの 802.11b/g/n パラメータの設定 728
デバイスのメッシュ パラメータの設定 729
1524 SB AP でのバックホール無線へのクライアント アクセスの無効化 731
コントローラでのバックホール チャネル選択解除の有効化 732
デバイスのポート パラメータの設定 733
コントローラの管理パラメータの設定 734
コントローラのトラップ レシーバの設定 734
コントローラ トラップの設定 735
コントローラの Telnet SSH セッション パラメータの設定 737
コントローラでの Syslog サーバの設定 738
ネットワーク アシュアランスの設定 739
コントローラでの Web 管理の設定 740
コントローラでのローカル管理ユーザの設定 741
コントローラの管理認証サーバ優先度の設定 742
コントローラのロケーション情報の設定 743
コントローラの IPv6 ネイバー バインドと RA パラメータの設定 745
コントローラのネイバー バインド タイマーの設定 745
コントローラでのルータ アドバタイズメント スロットリングの設定 746
コントローラでの RA ガードの設定 747
コントローラのプロキシ モバイル IPv6（PMIP）パラメータの設定 747
コントローラでの PMIP グローバル パラメータの設定 747
コントローラでの PMIP ローカル モビリティ アンカーの設定 749
コントローラでの PMIP プロファイルの設定 749
コントローラの EoGRE トンネリングの設定 750

コントローラのマルチキャスト DNS（mDNS）設定の構成 751
コントローラの Application Visibility and Control（AVC）パラメータの設定 753
コントローラでの AVC プロファイルの設定 753
コントローラの NetFlow 設定の構成 755
コントローラでの NetFlow モニタの設定 755
コントローラでの NetFlow エクスポータの設定 756
サードパーティ製コントローラまたはアクセス ポイントの設定 757
サードパーティ製コントローラの追加 757
サードパーティ製コントローラの動作ステータスの表示 758
サードパーティ アクセス ポイントの設定の表示 759
サードパーティ アクセス ポイントの削除 759
サードパーティ アクセス ポイントの動作ステータスの表示 760
スイッチ設定の表示 761
スイッチの詳細の表示 761
スイッチの SNMP パラメータの変更 761
スイッチの Telnet/SSH クレデンシャルの変更 762
スイッチの追加 762
例：スイッチでの SNMPv3 の設定 764
CSV ファイルからのスイッチのインポート 764
スイッチの削除 765
例：有線クライアントのスイッチ トラップと Syslog の設定 765
例：IOS を使用した Catalyst スイッチの Syslog 転送の設定 766
Cisco Prime Infrastructure での Cisco OfficeExtend AP の使用 766
AP とコントローラ間のリンクを測定するためのリンク遅延の設定 767
ユニファイド AP の設定 768
ユニファイド アクセス ポイントで Sniffer 機能を有効にする（AiroPeek） 768
リモート マシンでの AiroPeek スニファの設定 769
Cisco Prime Infrastructure を使用したスニファ モードでの AP の設定 770
AP での Flex+Bridge モードの有効化 770
コントローラ冗長性の設定 771
脅威からコントローラを保護するための Cisco Adaptive wIPS の設定 771

wIPS プロファイルの表示 772
wIPS プロファイルの追加 772
wIPS プロファイルの編集 773
wIPS プロファイルの適用 775
wIPS プロファイルの削除 776
SSID グループと wIPS プロファイルの関連付け 776
SSID グループの作成 777
SSID グループの編集 777
SSID グループの削除 777
MSE サーバの高可用性の設定 778
MSE HA サーバのフェールオーバーとフェールバック 778
MSE HA サーバの構成 779
プライマリおよびセカンダリ MSE HA サーバに関する詳細の表示 780
MSE サーバの HA ステータスの表示 781
MSE HA の手動フェールオーバーまたはフェールバックのトリガー 782
MSE サーバでの自動 HA フェールオーバーおよびフェールバックの設定 782
MSE HA サーバのペアリング解除 783
プラグ アンド プレイを使用したコントローラの設定 783

第 27 章 ワイヤレス テクノロジーの設定 785
AP 上で最適化されたモニタ モードを使用したタグ付きアセットの追跡 786
ワイヤレス チョークポイントの設定 787
ワイヤレス チョークポイントの作成 787
ネットワークからのワイヤレス チョークポイントの削除 787
統合 AP の管理 788
コンフィギュレーション 788
AP をメンテナンス状態にする 788
メンテナンス状態からの AP の削除 788
スケジューリング（Scheduling） 789
AP 無線ステータス変更のスケジュール設定 789
スケジュール済み AP 無線ステータス変更の表示 789

メンテナンス状態における AP のアラームの表示 790
AP イーサネット インターフェイスの設定 790
CSV ファイルのインポートによる AP の設定 791
アクセス ポイントでの CDP の設定 792
Autonomous AP の管理 792
デバイス情報を使用した自律 AP の追加 792
CSV ファイルを使用した自律 AP の追加 794
CSV ファイルを使用した自律 AP の一括更新 794
自律 AP の一括更新用のサンプル CSV ファイル 794
Prime Infrastructure からの自律 AP の削除 796
自律型 AP の表示 796
TFTP を介した自律 AP へのイメージのダウンロード 796
FTP を介した自律 AP へのイメージのダウンロード 797
ワークグループ ブリッジ（WGB）モードの自律 AP の表示 798
自律 AP の詳細のエクスポート 798
アクセス ポイント XOR アンテナの設定 799
一般 799
無線割り当て 800
アンテナ 800
RF チャネル割り当て 800
11n および 11ac のパラメータ 801
パフォーマンス プロファイル 801
送信電力レベル割り当て 801
11n アンテナ選択 802
[11n] パラメータ 802
AP オンボーディング プロファイルの設定 802
AP オンボーディング プロファイル グループの作成 803
AP オンボーディング プロファイルの編集 804
AP オンボーディング プロファイルの削除 805
アクセス ポイントの検索 805
ワイヤレス設定グループ 807

新しい設定グループの作成 807
ワイヤレス設定グループでのテンプレートの追加または削除 808
ワイヤレス設定グループの監査 809
メッシュ ネットワークにおけるリンクの表示 810
コントローラの不正 AP 分類ルールの定義 811
コントローラの自動プロビジョニングを使用した WLC の追加と置換 811
コントローラ自動プロビジョニング リストの表示 811
コントローラの自動プロビジョニング フィルタの作成 812
コントローラの自動プロビジョニングに使用されるプライマリ キーの検索順序の制御 813
AP オンボーディング プロファイルの設定 813
AP オンボーディング プロファイル グループの作成 814
AP オンボーディング プロファイルの編集 815
AP オンボーディング プロファイル グループの削除 816
9800 シリーズ構成モデルに関する情報 817
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの Cisco Umbrella ポリシーのローカル ドメインの設定 821
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの Cisco Umbrella ポリシーの設定 822
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラに Flex Sxp プロファイルを設定します 822
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラに Flex プロファイルを設定します 823
Catalyst 9800 シリーズ ワイヤレス コントローラの Airtime Fairness の設定 823
Catalyst 9800 シリーズ ワイヤレス コントローラの Airtime Fairness ポリシーの作成 823
ポリシー プロファイルへの Airtime Fairness ポリシーの追加 824
RF プロファイルで ATF ポリシーを有効にする 824
Catalyst 9800 シリーズ ワイヤレス コントローラのリモート LAN（RLAN）の設定 825
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの RLAN プロファイルの作成 825
Catalyst 9800 シリーズ ワイヤレス コントローラの RLAN ポリシー プロファイルの作成 825
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラに WLAN グループを設定します 826
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ上でルールを展開する 826

Cisco AireOS コントローラ設定を Cisco Catalyst 9800 シリーズ コントローラに変換する 827

第 28 章 ワイヤレス/データセンター設定タスクのスケジュール設定 829

スケジュール設定変更の表示 829

スケジュール済み設定変更の表示：アクセス ポイント無線 830

スケジュール設定変更の表示：WLAN 830

コントローラおよび AP へのソフトウェアのダウンロード 831

コントローラと AP へのソフトウェア ダウンロードのスケジュール設定 831

スケジュール済みソフトウェア ダウンロードの変更 833

ソフトウェア ダウンロードに関するコントローラのスケジュール設定 833

第 29 章 プラグ アンド プレイを使用した新しいデバイスの展開 835

プラグ アンド プレイについて 835

プラグ アンド プレイの使用時の前提条件 836

プラグ アンド プレイのワークフロー 836

[プラグアンドプレイ（Plug and Play）] ダッシュボードを使用した新しいデバイス展開のモニタ 838

APIC-EM でプラグ アンド プレイを使用するための前提条件 840

Nexus デバイスでプラグ アンド プレイを使用するための前提条件 840

DHCP サーバの設定 841

HTTP サーバの設定 841

プラグ アンド プレイへの APIC-EM ポリシー情報の統合 842

APIC-EM サイトの同期 843

デバイスの展開を定義するプラグ アンド プレイ プロファイルの作成 844

ルータおよびスイッチのプラグ アンド プレイ プロファイルの作成 845

プラグ アンド プレイ プロファイルのソフトウェア イメージのインポート 847

ワイヤレス AP のプラグ アンド プレイ プロファイルの作成 847

Nexus デバイスのプラグ アンド プレイ プロファイルの作成 848

Mobility Express WLC プラグ アンド プレイ プロファイルの作成 849

デバイスとプラグ アンド プレイ プロファイルの関連付け 850

新しいプラグ アンド プレイ プロファイルの作成とデバイス プロファイルの追加 851

既存のプラグ アンド プレイ プロファイルへのデバイス プロファイルの追加 852
ルータとスイッチのプラグ アンド プレイ プロファイルへのデバイス プロファイルの追加 853
デバイス プロファイルのエクスポート、編集、およびプラグ アンド プレイ プロファイルへのインポート 854
デバイス タイプに基づく展開 855
ワイヤレス AP プラグ アンド プレイ プロファイルへのデバイス プロファイルの追加 856
Nexus プラグ アンド プレイ プロファイルへのデバイス プロファイルの追加 857
Mobility Express WLC プラグ アンド プレイ プロファイル インスタンスへのデバイス プロファイルの追加 858
プラグ アンド プレイ でサポートされるデバイスとソフトウェア イメージ 860
デバイスにブートストラップ コンフィギュレーションを展開するための前提条件 860
プラグ アンド プレイ用のブートストラップ コンフィギュレーションの作成 861
ブートストラップ コンフィギュレーションをインストールする方法 862
ブートストラップ コンフィギュレーションのエクスポート 863
ターミナル サーバを使用したブートストラップ コンフィギュレーションの展開 864
TFTP によるブートストラップ コンフィギュレーションのエクスポート 864
電子メール ブートストラップ コンフィギュレーション 865
ブートストラップ コンフィギュレーションの PIN のメール送信 866
DHCP を使用したブートストラップ コンフィギュレーションのエクスポート 867
サンプル DHCP サーバ設定 867
プラグ アンド プレイを使用して展開されたデバイスの確認 868
マップ ビューと [プラグアンドプレイ（Plug and Play）] ダッシュボードの統合 869
プラグ アンド プレイ プロファイルの削除 871
APIC-EM サーバで削除されたデバイスとプロファイルを取得する方法 872
CNS プロファイルを APIC-EM プロファイルに変換する方法 873

第 VI 部： ネットワーク サービスの確保 875

第 30 章 Trustsec を使用したネットワーク サービスの確保 877
Cisco TrustSec の概要 877
Trustsec 準備状況評価レポートの生成 878

第 31 章 IWAN を使用したアプリケーション パフォーマンスの向上 881

シスコ インテリジェント WAN（IWAN）の概要 881

IWAN サービスをイネーブルにするための前提条件 882

IWAN ウィザードを使用した IWAN サービスの設定 884

IWAN（APIC-EM）を使用したデバイス上での PKI 証明書ベースの認証設定 885

第 32 章 統合アクセス導入テンプレートを使用したキャンパスおよびブランチ ネットワーク向けのデバイスの設定 887

統合アクセス ワークフローとは 887

サポート対象の Cisco IOS-XE プラットフォーム 889

統合アクセス導入の前提条件 890

レイヤ 2 およびレイヤ 3 の前提条件 891

サーバの構成の前提条件 894

統合アクセス テンプレートを使用したデバイスの設定 895

設定値入力のガイドライン 897

フィールド参照：統合アクセス テンプレート 897

例：コントローラなしの単一スイッチ ネットワーク 901

例：コントローラなしの単一/マルチドメイン ワイヤレス ネットワーク 906

例：コントローラベースの単一/マルチドメイン ワイヤレス ネットワーク 908

例：集中型ワイヤレス キャンパス 910

第 33 章 Branch Threat Defense の設定 913

Cisco Branch Threat Defense の概要 913

サポート対象の IOS-XE プラットフォーム 913

サポート対象の IOS-XE バージョン 914

Branch Threat Defense を有効にするための前提条件 914

Branch Threat Defense ウィザードの使用 914

第 34 章 アクセス ネットワーク ワークフロー 917

概要 917

Cisco アクセス ネットワーク ワークフローを使用するための前提条件 918
サポートされるデバイス 918

第 35 章 **Application Visibility and Control（AVC）によるアプリケーション パフォーマンスの向上 921**
Application Visibility and Control（AVC）によるアプリケーション パフォーマンスの向上 921
WSMA で AVC 機能を使用するためのデバイスの設定 921
AVC とは 923
AVC がサポートされるデバイス 924
Application Visibility and Control の使用時の前提条件 925
ASR デバイス上の CPU、メモリ、およびネットワーク リソースの推測 926
ルータの DMVPN 詳細の表示 927
NBAR プロトコル パックとは 927
アプリケーションの可視性テンプレートの作成 928
インターフェイスでデフォルトのアプリケーションの可視性を有効にする 929
AVC を使用したトラフィック フローのトラブルシューティング 931
AVC トラブルシューティング セッションのアクティブ化 933
AVC トラブルシューティング セッションの編集 933
AVC で使用するデータ ソースの設定 933
AVC データ重複除去の設定 935
設定テンプレートを使用した VPN IKE ポリシーと設定の構成 935
設定テンプレートを使用した VPN IPSec プロファイルの設定 936
設定テンプレートを使用した VPN 事前共有キーの設定 936
設定テンプレートを使用した VPN RSA キーの設定 937
設定テンプレートを使用した VPN トランスフォーム セットの設定 937
エンドポイント アソシエーションを使用した NetFlow データの分類 937
NetFlow テンプレートの表示 938
Easy VPN サーバとは 938
設定テンプレートを使用した Easy VPN サーバの Web ブラウザ プロキシ設定 939
設定テンプレートを使用した Easy VPN Remote の設定 939
設定テンプレートを使用した Easy VPN サーバの設定 941
設定テンプレートを使用した GSM プロファイルの設定 942

設定テンプレートを使用した セルラー プロファイルの設定 942
ScanSafe を使用した HTTP および HTTPS トラフィックのスキャンの有効化 943
CDMA セルラー WAN インターフェイスの設定 944
GSM セルラー WAN インターフェイスの設定 945
ネットワーク アドレス変換（NAT）の設定 945
NAT タイプ 946
IP アドレス節約のための NAT 設定 946
NAT IP プールの作成 946
NAT44 ルールの作成 947
インターフェイスの設定 948
NAT MAX 変換を使用したルータでの同時 NAT 操作数の制限 948
DMVPN を使用した IPSec トポロジの設定 949
DMVPN トンネルの作成 949
DMVPN ハブ アンド スポーク トポロジの設定 951
DMVPN フルメッシュ トポロジの設定 951
DMVPN クラスタ トポロジの設定 952
デバイスからの DMVPN トンネルの削除 952
デバイスの QoS 設定 953
GETVPN を使用した IPSec トポロジの設定 954
GETVPN グループ メンバーの設定 955
GETVPN キー サーバの設定 956
VPN のコンポーネント 957
VPN IKE ポリシーの設定 958
VPN IPSec プロファイルの設定 958
VPN 事前共有キーの設定 959
VPN RSA キーの設定 960
VPN トランスフォーム セットの設定 961
ゾーンベースのファイアウォールを使用したインターフェイス グループ間のファイアウォール ポリシーの制御 962
ゾーンベース ファイアウォールの設定：ワークフロー 964
ゾーンベース ファイアウォールのポリシー ルールの設定 964

CLI を使用したゾーンベース ファイアウォール設定の削除 965
単一デバイスのゾーン ベースのファイアウォールのポリシー ルールを構成します。 965
データ ソースとしての NAM アプリケーション サーバの追加 973

第 36 章 Prime Infrastructure によって、WAN エンド ユーザの一貫したアプリケーション エクスペリエンスが確保される仕組み。 975
WAN エンド ユーザの一貫したアプリケーション エクスペリエンスの確保 975
サイトのアプリケーション主要パフォーマンス評価指標の表示 977
パフォーマンスをモニタするカスタム アプリケーションの作成 978
[AVCサービスヘルス（AVC Service Health）] ウィンドウを使用したサービス ヘルスの表示 979
アプリケーション パフォーマンスのサービス ヘルス ルールのカスタマイズ 980
アプリケーション パフォーマンスを計算するためのベースラインの有効化 980
WAN 最適化のためのアプリケーション パフォーマンス ダッシュボードの設定 982
パフォーマンスの低い WAN アプリケーション、クライアント、サーバ、およびリンクの識別 983
WAN 最適化の結果の表示 984
WAN クライアント/サーバおよびサイト間最適化トラフィック フローの表示 984

第 37 章 Microsoft Lync トラフィックのモニタ 987
Microsoft Lync トラフィックをモニタする方法 987
Lync モニタリングのセットアップ 987
Microsoft Lync の一般データの表示 988
ユーザの Microsoft Lync コールの問題のトラブルシューティング 989
サイト間 Microsoft Lync データの表示 989

第 38 章 Mediatrace を使用した RTP および TCP フローのトラブルシューティング 991
Mediatrace とは 991
Mediatrace を使用した現在アクティブな RTP ストリームと TCP セッションの表示 991
RTP または TCP フローからの Mediatrace の起動 993
エンドポイントからの Mediatrace の起動 994

Mediatrace で報告された最も悪い RTP エンドポイントのトラブルシューティング 996
Mediatrace を使用した複数のソースからのフロー データの比較 998

第 39 章 Cisco モビリティ サービス エンジンおよびサービス 999
Cisco モビリティ サービス エンジン（MSE）の概要 999
Cisco Prime Infrastructure への MSE の追加 1000
MSE ライセンス 1005
MSE ライセンス ファイルの削除 1006
MSE の表示 1007
Prime Infrastructure からの MSE の削除 1007
MSE と同期される Cisco Prime Infrastructure データ 1008
製品データと MSE の同期 1009
ワイヤレス コントローラの MSE 割り当ての変更 1010
NMSP 接続ステータスのトラブルシューティング 1011
サード パーティ NE と MSE の同期 1012
MSE との適切な同期を実現するためのコントローラのタイム ゾーンの設定 1013
MSE データベースと製品データベース間の同期のセットアップ 1014
例：MSE との製品データの同期時におけるスマート コントローラの選択方法 1015
MSE データベースと製品データベースの同期ステータスの表示 1016
MSE データベースと製品データベースの同期の履歴表示 1017
MSE に関する通知統計情報の表示 1017
MSE サーバの基本プロパティの変更 1018
MSE の NMSP プロトコル プロパティの変更 1020
MSE アクティブ セッションの表示 1021
MSE トラップ接続先の表示 1022
MSE トラップ接続先の設定 1022
MSE サーバの詳細設定 1023
MSE サーバの再起動 1025
MSE サーバのシャット ダウン 1025
MSE データベースの工場出荷時設定の復元（クリア） 1025
MSE ロギング レベルの設定 1026

MSE MAC アドレス指定ベースのロギングの仕組み 1027
MSE ログ ファイルのダウンロード 1027
MSE ユーザ アカウントの設定 1028
読み取り/書き込みアクセスを制御する MSE ユーザ グループの設定 1029
MSE と製品サーバのモニタ 1030
製品関連 MSE アラームの表示 1030
MSE アラームとイベントの表示 1031
MSE 製品の Out-of-Sync アラームの検索とトラブルシューティング 1031
コントローラと MSE 間の接続ステータスのモニタ 1032
特定のデバイスと MSE 間の接続ステータスのモニタ 1033
MSE データベース バックアップの設定 1034
製品サーバへの MSE 履歴データのバックアップ 1034
製品サーバからの MSE 履歴データの復元 1035
MSE へのソフトウェアのダウンロード 1035
モバイル デバイスのナビゲーションを向上するための MSE パートナー システムの設定（Qualcomm PDS） 1036
MSE を使用するための Qualcomm PDS の設定 1036
Qualcomm PDS が MSE を使用する仕組み 1037
MSE wIPS サービス管理設定の構成 1038
MSE コンテキスト認識型サービス（ロケーション サービス）によるトラッキングの向上 1039
MSE CAS の使用時の前提条件、MSE コンテキスト認識型サービス（ロケーション サービス）によるトラッキングの向上 1039
コンテキスト認識型サービスの一般パラメータ 1040
MSE でのコンテキスト認識型サービスの有効化と設定 1041
コンテキスト認識型サービス フィルタを使用して追跡する MSE アセットのカスタマイズ 1045
クライアント ステーション、不正クライアント、およびアセット タグの履歴情報を保存するための設定 1047
ロケーション情報を強化するための MSE ロケーション プレゼンスの有効化 1048
MSE への MSE アセット、チョークポイント、TDOA レシーバ情報のインポートとエクスポート 1050

MSE への都市アドレス情報のインポート 1051
MSE と同期されている有線スイッチおよびクライアントに関する詳細の表示 1051
MSE と同期される有線スイッチの表示（CAS） 1051
MSE と同期される有線クライアントの表示（CAS） 1052
サードパーティ（ノースバウンド）アプリケーションにタグ通知を送信するための MSE CAS の設定 1054
MSE CAS ロケーション パラメータの設定 1055
MSE CAS イベント通知の設定 1056
MSE のコンテキスト認識型パートナーとタグ エンジン ステータスの表示 1057
MSE によって送信される通知の表示（CAS） 1057
MSE 通知のクリア方法（CAS） 1058
MSE 通知に関する現在の定義の表示（CAS） 1058
特定の MSE に関する通知統計情報の表示（CAS） 1059
MSE モバイル コンシェルジュ アドバタイズメントの表示 1060
MSE モバイル コンシェルジュ統計情報の表示 1060
MSE イベント グループとは 1061
MSE 通知に関するイベント グループの設定 1061
MSE 通知に関するイベント グループの削除 1061
新しい MSE イベントの設定（イベント定義） 1062
イベント グループへの MSE イベント定義の追加 1065
MSE 通知に関するイベント定義の削除 1069
特定の MSE ワイヤレス クライアントの検索（IPv6） 1069
すべての MSE クライアントの表示 1070
MSE を使用したモバイル コンシェルジュの設定 1071
モバイル コンシェルジュ（MSE）の場所の設定 1072
モバイル コンシェルジュ（MSE）のプロバイダーの設定 1073
モバイル コンシェルジュ ポリシー（MSE）の設定 1074
MSE ワイヤレス セキュリティ構成ウィザードを使用した wIPS の設定 1076
Connected Mobile Experience の設定 1079
Prime Infrastructure での CMX の管理 1080

第 40 章 Cisco AppNav を使用した WAN の最適化 1083

Cisco AppNav とは 1083

Cisco AppNav 設定の前提条件 1085

Cisco AppNav の設定方法 1085

単一デバイスでの Cisco AppNav の設定 1086

Cisco Prime Infrastructure のインターフェイス ロールと Cisco AppNav ソリューション 1087

テンプレートを使用した複数デバイス上での Cisco AppNav の設定 1088

Cisco AppNav テンプレートの展開 1089

ISR-WAAS コンテナで作成する場合の Cisco AppNav の設定方法 1090

第 41 章 Cisco WAAS コンテナを使用した WAN の最適化 1091

Cisco WAAS コンテナを使用して WAN を最適化する方法 1091

Cisco WAAS コンテナをインストールするための前提条件 1092

Cisco Prime Infrastructure と Cisco WAAS Central Manager の統合 1092

Cisco Prime Infrastructure から Cisco WAAS Central Manager を起動するためのシングル サイオンの設定 1093

Cisco WAAS Central Manager ユーザの作成 1094

Cisco Prime Infrastructure から Cisco WAAS Central Manager を起動する方法 1094

単一デバイスからの Cisco WAAS Central Manager の起動 1094

複数のデバイスからの Cisco WAAS Central Manager の起動 1095

Cisco WAAS コンテナの OVA イメージのインポート 1095

アクティブ化時に Cisco WAAS コンテナを自動的に設定する 1096

Cisco WAAS コンテナの作成 1096

単一デバイスでの Cisco WAAS コンテナのインストール 1097

複数デバイスでの Cisco WAAS コンテナのインストール 1097

Cisco WAAS コンテナをアンインストールおよび非アクティブ化する方法 1098

単一デバイスでの Cisco WAAS コンテナのアンインストール 1098

複数デバイスでの Cisco WAAS コンテナのアンインストール 1098

Cisco WAAS コンテナを非アクティブ化する方法 1099

単一の Cisco WAAS コンテナの非アクティブ化 1099

複数の Cisco WAAS コンテナの非アクティブ化 1099

第 42 章 ワイヤレス モビリティの使用 1101

モビリティとは 1101

WLAN 階層型モビリティとは 1102

モビリティ ワーク センターを使用したモビリティ ドメインの表示 1103

コントローラ グループからのモビリティ ドメインの作成 1104

スイッチ グループからのモビリティ スイッチ ピア グループの作成 1105

デバイスのモビリティ ロールの変更 1105

モビリティ アンカーとは 1106

WLAN のモビリティ ゲスト アンカー コントローラの設定 1107

Spectrum Expert とは 1108

干渉源データを収集するためのモビリティ Spectrum Expert の設定 1108

モビリティ ネットワークにおける脅威からの保護を目的とした Cisco Adaptive wIPS プロファイルの使用 1109

付録 A： Cisco Prime Infrastructure ユーザ インターフェイスの参照 1113

Cisco Prime Infrastructure ユーザ インターフェイスの参照 1113

Cisco Prime Infrastructure ユーザ インターフェイスについて 1113

[ドック（Dock）] ウィンドウ 1114

Filters 1115

データ入力機能 1117

インタラクティブ グラフ 1119

一般的な UI タスク 1120

[デバイス360度ビュー（Device 360° View）] からのデバイス詳細の取得 1121

Internet Explorer と Google Chrome で Telnet と SSH を使用してデバイスに接続する 1124

[ユーザ360度ビュー（User 360° View）] からのユーザ詳細の取得 1126

[ルータ360度ビュー（Router 360° View）] からの VRF 詳細の取得 1128

検索方法 1129

アプリケーション検索機能の使用 1129

詳細検索機能の使用 1129

保存した検索の使用 1141

付録 B： アイコンと状態の参照 1143

デバイスの到達可能性状態と管理状態 1143

ポートまたはインターフェイスの状態 1145

リンクの有用性状態 1147

リンクの特徴 1147

機器の動作状態（シャーシ ビュー） 1148

アラーム重大度アイコン 1149

デバイス タイプのアイコン 1149

付録 C： Cisco Prime Infrastructure でサポートされるタイム ゾーン 1153

Cisco Prime Infrastructure でサポートされるタイム ゾーン 1153

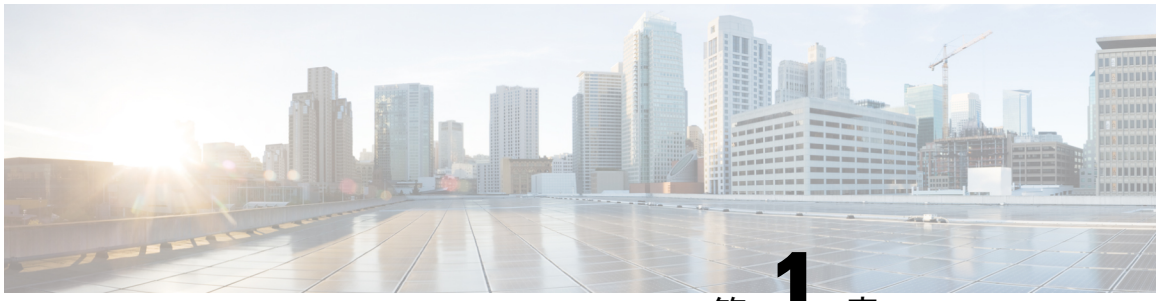
付録 D： よくある質問：オペレーション センターと Prime Infrastructure 1161

よくある質問：オペレーション センターと Cisco Prime Infrastructure 1161

第 I 部

Prime Infrastructure の概要

- Cisco Prime Infrastructure の概要 （1 ページ）
- Prime Infrastructure のユーザ設定の変更 （31 ページ）



第 1 章

Cisco Prime Infrastructure の概要

ここでは、次の内容について説明します。

- Prime Infrastructure の構成 （1 ページ）
- を使用する前に完了する必要のあるタスクのセットアップ Prime Infrastructure （2 ページ）
- ログインおよびログアウト （3 ページ）
- パスワードの変更 （4 ページ）
- メイン ウィンドウ コントロールの使用 （4 ページ）
- デフォルトのホーム ページの変更 （5 ページ）
- ダッシュボードのセットアップと使用 （6 ページ）
- ダッシュボードを使用したネットワーク ヘルスのトラブルシューティング （19 ページ）
- 別の仮想ドメインで作業する （27 ページ）
- ジョブ ダッシュボードを使用したジョブの管理 （27 ページ）
- Cisco Prime Infrastructure 機能の拡張 （29 ページ）
- 最新のインベントリに存在をチェック マニュアル （30 ページ）

Prime Infrastructure の構成

Prime Infrastructure の Web インターフェイスはライフサイクル ワークフローで構成され、次の表に示すようなハイレベルのタスク エリアがあります。このマニュアルでは、同じ一般構成に従います。

⚠

注意 サードパーティ製のブラウザ拡張機能を有効にしないことを強くお勧めします。Internet Explorer では、[ツール（Tools）] > [インターネット（Internet）] オプションを選択して、[詳細設定（Advanced）] タブで [サードパーティ製のブラウザ拡張を有効にする（Enable third-party browser extensions）] チェックボックスを選択解除することで、サードパーティ製のブラウザ拡張を無効にできます。

表 *1 : Prime Infrastructure* のタスク領域

タスク エリア	説明	使用者
ダッシュボード	ダッシュボードは、デバイス、パフォーマンス情報、およびさまざまなインシデントのクイック ビューを提供します。	ネットワーク オペレータおよびネットワーク エンジニア
モニタ（Monitor）	日単位でネットワークをモニタし、ネットワーク デバイス インベントリと設定管理に関連する他の毎日の操作または臨時の操作を実行します。[Monitor] タブには、毎日のモニタリング、トラブルシューティング、保守、および操作に必要なダッシュボードとツールが含まれています。	ネットワーク エンジニア、設計者、およびアーキテクト
Configuration	設計機能またはデバイス パターン、あるいはテンプレート。[Design] エリアでは、設定テンプレートなど、再利用可能な設計パターンを作成できます。事前定義されたテンプレートを使用することも、独自のテンプレートを作成することもできます。パターンとテンプレートはライフサイクルの展開段階で使用されます。また、プラグアンドプレイ プロファイルとモビリティ サービスを設計することもできます。	ネットワーク エンジニア、設計者、およびアーキテクト
Inventory	デバイスの追加、ディスカバリの実行、ソフトウェア イメージの管理、デバイス アーカイブの設定、デバイスでの設定変更の監査など、すべてのデバイス管理操作を実行します。	ネットワーク エンジニア、NOC オペレータ、サービス オペレータ
Maps	ネットワーク トポロジおよびワイヤレス マップを表示します。	ネットワーク エンジニア、NOC オペレータ、サービス オペレータ
Services	モビリティ サービス、Application Visibility and Control サービス、および IWAN 機能にアクセスします。	ネットワーク エンジニア、NOC オペレータ、サービス オペレータ
Report	レポートの作成、保存したレポート テンプレートの表示、スケジュール設定されたレポートの実行を行います。	ネットワーク エンジニア、NOC オペレータ、サービス オペレータ
Administration	システム コンフィギュレーションの設定とデータ収集の設定を指定し、アクセス コントロールを管理します。ジョブの表示と承認、ヘルス ルールの指定、およびライセンス管理を行うことができます。また、ソフトウェア アップデートの実行とハイ アベイラビリティの設定を行うこともできます。	ネットワーク エンジニア

を使用する前に完了する必要のあるタスクのセットアップ Prime Infrastructure

機能を使用するには、管理者が次のタスクを完了する必要があります。

表 *2:* セットアップ タスクと参照

を使用する前に完了する必要のあるタスク Prime Infrastructure	詳細については、次を参照してください。
Prime Infrastructure サーバのセットアップと設定を行います。	『Prime Infrastructure Administrator Guide』の「Server Setup Tasks」
デバイスとネットワークの管理を簡素化するために、デバイスをに追加してデバイス グループを作成します。	デバイスの追加と整理 （37 ページ）
ネットワークで使用されるインターフェイスとテクノロジーのモニタリングを有効にします。	デバイスおよびネットワークの健全性とパフォーマンスのモニタ （327 ページ）
展開に合わせアラームとイベントの動作（アラームやイベントの更新頻度、電子メール、トラップ レシーバなど）をカスタマイズします。	アラームとイベント管理の設定（360ページ）

ログインおよびログアウト

GUI にログインするには、Web ブラウザのアドレス フィールドに次のように入力します。*server-ip* は サーバの IP アドレスです。

https://*server-ip*

ネットワーク構成によっては、初めてブラウザを Web サーバに接続するときに、サーバのセキュリティ証明書を信頼するようにクライアントブラウザを更新する必要があります。これにより、クライアントと Web サーバ間の接続のセキュリティが保証されます。

ログアウトするには、 ウィンドウの右上にある ⚙ をクリックし、[**Log Out**] を選択します。

ユーザとそのユーザが実行できる操作については、次を参照してください。

- Prime Infrastructure で CLI ユーザ インターフェイスを切り替える方法： でサポートされているすべてのユーザクラス（さまざまなCLIユーザアカウントを含む）について説明します。
- ユーザ グループのタイプ：Web GUI ユーザが毎日実行できる機能を制御できるユーザ グループ メカニズムについて説明します。ユーザ インターフェイスで表示できるものと操作できるものは、ユーザアカウント権限によって制御されます。このトピックでは、デバイスのロールベース アクセス コントロール（RBAC）を管理する仮想ドメイン メカニズムについても説明します。

パスワードの変更

パスワードは、Prime Infrastructure ウィンドウの右上にある⚙をクリックし、[**Change Password**] を選択することによって、いつでも変更できます。?(**[ヘルプ（help）]**)アイコンをクリックして、パスワードポリシーを確認します。

（オプション）**[新しいパスワードを生成（Generate New Password）]** ボタンをクリックして、システムによって生成されるセキュアなパスワードを設定します。このボタンをクリックすると、新しいパスワードが隣のテキストボックスに表示されます。**[新しいパスワード（New password）]** および **[パスワードの確認（Confirm password）]** テキストボックスにも同じものが表示されます。目のアイコンをクリックするとパスワードの表示/非表示が切り替わります。**[コピー（Copy）]** ボタンをクリックして、パスワードをクリップボードにコピーすることもできます。

ダイアログボックス内の値をクリアするには、[リセット（Reset）] ボタンをクリックします。

メイン ウィンドウ コントロールの使用

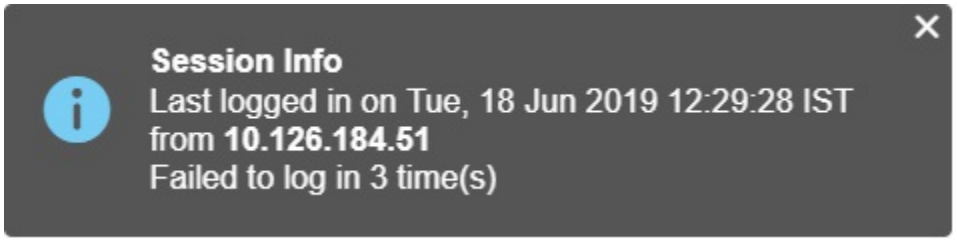
タイトル バーの左上には、次のコントロールがあります。

	[メニュー（Menu）] ボタン：左側のメインのナビゲーション メニューを切り替えます（左側のサイドバー メニューとも呼ばれます）
	[ホーム（Home）] ボタン：ホームページ（通常は [概要（Overview）] ダッシュボード）に戻ります。

タイトル バーの右側には、使用しているユーザ名と仮想ドメインが表示されます。仮想ドメインは、デバイスの論理的なグループです。仮想ドメインは、ネットワークのデバイスや領域にアクセスする人物を制御するために使用されます。割り当てられている仮想ドメインを切り替えるには、別の仮想ドメインで作業する （27 ページ） を参照してください。

（注） ログインに成功すると **[セッション情報（Session Info）]** ポップアップが表示され、前回ログインしたときの詳細と、過去 24 時間のログイン試行の失敗回数 (ある場合) が示されます。

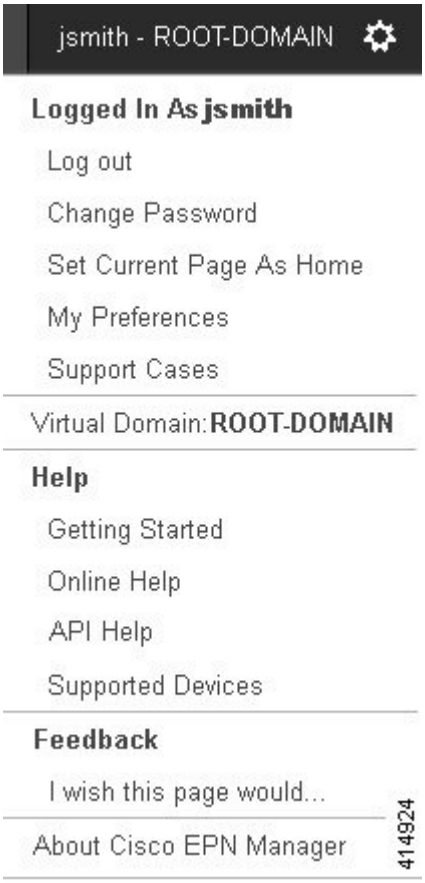
図 *1:* セッション情報（*Session Info*）



	Web GUI のグローバル設定ボタン：ログアウト、パスワードの変更、Cisco.com のアカウントプロファイルの表示、GUI 設定の調整、Cisco.com のサポート事例の確認、オンライン ヘルプの起動

タイトル バーの右側の をクリックすると、ウィンドウ設定メニューが開きます。

図 *2 :* ウィンドウ設定



最後に、[アラームのまとめ（Alarm Summary）] には、ネットワーク内のアラーム数が視覚的に示されます。色は最も重大度の高いアラームを示します。

	[アラームのまとめ（Alarm Summary）]：指定したカテゴリのアラーム数が視覚的に表示されます。この領域をクリックすると、[アラームのまとめ（Alarm Summary）] ポップアップ ウィンドウが開きます。

デフォルトのホーム ページの変更

次のタスクを実行したときに、どのページが表示されるようにするかを指定できます。

- Web GUI タイトル バーの左側にある をクリックしたとき

- Prime Infrastructure Web GUI にログインするとき

この設定はユーザ単位で保存されます。この設定は、他のユーザに影響を与えることなく、いつでも変更できます。

ステップ 1 希望のページが表示されている状態で、Prime Infrastructure Web GUI の右上にある ⚙ をクリックします。

ステップ 2 [現在のページをホームとして設定（Set Current Page as Home）] を選択します。

ダッシュボードのセットアップと使用

ダッシュボードには、ネットワークにおける最重要データの概要が表示されます。これらは、ステータス、アラート、モニタリング、パフォーマンス、レポートの情報を提供します。ユーザにとって重要な情報のみが表示されるように、これらのダッシュボードをカスタマイズできます。デフォルトのホームページとして [ネットワーク概要（Network Summary）] ダッシュボードを設定することをお勧めします。そうすれば、ログイン後にこのダッシュボードが表示され、何かを実行する前に、ネットワーク全体の健全性をすばやく確認できます。デフォルトのホームページとしてダッシュボードを設定するには、デフォルトのホーム ページの変更 （5 ページ）を参照してください。

以下のダッシュボードを使用して、ネットワークをモニタしたり、管理したりします。

- [ネットワーク概要（Network Summary）] ダッシュボード：ネットワーク全体の健全性を確認します。ネットワーク概要ダッシュボードを使用したネットワーク全体の健全性の確認 （10 ページ）を参照してください。
- [ワイヤレス（Wireless）] ダッシュボード：ワイヤレスセキュリティ、メッシュ、CleanAir、ContextAware ネットワーキングに関する詳細を含むワイヤレス情報を提供します。
- [パフォーマンス（Performance）] ダッシュボード：特定のデバイスやインターフェイスのパフォーマンスを確認します。[パフォーマンス（Performance）] ダッシュボードを使用して、特定のデバイスまたはインターフェイスのパフォーマンスをチェックする （13 ページ）を参照してください。

管理者権限を持つユーザは、次のダッシュボードも使用できます。

- [ライセンス（Licensing）] ダッシュボード：『Cisco Prime Infrastructure Administrator Guide』の「*View the Licencing Dashboard*」セクションを参照してください。
- [ジョブ（Jobs）] ダッシュボード：ジョブ ダッシュボードを使用したジョブの管理 （27 ページ）を参照してください。

次の点に注意してください。

- ダッシュボード ウィンドウの各部分の説明およびダッシュボード フィルタの使用方法については、ダッシュボードの使用方法 （7 ページ）を参照してください。

ダッシュボードの使用方法

次の図に、ダッシュボードウィンドウの主要な部分とそれらの調整に使用可能なコントロールを示します。

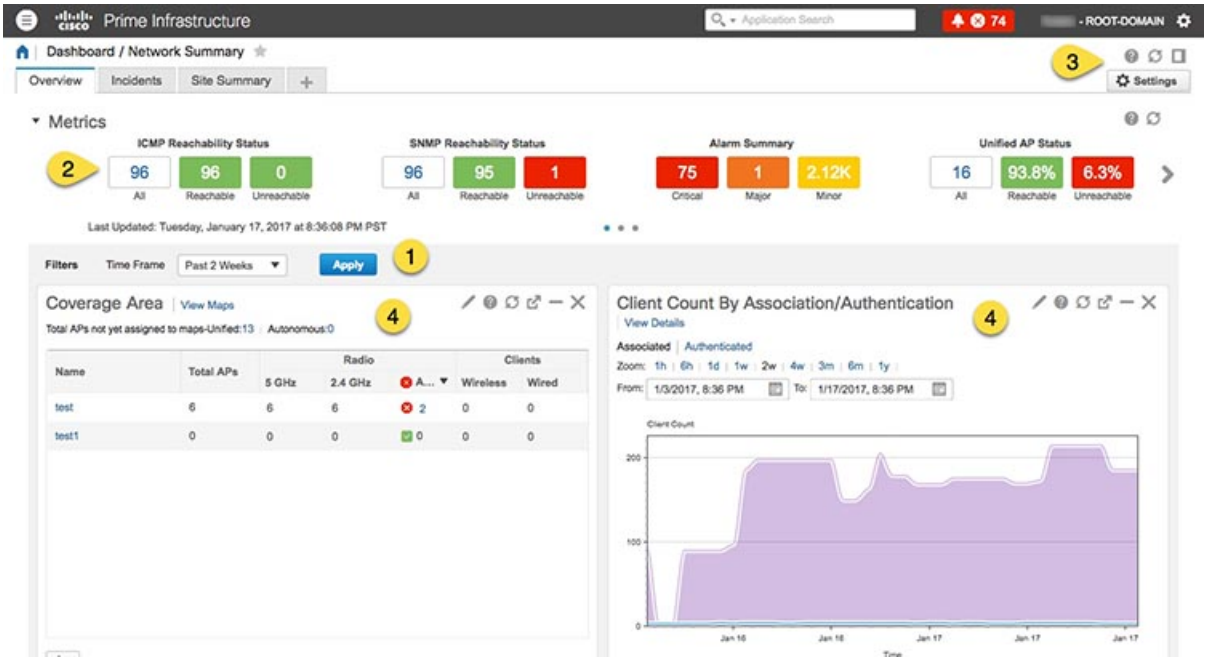
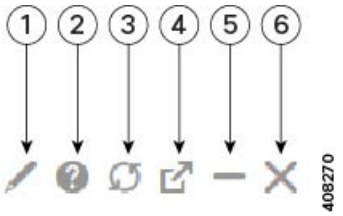


表 *3:* ダッシュボード要素

1	ダッシュボード フィルタ：選択に基づいてダッシュボード内のすべてのダッシュレットをフィルタ処理します。この例では、時間ベースのフィルタが使用されています。表示されるフィルタは、ダッシュボード タイプによって異なります。たとえば、パフォーマンス ダッシュボードでは、特定のインターフェイス、デバイス、回線、または VC を選択する必要があります。
2	メトリック ダッシュレット：アラームや使用可能なデバイスなどのクイック メトリックを提供します。

3	ダッシュボードの設定とコントロール： • ダッシュボードアイコン：オンラインヘルプを起動したり、ダッシュボード全体を更新したり、[ドッキング（Dock）] ウィンドウを開いたりできます。 • [ダッシュボード設定（Dashboard Settings）] メニュー：ダッシュボード タブを追加または名前変更したり、新しいダッシュレット（標準とメトリックの両方）を追加したり、ダッシュボードのレイアウトを調整したり、すべてのダッシュボードをデフォルト設定にリセットしたり、ダッシュボードをクローニングしたり（[ネットワーク サマリー（Network Summary）] ダッシュボードにのみ適用可能）、選択したダッシュレットからデータをエクスポートしたりできます。 （注） 新しく追加されたダッシュボード タブまたは名前を変更されたダッシュボードタブは、[タブ（Tab）] ビューにのみ表示できます。この変更はダッシュボード メニューには反映されません。
4	標準ダッシュレット：ダッシュボードに関連する概要データを示します。

各ダッシュレットの右上に、そのダッシュレットが使用されたときにアクティブになるアイコンがあります。ダッシュレットタイプによって、使用可能なアイコンが決定されます。最も一般的なアイコンを次の図に示します。



1	ダッシュレットオプションを編集します。これには、ダッシュレットタイトルの編集、ダッシュレットの更新、またはダッシュレット更新間隔の変更が含まれます。（更新を無効にするには、[ダッシュレットの更新（Refresh Dashlet）] をオフにします）。ダッシュレットに現在適用されているフィルタを表示するには、このツール アイコンの上にカーソルを移動します。
2	ダッシュレット ポップアップ ヘルプ ウィンドウ：ダッシュレットの図と説明、それを生成するために使用されたデータ ソース、およびダッシュレットのコンテンツに適用可能なフィルタを提供します。
3	ダッシュレットをリフレッシュします。
4	ダッシュレットを切り離し、新しいブラウザ ウィンドウで表示します。別のブラウザ ウィンドウでダッシュレットを編集する場合、変更はそのウィンドウにのみ適用され、保存されることはありません。
5	ダッシュレットを最小化して、タイトルのみが表示されるようにします。ダッシュレットが最小化されると、最大化（+）アイコンがこのツール アイコンの代わりに表示されます。

[6]	ダッシュボードからダッシュレットを削除します。

ダッシュボードの追加情報については、次のトピックを参照してください。

- ダッシュボードのタイプ （9 ページ）
- ダッシュボードへのダッシュレットの追加 （15 ページ）
- 新しいダッシュボードの追加 （18 ページ）

[ドック（Dock）] ウィンドウのカスタマイズ

[ドック（Dock）] ウィンドウを使用すると、頻繁に使用する Web GUI ページやポップアップ ウィンドウ（特定のデバイスの 360 度ビューなど）に素早く移動できます。このウィンドウでは、最近アクセスした 15 のページへのリンクと Prime Infrastructure トレーニング資料へのリンクにもアクセスできます。このウィンドウを開くには、（ページの右上の領域にある）[ドック（Dock）] アイコンをクリックします。

[ドック（Dock）] ウィンドウに表示されるリンクを更新するには、次の手順に従います。

ステップ 1 Web GUI ページのリンクを [お気に入り（Favorites）] タブ（[ドック（Dock）] アイコン > **[アクセスしたリンク（Links Visited）]** > **[お気に入り（Favorites）]**）に追加する場合：

a) 追加する Web GUI ページを開きます。

b) ページの左上の領域にある星の形をした（[お気に入り（Favorites）]）アイコンをクリックします。

ステップ 2 ポップアップ ウィンドウのリンクを [ドッキング アイテム（Docked Items）] 領域（[ドック（Dock）] アイコン > [ドッキング アイテム（Docked Items）]）に追加する場合：

a) 追加するポップアップ ウィンドウを開き、その 360 度ビューを開きます。

b) ポップアップ ウィンドウの右上隅にある [ドックに追加（Add to Dock）] アイコンをクリックします。

ダッシュボードのタイプ

以下のトピックでは、ネットワークをモニタするために使用できるダッシュボードについて説明します。

（注） Prime Infrastructure は、データ ソースではなく、サイトに割り当てられたエンド ポイントに基づいて、仮想ドメインのモニタリング データをフィルタリングします。したがって、ダッシュボードには、ユーザに割り当てられた仮想ドメインに関係なく、すべての仮想ドメインの情報が表示されます。

ネットワーク概要ダッシュボードを使用したネットワーク全体の健全性の確認

ネットワーク概要ダッシュボードには、最も重要なネットワークの問題のアラートが示されます。ネットワーク内のすべてのデバイスとインターフェイス（コントローラや AP などのワイヤレスデバイスを含む）に関するアラーム、ステータス、および使用状況に関する情報が表示されます。このダッシュボードには、小さなネットワーク トポロジ ダッシュレットも表示できます。

ダッシュボード上部のメトリックス ダッシュレットに表示される情報のタイプを理解するには、メトリック ダッシュレットにマウス カーソルを移動し、ポップアップ ヘルプ ボタン（[?]）が表示されたら、このボタンをクリックしてダッシュレット ヘルプを開きます。このページのその他のダッシュレットの説明については、各ダッシュレットの右上隅にあるダッシュレット コントロールに表示されるポップアップ ヘルプ ボタンをクリックしてください。

ネットワーク概要ダッシュボードを開いてカスタマイズするには、次の手順に従います。

ステップ 1 **[ダッシュボード（Dashboard）] > [ネットワーク概要（Network Summary）]** を選択し、次のいずれかをクリックします。

- [概要（Overview）] タブ：すべてのデバイスを確認します。
- [インシデント（Incidents）] タブ：syslog を含むアラームとイベントを中心に確認します。
- [クライアントの概要（Client Summary）] タブ：[クライアントの分散（Client Distribution）]、[クライアント カウント（Client Count）]、および [クライアント トラフィック（Client Traffic）] を確認します。

  （注） デフォルトでは、クライアント概要ダッシュボードにアクセスできるのは ROOT と SUPERUSER だけです。Admin ユーザおよび Config ユーザがこのダッシュボードにアクセスする必要がある場合は、Admin/Config ユーザの作成時に NBI READ アクセス権限を付与する必要があります。

- [サイトの概要（Site Summary）] タブ：特定サイトのすべてのデバイスを確認します。
- [ネットワーク ヘルス（Network Health）] タブ：一連のヘルス ルールに従ってネットワークの健全性を確認します。

ステップ 2 必要に応じて、ダッシュボードを調整します。ダッシュレットはダッシュボードのさまざまな場所にドラッグすることができます。または、[設定（Settings）] メニューを使用して、新しいダッシュレットを追加したり、ダッシュボード スタイルを変更したりできます。ダッシュボードにダッシュレットを追加するには、事前定義のダッシュレットをダッシュボードに追加する （15 ページ）を参照してください。

ステップ 3 フィルタの [タイム フレーム（Time Frame）] ドロップダウンリストから表示するタイム フレームを選択し、[適用（Apply）] をクリックします。選択されたタイム フレームは、すべてのダッシュレットで更新されます。

（注） 特定のダッシュレットのタイム フレームを変更するには、[ズーム（Zoom）] オプションで必要なタイム フレームをクリックします。グローバル タイム フレームにリセットするには、**[設定（Settings）] > [ダッシュボードの管理（Manage Dashboards）] > [ダッシュレットのタイムフィルタのリセット（Reset Dashlet Time Filters）]** を選択します。このリセット オプションは、[ネットワーク概要ダッシュボード（Network Summary Dashboard）] ページで利用可能なすべてのタブに適用されます。

概要ダッシュボードを使用したすべてのデバイスまたはすべてのインターフェイスのヘルスの確認

概要ダッシュボードは、ネットワーク デバイス、インターフェイス、クライアント、およびアプリケーションのすべてのヘルスについて、要約および集約したデータを、それらの可用性、ステータス、使用率、およびアラームと、それらに影響を及ぼすイベントを含めて提供することで、ネットワークのヘルスを維持するのに役立ちます。

ダッシュボード上部のメトリックス ダッシュレットに表示される情報のタイプを理解するには、メトリック ダッシュレットにマウス カーソルを移動し、ポップアップ ヘルプ ボタン（[?]）が表示されたら、このボタンをクリックしてダッシュレット ヘルプを開きます。このページのその他のダッシュレットの説明については、各ダッシュレットの右上隅にあるダッシュレット コントロールに表示されるポップアップ ヘルプ ボタンをクリックしてください。

概要ダッシュボードを開いてカスタマイズするには、次の手順を実行します。

ステップ 1 **[ダッシュボード（Dashboard）] > [概要（Summary）]** を選択し、次のいずれかをクリックします。

- デバイスが到達可能なカバレッジ領域やCPUおよびメモリの上位ユーザを含め、すべてのデバイスおよびインターフェイスのヘルスを確認するには、[一般（General）] タブをクリックします。
- ほとんどのアラームの発生元のサイト、デバイス到達可能性、アラームのタイプ、および syslog の詳細など、アラームとイベントに注目する場合は、[インシデント（Incidents）] タブをクリックします。
- ネットワーク クライアントのヘルスに注目する場合は、[クライアント（Client）] タブをクリックします。このタブは、トラブルシューティング ツール、有線およびワイヤレス クライアントの分布グラフおよび速度グラフ、クライアント ポスチャなど、クライアント指向のさまざまなダッシュレットをホストしています。
- デバイスの可用性、CPUおよびメモリの使用状況、および温度の問題を確認するには、[ネットワーク デバイス（Network Devices）] タブをクリックします。
- インターフェイスの可用性、ステータス、CPU およびメモリの使用状況、ならびにエラーや破棄を最も多く発生させているインターフェイスを確認するには、[ネットワーク インターフェイス（Network Interfaces）] タブをクリックします。
- 識別されたネットワーク サービスとアプリケーション、サーバ、ならびにそれらをサポートする NetFlow 監視リソース、ならびにそれらを消費するクライアントに関して確認するには、[Service Assurance（サービス保証）] タブをクリックします。

ステップ 2 必要に応じて、ダッシュボードを調整します。ダッシュレットはダッシュボードのさまざまな場所にドラッグすることができます。または、[設定（Settings）] メニューを使用して、新しいダッシュレットを追加したり、ダッシュボード スタイルを変更したりできます。ダッシュレットを追加するには、事前定義のダッシュレットをダッシュボードに追加する （15 ページ）を参照してください。

ステップ 3 フィルタの [タイム フレーム（Time Frame）] ドロップダウンリストから表示するタイム フレームを選択し、[適用（Apply）] をクリックします。

ワイヤレス ダッシュボードを使用したワイヤレス ネットワークのヘルスの確認

ワイヤレス ダッシュボードは、ネットワーク セキュリティ ステータスおよび攻撃、メッシュ ネットワークの効率性、電波品質、干渉などに関する集約されたデータを提供することで、ワイヤレス ネットワークのヘルスを維持するのに役立ちます。

ダッシュボード上部のメトリックス ダッシュレットに表示される情報のタイプを理解するには、メトリック ダッシュレットにマウス カーソルを移動し、ポップアップ ヘルプ ボタン（[?]）が表示されたら、このボタンをクリックしてダッシュレット ヘルプを開きます。このページのその他のダッシュレットの説明については、各ダッシュレットの右上隅にあるダッシュレット コントロールに表示されるポップアップ ヘルプ ボタンをクリックしてください。

ワイヤレス ダッシュボードを開いてカスタマイズするには、次の手順を実行します。

ステップ 1 **[ダッシュボード（Dashboard）] > [ワイヤレス（Wireless）]** を選択し、次のいずれかをクリックします。

- 上位のセキュリティ問題、すべてのタイプにおいて検出された不正、CleanAir セキュリティ、不正の抑制、およびシスコの適応型ワイヤレス侵入防御（wIPS）データを確認するには、[セキュリティ（Security）] タブをクリックします。
- メッシュ ネットワークのアラーム、SNR が最も悪いリンク、ノード ホップおよびパケット エラーの数に注目するには、[メッシュ（Mesh）] タブをクリックします。
- インターフェイスの総数および最も劣悪なインターフェイス、CAS 干渉通知、および一般的な電波品質など、非 802.11 インターフェイス ソースに注目する場合は、[CleanAir] タブをクリックします。
- MSE 追跡カウント、ロケーション支援クライアント トラブルシューティング、および検出された不正要素など、モビリティ サービス エンジンでサポートされている Cisco Context-Aware Mobility のデータに注目するには、[ContextAware] タブをクリックします。

ステップ 2 必要に応じて、ダッシュボードを調整します。ダッシュレットはダッシュボードのさまざまな場所にドラッグすることができます。または、[設定（Settings）] メニューを使用して、新しいダッシュレットを追加したり、ダッシュボード スタイルを変更したりできます。ダッシュレットを追加するには、事前定義のダッシュレットをダッシュボードに追加する （15 ページ）を参照してください。

ステップ 3 フィルタの [タイム フレーム（Time Frame）] ドロップダウンリストから表示するタイム フレームを選択し、[適用（Apply）] をクリックします。

[パフォーマンス（Performance）] ダッシュボードを使用して、特定のデバイスまたはインターフェイスのパフォーマンスをチェックする

[パフォーマンス（Performance）] ダッシュボードに自分が興味のある情報が表示されない場合は、独自のカスタマイズされたダッシュレットを作成できます。詳細については、[デバイストレンド（Device Trends）] ダッシュボードへのカスタマイズ済みダッシュレットの追加 （16 ページ）を参照してください。

表 *4:* パフォーマンス ダッシュボード

ダッシュボード タブ	内容：
デバイス	• 指定されたタイムラインのデバイス可用性 • デバイス CPU ごとの CPU 使用率 • メモリ使用率 • ポート カウントと動作上アップまたはダウンになっているポート • デバイスのアラームとイベント • デバイスの温度
インターフェイス（Interface）	• インターフェイスのプロパティ（IfType や IfIndex など） • 指定されたタイムラインのインターフェイス可用性 • インターフェイスの CPU 使用率とメモリ使用率 • Tx 使用率と Rx 使用率、およびパケットのエラーと破棄 • QoS クラス マップ統計情報

サイト、アクセス ポイント、アプリケーションなど	• クライアント トラフィック、最もアラーム数の多いデバイス、上位 N 個のアプリケーション、およびデバイス到達可能性ステータス
	• 特定のアクセス ポイントの場合：
	  • アクセス ポイントの詳細
	  • 上位のクライアントとアプリケーション
	  • チャネル使用率
	  • クライアント数
	• 特定のアプリケーションの場合：
	  • 上位のクライアントとサーバ
	  • アプリケーション トラフィック分析グラフ
	  • アプリケーション サーバのパフォーマンス
	  • 時系列の上位インターフェイス

ダッシュボードタブ	内容：

一部のダッシュレット（[トップNのクライアント（Top N Clients）]、[トップNのサーバ（Top N Servers）]、[トップNのアプリケーション（Top N Applications）]、[一定期間のクライアントカウント（Number of Clients Over Time）]、[クライアントトラフィック（Client Traffic）] ダッシュレットなど）には、関連テーブルのレコード数が 1 億を超えている場合に、それぞれの [レポート（Report）] ページに移動するための [対応するレポートを起動するにはここをクリック（click here to launch the corresponding report）] リンクがあります。このリンクは、ドロップダウンリストから [有効（Enable）] を選択し、[ダッシュボード設定（Dashboard Settings）] メニューの [適用（Apply）] をクリックした場合にのみ、ダッシュレットに表示されます。デフォルトでは、この設定は無効になっています。

関連するフィルタの一部は、[レポート（Reports）] ページに事前入力されています。たとえば、[トップNのクライアント（Top N Clients）] ダッシュレット、[ロケーショングループ（Location Groups）]、[ネットワーク認識（Network Aware）]、および [レポート期間（Reporting Period）] パラメータは事前入力されます。

（注） 関連テーブルのレコード数が 1 億を超えていても、レポート期間やアプリケーションなど、選択したフィルタに対応するデータがない場合は [レポート（Report）] ページにデータが表示されないことがあります。

（注） デフォルトでは、パフォーマンス ダッシュボード ダッシュレットの更新間隔は 30 分に設定されています。ユーザーは、必要に応じて **[ダッシュレットオプションの編集（Edit Dashlet Options）]** をクリックすることで、間隔を変更できます。

[パフォーマンス（Performance）] ダッシュボードを開いてカスタマイズするには、次の手順を使用します。

ステップ 1 **[ダッシュボード（Dashboards）] > [パフォーマンス（Performance）]** を選択してから、次のいずれかを実行します。

- 特定のデバイスをチェックするには、[デバイス（Devices）] タブをクリックしてから、フィルタの [デバイス（Device）] ドロップダウン リストからデバイスを選択します。
- 特定のインターフェイスをチェックするには、[インターフェイス（Interfaces）] タブをクリックしてから、フィルタの [インターフェイス（Interface）] ドロップダウン リストをクリックし、チェックするインターフェイスに移動します。

ステップ 2 必要に応じて、ダッシュボードを調整します。ダッシュレットはダッシュボードのさまざまな場所にドラッグすることができます。または、[設定（Settings）] メニューを使用して、新しいダッシュレットを追加し

たり、ダッシュボード スタイルを変更したりできます。ダッシュレットを追加するには、ダッシュボードへのダッシュレットの追加 （15 ページ）を参照してください。

ステップ 3 フィルタの [タイム フレーム（Time Frame）] ドロップダウン リストから表示するタイム フレームを選択してから、[実行（Go）] をクリックします。

ダッシュボードへのダッシュレットの追加

- Prime Infrastructure で提供される事前パッケージ ダッシュレット：ダッシュレットの一部はデフォルトでダッシュボードに表示されます。他のダッシュレットは、[設定（Settings）] メニューにリストされ、必要に応じて追加できます。これらのダッシュレットにより、モニタする可能性の高い情報が提供されます（たとえば、デバイスのCPU使用率、インターフェイスのエラーと破棄、トラフィック統計情報）。事前定義のダッシュレットをダッシュボードに追加する （15 ページ）を参照してください。
- デバイスのパフォーマンスをモニタするために作成するカスタム ダッシュレット：これらのダッシュレット タイプは、[デバイス トレンド（Device Trends）] ダッシュボードにのみ追加できます。「[デバイス トレンド（Device Trends）] ダッシュボードへのカスタマイズ済みダッシュレットの追加」を参照してください。

事前定義のダッシュレットをダッシュボードに追加する

Prime Infrastructure は、一般的に必要なネットワーク データを提供する、事前定義のダッシュレットのセットを提供します。デフォルトで、これらのダッシュレットのサブセットがすでにダッシュボードに含まれているため、すぐに使い始めることができます。これらの事前定義のダッシュレットとは別のダッシュレットをダッシュボードに追加するには、次の手順を実行します。

（注） ダッシュレットを編集または削除するには、その右上にある該当するアイコンをクリックします（「ダッシュボードの使用方法」を参照）。

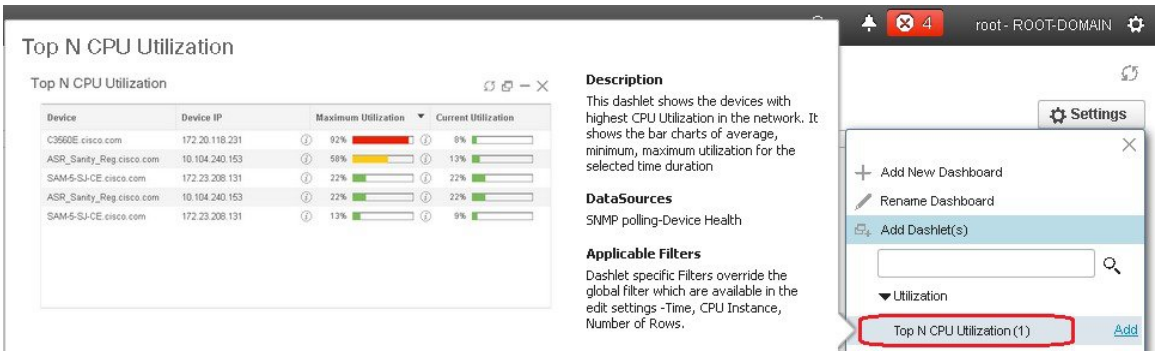
ステップ 1 サイドバー メニューで、[ダッシュボード（Dashboard）] を選択してから、ダッシュレットを追加するダッシュボードを選択します。

たとえば、[デバイス メモリ使用率（Device Memory Utilization）] ダッシュレットを [デバイス トレンド（Device Trends）] ダッシュボードに追加するには、**[ダッシュボード（Dashboard）] > [デバイス トレンド（Device Trends）] > [デバイス（Device）]** を選択します。

ステップ 2 追加するダッシュレットを特定して追加します。

a) ダッシュボードの右上で、[設定（Settings）] をクリックしてから [ダッシュレットの追加（Add Dashlets）] をクリックします。Prime Infrastructure にそのダッシュボードに追加可能なダッシュレットが一覧表示されます。

b) 特定のダッシュレットの概要を示すポップアップ ウィンドウを開くには、そのダッシュレットの名前の上にカーソルを置きます。次の図に示すように、ポップアップ ウィンドウには、ダッシュレットが提供するデータのソースと、ダッシュレットに適用可能なフィルタも表示されます。



c) [追加（Add）] をクリックして、選択したダッシュレットをダッシュボードに追加します。

ステップ 3 ダッシュレットにデータが入力されていることを確認します。

そうでない場合は、必要なモニタリング ポリシーが有効になっているかどうかをチェックします（デバイス ヘルス モニタリング ポリシーだけがデフォルトで有効になります。これは、デバイス可用性、CPU とメモリ プールの使用率、および環境温度をチェックします）。

a) ダッシュレットの右上で、その [?]（[ヘルプ（Help）]）アイコンをクリックして、ダッシュレットのポップアップ ウィンドウを開きます。

b) [データ ソース（Data Sources）] 領域に表示された情報をチェックします。モニタリング ポリシーが表示された場合は、そのポリシーがアクティブになっているかどうかをチェックします。Prime Infrastructure によるモニタリング対象のチェック （334 ページ）を参照してください。

[デバイストレンド（DeviceTrends）]ダッシュボードへのカスタマイズ済みダッシュレットの追加

[デバイス トレンド（Device Trends）] ダッシュボード内に、必要なデバイス パフォーマンス情報を提供するダッシュレットがない場合、カスタマイズしたテンプレートを使用するダッシュレットを追加して、デバイスに対して SNMP MIB 属性をポーリングすることができます。このようなダッシュレットをダッシュボードに追加するには、次の手順に従います。

始める前に

使用可能なモニタリング ポリシーを調べて、必要な情報を収集するポリシーを判断します。ダッシュレットの作成時にポリシーを指定する必要があります。ニーズを満たすポリシーがない場合は、新しいパラメータをポーリングするポリシーを作成できます。サポートされないパラメータとサードパーティ デバイスを対象としたモニタリング ポリシーの作成 （346 ページ）を参照してください。

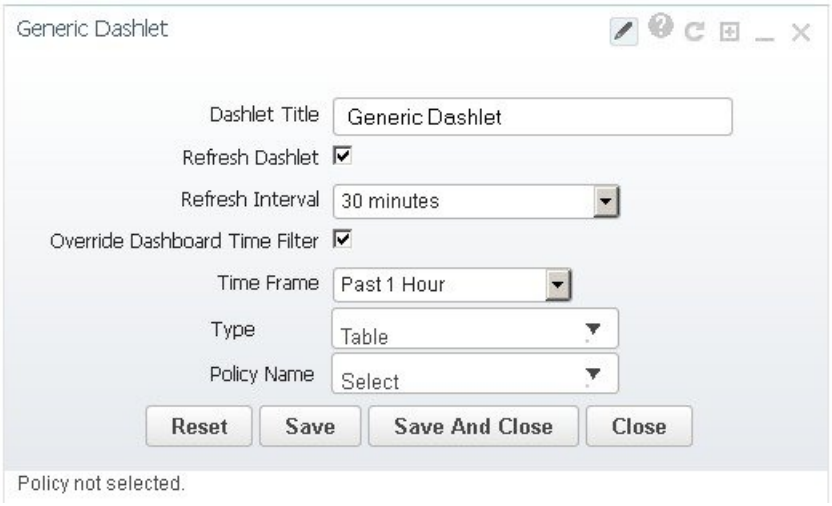
ステップ 1 **[ダッシュボード（Dashboard）] > [デバイス トレンド（Device Trends）] > [デバイス（Device）]** の順に選択します。

ステップ 2 ダッシュボードの右上隅にある **[設定（Settings）]** をクリックして、**[ダッシュレットの追加（Add Dashlets）]** を選択します。

ステップ 3 [デバイス ダッシュレット（Device Dashlets）] リストを展開します。

ステップ 4 [汎用ダッシュレット（Generic Dashlet）] を見つけて、**[Add]** をクリックします。

Prime Infrastructure により、空白の汎用ダッシュレットが [デバイス トレンド（Device Trends）] ダッシュボードに追加されます。



ステップ 5 必要に応じて新しいダッシュレットを設定します。

少なくとも、次の設定を行う必要があります。

- [ダッシュレット タイトル（Dashlet Title）] フィールドに、わかりやすいタイトルを入力します。
- ダッシュボード内のすべてのダッシュレットに時間フィルタを適用しない場合は、[ダッシュボードの時間フィルタをオーバーライドする（Override Dashboard Time Filter）] チェックボックスをオンにします。
- [タイプ（Type）] ドロップダウン リストで、ダッシュレットのデータを表または線グラフのどちらで表示するかを選択します。（どちらを選択するかに関わらず、Prime Infrastructure では、ダッシュレットの下部に、表示形式を変更するためのトグルが表示されます）。
- [ポリシー名（Policy Name）] ドロップダウン リストから、このダッシュレットのデータを収集するモニタリング ポリシーを選択します。

ステップ 6 **[保存して閉じる（Save and Close）]** をクリックします。

新しいダッシュボードの追加

新しいダッシュボードを作成するには、次の手順を実行します。新しいダッシュボードは、ダッシュボードのタイプ （9 ページ）にリストされているダッシュボードの 1 つに、新しいタブとして表示されます。

ステップ 1 関連する既存のダッシュボードを開きます。

たとえば、[パフォーマンス（Performance）] ダッシュボードに新しいタブを作成するには、**[ダッシュボード（Dashboard）] > [パフォーマンス（Performance）]** にあるいずれかのタブをクリックします。

ステップ 2 [+]（[新しいダッシュボードの追加（Add New Dashboard）]）タブをクリックします。

[設定（Settings）] メニューが開きます。

ステップ 3 新しいダッシュボードの名前を入力し、**[Apply]** をクリックします。

ステップ 4 新しいダッシュボード タブをクリックし、事前定義のダッシュレットをダッシュボードに追加する （15 ページ）の説明に従ってダッシュレットを追加します。

ダッシュレット データの CSV または PDF ファイルへのエクスポート

パフォーマンス ダッシュボード内のさまざまなコンポーネントのダッシュレット データを CSV または PDF ファイルにエクスポートできます。ダッシュレット データをエクスポートするには、次の手順を実行します。

ステップ 1 [ダッシュボード（Dashboards）] > [パフォーマンス（Performance）] を選択します。

ステップ 2 パフォーマンス ダッシュボードのダッシュボードを選択し、利用可能なダッシュレットを表示します。

ステップ 3 ダッシュレットデータをエクスポートするには、右上隅の [すべてをエクスポート（Export All）] をクリックします。[エクスポート（Export）] ダイアログ ボックスには、ファイル形式およびダッシュレットが表示されます。

（注） ダッシュレットが空の場合、[エクスポートできるコンテンツがありません（No exportable Content）] というポップアップ メッセージが表示されます。

ステップ 4 エクスポートするファイル形式（CSV または PDF）を選択します。

（注） PDF 形式を選択する場合は、テーブル、グラフ、またはその両方を選択できます。

ステップ 5 すべてのダッシュレットまたは必要なダッシュレットを選択し、[エクスポート（Export）] をクリックします。

（注） 次のダッシュレットでは、[すべてをエクスポート（Export All）] 機能はサポートされていません。

- デバイスの到達可能性ステータス
- トップ N のアラーム タイプ（Top N Alarm Types）
- アラーム数トップ N のデバイス（Top N Devices with Most Alarms）
- トップ N のイベント（Top N Events）
- トップ N の Syslog 送信者（Top N Syslog Sender）
- デバイス ポートの概要
- インターフェイスの詳細（Interface Details）

ダッシュボードを使用したネットワークヘルスのトラブルシューティング

Prime Infrastructure で **[ダッシュボード（Dashboard）] > [ネットワークサマリー（Network Summary）] > [ネットワークヘルス（Network Health）]** を選択すると、ネットワークおよびサイトのヘルスを簡単に確認できます。ロケーショングループを作成して、このロケーションにデバイスを追加する必要があります。Prime Infrastructure にすべてのサイトの全体的なヘルスを示すマップが表示されます。[ネットワークヘルス（Network Health）] ページでは、有線と無線のデバイス間で表示を切り替えることができます。デフォルトでは、ロケーション グループごとにロケーションと最大 500 個の AP がすべて表示されます。[有線（Wired）] ビューを選択した場合、[ネットワークヘルス（Network Health）] ページには、**WAN インターフェイスの使用率**の詳細と、すべてのロケーションの有線デバイスの全体的なヘルス ステータスを示すマップが表示されます。[ワイヤレス（Wireless）] ビューを選択した場合、[ネットワークヘルス（Network Health）]ページには、**ワイヤレス クライアント数**の詳細と、すべてのサイトのワイヤレス デバイスの全体的なヘルス ステータスを示すマップが表示されます。[ワイヤレス（Wireless）] ビューで、[エグゼクティブビュー（Executive View）] 展開アイコンをクリックして、クライアント、アクセスポイント、環境（Clean Air）、およびアプリケーションのダッシュボードのいずれかを選択します。[ネットワークヘルス（Network Health）] ページに、選択したダッシュボードに対応するダッシュレットが表示されます。設定アイコンをクリックすると、ダッシュレットをさらに追加できます。ダッシュボードをクロス起動するには、[その他（more）] をクリックします。

関連トピック

ヘルス ルールの定義 （20 ページ）
ネットワーク ヘルス マップ機能 （21 ページ）
ネットワーク ヘルスの概要 （23 ページ）

QoS およびインターフェイスの設定の定義 （21 ページ）
QoS メトリック （24 ページ）
トラフィック カンバセーション （25 ページ）
ロケーション グループの作成 （68 ページ）

ヘルス ルールの定義

サイトのルールおよびしきい値を指定できます。指定したルールに応じて、**[ダッシュボード（Dashboard）]** > **[ネットワークの概要（Network Summary）]** > **[ネットワーク ヘルス（Network Health）]** に表示される通知が決定されます。

ステップ 1 **[サービス（Services）]** > **[アプリケーションの可視性と制御（Application Visibility & Control）]** > **[ヘルス ルール（Health Rule）]** の順に選択します。ヘルス ルールを指定できる 3 つのタブがあります。

- [サービスヘルス（Service Health）]：ジッター、MOS スコア、ネットワーク時間、パケット損失、トラフィック レートなど、サービスのヘルス ルールを定義します。
- [インフラストラクチャヘルス（Infrastructure Health）]：CPU 使用率、メモリ ロス使用率、環境温度など、有線デバイスのヘルス ルールを定義します。
- [ワイヤレスヘルス（Wireless Health）]：クライアント カバレッジ、クライアント オンボーディング、クライアント数、CPU 使用率、メモリ使用率など、ワイヤレス デバイスのヘルス ルールを定義します。

（注） クライアント数に設定されているデフォルトの重大しきい値および警告しきい値は、それぞれ 40 と 36 です。クライアント数の最大の重大しきい値は、1000 に設定できます。

ステップ 2 新しいヘルス ルールを追加するには、[+] アイコンをクリックし、ロケーション、メトリック、およびしきい値を指定します。新しいインフラストラクチャ ヘルスおよびワイヤレス ヘルス ルールのみを追加できます。

ステップ 3 既存のヘルス ルールを編集するには、変更するヘルス ルールを選択し、[編集（Edit）] をクリックします。

ステップ 4 ヘルス ルールの詳細を入力し、[保存（Save）] をクリックします。

入力した値は、ヘルス ルールが適用されるロケーション グループ内にあるすべてのデバイスおよびインターフェイスに適用されます。

関連トピック

ネットワーク ヘルス マップ機能 （21 ページ）
ネットワーク ヘルスの概要 （23 ページ）
ロケーション グループの作成 （68 ページ）

QoS およびインターフェイスの設定の定義

ヘルス ページでは、[ネットワークヘルス（Network Health）] ページでのヘルス スコアの計算から QoS、管理上のダウン インターフェイス、CPU、およびメモリ インスタンスを除外できます。

ステップ 1 **[サービス（Services）] > [アプリケーションの可視性と制御（Application Visibility & Control）] > [ヘルス ルール（Health Rule）]** の順に選択します。

または、[ネットワーク ヘルス（Network Health）] ページで [ヘルス ルールの起動（Launch Health Rules）] リンクをクリックします。

ステップ 2 [インフラストラクチャ ヘルス（Infrastructure Health）] タブをクリックします。

ステップ 3 [詳細設定（Advanced Settings）] ボタンをクリックします。[QoS/設定（QoS/Settings）] タブおよび [CPU/メモリインスタンス（CPU/Memory Instance）] タブで、ヘルス スコアの計算から除外するチェック ボックスをオンにします。デフォルトでは、[Scavengerの除外（Exclude Scavenger）] チェック ボックスおよび [管理上のダウンインターフェイスの除外（Exclude Admin Down Interface）] チェック ボックスがオンになっており、ヘルス スコアの計算で考慮されなくなっています。これらを含める場合はオフにします。

ステップ 4 [保存して閉じる（Save and Close）] をクリックします。変更は、次回のジョブ実行時に適用されます。

ネットワーク ヘルス マップ機能

[ダッシュボード（Dashboard）] > [ネットワークサマリー（Network Summary）] > [ネットワークヘルス（Network Health）] を選択すると、以前に追加した地理的属性を持つすべてのロケーション グループがマップに表示されます。デフォルトでは、ロケーション グループごとに最大 500 個の AP が表示されます。

ロケーション グループは、ロケーション全体のヘルスに応じて色分けされます。

- 赤：ロケーションに重大な問題があることを示しています。
- 黄色：ロケーションに警告があることを示しています。
- 緑：エラーおよび警告がないことを示しています。
- 灰色：ロケーションにデバイスまたはデータがないことを示しています。

正常性を示す色に加えて、アイコンは次のようになります。

- 実線：親サイトを示します。つまり、このサイトに関連付けられた子ロケーションがあります。
- 破線：このロケーションに関連付けられた子がないことを示します。

マップの任意のロケーション上にマウスを移動すると、このロケーションのサイトとエラーおよび警告をデバイス タイプ別に示すポップアップ ウィンドウが表示されます。

サイト名をクリックすると、サイトの拡大マップが表示されます。

関連トピック

ヘルス ルールの定義 （20 ページ）
ネットワーク ヘルス表示オプション （22 ページ）
ネットワーク ヘルスの概要 （23 ページ）
ロケーション グループの作成 （68 ページ）

ネットワーク ヘルス表示オプション

[ダッシュボード（Dashboard）] > **[ネットワークサマリー（Network Summary）]** > **[ネットワークヘルス（Network Health）]** を選択すると、次の図に示すように、ページの右側に表示オプションが表示されます。

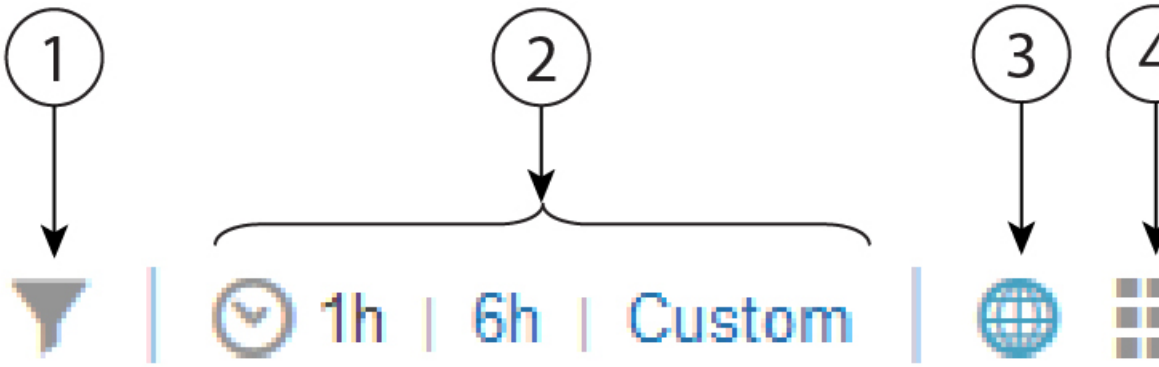


表 *5:* ネットワーク ヘルスの表示

1	フィルタ オプション。選択したオプションによって、マップおよび[ヘルスの概要（Health Summary）] ペインに表示される内容が変わります。すべてのフィルタを削除するには、**[クリア（Clear）]** > **[選択項目（Selection）]** をクリックします。
2	タイム フレーム。デフォルトでは、過去 6 時間の情報が [サイトの可視性（Site Visibility）] マップおよび [ヘルスの概要（Health Summary）] ペインに表示されます。
3	左側のペインにマップが表示されます。
4	[ヘルス インデックス（Health Index）] ビューにネットワーク ヘルスの概要が表示されます。
5	表形式でネットワーク ヘルスの概要が表示されます。
6	右側の [ヘルスの概要（Health Summary）] ペインの表示と非表示を切り替えます。

関連トピック

ヘルス ルールの定義 （20 ページ）
ネットワーク ヘルス マップ機能 （21 ページ）
ネットワーク ヘルスの概要 （23 ページ）

ロケーション グループの作成 （68 ページ）

ネットワーク ヘルスの概要

[ヘルスの概要（Health Summary）] ペインには、すべてのロケーション上のすべてのデバイスのエラーおよびしきい値違反が表示されます。Prime Infrastructure は、デバイスやサービスのヘルス データを、15 分ごとにサイトの概要情報として集約します。[有線（Wired）] タブをクリックすると、ルータ、スイッチ、およびサービス ヘルスの詳細のヘルスの概要が表示されます。[有線（Wired）] の [ヘルスの概要（Health Summary）] ペインに表示されたサイトまたはデバイスをクリックすると、詳細が表示されます。

[ルータ（Router）]：CPU、メモリ、温度などのサイト/デバイス ワイズ ルータ ステータスが表示されます。

[スイッチ（Switch）]：CPU、メモリ、温度などのサイト/デバイス ワイズ スイッチ ステータスが表示されます。

[サービスヘルス（Service Health）]：サービス ヘルスに関連するエラーまたは警告が発生する領域が表示されます。

[エグゼクティブ表示（Executive View）]

- [ネットワークデバイス（Network Devices）]：上位 N の CPU 使用率、上位 N のメモリ使用率などのネットワーク デバイスに関連するダッシュレットが表示されます。
- [ネットワークインターフェイス（Network Interfaces）]：上位 N の インターフェイス使用率 Tx、上位 N の インターフェイス使用率 Rx などのネットワーク インターフェイスに関連するダッシュレットが表示されます。
- [アプリケーション（Applications）]：有線デバイス データでフィルタリングされたアプリケーションに関連するダッシュレットが表示されます。

[ワイヤレス（Wireless）] タブをクリックすると、アクセス ポイント、コントローラ、クライアント %、サービス ヘルスの詳細が表示されます。[ワイヤレス（Wireless）] の [ヘルスの概要（Health Summary）] ペインに表示されたサイトまたはデバイスをクリックすると、詳細が表示されます。

[アクセスポイント（Access Point）]：クライアント数、可用性、カバレッジの問題、オンボーディングの問題など、アクセス ポイントのヘルス メトリックが表示されます。サイト ステータスに影響しない他のメトリックは、一般的なヘルス メトリックでグループ化されます。

[コントローラ（Controller）]：CPU とメモリに関連する問題が表示されます。

[クライアント（%）（Client (%)）]：カバレッジ、オンボーディングの問題などがあるクライアントが表示されます。

（注） ネットワーク ヘルス ダッシュボードのクライアント データ（カバレッジとオンボーディング）は WLC 8.6 以降のバージョンでサポートされます。

サイト名の横にある設定アイコンをクリックすると、サイトのヘルスルール設定を編集できます。変更されたヘルス ルール設定は、[ヘルスルール（Health Rules）] ページで自動的に更新されます。サイトにヘルスルールが割り当てられていない場合、そのサイトに表示されるヘルス ルールは親サイトのヘルス ルールを表します。

[エグゼクティブ表示（Executive View）]

- [クライアント（Client）]：クライアント カバレッジ、クライアントのオンボーディングの問題などがあるダッシュレットが表示されます。
- [アクセスポイント（Access Point）]：オンボーディングの問題、カバレッジの問題などのある上位 N の AP に関連するダッシュレットが表示されます。
- [電波品質（Air Quality）]：平均電波品質、最も深刻な干渉、干渉数など、電波品質に関連するダッシュレットが表示されます。
- [アプリケーション（Applications）]：有線デバイス データでフィルタリングされたアプリケーションに関連するダッシュレットが表示されます。

（注） [詳細（More）] をクリックすると、特定のダッシュボードが並列起動されます。

[マップビュー（Map view）]：サイト名をクリックすると、そのサイトのマップが拡大され、詳細情報が表示されます。マップ ビュー設定を変更するには、[ヘルスルールの起動（Launch Health Rules）] の横の右上にある設定アイコンをクリックします。

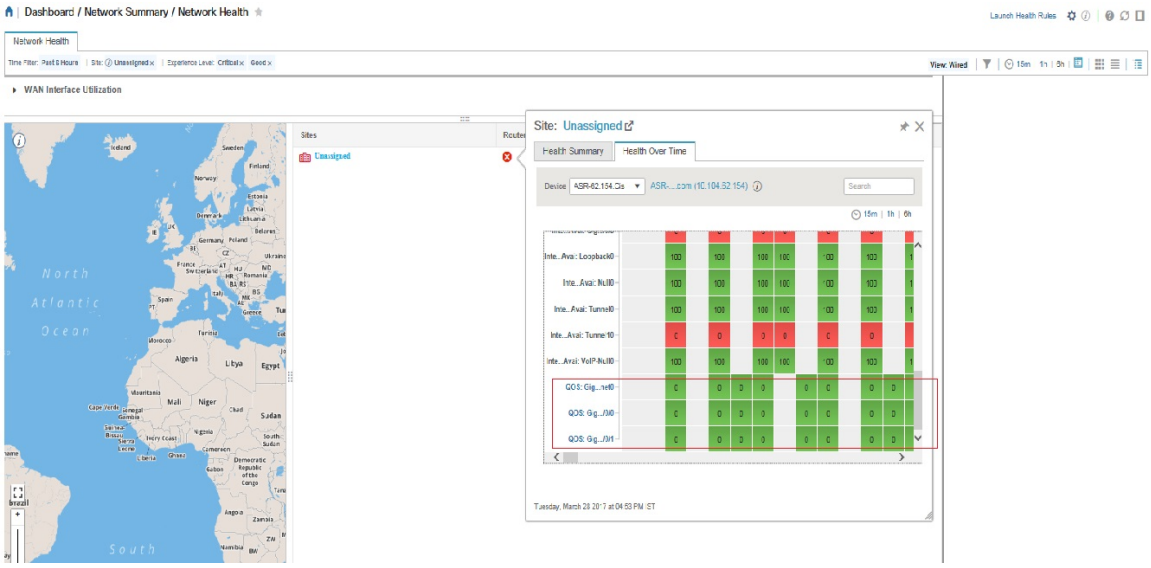
（注） デフォルトでは、マップ ビューは [エグゼクティブ表示（Executive View）] 内に含まれています。

関連トピック

ヘルス ルールの定義 （20 ページ）
ネットワーク ヘルス マップ機能 （21 ページ）
ロケーション グループの作成 （68 ページ）

QoS メトリック

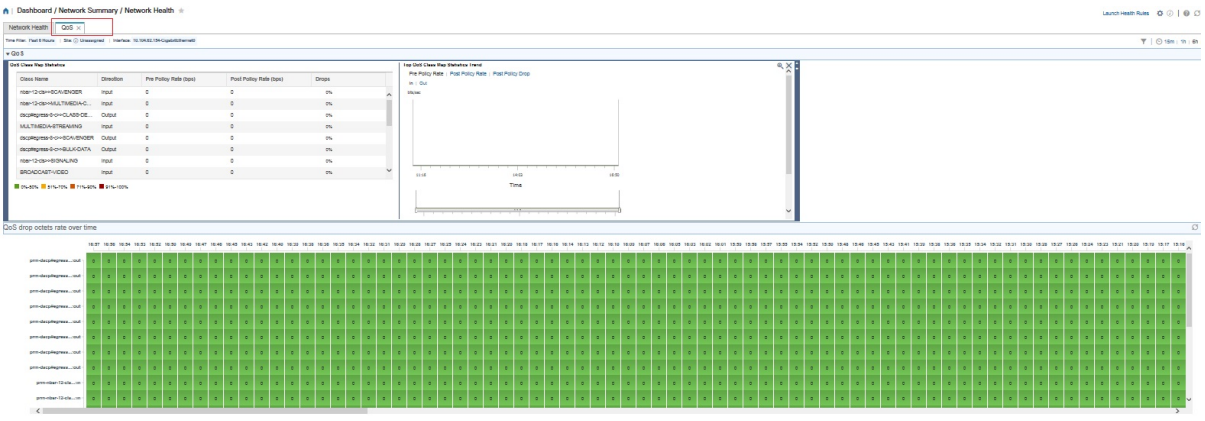
[ネットワークヘルス（Network Health）] ページには、ルータおよびスイッチの QoS メトリックが表示されます。ヒートマップの QoS ハイパーリンク、[ヘルスの概要（Health Summary）] ビュー、[ヘルスインデックス（Health index）] ビュー、および [テーブル（Table）] ビューをクリックして、[ネットワークヘルス（Network Health）] ページでルータ、スイッチ、およびインターフェイスの [QoS] タブを起動できます。ルータとスイッチのヒートマップには、インターフェイス レベルごとに集約された QoS データと、各インターフェイスのすべての QoS クラスおよびすべての方向の dropOctetsRate の平均値が表示されます。



[ネットワークヘルス（Network Health）] ページの [QoS] タブをクリックすると、選択したインターフェイスのクラス マップごとのデータがより詳細に表示されます。[QoS] タブには、次の詳細が表示されます。

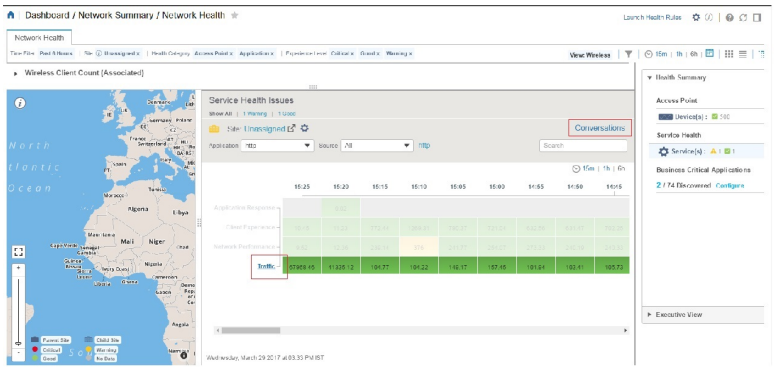
- QoS クラス マップの統計情報
- 上位の QoS クラス マップ統計情報の傾向
- 時系列の QoS ドロップ オクテット率

[QoS] タブには、特定のインターフェイスのクラス マップごとに詳細が表示されます。



トラフィック カンバセーション

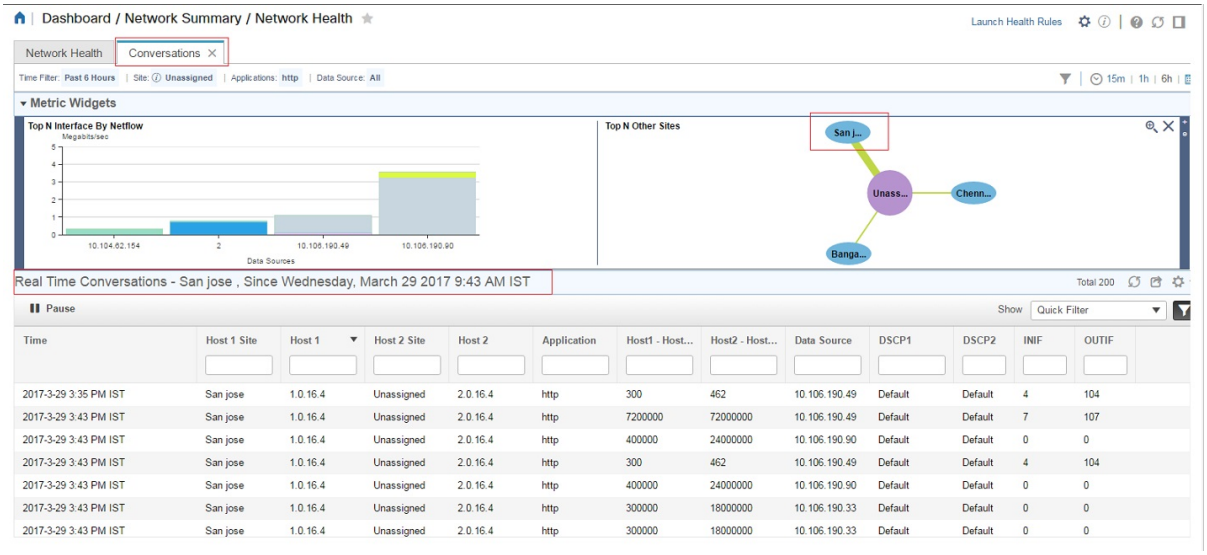
ヒートマップのトラフィック ハイパーリンクまたは下の図に示すように [会話（Conversations）] ハイパーリンクをクリックして、[ネットワークヘルス（Network Health）] ページの [会話（Conversation）] タブを起動できます。



[会話（Conversation）] タブには、次の詳細が表示されます。

- [Netflow別上位Nのインターフェイス（Top N Interface By Netflow）] チャート
- [上位Nのその他のサイト（Top N Other Sites）] グラフ
- [リアルタイムカンバセーション（Real Time Conversation）] テーブル

[リアルタイムカンバセーション（Real Time Conversation）] テーブルには、グローバル フィルタ（[サイト（Site）]、[アプリケーションデータソース（Application Data Source）]、および [時間（Time）] フィルタ）に基づくカンバセーションが表示されます。特定のサイトまたはインターフェイスのリアルタイム カンバセーションを表示する場合は、[上位Nのその他のサイト（Top N Other Sites）] グラフ内のサイトまたは [Netflow別上位Nのインターフェイス（Top N Interface By Netflow）] チャート内のインターフェイスをクリックします。[リアルタイムカンバセーション（Real Time Conversation）] テーブルでは最大 4000 のレコードを表示でき、レコードは 1 分ごとに自動的に更新されます。



別の仮想ドメインで作業する

仮想ドメインは、デバイスの論理的なグループであり、特定のサイトやデバイスへのアクセスを制御するために使用されます。仮想ドメインは、物理サイト、デバイス タイプ、ユーザ コミュニティ、または管理者が選択するあらゆる指定項目に基づいて設定できます。すべてのデバイスはROOT-DOMAINに属します。ROOT-DOMAINはすべての新しい仮想ドメインの親ドメインです。仮想ドメインの詳細については、『*Cisco Prime Infrastructure Administrator Guide*』の「Create Virtual Domains to Control User Access」を参照してください。

複数の仮想ドメインへのアクセスが許可されている場合は、次の手順に従って別のドメインに切り替えることができます。

ステップ 1 タイトル バーの右側にある ⚙ をクリックします。

ステップ 2 [**Virtual Domain:** *current-domain*] を選択します。

ステップ 3 [仮想ドメイン（Virtual Domain）] ドロップダウン リストで別のドメインを選択します。

Prime Infrastructure によって作業ドメインがただちに変更されます。

ジョブ ダッシュボードを使用したジョブの管理

適切なユーザ アカウント権限が付与されている場合は、ジョブ ダッシュボードを使用してPrime Infrastructure ジョブを管理できます。ジョブ ダッシュボードを表示するには、**[管理（Administration）] > [ダッシュボード（Dashboards）] > [ジョブ ダッシュボード（Job Dashboard）]** の順に選択します。ここでは、ジョブが正常に完了したか、部分的に成功したか、または失敗したかを確認できます。

実行中のジョブの数が多すぎると、Prime Infrastructure ではリソースが使用可能になるまで他のジョブがキューに入れられます。これが原因で、スケジュールされているジョブがその通常の開始時刻を超えて遅延されると、そのジョブは実行されません。このジョブは手動で実行する必要があります。

一部のジョブでは承認が必要です。この場合は、Prime Infrastructure から、管理者権限が付与されているユーザに対し、ジョブがスケジュールされており承認が必要であることを通知するメールが送信されます。ジョブの承認後にジョブが実行されます。

次の表に、ジョブ ダッシュボードに表示されるボタンの説明を示します。

表 *6:* ジョブ ダッシュボードのボタン

ボタン	説明
[ジョブの削除（Delete Job）]	ジョブ ダッシュボードからジョブを削除します。

ボタン	説明
[ジョブの編集（Edit Job）]	選択したジョブの設定を編集します。
[スケジュールの編集（Edit Schedule）]	シリーズのスケジュールを表示し、編集できるようにします（開始時刻、間隔、終了時刻）。 （注） スケジュール済みのジョブのスケジュールを編集すると、そのジョブのステータスが [承認待ち（Pending for Approval）] に変更されます。これは、ジョブを作成したユーザからの承認が編集のたびに必要になるためです。
[実行（Run）]	選択したジョブの新しいインスタンスを実行します。このボタンは、部分的に成功したジョブまたは失敗したジョブを再実行する場合に使用します。ジョブは、失敗したコンポーネントまたは部分的に成功したコンポーネントに対してのみ実行されます。
[中断（Abort）]	現在実行中のジョブを停止します。ただしこのジョブは後で再実行できます。すべてのジョブを中断することはできません。これに該当する場合、Prime Infrastructure がそのことを示します。
[シリーズをキャンセル（Cancel Series）]	現在実行中のジョブを停止し、このジョブを再実行できないようにします。ジョブがシリーズの一部の場合、今後の実行には影響しません。
[シリーズの一時停止（Pause Series）]	スケジュールされているジョブ シリーズを一時停止します。シリーズを一時停止にすると、（[実行（Run）]を使用して）そのシリーズのインスタンスを実行することはできません。
[シリーズの再開（Resume Series）]	一時停止になっていたスケジュール済みジョブ シリーズを再開します。

（注） [ジョブの削除（Delete Job）]、[中断（Abort）]、および[シリーズをキャンセル（Cancel Series）]ボタンは、システム ジョブとポーラー ジョブの場合は使用できません。

ジョブの詳細を表示するには、次の手順に従います。

ステップ 1 **[管理（Administration）] > [ダッシュボード（Dashboards）] > [ジョブ ダッシュボード（Job Dashboard）]** の順に選択します。

ステップ 2 [ジョブ（Jobs）]ペインで、基本的な情報（ジョブ タイプ、ステータス、ジョブ期間、次回開始時刻など）を取得するジョブ シリーズを選択します。

ステップ 3 ジョブ間隔を表示するには、ジョブ インスタンスのハイパーリンクをクリックします。

ジョブ ページ上部の [繰り返し（Recurrence）] フィールドに、ジョブの繰り返し頻度が表示されます。ジョブ間隔の詳細は、トリガーするすべてのジョブで追加されます。

ステップ 4 失敗したジョブまたは部分的に成功したジョブに関する詳細を確認するには、ジョブ インスタンスのハイパーリンクをクリックし、結果ページに表示されるエントリを展開します。

これは特に、インベントリ関連のジョブで便利です。たとえば、ユーザがCSVファイルを使用してデバイスをインポートした場合（一括インポート）、ジョブは [ジョブ（Jobs）] サイドバー メニューの **[ユーザ ジョブ（User Jobs）] > [デバイスの一括インポート（Device Bulk Import）]** に表示されます。ジョブの詳細には、正常に追加されたデバイスと、追加されなかったデバイスのリストが表示されます。

例

失敗したソフトウェア イメージ インポート ジョブのトラブルシューティングを行うには、次の手順に従います。

1. [ジョブ（Jobs）] サイドバー メニューから、**[ユーザ ジョブ（User Jobs）] > [ソフトウェア イメージのインポート（Software Image Import）]** を選択します。
2. テーブルにある失敗したジョブを見つけ、そのハイパーリンクをクリックします。
3. ジョブの詳細がまだ展開されていない場合には展開し、このジョブに関連付けられているデバイスのリストと、各デバイスのイメージ インポートのステータスを表示します。
4. 特定デバイスのインポートの詳細情報を表示するには、[ステータス（Status）] 列でそのデバイスの [i]（**情報**）アイコンをクリックします。こうすると、[イメージ管理ジョブの結果（Image Management Job Results）] ポップアップ ウィンドウが開きます。
5. 各ステップとステータスを確認します。たとえば、[プロトコル SFTP を使用したイメージの収集（Collecting image with Protocol: SFTP）] 列に、そのデバイスで SFTP がサポートされていないことが示されることがあります。

Cisco Prime Infrastructure 機能の拡張

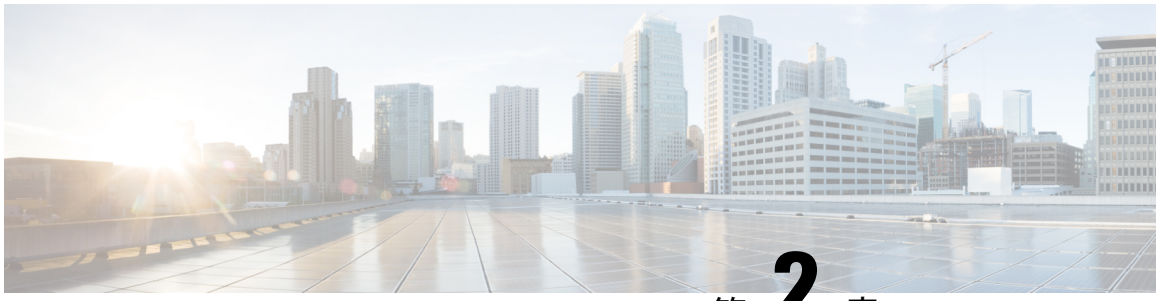
アドバンス ユーザは、Cisco Prime Infrastructure REST API を使用して Cisco Prime Infrastructure 機能を拡張し、管理オプションを管理できます。

このツールに関する情報を入手するには、Prime Infrastructure Web GUI の右上にある ⚙ をクリックし、**[ヘルプ（Help）] > [REST API]** を選択します。『Cisco Prime Infrastructure API Reference Guide』は Cisco.com から直接ダウンロードすることもできます。

最新のインベントリに存在をチェック マニュアル

Prime Infrastructure で提供されているすべてのドキュメントに関する情報およびリンクについては、『 Cisco Prime Infrastructure Documentation Overview 』を参照してください。

（注） マニュアルの発行後に、マニュアルをアップデートすることがあります。マニュアルのアップデートについては、Cisco.com で確認してください。



第 2 章

Prime Infrastructure のユーザ設定の変更

- ユーザ設定 （31 ページ）
- ユーザ設定の変更 （31 ページ）
- アイドル ユーザ タイムアウトの変更 （32 ページ）
- リストの長さの変更 （33 ページ）

ユーザ設定

Prime Infrastructure のユーザ プリファレンス設定を使用して、情報の表示方法を変更することができます。

- ユーザ設定の変更
- アイドル ユーザ タイムアウトの変更
- リストの長さの変更

ユーザ設定の変更

ユーザ プリファレンスを変更するには、[設定（Settings）] アイコン（メニュー バーの右側にある歯車アイコン）をクリックして [マイプリファレンス（My Preferences）] を選択し、[マイプリファレンス（My Preferences）] ページに表示される設定を変更します。

関連トピック

アイドル ユーザ タイムアウトの変更 （32 ページ）
リストの長さの変更 （33 ページ）
アラームとイベントの表示設定のセットアップ （360 ページ）
Prime Infrastructure の構成 （1 ページ）

アイドル ユーザ タイムアウトの変更

Prime Infrastructure は、アイドル ユーザが自動的にログアウトするタイミングと方法を制御する 2 つの方法を提供します。

- [ユーザ アイドル タイムアウト（User Idle Timeout）]：タイムアウトになったときにユーザセッションを自動的に終了するこの設定を無効にするか設定することができます。この設定はデフォルトで有効になっており、10 分に設定されています。[ユーザ アイドル タイムアウト（User Idle Timeout）] の値は、[グローバル アイドル タイムアウト（Global Idle Timeout）] の値未満にする必要があります。
- [グローバル アイドル タイムアウト（Global Idle Timeout）]：デフォルトで有効になっており、10 分に設定されています。管理者権限を持つユーザのみが [グローバル アイドル タイムアウト（Global Idle Timeout）] の設定を無効化したり、そのタイムリミットを変更できます。

（注） Prime Infrastructure は、より小さいタイムアウト値に基づいてアイドル ユーザをログアウトします。

たとえば、アイドルセッションによりオペレーションセンターのユーザが突然ログオフされ、オペレーション センターによって管理される 1 つ以上の Prime Infrastructure インスタンスがある場合には、ユーザアイドルタイムアウト機能を無効にすると役立ちます。詳細については、『Cisco Prime Infrastructure Administrator Guide』の「Set Up the Prime Infrastructure Server」の章の「*Disable Idle User Timeouts for Operations Center*」の項を参照してください。.

タイムアウト設定を変更するには、次の手順を実行します。

ステップ 1 [Settings] アイコンをクリックし、[My Preferences] を選択します。

ステップ 2 [User Idle Timeout] で次の手順を実行作します。

- [Logout all idle user] の横にあるチェックボックスのオン/オフを切り替えて、アイドル タイムアウトを有効化または無効化します。
- [Logout all idle user after] ドロップダウン リストから、いずれかのアイドル タイムアウト リミットを選択します。

ステップ 3 [Save] をクリックします。変更を有効にするには、いったんログアウトして再度ログインする必要があります。

詳細については、『Cisco Prime Infrastructure Administrator Guide』の「Set Up the Prime Infrastructure Server」の章の「*Disable Idle User Timeouts for Operations Center*」の項を参照してください。.

関連トピック

ユーザ設定の変更 （31 ページ）

リストの長さの変更

Prime Infrastructure では、一部のリストにデフォルトで表示されるエントリ数を変更できます。[リストあたりの項目数（Items Per List）] 設定は、以下のモニタリング ページに表示されるエントリの数に影響します。

- [AP]
- [コントローラ（Controllers）]
- [サイト マップ（Site Maps）]
- [メッシュ（Mesh）]
- [CleanAir]

[リストあたりの項目数（Items Per List）] 設定は、ネットワーク デバイス、アラームおよびイベント、設定アーカイブ、ソフトウェア イメージの管理、ソフトウェア イメージの管理、設定には適用されません。

50 項目の平均値が所定のページに表示されます。

ステップ 1 [Settings] アイコンをクリックし、[My Preferences] を選択します。

ステップ 2 [Items Per List Page] ドロップダウン リストで設定を変更します。

ステップ 3 [Save] をクリックします。

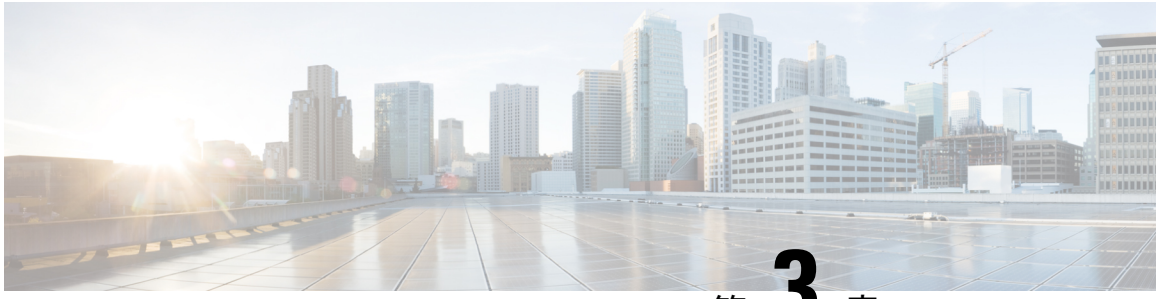
関連トピック

ユーザ設定の変更 （31 ページ）

第 II 部

インベントリの管理

- デバイスの追加と整理 （37 ページ）
- デバイスの表示 （77 ページ）
- コンピューティング リソースの管理 （91 ページ）
- デバイス コンフィギュレーション ファイルの管理 （95 ページ）
- デバイス ソフトウェア イメージの管理 （113 ページ）
- コンプライアンスを使用した設定の監査の実行 （153 ページ）



第 3 章

デバイスの追加と整理

この章は、次の内容で構成されています。

- Prime Infrastructure へのデバイスの追加 （37 ページ）
- 他のソースからのデバイスのインポート （44 ページ）
- デバイスのインポート CSV ファイルの作成 （44 ページ）
- 手動によるデバイスの追加（新規デバイス タイプまたはデバイス シリーズ） （46 ページ）
- ワイヤレス コントローラを追加するための前提条件 （50 ページ）
- 追加されたデバイスの検証と問題のトラブルシューティング （51 ページ）
- NAM HTTP/HTTPS クレデンシャルの追加 （56 ページ）
- CSV ファイルへのデバイス情報のエクスポート （57 ページ）
- クレデンシャル プロファイルを使用したデバイス クレデンシャルの一貫した適用 （58 ページ）
- 簡単な管理と設定のためのデバイス グループの作成 （60 ページ）

Prime Infrastructure へのデバイスの追加

Cisco Prime Infrastructure はデバイス、ロケーション、およびポート グループを使用して、ネットワーク内の要素を整理します。デバイスをテーブルまたはマップ（ネットワーク トポロジ）で表示すると、デバイスは属しているグループを単位として整理されます。デバイスが Prime Infrastructure に追加されると、**Unassigned Group** という名前のグループに割り当てられます。その後、簡単な管理と設定のためのデバイス グループの作成 （60 ページ） で説明されているように、デバイスを目的のグループに移動できます。

（注） Prime Infrastructure は、Cisco 9k デバイスの Stackwise Virtual Link（SVL）をサポートしていません。

メモ **Catalyst 9800 シリーズ** デバイスが AP およびクライアントの運用データを Prime Infrastructure に送信するように指定するには、次のことを確認します。

- NETCONF-YANG をグローバルに有効にします。次を使用して設定できます。

```
device# conf t
device(config)# netconf-yang
```

- アクセスに SSH/Telnet を使用するデバイスを Cisco Prime Infrastructure で管理できる特権 *15* を持ったユーザがいます。以下を使用できます。

```
username cisco1 privilege 15 password 0 cisco1
```

- 次のコマンドを使用して AAA new-model を有効にします。

```
device(config)# aaa new-model
```

NETCONF-SSH 接続および edit-config 操作を設定します。

```
aaa authorization exec default local
```

- Prime Infrastructure がクライアントを検出できない場合は、デバイスでクライアントの検出に必要な以下の CLI を検証してください。

```
wireless client onboarding-event
```

（注） ASR 9900 のデバイス セットは、Prime Infrastructure によって効果的に監視されるように、**netconf agent tty** コマンドと **xml agent tty** コマンドを使用して設定する必要があります。

表 *7:* デバイスの追加方法

サポートされているデバイスの追加方法	参照先：
以下を使用してシード デバイスのネイバーを検出して複数のデバイスを追加する	ディスカバリを使用したデバイスの追加（39 ページ）。
• Ping スイープと SNMP ポーリング（クイック ディスカバリ）	• クイック ディスカバリの実行 （41 ページ）
• カスタマイズされたプロトコル、クレデンシャル、およびフィルタ設定（ディスカバリ ジョブを繰り返す場合に便利）	• カスタマイズされたディスカバリ設定でのディスカバリの実行 （42 ページ）
CSV ファイルで指定された設定を使用して複数のデバイスを追加する	他のソースからのデバイスのインポート（44 ページ）

サポートされているデバイスの追加方法	参照先：
単一のデバイスを追加する（たとえば、新しいデバイス タイプの場合）	手動によるデバイスの追加（新規デバイス タイプまたはデバイス シリーズ） （46 ページ）

ディスカバリ プロセスについて

Prime Infrastructure は、ディスカバリ プロセス中に次の手順を実行します。

1. ICMP ping を使用して、各デバイスが到達可能かどうかを確認します。Prime Infrastructure がデバイスに到達できない場合は、デバイスの到達可能性ステータスが [到達不能（Unreachable）] となります。
2. SNMP クレデンシャルを確認します。デバイスが ICMP で到達できるが、SNMP クレデンシャルが無効な場合は、デバイスの到達可能性ステータスが [Ping Reachable] となります。

   デバイスが ICMP および SNMP の両方で到達できる場合は、デバイスの到達可能性ステータスが [到達可能（Reachable）] となります。
3. Telnet および SSH のクレデンシャルを確認します。
4. Prime Infrastructure が必要な通知を受信できるように、デバイス設定を変更してトラップ レシーバを追加します。
5. インベントリ収集プロセスを開始して、すべてのデバイス情報を収集します。
6. **[インベントリ（Inventory）]** > **[ネットワークデバイス（Network Devices）]** ページにデバイスを追加します。

検出を実行した後、**[インベントリ（Inventory）]** > **[デバイス管理（Device Management）]** > **[ネットワークデバイス（Network Devices）]** を選択して、その検出が完了したことを確認します。

ディスカバリを使用したデバイスの追加

Prime Infrastructure は、次の 2 つのディスカバリ方式をサポートしています。

- シード デバイスからの ping スイープ（クイック ディスカバリ）。デバイス名、SNMP コミュニティ、シード IP アドレス、およびサブネット マスクが必要です。クイック ディスカバリの実行 （41 ページ）を参照してください
- カスタマイズされたディスカバリ方法（ディスカバリ設定）の使用：設定を行い、今後ディスカバリを再実行する場合は、この方法をお勧めします。カスタマイズされたディスカバリ設定でのディスカバリの実行 （42 ページ）を参照してください。

（注）

- ディスカバリ ジョブが既存のデバイスを再検出し、デバイスの最後のインベントリ収集ステータスが [完了済み（Completed）] である場合、Prime Infrastructure は、既存のクレデンシャルを、ディスカバリ設定で指定されたクレデンシャルで上書きしません。他のすべてのステータス（既存のデバイス上）の場合、Prime Infrastructure は、デバイスのクレデンシャルを、ディスカバリ設定で指定されたクレデンシャルで上書きします。
- データベースのメンテナンス期間中に多数のデバイスが追加された場合、サービス検出に通常より時間がかかることがあります。したがって、夜間や週末には大規模な作業を回避することをお勧めします。
- 自律 AP がディスカバリ プロセスから除外され、検出時間が最適化されます。[デバイスのインポート（Import Devices）] または [クレデンシャルプロファイル（Credential Profile）] を使用して、自律 AP を手動で追加する必要があります。

デバイスのディスカバリ プロセスは、次に示す順序で実行されます。Prime Infrastructure はディスカバリの実行時に、デバイスの到達可能性状態（[到達可能（Reachable）]、[ping 到達可能（Ping Reachable）]、または [到達不能（Unreachable）]）を設定します。状態の詳細については、「デバイスの到達可能性状態と管理状態 （53 ページ）」を参照してください。

1. Prime Infrastructure は、ICMP ping を使用して、デバイスに到達可能であるかどうかを判別します。デバイスに到達できない場合、到達可能状態は [到達不能（Unreachable）] に設定されます。
2. サーバは、SNMP 通信が可能かどうかをチェックします。
   - ICMP がデバイスに到達可能で、SNMP 通信が不可能な場合、その到達可能性状態は [ping 到達可能（Ping Reachable）] に設定されます。
   - ICMP と SNMP の両方がデバイスに到達できる場合、その到達可能性状態は [到達可能（Reachable）] です。
3. デバイスの Telnet および SSH クレデンシャルが確認されます。クレデンシャルに障害が起きた場合は、障害に関する詳細が [ネットワークデバイス（Network Devices）] テーブルの [最後のインベントリ収集ステータス（Last Inventory Collection Status）] 列に表示されます（たとえば、「**Wrong CLI Credentials**」など）。到達可能性の状態は変更されません。
4. Prime Infrastructure が SNMP を使用して必要な通知を受信できるように、デバイス設定が変更されて、トラップの受信者が追加されます。
5. インベントリ収集プロセスが開始され、すべてのデバイス情報が収集されます。
6. Web GUI にすべての情報（ディスカバリが完全に成功したか、部分的に成功したかなど）が表示されます。

（注） Prime Infrastructure がデバイスの SNMP 読み取り/書き込みクレデンシャルを検証すると、デバイス ログが更新され、Prime Infrastructure（IP アドレスで識別される）によって構成が変更されたことが示されます。

検出されたデバイスの管理 IP アドレス タイプ（IPv4/IPv6）の指定

検出されたデュアルホーム（IPv4/IPv6）デバイスでは、Prime Infrastructure が管理 IP アドレスとして IPv4 アドレスまたは IPv6 アドレスを使用するかどうかを指定します。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** を選択し、**[インベントリ（Inventory）] > [検出（Discovery）]** を選択します。

ステップ 2 [管理アドレスに対する IPv4/IPv6 設定（IPv4/IPv6 Preference for Management Address）] ドロップダウンリストから [v4] または [v6] のいずれかを選択します。

ステップ 3 **[保存（Save）]** をクリックします。

クイック ディスカバリの実行

単一のシードデバイスを使用して ping スイープを実行する場合には、この方法を使用します。デバイス名、SNMP コミュニティ、シードの IP アドレスおよびサブネット マスクのみが必要です。構成管理機能の使用を計画している場合は、プロトコル、ユーザ名、パスワード、およびイネーブル パスワードを入力する必要があります。

[サービス（Services）] > [ネットワークサービス（Network Services）] > [ゲストユーザ（Guest Users）] の順に選択して、Prime Infrastructure によって検出されたゲスト ユーザを表示できます。検出後のゲスト ユーザ アカウントの正しいライフタイムを確認するには、デバイスに正しい時間設定が指定されていることを確認します。

ステップ 1 **[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ディスカバリ（Discovery）]** の順に選択して、ウィンドウ右上の [クイック ディスカバリ（Quick Discovery）] リンクをクリックします。

ステップ 2 少なくとも、名前、SNMP コミュニティ、シードの IP アドレス、およびサブネット マスクを入力します。

ステップ 3 [今すぐ実行（Run Now）] をクリックします。

次のタスク

結果を表示するには、[ディスカバリ ジョブ インスタンス（Discovery Job Instances）] 領域の、[ジョブ（Job）] ハイパーリンクをクリックします。

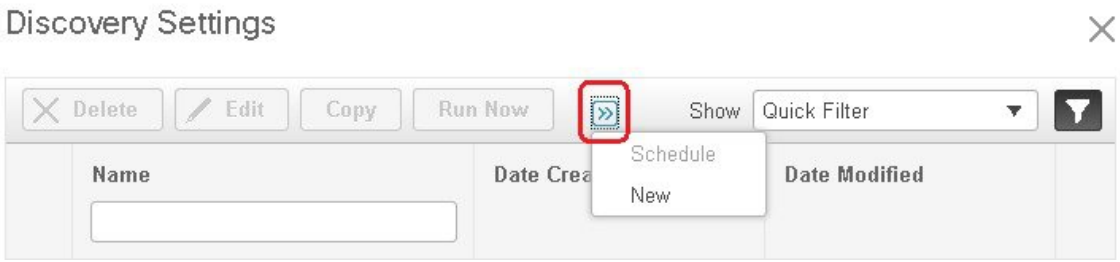
カスタマイズされたディスカバリ設定でのディスカバリの実行

Prime Infrastructure は、ディスカバリ プロファイルを使用してネットワーク デバイスを検出できます。ディスカバリ プロファイルには、ネットワーク要素を検索し、それらに接続してインベントリを収集する方法を Prime Infrastructure に指示する設定のコレクションが含まれています。たとえば、Prime Infrastructure に CDP、LLDP、OSPF を使用してデバイスを検出することや、単純な ping スイープの実行を指示できます（ping スイープの結果の例は「ping スイープのサンプルの IPv4 IP アドレス （42 ページ）」に記載されています）。フィルタを作成して、コレクションの微調整、クレデンシャルセットの指定、およびその他のディスカバリ設定を行うこともできます。プロファイルは必要な数だけ作成できます。

プロファイルの作成後、プロファイルを使用するディスカバリ ジョブを作成し、実行します。検出ジョブの結果は[検出（Discovery）]ページで確認できます。ジョブをスケジュールして、定期的に実行を繰り返すこともできます。

ステップ 1 [インベントリ（Inventory）] > [デバイス管理（Device Management）] > [検出（Discovery）] を選択して、ウィンドウ右上の [検出設定（Discovery Settings）] リンクをクリックします。（[ディスカバリ設定（Discovery Settings）] リンクが表示されない場合は、[クイック ディスカバリ（Quick Discovery）] リンクの隣の矢印アイコンをクリックします）。

ステップ 2 [検出設定（Discovery Settings）] ポップアップで、[新規（New）] をクリックします。



ステップ 3 [ディスカバリ設定（Discovery Settings）] ウィンドウに設定を入力します。その設定に関する情報を取得するには、設定の隣にある [?] をクリックします。たとえば、[SNMPv2 クレデンシャル（SNMPv2 Credentials）] の横にある [?] をクリックすると、ヘルプのポップアップにプロトコルと必須の属性がすべて表示されます。

ステップ 4 システムからディスカバリ設定をインポートするには、[インポート（Import）] ボタンをクリックします。

ステップ 5 ディスカバリ設定を XML 形式でエクスポートするには、[エクスポート（Export）] ボタンをクリックします。

ステップ 6 [今すぐ実行（Run Now）] をクリックしてジョブをすぐに実行するか、[保存（Save）] をクリックして設定を保存し、後で実行するようにディスカバリをスケジュールします。

ping スイープのサンプルの IPv4 IP アドレス

次の表に、ping スイープ結果の例を記載します。

サブネット範囲	ビット数	IP アドレスの数	サンプルのシード IP アドレス	開始 IP アドレス	終了 IP アドレス
255.255.240.0	。	4094	205.169.62.11	205.169.48.1	205.169.63.254
255.255.248.0	21	2046	205.169.62.11	205.169.56.1	205.169.63.254
255.255.252.0	22	1022	205.169.62.11	205.169.60.1	205.169.63.254
255.255.254.0	23	510	205.169.62.11	205.169.62.1	205.169.63.254
255.255.255.0	24	254	205.169.62.11	205.169.62.1	205.169.63.254
255.255.255.128	25	126	205.169.62.11	205.169.62.1	205.169.63.127
255.255.255.192	26	62	205.169.62.11	205.169.62.1	205.169.63.62
255.255.255.224	27	30	205.169.62.11	205.169.62.1	205.169.63.30
255.255.255.240	28	18	205.169.62.11	205.169.62.1	205.169.63.14
255.255.255.248	29	6	205.169.62.11	205.169.62.9	205.169.63.14
255.255.255.252	30	2	205.169.62.11	205.169.62.9	205.169.63.10
255.255.255.254	31	0	205.169.62.11		
255.255.255.255	32	1	205.169.62.11	205.169.62.11	205.169.62.11

検出の確認

検出が完了したら、プロセスが正常に完了したかどうかを確認できます。

ディスカバリの成功を確認するには、次の手順を実行します。

ステップ 1 **[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [検出（Discovery）]** を選択します。

ステップ 2 詳細を表示するディスカバリジョブを選択します。

ステップ 3 左側のナビゲーション ペインから **[ユーザ ジョブ（User Jobs）] > [検出（Discovery）]** を選択し、特定のジョブを選択します。

ステップ 4 **[ジョブ インスタンスの検出（Discovery Job Instances）]** の下で、矢印を展開して、検出されたデバイスの詳細を表示します。

デバイスが見つからない場合は、次を行います。

- ディスカバリ設定を変えてから、ディスカバリを再実行します。
- デバイスを手動で追加します。詳細については、「手動によるデバイスの追加（新規デバイス タイプまたはデバイス シリーズ） （46 ページ）」を参照してください。

[ジョブ インスタンスの検出 (Discovery Job Instances)] セクションに、**[エクスポート（Export）]** および **[更新（Refresh）]** ボタンが表示されます。ジョブ情報はPDFとCSVの両方としてエクスポートできます。

他のソースからのデバイスのインポート

デバイスのインポート元となる管理システムが他にある場合、またはすべてのデバイスとその属性がリストされたスプレッドシートをインポートする場合は、一括デバイス ファイルをインポートすることで、デバイス情報を Prime Infrastructure に追加できます。デバイスのインポート CSV ファイルの作成 （44 ページ）で説明するように、インポートする CSV ファイルが完全で、正しくフォーマットされていることを確認する必要があります。

ステップ 1 **[インベントリ（Inventory）]** > **[デバイス管理（Device Management）]** > **[ネットワーク デバイス（Network Devices）]** を選択し、[ネットワーク デバイス（Network Devices）] テーブルの上にある + アイコンをクリックしてから、[一括インポート（Bulk Import）] を選択します。

ステップ 2 [操作（Operation）] ドロップダウン リストから、[デバイス（Device）] を選択します。

ステップ 3 [CSV ファイルの選択（Select CSV File）] の横にある [参照（Browse）] をクリックし、インポートするデバイスが含まれている CSV ファイルまで移動して選択します。

ステップ 4 [インポート（Import）] をクリックします。

ステップ 5 **[管理（Administration）]** > **[ダッシュボード（Dashboards）]** > **[ジョブ ダッシュボード（Job Dashboard）]** > **[ユーザ ジョブ（UserJobs）]** > **[デバイスの一括インポート（Device Bulk Import）]** を選択して、インポートのステータスを確認します。

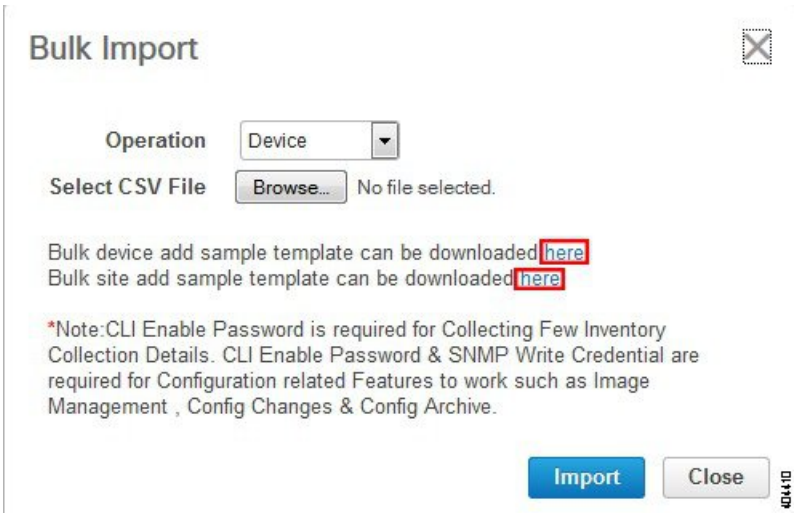
ステップ 6 矢印をクリックして、ジョブの詳細を展開し、インポート ジョブの詳細と履歴を表示します。

デバイスのインポート CSV ファイルの作成

CSV ファイルを使用してデバイスを別のソースから Prime Infrastructure にインポートする場合は、デバイス テンプレートを使用して CSV ファイルを準備する必要があります。このテンプレートは、次のように Prime Infrastructure からダウンロードできます。

1. **[インベントリ（Inventory）]** > **[デバイス管理（Device Management）]** > **[ネットワーク デバイス（Network Devices）]** [インベントリ（Inventory）] > [デバイス管理（Device Management）] > を選択します。次に、[一括インポート（Bulk Import）] をクリックします。

2. [一括デバイス追加サンプルテンプレートをダウンロードできます（Bulk device add sample template can be downloaded）] の横にある [ここ（here）] リンクをクリックします（下の図でハイライト表示されています）。テンプレートには、インポートする予定のCSVデバイスファイルに含める必要がある情報のすべてのフィールドと説明が含まれています。



CSV ファイルをインポートしてデバイスを追加する場合は、Prime Infrastructure がこれらのデバイスを管理できる範囲は、CSV ファイルで指定した情報によって異なることに注意してください。たとえば、CSV ファイル内のデバイスの CLI ユーザ名、CLI パスワード、CLI イネーブルパスワード、および CLI タイムアウト値のフィールドに値を入力しないと、Prime Infrastructure は、そのデバイスの設定を変更したり、デバイスのソフトウェアイメージを更新したり、その他の便利な機能を実行したりできません。

これは、完全なデバイス インベントリの収集にも影響します。Prime Infrastructure で部分的なインベントリ収集を行うには、CSV ファイルの少なくとも次のフィールド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

Prime Infrastructure で完全なインベントリ収集を行うには、[プロトコル（Protocol）] フィールドの値と、指定したプロトコルに対応するフィールドの値も指定する必要があります。たとえば、[プロトコル（Protocol）] フィールドに値 **SNMPv3** を指定する場合は、サンプル CSV ファイルの [SNMPv3] フィールドの値（SNMPv3 のユーザ名と認証パスワードなど）も指定する必要があります。

CSV ファイルでクレデンシャル プロファイルを指定し、クレデンシャルをデバイスのセットに適用できます。クレデンシャル プロファイルを指定し、CSV ファイルに手動で値を入力すると、手動で入力されたクレデンシャルとクレデンシャルプロファイルの組み合わせに基づいてデバイスが管理され、手動で入力されたクレデンシャルの優先順位が高くなります。たとえば、手動で入力した SNMP クレデンシャルに加えて SNMP および Telnet のクレデンシャルを

含むクレデンシャル 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 クレデンシャルとクレデンシャル プロファイル内の Telnet クレデンシャルに基づいて管理されます。

インポートする CSV ファイルにユーザ定義フィールド（UDF）パラメータが含まれている場合は、CSV ファイルをインポートする前にこれらの UDF パラメータを必ず追加する必要があります。これを行うには、**[管理（Administration）]** > **[設定（Settings）]** > **[システム設定（System Settings）]** > **[インベントリ（Inventory）]** > **[ユーザ定義フィールド（User Defined Fields）]** を選択し、各 UDF パラメータを追加します。CSV ファイルの [UDF] 列は、CSV テンプレートに示されているように、**UDF:** で始まる必要があります。UDF フィールドパラメータには、特殊文字 : ; および # を使用しないでください。

（注） 一括インポート時には、CSV ファイルに IP アドレスとクレデンシャルプロファイル名の情報のみを含める必要があります。

手動によるデバイスの追加（新規デバイスタイプまたはデバイス シリーズ）

新しいデバイス タイプを追加して、それらの設定をデバイスのグループに適用する前にテストするには、次の手順に従います。

ステップ 1 [インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ネットワーク デバイス（Network Devices）] の順に選択します。

ステップ 2 [ネットワーク デバイス（Network Devices）] テーブルの上にある ＋ アイコンをクリックし、[デバイスの追加（Add Device）] を選択します。

ステップ 3 [デバイスの追加（Add Device）] ダイアログボックスで、必須フィールドに値を入力します。フィールドの横にある [?] をクリックすると、そのフィールドの説明が表示されます。

（注） IE1k デバイスを追加する場合は、[デバイスの追加（Add Device）] ダイアログ ボックスに **HTTP/HTTPS パラメータ**を入力する必要があります。この情報を無視すると、デバイスは [収集の部分的な失敗（Partial Collection Failure）] 状態に移行します。

（注） コンプライアンス ポリシーを使用するデバイスには、Telnet/SSH 情報が必須です。Telnet/SSH（60 秒）と SNMP（10 秒）のデフォルト タイムアウトがネットワーク遅延に基づいてデバイスにより異なる場合でも、デバイスを構成できます。

[管理（Administration）] > [設定（Settings ）] > [システム設定（System Settings）] > [インベントリ（Inventory）] > [インベントリ（Inventory）] ページで [SSH の厳格なホスト チェック キー（Strict host check key for SSH）] チェック ボックスを選択して、追加したデバイスの SSH キーの検証を強制することができます。これにより、Telnet/SSH のパラメータの下でアルゴリズムおよび SSH キーを指定することができます。

デバイスを追加するときにアルゴリズムと SSH キーを手動で指定しない場合は、[管理（Administration）] > [設定（Settings ）] > [システム設定（System Settings）] > [インベントリ（Inventory）] > [インベントリ（Inventory）] ページで [最初の使用で SSH キーを信頼する（Trust SSH key on first use）] チェック ボックスを選択します。その最初の通信中にデバイスから送信された SSH キーは、信頼されデバイスのクレデンシャルに追加されます。この保存されたキーは、その後デバイスが追加されたときに自動入力され、検証に使用されます。

ステップ 4 （任意）デバイスを追加する前にクレデンシャルを確認するには、[クレデンシャルの確認（Verify Credentials）] をクリックします。

UCS シャーシなどのデバイスの HTTPS クレデンシャルを確認するには、デバイスから証明書を取得して Prime Infrastructure のトラストストアに追加してください。Prime Infrastructure のトラストストアに証明書を追加するには、次のコマンドを使用します。

- ncs key importcacert <*name*> <*certificate filename*> repository <*name of repository*>
- ncs stop
- ncs start

ステップ 5 [追加（Add）] をクリックして、指定した設定でデバイスを追加します。

（注） ユーザ定義フィールド（UDF）パラメータが新しいデバイスに使用可能になるのは、最初に **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] > [インベントリ（Inventory）] > [ユーザ定義フィールド（User Defined Fields）]** を選択して UDF パラメータを追加した場合のみです。UDF フィールド パラメータには、特殊文字 : ; および # を使用しないでください。

（注） NCS 2000 デバイスの場合、[シングルセッション TL1 を有効にする（Enable Single Session TL1）] の設定はリリース 11.0 以降を実行しているデバイスに対してのみ有効です。

（注） Prime Infrastructureは、デフォルトではUCSを自己署名証明書で承認しません。ユーザがこれを手動で有効にするには、*/opt/CSCOlumos/xmp_inventory/xde-home/inventoryDefaults/ncsCIMC.def*ファイルに次の行を追加します。

```
<default attribute="HTTPS_TRUST_CONDITION">always</default>

<default attribute="HTTPS_HOSTNAME_VERIFICATION_STRATEGY">allow_all</default>
```

仮想デバイス コンテキストの追加

Prime Infrastructure では、Cisco NX-OS ソフトウェアが仮想デバイス コンテキスト（VDC）をサポートします。これにより、単一のデバイスを複数の論理デバイスにパーティション分割して、障害の分離、管理の分離、アドレス割り当ての分離、サービス差別化ドメイン、および適応型リソース管理を実現します。VDC では、デバイス レベルでスイッチを仮想化できます。VDC は、実行中の独自のソフトウェア プロセスを保持する個別の論理エンティティとして実行し、独自の設定を持ち、管理者によって管理されます。**VDC1**は、特別なロールを持っているデフォルト（管理）VDC です。子 VDC を設定して、リソースを割り当てることができます。

Prime Infrastructure は、Cisco NX-OS ソフトウェア リリース 6.2(12) 以降を実行するデバイスで Cisco Nexus のすべてのスイッチ機能を管理します。

デフォルト VDC を備えた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 **[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ネットワーク デバイス（Network Devices）]** の順に選択します。

ステップ 2 [デバイスの追加（Add Device）] ドロップダウンリストから、[デバイスの追加（Add Device）] を選択します。

ステップ 3 さまざまなタブで必要な設定を指定します。

特定のパラメータの説明を表示するには、**[?]** アイコン上にカーソルを置きます。

ステップ 4 （任意）デバイスを追加する前に、[クレデンシャルの確認（Verify Credentials）] をクリックして、入力したクレデンシャルが有効であることを確認します。

ステップ 5 [追加（Add）] をクリックして、指定した設定でデバイスを追加します。

インベントリ収集が正常に実行された後に、デフォルトの VDC を備えたデバイスが追加されます。その後、子 VDC が自動的に追加され、その設定が Prime Infrastructure データベースに保存されます。

Prime Infrastructure への Meraki デバイスの追加

Cisco Prime Infrastructure では、すべての Meraki アクセス ポイント、Meraki セキュリティ アプライアンス、およびMeraki スイッチをモニタできます。Cisco Prime Infrastructure は、SNMP プロトコルを使用して、モニタリングとインベントリの両方の目的で、クラウドから、Merakiデバイスに関する情報を抽出します。

Cisco Meraki を Cisco Prime Infrastructure に統合するには、次のものが必要です。

- ダッシュボードで SNMP を有効にする
- Cisco Prime Infrastructure サーバへの Meraki ダッシュボードの追加
- 接続の確認

Meraki デバイスを Prime Infrastructure に追加するには、次の手順を実行します。

ステップ 1 **[インベントリ（Inventory）][デバイス管理（Device Management）][ネットワーク デバイス（Network Devices）]** を選択します。

ステップ 2 [ネットワーク デバイス（Network Devices）] テーブルの上にある + アイコンをクリックし、**[デバイスの追加（Add Device）]** を選択します。

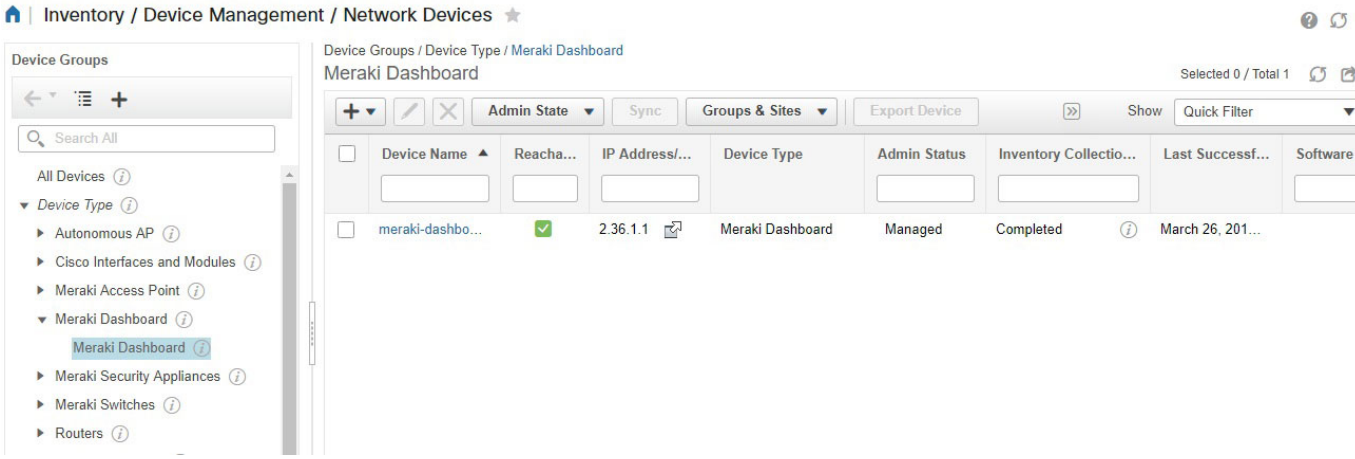
ステップ 3 Meraki ダッシュボードの **IP アドレス**または **DNS 名**を入力します。

ステップ 4 **[デバイスの追加 (Add Device)]** 画面で SNMP v2/v3 クレデンシャルを入力します。

ステップ 5 （任意）デバイスを追加する前にクレデンシャルを確認するには、[クレデンシャルの確認（Verify Credentials）] をクリックします。

ステップ 6 **[追加（Add）]** をクリックして、指定した設定でデバイスを追加します。デバイスの詳細が右側のペインに表示されます。次のようなものがあります。

- Device Name
- 到達可能性/ステータス
- IP アドレス/DNS名
- デバイス タイプまたはモデル
- MAC address
- クライアント数
- シリアル番号
- メッシュ ステータス
- ネットワーク名。



Meraki ダッシュボードは、複数のデバイスを構成するための単一ポイントの設定のままです。Cisco Prime を使用すると、デバイスの IP アドレスの横にデバイス リンクを含めることで、特定のデバイスに簡単にアクセスできます。これらのリンクにより、ブラウザ ウィンドウが起動します。これにより、管理者は特定

のデバイスに関する包括的な情報を抽出するのに役立つ、Meraki ダッシュボードのデバイスに対する権限を得ることができます。

（注） 必要なアクセスポイント、スイッチ、およびセキュリティアプライアンスを表示するには、**[ネットワーク デバイス (Network Devices)]** ページのグループ セレクタ/オブジェクト セレクタから適切なデバイス グループを選択する必要があります。

ワイヤレス コントローラを追加するための前提条件

Prime Infrastructure にワイヤレス デバイスを追加する場合は、次の情報に注意してください。

- Prime Infrastructure からワイヤレス コントローラを取り外すと、そのコントローラに関連付けられたアクセスポイントも削除する必要があるかどうかを確認する警告メッセージが表示されます。
- IPSec を使用する GRE リンク、または複数のフラグメントを含むより下位の MTU リンクを使用してコントローラを追加する場合は、[Get PDUあたりの最大VarBind（Maximum VarBinds per Get PDU）] と [Set PDUあたりの最大VarBind（Maximum VarBinds per Set PDU）] の値を調整する必要があります。これらの値が高すぎると、コントローラが Prime Infrastructure に追加されないことがあります。

  [Get PDUあたりの最大VarBind（Maximum VarBinds per Get PDU）] または [Set PDUあたりの最大VarBind（Maximum VarBinds per Set PDU）] の値を調整するには、Prime Infrastructure サーバを停止し、**[管理（Administration）]** > **[設定（Settings）]** > **[ネットワークとデバイス（Network and Device）]** > **[SNMP]** を選択し、[Get PDUあたりの最大VarBind（Maximum VarBinds per Get PDU）] と [Set PDUあたりの最大VarBind（Maximum VarBinds per Set PDU）] の値を 50 以下に編集します。
- ワイヤレス コントローラを追加していて、「スパーステーブルがサポートされていません（Sparse table not supported）」というエラー メッセージが表示された場合は、再試行する前に、Prime Infrastructure と WLC の両方の互換バージョンを実行していることを確認してください。2 つの製品の互換バージョンの詳細については、Cisco.com で Prime Infrastructure の『Cisco Wireless Solutions Software Compatibility Matrix』のエントリを参照してください。
- Prime Infrastructure は、追加するコントローラのトラップ受信機として機能します。コントローラ上では、802.11 Disassociation、802.11 Deauthentication、および 802.11 Authenticated というトラップが有効になっています。
- 新しいコントローラを追加すると、Prime Infrastructure が新しいコントローラとの通信を試行しているときに、コントローラの到達可能性が「不明（Unknown）」としてリストされます。コントローラとの通信が成功すると、コントローラの到達可能性が「到達可能（Reachable）」または「ping到達可能（Ping Reachable）」に変わります。
- コンプライアンスを有効にすると、WLC は次の理由により、部分的なインベントリ収集状態に移行します。

- CLI クレデンシャルに読み取り/書き込み権限がない。
- 同期時に WLC が接続を閉じる。
- WLC が設定したタイム アウト時間内に応答しない。

- 複数のコントローラのクレデンシャルをまとめて更新するには、**[インベントリ（Inventory）] > [ネットワークデバイス（Network Devices）] > [ワイヤレスコントローラ（Wireless Controllers）]** を選択します。次に、更新する必要があるコントローラを選択し、[編集（Edit）] アイコンをクリックします。最後に、クレデンシャル プロファイルを選択し、[更新（Update）] または [更新と同期（Update & Sync）] をクリックします。
- また、更新するコントローラのリストを含むCSVファイルを作成して、複数のコントローラのクレデンシャルを一括して更新することもできます。1 行に 1 つのコントローラが存在することを確認します。各行には、更新するコントローラ属性のカンマ区切りリストが表示されます。
  - **[インベントリ（Inventory）] > [ネットワークデバイス（Network Devices）] > [ワイヤレスコントローラ（Wireless Controllers）]** を選択します。
  - テーブルの上の ＋ アイコンをクリックします。
  - [一括インポート（Bulk Import）] を選択し、CSV ファイルを参照します。

追加されたデバイスの検証と問題のトラブルシューティング

ディスカバリ プロセスをモニタするには、次の手順を実行します。

ステップ 1 ディスカバリ プロセスを確認するには、**[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ディスカバリ（Discovery）]** を選択します。

ステップ 2 ジョブ インスタンスを展開して詳細を表示し、次の各タブをクリックして、そのデバイスのディスカバリに関する詳細を表示します。

- [到達可能（Reachable）] : ICMP を使用して到達したデバイス。デバイスは到達可能ですが、モデル化されていない可能性があります。これは、ディスカバリを使用したデバイスの追加 （39 ページ）で示されているように、さまざまな理由で発生する可能性があります。このタブの情報から問題がないか確認してください。
- [フィルタ済み（Filtered）] : カスタマイズされたディスカバリ設定に従ってフィルタ処理されたデバイス。
- [ping で到達可能（Ping Reachable）] : ICMP ping で到達可能だったものの、SNMP を使用して通信できなかったデバイス。これには、複数の理由（無効な SNMP クレデンシャル、SNMP がデバイスで有効になっていない、ネットワークで SNMP パケットが廃棄されたなど）が原因が考えられます。

- [到達不能（Unreachable）]：障害により ICMP ping に応答しなかったデバイス。
- [不明（Unknown）]：Prime Infrastructure は、ICMP または SNMP によってデバイスに接続できません。

（注） TL1 プロトコルを使用するデバイスの場合は、ノード名にスペースが含まれないようにしてください。そうでない場合、接続障害が発生します。

ステップ 3 デバイスが正常に Prime Infrastructure に追加されたことを確認するには、**[インベントリ（Inventory）]** > **[デバイス管理（Device Management）]** > **[ネットワーク デバイス（Network Devices）]** の順に選択します。次のアクションを実行します。

- 追加したデバイスがリストに表示されていることを確認します。Prime Infrastructure がデバイスから収集したデバイス設定とソフトウェア イメージを表示するには、デバイス名をクリックします。
- [インベントリ収集ステータス（Inventory Collection Status）] フィールドの上にマウス カーソルを合わせ、表示されるアイコンをクリックすると、デバイスから収集された情報の詳細が表示されます。
- デバイスの到達可能性ステータスの列と管理者ステータスの列を確認します。デバイスの到達可能性状態と管理状態 （53 ページ）を参照してください。

Prime Infrastructure がデバイスをサポートしていることを確認するには、『*Cisco Prime Infrastructure Supported Devices*』を参照してください。

デバイスの到達可能性の状態および管理ステータスの確認

次の手順を実行して、Prime Infrastructure がデバイスと通信できるか（到達可能性の状態）や、そのホストを管理しているか（管理ステータス）を判断します。また、管理ステータスでは、デバイスが Prime Infrastructure によって正常に管理されているかどうかの情報も提供されます。

ステップ 1 **[インベントリ（Inventory）]** > **[デバイス管理（Device Management）]** > **[ネットワーク デバイス（Network Devices）]** の順に選択します。

ステップ 2 [ネットワーク デバイス（Network Devices）] テーブルでデバイスを確認します。

a) [表示（Show）] ドロップダウン リスト（テーブルの右上）から [クイック フィルタ（Quick Filter）] を選択します。

b) [デバイス名（Device Name）] 列の下にあるテキスト ボックスにデバイスの名前（またはその一部）を入力します。

ステップ 3 [到達可能性（Reachability）] 列と [管理ステータス（Admin Status）] 列の情報を確認します。これらの状態の説明については、デバイスの到達可能性状態と管理状態 （53 ページ）を参照してください。

デバイスの到達可能性状態と管理状態

デバイスの到達可能性状態：Prime Infrastructure が設定されたすべてのプロトコルを使用してデバイスと通信できるかどうかを表します。

表 *8*：デバイスの到達可能性状態

アイコン	デバイスの到達可能性状態	説明	トラブルシューティング
	到達可能	Prime Infrastructure は、SNMP を使用してデバイスに、または ICMP を使用して NCS 2K デバイスにアクセスすることができます。	—
	ping 到達可能	Prime Infrastructure は、ping を使用してデバイスに到達できますが、SNMP 経由では到達できません。	ICMP ping は成功しますが、SNMP 通信が失敗する原因すべてをチェックします。デバイス SNMP クレデンシャルがデバイスと Prime Infrastructure の両方で同じであること、SNMP がデバイス上で有効になっているかどうか、またはトランスポートネットワークが設定ミスなどの理由で SNMP パケットをドロップしていないかどうかをチェックします。
	到達不能	Prime Infrastructure は、ping を使用してデバイスに到達できません。	物理デバイスが動作中でネットワークに接続されていることを確認します。
	不明	Prime Infrastructure は、デバイスに接続できません。	デバイスをチェックします。

デバイスの管理状態：デバイスの設定状態を表します（たとえば、デバイスが ping によって到達できないためにダウンしている場合や、管理者が手動でデバイスをシャットダウンした場合などです）。

表 *9*：デバイスの管理状態

デバイスの管理状態	説明	トラブルシューティング

管理対象	Prime Infrastructure は、デバイスを積極的にモニタしています。	該当なし。
メンテナンス	Prime Infrastructure は、デバイスの到達可能性をチェックしていますが、トラップ、syslog、または TL1 メッセージを処理していません。	デバイスを管理対象状態に移行するには、デバイスのメンテナンス状態の切り替え （54 ページ）を参照してください。
管理対象外	Prime Infrastructure は、デバイスをモニタしていません。	[ネットワーク デバイス（Network Devices）] テーブルで、デバイスを特定し、[最新のインベントリ収集ステータス（Last Inventory Collection Status）] 列でデータの横にある [i] アイコンをクリックします。ポップアップ ウィンドウに、詳細とトラブルシューティングのヒントが表示されます。収集問題の一般的な原因は次のとおりです。 • デバイス SNMP クレデンシャルが間違っている。 • Prime Infrastructure 展開がライセンスで許可されているデバイスの数を上回っている。 • デバイスがスイッチ パス トレース専用になっている。 デバイス タイプがサポートされていない場合は、その [デバイス タイプ（Device Type）] が [不明（Unknown）] になります。そのデバイス タイプのサポートが Cisco.com で提供されているかをチェックするには、**[管理（Administration）] > [ライセンスおよびソフトウェアアップデート（Licenses and Software Updates）] > [ソフトウェアアップデート（Software Update）]** を選択してから、[更新の確認（Check for Updates）] をクリックします。
不明	Prime Infrastructure は、デバイスに接続できません。	デバイスをチェックします。

デバイスのメンテナンス状態の切り替え

デバイスの管理ステータスが [メンテナンス（Maintenance）] に変更されると、Prime Infrastructure はデバイスのインベントリ変更用のポーリング操作も、デバイスで生成されたトラップまたは Syslog の処理も行わなくなります。ただし、Prime Infrastructure は引き続き既存のリンクを維持し、デバイスの到達可能性をチェックします。

すべての管理状態および対応するアイコンのリストについては、デバイスの到達可能性状態と管理状態 （53 ページ）を参照してください。

ステップ 1 [ネットワーク デバイス（Network Devices）] テーブルで、**[管理状態（Admin State）] > [メンテナンス ステートに設定（Set to Maintenance State）]** の順に選択します。

ステップ 2 デバイスを完全な管理状態に戻すには、**[管理状態（Admin State）] > [管理対象状態に設定（Set to Managed State）]** の順に選択します。

（注） [メンテナンス状態をスケジュール（Schedule Maintenance State）] および [管理状態をスケジュール（Schedule Managed State）] オプションを使用して、特定の日時にメンテナンスを行い、特定の日時に管理状態に戻すようにデバイスをスケジュールすることもできます。

デバイス パラメータの編集

[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ネットワーク デバイス（Network Devices）] の順に選択して、単一のデバイスまたは複数のデバイスのデバイス パラメータを編集できます。

デバイス パラメータを編集するには、次の手順を実行します。

ステップ 1 **[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ネットワーク デバイス（Network Devices）]** の順に選択します。

ステップ 2 単一のデバイスまたは複数のデバイスを選択し、[編集（Edit）] アイコンをクリックします。

9 台以上のデバイスを編集すると、**[ジョブ ダッシュボード (Job Dashboard)]** ページでジョブがトリガーされます。一括編集のステータスがそのページに表示されます。

ステップ 3 必須パラメータを更新します。

ステップ 4 選択したすべてのデバイスのパラメータを更新する場合は [更新（Update）] をクリックし、更新されたパラメータでデバイスを更新して同期する場合は [更新&同期（Update & Sync）] をクリックします。

デバイスの同期化

Prime Infrastructure データベースをデバイスで実行中の設定と同期するために、インベントリ収集を実行できます。

デバイスを同期するには、次の手順に従います。

ステップ 1 **[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ネットワーク デバイス（Network Devices）]** の順に選択します。

ステップ 2 Prime Infrastructure データベースに保存されている設定と同期する設定を持つデバイスを選択します。

ステップ 3 [同期（Sync）] をクリックします。

（注） 同期されたデバイスがデフォルト/管理 VDC の場合は、すべての子 VDC のすべての設定が自動的に同期され、その設定が Prime Infrastructure データベースで更新されます。管理 VDC の同期により、ハードウェアで新しく追加された VDC もユーザ インターフェイスに追加されます。また、ハードウェアで削除された VDC はユーザ インターフェイスから削除されます。

スマート インベントリ

スマート インベントリでは、デバイスの commitID が変更されない限り、限られた情報のみが収集されるようにすることができます。変更があった場合は、全情報の収集が行われます。スマート インベントリの目的は、Prime Infrastructure とデバイスの間で転送されるデータの量をスマートな方法で削減することです。Prime Infrastructure は主要なインベントリ収集を行い、デバイスの設定に変更があった場合のみ、完全なコンフィギュレーションアーカイブを行います。デバイスの実行コンフィギュレーションに変更がない場合は、イメージ、フラッシュ、ファイル、インターフェイス ステータスなど、物理的な情報のみがデバイスから収集されます。デバイスの実行コンフィギュレーションに変更がない場合は、コンフィギュレーション アーカイブはトリガーされません。

スマート インベントリを有効にするには、次の手順を実行します。

ステップ 1 **[管理（Administration）] > [システム設定（System Settings）] > [インベントリ（Inventory）] > [スマート インベントリ（Smart Inventory）]** を選択します。

ステップ 2 [スマートインベントリをグローバルで有効化（Enable Smart Inventory Globally）] チェック ボックスを選択します。サポートされているすべてのデバイスが一覧表示されます。

（注） スマートインベントリをデバイスごとに有効化/無効化することもできます。必要なデバイスを選択し、[有効化（Enable）] ボタンまたは [無効化（Disable）] ボタンをクリックします。

NAM HTTP/HTTPS クレデンシャルの追加

ネットワークのモニタリングに Cisco ネットワーク解析モジュール（NAM）を使用している場合は、Prime Infrastructure がそのモジュールからデータを取得できるように、HTTPS クレデンシャルを追加する必要があります。これは、ほとんどの保証機能は NAM データに依存して機能するため、ライセンス済みの保証機能を持つユーザに対して特に重要です。

Prime Infrastructure は、HTTP（または HTTPS）を介して NAM を直接ポーリングしてデータを収集します。このタイプのポーリングでは、Prime Infrastructure が各 NAM の HTTP クレデンシャルを保存する必要があります。SNMP コミュニティ ストリングおよび Telnet/SSH クレデンシャルとは異なり、ディスカバリ プロセス中に NAM HTTP クレデンシャルを入力できませ

ん。モジュールが検出された後またはインベントリに追加された後に実行できるのは、NAM HTTP クレデンシャルを指定することだけです。

単一の NAM の HTTP クレデンシャルを追加するには、次の手順を実行します。このタスクを、Prime Infrastructure でデータを収集するすべての NAM に繰り返すことができます。

ステップ 1 **[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ネットワークデバイス（Network Devices）] > [デバイスタイプ（Device Type）] > [Ciscoインターフェイスおよびモジュール（Cisco Interfaces and Modules）] > [ネットワーク解析モジュール（Network Analysis Modules）]** の順に選択します。

ステップ 2 NAM の 1 つを選択して、[Edit] をクリックします。

ステップ 3 [Edit Device] ウィンドウの、[Http Parameters] で以下を行います。

- [Protocol]：HTTP プロトコル、HTTP または HTTPS を選択します。TCP ポートは、選択したプロトコルのデフォルト ポートに自動的に変更されます。
- [TCP Port]：デフォルトを上書きする場合は、別の TCP ポートを入力します。
- [Username]：HTTP または HTTPS 経由で NAM にアクセスできるユーザの名前を入力します。
- [Password]：入力したユーザ名のパスワードを入力します。
- [パスワードの確認（Confirm Password）]：確認するパスワードをもう一度入力します。

ステップ 4 [更新（Update）] を選択します。

CSV ファイルへのデバイス情報のエクスポート

デバイス リストをファイルにエクスポートすると、すべてのデバイス情報が CSV ファイルにエクスポートされます。次に、選択したパスワードを使用してファイルが圧縮され、暗号化されます。エクスポートしたファイルには、デバイスの SNMP クレデンシャル、CLI 設定、および地理的座標に関する情報が含まれています。エクスポートされたファイルにはデバイスのクレデンシャルが含まれていますが、クレデンシャルのプロファイルは含まれていません。

⚠

注意 CSV ファイルにはエクスポートしたデバイスのすべてのクレデンシャルのリストが含まれるため、十分に注意して使用してください。デバイスのエクスポートは特殊な権限を持つユーザのみが実行できるようにする必要があります。

ステップ 1 **[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ネットワーク デバイス（Network Devices）]** を選択します。

ステップ 2 エクスポートするデバイスを選択し、[デバイスのエクスポート（Export Device）] を選択します（または、 をクリックして [デバイスのエクスポート（Export Device）] を選択します）。

ステップ 3 [デバイスのエクスポート（Export Device）] ダイアログボックスで、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。ユーザはエクスポートされたファイルを開くのにこのパスワードを指定する必要があります。必要に応じて、エクスポートするCSVファイルの名前を入力します。

ステップ 4 パスワード、確認パスワード、またはエクスポートファイル名を入力し、[エクスポート（Export）] をクリックします。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。

CSV ファイルにデバイスの詳細をエクスポートするもののデバイスのクレデンシャルは含めない場合は、設定アイコンの横にある をクリックします。この CSV ファイルには、デバイスの詳細を何件でもエクスポートできます。しかし、このCSVファイルを使用してデバイスをインポートすることはできません。

クレデンシャルプロファイルを使用したデバイスクレデンシャルの一貫した適用

資格情報のプロファイルは、TL1、HTTP、Telnet/SSH SNMP デバイスの認証情報のコレクションです。デバイスを追加するときは、デバイスを使用する必要があります資格情報のプロファイルを指定できます。これにより、デバイス間で一貫して資格情報の設定を適用できます。

資格情報の変更、デバイスのパスワードの変更などを行う必要がある場合は、設定がプロファイルを使用するすべてのデバイスにわたって更新されるプロファイルを編集できます。

既存のプロファイルを表示するには、[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [クレデンシャルプロファイル（Credential Profiles）] を選択します。

新しいクレデンシャル プロファイルの作成

この手順を使用して、新しいクレデンシャルプロファイルを作成します。次に、そのプロファイルを使用し、製品全体か、または新しいデバイスの追加時に、クレデンシャルを一貫して適用できます。

ステップ 1 **[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [クレデンシャル プロファイル（Credential Profiles）]** を選択します。

ステップ 2 既存のクレデンシャルプロファイルに必要な設定のほとんどがある場合は、それを選択し、[コピー（Copy）] をクリックします。それ以外の場合は、[追加（Add）] をクリックします。

ステップ 3 プロファイル名と説明を入力します。名前と説明が [クレデンシャルプロファイル（Credential Profiles）] ページに表示されるため、クレデンシャルプロファイルが多くなる場合は可能な限り識別しやすい名前と説明にします。

ステップ 4 プロファイルのクレデンシャルを入力します。このプロファイルを使用してデバイスを追加または更新すると、ここで指定した内容がそのデバイスに適用されます。

SNMP 読み取りコミュニティ ストリングは必須です。

ステップ 5 [Save Changes] をクリックします。

既存のデバイスへの新規または変更されたプロファイルの適用

次の手順を使用して、デバイスを一括編集し、そのデバイスが関連付けられているクレデンシャル プロファイルを変更します。この操作は、デバイスとクレデンシャル プロファイル間の既存の関連付けを上書きします。また、この操作を使用して、デバイス設定を新しい設定と同期させることもできます。

（注） この手順を実行して [**Update and Sync**] を選択する前に、プロファイルのクレデンシャル設定が正しいことを確認してください。この操作によって、デバイスは新しいプロファイルと同期します。

ステップ 1 次のいずれかの方法を使用して、クレデンシャル プロファイルを設定します。

- 新しいクレデンシャル プロファイルを作成するには、**[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [クレデンシャル プロファイル（Credential Profiles）]** を選択し、[追加（Add）] をクリックします。
- 既存のプロファイルを編集するには、**[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [クレデンシャル プロファイル（Credential Profiles）]** を選択し、プロファイルを選択し、[編集（Edit）] をクリックします。

ステップ 2 プロファイルに納得できたら、**[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ネットワーク デバイス（Network Devices）]** を選択します。

ステップ 3 変更するすべてのデバイスをフィルタリングして選択します（一括編集）。

ステップ 4 [編集（Edit）] をクリックし、[クレデンシャル プロファイル（Credential Profile）] ドロップダウン リストから新しいクレデンシャル プロファイルを選択します。

ステップ 5 次のように変更を保存します。

- [更新（Update）] は、変更を Prime Infrastructure データベースに保存します。
- [更新して同期（Update and Sync）] は、変更を Prime Infrastructure データベースに保存し、デバイスの物理インベントリと論理インベントリを収集して、インベントリのすべての変更を Prime Infrastructure データベースに保存します。

クレデンシャル プロファイルの削除

この手順で、クレデンシャル プロファイルを Prime Infrastructure から削除します。現在、プロファイルがデバイスに関連付けられている場合は、デバイスの関連付けをそのプロファイルから解除する必要があります。

ステップ 1 何らかのデバイスがプロファイルを使用しているかどうかを確認します。

a) **[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [クレデンシャル プロファイル（Credential Profiles）]** に移動します。

b) 削除するクレデンシャル プロファイルを選択します。

c) [編集（Edit）] をクリックし、[デバイス リスト（Device List）] ページにデバイスが一覧表示されているかどうかを確認します。デバイスが一覧表示されている場合は、それらをメモします。

ステップ 2 必要に応じて、プロファイルからデバイスの関連付けを解除します。

a) **[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ネットワーク デバイス（Network Devices）]** に移動します。

b) 変更するすべてのデバイスをフィルタリングして選択します（一括編集）。

c) [編集（Edit）] をクリックし、[クレデンシャル プロファイル（Credential Profile）] ドロップダウン リストから [--選択--（--Select--）] を選択します。

d) 警告ダイアログボックスで[OK]をクリックし、古いプロファイルからデバイスの関連付けを解除します。

ステップ 3 クレデンシャル プロファイルを削除するには、**[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [クレデンシャル プロファイル（Credential Profiles）]** を選択し、プロファイルを選択し、[削除（Delete）] をクリックします。

簡単な管理と設定のためのデバイス グループの作成

- グループの仕組み （61 ページ）
- ユーザ定義のデバイス グループの作成 （66 ページ）
- ロケーション グループの作成 （68 ページ）
- ポート グループの作成 （72 ページ）
- グループのコピーの作成 （74 ページ）
- メンバーがいないグループの非表示 （75 ページ）
- グループの削除 （75 ページ）

デバイスを論理グループに編成すると、デバイスの管理、モニタリング、設定が簡素化されます。グループに操作を適用できるため、グループ化によって時間が節約され、ネットワーク全体で設定が一貫して適用されます。すべてのデバイスを同じ設定で構成できる小規模の構成で

は、ただ1つの一般的なデバイス グループを作成するだけで済みます。グループ化メカニズムは、サブグループもサポートしています。これらのグループは、多くの Prime Infrastructure GUI ウィンドウに表示されます。

デバイスが Prime Infrastructure に追加されると、[未定義（Unassigned）] という名前のロケーション グループに割り当てられます。多数のデバイスを管理している場合は、デバイスを他のグループに移動して、[未定義（Unassigned）] のグループ メンバーシップが大きくなりすぎないようにしてください。

グループの仕組み

グループはアクセス制御を行いません。アクセス制御は仮想ドメインによって決まります。この違いについては、グループおよび仮想ドメイン （66 ページ） を参照してください。

特定のタイプのグループについては、関連項目 ネットワーク デバイス グループ （61 ページ） および ポート グループ （63 ページ） を参照してください。

グループに要素を追加する方法については、グループに要素を追加する方法：動的、手動、および混在グループ （65 ページ） を参照してください。

ネットワーク デバイス グループ

次の表に、サポートされているネットワーク デバイス グループのタイプを示します。デバイス グループにはインベントリからアクセスできます。

ネットワーク デバイス グループの種類	メンバーシップの条件	ユーザが作成または編集できるか

デバイス タイプ（Device Type）	デバイスはファミリごとにグループ化されます（たとえば、、ルータ、スイッチおよびハブなど）。各デバイス ファミリの下で、デバイスはさらにシリーズごとにグループ化されます。新しいデバイスは、適切なファミリおよびシリーズ グループに自動的に割り当てられます。たとえば、Cisco ASR 9006 は、ルータ（ファミリ）および Cisco ASR 9000 シリーズ アグリゲーション サービス ルータ（シリーズ）に属します。 次の点に注意してください。 • デバイス タイプ グループを作成することはできません。これらはシステム定義の動的グループです。代わりに、デバイス基準を使用してユーザ定義のグループを作成し、適切なデバイス名を付けます。 • デバイス タイプ グループはネットワーク トポロジ マップには表示されません。 • [Prime Infrastructure] で検出されたサポート対象外のデバイスには [サポート対象外のシスコデバイス（Unsupported Cisco Device）] デバイスタイプが自動的に割り当てられ、**[デバイスタイプ（Device Type）] > [サポート対象外のシスコデバイスファミリ（Unsupported Cisco Device Family）]** に表示されます。	いいえ
ロケーション（Location）	ロケーション グループを使用して、ロケーションごとにデバイスをグループ化できます。デバイスを手動で追加するか、またはデバイスを動的に追加して、ロケーション グループの階層（シアター、国、地域、キャンパス、ビルディング、フロアなど）を作成できます。 デバイスは 1 つのロケーション グループのみに表示されるはずですが、上位レベルの「親」グループにもそのデバイスが含まれています。たとえば、ビルディングのロケーション グループに属するデバイスは、親のキャンパス グループにも間接的に属している場合があります。 デフォルトでは、階層の上位のロケーションが [すべてのロケーション（All Locations）] グループとなります。ロケーションに割り当てられていないデバイスはすべて、[すべてのロケーション（All Locations）] の下の [未割り当て（Unassigned）] グループに表示されます。	はい

ユーザ定義（User Defined）	デバイスは、デバイスおよびロケーション条件のカスタマイズ可能な組み合わせによってグループ化されます。グループ名をカスタマイズして、必要なデバイスおよびロケーション基準を使用できます。 ユーザが作成したロケーション グループは、選択したグループ（キャンパス、建物、屋外領域、屋内区域など）に応じてワイヤレス マップと同期します。したがって、ユーザが作成したロケーション グループは **[マップ（Maps）] > [ワイヤレスマップ（Wireless Maps）] > [サイトマップ（Site Maps）]** の下に表示され、同様に、ユーザがマップの下に作成したサイトは**[インベントリ（Inventory）] > [グループ管理（Group Management）] > [ネットワークデバイスグループ（Network Device Groups）]** の下に階層形式で表示されます。	対応

ポート グループ

次の表に、サポートされているポート グループのタイプを示します。

ポート グループの種類	メンバーシップの条件	ユーザが作成または編集できるか
ポート タイプ（Port Type）	ポートの種類、速度、名前、または説明ごとにグループ化されます。新しいデバイスのポートは、適切なポート グループに自動的に割り当てられます。 ポート タイプのグループは作成できません。代わりに、デバイス基準を使用してユーザ定義グループを作成し、ユーザ定義グループの下にサブグループを作成します。	いいえ。代わりに、ユーザ定義グループを作成します。

システム定義（System Defined）	ポートの使用状況または状態別にグループ化されます。新しいデバイスのポートは、適切なポート グループに自動的に割り当てられます。 [リンクポート（Link Ports）]：別のシスコ デバイスまたは他のネットワーク デバイスに接続され、「VLAN」モードで動作し、VLAN に割り当てられるポート。 [Trunk Ports]：シスコ デバイスまたは他のネットワーク デバイス（スイッチ、ルータ、ファイアウォール、サードパーティ デバイス）に接続され、すべての VLAN のトラフィックを伝送する「トランク」モードで動作しているポート。 [アクセスポート（Access Ports）]：エンド ホスト、IP Phone、サーバ、アクセス ポイント（AP）またはビデオ エンド ポイントに接続され、ある特定の VLAN のみのトラフィックを伝送する「アクセス」モードで動作しているポート。[未接続ポート（Unconnected Ports）]：デバイスに接続されていない、管理ステータスがダウンしている、または動作状態がダウンしているポート。 ポートのステータスがダウンすると、そのポートは[未接続ポート（Unconnected Port）] グループに自動的に追加されます。このグループ内のポートを削除することはできません。また、このグループを他のグループのサブ グループとして再作成することはできません。 システム定義のポート グループは作成できません。代わりに、デバイス基準を使用してユーザ定義グループを作成し、ユーザ定義グループの下にサブグループを作成します。 （注） [WAN インターフェイス（WAN Interfaces）] はスタティック グループであるため、自動ポートの追加は適用されません。したがって、手動でグループにポートを追加する必要があります。	いいえ。代わりに、ユーザ定義グループを作成します。
ユーザ定義（User Defined）	ポート基準のカスタマイズ可能な組み合わせによってグループ化され、グループに名前を付けることができます。グループが動的でポートが条件に一致する場合は、そのグループに追加されます。	対応

データセンター グループ

次の表に、サポートされているデータセンター グループのタイプを示します。

表 *10* : サポートされているデータセンター グループのタイプ

データセンターグループのタイプ	メンバーシップの条件	ユーザが作成または編集できるか
システム定義	タイプ別にグループ化されます（データセンター、クラスタ、仮想マシン（VM）、ホスト）。 システム定義のデータセンター グループを作成することはできません。代わりに、デバイス基準を使用してユーザ定義のデータセンター グループを作成し、ユーザ定義グループの下にサブグループを作成します。	いいえ。VM およびホスト用のユーザ定義グループを作成できます。
ユーザ定義	デバイスおよびロケーション条件のカスタマイズ可能な組み合わせによってグループ化されます。グループ名をカスタマイズし、必要なデバイス基準を使用できます。	対応

グループに要素を追加する方法：動的、手動、および混在グループ

グループに要素を追加する方法は、グループが動的か、手動か、混在かによって異なります。

デバイスの追加方法	説明
動的	要素がグループ基準を満たしている場合、Prime Infrastructure はグループに新しい要素を自動的に追加します。指定できるルールの数に制限はありませんが、ルールを追加するにしたがい更新のパフォーマンスに影響が及ぶ場合があります。
手動	グループの作成時またはグループの編集時に、ユーザは手動で要素を追加します。
混合	要素は、動的ルールと手動追加の組み合わせによって追加されます。

デバイス名およびポート名の一致基準を指定する場合に * や ? などのワイルドカードを使用すると、グループ内の新しい要素を動的に追加できます。例：

- *a*：名前に文字「a」が含まれます。
- ?a*：名前の 2 番目の文字に「a」が含まれます。
- ?a：名前に含まれる文字は 2 つだけで、2 番目の文字は「a」になります。
- *a：名前の最後の文字は「a」です。

親/子のユーザ定義グループおよびロケーション グループにおけるデバイスの継承は次のとおりです。

- ユーザ定義グループ：子グループを作成する場合：

- 親グループと子グループの両方がダイナミックの場合、子グループは親グループ内のデバイスにのみアクセスできます。
- 親グループが静的で、子グループが動的である場合、子グループは親グループ外のデバイスにアクセスできます。
- 親グループと子グループが動的かつ静的である場合、子グループは親のデバイス グループからデバイスを「継承」します。

- ロケーション グループ：親グループは子のグループ デバイスを継承します。

（注） 親グループの下に作成する子グループの数に制限はありません。子グループの階層レベルにも制限はありません。

グループおよび仮想ドメイン

グループは要素の論理コンテナですが、要素へのアクセスは仮想ドメインによって制御されます。次の例は、グループと仮想ドメインの関係を示しています。

- **SanJoseDevices** という名前のグループに 100 台のデバイスが含まれています。
- **NorthernCalifornia** という名前の仮想ドメインに 400 台のデバイスが含まれています。これらのデバイスはさまざまなグループに属しており、**SanJoseDevices** グループのデバイスが 20 台含まれています。

NorthernCalifornia 仮想ドメインにアクセスできるユーザは、**SanJoseDevices** グループの 20 台のデバイスにアクセスできますが、このグループ内の他の 80 台のデバイスにはアクセスできません。詳細については、デバイスへのユーザアクセスを制御するための仮想ドメインの作成を参照してください。

ユーザ定義のデバイス グループの作成

新しいデバイス タイプ グループを作成するには、ユーザ定義グループのメカニズムを使用します。デバイス タイプ グループは Prime Infrastructure 全体で使用される特殊なカテゴリであるため、このメカニズムを使用する必要があります。作成するグループが [ユーザ定義（User Defined）] カテゴリに表示されます。

新しいグループを作成するには、次の手順を実行します。

ステップ 1 **[インベントリ（Inventory）] > [グループ管理（Group Management）] > [ネットワークデバイスグループ（Network Device Groups）]** の順に選択します。

ステップ 2 [[デバイスグループ（Device Groups）]] ペインで [+]（**追加**）アイコンをクリックし、[ユーザ定義グループの作成（Create User Defined Group）] を選択します。

ステップ 3 グループの名前と説明を入力します。他のユーザ定義デバイス タイプ グループが存在する場合、[親グループ（Parent Group）] ドロップダウン リストからグループを選択することで、そのグループを親グループとして設定できます。親グループを選択しなかった場合は、新しいグループが [ユーザ定義（User-Defined）] フォルダに配置されます（デフォルト）。

（注） グループ名に '、"、<、>、&、?、/ などの特殊文字は使用できません。

ステップ 4 次のように、デバイスを新しい グループに追加します。

条件を満たすデバイスを自動的に追加する場合は、[デバイスを動的に追加（Add Devices Dynamically）] 領域に条件を入力します。IP アドレスの特定の範囲内に入るデバイスをグループ化するには、角カッコ内にその範囲を入力します。たとえば、次を指定できます。

- IPv4-10.[101-155].[1-255].[1-255] および 10.126.170.[1-180]
- IPv6-2014::5217:[0000-ffff]:fe22:[1e40-1f41]

（注） ダイナミック グループに指定できるルールの数に制限はありませんが、ルールの数が増えるとグループの更新パフォーマンスが低下する可能性があります。

デバイスを手動で追加する場合は、次の手順を実行します。

1. [デバイスを手動で追加（Add Devices Manually）] 領域を展開し、[追加（Add）] をクリックします。
2. [デバイスの追加（Add Devices）] ダイアログボックスで、追加するデバイスのチェックボックスをオンにして、[追加（Add）] をクリックします。

ステップ 5 [プレビュー（Preview）] タブをクリックしてグループのメンバーを表示します。

ステップ 6 [保存（Save）] をクリックします。

ステップ 3 で選択したフォルダに新しいデバイス グループが表示されます。

デバイスが属するすべてのグループの表示

デバイスが属するデバイス グループのリストを表示するには、次の手順を実行します。

ステップ 1 **[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ネットワーク デバイス（Network Devices）]**、または **[インベントリ（Inventory）] > [グループ管理（Group Management）] > [ネットワーク デバイス グループ（Network Device Groups）]** を選択します。

ステップ 2 左側の [デバイス グループ（Device Group）] ペインの [検索（Search）] フィールドに IP アドレスまたはデバイス名を入力すると、デバイスが属するすべてのグループのリストが表示されます。

検索フィールドにグループ名を入力してグループを検索することもできます。

ロケーション グループの作成

ステップ 1 **[インベントリ（Inventory）] > [グループ管理（Group Management）] > [ネットワークデバイスグループ（Network Device Groups）]** の順に選択します。

ステップ 2 左側の [デバイス グループ（Device Groups）] ペインで、[追加（Add）] アイコンをクリックし、[ロケーション グループの作成（Create Location Group）] を選択します。

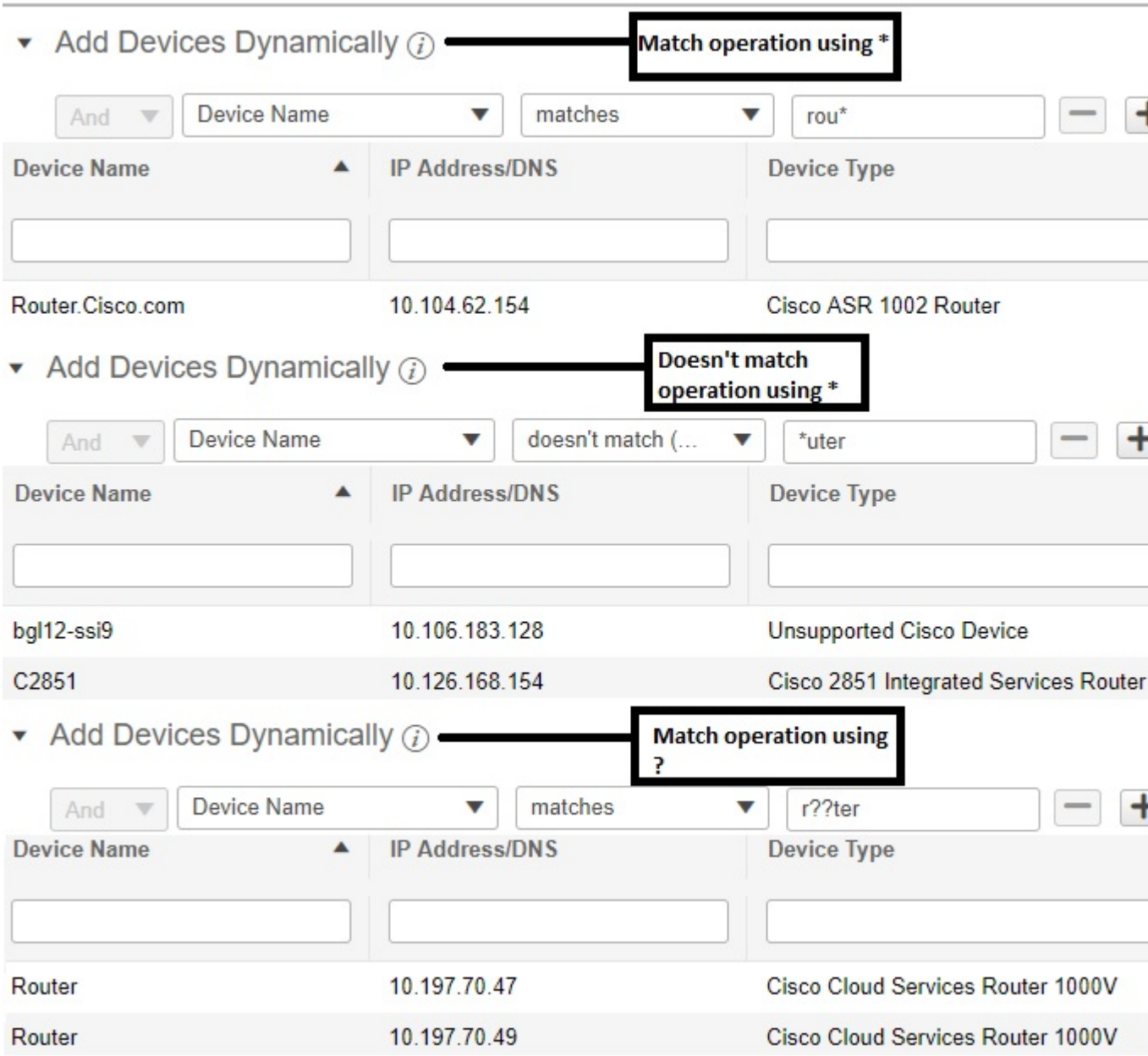
ステップ 3 名前と説明を入力し、[親グループ（Parent Group）] ドロップダウンリストからグループを選択します。デフォルトでは、[すべてのロケーション（All Locations）] のサブグループになります（つまり、[すべてのロケーション（All Locations] フォルダに表示されます）。

ステップ 4 たとえば、特定の住所のビルディングにあるすべてのデバイスなど、地理的なロケーションに基づいてデバイス グループを作成する場合は、[地理的なロケーション（Geographical Location）] チェックボックスをオンにしてグループの GPS 座標を指定するか、または [マップの表示（View Map）] リンクをクリックし、マップ内の必要な場所をクリックします。この場合は、GPS 座標が自動的に入力されます。地理的なロケーションで定義されたロケーション グループは、Geo マップのグループ アイコンで表されます。グループに追加するデバイスは、そのグループの GPS 座標を継承します。地理的なロケーションが一連のデバイスをグループ化する主たる理由の場合は、グループに追加するデバイスに、そのグループとは異なる独自の GPS 座標を持たせないことを推奨します。

[シビックロケーション（Civic Location）] を指定する場合は、検索キーワードを手動で入力して、ドロップダウンリストからロケーションを選択します。

ステップ 5 特定の基準を満たしている場合にデバイスが自動的に追加されるようにするには、[デバイスを動的に追加（Add Devices Dynamically）] 領域に基準を入力します。それ以外の場合は、この領域を空欄のままにします。

ルール（[一致（matches）] および [不一致（doesn't match）]）では、ワイルドカード文字がサポートされます。次に示すように、検索テキストにワイルドカード文字（* および ?）を含めることができます。



ダイナミック グループに指定できるルールの数に制限はありませんが、ルールの数が増えると、グループ更新のパフォーマンスが低下する可能性があります。

ステップ 6 デバイスを手動で追加する場合は、次の手順を実行します。

a) [デバイスを手動で追加（Add Devices Manually）] で、[追加（Add）] をクリックします。

b) [デバイスの追加（Add Devices）] ダイアログボックスで、追加するデバイスを見つけて、[追加（Add）] をクリックします。

ステップ 7 [プレビュー（Preview）] タブをクリックして、グループ メンバーを確認します。

ステップ 8 [保存（Save）] をクリックすると、ステップ 3 で選択したフォルダ（デフォルトでは [すべてのロケーション（All Locations）]）の下に新しいロケーション グループが表示されます。

CSV ファイルを使用したグループの作成

Prime Infrastructure に追加するグループのすべての属性が一覧表示されている CSV ファイルを使用してグループをインポートするには、次の手順を実行します。

ステップ 1 **[インベントリ（Inventory）][グループ管理（Group Management）][ネットワーク デバイス グループ（Network Device Groups）]** を選択し、**[グループのインポート（Import Groups）]** をクリックします。

ステップ 2 ここのリンクをクリックし、CSV ファイルのサンプル テンプレートをダウンロードします。

テンプレート内で示されているように、CSV ファイル内の必須情報は必ず保持してください。

ステップ 3 [グループのインポート（Import Groups）] ダイアログ ボックスで [ファイルの選択（Choose File）] をクリックし、インポートするグループが含まれている CSV ファイルを選択します。

ステップ 4 [インポート（Import）] をクリックします。

ステップ 5 **[管理（Administration）] > [ダッシュボード（Dashboards）] > [ジョブ ダッシュボード（Job Dashboard）]** を選択し、**[グループのインポート（Import Groups）]** をクリックしてジョブのステータスを表示します。

CSV ファイルへのグループのエクスポート

グループ情報を CSV ファイルとしてエクスポートするには、次の手順を実行します。

ステップ 1 [Inventory] > [Group Management] > [Network Device Groups] の順に選択します。

ステップ 2 PI または APIC EM を選択します。

ステップ 3 **[グループのエクスポート（Export Groups）]** をクリックして、すべてのロケーション グループの詳細が含まれている CSV ファイルをローカル システムにダウンロードします。

デバイス グループとロケーション グループへの AP の追加

手順の概要

1. **[インベントリ（Inventory）] > [グループ管理（Group Management）] > [ネットワークデバイスグループ（Network Device Groups）]** の順に選択します。
2. 左側の [デバイスグループ（Device Groups）] ペインで、[ユーザ定義（User Defined）] または [ロケーション（Location）] の横にある展開アイコンの上にマウスのカーソルを合わせ、[サブグループの追加（Add SubGroup）] をクリックします。

3. 名前、説明、および親グループ（該当する場合）を入力します。
4. 次のいずれかの方法で AP を追加します。
5. [プレビュー（Preview）] をクリックして、指定したルールと手動で追加した AP に基づいてグループに自動的に追加された AP を確認します。
6. [保存（Save）] をクリックします。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**[インベントリ（Inventory）] > [グループ管理（Group Management）] > [ネットワークデバイスグループ（Network Device Groups）]** の順に選択します。	
ステップ 2	左側の [デバイスグループ（Device Groups）] ペインで、[ユーザ定義（User Defined）] または [ロケーション（Location）] の横にある展開アイコンの上にマウスのカーソルを合わせ、[サブグループの追加（Add SubGroup）] をクリックします。	
ステップ 3	名前、説明、および親グループ（該当する場合）を入力します。	
ステップ 4	次のいずれかの方法で AP を追加します。	• 手動：[デバイスを手動で追加する（Add Devices Manually）] の下にある [追加（Add）] をクリックし、グループに追加する AP を選択します。 • 動的：このポート グループに追加される前に AP が従う必要のあるルールを指定します。ダイナミック グループには AP を追加しません。Prime Infrastructure が指定されたルールに一致する AP をダイナミック グループに追加します。 デフォルト以外のロケーション グループのタイプを選択すると、AP は動的には追加されません。
ステップ 5	[プレビュー（Preview）] をクリックして、指定したルールと手動で追加した AP に基づいてグループに自動的に追加された AP を確認します。	
ステップ 6	[保存（Save）] をクリックします。	グループにメンバーとして「**ユニファイド AP**」または「**サードパーティ AP**」がある場合、新しいタブがデバイス ワーク センターの右側のテーブルに追加され、AP が表示されます。

ポート グループの作成

ポート グループを作成するには、次の手順を実行します。

ステップ 1 **[インベントリ（Inventory）] > [グループ管理（Group Management）] > [ポート グループ（Port Groups）]** を選択します。

ステップ 2 **[ポートグループ（Port Groups）] > [ユーザ定義（User Defined）]** から、[ユーザ定義（User Defined）] の横にある [i] アイコンの上にカーソルを置き、ポップアップウィンドウの [サブグループの追加（Add SubGroup）] をクリックします。

ステップ 3 名前と説明を入力し、[親グループ（Parent Group）] ドロップダウンリストからグループを選択します。デフォルトでは、ポート グループは [ユーザ定義（User Defined）] フォルダに配置されます。

ステップ 4 グループに追加するためにポートが属している必要があるデバイスを選択します。[デバイスの選択（Device Selection）] ドロップダウンリストから、次を選択できます。

- [デバイス（Device）] : すべてのデバイスのフラット リストからデバイスを選択します。
- [デバイス グループ（Device Group）] : デバイス グループを選択します（[デバイス タイプ（Device Type）]、[ロケーション（Location）]、および [ユーザ定義（User Defined）] グループのリストが表示されます）。

ステップ 5 基準を満たしている場合にポートが自動的に追加されるようにするには、[ポートを動的に追加（Add Ports Dynamically）] 領域に基準を入力します。それ以外の場合は、この領域を空欄のままにします。

ダイナミックグループに指定できるルールの数に制限はありませんが、ルールの数が増えると、グループ更新のパフォーマンスが低下する可能性があります。

ステップ 6 デバイスを手動で追加する場合は、次の手順を実行します。

a) [ポートを手動で追加（Add Port Manually）] で、[追加（Add）] をクリックします。
b) [ポートの追加（Add Devices）] ダイアログボックスで、追加するデバイスを見つけて、[追加（Add）] をクリックします。

ステップ 7 [プレビュー（Preview）] タブをクリックして、グループ メンバーを確認します。

ステップ 8 [保存（Save）] をクリックすると、ステップ 3 で選択したフォルダ（デフォルトでは [ユーザ定義（User Defined）]）の下に新しいポート グループが表示されます。

ユーザ定義データセンター グループの作成

設定済みのデータセンターおよびクラスタのグループに加え、VMおよびホストにユーザ定義グループを作成できます。ユーザ定義グループを作成するには、次の手順を実行します。

ステップ 1 **[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [コンピューティング デバイス（Compute Devices）]** を選択します。

ステップ 2 [コンピューティング リソース（Compute Resources）] ペインで [ユーザ定義のホストおよび VM（User Defined Hosts and VMs）] を見つけ、[i]（**情報**）アイコンの上にカーソルを合わせます。

ステップ 3 [アクション（Actions）] 領域から、[サブグループの追加（Add Subgroup）] をクリックします。

[デバイス サブグループの追加（Add Device Subgroup）] ページが開きます。

ステップ 4 グループの名前と説明を入力し、グループを配置するフォルダを [親グループ（Parent Group）] ドロップダウン リストから選択します。

ステップ 5 次のように、デバイスをロケーション グループに追加します。

- 条件を満たすデバイスを自動的に追加する場合は、[デバイスを動的に追加（Add Devices Dynamically）] 領域に条件を入力します。

  （注） ダイナミック グループに指定できるルールの数に制限はありませんが、ルールの数が増えるとグループの更新パフォーマンスが低下する可能性があります。

- デバイスを手動で追加する場合は、次の手順を実行します。

  1. [デバイスを手動で追加（Add Devices Manually）] 領域を展開し、[追加（Add）] をクリックします。
  2. [デバイスの追加（Add Devices）] ダイアログボックスで、追加するデバイスのチェックボックスをオンにして、[追加（Add）] をクリックします。

ステップ 6 [プレビュー（Preview）] タブをクリックし、グループに所属させるデバイスを表示します。

ステップ 7 [保存（Save）] をクリックします。ステップ 4 で選択したフォルダに新しいグループが表示されます。

ユーザ定義グループの編集

編集オプションを使用して、親グループの変更、デバイスの追加、およびデバイス ルールの変更を行うことができます。

手順

	コマンドまたはアクション	目的
ステップ 1	**[インベントリ（Inventory）] > [グループ管理（Group Management）] > [ネットワーク デバイス グループ（Network Device Groups）]** を選択します。	
ステップ 2	左側の [デバイス グループ（Device Groups）] ペインで、編集するグループの名前をクリックします。	
ステップ 3	[編集（Edit）] をクリックして、詳細を変更します。	ロケーション グループを編集しているときに、次に該当する場合はグループ タイプをキャンパスに変更できます。 • グループ タイプがデフォルト。 • グループにサブグループがない。

	コマンドまたはアクション	目的
ステップ 4	[プレビュー（Preview）] をクリックして、更新されたデバイスの詳細を表示します。	
ステップ 5	[保存（Save）] をクリックして、更新されたデバイスの詳細を保存します。	

グループのコピーの作成

グループの複製を作成すると、Prime Infrastructure はデフォルトでそのグループに **CopyOf***group-name* という名前を付けます。名前は必要に応じて変更できます。

グループを複製するには、次の手順を実行します。

ステップ 1 **[インベントリ（Inventory）] > [グループ管理（Group Management）] > [ネットワークデバイスグループ（Network Device Groups）]** の順に選択します。

ステップ 2 左側の [デバイス グループ（Device Groups）] ペインから、グループを選択します。

ステップ 3 コピーするデバイス グループを見つけ、その横にある [i] をクリックするとポップアップ ウィンドウが開きます。

ステップ 4 [グループの複製（Duplicate Group）] をクリックし（この時点では変更を加えない）、[保存（Save）] をクリックします。Prime Infrastructure によって **CopyOf***group-name* という新しいグループが作成されます。

ステップ 5 ユーザ定義のデバイス グループの作成 （66 ページ）とロケーション グループの作成 （68 ページ）の説明に従ってグループを設定します。

ステップ 6 [プレビュー（Preview）] タブをクリックし、グループメンバーを調査して、グループの設定を確認します。

ステップ 7 [保存（Save）] をクリックして、グループを保存します。

ユーザ定義グループおよびロケーション グループのコピー

任意のユーザ定義のグループまたはロケーション グループを [グループの複製（Duplicate Group）] オプションを使用して複製できます。複製したグループには、元のグループのすべての値が含まれており、これらの値は変更できます。自動入力されたグループ名には、デフォルトで「CopyOf」のプレフィックスが追加されます。名前は必要に応じて変更できます。

子グループを複製すると、同じ親グループに子グループのコピーが作成されます

親グループを複製すると、それぞれの子グループのコピーが作成されます。

手順

	コマンドまたはアクション	目的
ステップ 1	**[インベントリ（Inventory）] > [グループ管理（Group Management）] > [ネットワークデバイスグループ（Network Device Groups）]** の順に選択します。	
ステップ 2	左側の [デバイス グループ（Device Groups）] ペインで、複製するデバイス グループを見つけます。グループの名前の横にある [i] アイコンをクリックし、ポップアップ メニューを表示します。	
ステップ 3	[グループの複製（Duplicate Group）] をクリックし、グループの詳細情報を更新します。	
ステップ 4	[プレビュー（Preview）] をクリックし、複製グループの詳細情報を表示します。	
ステップ 5	[保存（Save）] をクリックし、複製グループを保存します。	

メンバーがいないグループの非表示

デフォルトでは、グループにメンバーが存在しなくても、Prime Infrastructure は Web GUI にグループを表示します。管理者権限を持つユーザが、この設定を変更して空のグループが非表示になる、つまり Web GUI に表示されないようにすることができます。（非表示グループは Prime Infrastructure から削除されません）。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** を選択し、**[インベントリ（Inventory）] > [グループ化（Grouping）]** を選択します。

ステップ 2 [メンバーが存在しないグループの表示（Display groups with no members）] をオフにし、[保存（Save）] をクリックします。

グループやデバイスが多数ある場合は、[メンバーが存在しないグループの表示（Display groups with no members）]チェックボックスをオンのままにすることをお勧めします。これをオフにすると、システムのパフォーマンス速度が低下します。

グループの削除

削除するグループにメンバーが含まれていないことを確認します。メンバーが含まれている場合、Prime Infrastructure で操作を続行することはできません。

ステップ 1 **[インベントリ（Inventory）] > [グループ管理（Group Management）] > [ネットワークデバイスグループ（Network Device Groups）]** の順に選択します。

ステップ 2 削除するデバイス グループを左側の [デバイス グループ（Device Groups）] ペインで見つけ、その横にある [i] をクリックするとポップアップ ウィンドウが開きます。

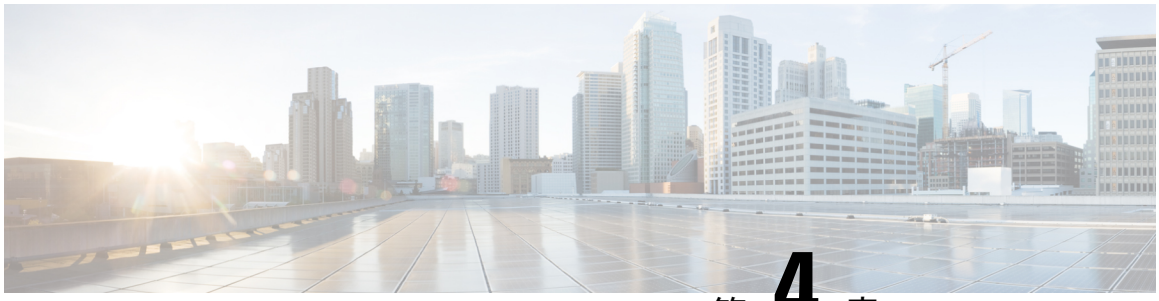
ステップ 3 [グループの削除（Delete Group）] をクリックし、[OK] をクリックします。

コンピューティング リソース グループの作成

データセンターやクラスタなどのコンピューティング サービスの設定済みグループの他に、UCS サーバ、ホスト、および VM にユーザ定義グループを作成できます。

手順

	コマンドまたはアクション	目的
ステップ 1	**[インベントリ（Inventory）] > [コンピューティング デバイス グループ（Compute Device Groups）]** を選択します。	
ステップ 2	左側の [コンピューティング リソース（Compute Resources）] で、**[ユーザ定義の UCS（User Defined UCS）]** または **[ユーザ定義のホストおよび VM（User Defined Hosts and VMs）]** の横にある展開アイコンの上にマウスを合わせ、[サブグループの追加（Add SubGroup）] をクリックします。	
ステップ 3	グループ名と説明を入力し、必要に応じて親グループを選択します。	
ステップ 4	[デバイスを動的に追加（Add Devices Dynamically）] ペインで、グループ内のデバイスに適用するルールを指定します。	
ステップ 5	[デバイスを手動で追加（Add Devices Manually）] ペインで、グループに割り当てるコンピューティング リソースを選択します。	
ステップ 6	[プレビュー（Preview）] をクリックして、指定したルールと手動で追加したデバイスに基づいてグループに自動的に追加されたデバイスを確認します。	
ステップ 7	**[保存（Save）]** をクリックして、指定した設定でデバイス グループを追加します。	



第 4 章

デバイスの表示

- ネットワーク デバイスの表示 （77 ページ）

ネットワーク デバイスの表示

[ネットワークデバイス（Network Devices）]ページ（**[インベントリ（Inventory）]>[デバイス管理（Device Management）]>[ネットワークデバイス（Network Devices）]**）または（**[モニタ（Monitor ）]>[管理対象要素（Managed Elements）]>[ネットワークデバイス（Network Devices）]**）から、デバイスのインベントリおよびデバイス設定情報を表示できます。このページには、次の表で説明する一般的な管理機能と構成機能が含まれています。

表 *11* : ネットワーク デバイスのタスク

タスク	説明	ネットワークデバイスページ内の場所
デバイスの管理	デバイスの追加、編集、削除、同期、エクスポート、デバイスの管理状態の設定、グループやサイトに対するデバイスの追加または削除、および一括インポートを実行できます。	これらの機能は、ページの上部にあるツールバーで使用できます。詳細については、「手動によるデバイスの追加（新規デバイス タイプまたはデバイス シリーズ）」、「CSV ファイルへのデバイス情報のエクスポート」、および「他のソースからのデバイスのインポート」を参照してください。
	デフォルトおよび子の VDC を追加、編集、削除、同期、およびエクスポートできます。	VDC の詳細については、「手動によるデバイスの追加（新規デバイス タイプまたはデバイス シリーズ）」を参照してください。

タスク	説明	ネットワークデバイスページ内の場所
基本的なデバイス情報と収集ステータスの表示	情報（到達可能性ステータス、IP アドレス、デバイス タイプ、収集ステータスなど）が表示されます。 （注） さらに、**[ネットワーク デバイス (Network devices)]** 画面で、デバイスの IP アドレス/DNS、ソフトウェア タイプ、場所、作成タイムスタンプ、デバイス ロール、製品ファミリ、シリアル番号、およびモデル番号の詳細を表示できます。右上隅の [設定 (settings)] アイコンをクリックし、**[カラム (Columns)]** メニューを展開して、特定の情報が **[ネットワークデバイス (Network Devices)]** 画面に表示されるようにする必要があるオプションを選択します。	[IPアドレス（IP Address）] 列から、[i]（**情報**）アイコンをクリックして、そのデバイスの 360 度ビューを開きます（[デバイス360度ビュー（Device 360° View）] からのデバイス詳細の取得 （1121 ページ）を参照）。 [最新のインベントリ収集（Last Inventory Collection）] 列から、[i]（**情報**）アイコンの上にカーソルを置くと、発生したインベントリ収集エラーがリストされたポップアップ ウィンドウが開きます。
デバイス グループの管理	デフォルトでは、Prime Infrastructure が動的デバイス グループを作成して、デバイスを適切な [デバイスタイプ（Device Type）] フォルダに割り当てます。新しいデバイス グループを作成でき、[ユーザ定義（User Defined）] フォルダに格納されます。	デバイス グループは、[デバイスグループ（Device Groups）] ペインに表示されます。
サイト グループへのデバイスの追加	サイト グループを設定した後、[ネットワーク デバイス（Network Devices）] ページからデバイスを追加できます。 サイトマップにデバイスを追加するには、**[マップ（Maps）]** > **[サイトマップ（Site Map）]** を選択します。 （注） 1 つのデバイスは 1 つのサイト グループ階層にのみ属することができます。	• [グループとサイト（Groups & Sites）] ドロップダウン リストから、[グループに追加（Add to Group）] を選択します。 • **[デバイスの追加（Add Device）]** ドロップダウン リストから、**[デバイスの追加（Add Device）]** を選択し、**[グループに追加（Add to Group）]** ドロップダウンリストから適切なグループを選択します。。 • デバイスを選択した状態で、[デバイスの編集（Edit Device）] をクリックし、[グループに追加（Add to Group）] ドロップダウンリストから適切なグループを選択します。 • [デバイスの追加（Add Device）] ドロップダウンリストから、[一括インポート（Bulk Import）] を選択して CSV ファイルを使用してデバイスをインポートします。

タスク	説明	ネットワークデバイスページ内の場所
デバイス詳細の表示	メモリ、ポート、環境、シャーシ ビュー、インターフェイス情報などのデバイス詳細が表示されます。	デバイスの [デバイスの詳細（Device Details）] ページを開くには、デバイス名のハイパーリンクをクリックします。
	デバイスの情報とステータス、および関連するモジュール、アラーム、ネイバー、インターフェイス、管理対象の VDC、VDC の詳細が表示されます。	[IPアドレス（IP Address）] 列から、デバイスの [i]（**情報**）アイコンをクリックして、360 度ビューを開きます。
コンフィギュレーションテンプレートの作成と展開	選択したデバイスでデバイス機能を設定できます。また、デバイスに展開された適用済みおよびスケジュール済みの機能テンプレートのリストを表示できます。 （**注**） [ネットワークデバイス（Network Devices）] ページからいくつかのコントローラ機能を設定できない場合があります。この場合は、[機能およびテクノロジー（Features & Technologies）] ページ（**[設定（Configuration）] > [テンプレート（Templates）] > [機能およびテクノロジー（Features & Technologies）]**）で新しいテンプレートを作成し、それをデバイスに展開します。	デバイス名のハイパーリンクをクリックして、[設定（Configuration）] タブをクリックします。
デバイス コンフィギュレーションの表示	アーカイブしたコンフィギュレーションを表示し、コンフィギュレーションのロールバックをスケジュールし、アーカイブ収集をスケジュールします。	デバイス名のハイパーリンクをクリックして、[設定アーカイブ（Configuration Archive）] タブをクリックします。
ソフトウェアイメージの表示	1 つのデバイスに対して推奨されるソフトウェア イメージを表示して、そのイメージをインポートまたは配布できます。	1. デバイス名のハイパーリンクをクリックして、[イメージ（Image）] タブをクリックします。 2. **[推奨イメージ（Recommended Images）]** エリアを展開して、選択したデバイスに推奨されるイメージを表示します。Prime Infrastructure は cisco.com とローカル リポジトリの両方から推奨イメージを収集します。 推奨されるイメージをインポートするか、または配布することができます。

タスク	説明	ネットワークデバイスページ内の場所
インターフェイス詳細の表示	インターフェイスの説明、管理ステータス、および動作ステータスを表示できます。	デバイス名のハイパーリンクをクリックして、[インターフェイス（Interfaces）] タブをクリックします。インターフェイスの 360 度ビューを開くには、[名前（Name）] 列の [i]（**情報**）アイコンをクリックします。
TrustSec 設定の表示および変更	TrustSec ベースのデバイスの Cisco TrustSec 設定を表示および変更できます。	**1.** デバイス名のハイパーリンクをクリックして、[設定（Configuration）] タブをクリックします。 **2.** **[セキュリティ（Security）] > [TrustSec] > [有線 802_1x（Wired 802_1x）]** を選択します。
シャーシ ビュー	デバイスの前面パネルまたは背面パネルをグラフィカルに表示できます。	[シャーシビュー（Chassis View）] が表示されるデバイスの [デバイスの詳細（Device Details）] ページを開くには、デバイス名のハイパーリンクをクリックします。 （注） 次のデバイスでは、シャーシ ビューをサポートします。 • すべての AireOS ワイヤレス LAN コントローラ • Cisco 5760 LAN コントローラ • Catalyst 3850 スイッチ • Catalyst 3650 –28 ポート、52 ポート ライン カードのみ • Catalyst 4500 –48 ポート ライン カードのみ • Catalyst 9300 • Catalyst 9400 • Catalyst 9500 • Catalyst 4000 スイッチ （注） Cat 9k デバイスでは、標準 PID のみがサポートされており、ポートモジュールの組み合わせはサポートされていません。
VDC の詳細の表示	VDC サマリ、VDC リソース、CPU 使用率の上位 3 つの VDC と割り当てられた CPU、および管理対象の VDC を表示できます。	デバイス名のハイパーリンクをクリックして、[VDC] タブをクリックします。

（注） デュアル スタック Prime Infrastructure マシンの場合、IPv4 アドレスはデフォルトで組み込まれています。

関連トピック

コンピューティング デバイスの表示 （81 ページ）

コンピューティング デバイスの表示

[コンピューティングデバイス（Compute Devices）]ページには、データセンター内で計算機能を提供している全デバイスの統合ビューがあります。このページを開くには、次のいずれかを実行します。

- **[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [コンピューティングデバイス（Compute Devices）]** を選択します。
- **[モニタ（Monitor）] > [管理対象要素（Managed Elements）] > [コンピューティングデバイス（Compute Devices）]** を選択します。

ここから、次の表に示す物理デバイス（データセンターの仮想化をサポートしている Cisco UCS B シリーズ、C シリーズ、E シリーズのデバイスなど）およびデータセンター コンポーネントのデバイス インベントリ情報を表示できます。

表 *12 :* コンピューティング デバイスのタスク

タスク	リスト ビュー	詳細ビュー
データセンターの表示	クラスタ、ホスト、およびVMの数、VM ステータス、ディスカバリ ソース、およびデータセンターのモニタリング ステータスが表示されます。	詳細ビューを開くには、データセンター名のハイパーリンクをクリックします。このビューには 4 つのタブが表示されます。 • [クラスタ（Clusters）] タブ：データセンターで使用可能なクラスタの数が表示されます。 • [全般（General）] タブ：選択したデータセンターのプロパティが表示されます。 • [ホスト（Host）] タブ：選択したデータセンターで使用可能なホストの詳細およびインストールされているオペレーティング システムの追加情報が表示されます。 • [仮想マシン（Virtual Machines）] タブ：選択したデータセンターで利用可能な仮想マシンの詳細、および付与されているメモリ量とディスク レートに関する追加情報が表示されます。

タスク	リスト ビュー	詳細ビュー
クラスタの表示	ホスト数、VM 数、VM 電源の状態、VM の電源オン/オフ ステータスおよびディスカバリ ソースが表示されます。	詳細ビューを開くには、クラスタ名のハイパーリンクをクリックします。このビューには 4 つのタブが表示されます。 • [全般（General）] タブ：選択したクラスタのプロパティが表示されます。 • [アラーム（Alarms）] タブ：クラスタに生成されたアラームが表示されます。 • [ホスト（Hosts）] と [仮想マシン（Virtual Machines）] タブ：クラスタに関連付けられているホストと VM の動作ステータス、CPU 使用率、メモリ使用率が表示されます。

タスク	リスト ビュー	詳細ビュー
ホストの表示	ホストの名前、ステータス、IP アドレス、ハイパーバイザ タイプ、VM の総数、VM ステータス、およびモニタリング ステータスが表示されます。 このページを設定して、ホストのディスカバリ ソースやアラーム数などの追加情報を表示することができます。これを行うには、[設定（Settings）] アイコンをクリックし、[列（Columns）] リストから追加する列を選択します。 （注） ホストが Prime Infrastructure で管理されている Cisco UCS ブレードサーバにインストールされている場合、[物理サーバ（Physical Server）] 列にはブレードサーバの名前が表示され、[物理デバイス名（Physical Device Name）] 列にはブレードサーバが配置されている Cisco UCS シャーシの名前が表示されます。	詳細ビューを開くには、ホスト名のハイパーリンクをクリックします。ここから、ホストとその親クラスタのパフォーマンス メトリックを表示できます。パフォーマンス メトリックでは、CPU 使用率、メモリ使用率、ネットワーク パフォーマンスがグラフ表示されます。 詳細ビューには、次の 4 つのタブも表示されます。 • [全般（General）] タブ：選択したホストのプロパティが表示されます。 • [仮想マシン（Virtual Machine）] タブ：ホストに属している VM の動作ステータス、CPU 使用率、メモリ使用率が表示されます。 • [アラーム（Alarms）] タブ：ホストに生成されたアラームが表示されます。 • [ユーザ定義フィールド（User Defined Fields）] タブ：ここから、ホスト用に設定されたユーザ定義の値を更新できます。

タスク	リスト ビュー	詳細ビュー
仮想マシンの表示	選択した VM の名前、動作ステータス、IP アドレス、ホスト名、オペレーティング システム、およびモニタリング ステータスが表示されます。 VM のディスカバリ ソースやアラーム数などの追加情報を表示するように、このページを設定できます。これを行うには、[設定（Settings）] アイコンをクリックし、[列（Columns）] リストから追加する列を選択します。	詳細ビューを開くには、VM 名のハイパーリンクをクリックします。ここから、VM とその親ホストおよびクラスタのパフォーマンス メトリックを表示できます。VM メトリックでは、CPU、メモリ、ディスク、およびネットワークの使用率がグラフ表示されます。親ホスト メトリックでは、CPU、メモリ、およびネットワークの使用率がグラフ表示されます。親クラスタ メトリックでは、CPU およびメモリの使用率がグラフ表示されます。 詳細ビューには、次の 4 つのタブも表示されます。 • [仮想マシン全般（Virtual Machine General）] タブ：選択した VM のプロパティが表示されます。 • [ホスト全般（Host General）] タブ：ホストが Cisco UCS ブレード サーバにインストールされている場合、物理サーバのプロパティが表示されます。 • [アラーム（Alarms）] タブ：VM に生成されたアラームが表示されます。 • [ユーザ定義フィールド（User Defined Fields）] タブ：ここから、デバイスに関する追加情報が格納されているユーザ定義属性（デバイスの場所属性など）を更新できます。

タスク	リスト ビュー	詳細ビュー
物理サーバの表示	ID、デバイス名、IP アドレス、動作ステータス、コア、メモリなど、Cisco UCS ブレード サーバの情報が表示されます。このページには、サーバに関連付けられているホストの IP アドレス、名前、および OS も表示されます。	[サーバID（Server ID）] 列から、サーバの ID ハイパーリンクをクリックすると、その詳細ビューと、CPU、メモリ、アダプタなどのサーバ コンポーネントに関する情報を提供するアクセス タブが開きます。
コンピューティング サービスの表示	コンピューティング サービスの名前、その動作ステータス、IP アドレス、タイプ、サービスに生成された最新のアラーム、および合計アラーム数が表示されます。	追加予定
Cisco UCS サーバの表示	名前、タイプ、IP アドレス、到達可能性ステータス、アラームの数など、基本的なデバイス情報が表示されます。ここから、サーバを選択してグループに追加したり、グループから削除することができます。	[デバイス名（Device Name）] 列で、サーバ名のハイパーリンクをクリックすると、Cisco UCS シャーシとブレード サーバ間の相互接続とその動作ステータスを示す図が開きます。
ディスカバリ ソースの表示	ディスカバリ ソースの名前、到達可能性ステータス、ディスカバリ ジョブ ステータス、および仮想インベントリ収集ステータスが表示されます。ここから、新しいデバイスを追加したり、既存のデバイスを編集または削除したり、選択したデバイスを同期することができます。	追加予定

タスク	リスト ビュー	詳細ビュー
ユーザ定義 UCS サーバの表示	Prime Infrastructure では、指定した条件を満たすデバイスに自動的に読み込まれるグループを作成できます。Cisco UCS サーバ グループを作成するには、次の手順に従います。 **1.** [コンピューティングリソース（Compute Resources）]ペインから、[i]（**情報**）アイコンの上にカーソルを置き、ポップアップ ウィンドウを開きます。 **2.** [アクション（Actions）]領域から、[サブグループの追加（Add Subgroup）]をクリックします。 **3.** 「ユーザ定義のデバイス グループの作成」で説明されている手順のステップ 3 ～ 6 を実行します。	追加予定

タスク	リスト ビュー	詳細ビュー
ユーザ定義のホストと VM の表示	Prime Infrastructure では、指定した条件を満たすデバイスおよび VM に自動的に読み込まれるグループを作成できます。ホストおよび VM グループを作成するには、次の手順に従います。 **1.** [コンピューティングリソース（Compute Resources）]ペインから、[i]（**情報**）アイコンの上にカーソルを置き、ポップアップ ウィンドウを開きます。 **2.** [アクション（Actions）]領域から、[サブグループの追加（Add Subgroup）]をクリックします。 **3.** 「ユーザ定義のデバイス グループの作成」で説明されている手順のステップ 3 ～ 6 を実行します。	追加予定

関連トピック

ユーザ定義の UCS グループの作成 （88 ページ）
ユーザ定義のホストと VM の作成 （89 ページ）

ユーザ定義の UCS グループの作成

コンピューティング デバイスの詳細を表示することに加えて、ユーザ定義の UCS サブグループを作成できます。[User Defined UCS] の横にある展開アイコンにマウスを移動し、[Add SubGroup] をクリックします。関連項目の「デバイス グループの作成」を参照してください。ただし、これらの **[ユーザ定義のUCS（User Defined UCS）] グループは [モニタ（Monitor）] > [モニタリングツール（Monitoring Tools）] > [アラームおよびイベント（Alarms and Events）]** に反映されません。

関連トピック

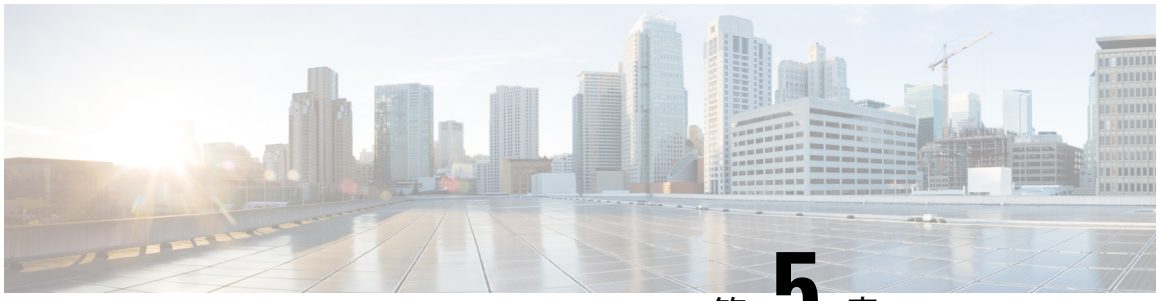
ユーザ定義のホストと VM の作成 （89 ページ）

ユーザ定義のホストと VM の作成

デバイス グループに類似したユーザ定義ホスト グループと VM サブ グループを作成できます。[ユーザ定義のホストとVM（User Defined Hosts and VMs）] の横にある展開アイコンにマウスを移動し、[サブグループの追加（Add SubGroup）] をクリックします。ただし、この [ユーザ定義のホストとVM（User Defined Hosts and VMs）] グループは **[モニタ（Monitor）]** > **[モニタリングツール（Monitoring Tools）]** > **[アラームおよびイベント（Alarms and Events）]** に反映され、このグループのあらゆるメンバがアラームやイベントをモニタできます。

関連トピック

ユーザ定義の UCS グループの作成 （88 ページ）



第 5 章

コンピューティング リソースの管理

- VMware vCenter Server の管理 （91 ページ）
- コンピューティング リソース パフォーマンスのモニタ （93 ページ）

VMware vCenter Server の管理

VMware vCenter Server の追加、削除、編集、同期、および一括インポートを行うことができ、さらに、データセンター、クラスタ、ホスト、および仮想マシン（VM）のようなコンピューティング リソースの完全なインベントリを表示することもできます。

関連トピック

VMware vCenter Server の追加 （91 ページ）

vCenter をインポートするための CSV ファイルの要件 （92 ページ）

VMware vCenter Server の追加

VMware vCenter Server を管理するために、手動でそのサーバを追加するには、次の手順を実行します。

はじめる前に

vCenter サーバのインベントリ情報を収集するには、データセンター ハイパーバイザ ライセンスをインストールする必要があります。このライセンスを追加する方法については、『Cisco Prime Infrastructure Admin Guide』ガイドの「Licenses and Software Updates」の章を参照してください。

ステップ 1 **[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [コンピューティングデバイス（Compute Devices）]** を選択します。

ステップ 2 [コンピューティングリソース（Compute Resources）]ペインから、[ディスカバリソース（Discovery Sources）] をクリックします。

ステップ 3 [デバイスの追加（Add Device）] ドロップダウンリストから、[デバイスの追加（Add Device）] を選択します。

ステップ 4 [ディスカバリ ソースの追加（Add Discovery Source）] ダイアログボックスに、次のパラメータを指定します。

1. [プロトコル（Protocol）：[HTTP] または [HTTPS] を選択します。
2. [サーバ（Server）]：vCenter サーバのホスト名または IP アドレスを入力します。
3. [ポート（Port）]：HTTP の場合は「80」、HTTPS の場合は「443」と入力します。
4. [ユーザ名とパスワード（Username and Password）]：vCenter サーバへのログインに必要なクレデンシャルを入力します。

   確認のために、パスワードをもう一度入力する必要があります。

   （注） パスワードにはカンマ（,）を使用しないでください。使用すると、Prime Infrastructure にデバイスを追加するときにパスワードが分割されます。

ステップ 5 （任意）vCenter サーバを追加する前に、[クレデンシャルの確認（Verify Credentials）] をクリックして、入力したクレデンシャルが有効であることを確認します。

ステップ 6 [追加（Add）] をクリックします。

ステップ 7 [ディスカバリ ソース（Discovery Sources）] ページから、追加したばかりの vCenter サーバを検索し、その値を [仮想インベントリ収集ステータス（Virtual Inventory Collection Status）] 列に表示します。

[ライセンスなし（No License）] が表示された場合は、データ センター ハイパーバイザ ライセンスをインストールする必要があります。サーバのインベントリ情報を収集するには、このライセンスが必要です。

関連トピック

vCenter をインポートするための CSV ファイルの要件 （92 ページ）

vCenter をインポートするための CSV ファイルの要件

CSV ファイルを使用して VMware vCenter Server を別のソースから Cisco Prime Infrastructure にインポートするには、次の手順を実行してサンプル テンプレートをダウンロードします。

1. **[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [コンピューティングデバイス（Compute Devices）]** を選択します。
2. [コンピューティングリソース（Compute Resources）] ペインから、[ディスカバリ ソース（Discovery Sources）] をクリックします。
3. [デバイスの追加（Add Device）] ドロップダウンリストから、[一括インポート（Bulk Import）] を選択します。

   [一括インポート（Bulk Import）] ダイアログボックスが開きます。
4. 一括の仮想ディスカバリのサンプルテンプレートをダウンロードするには、[ここ（here）] リンクをクリックします。

Cisco Prime Infrastructure で完全なインベントリ収集を有効にするには、ディスカバリ ソースの CSV ファイルに次のパラメータの値を指定する必要があります。

- IPアドレス/ホスト名
- [パスワード（Password）]
- ポート番号
- [ユーザ名（Username）]
- プロトコル

関連トピック

VMware vCenter Server の追加 （91 ページ）

コンピューティング リソース パフォーマンスのモニタ

Prime Infrastructure は、定期的にデバイスをポーリングすることによって管理対象のコンピューティング リソースをモニタします。

Prime Infrastructure は、仮想要素の健全性を監視するための CPU、メモリ、ディスク、およびネットワークに関連する Key Performance Indicator（KPI; 重要業績評価指標）の定義済みセットの定期的なポーリングをサポートしています。Prime Infrastructure は VM を直接ポーリングしませんンが、アプリケーション プログラミング インターフェイス（API）経由で Vcenter から定期的にデータを取得します。デフォルトのポーリング間隔は 5 分です。次に示すようにポーリング間隔を変更できます。

関連トピック

データセンター デバイスのポーリング間隔の設定 （93 ページ）
クラスタ モニタリングのセットアップ （94 ページ）

データセンター デバイスのポーリング間隔の設定

ポーリングは、データセンター、クラスタ、およびホストで有効にできます。これを行うと、ポーリングを選択したエンティティの子でポーリングが自動的に有効になります。たとえば、クラスタでのポーリングを有効にすると、そのクラスタに属しているすべてのホストと VM でもポーリングが有効になります。

ポーリング間隔を設定するには、次の手順を実行します。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** を選択し、**[インベントリ（Inventory）] > [データセンターの設定（Datacenter Settings）]** を選択します。

ステップ 2 ドロップダウン リストからポーリング間隔を選択します。

デフォルト値は **5 分**です。

ステップ 3 [保存（Save）] をクリックします。

関連トピック

クラスタ モニタリングのセットアップ （94 ページ）

クラスタ モニタリングのセットアップ

クラスタをモニタするには、次の手順を実行します。

ステップ 1 **[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [コンピューティングデバイス（Compute Devices）]** を選択します。

ステップ 2 [コンピューティング リソース（Compute Resources）] ペインから、[クラスタ（Clusters）] をクリックします。

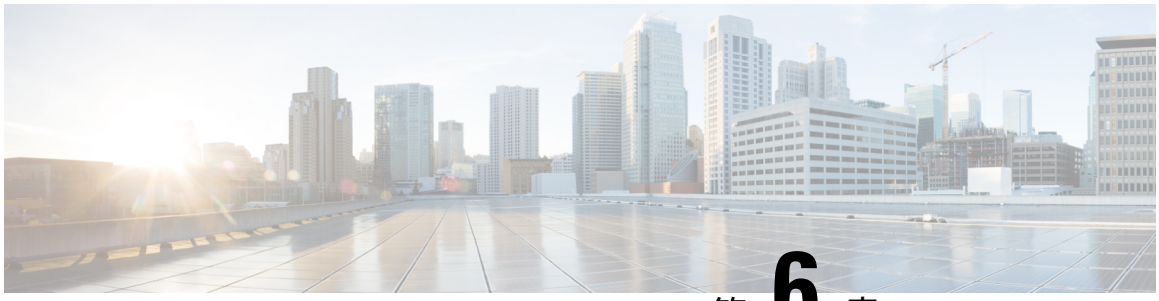
ステップ 3 モニタするクラスタのチェックボックスをオンにして [モニタリングの開始（Start Monitoring）] をクリックします。

次の点に注意してください。

- クラスタのモニタを停止するには、この手順を繰り返し、ステップ 3 の代わりに [モニタリングの停止（Stop Monitoring）] をクリックします。
- 親データセンターまたは親クラスタのモニタリングは子ホストまたは子クラスタからは停止できません。ただし、子ホストまたは子クラスタのモニタリングは親データセンターまたは親クラスタから停止できます。

関連トピック

データセンター デバイスのポーリング間隔の設定 （93 ページ）



第 6 章

デバイス コンフィギュレーション ファイルの管理

この章は、次の内容で構成されています。

- デバイス コンフィギュレーション ファイル管理のセットアップ （95 ページ）
- ファイルが最後にアーカイブされた時刻を確認する方法 （101 ページ）
- デバイス コンフィギュレーション ファイルのアーカイブへのバックアップ （101 ページ）
- アーカイブに保存されているデバイス コンフィギュレーション ファイルの表示 （103 ページ）
- タグを使用した重要なコンフィギュレーション ファイルのラベル付け （105 ページ）
- 実行デバイス コンフィギュレーションとスタートアップ デバイス コンフィギュレーションの同期 （106 ページ）
- デバイスのコンフィギュレーション ファイルの比較または削除 （107 ページ）
- デバイスへの外部コンフィギュレーション ファイルの展開 （108 ページ）
- 実行コンフィギュレーションによるスタートアップ コンフィギュレーションの上書き （109 ページ）
- アーカイブされたバージョンへのデバイス設定のロールバック （109 ページ）
- コンフィギュレーション ファイルのダウンロード （111 ページ）
- 設定アーカイブ操作に関する変更監査の確認 （112 ページ）

デバイスコンフィギュレーションファイル管理のセットアップ

- アーカイブのトリガー方法の制御 （96 ページ）
- イベント トリガー アーカイブをセットアップする （97 ページ）
- 設定ファイルの変更を確認する場合に除外する項目の指定 （98 ページ）
- 設定アーカイブ操作のタイムアウトの制御 （98 ページ）
- 並行してアーカイブできるファイル数の制御 （99 ページ）

• データベースからデバイス コンフィギュレーション ファイルを消去するタイミングの制御 （100 ページ）

アーカイブのトリガー方法の制御

デフォルトでは、Prime Infrastructure は次のタイミングでデバイス コンフィギュレーション ファイルをアーカイブに保存します。

- 新しいデバイスが Prime Infrastructure に追加された場合
- デバイスの変更通知を受信した場合
- 完全同期または詳細同期の場合にアーカイブ収集が実行されない

（注） イベントが発生すると、設定されたホールドオフ タイマーの期間後にアーカイブ データが収集されます。

管理者権限を持つユーザーはこれらの設定を変更できます。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** を選択し、**[インベントリ（Inventory）] > [設定アーカイブ（Configuration Archive）]** を選択します。

ステップ 2 次の条件に従って、アーカイブ設定を調整します。

このチェックボックスをオンした場合：	ファイルをアーカイブする条件：
デバイスを追加しながら設定をアーカイブする（Archive configuration while adding a device）	新しいデバイスが追加された場合（デフォルトで有効にされます）
設定が変更されるたびに、設定アーカイブを収集する（Collect Configuration Archive whenever configuration is changed）	設定の変更通知が送信された場合（デフォルトで有効にされます）。次を参照：イベント トリガー アーカイブをセットアップする （97 ページ）

ステップ 3 デバイスのグループ（または単一のデバイス）に対して定期的なアーカイブをスケジュールするには、次の手順に従います。

a) **[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [設定アーカイブ（Configuration Archive）]** の順に選択します。

b) [デバイス（Devices）] タブで、定期的にアーカイブする複数のデバイスまたはデバイス グループを選択します。

c) **[アーカイブ収集のスケジュール設定（Schedule Archive Collection）]** をクリックし、[繰り返し（Recurrence）] 領域でスケジュール設定を実行します。多数のデバイスに対してこの操作が行われるようにする場合、実稼働に影響を与える可能性が最も少ない時間にアーカイブをスケジュールしてください。

（注） SFTP を介したデバイス設定の収集を有効にするには、設定を「localdisk/sftp」ディレクトリにコピーします。デフォルトでは、このオプションは無効になっています。有効にするには、「/opt/CSCOlumos/conf/ifm」フォルダで「ifm_config_archive.properties」ファイルを見つけ、「**COPY_CONFIGURATIONS_TO_LOCAL_STORAGE**」の値を true に設定します。これは新しくアーカイブされたコンフィギュレーション ファイルにのみ適用されます。過去にアーカイブされたコンフィギュレーション ファイルは、このディレクトリにコピーされません。

d) [リポジトリへのバックアップ（Backup to Repository）] ボタンをクリックして、定期的にデバイス設定を外部リポジトリに転送します。リポジトリの設定や作成は CLI コマンドで行うことができます。サポートされているリポジトリは FTP、SSH FTP（SFTP）、ネットワーク ファイル システム（NFS）です。

イベント トリガー アーカイブをセットアップする

デフォルトで、Prime Infrastructure は、変更通知イベントを受信するたびに、デバイスのコンフィギュレーションファイルをバックアップします。この機能は、デバイスが適切に設定されている場合にのみ機能します。たとえば、Cisco IOS XR と Cisco IOS XE を実行しているデバイスの場合は、次の設定を行う必要があります。

```
logging server-IP
```

Prime Infrastructure は設定変更イベントを受信すると、さらに設定変更イベントを受信した場合に備えて 10 分間（デフォルト）待機してからアーカイブを実行します。これにより、複数の収集プロセスの同時実行が回避されます。この設定を確認または変更するには、**[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** を選択してから、**[インベントリ（Inventory）] > [設定アーカイブ（Configuration Archive）]** を選択し、[ホールドオフタイマー（Hold Off Timer）]を調整します。

イベント トリガー アーカイブをオフにするには、**[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** を選択してから、**[インベントリ（Inventory）] > [設定アーカイブ（Configuration Archive）]** を選択し、**[設定が変更されるたびに、設定アーカイブを収集する（Collect Configuration Archive whenever configuration is changed）]** チェックボックスをオフにします。

（注） [ジョブダッシュボード（Jobs Dashboard）] > [ユーザジョブ（User Jobs）] > [設定アーカイブ収集（Configuration Archive Collection）] ページの [アーカイブ（Archive）] 列には、設定が変更されていない収集済みアーカイブに対して「アーカイブがデバイスと一致しました（Archive matches device）」メッセージが表示されます。

（注） WLC では設定変更イベントに関する Syslog メッセージが送信されないため、この機能は WLC ではサポートされていません。

設定ファイルの変更を確認する場合に除外する項目の指定

Prime Infrastructureは、設定タイプが同じでバージョンの異なるデバイス コンフィギュレーションファイルを比較して違いを特定する際に、ファイルの一部の行を除外する必要があります。Prime Infrastructure はデフォルトでルータやスイッチのクロック設定など、一部の行を除外します。管理者権限がある場合は、除外される行を確認した上で、除外する行を追加できます。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** を選択し、**[インベントリ（Inventory）] > [設定アーカイブ（Configuration Archive）]** を選択します。

ステップ 2 [Advanced] タブをクリックします。

ステップ 3 [製品ファミリ（Product Family）] リストで、コマンドの除外を適用するデバイスまたはグループを選択します。

ステップ 4 [コマンド除外リスト（Command Exclude List）] に、その選択で除外するカンマ区切りのコンフィギュレーション コマンドのリストを入力します。これらは、コンフィギュレーションの変更についてデバイスを確認する際に Prime Infrastructure が無視するパラメータです。

ステップ 5 **[保存（Save）]** をクリックします。

設定アーカイブ操作のタイムアウトの制御

設定アーカイブタスクでは、フェッチアクティビティごとにデバイスのCLIタイムアウト値が使用されます。1 つの設定アーカイブタスクには 1 ～ 5 個のファイルが伴います。その結果、全体的なジョブタイムアウト値は次のロジックを使用して決定されます。**全体的なジョブタイムアウト = ファイルの数 * デバイスの CLI タイムアウト**。

CLI タイムアウト値を設定するには、**[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ネットワークデバイス（Network Devices）]** を選択し、デバイス編集アイコンをクリックし、[Telnet/SSH] オプションを選択し、[タイムアウト（Timeout）] フィールドに値を入力します。

（注） CLIのタイムアウトにより設定アーカイブ タスクが失敗した場合は、デバイスのCLIタイムアウト値を増加する必要があります。

アーカイブ サマリーの更新頻度の制御

選択すると **[在庫（Inventory）]** > **[デバイス管理（Device Management）]** > **[構成アーカイブ（Configuration Archive）]** 、 Prime Infrastructure を集めて構成アーカイブ一覧が表示されます。新しいアーカイブを収集するたびに、この集計データが更新されます。既定ではサマリの更新タイマーによると少なくとも 30 分も更新されます。時間設定を変更するには、**[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** を選択してから、

[インベントリ（Inventory）] > [設定アーカイブ（Configuration Archive）] を選択し、**[サマリー更新ホールドオフタイマー（Summary refresh Hold off timer）]** を調整します。

並行してアーカイブできるファイル数の制御

Prime Infrastructure は、コンフィギュレーション ファイルをアーカイブにコピーするために 10 個のスレッド プールを使用します。1,000 を超えるデバイスが関わる変更をアーカイブする場合は、数が大きいほど役立ちます。ただし、数が大きすぎると、システムのパフォーマンスに悪影響を与える可能性があります。この数を変更するには、**[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** を選択してから、**[インベントリ（Inventory）] > [設定アーカイブ（Configuration Archive）]** を選択し、[スレッドプール数（Thread Pool Count）] 値を調整します。

エクスポート中に設定ファイルのコンテンツをマスクするかどうかの制御

Prime Infrastructure起動および実行構成ファイルをローカル ファイル システムにエクスポートをサポートします。既定では、これらのファイルの内容は、彼らがエクスポートされるときにマスクされます。構成ファイルをエクスポートするのには 参照してくださいコンフィギュレーション ファイルのダウンロード （99 ページ） 。。

コンフィギュレーション ファイルのダウンロード

同時に最大 1000 台までのデバイスの起動および実行コンフィギュレーション ファイルをローカル システムにダウンロードできます。

ステップ 1 [インベントリ（Inventory）] > [デバイス管理（Device Management）] > [設定アーカイブ（Configuration Archive）] の順に選択します。

ステップ 2 [最新の設定をエクスポート（Export Latest Config）] ドロップダウンリストから次のいずれかのオプションを選択して、コンフィギュレーション ファイルをダウンロードします。

1. [サニタイズ（Sanitized）] : デバイスのクレデンシャル パスワードがダウンロードしたファイル内でマスクされます。
2. [非サニタイズ（Unsanitized）] : デバイスのクレデンシャル パスワードがダウンロード ファイル内に表示されます。

このオプションは、サポートされているすべての設定を csv ファイルとしてデバイスからダウンロードします。デバイスからスタートアップ コンフィギュレーションまたは実行コンフィギュレーションのみを指定してダウンロードするには、次の代替ステップを使用します。

[非サニタイズ（Unsanitized）] オプションは、ロールベース アクセス コントロール（RBAC）で設定されているユーザ権限に基づいて表示されます。

また、次の手順を実行しても、設定をダウンロードすることができます。

- [インベントリ（Inventory）]>[デバイス管理（Device Management）]>[設定アーカイブ（Configuration Archive）]ページで、設定ファイルをダウンロードするデバイスをクリックするか、または[インベントリ（Inventory）]>[デバイス管理（Device Management）]>[ネットワークデバイス（Network Devices）]ページで設定ファイルをダウンロードするデバイスをクリックし、[設定アーカイブ（Configuration Archive）] タブをクリックします。
- [展開（Expand）] アイコンを使用して、必要な設定の詳細をアーカイブから表示します。
- [詳細（Details）] をクリックします。
- [エクスポート（Export）] ドロップダウンリストから [サニタイズ（Sanitized）] または [非サニタイズ（Unsanitized）] を選択します。

メモ　このコンフィギュレーション ファイルを WLC にアップロードする前に、各行の先頭にキーワード **config** を追加する必要があります。

データベースからデバイス コンフィギュレーション ファイルを消去するタイミングの制御

デバイスのコンフィギュレーションファイルをデータベースから自動的に削除することはできません（ファイルは手動で削除できます）。ファイルは、ユーザの設定に基づき、Cisco Prime Infrastructure Prime Infrastructure によって定期的に消去することができます。管理者権限を持つユーザは、コンフィギュレーションファイルが消去されるタイミングを次のように調整できます。コンフィギュレーション ファイルを一切消去しない場合は、次の手順に従う際、両方のフィールドを空にしてください。

ステップ 1　**[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** を選択し、**[インベントリ（Inventory）] > [設定アーカイブ（Configuration Archive）]** を選択します。

ステップ 2　次の条件に従って、アーカイブ設定を調整します。

使用するフィールド	ファイルを消去する条件
1 デバイスあたり保持する設定アーカイブの最大バージョン（Maximum configuration archive versions to be retained per device）	デバイスのコンフィギュレーション ファイルの数がこの設定（デフォルトは 5）を超えた場合。
設定アーカイブを保持する最大日数（Maximum days to retain configuration archive）	コンフィギュレーションファイルの存続期間がこの設定（デフォルトは 7）を超えた場合。

ファイルが最後にアーカイブされた時刻を確認する方法

ステップ 1 デバイスの実行コンフィギュレーション ファイルがアーカイブにバックアップされた最終日を特定するには、[インベントリ（Inventory）]>[デバイス管理（Device Management）]>[設定アーカイブ（Configuration Archive）] を選択し、[デバイス（Devices）] タブをクリックします。[最新のアーカイブ（Latest Archive）] 列に、最新のアーカイブが最初に示された各デバイスのアーカイブ タイム スタンプのリストが表示されます。[作成者（Created By）] 列には、アーカイブのトリガー（たとえば、syslog）が表示されます。

ステップ 2 デバイスの最新のアーカイブ済み実行コンフィギュレーション ファイルの内容を表示するには、タイム スタンプのハイパーリンクをクリックします。[実行コンフィギュレーション（Running Configuration）] ウィンドウにファイルの内容が表示されます。

ステップ 3 デバイスのアーカイブ間で加えられた変更を表示するには、デバイスのコンフィギュレーション ファイルの比較または削除 （107 ページ）を参照してください。

デバイスコンフィギュレーションファイルのアーカイブへのバックアップ

- データベースにバックアップされる内容 （101 ページ）
- コンフィギュレーション ファイルをバックアップ（アーカイブ）する （102 ページ）

データベースにバックアップされる内容

設定アーカイブは、デバイス コンフィギュレーション ファイルのコピーを保持し、それらをデータベースに保存します。ほとんどのコンフィギュレーション ファイルは、デバイスから受信したものとして読み取り可能な形式に保存され、以前のバージョンと比較できます。デバイス設定は、アーカイブに保存されているファイルを使用して、前の状態に復元できます。

（注） デバイスの設定アーカイブ ファイルのサイズは、740 KB 以下である必要があります。

デバイス上の実行コンフィギュレーションとスタートアップ コンフィギュレーションが同じ場合、Prime Infrastructure は実行コンフィギュレーションのみをデータベースにコピーします。そのため、イメージ リポジトリを表示するときに、実行コンフィギュレーションのアーカイブのみが表示されることがあります。

コンフィギュレーション ファイルが前回のバックアップ以降に変更されていない場合、Prime Infrastructure はファイルをアーカイブしません。Prime Infrastructure によってジョブの成功が報告され、ジョブ結果に [**Already Exists**] が表示されます。

Prime Infrastructure は、次のデバイス コンフィギュレーション ファイルを収集およびアーカイブします。

デバイス/デバイス OS	バックアップ内容
Cisco IOS および Cisco IOS XE	最新のスタートアップ コンフィギュレーション、実行コンフィギュレーション、および VLAN 設定。
Cisco IOS XR	• 最新の実行コンフィギュレーション。アクティブなパッケージが含まれます。デバイスは、システム ユーザが管理する必要があります。これは、システム ユーザ以外のユーザはコマンドライン インターフェイス（CLI）で copy コマンドを使用できないためです。 • データベース設定（バイナリ ファイル） （注） Cisco NCS 4000 デバイスの場合、データベースは、ローカルマシン上のファイルシステムに .tgz ファイルとしてバックアップされます。

コンフィギュレーションファイルをバックアップ（アーカイブ）する

コンフィギュレーション ファイルをバックアップすると、Prime Infrastructure がデバイスからコンフィギュレーションファイルのコピーを取得して、設定アーカイブ（データベース）にコピー（バックアップ）します。コピーをアーカイブに保存する前に、Prime Infrastructure は取得したファイルとアーカイブ内の同じタイプの最新バージョン（実行と実行、スタートアップとスタートアップ）を比較します。Prime Infrastructure は、2 つのファイルが異なる場合にのみファイルをアーカイブします。アーカイブ済みのバージョンの数が最大値（デフォルトは 5）を超えると、最も古いアーカイブが消去されます。

実行コンフィギュレーションとスタートアップ コンフィギュレーションの両方をサポートするデバイスの場合は、Prime Infrastructure がスタートアップ コンフィギュレーションの最新バージョンと実行コンフィギュレーション ファイルの最新バージョンを比較することによって、バックアッププロセス中に「同期外れ」（非同期）のデバイスを特定します。同期外れのデバイスの詳細については、実行デバイス コンフィギュレーションとスタートアップ デバイス コンフィギュレーションの同期 （106 ページ）を参照してください。

次の表に、サポートされているバックアップ方式とそれらのトリガー方法の説明を示します。デフォルト設定をチェックまたは調整するには、アーカイブのトリガー方法の制御 （96 ページ）を参照してください。

（注） SFTP を介してデバイス コンフィギュレーション コレクションを有効にするために、コンフィギュレーションが「localdisk/sftp」ディレクトリに自動的にコピーされます。これは新しくアーカイブされたコンフィギュレーション ファイルにのみ適用されます。過去にアーカイブされたコンフィギュレーション ファイルは、このディレクトリにコピーされません。このオプションを無効にするには、「/opt/CSCOlumos/conf/ifm」フォルダで「ifm_config_archive.properties」ファイルを見つけ、**COPY_CONFIGURATIONS_TO_LOCAL_STORAGE** の値を false に設定します。

表 *13* : バックアップ方式

バックアップ方式	説明	注意
オンデマンド手動バックアップ	[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [設定アーカイブ（Configuration Archive）] を選択して、デバイスを選択し、**[アーカイブ収集のスケジュール設定（Schedule Archive Collection）]** をクリックします（ジョブをすぐに実行するか後で実行します）。	該当なし
定期的にスケジュールされたバックアップ	[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [設定アーカイブ（Configuration Archive）] を選択して、デバイスを選択し、**[アーカイブ収集のスケジュール設定（Schedule Archive Collection）]** をクリックします。スケジューラで、[**Recurrence**] を指定します。	該当なし
インベントリ収集バックアップ	Prime Infrastructure は、インベントリ収集中に変更が検出された場合に自動的にバックアップを実行します。	デフォルトで無効
新しいデバイスのバックアップ	Prime Infrastructure は、自動的に新しいデバイスのバックアップを実行します。	デフォルトで有効
イベントトリガーバックアップ（デバイス変更通知）	Prime Infrastructure は、管理対象デバイスから syslog を受信したときに自動的にバックアップを実行します。	デフォルトで有効

アーカイブに保存されているデバイスコンフィギュレーション ファイルの表示

• すべてのアーカイブされたファイルを表示する （104 ページ）
• 特定のデバイスのアーカイブされたファイルを表示する （104 ページ）

すべてのアーカイブされたファイルを表示する

データベースに保存されたコンフィギュレーション ファイルを表示するには、[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [設定アーカイブ（Configuration Archive）] を選択します。開始する場所に応じて、[アーカイブ（Archives）] タブまたは [デバイス（Devices）] タブをクリックします。

- **Archives** タブ：アーカイブされたコンフィギュレーション ファイルのリスト。最新のアーカイブが先頭に表示されます。[アウト オブ バンド（Out of Band）] 列は、Prime Infrastructure 以外のアプリケーションによって変更が行われたかどうかを示します。左側の [グループ（Groups）] リストを使用して、アーカイブをデバイス タイプ別とファミリ別で表示します。グローバル設定に関して実行できることは次のとおりです。
  - アーカイブされたバージョンへのデバイス設定のロールバック （109 ページ）
  - 実行コンフィギュレーションによるスタートアップ コンフィギュレーションの上書き（109 ページ）
  - タグを使用した重要なコンフィギュレーション ファイルのラベル付け （105 ページ）
- **Devices** タブ：アーカイブされた設定を含むデバイスのフラットなリスト。グローバル設定に関して実行できることは次のとおりです。
  - アーカイブへのバックアップをスケジュールします（デバイス コンフィギュレーション ファイルのアーカイブへのバックアップ （101 ページ）を参照）。
  - デバイス名のハイパーリンクをクリックして、特定のデバイスのアーカイブされたファイルを表示します（特定のデバイスのアーカイブされたファイルを表示する （104 ページ）を参照）。

デフォルトで、Prime Infrastructure は、ファイルの最大 5 つのバージョンを保存し、7 日前より古いファイルをすべて削除します。デバイス コンフィギュレーション ファイルは、データベースから手動で削除することはできません（現在の消去設定をチェックするには、データベースからデバイス コンフィギュレーション ファイルを消去するタイミングの制御 （100 ページ）を参照してください）。

特定のデバイスのアーカイブされたファイルを表示する

（注） 実行コンフィギュレーション ファイルのみが表示されてスタートアップ ファイルが表示されない場合、2 つのファイルは同じです。Prime Infrastructure は実行コンフィギュレーションと異なる場合にのみスタートアップ コンフィギュレーションをバックアップします。

ステップ 1 [**Inventory**] > [**Device Management**] > [**Configuration Archive**] を選択して、[**Devices**] タブをクリックします。

ステップ 2 デバイス名のハイパーリンクをクリックします。Prime Infrastructure は、タイムスタンプに基づいてアーカイブ済みファイルを一覧表示します。

アーカイブされた設定ファイルの raw コンテンツの表示

この手順を使用して、設定アーカイブに保存されているスタートアップ コンフィギュレーション ファイル、実行コンフィギュレーション ファイル、VLAN（サポートされている場合）コンフィギュレーション ファイル、データベース コンフィギュレーション ファイルおよび管理コンフィギュレーション ファイルを表示します。タイム スタンプに応じてバージョンを選択し、それらを別のバージョンと比較できます。

設定アーカイブに保存されている実行コンフィギュレーション ファイルの内容を表示するには、次の手順を実行します。

ステップ 1 **[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [設定アーカイブ（Configuration Archive）]** を選択し、**[デバイス（Devices）]** タブをクリックします。

ステップ 2 デバイス名のハイパーリンクをクリックします。Prime Infrastructure は、タイムスタンプに基づいてアーカイブ済みファイルを一覧表示します。

ステップ 3 タイム スタンプを展開して、その時点でアーカイブされたファイルを表示します。実行コンフィギュレーション、スタートアップ コンフィギュレーション、管理コンフィギュレーション、VLAN コンフィギュレーション、およびデータベース コンフィギュレーションの詳細が表示されます。これらのカテゴリの下にある [詳細（Details）] ハイパーリンクをクリックし、詳細を表示します。

（注） 実行コンフィギュレーション ファイルのみが表示されてスタートアップ ファイルが表示されない場合、2 つのファイルは同じです。Prime Infrastructure は実行コンフィギュレーションと異なる場合にのみスタートアップ コンフィギュレーションをバックアップします。

ステップ 4 [設定タイプ（Configuration Type）] の下にあるファイルをクリックし、その raw データを表示します。[Raw コンフィギュレーション（Raw Configuration）] タブの上から下へとファイルの内容が一覧表示されます。

ステップ 5 別のファイルの内容と比較するには、[比較対象（Compare With）] 列の下にある任意のハイパーリンクをクリックします。選択肢は、アーカイブにバックアップされたデバイスのタイプと設定ファイルの数によって異なります。カラー コードは、更新、削除、または追加されたものを示します。

タグを使用した重要なコンフィギュレーションファイルのラベル付け

コンフィギュレーション ファイルにタグを割り当てることは、重要な設定を識別し、必要な情報を伝えるためのわかりやすい方法です。タグは、[設定アーカイブ（Configuration Archive）] ページでファイルの一覧とともに表示されます。また、次の手順を使用して、タグを編集および削除することもできます。

ステップ 1 [インベントリ（Inventory）] > [デバイス管理（Device Management）] > [設定アーカイブ（Configuration Archive）] の順に選択します。

ステップ 2 [アーカイブ（Archives）] タブで、ラベル付けするコンフィギュレーション ファイルを見つけて [タグの編集（Edit Tags）] をクリックします。

ステップ 3 [タグの編集（Edit Tag）] ダイアログボックスに内容を入力するか、既存のタグを編集または削除して、[保存（**Save**）] をクリックします。

実行デバイスコンフィギュレーションとスタートアップ デバイス コンフィギュレーションの同期

スタートアップ コンフィギュレーション ファイルと実行コンフィギュレーション ファイルを持つデバイスは、同期が取れていない（非同期）場合があります。スタートアップ ファイル（デバイスの再起動時に読み込まれる）が実行コンフィギュレーションと異なる場合、デバイスは同期が取れていないと判断されます。変更された実行コンフィギュレーションはスタートアップ コンフィギュレーションとしても保存しない限り、デバイスを再起動すると、実行コンフィギュレーションの変更が失われます。上書き操作は、現在の実行コンフィギュレーションでデバイスのスタートアップ コンフィギュレーションを上書きして、ファイルを同期します。

（注） このデバイス コンフィギュレーション ファイルの同期操作は、デバイスの即時インベントリ収集を実行する同期操作とは異なります。

ステップ 1 同期が取れていないデバイスの特定。

a) [インベントリ（Inventory）] > [デバイス管理（Device Management）] > [設定アーカイブ（Configuration Archive）] の順に選択します。

b) **[デバイス]** タブで、フィールド [起動/実行の構成比較ステータス（Startup/Running Configuration comparision status）] フィールドを確認します。

c) いずれかのデバイスのリストに **[Yes]** と表示されている場合は、それらのデバイスをメモします。

ステップ 2 デバイスを同期するには。

a) **[デバイス（Devices）]** タブで同期されていないデバイスを選択し、**[アーカイブ上書きのスケジュール（Schedule Archive Overwrite）]** をクリックします（上書き操作の詳細については、実行コンフィギュレーションによるスタートアップ コンフィギュレーションの上書き （109 ページ）を参照してください）。

ステップ 3 ジョブの詳細を確認するには、**[管理（Administration）] > [ジョブダッシュボード（Job Dashboard）] > [ユーザジョブ（User Jobs）] > [設定アーカイブ上書き（Configuration Archive Overwrite）]** の順に選択して、上書きジョブの詳細を表示します。

特定のデバイスの上書きジョブが完了すると、[スタートアップ/実行コンフィギュレーション比較ステータス（Startup/Running Configuration comparison status）] フィールドに、[設定変更なし（No configuration changed）] と表示されます。

デバイスのコンフィギュレーションファイルの比較または削除

比較機能は、2つのコンフィギュレーションファイルを並べて表示し、追加、削除、および除外された値を異なる色で示します。この機能を使用して、同期されていないデバイスの起動時と実行時のコンフィギュレーションファイル間の違いを表示するか、または同様なデバイスの設定が異なっているかどうかを検出します。これで、設定アーカイブをデータベースから削除できるようになります。

Prime Infrastructure は、NTP クロック レート（管理対象のネットワーク要素上で絶えず変化していても、設定変更とは見なされない）のような、小型のコマンドセットをデフォルトで除外します。設定ファイルの変更を確認する場合に除外する項目の指定 （98 ページ）で説明するように、除外されたコマンドのリストは変更できます。

ステップ 1 [インベントリ（Inventory）] > [デバイス管理（Device Management）] > [設定アーカイブ（Configuration Archive）] の順に選択します。

ステップ 2 デバイスの設定アーカイブを削除するには、[デバイス] タブで設定を削除するデバイスを見つけ、[X]（削除）ボタンをクリックします。

ステップ 3 デバイスの設定アーカイブを比較するには、次の操作を実行します。

a) [デバイス（Devices）] タブで、比較する設定を持つデバイスを見つけ、そのデバイス名のハイパーリンクをクリックします。

b) タイム スタンプを展開して、その時点でアーカイブされたファイルを表示します。

c) [比較対象（Compare With）] 列の下にあるハイパーリンクのいずれかをクリックして比較ウィンドウを起動します。選択肢は、アーカイブにバックアップされたデバイスのタイプと設定ファイルの数によって異なります。カラー コードは、更新、削除、または追加されたものを示します。

[設定の比較（Configuration Comparison）] ウィンドウでは、raw ファイルに注目するか、またはファイルの特定の部分（configlet）に注目することで、設定を調べることができます。下部のウィンドウの色分けを使用して、何が更新、削除、または追加されたかを確認します。

デバイスへの外部コンフィギュレーションファイルの展開

展開のスケジュール操作は、外部ファイルを使用してデバイスの設定を更新します。ロールバックと定期展開の違いは、ロールバックではアーカイブから既存のファイルを使用するのに対して、定期展開では外部ファイルを使用することです。

デバイスのタイプによっては、展開ジョブに次の設定を指定できます。

- 現在のスタートアップ コンフィギュレーションを新しいバージョンで書き換え、必要に応じて展開後にデバイスを再起動します。
- 新しいファイルと現在実行中の設定をマージし、必要に応じてファイルを新しいスタートアップ コンフィギュレーションとしてアーカイブします。

ローカル マシンにファイルを作成する場所があることを確認します。

ステップ 1 デバイスの [デバイスの詳細（Device Details）] ページを開き、そのページから展開操作を実行します。

a) [インベントリ（Inventory）]>[デバイス管理（Device Management）]>[ネットワーク デバイス（Network Devices）] を選択します。

b) デバイス名のハイパーリンクをクリックし、[デバイスの詳細（Device Details）] ページを開きます。

ステップ 2 [設定アーカイブ（Configuration Archive）] タブをクリックしてデバイスの [設定アーカイブ（Configuration Archive）] ページを開きます。

ステップ 3 **[アーカイブ展開のスケジュール設定（Schedule Archive Deploy）]** をクリックして、展開ジョブ ダイアログ ボックスを開きます。

ステップ 4 [参照（Browse）] をクリックし、ファイルの場所まで移動してファイルを選択し、展開するファイルを選択します。

ステップ 5 展開するファイルのタイプに応じて、次のようにジョブ パラメータを設定します。

- [スタートアップ コンフィギュレーション（Startup configuration）] : [スタートアップ コンフィギュレーションの上書き（Overwrite Startup Configuration）] を選択します。展開操作の後にデバイスを再起動する場合は、[再起動（Reboot）] チェックボックスをオンにします。
- 実行コンフィギュレーション：[**Merge with Running Configuration**] を選択します。また、スタートアップ コンフィギュレーションとしてデバイスにファイルを保存するには、[**Save to Startup**] チェック ボックスをオンにします。

ステップ 6 展開ジョブをすぐに実行するか、後で実行するようにスケジュールを設定し、[送信（Submit）] をクリックします。

ステップ 7 **[管理（Administration）]>[ジョブダッシュボード（Job Dashboard）]>[ユーザジョブ（User Jobs）]>[設定アーカイブ展開（Configuration Archive Deploy）]** の順に選択して、スケジュール展開ジョブの詳細を表示します。

実行コンフィギュレーションによるスタートアップコンフィギュレーションの上書き

上書き操作により、デバイスの実行コンフィギュレーションがデバイスのスタートアップ コンフィギュレーションにコピーされます。実行コンフィギュレーションに変更を加えた後、デバイスのスタートアップ コンフィギュレーションを上書きしなければ、デバイスを再起動するとその変更内容が失われます。

ステップ 1 **[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ネットワーク デバイス（Network Devices）]** の順に選択します。

ステップ 2 デバイス名のハイパーリンクをクリックして [デバイスの詳細（Order Details）] ページを開き、[設定アーカイブ（Configuration Archive）] タブをクリックします。

ステップ 3 [上書きのスケジュール（Schedule Overwrite）] [アーカイブ上書きのスケジュール（Schedule Archive Overwrite）]をクリックし、ジョブを即時に実行するか、後で実行するかを設定してから、[送信（Submit）] をクリックします。

ステップ 4 **[管理（Administration）] > [ジョブダッシュボード（Job Dashboard）] > [ユーザジョブ（User Jobs）] > [設定アーカイブ上書き（Configuration Archive Overwrite）]** を選択して、上書きジョブの詳細を表示します。

アーカイブされたバージョンへのデバイス設定のロールバック

ロールバック操作により、アーカイブのファイルがデバイスにコピーされ、新しいファイルが現在の設定になります。実行コンフィギュレーション、スタートアップ コンフィギュレーション、VLAN設定をロールバックできます。デフォルトでは、この操作はファイルをマージして実行されます。実行コンフィギュレーションをロールバックする場合、ファイルをマージするのではなく、上書きするオプションを選択できます。コンフィギュレーションファイルを前のバージョンにロールバックするには、次の手順に従います。

ステップ 1 **Inventory** > **Device Management** > **Configuration Archive** を選択します。

ステップ 2 **[Archives]** タブをクリックし、コンフィギュレーション ファイルをロールバックするデバイスを選択してから **[アーカイブ ロールバックのスケジュール（Schedule Archive Rollback）]** をクリックします。

ステップ 3 ロールバックするファイルのタイプを選択します。[設定ロールバックのスケジュール（Schedule Configuration Rollback）] ダイアログボックスで次の操作を行います。

a) [ロールバックのオプション（Rollback Options）] 領域を展開します。

b) **[Files to Rollback]** ドロップダウンリストからファイル タイプを選択します。**[All]** を選択すると、この操作がスタートアップ コンフィギュレーション ファイル、実行コンフィギュレーション ファイル、および VLAN コンフィギュレーション ファイルに適用されます。

（注） Cisco IOS XR 64 ビットデバイスでは、**[管理設定（Admin Configuration）]** を選択した場合は、**[デバイスの VM 管理者パスワード（Device VM Admin Password）]** を入力します。

ステップ 4 ロールバック先の特定のコンフィギュレーション ファイルのバージョンをクリックします。

ステップ 5 **[アーカイブのロールバックのスケジュール設定（Schedule Archive Rollback）]** をクリックし、次を実行します。

表 *14* : デバイス設定のロールバック

領域	オプション	説明
ロールバック（Rollback）	[ロールバックするファイル（Files to rollback）]	[データベース設定（Database Configuration）]、[実行コンフィギュレーション（Running Configuration）]、[管理者設定（Admin Configuration）] のいずれかを選択します。
	[再起動（Reboot）]	（起動のみ）起動コンフィギュレーションをロールバックした後、デバイスを再起動すると、起動コンフィギュレーションが実行コンフィギュレーションになります。
	[スタートアップに保存（Save to startup）]	（実行のみ）実行コンフィギュレーションをロールバックした後、その実行コンフィギュレーションを起動コンフィギュレーションに保存します。
	[ロールバック前のアーカイブ（Archive before rollback）]	ロールバック操作を開始する前に、選択されたファイルをバックアップします。
	設定の上書き	古い実行コンフィギュレーションを（マージするのではなく）新しい実行コンフィギュレーションで上書きします。
	[アーカイブの失敗時ロールバックを続行（Continue rollback on archive failure）]	（[ロールバック前のアーカイブ（Archive before rollback）] が選択されている場合）選択されたファイルが正常にデータベースに保存されなくてもロールバックを続行します。
スケジュール	（Web GUI を参照）	ロールバックを即時に実行するか、後でスケジュールした時間に実行するかを指定します。

ステップ 6 **Submit** をクリックします。

ステップ 7 [管理（Administration）] > [ジョブダッシュボード（Job Dashboard）] > [ユーザジョブ（User Jobs）] > [設定アーカイブロールバック（Configuration Archive Rollback）] を選択して、ロールバック ジョブの詳細を表示します。

（注） プライムインフラストラクチャは、AireOSデバイスでロールバック操作を実行している間に、デバイスをリセットすることがあります。これにより、ネットワークが中断されます。

コンフィギュレーション ファイルのダウンロード

同時に最大 1000 台までのデバイスの起動および実行コンフィギュレーション ファイルをローカル システムにダウンロードできます。

ステップ 1 [インベントリ（Inventory）] > [デバイス管理（Device Management）] > [設定アーカイブ（Configuration Archive）] の順に選択します。

ステップ 2 [最新の設定をエクスポート（Export Latest Config）] ドロップダウンリストから次のいずれかのオプションを選択して、コンフィギュレーション ファイルをダウンロードします。

1. [サニタイズ（Sanitized）] : デバイスのクレデンシャル パスワードがダウンロードしたファイル内でマスクされます。
2. [非サニタイズ（Unsanitized）] : デバイスのクレデンシャル パスワードがダウンロード ファイル内に表示されます。

このオプションは、サポートされているすべての設定を csv ファイルとしてデバイスからダウンロードします。デバイスからスタートアップ コンフィギュレーションまたは実行コンフィギュレーションのみを指定してダウンロードするには、次の代替ステップを使用します。

[非サニタイズ（Unsanitized）] オプションは、ロールベース アクセス コントロール（RBAC）で設定されているユーザ権限に基づいて表示されます。

また、次の手順を実行しても、設定をダウンロードすることができます。

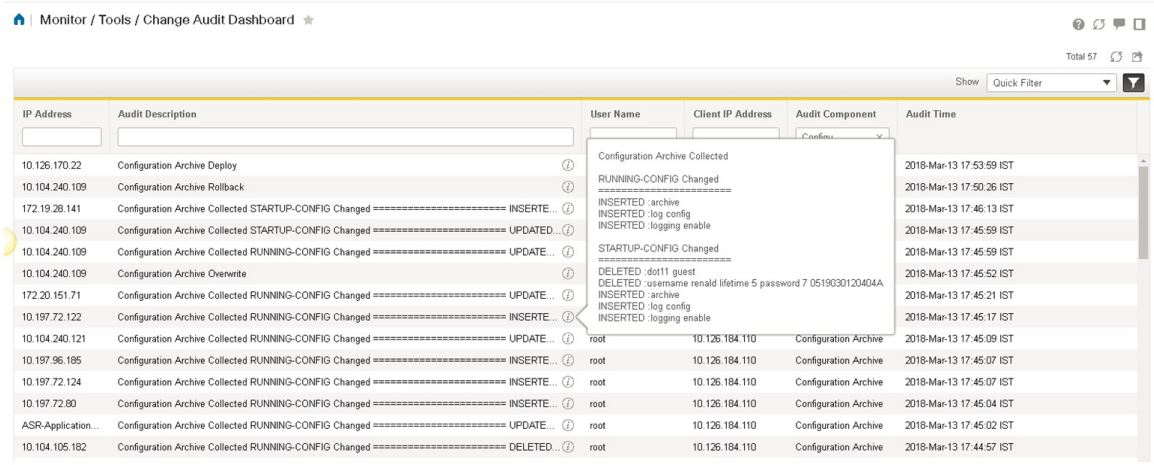
- [インベントリ（Inventory）] > [デバイス管理（Device Management）] > [設定アーカイブ（Configuration Archive）] ページで、設定ファイルをダウンロードするデバイスをクリックするか、または [インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ネットワーク デバイス（Network Devices）] ページで設定ファイルをダウンロードするデバイスをクリックし、[設定アーカイブ（Configuration Archive）] タブをクリックします。
- [展開（Expand）] アイコンを使用して、必要な設定の詳細をアーカイブから表示します。
- [詳細（Details）] をクリックします。
- [エクスポート（Export）] ドロップダウンリストから [サニタイズ（Sanitized）] または [非サニタイズ（Unsanitized）] を選択します。

メモ　このコンフィギュレーション ファイルを WLC にアップロードする前に、各行の先頭にキーワード **config** を追加する必要があります。

設定アーカイブ操作に関する変更監査の確認

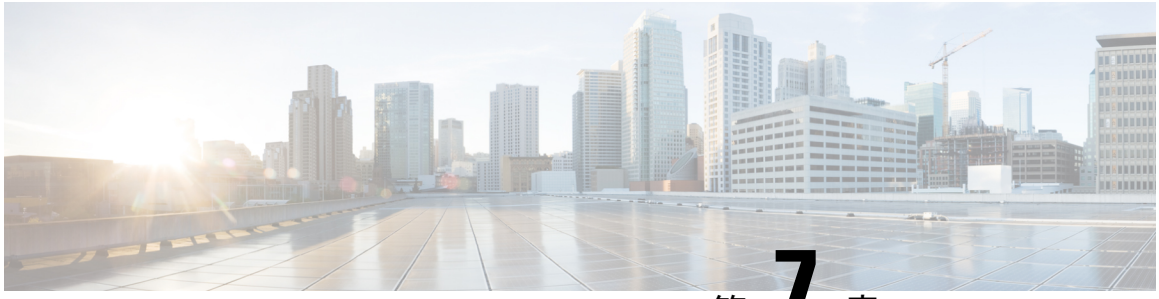
デバイスのソフトウェアイメージの変更に関する履歴情報を取得するには、変更監査ダッシュボードを確認します。

ステップ 1　**[モニタ（Monitor）] > [ツール（Tools）] > [変更監査ダッシュボード（Change Audit Dashboard）]** の順に選択します。イメージ管理の操作だけが表示されるように結果をフィルタリングするには、[監査コンポーネント（Audit Component）] フィールドに **archive** と入力します。



ステップ 2　イベント ドロワーを展開して、デバイスの変更に関する詳細情報を表示します。たとえば、ステップ 1 の上図で強調表示されているドロワーを展開すると、その時点でデバイスの実行コンフィギュレーション ファイルが正常にアーカイブにバックアップされていることがわかります。

Archive configuration	**Success**
Fetch DATABASE configuration	Unsupported operation
Fetch VLAN configuration	Unsupported operation
Fetch running configuration	Success
Fetch startup configuration	Success
Syslog Message	<189>308716: *Jan 27 01:25:41.622: %SYS-5-CONFIG_I: Configured from console by vty0 (10.127.101.52)



第 7 章

デバイス ソフトウェア イメージの管理

- ソフトウェア イメージ管理のセットアップ （113 ページ）
- デバイスからイメージ リポジトリへのソフトウェア イメージのコピー（ベースラインの作成） （128 ページ）
- ネットワーク デバイスでどのイメージが使用されているかを調べる方法 （129 ページ）
- デバイスに最新のイメージがあることを確認する方法 （129 ページ）
- Cisco.com からソフトウェアをダウンロードする権限があるかどうかを調べる方法 （130 ページ）
- イメージ リポジトリに保存されたイメージを表示する （130 ページ）
- イメージを使用しているデバイスの確認 （131 ページ）
- Cisco.com で推奨されるイメージの表示 （132 ページ）
- Cisco.com からのイメージのダウンロード （133 ページ）
- ソフトウェア イメージをリポジトリに追加（インポート）する （134 ページ）
- 仮想イメージ リポジトリへのソフトウェア イメージのインポート （138 ページ）
- ソフトウェア イメージをアップグレードするためのデバイス要件の変更 （139 ページ）
- デバイスがイメージ要件を満たしていることの確認（アップグレード分析） （139ページ）
- デバイスへの新しいソフトウェア イメージの配布 （140 ページ）
- デバイスで新しいソフトウェア イメージをアクティブにする （143 ページ）
- ワイヤレス/DC デバイスへのソフトウェア イメージの展開 （145 ページ）
- スタック デバイスのサポートされているイメージ形式 （146 ページ）
- デバイスのリロード間での Cisco ISO XR イメージのコミット （147 ページ）
- ソフトウェア イメージ操作に関する変更監査の確認 （148 ページ）
- ASD の例外とエラー条件 （149 ページ）
- ローリング AP アップグレードの使用によるコントローラ ソフトウェアのアップグレード （151 ページ）

ソフトウェア イメージ管理のセットアップ

デバイスを最新ソフトウェア バージョンに手動でアップグレードするとエラーが発生することがあり、時間もかかります。Cisco Prime Infrastructure は、ソフトウェア イメージの更新の計画、スケジュール設定、ダウンロード、およびモニタリングを支援することで、デバイスに対

するソフトウェア更新のバージョン管理とルーチン展開を簡素化します。また、ソフトウェアイメージの詳細の表示、推奨されるソフトウェアイメージの表示、およびソフトウェアイメージの削除を行うこともできます。ソフトウェア イメージの管理ページでは、ソフトウェア イメージ管理ライフサイクル ウィジェット、ソフトウェア イメージ概要、ジョブ詳細など、ソフトウェア イメージ管理をさまざまな面から確認できます。

Prime Infrastructure は、ネットワーク上にあるデバイスのすべてのソフトウェア イメージを保存します。イメージは、イメージのタイプとバージョンに従って保存されます。

ソフトウェア イメージをアップグレードする前に、Telnet または SSH のクレデンシャルでデバイスを設定する必要があります。また、デバイスが Prime Infrastructure に追加された際に入力されたコミュニティ ストリングと一致する、SNMP 読み取り/書き込みコミュニティ ストリングが設定されている必要があります。

SSH または Telnet は、デバイスからイメージをインポートできるように設定する必要があります。

- デバイスが正しく構成されていることを確認する （114 ページ）
- Prime Infrastructure サーバでの FTP/TFTP/SFTP/SCP 設定の確認 （115 ページ）
- インベントリ収集中にイメージ リポジトリに保存されたイメージの制御方法 （115 ページ）
- Cisco.com のイメージ推奨事項に応じた基準の調整 （124 ページ）
- イメージの転送および配布設定の調整 （125 ページ）
- ソフトウェア イメージ操作に関する Cisco.com クレデンシャルの変更 （128 ページ）

デバイスが正しく構成されていることを確認する

Prime Infrastructure場合、SNMP 読み取り/書き込みコミュニティをあなたのデバイスで構成されている文字列に一致にデバイスが追加されたときに指定された文字列にのみデバイスからファイルを転送できます Prime Infrastructure 。

（注） セキュリティを強化するために、Prime Infrastructure では、旧バージョンの Cisco IOS-XE と IOS-XR で使用される SSH CBC（暗号ブロック連鎖）暗号方式の一部を使用しなくなりました。それらは脆弱であると見なされたためです。Cisco IOS-XE を実行するデバイスの場合は、16.5.x 以降のバージョンにアップグレードしていることを確認します。Cisco IOS-XR を実行するデバイスの場合は、6.1.2 以降のバージョンにアップグレードします。それ以外の場合は、ソフトウェア イメージ管理の複数の操作が失敗します。

（注） Cisco Nexus 7000 シリーズ スイッチの NAT 環境および子の仮想デバイス コンテキスト（VDC）では SWIM 操作はサポートされていません。

Prime Infrastructure サーバでの FTP/TFTP/SFTP/SCP 設定の確認

FTP、TFTP、SFTP、または SCP を使用する場合は、それが有効で適切に設定されていることを確認してください。

インベントリ収集中にイメージリポジトリに保存されたイメージの制御方法

ソフトウェアイメージの収集はデータ収集プロセスを遅くする可能性があるため、デフォルトでは、Prime Infrastructure は、インベントリ収集の実行時には、イメージ リポジトリでのデバイス ソフトウェア イメージの収集および保存を実行しません。次に説明する手順を使用して設定を変更できるのは、管理権限を持つユーザです。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** を選択し、次に **[インベントリ（Inventory）] > [ソフトウェアイメージ管理（Software Image Management）]** を選択します。

ステップ 2 Prime Infrastructure によるインベントリ収集の実行時にデバイス イメージを取得してイメージ リポジトリに保存するには、[インベントリ収集と同時にイメージを収集（Collect images along with inventory collection）] チェック ボックスをオンにします。

ステップ 3 [保存（Save）] をクリックします。

ステップ 4 取得されたイメージを表示するには、**[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ソフトウェアイメージ（Software Images）]** を選択し、[便利なリンク（Useful Links）] セクションの [ソフトウェアイメージリポジトリ（Software Image Repository）] の隣にある [リンク（Link）] をクリックします。

（注） [ソフトウェアイメージ（Software Image）] ページの右上隅にある [イメージダッシュボード（Image Dashboard）] アイコンをクリックして、[ネットワークデバイス（Network Devices）] ページから上位 10 の実行中のソフトウェア イメージを表示します。

データ クリーンアップ ジョブが実行されている場合、[イメージダッシュボード（Image Dashboard）] ページに直近 10 回の SWIM ジョブは表示されません。ユーザ ジョブの保持日数は、デフォルトでは 7 日です。

ソフトウェアイメージの管理プロセスとサポートされているデバイス

次の表では、ソフトウェアイメージの管理に関与するさまざまなプロセスと、そのプロセスがユニファイド ワイヤレス LAN コントローラおよびデバイスでサポートされているかどうかについて説明します。

（注） イメージのインポート中にサポートされているプロトコル、ローカル ファイル サーバを介したイメージの配布、ソフトウェア イメージの管理サーバ、TFTP フォールバックのサポート、配布なしのISSUおよび有効化などのプラットフォームに関する追加情報については、「Supported Device List」を参照してください。

表 *15* : ソフトウェア イメージの管理プロセスとサポートされているデバイス

ソフトウェア イメージの管理プロセス	説明	Unified WLC	3850 Cisco IOS XE 3.2.2	5760 Cisco IOS XE 3.2.2	Mobility Express コントローラ
デバイスからのイメージのインポート	すでに Prime Infrastructure によって管理されているデバイスからソフトウェア イメージをインポートする機能。ソフトウェア イメージはその後、他のデバイスに配布できます。	ソフトウェア イメージはパッケージに再構築することができないため、サポートされていません。	サポートあり （注） デバイスがインストール モードで動作している場合、実行イメージは「packages.conf」となります。Prime Infrastructure では、インストール モードでこの形式のイメージをインポートすることはサポートしていません。	サポートあり （注） デバイスがインストール モードで動作している場合、実行イメージは「packages.conf」となります。Prime Infrastructure は、インストール モードでのこの形式のイメージのインポートはサポートしていません。	未サポート
ファイルからのイメージのインポート	ファイル サーバの既知の場所から Prime Infrastructure にソフトウェア イメージをインポートする機能。ソフトウェア イメージはその後、他のデバイスに配布できます。	サポート対象	サポート対象	サポート対象	サポート対象

ソフトウェア イメージの管理プロセス	説明	Unified WLC	3850 Cisco IOS XE 3.2.2	5760 Cisco IOS XE 3.2.2	Mobility Express コントローラ
URL からのイメージのインポート	ネットワーク上のアクセス可能な場所（URI/URL）から Prime Infrastructure にソフトウェア イメージをインポートする機能。ソフトウェア イメージはその後、他のデバイスに配布できます。	サポート対象	サポート対象	サポート対象	サポート対象
プロトコルを使用したイメージのインポート	FTP のロケーションから Prime Infrastructure にソフトウェア イメージをインポートする機能。ソフトウェア イメージはその後、他のデバイスに配布できます。	サポート対象	サポート対象	サポート対象	サポート対象

ソフトウェア イメージの管理プロセス	説明	Unified WLC	3850 Cisco IOS XE 3.2.2	5760 Cisco IOS XE 3.2.2	Mobility Express コントローラ
イメージのアップグレード/配布	から管理対象デバイスのソフトウェア イメージをアップグレードする機能。この機能を使用すると、オンデマンドまたは後でスケジュールされている時点で、複数デバイスのPrime Infrastructureソフトウェア イメージをアップグレードできます。フィードバックとステータスがアップグレード時に表示され、必要に応じてデバイスを再起動できます。大規模な展開では、あるサイトのサービスがアップグレード期間に完全にダウンしないように、リブートをずらすことができます。	サポート対象	サポート対象	サポート対象	

ソフトウェア イメージの管理プロセス	説明	Unified WLC	3850 Cisco IOS XE 3.2.2	5760 Cisco IOS XE 3.2.2	Mobility Express コントローラ
					配布とアクティブ化のサポート （注） • 28 イメージバージョンを実行しているデバイスで配布とアクティブ化に失敗しました。 • EM デ

ソフトウェア イメージの管理プロセス	説明	Unified WLC	3850 Cisco IOS XE 3.2.2	5760 Cisco IOS XE 3.2.2	Mobility Express コントローラ
					バイスがxS イメージバージョンで実行されるときHS プロトコルを使用した配布がサポートされます。

ソフトウェア イメージの管理プロセス	説明	Unified WLC	3850 Cisco IOS XE 3.2.2	5760 Cisco IOS XE 3.2.2	Mobility Express コントローラ
					• EM デバイスが x.8 イメージ バージョンで実行されるとき HS プロトコルを使用した外部サバのみへの

ソフトウェア イメージの管理プロセス	説明	Unified WLC	3850 Cisco IOS XE 3.2.2	5760 Cisco IOS XE 3.2.2	Mobility Express コントローラ
					配布がサポートされます

ソフトウェア イメージの管理プロセス	説明	Unified WLC	3850 Cisco IOS XE 3.2.2	5760 Cisco IOS XE 3.2.2	Mobility Express コントローラ
					• HTTP プロトコルを使用した外部サーバへの配布はサポートされていません。
イメージの推奨	Prime Infrastructure から管理され、Cisco.com からダウンロードされるデバイスに対し互換性のあるイメージを推奨する機能。	フラッシュ要件が使用できないため、サポートされません。	サポート対象	サポート対象	サポート対象

ソフトウェア イメージの管理プロセス	説明	Unified WLC	3850 Cisco IOS XE 3.2.2	5760 Cisco IOS XE 3.2.2	Mobility Express コントローラ
イメージのアップグレード分析	ソフトウェア アップグレードを実行する前にハードウェアのアップグレードが必要かどうかを判断するためにソフトウェア イメージを分析する機能。	RAM または ROM には最小要件がないため、サポートされません。新しくアップグレードされたイメージは、アップグレード後に既存のイメージに置き換わります。	サポート対象	サポート対象	未サポート

（注） Prime Infrastructure は、冗長スーパーバイザ エンジンで設定された Cisco Catalyst 4500 デバイスでのソフトウェア イメージの配布をサポートしていません。

Prime Infrastructure は、デュアル スーパーバイザを搭載した Cisco Catalyst 6000 および Cisco Catalyst 9400 デバイスでのソフトウェア イメージの配布をサポートしています。Prime Infrastructure は、アクティブとスタンバイの両方のスーパーバイザ エンジンでソフトウェア イメージを配布します。

（注） 現在、Prime Infrastructure では、eWLC デバイスの動作モードをインストールするためのインストールのみがサポートされています。バンドル モードでデバイスを管理できます。ただし、このモードでは、SWIM 操作を実行できません。

Cisco.com のイメージ推奨事項に応じた基準の調整

Cisco.com を使用して、指定した条件に基づいて推奨されるイメージに関する情報を取得できます。次に、これらの推奨事項を調整する手順を示します。また、次の表にデフォルトの設定も示します。

（注） これらの機能を使用するには、デバイスがイメージの推奨事項をサポートしている必要があります。

（注） 現在、Prime Infrastructure で推奨されているのは、Cisco.com で提供されるイメージ バージョンの最新リンクのみです。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** の順に選択し、次に **[インベントリ（Inventory）] > [ソフトウェアイメージ管理（Software Image management）]** を選択します。

ステップ 2 次のように、推奨設定を調整します。

設定	説明	デフォルト
[各メジャーリリースの最新の推奨メンテナンス バージョン（Recommend latest maintenance version of each major release）]	各メジャーリリースの最新のメンテナンス バージョンのイメージのみを考慮します。	無効
[推奨される同じイメージ機能（Recommend same image feature）]	デバイス イメージの実行と同じ機能セットを備えたイメージのみを考慮します。	無効
[現在のバージョンより高い推奨バージョン（Recommend versions higher than the current version）]	実行中のデバイス イメージより高いバージョンのイメージのみを考慮します。	無効
[推奨事項の CCO を含める（Include CCO for recommendation）]	Cisco.com およびイメージ リポジトリからイメージを取得します。	[有効（Enabled）]

ステップ 3 **[保存（Save）]** をクリックします。

イメージの転送および配布設定の調整

Prime Infrastructure がイメージをソフトウェア イメージ管理サーバからデバイスに転送する際にデフォルトで使用するプロトコルを指定するには、この手順を使用します。また、Prime Infrastructure がイメージの転送と配布に関連するさまざまなタスクをデフォルトで実行するように設定することもできます。たとえば、アップグレードの前に現在のイメージをバックアップする、アップグレード後にデバイスを再起動する、シリアルアップグレードが失敗した場合

に次のデバイスをアップグレードするなどのタスクを実行するように設定できます。次に説明する手順を使用して設定を変更できるのは、管理権限を持つユーザです。

この手順では、デフォルトのみを設定します。これらのデフォルトは、実際の配布操作を実行する際にオーバーライドできます。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** を選択し、次に **[インベントリ（Inventory）] > [ソフトウェアイメージ管理（Software Image Management）] > [プロトコル（Protocol）]** を選択します。

ステップ 2 [イメージ転送プロトコルの順序（Image Transfer Protocol Order）] で、Prime Infrastructure がイメージを転送する際にデフォルトで使用するプロトコルを指定します。優先順位でプロトコルを並べ替えます。最初にリストされているプロトコルが失敗した場合、Prime Infrastructure は次にリストされているプロトコルを使用します。

（注） デバイスへのイメージの配布には、デバイスでサポートされている最もセキュアなプロトコル（TFTP ではなく SCP など）を使用します。非常に大きなファイルを転送する場合、またはサーバとクライアントが地理的に離れている場合には、TFTP はタイムアウトになる傾向があります。イメージの配布に SCP を選択する場合は、デバイスがフルユーザ権限（特権 EXEC モード）を使用して Prime Infrastructure で管理されていることを確認してください。フル ユーザ権限を使用しないと、配布はコピー権限エラー（「SCP：プロトコル エラー：権限拒否（SCP: protocol error: Privilege denied）」）が原因で失敗します。

ステップ 3 [イメージ設定プロトコルの順序（Image Config Protocol Order）] 領域で、Prime Infrastructure がイメージをデバイスに設定する際にデフォルトで使用するプロトコルを指定します。優先順位でプロトコルを並べ替えます。

ステップ 4 Prime Infrastructure がイメージを配布する際に実行するタスクを指定します。

設定	説明	デフォルト
失敗した場合に配信を続けます（Continue distribution on failure）	複数のデバイスにイメージを配布する場合、あるデバイスへの配布が失敗しても、他のデバイスへの配布を続行します。	[有効（Enabled）]
TFTP フォールバック（TFTP fallback）	実行中のイメージを TFTP サーバに保存します。保存されたイメージは、配布/アクティブ化が失敗したときの再起動に使用されます。	無効
実行中のイメージのバックアップ（Backup running image）	イメージを配布する前に、実行中のイメージをソフトウェアイメージ リポジトリにバックアップします。	無効
起動コマンドを挿入する（Insert boot command）	イメージを配布した後、起動コマンドを実行中のイメージに挿入します。	無効

設定	説明	デフォルト
[配布前にスマート フラッシュ削除（Smart Flash Delete Before Distribution）]	配布の前に、フラッシュから不要なファイルを削除してメモリ スペースを解放します。	無効

ステップ 5 **[保存（Save）]** をクリックします。

デバイス グループを管理するソフトウェア イメージ管理サーバの追加

イメージをデバイスのグループに配布するには、ソフトウェアイメージ管理サーバを追加し、イメージ配布に使用するプロトコルを指定します。最大 3 つのサーバを追加できます。Prime Infrastructure は、外部サーバとして Linux サーバのみをサポートします。

開始する前に、**[インベントリ（Inventory）]** > **[グループ管理（Group Management）]** > **[ネットワークデバイスグループ（Network Device Groups）]** > **[ロケーショングループの作成（Create location group）]** で、ロケーション グループを作成する必要があります。この作成したロケーション グループは、**[管理（Administration）]** > **[サーバ（Servers）]** > **[ソフトウェアイメージ管理サーバ（Software Image Management Servers）]** の [対象サイト（Sites Served）] フィールドで選択できます。

ステップ 1 サーバを追加します。

a) **[管理（Administration）]** > **[サーバ（Servers）]** > **[ソフトウェアイメージ管理サーバ（Software Image Management Servers）]** の順に選択します。

b) [行の追加（Add Row）] アイコンをクリックし、サーバがサポートするサーバ名、IP アドレス、およびデバイス グループを入力します。

c) [保存（Save）] をクリックします。

ステップ 2 サーバ プロトコル設定を構成します。

a) サーバ名の横にあるチェックボックスをオンにし、[プロトコルの管理（Manage Protocols）] をクリックします。

b) [行の追加（Add Row）] アイコンをクリックし、ソフトウェア イメージ管理プロトコルの詳細（ユーザ名、パスワードなど）を入力します。

c) [保存（Save）] をクリックします。

（注） イメージ管理サーバを使用してイメージを配布する場合、イメージはサーバにコピーされ、ジョブが完了すると削除されます。このイメージ ファイルは、TFTP プロトコルの場合は削除されません。

プロトコル パスワードに特殊文字を使用している場合、ソフトウェア イメージの配布およびイメージのインポートが認証の問題で失敗する可能性があります。

ソフトウェア イメージ操作に関する Cisco.com クレデンシャルの変更

Prime Infrastructure が Cisco.com に接続してソフトウェア イメージの管理操作を実行する場合（たとえば、イメージ推奨事項の確認など）、[アカウント設定（Account Settings）] ページに保存されているクレデンシャルを使用します。これらの設定は、次の手順を使用して変更できます。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** を選択し、**[一般（General）] > [アカウント設定（Account Settings）]** を選択します。

ステップ 2 [Cisco.com クレデンシャル（Cisco.com Credentials）] タブをクリックします。

ステップ 3 設定を変更してから [保存（Save）] をクリックします。

デバイスからイメージ リポジトリへのソフトウェア イメージのコピー（ベースラインの作成）

システムの設定によっては、Prime Infrastructure がインベントリ収集時にデバイスのソフトウェア イメージをイメージ リポジトリにコピーすることがあります（インベントリ収集中にイメージ リポジトリに保存されたイメージの制御方法（115 ページ）を参照）。この操作を手動で実行する必要がある場合は、ソフトウェア イメージをデバイスからイメージ リポジトリへ次直接インポートする次の手順を実行します。

開始する前に、イメージが（リモートにロードされているのではなく）デバイス上に物理的に存在することを確認します。

（注） 多数のイメージをインポートする場合は、生産に影響を与える可能性が最も低い時間にこの操作を実行します。

プロトコル パスワードで特殊文字を使用すると、認証エラーによりソフトウェア イメージ インポートが失敗する場合があります。

ステップ 1 **[インベントリ（Inventory）]>[デバイス管理（Device Management）]>[ソフトウェア イメージ（Software Images）]** の順に選択します。

ステップ 2 [追加/インポート（Add/Import）] アイコンをクリックします。

ステップ 3 [イメージのインポート（Import Images）] ダイアログボックスで、次の情報を入力します。

a) [デバイス（Device）] を選択します。

b) [デバイスの選択（Device Selection）] タブをクリックします。

c) [デバイスの選択方法（Select devices by）] トグル ボタンをクリックして、[グループ（Group）] または [デバイス（Device）] オプションからデバイスを選択できます。

d) [グループ（Group）] オプションを選択した場合は、デバイス グループを選択し、[デバイスの選択（Choose Devices）] ペインに一覧表示されるデバイスを選択します。選択したデバイスは、[選択されたデバイス（Selected Devices）] ペインに表示されます。

e) [スケジュール（Schedule）]エリアで、ジョブを即時実行するか、後で実行するか、または定期的に実行するかをスケジュールします。

ステップ 4 [Submit] をクリックします。`

ネットワークデバイスでどのイメージが使用されているかを調べる方法

ネットワークデバイスで使用されるイメージのリストを表示するには、**[レポート（Reports）]>[レポート起動パッド（Reports Launch Pad）]>[デバイス（Device）]>[ソフトウェアの詳細情報（Detailed Software）]** を選択します。

ネットワーク デバイスで使用される上位 10 個のイメージ（およびそれらのイメージを使用しているデバイスの数）を一覧表示するには、**[インベントリ（Inventory）]>[デバイス管理（Device Management）]>[ソフトウェアイメージ（Software Images）]** を選択します。[便利なリンク（Useful Links）] の下にある [ソフトウェアイメージリポジトリ（Software Image Repository）] をクリックし、ページの右上隅にある [イメージダッシュボード（Image Dashboard）] アイコンをクリックします。

デバイスに最新のイメージがあることを確認する方法

デバイスタイプがイメージの推奨事項に対応している場合、次の手順を使用して、デバイスが Cisco.com からの最新のイメージが設定されているかどうかを確認できます。それ以外の場合は、Cisco.com の製品サポート ページを使用して、この情報を取得します。

ステップ 1 **[インベントリ（Inventory）]>[デバイス管理（Device Management）]>[ネットワーク デバイス（Network Devices）]** を選択し、デバイス名のハイパーリンクをクリックして [デバイスの詳細（Device Details）] ページを開きます。

ステップ 2 [ソフトウェアイメージ（Software Image）] タブをクリックし、[推奨されるイメージ（Recommended Images）] 領域までスクロールします。Prime Infrastructure には、デバイスに対して推奨される Cisco.com のすべてのイメージが一覧表示されます。

Cisco.comからソフトウェアをダウンロードする権限があるかどうかを調べる方法

Prime Infrastructure は、指定したデバイス タイプのソフトウェア イメージの推奨される最新の初期バージョンのみ表示します。 Cisco.com からソフトウェア イメージを直接ダウンロードできます。Cisco.com から EULA または K9 ソフトウェア イメージをダウンロードするには、EULA 契約または K9 契約を定期的に承認または更新する必要があります。

Prime Infrastructure には延期されたソフトウェア イメージは表示されません。詳細については、Cisco Prime Infrastructure 3.2 でサポートされるデバイスのリストを参照してください。

Cisco.com からソフトウェア イメージをインポート中にエラー メッセージが表示された場合は、ASD の例外とエラー条件 （149 ページ） を参照してください。

（注） .ASD の実装に基づいて、Cisco.com から提案されたイメージやその他のイメージのバージョンを取得することはできません。

イメージ リポジトリに保存されたイメージを表示する

この手順は、イメージ リポジトリに保存されたすべてのソフトウェア イメージを一覧表示する場合に使用します。イメージはイメージタイプ別に分類され、対応するソフトウェアイメージのグループ フォルダに保存されます。

ステップ 1 **[インベントリ（Inventory）]>[デバイス管理（Device Management）]>[ソフトウェアイメージ（Software Images）]** を選択します。Prime Infrastructure の [ソフトウェアイメージの概要（Software Image Summary）] パネルに、イメージ リポジトリに保存されたイメージが一覧表示されます。

[ソフトウェアイメージ管理ライフサイクル（Software Image Management Lifecyle）] ウィジェットでは、次のことを実行できます。

- ネットワークデバイス（クライアントマシン上のファイルシステム、IPv4またはIPv6サーバ（URL）、FTP サーバ、および Cisco.com）からイメージ リポジトリに新しいイメージをインポートする。ソフトウェア イメージをリポジトリに追加（インポート）する （134 ページ）を参照してください。
- デバイスがこのイメージにアップグレードするために満たす必要のある要件を調整する。ソフトウェア イメージをアップグレードするためのデバイス要件の変更 （139 ページ）を参照してください。
- アップグレード分析を実行する。デバイスがイメージ要件を満たしていることの確認（アップグレード分析） （139 ページ）を参照してください。
- 新しいソフトウェアイメージをデバイスにコピーする。デバイスへ新しいソフトウェアイメージを配布を参照してください。デバイスへの新しいソフトウェア イメージの配布 （140 ページ）を参照してください。
- イメージをアクティブにして、新しいイメージをデバイスの実行イメージにする。デバイスで新しいソフトウェア イメージをアクティブにする （143 ページ）を参照してください。
- Cisco IOS XR イメージをコミットすることにより、デバイスのリロード後もイメージを保持し、ロールバック ポイントを作成する。デバイスのリロード間での Cisco ISO XR イメージのコミット （147 ページ）を参照してください。

ステップ 2 ソフトウェア イメージ リポジトリに移動し、ソフトウェア イメージのハイパーリンクをクリックして、ファイル名、イメージ名、ファミリ、バージョン、ファイル サイズなどが一覧表示された [イメージ情報（Image Information）] ページを開きます。

グローバル設定に関して実行できることは次のとおりです。

- ページの下部にある [デバイスの詳細（Device Details）] 領域をチェックして、どのデバイスがこのイメージを使用しているかを確認します。
- デバイスがこのイメージにアップグレードするために満たす必要のある要件を調整する。（ソフトウェア イメージをアップグレードするためのデバイス要件の変更 （139 ページ） を参照）。

イメージを使用しているデバイスの確認

ステップ 1 [インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ソフトウェア イメージ（Software Images）] の順に選択します。

ステップ 2 [ソフトウェア イメージの概要（Software Image Summary）] パネルで、ナビゲーション領域のイメージ カテゴリを展開するか、または [クイック フィルタ（Quick Filter）] フィールドのいずれかにテキストの一部を入力して、対象のイメージを見つけます。たとえば、[バージョン（Version）] フィールドに **3.1** と入力すると、3.12.02S、3.13.01S などのバージョンが一覧表示されます。

ステップ 3 [カウント（Count）] ハイパーリンクをクリックして、[ソフトウェアイメージリポジトリ（Software Image Repository）] に移動します。

ステップ 4 イメージのハイパーリンクをクリックして [ソフトウェアイメージの詳細（Software Image Detail）] ページを開きます。選択されているイメージが管理対象デバイスのいずれかで実行されている場合のみ、Prime Infrastructure により、[デバイスリスト（Device List）] 領域にすべてのデバイスが一覧表示されます。

Cisco.com で推奨されるイメージの表示

デバイスが Cisco.com イメージの推奨事項をサポートしている場合は、次の手順を使用してそれらのデバイスで使用する必要があるイメージを確認できます。

ステップ 1 [インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ソフトウェア イメージ（Software Images）] の順に選択します。

ステップ 2 [便利なリンク（Useful Links）] の [ソフトウェア イメージ リポジトリ（Software Image Repository）] をクリックします。

ステップ 3 イメージの要件を配布または変更するには、イメージのハイパーリンクをクリックして、[ソフトウェアイメージの詳細（Software Image Detail）]ページに移動します（デバイスは、選択されているイメージが管理対象デバイスのいずれかで実行されている場合のみ、[デバイスリスト（Device List）] 領域に一覧表示されます）。

ステップ 4 [デバイスリスト（Device List）] ドロップダウン リストからイメージを配布するデバイスを選択し、[新規バージョンの配布（Distribute New Version）] をクリックします。

ステップ 5 次のいずれかのイメージ ソースを選択します。

- **Recommend Image from Cisco.com** Cisco.com で使用可能なイメージを選択する場合。シスコ クレデンシャルでログインする必要があります。CEC ユーザ名とパスワードを入力し、EULA および K9 を選択して [**Login**] をクリックします。オプションを指定して [**Start Recommendation**] をクリックします（Prime Infrastructure で現在推奨されているのは、Cisco.com で提供されるイメージ バージョンの最新リンクのみです）。
- **Select Image from Local Repository** ローカルに保存するイメージを選択する場合。次に、[ローカル リポジトリ（Local Repository）] で以下を行います。

ステップ 6 配布するイメージを選択して、[**Apply**] をクリックします。

ステップ 7 [配布イメージ名（Distribute Image Name）] フィールドでイメージ名を選択し、選択内容を変更して新しいイメージを選択してから、[**Save**] をクリックします。

ステップ 8 配布オプションを指定します。**Administration > System Settings >Inventory> SoftwareImage Management** でデフォルト オプションを変更できます。

ステップ 9 スケジュール配布オプションを指定し、[今すぐ（Now）] または [日付（Date）] を選択してから [**Submit**] をクリックします。

Cisco.com からのイメージのダウンロード

デバイスのタイプによっては、Prime Infrastructure では、Cisco.com から最初の最新のイメージバージョン リンクを表示できます。（Cisco.com のイメージ推奨事項に応じた基準の調整（124 ページ） を参照）。

Prime Infrastructure は、管理者が設定した Cisco.com のクレデンシャルを使用します。デフォルトのクレデンシャルが設定されていない場合は、有効なクレデンシャルを入力する必要があります（ソフトウェア イメージ操作に関する Cisco.com クレデンシャルの変更（128 ページ） を参照）。

ステップ 1 **[インベントリ（Inventory）]>[デバイス管理（Device Management）]>[ソフトウェア イメージ（Software Images）]** の順に選択します。

ステップ 2 [追加/インポート（Add/Import）] アイコンをクリックします。

ステップ 3 [イメージのインポート（Import Images）] ダイアログで、次の手順を実行します。

a) **[Cisco.com]** をクリックします。

b) クレデンシャルが自動的に入力されない場合は、有効な Cisco.com のユーザ名とパスワードを入力します。

c) [エンドユーザ ライセンス契約書（End User License Agreement）] と [強力な暗号化資格同意書（Strong Encryption Eligibility Agreement）] に同意します。

d) [ログイン（Login）] をクリックします。

ステップ 4 [デバイスの選択（Device Selection）] タブをクリックします。

ステップ 5 [デバイスの選択方法（Select devices by）] トグル ボタンをクリックして、[グループ（Group）] または [デバイス（Device）] オプションからデバイスを選択できます。最大 20 個のデバイスを選択できます。

ステップ 6 **[グループ（Group）]** オプションを選択した場合は、デバイス グループを選択し、**[デバイスの選択（Choose Devices）]**ペインに一覧表示されるデバイスを選択します。選択したデバイスは、[選択されたデバイス（Selected Devices）] ペインに表示されます。

ステップ 7 [イメージの選択（Image Selection）] タブをクリックします。

ステップ 8 イメージを選択し、[スケジュール（Schedule）] タブをクリックします。

ステップ 9 [送信（Submit）] をクリックします。

ステップ 10 イメージが [ソフトウェア イメージ（Software Images）] ページのリストに表示されていることを確認します（[便利なリンク（Useful Links）] セクションで [ソフトウェア イメージ リポジトリ（Software Image Repository）] リンクをクリックします）。

ソフトウェア イメージをリポジトリに追加（インポート）する

Prime Infrastructure では、指定したデバイス タイプに推奨される最新のソフトウェア イメージが表示され、Cisco.com からソフトウェア イメージを直接ダウンロードできます。Prime Infrastructure には、提供が停止されたソフトウェア イメージは表示されません。詳細については、「Cisco Prime Infrastructure 3.2 のサポート対象デバイス」のリストを参照してください。

（注） Cisco.com から K9 ソフトウェア イメージをダウンロードするには、定期的に https://software.cisco.com/download/eula.html K9 契約を確認して同意する必要があります。

次のトピックでは、ソフトウェア イメージをイメージ リポジトリに追加するさまざまな方法について説明します。失敗したインポートのトラブルシューティング方法の例については、ジョブ ダッシュボードを使用したジョブの管理 （27 ページ）を参照してください。

- 管理対象デバイスで実行されているソフトウェア イメージの追加 （134 ページ）
- IPv4 または IPv6 サーバからソフトウェア イメージを追加する（URL） （136 ページ）
- FTP プロトコル サーバのソフトウェア イメージの追加（プロトコル） （136 ページ）
- クライアント マシンのファイル システムからのソフトウェア イメージの追加 （137 ページ）

管理対象デバイスで実行されているソフトウェア イメージの追加

この方法では、管理対象デバイスからソフトウェア イメージを取得し、イメージ リポジトリにそのイメージを保存します。

（注） デバイスへのイメージの配布には、デバイスでサポートされている最もセキュアなプロトコル（TFTP ではなく SCP など）を使用します。非常に大きなファイルを転送する場合、またはサーバとクライアントが地理的に離れている場合には、TFTP はタイムアウトになる傾向があります。イメージの配布に SCP を選択する場合は、デバイスがフル ユーザ権限（特権 EXEC モード）を使用して Prime Infrastructure で管理されていることを確認してください。フル ユーザ権限を使用しないと、配布はコピー権限エラー（「SCP：プロトコルエラー：権限拒否（SCP: protocol error: Privilege denied）」）が原因で失敗します。

プロトコル パスワードに特殊文字を使用している場合、ソフトウェア イメージの配布およびイメージのインポートが認証エラーで失敗する可能性があります。

デバイスからサーバにイメージをコピーする場合のみ（その逆ではない）、TFTP がサポートされることに注意してください。

制限事項

- Cisco IOS XR デバイスの場合、デバイスからのイメージの直接インポートは、Prime Infrastructure によってサポートされていません。SMU と PIE のインポートも、これらのデバイスではサポートされていません。
- Cisco IOS-XE デバイスについては、デバイスが「packages.conf」ファイルを使用してロードされている場合、そのデバイスからイメージを直接インポートすることはできません。

ステップ 1 **[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ソフトウェア イメージ（Software Images）]** の順に選択します。

ステップ 2 [追加/インポート（Add/Import）] アイコンをクリックします。

ステップ 3 [イメージのインポート（Import Images）] ダイアログで、次の手順を実行します。

Cisco Catalyst 3850 イーサネット スタッカブル スイッチおよび Cisco 5760 シリーズ ワイヤレス コントローラの場合は、ソフトウェア イメージをインポートするための以下の 2 つのモードがあります。

- [インストール モード（Install mode）] : デバイスがインストール モードで動作している場合、実行イメージは「packages.conf」となります。Prime Infrastructure は、インストール モードでのイメージのインポートをサポートしていません。
- [バンドル モード（Bundle mode）] : デバイスがバンドル モードで動作している場合、実行イメージは「.bin」形式となります。Prime Infrastructure は、バンドル モードでのイメージのインポートをサポートしています。

次のいずれかの方法で実行イメージを確認できます。

- [インベントリ（Inventory）] > [ネットワーク デバイス（Network Devices）] の順に選択し、デバイス名をクリックして、デバイス ページの [イメージ（Image）] タブをクリックします。
- デバイス CLI で Show version コマンドを使用します。

a) [デバイス（Device）] を選択します。
b) [デバイスの選択（Device Selection）] タブをクリックします。
c) [デバイスの選択方法（Select devices by）] トグル ボタンをクリックして、[グループ（Group）] または [デバイス（Device）] オプションからデバイスを選択できます。
d) [グループ（Group）] オプションを選択した場合は、デバイス グループを選択し、[デバイスの選択（Choose Devices）] ペインに一覧表示されるデバイスを選択します。選択したデバイスは、[選択されたデバイス（Selected Devices）] ペインに表示されます。
e) [スケジュール（Schedule）]エリアで、ジョブを即時実行するか、後で実行するか、または定期的に実行するかをスケジュールします。
f) [送信（Submit）] をクリックします。

ステップ 4 ジョブのステータスを表示するには、ポップアップ メッセージ内のジョブ リンクをクリックするか、**Administration > Job Dashboard** を選択します。

ステップ 5 イメージが [ソフトウェア イメージ（Software Images）] ページ（**[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ソフトウェア イメージ（Software Images）]**）に表示されていることを確認します。

IPv4 または IPv6 サーバからソフトウェア イメージを追加する（URL）

ネットワーク可能な IPv4 や IPv6 サーバまたは FTP/HTTP サーバからソフトウェア イメージをインポートできます。Prime Infrastructure は、シスコ以外の標準イメージ（Cisco.com に掲載されていないエンジニアリング イメージ）のインポートをサポートしています。そのため、Prime Infrastructure では、任意のタイプのファイル形式をインポートできます。

Prime Infrastructure は、シスコ以外の標準イメージのインポートをサポートしています。

ステップ 1 [インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ソフトウェア イメージ（Software Images）] の順に選択します。

ステップ 2 [追加/インポート（Add/Import）] アイコンをクリックします。

ステップ 3 [イメージのインポート（Import Images）] ダイアログで、次の手順を実行します。

a) **URL** をクリックします。

b) [イメージを収集する URL（URL To Collect Image）] フィールドに、URL を次の形式で入力します（ユーザ クレデンシャルが必要ない HTTP URL を使用することもできます）。

http://*username***:***password***@***server-ip/filename*

c) [スケジュール（Schedule）] エリアで、ジョブを即時実行するか、後で実行するか、または定期的に実行するかをスケジュールします。

d) **Submit** をクリックします。

ステップ 4 ジョブのステータスを表示するには、ポップアップ メッセージ内のジョブ リンクをクリックするか、**Administration > Job Dashboard** を選択します。

ステップ 5 イメージが [ソフトウェア イメージ（Software Images）] ページ（**[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ソフトウェア イメージ（Software Images）]**）に表示されていることを確認します。

FTP プロトコル サーバのソフトウェア イメージの追加（プロトコル）

ステップ 1 [インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ソフトウェア イメージ（Software Images）] の順に選択します。

ステップ 2 [追加/インポート（Add/Import）] アイコンをクリックします。

（注） プロトコル パスワードで特殊文字を使用すると、認証エラーによりソフトウェア イメージ インポートが失敗する場合があります。

ステップ 3 [イメージのインポート（Import Images）] ダイアログで、次の手順を実行します。

a) **Protocol** をクリックします。

b) [プロトコル（Protocol）] フィールドに FTP と入力してから、FTP ユーザ名、パスワード、サーバ名または IP アドレス、およびファイル名を入力します。ファイル名の例は次のとおりです。

/*ftpfolder*/asr901-universalk9-mz.154-3.S4.bin

c) [スケジュール（Schedule）]エリアで、ジョブを即時実行するか、後で実行するか、または定期的に実行するかをスケジュールします。

d) **Submit** をクリックします。

ステップ 4 ジョブのステータスを表示するには、ポップアップ メッセージ内のジョブ リンクをクリックするか、**Administration > Job Dashboard** を選択します。

ステップ 5 [ソフトウェアイメージ（Software Images）]ページ（[インベントリ（Inventory）]>[デバイス管理（Device Management）]>[ソフトウェア イメージ（Software Images）]）に、イメージがリストされていることを確認します。

クライアント マシンのファイル システムからのソフトウェア イメージの追加

始める前に

ソフトウェア イメージ ファイルをインポートすると、ブラウザ セッションが一時的にブロックされます。アップロード処理がブラウザ セッションのアイドル タイムアウトの制限値を超えると、Prime Infrastructure からログアウトされて、ファイルのインポート操作が異常終了します。したがって、インポート操作を開始する前に、アイドル タイムアウトの制限値を増やすことを推奨します。アイドル タイムアウト値を増やすには、アイドル ユーザ用のグローバル タイムアウトを設定するを参照してください。

ステップ 1 [インベントリ（Inventory）]>[デバイス管理（Device Management）]>[ソフトウェア イメージ（Software Images）] の順に選択します。

ステップ 2 [追加/インポート（Add/Import）] アイコンをクリックします。

ステップ 3 [イメージのインポート（Import Images）] ダイアログで、次の手順を実行します。

a) **File** をクリックします。

b) [**Browse**] ボタンをクリックし、ソフトウェア イメージ ファイルに移動します。

c) [スケジュール（Schedule）]エリアで、ジョブを即時実行するか、後で実行するか、または定期的に実行するかをスケジュールします。

d) **Submit** をクリックします。

（注） [ファイル（File）]オプションを使用したインポートは推奨されないため、より大きなサイズ（200 MB より大きい場合など）のファイルをインポートするには URL または [プロトコル（Protocol）] オプションを使用する必要があります。

ステップ 4 ジョブのステータスを表示するには、ポップアップ メッセージ内のジョブ リンクをクリックするか、**Administration > Job Dashboard** を選択します。

ステップ 5 [ソフトウェア イメージ（Software Images）]ページ（[インベントリ（Inventory）]>[デバイス管理（Device Management）] > [ソフトウェア イメージ（Software Images）]）に、イメージがリストされていることを確認します。

（注） アクティブ化ジョブごとに [今すぐ（Now）] または [日付（Date）] を選択した場合のみ、[送信（Submit）] ボタンが有効になります。

仮想イメージリポジトリへのソフトウェアイメージのインポート

Prime Infrastructure の仮想イメージ リポジトリ（VIR）を使用すると、指定 URL またはファイルからデバイスイメージを自動的に取得および保存できます。これらのダウンロードを定期的に実行するようにスケジュールを設定できます。

現在、VIR は FTP または HTTP ダウンロードのみをサポートしています。

ソフトウェア イメージを VIR にインポートするには、次の手順を実行します。

ステップ 1 **[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [仮想イメージ リポジトリ（Virtual Image Repository）]** を選択します。ページには、リポジトリに現在保持されているイメージの数が表示されます。

ステップ 2 [インポート（Import）] をクリックします。

ステップ 3 ソフトウェア イメージのインポート元となる [送信元（Source）] を指定します。次のいずれかの送信元を指定できます。

- [URL]：ソフトウェア イメージのインポート元となる FTP または HTTP URL を指定します。ユーザ クレデンシャルが必要ない HTTP URL を使用できます。
- [ファイル（File）]：クライアント マシン上のローカル ファイル。

ステップ 4 [収集オプション（Collection Options）] をクリックし、必要な情報を入力します。

ステップ 5 [スケジュール（Schedule）]をクリックし、イメージファイルのインポートのスケジュールを指定します。収集ジョブをすぐに実行することも、後で実行するようにスケジュール設定することもできます。また、ジョブを自動的に繰り返すようにスケジュールを設定することもできます。

ステップ 6 [送信（Submit）] をクリックします。

ステップ 7 **[管理（Administration）] > [ダッシュボード（Dashboards）] > [ジョブ ダッシュボード（Jobs Dashboard）] > [ユーザ ジョブ（User Jobs）] > [ソフトウェア イメージのインポート（Software Image Import）]** を選択

し、イメージ収集ジョブのステータスを表示します。[期間（Duration）]フィールドは、ジョブが完了した後に更新されます。

関連トピック

ソフトウェア イメージをリポジトリに追加（インポート）する （134 ページ）
デバイスへの新しいソフトウェア イメージの配布 （140 ページ）

ソフトウェアイメージをアップグレードするためのデバイス要件の変更

以下の手順を使用して、ソフトウェアイメージをデバイスに配布するためにデバイスが満たす必要のある RAM、フラッシュ、およびブート ROM の要件を変更します。アップグレード分析を行う場合、これらの値を確認します（デバイスがイメージ要件を満たしていることの確認（アップグレード分析） （139 ページ）を参照）。

ステップ 1 [インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ソフトウェア イメージ（Software Images）] の順に選択します。

ステップ 2 [ソフトウェア イメージ サマリー（Software Image Summary）] パネルで、関連付けられたハイパーリンクをクリックすることによって、ソフトウェア イメージを検索および選択します。

ステップ 3 ソフトウェア イメージ名のハイパーリンクをクリックして、イメージ情報を開きます。

ステップ 4 以下のように、デバイス要件を調整します。

- 最小 RAM（1 ～ 999999999999999）
- 最小 FLASH（1 ～ 999999999999999）
- ブート ROM の最小バージョン

ステップ 5 **Save** をクリックします。

ステップ 6 以前の要件を維持するには、[デフォルトに戻す（Restore Defaults）] をクリックします。

デバイスがイメージ要件を満たしていることの確認（アップグレード分析）

アップグレード分析では、デバイスのハードウェアは RAM および FLASH に関連する新しいイメージを格納できるか、イメージはデバイスファミリと適合するか、およびソフトウェアのバージョンはデバイス上で実行中のイメージのバージョンと適合するかを確認できます。分析

の後、デバイスごとの結果を提供するレポートが Prime Infrastructure で表示されます。レポートデータは以下から収集されます。

- ソフトウェア イメージ リポジトリ。これには、イメージヘッダー内の最小 RAM、最小フラッシュなどの情報が含まれます。
- Prime Infrastructure インベントリ。これには、デバイス上のアクティブ イメージに関する情報と、フラッシュメモリ、モジュール、プロセッサの詳細が含まれます。

（注） アップグレード分析は、Cisco ASR 9000 デバイスを除くすべての Cisco IOS-XR デバイス（Cisco NCS 1000、Cisco NCS 4000、Cisco NCS 5000、Cisco NCS 5500、および Cisco NCS 6000）でサポートされています。

イメージのデバイス要件を調節する場合は、ソフトウェアイメージをアップグレードするためのデバイス要件の変更 （139 ページ）を参照してください。

ステップ 1 [インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ソフトウェア イメージ（Software Images）] の順に選択します。

ステップ 2 [便利なリンク（Useful Links）] で、**[ソフトウェアイメージアップグレード分析（Software Image Upgrade Analysis）]** をクリックします。（[ソフトウェア イメージ（Software Images）] ページから画像を選択しないでください）。

ステップ 3 [アップグレード分析（Upgrade Analysis）] ダイアログで以下を行います。

a) ソフトウェア イメージのソース（イメージ リポジトリまたは Cisco.com）を選択します。
b) [デバイスの選択（Device selection）] ページをクリックして、分析するデバイスを選択します。
c) [デバイスの選択方法（Select devices by）] トグル ボタンをクリックして、[グループ（Group）] または [デバイス（Device）] オプションからデバイスを選択できます。
d) [グループ（Group）] オプションを選択した場合は、デバイス グループを選択し、[デバイスの選択（Choose Devices）] セクションに一覧表示されるデバイスを選択します。選択したデバイスは、[選択されたデバイス（Selected Devices）] セクションに表示されます。
e) デバイスを分析するソフトウェア イメージを選択します。
f) [レポートの実行（Run Report）] をクリックします。

レポートでは、デバイスが IP アドレスでグループ化されます。

デバイスへの新しいソフトウェア イメージの配布

1 回の展開で、デバイス、または類似するデバイスのセットにソフトウェア イメージを配布できます。Prime Infrastructure は、デバイスとソフトウェア イメージに互換性があることを確認します。

デバイスの機能に基づき、Prime Infrastructure はさまざまな転送プロトコル（SCP、TFTP、FTP、SFTP）を使用してデバイスにイメージを配布できます。より高い信頼性とセキュリティを確保するため、ソフトウェア イメージの配布にはセキュア プロトコル（SFTP、SCP）のみを使用することを推奨します。イメージの配布に SCP プロトコルを選択する場合は、デバイスがフル ユーザ権限（特権 EXEC モード）を使用して Prime Infrastructure で管理されていることを確認してください。フルユーザ権限を使用しないと、配布はコピー権限エラー（「SCP：プロトコル エラー：権限拒否（SCP: protocol error: Privilege denied）」）が原因で失敗します。

TFTP または FTP の使用は推奨しません。イメージの配布に TFTP プロトコルを選択し、デバイスとサーバが別のサブネットにある場合は、アプリケーションで維持される指定セッション時間制限（1 時間）内にイメージをコピーする必要があります。そうしないと、配布はタイムアウト エラーが原因で失敗します。

ソフトウェアイメージ配布を効率的に実行するには、配布の実行元となるデバイスおよびサーバが、地理的に同じ場所または建物内にある必要があります。ソフトウェア イメージを Prime Infrastructure およびデバイスのさまざまな地理的位置に配信する場合は、ロケーション グループを作成し、その位置をソフトウェアイメージ管理サーバにマッピングします。この外部サーバが、イメージを Prime Infrastructure からソフトウェア イメージ管理サーバに転送し、マッピングされたデバイス位置への配布を開始します。ネットワークの速度低下により、配布に時間がかかる場合、ソフトウェア配布ジョブはエラーを返します。

（注） CISCO-FLASH-MIB へのアクセスをブロックする SNMP ビューがないようにするため、ソフトウェアイメージをダウンロードするすべてのルータとスイッチ（存在する場合）の設定から、次のコマンドを削除します。

プロトコル パスワードに特殊文字を使用している場合、ソフトウェア イメージの配布およびイメージのインポートが認証エラーで失敗する可能性があります。

```
snmp-server view ViewName ciscoFlashMIB excluded
```

ステップ 1 **[インベントリ（Inventory）]>[デバイス管理（Device Management）]>[ソフトウェア イメージ（Software Images）]** の順に選択します。

ステップ 2 ソフトウェア イメージ管理ライフサイクル ウィジェットの [配布（Distribute）] をクリックします。

ステップ 3 [イメージ選択（Image Selection）] ウィンドウで、配布するソフトウェア イメージを選択します。

ステップ 4 [デバイスの選択（Device Selection）] タブをクリックし、イメージを配布するデバイスを選択します。

a) [デバイスの選択方法（Select devices by）] トグル ボタンをクリックして、[グループ（Group）] または [デバイス（Device）] オプションからデバイスを選択できます。

b) [グループ（Group）] オプションを選択した場合は、デバイス グループを選択し、[デバイスの選択（Choose Devices）] ペインに一覧表示されるデバイスを選択します。選択したデバイスは、[選択されたデバイス（Selected Devices）] ペインに表示されます。

デフォルトで、選択したイメージを適用できるデバイスが表示されます。

ステップ 5 [イメージ詳細の検証（Image Details Verification）] タブをクリックし、イメージの行をクリックして次の操作を行います。

- 選択内容を変更するには [配布イメージ名（Distribute Image Name）] フィールドでイメージ名を選択し、新しいイメージを選択してから、[保存（Save）] をクリックします。
- [配布場所（Distribute Location）] フィールドに表示されている値を選択し、ソフトウェア イメージを保存する新しい場所を選択し、[保存（Save）] をクリックします。
- [ソフトウェアイメージ管理サーバ（Software Image Management Server）] フィールドに表示されている値を選択し、[保存（Save）] をクリックします。ローカル ファイル サーバ、または **[管理（Administration）] > [サーバ（Servers）] > [ソフトウェアイメージ管理サーバ（Software Image Management Servers）]** で作成したサーバの 1 つを選択できます。

[ステータス（Status）] フィールドと [ステータス メッセージ（Status Message）] フィールドに選択内容の有効性が表示されます。たとえば、ステータスが緑色の場合、デバイス上の指定された場所にイメージを保存するための十分なスペースがあることを示しています。

ステップ 6 [イメージ展開（Image Deployment）] タブをクリックし、必要に応じてイメージ展開オプションを設定します。

- [現行イメージのバックアップ（Back Up Current Image）]：新しいイメージを配布する前に、デバイスからソフトウェア イメージ リポジトリ ページに実行イメージをインポートします。
- [ブート コマンドの挿入（Insert boot command）]：デバイスのブート パス リストでブート変数を設定します。
- [アクティブ化（Activate）]：[アクティブ化（Activate）] オプションを有効にするには、[ブート コマンドの挿入（Insert Boot Command）] チェックボックスをオンにする必要があります。
  - [アクティブ化オフ（Activate OFF）]：新しいイメージが配布され、デバイスのブート パス リストでブート変数が設定されます。このモードではデバイスはリブートせず、引き続き実行イメージを使用して稼働します。
  - [順次アクティブ化（Activate Sequential）]：選択されているすべてのデバイスへのイメージ配布が完了すると、デバイスは順次リブートします。
  - [並行アクティブ化（Activate Parallel）]：選択されているすべてのデバイスへのイメージ配布が完了すると、デバイスは同時にリブートします。
- [配布前にスマートフラッシュ削除（Smart Flash Delete Before Distribution）]：デバイスに十分なメモリがない場合、イメージ配布前にフラッシュ メモリを消去します。
- [障害が発生しても続行（Continue on Failure）]：1 つのイメージのイメージ配布が失敗しても、キュー内の次のデバイスがアクティブ化対象としてピックアップされます。
- [TFTPフォールバック（TFTP Fallback）]：イメージ配布が失敗した場合に、TFTP サーバの場所から現行の実行イメージをリロードするよう、デバイスに指示します。
- [デバイスアップグレードモード（Device Upgrade Mode）]：詳細は、セクションワイヤレス/DC デバイスへのソフトウェア イメージの展開 （145 ページ）を参照してください。
- [ISSUオプション（ISSU Options）]：[ISSU] オプションを選択すると、デバイスのソフトウェア イメージがデバイスを再起動しなくてもアップグレードされます。Nexus デバイスの場合、サービス ソフト

ウェア ダウングレード（ISSD）は特定のイメージでサポートされていませんが、従来のリロード（シャーシ リロード）を実行するか、Prime Infrastructure の ISSU オプションを使用せずにイメージをアクティブにする必要があります。詳細については、Cisco Nexus 7000 シリーズ NX-OS リリース ノート（リリース 6.2）の「*Supported Upgrade and Downgrade Paths*」の項を参照してください。

ステップ 7 Prime Infrastructure では、ソフトウェア イメージの配布に最大で 1 台のローカル ファイル サーバと 3 台のソフトウェア イメージ管理サーバを使用できます。各サーバでは 1 回あたりイメージを 5 つのデバイスに配布できます。1 つのデバイスでイメージの配布が完了すると、後続の次のデバイスがイメージ配布対象になります。[配布のスケジュール（Schedule Distribution）] タブをクリックし、スケジュール オプションを指定して、[送信（Submit）] をクリックします。

イメージ配布ジョブの詳細は、ソフトウェア イメージ管理ダッシュボードに表示されます。また、[管理（Administration）] > [ダッシュボード（Dashboards）] > [ジョブダッシュボード（Jobs Dashboard）] > [ユーザジョブ（User Jobs）] > [ソフトウェアイメージの配布（Software Image Distribution）] から、イメージ配布ジョブの詳細を表示することもできます。[期間（Duration）] フィールドは、ジョブが完了した後に更新されます。

（注） [送信（Submit）] ボタンは、各アクティブ化ジョブに [今すぐ（Now）] または [日付（Date）] を選択しないと有効になりません。

デバイスで新しいソフトウェアイメージをアクティブにする

新しいイメージがデバイスでアクティブになっている場合、それがディスクで実行されているイメージになります。新しいイメージをアクティブにしても、非アクティブにされたイメージは削除されません。デバイスからイメージを手動で削除する必要があります。

同じジョブで、イメージの配布とアクティブ化を実行する場合、デバイスへの新しいソフトウェア イメージの配布 （140 ページ）を参照してください。

新しいイメージをデバイスに配布せずに、イメージをアクティブにするには（たとえば、デバイスにアクティブにしたいイメージが存在する）、次の手順を実行します。アクティブ化は配布操作を使用しますが、新しいイメージを配布しません。

ステップ 1 [インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ソフトウェア イメージ（Software Images）] の順に選択します。

ステップ 2 ソフトウェア イメージ管理ライフサイクル ウィジェットの [有効化（Activate）] アイコンをクリックします。

ステップ 3 [有効化ソース（Activation Source）] タブで、必要に応じて [ライブラリから有効化（Activate from Library）]、[完了した配布ジョブから有効化（Activate from Completed Distribution Jobs）]、または [スタンバイ/代替イメージから有効化（Activate from Standby/Alternate Images）] を選択します。

ステップ 4 [完了した配布ジョブから有効化（Activate from Completed Distribution Jobs）] を選択する場合は、ジョブ選択タブに移動して、配布に成功または一部成功したジョブを選択します。次に、[プレビューの有効化（Activate preview）] タブに移動し、イメージ名とフラッシュの詳細が表示されたデバイス リストを選択します。[ジョブオプションの有効化（Activate Job Options）] タブをクリックします。

ステップ 5 [ジョブ オプションの有効化（Activate Job Options）] ウィンドウで、必要な設定を選択し、ステップ 10 に移動します。

- [オプションのアクティブ化（Activate Options）] : [オフ（Off）]、[順次（Sequential）]、または [並行（Parallel）]
- [失敗後に続行（Continue on Failure）] : デバイスで配布が失敗した場合でも、アクティブ化を続行します。
- [コミット（Commit）] : 配布後にデバイスでイメージをコミットします。
- [ISSUオプション（ISSU Options）] : [ISSU] オプションを選択すると、デバイスのソフトウェア イメージがデバイスを再起動しなくてもアップグレードされます。Nexus デバイスの場合、サービス ソフトウェア ダウングレード（ISSD）は特定のイメージでサポートされていませんが、従来のリロード（シャーシ リロード）を実行するか、Prime Infrastructure の ISSU オプションを使用せずにイメージをアクティブにする必要があります。詳細については、Cisco Nexus 7000 シリーズ NX-OS リリース ノート（リリース 6.2）の「*Supported Upgrade and Downgrade Paths*」の項を参照してください。
- [デバイスアップグレードモード（Device Upgrade Mode）] : オプションは次のとおりです。
  - [バンドルモードに変換（Convert to Bundle Mode）] : アクティブ化されたイメージがバンドル モードでアップグレードまたはダウングレードされ、イメージ形式が .bin になります。
  - [インストールモードに変換（Convert to Install Mode）] : アクティブ化されたイメージはインストール モードでアップグレードまたはダウングレードされ、イメージ形式が packages.conf になります。
  - [現在の実行モードの保持（Retain Current Running Mode）] : アクティブ化されたイメージは、バンドル モードまたはインストール モードに関係なく、既存のデバイス実行モードでアップグレードまたはダウングレードされます。

ステップ 6 [有効化ソース（Activation Source）] タブの [ライブラリから有効化（Activate from Library）] を選択する場合は、[イメージ選択（Image Selection）] タブをクリックします。

ステップ 7 [イメージ選択（Image Selection）] タブで、配布するソフトウェア イメージを選択します。

ステップ 8 [デバイスの選択（Device Selection）] タブをクリックし、イメージをアクティブ化するデバイスを選択します。

a) [デバイスの選択方法（Select devices by）] トグル ボタンをクリックして、[グループ（Group）] または [デバイス（Device）] オプションからデバイスを選択できます。

b) [グループ（Group）] オプションを選択した場合は、デバイス グループを選択し、[デバイスの選択（Choose Devices）] ペインに一覧表示されるデバイスを選択します。選択したデバイスは、[選択されたデバイス（Selected Devices）] ペインに表示されます。

ステップ 9 [イメージ詳細の検証（Image Details Verification）] タブに移動して、[ロケーションのアクティブ化（Activate Location）] フィールドを変更し、検証ステータス メッセージを確認します。

ステップ 10 [イメージの有効化（Activate Image）] タブをクリックし、選択したデバイスおよびソフトウェア イメージを有効化するために正しくマッピングしているかどうかを確認します。アクティブ化にスタンバイ イメージを使用する場合は、[イメージ選択の確認（Verify Image Selection）] タブをクリックします。

（注） スタンバイ/代替イメージをアクティブにする際に、スタンバイ/代替イメージのバージョンがデバイスで実行されているイメージよりも古いバージョンである場合、[確認ステータス メッセージ（Verification Status Message）] 列に、赤色で古いバージョンにダウングレードしようとしていることが示されます。

ステップ 11 [ジョブ オプションの有効化（Activate Job Options）] タブをクリックし、必要なジョブの有効化オプションを選択します。

ステップ 12 [スケジュールのアクティブ化（Schedule Activation）] タブに移動し、[今すぐ（Now）] または [日付（Date）] を選択して、[送信（Submit）] をクリックし、選択したデバイスのソフトウェア イメージをアクティブにします。

（注） アクティブ化ジョブごとに [今すぐ（Now）] または [日付（Date）] を選択した場合のみ、[送信（Submit）] ボタンが有効になります。

ワイヤレス/DC デバイスへのソフトウェア イメージの展開

[デバイス アップグレード モード（Device Upgrade Mode）] オプションは、Cisco 5760 シリーズ ワイヤレス コントローラおよび Cisco Catalyst 3850 イーサネット スタッカブル スイッチのイメージ アップグレード時のみ表示されます。次の表では、Cisco 5760 シリーズ ワイヤレス コントローラおよび Cisco Catalyst 3850 イーサネット スタッカブル スイッチ向けの考えられるデバイス アップグレード オプションと対応するイメージ形式について説明します。

表 *16 :* アップグレード/ダウングレード モード オプション

デバイス アップグレード モード	配布前のデバイスイメージ形式	配布後のデバイスイメージ形式
インストール モードからバンドル モードへの変更	packages.conf	.bin
インストールモードから現在の実行モードの保持への変更	packages.conf	packages.conf
バンドル モードから現在の実行モードの保持への変更	.bin	.bin
バンドル モードからインストール モードへの変更	.bin	packages.conf

イメージ配布ステータスが「成功（Success）」の場合、次のオプションのいずれかを使用してイメージ バージョンを確認できます。

- **[インベントリ（Inventory）]** > **[ネットワークデバイス（Network Devices）]** を選択します。
  - [ネットワークデバイス（Network Devices）] ページの [ソフトウェアバージョン（Software Version）] 列を確認します。
  - デバイス名をクリックし、[イメージ（Image）] タブをクリックします。
- デバイス CLI で **show version** コマンドを使用します。

関連トピック

デバイスで新しいソフトウェア イメージをアクティブにする （143 ページ）

スタック デバイスのサポートされているイメージ形式

Prime Infrastructure は、スタック構成デバイスのアップグレードとダウングレードに対し、.tar イメージのみをサポートしています。スタック デバイスは .bin 形式をサポートしていません。サポートされるスタック デバイスのリストは次のとおりです。

- CBS3100 スイッチ モジュールのスタック
- Cisco Catalyst Switch Module 3110X for IBM Blade Center
- Cisco Catalyst Blade Switch 3120X for HP
- Cisco Catalyst Blade Switch 3130X for Dell M1000E
- Cisco Catalyst 2975 スイッチ
- Cisco 3750 スタッカブル スイッチ
- Cisco Catalyst 29xx スタッカブル イーサネット スイッチ
- Cisco ME 3600X-24FS-M スイッチ
- Cisco ME 3600X-24TS-M スイッチ
- Cisco ME 3800X-24FS-M スイッチ ルータ

（注） Cisco Catalyst 3650 および 3850 スイッチの .tar イメージは Cisco.com にはありません。これらのスイッチでは、Prime Infrastructure は .bin 形式をサポートします。

デバイスのリロード間でのCisco ISO XRイメージのコミット

（注） Cisco IOS XR デバイスの場合、デバイスがその設定で一定期間稼働し、パッケージの変更が適切であると確信できるまでは、パッケージ変更をコミットしないことが推奨されます。

デバイスにCisco IOS XRパッケージをコミットすると、パッケージの設定はデバイスのリロード後にも維持されます。また、コミット操作では、ロールバック操作に使用できるロールバック ポイントがデバイスに作成されます。

イメージの配布、アクティブ化、コミットを同一ジョブで行う場合は、「デバイスへの新しいソフトウェア イメージの配布」で説明する手順を使用します。

アクティブ化したイメージをコミットするには、次の手順に従います。

（注） 単一デバイスだけを使用している場合は、[デバイスの詳細（Device Details）] ページからコミット操作を実行します（[**Image**] タブをクリックしてイメージを選択し、[**Commit**] をクリックします）。

ステップ 1 [インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ソフトウェア イメージ（Software Images）] の順に選択します。

ステップ 2 ソフトウェア イメージ管理ライフサイクル ウィジェットの [コミット（Commit）] アイコンをクリックします。

ステップ 3 コミットするイメージのあるデバイスを選択して、[送信（Submit）] をクリックします。（アクティブ化されているイメージだけがコミット可能です。）

ステップ 4 [デバイスの選択方法（Select devices by）] トグル ボタンをクリックして、[グループ（Group）] または [デバイス（Device）] オプションからデバイスを選択できます。

ステップ 5 [グループ（Group）] オプションを選択した場合は、デバイス グループを選択し、[デバイスの選択（Choose Devices）] ペインに一覧表示されるデバイスを選択します。選択したイメージは、[選択されたデバイス（Selected Devices）] ペインに表示されます。

（注） （アクティブ化されているイメージだけがコミット可能です。）

ステップ 6 アクティブ化するソフトウェア イメージを選択し、[送信（**Submit**）] をクリックします。

ステップ 7 [配布スケジュール（Schedule Distribution）] エリアで、コミット ジョブを即時実行するか、後で実行するか、または定期的に実行するかをスケジュールします。

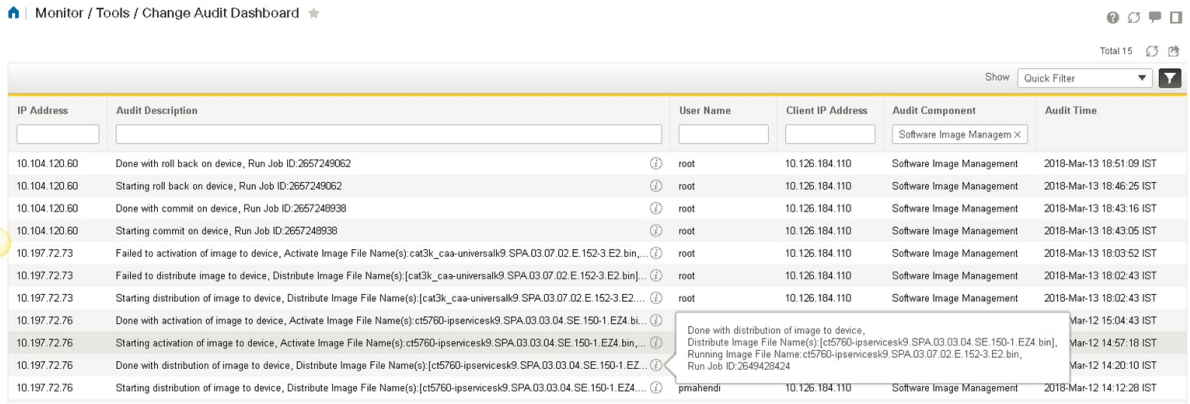
ステップ 8 [送信（Submit）] をクリックします。

ステップ 9 **Administration > Job Dashboard** を選択し、イメージ アクティブ化ジョブに関する詳細を確認します。

ソフトウェア イメージ操作に関する変更監査の確認

デバイスのソフトウェア イメージの変更に関する履歴情報を取得するには、を確認します。変更監査ダッシュボード。

ステップ 1 **[モニタ（Monitor）] > [ツール（Tools）] > [変更監査ダッシュボード（Change Audit Dashboard）]** の順に選択します。イメージ管理の操作だけが表示されるように結果をフィルタリングするには、[監査コンポーネント（Audit Component）] フィールドに **software image** と入力します。



ステップ 2 すべてのデバイス タイプのイメージの配布とアクティベーションの状態を表示するには、監査の説明の横にある情報アイコンをクリックします。

例：

デバイスへのイメージの配布を開始、

イメージ ファイル名を配布：[cat3k_caa-universalk9.SPA.03.07.02.E.152-3.E2.bin]、

実行イメージ ファイル名：cat3k_caa-universalk9.SPA.03.07.04.E.152-3.E4.bin、

ジョブ ID:2198989942 を実行

デバイスへのイメージの配布を終了、

イメージ ファイル名を配布：[cat3k_caa-universalk9.SPA.03.07.02.E.152-3.E2.bin]、

実行イメージ ファイル名：cat3k_caa-universalk9.SPA.03.07.04.E.152-3.E4.bin、

ジョブ ID:2198989942 を実行

ASD の例外とエラー条件

Cisco Prime Infrastructure では、Cisco Automated Software Distribution（ASD）サービスを使用してソフトウェア情報とダウンロード URL が提供されるので、デバイス/アプリケーションを最新バージョンにアップグレードする際に役立ちます。

次の表では、cisco.com からソフトウェア イメージをインポートする際に Prime Infrastructure の ASD API によって返される ASD の例外とエラー条件について説明します。

表 *17 : ASD* の例外とエラー条件

エラー コード	エラーの説明
PID_INVALID	要求で指定された PID が無効です。有効な PID でサービスを呼び出してください。
IMG_NM_INVALID	指定された image_name が無効です。有効な image_name を指定してください。
SWTID_INVALID	指定された software_type_id が無効です。有効な software_type_id を指定してください。
INVALID_INPUT	入力が無効か、または指定された入力に対してデータが見つかりません。
INVALID_MTRANSID	無効な metadata_trans_id。
INVALID_DWLDSID	無効な download_session_id。
INVALID_DRETRYID	無効な download_retry_id。
IMAGE_GUID_INVALID	要求で指定された image_guid が無効です。有効な image_guid を指定してください。
PID_MISSING	要求に PID がありません。要求に有効な PID を指定してください。
CUR_REL_MISSING	要求に current_release がありません。要求に有効な current_release を指定してください。
OUT_REL_MISSING	要求に output_release がありません。要求に有効な output_release を指定してください。
IMG_NM_MISSING	要求に image_names がありません。少なくとも 1 つの有効な image_names を指定してください。
MISSING_DW_RETRY_ID	要求に download_retry_id がありません。要求に有効な download_retry_id を指定してください。
MTRANSID_MISSING	要求に metadata_trans_id がありません。要求に有効な metadata_trans_id を指定してください。
IMAGE_LIMIT_EXCEEDED	要求に入力されたイメージ名の数が制限を超えています。
DRETRYID_EXPIRED	有効期限が切れている download_retry_id が以前に付与されました。
DWLDSID_EXPIRED	有効期限が切れている download_session_id が以前に付与されました。\ndownload_session_id なしでダウンロード サービスを開始してください。

エラー コード	エラーの説明
MTRANSID_EXPIRED	有効期間に時間制限があったため有効期限が切れている metadata_trans_id が以前に付与されています。メタデータ サービスを呼び出してダウンロードを開始してください。
NO_DATA_FOUND	データが見つかりません。
IMAGE_GUID_MISSING	要求に image_guid がありません。要求に有効な image_guid を指定してください。
TIMEOUT	10000
CART_EMPTY	チャートに項目がありません。
DWLD_WARN	この警告メッセージは、記録では次の製品をダウンロードすることを許可されていない可能性があることが示されているために表示されます。
DWLD_WARN1	このメッセージが間違いであると思われる場合は、テクニカル サポート <mailto:ent-dl@cisco.com> に電子メールでお問い合わせください（24 時間 365 日サポート体制）要求を迅速に処理するために、次の情報を含めてください：ユーザ ID（ソフトウェアのダウンロードに使用される Cisco.com ID）、連絡先名、会社名、契約番号、製品 ID、目的のソフトウェア リリースまたはファイル名。電子メールに上記のメッセージを含めてください。\上記の製品がお客様の Cisco.com プロファイルに関連付けられているサービス契約の対象であるかを確認するには、シスコ担当者、パートナーまたはリセラーにお問い合わせください。[Partner Locator]https://locatr.cloudapps.cisco.com/WWChannels/LOCATR/openBasicSearch.doリンクから、最寄りのパートナーを検索できます。Cisco Profile Manager を使用してこれらの製品のサービス契約をプロファイルに追加するか、またはサービス管理者に代行させることができます。
DWLD_WARN2	次のいずれかのオプションを使用して、将来的にサービスを十分受けることができること、および Cisco.com プロファイルが正確で最新のものであることを確認してください。シスコ担当者、パートナーまたはリセラーに連絡して、上記の製品が Cisco.com プロファイルに関連付けられているサービス契約の対象であることを確認してください。[Partner Locator]https://locatr.cloudapps.cisco.com/WWChannels/LOCATR/openBasicSearch.doリンクから、最寄りのパートナーを検索できます。Cisco Profile Manager を使用してこれらの製品のサービス契約をプロファイルに追加するか、またはサービス アクセス管理者に代行させることができます。ソフトウェアのダウンロード中に不必要な中断や遅延が発生しないように、この通知に従って迅速に対応していただければ幸いです。
K9_FORM_AR	K9 フォームが受け入れられなかったか、またはダウンロードを続行することを拒否されました。
EULA_FORM_AR	EULA フォームが受け入れられなかったか、またはダウンロードを続行することを拒否されました。
K9_FORM_ACC	K9 フォームがダウンロードの続行を認められませんでした。
EULA_FORM_ACC	EULA フォームがダウンロードの続行を認められませんでした。

エラー コード	エラーの説明
K9_EULA_FORM_AR	EULA フォームと k9 フォームの両方が受け入れられなかったか、またはダウンロードを続行することを拒否されました。
SER_UNEXPECT_FAIL	サービスに予期しないエラーが発生しました。要求されたデータを用意してサポートにお問い合わせください。

ローリング AP アップグレードの使用によるコントローラ ソフトウェアのアップグレード

ローリング AP アップグレード機能を使用すると、AP およびコントローラ ソフトウェアのバージョンを Prime Infrastructure からアップグレードできます。アップグレード グループに AP を追加すると、すべてのアクセス ポイントが同時にリブートすることを防止できます。AP アップグレード グループは、指定した優先順位に従って順番に再起動されます。

ローリング AP アップグレードを有効にするには、次の手順に従います。

始める前に

1. N+1 コントローラを新しいバージョンにアップグレードする必要があります。
2. プライマリ コントローラはプライマリ イメージから起動するように設定する必要があります。
3. Prime Infrastructure をトラップ レシーバとして追加し、両方のコントローラで AP レジスタ トラップ制御を有効にする必要があります。
4. N+1 コントローラには、プライマリ コントローラと同様に、次の設定が必要です。
   - WLAN
   - AP グループ
   - モビリティ グループ
   - RF グループ
   - RF プロファイル

ステップ 1 [設定（Configure）] をクリックし、次に [ネットワーク（Network）] で [ネットワークデバイス（Network Devices）] をクリックします。

ステップ 2 対応するチェックボックスをクリックして、グループに追加する AP を選択します。

ステップ 3 [グループとサイト（Groups and Sites）] をクリックし、次に [グループに追加（Add to Group）] をクリックします。

ステップ 4 AP を追加するグループを選択し、[追加（Add）] をクリックします。

コントローラごとに 10 個以上のグループや、グループごとに 1000 AP に設定することは推奨しません。現在、グループに AP を追加している場合は、アップグレード プロセスを初期化する必要があります。

ステップ 5 [設定（Configuration）] をクリックし、次に [ワイヤレステクノロジー（Wireless Technologies）] で [ローリングAPアップグレード（Rolling AP Upgrade）] をクリックします。

ステップ 6 プライマリ コントローラおよび N+1 コントローラを選択します。

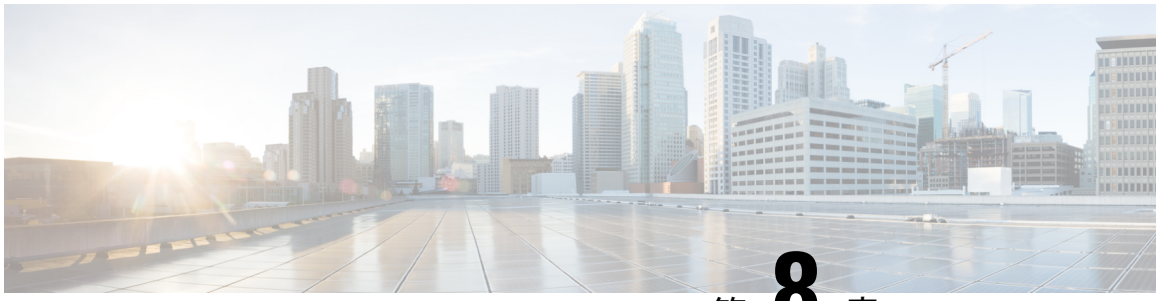
（注） コントローラは、スタンドアロンまたは冗長ペアのコントローラのいずれかを指定できます。

ステップ 7 AP を移動してプライマリ コントローラに戻す場合は、対応するチェックボックスをオンにします。そうしないと、それらの AP はリブート後に N+1 コントローラに関連付けられます。

ステップ 8 AP グループがリブートする順番を設定するには、AP グループを選択し、リスト上で上または下に移動させます。

ステップ 9 転送プロトコルを選択し、必要な詳細情報を入力します。

ステップ 10 ジョブのステータスを表示するには、[管理（Administration）] をクリックし、[ダッシュボード（Dashboards）] で [ジョブダッシュボード（Job Dashboard）] をクリックします。



第 8 章

コンプライアンスを使用した設定の監査の実行

この章は、次の内容で構成されています。

- コンプライアンス監査の実行方法 （153 ページ）
- コンプライアンス監査の有効化および無効化 （154 ページ）
- 新しいコンプライアンス ポリシーの作成 （155 ページ）
- コンプライアンス ポリシー ルールの作成 （155 ページ）
- ポリシーとルールが含まれているコンプライアンス プロファイルの作成 （162 ページ）
- コンプライアンス監査の実行 （164 ページ）
- コンプライアンス監査の結果の表示 （165 ページ）
- デバイスのコンプライアンス違反の修正 （166 ページ）
- 違反サマリーの詳細の表示 （167 ページ）
- 違反ジョブの詳細の表示 （168 ページ）
- コンプライアンス ポリシーのインポートおよびエクスポート （169 ページ）
- コンプライアンス ポリシー XML ファイルのコンテンツの表示 （169 ページ）
- PSIRT および EOX 情報の表示 （170 ページ）

コンプライアンス監査の実行方法

次の表に、コンプライアンス機能を使用するための基本的な手順を示します。

	説明	参照先：
1	名前と他の説明テキストを含むコンプライアンス ポリシーを作成します。	新しいコンプライアンス ポリシーの作成 （155 ページ）
2	コンプライアンス ポリシーにルールを追加します。ルールは違反を構成するものを指定します。	コンプライアンス ポリシー ルールの作成 （155 ページ）

3	（ネットワーク デバイスで監査を実行するために使用する）コンプライアンス プロファイルを作成し、次の手順を実行します。 • コンプライアンス ポリシーをそのプロファイルに追加します。 • 監査に含めるポリシー ルールを選択します。 同じプロファイルに複数のカスタム ポリシーや定義済みのシステム ポリシーを追加できます。	ポリシーとルールが含まれているコンプライアンス プロファイルの作成 （162 ページ）
4	プロファイルを選択し、監査ジョブをスケジューリングして、コンプライアンス監査を実行します。	コンプライアンス監査の実行 （164 ページ）
5	コンプライアンス監査の結果を表示し、必要に応じて違反を修正します。	コンプライアンス監査の結果の表示 （165 ページ）

コンプライアンス監査の有効化および無効化

コンプライアンス機能は、デバイス設定ベースラインと監査ポリシーを使用して、ネットワーク デバイスの設定の逸脱を検出して訂正します。一部のコンプライアンス レポートはシステムパフォーマンスに影響する可能性があるため、デフォルトではこれは無効になっています。コンプライアンス機能を有効にするには、次の手順を実行します。

（注） コンプライアンス機能を使用するには、システムが『Cisco Prime Infrastructure Quick Start Guide』で指定されているプロフェッショナル サイジング要件を満たす必要があります。

（注） Prime Infrastructure バージョン 3.0 でコンプライアンス監査を無効にすると、GUI からのコンプライアンスが無効になり、バックグラウンドでのコンプライアンス データ収集が停止されます。コンプライアンス設定を機能させるには、ユーザが Prime Infrastructure サーバを再起動してデバイスを再同期する必要があります。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** を選択し、**[一般（General）] > [サーバ（Server）]** を選択します。

ステップ 2 [コンプライアンス サービス（Compliance Services）] の横の [有効化（Enable）] をクリックし、次に [保存（Save）] をクリックします。

ステップ 3 アプリケーションを再起動します。

ステップ 4 デバイス インベントリを再同期します。手順としては、[インベントリ（Inventory）] > [ネットワークデバイス（Network Devices）] の順に選択し、すべてのデバイスを選択した後、[同期（Sync）] をクリックします。

（注） バージョン 3.0 にアップグレードする前に Prime Infrastructure でコンプライアンスが有効になっていた場合、アップグレード後は [システム設定（System Settings）] でコンプライアンスが無効になります。ユーザは、この項で説明する手順に従って手動でコンプライアンスを有効にする必要があります。この場合は、Prime Infrastructure サーバの再起動とデバイスの再同期は必要ありません。

新しいコンプライアンス ポリシーの作成

空のポリシー テンプレートから新しいコンプライアンス ポリシーを作成できます。

ステップ 1 **[設定（Configuration）] > [コンプライアンス（Compliance）] > [ポリシー（Policies）]** を選択します。

ステップ 2 左側の [コンプライアンス ポリシー（Compliance Policies）] ナビゲーション領域にある [コンプライアンス ポリシーの作成（Create Compliance Policy）]（+）アイコンをクリックします。

ステップ 3 ダイアログボックスに名前と任意の説明を入力し、[作成（Create）] をクリックします。ポリシーが左側の [コンプライアンス ポリシー（Compliance Policies）] ナビゲーション領域に追加されます。

ポリシーを複製するには、[i] アイコンをクリックし、[ポリシーの複製（Duplicate Policy）] を選択します。

次のタスク

コンプライアンス ポリシーにルールを追加します。コンプライアンス ポリシー ルールの作成（155 ページ）を参照してください。

コンプライアンス ポリシー ルールの作成

コンプライアンス ポリシー ルールはプラットフォーム固有であり、デバイスの違反と見なされるものを定義します。また、違反を修正する CLI コマンドをルールに含めることもできます。コンプライアンス監査ジョブを設定する際に監査に含めるルールを選択できます（コンプライアンス監査の実行 （164 ページ）を参照）。

ステップ 1 **[設定（Configuration）] > [コンプライアンス（Compliance）] > [ポリシー（Policies）]** を選択して、左側のナビゲーション領域からポリシーを選択します。

ステップ 2 作業領域ペインから [新規（New）] をクリックし、新しいルールを追加します。

類似するルールがある場合は、[複製（Duplicate）] をクリックし、ルールを編集して新しい名前で保存することができます。

ステップ 3 ルールの基準を入力して新しいルールを設定します。

（注） [新しいルール（New Rule）] ウィンドウに表示されるフィールドの説明については、『Cisco Prime Infrastructure Reference Guide』を参照してください（そのドキュメントの情報も Prime Infrastructure に適用されます）。

（注） Prime Infrastructure は、すべての Java ベースの正規表現をサポートしています。http://www.rexegg.com/regex-quickstart.htmlを参照してください。

a) タイトル、説明、およびその他の情報を [ルール情報（Rule Information）] テキスト フィールドに入力します。この情報は、フリー テキストであり、ルールの設定には影響しません。

b) このルールの対象デバイスを [プラットフォームの選択（Platform Selection）] 領域に指定します。

c) （任意）[ルールの入力（Rule Inputs）] 領域で、[新規（New）] をクリックし、このルールを含んでいるポリシーの実行時にユーザに表示する入力フィールドを指定します。たとえば、IP アドレスの入力を求めるプロンプトを表示できます。

（注） [複数の値の承認（Accept Multiple Values）] チェックボックスをオンにした場合は、すべてのルール入力が条件に一致している場合にのみ監査に合格します。

d) [条件とアクション（Conditions and Actions）] 領域で、[新規（New）] をクリックし、確認する基準を指定します。これにより、ルールの合否の条件が決定します。例：ルールの条件とアクション （157 ページ）の例を参考にしてください。

[ブロックオプション（Block Options）] セクションの [ブロックとして解析（Parse as Blocks）] チェック ボックスをオンにして、実行コンフィギュレーション全体をブロックに分割し、各ブロック内の条件一致基準値を検索します。

[ブロック開始式（Block Start Expression）] および [ブロック終了式（Block End Expression）] テキスト ボックスで指定した開始式と終了式に基づいて、ブロックが分割されます。ブロックが形成されると、各ブロックは [条件一致基準（Condition Match Criteria）] セクションの [値（Value）] フィールドで指定された条件と照合され、対応するアクションが実行されます。2 番目の条件では、[以前に一致したブロック（Previously Matched Blocks）] として [条件の範囲（Condition Scope）] を選択して解析する必要があります。

（注） [ブロックとして解析（Parse as Blocks）] チェック ボックスをオンにせずに一致条件値を検索すると、実行コンフィギュレーション全体が解析され、一致するすべてのインスタンスに対して 1 つの違反が発生します。

[一致アクションの選択（Select Match Action）] セクションで [続行（Continue）] オプションを選択し、[不一致アクションの選択（Select Does not Match Action）] セクションで [違反を発生させない（Does Not Raise a Violation）] オプションを選択することは避けてください（逆も同様）。新しいルールの作成ではこれらの組み合わせは無効です。

ステップ 4 [作成（Create）] をクリックします。ルールがコンプライアンス ポリシーに追加されます。

必要な数だけルールを作成できます。監査ジョブを実行する場合は、検証するルールを選択できることを覚えておいてください。

（注） 新しいコンプライアンス ポリシー ルールを作成し、正規表現を使用して（存在する場合は）ルールまたはコマンドを検証する間には、Java 正規表現を使用して式をテストすることをお勧めします。

次のタスク

コンプライアンス ポリシーとそのルールを含むプロファイルを作成し、そのプロファイルを使用して監査を実行します。ポリシーとルールが含まれているコンプライアンス プロファイルの作成 （162 ページ）を参照してください。

例：ルールの条件とアクション

- 例：ブロック オプション （157 ページ）
- 条件およびアクションの例：コミュニティ文字列 （159 ページ）
- 条件およびアクションの例：IOS ソフトウェア バージョン （161 ページ）
- 条件およびアクションの例：NTP サーバの冗長性 （161 ページ）

例：ブロック オプション

このコンプライアンス ポリシーでは、ある特定のブロック内に定義されている不正または未承認の SNMP コミュニティ文字列があるかどうかを確認します。ブロック内で検出された場合、ポリシーは「承認されていないコミュニティ文字列<1.1> を検出しました（Detected unauthorized community string <1.1>）」というメッセージで違反を報告し、すべての非準拠 SNMP 文字列をブロックから削除します。

タブ	タブ領域	フィールド	値
ルール情報（Rule Information）		ルール タイトル（Rule Title）	snmp-server community having non-standard entries
プラットフォームの選択（Platform Selection）			Cisco IOS デバイス、Cisco IOS-XE デバイス
Condition 1			

[条件の詳細（Condition Details）]	**[条件範囲の詳細（Condition Scope Details）]**	条件の範囲（Condition Scope）	設定（Configuration）
	ブロック オプション（Block Options）	ブロック開始表現（Block Start Expression） （このフィールドは、[ブロックとして解析（Parse as Blocks）] チェックボックスがオンになっている場合にのみ有効になります）	^snmp-server community .*
	条件一致基準（Condition Match Criteria）	演算子	Matches the expression
		値	snmp-server community (.*)
アクションの詳細（Action Details）	**一致アクションの選択（Select Match Action）**	アクションの選択（Select Action）	続行（Continue）
	不一致アクションの選択（Select Does Not Match Action）	アクションの選択（Select Action）	違反を発生させません（Does Not Raise a Violation）
Condition 2			

[条件の詳細（Condition Details）]	**[条件範囲の詳細（Condition Scope Details）]**	条件の範囲（Condition Scope）	以前に一致したブロック（Previously Matched Blocks）
	ブロック オプション（Block Options）	ブロック開始表現（Block Start Expression） （このフィールドは、[ブロックとして解析（Parse as Blocks）] チェックボックスがオンになっている場合にのみ有効になります）	^snmp-server community .*
	条件一致基準（Condition Match Criteria）	演算子	Matches the expression
		値	snmp-server community ((public RO)|(private RW))
アクションの詳細（Action Details）	**一致アクションの選択（Select Match Action）**	アクションの選択（Select Action）	続行（Continue）
	不一致アクションの選択（Select Does Not Match Action）	アクションの選択（Select Action）	違反を発生させます。
		違反メッセージ タイプ（Violation Message Type）	ユーザ定義の違反メッセージ
		違反テキスト（Violation Text）	承認されていないコミュニティ文字列 <1.1> を検出しました。（Detected unauthorized community string <1.1>.）

（注） 上記の例では、最初の条件での一致基準は 1.1、1.2 などと呼びます。2 番目の条件での一致基準は 2.1、2.2 などと呼びます。

条件およびアクションの例：コミュニティ文字列

このコンプライアンス ポリシーは、**snmp-server community public** または **snmp-server community private** が（望ましくない）デバイスに設定されているかを確認します。設定されている場合、ポリシーは「コミュニティストリングxxxxxが設定されています（Community string *xxxxx*

configured）」というメッセージで違反を発生させます。ここで、*xxx* は最初に見つかった違反です。

タブ	タブ領域	フィールド	値
[条件の詳細（Condition Details）]	**[条件範囲の詳細（Condition Scope Details）]**	条件の範囲（Condition Scope）	設定（Configuration）
	条件一致基準（Condition Match Criteria）	演算子	Matches the expression
		値	snmp-server community {public|private}
アクションの詳細（Action Details）	**一致アクションの選択（Select Match Action）**	アクションの選択（Select Action）	違反を発生させる
	不一致アクションの選択（Select Does Not Match Action）	アクションの選択（Select Action）	続行（Continue）
		違反メッセージ タイプ（Violation Message Type）	ユーザ定義の違反メッセージ
		違反テキスト（Violation Text）	コミュニティ ストリング *xxxxx* が設定されています。

（注） コンプライアンス ポリシーを設定すると、1 つの入力変数で複数の入力値を使用できます。ルール入力領域で [複数の値の使用（Accept Multiple Values）] チェックボックスを選択します。

次に、[条件一致基準（Condition Match Criteria）] 領域の [値（Value）] フィールドで指定された変数の例を示します。

[snmp-server community <_community> RO]：最後のルールが入力されるまで、すべてのルール入力値に基づいて違反を確認します。 この場合、違反メッセージには、すべての入力値がカンマ区切り値として含まれます。たとえば、SNMP コミュニティ [デモ、チェック] が見つかりません。

[snmp-server community <_community.4> RO]：4 番目のルール入力値のみに基づいて違反を確認します。

指定するルール入力値の数が、演算子「.」の後に記載された数字以外にならないようにします。

条件およびアクションの例：IOS ソフトウェア バージョン

このコンプライアンス ポリシーは、Cisco IOS ソフトウェアのバージョン **15.0(2)SE7** がデバイスにインストールされているかどうかを確認します。インストールされていない場合、ポリシーは「show versionの出力に文字列xxxxxが含まれています（Output of show version contains the string *xxxxx*）」というメッセージで違反を発生させます。ここで *xxxx* は 15.0(2)SE7 と一致しない Cisco IOS ソフトウェア バージョンです。

タブ	タブ領域	フィールド	値
[条件の詳細（Condition Details）]	**[条件範囲の詳細（Condition Scope Details）]**	条件の範囲（Condition Scope）	デバイス コマンド出力
		Show Commands	show version
	条件一致基準（Condition Match Criteria）	演算子	文字列を含む
		値	15.0(2)SE7
アクションの詳細（Action Details）	**一致アクションの選択（Select Match Action）**	アクションの選択（Select Action）	続行（Continue）
	不一致アクションの選択（Select Does Not Match Action）	アクションの選択（Select Action）	違反を発生させます。
		違反メッセージ タイプ（Violation Message Type）	ユーザ定義の違反メッセージ
		違反テキスト（Violation Text）	show version の出力に文字列 *xxxxx* が含まれています。

条件およびアクションの例：NTP サーバの冗長性

このコンプライアンス ポリシーは、デバイスでコマンド **ntp server** が少なくとも 2 回表示されるかどうかを確認します。表示されない場合、ポリシーは、「少なくとも2つのNTPサーバを構成する必要があります（At least two NTP servers must be configured）」というメッセージで違反を発生させます。

タブ	タブ領域	フィールド	値

[条件の詳細（Condition Details）]	**[条件範囲の詳細（Condition Scope Details）]**	条件の範囲（Condition Scope）	設定（Configuration）
	条件一致基準（Condition Match Criteria）	演算子	Matches the expression
		Value	(ntp server.*\n){2,}
アクションの詳細（Action Details）	**一致アクションの選択（Select Match Action）**	アクションの選択（Select Action）	続行（Continue）
	不一致アクションの選択（Select Does Not Match Action）	アクションの選択（Select Action）	違反を発生させる
		違反メッセージ タイプ（Violation Message Type）	ユーザ定義の違反メッセージ
		違反テキスト（Violation Text）	NTP サーバを 2 つ以上設定する必要があります。

ポリシーとルールが含まれているコンプライアンスプロファイルの作成

コンプライアンス プロファイルには、1 つ以上のコンプライアンス ポリシーが含まれています。コンプライアンス ポリシーをプロファイルに追加すると、すべてのポリシー ルールがプロファイルに適用されます。含めるポリシー ルールを選択すること（および、その他を無視すること）で、プロファイルをカスタマイズできます。複数のポリシーをプロファイルにグループ化すると、ルールをポリシーごとに選択したり、選択を解除することができます。

ルート ユーザ、管理者ユーザ、またはスーパー ユーザとしてログインする場合は、次の操作を行えます。

- プロファイルの作成、編集、削除。
- [ポリシー（Policies）] ページで作成したルールの選択。

（注） 「その他」のユーザが関連アクションを実行するには、次のタスク権限を有効にする必要があります。

- [コンプライアンス監査プロファイルアクセス（Compliance Audit Profile Access）]：プロファイルを実行および更新し、プロファイル内のポリシーを参照する。
- [コンプライアンス監査プロファイル編集アクセス（Compliance Audit Profile Edit Access）]：コンプライアンス監査プロファイルを作成および編集する。

タスク権限は、**[管理（Administration）]** > **[ユーザ（Users）]** > **[ユーザ、ロール、およびAAA（Users, Roles & AAA）]** > **[ユーザグループ（User Groups）]** ページで確認できます。

[コンプライアンス監査プロファイルへのアクセス（Compliance Audit Profile Access）] タスク権限を選択していないと、[コンプライアンス監査プロファイルの編集アクセス（Compliance Audit Profile Edit Access）] タスク権限を選択していても、[プロファイル（Profile）] ページを表示できません。

ステップ 1 **[設定（Configuration）]** > **[コンプライアンス（Compliance）]** > **[プロファイル（Profiles）]** を選択します。

ステップ 2 [コンプライアンス プロファイル（Compliance Profiles）] ナビゲーション領域にある [ポリシー プロファイルの作成（Create Policy Profile）]（+）アイコンをクリックします。この操作によって [コンプライアンス ポリシーの追加（Add Compliance Policies）] ダイアログボックスが開きます。

ステップ 3 プロファイルに含めるポリシーを選択します。ユーザ定義のポリシーが、[ユーザ定義（User Defined）] カテゴリで使用できるようになります。

a) [コンプライアンス ポリシーの追加（Add Compliance Policies）] ダイアログ ボックスで、追加するポリシーを選択します。

b) [OK] をクリックします。ポリシーが [コンプライアンス ポリシー セレクタ（Compliance Policy Selector）] 領域に追加されます。

ステップ 4 ポリシーに含めるルールを選択します。

a) [コンプライアンス ポリシー セレクタ（Compliance Policy Selector）] 領域でポリシーを選択します。ポリシーのルールは、右側の領域に表示されます。

b) 特定のルールを選択するか、または選択を解除して、[保存（Save）] をクリックします。

（注） ここで選択したルールのみが、このプロファイルのポリシー インスタンスに適用されます。この選択によって、コンプライアンス ポリシーの元のバージョンが変更されることはありません。

次のタスク

コンプライアンス監査の実行（164 ページ）の説明に従って、コンプライアンス監査ジョブをスケジュールします。

コンプライアンス監査の実行

コンプライアンス監査を実行するには、プロファイルを選択し、監査するデバイスを選択し（プロファイル内のポリシーとルールを使用）、監査ジョブのスケジュールを設定します。

ステップ 1 **[設定（Configuration）] > [コンプライアンス（Compliance）] > [プロファイル（Profiles）]** を選択します。

ステップ 2 左側の [コンプライアンス プロファイル（Compliance Profiles）] ナビゲーション領域でプロファイルを選択します。

ステップ 3 [コンプライアンス プロファイル（Compliance Profiles）] ナビゲーション領域で [コンプライアンス監査の実行（Run Compliance Audit）] アイコンをクリックします。

ステップ 4 [デバイスおよび設定（Devices and Configuration）] 領域で、目的のデバイスと監査するコンフィギュレーション ファイルを選択します。

a) デバイス（またはデバイス グループ）を選択します。

b) 監査するコンフィギュレーション ファイルを指定します。

- [最新のアーカイブ済みの設定を使用（Use Latest Archived Configuration）]：アーカイブから最新のバックアップ ファイルを監査します。使用可能なバックアップ ファイルがない場合、Prime Infrastructure はデバイスの監査を実行しません。
- [現在のデバイス設定を使用（Use Current Device Configuration）]：デバイスの実行コンフィギュレーションをポーリングし、監査します

  このオプションを選択すると、Prime Infrastructure は最初にデバイスからコンフィギュレーションのバックアップを取得してから監査を実行します。これは、定期的またはイベントがトリガーしたコンフィギュレーション バックアップが有効になっていない場合に役に立ち、また、Prime Infrastructure にアーカイブ済みのコンフィギュレーションがデバイスとの同期が取れていないことが頻繁にあるため、便利です。

（注） コンプライアンス ルールの指定時に [デバイス コマンドの出力（Device Commands Outputs）] に [条件付き範囲（Conditional Scope）] を選択した場合、show コマンドの出力は最新または現在のアーカイブ済み設定からではなく、デバイスから直接取得されます。

c) [次へ（Next）] をクリックします。

ステップ 5 [アイドル時間制限の設定（分）（Configure Idle Time Limit (min)）] フィールドに値を入力します。デフォルトでは、制限時間は 5 分に設定されます。ユーザが制限時間を変更する場合は、5 ～ 30 の数字を入力できます。設定された制限時間の間アイドル状態が続くと、監査ジョブは中止されます。

ステップ 6 すぐに監査ジョブをスケジュール設定する場合は [今すぐ（Now）] を選択し、後でスケジュール設定する場合は [日付（Date）] を選択して日時を入力します。

監査ジョブを定期的に繰り返すには、[定期（Recurrence）] オプションを使用します。

ステップ 7 [終了（Finish）]をクリックします。監査ジョブがスケジュール設定されます。監査ジョブがスケジュールされると、通知ポップアップが表示されます。監査ジョブのステータスを確認するには、[設定（Configuration）] > [コンプライアンス（Compliance）] > [ジョブ（Jobs）] を選択します。

ステップ 8 ジョブの完了後に電子メールが届きます。電子メールの件名には、ホスト名：ジョブ タイプ：プロファイル名：監査ジョブのジョブ ステータス、およびホスト名：ジョブ タイプ：修正ジョブのジョブ ステータスが含まれています。[メールサーバ設定（Mail Server Configuration）] 画面または [ジョブ通知メール（Job Notification Mail）] 画面でユーザが件名を指定している場合は、これも含まれます。

ステップ 9 監査ジョブに対してトリガーされた電子メールでは、ジョブ名、ジョブ タイプ、ステータス、前回の実行ステータス、PI ホスト名、PI ホスト IP、ポリシー プロファイル名、総デバイス数、監査対象デバイス数、非監査対象デバイス数、およびプロファイルとジョブの詳細を確認するためのリンクが提供されます。

ステップ 10 修正ジョブに対してトリガーされた電子メールでは、ジョブ名、ジョブ タイプ、ステータス、前回の実行ステータス、PI ホスト名、PI ホスト IP、およびジョブの詳細を確認するためのリンクが提供されます。

ステップ 11 ジョブの詳細は、CSV 形式の添付ファイルとして届きます。CSV ファイルはパスワードで保護されていません。

次のタスク

コンプライアンス監査の結果の表示（165 ページ）の説明に従って、監査結果を確認します。

コンプライアンス監査の結果の表示

この手順を使用して、監査ジョブの結果を確認します。結果から、監査したデバイス、スキップしたデバイス、違反があったデバイスなどがわかります。単一のデバイスでさまざまなコンプライアンス ポリシーが実行されている場合があります。

ジョブを作成したら、そのジョブに関して次の設定を行えます。

- [Pause Series]：後日に実行するようにスケジュール設定されているジョブのみに適用できます。実行中のジョブを一時停止することはできません。
- [Resume Series]：一時停止されているジョブのみに適用できます。
- [スケジュールを編集（Edit Schedule）]：スケジュール済みのジョブを別の時間に再度スケジュール設定します。

ステップ 1 **[管理（Administration）] > [ダッシュボード（Dashboards）] > [ジョブダッシュボード（Job Dashboard）] > [ユーザジョブ（User Jobs）] > [コンプライアンスジョブ（Compliance Jobs）]** を選択します。

ステップ 2 [監査ジョブ（Audit Jobs）] タブをクリックしてジョブを見つけ、[前回の実行（Last Run）] 列の情報を確認します。

最後の実行結果の値	説明

Failure	監査した 1 つ以上のデバイスが、プロファイルで指定されたポリシーに違反しています。
Partial Success	コンプライアンス ジョブに、監査済みおよび監査なしのデバイスが両方含まれ、監査済みデバイスのコンプライアンス ステータスは成功です。
Success	監査したすべてのデバイスは、プロファイルで指定されたポリシーに準拠しています。

コンプライアンス監査ジョブの場合、サポートされる違反の数は Prime Infrastructure の標準設定で 20,000 件、Pro 以上の設定では 80,000 件です。

ステップ 3 監査の確認が失敗した場合は、次の手順を実行します。

- 失敗したデバイスを確認するには、[失敗（Failure）] ハイパーリンクの横にある [i] アイコンにカーソルを合わせて詳細のポップアップを表示します。
- ジョブを選択し、[ジョブの詳細を表示（View Job Details）] をクリックし、ポップアップのデバイスの横にある [i] アイコンをクリックして [デバイス 360（Device 360）] ビューを起動します。

ステップ 4 最も詳細な情報を確認するには、[失敗（Failure）] ハイパーリンクをクリックして [コンプライアンス監査違反の詳細（Compliance Audit Violation Details）] ウィンドウを開きます。

（注） [コンプライアンス監査違反の詳細（Compliance Audit Violation Details）] ウィンドウを行き来するには、[次へ（Next）] および [前へ（Previous）] ボタンを使用します。

- 失敗のサマリーについては、[ジョブの詳細と違反（Job Details and Violations）] を確認します。フィールドの説明については、『Cisco Prime Infrastructure Field Reference』の *[管理（Administration）] > [ダッシュボード（Dashboards）] > [ジョブダッシュボード（Job Dashboard）] > [ユーザジョブ（User Jobs）] > [コンプライアンスジョブ（Compliance Jobs）]* のセクションを参照してください。
- デバイスごとの詳細については、[デバイス別の違反（Violations by Device）] 領域を確認します。

次のタスク

違反を修正するには、デバイスのコンプライアンス違反の修正（166 ページ）を参照してください。

デバイスのコンプライアンス違反の修正

Prime Infrastructure では、デバイスで発生するコンプライアンス違反を修正できます。

ステップ 1 [管理（Administration）] > [ダッシュボード（Dashboards）] > [ジョブ ダッシュボード（Job Dashboard）] > [ユーザ ジョブ（User Jobs）] > [コンプライアンス ジョブ（Compliance Jobs）] を選択します。

ステップ 2 コンプライアンス違反が検出されたいずれかのジョブの [最後の実行結果（Last Run Result）] 列で [失敗（Failure）] をクリックします。Prime Infrastructure に、コンプライアンス監査の一部として実行されたすべてのポリシーの違反ステータスが表示されます。

ステップ 3 [違反の詳細（Violation Details）] ページで単一または複数の修正可能な違反を選択し、[次へ（Next）] をクリックします。

修正可能なすべての違反を選択した場合や、修正可能な違反の数が 15,000 件を超える場合は、最初の 15,000 行のみが選択されます。

ステップ 4 [起動設定の保存（Save Startup Config）] をクリックし、[実行中の設定を起動設定にコピー（Copy Running Config to Startup）] オプションを選択して、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できます。

ステップ 5 展開矢印をクリックし、[修正の入力（Enter Fix Input）] オプションが有効になっているデバイスを表示します。

ステップ 6 修正を適用するデバイスを選択して [修正の入力（Enter Fix Input）] をクリックし、詳細を入力します。

ステップ 7 [次へ（Next）] をクリックします。

ステップ 8 設定変更をデバイスに適用するスケジュールを選択して、[修正ジョブのスケジュール（Schedule Fix Job）] をクリックします。

重要 コンプライアンス ポリシーは、すでに追加されている管理対象デバイスに対するデバイス OS、ファミリ、および製品の変更要求を無視します。デバイスの移行中にデバイスを削除して再追加することをお勧めします。

関連トピック

新しいコンプライアンス ポリシーの作成 （155 ページ）
ポリシーとルールが含まれているコンプライアンス プロファイルの作成 （162 ページ）
コンプライアンス監査の結果の表示 （165 ページ）
違反サマリーの詳細の表示 （167 ページ）
違反ジョブの詳細の表示 （168 ページ）

違反サマリーの詳細の表示

レポートを実行して、失敗したすべての監査ジョブの違反を要約した詳細を表示できます。レポートを生成するには、次の手順を実行します。

ステップ 1 [設定（Configuration ）] > [コンプライアンス（Compliance）] > [違反サマリー（Violation Summary）] を選択します。

レポートには、ジョブ失敗の要約情報が表示されます。

ステップ 2 PDF および CSV 形式でレポートをダウンロードできます。

サーバ メモリが設定されたメモリよりも少ない場合、次のコンプライアンス レポートをエクスポートすることはできません。また、1 つのコンプライアンス エクスポート ジョブが実行中の場合、別のコンプライアンス レポートをエクスポートすることはできません。

- 違反サマリ レポート
- PSIRT および EOX レポート（デバイス PSIRT、デバイス ハードウェア EOX、デバイス ソフトウェア EOX、フィールド通知）
- コンプライアンス ジョブ
  - 監査ジョブの障害 > 違反の詳細レポート
  - 監査ジョブの成功レポート
  - 修正ジョブの成功レポート
  - 修正ジョブの失敗レポート

違反ジョブの詳細の表示

次の表に、[違反の詳細（Violation Details）] ページから表示できる詳細を示します。

表示内容	選択方法
スケジュール済み修正可能違反ジョブのステータス。	**1.** [違反の詳細（Violation Details）] ページに移動します。 **2.** [修正可能（Fixable）] 列のフィルタ ボックスをクリックして、[実行中（Running）] を選択します。
修正済み違反ジョブの詳細。	**1.** [違反の詳細（Violation Details）] ページに移動します。 **2.** [修正可能（Fixable）] 列のフィルタ ボックスをクリックして、[修正済み（Fixed）] を選択します。 **3.** [修正済み（Fixed）] リンクをクリックします。
修正失敗違反ジョブの詳細。	**1.** [違反の詳細（Violation Details）] ページに移動します。 **2.** [修正可能（Fixable）] 列のフィルタ ボックスをクリックして、[修正失敗（Fix Failed）] を選択します。 **3.** [修正失敗（Fix Failed）] リンクをクリックします。

コンプライアンス ポリシーのインポートおよびエクスポート

コンプライアンス ポリシーはXMLファイルとして保存されます。個別のコンプライアンス ポリシーをエクスポートし、必要に応じて、それらのポリシーを別のサーバにインポートすることができます。ファイルは、XML 形式でのみインポートできます。

ステップ 1 **[設定（Configuration）] > [コンプライアンス（Compliance）] > [ポリシー（Policies）]** を選択します。

ステップ 2 コンプライアンス ポリシーをエクスポートするには、次の手順を実行します。

a) 左側の [コンプライアンス ポリシー（Compliance Policies）] ナビゲーション領域のポリシーの横にある [i] アイコンの上にマウスを合わせます。

b) ポップアップ ウィンドウで、[XML としてポリシーをエクスポート（Export Policy as XML）] ハイパーリンクをクリックし、ファイルを保存します。

ステップ 3 コンプライアンス ポリシーをインポートするには、次の手順を実行します。

a) 左側の [コンプライアンス ポリシー（Compliance Policies）] ナビゲーション領域の上にある [ポリシーのインポート（Import Policies）] アイコンをクリックします。

b) [ポリシーのインポート（Import Policies）] ダイアログボックスで、[ポリシーの選択（Choose Policies）] をクリックします。

c) XML ファイルを参照して選択します。

d) [インポート（Import）] をクリックします。

e) インポートに失敗したポリシーのログを確認するには、[ポリシーのインポート（Import Policies）] の横にある警告アイコンをクリックします。

コンプライアンスポリシーXMLファイルのコンテンツの表示

コンプライアンス ポリシーは XML ファイルとして保存されます。ポリシーの XML ファイルの内容を表示するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [コンプライアンス（Compliance）] > [ポリシー（Policies）]** を選択します。

ステップ 2 左側の [コンプライアンス ポリシー（Compliance Policies）] ナビゲーション領域でポリシーを見つけ、そのポリシーの横にある [i] アイコンの上にマウスを合わせます。

ステップ 3 ポップアップ ウィンドウで、[XMLとしてポリシーを表示（View Policy as XML）] ハイパーリンクをクリックします。Prime Infrastructure によって内容が XML 形式で表示されます。

PSIRT および EOX 情報の表示

• デバイスのセキュリティ脆弱性の表示 （170 ページ）
• デバイスのハードウェアとソフトウェアのサポート終了レポートの表示 （171 ページ）
• モジュール ハードウェアのサポート終了レポートの表示 （172 ページ）
• デバイスのフィールド通知の表示 （172 ページ）

（注） [PSIRTとEOX（PSIRT and EOX）] ページには、PAS および RBML バンドルの生成日が表示されます。PAS レポートには、バンドルの生成日以前に公開された PSIRT および EoX レコードが保持されます。バンドルの生成後に公開された PSIRT レコードは表示されません。

デバイスのセキュリティ脆弱性の表示

レポートを実行して、Cisco Product Security Incident Response Team（PSIRT）によって定義されているセキュリティの脆弱性が、ネットワーク内のデバイスにあるかどうかを判断できます。レポートには、[デバイスPSIRT（Device PSIRT）]、[デバイスハードウェアEOX（Device Hardware EOX）]、[デバイスソフトウェアEOX（Device Software EOX）]、[モジュールハードウェアEOX（Module Hardware EOX）]、および[フィールド通知（Field Notice）]の情報が含まれます。また、特定の脆弱性に関するマニュアルを参照できます。このマニュアルでは、脆弱性の影響と環境を保護するために必要と考えられる手順が説明されています。

PSIRT レポートには、セキュリティ影響評価（SIR）が「重要」または「高」であるデータのみが含まれます。現在 Prime Infrastructure では、PSIRT 脆弱性評価に CLI 出力を使用することはサポートされていません。

（注） PSIRT および EOX レポートを特定のデバイスに対して実行することはできません。PSIRT および EOX ジョブのスケジュールを設定すると、管理対象で完了状態にあるすべてのデバイスに対してレポートが生成されます（[インベントリ（Inventory）]>[設定（Configuration）]>[ネットワークデバイス（Network Devices）] ページ）。

始める前に

ジョブのスケジュールを設定する前にデバイスを同期します。**[設定（Configuration）]>[ネットワーク デバイス（Network Devices）]** を選択し、デバイスを選択して [同期（Sync）] をクリックします。

ステップ 1 **[レポート（Reports）]** > **[PSIRT と EOX（PSIRT and EoX）]** を選択します。

ステップ 2 ジョブのスケジュールを設定して実行します。[スケジュール（Schedule）]ダイアログボックスが表示されます。[開始時刻（Start Time）] オプションと [繰り返し（Recurrence）] オプションを設定してから、[送信（Submit）]ボタンをクリックしてジョブをスケジュールすることができます。表示されるポップアップで [OK] ボタンをクリックして、すでにスケジュールされているジョブを削除し、新しいジョブを作成します。

[デバイスPSIRT（Device PSIRT）]、[デバイスハードウェアEOX（Device Hardware EOX）]、[デバイスソフトウェアEOX（Device Software EOX）]、[モジュールハードウェアEOX（Module Hardware EOX）]、および [フィールド通知（Field Notice）] の情報を収集して報告するジョブが作成されます。作成する必要のないジョブはそれぞれのタブで区別します。

ステップ 3 PSIRT レポートの現在のステータスを表示するには、[ジョブの詳細を表示（View Job Details）] をクリックします。

ステップ 4 レポートが完了したら、[デバイス PSIRT（Device PSIRT）] タブをクリックして PSIRT 情報を表示します。

ステップ 5 [PSIRT タイトル（PSIRT Title）] 列のハイパーリンクをクリックすると、セキュリティの脆弱性の詳しい説明が表示されます。

ステップ 6 （任意）デバイスの PSIRT の詳細はデバイスごと、またはすべてのデバイスをまとめて PDF 形式および CSV 形式でエクスポートできます。

デバイスのハードウェアとソフトウェアのサポート終了レポートの表示

レポートを実行して、ネットワーク内のシスコ デバイス ハードウェアまたはソフトウェアがサポート終了（EOX）に到達しているかどうかを判断できます。これは、製品のアップグレードや代替オプションを決定する際に役立ちます。

ステップ 1 [レポート（Reports）] > [PSIRTとEOX（PSIRT and EOX）] を選択します。

ステップ 2 [ジョブのスケジュール（Schedule Job）] をクリックします。[スケジュール（Schedule）] ダイアログボックスが表示されます。[開始時刻（Start Time）] オプションと [繰り返し（Recurrence）] オプションを設定してから、[送信（Submit）] ボタンをクリックしてジョブをスケジュールすることができます。表示されるポップアップで [OK] ボタンをクリックして、すでにスケジュールされているジョブを削除し、新しいジョブを作成します。

[デバイスPSIRT（Device PSIRT）]、[デバイスハードウェアEOX（Device Hardware EOX）]、[デバイスソフトウェアEOX（Device Software EOX）]、[モジュールハードウェアEOX（Module Hardware EOX）]、および [フィールド通知（Field Notice）] の情報を収集して報告するジョブが作成されます。タブごとに個別のジョブは作成しません。

ステップ 3 ジョブの完了後に、次のEOXタブのいずれかをクリックすると、そのタブ固有のレポート情報が表示されます。

- **デバイス ハードウェア EOX（Device Hardware EOX）**
- **デバイス ソフトウェア EOX（Device Software EOX）**

ステップ 4 （任意）これらのデバイス EOX の詳細は、デバイスごとまたはすべてのデバイスをまとめて PDF 形式および CSV 形式でエクスポートできます。

モジュール ハードウェアのサポート終了レポートの表示

レポートを実行して、ネットワーク内のシスコモジュールハードウェアがサポート終了（EOX）に到達しているかどうかを判断できます。

ステップ 1 [レポート（Reports）] > [PSIRTとEoX（PSIRT and EoX）] を選択します。

ステップ 2 [ジョブのスケジュール（Schedule Job）] をクリックします。[スケジュール（Schedule）] ダイアログボックスが表示されます。[開始時刻（Start Time）] オプションと [繰り返し（Recurrence）] オプションを設定してから、[送信（Submit）] ボタンをクリックしてジョブをスケジュールすることができます。表示されるポップアップで [OK] ボタンをクリックして、すでにスケジュールされているジョブを削除し、新しいジョブを作成します。

[デバイスPSIRT（Device PSIRT）]、[デバイスハードウェアEOX（Device Hardware EOX）]、[デバイスソフトウェアEOX（Device Software EOX）]、[モジュールハードウェアEOX（Module Hardware EOX）]、および [フィールド通知（Field Notice）] の情報を収集して報告するジョブが作成されます。タブごとに個別のジョブは作成しません。

ステップ 3 [モジュールハードウェアEOX（Module Hardware EOX）] タブをクリックして、モジュール ハードウェアの情報を表示します。

[モジュールPID（Module PID）] 列に PID データが表示されます。これは、1 つの PID または PID のグループです。PID のグループの場合、特定のモジュール ハードウェアにマッピングされた PID に基づいてサポート終了の詳細が表示されます。同様に、別のサポート終了の詳細と PID をマッピングすることはできません。特定の EOL の詳細と PID をマッピングするには、レポートを手動で確認する必要があります。ハードウェアがコンテナで使用できない場合、[モジュールPID（Module PID）] 列にデータは表示されません。モジュール シャーシ PID とサブモジュール PID が同じ場合、PAS の詳細は表示されません。固定モジュールには PID がありません。したがって、EOL の詳細は表示されません。

ステップ 4 （任意）モジュール ハードウェア EOX の詳細は、デバイスごとまたはすべてのデバイスをまとめて PDF 形式および CSV 形式でエクスポートできます。

デバイスのフィールド通知の表示

レポートを実行して、完全なインベントリ収集が完了している管理対象シスコデバイスにField Noticeがあるかどうかを判断できます。FieldNoticeとは、セキュリティ脆弱性の問題以外でシスコ製品に直接関係する重要な問題に関する通知です。通常、アップグレード、回避策、またはその他の対策が必要となります。

ステップ 1 [レポート（Reports）] > [PSIRTとEOX（PSIRT and EOX）] を選択します。

ステップ 2 [ジョブのスケジュール（Schedule Job）] をクリックします。[スケジュール（Schedule）] ダイアログボックスが表示されます。[開始時刻（Start Time）] オプションと [繰り返し（Recurrence）] オプションを設定してから、[送信（Submit）] ボタンをクリックしてジョブをスケジュールすることができます。表示されるポップアップで [OK] ボタンをクリックして、すでにスケジュールされているジョブを削除し、新しいジョブを作成します。

[デバイスPSIRT（Device PSIRT）]、[デバイスハードウェアEOX（Device Hardware EOX）]、[デバイスソフトウェアEOX（Device Software EOX）]、[モジュールハードウェアEOX（Module Hardware EOX）]、および [フィールド通知（Field Notice）] の情報を収集して報告するジョブが作成されます。タブごとに個別のジョブは作成しません。

ステップ 3 [フィールド通知（Field Notice）] タブをクリックすると、フィールド通知の情報が表示されます。

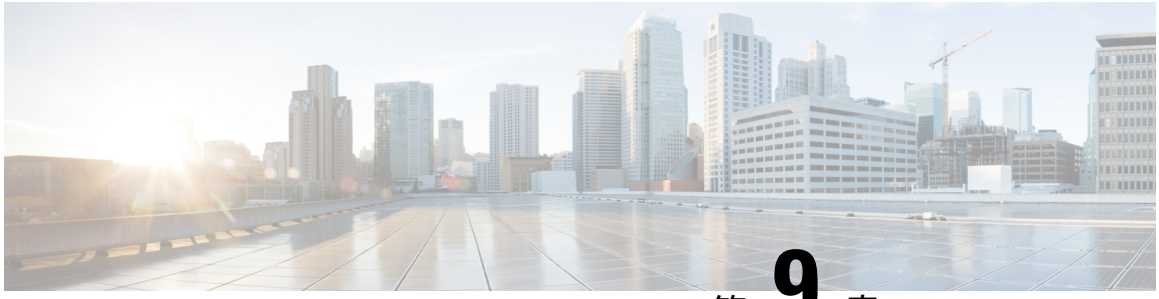
ステップ 4 [脆弱（Vulnerable）] 列の [i] アイコンをクリックして、[フィールド通知URL（Field Notice URL）] および [警告の詳細（Caveat Details）] ダイアログボックスを開きます。cisco.com で詳細を確認するには、[フィールド通知URL（Field Notice URL）] をクリックします。

ステップ 5 （任意）デバイスのフィールド通知の詳細はデバイスごと、またはすべてのデバイスをまとめて PDF 形式および CSV 形式でエクスポートできます。

第 III 部

ネットワークの視覚化

- ネットワーク トポロジの視覚化 （177 ページ）
- ワイヤレス サイト マップの使用 （191 ページ）



第 9 章

ネットワーク トポロジの視覚化

- ネットワーク トポロジの概要 （177 ページ）
- データセンター トポロジ （179 ページ）
- ネットワーク トポロジ マップでのアラームとリンクの詳細なテーブルの表示 （179 ページ）
- トポロジ マップの表示内容の決定 （181 ページ）
- デバイスの詳細情報の取得 （186 ページ）
- リンクの詳細情報の取得 （187 ページ）
- デバイスおよびリンクの障害情報の表示 （187 ページ）
- ネットワーク トポロジ マップのレイアウトの変更 （188 ページ）
- 将来の Web GUI セッション用にネットワーク トポロジ マップのレイアウトを保存する （188 ページ）
- ネットワーク トポロジ マップでのクロック同期ネットワークの表示 （189 ページ）
- イメージ ファイルとしてトポロジ マップを保存する （190 ページ）

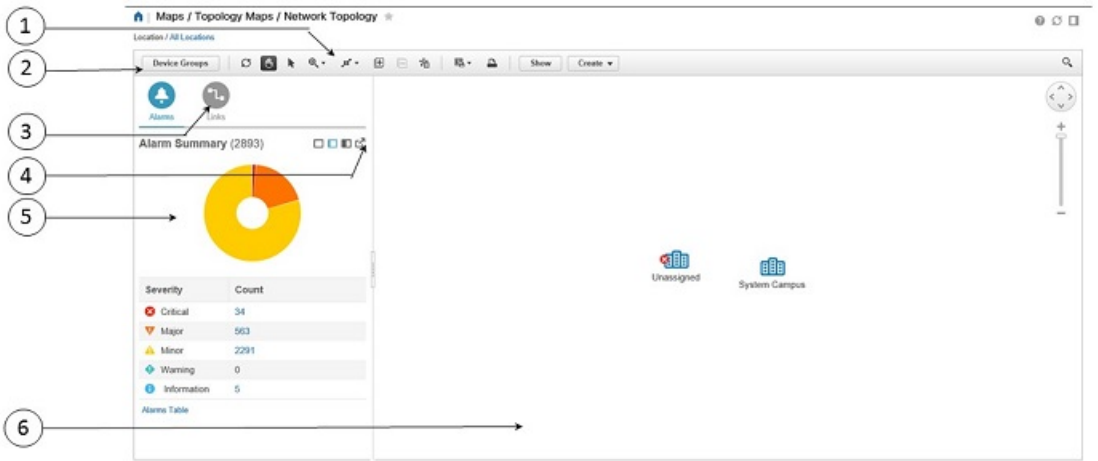
ネットワーク トポロジの概要

[ネットワークトポロジ（Network Topology）] ウィンドウには、デバイスのグラフ形式のトポロジ マップ ビュー、それらの間のリンク、およびマップ内の要素のアクティブなアラームが表示されます。また、[ネットワークトポロジ（Network Topology）] ウィンドウでは、マップ要素のツールと機能にアクセスでき、ドリルダウンしてマップ要素の詳細情報を取得できます。

[ネットワークトポロジ（Network Topology）] ウィンドウは、左側のサイドバーからアクセスします（**[マップ（Maps）]** > **[トポロジ（Topology）]** > **[ネットワークトポロジ（Network Topology）]**）。[ネットワークトポロジ（Network Topology）] ウィンドウの内容は、選択したデバイス グループによって決まります。デバイス グループを選択するには、左側の [デバイス グループ（Device Groups）] パネルを使用します。[デバイスグループ（Device Groups）] パネルから、中央のデバイス グループ化機能にアクセスして、新しいグループを作成したり、グループにデバイスを追加したりできます。詳細については、簡単な管理と設定のためのデバイス グループの作成 （60 ページ）を参照してください。

各ネットワーク トポロジ マップは、アラーム情報とリンク情報を含む左ペインと、マップ自体を表示する右ペインに分かれています。左ペインが展開されると、タブ内のテーブルに追加の列が追加されることがあります。

- [アラームおよびリンク情報（Alarm and Link Information）]（左ペイン）：マップに表示されているデバイスおよびトポロジに関連する情報が提供されます。
  - [アラームのまとめ（Alarm Summary）]：選択したグループのすべての現在のアラームが、アラーム重大度別に分類して表示されます。[アラームのまとめ（Alarm Summary）]タブには、各アラーム重大度のアラーム数を示すテーブルの他に、アラーム重大度に基づいて色分けされた現在のアラームの円グラフが表示されます。これにより、アラーム重大度の分布と各重大度のアラーム数を一目で確認することができます。テーブルと円グラフの両方でドリルダウンすると、その重大度の実際のアラームが一覧表示されたテーブルが表示されます。選択したデバイス グループのすべてのアラームを表示するには、[アラームのまとめ（Alarm Summary）]タブの下部にある [アラームテーブル（Alarms Table）] リンクをクリックします。
  - [リンク（Links）]：選択したデバイス グループに関連するリンクが一覧表示され、リンク上で最も重大度の高いアラームが表示されます。テーブル内のリンクを選択すると、トポロジ マップ内のリンクが強調表示されます。タブの下部にある [リンクテーブル（Links Table）]リンクをクリックすると、別のウィンドウが開き、リンクのテーブルが表示されます。
- [トポロジマップ（Topology map）]（右ペイン）：選択したデバイス グループのトポロジがグラフィカル形式で表示されます。グループのデバイスとサブグループ（存在する場合）と、それらの間のリンク（物理、イーサネット、およびテクノロジー固有のリンク）が表示されます。さらに、デバイスまたはリンクのアクティブ アラームも表示されるため、ネットワークの問題を簡単に特定できます。問題をトラブルシューティングするには、トポロジマップからデバイスやリンクの詳細情報にドリルダウンできます。トポロジマップは、カスタマイズ、フィルタリング、および必要な情報を正確に表示するための操作が可能です。



1	トポロジ ツールバー	2	[Device Groups] ペイン

3	[リンク（Links）] ペイン	4	[Detach] アイコン。このアイコンをクリックすると詳細ウィンドウが開きます。
5	[Alarm Summary] ペイン。アラームの詳細ウィンドウを表示するには、[アラームテーブル（Alarms Table）] をクリックします。	[6]	[トポロジマップ（Topology Map）] ペイン

データセンター トポロジ

データセンター トポロジにアイドル リンクは保持されません。次世代データセンターは、仮想ポート チャネル（vPC）などのテクノロジーを活用して LAN トポロジのすべてのリンクを使用する機能を提供します。vPC は、LAN スイッチ間およびサーバと LAN スイッチ間全体における横断的な帯域幅の使用を実現します。

ポート チャネルは、最大 8 個のインターフェイスを 1 つのグループにバンドルしたもので、帯域幅を広げ冗長性を高めることができます。これらの集約された各物理インターフェイス間でトラフィックのロード バランシングも行います。ポート チャネルの物理インターフェイスが少なくとも 1 つ動作していれば、そのポート チャネルは動作しています。

仮想ポート チャネル（vPC）は、2 つの異なるデバイスに物理的に接続されたリンクを、その他のデバイスから単一のポート チャネルとして見えるようにします。3 つ目のデバイスに他のネットワーク デバイスを使用できます。vPC では、帯域幅を大きくし、ノード間の複数のパラレル パスをイネーブルにし、存在する代替パスでトラフィックのロード バランシングを行うことによって、冗長性が確保されます。

vPC 機能をイネーブルにしたら、ピア キープアライブ リンクを作成します。このリンクは、2 つの vPC ピア デバイス間でのハートビート メッセージの送信を行います。

仮想デバイス コンテキスト（VDC）では、1 つ以上の論理デバイスで 1 つの物理デバイスを仮想化できます。プロビジョニングされた各論理デバイスは、個別の物理デバイスのように設定および管理できます。

ネットワーク トポロジマップでのアラームとリンクの詳細なテーブルの表示

[ネットワーク トポロジ（Network Topology）] ウィンドウでは、拡張テーブルにアクセスして、選択したデバイス グループのアラームとリンクの詳細を一覧表示できます。

拡張詳細テーブルを開くには、[アラームのまとめ（Alarm Summary）] の右上隅にある [切断（Detach）] アイコンをクリックします（または [アラームのまとめ（Alarm Summary）] または [リンク（Links）] の下部にあるハイパーリンクをクリックします）。開いたウィンドウには、[アラーム（Alarms）] タブと [リンク（Links）] タブがあります。

拡張テーブルを使用する場合は、次の点に注意してください。

- 拡張テーブル ウィンドウを開くと、[ネットワークトポロジ（Network Topology）] ウィンドウの左ペインが無効になります。拡張テーブル ウィンドウを閉じると、[ネットワークトポロジ（Network Topology）] ウィンドウの左ペインにあるタブが再び有効になります。
- 拡張テーブルのデータと [ネットワークトポロジ（Network Topology）] ウィンドウの左ペインにある情報は同期しています。たとえば、拡張リンク テーブルのリンクを選択すると、そのリンクも [ネットワークトポロジ（Network Topology）] ウィンドウの左ペインで選択され、回路/VC オーバーレイがトポロジ マップに表示されます。逆に、[ネットワークトポロジ（Network Topology）] ウィンドウの左ペインでリンクを選択してから拡張テーブルを開くと、同じリンクが拡張テーブルで選択されます。
- [ネットワークトポロジ（Network Topology）] ウィンドウと拡張テーブルの両方のアラームは、ユーザの設定に基づいて更新されます。アラームとイベントの表示設定のセットアップ（360ページ）およびアラーム サマリーのカスタマイズ（363ページ）を参照してください。
- テーブルの右上にある [エクスポート（Export）] アイコンをクリックすると、テーブルのデータがファイル（PDF または CSV 形式）にエクスポートされます。エクスポートは、アラームで利用可能です。

詳細テーブルでのデータのフィルタ処理

[表示（Show）] ドロップダウン リストからクイック フィルタまたは高度なフィルタを使用して、特定のアラームまたはリンクを見つけるためにデータをフィルタ処理することもできます。クイック フィルタでは、列の上部に入力したテキストに従って、列に表示されるコンテンツが絞り込まれます。高度なフィルタを使用すると、「次を含まない（Does not contain）」、「等しくない（Does not equal）」、「次で終わる（Ends with）」、「が空である（Is empty）」などの複数の演算子を使用してフィルタを適用し、テーブル内のデータを絞り込むことができます。また、ユーザ定義フィルタを作成することもできます。これを保存すると、[表示（Show）] ドロップダウン メニューに追加されます。

ユーザ定義フィルタを作成して保存するには、次の手順を実行します。

ステップ 1 アラームおよびリンクの拡張テーブルの上にある [表示（Show）] ドロップダウン リストから、[高度なフィルタ（Advanced Filter）] を選択します。

ステップ 2 [高度なフィルタ（Advanced Filter）] データ ポップアップ ウィンドウで、高度なフィルタ条件を入力し、[名前を付けて保存（Save As）] をクリックします。

ステップ 3 [フィルタの保存（Save Filter）] ダイアログボックスで、フィルタの名前を入力して [保存（Save）] をクリックします。

ユーザ定義フィルタを編集または削除するには、[表示（Show）] ドロップダウン リストから [ユーザ定義フィルタの管理（Manage User Defined Filters）] を選択します。

トポロジ マップの表示内容の決定

- ネットワーク トポロジ マップに表示するデバイス グループの選択 （181 ページ）
- トポロジ マップにサブグループのコンテンツを表示する （182 ページ）
- トポロジ マップへのリンクの手動による追加 （183 ページ）
- ネットワーク トポロジ マップに表示するリンクとデバイス タイプの変更 （184 ページ）
- トポロジ マップでのアラームとラベルの表示/非表示 （185 ページ）
- 大規模なトポロジ マップの特定のセクションを隔離する （186 ページ）

ネットワーク トポロジ マップに表示するデバイス グループの選択

トポロジマップを使用すると、1つまたは複数のデバイス グループのトポロジを視覚化できます。選択されたグループでは、特定のネットワーク セグメント、顧客ネットワーク、またはその他のネットワーク要素の組み合わせがカバーされている場合があります。デバイスのグループ化は、階層的に行われます。他の複数のサブグループを含む最上位の親グループが2つあります。それらは、ロケーション グループとユーザ定義グループです。同一の最上位の親グループ内に複数のグループを表示することができます。たとえば、ロケーション グループを複数表示することはできますが、1 つのロケーション グループと 1 つのユーザ定義グループを表示することはできません。

トポロジ マップに表示するデバイスを決定するには、左側の [デバイスグループ（Device Groups）] ペインでデバイス グループを選択します。

必要なグループをトポロジマップに表示させた後、任意のデバイスまたはリンクに関する追加情報にアクセスできます。「デバイスの詳細情報の取得

トポロジマップには、ユーザに割り当てられている仮想ドメインに基づき、ログインしているユーザがアクセス特権を持つデバイスのみが表示されます。詳細については、『Cisco Prime Infrastructure Administrator Guide』の「User Permissions and Device Access」章の「*Create Virtual Domains to Control User Access to Devices*」を参照してください。.

（注） トポロジ コンポーネントが適切に描画されない、あるいはコンポーネント データがマップに表示されないなど、トポロジに関する問題が発生した場合は、ブラウザ キャッシュをクリアして再試行することをお勧めします。

トポロジ マップにネットワーク要素を表示するには、次の手順を実行します。

ステップ 1 **[マップ（Maps）] > [トポロジ マップ（Topology Maps）] > [ネットワーク トポロジ（Network Topology）]** を選択します。

ステップ 2 左側の [デバイス グループ（Device Groups）] ペインでデバイス グループをクリックします。選択したデバイス グループがトポロジ マップの上に表示されます。

ステップ 3 必要に応じて特定のデバイス/リンク タイプを表示し、手動リンクを追加するなどを行って、トポロジマップをカスタマイズします。詳細については、次のトピックを参照してください。

- ネットワーク トポロジ マップに表示するリンクとデバイス タイプの変更 （184 ページ）
- トポロジ マップへのリンクの手動による追加 （183 ページ）
- ネットワーク トポロジ マップのレイアウトの変更 （188 ページ）

トポロジ マップにサブグループのコンテンツを表示する

サブグループを展開すると現在のコンテキストでそのコンテンツを表示できます。またはドリルダウンすると、現在のマップ コンテキストとは別にサブグループのコンテンツを表示できます。

（注） あるデバイスが複数のグループに属している場合、サブグループを展開すると、展開されたグループの 1 つにのみ、そのデバイスが表示されることに注意してください。デバイスは、属しているすべてのグループに表示されるわけではありません。複数のグループに属するデバイスが設定に含まれる場合は、この方法ではなく、[デバイス グループ（Device Groups）]ペインでそれらのグループを選択して、トポロジマップで個々にグループを表示してください。これにより、特定のグループに属するすべてのデバイスが常に表示されます。

サブグループの内容を表示するには、次の手順を実行します。

ステップ 1 トポロジ マップのサブグループをクリックします。

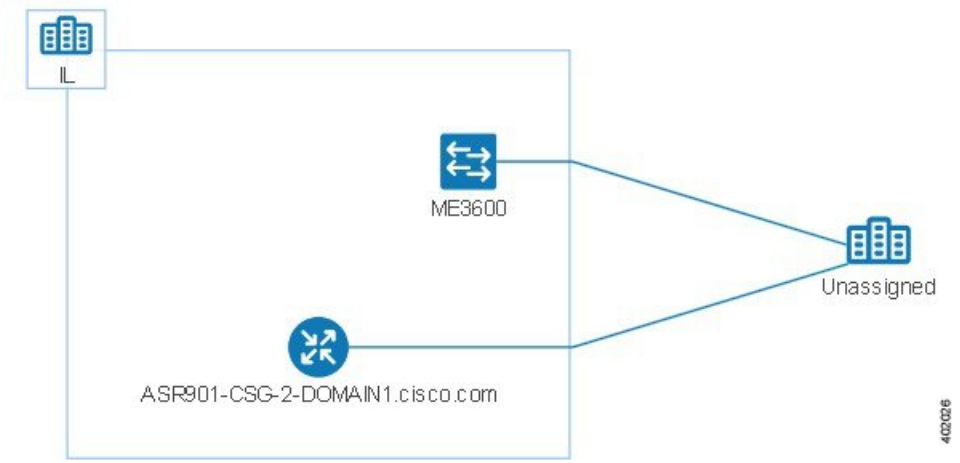
ステップ 2 表示されたポップアップで、次のいずれかをクリックします。

- [グループのドリルダウン（Drill down group）]：トポロジ マップにサブグループがそのまま表示されます。つまり、現在表示されているグループが、選択したサブグループに置き換えられます。サブグループ名が [デバイス グループ（Device Groups）] ペインで選択されることに注意してください。

  （注） サブグループをダブルクリックすると、グループへのドリル ダウンをすばやく実行できます。

- [グループの展開（Expand group）]：現在のトポロジマップ表示にサブグループのコンテンツが追加されます。

下の図では、IL グループが展開されています。



トポロジ マップへのデバイスとネットワークの手動による追加

システムで管理されていないデバイスやネットワークは、それらを手動で追加することでトポロジ マップや Geo マップに表示できます。

ステップ 1 トポロジ ツールバーで、[作成（Create）] > [管理対象外デバイスの作成（Create Unmanaged Device）] か、または [作成（Create）] > [管理対象外ネットワークの作成（Create Unmanaged Network）] を選択します。

ステップ 2 マップをクリックし、デバイスまたはネットワークをマップに追加します。

ステップ 3 マップに新たに追加したデバイスまたはネットワークをクリックします。表示されたパネルから、デバイスまたはネットワークをグループに追加する、デバイスまたはネットワークの名前を変更する、あるいはデバイスまたはネットワークを削除することができます。

デバイスまたはネットワークをトポロジ マップに追加した後は、Geo マップでも使用できるようになります。管理対象外デバイスがマップされていないデバイスのリストに表示され、その位置を設定することができます。

トポロジ マップへのリンクの手動による追加

2 台のデバイスが接続されていることがわかっているものの、Prime InfrastructurePrime Infrastructure がリンクを検出できず、それをマップに表示している場合は、そのリンクを手動で追加できます。このリンクを追加した後は、関連するグループがマップに表示される場合は常にデフォルトで表示されます。

手動リンクを使用できる最も一般的なシナリオを次に示します。

- IOS-XR（NCS 4000、9000、5000、1000）を実行している Cisco NCS デバイス上のトランク ポートの光/DWDM コントローラと NCS 2000 デバイスのアド/ドロップ ポート ペア間。

- IOS-XR（NCS 4000、9000、5000、1000）を実行している Cisco NCS デバイス上のクライアント ポートの光/DWDM コントローラと NCS 2000 トランスポンダ クライアント ポート間（10GE/100GE ポートの接続を表す）。
- IOS-XR（NCS 4000、9000、5000、1000）を実行している Cisco NCS デバイス上のポートの 10GE/100GE コントローラと NCS 2000 トランスポンダ クライアント ポート間（10GE/100GE ポートの接続を表す）。
- 400-G-XP ラインカードを搭載した Cisco NCS 2000 シリーズ デバイス上の 2 つのトランク ポート間。このリンクは、管理対象 OTU リンクとして作成する必要があります。
- 400-G-XP ラインカードを搭載した Cisco NCS 2000 シリーズ デバイスと、4H-OPW-QC2 ラインカードを搭載した Cisco NCS 4000 シリーズ デバイス間。このリンクは、管理対象 OTU リンクとして作成する必要があります。

手動リンクは、管理対象外にすることができます。

- 管理対象外のリンク：視覚化する場合に限ります。2 台のデバイスが接続されているものの、それらのデバイス間のリンクを完全に管理する必要がない場合は、管理対象外の手動リンクをマップに追加できます。このリンクは、グレーの破線で表示されます。

（注） Prime Infrastructure は管理対象の手動リンクをサポートしていません。

2 台のデバイス間にリンクを手動で追加するには、次の手順を実行します。

ステップ 1 トポロジ ツールバーで、**[作成（Create）] > [管理対象外リンクの作成（Create Unmanaged Link）]** を選択します。

ステップ 2 トポロジ マップ内で最初のデバイスをクリックし、マウス ボタンを押したまま 2 番目のデバイスまでドラッグします。

ステップ 3 [インターフェイスの詳細（Interface Details）] ダイアログで、使用可能なインターフェイスのドロップダウン リストから最初のデバイスの送信元インターフェイスと、2 番目のデバイスのターゲット インターフェイスを選択し、[OK] をクリックします。

選択した 2 台のデバイス間のリンクがマップに表示されます。

ネットワーク トポロジ マップに表示するリンクとデバイス タイプの変更

特定タイプのリンクやデバイスのみを選択してネットワーク トポロジ マップに表示することができます。[表示（Show）] ボタンをクリックして [リンク（Links）] または [デバイス ファミリ（Device Families）] を選択し、リンクとデバイス タイプの完全なリストを表示し、表示するものを選択します。

ステップ 1 左側のサイドバーから、**[マップ（Maps）] > [トポロジ マップ（Topology Maps）] > [ネットワーク トポロジ（Network Topology）]** の順に選択します。

ステップ 2 左側の [デバイス グループ（Device Groups）] パネルから、必要なデバイス グループを選択します。

ステップ 3 トポロジツールバーで[表示（Show）]をクリックし、[リンク（Links）]または[デバイス ファミリ（Device Families）] を選択します。

ステップ 4 [リンク（Links）] ダイアログで、次の手順を実行します。

- トポロジマップに表示するリンクのタイプ（たとえば、物理層リンク、イーサネット層リンクなど）を選択します。[リンク（Links）]ダイアログには、ネットワーク内に存在するリンク タイプのみが表示されます。ネットワーク内にリンク タイプが存在していても、選択したデバイス グループにない場合、そのリンク タイプは無効になります。
- 単一のリンクから集約リンクを差別化する場合は、チェックボックスとして[集約リンクの表示（Display Aggregated Links）] を選択します。
- [OK] をクリックします。トポロジ マップに選択内容が反映されます。選択したリンク タイプのみが表示されます。

ステップ 5 [デバイス（Devices）] ダイアログで次の手順を実行します。

- トポロジマップに表示するデバイス タイプ（たとえば、ルータ、スイッチおよびハブ、オプティカル ネットワーキングなど）を選択します。[デバイス（Device）] ダイアログには、ネットワーク内に存在するデバイス タイプのみが表示されます。ネットワーク内にデバイス タイプが存在していても、選択したデバイス グループにない場合、そのデバイス タイプは無効になります。
- [OK] をクリックします。トポロジ マップに選択内容が反映されます。選択したデバイス タイプのみが表示されます。

（注） マップ上にオプティカル ネットワークを表示する場合、デフォルトでは、光回線増幅器として機能するデバイスがある場合は、それらが表示されます。これらの光回線増幅器デバイスをマップに表示しない場合は、[デバイス機能（Device Functions）]の下にある [光回線増幅器の表示（Display Optical Line Amplifier）] チェックボックスをオフにします。[デバイスの機能（Device Functions）] の下にある [光回線増幅器の表示（Display Optical Line Amplifier）] チェックボックスは、回線増幅器の機能をサポートする光デバイスがセットアップに存在する場合にのみ表示されます。

トポロジ マップでのアラームとラベルの表示/非表示

デバイス名のラベルを非表示にする、アラームすべてを非表示にする、あるいは特定の重要度のアラームのみを表示することができます。

ステップ 1 左側のサイドバーから、**[マップ（Maps）] > [トポロジ マップ（Topology Maps）] > [ネットワーク トポロジ（Network Topology）]** の順に選択します。

ステップ 2 トポロジ ツールバーの [表示（Show）] ボタンをクリックします。

ステップ 3 トポロジ マップに表示させる項目を選択します。

- [ラベル（Labels）]：デバイスに関連するラベル（デバイス名など）。
- [リンク（Links）]：デバイス間のそれぞれのリンク。
- [Aggregated Links]：複数の基本的リンクを表すリンク。これらは点線で示されます。
- [デバイス ファミリ（Device Families）]：トポロジ マップに表示されるデバイス（ルータやワイヤレス コントローラなど）。
- [障害（Faults）]：チェックボックスをオフにして、障害情報すべてを非表示にします。すべてのアラームを表示するにはチェックボックスをオンにします。または、特定の重大度以上の障害のみを表示するには、スライダーを使用します。

ステップ 4 [表示（Show）] ダイアログを閉じます。選択内容がトポロジ マップに適用されます。

大規模なトポロジ マップの特定のセクションを隔離する

トポロジマップに何千ものデバイスが表示される場合は、特定のデバイスまたはデバイスセットのみを重点的に扱うことができます。[概要（Overview）]ペインにはトポロジマップ全体が縮小サイズで表示されるので、そこから大きなトポロジマップ内の表示させたい領域を選択できます。また、トポロジ マップ内の要素のアラーム ステータスも見やすく表示されます。

ステップ 1 トポロジ ツールバーで [概要（Overview）] アイコンをクリックします。トポロジ マップの右下に [概要（Overview）] ペインが表示され、次の項目が表示されます。

- ドット：ネットワークの任意の要素を示します。ドットの色は、ネットワーク要素に関連するアラームの重大度を示します。
- 実線：リンクを示します。線の色は、関連するアラームの重大度を示します。
- 青い四角：選択された領域を表します。四角内の領域がマップ ペインに表示されます。四隅のハンドルを使用して、選択領域のサイズを変更できます。
- パン モード カーソル：選択領域内に表示されるカーソル。このカーソルを使って選択領域を移動すると、マップ ペインのさまざまな要素を参照できます。
- ズーム モード カーソル：選択領域の外に表示されます。このカーソルを使用して、新しい選択領域を定義したり、既存の選択領域を拡大します。

ステップ 2 トポロジ マップに表示したい領域でマウスをドラッグし、四角形で囲みます。

ステップ 3 右上隅にある [x] をクリックして [概要（Overview）] ペインを閉じます。

デバイスの詳細情報の取得

トポロジ マップでドリルダウンすると、デバイスに関する詳細を得ることができます。

ステップ 1 トポロジ マップで該当するデバイスをクリックします。ポップアップが開き、デバイスの基本情報とアラーム情報が表示されます。

ステップ 2 [360 度表示（View 360）] をクリックすると、[デバイス 360（Device 360）] ビューにアクセスしてデバイスの詳細情報を表示できます。

詳細については、[デバイス360度ビュー（Device 360° View）] からのデバイス詳細の取得 （1121 ページ）を参照してください。

リンクの詳細情報の取得

トポロジ マップでのリンクの表示方法によって、リンクに関する一部の情報が示されます。

- 実線は、トポロジ マップ内の 2 つの要素間で検出されたリンクのタイプを表します。
- 点線は、トポロジ マップに手動で追加された管理対象外リンクを表します。
- 鎖線は、集約リンクを表します（[Show] ポップアップで [Aggregated Links] を選択した場合）。
- アラーム重大度バッジは、現在リンクに影響を及ぼしている重大度が最も高いアラームを示します。

トポロジマップで必要なリンクをクリックすると、ドリルダウンしてリンクに関する詳細情報を取得できます。

- 単純なリンクの場合、ポップアップにはリンク タイプおよびリンクの起点と終点が表示されます。
- 集約リンクの場合、ポップアップにはすべての基本的リンクを含むテーブルが表示されます。

デバイスおよびリンクの障害情報の表示

デバイスまたはリンクにアラームが関連付けられいる場合は、トポロジ マップのデバイス アイコンまたはリンクにアラーム バッジが表示されます。アラーム バッジの色はアラームの重大度に対応しており（マイナー（黄色）、メジャー（オレンジ）、クリティカル（赤））、[Alarm Browser] に表示されるアラームと一致しています。

グループの場合、アラーム バッジは、いずれかのグループ メンバーに対して現在アクティブな最も重大度が高いアラームを表します。

リンク ダウンなどのリンク関連のアラームは、トポロジ マップの関連リンクにアラーム バッジを生成します。リンク アップ アラームが受信されると、リンク アラームおよび対応するバッジがクリアされます。

詳細については、「アラーム重大度アイコン （364 ページ）」を参照してください。

ネットワーク トポロジ マップのレイアウトの変更

トポロジマップ内にデバイスおよびその他のネットワーク要素（ラベル、ノード、それらの間の接続など）を配置する方法を指定することができます。。

- [対称（Symmetrical）]（デフォルト）：トポロジ固有の対称性を維持します。これによって隣接ノードがさらに接近するので、ノードが重なるのを防ぐことができます。
- [円形（Circular）]：ネットワーク要素を円形に配置し、ネットワーク トポロジ固有のクラスタを強調表示します。
- [階層（Hierarchical）]：依存関係および要素間のフローが維持されるようにします。
- [増分（Incremental）]：特定要素の相対的な位置を維持し、新たに追加された要素の位置を調整します。ノード/リンクを再描画して重なりを解消するには、このレイアウトを使用します。

マップ レイアウトを選択すると、要素が適宜整列されます。また、要素をドラッグ アンド ドロップしてレイアウトを手動で変更することもできます。レイアウトを変更した後、それを保存すると、次回に [ネットワークトポロジ（Network Topology）] ウィンドウを開くときにレイアウトが保持されます。将来の Web GUI セッション用にネットワーク トポロジ マップのレイアウトを保存する （188 ページ）を参照してください

ステップ 1 左側のサイドバーから、[マップ（Maps）] > [トポロジマップ（Topology Maps）] >[ネットワークトポロジ（Network Topology）] の順に選択します。

ステップ 2 [デバイスグループ（Device Groups）] ボタンをクリックし、必要なデバイス グループを選択します。

ステップ 3 トポロジ ツールバーの [レイアウト（Layout）] アイコンをクリックし、必要なレイアウトを選択します。トポロジ マップの表示が適切に調整されます。

将来の Web GUI セッション用にネットワーク トポロジ マップのレイアウトを保存する

Prime InfrastructurePrime Infrastructure では、現在のブラウザ セッションのレイアウト変更や選択内容のみが保持されます。したがって、必要に応じてトポロジマップのレイアウトを変更した後には、トポロジマップを毎回手動で再配置しなくても済むように、レイアウトを保存することを強くお勧めします。

（注） レイアウトは、選択したデバイス グループに対してのみ保存されます。

[トポロジ（Topology）] ツールバーで **[レイアウト（Layout）] > [手動レイアウトを保存（Save Manual Layout）]** を選択します。**[レイアウト（Layout）] > [手動レイアウトのロード（Load Manual Layout）]** を選択することにより、いつでもレイアウトをリロードできます。

手動レイアウトを保存した後にデフォルトのシステム レイアウトに戻す場合は、手動レイアウトを削除する必要があります。**[レイアウト（Layout）] > [手動レイアウトを削除（Delete Manual Layout）]** を選択します。

ネットワーク トポロジ マップでのクロック同期ネットワークの表示

同期イーサネット（Sync-E）または Precision Time Protocol（PTP）によるクロック同期がネットワーク内のデバイスに設定されている場合、クロック同期ネットワークをトポロジマップ上に表示できます。

- Sync-E オーバーレイには、プライマリ クロックと、各デバイスのプライマリおよびセカンダリ クロック入力を含め、Sync-E ネットワークのトポロジと階層が表示されます。これにより、任意の Sync-E 対応デバイスからプライマリ クロックまでのクロック信号またはプライマリ クロックから Sync-E 対応デバイスまでのクロック信号をトレースできます。
- PTP オーバーレイには、クロック同期ツリー トポロジ、PTP 階層、ツリー上の各デバイスのクロック ロール（マスター、境界、スレーブ、またはトランスペアレント）が表示されます。

ステップ 1 左側のサイドバーから、**[マップ（Maps）] > [トポロジ マップ（Topology Maps）] > [ネットワーク トポロジ（Network Topology）]** の順に選択します。

ステップ 2 [デバイス グループ（Device Groups）] ボタンをクリックし、必要なデバイス グループを選択して、[ロード（Load）] をクリックします。

ステップ 3 トポロジ ルーツバーで [表示（Show）] をクリックし、[テクノロジー（Technology）] を選択します。各テクノロジーでマップに表示される内容についての説明を表示するには、疑問符アイコンをクリックします。

（注） [テクノロジー（Technology）] を選択する前に、[帯域幅使用率（Bandwidth Utilization）] オプションを無効にする必要があります。

ステップ 4 対象のテクノロジーを選択し、[OK] をクリックします。

クロック同期ネットワークが、マップ内の既存のネットワークの上にオーバーレイとして表示されます。右下の凡例に、選択したテクノロジーのマップで使用されている表記が説明されます。

（注） 別のデバイス グループを選択すると、テクノロジー オーバーレイが削除されます。

イメージ ファイルとしてトポロジ マップを保存する

トポロジ マップ全体、またはトポロジ マップから選択したオブジェクトをイメージ ファイルとして保存できます。これにより、特定の状態にあるトポロジマップのコピーを保存できるので、将来、トポロジに対して複数の変更を行う際にそれを基準として使用できます。

イメージ ファイルとしてトポロジ マップを保存するには、次の手順を実行します。

ステップ 1 **[マップ（Maps）] > [トポロジ マップ（Topology Maps）] > [ネットワーク トポロジ（Network Topology）]** を選択します。

ステップ 2 [デバイスグループ（Device Groups）] ボタンをクリックし、必要なデバイス グループを選択して、[ロード（Load）] をクリックします。

ステップ 3 必要に応じて、トポロジ マップの内容やレイアウトを変更します。

ステップ 4 トポロジ ツールバーの [イメージの保存（Save Image）] アイコンをクリックします。

ステップ 5 [イメージの保存（Save Image）] ドロップダウンリストから、保存するイメージのファイルタイプを選択します。

ローカルの Temp フォルダにイメージが保存されます。

第 10 章

ワイヤレス サイト マップの使用

この章は、次の内容で構成されています。

- 次世代ワイヤレス サイト マップの紹介 （191 ページ）
- サイト マップの使用 （193 ページ）
- マップ プロパティの編集 （199 ページ）
- 屋外領域の設定 （200 ページ）
- ビルディングの設定 （202 ページ）
- フロア領域のモニタ （204 ページ）
- フロア領域の設定 （208 ページ）
- さまざまなフロア要素の表示設定 （210 ページ）
- マップ プロパティの設定 （219 ページ）
- フロア要素の編集 （219 ページ）
- フロア ツールの使用 （234 ページ）
- モニタリング ツールの使用 （234 ページ）
- プランニング モードの使用 （244 ページ）
- データのフィルタリング （259 ページ）
- プランニング モードを使用したワイヤレス ワイト マップでの AP の配置 （263 ページ）
- 自動階層作成を使用したワイヤレス サイト マップの作成 （268 ページ）
- ワイヤレス サイト マップでの Google Earth マップの表示 （271 ページ）
- 地理座標を使用したワイヤレス サイト マップ上の屋外位置への AP のグループ化 （272 ページ）

次世代ワイヤレス サイト マップの紹介

Cisco Prime Infrastructure には、リリース 3.2 から次世代のワイヤレス サイト マップが導入されています。次世代のサイト マップは、より大きく詳細なマップを提供する新しいユーザ インターフェイスにより強化されています。

次世代ワイヤレス サイト マップにアクセスするには、**[マップ（Maps）] > [ワイヤレスマップ（Wireless Maps）] > [サイトマップ（新）（Site Maps (New)）]** を選択します。

[ドメインサイドバー（Domain Sidebar）] メニューには、キャンパス、ビルディング、屋外区域、およびフロアがツリー ビューで表示されます。ツリー ビューでキャンパス、ビルディング、屋外区域、またはフロアをクリックすると、対応するマップがさまざまなパネルとともに右側のペインに表示されます。

関連トピック

サイト マップの使用 （193 ページ）
マップ プロパティの設定 （219 ページ）
屋外領域の設定 （200 ページ）
ビルディングの設定 （202 ページ）
フロア領域の設定 （208 ページ）
フロア要素の編集 （219 ページ）
モニタリング ツールの使用 （234 ページ）
プランニング モードの使用 （244 ページ）
データのフィルタリング （259 ページ）

ワイヤレス サイト マップの構成方法

ワイヤレス サイト マップには、事前に設定された階層があります。

- **キャンパス**はマップ階層の最上位レベルです。キャンパスは単一の事業拠点またはサイトを表します。キャンパスは、1 つ以上のフロア領域を持つ少なくとも 1 つのビルディングと、多数の外部領域から構成されます。
- **ビルディング**はキャンパス内の単一の構造物を表し、組織に関連するフロア領域マップに役立ちます。1 つのキャンパス マップに必要な数だけビルディングを追加できます。ビルディングでは、1 つまたは複数のフロアとそれに関連する外部領域を使用します。ビルディングはキャンパス マップにのみ追加できます。
- **フロア領域**は、キュービクル、壁に囲まれたオフィス、配線クローゼットなどで構成されるビルディング内にあります。フロア領域をビルディング マップのみに追加できます。作成する各ビルディング マップには、最大 100 のフロアを追加できます。
- **地下レベル**はフロア領域と同じですが、フロア領域と逆の順序で番号が付けられています。地下はビルディング マップにのみ追加できます。100 のフロア領域に加え、作成する各ビルディング マップには最大 100 の地下レベルを追加できます。
- **外部領域**は外部の場所です。外部領域は通常、ビルディングに関連付けられていますが、ビルディングと同レベルでキャンパス マップに直接追加する必要があります。キャンパス マップには必要な数だけ外部領域を追加できます。

Cisco Prime Infrastructure にはデフォルトのキャンパス マップが 2 つ付属しています。

- [システムキャンパス（System Campus）]：デフォルトのキャンパス マップです。新しいビルディング、フロア、地下または外部領域を作成するが、キャンパス マップの一部として作成しない場合、それらの従属マップは自動的に [システムキャンパス（System Campus）] マップの子として作成されます。

- [未割り当て（Unassigned）]：他のマップ（[システムキャンパス（System Campus）] を含む）に割り当てられていないすべてのネットワーク エンドポイントとホストのデフォルト マップです。

ワイヤレス サイト マップ内で使用するためのイメージ ファイルの準備に関するガイドライン

- PNG、JPEG、GIF など、ラスタ イメージ ファイル形式に保存するグラフィック アプリケーションを使用します。
- フロアおよび屋外領域マップの場合、Cisco Prime Infrastructure では、PNG、JPEG、GIF、CAD ベクター形式（DXF および DWG）などのビットマップ イメージを使用できます。
- 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。
- ワイヤレス フロア プラン マップで使用されるイメージでサポートされる最大寸法は次のとおりです。
  - PNG イメージ: 2万ピクセル (15000 ピクセル)。
  - JPG イメージ: 2万ピクセル (2万ピクセル)。
- インポートする前に、サイトの水平および垂直の寸法をフィートまたはメートル単位で収集します。これにより、インポート時にこれらの寸法を指定できます。
- キャンパス、ビルディング、フロア、または外部領域をメートル単位で入力する場合は、デフォルトのマップ測定単位をメートルに変更します。
- マップを作成したら、それらにネットワーク要素を割り当てることができます。この操作を手動で行うには、必要に応じて個々のデバイスを選択して、キャンパス、ビルディング、フロア、外部領域に割り当てます。ワイヤレス アクセス ポイントおよびアクセス コントローラの場合、組織のアクセス ポイントまたはワイヤレス アクセス コントローラの命名階層を使用してマップに自動的に追加できます。

サイト マップの使用

（注） リリース 3.1 以降では、サイトマップおよびグループの作成時に、'&<>"/ を除くすべての特殊文字を使用できます。

[マップ（Maps）] > [ワイヤレスマップ（Wireless Maps）] > [サイトマップ（新）（Site Maps (New)）] を選択して、このページにアクセスします。

[サイトマップ（Site Maps）] ページの左上隅にある [サイト階層（Site Hierarchy）] アイコンをクリックして、[ドメインナビゲータ（Domain Navigator）] メニューを表示または非表示にします。[ドメインナビゲータ（Domain Navigator）] メニューには、ツリー階層内のすべてのキャンパス、ビルディング、フロア、および屋外領域が一覧表示されます。

ツリー階層を検索することで、キャンパス、ビルディング、屋外領域、またはフロアをすばやく見つけることができます。ツリー階層を検索するには、[ドメインナビゲータ（Domain Navigator）] メニューの [検索（Search）] テキスト ボックスにサイト名を入力します。ツリー階層は、入力されたパラメータに基づいてフィルタリングされます。検索結果をクリックすると、対応するマップと、右ペインにさまざまなサイト要素を含んでいるサービス ドメイン パネルが表示されます。たとえば、ドメイン ナビゲータ メニューでキャンパスを選択すると、右側のペインには対応するキャンパス マップとさまざまなサービス ドメイン パネルが表示されます。これらのサービス ドメイン パネルには、特定のキャンプのビルディング、屋外領域、フロア、AP、クライアント、重要な無線の数が表示されます。

（注）

- ドメイン ナビゲータ メニューの検索結果には、特定のフロアが属するビルディングの階層は表示されません。右ペインに詳細を表示するには、フロア アイコンをクリックします。
- 背景イメージが存在しない場合、サイト マップには、デフォルトでは geo 座標が (0, 0) であるため、大西洋海を介して相互にスタックされた建物が表示されます。
- フロアに直接表示されるデータとサービス ドメイン パネルに表示されるデータには一時的な違いがあります。

これらの操作は、**[サイトマップ（Site Maps）]** ページで実行できます。

- サイトの追加 （194 ページ）
- サイトの削除 （195 ページ）
- サイトの更新 （195 ページ）
- マップ アーカイブのインポート
- マップ アーカイブのエクスポート （197 ページ）
- CSV 形式での一括 AP のインポート （197 ページ）
- CSV 形式での一括 AP のエクスポート （198 ページ）

サイトの追加

ステップ 1 **[マップ（Maps）] > [ワイヤレスマップ（Wireless Maps）] > [サイトマップ（新）（Site Maps (New)）]** を選択して、このページに移動します。

ステップ 2 [ドメインナビゲータ（Domain Navigator）] で、サイト マップに移動します。使用可能なサイト パネルが右ペインに表示されます。

ステップ 3 [サイト（Sites）] ページの右上隅にある [サイトの追加（Add Site）] をクリックします。[新しいサイト（New Site）] ウィンドウが表示されます。すべての必須フィールドは黄色の背景で表示されます。

ステップ 4 [サイト名（Site Name）] テキスト ボックスにサイトの名前を入力します。サイト名には、最大で 32 文字まで使用できます。

ステップ 5 [連絡先（Contact）]テキスト ボックスに、電子メール アドレスを入力します。連絡先の詳細には、最大で 32 文字まで使用できます。

ステップ 6 [親のロケーショングループ（Parent Location Group）] ドロップダウンリストから親のロケーション グループを選択します。

ステップ 7 サイトマップをアップロードするには、[クリックしてファイルを選択するかまたはここにドラッグします（Click to select a file or drag it here）] をクリックします。サイト イメージ ファイルを参照するか、またはイメージ ファイルを [クリックしてファイルを選択するかまたはここにドラッグします（Click to select a file or drag it here）] 領域にドラッグ アンド ドロップします。

ステップ 8 [シビックロケーション（Civic Location）] テキスト ボックスにシビック ロケーションの詳細を入力します。[経度（Longitude）] と [緯度（Latitude）] のテキスト ボックスは、有効なシビック ロケーションの詳細を入力すると自動的に更新されます。

ステップ 9 [幅（Width）] と [長さ（Length）] のテキスト ボックスにサイトの実際の寸法を入力します。

ステップ 10 [保存（Save）] をクリックして、詳細を保存します。

サイトの削除

ステップ 1 **[マップ（Maps）] > [ワイヤレスマップ（Wireless Maps）] > [サイトマップ（新）（Site Maps (New)）]** を選択して、このページに移動します。

ステップ 2 [ドメインナビゲータ（Domain Navigator）] で、サイト マップに移動します。使用可能なサイト パネルが右ペインに表示されます。

ステップ 3 右側のペインのサイト パネルで、[削除（Delete）] をクリックします。

ステップ 4 [削除（Delete）] をクリックして、削除を確認します。

サイトの更新

ステップ 1 **[マップ（Maps）] > [ワイヤレスマップ（Wireless Maps）] > [サイトマップ（新）（Site Maps (New)）]** を選択して、このページに移動します。

ステップ 2 [ドメイン ナビゲータ（Domain Navigator）] から、サイト マップに移動します。使用可能なサイト パネルが右ペインに表示されます。

ステップ 3 [サイト（site）] パネルで、[編集（Edit）] をクリックします。

ステップ 4 [編集（Edit）] ウィンドウで、イメージ ファイルを含め、サイト属性を更新できます。

ステップ 5 **[保存（Save）]** をクリックします。

マップ アーカイブのインポート

ステップ 1 **[マップ（Maps）]** > **[ワイヤレスマップ（Wireless Maps）]** > **[サイトマップ（新）（Site Maps (New)）]** を選択して、このページに移動します。

ステップ 2 [ドメインナビゲータ（Domain Navigator）] で、サイト マップに移動します。使用可能なサイト パネルが右ペインに表示されます。

ステップ 3 [インポート（Import）] 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 4 [マップ アーカイブのインポート（Import Map Archive）] ウィザードが開きます。

- [形式の選択（Choose Format）] ページでは、次のマップ形式タイプのいずれかを選択できます。
  - **XML 形式**
  - **サードパーティ XML/Zip**

ステップ 5 [ファイルの選択（Select File）] ページで、[クリックしてファイルを選択するか、ここにドラッグ（Click to select file or drag it here）] をクリックしてインポートするマップの位置まで参照するか、またはマップ ファイルをドラッグして [クリックしてファイルを選択するか、ここにドラッグ（Click to select file or drag it here）] 領域にドロップします。zip 形式または tar 形式のいずれかのファイルをインポートできます。形式を理解するためにサンプルテンプレートをダウンロードするには、[サンプルテンプレートはここからダウンロードできます（Sample template can be downloaded here）] リンクをクリックします。

（注） リリース 3.4 以降、Prime Infrastructure はマップ アーカイブからのベクター形式の CAD イメージのインポートをサポートしています。

ステップ 6 [検証（Verify）] を選択します。「**サーバにファイルをアップロードしています。検証結果が出るまでお待ちください**」というメッセージが表示されます。検証が完了すると、マップ パス、メッセージ、およびステータスに関する情報と上書き情報を含む結果が表示されます。上書き、または無視することができます。

ステップ 7 [プロセス（Process）] をクリックします。マップのインポート プロセスを開始します。

[概要（Summary）] テーブルに **マップ パス**、**メッセージ**、および**ステータス**の情報が表示されます。[ステータス（Status）] 列の緑色のドットは、データベースへのインポートが成功したことを表します。赤色のドットは、マップのインポート中にエラーが発生したことを表します。

[表示（Show）] ドロップダウン リストから、[すべて（All）] または [クイック フィルタ（Quick Filter）] を選択し、[マップ パス（Map Path）] と [メッセージ（Message）] を使用して検索します。

ステップ 8 インポート プロセスが成功したら、[完了（Done）] をクリックします。
インポートされたマップが [サイト マップ（Site Maps）] ページの左側にあるサイドバーのメニューの [ドメイン ナビゲータ（Domain Navigator）] に表示されます。

マップ アーカイブのエクスポート

ステップ 1 **[マップ（Maps）] > [ワイヤレスマップ（Wireless Maps）] > [サイトマップ（新）（Site Maps (New)）]** を選択して、このページに移動します。

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 [マップ アーカイブのエクスポート（Export Map Archive）] ウィザードが開きます。

ステップ 4 [サイトの選択（Select Sites）]ページで、次のように設定します。マップ情報か、またはキャリブレーション情報のいずれをマップ アーカイブに含めるかを選択する必要があります。

- [マップ情報（Map Information）] : マップ情報をアーカイブに含めるには、[オン（On）]/[オフ（Off）] トグルを切り替えます。
- [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（On）]/[オフ（Off）] トグルを切り替えます。[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 ボタンかのいずれかを選択できます。[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。
- サイドバーのメニューの左側にある [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 5 [マップ アーカイブの生成（Generate Map Archive）] を選択します。「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 6 [Done] をクリックします。

CSV 形式での一括 AP のインポート

ステップ 1 **[マップ（Maps）] > [ワイヤレスマップ（Wireless Maps）] > [サイトマップ（新）（Site Maps (New)）]** を選択して、このページに移動します。

ステップ 2 ページの右上の隅にある [インポート（Import）] ドロップダウン リストから、[CSV での一括 AP（Bulk AP in CSV）] を選択します。

ステップ 3 [一括 AP のインポート（Import Bulk AP）] ウィザードが開きます。

ステップ 4 [CSV のアップロード（Upload CSV）] タブで、[ファイルの選択（Choose File）] をクリックし、インポートする CSV ファイルの位置まで参照します。サンプル テンプレートをダウンロードするには、[サンプル テンプレートはここからダウンロードできます（Sample template can be downloaded here）] リンクをクリックします。

ステップ 5 [概要（Summary）] タブをクリックし、CSV が正常にインポートされたかどうかを確認します。[概要（Summary）] テーブルには、**マップ パス**、**メッセージ**、および**ステータス**の情報が含まれています。

ステップ 6 [Done] をクリックします。

CSV 形式での一括 AP のエクスポート

ステップ 1 **[マップ（Maps）] > [ワイヤレスマップ（Wireless Maps）] > [サイトマップ（新）（Site Maps (New)）]** を選択して、このページに移動します。

ステップ 2 ページの右上の隅にある [エクスポート（Export）] ドロップダウン リストから、[一括 AP（Bulk AP）] を選択します。

[AP の一括エクスポート] ウィザードが開きます。

ステップ 3 [APの選択（Select APs）] ページには、使用可能なすべての AP が一覧表示されます。

- [検索パネル（Search Panel）] を使用して、エクスポートするアクセス ポイントを検索することができます。検索するには AP 名、MAC アドレス（イーサネットと無線）、または IP アドレスを使用し、[検索（Search）] をクリックします。
- 特定の屋外領域、サイト、キャンパス、またはフロアで使用可能な AP を選択できます。そのためには、次の手順を実行します。
  - [サイトの選択（Select Site）] テキスト ボックスをクリックし、対応する屋外領域、サイト マップ、キャンパス、またはフロアのチェック ボックスをオンにします。
  - [OK] をクリックします。[サイトの選択（Select Site）] フィールドに選択したサイトの詳細が表示されます。
  - [検索（Search）] をクリックします。選択したサイトで使用可能な AP が表示されます。
  - どのフロアにも割り当てられていない AP を含めるには、[未割り当てを含める（Select Site）] チェックボックスをオンにします。

ステップ 4 [表示（Show）] ドロップダウン リストから、[すべて（All）] または [クイック フィルタ（Quick Filter）] を選択し、[AP 名（AP Name）]、[MAC アドレス（MAC Address）]、[モデル（Model）]、[コントローラ（Controller）]、[ステータス（Status）]、または [フロア（Floor）] を使用してアクセス ポイントを検索します。

ステップ 5 1 つ以上の [AP 名（AP Name）] チェックボックスをオンにし、[フロアの割り当て（Assign Floor）] をクリックして、選択した AP をフロアに割り当てます。

ステップ 6 [フロアに割り当て（Assign To Floor）] をクリックし、AP を割り当てるフロアを [サイト（Sites）] ウィンドウで選択し、[OK] をクリックします。

ステップ 7 [CSV の生成（Generate CSV）] をクリックします。

CSV ファイルがエクスポートされます。

ステップ 8 [Done] をクリックします。

Geo マップのアクセス ポイントのインポート

ステップ 1 **[マップ（Maps）]** > **[ワイヤレスマップ（Wireless Maps）]** > **[サイトマップ（Site Maps）]** の順にクリックします。

ステップ 2 **[インポート（Import）]** > **[GeoマップのAP（APs for GeoMap）]** の順にクリックします。

ステップ 3 インポートするファイル（サンプル CSV ファイルがダウンロードできます）をクリックまたはドラッグし、[概要（Summary）] をクリックします。

ステップ 4 [Done] をクリックします。

Geo マップのアクセス ポイントのエクスポート

ステップ 1 **[マップ（Maps）]** > **[ワイヤレスマップ（Wireless Maps）]** > **[サイトマップ（Site Maps）]** の順にクリックします。

ステップ 2 **[エクスポート（Export）]** > **[GeoマップのAP（APs for GeoMap）]** の順にクリックします。

ステップ 3 [APの選択（Select APs）] タブで、地理位置情報をエクスポートする AP を選択します。

ここには、Prime Infrastructure で管理されているコントローラに関連付けられている AP が一覧表示されます。[検索パネル（Search Panel）] を使用して、AP を AP 名、Mac アドレス、または IP で検索することもできます。

ステップ 4 [APの編集（Edit APs）] をクリックし、選択した AP の [経度（Longitude）] および [緯度（Latitude）] の値を編集します。

ステップ 5 [CSVの生成（Generate CSV）] をクリックして、CSV ファイルを生成します。

マップ プロパティの編集

ステップ 1 **[マップ（Maps）]** > **[ワイヤレスマップ（Wireless Maps）]** > **[サイトマップ（新）（Site Maps (New)）]** を選択して、このページに移動します。

ステップ 2 [サイト（Sites）] ページの右上の隅にある [ユーザ プリファレンス（User Preferences）] アイコンをクリックし、次のマップ プロパティを編集します。

- [測定の単位（Units of Measure）] : [測定の単位（Units of Measure）] ドロップダウン リストから [フィート（Feet）] または [メートル（Meters）] を選択し、マップの寸法測定を設定します。

- [壁の使用のキャリブレーション（Wall Usage Calibration）]：[壁の使用のキャリブレーション（Wall Usage Calibration）] ドロップダウン リストから [自動（Auto）]、[壁を使用（Use Walls）]、または [壁を使用しない（Do Not Use Walls）] を選択します。壁の使用のキャリブレーションは、Cisco Prime Infrastructure が壁の描画をヒートマップの計算の際に考慮するのに役立ちます。
- [フロア開始インデックス（Floor Start Index）]：[フロア開始インデックス（Floor StartIndex）] ドロップダウン リストから、[0] または [1] のいずれかのフロア レベルを選択します。
- [ネットワークからのマップの更新（Refresh Map from Network）]：オペレータがマップの更新を要求するたびに Cisco WLAN ソリューションをポーリングすることでマップを更新するには、Cisco Prime Infrastructure の [有効化（Enable）] オプション ボタンを選択します。保存されたデータベースからマップを更新するには、Cisco Prime Infrastructure の [無効化（Disable）] オプション ボタンを選択します。
- [高度なデバッグ モード（Advanced Debug Mode）]：Location Appliance と Cisco Prime Infrastructure がロケーション精度のテストポイント機能を使用できるようにするには、[有効化（Enable）] オプション ボタンを選択します。
- [ダイナミック ヒートマップの使用（Use Dynamic Heatmaps）]：ダイナミック ヒートマップを使用するには、[有効化（Enable）] オプション ボタンを選択します。ダイナミック ヒートマップを有効にすると、Cisco Prime Infrastructure は変更された RSSI 値を表すためにヒートマップを再計算します。
- [ダイナミック ヒートマップの AP 最小数（Minimum Number of APs for Dynamic Heatmaps）]：ダイナミック ヒートマップの計算に使用する AP の最小数をテキスト ボックスに入力します。AP の必須最小数は 3、AP の必須最大数は 10 です。
- [再計算頻度（時間）（Recomputation Frequency (hours)）]：ヒートマップ再計算頻度をテキスト ボックスに入力します。デフォルトの頻度は 6 時間です。最小頻度は 1 時間、最大頻度は 24 時間です。

ステップ 3 **[保存（Save）]** をクリックします。

屋外領域の設定

屋外領域マップをデータベースに追加しているかどうかに関係なく、Cisco Prime Infrastructure データベース内のキャンパス マップに屋外領域を追加できます。領域の寸法を定義し、それをデータベースに追加できます。Cisco Prime Infrastructure はワークスペースに合わせてマップのサイズを自動的に変更するため、マップを任意のサイズにできます。

関連項目

- 屋外領域の追加 （201 ページ）
- 屋外領域の削除 （202 ページ）
- 屋外領域の編集 （201 ページ）

屋外領域の追加

ステップ 1 **[マップ（Maps）] > [ワイヤレスマップ（Wireless Maps）] > [サイトマップ（新）（Site Maps (New)）]** を選択して、このページに移動します。

ステップ 2 屋外領域マップを追加するキャンパス ページの右上隅にある [屋外の追加（Add Outdoor）] をクリックします。[新しい屋外領域（New Outdoor Area）] ウィンドウが表示されます。すべての必須フィールドは黄色の背景で表示されます。

- [屋外領域名（Outdoor Area Name）]：屋外領域の名前を入力します。屋外領域名には、最大で 32 文字まで使用できます。
- [連絡先（Contact）]：電子メール ID または連絡先の名前を入力します。連絡先の詳細には、最大で 32 文字まで使用できます。
- [高さ（フィート）（Height (Feet)）]：屋外領域の高さをフィート単位で入力します。これは、後で [ユーザ設定（User Settings）] で変更できます。
- [タイプ（RFモデル）（Type (RF Model)）]：ドロップダウン リストから、[立方体および壁に囲まれたオフィス（Cubes And Walled Offices）]、[乾式壁オフィスのみ（Drywall Office Only）]、または [屋外オープンスペース（デフォルト）（Outdoor Open Space (default)）] を選択します。
- [イメージファイル名（Image File Name）]：[ファイルの選択（Choose File）] をクリックして、イメージを参照してファイルをアップロードします。PNG、GIF、または JPEG のイメージ形式のみをインポートできます。
- [シビックロケーション（Civic Location）]：屋外領域のロケーションの詳細を入力します。
- [緯度と経度（Longitude and Latitude）]：屋外領域の北西角の座標値を入力します。
- [寸法（フィート）（Dimensions (Feet)）]：実際の屋外領域の寸法を入力します。この寸法は後で [ユーザ設定（User Settings）] で変更できます。

屋外領域の編集

ステップ 1 **[マップ（Maps）] > [ワイヤレスマップ（Wireless Maps）] > [サイトマップ（新）（Site Maps (New)）]** を選択して、このページに移動します。

ステップ 2 [ドメインナビゲータ（Domain Navigator）] から、キャンパス サイト マップに移動します。使用可能な屋外領域パネルが右ペインに表示されます。

ステップ 3 編集する屋外領域パネルの上にマウスのカーソルを合わせ、[編集（Edit）] アイコンをクリックします。

ステップ 4 [屋外領域の編集（Edit Outdoor Area）] ウィンドウで、イメージを含む屋外領域の属性を変更します。

ステップ 5 **[保存（Save）]** をクリックします。

屋外領域の削除

ステップ 1 **[マップ（Maps）] > [サイトマップ（新）（Site Maps (New)）]** を選択します。

ステップ 2 [ドメインナビゲータ（Domain Navigator）] から、キャンパス サイト マップに移動します。使用可能な屋外領域パネルが右ペインに表示されます。

ステップ 3 削除する屋外領域パネルの上にマウスのカーソルを合わせ、[削除（Delete）]アイコンをクリックします。

ステップ 4 [削除（Remove）] をクリックして、削除を実行します。

ビルディングの設定

ビルディングはキャンパスマップにのみ追加できます。作成したキャンパスマップにビルディングを追加しないと、Cisco Prime Infrastructure によってデフォルトのシステム キャンパス マップに自動的に追加されます。

関連項目

- 建物の追加 （203 ページ）
- ビルディングの編集 （204 ページ）
- ビルディングの削除 （204 ページ）

建物の 3D ビューの使用

Cisco Prime Infrastructure では、建物内のすべてのフロアを 3D ビューで表示できます。そのためには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**[マップ（Maps）] > [ワイヤレスマップ（Wireless Maps）] > [サイトマップ（Site Maps）]** の順にクリックします。	
ステップ 2	**[キャンパス（Campus）] > [建物（Building）]** に移動します。	デフォルト ビューは [建物の3Dビュー（Building 3D View）] なので、選択された建物内のフロアが表示されます。
ステップ 3	各フロアの情報バーで、右の情報を確認します。	• フロア名（Floor Name） • AP の数 • ワイヤレスクライアントの数（Number of Wireless Clients）

	コマンドまたはアクション	目的
		• クリティカルな無線の数（Number of Critical Radios）
ステップ 4	フロアの詳細を表示するには、そのフロアの情報バーで [詳細（Details）] アイコンをクリックします。	
ステップ 5	[編集（Edit）] アイコンをクリックすると、[フロア名（Floor Name）]、[連絡先（Contact）]、[フロア番号（Floor Number）]、[フロアの高さ（Floor Height）]、および [モデルタイプ（Model Type）] などのフロアの詳細を編集できます。	
ステップ 6	フロアを削除するには、[削除（Delete）] アイコンをクリックします。	

建物の追加

ステップ 1 **[マップ（Maps）]** > **[ワイヤレスマップ（Wireless Maps）]** > **[サイトマップ（新）（Site Maps (New)）]** を選択して、このページに移動します。

ステップ 2 この建物を追加するキャンパス ページの右上隅にある [建物の追加（Add Building）] をクリックします。[新しい建物（New Building）] ウィンドウが表示されます。すべての必須フィールドは黄色の背景で表示されます。

- [建物名（Building Name）]：建物の名前を入力します。同じキャンパスマップに追加する他のビルディンの名前に対して一意の名前を指定する必要があります。建物名には、最大で 32 文字まで使用できます。
- [連絡先（Contact）]：電子メール ID または連絡先の名前を入力します。連絡先の詳細には、最大で 32 文字まで使用できます。
- [フロア数（Num.Floors）]：1 階を含む建物の階数を入力します。
- **[地下数地下数**—建物の地下数を入力します。
- [シビックロケーション（Civic Location）]：建物のロケーション情報を入力します。
- [緯度と経度（Longitude and Latitude）]：建物の北西角の座標を入力します。
- [寸法（フィート）（Dimensions (Feet)）]：建物の実際の寸法を入力します。後で [ユーザ設定（User Settings）] で寸法を変更できます。

建物を配置するには、建物をフロアにドラッグ アンド ドロップして建物を配置します。

ビルディングの編集

ステップ 1 **[マップ（Maps）] > [ワイヤレスマップ（Wireless Maps）] > [サイトマップ（新）（Site Maps (New)）]** を選択して、このページに移動します。

ステップ 2 [ドメインナビゲータ（Domain Navigator）] から、キャンパス サイト マップに移動します。使用可能なビルディング パネルが右ペインに表示されます。

ステップ 3 編集するビルディング パネルの上にマウスのカーソルを合わせ、[編集（Edit）] アイコンをクリックします。

ステップ 4 [ビルディングの編集（Edit Building）] ウィンドウで、ビルディングの属性を編集します。

ステップ 5 **[保存（Save）]** をクリックします。

ビルディングの削除

ステップ 1 **[マップ（Maps）] > [ワイヤレスマップ（Wireless Maps）] > [サイトマップ（新）（Site Maps (New)）]** を選択して、このページに移動します。

ステップ 2 [ドメインナビゲータ（Domain Navigator）]から、ビルディング マップに移動します。使用可能なビルディング パネルが右ペインに表示されます。

ステップ 3 削除するビルディングの上にマウスのカーソルを合わせ、[削除（Delete）] アイコンをクリックします。

ステップ 4 [削除（Remove）] を確認して、削除を実行します。

（注） ビルディングを削除すると、そのコンテナマップもすべて削除されます。削除されるマップのAPが、未割り当ての状態に移行します。

フロア領域のモニタ

[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。

- [マップ上で検索（Search on map）]：検索機能を使用して、AP、クライアント、不正 AP などの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。
- [ズームイン/ズームアウト（Zoom in and out）]：ズームのレベルは画像の解像度に依存します。高解像度の画像の場合、より高倍率のズーム レベルを使用できます。さまざまなスケールでマップの表示状態を変えるたびにズーム レベルが変わり、表示が詳細になった

り、広範になったりします。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。

- [ズームイン（Zoom In）]：マップの詳細を表示するには、ズームインする必要があります。マップ左側のズーム バーを使用してこれを操作できます。マップの左上にあるズームイン（+）アイコンをクリックします。ある場所を中心にズームインするには、その場所をダブルクリックします。キーボードを使用してズームインしている場合は、+ 記号をクリックします。マウスを使用している場合は、マウス スクロール ホイールを使用してズームインします。

- **[ズームアウト（Zoom Out）]**：マップを広い範囲で表示するには、ズームアウトする必要があります。ズームアウトするには、マップの左上にあるズームアウト（-）アイコンをクリックします。キーボードを使用してズームアウトしている場合は、- 記号をクリックします。マウスを使用している場合は、マウス スクロール ホイールを使用してズームアウトします。

- [ヘルプを参照（Get Help）]：次世代のマップ アイコンを表示するには、マップの左側にある [ヘルプを参照（Get Help）]（i）記号をクリックします。次の表に、次世代マップ アイコンを示します。

表 *18*：次世代マップ アイコン

アイコン	説明
アイコン	
	802.11 タグ
	不正 AP
	アドホック不正
	不正クライアント
	干渉
	wIPS攻撃

アイコン	説明
	GPS マーカー
	チョークポイント
	WiFi TDOA レシーバ
	サービス
AP Status	
	不明（Unknown）
	Critical（重大）
	Major（やや重大）
	Minor（比較的重大でない）
	警告
	Information
	Ok
無線ステータス	

アイコン	説明
	関連付けなし
	Unreachable
	管理者無効
	Down
	マイナーな障害
	Ok
クライアント（RSSI/SNR 別）	
	使用不可
	Excellent
	Good
	可
	不良
A P モード	
A	Autonomous
L	[ローカル（Local）]

アイコン	説明
M	モニタ（Monitor）
F	FlexConnect
R	不正検出
S	スニファ
B	Bridge
C	SE-Connect
Se	センサー
無線帯域/モード	
a	802.11 a/n/ac（5GHZ）
b	802.11 b/g/n（2.5GHZ）
n	802.11 a/b/g/n（2.4GHZ）
m	XOR(モニタモード)

関連項目

- FlexConnect グループおよび CCKM

フロア領域の設定

キャンパスマップに追加済みのビルディングにフロアと地下領域を追加できます。フロアを追加する際は、次のガイドラインに従います。

- ビルディング マップにはフロアと地下領域のみを追加できます。
- 追加できるフロアと地下領域の最大数は、キャンパスマップにビルディングを追加したときに指定したフロアと地下領域の数です。これらを間違って入力した場合は、まずビルディング マップを編集してからフロア マップをアップロードする必要があります。

関連項目

- FlexConnect グループおよび CCKM
- FlexConnect グループおよびローカル認証

ビルディングへのフロア領域の追加

ステップ 1 **[マップ（Maps）]** > **[ワイヤレスマップ（Wireless Maps）]** > **[サイトマップ（新）（Site Maps (New)）]** を選択して、このページに移動します。

ステップ 2 **[ドメインナビゲータ（Domain Navigator）]** の左メニューで、フロア マップを追加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 ページの右上にある [フロアの追加（Add Floor）] をクリックします。

[新しいフロア（New Floor）] ウィンドウが表示されます。すべての必須フィールドは黄色の背景で表示されます。

- [フロア名（Floor）]：フロア名を入力します。 フロア名には、最大で 32 文字まで使用できます。
- [連絡先（Contact）]：連絡先の名前または電子メール ID を入力します。連絡先の詳細には、32 文字まで使用できます。
- [フロア数（Floor Number）]：ドロップダウン リストから、フロア数を選択します。
- [フロアの高さ（Floor Height）]：フロア間の高さをフィート単位で入力します。
- [タイプ（RFモデル）（Type (RF Model)）]：フロアまたは地下の RF モデル。選択したモデルは、フロアまたは地下領域のワイヤレス信号強度、ヒートマップ、その他のワイヤレス関連機能の計算に使用されます。
- [イメージファイル名（Image File Name）]：[ファイルの選択（Choose File）] をクリックして、アップロードするフロア マップを選択します。フロア マップのサイズは自動的に計算されて表示されます。Cisco Prime Infrastructure では、PNG、JPEG、GIF、CAD ベクター形式（DXF および DWG）などのビットマップ イメージを使用できます。

  （注） CAD イメージのレイヤをフィルタするには、フロア マップに移動し、**[ツール（Tools）]** > **[CADレイヤの表示/非表示（Show/Hide CAD Layers）]** の順にクリックします。

- [シビックロケーション（Civic Location）]：フロアのロケーション情報を入力します。経度、緯度、およびロケーション情報は、入力された有効なシビック ロケーションごとに更新されます。
- [緯度と経度（Longitude and Latitude）]：北西角の座標を入力します。
- [寸法（フィート）（Dimensions (Feet)）]：幅と高さの実際のサイズを入力します。サイズは、後で [ユーザ設定（User Settings）] で変更できます。
- [位置（フィート）（Position (Feet)）]：水平位置および垂直位置を入力します。水平位置は、フロア領域の左上隅からキャンパス マップの左端までの距離です。垂直位置は、フロア領域の左上隅からキャンパス マップの上端までの距離です。これらの寸法をフィートまたはメートル単位で入力できます。これを変更すると、マップ上の経度、緯度、およびロケーションのアイコンが更新されます。

ステップ 4 **[保存（Save）]** をクリックします。

さまざまなフロア要素の表示設定

さまざまなフロア要素を設定するには、フロアの右上隅にある [画面設定（Display Settings）] アイコンをクリックします。フロア マップが次のパネルとともに右側のペインに表示されます：[アクセスポイント（Access Point）]、[メッシュ（Mesh）]、[802.11タグ（802.11 Tags）]、[オーバーレイオブジェクト（Overlay Objects）]、[クライアント（Clients）]、[不正AP（Rogue AP）]、[アドホック不正（Adhoc Rogue）]、[不正クライアント（Rogue Client）]、[干渉源（Interferers）]、[wIPS攻撃（wIPS Attacks）]、[MSE/CMX設定（MSE/CMX Settings）]、[マッププロパティ（Map Properties）]。

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。

関連項目

- アクセス ポイントの表示設定の構成 （210 ページ）
- メッシュ アクセス ポイントの表示設定の構成 （213 ページ）
- 802.11 タグの表示の設定を構成します。 （215 ページ）
- オーバーレイ オブジェクトの表示設定を構成します。 （215 ページ）
- クライアントの表示設定を構成します。 （216 ページ）
- 不正アクセス ポイントの表示設定の構成 （216 ページ）
- アドホックの悪党の表示設定を構成します。 （217 ページ）
- 不正クライアントの表示設定の構成 （217 ページ）
- 干渉源の表示設定の構成 （217 ページ）
- wIPS 攻撃の表示設定の構成 （218 ページ）
- MSE/CMX サイト マップ統合の表示設定の構成 （218 ページ）

アクセス ポイントの表示設定の構成

マップ上のすべての AP を表示するには、[アクセスポイント（Access Points）] チェックボックスをオンにします。[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、アクセス ポイントのフロア 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。
  - [名前（Name）]：AP 名が表示されます。
  - [AP MACアドレス（AP MAC Address）]：AP MAC アドレスが表示されます。
  - [コントローラIP（Controller IP）]：AP が接続されている Cisco WLC の IP アドレスが表示されます。

- [無線MACチャネル（Radio MAC Channel）]：無線 MAC アドレスが表示されます。
- [チャネル（Channel）]：Cisco 無線のチャネル番号または [利用不可（Unavailable）]（アクセス ポイントが接続されていない場合）が表示されます。
- [TX Power]：現在の Cisco 無線の送信電力レベル（1 が高い）または [利用不可（Unavailable）]（アクセス ポイントが接続されていない場合）が表示されます。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 シリーズのアクセス ポイントでは 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。
- [Tx Power（dBm）]：AP 内のすべての無線の無線周波数（RF）電源がデシベル（dBm）で表示されます。

  （注） 無線がスキャンモードの場合または使用できない場合は、電力レベルに 0（ゼロ）が表示されます。
- [チャネルおよびTx Power（Channel and Tx Power）]：チャネルと送信電力レベルの両方が表示されます（アクセス ポイントが接続されていない場合は [利用不可（Unavailable）]）。
- [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くなったクライアントの割合が表示されます。接続されていないアクセス ポイントの場合は [利用不可（Unavailable）]、モニタ専用モードのアクセス ポイントの場合は [モニタ専用（MonitorOnly）] と表示されます。
- [MACアドレス(MAC Addresses)]：アクセス ポイントがコントローラに関連付けられているかどうかにかかわらず、アクセス ポイントの MAC アドレスが表示されます。
- [名前（**Names**）]：アクセス ポイント名を表示します。これはデフォルト値です。
- [コントローラIP（Controller IP）]：アクセス ポイントが関連付けられているコントローラの IP アドレス、または関連付けられていないアクセス ポイントの場合は [関連付けなし（Not Associated）] が表示されます。
- [使用率（Utilization）]：関連付けられているクライアント デバイスによって使用されている帯域幅のパーセンテージ（受信、送信、およびチャネル使用率を含む）が表示されます。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。
- [プロファイル（Profiles）]：対応するオペレータが定義したしきい値の負荷、ノイズ、干渉、カバレッジのコンポーネントが表示されます。超えていないしきい値には「OK（Okay）」、超えているしきい値には「問題（Issue）」、接続されていないアクセス ポイントには「使用不可（Unavailable）」を表示します。

  [プロファイルタイプ（Profile Type）] ドロップダウンリストから、[ロード（Load）]、[ノイズ（Noise）]、[干渉（Interference）]、[カバレッジ（Coverage）] を選択します。

- [CleanAirステータス（CleanAir Status）]：アクセス ポイントの CleanAir ステータス、および CleanAir がアクセス ポイントで有効になっているかどうかが表示されます。
- [平均電波品質（Average Air Quality）]：このアクセス ポイントの平均電波品質が表示されます。詳細には、帯域と平均電波品質が含まれます。
- [最小電波品質（Minimum Air Quality）]：このアクセス ポイントの最小電波品質が表示されます。詳細には、帯域と最小電波品質が含まれます。
- [平均および最小電波品質（Average and Minimum Air Quality）]：このアクセス ポイントの平均および最小電波品質が表示されます。詳細には、帯域、平均電波品質、および最小電波品質が含まれます。
- [関連付けられたクライアント（Associated Clients）]：関連付けられているクライアントの数、接続されていないアクセス ポイントの場合は [利用不可（Unavailable）]、モニタ専用モードのアクセス ポイントの場合は [モニタのみ（Monitor Only）] が表示されます。
- [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ラベル付けします。
- **[ブリッジ グループ名（Bridge Group Names）]**
- [アンテナ角度（Antenna Angle）]：すべての無線アンテナの方位角および垂直面が表示されます。

- [電波品質（Air Quality）]：[平均AQ（Average AQ）] または [最小AQ（Minimum AQ）] のいずれかを選択できます。アクセス ポイントのヒートマップ タイプを設定して、マップ上に選択した電波品質の詳細を表示できます。
- [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 カットオフの範囲は -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。
- [Mobility Expressの表示（Show Mobility Express）]：Mobility Express AP で管理される AP の表示を切り替えます。

AP の詳細はすぐにマップに反映されます。マップ上の AP アイコンの上にマウス カーソルを置くと、AP の詳細と RX ネイバー情報が表示されます。

関連項目

- AP のクイック ビュー （223 ページ）

メッシュ アクセス ポイントの表示設定の構成

（注） メッシュ オプションは、フロアに使用可能なメッシュ AP がある場合にのみ使用できます。

マップ上のすべてのメッシュ AP を表示するには、[メッシュ（Mesh）] チェックボックスを選択します。[メッシュ（Mesh）] パネルを展開して、次の設定を行います。

- [リンクラベル（Link Label）] : [リンクラベル（Link Label）] ドロップダウンリストから、メッシュ リンクのラベルを選択します。
  - **None**
  - **リンク SNR**
  - **パケット エラー率**
- [リンクの色（Link Color）] : [リンクの色（Link Color）] ドロップダウンリストから、メッシュ リンクの色を選択します。
  - **リンク SNR**
  - **パケット エラー率**

リンクのラベルおよび色の設定は、ただちにマップ上に反映されます。SNR と□パケット エラー レートの両方の値を同時に表示できます。

表 *19* : リンクの色 : *SNR* と *PER*

カラー	リンクの信号/ノイズ比（SNR）	パケット エラー率（PER）
グリーン	SNR が 25 dB を超えている（高い値）ことを表します。	PER が 1% 以下であることを表します。
オレンジ	SNR が 20 ～ 25dB（許容値）であることを表します。	PER が 1% より大きく 10% 未満であることを表します。
赤	SNR が 20dB を下回っている（低い値）ことを表します。	PER が 10% より大きいことを表します。

表 *20* : リンクの色 : *SNR* と *PER*

カラー	リンクの信号/ノイズ比（SNR）	パケット エラー率（PER）
グリーン	SNR が 25 dB を超えている（高い値）ことを表します。	PER が 1% 以下であることを表します。
オレンジ	SNR が 20 ～ 25dB（許容値）であることを表します。	PER が 1% より大きく 10% 未満であることを表します。

カラー	リンクの信号/ノイズ比（SNR）	パケット エラー率（PER）
赤	SNR が 20dB を下回っている（低い値）ことを表します。	PER が 10% より大きいことを表します。

表 *21 :* リンクの色：*SNR* と *PER*

カラー	リンクの信号/ノイズ比（SNR）	パケット エラー率（PER）
グリーン	SNR が 25 dB を超えている（高い値）ことを表します。	PER が 1% 以下であることを表します。
オレンジ	SNR が 20 ～ 25dB（許容値）であることを表します。	PER が 1% より大きく 10% 未満であることを表します。
赤	SNR が 20dB を下回っている（低い値）ことを表します。	PER が 10% より大きいことを表します。

メッシュ アクセス ポイントの表示をそれらの親との間のホップ数に基づいて変更するには、次の手順を実行します。

- [メッシュ親/子（Mesh Parent-Child）] 階層ビューで、[クイック選択（Quick Selections）] ドロップダウンリストから適切なオプションを選択します。オプションの説明は、次の表に記載されています。

  表 *22 : [Quick Selections]* オプション

フィールド	説明
Select only Root APs	マップ ビューにルートアクセスポイントだけを表示したい場合は、この設定を選択します。
Select up to 1st hops	マップ ビューに 1 番めのホップだけを表示したい場合は、この設定を選択します。
Select up to 2nd hops	マップ ビューに 2 番めのホップだけを表示したい場合は、この設定を選択します。
Select up to 3rd hops	マップ ビューに 3 番めのホップだけを表示したい場合は、この設定を選択します。
Select up to 4th hops	マップ ビューに 4 番めのホップだけを表示したい場合は、この設定を選択します。
Select All	マップ ビューにすべてのアクセス ポイントを表示したい場合は、この設定を選択します。

- [マップビューの更新（Update Map View）] をクリックして画面を更新し、選択したオプションでマップ ビューを表示します。

（注） マップ ビューの情報は Prime Infrastructure データベースから取得され、15 分ごとに更新されます。

（注） メッシュ階層ビューで、アクセス ポイントのチェックボックスをオンまたはオフにし、表示するメッシュ アクセス ポイントを変更することもできます。子アクセス ポイントを表示するには、ルート アクセス ポイントへの親アクセス ポイントを選択する必要があります。

802.11 タグの表示の設定を構成します。

選択、 **802.11 タグ** 地図上タグの場所の状態を表示するチェック ボックス。これらの設定を構成するのには、802.11 のタグ パネルを展開します。

- **全てのタグ表示** -を オン/オフのタグをマップ上に表示を切り替えます。
- **ラベルを表示** -地図表示したいタグ識別子を選択します。
  - **None**
  - **MAC アドレス**
  - **Asset Name**
  - アセット グループ
  - アセット カテゴリ

オーバーレイ オブジェクトの表示設定を構成します。

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。変えることができます、 **オン/オフ** 地図上に表示するオーバーレイ オブジェクトを切り替えます。

- **Coverage Areas**
- ロケーション リージョン
- 障害物
- レール
- **Markers**
- **GPS** マーカー
- チョークポイント

- **WiFi TDOA レシーバ**
- **Services**

クライアントの表示設定を構成します。

展開、 **クライアント** これらの設定を構成するパネル。

- **クラスター クライアントを表示** -オン、 **オン/オフ** 階マップにワイヤレス クライアントのクラスターを表示するを切り替えます。
- **色によってコード** -色コードを設定することによって、RSSI や sn 比情報でクライアントを表示できます: **RSSI** または **SNR** 。
- **ラベルを表示** -ドロップダウン リストから、マップに表示するクライアント識別子を選択。
  - **None**
  - **[ユーザ名（User Name）]**
  - **IP Address**
  - **MAC アドレス**
  - **アセット名**
  - **アセット グループ**
  - **アセット カテゴリ**

（注） 自律 AP クライアント トラッキングは、Cisco MSE ではサポートされていません。

不正アクセス ポイントの表示設定の構成

[不正AP（Rogue AP）] パネルを展開して、次の設定を行います。

- [不正APクラスタの表示（Show Rogue APs Cluster）]：[オン/オフ（On/Off）] 切り替えをオンにすると、フロア マップ上にクラスタ内のすべての不正 AP が表示されます
- [不正APの影響範囲の表示（Show Rogue AP Zone of Impact）]：[オン/オフ（On/Off）] 切り替えをオンにすると、不正 AP の影響範囲が表示されます。不正による影響ゾーンは、不正 AP の送信電力と、不正 AP に関連付けられたクライアントの数により決まります。マップ上の円の不透明度は、重大度を示します。赤一色の円は、非常に強く影響を受けたゾーンを表します。

アドホックの悪党の表示設定を構成します。

展開、 **アドホック不正な** パネルのこれらの設定を構成するのには。

- **アドホック悪党クラスターを表示** -オン、 **オン/オフ** アドホックを表示を切り替えますクラスター内の APs のローグします。
- **不正な AP インパクト ゾーンを表示** -オン、 **オン/オフ** アドホック悪党 APs のインパクト ゾーンを表示するを切り替えます。

不正クライアントの表示設定の構成

マップ上のすべての不正クライアントを表示するには、[不正クライアント（Rogue Client）] チェックボックスをオンにします。[不正クライアント（Rogue Client）] パネルを展開して、次の設定を行います。

- [不正クライアントクラスタの表示（Show Rogue Clients Cluster）] : [オン/オフ（On/Off）] 切り替えをオンにすると、クラスタ内の不正クライアントが表示されます

マップ上の不正クライアントのクイック ビュー

フロア マップの [不正クライアント（Rogue Clients）] アイコンの上にマウス カーソルを置くと、不正クライアントのMACアドレスが表示されます。[不正クライアント（Rogue Clients）] アイコンをクリックすると、不正クライアントの詳細を右ペインに表示できます。

- 検出条件（Detected By）
- 状態（State）
- 関連付けられた不正 AP（Rogue AP）
- AP の検出（Detecting APs）
- First Seen
- Last Seen
- 前回の場所（Last Located）
- 最後のレポート（Last Reported）

干渉源の表示設定の構成

マップ上のすべての干渉源を表示するには、[干渉源（Interferers）] チェックボックスをオンにします。[干渉（Interferes）] パネルを展開して、次の設定を行います。

- [影響を受けるゾーンの表示（Show Zone of Impact）] : おおまかな干渉の影響領域を表示します。円の不透明度はその重大度を示します。赤一色の円は Wi-Fi 通信を妨害する可能性がある非常に強い干渉を表し、薄いピンク色の円は弱い干渉を表します。

wIPS 攻撃の表示設定の構成

[wIPS攻撃（wIPS Attacks）] パネルを展開して、以下を構成します。

- [wIPS攻撃クラスタの表示（Show wIPS Attack Cluster）] : [オン/オフ（On/Off）] 切り替えをオンにすると、マップ上にすべての wIPS 攻撃が表示されます。

MSE/CMX サイト マップ統合の表示設定の構成

サイト マップを Cisco モビリティ サービス エンジン（MSE）または Cisco Connected Mobile Experience（CMX）と統合するには、[MSE/CMX設定（MSE/CMX Settings）] パネルを展開します。

- [データを表示（Show Data）] ドロップダウンリストから、過去 2 分間から最大 24 時間の範囲で、Mobility Services Engine のデータを表示できます。このオプションは、Mobility Services Engine が Cisco Prime Infrastructure に存在する場合のみ表示されます。
- マップを Cisco MSE と統合するには、[MSE] オプション ボタンを選択し、[MSE 割り当ての変更（Change MSE Assignment）] をクリックします。

（注） 自律 AP クライアント トラッキングは、Cisco MSE ではサポートされていません。

1. [割り当て済み MSE（Assigned MSEs）] テーブルで、マップを同期化する必要がある Mobility Services Engine を選択します。
2. [同期（Synchronize）] をクリックすると、同期プロセスが完了します。
3. Mobility Services Engine の割り当ての変更を破棄するには、[キャンセル（Cancel）] をクリックします。

- マップを Cisco CMX と統合するには、[CMX] オプション ボタンを選択し、[CMX割り当ての変更（Change CMX Assignment）] をクリックします。

（注） 次世代マップ フロアから AP を削除する場合は、CMX フロア マップを再度エクスポートして、CMX から最新のアップデートを取得する必要があります。そうしないと、CMX は同じフロア プランと AP の位置を使用しているとみなしてデータを送信するため、フロア クライアント数と他のモビリティ エンティティとの間に不一致が生じます。

1. [割り当て済みCMX（Assigned CMXs）] テーブルで、マップを同期化する必要がある CMX を選択します。

2. [同期（Synchronize）] をクリックして、マップ データを Cisco CMX に同期させます。
3. Mobility Services Engine の割り当ての変更を破棄するには、[キャンセル（Cancel）] をクリックします。

（注） コントローラがインベントリから削除された場合は、MSE または CMX 内の対応するサイト マップを手動で再同期する必要があります。

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）] : データベースからマップ データを更新する頻度を設定する間隔ドロップダウンリストが提供されます。[自動更新（Auto Refresh）] ドロップダウンリストで、時間間隔を次から選択します : [なし（None）]、[1分（1 mins）]、[2分（2 mins）]、[5分（5 mins）]、および [15分（15 mins）]。

フロア要素の編集

フロア領域で使用可能な [編集（Edit）] オプションを使用して、さまざまなフロア要素を追加、配置、定義、描画、および拡張することができます。フロア領域の右上隅にある [編集（Edit）] をクリックして、次の操作を行います。

- 次のフロア要素の追加、配置、および削除。
  - アクセス ポイント
  - チョークポイント
  - WiFi TDOA レシーバ
- 次のオーバーレイの追加、編集、および削除。
  - カバレッジ エリア
  - 障害物
  - ロケーション リージョン
  - Rails
  - マーカー
  - GPS マーカー

関連項目

- AP の追加、配置、および削除 （220 ページ）
- チョーク ポイントの追加、配置、および削除 （223 ページ）
- WiFi TDOA レシーバの追加、配置、および削除 （225 ページ）
- カバレッジ領域の追加 （227 ページ）
- 障害物の作成 （228 ページ）
- ロケーション リージョンの作成 （229 ページ）
- レールの作成 （232 ページ）
- GPS マーカーの配置 （233 ページ）

AP の追加、配置、および削除

Cisco Prime Infrastructure は、カバレッジ領域マップ上の RF 信号の相対強度を示すマップ全体のヒートマップを計算します。ここでは、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 信号強度の近似値だけが表示されています。

アンテナ ゲインの設定はヒートマップおよびロケーションの計算には影響を与えません。アンテナ ゲインはアンテナ名に暗黙的に関連付けられます。このため、次の条件が適用されます。

- アンテナが Prime Infrastructure で「その他（Other）」として使用およびマークされている場合、そのアンテナはすべてのヒートマップとロケーションの計算で無視されます。
- アンテナが Prime Infrastructure で Cisco アンテナとして使用およびマークされている場合は、コントローラに設定されているゲインに関係なく、そのアンテナ ゲインの設定（Prime Infrastructure 上の内部値）が使用されます。

ステップ 1 **[マップ（Maps）] > [サイト マップ（新）（Site Maps (New)）]** を選択します。

ステップ 2 左側のサイドバー メニュー [ドメイン ナビゲータ（Domain Navigator）] から、該当するフロアを選択してフロア ビュー ページを開きます。

ステップ 3 このページの右上隅にある [編集（Edit）] をクリックします。

ステップ 4 [フロア要素（Floor Elements）] パネルで、[アクセス ポイント（Access Points）] の横にある [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すべてのアクセス ポイントがリストに表示されます。

- [APの追加（Add APs）] ページで、フロア領域に追加するアクセス ポイントのチェックボックスをオンにし、[選択項目の追加（Add Selected）] をクリックします。
- すべてのアクセス ポイントを追加するには、[すべて選択（Select All）] をクリックし、[選択項目の追加（Add Selected）] をクリックします。
- フロア領域に直接アクセス ポイントを割り当てるには、[+] をクリックします。
- 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。**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。フロア領域に追加するには [+] アイコンをクリックします。

ステップ 5 フロア領域にアクセス ポイントを割り当てた後、[APの追加（Add APs）] ウィンドウを閉じます。

ステップ 6 フロア マップに追加した各アクセス ポイントは、マップの右側に表示されます。アクセス ポイントは正しく配置する必要があります。

ステップ 7 [フロア要素（Floor Elements）] ペインで、[アクセスポイント（Access Points）] の横にある [位置（Position）] をクリックして、マップ上に正しく配置します。

- 各アクセス ポイントをクリックして適切な場所にドラッグするか、[選択したAPの詳細（Selected AP Details）] ページで x 座標と y 座標および AP の高さを更新します。アクセス ポイントをマップ上にドラッグすると、横（x）と縦（y）の位置がテキスト ボックスに表示されます。選択すると、アクセス ポイントの詳細が右ペインに表示されます。[選択したAPの詳細（Selected AP Details）] ページには次の情報が表示されます。
  - [3ポイントによる位置付け（Position by 3 points）]：フロア マップ上に 3 つのポイントを描画し、作成したポイントを使用して AP を配置できます。手順は次のとおりです。
    - [3ポイントによる位置付け（Position by 3 points）] をクリックします。
    - 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。ポップアップが表示されるので、最初のポイントまでの距離を設定します。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。
    - 2 番目と 3 番目のポイントを同様の方法で定義し、[保存（Save）] をクリックします。
  - [2つの壁による位置付け（Position by 2 Walls）]：フロア マップ上に 2 つの壁を定義し、定義した壁の間に AP を配置できます。これにより、2 つの壁の間の AP の位置を把握できます。これは、壁の間の AP の位置を把握するのに役立ちます。
    - [2つの壁による位置付け（Position by 2 Walls）] をクリックします。
    - 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。ポップアップが表示されるので、最初の壁までの距離を設定します。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。
    - 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 名が表示されます。
  - **AP モデル**—選択したアクセス ポイントのモデル タイプを示します。
  - [MACアドレス（MAC Address）]：MAC アドレスが表示されます。
  - [x]：マップの水平方向スパンをフィート単位で入力します。
  - [y]：マップの垂直方向スパンをフィート単位で入力します。

- [APの高さ（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。
- [アンテナ画像（Antenna Image）]：AP イメージが表示されます。
- [アンテナ方向（Antenna Orientation）]：アンテナ タイプに応じて、[方位角（Azimuth）] と [垂直面（Elevation）] の方向を度数で入力します。

（注）
- 内部アンテナを備えた AP の場合、[方位角（Azimuth）] と [垂直面（Elevation）] の値は、すべての無線に対して一斉にロックされます。つまり、1 つの無線の設定を変更すると、方向パラメータは他の無線にもコピーされます。
- 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、[方位角（Azimuth）] オプションは表示されません。

（注） AP 方位角、垂直面、および電力レベルの値を変更すると、ヒート マップとカバレッジの値に影響します。

ステップ 8 各アクセス ポイントの配置と調整が完了したら、[保存（Save）] をクリックします。

[Save] をクリックすると、アクセス ポイントのアンテナ ゲインが選択したアンテナに一致します。これにより、無線がリセットされる可能性があります。

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。

ステップ 9 [フロア要素（Floor Elements）] パネルで、[アクセスポイント（Access Points）] の横にある [削除（Delete）] をクリックします。
[APの削除（Delete APs）] ページが表示され、割り当てられ配置されているすべてのアクセス ポイントが一覧表示されます。

- 削除するアクセス ポイントのチェックボックスをオンにして、[選択項目の削除（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、[選択項目の削除（Delete Selected）] をクリックします。
- フロアからアクセス ポイントを直接削除するには、[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。フロア領域から削除するには、[削除（Delete）] アイコンをクリックします。

AP のクイック ビュー

フロア マップ上の AP アイコンの上にマウス カーソルを置くと、AP の詳細と Rx ネイバー情報が表示されます。

- [情報（Info）] を選択すると、次の AP の詳細が表示されます。
  - [関連付けられました（Associated）]：AP が関連付けられているかどうかを示します。
  - [名前（Name）]：AP 名が表示されます。
  - [MACアドレス（MAC Address）]：AP MAC アドレスが表示されます。
  - [モデル（Model）]：AP モデル番号が表示されます。
  - [動作/管理/モード（Op./Admin/Mode）]：動作状態と AP モードが表示されます。
  - [タイプ（Type）]：無線タイプが表示されます。
  - [チャネル（Channel）]：アクセス ポイントのチャネル番号が表示されます。
  - [アンテナ（Antenna）]：アンテナ名が表示されます。
  - [方位角（Azimuth）]：アンテナの方向が表示されます。
- [Rxネイバー（Rx Neighbors）] オプション ボタンを選択すると、マップ上に選択した AP の隣接 Rx ネイバーが接続線で表示されます。また、AP が AP 名と関連付けられているかどうかも示されます。

チョーク ポイントの追加、配置、および削除

チョークポイントは、チョークポイントベンダーの推奨に従ってインストールおよび設定されます。チョーク ポイントのインストールが完了して動作可能になったら、チョークポイントをロケーション データベースに入力して、Prime Infrastructure マップ上に表示できます。

ステップ 1 **[マップ（Maps）] > [サイトマップ（新）（Site Maps (New)）]** を選択します。

ステップ 2 左側のサイドバー メニュー [ドメインナビゲータ（Domain Navigator）] から、該当するフロアを選択してフロア ビュー ページを開きます。

ステップ 3 このページの右上隅にある [編集（Edit）] をクリックします。

ステップ 4 [フロア要素（Floor Elements）] パネルで、[チョークポイント（Choke Points）] の横にある [追加（Add）] をクリックします。
[チョークポイントの追加（Add Choke Points）] ページには、データベースには存在しているが、まだマップされていない、最近追加されたチョークポイントがすべて一覧表示されます。

- フロアマップに追加するチョーク ポイントのチェックボックスをオンにして、[選択項目の追加（Add Selected）] をクリックします。
- すべてのチョーク ポイントを追加するには、[すべて選択（Select All）] をクリックし、[選択項目の追加（Add Selected）] をクリックします。
- 使用可能な検索オプションを使用して、チョーク ポイントを検索できます。**クイック フィルタ**を使用して、名前、MAC アドレス、または IP アドレスにより検索します。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。[チョークポイント（chokepoint）] チェックボックスを選択し、[選択項目の追加（Add Selected）] をクリックします。

ステップ 5 フロア領域にアクセス ポイントを割り当てた後、[チョークポイントの追加（Add Choke points）] ウィンドウを閉じます。

ステップ 6 フロアマップに追加したチョーク ポイントは、マップの右側に表示されます。これで、マップ上にチョークポイントを配置する準備ができました。

ステップ 7 [フロア要素（Floor Elements）] ペインで、[チョークポイント（Choke Points）] の横にある [位置（Position）] をクリックして、マップ上に正しく配置します。

- チョークポイント アイコンを左クリックし、マップ上の適切な位置までドラッグします。
- チョークポイント アイコンを配置するためにクリックすると、ダイアログボックスにチョークポイントの MAC アドレス、名前、およびカバレッジ範囲が表示されます。
- [Save] をクリックします。フロア マップに戻ると、マップ上に追加されたチョークポイントが表示されます。

（注） 新たに作成されたチョークポイント アイコンは、そのフロアの表示設定に応じて、マップに表示される場合と表示されない場合があります。チョーク ポイントがマップに表示されない場合は、[画面設定（Display Settings）] > [オーバーレイオブジェクト（Overlay Objects）] でチョーク ポイントの切り替えが [オン（On）] に設定されていることを確認します。

（注） チョークポイントの周囲の輪は、カバレッジ領域を示しています。CCX タグとそのアセットがカバレッジ領域内を通過すると、位置の詳細がブロードキャストされ、タグはチョークポイント カバレッジ円上に自動的にマップされます。タグがチョークポイントの範囲外に出ると、その位置は以前と同様に計算されるので、チョークポイントの輪の上にはマップされなくなります。

（注） チョークポイントのマップ アイコンの上にマウス カーソルを移動すると、チョークポイントの MAC アドレス、名前、Entry/Exit チョークポイント、スタティック IP アドレス、および範囲が表示されます。

（注） すべてのマップに対してこの表示条件を保存しない場合には、[Save Settings] をクリックしないでください。

ネットワーク設計を Mobility Services Engine またはロケーション サーバに同期して、チョークポイント情報をプッシュする必要があります。

ステップ 8 [フロア要素（Floor Elements）] パネルで、[チョークポイント（Choke Points）] の横にある [削除（Delete）] をクリックします。
[チョークポイントの削除（Delete choke points）] ページが表示され、割り当てられ配置されているすべてのチョーク ポイントが一覧表示されます。

- 削除するチョーク ポイントのチェックボックスをオンにして、[選択項目の削除（Delete Selected）] をクリックします。
- すべてのチョーク ポイントを削除するには、[すべて選択（Select All）] をクリックし、[選択項目の削除（Delete Selected）] をクリックします。
- フロアからチョーク ポイントを直接削除するには、[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、名前、MAC アドレス、または IP アドレスにより検索します。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。フロア領域から削除するには、[削除（Delete）] アイコンをクリックします。

ステップ 9 [(i)] 記号をクリックして、[AP 360度（AP 360°）] ビューを起動します。

WiFi TDOA レシーバの追加、配置、および削除

Wi-Fi TDOA レシーバは、追跡対象のタグ付き資産から送信される信号を受信するように設計された外部システムです。その後これらの信号は、資産の位置計算に役立つよう、Mobility Services Engine に転送されます。TDOA レシーバは、到達時間差（TDOA）の方法を使用して、タグの位置を計算します。この方法は、最小で 3 つの TDOA レシーバからのデータを使用して、タグ付き資産の位置を生成します。

ステップ 1 **[マップ（Maps）] > [サイトマップ（新）（Site Maps (New)）]** を選択します。

ステップ 2 左側のサイドバー メニュー [ドメインナビゲータ（Domain Navigator）] から、該当するフロアを選択してフロア ビュー ページを開きます。

ステップ 3 このページの右上隅にある [編集（Edit）] をクリックします。

ステップ 4 [フロア要素（Floor Elements）] パネルで、[Wifi TDOA レシーバ（Wifi TDOA Receivers）] の横にある [追加（Add）] をクリックします。

[Wifi TDOAレシーバの追加（Add Wifi TDOA Receivers）]ページには、データベースには存在しているが、まだマップされていない、最近追加された Wi-Fi TDOA レシーバがすべて一覧表示されます。

- フロア マップに追加する Wifi TDOA レシーバのチェックボックスをオンにして、[選択項目の追加（Add Selected）] をクリックします。
- すべての Wifi TDOA レシーバ ポイントを追加するには、[すべて選択（Select All）] をクリックし、[選択項目の追加（Add Selected）] をクリックします。
- 使用可能な検索オプションを使用して、Wifi TDOA レシーバを検索できます。**クイック フィルタ**を使用して、名前、MAC アドレス、または IP アドレスにより検索します。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。[Wifi TDOAレシーバ（Wifi TDOA receiver）] チェックボックスを選択し、[選択項目の追加（Add Selected）] をクリックします。

ステップ 5 緑色の Wi-Fi TDOA 受信機アイコンが左上隅に配置されたマップが表示されます。これで、マップ上に Wi-Fi TDOA 受信機を配置する準備ができました。

ステップ 6 フロア マップに追加した各アクセス ポイントは、マップの右側に表示されます。アクセス ポイントは正しく配置する必要があります。

ステップ 7 [フロア要素（Floor Elements）] ペインで、[Wifi TDOAレシーバ（Wifi TDOA Receivers）] の横にある [位置（Position）] をクリックして、マップ上に正しく配置します。

- Wifi TDOA レシーバ アイコンを左クリックし、マップ上の適切な位置までドラッグします。
- Wi-Fi TDOA レシーバ アイコンを配置するためにクリックすると、左側のペインに Wi-Fi TDOA レシーバの MAC アドレスと名前が表示されます。
- アイコンが正確にマップに配置されたら、[保存（Save）] をクリックします。Wi-Fi TDOA レシーバのマップ アイコンの上にマウス カーソルを移動すると、Wi-Fi TDOA レシーバの MAC アドレスが表示されます。

Wi-Fi TDOA レシーバがマップに表示されない場合は、**[画面設定（Display Settings）] > [オーバーレイオブジェクト（Overlay Objects）]** で Wifi TDOA レシーバの切り替えが [オン（On）] に設定されていることを確認します。

ステップ 8 [フロア要素（Floor Elements）] パネルで、[Wifi TDOAレシーバ（Wifi TDOA Receivers）] の横にある [削除（Delete）] をクリックします。
[Wifi TDOAレシーバの削除（Delete Wifi TDOA Receivers）] ページが表示され、割り当てられ配置された Wifi TDOA レシーバがすべて一覧表示されます。

- 削除する Wifi TDOA レシーバのチェックボックスをオンにして、[選択項目の削除（Delete Selected）] をクリックします。
- **クイック フィルタ**を使用して、名前、MAC アドレス、または IP アドレスにより検索します。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。フロア領域からチョーク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。

カバレッジ領域の追加

デフォルトでは、ビルディングの一部として定義されたフロア領域や外部領域は、無線カバレッジ領域と見なされます。

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 **[マップ（Maps）] > [サイトマップ（新）（Site Maps (New)）]** を選択します。

ステップ 2 左側のサイドバー メニュー [ドメインナビゲータ（Domain Navigator）] から、該当するフロアを選択してフロア ビュー ページを開きます。

ステップ 3 このページの右上隅にある [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。
ポップアップが表示されます。

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。

- 定義する領域の名前を入力し、[Ok] をクリックします。
- 輪郭を描く領域に描画ツールを移動します。
  - 左マウス ボタンをクリックして、線の描画を開始および終了します。
  - 領域の輪郭を完全に描いたら、左マウス ボタンをダブルクリックすると、ページ内で領域が強調表示されます。

    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。
- [保存（Save）] をクリックして、新たに描画した領域を保存します。

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。

- 定義する領域の名前を入力し、[Ok] をクリックします。
- 輪郭を描く領域に描画ツールを移動します。
  - 左マウス ボタンをクリックして、線の描画を開始および終了します。
  - 領域の輪郭を完全に描いたら、左マウス ボタンをダブルクリックすると、ページ内で領域が強調表示されます。

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

- 使用可能なカバレッジ領域がマップ上で強調表示されます。
- 変更を加え、変更後に [保存（Save）] をクリックします。

ステップ 8 カバレッジ領域を削除するのには、[オーバーレイ（Overlays）] パネルで、[カバレッジエリア（Coverage Areas）] の横にある [削除（Delete）] をクリックします。

- 使用可能なカバレッジ領域がマップ上で強調表示されます。
- カバレッジ領域にマウスのカーソルを置き、[削除（delete）] をクリックします。
- 削除後に [保存（Save）] をクリックします。

障害物の作成

アクセスポイントに対する RF 予測ヒートマップを計算するときに反映できるように、障害物を作成できます。

ステップ 1 **[マップ（Maps）] > [サイトマップ（新）（Site Maps (New)）]** を選択します。

ステップ 2 左側のサイドバー メニュー [ドメインナビゲータ（Domain Navigator）] から、該当するフロアを選択してフロア ビュー ページを開きます。

ステップ 3 このページの右上隅にある [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、[障害物（Obstacles）] の横にある [追加（Add）] をクリックします。

ステップ 5 [障害物の作成（Obstacle Creation）] ウィンドウで、[障害物タイプ（Obstacle Type）] ドロップダウン リストから障害物タイプを選択します。作成できる障害物のタイプは、[厚い壁（Thick Wall）]、[薄い壁（Light Wall）]、[重いドア（Heavy Door）]、[軽いドア（Light Door）]、[パーティション（Cubicle）]、[ガラス（Glass）] です。

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。

- 左マウス ボタンをクリックして、線の描画を開始および終了します。
- 領域の輪郭を完全に描いたら、左マウス ボタンをダブルクリックすると、ページ内で領域が強調表示されます。
- [完了（Done）] をクリックします。
- 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。
- [保存（Save）] をクリックして、障害物を保存します。

ステップ 8 障害物を編集するには、[オーバーレイ（Overlays）] パネルで、[障害物（Obstacles）] の横にある [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。
- 変更が完了したら、[保存（Save）] をクリックします。

ステップ 9 障害物を削除するには、[オーバーレイ（Overlays）] パネルで、[障害物（Obstacles）] の横にある [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。
- 障害物の上にマウス カーソルを合わせ、クリックして削除します。
- 削除後に [保存（Save）] をクリックします。

マーカーの配置

ステップ 1 **[マップ（Maps）] > [サイトマップ（新）（Site Maps (New)）]** を選択します。

ステップ 2 左側のサイドバー メニュー [ドメインナビゲータ（Domain Navigator）] から、該当するフロアを選択してフロア ビュー ページを開きます。

ステップ 3 このページの右上隅にある [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。

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。描画アイコンが表示されます。

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 Prime Infrastructure と Mobility Services Engine を再同期するには、**[サービス（Services）] > [サービスの同期（Synchronize Services）]** を選択します。

ステップ 9 [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。
- 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。
- 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 11 削除後に [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。

フロア上の包含リージョンの定義

フロアまたは外部領域マップにおいて、信号強度などのワイヤレス カバレッジ データをマッピング（包含）または無視（除外）する領域を定義します。

ステップ 1 **[マップ（Maps）] > [サイトマップ（新）（Site Maps (New)）]** を選択します。

ステップ 2 左側のサイドバー メニュー [ドメインナビゲータ（Domain Navigator）] から、該当するフロアを選択してフロア ビュー ページを開きます。

ステップ 3 このページの右上隅にある [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、[包含タイプ（Inclusion Type）] ドロップダウン リストを選択します。

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。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 7 包含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 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 9 領域の輪郭が描画されるまでステップ 8 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 10 [保存（Save）] を選択して、包含リージョンを保存します。

ステップ 11 [Location Regions] チェックボックスがまだオンになっていない場合にはオンにします。これをすべてのフロア マップに適用する場合は、[Save settings] をクリックします。[Layers configuration] ページを閉じます。

ステップ 12 Prime Infrastructure と MSE データベースを再同期するには、**[サービス（Services）] > [モビリティ サービス（Mobility Services）] > [サービスの同期（Synchronize Services）]** を選択します。

（注） 2 つの DB がすでに同期されている場合は、変更があるたびに自動的に再同期が実行されます。明示的に再同期する必要はありません。

ステップ 13 [同期（Synchronize）] ページで、[同期（Synchronize）] ドロップダウン リストから [ネットワーク設計（Network Designs）] を選択して、[同期（Synchronize）] をクリックします。
[Sync. Status] 列で 2 つの緑色の矢印を調べることで、同期が正常に行われたことを確認できます。

（注） 新たに定義された包含リージョンと除外リージョンは、Mobility Services Engine によってロケーションが再計算された後にヒートマップ上に表示されます。

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。通常、除外領域は包含領域の境界内に定義されます。

除外領域を定義するには、以下のステップに従います。

ステップ 1 **[マップ（Maps）] > [サイトマップ（新）（Site Maps (New)）]** を選択します。

ステップ 2 左側のサイドバー メニュー [ドメインナビゲータ（Domain Navigator）] から、該当するフロアを選択してフロア ビュー ページを開きます。

ステップ 3 このページの右上隅にある [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 除外する領域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 領域の輪郭が描画されるまでステップ 8 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。除外された領域は紫色で網掛けされます。

ステップ 10 さらに別の除外リージョンを定義するには、ステップ 5 ～ 9 を繰り返します。

ステップ 11 すべての除外領域を定義したら [保存（Save）] を選択して、除外領域を保存します。

ステップ 12 完了したら、[ロケーションリージョン（Location Regions）] チェックボックスがまだオンになっていない場合にはオンにし、[設定の保存（Save settings）] をクリックし、[レイヤの構成（Layers configuration）] ページを閉じます。

ステップ 13 Prime Infrastructure とロケーション データベースを再同期するには、**[サービス（Services）] > [サービスの同期（Synchronize Services）]** を選択します。

ステップ 14 [同期（Synchronize）] ページで、[同期（Synchronize）] ドロップダウン リストから [ネットワーク設計（Network Designs）] を選択して、[同期（Synchronize）] をクリックします。
[Sync. Status] 列で 2 つの緑色の矢印を調べることで、同期が正常に行われたことを確認できます。

ロケーション リージョンの編集

[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。
- 変更を加えて、[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

[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。
- 削除するロケーション リージョ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。
- **[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一層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 **[マップ（Maps）]** > **[サイトマップ（新）（Site Maps (New)）]** を選択します。

ステップ 2 左側のサイドバー メニュー [ドメインナビゲータ（Domain Navigator）] から、該当するフロアを選択してフロア ビュー ページを開きます。

ステップ 3 このページの右上隅にある [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 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 ラインを完全に描画したら、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。

レール ラインを削除するには、削除する領域をクリックします。選択された領域の輪郭が紫色の破線で描かれます。次に、ツールバーの [X] アイコンをクリックします。領域がフロア マップから削除されます。

ステップ 8 [保存（Save）] をクリックします。

ステップ 9 Prime Infrastructure と Mobility Services Engine を再同期するには、**[サービス（Services）] > [サービスの同期（Synchronize Services）]** を選択します。

ステップ 10 [同期（Synchronize）] ページで、[同期（Synchronize）] ドロップダウン リストから [ネットワーク設計（Network Designs）] を選択して、[同期（Synchronize）] をクリックします。

[Sync. Status] 列で 2 つの緑色の矢印を調べることで、同期が正常に行われたことを確認できます。

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 [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。
- 変更を加えて、[保存（Save）] をクリックします。

ステップ 12 [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。
- 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 削除後に [保存（Save）] をクリックします。

GPS マーカーの配置

ステップ 1 **[マップ（Maps）] > [サイトマップ（新）（Site Maps (New)）]** を選択します。

ステップ 2 左側のサイドバー メニュー [ドメインナビゲータ（Domain Navigator）] から、該当するフロアを選択してフロア ビュー ページを開きます。

ステップ 3 このページの右上隅にある [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、[GPS マーカー（ GPS Markers）] の横にある [追加（Add）] をクリックします。

ステップ 5 GPS マーカーの名前を入力します。

ステップ 6 [緯度と経度（Latitude and Longitude）] に値を入力します。GPS マーカーは経度と緯度でキャンパス、ビルディング、またはフロアを特定します。

ステップ 7 [GPS マーカーの追加（Add GPS Marker）] をクリックします。

ステップ 8 描画アイコンをクリックし、GPS マーカーをマップ上に配置します。

ステップ 9 [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、[GPS マーカー（ GPS 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。
- 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、[GPS マーカー（GPS 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 GPS マーカーがマップ上で強調表示されます。
- 削除する GPS 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 削除後に [保存（Save）] をクリックします。

フロア ツールの使用

検出された不正 AP の表示

AP がコントローラに関連付けられていない別の AP を検出した場合、その AP は、不正 AP としてマークされます。検出された不正 AP を表示するには、以下の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**[マップ（Maps）] > [ワイヤレスマップ（Wireless Maps）] > [サイトマップ（Site Maps）]** の順にクリックします。	
ステップ 2	**[キャンパス（Campus）] > [建物（Building）] > [フロア（Floor）]** の順に選択します。	
ステップ 3	右側のペインで、**[編集（Edit）] > [フロアツール（Floor Tools）] > [不正APの検出（Rogue AP Detection）]** の順にクリックします。	
ステップ 4	不正 AP の検出を有効にする AP をクリックします。	選択された AP によって不正として検出された AP を表示できるようになります。
ステップ 5	検出を無効にするには、AP を再度クリックします。	

モニタリング ツールの使用

チャートの表示

特定のフロアにおけるクライアント、アクセスポイント、および電波品質のメトリックを表示するには、次の操作を行います。

ステップ 1 [マップ（Maps）] > [ワイヤレス マップ（Wireless Maps）] > [サイト マップ（Site Maps）] の順に選択します。

ステップ 2 [キャンパス（Campus）] > [建物（Building）] > [サイト（Site）] の順に選択します。
ステップ 3 [チャート（Charts）] タブをクリックします。

クライアント プレイバックの使用によるクライアントの移動の追跡

Cisco Prime Infrastructure では、クライアント プレイバック機能を使用して、クライアントのフロア上での移動を追跡できます。この機能は、CMX によって検出されたクライアントに対してのみ使用可能です。

クライアントのフロアでの移動を表示するには、次の手順に従います。

ステップ 1 **[マップ（Maps）] > [ワイヤレスマップ（Wireless Maps）] > [サイトマップ（Site Maps）]** の順にクリックします。
ステップ 2 **[キャンパス（Campus）] > [建物（Building）] > [フロア（Floor）]** の順に選択します。
ステップ 3 クライアントが関連付けられている、またはプローブされている AP を追加します。
ステップ 4 **[サービス（Services）] > [モビリティサービス（Mobility Services）] > [Connected Mobile Experiences]** の順にクリックします。
ステップ 5 マップをエクスポートして、CMX にインポートします。
ステップ 6 目的のサイトマップに移動し、フロアを CMX に同期させます。
ステップ 7 フロア上で目的のクライアントをクリックします。
ステップ 8 **[データ（Data）] > [クライアント（Client）] > [再生（Playback）]** の順にクリックします。
一定期間におけるクライアントの移動がマップに表示されます。

位置の準備状態の調査

Prime Infrastructure を設定することで、既存のアクセス ポイント展開の能力を確認し、少なくとも 90 % の確率で、10 m 以内にあるクライアント、不正クライアント、不正アクセス ポイント、またはタグの真の位置を推定できます。位置の準備状態の計算は、アクセスポイントの数と配置に基づいています。

また、位置の品質と指定の位置の能力を確認し、実際の調査とキャリブレーションの際に収集されたデータ ポイントに基づいて、位置の仕様（10 m、90 %）を満たすこともできます。

位置の準備状態の調査機能は距離ベースの予測ツールで、アクセスポイントを配置した場合に起こる問題領域を指摘できます。

ステップ 1 **[マップ（Maps）] > [サイトマップ（新）（Site Maps (New)）]** を選択します。
ステップ 2 左側のサイドバー メニュー [ドメインナビゲータ（Domain Navigator）] から、該当するフロアを選択してフロア ビュー ページを開きます。

ステップ 3 ページの右上の隅にある [ツール（Tools）] をクリックし、[ロケーション準備状況の検査（Inspect Location Readiness）] をクリックします。

廃止予定の [サイトマップ（Site Maps）] ページが開きます。10 m、90 % の位置仕様を満たす領域（[はい（Yes）] で示される）と満たさない領域（[いいえ（No）] で示される）を示す、色分けされたマップが表示されます。

（注） RSSI が表示されない場合は、左側のサイドバー メニューの [AP Heatmaps] チェックボックスをオンにして、AP ヒートマップを有効にできます。

（注） クライアント、タグ、およびアクセスポイントが表示されない場合は、左側のサイドバー メニューでそれぞれの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。また、クライアントとタグをそれぞれ追跡するには、クライアントとタグの両方のライセンスを購入済みである必要もあります。

音声準備状況の検査

音声の準備状態ツールでは、RF カバレッジを確認し、音声のニーズを十分に満たすかどうか判断できます。このツールは、アクセス ポイントをインストールした後の RSSI レベルを確認します。

ステップ 1 **[マップ（Maps）] > [サイトマップ（新）（Site Maps (New)）]** を選択します。

ステップ 2 左側のサイドバー メニュー [ドメインナビゲータ（Domain Navigator）] から、該当するフロアを選択してフロア ビュー ページを開きます。

ステップ 3 ページの右上隅にある [ツール（Tools）] をクリックし、[音声準備状況の検査（Inspect Voice Readiness）] をクリックします。

廃止予定の [サイトマップ（Site Maps）] ページが開きます。

ステップ 4 ドロップダウン リストから、[Band]、[AP Transmit Power]、および [Client] パラメータのうち、該当するものを選択します。

（注） デフォルトでは、地域マップには Cisco 電話ベースの RSSI 閾値に対する b/g/n 帯域が表示されます。別の設定は保存できません。

ステップ 5 選択したクライアントによっては、次の RSSI 値が編集不可になる場合があります。

- [Cisco Phone]：RSSI 値を編集できません。
- [Custom]：RSSI 値を次の範囲で編集できます。
  - 低しきい値：-95 dBm ～ -45 dBm
  - 高しきい値：-90 dBm ～ -40 dBm

ステップ 6 領域が Voice Ready かどうかは、次の色で表示されます。

- 緑色：Yes
- 黄色：Marginal
- 赤色：No

緑色/黄色/赤色のリージョンの精度は、RF 環境およびフロアが調整されているかどうかによって異なります。フロアが調整されている場合、リージョンの精度は高まります。

RF キャリブレーション方法

ステップ 1 **[マップ（Maps）] > [サイトマップ（新）（Site Maps (New)）]** を選択します。

ステップ 2 左側のサイドバー メニュー [ドメインナビゲータ（Domain Navigator）] から、該当するフロアを選択してフロア ビュー ページを開きます。

ステップ 3 ページの右上隅にある [ツール（Tools）] をクリックし、[音声準備状況の検査（Inspect Voice Readiness）] をクリックします。

廃止予定の [サイトマップ（Site Maps）] ページが開きます。[RF キャリブレーション モデル（RF Calibration Models）] ページでは、次の操作を実行できます。

- マップへのキャリブレーション モデルの適用
- キャリブレーション モデル プロパティの表示
- キャリブレーション モデルの詳細の編集

ワイヤレス マップで使用される RF キャリブレーション モデルの調整

Prime Infrastructure では、作成されたワイヤレス サイト マップのフロア領域の減衰特性を特徴付ける複数の RF モデルが提供されます。これらのキャリブレーション モデルは、別々のフロア領域に適用できる測定済みの RF 信号特性を使用して RF オーバーレイとして使用されます。これらのいずれもニーズを十分に満たしていない場合は、実際のフロア領域の減衰特性をよりよく表す 1 つ以上のカスタム キャリブレーション モデルを作成し、これらのフロア領域のマップに適用できます。これにより、チームは次のことを行うことができます。

- 実際の建物に 1 つ以上のフロアを配置する。
- RF キャリブレーション ツールを使用して、実際のフロアの RF 減衰特性を測定する。
- そのフロアの RF 特性を新しいキャリブレーション モデルとして保存する。
- そのキャリブレーション モデルを同じ物理レイアウトの他のすべてのフロアに適用する。

2 つの方法のいずれかを使用してキャリブレーションのデータを収集できます。

- ポイント モード データ収集：キャリブレーション ポイントを選択して、そのカバレッジ領域を一度に 1 つのロケーションについて計算します。

- リニア モード データ収集：一連の直線状のパスを選択して、パスをたどりながら計算します。通常、このアプローチはポイントモードよりも速く計算できます。また、ポイントモードデータ収集を使用すると、直線状のパスで見つからないロケーションに対するデータ収集を増やすことができます。

キャリブレーション モデルは、クライアント、不正なクライアント、および不正なアクセスポイントのみに適用できます。タグに応じた校正は、Aeroscout System Manager を使用して行います（この製品の詳細および使用方法については、cisco-rtls@cisco.com までメールでお問い合わせください）。

ラップトップやその他のワイヤレス デバイスを使用して、Prime Infrastructure サーバへのブラウザを開き、校正プロセスを実行します。

両方のスペクトルの校正プロセスを迅速に行うため、802.11a/n と 802.11b/g/n の両方の無線をサポートするクライアント デバイスを使用することを推奨します。

校正プロセスの詳細については、以下の関連項目を参照してください。

- 現在の RF キャリブレーション モデルのリストを表示する
- 現在のキャリブレーション モデルへのアクセス
- ワイヤレス サイト マップへのワイヤレス キャリブレーション モデルの適用
- RF キャリブレーション モデルのプロパティの表示
- 新しい RF キャリブレーション モデルの作成
- 新しい RF キャリブレーション モデルの調整、コンピューティング、適用
- 新しい RF キャリブレーション モデルの収集された「ライブ」データ ポイントの計算
- ワイヤレス サイト マップのフロア領域への完全調整された新しい RF キャリブレーション モデルの適用
- RF キャリブレーション モデルの削除

新しい RF キャリブレーション モデルの作成

新しい校正モデルを作成するには、次の手順を実行します。

ステップ 1 **[マップ（Maps）] > [サイトマップ（Site Maps）]** を選択します。

ステップ 2 **[コマンドの選択（Select a command）] > [RF校正モデル（RF Calibration Models）] > [移動（Go）]** の順に選択します。

ステップ 3 **[コマンドの選択（Select a command）] > [新しいモデルの作成（Create New Model）] > [実行（Go）]** を選択します。

ステップ 4 新しい RF キャリブレーション モデルの名前を入力して、[OK] をクリックします。

[まだキャリブレーションされていない（Not Yet Calibrated）] ステータスの他の RF キャリブレーション モデルとともに、新しいモデルがリストに表示されます。モデルのキャリブレーションを行うには、「関連

項目」の「新しい RF キャリブレーション モデルの調整、コンピューティング、適用」を参照してください。

新しい RF キャリブレーション モデルの調整、コンピューティング、適用

新しく作成された RF モデルを完全に適用するには、次の作業を実行する必要があります。

1. 「ライブ」キャリブレーション データを収集すること。
2. そのデータを計算し、モデルが使用できるようにすること。
3. 必要なフロアにモデルを適用すること。

作成し、名前をつけたばかりの（ステータスは [未キャリブレーション（Not Calibrated）]）新しい RF キャリブレーション モデルでこのプロセスを完了するには、次の手順を実行します。開始する前に、Prime Infrastructure サーバへの接続とともに、データ収集デバイスを有効にしておく必要があります。シスコの集中管理型アーキテクチャを使用していない場合は、データ収集デバイスの MAC アドレスを把握しておく必要もあります。

ステップ 1 **[マップ（Maps）] > [サイトマップ（Site Maps）]** を選択します。

ステップ 2 **[コマンドの選択（Select a command）] > [RF校正モデル（RF Calibration Models）] > [移動（Go）]** の順に選択します。

ステップ 3 モデル名をクリックして、[キャリブレーション モデル（Calibration Model）] > [モデル名（Model Name）] ページを開きます。

ステップ 4 **[コマンドの選択（Select a command）] > [データ ポイントの追加（Add Data Points）] > [実行（Go）]** を選択します。

ステップ 5 キャリブレーションの実行に使用しているデバイスの MAC アドレスを入力します。手動で入力する MAC アドレスはコロンで区切る必要があります（例：FF:FF:FF:FF:FF:FF）。

このプロセスが Cisco Centralized アーキテクチャを介して Prime Infrastructure に接続されたモバイル デバイスから実行されている場合は、MAC アドレス テキスト ボックスに自動的にデバイスのアドレスが読み込まれます。

ステップ 6 該当するキャンパスとビルディングを選択し、キャリブレーションを実行するフロア エリア、地下レベル、または屋外領域を選択します。次に、[次へ（Next）] をクリックします。

ステップ 7 選択したフロア領域マップおよびアクセス ポイント（AP）のロケーションが表示される際には、データ収集を実行する必要があるロケーションがプラス マーク（+）のグリッドで示されます。

これらのロケーションをガイドラインとして使用して、データのポイント収集またはリニア収集を実行できます。オプションが表示されたときにマップ上にそれぞれ表示される [キャリブレーション ポイント（Calibration Point）] ポップアップ（ポイント）または [開始と終了（Start and Finish）] ポップアップ（リニア）のいずれかでの該当する配置で、これを実行できます。

ステップ 8 キャリブレーション用のデータのポイント収集を実行するには、次の手順を実行します。

a) **[収集方法（Collection Method）] > [ポイント（Point）]** を選択し、[データ ポイントの表示（Show Data Points）] チェックボックスをオンにします（まだオンになっていない場合）。マップ上に [Calibration Point] ポップアップが表示されます。

b) マップ上のデータ ポイント（+）の 1 つに [キャリブレーション ポイント（Calibration Point）] ポップアップの先端を配置し、[実行（Go）] をクリックします。データ収集の進捗を示すダイアログボックスが表示されます。

近辺にあるすべての AP でクライアントが均等に受信されるように、データ収集時にはキャリブレーション クライアント ラップトップを回転させます。

c) 選択したデータ ポイントでデータ収集が完了し、カバレッジ領域がマップ上に表示されたら、[Calibration Point] ポップアップを別のデータ ポイントに移動して [Go] をクリックします。

マップ上に表示されたカバレッジ領域は色分けされ、データを収集するために使用した特定の無線 LAN 規格に対応します。カラー コーディングに関する情報は、ページの左側の凡例に示されます。また、キャリブレーション処理の進捗は、凡例の上の 2 つのステータス バーに示されます。1 つは 802.11a/n 用、もう 1 つは 802.11b/g/n 用です。

誤って選択した位置のデータ ポイントを削除するには、[Delete] をクリックして適切なデータ ポイント上に表示される黒の四角形を移動します。必要に応じて、**Ctrl** キーを押しながらマウスを移動し、四角形のサイズを変更します。

d) 関連する周波数帯（802.11a/n、802.11b/g/n）のキャリブレーション ステータス バーの表示が [完了（Done）] になるまで、ポイント収集のステップの A ～ C を繰り返します。

キャリブレーション ステータス バーは、約 50 か所の異なる位置と 150 個の測定結果を収集すると、キャリブレーション用のデータ収集の完了を表示します。キャリブレーション プロセスで保存されたそれぞれの位置で、複数のデータ ポイントが収集されます。キャリブレーション処理の進捗は、凡例の上の 2 つのステータス バーに示されます。1 つは 802.11b/g/n 用、もう 1 つは 802.11a/n 用です。

ステップ 9 キャリブレーション用のデータのリニア収集を実行するには、次の手順を実行します。

a) **[収集方法（Collection Method）] > [リニア（Linear）]** を選択し、[データ ポイントの表示（Show Data Points）] チェックボックスをオンにします（まだオンになっていない場合）。[Start] ポップアップと [Finish] ポップアップの両方と共に、マップ上に線が表示されます。

b) 開始データ ポイントに [Start] ポップアップの先端を配置します。

c) 終了データ ポイントに [Finish] ポップアップを配置します。

d) 開始データ ポイントにラップトップを持って立ち、[Go] をクリックします。定義されたパスに沿ってエンド ポイントに向かってゆっくりと一定のペースで歩きます。データ収集が処理中であることを示すダイアログボックスが表示されます。

データ収集バーが完了を示したとしても、エンド ポイントに到達するまではデータ収集を中止しないでください。

Intel 製およびシスコ製のアダプタのみがこの方法でテストされています。[Cisco Compatible Extension オプション（Cisco Compatible Extension Options）] で、[Cisco Compatible Extensions を有効にする（Enable Cisco Compatible Extensions）] と [無線管理サポートを有効にする（Enable Radio Management Support）] の両方が有効になっていることを確認します。

e) 終了ポイントに到達したら、スペース バー（またはデータ収集パネル上の [完了（Done）]）を押します。収集ペインには、収集したサンプル数が表示されます。収集ペインが閉じると、マップが表示されます。マップには、データが収集されたすべてのカバレッジ領域が表示されます。

誤って選択した位置のデータ ポイントを削除するには、[Delete] をクリックして適切なデータ ポイント上に表示される黒の四角形を移動します。必要に応じて、**Ctrl** キーを押しながらマウスを移動し、四角形のサイズを変更します。

カバレッジ領域は色分けされ、そのデータを収集するために使用した特定の無線 LAN 規格に対応します。カラー コーディングに関する情報は、ページの左側の凡例に示されます。

f) 各周波数帯のステータス バーが [完了（done）] になるまで、リニア収集のステップ B ～ E を繰り返します。

リニア収集に加えてポイント モード データ収集を実行すると、見つからないカバレッジ領域に対応できます。

ステップ 10 データ ポイントの収集が終わったら、ページ上部のキャリブレーション モデルの名前をクリックし、もう一度モデルを表示します。

必要に応じて、この時点で中止し、保存したデータ ポイントの計算と適用を後で実行することができます。これを行う場合、関連項目の「新しい RF キャリブレーション モデルの収集された「ライブ」データ ポイントの計算」の手順と、その後で「ワイヤレス サイト マップのフロアへの完全調整された RF キャリブレーション モデルの適用」の手順に従って続行します。

ステップ 11 収集したデータ ポイントに対してモデルを校正するには、**[コマンドの選択（Select a command）]** > **[キャリブレーション（Calibrate）]** > **[実行（Go）]** を選択します。

ステップ 12 キャリブレーション処理が完了したら、[ロケーション品質の検査（Inspect Location Quality）] リンクをクリックします。RSSI 測定値を示すマップが表示されます。

ステップ 13 新たに校正したモデルを、作成したワイヤレス サイト マップのフロア領域（および類似する減衰特性を持つ他のフロア）に適用するには、**[マップ（Maps）]** > **[サイト マップ（Site Maps）]** を選択します。[マップ（Maps）] ページで、新しい RF キャリブレーション モデルを適用するフロア領域に対応するリンクを選択します。

ステップ 14 フロア領域マップを表示させて、**[コマンドの選択（Select a command）]** > **[フロア領域の編集（Edit Floor Area）]** > **[実行（Go）]** を選択します。

ステップ 15 [フロア タイプ（RF モデル）（Floor Type (RF Model)）] ドロップダウン リストから、新たに作成したキャリブレーション モデルを選択します。[OK] をクリックして、フロアにモデルを適用します。

このプロセスを、必要なモデルとフロアの数に応じて繰り返します。RF キャリブレーション モデルをフロアに適用した後、そのフロアで実行されるすべてのロケーション判定はキャリブレーション モデルの RF 減衰データを使用して実行されます。

新しい RF キャリブレーション モデルの収集された「ライブ」データ ポイントの計算

以前に収集したキャリブレーション データを計算して、RF キャリブレーションモデルで使用できるようにするには、次の手順を実行します。

ステップ 1 **[マップ（Maps）] > [サイトマップ（Site Maps）]** を選択します。

ステップ 2 [コマンドの選択（Select a command）] ドロップダウン リストから、[RF キャリブレーション モデル（RF Calibration Models）] を選択し、[実行（Go）] をクリックします。

ステップ 3 以前に「ライブ」データ ポイントを収集したモデルの名前をクリックします。[キャリブレーション モデル（Calibration Model）] > [モデル名（Model Name）] ページに、選択した RF キャリブレーション モデルが表示されます。

ステップ 4 [コマンドの選択（Select a command）] ドロップダウン リストから、[キャリブレーション（Calibrate）] を選択し、[Go] をクリックします。

ステップ 5 キャリブレーション処理が完了したら、[ロケーション品質の検査（Inspect Location Quality）] リンクをクリックします。RSSI 測定値を示すマップが表示されます。

ワイヤレス サイト マップのフロアへの完全調整された RF キャリブレーション モデルの適用

新しい RF キャリブレーション モデルを使用するには、それが作成されたフロアにモデルを適用する必要があります（類似する減衰特性を持つ他のフロアについても同様）。

フロアにモデルを適用するには、次の手順を実行します。

ステップ 1 **[マップ（Maps）] > [サイト マップ（Site Maps）]** を選択します。

ステップ 2 モデルを適用する特定のフロアを見つけます。

ステップ 3 [コマンドの選択（Select a command）] ドロップダウン リストから、[フロア領域の編集（Edit Floor Area）] を選択し、[実行（Go）] をクリックします。

ステップ 4 [フロア タイプ（RF モデル）（Floor Type (RF Model)）] ドロップダウン リストから、新たに作成した RF キャリブレーション モデルを選択します。

ステップ 5 [OK] をクリックして、フロアにモデルを適用します。

このプロセスを、必要なモデルとフロアの数に応じて繰り返します。モデルをフロアに適用すると、そのフロアで実行される位置判定はすべて、キャリブレーション モデルから収集した特定の減衰データを使用して実行されます。

RF キャリブレーション モデルの削除

キャリブレーション モデルを削除するには、以下のステップに従います。

ステップ 1 **[マップ（Maps）] > [サイトマップ（Site Maps）]** を選択します。

ステップ 2 **[コマンドの選択（Select a command）] > [RF校正モデル（RF Calibration Models）] > [移動（Go）]** の順に選択します。現在の RF キャリブレーション モデルのリストが表示されます。

ステップ 3 削除するモデルの名前をクリックします。[キャリブレーション モデル（Calibration Model）] > [モデル名（Model Name）] ページが表示されます。

ステップ 4 **[コマンドの選択（Select a command）] > [モデルの削除（Delete Model）] > [実行（Go）]** を選択します。Prime Infrastructure は、キャリブレーション モデルを削除します。

RF キャリブレーション モデルのプロパティの表示

現在の校正モデルを表示または編集するには、以下のステップに従います。

ステップ 1 **[マップ（Maps）] > [サイトマップ（Site Maps）]** を選択します。

ステップ 2 **[コマンドの選択（Select a command）] > [RF校正モデル（RF Calibration Models）] > [移動（Go）]** の順に選択します。

ステップ 3 モデル名をクリックし、表示または変更するプロパティを持つ RF キャリブレーション モデルにアクセスします。

ステップ 4 選択したモデルのプロパティを表示または編集するには、次の手順を実行します。

a) **[コマンドの選択（Select a Command）] > [プロパティ（Properties）] > [実行（Go）]** を選択します。

表示または編集できるプロパティは次のとおりです。

- [ロケーションのクライアント電力をスイープ（Sweep Client Power for Location）]：有効にするにはクリックします。アクセスポイント（AP）が高密度に存在し、送信電力が低下しているか、または不明である場合に有効にすると効果的です。スイープ レンジを使用するとロケーション データの精度は高くなりますが、拡張性には悪影響が及びます。
- [ヒートマップ ビンサイズ（HeatMap Binsize）]：このドロップダウン リストから、[4]、[8]、[16]、または [32] を選択します。
- [ヒートマップ カットオフ（HeatMap Cutoff）]：ヒートマップ カットオフを決定します。特に AP 密度が高く、RF 伝播条件が良好な場合は、低いヒートマップ カットオフを設定することを推奨します。高いカットオフ値により、拡張性は高まりますが、クライアントの検索が難しくなる可能性があります。

ステップ 5 操作が終了したら、[OK] をクリックします。

ワイヤレス サイト マップへの RF キャリブレーション モデルの適用

現在の校正モデルをマップに適用するには、以下のステップに従います。

ステップ 1 **[マップ（Maps）] > [サイトマップ（Site Maps）]** を選択します。

ステップ 2 **[コマンドの選択（Select a command）] > [RF校正モデル（RF Calibration Models）] > [移動（Go）]** の順に選択します。各校正モデルの [モデル名（Model Name）] と [ステータス（Status）] が表示されます。

ステップ 3 必要な RF キャリブレーション モデルにアクセスするには、モデル名をクリックします。

ステップ 4 **[コマンドの選択（Select a command）] > [マップに適用（Apply to Maps）] > [Go（実行）]** を選択します。

プランニング モードの使用

データ トラフィック、音声トラフィック、および位置がそれぞれアクティブかどうかに基づいて、アクセス ポイントの推奨される数および位置を計算できます。

プランニング モードでは、各プロトコル（802.11a または 802.11 b/g）に指定されるスループットに基づいて、ネットワーク内で最適カバレッジを提供するために必要な合計アクセス ポイント数が計算されます。

ステップ 1 **[マップ（Maps）] > [サイト マップ（新）（Site Maps (New)）]** を選択します。

ステップ 2 左側のサイドバー メニュー [ドメイン ナビゲータ（Domain Navigator）] から、該当するフロアを選択してフロア ビュー ページを開きます。

ステップ 3 ページの右上の隅にある [ツール（Tools）] をクリックし、[プランニング モード（Planning Mode）] をクリックします。

プランニング モードでは、必要なアクセス ポイント数の計算に AP タイプおよびアンテナ パターン情報を使用しません。計算はアクセス ポイントのカバレッジ領域または各アクセス ポイントのユーザ数に基づいています。

プランニング モードのオプションは次のとおりです。

- [AP の追加（Add APs）]：マップへのアクセス ポイントの追加を可能にします。詳細については、「アクセス ポイント要件の計算へのプランニング モードの使用」を参照してください。
- [Delete APs]：選択したアクセス ポイントを削除します。
- [マップ エディタ（Map Editor）]：[マップ エディタ（Map Editor）] ウィンドウを開きます。詳細については、「マップ エディタの使用」を参照してください。
- [Synchronize with Deployment]：プランニング モードのアクセス ポイントを現在の導入シナリオと同期します。
- [Generate Proposal]：現在のアクセス ポイント導入のプランニング概要を表示します。
- [Planned AP Association Tool]：Excel または CSV ファイルから AP アソシエーションの追加、削除、またはインポートを実行できます。アクセス ポイントを定義したら、[Planned AP Association Tool] を使用して、そのアクセス ポイントをベース無線の MAC アドレスにアソシエートできます。AP が検出されない場合はスタンバイ バケットに送られ、AP が検出されたときにアソシエートされます。

（注） AP アソシエーションには、AP はフロアまたは屋外領域に属さないという制限があります。AP がすでにフロアまたは屋外領域に割り当てられている場合は、スタンバイ バケットが AP を保持し、フロアまたは屋外領域から AP が削除されたときに、指定されたフロアに配置されます。1 つの MAC アドレスを複数のフロアまたは屋外領域のバケットに入力することはできません。

ステップ 4 マップの同期は、AP がベース無線の MAC アドレスにアソシエートされている場合のみ動作し、イーサネット MAC アドレスにアソシエートされている場合は動作しません。

ワイヤレス サイト マップ エディタの機能

マップ エディタを使って、フロア プラン情報を定義、描画、および拡張します。また、マップエディタでは、アクセスポイントに対する RF 予測ヒートマップを計算するときに反映できるように、障害物を作成できます。その特定の領域にあるクライアントとタグを特定する、Location Appliances のカバレッジ領域を追加することもできます。

プランニング モードでは、プランニング ツールが起動されるブラウザ ウィンドウでマップ エディタを開きます。元のブラウザ ウィンドウがフロアのページから移動している場合は、フロアのページに戻って、マップ エディタを起動する必要があります。

- マップ エディタの使用に関するガイドライン
- アクセス ポイントの配置に関するガイドライン
- フロア上の包含領域と除外領域に関するガイドライン
- マップ エディタの表示
- マップ エディタのアイコン
- マップ エディタを使用したカバレッジ領域の描画
- マップ エディタを使用した障害物の描画
- フロア上の包含リージョンの定義
- フロア上の除外リージョンの定義
- フロアでのレール ラインの定義

ワイヤレス サイト マップ エディタの使用に関するガイドライン

Map Editor を使用してビルディングまたはフロア マップを変更する際には、次の内容を考慮してください。

- 以前のフロア プラン エディタから FPE ファイルをインポートするのではなく、マップ エディタを使用して壁やその他の障害物を描画することを推奨します。
- 必要に応じて .PE ファイルをインポートすることはできます。次の手順を実行します。
  1. 目的のフロア領域に移動します。
  2. **[コマンドの選択（Select a command）] > [フロア領域の編集（Edit Floor Area）] > [移動（Go）]** の順に選択します。
  3. [FPEファイル（FPE File）] チェックボックスをオンにします。

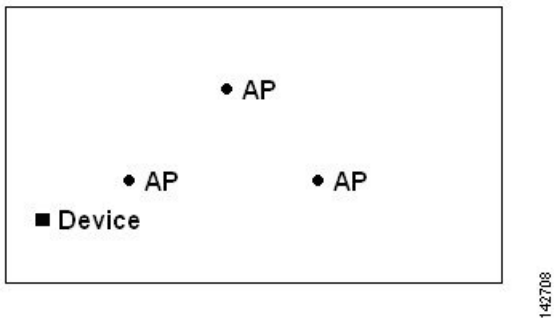
4. FPE ファイルを参照し、[OK] をクリックします。

- マップ エディタを使用して、任意の数の壁をフロア プランに追加できます。ただし、クライアント ワークステーションの処理能力とメモリによって、Prime Infrastructure の更新とレンダリングの側面が制限される場合があります。
- RAM が 1 GB 以下のコンピュータでは、実用的な制限として、フロアごとの壁数を 400 個までにすることを推奨します。
- すべての壁は、Prime Infrastructure が RF カバレッジ ヒートマップを生成する際に使用されます。

アクセス ポイントの配置に関するガイドライン

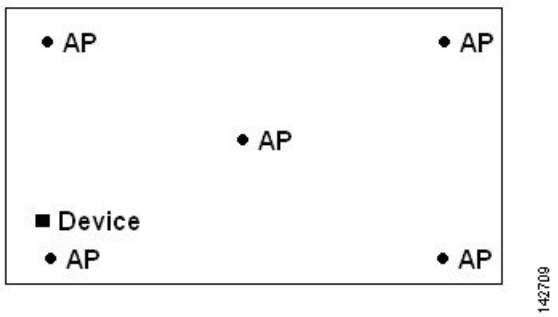
部屋や建物の屋外の近くにデバイスが置かれるように、カバレッジ領域の境界に沿ってアクセス ポイント（AP）を設置します。このようなカバレッジ領域の中心に設置されたアクセス ポイントからは、場合によっては他の全 AP から等距離に見えてしまうデバイスに関しても有益なデータが得られます。

図 *3:* 一塊に集めたアクセス ポイント



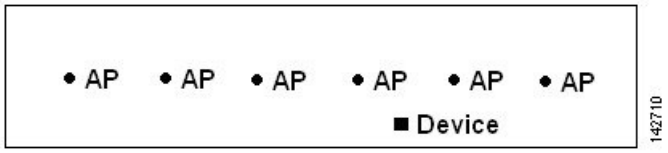
全体の AP の密度を高め、AP をカバレッジ領域の周辺方向へ移動することにより、位置精度が大幅に向上します。

図 *4:* 密度を高めることによる位置精度の向上



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。

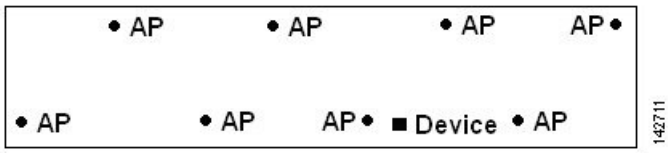
図 *5:* 直線的な配置を控える



この計画では高い帯域幅のアプリケーションに十分な AP 密度が提供されますが、ある 1 つのデバイスに対する、各 AP からの見え方があまり変化しないため、ロケーションの特定が困難になるという問題があります。

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。

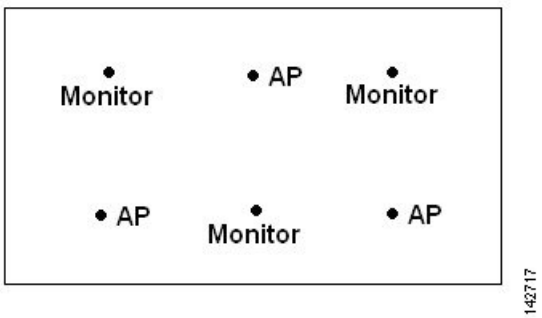
図 *6:* 周辺で交互にずらすことによる位置精度の向上



最も一般的な無線端末は、3 つの重複しないチャネルだけを提供する 802.11b/n しかサポートしていません。そのため、電話に対して設計された無線 LAN は、データを伝送するために計画されたものより密度が低い傾向があります。また、トラフィックが Platinum QoS バケット（通常は音声トラフィック、および遅延の影響を受けやすい他のトラフィック用に予約されている）にキューイングされると、Lightweight AP はスキャン機能を延期します。これにより、スキャン機能は他のチャネルで最大となり、アクセス ポイントは他の情報と共にデバイスの位置情報を収集します。ユーザは、monitor-only モードに設定した AP で無線 LAN 展開を補完できます。モニタリング機能だけを実行するアクセス ポイントは、クライアントにサービスを提供せず、干渉は引き起こしません。電波をスキャンしてデバイス情報を取得するだけです。

音声ネットワークなどの低密度の無線 LAN の導入では、それらの位置精度が、モニタ AP の追加および適切な配置によって非常に高まることがわかります。

図 *7:* 低密度の無線 *LAN* の設置



無線ラップトップ、ハンドヘルド、または電話を使用してカバレッジを検証し、3つ以上のAPがデバイスによって検出されることを確認します。クライアントとアセットタグのロケーションを確認するには、Prime Infrastructureによるクライアントのデバイスとタグの報告が、指定した精度範囲内（10 m、90 %）であることを確認します。

全方向性アンテナを内蔵した天井マウント型APがある場合は、Prime Infrastructureでアンテナの方向を必ずしも設定する必要はありません。ただし、同じAPを壁にマウントする場合は、アンテナの方向を90度に設定する必要があります。

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で表され、最低3点で構成される必要があります。

フロア上の包含リージョンを1つだけ定義できます。デフォルトでは、各フロア領域が作成されるときに、各フロア領域に対して包含領域が定義されます。包含領域は、水色の実線で示され、通常はフロア領域全体の輪郭を描きます。

フロア領域に複数の除外領域を定義することができます。

新たに定義された包含リージョンと除外リージョンは、Mobility Services Engineによってロケーションが再計算された後にヒートマップ上に表示されます。

ワイヤレス サイト マップ エディタの起動と使用

Map Editorを使用するには、以下のステップに従います。

ステップ1 **[マップ（Maps）]** > **[サイトマップ（Site Maps）]** を選択します。

ステップ2 目的のキャンパスとビルディングを選択します。

ステップ3 目的のフロア領域をクリックします。[サイト マップ（Site Maps）] > [キャンパス名（Campus Name）] > [ビルディング名（Building Name）] > [フロア領域名（Floor Area Name）] ページが表示されます。

ステップ4 **[コマンドの選択（Select a command）]** > **[マップエディタ（Map Editor）]** > **[移動（Go）]** の順に選択します。[Map Editor] ページが表示されます。

外壁より外部の空白部分がすべてなくなるように、フロア図面のイメージが適切に縮尺されていることを確認してください。フロアの寸法が正確かどうかを確認するには、[compass tool] をクリックします。

ステップ5 基準長を配置します。線の長さが指定された [フロアのスケーリング（Scale Floor）] メニューが表示されます。基準長の寸法（幅と高さ）を入力して、[OK] をクリックします。

ステップ6 [アンテナモード（Antenna Mode）] ドロップダウンリストから、伝播パターンを決定します。

ステップ7 アンテナ方向バーを目的の度の方向へスライドさせて、アンテナ調整をします。

ステップ8 目的のアクセス ポイントを選択します。

ステップ9 **[保存（Save）]** をクリックします。

ワイヤレス サイト マップ エディタのアイコン

表 *23 :* ワイヤレス サイト マップ エディタのアイコン

アイコン	説明
	フロアのスケーリング：線の描画を開始するマップ上の任意の場所をクリックします。ダブルクリックすると線を終了し、表示されるポップアップに新しい行の長さを入力します。これでフロア寸法を新しい寸法に変更します。
	距離の測定：線の描画を開始するマップ上の任意の場所をクリックします。ダブルクリックすると線が終了します。線の長さはフィート/メートル単位で上部に表示されます。
	障害物のコピー/移動：マップ上にボックスを描画するか、障害物をクリックして、障害物を選択します。障害物をコピーするには、[Copy]をクリックします。これで、選択された障害物のすぐ上に新しい障害物が作成されます。障害物を移動するには、選択した障害物を新しい位置にドラッグします。マップ上の任意の個所をクリックすると、すべての要素が選択解除されます。
	削除モード：マップ上にボックスを描画するか、各要素をクリックして、削除する要素を選択します。複数の要素を選択するには、**Shift**キーを使用します。要素の選択/選択解除を切り替えるには、**Ctrl** キーを 1 回ずつ使用します。マップ上の任意の個所をクリックすると、すべての要素が選択解除されます。選択した要素を削除するには、[Delete] をクリックします。
	変更モード：要素をクリックし、変形させる頂点をクリックするか、要素を新しい位置までドラッグします。マップ上の任意の場所をクリックすると、選択した要素が選択解除されます。
	カバレッジ領域の描画
	ロケーション リージョンの描画
	レールの描画
	障害物の描画：描画を開始するマップ上の任意の場所をクリックします。ダブルクリックすると描画を終了します。現在の描画を取り消す場合は Ctrl-z を、やり直す場合は Ctrl-y を、キャンセルする場合は Esc キーを使用します。
	マーカーの配置

アイコン	説明
	ナビゲーション：描画や編集など選択したモードをすべて削除し、ナビゲーション モードに切り替えます。このモードでは、マップを表示し、ズームまたはパンを実行できます。

ワイヤレス サイト マップでのカバレッジ領域の定義

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、Map Editor を使用してカバレッジ領域を描画できます。

ステップ 1 Prime Infrastructure にフロア図面がまだ表示されていない場合は、フロア図面を追加します。

ステップ 2 **[マップ（Maps）] > [サイトマップ（Site Maps）]** を選択します。

ステップ 3 編集する屋外領域、キャンパス、ビルディングまたはフロアに対応する [Map Name] をクリックします。

ステップ 4 **[コマンドの選択（Select a command）] > [マップエディタ（Map Editor）] > [移動（Go）]** の順に選択します。[Map Editor] ページが表示されます。

ステップ 5 ツールバーの [カバレッジ領域の描画（Draw Coverage Area）] アイコンをクリックします。

ポップアップが表示されます。

ステップ 6 定義する領域の名前を入力し、[OK] をクリックします。

描画ツールが表示されます。

ステップ 7 輪郭を描く領域に描画ツールを移動します。

- 左マウス ボタンをクリックして、線の描画を開始および終了します。
- 領域の輪郭を完全に描いたら、左マウス ボタンをダブルクリックすると、ページ内で領域が強調表示されます。

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 8 ツールバーのディスク アイコンをクリックして、新たに描画した領域を保存します。

ワイヤレス サイト マップにおける障害物のカラー コーディング

次の表では、ワイヤレス サイト マップ上の障害物に適用されるカラー コーディングと、これらの障害物の近くで RF 信号強度を計算するために使用される推定信号損失について説明します。

表 *24 :* 障害物のカラー コーディング

障害のタイプ	カラー コーディング	信号損失（dB 単位）
厚い壁		13
薄い壁		2
重いドア		15
軽いドア		4
パーティション		1
ガラス		1.5

ワイヤレス サイト マップでの包含リージョンの定義

ワイヤレス サイト マップのフロア領域に表示するデバイス ロケーション情報の精度を高めるために、ロケーションデータに含めるリージョン（包含リージョン）と、含めないリージョン（除外リージョン）を定義することができます。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共用領域を除外して、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。

デフォルトでは、Prime Infrastructure は、新たに追加された各フロアに対して包含リージョンを定義します。新しい包含リージョンを定義すると、以前に定義された包含リージョンが自動的に削除されます。包含リージョンは水色の実線で輪郭が示されます。

ステップ 1 **[マップ（Maps）] > [サイトマップ（Site Maps）]** を選択します。

ステップ 2 該当するフロア領域の名前をクリックします。

ステップ 3 **[コマンドの選択（Select a command）] > [マップエディタ（Map Editor）] > [移動（Go）]** の順に選択します。

ステップ 4 マップで、ツールバーの水色のボックスをクリックします。

一度に 1 つの包含領域のみ定義できることを示すメッセージ ボックスが表示されます。

ステップ 5 メッセージ ボックスで [OK] をクリックします。包含領域の輪郭の描画に役立つ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 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リージョンが定義されます。

ステップ 9 [Command] メニューから [Save] を選択するか、ツールバーの**ディスク** アイコンをクリックして、包含リージョンを保存します。

包含領域を誤って定義した場合は、領域をクリックします。選択された領域の輪郭が水色の破線で描かれます。次に、ツールバーの [X] アイコンをクリックします。領域がフロア マップから削除されます。

ステップ 10 フロア マップに戻ってヒートマップ上で包含リージョンを有効にするには、[Command] メニューから [Exit] を選択します。

ステップ 11 [Location Regions] チェックボックスがまだオンになっていない場合にはオンにします。変更をすべてのフロア マップに適用する場合は、[Save settings] をクリックします。

ステップ 12 Prime Infrastructure と MSE データベースを再同期するには、**[サービス（Services）]** > **[サービスの同期（Synchronize Services）]** を選択します。2 つの DB がすでに同期されている場合は、変更があるたびと、明示的な再同期が必要ない場合に、自動的に再同期が実行されます。

ステップ 13 [同期（Synchronize）] ページで、**[同期（Synchronize）]** > **[ネットワーク設計（Network Designs）]** を選択し、[OK] をクリックします。[Sync. Status] 列の 2 つの緑色の矢印を調べることで、同期が正常に行われたことを確認できます。

新たに定義された包含リージョンと除外リージョンは、Mobility Services Engine によってロケーションが再計算された後にヒートマップ上に表示されます。

ワイヤレス サイト マップでの除外リージョンの定義

フロアのロケーション計算の精度を高めるため、計算から除外するリージョン（除外リージョン）を定義できます。たとえば、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。通常、除外リージョンは包含リージョンの境界内に定義されます。

ステップ 1 **[マップ（Maps）]** > **[サイトマップ（Site Maps）]** を選択します。

ステップ 2 該当するフロア領域の名前をクリックします。

ステップ 3 **[コマンドの選択（Select a command）]** > **[マップエディタ（Map Editor）]** > **[移動（Go）]** の順に選択します。[Map Editor] ページが表示されます。

ステップ 4 マップで、ツールバーの紫色のボックスをクリックします。

ステップ 5 表示されるメッセージ ボックスで [OK] をクリックします。除外リージョンの輪郭の描画に役立つ描画アイコンが表示されます。

ステップ 6 除外リージョン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 7 除外するリージョン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 8 リージョン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。定義された除外リージョンは、そのリージョンが完全に定義されると紫色で網掛けされます。

ステップ 9 さらに別の除外リージョンを定義するには、ステップ 5 ～ 8 を繰り返します。

ステップ 10 すべての除外リージョンを定義したら、[コマンド（Command）] メニューから [保存（Save）] を選択するか、ツールバーの**ディスク** アイコンをクリックして、除外リージョンを保存します。

除外リージョンを削除するには、削除するリージョンをクリックします。選択したリージョンの輪郭が紫色の破線で描画されます。次に、ツールバーの [X] アイコンをクリックします。リージョンがフロア マップから削除されます。

ステップ 11 フロア マップに戻ってヒートマップ上で除外リージョンを有効にするには、[コマンド（Command）] メニューから [終了（Exit）] を選択します。

ステップ 12 完了したら、[ロケーションリージョン（Location Regions）] チェックボックスがまだオンになっていない場合にはオンにし、[設定の保存（Save settings）] をクリックし、[レイヤの構成（Layers configuration）] ページを閉じます。

ステップ 13 Prime Infrastructure とロケーション データベースを再同期するには、**[サービス（Services）] > [サービスの同期（Synchronize Services）]** を選択します。

ステップ 14 [同期（Synchronize）] ページで、**[同期（Synchronize）] > [ネットワーク設計（Network Designs）]** を選択してから、[同期（Synchronize）] をクリックします。**同期の際に緑の矢印が表示され、同期が正常に行われたことを確認できます。[ステータス（Status）]** カラム。

ワイヤレス サイト マップでのレール ラインの定義

任意のフロア領域にレール ラインを定義できます。レール ラインは、ロケーションの計算を効率化し、常に移動しているワイヤレス クライアントや、精密なロケーション データを必要としない（繁忙な製造フロア領域や屋外の建設現場などの）ワイヤレス クライアントのロケーション データの表示を要約します。

また、レール ライン周辺の領域をスナップ幅として定義することもできます。スナップ幅は、ローミング 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。スナップ幅は、レールのいずれか側（東西または南北）で監視する距離を表します。スナップ幅領域内に配置されたクライアントは、レール ライン上に直接表示されるか（ローミング クライアントの大多数）、スナップ幅領域の外側に表示されます（少数）。

レール ラインはタグには適用されません。フィートまたはメートルのいずれでもスナップ幅領域を定義できます。

ステップ 1 **[マップ（Maps）] > [サイトマップ（Site Maps）]** を選択します。

ステップ 2 該当するフロア領域の名前をクリックします。

ステップ 3 **[コマンドの選択（Select a command）] > [マップエディタ（Map Editor）] > [移動（Go）]** の順に選択します。[Map Editor] ページが表示されます。

ステップ 4 マップで、ツールバーの [レール（rail）] アイコン（紫色の除外領域アイコンの右側）をクリックします。

ステップ 5 表示されるメッセージ ダイアログボックスで、レールのスナップ幅（フィートまたはメートル）を入力し、[OK] 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 ラインを完全に描画したら、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。

レール ラインを削除するには、削除する領域をクリックします。選択された領域の輪郭が紫色の破線で描かれます。次に、ツールバーの [X] アイコンをクリックします。領域がフロア マップから削除されます。

ステップ 8 フロア マップに戻ってヒートマップ上でレールを有効にするには、[Command] メニューから [Exit] を選択します。

ステップ 9 表示されたフロア マップで、[レイヤ（Layers）] ドロップダウン リストを選択します。

ステップ 10 完了したら、[レール（Rails）] チェックボックスがまだオンになっていない場合はオンにし、[設定の保存（Save settings）] をクリックし、[レイヤ（Layers）] 設定パネルを閉じます。

ステップ 11 Prime Infrastructure と Mobility Services Engine を再同期するには、**[サービス（Services）]** > **[サービスの同期（Synchronize Services）]** を選択します。

ステップ 12 [同期（Synchronize）] ページで、**[同期（Synchronize）]** > **[ネットワーク設計（Network Designs）]** を選択してから、[同期（Synchronize）] をクリックします。

同期の際に緑の矢印が表示され、同期が正常に行われたことを確認できます。[ステータス（Status column.

ワイヤレス サイト マップの検索

[Search Maps] ページで、次のパラメータを使用できます。

- Search for
- Map Name
- Search in
- Save Search
- Items per page

[移動（Go）]をクリックすると、次の表に示すオプションとともに、マップ検索結果のページが表示されます。

表 *25 :* ワイヤレス サイト マップの検索結果

フィールド	オプション
Name	[Name] 列の項目をクリックすると、各フロアに対する個々のフロア領域マップとともに既存のビルディングのマップが表示されます。

フィールド	オプション
Type	キャンパス、ビルディングまたはフロア領域。
Total APs	検出された Cisco Radio の合計数が表示されます。
a/n Radios	802.11a/n Cisco Radio の数が表示されます。
b/g/n Radios	802.11b/g/n Cisco Radio の数が表示されます。

ワイヤレス サイト マップ エディタを使用した RF アンテナの調整

ワイヤレス サイト マップ エディタを使用して RF アンテナを調整するには、次の手順を実行します。

ステップ 1 **[マップ（Maps）] > [サイトマップ（Site Maps）]** を選択します。

ステップ 2 必要なビルディングとフロア領域を含むキャンパスをクリックします。[サイト マップ（Site Maps）] > [キャンパス名（Campus Name）] ページが表示されます。

ステップ 3 必要なビルディングをクリックします。[サイト マップ（Site Maps）] > [キャンパス名（Campus Name）] > [ビルディング名（Building Name）] ページが表示されます。

ステップ 4 必要なフロア領域、地下レベル、または外部領域をクリックします。[サイトマップ（Site Maps）] > [キャンパス名（Campus Name）] > [ビルディング名（Building Name）] > [フロア領域名（Floor Area Name）] ページが表示されます。

ステップ 5 **[コマンドの選択（Select a command）] > [マップエディタ（Map Editor）] > [移動（Go）]** の順に選択します。[Map Editor] ページが表示されます。

先に進む前に、外壁の外側にあるすべての空白が削除されるように、フロア領域のイメージの縮尺が正しいことを確認します。フロアの寸法が正確であることを確認するには、ツールバーの [コンパス ツール（compass tool）] をクリックし、必要に応じて調整します。

ステップ 6 基準長を配置します。これを行うと、指定した線の長さで [スケール（Scale）] メニューが表示されます。基準長の寸法（幅と高さ）を入力して、[OK] をクリックします。

ステップ 7 [アンテナモード（Antenna Mode）] ドロップダウンリストから、伝播パターンを決定します。

ステップ 8 アンテナ方向バーを目的の度の方向へスライドさせて、アンテナ調整をします。

ステップ 9 目的のアクセス ポイントを選択します。

ステップ 10 **[保存（Save）]** をクリックします。

AP ロケーション準備状況を使用した低カバレッジ領域の検索

Prime Infrastructure を設定することで、既存のアクセス ポイント（AP）展開の能力を確認し、少なくとも 90 パーセントの確率で、10 m 以内にあるクライアント、不正クライアント、不正 AP、またはタグの真の位置を推定できます。ロケーションの準備状況の計算は、AP の数と配

置に基づいています。Inspect Location Readiness 機能は距離ベースの予測ツールで、AP を配置した場合に起こる問題領域を指摘できます。

Inspect Location Readiness ツールを表示するには、以下のステップに従います。

ステップ 1 **[マップ（Maps）] > [サイトマップ（Site Maps）]** を選択します。

ステップ 2 該当するフロア領域名をクリックして、マップを表示します。

RSSI が表示されない場合は、左側のサイドバー メニューの [AP ヒートマップ（AP Heatmaps）] チェックボックスをオンにして、AP ヒートマップを有効にできます。

クライアント、タグ、およびAPが表示されない場合は、左側のサイドバーのメニューでそれぞれの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。また、クライアントとタグをそれぞれ追跡するには、クライアントとタグの両方のライセンスを購入済みである必要もあります。

ステップ 3 **[コマンドの選択（Select a command）] > [ロケーション準備状況の検査（Inspect Location Readiness）] > [実行（Go）]** を選択します。

10 メートル、90 パーセントの位置仕様を満たす領域（[はい（Yes）] で示される）と満たさない領域（[いいえ（No）] で示される）を示す、色分けされたマップが表示されます。

RF キャリブレーション データを使用した AP カバレッジの品質評価

領域を物理的に移動しているときに生成したデータ ポイントに基づいて RF キャリブレーション モデルを完成させると（関連項目の「新しい RF キャリブレーション モデルの調整、コンピューティング、適用」を参照）、アクセス ポイント（AP）のロケーション品質を検査できるようになります。ロケーション精度の仕様を満たす所定のロケーションの機能（つまり、10 メートル以内で、時間の 90 %）の評価は、物理検査およびキャリブレーション時に収集されたデータ ポイントに基づきます。

校正に基づき位置品質を調査するには、以下のステップに従います。

ステップ 1 **[マップ（Maps）] > [サイトマップ（Site Maps）]** を選択します。

ステップ 2 **[コマンドの選択（Select a command）] > [RF キャリブレーション モデル（RF Calibration Model）] > [実行（Go）]** を選択します。RF キャリブレーション モデルのリストが表示されます。

ステップ 3 該当する RF キャリブレーション モデルをクリックします。

RF キャリブレーション モデルの詳細が表示されます。これには、最終キャリブレーションの日付、キャリブレーションで使用された信号のタイプ別（802.11a、802.11 b/g）のデータ ポイントの数、ロケーション、およびカバレッジが含まれています。

ステップ 4 [キャリブレーション フロア（Calibration Floors）] という見出しの下にある [ロケーション品質の検査（Inspect Location Quality）] リンクをクリックします。Prime Infrastructure には、ロケーション エラーのパーセンテー

ジが示された色分けされたマップが表示されます。選択されている距離を変更して、位置エラーへの影響を確認できます。

RF カバレッジが音声対応に十分かどうかの判断

VoWLAN Readiness（音声の準備状態）ツールでは、RF カバレッジを確認し、音声のニーズを十分に満たすかどうか判断できます。このツールは、アクセス ポイント（AP）をインストールした後の RSSI レベルを確認します。

VoWLAN Readiness ツール（VRT）を表示するには、以下のステップに従います。

ステップ 1 **[マップ（Maps）] > [サイトマップ（Site Maps）]** を選択します。

ステップ 2 音声準備状況を検査するフロア領域、外部領域、または地下レベルの名前をクリックします。

ステップ 3 **[コマンドの選択（Select a command）] > [VoWLAN の準備状況の検査（Inspect VoWLAN Readiness）] > [実行（Go）]** を選択します。

ステップ 4 ドロップダウン リストから、[帯域（Band）]、[AP 送信電力（AP Transmit Power）]、および [クライアント（Client）] パラメータのうち、該当するものを選択します。

デフォルトでは、リージョン マップに Cisco Phone ベースの RSSI しきい値に対する b/g/n 帯域が表示されます。新しい設定は保存できません。選択したクライアントによっては、次の RSSI 値が編集不可になる場合があります。

- [Cisco Phone]：RSSI 値を編集できません。
- [カスタム（Custom）]：RSSI 値を次の範囲内で編集できます。
  - 低しきい値：-95 dBm ～ -45 dBm
  - 高しきい値：-90 dBm ～ -40 dBm

ステップ 5 問題のある領域のマップを調べます。マップは次のように色分けされます。

- 緑色：音声対応
- 黄色：しきい値周辺
- 赤色：音声対応不可

緑色/黄色/赤色のリージョンの色分け精度は、RF 環境や、フロア領域がキャリブレーションされているかどうかによって異なります（この詳細については、「関連項目」の「新しい RF キャリブレーション モデルの調整、コンピューティング、適用」を参照）。フロア領域マップがキャリブレーションされている場合は、リージョンの色分けの精度が高くなります。

ステップ 6 カバレッジが狭いか、またはない領域をトラブルシューティングするには、[AP 送信電力（AP Transmit Power）] の設定を次のように調整します。

- [AP 送信電力（AP Transmit Power）] フィールドを [最大（Max）]（最大ダウンリンク電力設定）に設定します。マップに黄色か赤色のリージョンがまだ表示される場合は、アクセス ポイントを増やして VoWLAN を完全にカバーする必要がある可能性があります。
- [AP 送信電力（AP Transmit Power）] フィールドを [電流（Current）] に設定します。キャリブレーションされたモデルに音声が展開さるリージョンが赤色または黄色で表示される場合は、APの電力レベルを引き上げると役に立つ場合があります。

有線デバイス情報の表示

ステップ 1 **[マップ（Maps）] > [サイトマップ（新）（Site Maps (New)）]** を選択します。

ステップ 2 左側のサイドバー メニュー [ドメインナビゲータ（Domain Navigator）] から、該当するフロアを選択してフロア ビュー ページを開きます。

ステップ 3 ページの右上の隅にある [ツール（Tools）] をクリックし、[有線デバイスの表示（Show Wired Device Info）] をクリックします。

ポップアップ ページが表示され、次の情報が示されます。

- 有線スイッチに関する概要と詳細
- 有線クライアントに関する概要と詳細

ステップ 4 [OK] をクリックして戻り、ウィンドウを閉じます。

干渉源通知の設定

ステップ 1 **[マップ（Maps）] > [サイトマップ（新）（Site Maps (New)）]** を選択します。

ステップ 2 左側のサイドバー メニュー [ドメインナビゲータ（Domain Navigator）] から、該当するフロアを選択してフロア ビュー ページを開きます。

ステップ 3 ページの右上の隅にある [ツール（Tools）] をクリックし、[干渉源通知の設定（Configure Interferer Notification）] をクリックします。

ステップ 4 [干渉に関する CAS 通知の設定（Interferer CAS Notification Configuration）] ウィンドウで、通知を生成するデバイスのチェックボックスをオンにします。

- Bluetooth リンク
- 電子レンジ
- 802.11FH
- Bluetooth 検出
- TDD トランスミッタ

- Jammer
- 連続トランスミッタ
- DECT 類似の電話機
- ビデオ カメラ
- 802.15.4
- WiFi Inverted
- WiFi 無効チャネル
- SuperAG
- レーダー
- Canopy
- XBox
- WiMax Mobile
- WiMax Fixed

ステップ 5 **[保存（Save）]** をクリックします。

表示/非表示

ページの右上隅にある [ツール（Tools）] をクリックし、[表示/非表示（Show/Hide）] をクリックしてマップ上の距離をフィート単位で表示するグリッドを表示または非表示にします。

PDF へのエクスポート

クリックして **ツール** ページ、およびクリックの右上隅で **エクスポート** フロア プランを pdf ファイルとしてエクスポートするのに PDF に。

距離の測定

ステップ 1 ページの右上の隅にある [ツール（Tools）] をクリックし、[距離の測定（Measure Distance）] をクリックします。

ステップ 2 線の描画を開始するマップ上の任意の場所をクリックします。フィート単位で測定した線がツールチップに表示されます。

データのフィルタリング

アクセス ポイント データのフィルタリング

アクセス ポイントのフィルタリング オプションには、次の項目が含まれます。

- 無線タイプ [2.4 GHz] または [5 GHz] を選択します。
- 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 ポイント識別子を次から選択します：[名前（Name）]、[MACアドレス（MAC Address）]、[Tx Power]、[チャネル（Channel）]、[平均電波品質（Avg Air Quality）]、[最小電波品質（Min. Air Quality）]、[コントローラIP（Controller IP）]、[カバレッジホール（Coverage Holes）]、[Tx使用率（Tx Utilization）]、[Rx使用率（Rx Utilization）]、[プロファイル（Profiles）]、[CleanAirステータス（CleanAir Status）]、[関連付けられたクライアント（Associated Clients）]、[デュアルバンド無線（Dual-Band Radios）]、[無線（Radio）]、または [ブリッジグループ名（Bridge Group Name）]。
  - アクセス ポイントのフィルタリングの基準にするパラメータを選択します。
  - 該当するパラメータのテキストボックスに特定のフィルタ条件を入力し、[移動（Go）] をクリックします。アクセス ポイントの検索結果が表示されます。
  - [フィルタを適用（Apply Filter）] をクリックして、フィルタ結果をマップに表示します。

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

クライアント データのフィルタリング

MSE が Cisco Prime Infrastructure に追加されている場合、[クライアント（Clients）] フィルタ オプションが表示されます。[クライアント（Clients）] フィルタリング オプションには、次の項目が含まれます。

- 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クライアント識別子を次から選択します：[IPアドレス（IP Address）]、[ユーザ名（User Name）]、[MACアドレス（MAC Address）]、[アセット名（Asset Name）]、[アセットグループ（Asset Group）]、[アセットカテゴリ（Asset Category）]、[コントローラ（Controller）]、[SSID]、[プロトコル（Protocol）]、または [状態（State）]。
  - 該当するパラメータのテキストボックスに特定のフィルタ条件を入力し、[移動（Go）] をクリックします。クライアントの検索結果が表に表示されます。
  - [フィルタを適用（Apply Filter）] をクリックして、フィルタ結果をマップに表示します。

クライアントに複数の IPv6 アドレスが存在する場合は、いずれか 1 つの IP アドレスを指定して、クライアントを一意に識別できます。

テーブルの検索結果にマウスのカーソルを合わせると、クライアントの位置がマップ上に線で示されます。

タグ データのフィルタリング

タグ フィルタリング オプションには、次の項目が含まれます。

- マップ上に表示するタグ識別子を次から選択します：[MACアドレス（MAC Address）]、[アセット名（Asset Name）]、[アセットグループ（Asset Group）]、[アセットカテゴリ（Asset Category）]、または [コントローラ（Controller）]。
- タグのフィルタリングの基準にするパラメータを選択します。選択したら、特定のデバイスをテキスト ボックスに入力します。[移動（Go）] をクリックします。検索結果が表に表示されます。
- [フィルタを適用（Apply Filter）] をクリックして、フィルタ結果をマップに表示します。

不正な ap 通信データのフィルタ リング

[フィルタを適用（Apply Filter）] をクリックして、フィルタ結果をマップに表示します。

- 選択、 **非認識の AP** 地図を表示する識別子: MAC アドレス、分類型、または状態。
- 状態を選択-保留中のアイドル、関連付けられている、認証済みアラートから選択する使用ドロップ ダウン リストまたはプローブ。
  - 分類型-分類型をテキスト ボックスに入力します。
  - [移動（Go）] をクリックします。検索結果が表に表示されます。
- [フィルタを適用（Apply Filter）] をクリックして、フィルタ結果をマップに表示します。

アドホックの不正なデータをフィルタ リング

[不正なアドホック（Rogue Adhoc）] フィルター ダイアログ ボックスが表示されますこれらのパラメーターが含まれています。

- [MAC Address]：特定の MAC アドレスを表示する場合は、その MAC アドレスを [MAC Address] テキスト ボックスに入力します。
- [State]：ドロップダウン リストを使用して、[Alert]、[Known]、[Acknowledged]、[Contained]、[Threat]、または [Unknown] から封じ込めステートを選択します。
- [On Network]：ドロップダウン リストを使用して、ネットワーク上の不正アドホックを表示するかどうか指定します。
- [移動（Go）] をクリックします。検索結果が表に表示されます。
- [フィルタを適用（Apply Filter）] をクリックして、フィルタ結果をマップに表示します。

干渉源データのフィルタリング

[Interferer] フロア設定を有効にし、右側の青い矢印をクリックすると、[Interferers filter] ダイアログボックスが表示されます。干渉のフィルタリング オプションには、次の項目が含まれます。

- 干渉状態
- 干渉源の種類
- 該当するすべてのフィルタリング基準を選択したら、[OK] をクリックします。

アクセス ポイント ヒートマップ データのフィルタリング

RF 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、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。

アクセス ポイント ヒートマップのフロア設定を有効にし、[フロア設定（Floor Settings）] の右側にある青色の矢印をクリックすると、[関与するAP（Contributing APs）] ダイアログにヒートマップのフィルタリング オプションが表示されます。

Prime Infrastructure にダイナミック ヒートマップが導入されました。ダイナミック ヒートマップを有効にすると、Prime Infrastructure は変更された RSSI 値を表すためにヒートマップを再計算します。

アクセス ポイント ヒートマップのフィルタリング オプションには、次の項目が含まれます。

- **ヒートマップ タイプ**
  - [カバレッジ（Coverage）] : フロア プランにモニタ モードのアクセス ポイントがある場合は、IDS またはカバレッジ ヒートマップ タイプのいずれかを選択できます。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。

    （注） カバレージ超過領域ヒートマップには、信号の長さ（領域の観点で）と信号の強度が示されます。RSSI カットオフは、使用可能な信号と考えられる dBM 単位の RSSI の最低値であり、暗い青色で示されます。レンダリング ヒートマップにおける RSSI カットオフ値は、信号が指定された RSSI カットオフ値より高いスパンを識別します。

  - [電波品質（Air Quality）] : XOR モニタ モード無線には適用されません。[Air Quality] を選択した場合は、アクセス ポイントのヒート マップ タイプを平均電波品質または最小電波品質でさらにフィルタリングできます。該当するオプション ボタンを選択します。クライアント サービス モードで動作する無線のヒートマップが表示されます。Cisco Aironet 2800 および 3800 シリーズ AP は、固定 A 帯域と XOR 2.4 GHz または 5.4 GHz 無線モードで動作します。

- [IDS]：モニタ モードで動作する無線にのみ使用できます。IDS ヒートマップ オプションは、フロアにモニタ モードの AP または XOR 無線が 1 つ以上ある場合に表示されます。

（注） カバレッジ ヒートマップおよび電波品質ヒートマップには、ローカル モード、FlexConnect モード、またはブリッジ モードの AP のみが関係します。

- [XOR のみを表示（Show only XOR）]：XOR 無線のみのヒートマップが表示されます。このオプションを使用すると、固定バンドとデュアルバンド無線のヒートマップを区別できます。
- [AP総数（Total APs）]：マップ上に配置されたアクセス ポイントの数を表示します。
- アクセス ポイントのチェックボックスをオンにして、イメージ マップ上に表示するヒートマップを決定します。

該当するすべてのフィルタリング基準を選択したら、[OK] をクリックします。

プランニング モードを使用したワイヤレス ワイト マップでの AP の配置

データ トラフィック、音声トラフィック、およびロケーションの組み合わせに基づいて、アクセス ポイント（AP）の推奨される数とロケーションを計算できます。

プランニング モードでは、各プロトコル（802.11a または 802.11 b/g）に指定されるスループットに基づいて、ネットワーク内で最適なワイヤレス カバレッジを提供するために必要な合計アクセス ポイント数が計算されます。

プランニング モードのオプションには次が含まれます。

- [AP の追加（Add APs）]：マップへの AP の追加を可能にします。詳細については、「関連項目」の「プランニング モードを使用したアクセス ポイント カバレッジ要件の計算」を参照してください。
- [AP の削除（Delete APs）]：選択した AP を削除します。
- [Map Editor]：[Map Editor] ウィンドウを開きます。
- [導入と同期（Synchronize with Deployment）]：プランニング モードの AP を現在の導入シナリオと同期します。
- [提案の生成（Generate Proposal）]：現在の AP 導入のプランニング概要を表示します。
- [AP アソシエーション計画ツール（Planned AP Association Tool）]：Excel または CSV ファイルから AP アソシエーションの追加、削除、またはインポートを実行できます。AP を

定義したら、[AP アソシエーション計画ツール（Planned AP Association Tool）] を使用して、そのアクセス ポイントをベース無線の MAC アドレスにアソシエートできます。AP が検出されない場合はスタンバイ バケットに送られ、AP が検出された際にアソシエートされます。

AP の関連付けは、AP がフロア領域や屋外領域に属していないことが条件となります。AP がすでにフロア領域または屋外領域に割り当てられている場合は、スタンバイ バケットが AP を保持し、フロア領域または屋外領域から AP が削除されたときに、指定されたフロアに配置されます。1 つの MAC アドレスを複数のフロアまたは屋外領域のバケットに入力することはできません。

マップの同期は、AP がベース無線の MAC アドレスに関連付けられている場合のみ動作し、イーサネット MAC アドレスに関連付けられている場合は動作しません。

プランニング モードでは、必要な AP 数の計算に AP タイプまたはアンテナ パターン情報を使用しません。計算は AP のカバレッジ領域または各AP のユーザ数に基づきます。

ステップ 1 **[マップ（Maps）] > [サイト マップ（Site Maps）]** を選択します。

ステップ 2 目的のキャンパス、ビルディング、フロア領域を選択します。

ステップ 3 **[コマンドの選択（Select a command）] > [プランニング モード（Planning Mode）] > [移動（Go）]** の順に選択します。

プランニング モードを使用したアクセス ポイント カバレッジ要件の計算

Prime Infrastructure プランニング モードを使用すると、マップ上に架空のアクセス ポイント（AP）を配置してカバレッジ領域を表示することで、その領域をカバーするのに必要なアクセス ポイントの数を計算できます。プランニング モードでは、各プロトコル（802.11a/n または 802.11b/g/n）に指定されるスループットに基づいて、ネットワーク内で最適なカバレッジを提供するために必要な合計アクセス ポイント数が計算されます。次の条件に基づいて、AP の推奨される数および位置を計算できます。

- ネットワーク上でアクティブなトラフィックのタイプ：データ トラフィック、音声トラフィック、または両方
- 位置精度の要件
- アクティブなユーザの数
- 1 平方フィートあたりのユーザ数

ステップ 1 **[マップ（Maps）] > [サイト マップ（Site Maps）]** を選択します。

ステップ 2 目的のキャンパス、ビルディング、フロア領域を選択します。すべての要素（AP、クライアント、タグ）とその相対的な信号強度を示す、色分けされたマップが表示されます。

ステップ 3 **[コマンドの選択（Select a command）] > [プランニングモード（Planning Mode）] > [移動（Go）]** の順に選択します。空白のフロア領域のマップが表示されます。

ステップ 4 [AP の追加（Add APs）] をクリックします。

表示されたページで、推奨される AP の合計数を計算するマップの領域周辺に破線の四角形をドラッグします。

四角形の端を選択し、Ctrl キーを押したままにして、四角形のサイズまたは配置を調整します。四角形のサイズは、辺と頂点にあるハンドルをドラッグして変更できます。

ステップ 5 [AP の追加（Add APs）] ドロップダウン リストから [自動（Automatic）] を選択します。

ステップ 6 [AP タイプ（AP Type）] と、選択した AP に適したアンテナとプロトコルを選択します。

ステップ 7 AP のターゲット スループットを選択します。

ステップ 8 フロアで使用される**サービス**の横にあるチェックボックスをオンにします。少なくとも 1 つのサービスを選択する必要があります。

ステップ 9 [詳細オプション（Advanced Options）] チェックボックスをオンにして、次の AP プランニング オプションを選択します。

- [需要（Demand）] および [AP ごとにカバレッジを上書き（Override Coverage per AP）]
- Safety Margin（[Data/Coverage] および [Voice] セーフティ マージン オプションの場合）

ステップ 10 [Calculate] をクリックします。

選択したパラメータに推奨される AP の数が表示されます。推奨される計算では、[詳細オプション（Advanced Options）] の [セーフティ マージン（Safety Margin）] で下方に調整されていない限り、常に強力な信号が必要であると見なされます。推奨される AP の数が実際に必要な数よりも多い場合があります。

プランニング モードの計算では、壁は使用または考慮されません。

ステップ 11 [適用（Apply）] をクリックし、選択した領域に推奨される AP の導入案を示したマップを生成します。

ステップ 12 [提案の生成（Generate Proposal）] を選択して、指定された入力に基づいて推奨される AP の数および導入のレポートを、テキストおよびグラフィックで表示します。

ワイヤレス サイト マップの更新設定の構成

Prime Infrastructure では、ワイヤレス サイト マップのさまざまな更新オプションが提供されます。

- [ロード（Load）]：必要に応じて、Prime Infrastructure データベースからマップ データを更新します。
- [自動更新（Auto Refresh）]：データベースからマップ データを更新する頻度を設定する間隔ドロップダウンリストが提供されます。

- [ネットワークから更新（Refresh from network）]：Prime Infrastructure データベースからポーリングされたデータではなく、SNMP 取得を通じてコントローラからマップのステータスと統計情報を直接更新します。
- [ブラウザの更新（Refresh browser）]：完全なページを更新するか、またはユーザがマップページを使用している場合はマップとそのステータスおよび統計情報を更新します。

フロア計画にモニタ モード アクセス ポイントがある場合、IDS ヒートマップ タイプまたはカバレッジ ヒートマップ タイプのいずれかを選択できます。カバレッジ ヒートマップでは、モニタ モード アクセス ポイントが除外され、IDS ヒートマップでは含められます。

RF ヒートマップの計算方法

無線周波数ヒートマップは、フロア領域、地下レベルをカバーする Wi-Fi アクセス ポイントによって生成された RF 信号の強度をグラフで表したものです。WLAN は非常に動的で非決定性を備えているため、管理者は特定の瞬間の任意のスポットでカバレッジを確実に把握することは困難です。この課題への対処をサポートするため、Prime Infrastructure では、フロアの Wi-Fi カバレッジに関して、視覚的な指示を含むフロア図面のマップを提供しています。これらのマップは、海洋学や地理科学でさまざまなレベルの温度を示す際に使用される色付きマップと似ていることから、ヒートマップと呼ばれます。色はさまざまなレベルの信号強度を示すために使用されます。ヒートマップのさまざまな色合いは、異なる RF 信号強度を反映しています。

この色による視覚化によって、カバレッジの現在の状態、信号強度、WLAN のすき間や「穴」を簡単に確認できます。動き回ってカバレッジの状態を測定する必要はありません。これにより、組織に対するサポートおよび特定の問題のトラブルシューティングにかかる時間と手間が大幅に軽減されます。

RF ヒートマップの計算は内部グリッドに基づいています。グリッド内の障害物の正確な場所に応じて、障害物から数フィートまたは数メートルの範囲において、RF ヒートマップが障害物による減衰を考慮できるかどうかが異なります。アクセス ポイントの RF 予測ヒートマップは、実際の RF 信号強度を近似したものです。このヒートマップでは Map Editor を使用して描画された障害物の減衰が考慮されていますが、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ません。13 dB の損失を与える厚い壁（オレンジに色分けされている）では、ヒートマップの壁を超える RF 信号を十分に封じ込められない場合があります。

詳細には、交差する障害物に部分的に影響を受けているグリッドの正方形が障害物の減衰を反映できるかどうかは、アクセス ポイント、障害物、およびグリッドの配置によって異なります。

たとえば、グリッドの正方形に交差する壁があるとします。グリッドの正方形の中心点は AP から見ると壁の背後にあります。このため、グリッドの正方形では、実際には壁の前にある左上隅も含めて（残念ながら）、全体に減衰を示す色が設定されます。

グリッドの正方形の中心点は壁に対して AP と同じ側にあります。このため、グリッドの正方形では、実際には AP から見て壁の背後にある右下隅も含めて（残念ながら）、全体に減衰を示す色は設定されません。

RF ヒートマップの計算は、静的または動的に実行できます。デフォルトでは、ダイナミックになります。ダイナミック ヒートマップ機能の主な目的は、障害物による RF ヒートマップの再計算を行うことです。Prime Infrastructure サーバは、現在の全 AP の RSSI 強度リストを保持します。Prime Infrastructure は隣接 AP の RSSI 強度を使用して、すべての AP の RF ヒートマップを変更します。

スタティック ヒートマップ計算を設定するには、マップ プロパティ ページでダイナミック ヒートマップ オプションを無効にする必要があります。

[フロアビュー（Floor View）] ナビゲーション ウィンドウのツール

[フロア ビュー（Floor View）] メイン ナビゲーション ペインでは、複数のマップ機能にアクセスでき、さらに以下の機能が含まれています。

- [Zoom In/Zoom Out]：プラス記号（+）の付いた虫眼鏡アイコンをクリックすると、マップ ビューが拡大します。マイナス記号（-）の付いた虫眼鏡アイコンをクリックすると、マップ ビューのサイズが縮小します。
- [マップサイズ（Map Size）]：関連項目「次世代マップのパンとズーム」を参照してください。
- [グリッドを表示（Show Grid）]：クリックすると、マップ上の距離をフィート単位で表示するグリッドが表示されたり、非表示になったりします。
- [RSSI 凡例（RSSI Legend）]：マウス カーソルを RSSI 凡例アイコンの上に移動すると、RSSI の配色（赤色/-35 dBm から紺青色/-90 dBm までの範囲）が表示されます。
- [アクセス ポイントの追加（Add Access Points）]：クリックすると、[アクセス ポイントの追加（Add Access Points）] ページが開きます。詳細については、関連項目「フロア領域へのアクセス ポイントの追加」を参照してください。
- [Remove Access Points]：クリックすると、[Remove Access Points] ページが開きます。削除するアクセス ポイントを選択し、[OK] をクリックします。
- [Position Access Points]：クリックすると、[Position Access Points] ページが開きます。
- [Add Chokepoints]：クリックすると、[Add Chokepoints] ページが開きます。詳細については、『Cisco Context-Aware Services Configuration Guide』を参照してください。
- [Add WiFi TDOA Receivers]：クリックすると、[Add Wi-Fi TDOA Receivers] ページが開きます。詳細については、『Cisco Context-Aware Services Configuration Guide』を参照してください。
- [自動更新（Auto Refresh）]：ドロップダウン リストから、システム更新間隔を選択します。
- [ネットワークから更新（Refresh from Network）]：クリックすると、現在のデータの即時リフレッシュが開始されます。
- [計画モード（Planning Mode）]：クリックすると、[計画モード（Planning Mode）] ウィンドウが開きます。

- [Map Editor]：クリックすると、[Map Editor] ウィンドウが開きます。
- [Full Screen]：クリックすると、マップのサイズが全画面に拡大します。ここで、[全画面表示を終了（Exit Full Screen）] をクリックすると通常の表示に戻ります。

自動階層作成を使用したワイヤレスサイトマップの作成

始める前に

自動階層の作成機能は、正規表現を使用して迅速かつ容易にワイヤレス サイト マップを作成し、アクセスポイント（AP）を割り当てるのに役立ちます。この機能を使用するには、まず、次の作業が必要です。

- ワイヤレス AP の命名パターンを作成します。AP の命名パターンには、ワイヤレス サイト マップの作成のために作成したか、または作成を計画しているキャンパスおよびビルディングの名前と、フロア領域、地下、および屋外領域の名前を含める必要があります。これらのワイヤレス サイト マップをすでに作成している場合は、ワイヤレス AP 命名パターンに使用している名前と、ワイヤレス サイト マップに使用している名前が一致する必要があります（スペルおよび大文字化を含む）。また、AP 命名パターンの部分を区切るための区切り文字も選択します。たとえば、「San Jose」というキャンパスがあり、「01」というビルディング、「GroundFloor」というフロア領域、およびそのフロアに「AP3500il」という AP がある場合は、「San Jose-01-GroundFloor-AP3500i1」というような AP の命名パターンを作成します。
- AP とワイヤレス LAN コントローラの検出に Prime Infrastructure をすでに使用している場合は、命名パターンを使用して AP の名前が変更されています。

警告 マップのロケーション情報で行った変更を元に戻すことはできないため、先に進む前にマップのバックアップを実行することをお勧めします。

ステップ 1 **[マップ（Maps）] > [自動階層の作成（Automatic Hierarchy Creation）]** を選択して、[自動階層の作成（Automatic Hierarchy Creation）] ページを表示します。

ステップ 2 ネットワーク上の AP の名前をテキスト ボックスに入力するか、またはリストからいずれか 1 つを選択します。

この名前は、マップを作成する正規表現を作成するために使用されます。

以前に作成した正規表現を更新するには、その正規表現の横にある [ロードして続行（Load and Continue）] をクリックして正規表現を適宜更新します。正規表現を削除するには、式の横にある [Delete] をクリックします。

ステップ 3 [次へ（Next）] をクリックします。

ステップ 4 AP の名前に区切り文字が含まれている場合は、その文字をテキスト ボックスに入力して [区切り文字に基づき基本的な正規表現を生成（Generate basic regex based on delimiter）] をクリックします。システムでは区切り文字に基づいて AP の名前と一致する正規表現が作成されます。

たとえば、区切り文字がダッシュ（-）の AP 名を San Jose-01-GroundFloor-AP3500i1 で使用すると、正規表現 /(.*)-(.*)-(.*)-(.*)/ が作成されます。より複雑な AP 名がある場合は、手動で正規表現を入力できます。

先頭と末尾のスラッシュを入力する必要はありません。

規則として、Prime Infrastructure ではスラッシュ内に正規表現を表示します。

ステップ 5 [テスト（Test）] をクリックします。システムは、AP 名に対して作成されたマップと、入力された正規表現を表示します。

ステップ 6 [グループ（Group）] のフィールドを使用して、階層型に一致するグループを割り当てます。

たとえば、AP に SJC14-4-AP-BREAK-ROOM という名前を付けたとします。

この例では、キャンパス名が SJC、ビルディング名が 14、フロア名が 4、AP 名が AP-BREAK-ROOM です。

正規表現 /([A-Z]+)(\d+)-(\d+)-(.*)/ を使用します。

AP 名から、次のグループが抽出されます。

1. SJC
2. 14
3. 4
4. AP-BREAK-ROOM

一致するグループは、1 から始めて、左から右へ割り当てられます。

一致するグループを階層要素と一致させるには、各グループ番号のドロップダウン リストを使用して、適切な階層要素を選択します。

これにより、AP 名内の位置は、ほとんどどのような順番でも可能になります。

たとえば、AP に EastLab-Atrium2-3-SanFrancisco という名前が付けられている場合

正規表現 /(.*)-(.*)-(.*)-(.*)/ と

次のグループ マッピングを併用する場合：

1. Building
2. Device Name
3. Floor
4. Campus

自動階層作成では、SanFrancisco というキャンパス、EastLab というビルディング、EastLab の 3 というフロアを作成します。

デバイス名がない、またはデバイスが影響を与えない 2 つの階層タイプでは、他の目的で一致するグループを使用する必要がある場合は、グループを省略できます。

自動階層作成では、AP を配置するマップを計算するためにマップする次のグループが必要です。

キャンパス グループは一致しているか?	ビルディング グループは一致しているか?	フロア グループは一致しているか?	結果の位置
対応	対応	対応	キャンパス > ビルディング > フロア
対応	対応	非対応	不一致
対応	非対応	対応	キャンパス > フロア（フロアが屋外領域の場合）
対応	非対応	非対応	不一致
非対応	対応	対応	システム キャンパス > ビルディング > フロア
非対応	対応	非対応	不一致
非対応	非対応	対応	不一致
非対応	非対応	非対応	不一致

自動階層作成では、フロア名からフロア インデックスを推測しようとします。フロア名が数値の場合、AHC はフロアを正数のフロア インデックスに割り当てます。フロア名が負の数値または文字 B で始まる場合（b1、-4、または B2 など）、AHC はフロアを負数のフロア インデックスに割り当てます。これは、フロアが地下であることを示します。

AP を配置する既存のマップを検索する場合、AHC は、AP の名前と同じフロア インデックスを持つ AP のビルディング内のフロアを考慮します。

たとえば、SF > MarketStreet > Sublevel1 というマップがあり、フロア インデックスが -1 の場合、そのフロアには AP の F-MarketStreet-b1-MON1 が割り当てられます。

ステップ 7 [次へ（Next）] をクリックします。AP の対象を増やしてテストできます。[デバイス名を追加してテストする対象（Add more device names to test against）] フィールドに AP を入力して [追加（Add）] をクリックすると、より多くの AP に対する正規表現と一致グループのマッピングをテストできます。

次に、[テスト（Test）] をクリックして、テーブル内の各 AP 名をテストします。各テストの結果がテーブルに表示されます。

必要に応じて、現在の正規表現の正規表現またはグループ マッピングを編集するには、前のステップに戻ります。

ステップ 8 [Next] をクリックしてから、[Save and Apply] をクリックします。これでシステムに正規表現が適用されます。システムはマップに割り当てられていないすべての AP を処理します。

フロア イメージ、正しい寸法などを含めるようにマップを編集できます。自動階層作成でマップを作成する場合は、20 フィート X 20 フィートのデフォルト寸法が使用されます。正しい寸法などの属性を指定するには、作成されたマップを編集する必要があります。

自動階層作成を使用して作成されるマップは、不完全なアイコンがマップ リストに表示されます。マップの編集が完了すると、[未完了（incomplete）] アイコンが消えます。[ビューの編集（Edit View）] リンクをクリックして、未完了マップの列を非表示にできます。

ワイヤレス サイト マップでの Google Earth マップの表示

コンピュータに Google Earth をインストールし、サーバからデータを受信した際に自動的に起動するように設定しておく必要があります。

Google Earth は、通信に SSL 3.0 を使用します。ただし、Cisco Prime Infrastructure 3.2 リリースでデフォルトによりサポートされているのは TLSv1.2 のみです。Google Earth をサポートする場合は、次の手順を実行する必要があります。

- Cisco Prime Infrastructure サーバに管理者権限で ssh ログインを実行します。
- **ncs run set-tls-versions <tls-versions>** コマンドを使用して、必要な TLS バージョンを有効にします。たとえば、TLSv1.2、TLSv1.1、および TLSv1.0 を有効にするには、コマンド **prime-server/admin# ncs run tls-server-versions TLSv1.2 TLSv1.1 TLSv1** を発行します。
- アプリケーションを再起動します。

ワイヤレス サイト マップで Google Earth マップを表示するには、次の手順を実行します。

ステップ 1 **[マップ（Maps）] > [Google Earth]** を選択します。[Google Earth マップ（Google Earth Maps）] ページが開き、すべてのフォルダと、各フォルダに含まれるアクセス ポイントの数が表示されます。

ステップ 2 表示するマップの [起動（Launch）] をクリックします。Google Earth が起動して新しいページが開き、ロケーションとそのアクセス ポイントが表示されます。

ワイヤレス サイト マップでの Google Earth マップ詳細の表示

Google Earth Map フォルダの詳細を表示する手順は、以下のとおりです。

ステップ 1 **[マップ（Maps）] > [Google Earth]** を選択します。

ステップ 2 フォルダ名をクリックしてフォルダの詳細ページを開きます。[Google Earth Details] ウィンドウでは、アクセス ポイント名と、MAC アドレスまたは IP アドレスを確認できます。

ステップ 3 アクセス ポイントを削除するには、該当するチェックボックスをオンにして [Delete] をクリックします。

ステップ 4 フォルダを削除するには、フォルダ名の横にあるチェックボックスをオンにして [Delete] をクリックします。フォルダを削除すると、そのフォルダ内のすべてのサブフォルダとアクセス ポイントが削除されます。

ステップ 5 [Cancel] をクリックして、詳細ページを閉じます。

地理座標を使用したワイヤレスサイトマップ上の屋外位置への AP のグループ化

アクセス ポイントを屋外位置に基づいてグループ化するには、各アクセス ポイントの緯度/経度座標を使用します。最初に、Prime Infrastructure にインポートできる必要なアクセス ポイントの地理座標を作成する必要があります。次のファイル タイプのいずれかを作成して座標を設定できます。

- KML（Google Keyhole Markup Language）ファイル
- CSV ファイル（各値がカンマで区切られたスプレッドシート形式のファイル）

地理座標を使用して屋外位置を作成するための前提条件

各アクセス ポイントに対して次の地理情報を設定する必要があります。Google Earth で地理座標を作成して Prime Infrastructure にインポートできます。標準マップに AP を関連付けることなく、その AP を Google Earth マップに追加すると、Google Earth で AP を表示したときにヒートマップが表示されません。

- longitude（東または西）：グリニッジ子午線を基準とする角距離（度数）。子午線より西側の値の範囲は -180 ～ 0 度。子午線より東側の値の範囲は 0 ～ 180 度。デフォルトは 0 です。

  度、分、秒、方位による座標表記

  - 度（–180 ～ 180）
  - 分（0 ～ 59）
  - 秒（00.00 ～ 59.99）
  - 方位：東（E）または西（W）

  10 進法表記（「度分秒」表記から変換）

  - 経度の範囲は -179.59.59.99 W ～ 179.59.59.99 E。

- [経度（Latitude）]（北または南）：赤道を基準とする角距離（度数）。赤道より南側の値の範囲は -90 ～ 0 度。赤道より北側の値の範囲は 0 ～ 90 度。デフォルトは 0 です。

  度、分、秒、方位による座標表記

- 度（–90 ～ 90）
- 分（0 ～ 59）
- 秒（00.00 ～ 59.99）
- 方位：北（N）または南（S）

10 進法表記（「度分秒」表記から変換）

- 緯度の範囲は -89.59.59.99 S ～ 89.59.59.99 N

- [Altitude（標高）]：地表からアクセス ポイントまでの高さまたは距離（メートル）。指定しない場合は、デフォルト値の 0 が適用されます。値の範囲は 0 ～ 99999 です。
- [Tilt（傾斜）]：0 ～ 90 度（負の値は指定できません）。<tilt>値が 0 度の場合は、アクセス ポイントを真上から眺めることができます。<tilt>値が 90 度の場合は、水平線に沿った眺めになります。値の範囲は 0 ～ 90 です。デフォルトの方位角は 0 です。
- [Range]：[Longitude] と [Latitude] で指定した地点から、アクセス ポイントを眺める視点までの距離をメートルで指定します（海面からのカメラ高度）。値の範囲は 0 ～ 999999 です。
- [Heading]：コンパス方位を度数で指定します。デフォルトは 0（北）です。値の範囲は 0 ～ ±180 度です。
- [Altitude Mode]：<LookAt> で指定した <altitude>の解釈方法を指定します。
  - [地面に固定（Clamped to ground）]：<altitude>の指定を無視し、地表面に <LookAt>位置（視点）を配置します。これがデフォルトです。
  - [地面に対する相対値（Relative to ground）]：<altitude> を、地表面から測定した高度値（メートル）と見なします。
  - [絶対値（Absolute）]：<altitude>を、海面からの高度値（メートル）と見なします。
- [地面に延長（Extend to ground）]：アクセス ポイントをマストにアタッチするかどうかを指定します。

Google Earth を使用してワイヤレス サイト マップ上の屋外位置に地理座標をインポートする

Google Earth で地理座標を作成して Prime Infrastructure にインポートできます。フォルダまたは個別の目印を作成できます。フォルダを作成する方法の利点は、すべての目印を 1 つのフォルダにまとめ、そのフォルダ自体を KML（XML）ファイルとして保存できることです。KML は、Google Earth で地理データを表示するために使用されるファイル形式です。目印を作成する場合は、それらを個別に保存する必要があります。

KMLファイルを使用すると、任意の深さでフォルダを階層的に作成できます。たとえば、国、都市、州、郵便番号別に構成されたフォルダと目印を作成できます。CSVファイルでは、階層は 1 レベルのみです。

ステップ 1 Google Earth を起動します。

ステップ 2 左側のサイドバー メニューの [プレイス（Places）] ページで、[マイ プレイス（My Places）] または [一時プレイス（Temporary Places）] を選択します。

ステップ 3 [一時プレイス（Temporary Places）] を右クリックして、ドロップダウン リストから **[追加（Add）]** > **[フォルダ（Folder）]** を選択します。

ステップ 4 必要な情報を入力します。

[View] で座標（緯度、経度、範囲、方位、傾斜）を指定した場合、それらの情報は、Google Earth の最初の読み込み時に正しい場所へ「飛行」または移動するために使用されます。座標を指定しない場合、緯度と経度情報は、指定されたグループまたはフォルダ内の全アクセス ポイントの最小緯度、最小経度、最大緯度、および最大経度に基づいて取得されます。

ステップ 5 [OK] をクリックします。

フォルダの作成後は、そのフォルダを [プレイス（Places）] ページで選択して目印を作成できます。

ワイヤレス サイト マップで使用される KML ファイルの目印の作成

目印を作成するには、次の手順を実行します。

ステップ 1 Google Earth を起動します。

ステップ 2 左側のサイドバーの [Places] ページで、[My Places] または [Temporary Places] を選択します。

ステップ 3 前に作成したフォルダを選択します。

ステップ 4 作成したフォルダを右クリックして、ドロップダウン リストから **[追加（Add）]** > **[Placemark]** を選択します。

ステップ 5 必要なフィールドに入力します。Google Earth の詳細については、Google Earth のオンライン ヘルプを参照してください。

目印名には、該当するアクセス ポイントの名前、MAC アドレス（Ethernet MAC 以外の無線 MAC）、または IP アドレスを含める必要があります。

ステップ 6 [Snapshot current view] をクリックします。または、[Reset] をクリックして元の座標設定に戻します。

ステップ 7 [OK] をクリックします。

ステップ 8 追加するすべての目印について、上記の手順を繰り返します。

ステップ 9 すべての目印を作成したら、そのフォルダを .kmz ファイル（KML Zip ファイル）または .kml ファイルとして保存します.kmz ファイルと .kml ファイルの両方を Prime Infrastructure にインポートできます。

ワイヤレスサイトマップに地理座標をインポートするためのCSVファイルの作成

必要なアクセス ポイントの地理座標を含む CSV ファイルを作成して、Prime Infrastructure にその CSV ファイルをインポートできます。

ステップ 1 テキスト エディタを使用し、次の表で説明するように、カンマで区切った必要なフィールドを含む新しいファイルを作成します。

表 *26 :* 地理座標付き *CSV* ファイルのサンプル フィールド

“FolderName”	“Value Optional”	最長：32
“FolderState”	“Value Optional”	設定可能な値：true/false
“FolderLongitude”	“Value Optional”	範囲：0 ～ ±180
“FolderLatitude”	“Value Optional”	範囲：0 ～ ±90
“FolderAltitude”	“Value Optional”	範囲：0 ～ 99999
“FolderRange”	“Value Optional”	範囲：0 ～ 99999
“FolderTilt”	“Value Optional”	範囲：0 ～ 90
“FolderHeading”	“Value Optional”	範囲：0 ～ ±180
“FolderGeoAddress”	“Value Optional”	最長：128
“FolderGeoCity”	“Value Optional”	最長：64
“FolderGeoState”	“Value Optional”	最長：40
“FolderGeoZip”	“Value Optional”	最長：12
“FolderGeoCountry”	“Value Optional”	最長：64

“AP_Name”	“Value Required”	最長：32
“AP_Longitude”	“Value Required”	範囲：0 ～ ±180
“AP_Latitude”	“Value Required”	範囲：0 ～ ±90

ステップ 2 CSV ファイル名拡張子でファイルを保存した後、ブラウザからアクセスできる場所にそのファイルをコピーします。

ワイヤレス サイト マップで屋外位置を作成するための地理座標ファイルのインポート

アクセス ポイントを屋外位置に基づいてグループ化するには、各アクセス ポイントの緯度/経度座標を使用します。Prime Infrastructure にインポートできる必要なアクセス ポイントの地理座標ファイルを最初に作成する必要があります。アクセス ポイントの地理座標を含む Google KML ファイルまたは CSV ファイルを Prime Infrastructure にインポートできます。

ステップ 1 **[マップ（Maps）] > [Google Earth]** を選択します。

ステップ 2 **[コマンドの選択（Select a command）] > [Google KML のインポート（Import Google KML）] > [実行（Go）]**（または、CSV ファイルをインポートする場合は、**[コマンドの選択（Select a command）] > [CSV のインポート（Import CSV）] > [実行（Go）]** を選択します。

ステップ 3 KML、KMZ、または .CSV ファイルに移動し、[次へ（Next）] をクリックします。

選択したファイルが解析され、次の処理が行われます。

- アップロードしたファイルで指定されているアクセス ポイントの有効性（指定されたアクセス ポイントが Prime Infrastructure 内で使用できること）が検証されます。
- 傾斜、機首方位、範囲、および他の地理座標フィールドに対して、範囲の検証が実行されます。経度および緯度が指定されると、範囲の検証が実行されます。指定されていない場合、値はデフォルトで 0 になります。

ステップ 4 有効性チェックが正常に終了したら、ファイルの詳細を確認して [Save] をクリックします。

以前のアップロード情報が保存されている場合は、その情報が次のように上書きされます。

- 以前にフォルダをアップロードした場合は、そのフォルダの座標が更新されます。
- 以前にアクセス ポイントをアップロードした場合は、そのアクセス ポイントの座標が更新されます。
- フォルダ内の既存のアクセス ポイントは削除されません。

• 必要に応じて、新しいフォルダが作成され、アクセスポイントが適宜配置されます。

Google Earth のロケーション起動ポイントをアクセス ポイントの詳細に追加する

Google Earth ロケーション起動ポイントを [アクセスポイント（Access Point）] の概要および詳細ページに追加することで、Prime Infrastructure 内の Google Earth ロケーション起動ポイントの数を増やすことができます。

ステップ 1 **[モニタ（Monitor）] > [ワイヤレステクノロジー（Wireless Technologies）] > [アクセスポイントの無線（Access Point Radios）]** の順に選択します。

ステップ 2 [Access Point] 概要ページで、ページ見出しの隣の [Edit View] リンクをクリックします。

ステップ 3 [Edit View] ページで、左側の列の [Google Earth Location] を強調表示し、[Show] をクリックします。

[Google Earth Location] 列見出しは [View Information] 列内に移動します。

ステップ 4 列の表示順序を変更するには、[Google Earth Location] エントリを強調表示して、必要に応じて [Up] または [Down] ボタンをクリックし、[Submit] をクリックします。

[Access Points] 概要ページに戻され、Google Earth 起動リンクが画面に表示されます。起動リンクは、[Access Points] 詳細ページの一般概要ページにも表示されます（[Monitor] > [Wireless Technologies] > [Access Point Radios] > [AP Name]）。

Google Earth のマップ設定

Google Earth Maps 機能用にアクセス ポイントを設定できます。

ステップ 1 **[マップ（Maps）] > [Google Earth]** を選択します。

ステップ 2 次のパラメータを設定します。

- 設定の更新：[（ネットワークからの更新（Refresh from Network）] チェックボックスをオンにして、オンデマンド更新を有効にします。このオプションは一度だけ適用されて、無効になります。ネットワーク内のアクセス ポイントの数によっては、リフレッシュに時間がかかることがあります。
- [Layers]：アクセス ポイント、アクセス ポイント ヒート マップ、およびアクセス ポイント メッシュ情報のレイヤ フィルタを選択して保存できます。チェックボックスをオンにして適切なレイヤをアクティブにし、[>] をクリックしてフィルタ ページを開きます。Google Earth が次の更新要求を送信する時点で、これらの設定が適用されます。

- [Access Points]：[AP Filter] ドロップダウン リストから、表示する情報（チャネル、Tx 電力レベル、カバレッジ ホール、MAC アドレス、名前、コントローラ IP、使用率、プロファイル、またはクライアント）を選択します。

  アクセス ポイント レイヤがオンになっていない場合は、データが返されず、エラー メッセージ（アイコンのない目印）が Google Earth に返されます。

- [AP Heatmap]：[Protocol] ドロップダウン リストから、[802.11a/n]、[802.11b/g/n]、[802.11a/n & 802.11b/g/n]、または [None] を選択します。[RSSI Cutoff] ドロップダウン リストからカットオフを選択します（-60 ～ -90 dBm）。

  802.11a/n と 802.11b/g/n の両方のプロトコルを選択した場合は、それら両方のヒート マップが生成され、互いに重なり合って配置されます。重なり順序は指定できません。このオーバーレイを防ぐには、Google Earth で個々のオーバーレイをオフにするか、Prime Infrastructure で [Google Earth の設定（Google Earth Settings）] で変更する必要があります。

- [AP Mesh Info]：[Link SNR]、[Packet Error Rate]、または [none] を選択します。[Link Color] ドロップダウン リストから、[Link SNR] または [Packet Error Rate] を選択します。[AP Mesh Info] をオンにすると、[Mesh Links] も自動的に表示されます。

ステップ 3 [設定の保存（Save Settings）] をクリックして変更を確定するか、または [キャンセル（Cancel）] をクリックして変更を保存せずにページを閉じます。

マップを使用したメッシュ アクセス ポイントのモニタ

メッシュ ネットワーク マップから、メッシュ アクセス ポイント（AP）の概要を表示することができます。この情報は、すべての AP に表示される情報（MAC アドレス、AP モデル、コントローラ IP アドレス、位置、AP の高さ、AP の稼働時間、および LWAPP の稼働時間）に追加して表示されます。

メッシュ AP の設定情報の概要と詳細をメッシュ ネットワーク マップから表示するには、次の手順を実行します。

ステップ 1 **[マップ（Maps）] > [サイト マップ（Site Maps）]** を選択します。

ステップ 2 モニタする AP を含むキャンパス、ビルディング、フロア領域、地下レベル、または屋外領域を選択します。

ステップ 3 AP の設定情報の概要を表示するには、マウス カーソルをモニタする AP 上に移動します。選択した AP の設定情報が記載されたダイアログボックスが表示されます。

ステップ 4 AP の設定情報の詳細を表示するには、マップに表示されている AP をダブルクリックします。AP の設定の詳細が表示されます。

AP に IP アドレスがある場合には、メッシュ AP ダイアログボックスの下部に [ping テストの実行（Run Ping Test）] リンクも表示されます。

ワイヤレス サイト マップを使用したメッシュ アクセス ポイント構成の表示

メッシュ アクセス ポイント（AP）の詳細な設定情報をメッシュ ネットワーク マップから表示するには、次の手順を実行します。

ステップ 1 **[マップ（Maps）] > [サイトマップ（Site Maps）]** を選択します。

ステップ 2 モニタする AP を含むキャンパス、ビルディング、フロア領域、地下レベル、または屋外領域を選択します。

ステップ 3 詳細な設定情報を表示する AP をダブルクリックします。

ステップ 4 次のいずれかのタブをクリックして、必要な情報を表示します。

- [一般（General）]：AP 名、MAC アドレス、AP の稼働時間、関連付けられているコントローラ（登録済みおよびプライマリ）の動作ステータス、ソフトウェア バージョンなど、メッシュ AP の全般的な設定を表示します。

  メッシュ AP のソフトウェア バージョンには、*m* の文字と *mesh* という単語をカッコで囲んだものが付加されます。

- [インターフェイス（Interface）]：メッシュ AP でサポートされるインターフェイスの設定詳細を表示します。インターフェイスのオプションは無線とイーサネットです。

- [メッシュリンク（Mesh Links）]：メッシュ AP の親およびネイバーの詳細（名前、MAC アドレス、パケットエラー率、およびリンクの詳細）を表示します。このページからリンク テストを開始することもできます。

- [メッシュリンク（Mesh Links）]：メッシュ AP の親およびネイバーの詳細（名前、MAC アドレス、パケットエラー率、およびリンクの詳細）を表示します。このページからリンク テストを開始することもできます。

ワイヤレス サイト マップでのデバイス詳細の表示

デバイスの詳細を表示するには、マップ上のデバイス アイコンにカーソルを移動します。

モニタ モードのアクセス ポイントは、他のアクセス ポイントと区別するために灰色のラベルで表示されます。

ワイヤレス ネットワーク サイト マップとは

ワイヤレス ネットワーク サイト マップは、Prime Infrastructure 内で、施設全体のアクセス ポイントと施設自体の物理的配置を表現したものです。1 つの物理キャンパスの階層、そのキャンパスを構成するビルディング、各ビルディングのフロア、およびその階層内のアクセス ポイントの物理的な場所によって、単一のワイヤレス ネットワーク マップが構成されます。

簡単なワイヤレス ネットワーク サイト マップの作成

アクセスポイントを配置してコントローラに接続し、そのコントローラを管理するようにPrime Infrastructure を設定したら、ネットワーク設計を作成します。

環境内のデバイスを追跡するには、そのネットワーク内のコントローラをポーリングするようにロケーションアプライアンスを設定し、さらに、特定のネットワーク設計と同期するように設定する必要があります。Prime Infrastructure とモビリティ サービス エンジン間の同期を実行する概念と手順については、『Cisco Mobility Services Engine Configuration Guide』を参照してください。

ステップ 1 SuperUser、Admin、または ConfigManager のアクセス権限で Prime Infrastructure にログインします。

ステップ 2 **[マップ（Maps）] > [サイトマップ（Site Maps）]** を選択します。

ステップ 3 新しいキャンパスと 1 つ以上のビルディングを作成します。

ステップ 4 ビルディングの 1 つで新しいフロア領域を作成します。

ステップ 5 フロア領域に配置するアクセス ポイントを選択します。

フロア領域に追加する各アクセス ポイントは、灰色の円で表され（アクセス ポイント名またはMAC アドレスのラベルが付与）、フロア マップの左上に並べられます。

ステップ 6 各アクセスポイントを適切な位置にドラッグします（アクセスポイントをクリックして再配置すると、その色が青色に変わります）。各アクセスポイントの横にある小さい黒矢印は、各アクセスポイントのSide A を表します。各アクセスポイントの矢印は、アクセスポイントの設置方向と一致している必要があります。（Side A はそれぞれの 1000 シリーズ アクセス ポイント上で明確に記されており、802.11a/n 無線とは関連なし）。

ステップ 7 アクセスポイントの方向矢印を調整するには、[Antenna Angle] ドロップダウン リストで適切な方向を選択します。

アクセスポイントの配置と方向は、実際のアクセスポイントの展開を直接反映している必要があります。反映していないと、システムによってデバイス位置を特定できません。

ステップ 8 各アクセス ポイントの配置と方向の調整が完了したら、[Save] をクリックします。

ステップ 9 各デバイス位置がネットワーク設計に正確に列挙されるまで、これらの手順を繰り返してキャンパス、ビルディング、およびフロアを作成します。

第 IV 部

ネットワークの監視

- ネットワーク モニタリングのセットアップ （283 ページ）
- デバイスのモニタリング （297 ページ）
- ワイヤレス デバイスのモニタ （303 ページ）
- デバイスおよびネットワークの健全性とパフォーマンスのモニタ （327 ページ）
- アラームとイベントのモニタリング （353 ページ）
- ネットワーク クライアントとユーザのモニタ （385 ページ）
- PfRv3 モニタリングを使用したネットワーク パフォーマンスのモニタ （421 ページ）
- ワイヤレス ネットワークのモニタ （431 ページ）
- モニタリング ツールの使用 （445 ページ）
- パフォーマンス グラフを使用したワイヤレスおよびデータセンターのパフォーマンスのモニタ （455 ページ）
- トラブルシューティング （459 ページ）
- オペレーション センターを使用した複数の Prime Infrastructure インスタンスのモニタ （469 ページ）
- 高度なモニタリング （485 ページ）
- レポートの管理 （489 ページ）

第 11 章

ネットワーク モニタリングのセットアップ

- ポートおよびインターフェイス モニタリングのセットアップ （283 ページ）
- Cisco ISE を使用した拡張ワイヤレス クライアント モニタリングのセットアップ （284 ページ）
- パフォーマンスのモニタリングを目的とした NAM および NetFlow データ収集のセットアップ （286 ページ）

ポートおよびインターフェイス モニタリングのセットアップ

デバイス ポートをモニタするには、ポート グループを作成し、モニタリング情報を Prime Infrastructure のダッシュボードに表示します。ポート グループとはインターフェイスの論理グループであり、提供される機能によってデバイス ポートをモニタできます。たとえば、WAN ポート用のポート グループを作成し、同じルータ上の内部分散ポート用に別のポート グループを作成できます。

グループを作成したら、次のステップの説明に従って、それらのポートのインターフェイス ヘルス モニタリング ポリシーを作成できます。

ステップ 1 **Monitor > Monitoring Tools > Monitoring Policies**を選択します。

ステップ 2 **My Policies** をクリックします。

ステップ 3 クリック **Add.**

ステップ 4 **Policy Types** の下にある **Interface Health** を選択します。

ステップ 5 **Device Selection** ドロップダウン リストから、**Port Group** を選択します。

ステップ 6 **User Defined** グループを選択して、**OK** をクリックします。

ステップ 7 ポリシー名を入力します。

ステップ 8 必要なパラメータとしきい値を選択し、必須フィールドに入力します。

ステップ 9 **OK** をクリックします。

ステップ 10 **Save and Activate** をクリックします。

ステップ 11 結果を表示するには、**Dashboards > Overview > Network Interface** を選択して、[上位 N 件のインターフェイス使用率（Top N Interface Utilization）] ダッシュレットを表示します。

ステップ 12 [上位 N 件のインターフェイス使用率（Top N Interface Utilization）] ダッシュレットを編集し、以前に作成したポート グループを追加します。

WAN インターフェイス モニタリングのセットアップ

WAN インターフェイス ポート グループを作成すると、特定のポート グループ内のあらゆる WAN インターフェイスを効率的にモニタできます。たとえば、多数の小規模ブランチ オフィスで低帯域幅の問題が生じている場合は、各ブランチ オフィスからの WAN インターフェイスをすべて含むポート グループを作成し、問題についてこのポート グループをモニタします。

Prime Infrastructure には、デフォルトとして、スタティック WAN インターフェイス ポート グループが用意されており、このグループにはヘルスモニタリングが自動的に展開されます。下記の手順は、次の作業の実行方法を示しています。

1. WAN インターフェイス ポート グループにインターフェイスを追加する。
2. [Site] ダッシュボードから WAN インターフェイスの使用率と可用性を確認する。

ステップ 1 WAN インターフェイス ポート グループにインターフェイスを追加するには：

a) [インベントリ（Inventory）] > [グループ管理（Group Management）] > [ポート グループ（Port Groups）] を選択します。

b) 左側のメニューから、**System Defined** > **WAN Interfaces** を選択します。

c) デバイスを選択して、**Add to Group** をクリックします。

ステップ 2 結果を表示するには：

a) **Dashboard Overview Add Dashlets** を選択します。

b) 次のいずれかをクリックします。

- **Top N WAN Interfaces by Utilization**
- **Top N WAN Interfaces with Issues**

Cisco ISE を使用した拡張ワイヤレス クライアント モニタリングのセットアップ

Prime Infrastructure は、ネットワーク上の有線クライアントとワイヤレス クライアントの両方を管理します。Cisco ISE を RADIUS サーバとしてクライアントの認証に使用する場合、Prime

InfrastructureはCisco ISEからクライアントについての追加情報を収集し、クライアント関連の情報すべてを Prime Infrastructure に提供して、単一のコンソールで表示可能にします。

ネットワーク内でポスチャ プロファイリングが実施されている場合、Prime Infrastructure は Cisco ISE と通信してクライアントのポスチャ データを取得し、クライアントの他の属性とともに表示します。Cisco ISE を使用してネットワーク内のクライアントやエンドポイントのプロファイリングを行う場合、Prime Infrastructure はプロファイルされたデータを収集して、クライアントの種類（iPhone、iPad、Android デバイス、その他のデバイス）を識別します。

Cisco ISE サーバを使用して、管理対象クライアントに関する拡張情報を取得できます。

（エンドポイント情報にアクセスするために）Prime Infrastructure が ISE サーバと統合されている場合は、以下の操作を実行できます。

- エンド ユーザのネットワーク セッション ステータスの確認。
- [User 360° View] を使用すると、ネットワーク アクセスに対するエンドユーザの認証や許可について可能性がある問題を特定できます。
- ユーザ アプリケーションとサイトの帯域使用率に関するトラブルシューティング。

Prime Infrastructure は、認証されたエンドポイントに対してのみ ISE プロファイリング属性を表示します。

Cisco アイデンティティ サービス エンジンの追加

Prime Infrastructure には最大 2 つの ISE を追加できます。ISE を 2 つ追加する場合、1 つをプライマリに、もう1つをスタンバイにする必要があります。スタンドアロン ノードを追加する場合は、1 つのスタンドアロン ノードだけを追加できます。2 つ目のノードは追加できません。

アイデンティティ サービス エンジンを追加するには、次の手順を実行します。

ステップ 1 **Administration > Servers > ISE Servers**を選択します。

ステップ 2 [コマンドの選択（Select a command）]ドロップダウン リストから、**Add ISE Server** を選択して **Go** をクリックします。

ステップ 3 必要フィールドに入力して、**Save** をクリックします。

クレデンシャルは ISE に対してローカルなスーパーユーザ クレデンシャルでなければなりません。それ以外の場合、ISE の統合は機能しません。

パフォーマンスのモニタリングを目的とした NAM および NetFlow データ収集のセットアップ

Prime Infrastructure の実装に保証ライセンスが含まれている場合は、NAM および NetFlow の設定を介してデータ収集を有効にする必要があります。これは、保証によって提供される追加のダッシュレット、レポート、その他の機能を取り込むために必要です。

NAM データ収集の有効化

ネットワーク解析モジュール（NAM）からデータを収集できるようにするには、NAMデータ収集を有効にする必要があります。これは、検出されたまたは追加した各 NAM に実行するか、またはすべての NAM に同時に実行することで行えます。

始める前に

各 NAM の HTTP/HTTPS クレデンシャルを指定する必要があります。「NAM HTTP/HTTPS クレデンシャルの追加」を参照してください。

ステップ 1 選択項目 **Services > Application Visibility & Control > Data Sources.**

ステップ 2 **NAM Data Collector** セクションで、データ収集を有効にするのに必要な NAM データソースを選択します。

ステップ 3 **Enable** をクリックします。

（注） NAM ポーリングを有効にした後、[アプリケーション（Application）] ダッシュボードから [上位 N のアプリケーション（Top N Application）] ダッシュレットの NAM データを確認できます。

NAMデータの収集を無効にするには、必要な（有効になっている）NAMまたはNAMデータソースを [NAM データ コレクタ（NAM Data Collector）] セクションから選択し、[無効化（Disable）] をクリックします。

NAM ポーリング パラメータの定義

NAM から収集するデータを指定できます。

ステップ 1 **Monitor > Monitoring Policies**を選択します。

ステップ 2 **Add** をクリックし、左側のサイドバー メニューの [ポリシー タイプ（Policy Types）] リストから **NAM Health** を選択します。

ステップ 3 データを収集する NAM デバイスを選択し、必要なフィールドに入力します。

ステップ 4 [パラメータとしきい値（Parameters and Thresholds）] で、NAM デバイスからポーリングするパラメータとしきい値条件を指定します。

ステップ 5 **Save and Activate** をクリックします。

NetFlow データ収集の有効化

NetFlow と Flexible NetFlow データの収集を開始するには、Prime Infrastructure にデータをエクスポートするように NetFlow 対応のスイッチ、ルータ、その他のデバイス（ISR/ASR）を設定する必要があります。次の表は、NetFlow 対応の各種デバイス、および NetFlow データを Prime Infrastructure にエクスポートするためのデバイスの設定方法を示しています。

次の表に、NetFlow サポートの概要の詳細情報を示します。

表 *27 : NetFlow* サポートの概要

デバイス タイプ	**NetFlow** をサポートしている **IOS** バージョン	サポートされる **NetFlow** エクスポート タイプ	**Prime Infrastructure** での **NetFlow** 設定	テンプレートの命名規則
Cisco ASR	IOS XE 3.11 ～ 15.4(1) S 以降 Easy PerfMon ベースの構成（EzPM）	TCP/UDP カンバセーション トラフィック アプリケーション応答時間（ART） 音声とビデオ HTTP URL 可視性 アプリケーション トラフィック統計	選択項目 **Services > Application Visibility & Control > Interfaces Configuration** 形式：V9 および IPFIX	Netflow-Traffic-Conv- Netflow-App-Traffic- Netflow-Traffic-Voice-Video- Netflow-URL- Netflow-Aggregated-Traffic-Stats-
	IOS XE 3.9、3.10	TCP/UDP カンバセーション トラフィック アプリケーション応答時間（ART） 音声とビデオ HTTP URL 可視性 AVC トラブル シューティング	選択項目 **Services > Application Visibility & Control > Interfaces Configuration** 形式：V9 および IPFIX	Netflow-Traffic-Host- Netflow-App-Traffic- Netflow-Voice-Video- Netflow-URL- Netflow-AVC-Troubleshooting-

デバイス タイプ	NetFlow をサポートしている IOS バージョン	サポートされる NetFlow エクスポート タイプ	Prime Infrastructure での NetFlow 設定	テンプレートの命名規則
Cisco ISR	15.1(3) T	TCP/UDP カンバセーション トラフィック 音声とビデオ	TCP/UDP：選択 **Configuration > Templates > Features & Technologies > CLI Templates > System Templates - CLI > Collecting Traffic Statistics** 音声ビデオ：Medianet Perfmon CLI テンプレートを使用。**Configuration>Templates>**機能とテクノロジ **>CLI Templates>System Templates-CLI>Medianet Perfmon** の選択 形式：V9	Netflow-Traffic-Conv- Netflow-Voice-Video-
	IOS XE 3.11 ～ 15.4(1) S 以降 Easy PerfMon ベースの構成（EzPM）	TCP/UDP カンバセーション トラフィック アプリケーション応答時間（ART） 音声とビデオ HTTP URL 可視性 アプリケーション トラフィック統計	選択項目 **Services > Application Visibility & Control > Interfaces Configuration** 形式：V9 および IPFIX	Netflow-Traffic-Conv- Netflow-App-Traffic- Netflow-Traffic-Voice-Video- Netflow-URL- Netflow-Aggregated-Traffic-Stats-
	IOS XE 3.9、3.10	TCP/UDP カンバセーション トラフィック アプリケーション応答時間（ART） 音声とビデオ HTTP URL 可視性 AVC トラブルシューティング	選択項目 **Services > Application Visibility & Control > Interfaces Configuration** 形式：V9 および IPFIX	Netflow-Traffic-Host- Netflow-App-Traffic- Netflow-Voice-Video- Netflow-URL- Netflow-AVC-Troubleshooting-

デバイス タイプ	NetFlow をサポートしている IOS バージョン	サポートされる NetFlow エクスポート タイプ	Prime Infrastructure での NetFlow 設定	テンプレートの命名規則
Cisco ISR G2	15.1(4) M および 15.2(1) T	TCP/UDP カンバセーション トラフィック アプリケーション応答時間（ART） 音声とビデオ	TCP/UDP、ART：MACE CLI テンプレートを作成。「IRS デバイスでの NetFlor の設定」を参照してください。 音声ビデオ：Medianet Perfmon CLI テンプレートを使用。選択項目 **Configuration > Templates > Features & Technologies > CLI Templates > System Templates - CLI >Medianet – PerfMon** 形式：V9	Netflow-Traffic-Conv- Netflow-App-Traffic- Netflow-Voice-Video-
	15.2(4) M および 15.3(1) T	TCP/UDP カンバセーション トラフィック アプリケーション応答時間（ART） 音声とビデオ	次のどちらかを選択します。**Services > Application Visibility & Control >Interfaces Configuration** 形式：V9 および IPFIX	Netflow-Traffic-Conv- Netflow-App-Traffic- Netflow-Voice-Video-
	15.4(1)T 以降 Easy PerfMon ベースの構成（EzPM）	TCP/UDP カンバセーション トラフィック アプリケーション応答時間（ART） 音声とビデオ HTTP URL 可視性	選択項目 **Services > Application Visibility & Control > Interfaces Configuration** 形式：V9 および IPFIX	Netflow-Traffic-Conv- Netflow-App-Traffic- Netflow-Traffic-Voice-Video- Netflow-App-Traffic-URL-
Cisco Catalyst 2000	15.0(2) UCP 以降	TCP/UDP カンバセーション トラフィック	カスタム CLI テンプレートを作成。「Catalyst 2000 スイッチにおける NetFlow エクスポートの設定」を参照してください。 形式：V5、V9	Netflow-Traffic-Conv-

デバイス タイプ	NetFlow をサポートしている IOS バージョン	サポートされる NetFlow エクスポート タイプ	Prime Infrastructure での NetFlow 設定	テンプレートの命名規則
Cisco Catalyst 3750-X、3560-X	15.0(1)SE IP ベースまたは IP サービス フィーチャ セット、およびネットワーク サービス モジュールを装備。	TCP/UDP カンバセーション トラフィック	カスタム CLI テンプレートを作成。「Catalyst 3000、4000、6000 スイッチ ファミリにおける NetFlow の設定」を参照してください。 形式：V9	Netflow-Traffic-Conv-
Cisco Catalyst 3850（有線）	15.0(1)EX 以降	TCP/UDP カンバセーション トラフィック 音声とビデオ	TCP/UDP：カスタム CLI テンプレートを作成。Catalyst 3000、4000、6000 スイッチ ファミリにおける NetFlow の設定。 音声ビデオ：Medianet Perfmon CLIテンプレートを使用。選択項目 **Configuration > Templates > Features & Technologies > CLI Templates > System Templates - CLI >Medianet – PerfMon** 形式：V9	Netflow-Traffic-Conv- Netflow-Voice-Video-
Cisco Catalyst 3850（ワイヤレス）	Cisco IOS XE Release 3SE（Edison）	TCP/UDP カンバセーション トラフィック	「Flexible NetFlow の設定」を参照してください。 形式：V9	Netflow-Traffic-Conv-
Cisco CT5760 コントローラ（ワイヤレス）	Katana 5760	TCP/UDP カンバセーション トラフィック	「アプリケーションの可視性および Flexible NetFlow」を参照してください。 形式：V9	Netflow-Traffic-Conv-

デバイス タイプ	NetFlow をサポートしている IOS バージョン	サポートされる NetFlow エクスポート タイプ	Prime Infrastructure での NetFlow 設定	テンプレートの命名規則
Cisco Catalyst 4500	15.0(1)XO および 15.0(2)SG 以降	TCP/UDP カンバセーション トラフィック 音声とビデオ	TCP/UDP：カスタム CLI テンプレートを作成。「Catalyst 3000、4000、6000 スイッチ ファミリにおける NetFlow の設定」を参照してください。 音声ビデオ：Medianet Perfmon CLI テンプレートを使用。選択項目 **Configuration > Templates > Features & Technologies > CLI Templates > System Templates - CLI >Medianet – PerfMon** 形式：V9	Netflow-Traffic-Conv- Netflow-Voice-Video-
Cisco Catalyst 6500	15.1(1)SY 以降	TCP/UDP カンバセーション トラフィック 音声とビデオ	TCP/UDP：カスタム CLI テンプレートを作成。「Catalyst 3000、4000、6000 スイッチ ファミリにおける NetFlow の設定」を参照してください。 音声ビデオ：Medianet Perfmon CLI テンプレートを使用。選択項目 **Configuration > Templates > Features & Technologies > CLI Templates > System Templates - CLI >Medianet – PerfMon** 形式：V9	Netflow-Traffic-Conv- Netflow-Voice-Video-

Catalyst 2000 スイッチにおける NetFlow エクスポートの設定

手動で Catalyst 2000 デバイスに NetFlow エクスポートを設定するには、次の手順に従って、ユーザ定義の CLI テンプレートを作成します。

ステップ 1 **Configuration > Templates > Features & Technologies > CLI Templates > CLI**を選択します。

ステップ 2 情報アイコンの上にマウス カーソルを移動し、**New** をクリックして新しい CLI テンプレートを作成します。

ステップ 3 新しい CLI テンプレートの名前を入力します（例：Prime_NF_CFG_CAT2K）。

ステップ 4 [Device Type] リストから、[Switches and Hubs] を選択します。

ステップ 5 [テンプレート詳細（Template Detail）] > [CLIコンテンツ（CLI Content）] テキスト ボックスに以下のコマンドを入力し、各自のネットワークの必要に応じてそれらを変更します（これらのコマンドは一例にすぎません）。

```
flow record PrimeNFRec
 match ipv4 protocol
 match ipv4 source address
 match ipv4 destination address
 match transport source-port
 match transport destination-port
 collect counter bytes long
 collect counter packets long
!
!
flow exporter PrimeNFExp
 destination 172.18.54.93
 transport udp 9991
 option exporter-stats timeout 20
!
!
flow monitor PrimeNFMon
 record PrimeNFRec
 exporter PrimeNFExp

interface GigabitEthernet3/0/1
  ip flow monitor PrimeNFMon input
```

ステップ 6 [新しいテンプレートとして保存（Save as New Template）] をクリックします。テンプレートを保存した後、デバイスに展開します。「Prime Infrastructure を使用して設定テンプレートを作成する方法」を参照してください。

Catalyst 3000、4000、6000 スイッチ ファミリにおける NetFlow の設定

Catalyst 3000/4000/6000 デバイスに手動で NetFlow を設定して TCP および UDP トラフィックをエクスポートするには、次の手順に従って、ユーザ定義の CLI テンプレートを作成します。

ステップ 1 選択項目 **Configuration > Templates > Features & Technologies > CLI Templates > CLI.**

ステップ 2 情報アイコンの上にマウス カーソルを移動し、**New** をクリックして新しい CLI テンプレートを作成します。

ステップ 3 新しい CLI テンプレートの名前を入力します（例：「Prime_NF_CFG_CAT3K_4K」）。

ステップ 4 [デバイス タイプ（Device Type）] リストから、[スイッチおよびハブ（Switches and Hubs）] を選択します。

ステップ 5 [テンプレート詳細（Template Detail）] > [CLIコンテンツ（CLI Content）] テキスト ボックスに以下のコマンドを入力し、各自のネットワークの必要に応じてそれらを変更します（これらのコマンドは一例にすぎません）。

```
flow record PrimeNFRec

 match ipv4 protocol

 match ipv4 source address

 match ipv4 destination address

 match transport source-port

 match transport destination-port

 collect counter bytes long

 collect counter packets long



flow exporter PrimeNFExp

 destination 172.18.54.93

 transport udp 9991

 option exporter-stats timeout 20
```

```
flow monitor PrimeNFMon

 record PrimeNFRec

 exporter PrimeNFExp


interface GigabitEthernet3/0/1

  ip flow monitor PrimeNFMon input
```

ステップ 6 [新しいテンプレートとして保存（Save as New Template）] をクリックします。テンプレートを保存した後、そのテンプレートをデバイスに展開します。「Prime Infrastructure を使用して設定テンプレートを作成する方法」を参照してください。

ISR デバイスにおける NetFlow の設定

ISR デバイスに手動で NetFlow を設定して MACE トラフィックをエクスポートするには、次の手順に従って、ユーザ定義の CLI テンプレートを作成します。

ステップ 1 選択項目 **Configuration > Templates > Features & Technologies > CLI Templates > CLI.**

ステップ 2 情報アイコンの上にマウス カーソルを移動し、**New** をクリックして新しい CLI テンプレートを作成します。

ステップ 3 新しい CLI テンプレートの名前を入力します（例：「Prime_NF_CFG_MACE」）。

ステップ 4 [デバイス タイプ（Device Type）] リストから、[ルータ（Routers）] を選択します。

ステップ 5 [テンプレート詳細（Template Detail）] > [CLI コンテンツ（CLI Content）] テキスト ボックスに以下のコマンドを入力し、ネットワークの必要に応じてそれらを変更します（これらのコマンドは一例にすぎません）。

```
flow record type mace mace-record

collect application name

collect art all

!

flow exporter mace-export

destination <PI_SERVER_IP_ADDRESS>
```

```
source GigabitEthernet0/1

transport udp 9991

!


flow monitor type mace mace-monitor

record mace-record

exporter mace-export

cache timeout update  600


class-map match-all PrimeNFClass

      match protocol ip

      exit


policy-map type mace mace_global

 class PrimeNFClass

 flow monitor mace-monitor

 exit

exit


interface GigabitEthernet 0/1

 mace enable
```

ステップ 6 [新しいテンプレートとして保存（Save as New Template）] をクリックします。テンプレートを保存した後、デバイスに展開します。「Prime Infrastructure を使用して設定テンプレートを作成する方法」を参照してください。

（注） NetFlow を使用したアプリケーション モニタリングの詳細については、次を参照してください。
https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Aug2014/CVD-ApplicationMonitoringUsingNetFlowDesignGuide-AUG14.pdf

第 12 章

デバイスのモニタリング

- ネットワーク トラフィックをモニタするパケット キャプチャのセットアップ （297 ページ）
- ジョブ ダッシュボードを使用したジョブの管理 （299 ページ）

ネットワークトラフィックをモニタするパケットキャプチャのセットアップ

複数の NAM からデータを集約する以外に、Prime Infrastructure を使用すると、複数の NAM および ASR を使用してネットワークの問題をアクティブに管理およびトラブルシューティングすることが簡単になります。

（注） この機能は、NAM および ASR に対してサポートされます。ASR でサポートされる最小の Cisco IOS XE バージョンの詳細については、『Cisco ASR 1000 Series Aggregation Services Routers Release Notes』を参照してください。

次のワークフローでは、ネットワーク オペレータが、複数のブランチで発生している一連の類似の認証違反をトラブルシューティングする必要があります。オペレータは認証問題の原因が進行中のネットワーク攻撃であると判断したため、各ブランチの NAM または ASR に対してパケット キャプチャ機能を実行し、次に疑いのあるトラフィックを検査するためにパケット デコーダを実行します。

（注） レガシー暗号は、プライムインフラストラクチャサーバの [**パケットキャプチャ (Packet Capture**)] 画面でのコピーまたはマージ機能の実行に役立つ、デフォルトで有効になっています。

コピー先/マージ機能が動作しない場合は、Prime Infrastructure の CLI で次のコマンドを入力して、手動で有効にする必要があります。

#admin ncs run ssh-server-security-legacy-algorithms enable

これらのアクションを実行した後、無効にする必要があります。次のコマンドを入力して無効にします。

admin# ncs run ssh-server-legacy-algorithms disable

ステップ 1 次の手順を実行して、キャプチャ セッションの定義を作成します。

a) **[モニタ（Monitor）]** > **[ツール（Tools）]** > **[パケット キャプチャ（Packet Capture）]** を選択して新しいキャプチャ セッションの定義を作成します。

b) 必要に応じて、[General] セクションに値を入力します。セッション定義に一意の名前を付け、キャプチャされたデータをどのように保存するかを指定します。フルパケットをキャプチャするには、[Packet Slice Size] に 0 と入力します。

c) キャプチャ対象トラフィックを特定の送信元または宛先 IP、VLAN、アプリケーション、またはポートに制限する場合は、[ソフトウェア フィルタ（Software Filters）] セクションで [追加（Add）] をクリックし、必要に応じてフィルタを作成します。ソフトウェア フィルタを作成しない場合、すべてがキャプチャされます。

d) [デバイス（Devices）] 領域で NAM およびそのデータ ポートを選択します。キャプチャ セッションが実行されているかどうかにかかわらず、NAM ごとに作成できるキャプチャ セッションは 1 つだけです。ASR とそのインターフェイス。

e) [作成（Create）] と [すべてのセッションの開始（Start All Sessions）] をクリックします。Prime Infrastructure により新しいセッション定義が保存され、指定した各デバイスに対して個別のキャプチャ セッションが実行されます。また、セッションがファイルとしてデバイスに保存され、[キャプチャ ファイル（Capture Files）] 領域にパケット キャプチャ ファイルのリストが表示されます。

ステップ 2 パケット キャプチャ ファイルを復号化するには、次の手順を実行します。

a) **[モニタ（Monitor）]** > **[ツール（Tools）]** > **[パケット キャプチャ（Packet Capture）]** を選択します。

b) NAM または ASR デバイスの PCAP ファイルを選択します。

c) [コピー先（Copy To）] を選択して PCAP ファイルを PI サーバにコピーします（デコード操作は PI サーバのファイルでのみ実行されます）。

d) [ジョブの表示（View Jobs）] をクリックしてコピー ジョブが正常に完了したことを確認します。

e) localhost フォルダを開いて新しいキャプチャ ファイルのチェックボックスを選択し、[復号化（Decode）] をクリックします。復号化されたデータが一番下のペインに表示されます。

f) TCP ストリームには、アプリケーション層に表示されるようにデータが表示されます。復号化されたファイルの TCP ストリームを表示するには、[パケット リスト（Packet List）] から TCP パケットを選択し、[TCP ストリーム（TCP Stream）] をクリックします。データは ASCII テキストまたは 16 進ダンプで表示できます。

ステップ 3 パケット キャプチャ セッションを再び実行するには、[キャプチャ セッション（Capture Sessions）] 領域でセッション定義を選択し、[開始（Start）] をクリックします。

ジョブ ダッシュボードを使用したジョブの管理

適切なユーザ アカウント権限が付与されている場合は、ジョブ ダッシュボードを使用して Prime Infrastructure ジョブを管理できます。ジョブ ダッシュボードを表示するには、**[管理（Administration）] > [ダッシュボード（Dashboards）] > [ジョブ ダッシュボード（Job Dashboard）]** の順に選択します。ここでは、ジョブが正常に完了したか、部分的に成功したか、または失敗したかを確認できます。

実行中のジョブの数が多すぎると、Prime Infrastructure ではリソースが使用可能になるまで他のジョブがキューに入れられます。これが原因で、スケジュールされているジョブがその通常の開始時刻を超えて遅延されると、そのジョブは実行されません。このジョブは手動で実行する必要があります。

一部のジョブでは承認が必要です。この場合は、Prime Infrastructure から、管理者権限が付与されているユーザに対し、ジョブがスケジュールされており承認が必要であることを通知するメールが送信されます。ジョブの承認後にジョブが実行されます。

次の表に、ジョブ ダッシュボードに表示されるボタンの説明を示します。

表 *28 :* ジョブ ダッシュボードのボタン

ボタン	説明
[ジョブの削除（Delete Job）]	ジョブ ダッシュボードからジョブを削除します。
[ジョブの編集（Edit Job）]	選択したジョブの設定を編集します。
[スケジュールの編集（Edit Schedule）]	シリーズのスケジュールを表示し、編集できるようにします（開始時刻、間隔、終了時刻）。 （注） スケジュール済みのジョブのスケジュールを編集すると、そのジョブのステータスが [承認待ち（Pending for Approval）] に変更されます。これは、ジョブを作成したユーザからの承認が編集のたびに必要になるためです。
[実行（Run）]	選択したジョブの新しいインスタンスを実行します。このボタンは、部分的に成功したジョブまたは失敗したジョブを再実行する場合に使用します。ジョブは、失敗したコンポーネントまたは部分的に成功したコンポーネントに対してのみ実行されます。

ボタン	説明
[中断（Abort）]	現在実行中のジョブを停止します。ただしこのジョブは後で再実行できます。すべてのジョブを中断することはできません。これに該当する場合、Prime Infrastructure がそのこのことを示します。
[シリーズをキャンセル（Cancel Series）]	現在実行中のジョブを停止し、このジョブを再実行できないようにします。ジョブがシリーズの一部の場合、今後の実行には影響しません。
[シリーズの一時停止（Pause Series）]	スケジュールされているジョブ シリーズを一時停止します。シリーズを一時停止にすると、（[実行（Run）]を使用して）そのシリーズのインスタンスを実行することはできません。
[シリーズの再開（Resume Series）]	一時停止になっていたスケジュール済みジョブ シリーズを再開します。

（注） [ジョブの削除（Delete Job）]、[中断（Abort）]、および[シリーズをキャンセル（Cancel Series）]ボタンは、システム ジョブとポーラー ジョブの場合は使用できません。

ジョブの詳細を表示するには、次の手順に従います。

ステップ 1 **[管理（Administration）]** > **[ダッシュボード（Dashboards）]** > **[ジョブ ダッシュボード（Job Dashboard）]** の順に選択します。

ステップ 2 [ジョブ（Jobs）]ペインで、基本的な情報（ジョブ タイプ、ステータス、ジョブ期間、次回開始時刻など）を取得するジョブ シリーズを選択します。

ステップ 3 ジョブ間隔を表示するには、ジョブ インスタンスのハイパーリンクをクリックします。

ジョブ ページ上部の [繰り返し（Recurrence）]フィールドに、ジョブの繰り返し頻度が表示されます。ジョブ間隔の詳細は、トリガーするすべてのジョブで追加されます。

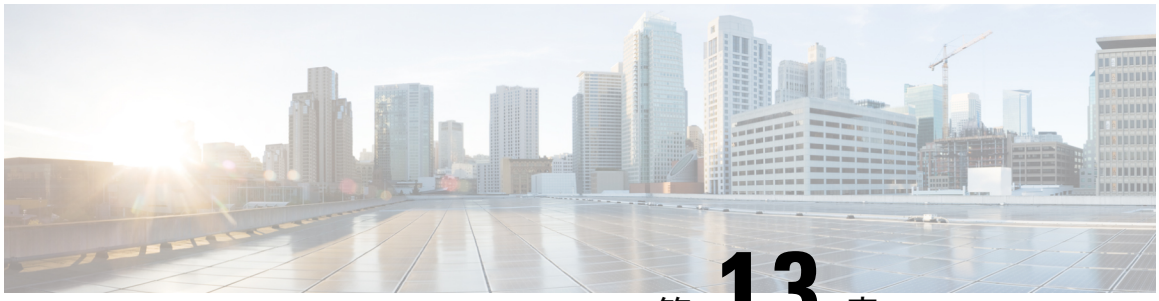
ステップ 4 失敗したジョブまたは部分的に成功したジョブに関する詳細を確認するには、ジョブ インスタンスのハイパーリンクをクリックし、結果ページに表示されるエントリを展開します。

これは特に、インベントリ関連のジョブで便利です。たとえば、ユーザがCSVファイルを使用してデバイスをインポートした場合（一括インポート）、ジョブは [ジョブ（Jobs）] サイドバー メニューの **[ユーザ ジョブ（User Jobs）]** > **[デバイスの一括インポート（Device Bulk Import）]** に表示されます。ジョブの詳細には、正常に追加されたデバイスと、追加されなかったデバイスのリストが表示されます。

例

失敗したソフトウェア イメージ インポート ジョブのトラブルシューティングを行うには、次の手順に従います。

1. [ジョブ（Jobs）] サイドバー メニューから、**[ユーザ ジョブ（User Jobs）] > [ソフトウェア イメージのインポート（Software Image Import）]** を選択します。
2. テーブルにある失敗したジョブを見つけ、そのハイパーリンクをクリックします。
3. ジョブの詳細がまだ展開されていない場合には展開し、このジョブに関連付けられているデバイスのリストと、各デバイスのイメージ インポートのステータスを表示します。
4. 特定デバイスのインポートの詳細情報を表示するには、[ステータス（Status）] 列でそのデバイスの [i]（**情報**）アイコンをクリックします。こうすると、[イメージ管理ジョブの結果（Image Management Job Results）] ポップアップ ウィンドウが開きます。
5. 各ステップとステータスを確認します。たとえば、[プロトコル SFTP を使用したイメージの収集（Collecting image with Protocol: SFTP）] 列に、そのデバイスで SFTP がサポートされていないことが示されることがあります。



第 13 章

ワイヤレス デバイスのモニタ

- コントローラのモニタ （303 ページ）
- アクセス ポイント無線 Air Time Fairness 情報の表示 （312 ページ）
- 不正アクセス ポイントとは （313 ページ）
- アドホック不正とは （320 ページ）
- Spectrum Expert からのアクセス ポイント干渉情報の表示 （322 ページ）
- WiFi TDOA レシーバのモニタ （323 ページ）
- [無線リソース管理（Radio Resource Management Dashboard）] ダッシュボードを使用した RF パフォーマンスの表示 （323 ページ）
- アクセス ポイントのアラームとイベントの表示 （324 ページ）

コントローラのモニタ

すべてのワイヤレス コントローラを表示するには、[モニタ（Monitor）] > [管理対象要素（Managed Elements）] > [ネットワークデバイス（Network Devices）] の順に選択し、次に [デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）] の順に選択します。

関連トピック

システム パラメータのモニタ （303 ページ）

システム パラメータのモニタ

すべてのワイヤレス コントローラを表示するには、[モニタ（Monitor）] > [管理対象要素（Managed Elements）] > [ネットワークデバイス（Network Devices）] の順に選択し、次に [デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）] の順に選択します。デバイス名をクリックすると、詳細が表示されます。

リリース 3.2 以降では、**[デバイスの詳細（Device Details）] > [システム（System）]** の下にある次の [モニタ（Monitor）] ページでは、デフォルトで Prime Infrastructure データベースからデータが取得されます。ページの右上隅にある [デバイスから更新（Refresh from Device）] リンクをクリックすると、デバイスから更新するオプションを使用できます。Prime Infrastructure でデータが最後に更新された日時も表示されます。

- 要約
- CDP ネイバー
- WLAN

リリース 3.2 以降では、**[デバイスの詳細（Device Details）] > [システム（System）]** の下にある次の [モニタ（Monitor）] ページでは、データがデバイスから直接取得されます。

- CLIセッション
- DHCP 統計情報

表 *29*：モニタ ネットワーク デバイス ワイヤレス コントローラの詳細

表示する内容	選択するメニュー
システム情報（System Information）	[デバイスの詳細（Device Details）] タブの [システム（System）] > [概要（Summary）]
IP アドレス、デバイス タイプ、場所、到達可能性ステータス、説明、デバイス総数などの要約情報	
CLI セッションの詳細	[デバイスの詳細（Device Details）] タブの [システム（System）] > [CLIセッション（CLI Sessions）]
送受信されたパケット、DHCP サーバ応答情報、最新の要求タイムスタンプなどの DHCP 統計情報（バージョン 5.0.6.0 以降のコントローラ向け）	[デバイスの詳細（Device Details）] タブの [システム（System）] > [DHCP統計情報（DHCP Statistics）]
マルチキャスト情報	[設定（Configuration）] タブの [システム（System）] > [マルチキャスト（Multicast）]
MAC アドレス、ロール、状態などのスタック情報	[デバイスの詳細（Device Details）] タブの [システム（System）] > [スタック（Stacks）]
STP 統計情報	[設定（Configuration）] タブの [システム（System）] > [スパニングツリープロトコル（Spanning Tree Protocol）]
ユーザ定義フィールドに関する情報	[デバイスの詳細（Device Details）] タブの [システム（System）] > [ユーザ定義フィールド（User Defined Field）]
コントローラで設定したワイヤレス ローカル アクセス ネットワーク（WLAN）	[デバイスの詳細（Device Details）] タブの [システム（System）] > [WLAN（WLANs）]
モビリティ（Mobility）	[デバイスの詳細（Device Details）] タブの [モビリティ（Mobility）] > [モビリティステータス（Mobility Stats）]
送受信エラー、ハンドオフ要求などのモビリティ グループ イベントの統計情報	
ポート	

表示する内容	選択するメニュー
選択したコントローラの物理ポートに関する情報	[設定（Configuration）] タブの [ポート（Ports）] > [全般（General）]
CDP インターフェイス	[設定（Configuration）] タブの [ポート（Ports）] > [CDPインターフェイスネイバー（CDP Interface Neighbors）]
セキュリティ	[デバイスの詳細（Device Details）] タブの [セキュリティ（Security）] > [RADIUSアカウンティング（RADIUS Accounting）]
RADIUS アカウンティング サーバ情報と統計情報	
RADIUS 認証サーバ情報	[デバイスの詳細（Device Details）] タブの [セキュリティ（Security）] > [RADIUS認証（RADIUS Authentication）]
ネットワーク アクセス コントロール リストに関する情報	**[System] > [Security] > [Network Access Control]**
ゲスト アクセスの展開とネットワーク ユーザ	[デバイスの詳細（Device Details）] タブの [セキュリティ（Security）] > [ゲストユーザ（Guest Users）]
管理フレーム保護（MFP）の要約情報	[デバイスの詳細（Device Details）] タブの [システム（System）] > [セキュリティ（Security）] > [管理フレーム保護（Management Frame Protection）]
現在コントローラに適用されているすべての不正アクセス ポイント ルールのリスト。	[デバイスの詳細（Device Details）] タブの [システム（System）] > [セキュリティ（Security）] > [不正APルール（Rogue AP Rules）]
スリープ状態にあるクライアントのリスト。スリープ状態にあるクライアントとは、Web 認証に成功したゲスト アクセスを持ち、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るクライアントです。	[デバイスの詳細（Device Details）] タブの [セキュリティ（Security）] > [スリープ状態にあるクライアント（Sleeping Clients）]
IPv6	[設定（Configuration）] タブの [IPv6] > [ネイバーバインディングタイマー（Neighbor Binding Timers）]
IPv6 アドレス、リンク、MTU などを生成および取得するために、ホストまたはクライアントとルータの間で交換されたメッセージ数の統計情報。	
冗長性	[デバイスの詳細（Device Details）] タブの [システム（System）] > [冗長性の概要（Redundancy Summary）]
冗長性情報	
mDNS	

表示する内容	選択するメニュー
mDNS サービスおよびサービス プロバイダー情報のリスト。	[デバイスの詳細（Device Details）] タブの [mDNS] > [mDNSサービスプロバイダー（mDNS Service Provider）]

関連トピック

スパニング ツリー プロトコルとは （306 ページ）
管理フレーム保護とは （306 ページ）
不正アクセス ポイント ルールとは （306 ページ）

スパニング ツリー プロトコルとは

スパニング ツリー プロトコル（STP）はリンク管理プロトコルの 1 つです。Cisco WLAN ソリューションでは、メディア アクセス コントロール ブリッジ用に IEEE 802.1D 標準が実装されています。

スパニング ツリー アルゴリズムは、ステーション間の複数のアクティブ パスによって作成される、ネットワーク内の無用なループを避けるとともに、冗長性を備えています。STP では、任意の 2 台のネットワーク デバイス間で同時に 1 つのアクティブなパスのみが存在できますが（これによりループが防止されます）、初期リンクが障害になった場合のバックアップとして冗長リンクが確立されます。

スパニング ツリー プロトコルをサポートしていないコントローラは、WISM、2500、5500、7500、および SMWLC です。

管理フレーム保護とは

管理フレーム保護（MFP）は、802.11 管理フレームの認証を提供します。管理フレームを保護することにより敵対者を検知できるようになり、DoS 攻撃や、プローブのフラッディング、不正 AP の設置を検知でき、QoS および無線測定フレームへの攻撃を防止しネットワーク パフォーマンスへの影響を抑えます。

コントローラの 1 つ以上の WLAN で MFP が有効になっている場合、コントローラは各登録済みアクセス ポイントに、それらの WLAN についてアクセス ポイントが使用する各 BSSID の一意のキーを送信します。MFP が有効になっている WLAN 経由でアクセス ポイントによって送信された管理フレームは、フレーム保護情報要素（IE）で署名されます。フレームを変更しようとするとメッセージが無効になり、MFP フレームを検出するように設定されている受信側アクセス ポイントが WLAN コントローラに不一致を報告します。

不正アクセス ポイント ルールとは

不正アクセス ポイント ルールは、認証タイプ、一致する設定された SSID、クライアント カウント、および RSSI 値などの条件に基づいて、不正なアクセス ポイントを自動的に分類します。Prime Infrastructure では、不正アクセス ポイントの分類ルールをコントローラおよびそれぞれのアクセス ポイントに適用します。

これらのルールでは、RSSI レベル（それよりも弱い不正アクセス ポイントを無視）、または時間制限（指定された時間内に表示されない不正アクセス ポイントにはフラグを立てない）に基づいて、マップ上の不正表示を制限できます。

不正アクセス ポイントのルールは、誤アラームを減らすのにも役立ちます。

不正クラスには以下の種類があります。

- [悪意のある不正（Malicious Rogue）]：検出されたアクセス ポイントのうち、ユーザが定義した Malicious ルールに一致したアクセス ポイント、または危険性のないアクセス ポイント カテゴリから手動で移動されたアクセス ポイント。
- [危険性のない不正（Friendly Rogue）]：既知、認識済み、または信頼できるアクセス ポイント、または検出されたアクセス ポイントのうち、ユーザが定義した Friendly ルールに該当するアクセス ポイント。
- [未分類の不正（Unclassified Rogue）]：検出されたアクセス ポイントのうち、Malicious ルールにも Friendly ルールにも該当しないアクセス ポイント。

関連トピック

システム パラメータのモニタ （303 ページ）

サードパーティ製コントローラに関するシステム詳細の表示

Prime Infrastructure によって管理されているサードパーティ（シスコ以外の）コントローラに関する詳細情報を表示するには、[モニタ（Monitor）] > [管理対象要素（Managed Elements）] >[ネットワークデバイス（Network Devices）]>[サードパーティワイヤレスコントローラ（Third Party Wireless Controllers）] の順に選択します。

スイッチ コントローラに関するシステム詳細の表示とスイッチ リストの設定

スイッチに関する次の詳細情報を表示するには、[モニタ（Monitor）]>[管理対象要素（Managed Elements）] > [ネットワークデバイス（Network Devices）] > [スイッチとハブ（Switches and Hubs）] の順に選択します。

- スイッチの検索

特定のスイッチを検索するか、またはカスタム検索を作成して保存するには、Prime Infrastructure の検索機能を使用します。

- スイッチの表示

[スイッチリスト（Switch List）] ページの設定

[Edit View] ページでは、[Switches] テーブルの列を追加、削除、または並べ替えができます。

テーブルの列を編集する手順は、次のとおりです。

ステップ 1 [モニタ（Monitor）] > [管理対象要素（Managed Elements）] > [ネットワーク デバイス（Network Devices）] > [スイッチとハブ（Switches and Hubs）] の順に選択します。

ステップ 2 [Edit View] リンクをクリックします。

ステップ 3 テーブルに新しい列を追加するには、左側の列で、追加する列見出しをクリックして強調表示します。[Show] をクリックして、選択した列見出しを右側の領域へ移動します。右側の領域にあるすべての項目が表に表示されます。

ステップ 4 テーブルから列を削除するには、右側の列で、削除する列見出しをクリックして強調表示します。[Hide] をクリックして、選択した列見出しを左側の領域へ移動します。左側の領域にある項目はすべて、表に表示されません。

ステップ 5 [Up] ボタンと [Down] ボタンを使用して、表内での情報の並び順を指定します。目的の列見出しを選択し、[Up] または [Down] をクリックして、現在のリスト内での位置を変更します。

ステップ 6 デフォルト表示に戻すには、[Reset] をクリックします。

ステップ 7 [Submit] をクリックして、変更内容を確定します。

モニタ アクセス ポイント

この項では、コントローラのアクセス ポイントの概要の詳細へのアクセスについて説明します。それぞれのアクセス ポイントの詳細にアクセスするには、メインの日付領域を使用します。

このページにアクセスするには、[モニタ（Monitor）] > [ワイヤレス テクノロジー（Wireless Technologies）] > [アクセス ポイントの無線（Access Point Radios）] の順に選択します。

関連トピック

アクセス ポイントの表示 （308 ページ）
アクセス ポイントに関するシステムの詳細の表示 （311 ページ）

アクセス ポイントの表示

デフォルト情報を含むアクセス ポイントの概要を表示するには、[モニタ（Monitor）] > [ワイヤレステクノロジー（Wireless Technologies）]>[アクセスポイントの無線（Access Point Radios）] の順に選択するか、またはアクセス ポイントの検索を実行します。

関連トピック

アクセス ポイントのレポート タイプ （309 ページ）
スイッチ コントローラに関するシステム詳細の表示とスイッチ リストの設定 （307 ページ）

アクセス ポイントのレポート タイプ

次のレポートは、アクセスポイントに対して生成できます。次のレポートは、カスタマイズできません。

- [ロード（Load）]：トラフィック負荷は、トラフィックの送受信のために使用される合計帯域幅です。これにより、WLAN管理者は、ネットワークの拡大状況を追跡し、クライアントの需要を見越してネットワーク拡張の計画を立てることができます。
- [Dynamic Power Control]：動的電力制御情報が含まれるレポートを生成します。
- [Noise]：ノイズ情報が含まれるレポートを生成します。ノイズ レポートには、選択したアクセス ポイントの各チャネルのノイズ（dBm 単位の RSSI）の棒グラフが表示されます。
- [干渉（Interference）]：[干渉（Interference）] レポートには、各チャネルの干渉（dBm 単位の RSSI）の棒グラフが表示されます。
  - 高干渉：40 ～ 0 dBm
  - 中程度干渉：100 ～ -40 dBm
  - 低干渉：110 ～ -100 dBm
- [カバレッジ（RSSI）（Coverage (RSSI)）]：[カバレッジ（RSSI）（Coverage (RSSI)）] レポートには、クライアント数対 dBm 単位の RSSI を示す、受信信号強度ごとのクライアント分布の棒グラフが表示されます。
- [カバレッジ（SNR）（Coverage (SNR)）]：[アクセスポイントのカバレッジ（SNR）（Access Points Coverage (SNR)）] レポートには、クライアント数対 SNR を示す、信号対雑音比ごとのクライアント分布の棒グラフが表示されます。
- [アップ/ダウン統計情報（Up/Down Statistics）]：[アップ/ダウン統計情報（Up/Down Statistics）] レポートには、時間に対するアクセス ポイントのアップ タイムの折れ線グラフが表示されます。最後のリブートからの経過時間（日数、時間、および分単位）。
- [ネットワークエアタイムフェアネス統計情報（Network Airtime Fairness Statistics）]：[ネットワークエアタイムフェアネス統計情報（Network Airtime Fairness Statistics）] は、選択した時間間隔で複数の異なる WLAN プロファイルで使用された平均エアタイムの表形式の表示です。
- [音声統計情報（Voice Statistics）]：音声トラフィックによる無線使用率を示す、選択したアクセス ポイントのレポートを生成します。[音声統計情報（Voice Statistics）] レポートには、音声トラフィックごとの次の無線使用率の統計情報が表示されます。
  - アクセス ポイント名
  - 無線
  - 進行中のコール
  - 進行中のローミング コール
  - 使用中の帯域幅

Voice Statistics レポートは、CAC/WMM クライアントのみに適用されます。

- [音声TSMテーブル（Voice TSM Table）]：[音声トラフィックストリームメトリックテーブル（Voice Traffic Stream Metrics Table）] は、選択したアクセス ポイントと無線に対して生

成します。クライアント デバイスごとに、その音声トラフィック ストリームの QoS ステータス、PLR、および遅延が表示されます。

- [音声TSMレポート（Voice TSM Reports）]：[音声トラフィックストリームメトリックテーブル（Voice Traffic Stream Metrics Table）] レポートは、[音声トラフィックストリームメトリックテーブル（Voice Traffic Stream Metrics Table）] をグラフィカル表示したものです。ただし、複数のクライアントからのメトリックが選択したアクセスポイントのグラフ上で平均されています。
- [802.11のカウンタ（8o2.11 Counters）]：[8o2.11のカウンタ（8o2.11 Counters）] レポートには、MAC レイヤでのアクセス ポイントのカウンタが表示されます。エラー フレーム、フラグメント数、RTS/CTS フレーム数、再試行フレームなどの統計情報は、フィルタリング基準に基づいて生成され、MAC 層のパフォーマンス（および問題）を解釈するために役立ちます。
- [アクセスポイントのプロファイルステータス（Access Points Profile Status）]：[アクセスポイントのプロファイルステータス（Access Points Profile Status）] には、アクセス ポイントの負荷、ノイズ、干渉、およびカバレッジ プロファイルのステータスが表示されます。
- [電波品質と時間の対比（Air Quality vs. Time）]：[無線使用率（Radio Utilization）] レポートには、レポート生成時に使用したフィルタリング基準に基づき、アクセスポイント無線の使用率の傾向が表示されます。このレポートは、現在のネットワークのパフォーマンスを識別し、今後のスケーラビリティの必要性に応じて容量を計画するうえで役立ちます。[無線使用率（Radio Utilization）] レポートには、設定された期間の間のワイヤレス ネットワークの電波品質の指標が表示されます。
- [トラフィックストリームメトリック（Traffic Stream Metrics）]：[トラフィックストリームメトリック（Traffic Stream Metrics）] レポートは、指定したクライアントの現在および過去の Quality of Service（QoS）を無線レベルで判断する場合に役立ちます。また、パケット損失率、平均キューイング遅延、遅延パケットの配布、ローミング遅延などのアップリンクおよびダウンリンク統計情報も表示されます。
- [Tx Powerおよびチャネル（Tx Power and Channel）]：[Tx Powerおよびチャネル（Tx Power and Channel）] レポートには、レポートの生成時に使用したフィルタリング基準に基づき、デバイスのチャネル計画の割り当ておよび送信電力レベルの傾向が表示されます。予期しない動作やネットワークのパフォーマンスの問題を識別するために役立ちます。

Current Tx Power Level 設定は、最大伝導送信電力を制御します。最大使用可能送信電力は、設定されたチャネル、個々の国の規制、およびアクセス ポイントの機能に応じて異なります。アクセス ポイントの機能を確認するには、『Product Guide』または各モデルのデータ シートを参照してください。

[現在のTx Powerレベル（Current Tx Power Level）] の設定 1 は、アクセス ポイントの最大伝導電力設定を表します。以降の電力レベル（たとえば、2、3、4 など）は、直前の電力レベルからの約 50 %（または 3dBm）の送信電力の低下を表します。実際の電力低下は、アクセス ポイントのモデルによって若干異なる場合があります。

設定されたアンテナのゲイン、設定されたチャネル、および設定された電力レベルに基づき、特定の国の規制を超えないように、アクセス ポイントでの実際の送信電力が低減されることがあります。

割り当て方式に[グローバル（Global）]と[カスタム（Custom）]のいずれを選択したかにかかわらず、アクセスポイントでの実際の伝導送信電力は、国固有の規制を超えないように確認されます。

次のコマンド ボタンは伝送レベルを設定するために利用できます。

- [Save]：現在の設定を保存します。
- [Audit]：このアクセス ポイントの現在のステータスを検出します。
- [VoIPコールのグラフ（VoIP Calls Graph）]：[VoIPコールのグラフ（VoIP Calls Graph）]は、ネットワーク上の VoIP コール（無線ごと）の数と期間の詳細を時間とともに表示するなど、音声の観点からワイヤレス ネットワークの使用状況を分析します。このレポートから有益なデータを収集できるようにするには、WLAN で VoIP スヌーピングを有効にする必要があります。このレポートでは、グラフで情報が表示されます。
- [VoIPコールの表（VoIP Calls Table）]：[VoIPコールの表（VoIP Calls Table）]には、[VoIPコールのグラフ（VoIP Calls Graph）] レポートと同じ情報が表形式で表示されます。
- [音声統計情報（Voice Statistics）]：[音声統計情報（Voice Statistics）] レポートは、ネットワーク上の音声クライアント、ボイス コール、ローミング コール、および拒否されたコール（無線ごと）によって使用された帯域幅のパーセンテージなどの詳細を表示することで、音声の観点からワイヤレス ネットワークの使用状況を分析します。このレポートから有用なデータを収集するためには、コール アドミッション制御（CAC）が音声クライアントでサポートされていることを確認してください。
- [Worst Air Quality APs]：干渉の問題がネットワークに影響を与えている箇所を理解できるように、概要的なわかりやすいメトリックが提供されます。電波品質（AQ）はチャネル、フロア、およびシステム レベルで報告され、AQ が望ましいしきい値を下回った場合に自動的に通知されるように AQ アラートがサポートされています。

アクセス ポイントに関するシステムの詳細の表示

[アクセスポイントの詳細（Access Points Details）] ページでは、1 つのアクセス ポイントのアクセス ポイント情報を参照できます。

このページにアクセスするには、[Monitor] > [Wireless Technologies] > [Access Point Radios] を選択して、[AP Name] 列のアクセス ポイント名をクリックします。アクセス ポイントの種類に応じて、次のタブが表示されます。

- [全般（General）] タブ

[General] タブのフィールドは、Lightweight アクセス ポイントと Autonomous アクセス ポイントで異なります。

自律クライアントについては、Prime Infrastructure はクライアント数のみを収集します。[Monitor] ページとレポートのクライアント数には、自律クライアントが含まれています。クライアント検索、クライアント トラフィック グラフ、その他のクライアント レポート（[Unique Clients]、[Busiest Clients]、[Client Association] など）には、Autonomous アクセス ポイントからのクライアントは含まれていません。

- [インターフェイス（Interfaces）] タブ
- [CDP ネイバー（CDP Neighbors）] タブ

このタブは、CDP が有効になっている場合のみ表示されます。

- [現在関連付けられているクライアント（Current Associated Clients）] タブ

このタブは、アクセス ポイント（CAPWAP またはAutonomous アクセス ポイント）に関連付けられているクライアントがある場合にのみ表示されます。

- [SSID] タブ

このタブは、アクセス ポイントが Autonomous アクセス ポイントであり、アクセス ポイントで SSID が設定されている場合のみ表示されます。

- [一定期間のクライアント（Clients Over Time）] タブ

このタブには、次のチャートが表示されます。

- [アクセスポイントでのクライアント数（Client Count on Access Point）]：アクセス ポイントに現在関連付けられているクライアントの総数が、時間とともに表示されます。
- [アクセスポイントでのクライアントトラフィック（Client Traffic on Access Point）]：アクセスポイントに接続されているクライアントによって生成されたトラフィックが、時間とともに表示されます。

これらのチャートに表示される情報は、時間ベースのグラフに表示されます。時間ベースのグラフには、グラフ ページの上部に、6 時間、1 日、1 週間、2 週間、4 週間、3 ヵ月、6 ヵ月、1 年、およびカスタムを表示するリンク バーがあります。選択すると、そのタイム フレームのデータが取得され、対応するグラフが表示されます。

関連トピック

アクセス ポイントのレポート タイプ （309 ページ）

アクセス ポイント無線 Air Time Fairness 情報の表示

High Density Experience（HDX）向けの Cisco Air Time Fairness（ATF）を利用してネットワーク管理者は、定義したカテゴリでデバイスをグループにまとめて、一部のグループに、他のグループよりも頻繁に WLAN からトラフィックを受信させることができます。したがって、あるグループには他のグループよりも多くのエア タイムが割り当てられます。

Cisco ATF には次の機能があります。

- ユーザ グループまたはデバイス カテゴリに対して Wi-Fi のエア タイムを割り当てる
- Air Time Fairness は、ネットワークではなくネットワーク管理者が定義する
- 簡単な仕組みで通信時間を割り当てることができる
- WLAN の状態の変化に動的に対応できる
- サービス レベル契約を効率的に実行できる
- 各種の標準規格に準拠した Wi-Fi QoS のメカニズムを強化できる

ATF の統計情報をモニタするには、次の手順を実行します。

ステップ 1 **[モニタ（Monitor）] > [ワイヤレステクノロジー（Wireless Technologies）] > [アクセスポイントの無線（Access Point Radios）]** の順に選択します。

ステップ 2 [無線（Radio）] 列から、目的の無線名をクリックします。

アクセス ポイントの種類に応じて、異なるタブが表示されます。

ステップ 3 [アクセス ポイントの無線の詳細（Access Point Radio Details）] で、[エア タイム フェアネス（Air Time Fairness）] タブを選択します。

次のチャートが表示されます。

- [エア タイム絶対使用率（Air Time Usage Absolute）]：このチャートは、測定された時間間隔における、無線上での WLAN のエア タイム使用率をパーセンテージで表します。
  - カレンダー アイコンをクリックして、開始日と年、および終了日と年を選択するか、プリセット値を選択します。利用可能なプリセット値は、1h、6h、1d、1w、2w、4w、3m、6m および 1y です。
- [エア タイム相対使用率（Air Time Usage Relative）]：このチャートは、無線上での WLAN 全体のうち、ある WLAN のエア タイム使用率をパーセンテージで表します。
- カレンダー アイコンをクリックして、開始日と年、および終了日と年を選択するか、プリセット値を選択します。利用可能なプリセット値は、1h、6h、1d、1w、2w、4w、3m、6m および 1y です。

不正アクセス ポイントとは

不正なデバイスとは、ネットワーク内で管理対象のアクセス ポイントによって検出される、未知（管理対象外）のアクセス ポイントまたはクライアントのことです。不正なアクセス ポイントは、正規のクライアントをハイジャックし、プレーンテキストまたは他の DoS 攻撃や中間者攻撃を使用して無線 LAN の運用を妨害する可能性があります。つまり、ハッカーは、不正なアクセス ポイントを使用することで、ユーザ名やパスワードなどの機密情報を入手することができます。すると、ハッカーは一連の Clear To Send（CTS; クリア ツー センド）フレームを送信できるようになります。アクセス ポイントになりすましてこの CTS フレームが送信され、特定のクライアントには送信を許可し、他のすべてのクライアントには待機するように指示が送られると、正規のクライアントは、ネットワーク リソースに接続できなくなってしまいます。したがって、無線 LAN サービス プロバイダーは、境域からの不正なアクセス ポイントの締め出しに強い関心を持っています。

不正なアクセス ポイントは安価で簡単に利用できることから、企業の従業員は、IT 部門に報告して同意を得ることなく、許可されていない不正なアクセス ポイントを既存の LAN に接続し、アドホック無線ネットワークを確立することがあります。これらの不正なアクセス ポイントは、企業のファイアウォールの背後にあるネットワーク ポートに接続可能であるため、重大なネットワーク セキュリティ侵犯につながるおそれがあります。通常、従業員は不正なアクセス ポイントのセキュリティ設定を有効にしないので、権限のないユーザがこのアクセス ポイントを使って、ネットワーク トラフィックを傍受し、クライアント セッションをハイジャッ

クすることは簡単です。さらに警戒すべきことは、セキュリティで保護されていないアクセス ポイントの場所が無線ユーザにより頻繁に公開されるため、企業のセキュリティが侵害される可能性も増大します。

関連トピック

Cisco Prime Infrastructure が不正アクセス ポイントを検出する仕組み （314 ページ）
不正アクセス ポイント状態の判断方法 （315 ページ）
不正アクセス ポイント アラームの表示 （318 ページ）
アドホック不正とは （320 ページ）
不正アクセス ポイント クライアントの表示 （319 ページ）
Prime Infrastructure が不正アクセス ポイントを検索、タグ付け、および包含する方法 （321 ページ）

Cisco Prime Infrastructure が不正アクセス ポイントを検出する仕組み

コントローラは、すべての近隣のアクセス ポイントを継続的にモニタし、不正なアクセス ポイントおよびクライアントに関する情報を自動的に検出して収集します。コントローラで不正なアクセス ポイントが検出されると、不正ロケーション検出プロトコル（RLDP）を使用して、不正なアクセスポイントがネットワークに接続されているかどうかが判定されます。Prime Infrastructure は、すべてのコントローラの不正アクセス ポイント データを統合します。

管理者は、すべてのアクセス ポイント上、もしくはモニタ モード（受信専用）アクセス ポイント上でのみ、RLDP を使用するようコントローラを設定することが可能です。この後者のオプションでは、輻輳している RF 空間での不正なアクセス ポイントを簡単に自動検出できるようになります。そして、不要な干渉を生じさせたり、通常のデータ アクセス ポイント機能に影響を与えたりすることなく、モニタリングを行えるようになります。すべてのアクセス ポイントで RLDP を使用するようにコントローラを設定した場合、モニタ モード アクセス ポイントとローカル（データ）通信用アクセス ポイントの両方が近くにあると、コントローラは常に RLDP 処理用アクセス ポイントとして、モニタ モード アクセス ポイントを選択します。ネットワーク上に不正があると RLDP で判断された場合は、検出された不正を手動で封じ込め処理を行うことも、自動的に封じ込め処理を行うこともできます。

不正アクセス ポイントのパーティションは、検出中のいずれかのアクセス ポイント（最新または最も強い RSSI 値を持つアクセス ポイント）と関連付けられます。検出中のアクセス ポイント情報がある場合、Prime Infrastructure は検出中のコントローラを使用します。不正アクセス ポイントが異なるパーティションに存在する 2 つのコントローラによって検出された場合、不正アクセス ポイントのパーティションは随時変更される場合があります。

関連トピック

不正アクセス ポイントとは （313 ページ）
不正アクセス ポイント状態の判断方法 （315 ページ）
不正アクセス ポイント アラームの表示 （318 ページ）
アドホック不正アクセス ポイント アラームの表示 （320 ページ）

不正アクセス ポイント状態の判断方法

不正なアクセス ポイントの分類および報告は、不正の状態と、不正なアクセス ポイントの状態を自動的に移行できるようにする、ユーザ定義の分類規則に従って行われます。コントローラに対し、不正なアクセス ポイントを Friendly、Malicious、または Unclassified に分類して表示させる各種ルールを作成できます。

デフォルトでは、いずれの分類ルールも有効になっていません。したがって、すべての未知（管理対象外）のアクセス ポイントは Unclassified に分類されます。ルールを作成し、その条件を設定して、ルールを有効にすると、未分類のアクセスポイントは分類し直されます。ルールを変更するたびに、Alert 状態にあるすべてのアクセス ポイント（Friendly、Malicious、および Unclassified）にそのルールが適用されます。ルール ベースの分類は、アドホック不正クライアントおよび不正クライアントには適用されません。

5500 シリーズ コントローラは最大で 2000 個の不正（認知済みの不正情報含め）に対応します。4400 シリーズ コントローラ、Cisco WiSM、および Catalyst 3750G 統合型無線 LAN コントローラ スイッチは最大で 625 個の不正に対応します。2100 シリーズ コントローラおよびサービス統合型ルータのコントローラ ネットワーク モジュールは最大で 125 個の不正に対応します。各コントローラは、不正アクセス ポイントの封じ込めを無線チャンネルごとに 3 台（モニタ モード アクセス ポイントの場合、無線チャネルごとに 6 台）に制限します。

コントローラは、管理対象のアクセス ポイントの 1 つから不正レポートを受信すると、次のように応答します。

1. コントローラは、未知のアクセス ポイントが安全な MAC アドレスのリストに含まれているか確認します。そのリストに含まれている場合、コントローラはそのアクセス ポイントを Friendly として分類します。
2. 未知（管理対象外）のアクセス ポイントが危険性のない MAC アドレスのリストに含まれていない場合、コントローラは、不正状態の分類ルール適用処理を開始します。
3. 不正なアクセス ポイントが Malicious、Alert または Friendly、Internal または External にすでに分類されている場合は、コントローラはそのアクセス ポイントを自動的に分類しません。不正なアクセス ポイントがそれ以外に分類されており、Alert 状態にある場合に限り、コントローラはそのアクセス ポイントを自動的に分類し直します。
4. コントローラは、優先度の一番高いルールを適用します。不正なアクセス ポイントがルールで指定された条件に一致すると、コントローラはそのアクセス ポイントをルールに設定された分類タイプに基づいて分類します。
5. 不正なアクセス ポイントが設定されたルールのいずれにも一致しないと、コントローラはそのアクセス ポイントを Unclassified に分類します。
6. コントローラは、すべての不正なアクセス ポイントに対して上記の手順を繰り返します。
7. 不正なアクセス ポイントが社内ネットワーク上にあると RLDP で判断されると、ルールが設定されていない場合でも、コントローラは不正の状態を Threat とマークし、そのアクセス ポイントを自動的に Malicious に分類します。その後、不正なアクセス ポイントに対して手動で封じ込め処理を行うことができますが（不正を自動的に封じ込めるよう RLDP が設定されていない限り）、その場合は不正の状態が Contained に変更されます。不正なアクセス ポイントがネットワーク上にないと、コントローラによって不正の状態が Alert とマークされ、そのアクセス ポイントを手動で封じ込め処理を行うことができるようになります。

8. 必要に応じて、各アクセスポイントを本来とは異なる分類タイプや不正の状態に手動で変更することも可能です。

前述のように、コントローラでは、ユーザ定義のルールに基づいて未知（管理対象外）のアクセスポイントの分類タイプと不正の状態が自動的に変更されます。もしくは、未知（管理対象外）のアクセスポイントを本来とは異なる分類タイプと不正の状態に手動で変更することができます。

関連トピック

不正アクセス ポイントとは （313 ページ）
Cisco Prime Infrastructure が不正アクセス ポイントを検出する仕組み （314 ページ）
不正アクセス ポイントの分類方法 （316 ページ）

不正アクセス ポイントの分類方法

次の表に、未知のアクセスポイントに設定できる分類タイプや不正の状態の推移の組み合わせを示します。

表 *30*：設定可能な分類タイプ/不正の状態の推移

遷移元	目的
Friendly（Internal、External、Alert）	Malicious（Alert）
Friendly（Internal、External、Alert）	Unclassified（Alert）
Friendly（Alert）	Friendly（Internal、External）
Malicious（Alert、Threat）	Friendly（Internal、External）
Malicious（Contained、Contained Pending）	Malicious（Alert）
Unclassified（Alert、Threat）	Friendly（Internal、External）
Unclassified（Contained、Contained Pending）	Unclassified（Alert）
Unclassified（Alert）	Malicious（Alert）

不正の状態が Contained の場合、不正なアクセス ポイントの分類タイプを変更する前に、そのアクセス ポイントが封じ込められないようにする必要があります。不正なアクセス ポイントを Malicious から Unclassified に変更する場合は、そのアクセス ポイントを削除して、コントローラで分類し直せるようにする必要があります。

悪意のある不正アクセス ポイント

悪意のある不正アクセスポイントとは、システム内で検出される悪意のある信頼できないアクセスポイントまたは未知（管理対象外）のアクセスポイントです。また、これらの分類には、ユーザが定義した Malicious ルールに合致したアクセス ポイント、または危険性のないアクセス ポイント分類から手動で移動したアクセス ポイントも含まれます。

Prime Infrastructure ホーム ページの [セキュリティ（Security）] ダッシュボードには、過去 1 時間、過去 24 時間の各状態の悪意のある不正アクセス ポイントの数と、アクティブな悪意のある不正アクセス ポイントの総数が表示されます。

悪意のある不正アクセス ポイントの状態には次のものがあります。

- Alert：該当アクセスポイントがネイバーリストまたはユーザ設定の [危険性のないアクセスポイント（Friendly Access Point）] リストにないことを示します。
- Contained：未知（管理対象外）のアクセス ポイントが封じ込められています。
- Threat：未知（管理対象外）のアクセス ポイントがネットワーク上に発見され、WLAN のセキュリティに脅威を与えています。
- Contained Pending：リソースを利用できないため、封じ込め処理が遅延することを示します。
- Removed：この未知（管理対象外）のアクセス ポイントは以前検出されたものの、現在は見つかりません。

悪意のある不正アクセスポイントに関する詳細な情報を表示するには、いずれかの期間のカテゴリにある下線付きの数値をクリックします。

危険性のない不正アクセス ポイント

危険性のない不正アクセス ポイントとは、既知のアクセス ポイント、認知済みアクセス ポイント、または信頼されたアクセスポイントです。また、ユーザ定義の Friendly ルールと一致するアクセス ポイントを指します。危険性のない不正アクセス ポイントに対して封じ込め処理は実行できません。

ユーザのみが不正アクセス ポイントの MAC アドレスを [危険性のないアクセスポイント（Friendly Access Point）] リストに追加できます。Prime Infrastructure では、危険性のないアクセス ポイントの MAC アドレスはコントローラに適用されません。

Prime Infrastructure ホーム ページの [セキュリティ（Security）] ダッシュボードには、過去 1 時間および過去 24 時間の各状態の危険性のない不正アクセス ポイントの数と、アクティブな危険性のない不正アクセス ポイントの総数が表示されます。

危険性のない不正アクセス ポイントの状態には次のものがあります。

- Internal：不明なアクセス ポイントがネットワーク内に存在し、WLAN のセキュリティに脅威を与えない場合、手動で Friendly、Internal に設定します。たとえば、ラボ ネットワーク内のアクセス ポイントなどです。
- External：不明なアクセス ポイントがネットワーク外に存在し、WLAN のセキュリティに脅威を与えない場合、手動で Friendly、External に設定します。たとえば、近所のコーヒーショップ設置されているアクセス ポイントなどです。
- Alert：未知のアクセスポイントはネイバーリストにもユーザ設定の [危険性のないアクセスポイント（Friendly Access Point）] リストにもありません。

危険性のない不正アクセスポイントの詳細を参照するには、いずれかの分類期間にある下線付きの数字をクリックします。

[危険性のないアクセスポイント（Friendly Access Point）] リストから不正アクセス ポイントを削除するには、Prime Infrastructure とコントローラの両方で不正アクセス ポイントが [危険性の

ないアクセスポイント（Friendly Access Point）] リストから削除されることを確認します。不正アクセス ポイントを、[危険性のない内部アクセスポイント（Friendly Access Point Internal）] または [危険性のない外部アクセスポイント（Friendly Access Point External）] から [未分類アラート（Unclassified Alert）] または [悪意のあるアラート（Malicious Alert）] に変更します。

未分類の不正アクセス ポイント

不正アクセス ポイントは、[悪意のある（Malicious）] または [危険性のない（Friendly）] に分類されていない場合、未分類と呼ばれます。これらのアクセス ポイントは封じ込め処理を行うことができ、また、危険性のない不正なアクセス ポイント リストへ手動で変更することもできます。

Prime Infrastructure ホーム ページの [セキュリティ（Security）] ダッシュボードには、過去 1 時間および過去 24 時間の各状態の未分類の不正アクセス ポイントの数と、アクティブな未分類の不正アクセス ポイントの総数が表示されます。

未分類の不正アクセス ポイントの状態には次のものがあります。

- Pending：最初の検出で、不明なアクセス ポイントは 3 分間 Pending 状態に置かれます。この間に、管理対象のアクセス ポイントでは、不明なアクセス ポイントがネイバー アクセス ポイントであるかどうかが判定されます。
- Alert：未知のアクセス ポイントはネイバー リストにもユーザ設定の [危険性のないアクセスポイント（Friendly Access Point）] リストにもありません。
- Contained：未知（管理対象外）のアクセス ポイントが封じ込められています。
- Contained Pending：不明なアクセス ポイントが Contained とマークされましたが、リソースを使用できないため対処が遅れています。

詳細情報を参照するには、いずれかの分類期間にある下線付きの数字をクリックします。

関連トピック

不正アクセス ポイントとは （313 ページ）
Cisco Prime Infrastructure が不正アクセス ポイントを検出する仕組み （314 ページ）

不正アクセス ポイント アラームの表示

不正アクセス ポイント無線は、1 つ以上の Cisco 1000 シリーズ Lightweight アクセス ポイントによって検出された無認可のアクセス ポイントです。[不正アクセスポイントアラーム（Rogue Access Point Alarms）] ページを開くには、次の手順を実行します。

- 不正 AP を検索します。
- [Dashboard] > [Wireless] > [Security] に移動します。このページには、過去 1 時間と過去 24 時間に検出された不正アクセス ポイントがすべて表示されます。不正アクセス ポイント アラームを表示するには、不正アクセス ポイント番号をクリックします。
- [Alarm Summary] の [AP number] リンクをクリックします。

アラーム ページが複数ある場合は、ページ番号および他のページへ移動するためのスクロール矢印がページ上部に表示されます。スクロール矢印を使用して、その他のアラームを表示します。

不正アクセス ポイントのパーティションは、検出中のいずれかのアクセス ポイント（最新または最も強い RSSI 値を持つアクセス ポイント）と関連付けられます。検出中のアクセス ポイント情報がある場合、Prime Infrastructure は検出中のコントローラを使用します。不正アクセス ポイントが異なるパーティションに存在する 2 つのコントローラによって検出された場合、不正アクセス ポイントのパーティションは随時変更される場合があります。

Prime Infrastructure によるポーリング時に、一部のデータが変更または更新されることがあります。このため、表示される不正データの一部（[Strongest AP RSSI]、[No. of Rogue Clients]、[Channel]、[SSID]、および [Radio Types]）が不正の存続期間中に変わることがあります。

[不正アクセスポイントアラーム（Rogue Access Point Alarms）] リスト ページで、各不正アクセス ポイントに関するアラーム イベントの詳細を参照できます。

不正アクセス ポイント無線のアラーム イベントを確認するには、[モニタ（Monitor）] > [モニタリングツール（Monitoring Tools）] > [アラームおよびイベント（Alarms and Events）] の順に選択して、任意の行の矢印アイコンをクリックして [不正アクセスポイントアラームの詳細（Rogue Access Point Alarm Details）] ページを表示します。

[All Alarm Details] ページのフィールド（[No. of Rogue Clients] 以外）は、ポーリングを通じてデータが設定され、2 時間ごとに更新されます。不正クライアントの数はリアルタイムの数であり、不正アクセス ポイント アラームの [Alarm Details] ページにアクセスするたびに更新されます。

コントローラ（バージョン 7.4 または 7.5）がカスタムの不正アクセス ポイント アラームを送信すると、Prime Infrastructure は未分類の不正アラームとしてこれを表示します。これは、Prime Infrastructure がカスタムの不正アクセス ポイント アラームをサポートしていないためです。

Prime Infrastructure によるポーリング時に、一部のデータが変更または更新されることがあります。このため、表示される不正データの一部（[Strongest AP RSSI]、[No. of Rogue Clients]、[Channel]、[SSID]、および [Radio Types]）が不正の存続期間中に変わることがあります。

不正アクセス ポイント クライアントの表示

不正クライアントは、次のいくつかの方法で表示できます。

- Prime Infrastructure 機能を使用して不正クライアントを検索します。
- 該当する不正アクセス ポイントの [Alarm Details] ページから、特定の不正アクセス ポイントの不正クライアントのリストを表示します。該当する不正クライアントの不正 MAC アドレスをクリックし、[Rogue Client details] ページを表示します。
- 不正アクセス ポイントの [Alarms Details] ページで、[Select a command] ドロップダウン リストから [Rogue Clients] を選択します。

[Rogue Clients] ページには、クライアントの MAC アドレス、最終通信日時、現在のステータス、そのコントローラ、および関連付けられている不正アクセス ポイントが表示されます。

不正クライアントのステータスには、Contained（コントローラにより、攻撃しているデバイスの信号が認可されたクライアントに干渉しないように封じ込められています）、Alert（コントローラは即時アラートをシステム管理者に転送し、さらなる処置を求めます）、および Threat（不正は既知の脅威です）があります。不正アクセス ポイントの脅威が高いほど、高い封じ込め処理が必要です。

不正クライアントの**クライアント MAC アドレス**をクリックすると、[不正クライアントの詳細（Rogue Client details）] ページが表示されます。

関連トピック

不正アクセス ポイントとは （313 ページ）
不正アクセス ポイント アラームの表示 （318 ページ）
アドホック不正アクセス ポイント アラームの表示 （320 ページ）

アドホック不正とは

アドホック ネットワークで動作しているモバイル クライアントの MAC アドレスが認可された MAC アドレスのリストにない場合は、アドホックの不正であると識別されます。

関連トピック

アドホック不正アクセス ポイント アラームの表示 （320 ページ）
不正アクセス ポイント クライアントの表示 （319 ページ）

アドホック不正アクセス ポイント アラームの表示

[アドホック不正アラーム（Adhoc Rogue Alarms）] ページには、アドホック不正のアラーム イベントが表示されます。[アドホック不正アラーム（Adhoc Rogue Alarms）] ページにアクセスするには、次の手順を実行します。

- アドホック不正のアラームの検索を実行します。
- [ダッシュボード（Dashboard）] > [ワイヤレス（Wireless）] > [セキュリティ（Security）] に移動します。このページには、過去 1 時間と過去 24 時間に検出されたアドホック不正がすべて表示されます。アドホック不正の番号をクリックすると、アドホック不正のアラームが表示されます。

アラーム ページが複数ある場合は、ページ番号および他のページへ移動するためのスクロール矢印がページ上部に表示されます。これらのスクロール矢印を使用して、その他のアラームを表示します。

Prime Infrastructure によるポーリング時に、一部のデータが変更または更新されることがあります。このため、表示される不正データの一部（[Strongest AP RSSI]、[No. of Rogue Clients]、[Channel]、[SSID]、および [Radio Types]）が不正の存続期間中に変わることがあります。

[アドホック不正アラーム（Adhoc Rogue Alarms）] ページから、各アドホック不正に関するアラーム イベント情報を参照できます。不正アクセス ポイント無線は、Cisco 1000 シリーズ Lightweight AP によって検出された未許可のアクセス ポイントです。

アドホック不正無線のアラーム イベントを表示するには、[アドホック不正アラーム（Adhoc Rogue Alarms）] ページで該当する不正 MAC アドレスをクリックします。

Prime Infrastructure によるポーリング時に、一部のデータが変更または更新されることがあります。このため、表示される不正データの一部（[Strongest AP RSSI]、[No. of Rogue Clients]、[Channel]、[SSID]、[Radio Types] など）が不正の存続期間中に変更される可能性があります。

スイッチポートトレースは、重大度、状態などの不正の属性を更新しないので、不正がスイッチ ポート トレースを使用して検出された場合はアラームはトリガーされません。

Prime Infrastructure が不正アクセス ポイントを検索、タグ付け、および包含する方法

Prime Infrastructure は、不正なアクセス ポイント トラップとしてフラグを生成し、既知の不正アクセス ポイントを Cisco Unified Network Solution が監視している MAC アドレスで表示します。

オペレータは、それぞれの不正アクセス ポイントに最も近いアクセス ポイントの場所を示すマップを表示します。これらのアクセス ポイントは次のように分類されます。

- 既知または承認済みの不正アクセス ポイント（追加のアクションなし）
- アラートの不正アクセス ポイント（アクティブの場合は監視して通知）
- 封じ込められている不正アクセス ポイント

この組み込み型の検出、タギング、モニタリング、および封じ込めの機能を使用すると、システム管理者は、次に挙げる適切な処理を実行できます。

- 不正アクセス ポイントを特定します。
- 新しい不正アクセスポイントの通知を受け取ります（通路をスキャンして歩く必要なし）。
- 未知（管理対象外）の不正アクセスポイントが削除または認知されるまでモニタします。
- 最も近い場所の認可済みアクセスポイントを特定して、高速かつ効果的に誘導スキャンを行えるようにします。
- 1～4台のアクセスポイントから、不正アクセスポイントのクライアントに認証解除とアソシエーション解除のメッセージを送信して、不正アクセスポイントを封じ込めます。この封じ込め処理は、MAC アドレスを使って個々の不正アクセス ポイントに対して行うことも、企業サブネットに接続されているすべての不正アクセスポイントに対して要求することもできます。
- 不正アクセス ポイントにタグを付けます。
  - 不正アクセス ポイントが LAN の外部にあり、LAN または WLAN のセキュリティを脅かさない場合は認知します。
  - 不正アクセス ポイントが LAN または WLAN のセキュリティを脅かさない場合は容認します。
  - 不正アクセスポイントが削除または認識されるまで、未知（管理対象外）のアクセスポイントとしてタグ付けします。
- 不正アクセス ポイントを封じ込め処理済みとしてタグ付けし、1～4台のアクセス ポイントから、すべての不正アクセス ポイント クライアントに認証解除およびアソシエーション解除のメッセージを転送することにより、クライアントが不正アクセスポイントにアソシエートしないようにします。この機能は、同じ不正アクセスポイント上のすべてのアクティブなチャネルに適用されます。

関連トピック

不正アクセス ポイントを検出する Lightweight アクセス ポイントの識別 （322 ページ）

不正アクセス ポイントを検出する Lightweight アクセス ポイントの識別

不正アクセス ポイントを検出している Cisco Lightweight AP に関する情報を表示するには、アクセス ポイントの検出機能を使用します。

[不正アクセス ポイント アラーム（Rogue Access Point Alarms）] ページにアクセスするには、次の手順を実行します。

ステップ 1 [不正アクセス ポイント アラーム（Rogue Access Point Alarms）] ページを表示するには、次のいずれかを実行します。

- 不正アクセス ポイントの検索を実行します。
- [Dashboard] > [Wireless] > [Security] に移動します。このダッシュボードには、過去 1 時間と過去 24 時間に検出された不正アクセス ポイントがすべて表示されます。不正アクセス ポイント アラームを表示するには、不正アクセス ポイント番号をクリックします。
- [Alarm Summary] ボックスの [Malicious AP] の件数のリンクをクリックします。

ステップ 2 [不正アクセス ポイント アラーム（Rogue Access Point Alarms）] ページで、該当する不正アクセス ポイントの [不正 MAC アドレス（Rogue MAC Address）] をクリックします。[不正アクセス ポイント アラーム（Rogue Access Point Alarms）] の詳細ページが表示されます。

ステップ 3 [コマンドの選択（Select a command））] ドロップダウン リストから、**Detecting APs** を選択します。

ステップ 4 **Go** をクリックします。

いずれかのリスト項目をクリックすると、その項目に関するデータが表示されます。

関連トピック

Prime Infrastructure が不正アクセス ポイントを検索、タグ付け、および包含する方法 （321 ページ）

Spectrum Expert からのアクセス ポイント干渉情報の表示

Spectrum Expert クライアントは、リモート干渉センサーとして機能し、動的な干渉データを Prime Infrastructure に送信します。この機能により、Prime Infrastructure はネットワーク内の Spectrum Expert から詳細な干渉データと電波品質データを収集、保管、およびモニタできます。

[Monitor Spectrum Experts] ページにアクセスするには、次の手順を実行します。

[Services] > [Mobility Services] > [Spectrum Experts] の順に選択します。

左側のサイドバーのメニューから、[Spectrum Experts Summary] ページにアクセスできます。

WiFi TDOA レシーバのモニタ

WiFi TDOA レシーバは、追跡対象のタグ付き資産から送信される信号を受信するように設計された外部システムです。その後これらの信号は、資産の位置計算に役立つよう、Mobility Services Engine に転送されます。

関連トピック

WiFi TDOA レシーバによるタグ位置レポートの強化 （441 ページ）
Cisco Prime Infrastructure およびマップへの WiFi TDOA レシーバの追加 （442 ページ）

[無線リソース管理（Radio Resource Management Dashboard）]ダッシュボードを使用したRFパフォーマンスの表示

無線リソース管理（RRM）は Cisco Unified Wireless Network に組み込まれており、RF 環境で見つかったパフォーマンス上の問題をモニタし動的に修正します。Prime Infrastructure は、アクセス ポイントの送信電力またはチャネルが変化した際にトラップを受信します。こうしたトラップ イベントまたは RF の再グループ化などの同様のイベントは、Prime Infrastructure に記録され、イベント ディスパッチャによって保持されます。

RRM は、ネットワークに追加された新しいコントローラや Lightweight アクセス ポイントを自動的に検出して設定します。それは、アソシエートされている近くの Lightweight アクセス ポイントを自動的に調整して、カバレッジとキャパシティを最適化します。Lightweight アクセス ポイントは、使用国で有効なすべての 802.11b/g チャネルに加えて、他の地域で使用可能なチャネルも同時にスキャンできます。アクセス ポイントは、これらのチャネルのノイズや干渉を監視する際、最大で 60 ミリ秒の間オフチャネルになります。不正アクセス ポイント、不正クライアント、アドホック クライアント、干渉しているアクセス ポイントを検出するために、この間に収集されたパケットが解析されます。

次の通知は RRM ダッシュボードに送信されます。

- チャネルの変更通知は、チャネルの変更が発生すると送信されます。チャネルの変更は、動的チャネル割り当て（DCA）設定に左右されます。
- 送信電力の変更通知は、送信電力の変更が発生すると送信されます。原因コードは、イベントが発生した理由の数に関係なく、1 という係数が与えられます。

- RF グループ化通知は、RF グループ化のコンテンツの変更があり、自動グループ化がイネーブルの場合に送信されます。

RRM ダッシュボード情報を表示するには、[モニタ（Monitor）] > [ワイヤレステクノロジー（Wireless Technologies）] > [無線リソースの管理（Radio Resource Management）] を選択します。

アクセス ポイントのアラームとイベントの表示

ネットワークのアクセス ポイントのアラームをモニタリングするには、次の手順を実行します。

ステップ 1 次に対して詳細検索を実行します。

a) パフォーマンス アラーム
b) CleanAir セキュリティ アラーム
c) wIPS DoS アラーム

ステップ 2 アラームの横にあるチェックボックスを選択し、[アラーム ブラウザ（Alarm Browser）] ツールバーで必要なフィールドを変更します。

アクセス ポイント障害オブジェクトの表示

障害のあるオブジェクトをモニタリングするには、次の手順を実行します。

ステップ 1 [モニタ（Monitor）] > [モニタリングツール（Monitoring Tools）] > [アラームおよびイベント（Alarms and Events）] の順に選択し、[イベント（Events）] タブをクリックします。

ステップ 2 [Description]列の左側にある展開アイコンをクリックします。選択したイベントの種類に応じて、関連付けられている詳細が異なります。

アクセス ポイントの不正アクセス ポイントの表示

不正アクセス ポイントのイベントをモニタリングするには、次の手順を実行します。

ステップ 1 [モニタ（Monitor）] > [モニタリングツール（Monitoring Tools）] > [アラームおよびイベント（Alarms and Events）] の順に選択し、[イベント（Events）] タブをクリックします。

ステップ 2 不正 AP をモニタするには、クイック フィルタまたは高度なフィルタ機能を使用します。

ステップ 3 不正アクセス ポイント無線のアラーム イベントを表示するには、展開アイコンをクリックします。

アクセス ポイントのアドホック不正の表示

アドホック不正のイベントをモニタリングするには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	[モニタ（Monitor）] > [モニタリングツール（Monitoring Tools）] > [アラームおよびイベント（Alarms and Events）] の順に選択し、[イベント（Events）] タブをクリックします。	
ステップ 2	アドホック不正 AP のイベントをモニタするには、クイック フィルタまたは高度なフィルタ機能を使用します。	
ステップ 3	アドホック不正アクセス ポイントのアラーム イベントを表示するには、展開アイコンをクリックします。	

関連トピック

不正アクセス ポイントとは （313 ページ）

アクセス ポイントの適応型 wIPS イベントの表示

Cisco Adaptive wIPS のイベントをモニタリングするには、次の手順を実行します。

ステップ 1 [モニタ（Monitor）] > [モニタリングツール（Monitoring Tools）] > [アラームおよびイベント（Alarms and Events）] の順に選択し、[イベント（Events）] タブをクリックします。

ステップ 2 検索結果を絞り込んで wIPS イベントをモニタするには、クイック フィルタまたは高度なフィルタ機能を使用します。1 つ以上のイベントによって、異常ステートまたはアラームが生成されることがあります。アラームはクリアできますが、イベントは残ります。

アクセス ポイントの CleanAir 電波品質イベントの表示

ワイヤレス ネットワークの CleanAir 電波品質に関して生成されたイベントを表示するには、次の手順を実行します。

パフォーマンス イベントの詳細検索を実行します。

[詳細検索（Search Results）] ページには、重大度、障害の発生源、および日時に関する情報が表示されます。

次のタスク

電波品質イベントの詳細を表示するには、[電波品質イベント（Air Quality Events）] ページの [重大度（Severity）] 列の横にある展開アイコンをクリックします。

アクセス ポイントの干渉源セキュリティ リスク イベントの表示

干渉源セキュリティ リスク イベントをモニタリングするには、次の手順を実行します。

ワイヤレス ネットワークで生成されたセキュリティ リスク イベントを表示するには、セキュリティ イベントの詳細検索を実行します。

[詳細検索（Search Results）] ページには、重大度、障害の発生源、日時に関する次の CleanAir 電波品質イベントの情報が表示されます。

次のタスク

干渉原セキュリティ イベントの詳細を表示するには、[重大度（Severity）] 列の横にある展開アイコンをクリックします。

アクセス ポイントのヘルス モニタ イベントの表示

ヘルス モニタ イベントを表示するには、次の手順を実行します。

Prime Infrastructure イベントの詳細検索を実行します。

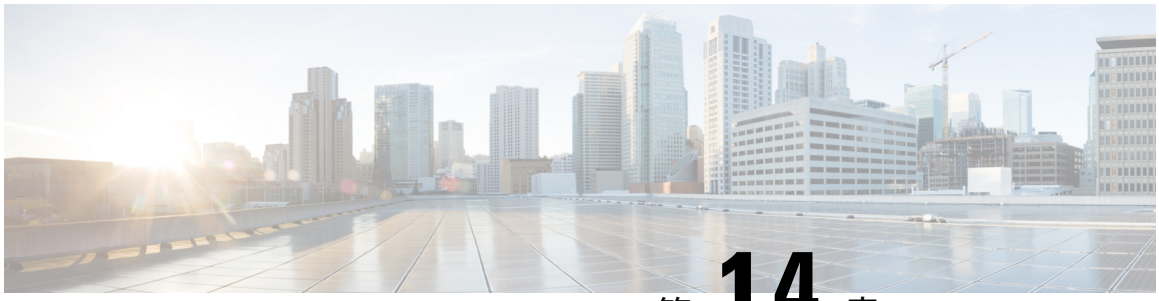
[検索結果（Search Results）] ページには、重大度、障害の発生源、メッセージ、および日時に関する情報が表示されます。

ヘルス モニタ イベントの詳細の表示

ヘルス モニタ イベントの詳細を表示するには、[重要度（Severity）] 列の隣にある展開アイコンをクリックし、アラームの詳細ページにアクセスします。

関連トピック

アクセス ポイントのヘルス モニタ イベントの表示 （326 ページ）



第 14 章

デバイスおよびネットワークの健全性とパフォーマンスのモニタ

この章は、次の内容で構成されています。

- デバイスのヘルスとパフォーマンスのモニタ方法：モニタリング ポリシー （327 ページ）
- 基本的なデバイス ヘルス モニタリングのセットアップ （329 ページ）
- 基本的なインターフェイス モニタリングの設定 （329 ページ）
- デフォルトのモニタリング ポリシー （330 ページ）
- ダッシュボードを使用したネットワークとデバイスの状態の確認 （334 ページ）
- Prime Infrastructure によるモニタリング対象のチェック （334 ページ）
- モニタリング ポリシーのデバイス、ポーリング、しきい値、およびアラーム設定の確認 （337 ページ）
- モニタ対象を調整する （338 ページ）
- 過去のモニタリング ポリシー データ収集のステータスの確認 （348 ページ）
- ポリシーでモニタするデバイス セットの変更 （348 ページ）
- モニタリング ポリシーのポーリングの変更 （349 ページ）
- モニタリング ポリシーのしきい値およびアラーム動作の変更 （349 ページ）
- レポートを使用したネットワーク パフォーマンスのモニタ （352 ページ）

デバイスのヘルスとパフォーマンスのモニタ方法：モニタリング ポリシー

モニタリング ポリシーは、Prime Infrastructure が以下を制御することによってどのようにネットワークをモニタするかを制御します。

- モニタ対象：Prime Infrastructure がモニタするネットワークとデバイスの属性。
- モニタ頻度：パラメータをポーリングするレート。
- 問題を指摘するタイミング：ポーリングする属性の受け入れ可能な値。

- 問題の指摘方法：しきい値を超えた場合に Prime Infrastructure がアラームを生成するかどうかとアラームの重大度。

モニタリング ポリシーは、モニタ対象の制御は別として、レポート、ダッシュボード、および Prime Infrastructure のその他の領域に表示可能なデータを決定する点で重要です。モニタリング ポリシーは、デバイス上の変更を行いません。

デフォルトで、デバイス ヘルス モニタリング（つまり、デバイス ヘルス モニタリング ポリシー）のみが有効になります。インターフェイス ヘルス モニタリングは、大規模な展開でシステム パフォーマンスを保護するためにデフォルトでは有効になりません。に記載された光モニタリング ポリシーを使用します。

次の手順は、モニタリング ポリシーの設定方法を要約したものです。

1. モニタリング ポリシー用のテンプレートとしてモニタリング **ポリシー タイプ**を使用し、ポリシーにわかりやすい名前を付けます。ポリシー タイプは、Prime Infrastructure に同梱されており、などのさまざまなテクノロジーとサービスのモニタリングを簡単に開始できるようにします。
2. ポリシーのポーリング頻度を調整するか、特定のパラメータのポーリングをすべて無効にします。
3. パラメータのしきい値を超えたときに Prime Infrastructure が生成する Threshold Crossing Alarm（TCA）を指定します。一部の TCA はデフォルトで設定されます。これらを調整または無効にしたり、新しい TCA を設定したりできます。
4. ポリシーでモニタするデバイスを指定します。デバイスは、ポリシー タイプに基づいてフィルタ処理されます。
5. ポリシーをアクティブにします。ポーリングされたデータが Web GUI のダッシュボード、レポート、[アラームおよびイベント（Alarms and Events）] テーブルなどの領域に表示されます。

モニタリング ポリシーを表示して管理するには、**[モニタ（Monitor）] > [モニタリング ツール（Monitoring Tools）] > [モニタリング ポリシー（Monitoring Policies）]** を選択します。

ナビゲーション	説明
自動監視（Automonitoring）	Prime Infrastructure でデフォルトで有効になるポリシーが一覧表示されます。デバイス ヘルス モニタリング ポリシーだけがデフォルトで有効になります。このポリシーの設定を調整できます。
マイ ポリシー（My Policies）	自分が作成したポリシーがここに表示されます。[マイ ポリシー（My Policies）] からポリシーを選択すると、そのポリシーの詳細を表示できます。

基本的なデバイス ヘルス モニタリングのセットアップ

デバイス ヘルス モニタリング ポリシーは、デフォルトで有効になっています。シスコ デバイスとサードパーティ デバイスの両方をモニタします。シスコ デバイスの場合、デバイス ヘルス モニタリングは管理対象デバイスで CPU 使用率、メモリ プールの使用率、環境温度、デバイスの可用性をチェックします。サードパーティ デバイスの場合、デバイス ヘルス モニタリングは管理対象デバイスの可用性のみをチェックします。このポリシーに、使用率や温度のしきい値を指定します。もしこのしきい値を超えた場合、GUI クライアントに表示されるアラームをトリガーします。

このポリシーの現在の設定を表示するには、**[モニタ（Monitor）] > [モニタリング ツール（Monitoring Tools）] > [モニタリングポリシー（Monitoring Policies）]** の順に選択し、左側のリストから [自動モニタ（Automonitoring）] を選択します。また、ポーリング頻度やさまざまなパラメータのしきい値を調整できます。ポーリング頻度やしきい値を調整するには、GUI クライアントに表示されるドロップダウン リストを使用します。

また、特定のデバイス（たとえば、特定のタイプのデバイスや特定の地理的場所に位置するデバイスなど）をモニタするデバイス ヘルス モニタリング ポリシーを作成することもできます。その実行方法については、モニタ対象を調整する （338 ページ）を参照してください。

基本的なインターフェイス モニタリングの設定

デフォルトでは、インターフェイスはモニタされません。これにより、多数のインターフェイスがあるネットワークのシステム パフォーマンスが保護されます。

インターフェイスのヘルス モニタリングは、シスコ デバイスとサードパーティ デバイスの両方に対して実行されます。シスコ デバイスの場合、インターフェイス ヘルス モニタリングは管理対象デバイスの入力使用率、出力使用率、入力キューのパーセンテージの低下、出力キューのパーセンテージの低下、および QoS をチェックします。サード パーティは、入力キューのパーセンテージの低下、出力キューのパーセンテージの低下、および QoS のモニタリングをサポートしていません。

基本的なインターフェイス モニタリングを設定するには、次の手順を使用します。

インターフェイス モニタリングを設定して有効するには、次の手順に従います。

ステップ 1 **[モニタ（Monitor）] > [モニタリング ツール（Monitoring Tools）] > [モニタリング ポリシー（Monitoring Policies）]** の順に選択し、左側のリストから [マイ ポリシー（My Policies）] を選択します。

ステップ 2 [追加（Add）] をクリックして、新しいポリシーを作成します。

ステップ 3 汎用インターフェイス モニタリングの場合は [インターフェイス ヘルス（Interface Health）] を選択します。

ポリシーを選択すると、Prime Infrastructure によりこのウィンドウにポリシー設定が読み込まれます。

ステップ 4 わかりやすい名前と説明を入力します。

ステップ 5 [デバイスの選択（Device Selection）] ドロップダウン リストから適切なオプション ボタンをクリックし、モニタするデバイスまたはデバイス グループを選択します。インターフェイス ヘルスのモニタリング ポリシーを選択した場合は、ポート グループも選択できます。

Prime Infrastructure では、ステップ 3 で選択したポリシーに該当するデバイスまたはポートのみが一覧表示されます。

次の点に注意してください。

- ポーリングとしきい値にデフォルト設定を使用するには、ステップ 8 に進みます。
- 現在のリリースの制約により Prime Infrastructure では、インターフェイス ヘルスのモニタリング ポリシーは、巡回冗長検査（CRC）エラーデータについて、選択したポート グループに関連付けられているインターフェイスだけでなく、ネットワーク内のすべてのインターフェイスをポーリングします。CRC エラーのデータを確認するときは、常にこのことに注意してください。

ステップ 6 インターフェイスのポーリング頻度を調整するには、[ポーリング頻度（Polling Frequency）] ドロップダウンリストから値を選択します。異なるパラメータのポーリング頻度を設定できるポリシーと、すべてのパラメータに 1 つのポーリング頻度だけが適用されるポリシーがあります。

ステップ 7 ポリシーで TCA カスタマイズがサポートされている場合は、しきい値を調整できます。モニタリング ポリシーのしきい値およびアラーム動作の変更 （349 ページ）を参照してください。

ステップ 8 次をクリックします。

- モニタリングを今すぐ開始する場合は、[保存してアクティブにする（Save and Activate）] をクリックします。
- ポリシーを保存して後でアクティブ化する場合は [保存して閉じる（Save and Close）] をクリックします。

デフォルトのモニタリング ポリシー

Prime Infrastructure は、[モニタ（Monitor）] > [モニタリングツール（Monitoring Tools）] > [モニタリングポリシー（Monitoring Policies）] > [自動モニタリング（Automonitoring）] の下で SNMP オブジェクトをポーリングし、次のヘルス モニタリング ポリシーのモニタリング情報を収集します。

- デバイス パラメータ：デバイス パラメータ自動モニタリング メトリックの表では、ポーリングされるデバイス ヘルス パラメータについて説明します。
- インターフェイス パラメータ：インターフェイス パラメータ自動モニタリング メトリックの表では、以下についてポーリングされるインターフェイス パラメータについて説明します。
  - トランク ポートおよびリンク ポート
  - WAN インターフェイス

保証情報を提供する次のモニタリング ポリシーの場合、データはNetFlow またはNAM を通じて収集されます。

- アプリケーション応答時間
- NAM 正常性
- トラフィック分析
- 音声ビデオ データ
- 音声ビデオ シグナリング

表 *31 :* デバイス パラメータ自動モニタリング メトリック

メトリック	ポーリングされるデバイス	MIB	含まれている MIB オブジェクト
デバイス アベイラビリティ	すべての SNMP デバイス、サードパーティ製デバイス	SNMPv2-MIB	sysUpTime
CPU 使用率	Cisco IOS デバイス、サポート対象のすべての Nexus デバイス、Cisco UCS デバイス	CISCO-PROCESS-MIB	cpmCPUTotalPhysicalIndex cpmCPUTotal1minRev
	Cisco ASR デバイス	CISCO-ENTITY-QFP-MIB	
[メモリ プール使用率（Memory Pool Utilization）]	Cisco IOS デバイス、ISR デバイス。	CISCO-MEMORY-POOL-MIB	ciscoMemoryPoolName ciscoMemoryPoolType ciscoMemoryPoolUsed ciscoMemoryPoolFree
	サポート対象のすべての Cisco Nexus デバイス、Cisco UCS デバイス、および Cisco IOS XE デバイス	CISCO-PROCESS-MIB	cpmCPUTotalIndexcpmCPUMemoryUsedcpmCPUMemoryFree
	Cisco ASA デバイス、IOS XR および Edison デバイス	CISCO-ENHANCED-MEMPOOL-MIB	cempMemPoolTypecempMemPoolNamecempMemPoolUsedcempMemPoolFree
	Cisco IOS ASR デバイス	CISCO-ENTITY-QFP-MIB	ceqfpMemoryResTypeceqfpMemoryResInUseceqfpMemoryResFree

メトリック	ポーリングされるデバイス	MIB	含まれている MIB オブジェクト
[環境温度（Environment Temp）][1]	ASR、サポート対象のすべての Nexus デバイス、Cisco UCS デバイス	CISCO-ENVMON-MIB	entSensorValue
	Catalyst 2000、3000、4000、6000、ISR	CISCO-ENVMON-MIB	ciscoEnvMonTemperatureStatusValue

[1] スタック構成のスイッチ デバイスの場合、[環境温度（Environment Temp）] には各スタック構成インスタンスの温度が表示されます。

表 *32*：インターフェイス パラメータ自動モニタリング メトリック

メトリック	ポーリングされるデバイス	MIB	含まれている MIB オブジェクト
インターフェイスのアベイラビリティ	Cisco IOS デバイス、すべてのサポートされている Nexus デバイス、サードパーティ デバイス	IF-MIB	ifOperStatus
入力使用率	Cisco IOS デバイス、サードパーティ デバイス	IF-MIB、Old-CISCO-Interface-MIB	ifHCInBroadcastPkts, ifHCInMulticastPkts, ifInErrors, ifInDiscards, ifInUnknownProtos ifHCInBroadcastPkts, ifHCInMulticastPkts, locIfInputQueueDrops
出力使用率	Cisco IOS デバイス、サードパーティ デバイス	IF-MIB、Old-CISCO-Interface-MIB	ifHCOutBroadcastPkts、ifHCOutMulticastPkts、ifHCOutUcastPkts、ifOutDiscards、ifOutUnknownProtos、locIfOutputQueueDrops
QoS クラスあたりのドロップ パーセンテージ	Cisco IOS デバイス	IF-MIB、Old-CISCO-Interface-MIB	cbQosCMDropBitRate,cbQosCMPrePolicyBitRate

（注） locIfIn、outQueueDrops、および QOS モニタリングは、サードパーティ製デバイスではサポートされていません。

表 *33 :* クラスベース、*QoS*、ヘルス モニタリング メトリック

メトリック	ポーリングされるデバイス	MIB	含まれている MIB オブジェクト
QOS 計算	Cisco IOS デバイス	CISCO-CLASS-BASED-QOS-MIB	cbQosCMDropByte64 cbQosCMPostPolicyByte64 cbQosCMPrePolicyByte64
インターフェイス インバウンド エラー	Cisco IOS デバイス、サードパーティ デバイス	IF-MIB	ifInErrors
インターフェイス アウトバウンド エラー	Cisco IOS デバイス、サードパーティ デバイス	IF-MIB	ifOutErrors
インターフェイス インバウンドの破棄	Cisco IOS デバイス、サードパーティ デバイス	IF-MIB	ifInDiscards
インターフェイス アウトバウンドの破棄	Cisco IOS デバイス、サードパーティ デバイス	IF-MIB	ifOutDiscards

デフォルトのモニタリング ポリシーの変更

Prime Infrastructure のモニタリング ポリシーは、ネットワーク デバイスのメトリックを監視して、問題が操作に影響する前に条件を変更するよう警告します。デフォルトでは、Prime Infrastructure はサポート対象のルータ、スイッチ、およびハブとサードパーティ製デバイスのデバイス ヘルス メトリックのみをポーリングし、WAN インターフェイス、リンク、およびトランク ポートではインターフェイス ヘルス メトリックをポーリングします。ストレージ デバイスおよび UCS シリーズ デバイスではポーリングされません。しきい値に 3 回違反すると、Prime Infrastructure は重大アラームを生成します。そのアラームは [モニタ（Monitor）] > [モニタリング ツール（Monitoring Tools）] > [アラームおよびイベント（Alarms and Events）] ページに表示されます。

ポーリング頻度としきい値パラメータを変更またはディセーブルにするには、次の手順に従います。

ステップ 1 [Monitor] > [Monitoring Tools] > [Monitoring Policies] > [Automonitoring] の順に選択します。

ステップ 2 [Device Health] を選択し、目的どおりにポーリング頻度としきい値を変更します。

ステップ 3 次のいずれかをクリックします。

- ポリシーを保存して選択したデバイスで即座にアクティブ化する場合は [Save and Activate]。
- ポリシーを保存して後でアクティブ化する場合は [保存して閉じる（Save and Close）]。

ダッシュボードを使用したネットワークとデバイスの状態の確認

Prime Infrastructure は、デバイスとネットワークをモニタするためのさまざまなダッシュボードを提供します。ダッシュボードが提供できる内容の例を次に示します。

- ネットワーク全体のリアルタイムのステータス情報（到達不能なデバイス、ダウンしているインターフェイス、最新のアラームなど）。
- 履歴情報の要約（最も頻繁に発生するアラーム、メモリと CPU の使用率が最も高いデバイスとインターフェイスなど）。
- デバイス固有の情報（デバイスの可用性履歴、使用率、インターフェイス統計情報、アラームなど）。
- テクノロジー固有の情報。

（注） 「デバイスがメンテナンス状態に設定されると、CPUやメモリなどのメトリックのポーリングは発生しません。ただし、デバイスの可用性がポーリングされます。NAM デバイスの場合、ポーリングされるメトリックはありません。」

ダッシュボードの詳細については、ダッシュボードのセットアップと使用 （6 ページ） を参照してください。

Prime Infrastructure によるモニタリング対象のチェック

このトピックでは、次の情報を取得する方法について説明します。

- 有効化されているポリシー、そのステータス、およびその履歴。
- Prime Infrastructure がポーリングしている特定のパラメータ、ポーリング頻度、およびそのしきい値超過アラーム（TCA）の設定。
- ポリシーの作成者、およびポリシーのベースとして使用されたポリシー タイプ。

ポリシーによるポーリング対象、ポリシーの前回の実行時間、およびポリシーが現在アクティブかどうかを確認するには、**[モニタ（Monitor）]**>**[モニタリングツール（Monitoring Tools）]**>**[モニタリングポリシー（Monitoring Policies）]** を選択してから、[マイポリシー（My Policies）] を選択します。 Prime Infrastructure に、作成したモニタリング ポリシー、またはアクセス権のあるモニタリング ポリシーが、次の情報とともに一覧表示されます。

ポリシーのフィールド	説明
Name	ポリシー名（ポリシーの作成者が指定します）。ポリシーの作成者を確認するには、この表の後にある手順を参照してください。
[メッセージ（Message）]	ポリシーの説明（ポリシーの作成者が指定します）。
[タイプ（Type）]	このポリシーを作成するときに使用されたテンプレート（ポリシータイプ）。ポリシータイプの詳細については、デバイスのヘルスとパフォーマンスのモニタ方法：モニタリングポリシー（327ページ）を参照してください。
[ステータス（Status）]	[アクティブ（Active）] または [非アクティブ（Inactive）]
[しきい値（Threshold）]	ポリシーがパラメータしきい値をモニタし、TCA を生成するかどうか。「はい（Yes）」が表示される場合、この表の後にある手順を使用して TCA 設定を確認できます。
[有効化履歴（Activation History）]	アクティブなモニタリングポリシー：ポリシーが有効化された回数を表示し、次の情報が含まれる [有効化履歴（Activation History）] ポップアップ ウィンドウへのハイパーリンクを提供します。 • ポリシーが有効化された時間。 • 各ポリシー実行でポーリングされたデバイス。非常に長い一覧の場合は、マウスカーソルを一覧の [有効化対象（Activated for）] 列にホバーし、ポップアップ ウィンドウを起動します。 非アクティブなモニタリングポリシー：[使用できません（Not Available）] が表示されます。

ポリシーのフィールド	説明
[収集ステータス（Collection Status）]	アクティブなモニタリング ポリシー：次の情報が含まれる [収集ステータス（Collection Status）]ポップアップ ウィンドウへのハイパーリンクを提供します。 • 各ポリシー実行でポーリングされたパラメータ。非常に長い一覧の場合は、マウス カーソルを一覧の [パラメータ（Parameters）]列にホバーし、ポップアップ ウィンドウを起動します。 非アクティブなモニタリングポリシー：[使用できません（Not Available）]が表示されます。

ポーリング頻度と TCA の詳細を表示するには、[ポリシー（My Policies）]で、左側の一覧からポリシーを選択します。ポリシー タイプに応じて次の情報が表示されます。

ポリシーのフィールド	説明
全般情報（General Information）	名前、説明、作成者、ステータス、ポリシー タイプ（機能カテゴリ）。ポリシー タイプの詳細については、デバイスのヘルスとパフォーマンスのモニタ方法：モニタリング ポリシー（327 ページ）を参照してください。
[デバイスの選択（Device Selection）]	ポリシーがモニタするデバイス。
[ポーリング頻度（Polling Frequency）]	Prime Infrastructure がデバイス パラメータをポーリングする頻度。
[パラメータとしきい値（Parameters and Thresholds）]	ポーリングされたパラメータとその TCA 設定（ある場合）。TCA 設定を表示するには、パラメータ名の横にある矢印をクリックします。さまざまなポリシー タイプによってポーリングされるパラメータを表示する方法については、モニタリング ポリシーによりポーリングされるパラメータとカウンタの確認（337 ページ）を参照してください。

モニタリングポリシーによりポーリングされるパラメータとカウンタの確認

Prime Infrastructure によるモニタリング対象のチェック （334 ページ） 現在アクティブなモニタリングポリシーを確認する方法を説明します。ポリシーでポーリングされるパラメータを確認するには、次の手順に従います。

この手順では、次のパラメータを確認できます。

- 既存のポリシーにより（ポリシーがアクティブ/非アクティブであるかどうかに関係なく）ポーリングされるパラメータ。
- 1 つのポリシー タイプで使用されるパラメータ。ポリシーの作成前に、新しいポリシーでポーリングされる内容を確認する場合に便利です。

ステップ 1 **[モニタ（Monitor）] > [モニタリング ツール（Monitoring Tools）] > [モニタリング ポリシー（Monitoring Policies）]** を選択し、[マイ ポリシー（My Policies）] を選択します。Web GUI に、既存のアクティブなモニタリング ポリシーと非アクティブなモニタリング ポリシーのリストが表示されます。

ステップ 2 **既存のポリシーで使用されるパラメータを確認するには**：

- 最後にポーリングされたパラメータを確認するには、右側のウィンドウでポリシーを見つけ、[収集ステータス（Collection Status）] 列の [詳細（Details）] をクリックします。[収集データ（Collection Data）] ダイアログボックスの [パラメータ（Parameter）] 列のテキストにマウス カーソルを合わせます。ポーリングされたパラメータのリストが表示されます。
- パラメータとそのポーリング設定を確認するには、左側のナビゲーション エリアで [マイ ポリシー（My Policies）] を展開し、確認するポリシーを選択します。右側のウィンドウに、パラメータとそのポーリング設定が表示されます。

ステップ 3 **特定のポリシー タイプで使用されるパラメータを確認するには**：

a) [編集（Edit）] をクリックします。左側のナビゲーション エリアに、サポートされるポリシー タイプのリストが表示されます。

b) ポリシータイプを選択します。右側のウィンドウに、そのポリシーでポーリングされるパラメータと、デフォルトのポーリング設定および TCA 設定が表示されます。（モニタリング ポリシーの作成時にこれらの設定をカスタマイズできます。）

モニタリングポリシーのデバイス、ポーリング、しきい値、およびアラーム設定の確認

モニタリング ポリシーのしきい値とアラーム設定を確認するには、次の手順を実行します。

ステップ 1 **[モニタ（Monitor）] > [モニタリング ツール（Monitoring Tools）] > [モニタリング ポリシー（Monitoring Policies）]** を選択してから、[マイ ポリシー（My Policies）] を選択します。

ステップ 2 モニタリング ポリシーを選択し、[編集（Edit）] をクリックしてポリシーの詳細を開きます。

ステップ 3 ポリシーで監視するデバイスを確認するには、[デバイスの選択（Device Selection）] ドロップダウン リストをクリックします。監視されているデバイスは、チェック マークで示されます。デバイスを追加または削除するには、ポリシーでモニタするデバイス セットの変更 （348 ページ）を参照してください。

（注） デバイス ヘルス ポリシーを選択すると、[デバイスの選択（Device Selection）] ドロップダウン リストには、UCS B シリーズのデバイスだけが表示されます。

ステップ 4 ポリシーで使用されているポーリング間隔を確認するには、[ポーリング間隔（Polling Interval）] の設定をクリックします。パラメータごとのポーリングについては、個別のパラメータを展開して設定を確認します。ポーリングの設定を調整するには、モニタリング ポリシーのポーリングの変更 （349 ページ）を参照してください。

ステップ 5 ポリシーで使用されているしきい値とアラームの設定を確認するには、[ポーリングとしきい値（Polling and Thresholds）] 領域のパラメータを展開します。しきい値とアラームの設定を変更するには、モニタリング ポリシーのしきい値およびアラーム動作の変更 （349 ページ）を参照してください。

モニタ対象を調整する

Prime Infrastructure のモニタ対象を調整するには、次の表のガイダンスに従って、必要な最良の方法を見つけてください。

条件：		参照先：
Prime Infrastructure が必要なデータを収集している	ポーリング頻度を変更する必要がある	モニタリング ポリシーのポーリングの変更 （349 ページ）
	アラーム動作を調整する必要がある	モニタリング ポリシーのしきい値およびアラーム動作の変更 （349 ページ）
	モニタするデバイスを調整する必要がある	ポリシーでモニタするデバイス セットの変更 （348 ページ）

条件：		参照先：
Prime Infrastructure が必要なデータを収集してない	同様のモニタリング ポリシーがすでに存在する	既存のポリシーベースの新規モニタリング ポリシーの作成 （339 ページ）
	同様のモニタリング ポリシーは存在しないが、ポリシー タイプの1つにモニタするパラメータが含まれている	事前設定されたポリシー タイプを使用した新規モニタリング ポリシーの作成 （340 ページ）
	同様のモニタリング ポリシーは存在せず、どのポリシー タイプにもモニタするパラメータが含まれていない	サポートされないパラメータとサードパーティ デバイスを対象としたモニタリング ポリシーの作成 （346 ページ）
	サポートされていないデバイスまたはサードパーティ デバイスをモニタする必要がある	

既存のポリシー ベースの新規モニタリング ポリシーの作成

ステップ 1 現在のモニタ対象を調べて、新しいポリシーを作成する必要があるかどうかを確認します。Prime Infrastructure によるモニタリング対象のチェック （334 ページ）を参照してください。

ステップ 2 既存のポリシーの複製を作成します。

a) **[モニタ（Monitor）]>[モニタリング ツール（Monitoring Tools）]>[モニタリング ポリシー（Monitoring Policies）]** の順に選択し、左側にあるリストで [マイ ポリシー（My Policies）] をクリックします。
b) 複製するポリシーを見つけます。
c) ポリシーを選択し、[複製（Duplicate）] をクリックします。
d) [複製ポリシーの作成（Duplicate Policy Creation）] ダイアログで、親フォルダを選択し、ポリシーの名前と説明を入力して [OK] をクリックします。

ステップ 3 複製したポリシーに変更を加えます。

a) [マイ ポリシー（My Policies）] でポリシーを見つけます。
b) ポリシーを選択して、[編集（Edit）] をクリックします。
c) 必要に応じて、設定を変更します。参照先：

- ポリシーでモニタするデバイス セットの変更 （348 ページ）
- モニタリング ポリシーのポーリングの変更 （349 ページ）
- モニタリング ポリシーのしきい値およびアラーム動作の変更 （349 ページ）

ステップ 4 次をクリックします。

- ポリシーを保存し、選択したデバイスで即座にアクティブ化する場合には、[保存してアクティブにする（Save and Activate）]。

- ポリシーを保存して後でアクティブ化する場合は [保存して閉じる（Save and Close）]。

事前設定されたポリシータイプを使用した新規モニタリングポリシーの作成

ステップ 1 現在モニタされている対象を確認します。Prime Infrastructure によるモニタリング対象のチェック （334 ページ）を参照してください。

ステップ 2 **[モニタ（Monitor）] > [モニタリング ツール（Monitoring Tools）] > [モニタリング ポリシー（Monitoring Policies）]** を選択し、[追加（Add）] をクリックします。

ステップ 3 [ポリシー タイプ（Policy Types）] メニューから、使用するポリシー タイプ テンプレートを選択します。

ステップ 4 新しいポリシーを設定します。

a) [デバイスの選択（Device Selection）] ドロップダウン リストから、デバイス、デバイス グループ、またはポート グループを選択します。（すべてのモニタリング タイプをポート グループに適用できるわけではありません。）

b) 名前と連絡先を入力し、説明を編集します。

c) [パラメータとしきい値（Parameters and Thresholds）] で、ポーリング設定、パラメータ値、およびアラームの条件を設定します。モニタリング ポリシーのポーリングの変更 （349 ページ）およびモニタリング ポリシーのしきい値およびアラーム動作の変更 （349 ページ）を参照してください。

ステップ 5 次をクリックします。

- ポリシーを保存し、選択したデバイスで即座にアクティブ化する場合には、[保存してアクティブにする（Save and Activate）]。
- ポリシーを保存して後でアクティブ化する場合は [保存して閉じる（Save and Close）]。

GETVPN モニタリング ポリシー

GETVPN ポリシー タイプの場合、Prime Infrastructure は次の表に示すメトリックを使用します。

表 *34 :*

GETVPN モニタリング パラメータ	MIB	含まれている MIB オブジェクト
グループ名（Group Name） グループ ID（Group ID） グループ ID タイプ（Group ID Type） グループ ID の長さ（Group ID Length） キー サーバ ID（Key Server ID） グループ メンバー ID（Group Member ID） デバイスタイプ（Device Type） デバイスID （Device ID） デバイス ID タイプ（Device ID Type） デバイス ID の長さ（Device ID length） 登録済みキーサーバID（Registered Key Server ID） 登録済みキーサーバIDのタイプ（Registered Key Server ID Type） 登録済みキーサーバIDの長さ（Registered Key Server ID Length）	CISCO-GDOI-MIB	**gmGdoiGroupTable** cgmGdoiGroupName、cgmGdoiGroupIdValue、cgmGdoiGroupIdType、cgmGdoiGroupIdLength **cgmGdoiKeyServerTable** cgmGdoiGroupIdValue、cgmGdoiGroupIdType、cgmGdoiKeyServerIdValue、cgmGdoiKeyServerIdType、cgmGdoiKeyServerIdLength、cgmGdoiKeyServerActiveKEK、cgmGdoiKeyServerRekeysPushed **cgmGdoiKsKekTable** cgmGdoiGroupIdValue、cgmGdoiGroupIdType、cgmGdoiKeyServerIdValue、cgmGdoiKeyServerIdType、cgmGdoiKsKekIndex、cgmGdoiKsKekSPI、cgmGdoiKsKekSrcIdValue、cgmGdoiKsKekSrcIdType、cgmGdoiKsKekSrcIdLength、cgmGdoiKsKekDstIdValue、cgmGdoiKsKekDstIdType、cgmGdoiKsKekDstIdLength、cgmGdoiKsKekOriginalLifetime、cgmGdoiKsKekRemainingLifetime

GETVPN モニタリング パラメータ	MIB	含まれている MIB オブジェクト
	CISCO-GDOI-MIB	**cgmGdoiKsTekSelectorTable** cgmGdoiGroupIdValue、cgmGdoiGroupIdType、cgmGdoiKeyServerIdValue、cgmGdoiKeyServerIdType、cgmGdoiKsTekSelectorIndex、cgmGdoiKsTekSrcIdValue、cgmGdoiKsTekSrcIdType、cgmGdoiKsTekSrcIdLength、cgmGdoiKsTekDstIdValue、cgmGdoiKsTekDstIdType、cgmGdoiKsTekDstIdLength **cgmGdoiKsTekPolicyTable** cgmGdoiGroupIdValue、cgmGdoiGroupIdType、cgmGdoiKeyServerIdValue、cgmGdoiKeyServerIdType、cgmGdoiKsTekPolicyIndex、cgmGdoiKsTekSPI、cgmGdoiKsTekOriginalLifetime、cgmGdoiKsTekRemainingLifetime、cgmGdoiKsTekWindowSize **cgmGdoiGmTable** cgmGdoiGroupIdValue、cgmGdoiGroupIdType、cgmGdoiGmIdValue、cgmGdoiGmIdType、cgmGdoiGmIdLength、cgmGdoiGmRegKeyServerIdValue、cgmGdoiGmRegKeyServerIdType、cgmGdoiGmRegKeyServerIdLength、cgmGdoiGmActiveKEK、cgmGdoiGmRekeysReceived **cgmGdoiGmKekTable** cgmGdoiGroupIdValue、cgmGdoiGroupIdType、cgmGdoiGmIdValue、cgmGdoiGmIdType、cgmGdoiGmKekIndex、cgmGdoiGmKekSPI、cgmGdoiGmKekSrcIdValue、cgmGdoiGmKekSrcIdType、cgmGdoiGmKekSrcIdLength、cgmGdoiGmKekDstIdValue、cgmGdoiGmKekDstIdType、cgmGdoiGmKekDstIdLength、cgmGdoiGmKekOriginalLifetime、cgmGdoiGmKekRemainingLifetime **cgmGdoiGmTekSelectorTable** cgmGdoiGroupIdValue、cgmGdoiGroupIdType、cgmGdoiGmIdValue、cgmGdoiGmIdType、cgmGdoiGmTekSelectorIndex、cgmGdoiGmTekSrcIdValue、cgmGdoiGmTekSrcIdType、cgmGdoiGmTekSrcIdLength、cgmGdoiGmTekDstIdValue、cgmGdoiGmTekDstIdType、cgmGdoiGmTekDstIdLength **cgmGdoiGmTekPolicyTable** cgmGdoiGroupIdValue、cgmGdoiGroupIdType、cgmGdoiGmIdValue、cgmGdoiGmIdType、cgmGdoiGmTekPolicyIndex、cgmGdoiGmTekSPI、cgmGdoiGmTekOriginalLifetime、cgmGdoiGmTekRemainingLifetime、cgmGdoiGmTekWindowSize

GETVPN モニタリング パラメータ	MIB	含まれている MIB オブジェクト
アクティブ KEK（Active KEK） キー再生成回数（Rekeys Count） KEK インデックス（KEK Index） KEK SPI KEK 送信元 ID（KEK Source ID） KEK 送信元 ID のタイプ（KEK Source ID Type） KEK 送信元 ID の長さ（KEK Source ID Length） KEK 宛先 ID（KEK Destination ID） KEK 宛先 ID のタイプ（KEK Destination ID Type） KEK 宛先 ID の長さ（KEK Destination ID Length） KEK の元のライフタイム（KEK Original Lifetime） KEK の残りのライフタイム（KEK Remaining LIfetime） TEK セレクタインデックス（TEK Selector Index） TEK 送信元 ID（TEK Source ID） TEK 送信元 ID のタイプ（TEK Source ID		

GETVPN モニタリング パラメータ	MIB	含まれている MIB オブジェクト
Type） TEK 送信元 ID の長さ（TEK Source ID Length） TEK 宛先 ID（TEK Destination ID） TEK 宛先 ID のタイプ（TEK Destination ID Type） TEK 宛先 ID の長さ（TEK Destination ID Length） TEK ポリシーインデックス（TEK Policy Index） TEK SPI TEK の元のライフタイム（TEK Original Lifetime） TEK の残りのライフタイム（TEK Remaining LIfetime） TEK ウィンドウサイズ（TEK Window Size）		

DMVPN モニタリング ポリシー

DMVPN ポリシー タイプの場合、Prime Infrastructure は次の表に示すメトリックを使用します。

表 *35 : [*モニタ（*Monitor*）*] > [*モニタリングツール（*Monitoring Tools*）*] > [*モニタリングポリシー（*Monitoring Policies*）*] > [DMVPN*メトリック（*DMVPN Metrics*）*]*

DMVPN モニタリング パラメータ	MIB	含まれている MIB オブジェクト
リモート ピア物理 IP（Remote Peer Physical IP） 復号化バイト数（Decrypted Byte Count） 暗号化バイト数（Encrypted Byte Count） リモート トンネル IP（Remote Tunnel IP） NHRP 有効期限（NHRP Expiration） リモート サブネット IP（Remote Subnet IP） リモート サブネット マスク（Remote Subnet Mask）	CISCO-IPSEC-FLOW-MONITOR-MIB	**cipSecTunnelTable** cipSecTunRemoteAddr、cipSecTunInOctets、cipSecTunOutOctets
	NHRP-MIB	**nhrpCacheTable** nhrpCacheInternetworkAddr、nhrpCacheHoldingTime、nhrpCacheNbmaAddr、nhrpCacheType
	IP-FORWARD-MIB	**pCidrRouteTable** ipCidrRouteNextHop、ipCidrRouteDest、ipCidrRouteMask

LISP モニタリング ポリシー

LISP モニタリング ポリシー タイプの場合、<Product Name> は次の表に示すメトリックを使用します。

表 *36 : [*モニタ（*Monitor*）*] > [*モニタリングツール（*Monitoring Tools*）*] > [*モニタリングポリシー（*Monitoring Policies*）*] > [LISP*モニタリング（*LISP Monitoring*）*]*

LISP モニタリング パラメータ	MIB	含まれている MIB オブジェクト
LISP マッピング キャッシュ サイズ（LISP Map Cache Size）	LISP-MIB	lispFeaturesMapCacheSize
LISP マッピング キャッシュ制限（LISP Map Cache Limit）	LISP-MIB	lispFeaturesMapCacheLimit

[デバイス（Device）] ダッシュボードの [デバイスLISPマッピングキャッシュエントリ（Device Lisp Map Cache Entries）] ダッシュレットおよび [ネットワークデバイス（Network Devices）] ダッシュボードの [上位NのLISPマッピングキャッシュエントリ（Top N Lisp Map Cache Entries）] ダッシュレットでポーリングしたデータを表示できます。

Nexus 仮想ポート チャネル（VPC）のヘルス モニタリング ポリシー

Nexus VPC のヘルス モニタリング ポリシーは、プライマリ VPC が設定された Nexus スイッチから設定パラメータを定期的に取得し、セカンダリ VPC が設定された Nexus スイッチと関連付けることで、不整合の原因となる可能性がある設定上の不一致を探します。不整合が検出さ

れると、モニタリング ポリシーがアラームを生成し、グローバル レベルおよびVPC レベルでの不整合の詳細を取得します。次の表では、Nexus VPC ヘルス モニタリング ポリシーのパラメータについて説明します。

表 *37 : [*モニタ（*Monitor***）*] > [*モニタリングツール（***Monitoring Tools***）*] > [*モニタリングポリシー（***Monitoring Policies***）*] > [Nexus VPC*ヘルス（***Nexus VPC Health***）*]***

カテゴリ	**Nexus VPC** モニタリング パラメータ
グローバル エラー（Global Fault）	stpModestp、Disabled、stpMstRegionName、stpMstRegionRevision、stpMstRegionVlanMap、stpLoopguard、stpBridgeAssurance、stpEdgePortType、bpduFilterGuard、stpMstSimulatePvst、passVlans
VPC エラー（VPC Fault）	VpcCardType、OperationalPortMode、Mode、LacpMode、InterfaceType、AdminPortMode、Speed、Duplex、Mtu、NativeVlan、StpPortType、StpPortGuard、StpMstSimulatePvst

サポートされないパラメータとサードパーティデバイスを対象としたモニタリング ポリシーの作成

サードパーティまたはシスコのデバイスおよびデバイス グループをモニタするためのカスタム MIB ポーリング ポリシーを設計できます。また、Prime Infrastructure がデフォルト ポリシーを提供していないデバイスの機能をモニタするためのカスタム MIB ポリシーを作成することもできます。この機能を使用して、以下の操作を実行することができます。

- デバイス タイプの SNMP MIB をアップロードし、ポーリングするデバイスと属性およびポーリング頻度を選択する。
- 単一の MIB 定義ファイルまたは依存関係がある MIB のグループを ZIP ファイルとしてアップロードする。
- 折れ線グラフまたは表として結果を表示する。

この機能により、同じデバイスおよび属性に対するポーリングを容易に繰り返すことができ、SNMP を使用してシスコ デバイスをポーリングする方法をカスタマイズできます。

最大 25 のカスタム MIB ポーリング ポリシーを作成できます。

カスタム MIB ポーリング ポリシーを作成するには、次の手順を実行します。

ステップ 1 **[モニタ（Monitor）] > [モニタリング ツール（Monitoring Tools）] > [モニタリング ポリシー（Monitoring Policies）]** を選択し、[マイ ポリシー（My Policies）] を選択し、[追加（Add）] をクリックします。

ステップ 2 [ポリシー タイプ（Policy Types）] メニューから、[カスタム MIB ポーリング（Custom MIB Polling）] を選択します。

ステップ 3 ポリシーの名前を入力します。

ステップ 4 [MIB の選択（MIB Selection）] タブで、ポーリング頻度を指定し、MIB 情報を入力します。

- Prime Infrastructure でモニタする MIB が [MIB（MIBs）] ドロップダウンリストに表示されない場合は、URL http://tools.cisco.com/Support/SNMP/do/BrowseMIB.do?local=en&step=2 からモニタする MIB をダウンロードします。
- MIB をアップロードするには、ZIP ファイルをアップロードする場合にのみファイル名の拡張子を指定します。
- ZIP ファイルをアップロードする場合は、すべての依存 MIB ファイルが ZIP に含まれているか、またはすでにシステムに存在することを確認してください。
- ファイルをアップロードし、MIB 定義に同じ名前が付いていることを確認します。ZIP ファイルをアップロードする場合、そのファイル名を好きなように指定できますが、その中に含まれている MIB ファイルも同じ規則に従う必要があります（例：MyMibs.zip は、ZIP 内のすべての MIB ファイルがその MIB 名に一致していれば許容可能です）。

ステップ 5 デバイスで作成したポリシーをアクティブ化する前にテストするには、[テスト（Test）] タブをクリックして、新しいポリシーをテストするデバイスを選択します。

ステップ 6 指定したデバイスでポリシーを即座にアクティブ化するには、[保存してアクティブにする（Save and Activate）] をクリックします。

ステップ 7 MIB ポーリングデータを表示するには、作成したポリシーの名前を使用して [パフォーマンス（Performance）] ダッシュボードの汎用ダッシュレットを作成します。

（注） Cisco ASR デバイスの SNMP ポーリングの日付を表示するには、CPU 使用率の場合は show platform hardware qfp active datapath utilization | inc Processing コマンドを、メモリ使用率の場合は show platform hardware qfp active infrastructure exmem statistics | sec DRAM コマンドを使用する必要があります。

例：IP SLA のモニタ

ネットワークベースのアプリケーションおよびサービスの IP サービス レベルを表示するためのモニタリング ポリシーを作成できます。約 7 つの IP SLA 関連 MIB があります。この例では、ビデオ MIB のみがモニタされます。

ステップ 1 次の URL から IP SLA ビデオ MIB をダウンロードします。 http://tools.cisco.com/Support/SNMP/do/BrowseMIB.do?local=en&step=2

ステップ 2 **[モニタ（Monitor）] > [モニタリング ポリシー（Monitoring Policies）] > [マイ ポリシー（My Policies）]** を選択し、[追加（Add）] をクリックします。

ステップ 3 [Custom MIB Polling] をクリックします。

ステップ 4 ポリシーの名前を入力します。

ステップ 5 [MIB の選択（MIB Selection）] タブで、[MIB のアップロード（Upload MIB）] をクリックして、ステップ 1 でアップロードした **MIB** に移動します。

ステップ 6 [Tables] プルダウン メニューから、テーブルを選択し、モニタする特定のメトリックを選択します。

ステップ 7 デバイスで作成したポリシーをアクティブ化する前にテストするには、[Test] タブをクリックして、新しいポリシーをテストするデバイスを選択します。

ステップ 8 IP SLA メトリックをモニタするデバイスを選択します。

ステップ 9 指定したデバイスでポリシーを即座にアクティブ化するには、[Save and Activate] をクリックします。

ステップ 10 ダッシュボードからこの情報をモニタするには、汎用ダッシュレットを作成する必要があります。詳細については、「事前定義のダッシュレットをダッシュボードに追加する（15 ページ）」を参照してください。

過去のモニタリングポリシーデータ収集のステータスの確認

モニタリング ポリシーの過去のデータ収集を確認するには、次の手順を実行します。

ステップ 1 **[モニタ（Monitor）] > [モニタリング ツール（Monitoring Tools）] > [モニタリング ポリシー（Monitoring Policies）]** を選択し、[マイ ポリシー（My Policies）] をクリックします。

ステップ 2 ポリシーを見つけ、[収集ステータス（Collection Status）] の下にある [詳細（Details）] をクリックして [収集データ（Collection Data）] ダイアログを開きます。デバイスに対してポーリングを行ったパラメータを確認するには、[パラメータ（Parameter）] 列のテキストの上にマウスを重ねます。

ポリシーでモニタするデバイス セットの変更

モニタリング情報の収集頻度（ポーリング間隔）をカスタマイズできます。すべてのポリシーにこれらの設定がすべて含まれているわけではありません。たとえば、統計情報だけを収集するポリシーには、しきい値やアラームが関連付けられていない可能性があります。

ステップ 1 **Monitor > Monitoring Policies > My Policies** を選択してから、編集するポリシーを選択します。

ステップ 2 編集するポリシーを確認して **[Edit]** をクリックします。

ステップ 3 [デバイスの選択（Device Selection）] ドロップダウン リストをクリックします。

（注） [デバイス グループ（Device Groups）] オプションを使用してデバイスを選択する際に、レコード件数が 100 を超えるグループに対応するチェックボックスをオンにした場合、最初のデバイスを選択するページには最初の 100 件のレコードが表示されて、それらのレコードだけが選択されます。残りのレコードを選択するには、次のページにスクロールダウンする必要があります。

ステップ 4 必要に応じてデバイスを選択および選択解除します。

ステップ 5 **[Save and Activate]** をクリックしてポリシーを保存し、選択したデバイスですぐにアクティブ化します。

モニタリング ポリシーのポーリングの変更

モニタリング情報の収集頻度（ポーリング間隔）をカスタマイズできます。すべてのポリシーにこれらの設定がすべて含まれているわけではありません。たとえば、統計情報だけを収集するポリシーには、しきい値やアラームが関連付けられていない可能性があります。

ステップ 1 **[モニタ（Monitor）] > [モニタリング ツール（Monitoring Tools）] > [モニタリング ポリシー（Monitoring Policies）]** を選択し、[マイ ポリシー（My Policies）] をクリックします。

ステップ 2 編集するポリシーを選択して、[編集（Edit）] をクリックします。

ステップ 3 ポーリング頻度を調整します。ポーリングの調整方法は、モニタリング ポリシーのタイプに応じて異なります。

ステップ 4 ポリシーを保存して選択したデバイスで即座にアクティブ化する場合は[保存してアクティブにする（Save and Activate）] をクリックします。

モニタリングポリシーのしきい値およびアラーム動作の変更

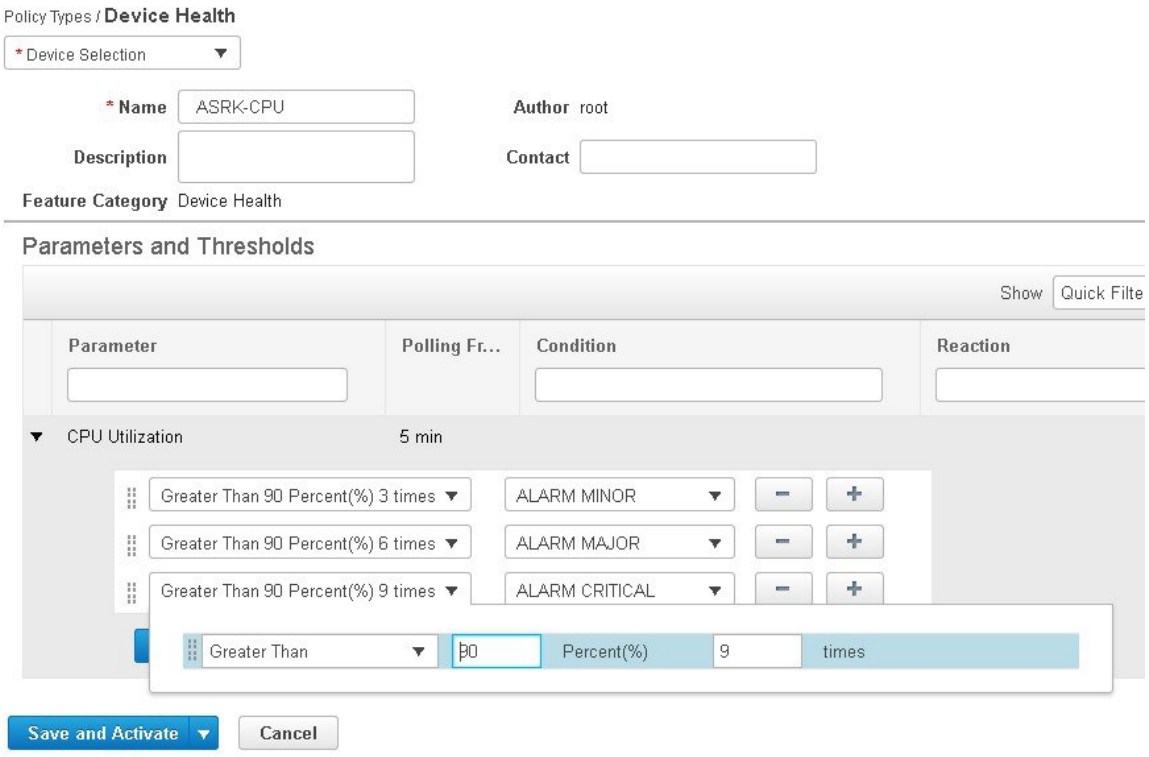
問題を示すしきい値と、問題が検出された場合にPrime Infrastructureで情報イベントまたは（任意の重大度の）アラームを生成するかどうかをカスタマイズできます。すべてのポリシーにこれらの設定がすべて含まれているわけではありません。たとえば、統計情報だけを収集するポリシーには、しきい値やアラームが関連付けられていない可能性があります。

ステップ 1 **[モニタ（Monitor）] > [モニタリング ツール（Monitoring Tools）] > [モニタリング ポリシー（Monitoring Policies）]** を選択し、[マイ ポリシー（My Policies）] を選択します。

ステップ 2 編集するポリシーを選択して、[編集（Edit）] をクリックします。

ステップ 3 変更するパラメータを検索します。

ステップ 4 パラメータを展開します。既存の条件を変更するか、新しい条件を追加することができます。次の図では、Cisco ASR 9000 デバイスの CPU 使用率のしきい値とアラームが指定されています。



（注） 次の表に示すように、各メトリックに対して設定できるしきい値は合計 50 個までです。

ステップ 5 操作が完了したら、[保存してアクティブにする（Save and Activate）] をクリックして、選択したデバイスにポリシーを保存して即座にアクティブにします。

メトリック	パラメータ
CPU	CPU 使用率
MEMORY	[メモリ プール使用率（Memory Pool Utilization）]
ENVTEMP	環境温度（Environment Temperature）

メトリック	パラメータ
INTERFACE	インターフェイスインバウンドエラー（Interface Inbound Errors）、インターフェイスアウトバウンドエラー（Interface Outbound Errors）、インターフェイスインバウンド破棄（Interface Inbound Discards）、インターフェイスアウトバウンド破棄（Interface Outbound Discards）、入力使用率（Input Utilization）、出力使用率（Output Utilization）、入力パケットブロードキャストパーセント（Input Packet Broadcast Percent）、入力キューのパーセンテージの低下（Percentage drops in input queue）、出力キューのパーセンテージの低下（Percentage drops in output queue）
QOS	QoS クラスあたりのドロップ パーセンテージ

ポリシー名	パラメータ
トラフィック分析（Traffic Analysis）	受信バイト（In Bytes）、受信パケット（In Packets）、送信バイト（Out Bytes）、送信パケット（Out Packets）
トラフィック分析（Traffic Analysis）	合計バイト数（Total Bytes）、合計パケット数（Total Packets）、受信バイト（In Bytes）、受信パケット（In Packets）、送信バイト（Out Bytes）、送信パケット（Out Packets）
アプリケーション応答時間（Application Response Time）	平均ネットワーク時間（Average Network Time）、平均クライアントネットワーク時間（Average Client Network Time）、平均サーバネットワーク時間（Average Server Network Time）、平均トランザクション時間（Average Transaction Time）、平均サーバ応答時間（Average Server Response Time）、最大ネットワーク時間（Maximal Network Time）、最大クライアントネットワーク時間（Maximal Client Network Time）、最大サーバネットワーク時間（Maximal Server Network Time）、最大トランザクション時間（Maximal Transaction Time）
音声ビデオ データ	平均MOS（Average MOS）、最低MOS（Worst MOS）、ジッター（Jitter）、実際のパケット損失（Actual Packet Loss）、調整されたパケット損失（Adjusted Packet Loss）

レポートを使用したネットワークパフォーマンスのモニタ

Prime Infrastructure は、ネットワークのパフォーマンスをモニタするのに役立つさまざまなレポートを提供します。次に例を示します。

- 環境温度、CPU とメモリの使用率
- インターフェイス エラーと破棄

パフォーマンス レポートを実行すると、データベースに保存されている履歴データが取得されます。レポートには、Prime Infrastructure が収集するように設定されているデータ、つまりモニタリング ポリシーを使用して収集およびモニタされるデータのみが表示されます。（イベントおよびアラーム関連のレポートではモニタリング ポリシーを有効にする必要はありません。そのデータは自動的に収集されます。）

第 15 章

アラームとイベントのモニタリング

この章は、次の内容で構成されています。

- アラームおよびイベントとは （353 ページ）
- アラームおよびイベントはどのように作成および更新しますか。 （354 ページ）
- アラームの検索および表示 （356 ページ）
- 既存のアラームの抑制 （358 ページ）
- 既存のアラームの重大度の変更 （359 ページ）
- アラームとイベント管理の設定 （360 ページ）
- イベントとアラームのバッジと色の解釈 （364 ページ）
- トラブルシューティングと詳細なアラーム情報の取得 （364 ページ）
- アラームの確認とクリア （366 ページ）
- アラームへの注釈の追加 （367 ページ）
- アラームがトリガーされる方法の管理（アラームしきい値） （368 ページ）
- サポートされるイベント （368 ページ）
- イベントの表示 （369 ページ）
- Syslog ポリシーの表示 （370 ページ）
- Syslog の表示 （373 ページ）
- CSV ファイルまたは PDF ファイルへのアラーム、イベント、または syslog のエクスポート （374 ページ）
- アラーム、イベント、および Syslog レポートの操作 （374 ページ）
- シスコからサポートを受ける （378 ページ）
- Prime Infrastructure 内の問題への対応 （378 ページ）
- アラーム ポリシーとは （378 ページ）
- アラームおよびイベントの通知ポリシー （384 ページ）

アラームおよびイベントとは

イベントとは、特定の時点で発生する個別のインシデントです（ポートステータスの変更、デバイスが到達不能になるなど）。イベントは、ネットワーク内のエラー、障害、または例外的

な状況を示す場合があります。また、イベントは、それらのエラー、障害、または状況のクリアを示す場合もあります。

アラーム は、1 つ以上の関連イベントへの Prime Infrastructure 応答です。特定のイベントだけがアラームを生成します。アラームには、状態（クリア済みまたはクリアされていない）と重大度（クリティカル、メジャー、マイナーなど）があります。アラームは、最新のイベントの重大度を継承します。クリアイベントが生成されるまで（またはアラームが手動でクリアされるまで）、アラームは開いたままです。

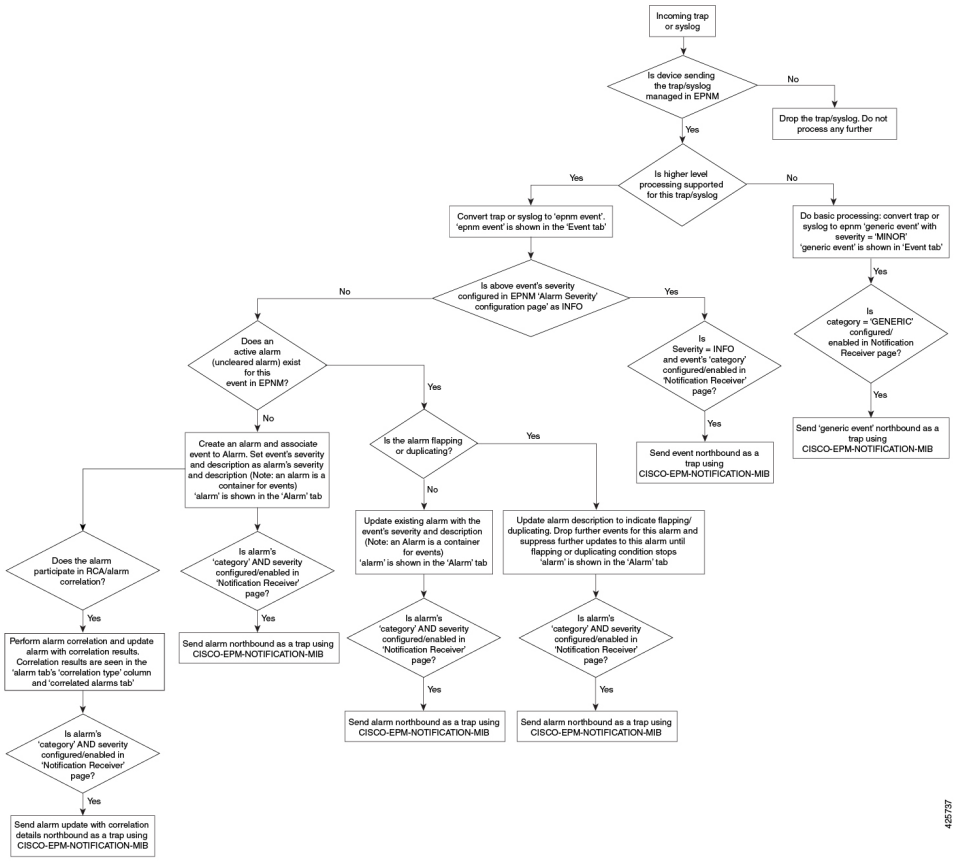
関連トピック

アラームおよびイベントはどのように作成および更新しますか。 （354 ページ）
アラームの確認とクリア （366 ページ）
イベントとアラームのバッジと色の解釈 （364 ページ）

アラームおよびイベントはどのように作成および更新しますか。

Prime Infrastructure は、IPv4 と IPv6 の両方のデバイスの SNMP トラップ、syslog、および TL1 メッセージを処理します。これは、これらのイベントに対する応答方法を決定するイベントカタログを維持します。以下のフローチャートは、これらのアラームやイベントの処理方法を表します。

図 *8 :* アラーム処理フローチャート



Prime Infrastructure は、イベントを処理するときに次の一般的手順を実行します。

1. トラップまたは syslog が Prime Infrastructure でサポートされていない場合、イベントは作成されません。サポートされている場合、トラップまたは syslog は上位レベルの処理の対象と見なされ、Prime Infrastructure によって、処理済みイベントが重大度および（場合によっては）アラームとともに作成されます。
2. イベントの原因となっているデバイスおよびデバイス コンポーネントを特定します（イベントの場所を特定します）。
3. サポートされているイベントによってインベントリ収集がトリガーされるかどうかをチェックします。

   一部のイベントには、収集が必要な情報を Prime Infrastructure に指示する特定のルールがあります。

4. イベントの重大度が [情報（INFO）] または [クリア済み（CLEARED）] かどうかを確認します。

   - [情報（INFO）] または [クリア済み（CLEARED）] の場合、Prime Infrastructure はイベントを保存し、GUI に表示します。

- 他の重大度の場合、Prime Infrastructure は新しいアラームを作成する必要があるかどうかを評価します（次のステップ）。

5. アラームがすでに存在するか、新しいアラームを作成する必要があるかどうかを確認します。
   - アラームが存在する場合、Prime Infrastructure は、イベントを既存のアラームに関連付けます。アラームの重大度が、新しいイベントの重大度に対応するように変更され、アラームのタイム スタンプが更新されます。これがクリア イベント（リンク アップ イベントなど）の場合、アラームが作成されます。

     （注） 場合によっては、デバイスがクリアアラームを生成しないことがあります。管理者は、アラームの自動クリア間隔を設定する必要があります。

   - アラームが存在しない場合、Prime Infrastructure は新しいアラームを作成し、これにイベントと同じ重大度を割り当てます。

リンク アップ/ダウン フラッピング

羽ばたきは、リンクから連続した遷移の洪水をリンク (またはその逆) にデバイス上で同じインターフェイスです。これは、障害によってイベント通知が繰り返し発生する場合に発生します (たとえば、コネクタのはめ方が甘いケーブルなど)。Prime Infrastructure では、60 秒以内にリンクアップ/ダウン遷移が5回発生した場合に、アラームをフラッピングとしてマークします。ダウン、インターフェイスをインターフェイスをインターフェイスをインターフェイスをインタフェースなど一連の 5 つの出現可能性があります。

羽ばたきとしてマークされているアラームが消去またはリンク アップ/ダウン 60 秒間の転移の出現がない場合のリンクとしてマークします。アラームは、(アップまたはダウン) を受信した最後の非羽ばたきイベントに基づいて更新されます。これはアラームの状態と関連付けられている通知 (表示、電子メール、北回りトラップ) の更新定数とイベントの流れを制御するのに役立ちます。

アラームの検索および表示

アラームを表示するには、[モニタ（Monitor）] > [モニタリングツール（Monitoring Tools）] > [アラームおよびイベント（Alarms and Events）] を選択します。アラームは、次の 4 つのカテゴリに分類され、[アラーム（Alarms）] テーブルの個別のタブに表示されます。

- [ネットワークの健全性 (Network Health)]: コントローラ、スイッチ、およびルータ カテゴリのアラームが表示されます。
- [不正AP（Rogue AP）] : [不正AP（Rogue AP）] および [アドホック不正（Adhoc Rogue）] カテゴリのアラームを表示します。

- [セキュリティ（Security）]：セキュリティ カテゴリのアラームを表示します。
- [システム（System）]：システム カテゴリのアラームを表示します。

各タブ名の横にある数は、その特定のアラーム カテゴリ内のアラームの総数を示します。

[アクティブなアラームを表示する（Show Active Alarms）]：次の表にある手順で説明されているように、特定のアラームを検索したり、カスタマイズ（プリセット）されたフィルタを作成して保存することができます。デフォルトでは、[アラームおよびイベント（Alarms and Events）]ページにはクリアされたアラームを除く最新の4000個のアクティブアラームが表示されます。アクティブなアラームは、[マイプリファレンス（My Preferences）]ページで選択した設定に基づいて自動的に更新されます。詳細については、アラームとイベントの表示設定のセットアップ（360ページ）を参照してください。[自動更新を一時停止（Pause Auto-Refresh）]ボタンをクリックすると、アラームの自動更新を一時的に無効にすることができます。

[アラーム履歴の表示（Show Alarm History）]：[アラームおよびイベント（Alarms and Events）]ページで[アラーム履歴の表示（Show Alarm History）]をクリックすると、最大20,000個のアラームが表示されます。クリアされたアラームを表示する場合は、クリア済み（366ページ）を参照してください。[アラーム履歴の表示（Show Alarm History）]モードでは、アラームは自動的に更新されません。ただし、[アラームおよびイベント（Alarms and Events）]テーブルの[更新（Refresh）]アイコンをクリックすると、アラームを手動で更新できます。

次の表では、[表示（show）]ドロップダウン フィルタ リストで使用可能なアラーム表示オプションについて説明します。

検索対象のアラーム	[モニタ（Monitor）]>[モニタリング ツール（Monitoring Tools）]>[アラームおよびイベント（Alarms and Events）]の順に選択した後の操作
特定のデバイスによって生成されたアラーム	アクティブなアラームの場合は、デバイス名の横にある[I]アイコンをクリックして[デバイス360（Device 360）]ビューを開き、[アラーム（Alarms）]タブをクリックします。クリアされたアラームを確認する場合は、表「アラームおよびイベント」を参照してください。 特定のデバイスについて、シャーシ ビューを使用してデバイスのアラームを確認することもできます。
自分に割り当てられているアラーム	[表示（Show）]ドロップダウン フィルタ リストをクリックし、[自分に割り当てられているアラーム（Alarms assigned to me）]を選択します。このフィルタは、クリアされたアラームと相関付けられたアラームにも使用できます。
未割り当てのアラーム	[表示（Show）]ドロップダウン フィルタ リストをクリックし、[未割り当て（Unassigned）]を選択します。このフィルタは、クリアされたアラームと相関付けられたアラームにも使用できます。

検索対象のアラーム	**[モニタ（Monitor）] > [モニタリング ツール（Monitoring Tools）] > [アラームおよびイベント（Alarms and Events）]** の順に選択した後の操作
Prime Infrastructure タイムスタンプに基づく最新のアラーム	アクティブなアラームを確認する場合：: • 過去 30 分間に発生したアラーム：[表示（Show）] ドロップダウン フィルタをクリックし、[過去 5 分（last 5 minutes）]、[過去 15 分（last 15 minutes）]、または [過去 30 分（last 30 minutes）]（**PI タイムスタンプ**）を選択します。 • 過去 24 時間に発生したアラーム：[表示（Show）] ドロップダウン フィルタをクリックし、[過去 1 時間（last 1 hour）]、[過去 8 時間（8 hours）]、または [過去 24 時間（last 24 hours）]（**PI タイムスタンプ**）を選択します。 • 過去 7 日間に発生したアラーム：[表示（Show）] ドロップダウン フィルタをクリックし、[過去 7 日間（last 7 days）]（**PI タイムスタンプ**）を選択します。
デバイスのタイムスタンプに基づく最新のアラーム	前の行の場合と同じ手順を実行します。ただし、サフィックス付きのフィルタ（**デバイス タイムスタンプ**）を選択します。
デバイスのグループ、シリーズ、またはタイプによって生成されたすべてのアラーム	左側のナビゲーション ペインで、グループを選択します。このフィルタは、クリアされたアラームと相関付けられたアラームにも使用できます。
カスタマイズされたフィルタを使用したアラーム	高度なフィルタを作成して保存します（この表の後に続く手順を参照）。

既存のアラームの抑制

アラーム ポリシーを作成することにより、既存のアラームを特定の期間または永続的に非表示にできます。

アラームを非表示にするには、次の手順を実行します。

ステップ 1 **[モニタ（Monitor）] > [モニタリング ツール（Monitoring Tools）] > [アラームとイベント（Alarms and Events）]** を選択します。

ステップ 2 非表示にするアラームを選択します。

ステップ 3 [アラームポリシーの作成（Create Alarm Policy）] ドロップダウン リストをクリックし、[抑制（Suppress）] を選択します。

（注） アラームを選択している場合のみ、[アラームポリシーの作成（Create Alarm Policy）] ドロップダウン リストが有効になります。

ステップ 4 [新規アラームポリシーの作成（Create New Alarm Policy）] ダイアログで、非表示オプションのいずれかを必要に応じて選択します。

- [完全に抑制（Suppress Permanently）]。
- [この期間に条件が改善されない場合に表示（分）（Display if the condition persists for this duration (minutes)）]：タイム スライダを使用して期間を選択します。

ステップ 5 [概要（Summary）] をクリックして、ポリシーの詳細を表示します。設定を変更する場合は、以前のページに移動し、必要な変更を行います。

ステップ 6 [終了（Finish）] をクリックします。新しいポリシーが作成されます。

（注） **[モニタ（Monitor）] > [モニタリングツール（Monitoring Tool）] > [アラームポリシー（Alarm Policies）]** ページからこのポリシーの表示、編集、削除、および並べ替えを行います。

（注） [アラームおよびイベント（Alarms and Events）] ページで作成されたポリシーは既存のアラームに影響しません。以降のアラームにのみ適用されます。

関連トピック

アラーム ポリシーの削除 （383 ページ）
既存のアラーム ポリシーの編集 （383 ページ）
アラーム ポリシーとは （378 ページ）

既存のアラームの重大度の変更

既存のアラームの重大度を変更するには、アラーム ポリシーを作成します。

重大度を変更するには：

ステップ 1 **[モニタ（Monitor）] > [モニタリング ツール（Monitoring Tools）] > [アラームとイベント（Alarms and Events）]** を選択します。

ステップ 2 重大度を変更するアラームを選択します。

ステップ 3 **[アラームポリシーの作成（Create Alarm Policy）]** ドロップダウン リストをクリックし、**[重大度の変更....（Change Severity....）]** を選択します。. 選択したアラームのイベント タイプは [新規アラームポリシーの作成（Create New Alarm Policy）] ダイアログに表示されます。

（注） アラームを選択している場合のみ、[アラームポリシーの作成（Create Alarm Policy）] ドロップダウン リストが有効になります。

ステップ 4 イベント タイプに新しい重大度を選択するには、表の行をクリックします。

ステップ 5 選択したイベント タイプの [重大度（Severity）] ドロップダウン リストをクリックし、重大度を変更します。

ステップ 6 [保存（Save）] をクリックします。

（注） デフォルト以外の重大度を選択するまで、ポリシーは保存できません。

ステップ 7 [概要（Summary）] をクリックすると、詳細が表示されます。このポリシーの名前および説明が自動的に生成され、送信元からアラームに適用されます。

ステップ 8 [終了（Finish）] をクリックします。

（注） **[モニタ（Monitor）] > [モニタリングツール（Monitoring Tool）] > [アラームポリシー（Alarm Policies）]** ページからこのポリシーの表示、編集、削除、および並べ替えを行います。

（注） [アラームおよびイベント（Alarms and Events）] ページで作成されたポリシーは既存のアラームに影響しません。以降のアラームにのみ適用されます。

関連トピック

アラーム ポリシーの削除 （383 ページ）
既存のアラーム ポリシーの編集 （383 ページ）
アラーム ポリシーとは （378 ページ）

アラームとイベント管理の設定

• アラームとイベントの表示設定のセットアップ （360 ページ）
• アラーム サマリーのカスタマイズ （363 ページ）

（注） アドバンス ユーザは、Prime Infrastructure の Representational State Transfer（REST）API を使用して、デバイスの障害情報にアクセスすることもできます。API の詳細については、Prime Infrastructure ウィンドウの右上にある ⚙ をクリックし、**[ヘルプ（Help）] > [REST API]** を選択します。

アラームとイベントの表示設定のセットアップ

（注） 4000 のアラームとイベントの一覧には、表示されないクリアされたアラームも含まれています。開いているアラームをすべて表示するには、[すべて表示（Show All）] をクリックします。

Prime Infrastructure ウィンドウの右上にある ⚙ をクリックし、[マイプリファレンス（My Preferences）] を選択すると、次のアラームおよびイベントの表示をカスタマイズできます。変

更を加えたら、[保存（Save）]をクリックして新しい設定を適用します。確認済み、クリア済み、割り当て済みアラームを表示するかどうかなどのその他の設定は、管理者によってグローバルに制御されます。

ユーザ プリファレンス設定	説明
[アラームおよびイベント（Alarms & Events）] ページの自動更新	[アラームおよびイベント（Alarms and Events）]ページでアクティブなアラームおよびイベントのデータの自動更新を有効または無効にします。有効にすると、**[アラームのまとめ（Alarm Summary）] のアラーム数を更新**の設定に従ってページが更新されます。
[アラームのまとめ]のアラームカウントを___分/秒ごとに更新（Refresh Alarm count in the Alarm Summary every ___ minutes/seconds）	[アラームのまとめ（Alarm Summary）]のアラーム カウントの更新間隔を設定します（デフォルトは 1 分です）（アラーム サマリーのカスタマイズ （363 ページ） を参照）。
[アラームおよびイベント（Alarms & Events）] ページの [アラームバッジング（Alarm Badging）] の有効化	ユーザが [アラームバッジング（Alarm Badging）] を有効にすると、**[モニタ（Monitor）] > [モニタリングツール（Monitoring Tools）] > [アラームおよびイベント（Alarms & Events）]** ページでデバイス グループの横にアラーム重大度のアイコンが表示されます。
[アラーム（Alarm）]の有効化 [確認（Acknowledge）] [警告メッセージ（Warning Message）]	（注） この設定は、[確認済みのアラームを非表示（Hide Acknowledged Alarms）]も有効になっている場合にのみ設定できます。その設定はデフォルトで無効になっています（前の表を参照）。 ユーザがアラームを選択して **[ステータスの変更（Change Status）] > [確認（Acknowledge）]** を選択したときに、次のメッセージが表示されないようにします。 **「警告：今このアラームを確認すると、7日以内に元のイベントが再び発生した場合は、このアラームは生成されません。（Warning: This alarm will not be generated, if the original event recurs again, within next 7 days, as it is acknowledged now.）」「確認せずにアラームをクリアすると、イベントが再び発生した場合にアラームが生成されます。（Clearing the alarm instead of acknowledging will cause the alarm to be generated if the event recurs again.）」「アラーム確認を続行しますか。（Proceed with alarm acknowledgment?）」**

ユーザ プリファレンス設定	説明
「この状態のすべてをクリア」に対する確認プロンプトの無効化	ユーザがアラームを選択して **[ステータスの変更（Change Status）] > [この状態のすべてをクリア（Clear all of this condition）]** を選択したときに、次のメッセージが表示されないようにします。 **「この状態のすべてのアラームをクリアしてよろしいですか。（Are you sure you want to clear all alarms of this condition?）」** （デフォルトでは無効）
「この状態のすべてをクリア」に対する「重大度を [情報（Information）] に設定」プロンプトの無効化	ユーザがアラームを選択して **[ステータスの変更（Change Status）] > [この状態のすべてをクリア（Clear all of this condition）]** を選択したときに表示される次のメッセージを無効化します。 **「選択したアラームの状態の重大度を[情報（Information）]に設定しますか。（Do you want to set the severity for the selected alarm's condition to Information?）」** **「警告：これはシステム全体の変更で、この状態に関する今後のアラームが作成されなくなります。（WARNING: This is a system-wide change that will prevent creation of future alarms of this condition.）」「この変更は、[システム設定（System Settings）]の[重要度設定（Severity Configuration）]ページで元に戻すことができます。（You can undo this change on the Severity Configuration page under System Settings.）」** （デフォルトでは無効） （注） 十分な権限を持つユーザは、の手順を使用して重大度を元の値にリセットできます。
[アラームのまとめ（Alarm Summary）] ツールバーのアラーム カテゴリの選択	[アラームのまとめ（Alarm Summary）] に表示される内容を管理します（アラーム サマリーのカスタマイズ （363 ページ） を参照）。
特定の状態のアラームをすべてクリアする場合、状態の重大度を常に [情報（Information）] に設定する	ユーザがアラームを選択し、**[ステータスの変更（Change Status）] > [この状態のすべてをクリア（Clear all of this condition）]** を選択した場合。（デフォルトでは無効）

ユーザ プリファレンス設定	説明
新規の重大なアラームカウントの通知の有効化	重大なアラームのカウントを表示する通知ポップアップを有効にします。このカウントは、[アラームのまとめ（Alarm Summary）] の [アラーム カウントの更新（Refresh Alarm count）] に設定されている間隔（アラーム サマリーのカスタマイズ（363ページ）を参照）に応じてアラーム間隔が更新されると更新されます。未処理の重大なアラームのみが表示されます。

アラーム サマリーのカスタマイズ

表示するアラーム カテゴリを指定できます。

- Prime Infrastructure [Cisco Prime Infrastructure] タイトル バーのアラーム カウント（ベル）では、関心のあるアラーム カウントを視覚的に容易に確認できます。
- アラーム カウントをクリックしたときに起動する [アラームのまとめ（Alarm Summary）] ポップアップ ウィンドウでは、次の図に示すように、アラーム カウントを重大度ともに視覚的に容易に確認できます。

この情報をカスタマイズするには、次の手順を実行します。

ステップ 1 [アラームのまとめ（Alarm Summary）] ポップアップ ウィンドウの左上にある [編集（Edit）] をクリックします。これにより、[マイ プリファレンス（My Preferences）] が開きます。また、Web の GUI ウィンドウの右上にある ⚙ をクリックし、[マイ プリファレンス（My Preferences）] を選択しても、このページを開くことができます。

ステップ 2 [アラームおよびイベント（Alarms & Events）] タブをクリックします。

ステップ 3 [アラームのまとめ（Alarm Summary）] の更新間隔を変更するには、[[アラームおよびイベント]ページと[アラームのまとめ]のアラームカウントを次の間隔で更新（Refresh Alarms & Events page and Alarm count in the Alarm Summary every）] ドロップダウンリストから数値を選択します。

ステップ 4 [アラームのまとめ（Alarm Summary）] に表示する情報を指定するには、[アラームカテゴリ（Alarm Categories）] 領域に移動します。[表示するデフォルトカテゴリ（Default category to display）] ドロップダウンリストから [アラームのまとめ（Alarm Summary）] を選択します。対応するチェックボックスを選択または選択解除して、必要なアラーム カテゴリを有効または無効にします。

ステップ 5 [保存（Save）] をクリックして、[自分の環境設定（My Preferences）] ウィンドウで行った変更を確定します。

イベントとアラームのバッジと色の解釈

ネットワークに問題がある場合、Prime Infrastructure は問題が発生している要素にアラームまたはイベントのアイコンを表示して、問題をフラグします。アラーム重大度アイコン （364ページ）にアイコンとその色を示します。

アラーム重大度アイコン

次の表に、Web GUI のさまざまな部分に表示されるアイコンのアラームの色とその重大度を示します。

重大度アイコン	説明	色
	クリティカル アラーム	赤
	メジャーアラーム	オレンジ
	マイナーアラーム	黄
	警告アラーム	ライト ブルー
	アラームはクリア済み。正常、OK	緑
	情報アラーム	青
	不確定アラーム	暗い青色

トラブルシューティングと詳細なアラーム情報の取得

- アラームの詳細を表示する （364 ページ）
- アクティブ アラームのトラブルシューティング情報の検索 （365 ページ）
- アラームに関連付けられているイベントの検索 （365 ページ）

アラームの詳細を表示する

アラームの詳細を取得するには、それを展開します。[アラーム（Alarms）] リストからこれを行うことができます（**[モニタ（Monitor）] > [モニタリング ツール（Monitoring Tools）] > [アラームおよびイベント（Alarms and Events）]** を選択するか、[アラームのまとめ（Alarm Summary）] ポップアップで [詳細（Details）] をクリックします）。

General Information：アラームの検出日と最終更新日、現在の重大度と最新の重大度、およびアラームの検出方法	**Device Details**：管理対象デバイスの名前、アドレス、稼働時間、到達可能性ステータス、収集ステータスなど
Messages：トラップ、syslog、または TL1 メッセージ	**Device Events**：過去 1 時間の最近のデバイス イベント（任意のタイプ、時系列順）

アクティブ アラームのトラブルシューティング情報の検索

この手順を使用して、アクティブなアラームの発生原因の説明や、そのアラームに対して推奨される対応を把握します。

（注） すべてのアラームにこの情報があるとは限りません。十分な権限を持つユーザが、ポップアップ ウィンドウに表示される情報を追加または変更できます。

ステップ 1 **[モニタ（Monitor）] > [モニタリング ツール（Monitoring Tools）] > [アラームおよびイベント（Alarms and Events）]** を選択し、[アラーム（Alarms）] タブをクリックします（インターフェイス アラームの場合は、[アラーム（Alarms）] タブの下の [インターフェイス 360（Interface 360）] ビューからこの情報を取得することもできます）。

ステップ 2 アラームを見つけて [重大度（Severity）] 列の [i] アイコンをクリックし、アラームの説明とトラブルシューティングの推奨アクションが表示されたポップアップ ウィンドウを開きます。

何らかのアクションを取る場合は、そのアクションを文書化することをお勧めします。アラームを選択し、[注釈（Annotation）] をクリックします。

アラームに関連付けられているイベントの検索

アラームに関連付けられているイベントを表示するには、[アラーム（Alarms）] テーブルから [重要度（Severity）] の横にある [i] アイコンをクリックします。

アラームの確認とクリア

アラームの有効なステータスは、[未確認（Not Acknowledged）]、[確認済み（Acknowledged）]、または [クリア済み（Cleared）] です。

未確認

[未確認（Not Acknowledged）] は、問題が対応されていないことを表します。ネットワーク内の新しい障害状態、または再発したクリア済みの障害状態を示す場合があります。[未確認（Not Acknowledged）] アラームは、確認応答またはクリアされるまで、[アラームおよびイベント（Alarms and Events）] テーブルから削除されません。

確認済み

[確認済み（Acknowledged）] とは、障害状態が認識されて対応されているか、または無視できることを表します。アラームを確認済みステータスに移行することは手動操作であり、その際にアラームのステータスが [確認済み（Acknowledged）] に変わります。確認されたイベントは引き続き未解決とみなされる（つまり、クリアされていない）ので、関連するイベントが再発すると、イベントがアラームに追加されます。

デフォルトでは、確認済みのアラームは [アラーム（Alarms）] リストから削除されません。この動作は、管理者によって制御される **[Hide Acknowledge Alarms]** 設定によって異なります。

確認されたアラームは、[未確認（Not Acknowledged）] ステータスに戻すことができます（たとえば、誤ったアラームを確認した場合など）。

クリア済み

クリア済みとは、障害状態が現在は存在しないことを意味します。アラームがクリアされていても、関連するイベントが繰り返される場合、Prime Infrastructure は新しいアラームを表示します。

デフォルトでは、クリア済みのアラームは [アラームおよびイベント（Alarms and Events）] ページに表示されません。クリア済みのアラームを [アラームおよびイベント（Alarms and Events）] ページの [アラーム履歴（Alarms History）] テーブルに表示するには、次の手順を実行します。

（注） FRU アラームの生成時にインベントリにロケーション パラメータがない場合、生成されたアラームにはロケーション パラメータがありません。この FRU アラームがクリアされると、アラームにはインベントリ ロケーション パラメータがない可能性があります。

- **[管理（Administration）] > [設定（Settings）] > [システム設定（System settings）]** を選択し、[アラームおよびイベント（Alarms and Events）] を選択します。
- [アラームの表示オプション（Alarm Display Options）] の下にある [クリア済みのアラームを非表示（Hide cleared Alarms）] チェックボックスをオフにします。

アラームのステータスを変更するには、次の手順を実行します。

ステップ 1 **Monitor > Monitoring Tools > Alarms & Events**を選択します。

ステップ 2 アラームを選択し、[**Change Status**] と該当するステータス（[確認（Acknowledge）]、[未確認（Unacknowledge）]、[クリア（Clear）]、[この条件のすべてをクリア（Clear all of this Condition）]）を選択します。

（注） [**Clear all of this Condition**] により、選択したアラームと同じ条件のすべてのアラームに対してイベントのクリアがトリガーされます。このステータスを選択すると、Prime Infrastructure は選択したアラーム条件の重大度を [情報（Information）] に変更するかどうかを確認するダイアログを表示します。これにより、Prime Infrastructure では指定した条件のアラームが作成されなくなります。条件の重大度を後でリセットするには、**Administration > System Settings > Severity Configuration** を選択して重大度を変更します。

ステップ 3 [**Yes**] をクリックして、指定した条件のすべてのアラームをクリアすることを確認します。

アラームへの注釈の追加

注釈機能では、自由形式のテキストをアラームに追加できます。テキストはアラーム詳細の [メッセージ（Messages）] 領域に表示されます。アラームにテキストを追加するには、[アラームおよびイベント（Alarms and Events）] テーブルでアラームを選択し、[注釈（Annotate）] をクリックしてテキストを入力します。確認応答と同様に、アラームに注釈を付けると、Prime Infrastructure はユーザ名と注釈のタイム スタンプをアラーム詳細の [メッセージ（Messages）] 領域に追加します。

アラームがトリガーされる方法の管理（アラームしきい値）

情報の収集頻度（ポーリング間隔）、問題を示すしきい値、および問題が検出された場合に Prime Infrastructure で情報イベントまたは（ある重大度の）アラームを生成するかどうかをカスタマイズできます。すべてのポリシーにこれらの設定がすべて含まれているわけではありません。たとえば、統計情報だけを収集するポリシーには、しきい値やアラームが関連付けられていない可能性があります。

ステップ 1 **Monitor > Monitoring Tools > Monitoring Policies > My Policies** を選択してから、編集するポリシーを選択します。

ステップ 2 変更するパラメータを検索します。パラメータを検索するには、[パラメータ（Parameters）]テキストボックスに文字列を入力します。

ステップ 3 ポーリング間隔を調整するには、[ポーリング頻度（Polling Frequency）] ドロップダウンリストから新しい間隔を選択します。ポーリングを無効にするには、**[No Polling]** を選択します。パラメータのグループに適用されるポーリング頻度があることに注意してください。グループ間隔を変更すると、そのグループのすべての設定のポーリングが変更されます。ポリシーに、関連付けられたしきい値またはイベントがない場合、Prime Infrastructure は変更を保存するように求めるプロンプトを表示します。

ステップ 4 しきい値を変更するには、パラメータを展開し、パラメータのドロップダウン リストから値を選択します。

ステップ 5 しきい値を超過した場合に Prime Infrastructure が何を実行するかを指定するには、パラメータのドロップダウンリストからアラーム値を選択します。指定した重要度のアラームを生成する、情報イベントを生成する、または何もしない（何の対応も指定しない場合）ように Prime Infrastructure を設定できます。

ステップ 6 次をクリックします。

- **Save and Activate** ポリシーを保存し、選択したデバイスですぐに有効化します。
- **Save and Close** ポリシーを保存し、後で有効にします。

（注） アクセス ポイントが他の AP によって不正と認識されても、Prime Infrastructure で管理されている場合は、アラームは発生しません。

サポートされるイベント

Cisco Prime Infrastructure でサポートされているイベントの詳細については、「Cisco Prime Infrastructure Alarms, Events, and Supported SNMP Traps and Syslogs」を参照してください。

イベントの表示

アラームを表示するには、[モニタ（Monitor）] > [モニタリングツール（Monitoring Tools）] > [アラームおよびイベント（Alarms and Events）] の順に選択し、[イベント（Events）] タブをクリックします。

[アクティブなイベントを表示（Show Active Events）]：デフォルトでは、[アラームおよびイベント（Alarms and Events）] ページには、クリアされたイベントを含む最新の 4000 のアクティブなイベントが表示されます。アクティブなイベントは、[マイプリファレンス（My Preferences）] ページで選択した設定に基づいて自動的に更新されます。詳細については、アラームとイベントの表示設定のセットアップ（360ページ）を参照してください。[自動更新を一時停止（Pause Auto-Refresh）] ボタンをクリックすると、イベントの自動更新を一時的に無効にすることができます。

[イベント履歴の表示（Show Event History）]：[アラームおよびイベント（Alarms and Events）] ページで [イベント履歴の表示（Show Event History）] をクリックすると、最大 20,000 個のイベントが表示されます。[イベント履歴の表示（Show Event History）] モードでは、イベントは自動的に更新されません。ただし、[アラームおよびイベント（Alarms and Events）] テーブルの [更新（Refresh）] アイコンをクリックすると、イベントを手動で更新できます。

[イベント（Events）] タブにはさまざまなフィルタが用意されており、それを使用して探している情報を見つけることができます。アラームの検索および表示（356ページ） で説明されている同じ手順を使用して、カスタマイズ（プリセット）したフィルタを作成して保存することもできます。次の表に、イベントをフィルタリングする方法の一部を示します。

[スナップショットの作成 (Take Snapshot)] タブをクリックして、ページングされたイベントを表示します。最大 2 万ページのイベントを表示できます。タブ名は、**現在の日付と時刻**のスナップショットとして変更されます。デフォルトでは、50イベントがページごとに表示されます。**ページ サイズ**は 50 ~ 200 の範囲で変更できます。

検索するイベント	**[モニタ（Monitor）] > [モニタリングツール（Monitoring Tools）] > [アラームおよびイベント（Alarms and Events）] を選択し、[イベント（Events）] タブをクリックして、次の手順を実行します。**
デバイス グループ、シリーズ、タイプ、ロケーション グループ、またはユーザ定義グループによって生成されたすべてのイベント	左側のサイドバー メニューからグループを選択します。
最後の *x* 分、時間、または日のイベント	[表示（Show）] ドロップダウン フィルタ リストをクリックし、適切なフィルタを選択します。
直前の 1 時間に生成された非情報イベント	[表示（Show）] ドロップダウン フィルタ リストから、[過去1時間の非情報イベント（Non-info events in last hour）] を選択します。

検索するイベント	**[モニタ（Monitor）] > [モニタリングツール（Monitoring Tools）] > [アラームおよびイベント（Alarms and Events）]** を選択し、**[イベント（Events）]** タブをクリックして、次の手順を実行します。
カスタマイズされたフィルタを使用したイベント	高度なフィルタを作成して保存します（アラームの検索および表示 （356 ページ） を参照）。

Syslog ポリシーの表示

Syslog ポリシーを表示するには、次の手順を実行します。

ステップ 1 **[モニタ（Monitor）] > [モニタリング ツール（Monitoring Tools）] > [Syslog ポリシー（Syslog Policies）]** の順に選択します。すべての syslog ポリシーが [Syslog ポリシー（Syslog Policies）] ページに表示されます。

ステップ 2 ポリシーを表示するには、展開アイコンをクリックします。

関連トピック

新しい syslog ポリシーの作成 （370 ページ）
Syslog ポリシーの編集 （372 ページ）
Syslog ポリシー ランクを変更します （372 ページ）
Syslog ポリシー ランクを変更します

新しい syslog ポリシーの作成

新しい Syslog ポリシーを作成するには、次の手順を実行します。

ステップ 1 **[モニタ（Monitor）] > [モニタリング ツール（Monitoring Tools）] > [Syslog ポリシー（Syslog Policies）]** の順に選択します。

ステップ 2 [Add] アイコンをクリックします。**[新しい Syslog ポリシーの作成（Create New Syslog Policy）]** ウィンドウを表示します。

ステップ 3 **[ポリシー属性（Policy Attributes）]** ページで、固有の名前、説明 (オプション) を入力し、ポリシーを実行する希望のアクション タイプを選択します。

ステップ 4 [Next] をクリックします。

ステップ 5 [ポリシー属性（Policy Attributes）] ウィンドウで選択したポリシー アクションに基づいて、**[メールの送信（Send Email）]** オプションまたは **[スクリプトの実行（Run Script）]** オプションが表示されます。

- **[電子メールの送信 (Send Email)] オプション**
  - **[新規電子メール受信者の作成（Create New Email Recipient）]** をクリックし、新しい受信者を作成するための名前と電子メールアドレスを入力します。

- または、ドロップダウン リストから受信者と通知の時間範囲を選択します。
- 複数の受信者を指定するには、**[追加（(Add）]** アイコンをクリックします。電子メールを送信すると、対応する特定の時間帯に syslog の一致を受信したときに、複数の受信者にメールで通知します。

- **スクリプトの実行オプション**
  - システムから新しいスクリプトをアップロードするには、**[スクリプトのアップロード (Upload Scripts)]** ボタンをクリックします。Prime Infrastructure は、すべてのタイプの syslog スクリプトとパラメータを承認します。したがって、任意のタイプのスクリプトをアップロードし、それらのスクリプトに関連するパラメータを指定できます。アップロードするスクリプトが **[スクリプトファイル (Script file)]** ドロップダウン リストに表示されます。ドロップダウン リストからアップロードされたスクリプトのいずれかを選択し、新しい syslog ポリシーを作成できます。

デフォルトでは、**[スクリプトの実行（Run Script）]** オプションが無効です。**[スクリプトの実行（Run Script）]** オプションを有効にするには、**[管理者（Administration）] > [設定（Settings）] > [システム設定（System Settings）] > [アラームおよびイベント（alarm And Events）] > [Syslog ポリシー（Syslog Policies）]** に移動します。Syslog ポリシーのシステム設定ページにアクセスするには、Syslog ポリシーの設定にアクセス権限が必要です。

ステップ 6 [Next] をクリックします。

ステップ 7 **[デバイス グループ (Device Groups)]** ウィンドウで、syslog ポリシーを適用するデバイス グループを選択します。デバイス グループを選択しないと、ポリシーがすべてのデバイスに適用されます。

ステップ 8 [Syslog フィールド (Syslog Fields)] ウィンドウで、syslog フィールドに次のフィルタを設定します。

- すべてのメッセージ: ポリシーは、その他の条件 (デバイス グループなど) を満たすすべての syslog に対してアクティブ化されます。Syslog メッセージの内容は、ポリシーがアクティブ化されているかどうかに影響しません。
- メッセージ タイプ: ポリシーは、ファシリティ、重大度、およびニーモニック フィールドの特定の組み合わせなど、特定のメッセージ タイプに一致する syslog にのみ適用されます。
- 高度なフィルタ: ファシリティ、重大度、およびニーモニックの各フィールドにより複雑なフィルタを作成します。
  - フィールド (ファシリティ、重大度、またはニーモニック) を選択します。
  - フィルタ操作を選択します。ほとんどのフィルタには、値も必要です。フィルタのリストの上にある [一致（Match）] オプション ボタンでは、特定の条件をすべて true にする必要があるか、または少なくとも 1 つを true にする必要があるかどうかを決定します。

ステップ 9 **[サマリ（Summary）]** をクリックして、syslog ポリシーの詳細を表示します。設定を変更する場合は、それぞれのウィンドウに移動し、必要な変更を行います。

ステップ 10 [Finish] をクリックします。

Syslog ポリシーの編集

新しい Syslog ポリシーを編集するには、次の手順を実行します。

ステップ 1 **[モニタ（Monitor）] > [モニタリング ツール（Monitoring Tools）] > [Syslog ポリシー（Syslog Policies）]** の順に選択します。

ステップ 2 ポリシーを選択して、**[編集（Edit）]** アイコンをクリックします。**[Syslog ポリシーの編集（Edit Syslog policy））]** ウィザードが表示されます。

ステップ 3 **[ポリシーの属性（Policy Attributes）]** ウィンドウで、必要に応じて [説明（Description）] を確認し、変更します。

（注） ポリシーの作成後にポリシー名とアクション タイプを変更することはできません。

ステップ 4 [Syslog ポリシーの編集 (Edit Syslog Policy)] ウィザードで必要な変更を行うには、「新しい Syslog ポリシー ウィザードの作成」の手順と同じ手順を実行します。

ステップ 5 **[終了（Finish）]** をクリックして、変更を保存するか、または [キャンセル（Cancel）] をクリックして、変更を廃棄します。

syslog ポリシーの削除

Syslog ポリシーを削除するには、次の手順を実行します。

ステップ 1 **[モニタ（Monitor）] > [モニタリング ツール（Monitoring Tools）] > [Syslog ポリシー（Syslog Policies）]** の順に選択します。

ステップ 2 削除する syslog ポリシーを選択し、**[削除（Delete）]** アイコンをクリックします。

ステップ 3 [削除の確認（Delete Confirmation）] ダイアログボックスで [はい（yes）] をクリックして削除するか、または [いいえ（No）] をクリックしてキャンセルします。

Syslog ポリシー ランクを変更します

既存の syslog ポリシーランクを変更するには、次の手順を実行します。

ステップ 1 **[モニタ（Monitor）] > [モニタリング ツール（Monitoring Tools）] > [Syslog ポリシー（Syslog Policies）]** の順に選択します。

ステップ 2 ランクを変更する syslog ポリシーを選択します。

ステップ 3 [**Move Up**] または [**move Down**] ボタンをクリックして、選択したポリシーのランクを拡大または縮小します。[Move Up] または [move Down] ボタンをクリックして、選択したポリシーのランクを拡大または縮小します。または

ステップ 4 **[移動（Move）]** ボタンをクリックします。ドロップダウン ボックスに目的のランクを入力し、[enter] をクリックして変更を保存できます。

Syslog の表示

Prime Infrastructure は、Prime Infrastructure のすべての管理対象デバイスによって生成される、重大度 0 ～ 7（緊急メッセージ～デバッグ メッセージ）の syslog をすべてログに記録します。管理対象外デバイスからの syslog は、ログに記録されることも表示されることもありません。また、Prime Infrastructure はすべての SNMP メッセージもログに記録します。

Prime Infrastructure は最大 2,000,000 件の syslog を保存しますが、次の表示制限があります。

- syslog のライブ ストリーミング：最新の 2,000 件の syslog
- syslog の履歴：最大 100,000 件の syslog
- スナップショット: 制限なし

ステップ 1 syslog を表示するには、**[モニタ（Monitor）]** > **[モニタリング ツール（Monitoring Tools）]** > **[Syslog ビューア（Syslog Viewer）]** を選択します。

異なる syslog を見つけるには、フィルタを使用します。フィールドに正規表現を使用できます。次に例を示します。

```
^Auth, V|violation|$,^Sec*V|violation$
```

ステップ 2 syslog をライブで表示するには、[ライブ（Live）] タブをクリックします。データが多すぎる場合は、[一時停止（Pause）] アイコンをクリックします。[再開（Resume）] ボタンをクリックして、いつでも再開できます。

ステップ 3 重複する syslog を表示するには、**[重複排除（Deduplicate）]** をクリックします。Prime Infrastructure はそのタイプの syslog を 1 行の項目に集約し、**[カウント（Count）]** フィールドにカウントを表示します。

ステップ 4 古い syslog（[ライブ（Live）] タブをクリックする前に受信した syslog）を表示するには、[履歴（Historic）] タブをクリックします。**[Syslog ポリシーの作成（Create Syslog policy）]** ボタンをクリックして、新しい Syslog ポリシーを作成します。

ステップ 5 静的な syslog を表示するには、[スナップショット（SnapShot）] タブをクリックします。タブでは、現在の日付と時刻がタブ名になっています。

（注） デフォルトでは、syslog は、タイムスタンプの降順にソートされます。

ステップ 6 1 ページに表示する syslog の数を選択するには、[ページサイズ（Page Size）] を入力します。ページごとのレコード数の範囲は 50 ～ 200 です。

（注） [ページ（Page）] ドロップダウン リストには、各ページのレコードの日付と時刻の範囲がツールヒントとして表示されます。これにより、レコードが追跡しやすくなっています。

ステップ 7 ライブ/履歴/スナップショットの syslog を CSV にエクスポートするには、特定の syslog タブのテーブル/ページの右上隅にある をクリックして、[エクスポート（Export）] ダイアログ ボックスを開きます。

ステップ 8 [エクスポート（Export）] をクリックします。最初の 1000 レコードがエクスポートされます。

CSV ファイルまたは PDF ファイルへのアラーム、イベント、または syslog のエクスポート

この手順を使用して、アラーム、イベント、または syslog を CSV ファイルまたは PDF ファイルとして保存します。

ステップ 1 エクスポートするデータに移動します。

アラーム：**[モニタ（Monitor）] > [モニタリングツール（Monitoring Tools）] > [アラームおよびイベント（Alarms and Events）]** を選択し、[アラーム（Alarms）] タブをクリックします。

ステップ 2 データが大量にある場合はフィルタを適用します。フィルタを適用しないと、エクスポートの処理に時間がかかることがあります。

ステップ 3 テーブルの右上にある をクリックし、[エクスポート（Export）] ダイアログボックスを開きます。

ステップ 4 [CSV] または [PDF] を選択して [OK] をクリックし、ファイルを保存します。

アラーム、イベント、および Syslog レポートの操作

このセクションでは、アラーム、イベント、および syslog レポートを作成、スケジュール、実行する方法について説明します。

関連トピック

新しいアラームレポートを作成する （374 ページ）
新しいイベントレポートを作成する （375 ページ）
新しい Syslog レポートの作成 （377 ページ）

新しいアラームレポートを作成する

アラーム レポートを作成するには、次の手順を実行します。

ステップ 1 **[レポート（Report）] > [レポート起動パッド（report Launch Pad）] > [障害（Fault）] > [アラーム レポート（Alarm Reports）]** に移動します。

ステップ 2 [新規（New）] ボタンをクリックします。**[新規アラーム レポート（New Alarm Reports）]** ページが表示されます。

ステップ 3 メイン ドメインとサブ ドメインの両方に対してアラーム レポートを作成する場合は、**[現在の仮想ドメインと各サブドメインにレポートを作成する（Create the report in the current virtual domain and the sub domains）]** チェックボックスをオンにします。

ステップ 4 **[レポート タイトル（Report Title）]** テキスト ボックスにレポートのタイトルを入力します。

ステップ 5 **[レポート（Report By）]** リスト ボックスからオプションを選択します。

ステップ 6 **[編集（Edit）]** ボタン (**[レポート条件（Report Criteria）]** フィールドに隣接) をクリックして、条件を変更します。

ステップ 7 **[重大度（Severity）]** リストボックスからレポートの重大度レベルを選択します。使用可能なオプションは、クリア、重大、情報、メジャー、マイナー、警告です。

ステップ 8 **[アラーム カテゴリ (Alarm Category)]** リスト ボックスから任意のオプションを選択します。

ステップ 9 **[レポート期間（Reporting Period）]** を選択します。リスト ボックスからオプションを選択するか、開始日と終了日を指定できます。

ステップ 10 **[カスタマイズ（Customize）]** ボタンをクリックして、レポートをカスタマイズします。

ステップ 11 **[有効化（Enable）]** チェックボックスをオンにして、スケジュールを許可します。

ステップ 12 **[形式のエクスポート（Export Format）]** リストボックスからエクスポートする必要があるレポートの形式を選択します。使用可能な形式は CSV と PDF です。

ステップ 13 レポートを配信する宛先を入力します。メール ID または SFTP サーバ名にできます。

ステップ 14 **[開始日/時間（Start Date/Time）]** テキスト ボックスをクリックして、日付と時間を設定します。デフォルトでは、現在の日時が表示されます。

ステップ 15 希望の繰り返し期間を設定します。

ステップ 16 **[レポート実行結果（Report Run Result）]** ラベルに隣接する [保存（save）] アイコンをクリックして、**[履歴の実行（Run History）]** ページを開きます。

ステップ 17 **[実行（Run）]** ボタンをクリックして、レポートを生成します。

ステップ 18 **[保存（Save）]** ボタンをクリックして、レポートを保存します。

ステップ 19 **[実行して保存（Run and Save）]** ボタンをクリックして、レポートを生成し、後で使用するために保存します。

ステップ 20 **[保存してエクスポート（Save and Export）]** ボタンをクリックして、レポート パラメータを保存して、CSV または PDF ファイルとしてエクスポートします。

ステップ 21 **[保存してメール（Save and Email））]** ボタンをクリックして、レポート パラメータを保存し、メールで送信します。

ステップ 22 **[キャンセル（Cancel）]** ボタンをクリックして、変更を破棄します。

新しいイベントレポートを作成する

イベント レポートを作成するには、次の手順を実行します。

ステップ 1 **[レポート（Report）]** > **[レポート起動パッド（report Launch Pad）]** > **[障害（Fault）]** > **[イベント レポート（Events Reports）]** に移動します。

ステップ 2 [新規（New）] ボタンをクリックします。**[新規イベント レポート（New Events Reports）]** ページが表示されます。

ステップ 3 メイン ドメインとサブ ドメインの両方に対してイベント レポートを作成する場合は、**[現在の仮想ドメインと各サブドメインにレポートを作成する（Create the report in the current virtual domain and the sub domains）]** チェックボックスをオンにします。

ステップ 4 **[レポート タイトル（Report Title）]** テキスト ボックスにレポートのタイトルを入力します。

ステップ 5 **[レポート（Report By）]** リスト ボックスからオプションを選択します。

ステップ 6 **[編集（Edit）]** ボタン (**[レポート条件（Report Criteria）]** フィールドに隣接) をクリックして、条件を変更します。

ステップ 7 **[重大度（Severity）]** リスト ボックスからレポートの重大度レベルを選択します。使用可能なオプションは、クリア、重大、情報、メジャー、マイナー、警告です。

ステップ 8 **[イベント カテゴリ (Event Category)]** リスト ボックスから任意のオプションを選択します。

ステップ 9 **[レポート期間（Reporting Period）]** を選択します。リスト ボックスからオプションを選択するか、開始日と終了日を指定できます。

ステップ 10 **[カスタマイズ（Customize）]** ボタンをクリックして、レポートをカスタマイズします。

ステップ 11 **[有効化（Enable）]** チェックボックスをオンにして、スケジュールを許可します。

ステップ 12 **[形式のエクスポート（Export Format）]** リスト ボックスからエクスポートする必要があるレポートの形式を選択します。使用可能な形式は CSV と PDF です。

ステップ 13 レポートを配信する宛先を入力します。メール ID または SFTP サーバ名にできます。

ステップ 14 **[開始日/時間（Start Date/Time）]** テキスト ボックスをクリックして、日付と時間を設定します。デフォルトでは、現在の日時が表示されます。

ステップ 15 希望の繰り返し期間を設定します。

ステップ 16 **[レポート実行結果（Report Run Result）]** ラベルに隣接する [保存（save）] アイコンをクリックして、**[履歴の実行（Run History）]** ページを開きます。

ステップ 17 **[実行（Run）]** ボタンをクリックして、レポートを生成します。

ステップ 18 **[保存（Save）]** ボタンをクリックして、レポートを保存します。

ステップ 19 **[実行して保存（Run and Save）]** ボタンをクリックして、レポートを生成し、後で使用するために保存します。

ステップ 20 **[保存してエクスポート（Save and Export）]** ボタンをクリックして、レポート パラメータを保存して、CSV または PDF ファイルとしてエクスポートします。

ステップ 21 **[保存してメール（Save and Email）]** ボタンをクリックして、レポート パラメータを保存し、メールで送信します。

ステップ 22 **[キャンセル（Cancel）]** ボタンをクリックして、変更を破棄します。

新しい Syslog レポートの作成

Syslog レポートを作成するには、次の手順を実行します。

ステップ 1 **[レポート（Report）] > [レポート起動パッド（report Launch Pad）] > [障害（Fault）] > [Syslog レポート（Syslog Reports）]** に移動します。

ステップ 2 [新規（New）] ボタンをクリックします。**[新規 Syslog レポート（New Syslog Reports））]** ページが表示されます。

ステップ 3 メイン ドメインとサブ ドメインの両方に対して syslog レポートを作成する場合は、**[現在の仮想ドメインと各サブドメインにレポートを作成する（Create the report in the current virtual domain and the sub domains）]** チェックボックスをオンにします。

ステップ 4 **[レポート タイトル（Report Title）]** テキスト ボックスにレポートのタイトルを入力します。

ステップ 5 **[レポート（Report By）]** リスト ボックスからオプションを選択します。

ステップ 6 **[編集（Edit）]** ボタン (**[レポート条件（Report Criteria）]** フィールドに隣接) をクリックして、条件を変更します。

ステップ 7 **[重大度（Severity）]** リストボックスからレポートの重大度レベルを選択します。使用可能なオプションは、アラート、重大、デバッグ、緊急、エラー、情報、通知、警告です。

ステップ 8 **[レポート期間（Reporting Period）]** を選択します。リスト ボックスからオプションを選択するか、開始日と終了日を指定できます。

ステップ 9 **[カスタマイズ（Customize）]** ボタンをクリックして、レポートをカスタマイズします。

ステップ 10 **[有効化（Enable）]** チェックボックスをオンにして、スケジュールを許可します。

ステップ 11 **[形式のエクスポート（Export Format）]** リストボックスからエクスポートする必要があるレポートの形式を選択します。使用可能な形式は CSV と PDF です。

ステップ 12 レポートを配信する宛先を入力します。メール ID または SFTP サーバ名にできます。

ステップ 13 **[開始日/時間（Start Date/Time）]** テキスト ボックスをクリックして、日付と時間を設定します。デフォルトでは、現在の日時が表示されます。

ステップ 14 希望の繰り返し期間を設定します。

ステップ 15 **[レポート実行結果（Report Run Result）]** ラベルに隣接する [保存（save）] アイコンをクリックして、**[履歴の実行（Run History）]** ページを開きます。

ステップ 16 **[実行（Run）]** ボタンをクリックして、レポートを生成します。

ステップ 17 **[保存（Save）]** ボタンをクリックして、レポートを保存します。

ステップ 18 **[実行して保存（Run and Save）]** ボタンをクリックして、レポートを生成し、後で使用するために保存します。

ステップ 19 **[保存してエクスポート（Save and Export）]** ボタンをクリックして、レポート パラメータを保存して、CSV または PDF ファイルとしてエクスポートします。

ステップ 20 **[保存してメール（Save and Email）））]** ボタンをクリックして、レポート パラメータを保存し、メールで送信します。

ステップ 21 **[キャンセル（Cancel）]** ボタンをクリックして、変更を破棄します。

シスコからサポートを受ける

Monitor > Monitoring Tools > Alarms and Events でアラームを受信し、シスコ サポート コミュニティ（アラームをクリックして **Troubleshoot > Support Forum** を選択）で解決策が見つからない場合は、Prime Infrastructure を使用してサポート要求を開きます（アラームをクリックして **Troubleshoot > Support Case** を選択）。

Prime Infrastructure 内の問題への対応

Prime Infrastructure は、サーバの CPU とディスクの使用率、ファンと電源装置の障害、高可用性（HA）状態の変化など、独自の機能を監視するための内部 SNMP トラップを生成します。

アラーム ポリシーとは

アラーム ポリシーはフィルタリングの方法で、これを使用することでネットワークの状況に関するアラームを制御し、システムのノイズを削減することができます。アラーム ポリシーを表示するには、[モニタ（Monitor）]>[モニタリングツール（Monitoring Tools）]>[アラームポリシー（Alarm Policies）] を選択します。アラーム ポリシーを作成、編集、削除、およびランク付けすることができます。アラーム ポリシーには、1 つ以上の条件と、すべての定義された条件を満たすすべてのイベント/アラームに適用されるアクションが含まれます。

新しいアラーム ポリシーは、Prime Infrastructure ですでに生成されているアラームには適用されません。Prime Infrastructure でアラーム ポリシーを有効にするには、既存のアラームを削除またはクリアする必要があります。

次の操作を実行するアラーム ポリシーを作成できます。

- アラームの抑制：選択したイベントのアラームを生成しません。しかし、イベントは作成され、正常に保存されます。
- イベントおよびアラームの抑制：イベントおよびアラームを作成しません。
- アラーム重大度の変更：ポリシーに設定された条件を満たすアラーム/イベントのシステム全体のデフォルト重大度を上書きします。
- 関連付けの解除しきい値アラームの作成：1 つ以上のデバイス グループにまたがる一定の割合のアクセス ポイントがコントローラから関連付け解除されたときにアラームを生成します。
- AP の関連付け解除アラーム抑制の設定：「AP がコントローラから関連付け解除されました」という状態のアラームを、永続的または一時的に抑制します。

関連トピック

新しいアラーム ポリシーの作成 （381 ページ）
アラーム ポリシーのタイプ （379 ページ）
既存のアラーム ポリシーの編集 （383 ページ）
アラーム ポリシーのランク （380 ページ）

アラーム ポリシーのタイプ

次の表に、アラーム ポリシー タイプと、各アラーム ポリシー タイプで使用可能なさまざまなアラーム アクションを示します。

ポリシー タイプ	使用可能なアクション オプション
アクセス ポイント（Access Point）	• アラームの抑制 • アラームとイベントの抑制 • アラーム重大度の変更
APの関連付けの解除（AP Disassociation）	• 関連付け解除しきい値アラームの作成 • AP の関連付け解除アラームの抑制の設定
コントローラ（Controller）	• アラームの抑制 • アラームとイベントの抑制 • アラーム重大度の変更
インターフェイス（Interface）	• アラームの抑制 • アラームとイベントの抑制 • アラーム重大度の変更
レイヤ 2 スイッチ	• アラームの抑制 • アラームとイベントの抑制 • アラーム重大度の変更
システム	• アラームの抑制 • アラームとイベントの抑制 • アラーム重大度の変更
Unclassified	• アラームの抑制 • アラームとイベントの抑制 • アラーム重大度の変更

ポリシー タイプ	使用可能なアクション オプション
有線インフラストラクチャ（Wired Infrastructure）	• アラームの抑制 • アラームとイベントの抑制 • アラーム重大度の変更

（注） [Unclassified（未分類）] ポリシー タイプでは、別のポリシー タイプに関連付けられていないすべてのサポート対象イベント タイプが表示されます。[Unclassified（未分類）] ポリシーで利用可能な条件とアクションは、[コントローラ（Controller）] など、利用可能な他のポリシー タイプと同じです。

アラーム ポリシーのランク

ランクによって、2 つ以上のポリシーを同じアラームまたはイベントに適用する場合のアラーム ポリシーの優先度または実行順序が決まります。デフォルトでは、作成順にアラーム ポリシーがランク付けされます。

次に、アラーム ポリシーにランク付けをするときに覚えておくべきポイントを示します。

1. ランクの数字が小さいほど、優先度が高くなります。
2. ランクが最も高いポリシーが最初に適用され、以降はランクが次に高いポリシーから順に適用されていきます。
3. ランクが高いポリシーがランクが低いポリシーの動作に影響を与えたり、低いランクのポリシーを完全にオーバーライドすることがあります。
   - ランクが高いアラームの抑制ポリシーがすでにイベントに適用されている場合、アラームの抑制は適用されません。
   - アラームとイベントの抑制は、次のいずれの場合も適用されません。
     - ランクが高い抑制ポリシーがすでにイベントに適用されている。
     - イベントに AP との関連付けが長期間に渡って解除されていることが示されている。
   - ランクが高い重大度変更ポリシーがすでにイベントまたはアラームに適用されている場合、アラーム重大度の変更は適用されません。
   - [関連付け解除しきい値アラームの作成（Create Disassociation Threshold Alarm）]：ランクが高い抑制ポリシーによって抑制されている AP の関連付け解除アラームはカウントしません。AP 関連付け解除アラームが一時的に抑制されている場合、それらのアラームは抑制期間が満了するとカウントされるようになります。
   - [AP 関連付け解除アラームの設定（Create Disassociation Threshold Alarm）]：ランクの高い抑制ポリシーがすでにアラームに適用されている場合、抑制は適用されません。

アラーム ポリシーを変更するには、次の手順を実行します。

ステップ 1 **[モニタ（Monitor）] > [モニタリングツール（Monitoring Tools）] > [アラームポリシー（Alarm Policies）]** の順に選択します。

すべてのアラーム ポリシーが作成された順序で一覧表示されます。

ステップ 2 順序を変更するアラーム ポリシーを選択します。

ステップ 3 [移動先（Move To）] アイコンをクリックし、[行（Row）] フィールドに順位を入力するか、[上へ移動（Move up）] アイコンまたは [下へ移動（Move down）] アイコンをクリックして順位を変更します。

アラーム ポリシーの表示

ステップ 1 **[モニタ（Monitor）] > [モニタリングツール（Monitoring Tools）] > [アラームポリシー（Alarm Policies）]** の順に選択します。

[アラーム ポリシー（Alarm Policies）] ページにすべてのアラーム ポリシーが一覧表示されます。

ステップ 2 ポリシーを表示するには、展開アイコンをクリックします。

新しいアラーム ポリシーの作成

新しいアラーム ポリシーを作成するには、次の手順を実行します。

ステップ 1 **[モニタ（Monitor）] > [モニタリングツール（Monitoring Tools）] > [アラームポリシー（Alarm Policies）]** の順に選択します。

ステップ 2 [追加（Add）] アイコンをクリックし、[ポリシー タイプの選択（Select A Policy Type）] ウィンドウからポリシー タイプを選択します。

[新しいアラーム ポリシーの作成（Create a New Alarm Policy）] ウィザードが表示されます。

ステップ 3 [ポリシーの属性（Policy Attributes）] ページで [名前（Name）]、[説明（Description）]（任意）に入力し、実行するアクションのタイプを選択します。

ここに表示されるアクションのタイプは、前のステップで選択したポリシーに基づきます。「関連リンク」の「アラーム ポリシーのタイプ」を参照してください。

ステップ 4 ポリシー タイプがアクセス ポイント、コントローラ、インターフェイス、レイヤ 2 スイッチ、未分類、システム、および有線インフラストラクチャの場合は、次の手順を実行します。

a) [アクションオプション（Action Options）] タブにある次のオプションのうち、いずれか 1 つを選択します。

- 完全に抑制（Suppress Permanently）

- [この期間に条件が改善されない場合に表示（分）（Display if the condition persists for this duration (minutes)）]：タイム スライダを使用して期間を選択します。

（注） このタブは、ステップ 3 で [アラームの抑制（Suppress Alarms）] を選択した場合のみ有効になります。

b) デバイス グループを選択します。

デバイスを選択しないと、ポリシーがすべてのデバイスに適用されます。

c) （インターフェイス ポリシーの場合のみ）ポート グループを選択します。

ポートを選択しないと、ポリシーがすべてのポート デバイスに適用されます。

d) 抑制するアラームまたはイベント、あるいは [ポリシーの属性（Policy Attributes）] ページで選択したアクションに基づいて重大度を変更するアラームまたはイベントを選択します。

e) [概要（Summary）] をクリックして、ポリシーの詳細を表示します。設定を変更する場合は、それぞれのページに移動し、必要な変更を行います。

f) [終了（Finish）] をクリックします。

ステップ 5 AP の関連付け解除ポリシー タイプの場合は、次の手順を実行します。

（注） AP の解除アラーム ポリシーは、リーフ ノードにのみ適用されます。

a) [アクションオプション（Action Options）] タブにある次のオプションのうち、いずれか 1 つを選択します。

ステップ 3 で [APの関連付け解除アラームの抑制の設定（Configure Suppression for AP Disassociated Alarms）] を選択している場合は、次のオプションを選択します。

- 完全に抑制（Suppress Permanently）
- [この期間に条件が改善されない場合に表示（分）（Display if the condition persists for this duration (minutes)）]：タイム スライダを使用して期間を選択します。

ステップ 3 で [関連付け解除しきい値アラームの作成（Create Disassociation Threshold Alarm）] を選択している場合は、次のオプションを選択します。

- 完全に抑制（Suppress Permanently）
- 設定された関連付け解除のしきい値に達したら非表示にする（Suppress after the configured disassociation threshold is reached）
- 非表示にしない（Do not Suppress）

b) デバイス グループを選択します。

[ポリシーの属性（Policy Attributes）] ページで [関連付け解除しきい値アラームの作成（Create Diassociation Threshold Alarm）] アクションを選択した場合、これは必須ステップです。[AP の関連付け解除アラームの抑制の設定（Configure Suppression for AP Disassociated Alarms）] アクションを選択しなかった場合は、ポリシーがすべてのデバイスに適用されます。

c) [関連付け解除しきい値アラームの作成（Create Diassociation Threshold Alarm）] アクションの場合は、必要な関連付け解除しきい値のパーセンテージを選択します。

d) [AP の関連付け解除アラームの抑制の設定（Configure Suppression for AP Disassociated Alarms）] アクションの場合、アラームを完全に抑制するには [完全に抑制（Suppress Permanently）] をクリックするか、または [この期間に条件が改善されない場合に表示（Display if the condition persists for this duration）] をクリックし、スライダーを使用して抑制する期間を選択します。

e) [概要（Summary）] をクリックして、ポリシーの詳細を表示します。設定を変更する場合は、それぞれのページに移動し、必要な変更を行います。

f) [終了（Finish）] をクリックします。

関連トピック

アラーム ポリシーのタイプ （379 ページ）
既存のアラーム ポリシーの編集 （383 ページ）

既存のアラーム ポリシーの編集

アラーム ポリシーを編集するには、次の手順を実行します。

ステップ 1 **[モニタ（Monitor）] > [モニタリングツール（Monitoring Tools）] > [アラームポリシー（Alarm Policies）]** の順に選択します。

ステップ 2 ポリシーを選択し、[編集（Edit）] アイコンをクリックします。

[アラーム ポリシーの編集（Edit Alarm Policy）] ウィザードが表示されます。

ステップ 3 [ポリシーの属性（Policy Attributes）] ページで、必要に応じて [説明（Description）] を確認し、変更します。

ポリシー作成中は、選択したポリシー名およびアクションを編集できません。

ステップ 4 [アラーム ポリシーの編集（Edit Alarm Policy）] ウィザードでの残りのステップは、[新しいアラーム ポリシーの作成（Create a New Alarm Policy）] ウィザードの手順と同じです。新しいアラーム ポリシーの作成（381 ページ）を参照してください。.

ステップ 5 [終了（Finish）] をクリックして、変更を保存するか、または [キャンセル（Cancel）] をクリックして、変更を廃棄します。

関連トピック

アラーム ポリシーとは （378 ページ）
新しいアラーム ポリシーの作成 （381 ページ）

アラーム ポリシーの削除

アラーム ポリシーを削除するには、次の手順を実行します。

ステップ 1 **[モニタ（Monitor）] > [モニタリングツール（Monitoring Tools）] > [アラームポリシー（Alarm Policies）]** の順に選択します。

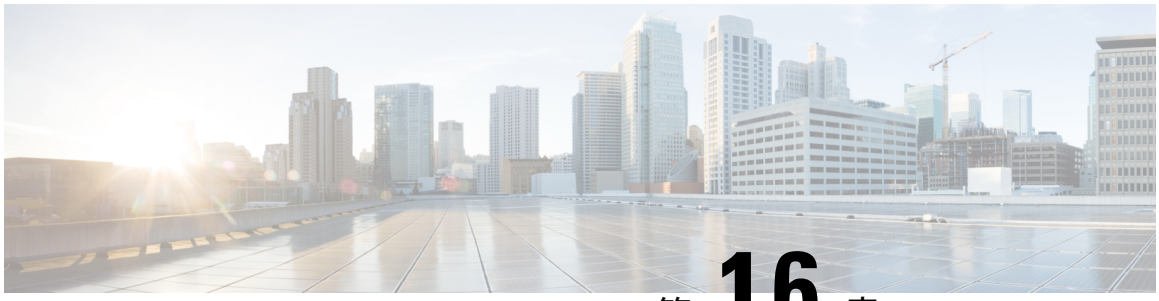
ステップ 2 削除するアラーム ポリシーを選択し、[削除（Delete）] アイコンをクリックします。

ステップ 3 [削除の確認（Delete Confirmation）] ダイアログボックスで [はい（yes）] をクリックして削除するか、または [いいえ（No）] をクリックしてキャンセルします。

アラームおよびイベントの通知ポリシー

特定のデバイス グループから特定の受信者グループに生成された特定の対象アラームに関する通知を送信するためのポリシーを作成できます。

詳細については、『Cisco Prime Infrastructure Administrator Guide』の「Fault Management Administration Tasks」の章の「*Event Receiving, Forwarding, and Notifications*」の項を参照してください。



第 16 章

ネットワーク クライアントとユーザのモニタ

- ネットワーク有線/ワイヤレス クライアントとは （385 ページ）
- クライアントサマリ ダッシュボードを使用したネットワーク ユーザーおよびクライアントのモニタ （387 ページ）
- ネットワーク クライアント トラブルシューティング ツールの起動 （391 ページ）
- ネットワーク クライアント トラブルシューティング ツールを使用する方法 （396ページ）
- ネットワーク クライアントの接続時の確認 （404 ページ）
- 不明なネットワーク ユーザの識別 （406 ページ）
- [コントローラクライアントとユーザ（Controller Client and Users）] ページのカスタマイズ （409 ページ）
- 診断チャネルでの自動コントローラ クライアント トラブルシューティングのセットアップ （410 ページ）
- ワイヤレス ネットワーク クライアントの無線測定値の取得 （410 ページ）
- ネットワーク クライアント V5 の統計情報を表示するためのテストの実行 （411 ページ）
- ネットワーク クライアントの動作パラメータを表示するためのテストの実行 （413 ページ）
- ネットワーク クライアントの詳細の表示 （415 ページ）
- ネットワーク クライアントの無効化 （416 ページ）
- Prime Infrastructure からのネットワーク クライアントの削除 （417 ページ）
- ワイヤレス マップでのネットワーク クライアントの検索 （417 ページ）
- レポートを使用したネットワーク クライアント ローミングの表示 （418 ページ）
- ネットワーク クライアントを聞くことができるアクセス ポイントの特定 （419 ページ）
- ネットワーク クライアントのロケーション履歴の表示 （419 ページ）

ネットワーク有線/ワイヤレス クライアントとは

クライアントは、アクセス ポイントまたはスイッチに接続されたデバイスです。Prime Infrastructure は有線および無線クライアントをサポートします。コントローラおよびスイッチを Prime Infrastructure に追加すると、クライアント検出プロセスが開始されます。ワイヤレス

クライアントは、管理対象のコントローラまたはAutonomousアクセス ポイントから検出されます。コントローラは通常のクライアント ステータス ポーリング時にポーリングされます。ワイヤレス クライアント数には、Autonomous型のクライアントも含まれます。スイッチの場合は、デバイスが追加された直後にクライアントをポーリングし、データベースのデバイス情報を更新します。有線クライアントの場合、クライアントアソシエーションを検出するためのクライアント ステータス ポーリングは、2時間ごとに行われます（デフォルトの場合）。すべてのスイッチについて、接続されているすべての有線クライアントの完全な情報をポーリングする完全ポーリングが、毎日 2 回実施されます。

Prime Infrastructure では、バックグラウンド タスクを使用して、データ ポーリング操作を実行します。クライアントと関連するタスクは 3 つあります。

1. Autonomous AP Client Status
2. Lightweight Client Status
3. Wired Client Status

[管理（Administration）]>[設定（Settings）]>[バックグラウンドタスク（Background Tasks）] ページから、データ収集タスク（ポーリング間隔など）を更新できます。『データ収集および保持の管理』を参照してください。

クライアント ステータス（有線クライアントのみ該当）は、接続、切断、または不明で示されます。

- [Connected clients]：有線スイッチに接続しているアクティブなクライアント。
- [Disconnected clients]：有線スイッチから接続が解除されたクライアント。
- [Unknown clients]：有線スイッチとの SNMP 接続が失われた時点で、不明としてマークされたクライアント。

Prime Infrastructure が管理する Autonomous アクセス ポイントのクライアントと、ローカル拡張可能認証プロトコル（LEAP）を使用して認証されたクライアントの場合、ユーザ名は登録されず、不明として表示されます。

Prime Infrastructure では、アイデンティティと非アイデンティティの両方の有線クライアントをサポートしています。有線クライアントのサポートは、アイデンティティ サービスに基づきます。アイデンティティ サービスによって、ユーザおよびデバイスに対するセキュアなネットワーク アクセスが実現される他、ネットワーク管理者は、ユーザの職務権限に基づいて、サービスとリソースをユーザにプロビジョニングできるようになります。

Prime Infrastructure は VLAN 1000 ～ 1024 で接続されているエンド ホストをポーリングしません。

Prime Infrastructure では、VRF はサポートされていません。したがって、クライアントが VRF 設定されたデバイスに接続されていても、クライアント情報は表示できません。

（注） Prime Infrastructure が SNMPv3 を使用して有線デバイスに関する情報を取得できない場合は、SNMPv2 を適用します。

関連トピック

ネットワーク クライアントの接続時の確認 （404 ページ）

クライアントサマリ ダッシュボードを使用したネットワーク ユーザーおよびクライアントのモニタ

クライアント サマリ ダッシュボードを使用して、ネットワーク ユーザーとクライアントをモニタできます。

クライアント サマリ ダッシュボード

クライアント ダッシュボード (**[ダッシュボード（Dashboard）] > [概要（Overview）] > [クライアント サマリ（Client Summary）]**)ページで、クライアント関連のダッシュレットが表示されます。これらのダッシュレットにより、ネットワーク上のクライアントをモニタできます。グラフ用のデータも定期的にポーリングおよび更新されて、Cisco Prime Infrastructure データベースに保存されます。一方、[クライアント詳細（Client Details）] ページにある情報の大部分は、コントローラまたはスイッチから直接ポーリングされます。

Cisco Prime Infrastructure にログインすると、クライアント サマリ ダッシュボードに、クライアント関連のいくつかのダッシュレットが表示されます。

- [アソシエーション/認証別のクライアントカウント（Client Count By Association/Authentication）]：選択した期間について、Cisco Prime Infrastructure でのアソシエーションおよび認証ごとのクライアントの総数が表示されます。
  - [Associated client]：認証されているかどうかに関係なく接続されているすべてのクライアント。
  - [Authenticated client]：接続されて、認証、認可、およびその他のポリシーをパスし、ネットワークを使用できる状態になったすべてのクライアント。
- クライアント配信: プロトコル、使用するEAPタイプ、認証タイプなど、現在の分布に基づいて、クライアント数が表示されます
- [ワイヤレス/有線別のクライアントカウント（Client Count By Wireless/Wired）]：選択した期間について、Cisco Prime Infrastructure での有線およびワイヤレスのクライアントの総数が表示されます。
- クライアント トラフィック: 一定期間における有線およびワイヤレス クライアントのトラフィックを表示します。
- クライアントの確認ステータス: 各 postrure のクライアント数が表示されます。

関連トピック

インタラクティブ グラフ （1119 ページ）
ダッシュボードへのダッシュレットの追加

ネットワーク クライアントとユーザを表示する方法

ネットワークの有線クライアントとワイヤレス クライアントをすべて表示するには、**[モニタ（Monitor）]**>**[モニタリング ツール（Monitoring Tools）]**>**[クライアントおよびユーザ（Clients and Users）]** を選択します。クライアント アソシエーション履歴と統計情報を表示することもできます。これらのツールは、ユーザがラップトップ コンピュータを持って建物の中を移動したときに、ネットワークのパフォーマンスについて苦情があった場合に有用です。この情報は、カバレッジが一貫していないエリアや、カバレッジがドロップする可能性があるエリアを評価するために役立ちます。

MAC アドレスをクリックして [Client Detail] ページにアクセスすると、クライアントの問題を特定、診断、および解決する際に役立ちます。

クライアントとユーザのフィルタリング

[モニタ（Monitor）] > **[モニタリング ツール（Monitoring Tools）]** > **[クライアントおよびユーザ（Clients and Users）]** ページに、デフォルトで関連付けられているすべてのクライアントが表示されます。クライアントのサブセットを表示できるプリセット フィルタがあります。

WGB、有線ゲスト、およびオフィス拡張アクセスポイント 600 (OEAP 600) は、ワイヤレス クライアントとして追跡されます。Prime Infrastructure mac アドレス、IP アドレス、ユーザ名、AP mac アドレス、SSID などのインデックスが付けられた列のソートのみを記憶します。インデックスなしの列でソートを行うと、クライアント一覧ページをロードする際に、重大なパフォーマンスの問題が発生しますが、列でテーブルをソートすることはできます。ただし、列にインデックスが付加されていない場合、このページから移動した後は、Prime Infrastructure では、最後に使用した列のソートは記憶されません。

フィルタ アイコン を使用して、フィルタのルールと一致するレコードをフィルタリングすることもできます。フィルタのルールを指定するには、[表示（Show）] ドロップダウンリストから [すべて（All）] を選択してから をクリックします。

プリセット フィルタを選択してフィルタ アイコンをクリックすると、フィルタ条件は無効になります。そのフィルタ基準は参照可能ですが変更できません。[All] オプションを選択してすべてのエントリを表示し、フィルタ アイコンをクリックすると、クイック フィルタのオプションが表示されます。ここで、フィールドを使用してデータをフィルタできます。自由形式のテキスト ボックスに、表のフィルタリング用のテキストを入力することもできます。

詳細検索機能を使用して、特定のカテゴリおよびフィルタに基づいて、クライアント リストを絞り込むことができます。

IP アドレスでのフィルタリング

IPv6アドレスに対する詳細クライアントフィルタリングを実行する場合、指定する各オクテットは、完全なオクテットである必要があります。オクテットの一部を指定した場合は、フィルタリングで正しい結果が表示されないことがあります。

次に、IPv6 アドレスに対する詳細クライアント フィルタリングの動作の例を示します。次の例では、システムに IP アドレス、10.10.40.110.10.40.210.10.40.310.10.240.1Fec0::40:20Fe80::240:20 があることを想定しています。40 を含むすべての IP アドレスを検索すると、

10.10.40.110.10.40.210.10.40.3Fec0::40:20 という結果が得られます。このフィルタリング機能では、完全なオクテットを入力することを前提としているため、240 を含む IP アドレスはフィルタ基準と一致しません。

クライアントとユーザの表示

[モニタ（Monitor）] > [モニタリング ツール（Monitoring Tools）] > [クライアントおよびユーザ（Clients and Users）] ページで完全な詳細を表示したり、無線測定などの操作を実行するには、ユーザ定義グループのユーザが [クライアントのモニタ（Monitor Clients）]、[アラートおよびイベントの表示（View Alerts & Events）]、[コントローラの設定（Configure Controllers）]、および [クライアント ロケーション（Client Location）] のページにアクセスするための必要な権限を持っている必要があります。

次の属性は、ISE が Prime Infrastructure に追加された場合にのみ自動的に入力されます。

- ISE
- エンドポイント タイプ
- ポスチャ（Posture）
- 認可プロファイル名

Prime Infrastructure は、このデータを設定するために、至近の 24 時間のクライアント認証レコードを ISE に問い合わせます。Prime Infrastructure での検出の 24 時間前にクライアントがネットワークに接続されていた場合、ISE 関連のデータはこのテーブルには表示されない場合があります。このデータは、クライアント詳細ページに表示される可能性があります。これを回避するには、クライアントをネットワークに接続し直します。次回のクライアント バックグランド タスクの実行後に、ISE 情報がテーブルに表示されます。

クライアントおよびユーザを表示するには、次の手順を実行します。

ステップ 1 **[モニタ（Monitor）] > [モニタリング ツール（Monitoring Tools）] > [クライアントおよびユーザ（Clients and Users）]** を選択して、有線クライアントとワイヤレス クライアントの両方の情報を表示します。[Clients and Users] ページが表示されます。

[Clients and Users] テーブルにはデフォルトでいくつかの列が表示されます。使用可能な追加の列を表示するには、 をクリックし、[Columns] をクリックします。使用可能な列が表示されます。[Clients and Users] 表に表示する列を選択します。列内の任意の場所をクリックすると、その列が選択され、クライアントの詳細が表示されます。

（注） クライアントがローミング中で、選択したプロトコルが [モバイル（Mobile）] の場合は、クライアントのユーザ名は表示されません。

ステップ 2 クライアントまたはユーザを選択します。選択したクライアントまたはユーザに応じて、次の情報が表示されます。

- クライアント属性
- クライアント統計情報
- クライアント統計情報
- クライアント アソシエーション履歴

- クライアント イベント情報
- クライアント ロケーション情報
- 有線ロケーション履歴
- クライアント CCXv5 情報

関連トピック

検索方法 （1129 ページ）
[コントローラクライアントとユーザ（Controller Client and Users）] ページのカスタマイズ（409 ページ）

ネットワーク クライアントとユーザのリストを CSV ファイルにエクスポートする

クライアントとユーザのリストを CSV ファイル（カンマ区切りの値を含むスプレッドシート形式）に簡単にエクスポートできます。

[Clients and Users] テーブルに表示される列は、CSV ファイルのみにエクスポートされます。

クライアントとユーザのリストをエクスポートするには、次の手順を実行します。

手順の概要

1. **[モニタ（Monitor）] > [モニタリングツール（Monitoring Tools）] > [クライアントおよびユーザ（Clients and Users）]** を選択します。
2. ツールバーの [export] アイコンをクリックします。ダイアログボックスが表示されます。
3. [File Download] ダイアログボックスで、[Save] をクリックします。

手順の詳細

ステップ 1 **[モニタ（Monitor）] > [モニタリングツール（Monitoring Tools）] > [クライアントおよびユーザ（Clients and Users）]** を選択します。

ステップ 2 ツールバーの [export] アイコンをクリックします。ダイアログボックスが表示されます。

ステップ 3 [File Download] ダイアログボックスで、[Save] をクリックします。

関連トピック

ネットワーク クライアントとユーザを表示する方法 （388 ページ）
[コントローラクライアントとユーザ（Controller Client and Users）] ページのカスタマイズ（409 ページ）

ネットワーククライアントトラブルシューティングツールの起動

どのクライアントでもクライアント トラブルシューティング ツールを、[クライアントおよびユーザ（Clients and Users）] ページから起動できます。

ステップ 1 **[モニタ（Monitor）] > [モニタリングツール（Monitoring Tools）] > [クライアントおよびユーザ（Clients and Users）]** を選択します。[Clients and Users] ページに、システムが認識するすべてのクライアント（現在アソシエートされていないクライアントを含む）が表示されます。

ステップ 2 トラブルシューティングの対象となる接続の問題が発生しているクライアントの MAC アドレスをクリックします。

検索機能を使用して最初にクライアント リストを絞り込むと便利です。

ステップ 3 [トラブルシューティングおよびデバッグ（Troubleshoot and Debug）] をクリックします。

関連トピック

クライアント トラブルシューティング ツールによるヒントの仕組み （393 ページ）

[クライアントのトラブルシューティング（Client Troubleshooting）] ページについて

[Client Troubleshooting] ページには次の情報が表示されます。

- 選択した有線クライアントまたはワイヤレス クライアントの現在または最後のセッションの詳細情報。
- 一連のグラフィック アイコンとして表示される、クライアントの現在および最後の接続ステータス。
- 接続の問題が検出された場合は次の情報が表示されます。
  - 接続問題の性質（グラフィック アイコンでも示されます）。
  - その問題のトラブルシューティングの方法に関するヒント。

（注） クライアントがポート チャネル経由でスイッチに接続されている場合、Prime Infrastructure はポート チャネルの MAC アドレスを VLAN または通常のポートとして解釈します。したがって、[クライアントのトラブルシューティング（Client Troubleshooting）] ページに正しいスイッチ情報が表示されない場合があります。

デフォルトでは、クライアントのデータは Prime Infrastructure データベースから取得されます。ページの右上隅にある [デバイスから更新（Refresh from Device）] リンクをクリックすると、

デバイスから更新するオプションを使用できます。Prime Infrastructure でデータが最後に更新された日時も表示されます。[自動更新（Auto Refresh）] がオンになっている場合、[デバイスから更新（Refresh from Devices）] オプションは無効になります。

デフォルトでは、[自動更新（Auto Refresh）] が有効になっています。デバイスでは、1 分ごとに自動的に更新し、ライブデータを収集します。また、クライアントが検出された時刻も表示されます。これを無効にするには、ページの右上隅にある [自動更新（Auto Refresh）] ボタンをクリックします。

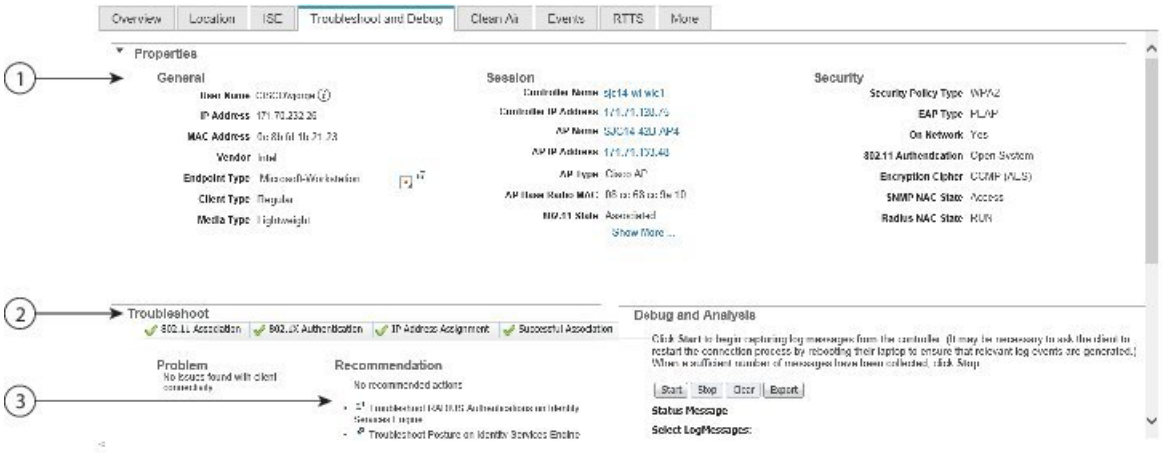
[クライアントのトラブルシューティング（Client Troubleshooting）] ページには次の情報が表示されます。

次の図に、正常に接続されたワイヤレス クライアントの完全な[クライアントのトラブルシューティング（Client Troubleshooting）] ページを示します。ページ上部の [Properties] セクションには、[Clients and Users] ページにも表示される、正常に接続されたクライアントのセッションの詳細が表示されています。

また、これは接続に問題がない場合の表示なので、下方の [Troubleshoot] セクションではワイヤレス接続プロセスの各段階のステータスに緑色のチェック マークが表示され、接続のトラブルシューティングに関するヒントは提示されていないことに注意してください。

（注） Cisco Catalyst 9800 シリーズのワイヤレス コントローラに接続されているクライアントでは、トラブルシューティングはサポートされていません。

図 *9 :* 成功したワイヤレス クライアントの *[クライアントのトラブルシューティング（Client Troubleshooting）] ページ*



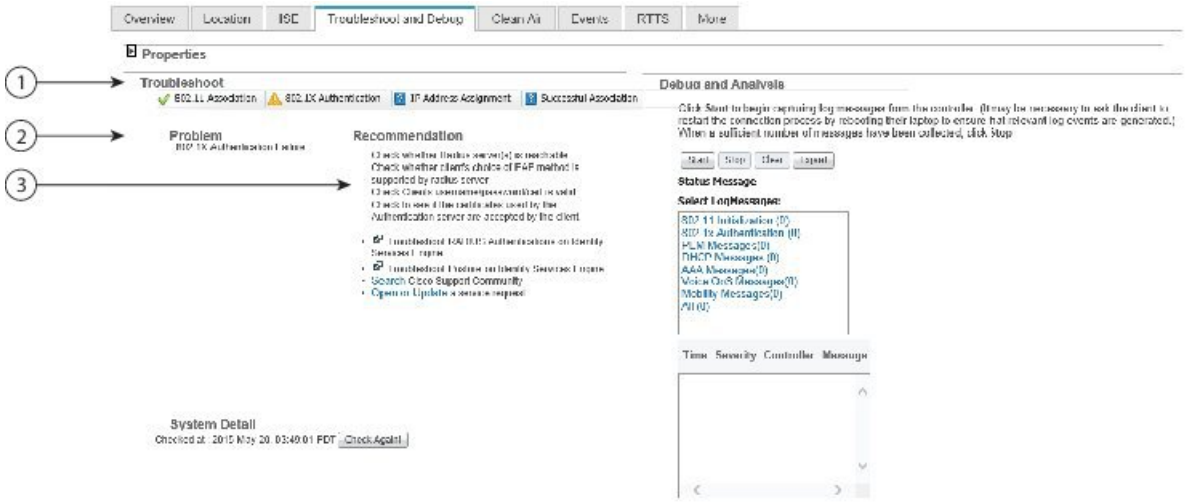
1	Properties
2	Troubleshoot
3	推奨事項

次の図に、異なるワイヤレス クライアントの[クライアントのトラブルシューティング（Client Troubleshooting）] ページの [トラブルシューティング（Troubleshoot）] セクションを示します

（簡単にするため、セクションの右矢印アイコンをクリックして[プロパティ（Properties）]セクションを折りたたんでいます）。このクライアントの接続には問題が発生しています。ご覧のように、接続プロセスの[802.1x Authentication]部分にアラートが付いており、このアラートの厳密な理由を特定するための手順リストが表示されています。

[Troubleshoot]セクションに表示される接続ステータスアイコンの数とタイプおよびヒントは、クライアントのタイプ、問題が発生した接続プロセスの段階、考えられる問題の原因によって異なります。詳細については、「関連項目」の「クライアント トラブルシューティング ツールによるヒントの仕組み」を参照してください。

図 *10*：失敗したワイヤレス クライアントの *[クライアントのトラブルシューティング（Client Troubleshooting）]* ページ



1	Troubleshoot
2	Problem
3	推奨事項

関連トピック

ネットワーク クライアント トラブルシューティング ツールの起動 （391 ページ）
クライアント トラブルシューティング ツールによるヒントの仕組み （393 ページ）

クライアント トラブルシューティング ツールによるヒントの仕組み

Prime Infrastructure は、各段階で接続と接続プロトコルを確立する際にクライアントが通過する段階に基づいて、[クライアントのトラブルシューティング（Client Troubleshooting）]ページに表示する接続領域の数とトラブルシューティングのアドバイスの種類を決定します。次の表は、各段階に含まれるこれらの段階とプロトコルをまとめたものです。

表 *38* : クライアント接続の段階とプロトコル

接続の段階	リンク接続	802.1X 認証	MAC 認証	Web 認証	IP 接続	認証
802.1X	×	×	–	–	×	×
MAC 認証	×	–	×	–	×	×
Web 認証	×	–	–	×	×	×

次の表に、接続の構築段階で検出された問題の種類ごとに表示されるトラブルシューティングのアドバイスを示します。

表 *39* : 各接続の段階と問題に関するトラブルシューティングのアドバイス

クライアントの状態	問題	推奨措置
リンク接続	ネットワークでクライアントが見つからない	• クライアントのケーブルがネットワークに接続されているかどうかを確認します。 • クライアントで適切なケーブルを使用してネットワークに接続しているかどうかを確認します。 • クライアントの接続先のポートが管理目的で無効になっていないことを確認します。 • クライアントの接続先のポートがエラーによって無効になっていないことを確認します。 • クライアントの接続先のポートで、速度およびデュプレックスが自動に設定されているかどうかを確認します。

	認証の進行中	• クライアントが長時間この状態の場合は、次の点を確認します。
		  • クライアント上のサプリカントが必要に応じて適切に設定されているかどうかを確認します。
		  • 認証方式に関連するタイマーを変更し、再試行します。
		  • そのクライアントで機能する認証方式が不明な場合は、フォールバック認証機能を使用します。
		  • 切断と再接続を試行します。

802.1X 認証	802.1X 認証の失敗	• スイッチから RADIUS サーバに到達可能かどうかを確認します。 • クライアントで選択されている EAP が RADIUS サーバでサポートされているかどうかを確認します。 • クライアントのユーザ名、パスワード、証明書が有効かどうかを確認します。 • RADIUS サーバで使用している証明書がクライアントで受け入れられていることを確認します。

クライアントの状態	問題	推奨措置
MAC 認証	MAC 認証の失敗	• スイッチから RADIUS サーバに到達可能かどうかを確認します。 • クライアントの MAC アドレスが RADIUS サーバにある既知クライアントのリストにあるかどうかを確認します。 • クライアントの MAC アドレスが除外されたクライアントのリストにないことを確認します。
Web 認証	Web/ゲスト インターフェイスを介してクライアントを認証できない	• ゲスト クレデンシャルが有効で、期限が切れていないかどうかを確認します。 • クライアントをログイン ページにリダイレクトできるかどうかを確認します。 • RADIUS サーバに到達可能かどうかを確認します。 • ポップアップがブロックされていないことを確認します。 • クライアント上の DNS 解決が機能しているかどうかを確認します。 • クライアントでいずれのプロキシ設定も使用していないことを確認します。 • クライアントで https://<virtual-ip>/login.html にアクセスできるかどうかを確認します。 • クライアントのブラウザで、コントローラの提供する自己署名証明書を受け入れるかどうかを確認します。
IP 接続	クライアントで DHCP インタラクションを完了できない	• DHCP サーバに到達可能かどうかを確認します。 • その WLAN で使用できるように DHCP サーバが設定されているかどうかを確認します。 • DHCP スコープをすべて使用したかどうかを確認します。 • 複数の DHCP サーバでオーバーラップするスコープが設定されているかどうかを確認します。 • ローカル DHCP サーバが存在するかどうかを確認します。DHCP ブリッジ モードが有効になっている（このサーバをセカンドに移動）場合は、DHCP サーバからアドレスを取得するようにクライアントが設定されています。 • クライアントに静的 IP が設定されており、クライアントで IP トラフィックを生成しているかどうかを確認します。
認証	認可の失敗	• 認可用に定義されている VLAN がスイッチで使用可能であることを確認します。 • デフォルト ポート ACL が ACL 許可用に設定されていることを確認します。
正常接続	なし	なし。これは、上記のすべての段階が正常に完了されたことを示します。

関連トピック

ネットワーク クライアント トラブルシューティング ツールを使用する方法（396 ページ）
ネットワーク クライアント トラブルシューティング ツールの起動（391 ページ）

ネットワーククライアントトラブルシューティングツールを使用する方法

分析するクライアントのクライアント トラブルシューティング ツールを起動します。関連項目の「ネットワーク クライアント トラブルシューティング ツールの起動」を参照してください。次の表では、[クライアントのトラブルシューティング（Client Troubleshooting）] ページのトラブルシューティング タブの使用方法について説明します。

タスク	操作
クライアント接続ログの分析	• [ログ分析（Log Analysis）] タブをクリックすると、クライアントに対して記録されたログ メッセージが表示されます。 • [開始（Start）] をクリックして、コントローラからクライアントに関するログ メッセージのキャプチャを開始します。 • ログ メッセージのキャプチャを停止するには、[Stop] をクリックします。 • すべてのログ メッセージをクリアするには、[Clear] をクリックします。ログ メッセージは 10 分間取得され、自動的に停止されます。[開始] をクリックして続行します。 • [ログメッセージの選択（Select Log Messages）] の下にあるいずれかのリンクをクリックすると、ログ メッセージが表示されます（括弧内の数字はメッセージ数を示します）。
クライアント イベント履歴とイベント ログの表示	• [イベント（Events）] タブをクリックすると、クライアントのイベント履歴が表示されます。 • イベント ログを表示するには、[Event Log] タブをクリックします。 • クライアントからのログ メッセージの取得を開始するには、[Start] をクリックします。 • 十分な数のメッセージが収集されたら、[Stop] をクリックします。 • クライアント トラブルシューティング イベント ログおよびメッセージング機能は、Management Service のバージョンが 2 以降の場合のみ CCX バージョン 6 クライアントに対して使用できます。

タスク	操作
クライアント ISE 認証履歴とアイデンティティ サービスの確認	• ISE 認証に関する情報を表示するには、[Identity Services Engine] タブをクリックします。 • 日付と時刻の範囲を入力して、履歴認証と認証情報を取得し、[送信（Submit）] をクリックします。照会の結果は、ページの [Authentication Records] 部分に表示されます。 • アイデンティティ サービス パラメータに関する情報を表示するには、[Identity Services Engine] タブをクリックします。このタブにアクセスするには、まずアイデンティティ サービス エンジン（ISE）を設定する必要があります。 • ISE が設定されていない場合、ISEを Prime Infrastructure に追加するためのリンクが提供されます。ISE は、REST API 経由で認証レコードを Prime Infrastructure に提供します。ネットワーク管理者は ISE から認証レコードを取得するための期間を選択できます。
クライアント CleanAir 環境の確認	• [CleanAir] タブをクリックすると、CleanAir 対応アクセス ポイントの電波品質パラメータとアクティブな干渉源に関する情報が表示されます。 • 電波品質の指標の詳細を参照するには、[CleanAir 詳細（CleanAir Details）] をクリックします。

タスク	操作
問題のあるクライアントでの診断テストの実行	• Cisco Compatible Extension バージョン 5 またはバージョン 6 のクライアントが利用可能な場合は、[テスト分析（Test Analysis）] タブをクリックします。 • 該当する診断テストのチェックボックスをオンにして、適切な入力情報を入力して、[開始（Start）] をクリックします。[Test Analysis] タブにより、クライアントでさまざまな診断テストを実行することができます。 [テスト分析（Test Analysis）] タブでは、次の診断テストを利用できます。 • [DHCP]：DHCP がコントローラとクライアント間で正常に動作していることを確認するために、完全な Discover/Offer/Request/ACK 交換を実行します。 • [IP 接続（IP Connectivity）]：クライアントが DHCP テストで取得したデフォルト ゲートウェイの ping テストを実行して、IP 接続がローカル サブネット上に存在することを確認します。 • [DNS Ping]：クライアントが DHCP テストで取得した DNS サーバの ping テストを実行して、IP 接続が DNS サーバに存在することを確認します。 • [DNS 解決（DNS Resolution）]：名前解決が正しく機能していることを確認するために、DNS クライアントが解決可能であることがわかっているネットワーク名の解決を試行します。 • [802.11 割り当て（802.11 Association）]：特定のアクセス ポイントとの完全な関連付けを指示して、クライアントが指定された WLAN に適切にアソシエートできることを確認します。 • [802.1X 認証（802.1X Authentication）]：特定のアクセス ポイントとの完全な関連付けおよび 802.1X 認証を指示し、クライアントが 802.1x 認証を正しく完了できることを確認します。 • [プロファイルのリダイレクト（Profile Redirect）]：診断システムは、いつでもクライアントに設定された WLAN プロファイルの 1 つをアクティブにし、そのプロファイルの下で操作を続けるように指示することができます。 • プロファイルの診断テストを実行する場合、クライアントは診断チャネル上になければなりません。このテストでは、プロファイル番号を入力として使用します。ワイルドカードリダイレクトを指定するには、0 を入力します。このリダイレクトによって、クライアントは診断チャネルとのアソシエーションを解除し、任意のプロファイルとアソシエートすることを求められます。また、有効なプロファイル ID を入力することもできます。テストが実行されているときにクライアントが診断チャネル上にあるため、プロファイル リストで返されるプロファイルは 1 つだけです。プロファイル リダイレクト テストでは、このプロファイル ID を使用する必要があります（ワイルドカードリダイレクトが必要でない場合）。

タスク	操作
問題のあるクライアントを ping テストした場合のテキスト メッセージ	Cisco Compatible Extension バージョン 5 またはバージョン 6 のクライアントの場合は、このクライアントのユーザにインスタント テキスト メッセージを送信するために使用できる [メッセージング（Messaging）] タブが表示されます。[メッセージ カテゴリ（Message Category）] ドロップダウンリストからメッセージを選択し、[送信（Send）] をクリックします。
リアルタイム トラブルシューティング（RTTS）の詳細の表示	リアルタイム トラブルシューティング（RTTS）の詳細を表示するには、[RTTS] タブをクリックします。 デバッグするモジュールとデバッグ レベルを選択します。 [実行（Run）] をクリックします。RTTS マネージャは、選択されたデバッグ モジュールとデバッグ レベルに基づいて、クライアントに接続されているコントローラの一連のコマンドを実行し、RTTS の詳細を表示します。 [フィルタ（Filter）] タブをクリックして、デバッグ時間、コントローラ名、コントローラ IP、重大度、デバッグ メッセージに基づいて RTTS の詳細をフィルタします。 [エクスポート（Export）] タブをクリックして、デバッグの詳細を csv ファイルとしてエクスポートします。 [他のコントローラを選択します（Choose different controllers）] オプションを使用して、選択したデバッグ モジュールとデバッグ レベルに基づいて他のコントローラをデバッグすることもできます。 RTTS マネージャは同時に 5 つの RTTS デバッグ セッションに対応し、各デバッグ セッションは 5 つのデバイスに制限されています。

タスク	操作
クライアントの音声メトリックの表示	

タスク	操作
	このクライアントのトラフィック ストリーム メトリックを表示するには、次の手順を実行します。 • **[モニタ（Monitor）] > [モニタリングツール（Monitoring Tools）] > [クライアントおよびユーザ（Clients and Users）]** を選択します。 • クライアントを選択します。 • [More] ドロップダウン リストから [Voice Metrics] を選択します。 • [Go] をクリックします。 次の情報が表示されます。 • [Time]：アクセス ポイントから統計情報が収集された時刻。 • QoS • [APイーサネットMAC無線（AP Ethernet MAC Radio）] • QoS • AP Ethernet MAC • Radio • [Time]：アクセス ポイントから統計情報が収集された時刻。 • QoS • [APイーサネットMA（AP Ethernet MA）] • QoS • [無線（Radio）] • AP Ethernet MAC • Radio • [% PLR (Downlink)]：90 秒の間隔中にダウンリンク（アクセス ポイントからクライアント）で失われたパケットの割合。 • [% PLR (Uplink)]：90 秒の間隔中にアップリンク（クライアントからアクセス ポイント）で失われたパケットの割合。 • [Avg Queuing Delay (ms) (Uplink)]：アップリンクの平均キューイング遅延（ミリ秒）。パケット キューイング遅延の平均は、音声キューを横断する音声パケットの平均遅延です。パケット キュー遅延は、パケットが送信のためにキューに入れられた時点から、パケットが正常に送信される時点まで測定されます。これには、必要に応じて再試行時間が含まれます。 • [%パケット（% Packets）] > [40 msキューイング遅延（ダウンリンク）（40 ms Queuing Delay (Downlink)）]：40 ms を超えるキューイング遅延パケットの割合。

タスク	操作
	• [% Packets 20ms-40ms Queuing Delay (Downlink)]：20 ms を超えるキューイング遅延パケットの割合。 • [Roaming Delay]：ローミング遅延（ミリ秒）。クライアントによって測定されるローミング遅延は、古いアクセスポイントから最後のパケットを受信した時点から、ローミングが正常に行われた後で新しいアクセス ポイントから最初のパケットを受信した時点まで測定されます。

関連トピック

ネットワーク クライアント トラブルシューティング ツールの起動 （391 ページ）
RTTS のデバッグ コマンド （402 ページ）

RTTS のデバッグ コマンド

次の表は、レガシー コントローラおよび統合アクセス コントローラの 5760/3850/3650 ワイヤレス LAN コントローラ（WLC）のデバッグ コマンド一覧です。

表 *40*：従来のコントローラおよび *NGWC* コントローラのデバッグ コマンドの一覧

コントローラ	デバッグするモジュール	デバッグ レベル	コマンド
レガシー	すべて		debug capwap info enable debug dot1x all enable debug mobility directory enable
	Dot1.x	Detail	debug dot1x all enable
		Error	debug dot1x events enable
		High Level	debug dot1x states enable

コントローラ	デバッグするモジュール	デバッグ レベル	コマンド
レガシー	Mobility	Detail	debug mobility packet enable debug mobility keepalive enable
		Error	debug mobility directory enable debug mobility config enable
		High Level	debug mobility handoff enable
	Wireless Client Join	Detail	debug client <macAddress> debug aaa all enable debug dot1x all enable
		Error	debug client <macAddress>
		High Level	debug client <macAddress>
NGWC	すべて		debug capwap ap error debug dot1x events debug capwap ios detail
Dot1.x	Detail	debug wcm-dot1x detail debug wcm-dot1x all debug dot1x all	
	Error	debug wcm-dot1x errors debug dot1x errors	
	High Level	debug wcm-dot1x trace debug wcm-dot1x event debug wcm-dot1x error debug client mac-address <macAddress>	
Mobility	Detail	debug mobility all	
	Error	debug mobility error	
	High Level	debug mobility handoff	

コントローラ	デバッグするモジュール	デバッグ レベル	コマンド
Wireless Client Join	Detail	debug wcdb error debug wcdb event debug wcdb db debug ip dhcp snooping events debug ip dhcp server events debug client mac <macAddress>	
	Error	debug client mac <macAddress>	
	High Level	debug client mac <macAddress>	

関連トピック

ネットワーク クライアント トラブルシューティング ツールの起動 （391 ページ）

ネットワーク クライアントの接続時の確認

この機能を使用すると、クライアントを追跡でき、このクライアントがネットワークに接続した際に通知を受けることができます。

手順の概要

1. **[モニタ（Monitor）] > [モニタリング ツール（Monitoring Tools）] > [クライアントおよびユーザ（Clients and Users）]** を選択します。
2. [Track Clients] をクリックします。現在追跡されているクライアントをリストした [Track Clients] ダイアログボックスが表示されます。
3. 1つのクライアントを追跡するには、[Add] をクリックして次のパラメータを入力します。
4. クライアント リストが長い場合、複数のクライアントを追跡するには、[Import] をクリックします。これにより、CSV ファイルからクライアント リストをインポートできます。MAC アドレスおよびユーザ名を入力します。

手順の詳細

ステップ 1 **[モニタ（Monitor）] > [モニタリング ツール（Monitoring Tools）] > [クライアントおよびユーザ（Clients and Users）]** を選択します。

ステップ 2 [Track Clients] をクリックします。現在追跡されているクライアントをリストした [Track Clients] ダイアログボックスが表示されます。

このテーブルは、最大2000行に対応しています。新規の行を追加またはインポートするには、古いエントリをいくつか削除する必要があります。

ステップ 3 1 つのクライアントを追跡するには、[Add] をクリックして次のパラメータを入力します。

- Client MAC address
- [Expiration]：[Never] を選択するか、日付を入力します。

ステップ 4 クライアント リストが長い場合、複数のクライアントを追跡するには、[Import] をクリックします。これにより、CSV ファイルからクライアント リストをインポートできます。MAC アドレスおよびユーザ名を入力します。

データ形式を規定した、サンプル CSV ファイルをダウンロードできます。

例：

```
# MACAddress, Expiration: Never/Date in MM/DD/YYYY format, Note
00:40:96:b6:02:cc, 10/07/2010, Sample Test Client
00:02:8a:a2:2e:60, Never, NA
```

最大2000のクライアントを追跡できます。この上限に達した場合、新たに追加するには、リストからクライアントをいくつか削除する必要があります。

関連トピック

ネットワークに接続しているクライアントに関する通知のセットアップ （405 ページ）
ネットワーク クライアント トラブルシューティング ツールの起動 （391 ページ）

ネットワークに接続しているクライアントに関する通知のセットアップ

手順の概要

1. **[モニタ（Monitor）] > [モニタリングツール（Monitoring Tools）] > [クライアントおよびユーザ（Clients and Users）]** を選択します。
2. [Track Clients] をクリックします。現在追跡されているクライアントをリストした [Track Clients] ダイアログボックスが表示されます。
3. 通知設定を指定する、追跡されるクライアントを選択します。
4. 通知設定オプションを以下から選択します。
5. メール アドレスを入力します。
6. [Save] をクリックします。

手順の詳細

ステップ 1 **[モニタ（Monitor）] > [モニタリングツール（Monitoring Tools）] > [クライアントおよびユーザ（Clients and Users）]** を選択します。

ステップ 2 [Track Clients] をクリックします。現在追跡されているクライアントをリストした [Track Clients] ダイアログボックスが表示されます。

ステップ 3 通知設定を指定する、追跡されるクライアントを選択します。

ステップ 4 通知設定オプションを以下から選択します。

- [消去された期限切れエントリ（Purged Expired Entries）]：追跡対象クライアントを Prime Infrastructure データベースに保持する期間を設定できます。クライアントは、次の期間で削除できます。
  - 1 週間後
  - 2 週間後
  - 1 ヵ月後
  - 2 ヵ月後
  - 6 ヵ月後
  - 無期限で保持
- [通知の頻度（Notification Frequency）]：Prime Infrastructure で追跡対象クライアントの通知をいつ送信するかを指定できます。
  - 最初の検出時
  - 検出ごと
- [Notification Method]：追跡対象クライアント イベントによりアラームを生成するか、電子メール メッセージを送信するかを指定できます。

ステップ 5 メール アドレスを入力します。

ステップ 6 [Save] をクリックします。

関連トピック

ネットワーク クライアントの接続時の確認 （404 ページ）
不明なネットワーク ユーザの識別 （406 ページ）

不明なネットワーク ユーザの識別

802.1x を介して認証されないユーザやデバイス（プリンタなど）もあります。その場合は、ネットワーク管理者がデバイスにユーザ名を割り当てできます。

クライアントデバイスが Web 認証を介してネットワークに認証される場合、Prime Infrastructure では、クライアントのユーザ名情報を取得できないことがあります（有線クライアントのみ該当）。

クライアントは、有線スイッチとの NMSP 接続が失われた時点で、[Unknown（不明）] とマークされます。クライアント ステータス（有線クライアントのみ該当）は、接続、切断、または不明で示されます。

- [Connected clients]：有線スイッチに接続しているアクティブなクライアント。
- [Disconnected clients]：有線スイッチから接続が解除されたクライアント。
- [Unknown clients]：有線スイッチとの NMSP 接続が失われた時点で、不明としてマークされたクライアント。

[Unknown users（不明ユーザ）] リストにユーザを追加するには、次の手順を実行します。

手順の概要

1. **[モニタ（Monitor）] > [モニタリングツール（Monitoring Tools）] > [クライアントおよびユーザ（Clients and Users）]** を選択します。
2. [Identify Unknown Users] をクリックします。
3. [Add] をクリックして、ユーザを追加します。
4. MAC アドレスとユーザ名を入力し、[Add] をクリックします。
5. ステップ 3 からステップ 4 を繰り返して、各クライアントの MAC アドレスおよび対応するユーザ名を入力します。
6. [Save] をクリックします。

手順の詳細

ステップ 1 **[モニタ（Monitor）] > [モニタリングツール（Monitoring Tools）] > [クライアントおよびユーザ（Clients and Users）]** を選択します。

ステップ 2 [Identify Unknown Users] をクリックします。

ステップ 3 [Add] をクリックして、ユーザを追加します。

ステップ 4 MAC アドレスとユーザ名を入力し、[Add] をクリックします。

ユーザ名と MAC アドレスが追加されると、Prime Infrastructure では、MAC アドレスの照合によるクライアントの検索に、このデータが使用されます。

ステップ 5 ステップ 3 からステップ 4 を繰り返して、各クライアントの MAC アドレスおよび対応するユーザ名を入力します。

ステップ 6 [Save] をクリックします。

（注）
- ユーザ名は、クライアントのアソシエーションが新たに発生した場合にのみ更新されます。
- このテーブルは、最大 10,000 行に対応しています。新規の行を追加またはインポートするには、古いエントリをいくつか削除する必要があります。

不明ネットワーク ユーザのリストのインポート

不明ユーザのリストを表示するには、次の手順を実行します。

手順の概要

1. **[モニタ（Monitor）] > [モニタリングツール（Monitoring Tools）] > [クライアントおよびユーザ（Clients and Users）]** を選択します。
2. [不明ユーザの特定（Identify Unknown Users）] をクリックします。
3. [ファイルの選択（Choose File）] をクリックしてファイル インポート ウィザードを開きます。

4. 必要な *.csv* ファイルまで移動して [選択（Choose）] をクリックします。
5. [インポート（Import）] をクリックしてリストをインポートします。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**[モニタ（Monitor）] > [モニタリングツール（Monitoring Tools）] > [クライアントおよびユーザ（Clients and Users）]** を選択します。	
ステップ 2	[不明ユーザの特定（Identify Unknown Users）] をクリックします。	
ステップ 3	[ファイルの選択（Choose File）] をクリックしてファイル インポート ウィザードを開きます。	
ステップ 4	必要な *.csv* ファイルまで移動して [選択（Choose）] をクリックします。	サンプル CSV ファイルは、次のデータ形式でダウンロードすることができます。 **例**： # MacAddress, Username 00:11:22:33:44:55, username
ステップ 5	[インポート（Import）] をクリックしてリストをインポートします。	

不明ネットワーク ユーザのリストのエクスポート

不明ユーザのリストを表示するには、次の手順を実行します。

手順の概要

1. **[モニタ（Monitor）] > [モニタリングツール（Monitoring Tools）] > [クライアントおよびユーザ（Clients and Users）]** を選択します。
2. [不明ユーザの特定（Identify Unknown Users）] をクリックし、[エクスポート（Export）] をクリックします。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**[モニタ（Monitor）] > [モニタリングツール（Monitoring Tools）] > [クライアントおよびユーザ（Clients and Users）]** を選択します。	
ステップ 2	[不明ユーザの特定（Identify Unknown Users）] をクリックし、[エクスポート（Export）] をクリックします。	この操作で *.csv* ファイルがシステムにエクスポートされます。

関連トピック

[コントローラクライアントとユーザ（Controller Client and Users）] ページのカスタマイズ（409 ページ）
ネットワーク クライアントの接続時の確認 （404 ページ）

[コントローラクライアントとユーザ（Controller Client and Users）] ページのカスタマイズ

[クライアント（Clients）] テーブルの列を追加、削除、または並べ替えることができます。

手順の概要

1. **[モニタ（Monitor）] > [モニタリングツール（Monitoring Tools）] > [クライアントおよびユーザ（Clients and Users）]** を選択します。
2. [設定（Settings）] アイコン > [列（Columns）] の順にクリックします。
3. 表示する列を選択します。
4. デフォルト表示に戻すには、[Reset] をクリックします。
5. [Close] をクリックすると、変更が確定されます。

手順の詳細

ステップ 1 **[モニタ（Monitor）] > [モニタリングツール（Monitoring Tools）] > [クライアントおよびユーザ（Clients and Users）]** を選択します。
ステップ 2 [設定（Settings）] アイコン > [列（Columns）] の順にクリックします。
ステップ 3 表示する列を選択します。
ステップ 4 デフォルト表示に戻すには、[Reset] をクリックします。
ステップ 5 [Close] をクリックすると、変更が確定されます。

関連トピック

ネットワーク クライアントの接続時の確認 （404 ページ）
診断チャネルでの自動コントローラ クライアント トラブルシューティングのセットアップ （410 ページ）

診断チャネルでの自動コントローラクライアントトラブルシューティングのセットアップ

[設定（Settings）] > [クライアント（Client）] ページでは、診断チャネルでの自動クライアント トラブルシューティングを有効にできます。この機能は、Cisco Compatible Extension クライアントのバージョン 5 でのみ使用できます。

自動クライアント トラブルシューティングを有効にするには、次の手順を実行します。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** を選択します。

ステップ 2 左側のサイドバーのメニューから、[Client] を選択します。

ステップ 3 [Automatically troubleshoot client on diagnostic channel] チェックボックスをオンにします。

このチェックボックスがオンの場合、Prime Infrastructure は診断アソシエーション トラップを処理します。このチェックボックスがオフの場合、Prime Infrastructure はトラップを発生させますが、自動トラブルシューティングは開始されません。

ステップ 4 [保存（Save）] をクリックします。

関連トピック

ワイヤレス ネットワーク クライアントの無線測定値の取得 （410 ページ）
[コントローラクライアントとユーザ（Controller Client and Users）] ページのカスタマイズ（409 ページ）

ワイヤレスネットワーククライアントの無線測定値の取得

クライアント ページで、無線測定を取得できるのは、クライアントが Cisco Compatible Extensions v2（以上）であり、Associated 状態（有効な IP アドレスを持つ）である場合だけです。測定が問い合わせられたときクライアントがビジー状態の場合、測定を引き受けるかどうかが検討されます。クライアントが測定の実行を拒否する場合、クライアントからのデータは表示されません。

この機能は、Foundation サービスのバージョンが 1 以降の場合のみ、CCX バージョン 6 クライアントで使用できます。

無線測定を受信するには、次の手順を実行します。

ステップ 1 **[モニタ（Monitor）] > [モニタリングツール（Monitoring Tools）] > [クライアントおよびユーザ（Clients and Users）]** を選択します。

ステップ 2 クライアントの横にある円をクリックします。

Prime Infrastructure 検索機能を使用して特定のクライアントの検索を実行することもできます。

ステップ 3 [Test] ドロップダウン リストから [Radio Measurement] を選択します。

[Radio Measurement] オプションは、クライアントが Cisco Compatible Extensions v2（以上）であり、Associated 状態（有効な IP アドレスを持つ）である場合に限り表示されます。

ステップ 4 チェックボックスをオンにして、ビーコンの測定、フレームの測定、チャネルの負荷、またはノイズ ヒストグラムを指定するかどうかを示します。

[Initiate] をクリックします。測定が異なると、生成される結果も異なります。「関連項目」の「ネットワーク クライアント無線測定結果の表示」を参照してください。

測定には、約 5 ミリ秒かかります。Prime Infrastructure からのメッセージに進捗状況が示されます。クライアントが測定を実行しないと選択した場合は、そのことが通知されます。

関連トピック

ネットワーク クライアント無線測定結果の表示 （411 ページ）

ネットワーク クライアント無線測定結果の表示

要求した測定のタイプに応じて、次のような情報が表示されます。

- Beacon Response
- フレーム測定
- チャネル負荷
- ノイズ ヒストグラム

測定パラメータの詳細については、モニタのフィールド参照のページを参照してください。

関連トピック

ワイヤレス ネットワーク クライアントの無線測定値の取得 （410 ページ）

ネットワーク クライアント V5 の統計情報を表示するためのテストの実行

[統計要求（Statistics request）] ページにアクセスするには、次の手順を実行します。

手順の概要

1. **[モニタ（Monitor）] > [モニタリングツール（Monitoring Tools）] > [クライアントおよびユーザ（Clients and Users）]** を選択します。
2. クライアントを選択します。

3. **[テスト（Test）]** ドロップダウン リストから、**[CCX 統計情報（CCX statistics）]** を選択します。
4. [Go] をクリックします。
5. 必要な統計のタイプ（[Dot11 Measurement] または [Security Measurement]）を選択します。
6. [Initiate] をクリックして測定を開始します。
7. 要求した V5 統計のタイプに応じて、次のカウンタが結果ページに表示されます。

手順の詳細

ステップ 1 **[モニタ（Monitor）]** > **[モニタリングツール（Monitoring Tools）]** > **[クライアントおよびユーザ（Clients and Users）]** を選択します。

ステップ 2 クライアントを選択します。

ステップ 3 **[テスト（Test）]** ドロップダウン リストから、**[CCX 統計情報（CCX statistics）]** を選択します。

このメニューは、CCX v5 以降のクライアントだけに表示されます。

ステップ 4 [Go] をクリックします。

ステップ 5 必要な統計のタイプ（[Dot11 Measurement] または [Security Measurement]）を選択します。

ステップ 6 [Initiate] をクリックして測定を開始します。

測定期間は 5 秒間です。

ステップ 7 要求した V5 統計のタイプに応じて、次のカウンタが結果ページに表示されます。

- Dot11 測定
  - 送信フラグメント数
  - マルチキャスト送信フレーム数
  - 失敗数
  - 再試行数
  - 複数再試行数
  - フレーム重複数
  - Rts 成功数
  - Rts 失敗数
  - Ack 失敗数
  - 受信フラグメント数
  - マルチキャスト受信フレーム数
  - [FCS Error Count]：このカウンタは、受信した MPDU で FCS エラーが検出されたときに増分されます。
  - 送信フレーム数
- セキュリティ
  - ペアワイズ暗号
  - Tkip ICV エラー数

- Tkip ローカル MIC 失敗数
- Tkip 再試行数
- Ccmp 再試行数
- Ccmp 復号化エラー数
- 管理統計 Tkip ICV エラー数
- 管理統計 Tkip ローカル MIC 失敗数
- 管理統計 Tkip 再試行数
- 管理統計 Ccmp 再試行数
- 管理統計 Ccmp 復号化エラー数
- 管理統計 Tkip MHDR エラー数
- 管理統計 Ccmp MHDR エラー数
- 管理統計ブロードキャスト アソシエーション解除数
- 管理統計ブロードキャスト認証解除数
- [管理統計ブロードキャスト アクション フレーム数（Mgmt Stats Broadcast Action Frame Count）]

関連トピック

ネットワーク クライアントの動作パラメータを表示するためのテストの実行 （413 ページ）

ネットワーククライアントの動作パラメータを表示するためのテストの実行

特定のクライアント動作パラメータを表示するには、次の手順に従います。

手順の概要

1. **[モニタ（Monitor）] > [モニタリングツール（Monitoring Tools）] > [クライアントおよびユーザ（Clients and Users）]** を選択します。
2. クライアントを選択します。
3. [Test] ドロップダウン リストから [Operational Parameters] を選択します。

手順の詳細

ステップ 1 **[モニタ（Monitor）] > [モニタリングツール（Monitoring Tools）] > [クライアントおよびユーザ（Clients and Users）]** を選択します。

ステップ 2 クライアントを選択します。

ステップ 3 [Test] ドロップダウン リストから [Operational Parameters] を選択します。

次の情報が表示されます。

動作パラメータ：

- [Device Name]：デバイスのユーザ定義の名前。
- [Client Type]：クライアントの種類は次のいずれかになります。
  - laptop(0)
  - pc(1)
  - pda(2)
  - dot11mobilephone(3)
  - dualmodephone(4)
  - wgb(5)
  - scanner(6)
  - tabletpc(7)
  - printer(8)
  - projector(9)
  - videoconfsystem(10)
  - camera(11)
  - gamingsystem(12)
  - dot11deskphone(13)
  - cashregister(14)
  - radiotag(15)
  - rfidsensor(16)
  - server(17)
  - [SSID]：クライアントで使用している SSID。
  - [IP Address Mode]：静的設定、DHCP などの IP アドレス モード。
  - [IPv4 Address]：クライアントに割り当てられた IPv4 アドレス。
  - [IPv4 Subnet Address]：クライアントに割り当てられた IPv4 サブネット アドレス。
  - [IPv6 Address]：クライアントに割り当てられた IPv6 アドレス。
  - [IPv6 Subnet Address]：クライアントに割り当てられた IPv6 サブネット アドレス。
  - [Default Gateway]：このクライアントで選択されているデフォルト ゲートウェイ。
  - [Operating System]：ワイヤレス ネットワーク アダプタを使用しているオペレーティング システムを識別します。
  - [Operating System Version]：ワイヤレス ネットワーク アダプタを使用しているオペレーティング システムのバージョンを識別します。
  - [WNA Firmware Version]：クライアントに現在インストールされているファームウェアのバージョン。
  - ドライバのバージョン
  - [Enterprise Phone Number]：クライアントの企業電話番号。
  - [Cell Phone Number]：クライアントの携帯電話番号。
  - [Power Save Mode]：省電力モードとして awake、normal、または maxPower のいずれかが表示されます。
  - システム名
  - ローカリゼーション

無線情報：

- [Radio Type]：次の無線の種類が使用可能です。
  - unused(0)
  - fhss(1)
  - dsss(2)
  - irbaseband(3)
  - ofdm(4)
  - hrdss(5)
  - erp(6)
- [Radio Channel]：使用中の無線チャネル。

DNS/WNS 情報：

- [DNS Servers]：DNS サーバの IP アドレス。
- [WNS Servers]：WNS サーバの IP アドレス。

セキュリティ情報：

- [Credential Type]：クライアントに設定されているクレデンシャルの方法を示します。
- [Authentication Method]：クライアントで使用する認証方式。
- [EAP Method]：クライアントで使用する拡張認証プロトコル（EAP）の方式。
- [Encryption Method]：クライアントで使用する暗号化方式。
- [Key Management Method]：クライアントで使用するキー管理方式。

関連トピック

ネットワーク クライアント V5 の統計情報を表示するためのテストの実行 （411 ページ）
ネットワーク クライアントの詳細の表示 （415 ページ）

ネットワーク クライアントの詳細の表示

特定のクライアント プロファイル情報を表示するには、次の手順を実行します。

手順の概要

1. **[モニタ（Monitor）] > [モニタリングツール（Monitoring Tools）] > [クライアントおよびユーザ（Clients and Users）]** を選択します。
2. クライアントを選択します。
3. [More] ドロップダウン リストから [Profiles] を選択します。

手順の詳細

ステップ 1 **[モニタ（Monitor）] > [モニタリングツール（Monitoring Tools）] > [クライアントおよびユーザ（Clients and Users）]** を選択します。

ステップ 2 クライアントを選択します。

ステップ 3 [More] ドロップダウン リストから [Profiles] を選択します。

次の情報が表示されます。

- [Profile Name]：ハイパーリンクになったプロファイル名のリスト。ハイパーリンクをクリックすると、プロファイルの詳細が表示されます。
- [SSID]：このクライアントをアソシエートする WLAN の SSID。

関連トピック

ネットワーク クライアントの無効化 （416 ページ）

ネットワーク クライアントの無効化

現在のクライアントを無効にするには、次の手順を実行します。

手順の概要

1. [Monitor] > [Monitoring Tools] > [Clients and Users] を選択します。
2. クライアントを選択します。
3. [Disable] をクリックします。[Disable Client] ページが表示されます。
4. [Description] テキスト ボックスに説明を入力します。
5. [OK] をクリックします。

手順の詳細

ステップ 1 [Monitor] > [Monitoring Tools] > [Clients and Users] を選択します。

ステップ 2 クライアントを選択します。

ステップ 3 [Disable] をクリックします。[Disable Client] ページが表示されます。

ステップ 4 [Description] テキスト ボックスに説明を入力します。

ステップ 5 [OK] をクリックします。

無効にしたクライアントは、コントローラ上のいずれのネットワークおよび SSID にも接続できません。**[設定（Configuration）]** > **[ネットワーク（Network）]** > **[ネットワーク デバイス（Network Devices）]** > **[ワイヤレス コントローラ（Wireless Controller）]** >[デバイス名（*Device Name*）]>[セキュリティ（Security）] > [手動で無効化されたクライアント（Manually Disabled Clients）] を選択し、クライアント エントリを削除します。

関連トピック

ネットワーク クライアントの詳細の表示 （415 ページ）
Prime Infrastructure からのネットワーク クライアントの削除 （417 ページ）

Prime Infrastructure からのネットワーク クライアントの削除

現在のクライアントを削除するには、次の手順を実行します。

手順の概要

1. [Monitor] > [Monitoring Tools] > [Clients and Users] を選択します。
2. クライアントを選択します。
3. [Remove] を選択します。
4. [Remove] をクリックして、削除を実行します。

手順の詳細

ステップ 1 [Monitor] > [Monitoring Tools] > [Clients and Users] を選択します。
ステップ 2 クライアントを選択します。
ステップ 3 [Remove] を選択します。
ステップ 4 [Remove] をクリックして、削除を実行します。

ワイヤレスマップでのネットワーククライアントの検索

クライアントの位置を示す高解像度マップを表示するには、次の手順を実行します。

手順の概要

1. **[モニタ（Monitor）] > [モニタリングツール（Monitoring Tools）] > [クライアントおよびユーザ（Clients and Users）]** を選択します。
2. [クライアントユーザ名（Client Username）] 列からクライアントを選択します。
3. [その他（More）] ドロップダウン リストから、次の操作を行います。
4. [移動（Go）] をクリックします。

手順の詳細

ステップ 1 **[モニタ（Monitor）] > [モニタリングツール（Monitoring Tools）] > [クライアントおよびユーザ（Clients and Users）]** を選択します。
ステップ 2 [クライアントユーザ名（Client Username）] 列からクライアントを選択します。
ステップ 3 [その他（More）] ドロップダウン リストから、次の操作を行います。

- クライアントの最近の位置を表示するには、[最近のマップ（Recent Map）] を選択します。
- クライアントの現在の位置の高解像度マップを表示するには、[現在のマップ（Present Map）] を選択します。
- クライアントの最新のクライアント セッション レポートの結果を表示するには、[クライアント セッション レポート（Client Sessions Report）] を選択します。

（注） Prime Infrastructure 3.3 以降では、クライアントの最近および現在の位置は、サイトマップに表示されません。

ステップ 4 [移動（Go）] をクリックします。

関連トピック

レポートを使用したネットワーク クライアント ローミングの表示 （418 ページ）

レポートを使用したネットワーククライアントローミングの表示

このクライアントの最新のローミング レポートを表示するには、次の手順を実行します。

手順の概要

1. **[モニタ（Monitor）] > [モニタリングツール（Monitoring Tools）] > [クライアントおよびユーザ（Clients and Users）]** を選択します。
2. クライアントを選択します。
3. [More] ドロップダウン リストから [Roam Reason] を選択します。
4. [Go] をクリックします。

手順の詳細

ステップ 1 **[モニタ（Monitor）] > [モニタリングツール（Monitoring Tools）] > [クライアントおよびユーザ（Clients and Users）]** を選択します。

ステップ 2 クライアントを選択します。

ステップ 3 [More] ドロップダウン リストから [Roam Reason] を選択します。

ステップ 4 [Go] をクリックします。

このページには、クライアントの最新のローミング レポートが表示されます。各ローミング レポートには、次の情報が含まれます。

- 新規 AP MAC アドレス
- 旧（前）AP MAC アドレス
- 前の AP SSID

- 前の AP チャネル
- 遷移時間：クライアントを新しいアクセス ポイントにアソシエートするためにかかった時間。
- ローミング理由：クライアントのローミング理由。

関連トピック

ネットワーク クライアントを聞くことができるアクセス ポイントの特定 （419 ページ）

ネットワーククライアントを聞くことができるアクセス ポイントの特定

信号強度や SNR など、クライアントと通信できるアクセス ポイントの詳細を表示するには、次の手順を実行します。

手順の概要

1. **[モニタ（Monitor）] > [モニタリング ツール（Monitoring Tools）] > [クライアントおよびユーザ（Clients and Users）]** を選択します。
2. クライアントを選択します。
3. [More] ドロップダウン リストから [Detecting APs] を選択します。
4. [Go] をクリックします。

手順の詳細

ステップ 1 **[モニタ（Monitor）] > [モニタリング ツール（Monitoring Tools）] > [クライアントおよびユーザ（Clients and Users）]** を選択します。

ステップ 2 クライアントを選択します。

ステップ 3 [More] ドロップダウン リストから [Detecting APs] を選択します。

ステップ 4 [Go] をクリックします。

関連トピック

ネットワーク クライアントのロケーション履歴の表示 （419 ページ）

ネットワーク クライアントのロケーション履歴の表示

RF フィンガープリントに基づくクライアント ロケーションの履歴を表示するには、次の手順を実行します。

手順の概要

1. **[モニタ（Monitor）] > [モニタリングツール（Monitoring Tools）] > [クライアントおよびユーザ（Clients and Users）]** を選択します。
2. クライアントを選択します。
3. [More] ドロップダウン リストから [Location History] を選択します。
4. [Go] をクリックします。

手順の詳細

ステップ 1 **[モニタ（Monitor）] > [モニタリングツール（Monitoring Tools）] > [クライアントおよびユーザ（Clients and Users）]** を選択します。

ステップ 2 クライアントを選択します。

ステップ 3 [More] ドロップダウン リストから [Location History] を選択します。

ステップ 4 [Go] をクリックします。

関連トピック

ネットワーク クライアント トラブルシューティング ツールを使用する方法（396 ページ）

第 17 章

PfRv3 モニタリングを使用したネットワーク パフォーマンスのモニタ

- PfRv3 とは （421 ページ）
- ユーザ グループの PfR モニタリングへのアクセス （422 ページ）
- [PfRモニタリング（PfR Monitoring）] ページの使用 （422 ページ）
- PfRv3 を使用したサイト間イベントに関する詳細の表示 （427 ページ）
- PfRv3 を使用した WAN インターフェイスの使用状況の比較 （430 ページ）

PfRv3 とは

Performance Routing Version 3（PfRv3）は、シスコが提供するインテリジェント パス制御機能向けの第三世代の拡張機能です。PfR はネットワーク パフォーマンスをモニタし、到達可能性、遅延、ジッター、パケット損失などの詳細な条件に基づいて、各アプリケーションに最適なパスを選択します。PfRは高度なロードバランシング技術を使用して、トラフィックを均等に分散し、リンク使用レベルを同等に維持します。

PfRv3 は IWAN イニシアティブのインテリジェント パス制御機能であり、インターネット トランスポートにビジネスクラスの WAN を提供します。PfR を使用すると、顧客は WAN パフォーマンスの変動から重要なアプリケーションを保護すると同時に、すべての WAN パス全体にトラフィックをインテリジェントに負荷分散できます。

PfR は 2 つの主要な Cisco IOS コンポーネントから構成されています。

- マスター コントローラ：マスター コントローラは、境界ルータ システムを通過するさまざまなトラフィック クラスに対して、ポリシーを定義して適用するポリシー決定ポイントです。マスター コントローラは、ネットワークのトラフィック クラスを学習して制御するように設定できます。
- 境界ルータ（BR）：境界ルータはデータ転送パス内にあります。境界ルータは、Performance Monitor のキャッシュとスマート プローブの結果からデータを収集します。境界ルータは、マスター コントローラの指示どおりにユーザ トラフィックを管理するので、パケット転送パスに影響を及ぼします。

関連トピック

[PfRモニタリング（PfR Monitoring）] ページの使用 （422 ページ）
PfRv3 を使用したサイト間イベントに関する詳細の表示 （427 ページ）
PfRv3 を使用した WAN インターフェイスの使用状況の比較 （430 ページ）

ユーザ グループの PfR モニタリングへのアクセス

デフォルトでは、PfR モニタリングは、Prime Infrastructure の root ユーザ グループに対して有効になります。

他のユーザ グループから PfR モニタリング ランディング ページにアクセスするには、次の手順を実行します。

ステップ 1 [管理（Administration）] > [ユーザ、ロール、および AAA（Users, Roles, & AAA）] > [ユーザ（User）] を選択します。

ステップ 2 左側のペインで [Users] をクリックし、[Select a command] > [Add User] を選択して [Go] をクリックします。

ステップ 3 新しいユーザのユーザ名とパスワードを入力してから、パスワードを確認します。

ステップ 4 タスク リストに [PfR Monitoring Access] エントリがある各ユーザ グループの横のチェックボックスをオンにして、新規ユーザにユーザ グループを割り当てます。

ステップ 5 [保存（Save）] をクリックします。

ステップ 6 新しいユーザ名とパスワードを使用して、Prime Infrastructure にログインします。

ステップ 7 [サービス（Services）] > [アプリケーションの可視性と制御（Application Visibility & Control）] > [PfR モニタリング（PfR Monitoring）] を選択します。

ステップ 8 [PfR モニタリング（PfR Monitoring）] が表示されない場合は、[管理（Administration）] > [ユーザ、ロール、および AAA（User, Roles & AAA）] > [ユーザ グループ（User Groups）] に移動します。

ステップ 9 割り当てられているユーザ グループに対応する [タスク リスト（Task List）] をクリックして、[PfR モニタリング（PfR Monitoring）] が使用可能かどうかを確認します。

ステップ 10 [PfR モニタリング（PfR Monitoring）] がタスク リストにない場合は、[タスク権限（Task Permissions）] タブをクリックし、[ネットワーク モニタリング（Network Monitoring）] リストの [PfR モニタリング アクセス（PfR Monitoring Access）] チェックボックスをオンにします。

ステップ 11 [Submit] をクリックします。`

[PfRモニタリング（PfR Monitoring）] ページの使用

[サービス（Services）] > [アプリケーションの可視性と制御（Application Visibility & Control）] > [PfRモニタリング（PfR Monitoring）] を選択すると、PfR モニタリング ページを起動できます。PfR モニタリング ページには、[サイト間PfRイベント（Site to Site PfR Events）] テーブルを含む [PfRイベント（PfR Events）] タブ、フィルタ パネル、[メトリック（Metrics）] パネル

（[サービスプロバイダー（Service Provider）] ビューと [DiffServコードポイント（DSCP）（Differentiated Services Code Point (DSCP)）] ビュー チャート）、タイム スライダー、[WANリンクの比較（Compare WAN Links）] タブおよび [SPのヘルストレンド（SP Health Trend）] があります。

[サイト間PfRイベント（Site to Site PfR Events）] テーブル

[サイト間PfRイベント（Site to Site PfR Events）] テーブルには、サイト(ハブ、ブランチ、トランジット サイト)と次のイベントが表示されます。

（注） [インベントリ（Inventory）] > [グループ管理（Group Management）] > [ネットワークデバイス グループ（Network Device Groups）] を使用してロケーション グループを作成します。サイトの横に表示されるハブ、ブランチ、トランジットのアイコンはロケーション グループの説明に応じて読み込まれるため、ロケーション グループの適切な説明（ハブ、ブランチ、トランジットなど）を入力します。

- しきい値超過アラート（TCA）イベントとルート変更（RC）イベント：PfRによって特定され修正されるネットワーク パフォーマンスの低下を表し、青色の点で示されます。
- 緩和できないイベント（IME）：PfR によって修正できなかったメトリック違反を表し、赤色の点で示されます。

（注） デフォルトでは、直近 72 時間以内に発生した PfR イベントが表示されます。

サイトの組み合わせは、次の方法でソートされます。

- 最大数の IME を持つサイトの組み合わせは、テーブルの一番上の行に表示されます。
- 2 つのサイトの IME が同数の場合は、イベント（IME、TCA、RC など）数が最も多いサイトがテーブルの一番上に配置され、赤色で表示されます。

[PfRフィルタ（PfR Filter）] パネル

[PfRフィルタ（PfR Filter）] パネルでは、さまざまなフィルタに基づいてイベントをフィルタリングできます。[メトリック（Metrics）] パネルと [サイト間 PfR イベント（Site to Site PfR Events）] テーブルには、選択したフィルタ オプションに基づいて詳細が表示されます。選択したフィルタ オプションはフィルタ パネルの上部で確認できます。フィルタ オプションの説明については、『*Cisco Prime Infrastructure Reference Guide*』を参照してください。

[SPのヘルストレンド（SP Health Trend）] タブ

[SPのヘルストレンド（SP Health Trend）] タブには、SP キャリング未補正トラフィック、SP 到達不能トレンドおよび SP の全体的なヘルス トレンドなどのダッシュレットが時間に対して描画されます。チャート ビューとテーブル ビューを切り替えることができます。

エクスポートアイコンをクリックすると、pdfまたはCSV形式でダッシュレットをエクスポートできます。ダッシュレットの [概要（Summary）] をクリックすると、すべてのサービス プ

ロバイダーの障害トラフィック、リンク ダウンタイム、またはリンク状態の全体的な平均が表形式で表示されます。

時間フィルタを使用してダッシュレットをフィルタリングする場合は、60 日を超える時間範囲を選択しないことをお勧めします。[SPのヘルストレンド（SP Health Trend）] タブのパフォーマンスが低下するためです。さらに、**[サービス プロバイダー フィルター（Service Provider Filter）]** フィールドで目的のサービス プロバイダを選択し、**[送信（Submit）]** ボタンをクリックして、サービス プロバイダに基づいてデータをフィルタ処理できます。

PfR モニタリング ページでは、次のタスクが実行できます。

表 *41 : [PfRモニタリング（PfR Monitoring）] ページのタスク*

タスク	説明
ページの更新	PfR ランディング ページを手動で更新するには、PfR モニタリング ページの右上隅にある [更新（Refresh）] アイコン をクリックします。
設定の変更	PfR モニタリング ページの右上隅にある設定アイコンをクリックします。[PfR 設定（PfR Settings）] ポップアップ ウィンドウが表示されます。 次の項目に関して設定を選択します。 • [グローバル（Global）] : VRF とその他の共通設定を選択します。情報アイコンの上にマウスを置くと、各オプションについてのツール ヒントが表示されます。 • [SPのヘルストレンド（SP Health Trend）] タブ：[SPのヘルストレンド（SP Health Trend）] タブで、行ごとに表示されるチャートの数を選択します。 • **[PfRイベント（PfR Events）]** タブ：自動更新、イベント テーブル、ライブ トポロジ ポップアップ、サービス プロバイダー チャート、DSCP チャートの選択を行います。 • [サイト間（Site to Site）] タブ：[チャートの上位N設定（Top N settings for Charts）] に必要な値を選択します。 • **[WANリンクの比較（Compare WAN Links）]** タブ：[チャートの上位 N 設定（Top N settings for Charts）] に必要な値を選択します。 • [FAQ] セクション：トラブルシューティングの詳細情報が提供されます。 [保存して閉じる（Save and Close）] をクリックして、設定を保存します。
インライン ヘルプの表示	各ページのインライン ヘルプを表示するには、PfR モニタリング ページの右上隅にある情報アイコンをクリックします。

タスク	説明
ライブ トポロジの表示	別の DSCP に対応するトラフィックを示すライブ トポロジ ポップアップを表示するには、サイト ペアの横にあるトポロジ アイコン をクリックします。[サイト間（site to site）] タブに移動するには [サイト間の詳細（Site to Site details）] をクリックします。詳細については、PfRv3 を使用したサイト間イベントに関する詳細の表示 （427 ページ） を参照してください。 [VRF] ドロップダウン リストからトポロジを表示する VRF を選択します。リストされた VRF は選択したサイト ペアに対応します。 その時間に描画されたライブ トポロジを表示するには、必要な時間オプションをクリックします。 • トポロジを 5 分ごとに更新するには、[自動更新（Auto refresh）] チェックボックスをオンにします。 • カスタム時間を選択することもできます。時間の差が 5 分以上になるように時間範囲を選択してください。このオプションでは、自動更新は無効になります。 • 最後の 1 分間に対応するトポロジを表示するには、[ライブ（Live）] をクリックします。[ライブ（Live）] オプションを選択すると、[サイト間の詳細（Site to Site details）] ボタンは無効になり、[自動更新（Auto Refresh）] を選択すると 30 秒ごとにトポロジが自動的に更新されます。
境界ルータまたはリンク メトリックの表示	オプションのリストを表示するには、ライブ トポロジのリンク、マスター コントローラ アイコン、または境界ルータ アイコンをクリックします。それぞれの詳細情報を表示するのには各オプションをクリックします。詳細については、PfRv3 を使用したサイト間イベントに関する詳細の表示 （427 ページ） を参照してください。
アプリケーション トラフィック パスの追跡	アプリケーション トラフィック パスを追跡するには、[アプリケーション パスの追跡（Trace Application Path）] ドロップダウン リストから必要なアプリケーションを選択します。これらのアプリケーションは、選択した時間間隔で境界ルータの出力 NetFlow から自動的に読み込まれます。
サイト間トポロジの表示	[サイト間の詳細（Site to Site Details）] タブに移動するには、ライブ トポロジの [サイト間の詳細（Site to Site Details）] をクリックします。詳細については、PfRv3 を使用したサイト間イベントに関する詳細の表示 （427 ページ） を参照してください。

関連トピック

PfRv3 サービス プロバイダーおよび DSCP チャートの表示 （426 ページ）
ユーザ グループの PfR モニタリングへのアクセス （422 ページ）
PfRv3 を使用したサイト間イベントに関する詳細の表示 （427 ページ）
PfRv3 を使用した WAN インターフェイスの使用状況の比較 （430 ページ）

PfRv3 サービス プロバイダーおよび DSCP チャートの表示

[メトリック（Metrics）] パネルには、[サービス プロバイダー（Service Provider）] ビューおよび [DSCP] ビューのチャートが表示されます。

[サービス プロバイダー（Service Provider）] ビュー チャート：TCA を使用して収集したメトリックを表示します。各サービス プロバイダーは、独自の色でチャートに表されます。このビューで利用可能なチャートは次のとおりです。

- 時系列の到達不能性イベント カウント
- 時系列の最大遅延
- 時系列の最大ジッター
- 時系列の最大パケット損失（%）

[DSCP] ビュー チャート：さまざまな DSCP について 6 つの異なるメトリックを表示します。チャートを最大化すると、最大 5 つの DSCP を表示できます。また、DSCP フィルタを使用して必要な DSCP を選択することもできます。このビューで利用可能なチャートは次のとおりです。

- DSCP ごとのサービス プロバイダー（SP）帯域幅（B/W）使用率
- DSCP と TCA
- DSCP と到達不可能な TCA
- 時系列の最大遅延
- 時系列の最大ジッター
- 時系列の最大パケット損失（%）

[メトリック（Metrics）] パネルから実行できるタスクは次のとおりです。

- 異なるチャートの表示：[メトリック（Metrics）] パネルの矢印アイコン パネルをクリックします。
- チャートの追加：追加アイコン [コンポーネントの追加（Add components）] をクリックします。ダイアログボックスで必要なコンポーネントを選択し、[保存（Save）] をクリックします。

時間スライダ

ページの下部にある時間スライダは、フィルタを使用して選択された時間範囲を表します。スライダをドラッグして、特定の時間範囲を設定できます。[Metrics] パネルと [Site to Site PfR Eevents] テーブルは、設定された時間範囲に応じて変化します。

関連トピック

[PfRモニタリング（PfR Monitoring）] ページの使用 （422 ページ）
PfRv3 を使用したサイト間イベントに関する詳細の表示 （427 ページ）
PfRv3 を使用した WAN インターフェイスの使用状況の比較 （430 ページ）

PfRv3 を使用したサイト間イベントに関する詳細の表示

[サービス（Services）] > **[アプリケーションの可視性と制御（Application Visibility & Control）]** > **[PfRモニタリング（PfR Monitoring）]** から、次の表に示すようにさまざまなサイト間の詳細を表示できます。

表 *42 :* サイト間トポロジのタスク

タスク	説明
サイト間イベントの詳細情報の表示	サイト間イベント テーブルのドットをクリックします。 [サイト間（Site to Site）] ポップアップ ウィンドウが表示されます。このポップアップ ウィンドウには、表形式のイベント詳細と共に、指定した時間範囲に発生したイベントタイプを表示します。このウィンドウを必要なサイズに拡張できます。 IME が発生する違反メトリック（バイト損失（%）、遅延、ジッター、パケット損失（%））は、角カッコ [] 内に表示されます。
サイト間トポロジの表示	ポップアップ ウィンドウの [サイト間の詳細（Site to Site Details）] をクリックすると、サイト間トポロジ表現の概略図と、すべてのイベントの詳細を含む [すべてのイベント（All Events）] テーブルが表示されます。 トポロジには、境界ルータ、マスター コントローラ、サービス プロバイダー、内部リンクと外部リンクを表す記号が含まれています。時間フィルタで 72 時間未満の時間枠を選択した場合でも、このトポロジは最小 72 時間のデータに基づいてプロットされます。 境界ルータと対応するリンクが灰色に表示され、次のような理由からこのリンクをクリックできなくなります。 • 境界ルータのインベントリ収集が失敗した場合。 • 境界ルータが管理されていない場合。 • ユーザに境界ルータへのアクセスが許可されていない場合（ロールベースアクセス コントロールに基づいて）。 [VRF] ドロップダウン リストからトポロジを表示する VRF を選択します。

タスク	説明
PfRv3 を使用したデバイス使用率メトリックの表示	[マスターコントローラ（Master Controller）] アイコンをクリックして、次のいずれかのオプションを選択します。 • [デバイスメトリック（Device Metrics）]：CPU とメモリ使用率を含むデバイス メトリック ポップアップ ウィンドウが開きます。 • [PfRポリシー（PfR Policy）]：異なる VRF に対しマスター コントローラで設定されたポリシーを含むポリシー ウィンドウが開きます。各 VRF をクリックするとそれぞれのポリシーが表示されます。最新のポリシー情報を表示するには、[デバイスと同期（Sync with Device）] をクリックします。 [境界ルータ（Border Router）] アイコンのいずれかをクリックし、次のいずれかのオプションを選択します。 • [デバイスメトリック（Device Metrics）]：CPU とメモリ使用率を含むデバイス メトリック ポップアップ ウィンドウが開きます。 • [デバイスダッシュボードの起動（Launch Device Dashboard）]：[パフォーマンス（Performance）] ダッシュボードで [デバイス（Device)] ダッシュレットが開きます。 • [WANリンクの比較（Compare WAN Links）]：[WANリンクの比較（Compare WAN Links）] タブが開きます。詳細については、PfRv3 を使用した WAN インターフェイスの使用状況の比較（430 ページ） を参照してください。 • [分析（Analayze）]：デバイス コンテキスト タブが開きます。次の内容を表示できます。 • 境界ルータ メトリック：サービス プロバイダーの帯域幅、メモリ、および CPU の使用率が選択した時間間隔で記された 3 つのチャート、トラフィックに対するサービス プロバイダーの使用率が記されたチャートを表示します。チャートを拡大表示するには、ズームアイコンをクリックします。スライダを移動すると、チャートをさらに拡大して、特定の時間間隔におけるデータ パターンを表示できます。 • [WAN Link Usage and Performance]：選択した境界ルータの WAN インターフェイスの DSCP マーキングに対して、WAN リンクの使用率とパフォーマンスを示すテーブルが表示されます。データには、出力帯域幅（B/W）使用率、発生した TCA/RC/IME の数、DSCP マーキングに関連付けられているアプリケーションの数が含まれます。アプリケーションの数は、AVC NetFlow がこの WAN リンクの Cisco Prime Infrastructure で受信された場合にのみ表示されます。 • DSCP の横にある展開矢印をクリックすると、その他の詳細がドリルダウンされます。

タスク	説明
PfRv3 を使用したリンク使用率メトリックの表示	トポロジの出力リンクまたは入力リンクをクリックし、次のいずれかのオプションを選択します。 • [リンクメトリック（Link Metrics）] : [リンクメトリック（Link Metrics）] ポップアップ ウィンドウが開きます。 • [インターフェイスダッシュボードの起動（Launch Interface Dashboard）] : [パフォーマンス（Performance）] ダッシュボードで [インターフェイス（Interface)] ダッシュレットが開きます。 • [比較のため追加（Add to Compare）] : [WANリンクの比較（Compare WAN Links）] タブが開きます。詳細については、PfRv3 を使用した WAN インターフェイスの使用状況の比較 （430 ページ） を参照してください。 • [分析（Analayze）] : デバイス コンテキスト タブが開きます。次の内容を表示できます。 • WAN リンク メトリック：SP の使用傾向、上位 10 件のアプリケーション トラフィック（In と Out）、上位 10 件のアプリケーション使用率（Out）、上位の QoS クラス マップ統計情報の傾向、送信元サイトとすべてのサイト間の SP の使用とトラフィック、インターフェイスのアベイラビリティの傾向チャートを表示します。 • [WAN リンクの使用率とパフォーマンス（WAN Link Usage and Performance）] : WAN インターフェイスの DSCP マーキングに対して、WAN リンクの使用率とパフォーマンスを示すテーブルが表示されます。 • DSCP の横にある展開矢印をクリックすると、その他の詳細がドリルダウンされます。

トポロジ図のトラブルシューティング

トポロジが読み込まれない場合は、次の点を確認してください。

- 境界ルータ、マスター コントローラ、またはサービス プロバイダーいずれかの可用性。
- 選択した時間間隔でのサイト間の PfR 帯域幅および出力の可用性。
- プロトコル エンドポイントにインベントリ エラーはありません。
- インターフェイスは Cisco Prime Infrastructure によって管理されます。
- WAN リンク の可用性
- *root* ユーザでログインし、必要なデバイスにアクセスできるかどうか。

関連トピック

[PfRモニタリング（PfR Monitoring）] ページの使用 （422 ページ）
PfRv3 を使用した WAN インターフェイスの使用状況の比較 （430 ページ）

PfRv3 を使用した WAN インターフェイスの使用状況の比較

[WAN リンクの比較（Compare WAN Links）] タブには、WAN リンクの使用と選択した WAN リンクのパフォーマンスを比較するガイド付きワークフローが表示されます。

ステップ 1 **[サービス（Services）] > [アプリケーションの可視性と制御（Application Visibility & Control）] > [PfR のモニタリング（PfR Monitoring）]** を選択します。

また、[デバイス メトリック（Device Metrics）]ポップアップ ウィンドウの [WAN リンクの比較（Compare WAN Links）] をクリックするか、または [リンク メトリック（Link Metrics）] ポップアップ ウィンドウの [比較に追加（Add To Compare）] をクリックして [WAN リンクの比較（Compare WAN Links）] タブを表示します。境界ルータおよび WAN インターフェイスの詳細は、選択したデバイスまたはリンクに基づいて自動的に入力されます。

ステップ 2 [WAN リンクの比較（Compare WAN Links）] タブをクリックします。

ステップ 3 必要に応じて、フィルタ アイコンをクリックして、時間フィルタを表示します。

ステップ 4 比較する WAN リンクそれぞれの [PfR 制御サイト（PfR Controlled Site）] ドロップダウン リスト、[境界ルータ（Border Router）] ドロップダウン リスト、および [WAN インターフェイス/SP（WAN Interface/SP）] から必要なオプションを選択します。

ステップ 5 [比較（Compare）] をクリックすると、選択した WAN リンクを比較できます。

ステップ 6 比較に 3 つ目の WAN リンクを追加する場合は、[+] アイコンをクリックして必要なオプションを選択し、[更新（Update）] をクリックします。

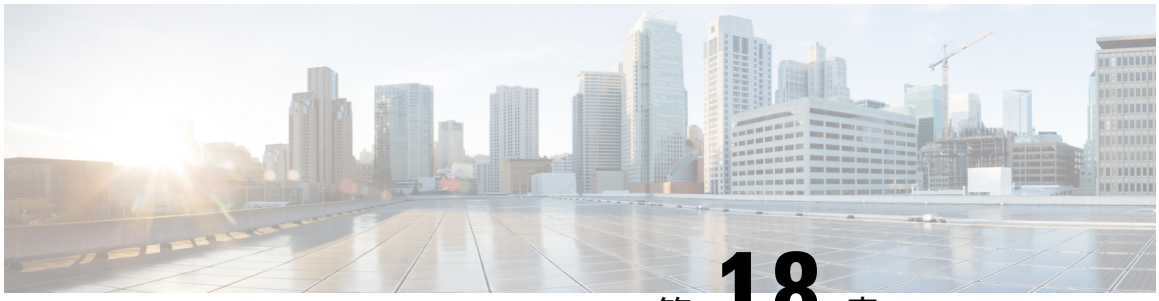
ステップ 7 編集アイコンをクリックすると、以前の選択内容を変更できます。

WAN リンクの使用状況、上位 N 件のアプリケーション、選択した WAN リンクの上位 QOS の傾向とインターフェイス アベイラビリティ、出力帯域幅（B/W）の使用率を比較するテーブル、選択した WAN で発生した TCA、RC、IME の数とルーティングしたアプリケーションの数を示すチャートを表示できます。

ステップ 8 必要な WAN リンク メトリックをクリックすると、それぞれのチャートが表示されます。

関連トピック

[PfRモニタリング（PfR Monitoring）] ページの使用 （422 ページ）
PfRv3 を使用したサイト間イベントに関する詳細の表示 （427 ページ）



第 18 章

ワイヤレス ネットワークのモニタ

- 無線リソース管理（RRM）とは （431 ページ）
- Prime Infrastructure に送信される RRM 通知 （432 ページ）
- [RRM] ダッシュボードを使用した AP のモニタ （433 ページ）
- AP 干渉源の表示 （434 ページ）
- RFID タグ付き AP の表示 （436 ページ）
- ワイヤレス メディア ストリームのモニタ （438 ページ）
- 非結合 AP のトラブルシューティング （438 ページ）
- 低周波送信 AP デバイス（チョークポイント）の識別 （439 ページ）
- MSE への WiFi TDOA レシーバの追加 （442 ページ）
- Cisco Prime Infrastructure およびマップへの WiFi TDOA レシーバの追加 （442 ページ）

無線リソース管理（RRM）とは

オペレーティング システムのセキュリティ ソリューションでは、Radio Resource Management（RRM; 無線リソース管理）機能を使用して、すべての近隣アクセス ポイントを継続的にモニタし、不正アクセス ポイントを自動的に検出します。

Cisco Unified Wireless Network に内蔵されている RRM は、RF 環境をモニタし、検出されたパフォーマンスの問題を動的に修正します。

Prime Infrastructure は、アクセス ポイントの送信電力またはチャネルが変化したときにトラップを受信します。こうしたトラップ イベントまたは RF の再グループ化などの同様のイベントは、Prime Infrastructure イベントに通知として記録され、イベント ディスパッチャによって保持されました。近隣のアクセス ポイントからの信号、干渉、ノイズ、負荷など、送信電力またはチャネルの変化の理由は明らかではありませんでした。これらのイベントや統計を表示してトラブルシューティングを実行できませんでした。

RRM 統計情報を使用して、障害のある場所を特定し、チャネルまたは電力レベルの変更について考えられる理由を示すことができます。ダッシュボードでは、ネットワーク全体の RRM パフォーマンスの統計情報が表示され、イベントのグループ化に基づいてチャネル変更の理由が予測されます。イベントのグループ化には次のものが含まれます。

- パフォーマンスが最も低いアクセス ポイント

- 同じ RF グループ内のコントローラ間の設定の不一致
- しきい値に基づいてアクセス ポイントによって検出されたカバレッジ ホール
- コントローラによって検出されたプリカバレッジ ホール
- 最大電力で動作しているアクセス ポイントの比率

（注） RRM ダッシュボードの情報は、Lightweight アクセス ポイントのみで使用できます。

Prime Infrastructure に送信される RRM 通知

チャネルが変更されると、Prime Infrastructure RRM ダッシュボードに通知が送信されます。チャネルの変更は、モードを [自動（auto）] または [オン デマンド（on demand）] に設定できる動的チャネル割り当て（DCA）設定によって異なります。モードが [auto] の場合、この操作を許可するすべての Lightweight アクセス ポイントに対し、チャネル割り当てが定期的に更新されます。モードが [on demand] に設定されている場合、要求に基づいてチャネル割り当てが更新されます。DCA が静的である場合、動的チャネル割り当ては行われず、値はグローバル デフォルトに設定されます。

チャネル変更のトラップが前のチャネル変更の後に受信されると、イベントは [Channel Revised] とマークされます。そうでない場合、[Channel Changed] とマークされます。チャネル変更イベントには、複数の原因がある場合があります。原因コードには、考えられる理由の数に関係なく、1 という係数が与えられます。たとえば、チャネル変更が信号、干渉、またはノイズによって発生するとします。通知の理由コードは、すべての原因を対象として係数が変更されます。そのイベントの理由が 3 つある場合は、原因コードの係数は理由 1 つあたり 1/3 または 0.33 に変更されます。10 件のチャネル変更イベントが同じ原因コードである場合、3 つの原因すべてに同じ係数が与えられて、チャネル変更の原因が判定されます。

送信電力が変更されると、Prime Infrastructure RRM ダッシュボードに通知が送信されます。送信電力変更の各イベントには、いくつかの理由があります。原因コードは、イベントが発生した理由の数に関係なく、1 という係数が与えられます。

RRM がコントローラで実行されると、動的グループ化が行われ、新しいグループ リーダーが選択されます。動的グループ化には、Automatic、Off、および Leader の 3 つのモードがあります。グループ化を Off にすると、動的グループ化は行われなくなり、各スイッチは自身の Lightweight アクセス ポイント パラメータのみを最適化します。グループ化を Automatic にすると、スイッチはグループを形成し、リーダーを選択してより適切な動的パラメータの最適化を実行します。自動グループ化では、設定した間隔（秒）はグループ化アルゴリズムが実行される期間を示します。（グループ化アルゴリズムは、グループに変更があり、自動グループ化が有効である場合にも実行されます）。

[RRM] ダッシュボードを使用した AP のモニタ

RRM ダッシュボードは、**[モニタ（Monitor）] > [ワイヤレステクノロジー（Wireless Technologies）] > [無線リソース管理（Radio Resource Management）]** から使用できます。

このダッシュボードは、次の部分で構成されています。

- [RRM RF Group Summary] には、異なる RF グループの数が表示されます。最新の RF グループ数を取得するには、設定の同期バックグラウンド タスクを実行します。
- [RRM Statistics] 部分には、ネットワーク全体の統計が表示されます。
- [Channel Change Reason] 部分には、802.11a/b/g/n 無線のチャネルが変更した理由が表示されます。
  - 信号：他のいくつかの近隣する無線のチャネル品質が改善されたためにチャネルが変更されました。他のいくつかの近隣無線のチャネル品質の改善により、アルゴリズムによって評価されるシステムのチャネル計画が改善しました。
  - WiFi 干渉
  - 負荷
  - レーダー
  - ノイズ
  - 永続的な WiFi 以外の干渉
  - 主要な電波品質イベント
  - その他
- [Channel Change] には、完了したすべてのイベントが原因とともに表示されます。
- [Configuration Mismatch] 部分には、リーダーとメンバの比較が表示されます。
- [Coverage Hole] 部分には、カバレッジ ホールがどれほど深刻かを評価し、その位置を示します。
- [Percent Time at Maximum Power] には、アクセス ポイントが最大電力に達した時間の割合が表示され、これらのアクセス ポイントを示します。

次の統計情報が表示されます。

- [Total Channel Changes]：チャネルが更新または変更されたかどうかに関係なく、802.11a/b/g/n 無線のチャネル変更数の合計。カウントは、24 時間および 7 日間の期間に分割されます。割合のリンクまたは [24-hour] 列の下にあるリンクをクリックすると、そのアクセス ポイントのみの詳細を示すページが表示されます。
- [Total Configuration Mismatches]：24 時間に検出された設定の不一致数の合計。

- [Total Coverage Hole Events]：24 時間および 7 日間のカバレッジ ホール イベント数の合計。
- [PRグループ数（Number of RF Groups）]：RF グループの総数（現在 Prime Infrastructure によって管理されているすべてのコントローラから計算されます）。
- [Configuration Mismatch]：24 時間に発生した設定の不一致を RF グループごとにグループ リーダーの詳細とともに表示します。
- [APs at MAX Power]：802.11a/n 無線のアクセス ポイントの割合を、最大電力に達したすべてのアクセス ポイントの割合の合計として表示します。最大電力レベルはプリセットされ、プリセット値を基準にして計算されます。

  最大電力は、RRM ダッシュボードの 3 つの領域に表示されます。この最大電力の部分には、現在の値が表示され、ポーリングされます。
- [Channel Change Causes]：802.11a/n 無線のグラフィック棒グラフ。グラフは、チャネル変更が行われた理由に基づいて作成されます。グラフは2つの部分に分割され、それぞれ24時間および7日間に発生するイベントを引き起こす理由の重み付けされた理由の割合を示します。チャネル変更の各イベントにはいくつかの理由があり、その重みはそれらの理由に均等に分けられます。ネット原因コードは、イベントが発生した理由の数に関係なく、1 という係数が与えられます。
- [Channel Change - APs with channel changes]：チャネル変更の各イベントには、Lightweight アクセス ポイントの MAC アドレスが含まれます。各理由コードについて、チャネル イベントの重み付き理由に基づいて 802.11a/n アクセス ポイントに発生したチャネル変更の多くが表示されます。カウントは、24 時間および 7 日間の期間に分割されます。
- [Coverage Hole - APs reporting coverage holes]：カバレッジ ホール イベント（しきい値に基づく）を生成した、IF Type 11 a/n でフィルタされた上位 5 つのアクセス ポイントが表示されます。
- [Aggregated Percent Max Power APs]：カバレッジ ホール イベントを調整するために最大電力で動作している 802.11a/n Lightweight アクセス ポイントの割合の合計を示すグラフィカルな進捗状況グラフ。カウントは、24 時間および 7 日間の期間に分割されます。

  この最大電力の部分には、最近 24 時間の値が表示され、ポーリング主導となります。これは、15 分ごとまたは無線パフォーマンスの設定に応じて発生します。
- [Percent Time at Maximum Power]：最大電力で動作している上位 5 つの 802.11a/n Lightweight アクセス ポイントのリスト。この最大電力の部分には、最近 24 時間の値が表示され、イベント駆動となります。

AP 干渉源の表示

[モニタ（Monitor）] > [ワイヤレステクノロジー（Wireless Technologies）] > [干渉源（Interferers）] ページでは、CleanAir 対応アクセス ポイントで検出された干渉デバイスをモニタできます。デフォルトでは、[干渉源検出 AP モニタリング（Monitoring AP Detected Interferers）] ページが表示されます。

表 *43 :* 干渉源をモニタするためのメニュー パス

確認内容	次に移動します。
AP に検出された干渉源	**[Monitor] > [Wireless Technologies] > [Interferers]** （注） CMX を使用している場合、このページに干渉源は表示されません。
AP に検出された干渉源の詳細	**[モニタ（Monitor）] > [ワイヤレス テクノロジー（Wireless Technologies）] > [干渉源（Interferers）] > [干渉源 ID（Interferer ID）]**
AP に検出された干渉源の詳細のロケーション履歴	**[モニタ（Monitor）] > [ワイヤレステクノロジー（Wireless Technologies）] > [干渉源（Interferers）] > [干渉源ID（Interferer ID）]**、次に [ロケーション履歴（Location History）] を選択して、[移動（Go）] をクリックします。

[APが検出した干渉源（AP Detected Interferers）] ページの編集

[Edit View] ページでは、[AP Detected Interferers Summary] ページの列を追加、削除、並べ替えできます。[AP Detected Interferers] ページの列を編集するには、次の手順に従います。

手順の概要

1. **Monitor > Wireless Technologies > Interferers**を選択します。[AP Detected Interferers] ページが表示されます。このページには、CleanAir 対応アクセス ポイントにより検出された干渉源の詳細が表示されます。
2. [**Edit View**] リンクをクリックします。
3. アクセスポイント表に新しい列を追加するには、左側の領域で、列見出しをクリックして選択します。**Show** をクリックして、選択した列見出しを右側の領域へ移動します。右側の領域にあるすべての項目が表に表示されます。
4. アクセスポイント表から列を削除するには、右側の領域で、削除する列見出しをクリックして選択します。**Hide**をクリックして、選択した列見出しを左側の領域へ移動します。左側の領域にある項目はすべて、表に表示されません。
5. **Up/Down** ボタンを使用して、テーブル内での情報の並び順を指定します。目的の列見出しを選択し、**Up** または **Down** をクリックして、現在のリスト内での位置を変更します。
6. デフォルト表示に戻すには、**Reset** をクリックします。
7. **Submit** をクリックして、変更内容を確定します。

手順の詳細

ステップ 1 **Monitor > Wireless Technologies > Interferers**を選択します。[AP Detected Interferers] ページが表示されます。このページには、CleanAir 対応アクセス ポイントにより検出された干渉源の詳細が表示されます。

ステップ 2 [**Edit View**] リンクをクリックします。

ステップ 3 アクセス ポイント表に新しい列を追加するには、左側の領域で、列見出しをクリックして選択します。**Show**をクリックして、選択した列見出しを右側の領域へ移動します。右側の領域にあるすべての項目が表に表示されます。

ステップ 4 アクセス ポイント表から列を削除するには、右側の領域で、削除する列見出しをクリックして選択します。**Hide** をクリックして、選択した列見出しを左側の領域へ移動します。左側の領域にある項目はすべて、表に表示されません。

ステップ 5 **Up/Down** ボタンを使用して、テーブル内での情報の並び順を指定します。目的の列見出しを選択し、**Up** または **Down** をクリックして、現在のリスト内での位置を変更します。

ステップ 6 デフォルト表示に戻すには、**Reset** をクリックします。

ステップ 7 **Submit** をクリックして、変更内容を確定します。

RFID タグ付き AP の表示

[モニタ（Monitor）] > [ワイヤレステクノロジー（Wireless Technologies）] > [RFIDタグ（RFID Tags）] ページでは、タグの詳細の確認に加えて、タグ ステータスと Prime Infrastructure マップ上のロケーションをモニタできます。

このページは、Prime Infrastructure の Location バージョンのみで使用できます。

このセクションには、ロケーションアプライアンスにより検出されるタグについての情報が表示されます。

[タグサマリ（Tag Summary）] ページは、**[モニタ（Monitor）] > [ワイヤレステクノロジー（Wireless Technologies）] > [RFIDタグ（RFID Tags）]** で使用できます。

RFID タグの検索

特定のタグまたはすべてのタグを検索するには、Prime Infrastructure の [詳細検索（Advanced Search）] 機能を使用します。

タグを検索するには、次の手順を実行します。

手順の概要

1. **Advanced Search** をクリックします。
2. [検索カテゴリ（Search Category）] ドロップダウン リストから、**Tags**[タグ（Tags）]**Tags** を選択します。

3. 必要な情報を入力します。選択したカテゴリによって、検索フィールドが変わることがあることに注意してください。
4. **Go** をクリックします。

手順の詳細

ステップ 1 **Advanced Search** をクリックします。

ステップ 2 [検索カテゴリ（Search Category）] ドロップダウン リストから、**Tags**[タグ（Tags）]**Tags** を選択します。

ステップ 3 必要な情報を入力します。選択したカテゴリによって、検索フィールドが変わることがあることに注意してください。

ステップ 4 **Go** をクリックします。

RFID タグの検索結果の確認

検索結果を確認するには、検索結果ページでタグ ロケーションの MAC アドレスをクリックします。

次の点に注意してください。

- [Tag Vendor] オプションは、検索基準が [Asset Name]、[Asset Category]、[Asset Group]、または [MAC Address] の場合は表示されません。
- テレメトリをサポートしているベンダー タグのみが表示されます。
- [Telemetry data] オプションは、[Search for tags by] オプションで [MSE]（ロケーション サーバで選択）、[Floor Area]、または [Outdoor Area] が選択されている場合にのみ表示されます。
- 表示されるテレメトリ データはベンダー固有ですが、GPS の場所、バッテリー拡張情報、圧力、温度、湿度、動作、ステータス、および緊急コードなど、いくつかの内容が共通して報告されます。
- アセット情報、統計情報、ロケーション、およびロケーション通知の詳細が表示されます。
- 緊急データについては、CCX v1 に準拠したタグのみが表示されます。

タグ リストの表示

[タグ総数（Total Tags number）] リンクをクリックすると、該当するデバイス名のタグ リストが表示されます。タグ リストには、MAC アドレス、資産の詳細、ベンダー名、モビリティ サービス エンジン、コントローラ、バッテリ ステータス、およびマップ ロケーションが含まれています。

ワイヤレス メディア ストリームのモニタ

メディア ストリームの設定をモニタするには、次の手順を実行します。

ステップ 1 **[モニタ（Monitor）] > [ワイヤレス テクノロジー（Wireless Technologies）] > [メディア ストリーム（Media Streams）]** を選択します。[メディア ストリーム（Media Streams）] ページが開き、コントローラ全体で設定されているメディア ストリームの一覧が表示されます。

ステップ 2 メディア ストリームの詳細を表示するには、[Stream] 列のメディア ストリーム名をクリックします。[Media Streams] ページが表示されます。

非結合 AP のトラブルシューティング

Lightweight アクセス ポイントは、初回起動時に、ワイヤレス LAN コントローラを検出し、接続しようとします。アクセス ポイントは、ワイヤレス コントローラに接続した後、必要に応じてそのソフトウェア イメージを更新し、デバイスとネットワークの構成の詳細をすべて受信します。アクセス ポイントが正常にワイヤレス コントローラを接続した後、そのアクセス ポイントは Prime Infrastructure で検出および管理できます。アクセス ポイントが正常にワイヤレス コントローラを接続するまで、そのアクセス ポイントは Prime Infrastructure で管理できないため、クライアント アクセスを可能にする適切な設定は組み込まれません。

Prime Infrastructure は、アクセス ポイントがコントローラに接続できない理由を診断し、対処方法を一覧表示するツールを提供しています。

[Unjoined AP] ページには、ワイヤレス コントローラに接続していないアクセス ポイントが一覧表示されます。このページには、未接続アクセス ポイントについて収集されたすべての情報が含まれます。この情報には、名前、MAC アドレス、IP アドレス、コントローラの名前と IP アドレス、アクセス ポイントの接続先のスイッチとポート、および接続が失敗した理由（判明している場合）が含まれます。

未接続アクセス ポイントのトラブルシューティングを行うには、次の手順を実行します。

ステップ 1 **[モニタ（Monitor）] > [ワイヤレス テクノロジー（Wireless Technologies）] > [未接続アクセス ポイント（Unjoined Access Points）]** を選択します。[Unjoined APs] ページが表示され、ワイヤレス コントローラに接続できなかったアクセス ポイントの一覧が表示されます。

ステップ 2 診断するアクセス ポイントを選択し、[Troubleshoot] をクリックします。アクセス ポイントに対して分析が実行され、アクセス ポイントがワイヤレス コントローラに接続できなかった理由が特定されます。分析の実行後、[Unjoined APs] ページに結果が表示されます。

ステップ 3 アクセス ポイントが複数のワイヤレス コントローラに接続しようとし、失敗した場合、それらのコントローラが左ペインに一覧表示されます。コントローラを選択します。

ステップ 4 中央のペインで、問題を確認できます。このペインには、エラー メッセージとコントローラのログ情報も一覧表示されます。

ステップ 5 右側のペインに、問題を解決するための推奨事項が表示されます。推奨処置を実行します。

ステップ 6 さらに問題を診断する必要がある場合、[Unjoined AP] ページから RTTS を実行できます。これにより、アクセス ポイントが同時に接続しようとしたすべてのワイヤレス コントローラからのデバッグ メッセージが表示されます。

低周波送信 AP デバイス（チョークポイント）の識別

チョークポイントは、低周波の送信デバイスです。配置されたチョークポイントの範囲内でタグが渡されると、低周波電磁界がタグを認識し、チョークポイント デバイス ID を含むメッセージを Cisco Unified Wireless Network 経由で送信します。送信されるメッセージには、センサー情報（温度や圧力など）が含まれます。チョークポイント ロケーション システムは、部屋レベルの精度（ベンダーによって数インチから 2 フィートまで）を提供します。

チョークポイントは、チョークポイントのベンダーによって推奨されるとおりに設置および設定されます。チョークポイントがインストールされ動作可能になったら、チョークポイントをロケーション データベースに入力して、Prime Infrastructure マップ上に表示できます。

Prime Infrastructure への AP チョークポイントの追加

チョークポイントを Prime Infrastructure データベースに追加するには、次の手順を実行します。

ステップ 1 **[モニタ（Monitor）] > [ワイヤレステクノロジー（Wireless Technologies）] > [チョークポイント（Chokepoints）]** の順に選択します。

ステップ 2 [コマンドの選択（Select a command）] ドロップダウン リストから [チョークポイントの追加（Add Chokepoint）] を選択します。

ステップ 3 [Go] をクリックします。

ステップ 4 チョークポイントの MAC アドレスと名前を入力します。

ステップ 5 Entry または Exit チョークポイントを指定します。

ステップ 6 チョークポイントのカバレッジ範囲を入力します。

チョークポイントの範囲は、視覚的な表示のみです。これは製品固有です。実際の範囲は、該当するチョークポイント ベンダー ソフトウェアを使用して別個に設定する必要があります。

ステップ 7 [Save] をクリックします。

データベースにチョークポイントを追加したら、適切な Prime Infrastructure フロア マップに配置できます。

Prime Infrastructure からの AP チョークポイントの削除

チョークポイントを Prime Infrastructure データベースから削除するには、次の手順を実行します。

ステップ 1 **[モニタ（Monitor）] > [ワイヤレステクノロジー（Wireless Technologies）] > [チョークポイント（Chokepoints）]** の順に選択します。

ステップ 2 削除するチョークポイントのチェックボックスを選択します。

ステップ 3 [コマンドの選択（Select a command）] ドロップダウン リストから、[削除（Remove）] を選択します。

ステップ 4 [Go] をクリックします。

ステップ 5 [OK] をクリックして、削除を実行します。

Prime Infrastructure マップからのチョークポイントの削除

Prime Infrastructure マップからチョークポイントを削除するには、次の手順を実行します。

手順の概要

1. **Maps > Wireless Maps > Site Maps**を選択します。
2. [Maps]ページで、チョークポイントのフロアの位置に対応するリンクをクリックします。
3. [コマンドの選択（Select a command）] ドロップダウン リストから、次を選択します。 **Remove Chokepoints.**
4. **Go** をクリックします。
5. **OK** をクリックして削除を確認します。

手順の詳細

ステップ 1 **Maps > Wireless Maps > Site Maps**を選択します。

ステップ 2 [Maps] ページで、チョークポイントのフロアの位置に対応するリンクをクリックします。

ステップ 3 [コマンドの選択（Select a command）] ドロップダウン リストから、次を選択します。 **Remove Chokepoints.**

ステップ 4 **Go** をクリックします。

ステップ 5 **OK** をクリックして削除を確認します。

AP チョークポイントの編集

Prime Infrastructure データベースと適切なマップでチョークポイントを編集するには、次の手順を実行します。

ステップ 1 **[モニタ（Monitor）] > [ワイヤレステクノロジー（Wireless Technologies）] > [チョークポイント（Chokepoints）]** の順に選択します。

ステップ 2 [MAC Address] カラムで、編集するチョークポイントをクリックします。

ステップ 3 変更するパラメータを編集します。

チョークポイントの範囲は製品固有であり、チョークポイントのベンダーにより供給されます。

ステップ 4 **[保存（Save）]** をクリックします。

WiFi TDOA レシーバによるタグ位置レポートの強化

TDOA レシーバは、到達時間差（TDOA）の方法を使用して、タグの位置を計算します。この方法は、最小で 3 つの TDOA レシーバからのデータを使用して、タグ付き資産の位置を生成します。

（注） TDOA レシーバが使用中ではなく、パートナー エンジン ソフトウェアが Mobility Service Engine にある場合は、タグの位置計算は、アクセス ポイントからの RSSI の読み取りを使用して生成されます。

（注） シスコのタグ エンジンは、アクセス ポイントからの RSSI 読み取りを使用してタグの位置を計算できます。

Cisco Unified Wireless Network 内で TDOA レシーバを使用する前に、次の手順を実行する必要があります。

1. ネットワークで Mobility Services Engine をアクティブにします。Cisco Prime Infrastructure への MSE の追加 （1000 ページ）を参照してください。
2. TDOA レシーバを Prime Infrastructure データベースとマップに追加します。Cisco Prime Infrastructure およびマップへの WiFi TDOA レシーバの追加 （442 ページ）を参照してください。
3. Prime Infrastructure を使用して MSE でパートナー エンジン サービスをアクティブ化または開始します。
4. Prime Infrastructure およびモビリティ サービス エンジンを同期します。MSE と同期される Cisco Prime Infrastructure データ （1008 ページ）を参照してください。
5. AeroScout システム マネージャを使用して TDOA レシーバを設定します。設定の詳細については、http://support.aeroscout.com で『AeroScout Context-Aware Engine for Tags, for Cisco Mobility Services Engine User's Guide』を参照してください。

MSE への WiFi TDOA レシーバの追加

AeroScout システム マネージャによって Wi-Fi TDOA レシーバをインストールして設定し、パートナー ソフトウェアをモビリティ サービス エンジンにダウンロードすると、TDOA レシーバをモビリティ サービス エンジン データベースに追加して、Prime Infrastructure マップ上に配置することができます。

TDOA レシーバを Prime Infrastructure マップに追加した後で、Prime Infrastructure ではなく、AeroScout システム マネージャ アプリケーションを使用して TDOA レシーバに対する設定の変更を続行します。

設定オプションの詳細については、XREF http://support.aeroscout.com にある『*AeroScout Context-Aware Engine for Tags, for Cisco Mobility Services Engine User Guide*』を参照してください。

TDOA レシーバを Prime Infrastructure データベースと適切なマップに追加するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ワイヤレス テクノロジー（Wireless Technologies）] > [WiFi TDOA レシーバ（WiFi TDOA Receivers）]** を選択して、[すべての WiFi TDOA レシーバ（All WiFi TDOA Receivers）] サマリー ページを開きます。

現在の WiFi TDOA レシーバの詳細を表示または編集するには、[MAC Address] リンクをクリックして、詳細ページを開きます。

ステップ 2 [Select a command] ドロップダウン リストから、[Add WiFi TDOA Receivers] を選択し、[Go] をクリックします。

ステップ 3 TDOA レシーバの MAC アドレス、名前、およびスタティック IP アドレスを入力します。

ステップ 4 [OK] をクリックして、TDOA レシーバ エントリをデータベースに保存します。

TDOA レシーバをデータベースに追加したら、適切な Prime Infrastructure フロア マップに TDOA レシーバを配置できます。

WiFi TDOA レシーバは、レシーバ ベンダー ソフトウェアを使用して別個に設定する必要があります。

Cisco Prime Infrastructure およびマップへの WiFi TDOA レシーバの追加

AeroScout システム マネージャによって WiFi TDOA レシーバをインストールして設定し、パートナー ソフトウェアをモビリティ サービス エンジンにダウンロードすると、TDOA レシーバをモビリティ サービス エンジンのデータベースに追加して、Prime Infrastructure マップ上に配置することができます。

TDOA レシーバを Prime Infrastructure マップに追加した後で、Prime Infrastructure ではなく、AeroScout システム マネージャ アプリケーションを使用して TDOA レシーバに対する設定の変更を続行します。

設定オプションの詳細については、http://support.aeroscout.com にある『*AeroScout Context-Aware Engine for Tags, for Cisco Mobility Services Engine User Guide*』を参照してください。

TDOA レシーバを Prime Infrastructure データベースと適切なマップに追加するには、次の手順を実行します。

ステップ 1 [Monitor] > [Wireless Technologies] > [WiFi TDOA Receivers] の順に選択して、[All WiFi TDOA Receivers] 概要ページを開きます。

現在の WiFi TDOA レシーバの詳細を表示または編集するには、[MAC Address] リンクをクリックして、詳細ページを開きます。

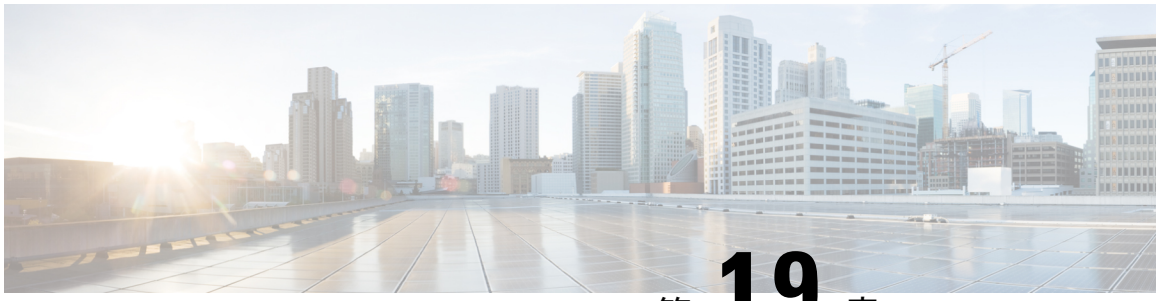
ステップ 2 [Select a command] ドロップダウン リストから、[Add WiFi TDOA Receivers] を選択します。

ステップ 3 [Go] をクリックします。

ステップ 4 TDOA レシーバの MAC アドレス、名前、およびスタティック IP アドレスを入力します。

ステップ 5 [Save] をクリックして、TDOA レシーバ エントリをデータベースに保存します。

（注） WiFi TDOA レシーバは、レシーバ ベンダー ソフトウェアを使用して別個に設定する必要があります。



第 19 章

モニタリング ツールの使用

- ワイヤレス コントローラの音声監査の実行 （445 ページ）
- 音声診断ツールを使用した AP パフォーマンスの確認 （446 ページ）
- ワイヤレス設定の監査 （447 ページ）
- Lightweight AP に移行できる自律 AP の決定 （447 ページ）
- ロケーション精度ツールによる AP ロケーション精度の確保 （448 ページ）
- IPSLA のモニタリング （453 ページ）

ワイヤレス コントローラの音声監査の実行

Prime Infrastructure には、コントローラの設定を確認し、導入ガイドラインからの逸脱を Audit Violation として強調表示するための、音声監査メカニズムが用意されています。1 回の操作で、最大 50 台のコントローラで音声監査を実行できます。

音声監査を実行するには、次の手順を実行します。

ステップ 1 **[モニタ（Monitor）] > [ツール（Tools）] > [ワイヤレス音声の監査（Wireless Voice Audit）]** の順に選択します。

ステップ 2 [コントローラ（Controllers）] タブをクリックし、http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-infrastructure/products-user-guide-list.html の「*Voice Audit Field Descriptions*」の項の説明に従ってフィールドに入力します。

ステップ 3 **[ルール（Rules）]** タブをクリックします。

ステップ 4 [VoWLAN SSID] テキスト ボックスに、適切な VoWLAN SSID を入力します。

（注） 赤い円は無効なルールを示します（データが不十分なため）。緑の円は有効なルールを示します。

ステップ 5 次のいずれかを実行します。

- レポートを実行しないで設定を保存するには、[保存（Save）] をクリックします。
- 設定を保存し、レポートを実行するには、[Save and Run] をクリックします。

ステップ 6 レポート結果を表示するには [Report] タブをクリックします。

音声診断ツールを使用した AP パフォーマンスの確認

音声診断ツールは、リアルタイムでボイスコールを診断するインタラクティブ ツールです。このツールは、コール制御エラー、クライアントのローミング履歴、および関連 AP で許可および拒否されたアクティブ コールの合計数をレポートします。

音声診断テストは複数のコントローラに対してプロビジョニングされます。つまり、ローミング時に AP が複数のコントローラにアソシエートされた場合、音声診断ツールにより、アソシエートされたすべてのコントローラがテストされます。Prime Infrastructure は AP が最大 3 フロアに配置されているコントローラで、テストをサポートします。たとえば、Prime Infrastructure マップに 1 ～ 4 のフロアがあり、すべての AP がコントローラー（WLC1、WLC2、WLC3、および WLC4）に関連付けられ、Prime Infrastructure マップに配置されている場合があります。任意の AP のクライアントが最初のフロアで WLC1 に関連付けられ、音声診断テストがそのクライアントに対して開始されると、テストは WLC2 および WLC3 に対してもプロビジョニングされます。

[Voice Diagnostic] ページには、以前に実行されたテストがリストされます（ある場合）。このページのフィールドについては、 http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-infrastructure/products-user-guide-list.html の「Voice Diagnostic Field Descriptions」の項を参照してください。

[コマンドの選択（Select a command）] ドロップダウン リストから、新しいテストの開始、既存のテストの結果の確認、またはテストの削除を実行できます。

（注） このツールは、ローミングをサポートするために、同じビルディング内のコントローラを、クライアントのアソシエート AP ビルディングのコントローラとして認識し、すべてのコントローラの監視リストに追加します。このツールは、コントローラで設定するために、クライアントの現在のアソシエーション A の場所から上下 5 階のコントローラを検索します。コントローラの監視リストの設定は、10 分で終わります。10 分後に、コントローラは監視リストからエントリを削除します。

音声診断テストを実行するには、次の手順を実行します。

ステップ 1 **[モニタ（Monitor）] > [ツール（Tools）] > [ワイヤレス音声の監査（Wireless Voice Audit）]** の順に選択します。

ステップ 2 [コマンドの選択（Select a command）] ドロップダウン リストから、[新規テスト（New test）] を選択し、[実行（Go）] をクリックします。

（注） ボイスコール診断の目的で最大 2 つのクライアントを設定できます。両方のクライアントを同じコールで診断すること、または別のコールで診断することができます。

ステップ 3 テスト名およびボイスコールを監視する期間を入力します。
ステップ 4 音声診断テストの対象となるデバイスの MAC アドレスを入力します。
ステップ 5 デバイス タイプを選択します。カスタム電話を選択した場合は、RSSI 範囲を入力します。
ステップ 6 [テスト開始（Start Test）] をクリックします。

ワイヤレス設定の監査

[設定の監査の概要（Configuration Audit Summary）] ページを起動するには、**[モニタ（Monitor）] > [ツール（Tools）] > [ワイヤレス設定の監査（Wireless Configuration Audit）]** の順に選択します。

このページには、次の概要が表示されます。

- [有効な設定グループの合計数（Total Enforced Config Groups）]：バックグラウンド監査用に設定され適用が有効になっているテンプレート。
- [一致しないコントローラの合計数（Total Mismatched Controllers）]：最後の監査時に Prime Infrastructure とコントローラ間で検出される設定の差異。
- [設定監査アラームの合計数（Total Config Audit Alarms）]：監査の矛盾が設定グループに施行されると生成されるアラーム。施行が失敗すると、設定グループに重大なアラームが生成されます。施行が成功すると、設定グループにマイナーアラームが生成されます。アラームには監査レポートへのリンクがあり、各コントローラの矛盾のリストを表示できます。
- [最新の 5 つの設定監査アラーム（Most recent 5 config audit alarms）]：監査アラームのオブジェクト名、イベントのタイプ、日付と時刻が含まれます。

[すべて表示（View All）] をクリックすると該当する [アラーム（Alarm）] ページが開き、すべての設定監査アラームが表示されます。

Lightweight AP に移行できる自律 AP の決定

[モニタ（Monitor）] > [ツール（Tools）] > [自律型AP移行分析（Autonomous AP Migration Analysis）] を選択して、[移行分析の概要（Migration Analysis Summary）] ページを起動します。Autonomous アクセス ポイントは、すべての基準が成功ステータスの場合だけ移行できます。赤い X は適格でないことを示し、緑のチェック マークは適格であることを示します。これらの列は次のものを表しています。

- [Privilege 15 Criteria]：Autonomous アクセス ポイントの検出の一部として指定された Telnet クレデンシャルは、特権 15 であることが必要です。
- [Software Version]：Cisco IOS 12.3(7)JA リリースからの変換のみがサポートされています。ただし、Cisco IOS 12.3(11)JA、Cisco IOS 12.3(11)JA1、Cisco IOS 12.3(11)JA2、および Cisco IOS 12.3(11)JA3 を除きます。

- [Role Criteria]：アソシエーション要求を送信するには、アクセス ポイントとコントローラの間の有線接続が必要です。そのため、次の Autonomous アクセス ポイント ロールが必要です。
  - root
  - root access point
  - root fallback repeater
  - root fallback shutdown
  - root access point only
- [Radio Criteria]：デュアル無線アクセス ポイントの場合、1 つの無線の種類のみがサポートされている場合でも変換を実行できます。

ロケーション精度ツールによる AP ロケーション精度の確保

Location Accuracy Tool を使用すると、不正でないクライアント、不正クライアント、干渉源、およびアセット タグの位置精度を分析できます。

位置精度を確認することによって、既存のアクセス ポイントの導入が、少なくとも 90 % の確率で、10 m 以内にある要素の真の位置を推定できることを確認できます。

Location Accuracy Tool では、次のいずれかのテストを実行できます。

- スケジュール設定された精度テスト：クライアント、タグ、および干渉源がすでに展開され、無線 LAN インフラストラクチャに関連付けられている場合に使用されます。クライアント、タグ、干渉源がすでに事前に配置されている場合は、テストが定期的なスケジュールに基づいて実行できるように、スケジュール設定されたテストを設定して保存できます。
- オンデマンド精度テスト：要素はアソシエートされているが、事前に配置されていない場合に使用します。オンデマンドテストでは、さまざまな場所でクライアント、タグ、および干渉源のロケーション精度をテストできます。通常は、少数のクライアント、タグ、干渉源の位置精度をテストするために使用します。

両方のテストとも、1 つのページで設定および実行されます。

関連トピック

AP ロケーション精度ツールのセットアップ （448 ページ）
ロケーション精度テストのスケジューリング （449 ページ）
オンデマンド ロケーション精度テストの実行 （451 ページ）

AP ロケーション精度ツールのセットアップ

スケジュール設定済みおよびオンデマンドのロケーション精度ツールのテスト機能を使用するには、Prime Infrastructure で [詳細デバッグ（Advanced Debug）] オプションを有効にする必要があります。[詳細デバッグ（Advanced Debug）] オプションが有効になっていない場合、Location

Accuracy Tool は [モニタ（Monitor）] > [ツール（Tools）] メニューに選択肢として表示されません。

Prime Infrastructure で [詳細デバッグ（Advanced Debug）] オプションを有効にするには、次の手順を実行します。

ステップ 1 Prime Infrastructure で、**[マップ（Maps）]** > **[ワイヤレス マップ（Wireless Maps）]** > **[サイト マップ（Site Maps）]** を選択します。

ステップ 2 [コマンドの選択（Select a command）] ドロップダウン リストから [プロパティ（Properties）] を選択し、[実行（Go）] をクリックします。

ステップ 3 詳細デバッグ モードを有効にするには、[有効（Enabled）] チェックボックスをオンにします。[OK] をクリックします。

（注） [Advanced Debug] がすでに有効になっている場合は、さらに操作を行う必要はありません。[Cancel] をクリックします。

新しいスケジュール設定された精度テストまたはオンデマンドの精度テストの作成、最後の実行のログのダウンロード、すべてのログのダウンロード、現在の精度テストの削除を行うには、[Location Accuracy] ページの [Select a command] ドロップダウン リストを使用します。

（注） [Accuracy Tests] 概要ページから精度テストのログをダウンロードできます。これを行うには、精度テストを選択し、[コマンドの選択（Select a command）] ドロップダウン リストから、[ログのダウンロード（Download Logs）] または [最後の実行のログのダウンロード（Download Logs for Last Run）] を選択します。[Go] をクリックします。

- [Download Logs] オプションは、選択したテストのすべての精度テストのログをダウンロードします。
- [Download Logs for Last Run] オプションは、選択したテストの最新のテスト実行のログのみをダウンロードします。

関連トピック

ロケーション精度ツールによる AP ロケーション精度の確保 （448 ページ）
ロケーション精度テストのスケジューリング （449 ページ）
オンデマンド ロケーション精度テストの実行 （451 ページ）

ロケーション精度テストのスケジューリング

不正でないクライアント、不正クライアント、干渉源、およびアセット タグの現在の位置の精度を確認するには、スケジュール設定された精度テストを使用します。**[精度テスト（Accuracy Tests）]** > **[結果（Results）]** でテスト結果の PDF を取得できます。[Scheduled Location Accuracy] レポートには、次の情報が含まれています。

- さまざまなエラー範囲内の要素の割合を説明する概要の位置精度レポート。
- エラー距離ヒストグラム。
- 累積エラー分布グラフ。

- エラー距離経時グラフ。
- 位置精度がテストされた各MACアドレスの概要（実際の位置とエラー距離の記載付き）、および各 MAC の空間精度（実際の位置対計算された位置）と経時的エラー距離を示すマップの概要が表示されます。

ロケーション精度テストをスケジュール設定するには、次の手順を実行します。

手順の概要

1. **[モニタ（Monitor）] > [ツール（Tools）] > [ロケーション精度（Location Accuracy）]** を選択します。
2. [コマンドの選択（Select a Command）] ドロップダウン リストから [新規のスケジュール設定された精度テスト（New Scheduled Accuracy Test）] を選択します。
3. テスト名を入力します。
4. 対応するドロップダウン リストからエリア タイプ、ビルディング、およびフロアを選択します。
5. 日、時、分を入力して、テストの開始時間および終了時間を選択します。時間は、24 時間表記で入力します。
6. テスト結果の宛先を選択します。（電子メール オプションを選択する場合は、まず目的の電子メール アドレスの SMTP メール サーバを定義する必要があります。[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] > [メール サーバ設定（Mail Server Configuration）] を選択して、適切な情報を入力します）。
7. [Position Test Points] をクリックします。
8. フロアマップで、位置精度を確認する各クライアント、タグ、および干渉源の隣のチェックボックスをオンにします。
9. （任意）一覧表示されないクライアント、タグ、または干渉源の MAC アドレスを入力するには、[Add New MAC] チェックボックスをオンにして MAC アドレスを入力し、[Go] をクリックします。
10. すべての要素が配置されたら、[保存（Save）] をクリックします。
11. [OK] をクリックして、確認ダイアログボックスを閉じます。
12. テスト結果を確認するには、テスト名をクリックし、表示されるページで [Results] タブをクリックして、[Saved Report] の下の [Download] をクリックします。

手順の詳細

ステップ 1 **[モニタ（Monitor）] > [ツール（Tools）] > [ロケーション精度（Location Accuracy）]** を選択します。

ステップ 2 [コマンドの選択（Select a Command）] ドロップダウン リストから [新規のスケジュール設定された精度テスト（New Scheduled Accuracy Test）] を選択します。

ステップ 3 テスト名を入力します。

ステップ 4 対応するドロップダウン リストからエリア タイプ、ビルディング、およびフロアを選択します。

（注） キャンパスは、デフォルトでルート領域として設定されています。この設定を変更する必要はありません。

ステップ 5 日、時、分を入力して、テストの開始時間および終了時間を選択します。時間は、24 時間表記で入力します。

（注） テスト開始時間を入力する場合には、マップ上にテストポイントを配置するためにテスト開始前に十分な時間があることを確認します。

ステップ 6 テスト結果の宛先を選択します。（電子メール オプションを選択する場合は、まず目的の電子メール アドレスの SMTP メール サーバを定義する必要があります。[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] > [メール サーバ設定（Mail Server Configuration）] を選択して、適切な情報を入力します）。

ステップ 7 [Position Test Points] をクリックします。

ステップ 8 フロア マップで、位置精度を確認する各クライアント、タグ、および干渉源の隣のチェックボックスをオンにします。

[MAC Address] チェックボックスをオンにすると、2 つのアイコンがマップに表示されます。一方のアイコンは実際の位置を表し、もう一方のアイコンは報告された位置を表しています。要素の実際の位置が報告された位置と同じではない場合、その要素の実際の位置アイコンをマップ上の正しい位置にドラッグします。（報告された位置はドラッグできません。）

ステップ 9 （任意）一覧表示されないクライアント、タグ、または干渉源の MAC アドレスを入力するには、[Add New MAC] チェックボックスをオンにして MAC アドレスを入力し、[Go] をクリックします。

新しく追加された要素のアイコンがマップに表示されます。要素が別のフロアのロケーション サーバ上にある場合は、左端の隅（0,0 の位置）にアイコンが表示されます。

ステップ 10 すべての要素が配置されたら、[保存（Save）] をクリックします。

ステップ 11 [OK] をクリックして、確認ダイアログボックスを閉じます。

[Accuracy Tests] 概要ページに戻ります。

ステップ 12 テスト結果を確認するには、テスト名をクリックし、表示されるページで [Results] タブをクリックして、[Saved Report] の下の [Download] をクリックします。

関連トピック

ロケーション精度ツールによる AP ロケーション精度の確保 （448 ページ）
AP ロケーション精度ツールのセットアップ （448 ページ）
オンデマンド ロケーション精度テストの実行 （451 ページ）

オンデマンド ロケーション精度テストの実行

要素はアソシエートされているが事前に配置されていない場合に、オンデマンド精度テストを実行できます。オンデマンドテストを使用すると、多数のさまざまな位置のクライアント、タグ、および干渉源の位置精度をテストできます。通常は、少数のクライアント、タグ、干渉源の位置精度をテストするために使用します。[精度テストの結果（Accuracy Tests Results）] でテスト結果の PDF を取得できます。[On-Demand Accuracy] レポートには、次の情報が含まれています。

- さまざまなエラー範囲内の要素の割合を説明する概要の位置精度レポート。
- エラー距離ヒストグラム。
- 累積エラー分布グラフ。

オンデマンド精度テストを実行するには、次の手順を実行します。

ステップ 1 **[モニタ（Monitor）] > [ツール（Tools）] > [ロケーション精度（Location Accuracy）]** を選択します。

ステップ 2 [コマンドの選択（Select a command）] ドロップダウン リストから、[新規のオンデマンド精度テスト（New On demand Accuracy Test）] を選択します。

ステップ 3 テスト名を入力します。

ステップ 4 対応するドロップダウン リストからエリア タイプ、ビルディング、およびフロアを選択します。

（注） キャンパスは、デフォルトでルート領域として設定されています。この設定を変更する必要はありません。

ステップ 5 テスト結果の宛先を選択します。（電子メール オプションを選択する場合は、まず目的の電子メール アドレスの SMTP メール サーバを定義する必要があります。**[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] > [メール サーバ設定（Mail Server Configuration）]** を選択して、適切な情報を入力します）。

ステップ 6 [Position Test Points] をクリックします。

ステップ 7 特定の位置の位置精度と RSSI をテストするには、左側のドロップダウン リストからクライアント、タグ、または干渉源を選択します。選択したオプション（クライアント、タグ、または干渉源）のすべての MAC アドレスのリストが、右側のドロップダウン リストに表示されます。

ステップ 8 ドロップダウン リストから MAC アドレスを選択し、赤色の十字線をマップ位置に移動して、マウスをクリックして配置します。

ステップ 9 [Zoom percentage] ドロップダウン リストから、マップのズーム パーセンテージを選択します。

[X]および[Y]テキスト ボックスには、マップ内の赤色の十字線の位置に基づいて座標が入力されます。

ステップ 10 [開始（Start）]をクリックして精度データの収集を開始し、[停止（Stop）]をクリックして収集を終了します。テストを終了する前に少なくとも 2 分間テストを実行してください。

ステップ 11 マップ上にプロットする各テスト ポイントについてステップ 7 ～ステップ 10 を繰り返します。

ステップ 12 テストポイントのマッピングを終了したら [結果の分析（Analyze Results）]をクリックし、そのページの [結果（Results）] タブをクリックするとレポートが表示されます。

関連トピック

ロケーション精度ツールによる AP ロケーション精度の確保 （448 ページ）
AP ロケーション精度ツールのセットアップ （448 ページ）
ロケーション精度テストのスケジューリング （449 ページ）

IPSLA のモニタリング

IPSLA リアルタイム モニタリングを実装するには、次の手順を実行します。

始める前に

[IPSLA リアル タイム モニタリング（IPSLA Real Time Monitoring）] ページでは、ユーザーがデバイスを分析およびモニタして、応答時間、パケット損失、アプリケーションのパフォーマンスなどのパラメータに関する詳細情報を抽出することができます。

ステップ 1 **[モニタ（Monitor）]** > **[ツール（Tools）]** > **[IPSLA リアル タイム モニタリング（IPSLA Real Time Monitoring）]** に移動します。

ステップ 2 [**開始 (Begin)**] ページの [**次へ (Next)**] ボタンをクリックします。

ステップ 3 ソースおよび宛先デバイスを選択します。デバイス名に基づいてデバイスをフィルタリングできます。

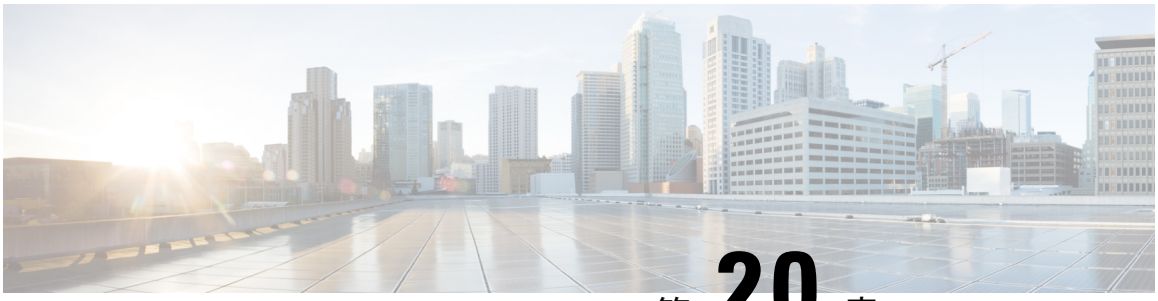
ソースおよび宛先デバイスは同じにできません。

ステップ 4 **[オペレーション タイプ（Operation Type）]** を選択します。**UDP エコー** または **UDP ジッター** として動作タイプを選択する場合は、ポート番号を入力する必要があります。値は 1 ～ 65535 までで指定する必要があります。**[HTTP/TCP]** としてオペレーション タイプを選択した場合は、有効な URL を入力します。

ステップ 5 選択内容を破棄するには、**[選択を消去（Clear Selections）]** ボタンをクリックします。

ステップ 6 モニタリング チャートを表示するには、**[次へ（Next）]** ボタンをクリックします。チャートは 1 分ごとに再生成されます。キャプチャの数が 10 に達すると、以前のデータがチャートから消え、最新のキャプチャ情報が表示されます。

（注） データを保存せずに **[開始（Begin）]** ページに移動する場合は、更新アイコンをクリックします。



第 20 章

パフォーマンス グラフを使用したワイヤレスおよびデータセンターのパフォーマンスのモニタ

デバイスとインターフェイスの主要業績評価指標（KPI）を比較するには、**[モニタ（Monitor）]> [モニタリングツール（Monitoring Tools）] > [パフォーマンスグラフ（Performance Graphs）]** を選択します。指定した時間にわたって表示させるデバイスまたはインターフェイスのメトリックを選択できます。これにより、パフォーマンス グラフでパフォーマンスを迅速にモニタできます。

- パフォーマンス グラフの作成 （455 ページ）
- パフォーマンス グラフのオプション （457 ページ）

パフォーマンス グラフの作成

ステップ 1 **[モニタ（Monitor）]> [モニタリング ツール（Monitoring Tools）] > [パフォーマンス グラフ（Performance Graphs）]** を選択します。

このページに初めてアクセスしたときに、オーバーレイ ヘルプ ウィンドウに有用な情報が表示されます。

ステップ 2 左フレームの上部にある次のいずれかのタブを選択します。

- [Devices]：パフォーマンス グラフを作成するデバイスを選択できます。
- [Interfaces]：パフォーマンス グラフを作成するインターフェイスを選択できます。

選択内容に応じて、そのデバイスタイプまたはインターフェイスタイプの使用可能なメトリックが [Metrics] パネルに表示されます。

ステップ 3 パフォーマンスを測定するメトリックの上にカーソルを移動し、メトリックをクリックしてウィンドウの [Graphs] 部分にドラッグします。

オーバーレイ ヘルプ ウィンドウに、アイコン、日付範囲、その他の情報に関する説明が表示されます。

関連トピック

1 つのパフォーマンス グラフにおける複数のメトリックの表示 （456 ページ）
パフォーマンス グラフのオプション （457 ページ）

1 つのパフォーマンス グラフにおける複数のメトリックの表示

1 つのパフォーマンス グラフに複数のメトリックを表示したい場合もあります。たとえば、CPU使用率のスパイクを表示する際に、パフォーマンス グラフにメモリ使用率を追加し、CPU使用率の変化によりメモリ使用率が影響を受けたかどうか確認する場合などです。

1 つのパフォーマンス グラフに最大 10 個のメトリックを追加できます。

（注） Prime Infrastructure は、ファブリック インターコネクトを使用する UCS デバイスのインターフェイスをモニタしません。したがって、Tx および Rx の使用率の詳細は、**[パフォーマンス グラフ（Performance details）]** 画面に表示されません。

ステップ 1 **[モニタ（Monitor）] > [モニタリング ツール（Monitoring Tools）] > [パフォーマンス グラフ（Performance Graphs）]** を選択します。

ステップ 2 左フレームの上部にある次のいずれかのタブを選択します。

- [Devices]：パフォーマンス グラフを作成するデバイスを選択できます。
- [Interfaces]：パフォーマンス グラフを作成するインターフェイスを選択できます。

選択内容に応じて、そのデバイス タイプまたはインターフェイス タイプの使用可能なメトリックが [Metrics] パネルに表示されます。

ステップ 3 パフォーマンスを測定するメトリックの上にカーソルを移動し、メトリックをクリックしてウィンドウの [Graphs] 部分にドラッグします。

ステップ 4 同じグラフに2つ目のメトリックを追加するには、追加するメトリックの上にカーソルを移動し、メトリックをクリックして、前のステップでメトリックを追加した同じグラフまでドラッグします。

1 つのグラフで複数のメトリックを使用したくない場合は、[Graphs] ウィンドウ下部の [Drop item here] と表示されている個所にメトリックをドラッグすると、同じページに新しいグラフを作成できます。

ステップ 5 [Device 360° View] を起動するには、グラフの上部にある IP アドレスのハイパーリンクをクリックします。

関連トピック

パフォーマンス グラフの作成 （455 ページ）
パフォーマンス グラフのオプション （457 ページ）

パフォーマンス グラフのオプション

パフォーマンス チャートの上部にある [Show] メニューを使用して、次のグラフ表示オプションを変更することができます。

- [Legend Options]：凡例の表示または非表示を指定します。
- [Show Legends]：凡例をパフォーマンス チャートの右側に表示するか、上部に表示するかを指定します。
- [Show Alarms]：アラームを表示するかどうかを指定します。色付きのフラグがパフォーマンス グラフに表示され、その時点でアラームが発生したことが示されます。アラームの詳細を表示するには、色付きのフラグをクリックします。
- [設定変更の表示（Show Config Changes）]：設定変更を表示するかどうかを指定します。デバイスの設定がその時点で変更されたことを示す黒いフラグがパフォーマンス グラフに表示されます。設定変更の詳細を表示するには、フラグをクリックします。

また、グラフの上部にある矢印をクリックすると、パフォーマンス グラフをエクスポートして印刷できます。

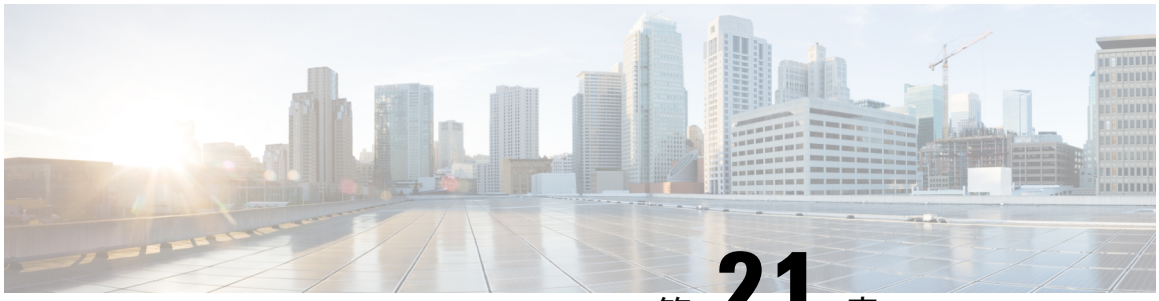
パフォーマンス グラフ ページの右上にある [Detach] をクリックし、新しいブラウザ ウィンドウにパフォーマンス グラフを表示します。これにより、一方のウィンドウで操作を実行しながら、もう一方のウィンドウでパフォーマンス グラフを引き続きモニタできます。

各タブで最大 10 個のチャートを作成し、各チャートで最大 7 つのシリーズを作成できます。チャートまたはシリーズをこれ以上追加しても表示されず、警告メッセージが表示されます。別のチャートを追加するには、新しいタブを追加し、新しいタブで描画する新たなチャートを追加します。

親グループを 7 回以上描画すると、それらは 1 つのチャートに描画され、グループ全体のデータを表示できます。

関連トピック

パフォーマンス グラフの作成 （455 ページ）
1 つのパフォーマンス グラフにおける複数のメトリックの表示 （456 ページ）



第 21 章

トラブルシューティング

Cisco Prime Infrastructure は、エンドユーザのネットワーク アクセスをモニタリングしてトラブルシューティングするために以下の高度な機能を備えています。

以下の項では、いくつかの一般的なトラブルシューティング タスクについて説明します。

- シスコ サポート コミュニティとテクニカル アシスタンス センター（TAC）から支援を受ける （459 ページ）
- ユーザの問題に関するトラブルシューティング （461 ページ）
- アプリケーションとそのパフォーマンスのモニタ （465 ページ）
- ワイヤレス デバイスのパフォーマンスの問題のトラブルシューティング （465 ページ）
- 物理および仮想データセンター コンポーネントの根本原因およびインパクト分析 （466 ページ）

シスコ サポート コミュニティとテクニカル アシスタンス センター（TAC）から支援を受ける

- シスコ サポート ケースの登録 （459 ページ）
- シスコ サポート コミュニティへの参加 （460 ページ）

シスコ サポート ケースの登録

Web GUI からサポート ケースを登録すると、Prime Infrastructure ではデバイスから取得できる情報が、このケース フォームに自動的に読み込まれます。これには、デバイスの技術的な詳細、デバイスでの設定変更、および過去 24 時間以内に発生したすべてのデバイス イベントなどがあります。また、ケースに各自のファイルを添付することもできます。

始める前に

次の状況では、Web GUI でサポート ケースを登録できます。

- 管理者により、ユーザがこの作業を実行できるように Prime Infrastructure が設定されている。『Cisco Prime Infrastructure Administrator Guide』の「*Set Up Defaults for Cisco Support Requests*」を参照してください。
- Prime Infrastructure サーバがインターネットに直接接続しているか、またはプロキシ サーバ経由で接続している。
- Cisco.com のユーザ名とパスワードがある。

ステップ 1 次のいずれかを実行します。

- **[モニタ（Monitor）]** > **[モニタリング ツール（Monitoring Tools）]** > **[アラームおよびイベント（Alarms and Events）]** の順に選択します。アラームを 1 つクリックし、**[トラブルシュート（Troubleshoot）]** > **[サポート ケース（Support Case）]** を選択します。[トラブルシュート（Troubleshoot）] ボタンが表示されない場合は、ブラウザ ウィンドウを拡大します。
- [デバイス 360（Device 360）] ビューで、次の手順に従います。デバイスの IP アドレスの上にマウスを移動し、情報アイコンをクリックします。[アクション（Actions）] ドロップダウン メニューから [サポート リクエスト（Support Request）] を選択します。

ステップ 2 Cisco.com ユーザ名とパスワードを入力します。

ステップ 3 [作成（Create）] をクリックします。Prime Infrastructure は、デバイスから取得したデータをフォームに読み込みます。

ステップ 4 （オプション）組織のトラブル チケット システムに対応したトラッキング番号を入力します。

ステップ 5 [次へ（Next）] をクリックして、問題の説明を入力します。

Prime Infrastructure では、デバイスから取得したデータがフォーム読み込まれ、必要なサポート ドキュメントが自動的に生成されます。

必要に応じて、ローカル マシンからファイルをアップロードします。

ステップ 6 [サービス リクエストの作成（Create Service Request）] をクリックします。

シスコ サポート コミュニティへの参加

オンライン シスコ サポート コミュニティ内のディスカッション フォーラムにアクセスして、参加できます。Cisco.com のユーザ名とパスワードが必要です。

ステップ 1 次のいずれかを実行します。

- **[Monitor] [>] [Monitoring Tools] [>] [Alarms and Events]** に移動します。いずれかのアラームをクリックし、**Troubleshoot > Support Forum** を選択します。**[Troubleshoot]** ボタンが表示されない場合は、ブラウザ ウィンドウの幅を広げてください。

- [デバイス 360（Device 360）] ビューで、次の手順に従います。デバイスの IP アドレスの上にマウスを移動し、情報アイコンをクリックします。[アクション（Actions）] ドロップダウン メニューから、[サポート コミュニティ（Support Community）] を選択します。

ステップ 2 シスコ サポート コミュニティ フォーラムのページで、必要な情報を見つけるための検索パラメータを入力します。

ユーザの問題に関するトラブルシューティング

[ユーザ 360° ビュー（User 360° View）] を使用して、ユーザから報告された問題をトラブルシューティングできます。

ステップ 1 任意のページの [検索（Search）] フィールドで、エンドユーザの名前を入力します。

ステップ 2 [検索結果（Search Results）] ウィンドウで、[ユーザ名（User Name）] 列のエンドユーザ名にマウス カーソルを移動し、[ユーザ 360 度ビュー（User 360° View）] アイコンをクリックします。[ユーザ360度ビュー（User 360° View）] からのユーザ詳細の取得 （1126 ページ）を参照してください。

ステップ 3 表示された [ユーザ 360 度ビュー（User 360° View）] で、次のテーブルで説明する情報を使用して問題の発生個所を特定します。

収集するデータ	[User 360° View] でクリックする項目	その他の情報
ユーザが接続しているデバイスに関する情報（エンドポイント、場所、接続、セッション情報など）。	[User 360° View] の上部にあるデバイスアイコンをクリックします。	追加情報を表示するには使用可能なリンクをクリックします。たとえば、ISE を起動するには [Authorization Profile] リンクをクリックします。 エンドユーザが適切なポリシー カテゴリに関連付けられていない場合は、（ISE 管理者、ヘルプ技術者などに）問題を引き継ぐか、Prime Infrastructure の外部でアクションを実行して、ユーザが現在のポリシー カテゴリ（許可プロファイル）に分類されている理由を調査できます。 認証エラーの兆候を調べます（認証の失敗は、パスワードの期限切れなど、さまざまな原因で発生します）。認証エラーは視覚的に表示されるので、エラーに関する詳細を確認できます。この時点で、（ISE 管理者、ヘルプ テクニカルなどに）問題を引き渡すことが必要になる場合があります。
ユーザが接続しているデバイスに関連するアラーム	[User 360° View] の上部にあるデバイス アイコンをクリックし、[Alarms] タブをクリックします。	[クライアントのトラブルシュート（Troubleshoot Client）] アイコン（）をクリックして、クライアントのトラブルシューティングに移動します。

収集するデータ	[User 360° View] でクリックする項目	その他の情報
ユーザが接続しているデバイスで実行中のアプリケーションとサイトの帯域幅使用率	[User 360° View] の上部にあるデバイス アイコンをクリックし、[Applications] タブをクリックします。	特定ユーザのフィルタリングしたエンドユーザデータを表示するには、アプリケーションをクリックします。 アプリケーションの詳細情報を表示するには、[ダッシュボード（Dashboard）] > [パフォーマンス（Performance）] > [アプリケーション（Application）] を選択します。 エンドユーザが消費しているアプリケーションの帯域幅使用率（カンバセーションで消費される帯域幅）など、アプリケーションに関する詳細情報を表示するには、[ダッシュボード（Dashboard）] > [パフォーマンス（Performance）] > [アプリケーション（Application）] を選択します。 （注） この機能を使用するための要件： • ISE サーバとの統合（エンドポイント情報にアクセスするため）。 • 有線セッションの場合は、その AAA アカウンティング情報が ISE に送信されます。 • セッション情報（NetFlow/NAM データ、保証ライセンス）が使用可能であること。

収集するデータ	[User 360° View] でクリックする項目	その他の情報
サイトのネットワークデバイスに関する情報	ユーザ 360°ビューの上部にあるデバイスアイコンをクリックし、[アラーム（Alarms）]タブをクリックします。	次のいずれかを選択して表示できます。 • サイトのアクティブアラームのリスト • すべてのサイトデバイスのリスト（アラーム表示付き） • サイトのトポロジマップ（アラーム表示付き） サイトの問題が検出済みの場合は、サイトロケーションの横にアラームアイコンが表示されます。そのサイトに関連するアラームをすべて表示するには、アイコンをクリックします。 問題が検出済みで、トラブルシューティングを続行することが適切でない場合は、現状を記録して、次の段階のサポートに引き渡すだけで十分です。クライアントの詳細なトラブルシューティングを続行する場合は、[ユーザ 360 度ビュー（User 360° View）] を終了し、クライアントとユーザの完全なトラブルシューティングページを起動します（[モニタ（Monitor）] > [モニタリング ツール（Monitoring Tools）] > [クライアントおよびユーザ（Clients and Users）] を選択）。
ネットワーク接続デバイスに関する情報	ユーザ 360°ビューの上部にあるデバイスアイコンをクリックし、[アラーム（Alarms）]タブをクリックします。	[クライアントの詳細に移動（Go to Client Details）] アイコンをクリックします。

アプリケーションとそのパフォーマンスのモニタ

エンドユーザがネットワーク上で実行している特定のアプリケーションに関連する問題がないかどうか、その兆候を調べるには次の手順を実行します。

はじめる前に

この機能を使用するための要件：

- ISE サーバとの統合（エンドポイント情報にアクセスするため）。
- セッション情報（NetFlow/NAM データ、保証ライセンス）が使用可能であること。

ステップ 1 エンドユーザがアクセスしているアプリケーション、およびそのユーザのデバイスに対するアプリケーションの応答時間を表示するには、ユーザの [User 360° View] を開き、[Applications] タブをクリックします。

ステップ 2 このタブには、次の情報が表示されます。

1. エンドポイント
2. MAC アドレス
3. アプリケーション
4. 直近 1 時間のボリューム（MB 単位）

アプリケーションの詳細情報を表示するには、[Dashboard] > [Performance] > [Application] を選択します。

ワイヤレスデバイスのパフォーマンスの問題のトラブルシューティング

エンドユーザからワイヤレス デバイスの問題が報告された場合は、[Site] ダッシュボードを使用して、問題が発生している AP を判別できます。

はじめる前に

この機能を使用するには、セッション情報（Netflow/NAMデータ、保証ライセンス）が使用可能である必要があります。

ステップ 1 [Dashboard] > [Performance] > [Site] を選択して、問題が発生したクライアントが属するサイトを表示します。

ステップ 2 このサイトの問題が発生している AP を表示するには、[設定（Settings）] アイコンをクリックし、[最もビジーなアクセス ポイント（Busiest Access Points）] の横にある [追加（Add）] をクリックします。

ステップ 3 [Busiest Access Points] ダッシュレットまでスクロール ダウンします。次のことを行えます。

1. デバイス情報を表示するデバイスの上にマウスを移動します。[デバイス360度ビュー（Device 360° View）] からのデバイス詳細の取得 （1121 ページ）を参照してください。
2. AP 名をクリックして [AP] ダッシュボードに移動すると、AP フィルタリング オプションを使用して、クライアント数やチャネル使用率などの AP の詳細を表示できます。さらに、保証ライセンスを所有している場合は、上位 N のクライアントと上位 *N* のアプリケーションも表示できます。

- AP の SNMP ポーリングに基づく使用率。
- 保証ライセンスがある場合は、Assurance NetFlow データに基づくボリューム情報。たとえば、AP ごとのトラフィック量を表示できます。

物理および仮想データセンターコンポーネントの根本原因およびインパクト分析

物理サーバは、Prime Infrastructure によって管理されている UCS B シリーズおよび C シリーズ サーバのリストを表示します。また、これらのサーバで稼動しているホスト/ハイパーバイザも表示されます（ただし対応する vCenter が追加されている場合のみ）。

Cisco UCS Server Schematic は、UCS デバイスの完全なアーキテクチャを表示します。[Schematic] タブに拡大可能なグラフが表示され、シャーシやブレードなど、UCS デバイスのさまざまな要素が示されます。シャーシまたはブレードの横にある動作ステータス アイコンにマウスを移動すると、要素の概要を表示できます。また、各要素（シャーシまたはブレード）を記号化した動作ステータス アイコンをクリックすると、後続の接続が表示されます。ホストとその VM が Prime Infrastructure によって管理されている場合は、動作ステータス アイコンをクリックすると、それらとの接続を確認できます。[概略図（Schematic）] ビューには、データセンター コンポーネントの動作ステータスと関連アラームもまた表示されます。これらを使用してアプリケーション配信エラーの根本原因をトレースし、Cisco UCS デバイスの UCS ハードウェア問題を特定することができます。

UCS デバイスのハードウェアの問題のトラブルシューティング

アプリケーション配信エラーの根本原因をトレースして、Cisco UCS B シリーズや C シリーズ サーバの UCS ハードウェアの問題を特定するには、次の手順を実行します。ファブリック インターコネクト ポート、シャーシまたはブレードのいずれに問題があるかを特定できます。

UCS シャーシ、ブレード サーバ、ファブリック インターコネクト ポートにおける問題を特定するには：

ステップ 1 [インベントリ（Inventory）] > [デバイス管理（Device Management）] > [コンピューティング デバイス（Compute Devices）] を選択します。

ステップ 2 [コンピューティング デバイス（Compute Devices）] ペインで [Cisco UCS サーバ（Cisco UCS Servers）] を選択します。

ステップ 3 [Cisco UCS サーバ（Cisco UCS Servers）] ペインで、障害がある UCS デバイスをクリックして [概略図（Schematic）] タブを開き、UCS シャーシとブレードの相互接続、シャーシおよびブレード サーバのアップ/ダウン ステータスを表示します。障害があるシャーシまたはブレード サーバ名にマウスを重ねて、要素の [クイック サマリ（Quick Summary）] を表示します。

障害があるシャーシまたはブレード サーバの詳細情報を表示するには、[360 度表示（View 360）] をクリックします。

ステップ 4 [シャーシ（Chassis）] タブをクリックして、障害があるシャーシの名前の上にマウス カーソルを移動し、情報アイコンをクリックして [シャーシ 360 度 ビュー（chassis 360° view）] を起動し、電源装置とファン モジュールのアップ/ダウン ステータスを表示します。

ステップ 5 [サーバ（Servers）] タブをクリックして、障害があるブレード サーバの名前の上にマウス カーソルを移動し、情報アイコンをクリックして [サーバ 360 度 ビュー（Server 360° View）] を起動します。

[サーバ 360° ビュー（Server 360° View）] には、プロセッサの数、メモリ容量、アダプタのアップ/ダウン ステータス、ネットワーク インターフェイス カード（NIC）、ホスト バス アダプタ（HBA）およびサービス プロファイルなど、ブレード サーバの詳細情報が表示されます。

ステップ 6 [ネットワーク（Network）] タブをクリックし、ポート チャネル、イーサネット インターフェイス、vEthernet、vFabric チャネルなど、ファブリック インターコネクトのネットワーク インターフェイス全体の詳細を表示します。

ステップ 7 [IO モジュール（IO Modules）] タブをクリックし、バックプレーン ポートとファブリック ポートの動作ステータスを表示します。

ステップ 8 [サービス プロファイル（Service Profile）] タブをクリックすると、サービスに影響を与えるハードウェアの障害が表示されます。

ステップ 9 左側の [サービス プロファイル（Service Profile）] ペインで、展開アイコンをクリックしてサービス プロファイルを表示します。

ステップ 10 サービス プロファイルに対応する情報アイコンをクリックし、そのサービス プロファイルのアラーム重大度レベルを表示します。

ステップ 11 左側の [サービス プロファイル（Service Profile）] ペインで障害があるサービス プロファイルをクリックし、[サービス プロファイル（Service Profile）] テーブルを表示します。ここにはプロファイル名、サービス プロファイル テンプレート、サーバ、全体のステータス、関連付けられたステータスおよび関連付けられたアラームが表示されます。

ステップ 12 [サービス プロファイル（Service Profile）] テーブルでプロファイル名に対応する情報アイコンをクリックすると、サービス プロファイルの基本の概要情報を示す [サービス プロファイル 360° ビュー（Service Profile 360° view）] が起動します。

ファブリック インターコネクト ポートでの帯域幅の問題の特定

ステップ 1 [インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ネットワーク デバイス（Network Devices）] を選択します。

ステップ 2 [All Devices] ペインで障害がある UCS デバイスをクリックします。

ステップ 3 ファブリック インターコネクト スイッチに対応する展開アイコンをクリックします。

ステップ 4 [固定モジュール（Fixed Modules）] をクリックし、ファブリック インターコネクト ポートの動作ステータスを表示します。

ステップ 5 [Interfaces] をクリックし、ファブリック インターコネクト ポートとインターフェイスの動作ステータスを表示します。これは、[Compute Devices] ページの [Network] タブで表示されるファブリック インターコネクト ポートとインターフェイスの動作ステータスと同じです。

UCS デバイスの帯域幅の問題のトラブルシューティング

[Overview] および [Performance] ダッシュボードの [Top-N Interface Utilization] ダッシュレットを使用すると、ファブリック インターコネクト ポートまたはファブリック インターコネクト ポート グループの詳細を表示できます。ファブリック インターコネクトを UCS シャーシに接続しているポートでの過剰な帯域幅使用が、Cisco UCS の低速化などのアプリケーション パフォーマンスの問題を引き起こしているかどうかを確認するには、次の手順を実行します。

帯域幅使用率の詳細を表示するには、ファブリック インターコネクト ポート グループを作成し、ダッシュレットでそのポート グループを選択することを推奨します。

ファブリック インターコネクト ポートでの過剰な帯域幅使用を確認するには：

ステップ 1 [ダッシュボード（Dashboard）] > [パフォーマンス（Performance）] > [インターフェイス（Interface）] を選択し、[インターフェイス（Interface）] ドロップダウン リストから UCS デバイス インターフェイスを選択します。

または

[Dashboard] > [Overview] > [Network Interface] を選択します。

ステップ 2 示されているように [設定（Settings）] アイコンをクリックし、[ダッシュレットを追加（Add Dashlets）] を選択します。

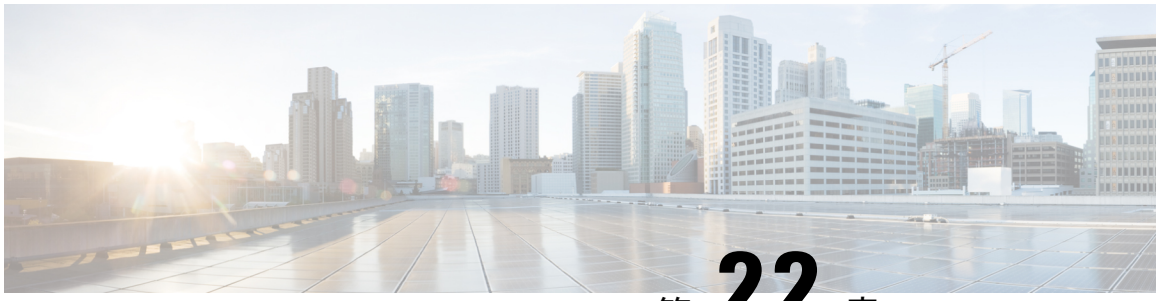
ステップ 3 [トップ N のインターフェイス使用率（Top N Interface Utilization）] ダッシュレットを選択し、[追加（Add）] をクリックします。

ステップ 4 ファブリック インターコネクト ポート グループが作成済みの場合は、次の手順を実行します。

a) [トップ N のインターフェイス使用率（Top N Interface Utilization）] ダッシュレットで [ダッシュレット オプション（Dashlet Options）] アイコンをクリックします。

b) [ポート グループ（Port Group）] でファブリック インターコネクト ポート グループを選択し、[保存して閉じる（Save and Close）] をクリックします。

[トップ N のインターフェイス使用率（Top N Interface Utilization）] ダッシュレットに、使用率が最大のインターフェイスのリストが表示されます。このダッシュレットには、ファブリック インターコネクト ポートの平均データ送受信と最大データ送受信の詳細も表示されます。



第 22 章

オペレーション センターを使用した複数の Prime Infrastructure インスタンスのモニタ

- 複数の Cisco Prime Infrastructure インスタンスのモニタ方法 （469 ページ）
- オペレーション センターの構成ダッシュボードを使用した複数の Cisco Prime Infrastructure サーバの管理 （470 ページ）
- オペレーション センターを使用した複数の Cisco Prime Infrastructure サーバを含む展開でのレポートの実行 （482 ページ）

複数の Cisco Prime Infrastructure インスタンスのモニタ方法

ネットワークを管理するために複数の Cisco Prime Infrastructure サーバ インスタンスを使用する必要がある状況が 3 つあります。

- ネットワーク内のデバイスを論理グループに分類し、別の Cisco Prime Infrastructure インスタンスにそれぞれのグループを管理させる場合。たとえば、1 つのインスタンスでネットワーク内のすべての有線デバイスを管理し、別のインスタンスですべてのワイヤレスデバイスを管理することができます。
- ネットワークを管理するには実行している 1 つの Cisco Prime Infrastructure インスタンスで十分だが、1つ以上のインスタンスを追加すると、複数のインスタンス間でCPUとメモリの負荷が分散されることで、Cisco Prime Infrastructure のパフォーマンスが向上する場合。
- ネットワークに世界中に配置されたサイトがあり、データを個別に保持するために異なる Cisco Prime Infrastructure インスタンスにそれぞれのサイトを管理させたい場合。

ネットワークで複数の Cisco Prime Infrastructure インスタンスが実行されている場合は、オペレーションセンターからそれらのインスタンスをモニタできます。この章では、オペレーションセンターを使用する場合に使用できる標準ワークフローについて説明します。このワークフローは、次の作業で構成されます。

- オペレーション センターの構成ダッシュボードを使用した複数の Cisco Prime Infrastructure サーバの管理
- オペレーション センターを使用した複数の Cisco Prime Infrastructure サーバを含む展開でのレポートの実行

詳細については、次の関連項目を参照してください。

関連トピック

オペレーション センターを使用した複数の Cisco Prime Infrastructure サーバを含む展開でのレポートの実行 （482 ページ）
オペレーション センターの構成ダッシュボードを使用した複数の Cisco Prime Infrastructure サーバの管理 （470 ページ）
よくある質問：オペレーション センターと Prime Infrastructure （1161 ページ）

オペレーションセンターの構成ダッシュボードを使用した複数の Cisco Prime Infrastructure サーバの管理

オペレーションセンターで使用可能なさまざまなダッシュボードを表示した後は、ネットワークで何が起こっているかをより詳しく確認することができます。特に、以下についてモニタできます。

- ネットワークに属するデバイス。
- それらのデバイスを管理する Cisco Prime Infrastructure サーバ。
- ネットワークで発生したアラーム、イベント、およびその他のインシデント。
- ネットワークを使用するように設定されたクライアントおよびユーザ。

次の関連項目では、これらの項目についてさらに詳しく説明します。

関連トピック

オペレーション センターによるすべての Cisco Prime Infrastructure サーバの管理対象デバイスの表示 （472 ページ）
オペレーション センターを使用した複数の Cisco Prime Infrastructure サーバを含む展開での仮想ドメインの使用 （474 ページ）
オペレーション センターを使用した Prime Infrastructure サーバの管理 （478 ページ）
オペレーション センターを使用した複数の Prime Infrastructure サーバのステータスの表示 （479 ページ）
オペレーション センターを使用した複数の Prime Infrastructure サーバのソフトウェア アップデートの表示
オペレーション センターによる複数の Cisco Prime Infrastructure サーバによって管理されるデバイスでのアラームの表示 （481 ページ）
オペレーション センターによる複数の Cisco Prime Infrastructure サーバの管理対象クライアントおよびユーザの表示 （482 ページ）

オペレーション センターを使用したデバイスの追加

Cisco Prime Infrastructure のオペレーション センターでは、オペレーション センターのユーザインターフェイスから 1 つ以上の管理対象インスタンスにデバイスを追加できます。デバイスを手動で追加するだけでなく、[一括インポート（Bulk Import）] オプションを使用してデバイスをインポートすることもできます。

ステップ 1 [モニタ（Monitor）] > [管理対象要素（Managed Elements）] > [ネットワークデバイス（Network Devices）] を選択します。

ステップ 2 デバイスを手動で追加するには、次の手順を実行します。

a) [ネットワーク デバイス（Network Devices）] テーブルの上にある ＋ アイコンをクリックし、[デバイスの追加（Add Device）] を選択します。

b) [デバイスの追加（Add Device）] ダイアログボックスで、デバイスを追加する Prime Infrastructure サーバを選択します。

c) 必要なフィールドに入力します。フィールドの横にある [?] をクリックすると、そのフィールドの説明が表示されます。

（注） ほとんどの Cisco NCS デバイスなどのデバイスには、Telnet/SSH 情報が必須です。

d) （任意）デバイスを追加する前にクレデンシャルを確認するには、[クレデンシャルの確認（Verify Credentials）] をクリックします。

Prime Infrastructure は、NAM デバイスに対してのみ、HTTP クレデンシャルの検証をサポートしています。

e) [追加（Add）] をクリックして、指定した設定でデバイスを追加します。

（注） ユーザ定義フィールド（UDF）パラメータが新しいデバイスに使用可能になるのは、最初に **[管理（Administration）]** > **[設定（Settings）]** > **[システム設定（System Settings）]** > **[インベントリ（Inventory）]** > **[ユーザ定義フィールド（User Defined Fields）]** を選択して UDF パラメータを追加した場合のみです。UDF フィールド パラメータには、特殊文字 : ; および # を使用しないでください。

ステップ 3 CSV ファイルを使用して別のソースからデバイスをインポートするには、次の手順を実行します。

a) [ネットワーク デバイス（Network Devices）] テーブルの上にある ＋ アイコンをクリックし、[一括インポート（Bulk Import）] を選択します。

b) [一括デバイスインポート（Bulk Device Import）] ダイアログボックスで、デバイスをインポートする Prime Infrastructure サーバを選択します。

c) [ファイルの選択（Choose File）] をクリックして、一括インポートするデバイスの詳細を含む CSV ファイルを選択します。

CSV ファイルの作成の詳細については、を参照してください。 デバイスのインポート CSV ファイルの作成 （44 ページ）

d) [Import] をクリックします。

1 つの Prime Infrastructure インスタンスから別の Prime Infrastructure インスタンスへのデバイスの移動

他の管理対象 Prime Infrastructure インスタンス間のロードバランシングのため、ある Prime Infrastructure インスタンスで管理されているデバイスを別の Prime Infrastructure インスタンスに移動することができます。

ステップ 1 **[モニタ（Monitor）] > [管理対象要素（Managed Elements）] > [Network Devices（ネットワーク デバイス）]** を選択します。

ステップ 2 [ネットワーク デバイス（Network Devices）] テーブルで、デバイスを選択し、[デバイスの移動（Move Device）] をクリックします。

ステップ 3 [デバイスの移動（Moving Devices）] ダイアログボックスで、デバイスの移動先の Prime Infrastructure サーバを選択します。

ステップ 4 [送信元サーバからのデバイスの削除（Remove device from source server）] チェックボックスをオンにし、[OK] をクリックします。

[送信元サーバからのデバイスの削除（Remove device from source server）] チェックボックスをオフにすると、デバイスは複数の Prime Infrastructure インスタンスで管理されますが、これは推奨されていません。

オペレーションセンターによるすべての Cisco Prime Infrastructure サーバの管理対象デバイスの表示

[モニタ（Monitor）] > [管理対象要素（Managed Elements）] > [ネットワークデバイス（Network Devices）] の順に選択して、オペレーション センターの [ネットワークデバイス（Network Devices）] ページを開きます。ここでは、Cisco Prime Infrastructure インスタンスが管理しているネットワークに属するすべてのデバイスの情報を表示できます。この情報には、デバイスのホスト名/IP アドレス、現在の到達可能性ステータス、およびインベントリ データがそのデバイスから正常に収集された最終時刻が含まれます。[デバイス360度（Device 360°）] ビューを起動して、Telnet、Ping、および Traceroute アクションを実行することもできます。

最初に [Network Devices] ページを開くと、すべてのネットワーク デバイスが表示されます。表示されるデバイスを絞り込むには、次のいずれかの操作を実行します。

- [デバイスグループ（Device Group）] ペインから、該当するデバイス タイプ、ロケーション、またはユーザー定義グループを選択し、サブグループまでドリルダウンします。いずれかのロケーション グループを選択すると、**[統合AP（Unified AP）]** タブおよび **[サードパーティ製AP（Third Party AP）]** タブを表示することもできます。

（注） Cisco Prime Infrastructure オペレーション センターでは、追加されたデバイスのグループがサポートされるようになりました。これには、アクセスポイント、その他の機能のダッシュボード、保護セキュリティ アプライアンス、およびスイッチが含まれます。その特定のグループに関連付けられているデバイスのリストを表示するには、いずれかのデバイス グループをクリックします。

- カスタム フィルタを適用するか、または [Show] ドロップダウン リストから定義済みフィルタの 1 つを選択します。オペレーション センターではカスタム フィルタが提供されており、それを使用して管理対象インスタンス全体で重複したデバイスを表示することができます。フィルタの使用方法の詳細については、関連項目「クイック フィルタ」を参照してください。
- 特定のデバイスを検索します。詳細については、関連項目「検索方法」を参照してください。
- 空のデバイス グループを非表示にするには、次の手順を実行します。
  - [管理（Administration）] > [システム設定（System Settings）] > [インベントリ（Inventory）] > [グループ化（Grouping）] の順に選択します。
  - [メンバーがいないグループを表示（Display groups with no members）] チェックボックスをオフにします。
  - [保存（Save）] をクリックします。

オペレーション センターの [ネットワークデバイス（Network Devices）] ページからデバイスを削除すると、そのデバイスをモニタしているすべての管理対象 Cisco Prime Infrastructure インスタンスからもデバイスが削除されます。

関連トピック

オペレーション センターの構成ダッシュボードを使用した複数の Cisco Prime Infrastructure サーバの管理 （470 ページ）
オペレーション センターを使用した複数の Cisco Prime Infrastructure サーバを含む展開での仮想ドメインの使用 （474 ページ）
クイック フィルタ （1115 ページ）
検索方法 （1129 ページ）

オペレーション センターを使用したデバイスの同期

Prime Infrastructure オペレーション センター データベースを Prime Infrastructure デバイスで実行中の設定と同期するために、インベントリ収集を実行できます。

デバイスを同期するには、次の手順に従います。

ステップ 1 **[モニタ（Monitor）] > [管理対象要素（Managed Elements）] > [Network Devices（ネットワーク デバイス）]** を選択します。

ステップ 2 Prime Infrastructure オペレーション センター データベースに保存されている設定と同期する設定を持つデバイスを選択します。

ステップ 3 [同期（Sync）] をクリックします。

（注） 同期されたデバイスがデフォルト/管理 VDC の場合は、すべての子 VDC のすべての設定が自動的に同期され、その設定が Prime Infrastructure オペレーション センター データベースで更新されます。管理 VDC の同期により、ハードウェアで新しく追加された VDC もユーザ インターフェイスに追加されます。また、ハードウェアで削除された VDC はユーザ インターフェイスから削除されます。

オペレーション センターを使用した複数の Cisco Prime Infrastructure サーバを含む展開での仮想ドメインの使用

「ユーザ アクセスの制御」で説明しているように、この機能を使用すると、オペレーション センターの管理者は管理対象 Cisco Prime Infrastructure インスタンスで仮想ドメインを定義することができます。[仮想ドメイン（Virtual Domains）]ページが変更されて、管理対象 Cisco Prime Infrastructure インスタンスで定義された各仮想ドメインをオペレーション センター管理者が確認できるようになります。ドメインのリストが統合されて、オペレーション センターに表示されます。

オペレーション センターから、オペレーション センターで管理されているすべての Cisco Prime Infrastructure インスタンスで使用できるすべての仮想ドメインを表示できます。

また、オペレーション センター自体から仮想ドメインを作成または編集することもできます。同じ仮想ドメインが複数の Cisco Prime Infrastructure インスタンスでアクティブな場合、オペレーション センターには仮想ドメインが一度表示され、すべての管理対象 Cisco Prime Infrastructure インスタンス上で同じ名前を持つすべてのアクティブな仮想ドメインのデータがそこに集約されます。

インスタンスが存在する場合（または到達可能な状態にある場合）にのみ、仮想ドメインを作成できます。[仮想ドメイン（Virtual Domain）]には管理対象ネットワーク要素のみが表示されるため、[仮想ドメイン（Virtual Domains）] 内のネットワーク要素の数は、Cisco Prime Infrastructure に比べて限定的です。仮想ドメインにデバイス グループを割り当てたり、オペレーション センターを使用して仮想ドメインを配布するインスタンスを選択することもできます。

オペレーション センターの中から仮想ドメインを作成、編集、インポートおよびエクスポートする方法は、Cisco Prime Infrastructure の 1 つのインスタンスで仮想ドメインを作成、編集、インポートおよびエクスポートする方法と同じです。詳細については、「Using Virtual Domains to Control Access」を参照してください。

関連トピック

オペレーション センターの構成ダッシュボードを使用した複数の Cisco Prime Infrastructure サーバの管理 （470 ページ）

オペレーション センターによるすべての Cisco Prime Infrastructure サーバの管理対象デバイスの表示 （472 ページ）
オペレーション センターを使用した Prime Infrastructure サーバの管理 （478 ページ）
Cisco Prime Infrastructure への仮想ドメインの配布 （475 ページ）

Cisco Prime Infrastructure への仮想ドメインの配布

オペレーションセンターで、インスタンスに既存の仮想ドメインを配布するには、次の手順を実行します。

ステップ 1 **[管理（Administration）] > [ユーザ（Users）] > [仮想ドメイン（Virtual Domains）]** を選択します。
ステップ 2 [仮想ドメイン（Virtual Domains）] サイドバー メニューから、新しいインスタンスで作成する既存の仮想ドメインをクリックします。
ステップ 3 [管理対象サーバ（Managed Servers）] タブをクリックします。
ステップ 4 [追加（Add）] をクリックし、仮想ドメインを配布する Prime Infrastructure 管理インスタンスを選択します。
ステップ 5 **OK** をクリックします。
ステップ 6 **Submit** をクリックします。

詳細については、『Cisco Prime Infrastructure Administrator Guide』の「*User Permissions and Device Access*」の章を参照してください。

関連トピック

オペレーション センターの構成ダッシュボードを使用した複数の Cisco Prime Infrastructure サーバの管理 （470 ページ）

オペレーション センター RBAC サポートの有効化

オペレーション センターでのロールベース アクセス コントロール（RBAC）のサポートにより、複数の管理対象インスタンスからのデバイス コレクションを仮想ドメイン経由でユーザに関連付けることができます。この機能によって、[サーバのモニタリングと管理（Monitor and Manage server）] ページへのアクセス、管理対象インスタンスの追加、変更または削除、および特定のユーザへの特定のダッシュレットの入力を行うことができます。

オペレーションセンターでRBAC（ロールベースアクセス コントロール）を有効にするには、次の手順に従います。

ステップ 1 管理者として Prime Infrastructure にログインします。
ステップ 2 **[管理（Administration）] > [ユーザ（Users）] > [ユーザ、ロール、および AAA（Users, Roles & AAA）] > [ユーザ グループ（User Groups）]** を選択します。
ステップ 3 RBAC が提供されるグループ名をクリックします。
ステップ 4 [Task Permissions] タブをクリックします。

ステップ 5 オペレーション センター タスクで次のチェックボックスをオンにします。

- [サーバ ページへのアクセスのモニタリングと管理（Monitor and Manage Servers Page Access）]。
- [サーバ ページの管理とモニタリングでの管理特権（Administrative Privileges under Manage and Monitor Server Pages）]。

これらのオプションは、管理者およびスーパー ユーザではデフォルトで有効になっています。

ステップ 6 [保存（Save）] をクリックします。

詳細については、『Cisco Prime Infrastructure Administrator Guide』の「User Access and Device Permissions」の章を参照してください。

関連トピック

オペレーション センターを使用した複数の Cisco Prime Infrastructure サーバを含む展開での仮想ドメインの使用 （474 ページ）

オペレーション センターを使用した Prime Infrastructure サーバ間のデバイス設定テンプレートの共有

オペレーションセンターは、ネットワーク内のデバイスを直接管理または設定しませんが、管理する Prime Infrastructure サーバ インスタンスで保存された設定テンプレートにユーザがアクセスできるようにします。オペレーション センターを使用して、次の操作を実行できます。

- Prime Infrastructure サーバのいずれかの設定テンプレートを表示できます。
- あるサーバに存在するテンプレートをオペレーションセンターが管理する他のサーバに配布できます。ネットワーク全体にテンプレートを展開する場合などは、このようにテンプレートを配布する必要があります。

これらの操作を実行する際の手順は、スタンドアロンの Prime Infrastructure サーバで同じ操作を実行する場合と一緒です。最初にオペレーション センター インスタンスにログインする必要があるだけで、次に作業するテンプレートの Prime Infrastructure サーバ インスタンスを選択します。

オペレーション センターを使用した設定テンプレートの表示

オペレーションセンターの [設定（Configuration）] メニュー オプションを選択し、テンプレートを見つけるまでリストを展開すると、管理対象の Prime Infrastructure インスタンスの設定テンプレートを表示できます。

ステップ 1 オペレーション センターにログインし、**[設定（Configuration）] > [テンプレート（Templates）] > [機能およびテクノロジー（Features & Technologies）]** を選択します。

ステップ 2 表示するテンプレート カテゴリを展開します（[自分のテンプレート（My Templates）] など）。オペレーション センターは、このカテゴリ内で管理対象の Prime Infrastructure インスタンスとテンプレートのリストを表示します。

ステップ 3 表示するテンプレートの管理対象インスタンスを展開します。必要に応じてテンプレートのサブカテゴリを展開します。

オペレーション センターを使用した設定テンプレートの展開

ステップ 1 設定テンプレートを作成したら、[展開（Deploy）] をクリックします。
[展開（Deployment）] ウィザードが表示されます。

ステップ 2 テンプレートを展開するデバイスを選択し、[次へ（Next）] をクリックして入力値を選択します。

ステップ 3 [入力値（Input Values）] タブでは、[フォーム（Form）] ビューと [CLI] ビューを切り替えることができます。

ステップ 4 必要な設定値を入力したら、[CLI] をクリックして、デバイスおよびテンプレートの設定値を確認します。

ステップ 5 [次へ（Next）] をクリックしてジョブ展開サマリーを表示します。

ステップ 6 各デバイスの CLI ビューを [展開サマリー（Deployment Summary）] タブに表示できます。

ステップ 7 [終了（Finish）] をクリックしてテンプレートを展開します。

管理対象サーバへの設定テンプレートの配布

ユーザ定義の設定テンプレートをある Prime Infrastructure 管理対象インスタンスから別の管理対象インスタンスに配布できます。

テンプレートをインスタンスなどの別のデバイスに展開する場合、他のインスタンスにこのテンプレートを最初にコピー（配布）しないと、テンプレートは別の Prime Infrastructure サーバインスタンスに配布されます。

ステップ 1 オペレーション センターにログインし、[設定（Configuration）] > [テンプレート（Templates）] > [機能およびテクノロジー（Features & Technologies）] を選択します。

ステップ 2 表示するテンプレート カテゴリを展開します（[自分のテンプレート（My Templates）] など）。オペレーション センターは、このカテゴリ内で管理対象の Prime Infrastructure インスタンスとテンプレートのリストを表示します。

ステップ 3 表示するテンプレートの管理対象インスタンスを展開します。必要に応じてテンプレートのサブカテゴリを展開します。

ステップ 4 （任意）配布する前にテンプレートを編集するには、次の手順を実行します。

a) [変数の追加（Add Variable）] をクリックし、テンプレート変数を選択します。
b) [編集（edit）] アイコンをクリックし、必要な変更を加えます。
c) [保存（Save）] をクリックします。

ステップ 5 配布するテンプレートが表示されたら、このテンプレートをクリックして選択します。オペレーション センターでは、選択したテンプレートの詳細が表示されます。

ステップ 6 [配布（Distribute）] をクリックします。オペレーション センターが管理し、現在アクセス可能な Prime Infrastructure サーバ インスタンスすべてのリストが表示されます。

ステップ 7 テンプレートを配布する各Prime Infrastructure サーバインスタンスの横にあるチェックボックスを選択します。

ステップ 8 [テンプレートを同じ名前で上書きする（Overwrite template with the same name）] チェックボックスをオンにして [OK] をクリックします。

[テンプレートを同じ名前で上書きする（Overwrite template with the same name）] チェックボックスをオフにした場合で、他のサーバにそのテンプレートがすでに存在していると、オペレーション センターはテンプレートを配布できず、[テンプレートを同じ名前で上書きする（Overwrite template with the same name）] チェックボックスをオンにすることを求めるアラートが表示されます。

オペレーション センターを使用した Prime Infrastructure サーバの管理

[サーバの管理とモニタリング（Manage and Monitor Servers）] ページを開くには、**[モニタ（Monitor）] > [モニタリングツール（Monitoring Tools）] > [サーバの管理とモニタリング（Manage and Monitor Servers）]** の順に選択します。ここでは、次の操作が可能です。

- 新しい Cisco Prime Infrastructure サーバの追加（ライセンス制限まで）。
- 現在の Cisco Prime Infrastructure サーバの編集、削除、アクティブ化および非アクティブ化。
- Cisco Prime Infrastructure サーバをトラブルシューティングします。Cisco Prime Infrastructure サーバのいずれかを選択し、**[トラブルシューティング (Troubleshoot)]** ボタンをクリックします。ポップアップ ウィンドウで、**[アクション (Actions)]** リスト ボックスから必要なトラブルシューティング オプションを選択します。使用可能なオプションは、Nslookup、Ping、および Traceroute です。
- 各サーバの到達可能性、CPU使用率、メモリ使用率、ソフトウェアアップデートのステータス（最新パッチとそのバージョンなど）とセカンダリ サーバの詳細（設定されている場合）、購入したライセンス、使用済みライセンス、およびCisco Prime Infrastructureインスタンスに生成されたアラームの概要の表示。
- ダウンしているサーバの特定。
- 個々の Cisco Prime Infrastructure インスタンスのクロス起動。
- バックアップ サーバが実行中かどうかの確認。管理者は Cisco Prime Infrastructure の高可用性（HA）フレームワークを使ってバックアップ Cisco Prime Infrastructure サーバを設定できます。これにより、関連付けられているプライマリ サーバがダウンした際にこのサーバが自動的にオンラインになり、操作を引き継ぎます。Cisco Prime Infrastructure HA フレームワークの詳細については、関連項目の「ハイ アベイラビリティの設定」を参照してください。管理者は、「Before You Begin Setting Up High Availability」に記載されているオペレーション センターでの HA の使用に関する制限事項に従う必要があります。

サーバの到達可能性ステータスとは別に、注目すべき 3 つのサーバ メトリックがあります。

- CPU 使用率
- メモリ使用率

サーバに1秒を超えるネットワーク遅延がある場合、またはCPUまたはメモリの使用率が80%を超える場合は、そのサーバに問題が存在する可能性があります。

サーバのステータスが [Unreachable] と表示されている場合、[?] アイコンが到達可能性ステータス メッセージの横に表示されます。サーバのステータスに関して考えられる原因を示すポップアップ メッセージ表示するには、アイコンの上にマウスのカーソルを合わせます（たとえば、サーバを ping できない、API 応答（遅延）が非常に遅い、SSO が正しく設定されないなど）。

関連トピック

ハイ アベイラビリティの設定
ハイ アベイラビリティをセットアップする前に
オペレーション センターの構成ダッシュボードを使用した複数の Cisco Prime Infrastructure サーバの管理 （470 ページ）
オペレーション センターを使用した複数の Cisco Prime Infrastructure サーバを含む展開での仮想ドメインの使用 （474 ページ）
オペレーション センターを使用した複数の Prime Infrastructure サーバのステータスの表示（479 ページ）

オペレーション センターを使用した複数の Prime Infrastructure サーバのステータスの表示

開いているダッシュボードまたはページから移動することなく Prime Infrastructure サーバの現在のステータスを表示するには、[サーバ ステータスの概要（Server Status Summary）] を使用します。それを開くには、オペレーション センターのメイン ページの上部にある [Server Status] 領域の任意の部分にカーソルを置きます。ここから、現在ダウンしているサーバがあるかどうかをすぐに判断できます。また、選択したサーバ用に別の Prime Infrastructure インスタンスを起動することもできます。

オペレーション センターで管理する Prime Infrastructure サーバの到達可能性履歴を簡単に確認できます。

ステップ 1 **[モニタ（Monitor）] > [モニタリング ツール（Monitoring Tools）] > [サーバの管理とモニタリング（Manage and Monitor Servers）]** の順に選択します。オペレーション センターが管理する Prime Infrastructure サーバのリストが表示されます。

ステップ 2 管理対象サーバのいずれかを選択します。ページには、このサーバのサマリー ステータスが表示されます。

ステップ 3 ページ下部の [到達可能性履歴（Reachability History）] タブをクリックします。オペレーション センターは、選択した Prime Infrastructure サーバに関する到達可能性の最新の変更をリストで表示します。

ステップ 4 到達可能性の履歴をクリアするには、[履歴のクリア（Clear History）] をクリックし、ポップアップ ウィンドウで [はい（Yes）] をクリックします。

関連トピック

オペレーション センターの構成ダッシュボードを使用した複数の Cisco Prime Infrastructure サーバの管理 （470 ページ）

スマートライセンシングを使用したオペレーションのアクティベート

スマート ライセンスは、時間のかかる手動のライセンス タスクを自動化できるクラウドベースのソフトウェア ライセンス管理ソリューションです。このソリューションを使用すると、ライセンスのステータスとソフトウェアの使用傾向を簡単に追跡できます。

シスコ スマート ライセンスを使うと次の 3 つのコア機能が簡素化されます。

- **購入**：ネットワークにインストールされているソフトウェアを、製品アクティベーション キー（PAK）を指定せずに自動的に登録できます。
- **管理**：ライセンスエンタイトルメントの有効化を自動的に追跡できます。また、すべてのノードにライセンス ファイルをインストールする必要はありません。
- **レポート**: スマート ライセンスでは、ポータルを使用することで、購入したライセンスとネットワークに実際に展開された製品を統合して表示できます。このデータを使用すると、購入の意思決定を実際の使用状況に基づいてより適切に行うことができます。

スマートソフトウェアライセンスを選択するには、『Cisco Prime Infrastructure Administrator Guide』の「スマートソフトウェアライセンスの選択」の項を参照してください。

オペレーション センターで管理されている Prime Infrastructure インスタンスにソフトウェア更新を配信します

オペレーション センターでは、ソフトウェア更新を複数の Prime Infrastructure インスタンスに配信することができます。

ソフトウェア更新を配信するには、次のようにします。

ステップ 1 **[管理（Administration）] > [ライセンスおよびソフトウェア更新（Licenses and Software Updates）] > [ソフトウェア更新（Software Update）]** に移動します。

ステップ 2 **[Prime Infrastructure]** タブをクリックし、**[アップロード（upload）]** リンクをクリックします。**[更新のアップロード（Upload Update）]** ダイアログで、必要に応じて **[ローカル コンピュータからアップロード（upload from local computer）]** または **[サーバのローカル ディスクからコピー（Copy from server's local disk）]** オプション ボタンをクリックします。

ステップ 3 **[参照（Browse）]** をクリックして、保存場所から dowloaded パッチファイルを選択し、**[OK]** をクリックします。

ステップ 4 **[配信 (Distribute)]** をクリックして、パッチ ファイルを Prime Infrastructure サーバに配信します。

（注） これで、Prime Infrastructure のオペレーション センターから Prime Infrastructure のセカンダリ サーバにパッチ ファイルを配信するように選択できるようになりました。ペアリングされているのハイ アベイラビリティ サーバへのパッチのインストールは許可されていないことに注意してください。詳細については、『*Cisco Prime Infrastructure* 管理ガイド』の「ペアリングされた HA サーバのパッチ適用方法」の項を参照してください。

ステップ 5 サーバのリストから必要な Prime Infrastructure サーバを選択し、**[OK]** をクリックします。更新成功のポップアップ メッセージが表示されます。

ステップ 6 **[Prime infrastructure]** タブを選択し、**[インストール (Install)]** ボタンをクリックして、更新を Prime Infrastructure インスタンスにインストールします。

ステップ 7 更新のステータスは、**[更新のステータス (Status of Updates)]** セクションで確認できます。

（注） [Prime Infrastructure] タブの **[配信 (Distribute)]** ボタンを使用して、任意の数の使用可能な Prime Infrastructure サーバにソフトウェア更新を配信できます。ソフトウェアの更新に関する詳細は、『Cisco Prime Infrastructure 管理者ガイド』の「ライセンスおよびソフトウェア更新」の章を参照してください。

オペレーション センターによる複数の Cisco Prime Infrastructure サーバによって管理されるデバイスでのアラームの表示

[モニタ（Monitor）] > [モニタリングツール（Monitoring Tools）] > [アラームおよびイベント（Alarms and Events）] の順に選択して、[アラームおよびイベント（Alarms and Events）] ページを開きます。ここから、ネットワークのアラーム、イベント、1 つまたは複数のアラームを選択すると、そのアラームが確認済みであるかどうかを判断したり、そのアラームについて詳細を記載したメモを追加したり、ページからそのアラームを削除することもできます。

[Alarm Summary] には、管理対象の Cisco Prime Infrastructure インスタンスから集約されたクリティカル アラーム、メジャー アラーム、およびマイナー アラームの数が表示されます。

ここに表示されるアラームとイベントを絞り込むには、以下のいずれかを実行します。

- [Device Group] ペインから、目的のデバイス タイプ、ロケーション、またはユーザ定義グループを選択します。
- カスタム フィルタを適用するか、または [Show] ドロップダウン リストから定義済みフィルタの 1 つを選択します。フィルタの使用方法の詳細については、関連項目「クイック フィルタ」を参照してください。
- 特定のアラームまたはイベントを探します。詳細については、関連項目「検索方法」を参照してください。
- 管理対象の Cisco Prime Infrastructure インスタンスのアラームの合計数を表示するには、[Alarm Browser] 画面にカーソルを合わせます。アラームの確認応答、注釈付け、および削除を行うこともできます。そのアクションは、各 Cisco Prime Infrastructure インスタンスに複製されます。

関連トピック

クイック フィルタ （1115 ページ）
検索方法 （1129 ページ）
オペレーション センターの構成ダッシュボードを使用した複数の Cisco Prime Infrastructure サーバの管理 （470 ページ）

オペレーション センターによる複数の Cisco Prime Infrastructure サーバの管理対象クライアントおよびユーザの表示 （482 ページ）

オペレーションセンターによる複数の Cisco Prime Infrastructure サーバの管理対象クライアントおよびユーザの表示

[モニタ（Monitor）] > [モニタリングツール（Monitoring Tools）] > [クライアントおよびユーザ（Clients and Users）] の順に選択して、[クライアントおよびユーザ（Clients and Users）] ページを開きます。このページには、すべての管理対象 Cisco Prime Infrastructure インスタンスの集約されたクライアントが含まれています。ここから、クライアントの MAC アドレス、クライアントに関連付けられているユーザ、クライアントをホストするデバイスの名前など、ネットワーク上で設定されたクライアントの情報を表示できます。クライアントまたはユーザを選択して、クライアントの関連付け履歴と統計情報を表示できます。[360度（360° Degree）] ビューを起動して、デバイスおよび関連するクライアントに関する詳細情報を表示することもできます。

ここに表示されるクライアントのリストを絞り込むには、次のいずれかを実行します。

- カスタム フィルタを適用するか、または [Show] ドロップダウン リストから定義済みフィルタの 1 つを選択します。フィルタの使用方法の詳細については、関連項目「クイック フィルタ」を参照してください。
- 特定のクライアントを検索します。詳細については、関連項目「検索方法」を参照してください。

関連トピック

クイック フィルタ （1115 ページ）
検索方法 （1129 ページ）
オペレーション センターの構成ダッシュボードを使用した複数の Cisco Prime Infrastructure サーバの管理 （470 ページ）

オペレーション センターを使用した複数の Cisco Prime Infrastructure サーバを含む展開でのレポートの実行

オペレーションセンターのダッシュボードとモニタ ページに加えて、オペレーションセンターには Cisco Prime Infrastructure レポートのサブセットがあります。これらのレポートは、Cisco Prime Infrastructure のすべての管理対象インスタンスにおけるネットワーク管理データとパフォーマンス データを組み合わせたものです。グローバル ネットワークの管理をセグメント化し合理化するためにオペレーション センターを使用している場合は、これらの特殊なバージョンの標準レポートは、ネットワークを全体としてより間近で確かめたり、全世界の健全性を監視したり、緊急問題をトラブルシューティングする際に役立ちます。

オペレーション センターのレポートには、すべての管理対象の Cisco Prime Infrastructure インスタンスからの集約データが含まれています。この集約を特定の管理対象インスタンスのサブセットに制限する必要がある場合、最も良い方法は次のとおりです。

- 集約されたオペレーション センターのレポート データに含めたくないデータを持つ Cisco Prime Infrastructure 管理対象インスタンスを、一時的に非アクティブ化します。これを行うには、**[モニタ（Monitor）]** > **[モニタリングツール（Monitoring Tools）]** > **[サーバの管理とモニタリング（Manage and Monitor Servers）]** の順に選択し、無視するサーバを非アクティブにすることを選択します。
- 仮想ドメインを使用して、該当するインスタンスのデータを制限します。詳細については、関連項目の「オペレーション センターを使用した複数の Prime Infrastructure サーバを含む展開での仮想ドメインの使用」を参照してください。

管理対象インスタンスでのデータの集約を除き、オペレーションセンターでレポートを生成する方法は、Cisco Prime Infrastructure での方法と同じです。Cisco Prime Infrastructure レポートとその生成方法の詳細については、関連項目の「新しいレポートの作成、スケジュール設定、実行」を参照してください。

関連トピック

新しいレポートの作成、スケジュール設定、実行

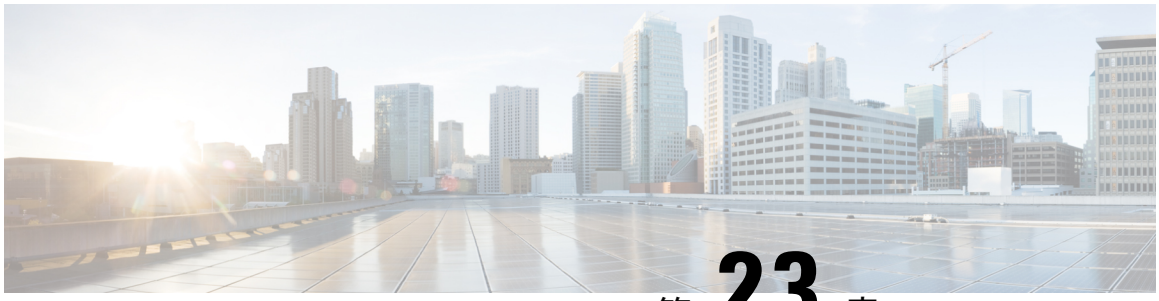
オペレーション センターの構成ダッシュボードを使用した複数の Cisco Prime Infrastructure サーバの管理 （470 ページ）

オペレーション センターを使用した複数の Cisco Prime Infrastructure サーバを含む展開での仮想ドメインの使用 （474 ページ）

オペレーション センターによる複数の Cisco Prime Infrastructure サーバによって管理されるデバイスでのアラームの表示 （481 ページ）

オペレーション センターによる複数の Cisco Prime Infrastructure サーバの管理対象クライアントおよびユーザの表示 （482 ページ）

よくある質問：オペレーション センターと Prime Infrastructure （1161 ページ）



第 23 章

高度なモニタリング

- サイト ダッシュレットで使用されるデータ ソースとは （485 ページ）
- WAN 最適化の有効化 （487 ページ）

サイト ダッシュレットで使用されるデータ ソースとは

Cisco Prime Infrastructure は、NAM、NetFlow、NBAR、Cisco Medianet、PerfMon、Performance Agent などのさまざまなソースからの情報を処理します。次の表に、Prime Infrastructure で使用されるサイト ダッシュレットに関するデータのソースを示します。

表 *44*：サイト ダッシュレット データ ソース

ダッシュレットの名前	NAM	Cisco メディアネット	NetFlow	PA	NBAR2
Application Usage Summary	y	y	y	y	y
Top N Application Groups	y	y	y	y	y
Top N Applications	y	y	y	y	y
Top N Applications with Most Alarms	y	y	y	y	y
Top N Clients (In and Out)	y	y	y	y	y
Top N VLANs	y	_	y	y	_
Worst N RTP Streams by Packet Loss	y	y	_	_	_
Worst N Clients by Transaction Time	y	_	_	y	_

次の表に、Prime Infrastructure によって生成されるアプリケーション固有のダッシュレットを示します。

表 *45 :* アプリケーション固有のダッシュレット データ ソース

ダッシュレットの名前	NAM	Cisco メディアネット	NetFlow	PA	NBAR2
Application Configuration	y	y	y	y	y
Application ART Analysis	y	_	_	y	_
App Server Performance	y	_	_	y	_
Application Traffic Analysis	y	y	_	y	y
Top N Clients (In and Out)	y	_	_	y	_
Worst N Clients by Transaction Time	y	_	_	y	_
Worst N Sites by Transaction Time	y	_	_	y	_
KPI Metric Comparison	y	y	_	y	_
DSCP Classification	y	_	y	_	_
Number of Clients Over Time	y	_	y	_	_
Top Application Traffic Over Time	y	_	y	_	_
Top N Applications	y	_	y	y	_
Top N Clients (In and Out)	y	_	y	y	_
Average Packet Loss	y	y	_	_	_
Client Conversations	y	_	y	_	_
Client Traffic	y	_	y	_	_
IP Traffic Classification	y	_	y	_	_
Top N Applications	y	_	y	_	_
DSCP Classification	y	_	y	_	_
RTP Conversations Details	y	y	_	_	_
Top N RTP Streams	y	y	_	_	_
Voice Call Statistics	Y	y	_	_	_
Worst N RTP Streams by Jitters	y	y	_	_	_
Worst N RTP Streams by MOS	y	_	_	_	_
Worst N Sites by MOS	y	_	_	_	_
Worst N Site to Site Connections by KPI	y	y	_	y	_

関連項目

- Medianet NetFlow の有効化
- NetFlow と Flexible NetFlow の有効化

WAN 最適化の有効化

Cisco Wide Area Application Services（WAAS）デバイスとソフトウェアは、複数サイトのアプリケーション全体での高品質な WAN エンドユーザ エクスペリエンスを保証するのに役立ちます。ネットワークに WAAS を展開するためのさまざまなシナリオについては、「WAAS 展開での Cisco NAM ハードウェアの使用」を参照してください。

候補サイトで WAAS 変更を展開したら、[Dashboards] > [Performance] > [WAN Optimization] の順に選択して、最適化の投資効果を検証することができます。このダッシュボードから、[マルチセグメント分析の表示（View Multi-Segment Analysis）] をクリックして、WAAS に最適化された WAN トラフィックをモニタすることができます。[Multi-Segment Analysis] 表示では、次の項目を選択できます。

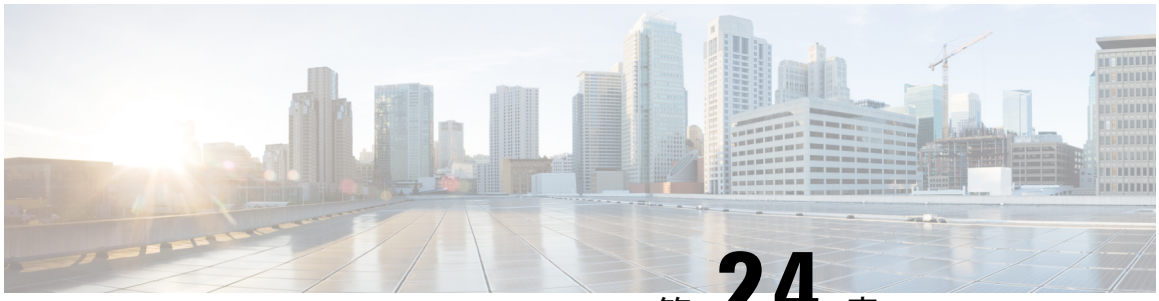
- 個々のクライアント/サーバ セッションを確認するための [Conversations] タブ。
- 集約されたサイト トラフィックを確認するための [Site to Site] タブ。

次の表に、主要な WAAS モニタリング ダッシュレットの説明を示します。

表 *46 :* 主要な *WAAS* モニタリング ダッシュレット

ダッシュレット	説明
Average Concurrent Connections (Optimized versus Pass-through)	指定された期間の同時クライアントおよびパススルー接続数の平均をグラフ表示します。
Multi-segment Analysis	カンバセーション内またはサイト間の複数のセグメントにわたる WAAS トラフィックを表示します。
Multi-segment Network Time (Client LAN-WAN - Server LAN)	複数のセグメント間のネットワーク時間をグラフ表示します。
Transaction Time (Client Experience)	過去 24 時間の平均クライアント トランザクション時間（ミリ秒単位）をグラフ表示します。最適化されたトラフィックとパススルー トラフィック（最適化が無効）で行が分かれています。最適化が有効になっている場合は、パススルー時間と比較して、最適化されたトラフィック時間の方が短くなっているはずです。
Traffic Volume and Compression Ratio	圧縮前のバイト数と圧縮後のバイト数の帯域幅減少率をグラフ表示します。

Prime Infrastructure Assurance ライセンスを購入して適用しない限り、マルチセグメント分析にアクセスすることはできません。候補サイトに WAAS が実装されていない場合は、WAAS モニタリング ダッシュレットに何もデータが表示されません。



第 24 章

レポートの管理

この章は、次の内容で構成されています。

- レポートの概要 （489 ページ）
- 新しいレポートの作成、スケジュール設定、実行 （490 ページ）
- Prime Infrastructure でのレポートの結合 （492 ページ）
- カスタム レポートの作成 （493 ページ）
- レポート結果のカスタマイズ （496 ページ）
- Cisco Prime Infrastructure でスケジュール設定されたレポート （496 ページ）
- 保存済みレポートのテンプレート （499 ページ）
- Prime Infrastructure レポートのデータ保持期間 （500 ページ）

レポートの概要

Prime Infrastructure レポートでは、システムおよびネットワークの健全性に関する情報と障害情報が提供されます。定期的にレポートが実行されるようにカスタマイズしてスケジュールすることができます。レポートは、表形式またはグラフィック形式（またはこれらの形式の混合）でデータを表示できます。レポートは CSV または PDF 形式で保存することもできます。CSV または PDF ファイルは、後でダウンロードするために Prime Infrastructure サーバに保存するか、または電子メール アドレスに送信できます。

Prime Infrastructure では、次のタイプのデータが提供されます。

- 現在：時間に依存しないデータのスナップショットを提供します。
- 履歴：デバイスから定期的にデータを取得し、そのデータを Prime Infrastructure データベースに保存します。
- 傾向：最小値、最大値、および平均値として集計された集約データを使用してレポートを生成します。

Prime Infrastructure では、特定の基準に基づいてこれらのレポートをフィルタリングできます。また、レポートをエクスポートしたり、レポートを論理グループにソートしたり、長期間保存するためにレポートをアーカイブすることもできます。

新しいレポートの作成、スケジュール設定、実行

[レポート起動パッド（Report Launch Pad）] では、1 つのページからすべての Prime Infrastructure レポートにアクセスできます。このページでは、すべてのレポート操作（作成、保存、表示、スケジュール設定、カスタマイズ）を実行できます。

レポートの詳細を表示するには、レポートの種類の横にあるツールチップにカーソルを移動します。

新しいレポートを作成してスケジュール設定し、実行するには、次の手順に従います。

ステップ 1 左側のサイドバーから、**[レポート（Reports）] > [レポート起動パッド（Report Launch Pad）]** を選択します。

ステップ 2 起動するレポートを見つけ、[新規作成（New）] をクリックします。

ステップ 3 [レポートの詳細（Report Details）] ページで、レポートのタイトルを入力します。

[レポート タイトル（Report Title）] フィールドを編集できます。

ステップ 4 ドロップダウンリストから適切な [レポート作成者（Report By）] カテゴリを選択します。

ステップ 5 [レポート基準（Report Criteria）] フィールドでは、前の [レポート作成者（Report By）] で行った選択に応じて結果を分類できます。

（注） 既存のデバイスに表示されている [レポート条件（Report Criteria）] フィールドに新しいデバイスを追加する場合は、必ず既存のデバイスと新しいデバイスとを選択してください。そうしないと、新しいデバイスで既存のデバイスが置き換えられます。

[グループによるデバイス]ダイアログボックスにデバイスを追加するには、そのグループ内の親グループまたはデバイスを選択する必要があります。異なるグループに属する親グループとデバイスは選択できません。

（注） 上部の仮想ドメイン チェックボックスを選択した場合、レポート条件フィルタに 1 つ以上の値が存在する場合は、編集ボタンが有効になります。

ステップ 6 [編集（Edit）] をクリックしてデバイス選択ウィザードを開き、必要なデバイスを選択します。デバイスの選択中にデバイス ホスト名とデバイス IP を表示できます。[プレビュー（Preview）] タブをクリックして、選択したデバイスを確認し、[OK] をクリックします。選択したデバイスを削除することもできます。

[レポートの詳細（Report Details）] ページに表示されるパラメータは、選択するレポートのタイプによって異なります。一部のレポートでは、レポートの結果をカスタマイズする必要があります。レポート結果のカスタマイズ方法の詳細については、レポート結果のカスタマイズ（496ページ）を参照してください。

（注） クライアント レポートには、ワイヤレス LAN コントローラが仮想ドメインにマッピングされている場合のみ、SSID が記載されます。

ステップ 7 このレポートを後で実行するか、繰り返しのレポートとして実行する場合は、[スケジュール設定（Schedule）] の必須パラメータを入力します。

ステップ 8 レポートを実行するには、次のいずれかのオプションを選択します。

- [実行（Run）]：レポート設定を保存せずにレポートを実行します。

  （注） デフォルトでは、[一意のクライアントとユーザの概要（Unique Clients and Users Summary）] レポートの [実行（Run）] ボタンは無効になっています。このレポートは、Prime Infrastructure の使用率が低い時間帯に実行されるようにスケジュールできます。

- [保存（Save）]：レポートをすぐに実行せずにこのレポート設定を保存します。スケジュール パラメータが入力済みの場合は、スケジュールされた日時にレポートが自動的に実行されます。

- [実行して保存（Run and Save）]：レポートの設定を保存し、ただちにレポートを実行します。

  （注） デフォルトでは、[一意のクライアントとユーザの概要（Unique Clients and Users Summary）] レポートの [実行して保存（Run and Save）] ボタンは無効になっています。このレポートは、Prime Infrastructure の使用率が低い時間帯に実行されるようにスケジュールできます。

- [保存してエクスポート（Save and Export）]：レポートを保存して実行し、結果をファイルにエクスポートします。以下を要求するプロンプトが表示されます。

  - エクスポートするレポートのファイル形式を選択します（CSV または PDF）。エクスポートされる CSV ファイルは、100 万レコードを保持できる単一の .csv ファイルです。レコード数が 100 万を超えると、残りのレコードを収容する別の CSV ファイルが生成されます。最後に、両方の CSV ファイルが zip 形式で提供されます。
  - レポートが生成された際に電子メールを送信するかどうかを選択します。このオプションを選択する場合は、宛先メール アドレスと電子メールの件名を入力し、エクスポート ファイルを添付ファイルとして電子メールに含めるかどうかを選択する必要があります。

  操作が終了したら、[OK] をクリックします。

  （注） [ステータス（Status）] 列には、レポートの進行状況が表示されます。更新されたステータスを確認するには、ページを更新します。

- [保存して電子メール送信（Save and Email）]：レポートを保存して実行し、結果をファイルにエクスポートして電子メールで送信します。以下を要求するプロンプトが表示されます。

  - エクスポートするレポートのファイル形式を選択します。

    （注） ファイル サイズは 25 MB を超えてはなりません。

  - 宛先メール アドレスと電子メールの件名を入力します。

  操作が終了したら、[OK] をクリックします。

  （注） [ステータス（Status）] 列には、レポートの進行状況が表示されます。更新されたステータスを確認するには、ページを更新します。

- [キャンセル（Cancel）]：このレポートを実行も保存もせずに前のページに戻ります。

関連トピック

カスタム レポートの作成 （493 ページ）

Prime Infrastructure でのレポートの結合

複数のレポートを結合し、要件に基づいて情報をフィルタリングできます。ユーザは、それぞれのシナリオ向けに特別なレポートを作成するのではなく、複数のレポートを選択して結合できます。複合レポートは、サポートされているレポートの定義済みリストから作成できます。

新規の複合レポートを作成するには：

ステップ 1 **[レポート（Reports）]** > **[レポート起動パッド（Reports Launch Pad）]** を選択します。次のいずれかの方法で新しいレポートを作成できます。

a) 左側のサイドバーのメニューで **[複合（Composite）]** > **[複合レポート（Compostie Report）]** を選択し、[新規（New）] をクリックします。

b) [Report Launch Pad] ページで、[Composite] セクションを下方にスクロールして [New] をクリックします。

ステップ 2 [New Custom Composite Report] ページで、レポートのタイトルを入力します。

ステップ 3 [Report Category] ドロップダウン リストからカテゴリを選択します。

ステップ 4 使用可能なリストから必要なレポートを選択して [Selected Reports] テキストボックスに追加します。レポートを選択して削除することもできます。

ステップ 5 ドロップダウン リストから適切な [Report By] カテゴリを選択します。カテゴリはレポートごとに異なります。

ステップ 6 [Report Criteria] フィールドでは、前の [Report By] で行った選択に応じて結果を分類できます。[Edit] をクリックして [Filter Criteria] ページを開き、必要なフィルタ基準を選択します。

ステップ 7 レポートを後で実行する場合や繰り返しレポートとして実行する場合は、[Schedule] セクションでスケジュール パラメータを入力します。

ステップ 8 レポートを実行するには、次のいずれかのオプションを選択します。

- [Run]：レポート設定を保存せずにレポートを実行する場合にクリックします。
- [Save]：レポートをただちに実行せずに、レポート設定を保存する場合にクリックします。スケジュール パラメータが入力済みの場合は、スケジュールされた日時にレポートが実行されます。
- [Run and Save]：レポート設定を保存し、ただちにレポートを実行する場合にクリックします。
- [Save and Export]：レポートを保存して実行し、結果をファイルまたは電子メールの添付ファイルにエクスポートする場合にクリックします。その場合は、以下を実行する必要があります。
  - エクスポートするレポートのファイル形式を選択します（CSV または PDF）。エクスポートされる CSV ファイルは、100 万レコードを保持できる単一の .csv ファイルです。
  - レポートが生成されたときに電子メールを送信する場合は、最初のチェックボックスをオンにします。宛先メール アドレスと電子メールの件名を入力する必要があります。
  - エクスポート ファイルを添付ファイルとして電子メールに含める場合は、2 番目のチェックボックスをオンにします。

[OK] をクリックします。

- [Save and Email]：レポートを保存して実行し、結果をファイルにエクスポートして電子メールで送信する場合にクリックします。以下を要求するプロンプトが表示されます。
  - エクスポートするレポートのファイル形式を選択します。

    （注）　ファイル サイズは 25 MB を超えてはなりません。

  - 宛先メール アドレスと電子メールの件名を入力します。

[OK] をクリックします。

- [Cancel]：このレポートを実行も保存もせずに、前のページに戻る場合にクリックします。

保存されている複合レポートには [Saved Reports Template] からアクセスできます。

カスタム レポートの作成

オペレーション センター環境では、カスタム レポート機能はサポートされていません。

ステップ 1　**[レポート（Reports）]** > **[カスタム レポート（Custom Reports）]** を選択します。

ステップ 2　[カスタム レポート（Custom Reports）] ページに **レポートのタイトル**を入力します。

ステップ 3　必要なレポートを [使用可能なオプション（Available Options）] ペインからドラッグし、[選択済みオプション（Selected Options）] ペインにドロップします。

ステップ 4　[レポート期間（Reporting Period）] ドロップダウン リストまたは [日付の選択（Select date）] 範囲から、レポート期間を選択します。

ステップ 5　必要に応じて、[概要ビュー（Summary View）] または [詳細ビュー（Detailed View）] を選択します。

- **[概要ビュー（Summary view）]**
  - レポートの実行時：表形式のサブレポートごとに上位 10 個のレコードを表示します。
  - CSV/PDF としてのレポートのエクスポート時：表形式のサブレポートごとに上位 20 個のレコードを表示します。
- **[詳細ビュー（Detailed view）]**
  - レポートの実行時：表形式のサブレポートごとに最大で上位 1000 個のレコードを表示します。この場合、各テーブルは画面上にページ分けされます。
  - PDF としてのレポートのエクスポート時：表形式のサブレポートごとに最大 1000 個のレコードを表示します。
  - CSV としてのレポートのエクスポート時：表形式のサブレポートごとにすべてのレコードを表示します。

（注）　上記のビューは、表形式のデータにのみ有効です。

ステップ 6 [レポート基準（CSV ）] に入力します。このフィールドには、選択したレポートに基づいた詳細を入力できます。

ステップ 7 [編集（Edit）] をクリックして [フィルタ基準（Filter Criteria）] ページを開き、必要なフィルタ基準を選択します。

ステップ 8 [サブレポートの編集（Edit Sub Report）] をクリックし、サブレポートを選択します。各レポートは、レポートをカスタマイズするレポート基準に基づいた異なる値でロードされます。

ステップ 9 要件に応じて、サブレポートを [すべて有効化（Enable）] または [すべて無効化（Disable All）] するか、あるいは選択したサブレポートを [有効化（Enable）] または [無効化（Disable）] します。レポートの組み合わせを複合レポートと呼びます。

（注） 有効または無効になっているレポートを確認するには、[有効化（Enable）] または [無効化（Disable）] のリンクの上にマウス カーソルを合わせます。

ステップ 10 レポートが結合されている複合レポートの場合は、[サブレポート（Sub reports）] を [有効化（Enable）] または [無効化（Disable）] することができます。

ステップ 11 サブレポートを有効にした場合は、サブレポートの値を選択します。各サブレポートをカスタマイズするには、ユーザは、どの表形式レポートを昇順または降順で保存する必要があるかに基づいて表形式レポートとフィールドに表示される属性を選択します。属性の順序を並び替えるには、それらの属性をドラッグし、特定の位置にドロップします。

ステップ 12 [適用（Apply）] をクリックし、レポートを [実行（Run）] します。レポートの概要が収集されると、選択したフィールドの値がテーブルに表示されます。

ステップ 13 サブレポートを無効にすると、他のレポート基準の残りのサブレポートがテーブルに表示され、レポートの概要にはデフォルトのフィールド値が表示されます。

ステップ 14 このレポートを後で実行するか、定期的なレポートとして実行する場合は、[定期レポート（Schedule Report）] タブをクリックし、次のパラメータを設定します。

- スライダをドラッグして [スケジューリング（Scheduling）] をオンにします。
- [エクスポート形式（Export Format）] として [CSV] または [PDF] を選択します。エクスポートされる CSV ファイルは、100 万レコードを保持できる単一の .csv ファイルです。
- [宛て先（Destination）] に [ファイル（File）] または [電子メール（Email）] を選択します。宛て先として電子メールを選択した場合は、電子メール ID を入力します。
- [開始日時（Start/Date time）] を選択します。
- 適切な繰り返しオプションを選択します。

ステップ 15 レポートを実行するには、次のいずれかのオプションを選択します。

- [実行（Run）]：レポート設定を保存せずにレポートを実行します。
- [保存（Save）]：レポートをすぐに実行せずにこのレポート設定を保存します。スケジュール パラメータが入力済みの場合は、スケジュールされた日時にレポートが自動的に実行されます。
- [実行して保存（Run and Save）]：レポートの設定を保存し、ただちにレポートを実行する場合にクリックします。

- [保存してエクスポート（Save and Export）]：レポートを保存して実行し、結果をファイルにエクスポートする場合にクリックします。以下を要求するプロンプトが表示されます。
  - エクスポートするレポートのファイル形式（CSV または PDF）を選択します。
  - レポートが生成されたら電子メールを送信するかどうかを選択します。このオプションを選択する場合は、宛先メールアドレスと電子メールの件名を入力し、エクスポートファイルを添付ファイルとして電子メールに含めるかどうかを選択する必要があります。
  - [OK] をクリックします。CSV ファイルが正しく開かない場合は、次のいずれかの場所で区切り記号としてカンマが指定されていることを確認してください。
    - [コントロールパネル（Control Panel）] > [地域と言語（Region/Language/Region and Language）] > [形式（Formats）] > [追加の設定（Additional Settings）]
    - Excel：[ファイル（File）] > [オプション（Options）] > [詳細設定（Advanced）] > [システムの桁区切りを使用する（Use System Separators）]

- [保存して電子メール送信（Save and Email）]：レポートを保存して実行し、結果をファイルとしてエクスポートし、そのファイルを電子メールで送信する場合にクリックします。以下を要求するプロンプトが表示されます。
  - エクスポートするレポートのファイル形式を選択します。

    （注）　ファイル サイズは 25 MB を超えてはなりません。

  - 宛先メール アドレスと電子メールの件名を入力します。
  - [OK] をクリックします。

- [キャンセル（Cancel）]：このレポートを実行も保存もせずに前のページに戻る場合にクリックします。

ステップ 16　[カスタム チャート オプション（Custom Chart Options）]：レポートが生成されると、[レポートの表示（View Report）] タブが自動的に有効になり、レポートの出力が表示されます。チャートとして生成されたサブレポートには、各チャートの左上に小さなチャートアイコンが表示されます。スマートチャートアイコンをクリックすると、円グラフ、棒グラフ、折れ線グラフなど、データを視覚的にさまざまにカスタマイズしたチャートを作成できます。

（注）　これらのカスタムチャートは、画面モード（ライブインタラクティブモード時）にのみ適用され、レポートの保存やレポートのエクスポートのアクション時には適用されません。

ステップ 17　[管理（Administration）] > [ダッシュボード（Dashboards）] > [ジョブ ダッシュボード（Job Dashboard）] > [ユーザ ジョブ（User Jobs）] を選択します。

ステップ 18　[レポート ステータス（Report Status）] をクリックし、ジョブのステータスを表示します。

ステップ 19　レポート名をクリックし、最新の 5 つのジョブ インスタンスを表示します。ただし、[編集（Edit）] および [ジョブ シリーズ（Job Series）] ドロップダウン リストで使用可能なアクションを実行できなくなります。

特定のレポートタイプに対するレポートが保存されている場合は、レポートラウンチパッドから現在のレポートにアクセスできます。すべてのサブドメイン用に生成されたレポートを同時に変更したり更新することはできません。それぞれのサブドメインで、個々にレポートを開いたり、変更することができます。すべてのレポートを更新するには、サブドメインで生成されたレポートを削除し、仮想ドメインレポートを再生成して変更を反映させます。Prime Infrastructure サーバを新しいバージョンにアップグレードする場合、旧バージョンですでに変更および保存されたレポートを削除および再作成する必要があります。

レポート結果のカスタマイズ

多くのレポートでは、結果をカスタマイズして各種の情報を含めたり、除外したりすることができます。この機能をサポートしているレポートには、[カスタマイズ（Customize）]ボタンが表示されます。このボタンをクリックして[カスタム レポートの作成（Create Custom Report）]ページにアクセスし、レポートの結果をカスタマイズできます。

レポート結果をカスタマイズするには、次の手順に従います。

ステップ 1 カスタマイズするレポートを選択します。

a) 新しいレポートを作成します。**[レポート（Reports）]** > **[レポート起動パッド（Report Launch Pad）]** をクリックします。

b) 定期レポートをカスタマイズします。**[レポート（Reports）]**>**[保存済みレポートのテンプレート（Saved Report Templates）]** をクリックし、レポート名のハイパーリンクをクリックします。

ステップ 2 [レポートの詳細（Report Details）] ページで [カスタマイズ（Customize）] をクリックします。

ステップ 3 [カスタム レポートの作成（Create Custom Report）] ページで、必要な情報を入力し、[適用（Apply）] をクリックして変更を確定します。

ステップ 4 [レポートの詳細（Report Details）] ページで [保存（Save）] をクリックします。

CiscoPrimeInfrastructureでスケジュール設定されたレポート

レポートをスケジュール設定することで、レポートが毎時、毎日、毎週、または毎月自動的に実行され、結果が自動的に電子メールで、または SFTP を使用して別のサーバに送信されるようにすることができます。レポートをスケジュール設定する前に、レポートが保存されるリポジトリを指定する必要があります。

（注） SFTP機能の設定は必須ではありません。ただし、SFTP機能を使用する必要がある場合は、システム設定で外部リポジトリを保存する必要があります。設定が完了すると設定値を変更できるようになりますが、設定値を削除することはできません。

リポジトリのパスを設定するには、次の手順を実行します。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** を選択します。

ステップ 2 [システム設定（System Settings）] タブで、**[全般（General）] > [レポート（Report）]** を選択します。

ステップ 3 スケジュール設定されたレポートおよびオンデマンドレポートに対し、[リポジトリのパス（Repository Path）] および [ファイルの保持期間（File Retain Period）] を指定します。

ステップ 4 レポートを SFTP 経由で外部サーバに送信する必要がある場合は、[外部サーバ設定（External Server Settings）] の詳細情報（[サーバのホスト（Server Host）]、[サーバのポート（Server Port）]、[ユーザ名（User Name）]、[パスワード（Password）]、および [リポジトリのパス（Repository Path）]（外部サーバでのレポートの保存先）など）を指定します。

ステップ 5 [保存（Save）] をクリックします。

レポートをスケジュール設定するには、次の手順を実行します。

ステップ 6 **[レポート（Reports）] > [レポート起動パッド（Report Launch Pad）]** の順に選択します。

ステップ 7 [レポート起動パッド（Report Launch Pad）] ページで、スケジュール設定が必要なレポートを選択します。

ステップ 8 レポートのページで、[設定（Settings）] の各パラメータを更新します。

ステップ 9 [スケジューリング（Scheduling）] チェックボックスをオンにして、スケジュール設定を有効にします。

a) [エクスポート形式（Export Format）] として [CSV] または [PDF] を選択します。エクスポートされる CSV ファイルは、100 万レコードを保持できる単一の .csv ファイルです。

b) [宛て先（Destination）] に [ファイル（File）]、[電子メール（Email）]、または [SFTP（Sftp）] を選択します。宛て先として電子メールを選択した場合は、電子メール ID を入力します。

（注） [ファイル（File）] パラメータと [SFTP（Sftp）] パラメータは編集できません。パスは、[レポート設定（Report Settings）] から入力されます。

c) [開始日時（Start/Date time）] を選択します。

d) • 適切な [繰り返しオプション（Recurrence Option）] を選択します。

ステップ 10 レポートを実行するには、次のいずれかのオプションを選択します。

- [実行（Run）]：レポート設定を保存せずにレポートを実行します。
- [保存（Save）]：レポートをすぐに実行せずにこのレポート設定を保存します。スケジュール パラメータが入力済みの場合は、スケジュールされた日時にレポートが自動的に実行されます。
- [実行して保存（Run and Save）]：レポートの設定を保存し、ただちにレポートを実行する場合にクリックします。

- [保存してエクスポート（Save and Export）]：レポートを保存して実行し、結果をファイルにエクスポートする場合にクリックします。以下を要求するプロンプトが表示されます。
  - エクスポートするレポートのファイル形式（CSV または PDF）を選択します。エクスポートされる CSV ファイルは、100 万レコードを保持できる単一の .csv ファイルです。
  - レポートが生成されたら電子メールを送信するかどうかを選択します。このオプションを選択する場合は、宛先メールアドレスと電子メールの件名を入力し、エクスポートファイルを添付ファイルとして電子メールに含めるかどうかを選択する必要があります。
  - [OK] をクリックします。CSV ファイルが正しく開かない場合は、次のいずれかの場所で区切り記号としてカンマが指定されていることを確認してください。
    - [コントロールパネル（Control Panel）]>[地域と言語（Region/Language/Region and Language）]>[形式（Formats）]>[追加の設定（Additional Settings）]
    - Excel：[ファイル（File）]>[オプション（Options）]>[詳細設定（Advanced）]>[システムの桁区切りを使用する（Use System Separators）]

- [保存して電子メール送信（Save and Email）]：レポートを保存して実行し、結果をファイルとしてエクスポートし、そのファイルを電子メールで送信する場合にクリックします。以下を要求するプロンプトが表示されます。
  - エクスポートするレポートのファイル形式を選択します。

    （注）　ファイル サイズは 25 MB を超えてはなりません。

  - 宛先メール アドレスと電子メールの件名を入力します。
  - [OK] をクリックします。

- [キャンセル（Cancel）]：このレポートを実行も保存もせずに前のページに戻る場合にクリックします。

Prime Infrastructure でスケジュール設定されているレポートをすべて表示するには、**[レポート（Report）]>[スケジュール設定された実行結果（Scheduled Run Results）]** の順に選択します。

スケジュール設定されたレポートタスクは、それが実行される仮想ドメインの外部では表示されません。スケジュール設定されたレポートタスクの結果は、対応するドメインの [Scheduled Run Results] ページで表示できます。

スケジュールされた実行のリストは、レポートカテゴリ、レポートタイプ、タイムフレーム、およびレポート生成方法でソートできます。

[移動 (Go)] ボタンの横にあるアイコンをクリックすると、レポートが使用可能な場合にのみ、スケジュール設定されたレポートのリストを CSV にエクスポートできます。

このページのフィールドの詳細については、『Field Reference for Cisco Prime Infrastructure Reports』の「Scheduled Run Results」ページを参照してください。

保存済みレポートのテンプレート

保存されているレポート テンプレートは、**[レポート（Reports）]** > **[保存済みレポートテンプレート（Saved Report Templates）]** で使用できます。[Saved Report Templates] ページでは、レポート テンプレートを作成したり、保存されているレポート テンプレートを管理することができます。保存されているレポートは有効化、無効化、削除、コピーまたは実行することができます。また、レポートテンプレートをカテゴリ別、タイプ別、ステータス別にフィルタリングしてソートできます。**[移動(Go)]** ボタンの横にあるアイコンをクリックすると、レポートが利用可能な場合にのみ、保存したレポートを CSV にエクスポートできます。[保存済みレポートテンプレート（Saved Report Templates）]ページのフィールド、および保存されているレポート テンプレートのフィルタリングの詳細については、『Field Reference for Cisco Prime Infrastructure Reports』を参照してください。

[Saved Report Templates] ページには、次の情報が表示されます。

- [Report Title]：ユーザが割り当てたレポート名を示します。

このレポートの詳細を表示するには、レポート タイトルをクリックします。

- [Report Type]：特定のレポート タイプを示します。
- [Scheduled]：このレポートが有効か無効かを示します。
- [Virtual Domain]：このレポートがスケジュールされている仮想ドメインの名前を指定します。
- [今すぐ実行（Run Now）]：現在のレポートをただちに実行するには、**run** アイコンをクリックします。

（注） Prime Infrastructure バージョンのアップグレードを 3.7 にポストします。カラム レベルが更新された保存済みレポートを実行する場合は、レポートの詳細を1回保存してから、**[実行(Run)]** ボタンをクリックする必要があります。これは、レポートに対してオーナー/所有者によって行われた進捗が欠落しないようにするために推奨されます。

サブ仮想ドメインに対してドメインベースのレポートを実行すると、レポートには、現在ログインしている仮想ドメインにマッピングされているデバイス属性がすべて表示されます。

[Saved Report Templates（保存されたレポートテンプレート）] からレポートを選択し、**[コピー(Copy)]** ボタンをクリックして、その特定のレポートのレプリカを作成します。

（注） 単純なレポートの複製のみ作成でき、カスタム レポート、複合レポート、および期限切れレポートは作成できません。

Prime Infrastructure レポートのデータ保持期間

[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] > [データ保持期間（Data Retention）] での選択に基づいて設定されるデータ保持期間に応じて、レポートには毎時、毎日、または毎週のデータが表示されます。データは、次の基準に基づいてデータベースから取得されます。

期間が以下の場合：

1. 直近 1 日まで：データは raw テーブルから取得されます。
2. 直近 2 日から 4 週間：データは毎時の集約テーブルから取得されます。
3. 前月から直近 12 週間：毎日の集約テーブルから取得されます。
4. 直近 6 か月から直近 1 年：データは毎週の集約テーブルから取得されます。

パフォーマンス データの保持期間の有効範囲は次のとおりです。

1. 短期データ保持期間：1 ～ 31 日。
2. 長短期データ保持期間：2 ～ 756 日。
3. 中期データ保持期間：7 ～ 365 日。
4. 毎時データ保持期間：有効範囲は 1 ～ 31 時間です。
5. 日次データ保持期間：7 ～ 365 時間。
6. 週次データ保持期間：2 ～ 108 時間。

各テーブルの期間経過と最大レコード数を編集するには、[詳細設定（Advanced Settings）] オプションをクリックします。保存時に期間経過と最大レコード数の両方の値がデータベースに保存されます。次のデータ クリーンアップ ジョブの実行時に、期間経過または最大レコード数のいずれかの上限に最初に到達したほうに基づいて、プルーニングが実行されます。

Prime Infrastructure レポートの詳細については、『Field Reference for Cisco Prime Infrastructure Reports』を参照してください。

第 V 部

デバイスの設定

- デバイス設定の変更を自動化するテンプレートの作成 （503 ページ）
- ワイヤレス デバイスの設定 （587 ページ）
- ワイヤレス テクノロジーの設定 （785 ページ）
- ワイヤレス/データセンター設定タスクのスケジュール設定 （829 ページ）
- プラグ アンド プレイを使用した新しいデバイスの展開 （835 ページ）

第 25 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

この章は、次の内容で構成されています。

- 新しい設定テンプレートを作成する理由 （504 ページ）
- Prime Infrastructure を使用して設定テンプレートを作成する方法 （504 ページ）
- 既存のテンプレートを使用した新機能およびテクノロジー テンプレートの作成 （505 ページ）
- CLI テンプレートを作成するための前提条件 （506 ページ）
- 空白テンプレートを使用した新しい CLI 設定テンプレートの作成 （506 ページ）
- 既存のテンプレートを使用した新規 CLI 設定テンプレートの作成 （507 ページ）
- 例：CLI テンプレートを使用したパスワードの更新 （508 ページ）
- テンプレートへの変数の入力 （509 ページ）
- CLI 設定テンプレートのインポートとエクスポート （513 ページ）
- 新規複合テンプレートの作成 （514 ページ）
- タグを使用したテンプレートへのショートカットの作成 （514 ページ）
- デバイスへのテンプレートの展開 （515 ページ）
- コントローラ WLAN クライアント プロファイルの設定 （528 ページ）
- モバイル コンシェルジュ（802.11u）を使用するようにコントローラを設定する （529 ページ）
- AP グループを使用した WLAN 構成と展開の管理 （530 ページ）
- FlexConnect グループの一括更新の管理 （552 ページ）
- FlexConnect グループの一括作成 （552 ページ）
- 一括で FlexConnect グループへのユーザーの追加 （553 ページ）
- 一括で FlexConnect グループへの AP の追加 （555 ページ）
- コントローラ CPU と NPU 間のアクセス コントロール リスト トラフィック制御の設定 （556 ページ）
- コントローラでの不正 AP およびクライアント セキュリティ ポリシーの設定 （557 ページ）
- テンプレートを使用したスイッチの場所情報の設定 （567 ページ）

• 自律 AP 移行の影響の分析 （568 ページ）
• 設定テンプレートの展開 （569 ページ）
• グローバル変数 （572 ページ）
• 共有ポリシー オブジェクト （572 ページ）
• 設定グループとは （576 ページ）
• WLAN コントローラ設定グループとは （577 ページ）
• ワイヤレス設定テンプレートの作成 （583 ページ）

新しい設定テンプレートを作成する理由

Prime Infrastructure には、ネットワーク デバイスで変更を加えるために使用できる多数の設定済みの設定テンプレートが用意されています。これらについては、既存のテンプレートを使用した新機能およびテクノロジー テンプレートの作成 （505 ページ） で説明しています。

十分な権限を持っている場合は、ご使用の環境のニーズに完全に合う新しいテンプレートを作成し、そのテンプレートを他の人が使用できるようにすることもできます。複数のテンプレートをまとめて 1 つの複合テンプレートにグループ化するなど、テンプレートを必要に応じて単純または複雑にすることができます。最後に、設定グループを作成してテンプレートを特定のデバイスに関連付けることができます。

Prime Infrastructure には、テンプレートで使用できる設定済みの CLI コマンドが用意されています。また、新しい CLI コマンドを作成するために使用できる空白の CLI テンプレートも用意されています。それらは単独で使用することも、複合テンプレートで他のコマンドと組み合わせて使用することもできます。

設定テンプレートをどのように使用するかは、ネットワークの大きさ、組織内の設計者の数、およびデバイス構成の変化量などの要素によって異なる場合があります。次に例を示します。

- 設計者の人数が 1 人または 2 人で、デバイス構成の数も限定的な小規模なネットワークの場合は、「良好」とわかっている CLI 構成を一連のテンプレートにコピーすることから開始します。その後、それらを複合テンプレートに結合して、オペレータが利用できるようにすることができます。
- 多くの異なるデバイス構成を含む大規模ネットワークの場合は、標準化できる設定の識別を試行します。これにより、これらの標準への例外の量を制御したり、必要に応じて機能のオン/オフを切り替えることができます。

PrimeInfrastructureを使用して設定テンプレートを作成する方法

Cisco Prime Infrastructure には、次のタイプの機能レベルの設定テンプレートがあります。

- 機能およびテクノロジーテンプレート：デバイスの設定の機能またはテクノロジーに固有な設定。

- CLIテンプレート：独自のパラメータに基づいて作成されるユーザ定義テンプレート。CLIテンプレートを使用すると、コンフィギュレーションの要素を選択できます。Prime Infrastructureには、実際の値や論理ステートメントと置き換える変数が用意されています。Cisco Prime LAN Management Systemからテンプレートをインポートすることもできます。
- 複合テンプレート：2つ以上の機能テンプレートまたはCLIテンプレートを1つのテンプレートにグループ化したもの。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ます。

関連トピック

空白テンプレートを使用した新しいCLI設定テンプレートの作成 （506ページ）
新規複合テンプレートの作成 （514ページ）
既存のテンプレートを使用した新機能およびテクノロジーテンプレートの作成 （505ページ）

既存のテンプレートを使用した新機能およびテクノロジーテンプレートの作成

機能およびテクノロジーテンプレートは、デバイスの設定内の特定の機能またはテクノロジーに焦点を合わせるデバイス構成に基づくテンプレートです。

Prime Infrastructure にデバイスを追加すると、Prime Infrastructure は追加されたモデルのデバイス設定を収集します。Prime Infrastructure では、すべてのデバイス タイプに対してすべての設定オプションがサポートされているわけではありません。設定する特定の機能またはパラメータに対して、Prime Infrastructure に機能およびテクノロジー テンプレートがない場合は、CLIテンプレートを作成します。

機能およびテクノロジーテンプレートは、設定変更の展開を単純化します。たとえば、SNMPの機能およびテクノロジーテンプレートを作成してから、指定したデバイスにすばやく適用できます。複合テンプレートにこのSNMPテンプレートを追加することもできます。その後、SNMPテンプレートを更新した際に、そのSNMPテンプレートが含まれる複合テンプレートには、最新の変更が自動的に適用されます。

機能およびテクノロジー テンプレートを作成するには、次の手順を実行します。

ステップ1 [設定（Configuration）] > [テンプレート（Templates）] > [機能およびテクノロジー（Features and Technologies）] の順に選択します。

ステップ2 左側の [Features and Technologies] メニューで、作成するテンプレートのタイプを選択します。

ステップ3 そのテンプレートのフィールドに値を入力します。

特定のデバイス タイプだけに適用する機能テンプレートを作成している場合は、[デバイス タイプ（Device Type）] フィールドには、該当するデバイス タイプだけがリストされ、選択を変更することはできません。デバイス タイプを指定することで、不一致を防止できます。つまり、設定を作成して、間違ったデバイスにその設定を適用することはできません。

ステップ 4 [新しいテンプレートとして保存（Save as New Template）] をクリックします。テンプレートを保存した後、デバイスに適用します。

ステップ 5 テンプレートの展開のステータスを確認するには、[Administration] > [Dashboard] > [Jobs Dashboard] の順に選択します。

後続の設定テンプレートの導入に関する導入パラメータを変更するには、コンフィギュレーション ジョブを選択し、[スケジュールの編集（Edit Schedule）] をクリックします。

関連トピック

ウィザードを使用した設定グループの展開フロー （516 ページ）

CLI テンプレートを作成するための前提条件

CLI テンプレートを作成するには、次の条件を満たしている必要があります。

- CLI の専門知識を持ち、CLI をよく理解し、Apache VTL で CLI を記述できる。
- 作成する CLI を適用可能なデバイスについて理解している。
- Cisco Prime Infrastructureでサポートされるデータ型を理解している。
- テンプレート内の設定を理解し、手動でラベルを付けることができる。

空白テンプレートを使用した新しい CLI 設定テンプレートの作成

テンプレートを使用して、一連の再利用可能なデバイス設定コマンドを定義します。CLIテンプレートとその使用法の説明は、**[設定（Configuration）] > [テンプレート（Templates）] > [機能およびテクノロジー（Features & Technologies）]** を選択し、続いて **[CLI テンプレート（CLI Templates）]** を選択すると、Web GUI に表示されます。

Cisco Prime Infrastructure に付属のテンプレートを編集する場合は、そのテンプレートのコピーを作成し、コピーに新しい名前を付けて編集します。既存のテンプレートを使用した新規 CLI 設定テンプレートの作成 （507 ページ）を参照してください。

作成したテンプレートは [マイ テンプレート（My Templates）] に保存されます。

ステップ 1 **[設定（Configuration）] > [テンプレート（Templates）] > [機能およびテクノロジー（Features & Technologies）]** の順に選択します。

ステップ 2 [CLI テンプレート（CLI Templates）] を展開し、[CLI] を選択します。

ステップ 3 [テンプレートの基本設定（Template Basic）] エリアの必須フィールドに入力します。

ステップ 4 選択したデバイス全体にわたって選択した一連のインターフェイスにテンプレートを適用する場合は、[ポート（Ports）] オプション ボタンをクリックします。
テンプレートは、ポート ベースのテンプレートとしてタグ付けされます。

ステップ 5 [テンプレートの詳細（Template Detail）] エリアで、次のように設定します。

- [変数の追加（Add Variable）] タブをクリックします。これにより、テンプレートの適用時に値を定義する変数を指定できます。[行の追加（Add Row）] をクリックし、新しい変数のパラメータを入力してから、[保存（Save）] をクリックします。

  または

  [グローバル変数の追加（Add Global Variable）] にグローバル変数名の最初の数文字を入力してグローバル変数を検索し、適用する目的のグローバル変数を選択します。

- CLI 情報を入力します。[CLI] タブでは、Apache VTL を使用してコードを入力する必要があります。『Apache Velocity Language Template Guide』を参照してください。

- 変数を表示するには、[フォーム ビュー（Form View）]（読み取り専用ビュー）をクリックします。

ステップ 6 テンプレートを保存します。[新しいテンプレートとして保存（Save as New Template）] をクリックして、[マイテンプレート（My Template）] でテンプレートを保存するフォルダを指定し、[保存（Save）] をクリックします。

関連トピック

ウィザードを使用した CLI テンプレートの展開フロー （517 ページ）
データ型 （509 ページ）
CLI テンプレートのデータベース変数の管理 （510 ページ）

既存のテンプレートを使用した新規 CLI 設定テンプレートの作成

新しい設定テンプレートを作成するのに最も簡単な方法は、同様の既存のテンプレートを見つけてコピーし、そのコピーを編集することです。作成済みのテンプレートも、この手順を使用して編集できます（編集できるテンプレートは、自分が作成したものだけです）。

ステップ 1 **[構成（Configuration）] > [テンプレート（Templates）] > [機能およびテクノロジー（Features & Technologies）]** の順に選択します。

ステップ 2 [CLI テンプレート（CLI Templates）] を展開し、[システム テンプレート - CLI（System Templates - CLI）] を選択します。

ステップ 3 右側のパネルで、コピーするテンプレートを見つけて、そのテンプレート名の横に表示されている [i] アイコンにマウスのカーソルを重ね、表示されるポップアップ ウィンドウで [複製（Duplicate）] をクリックします。

ステップ 4 [複製テンプレートの作成（Duplicate Template Creation）] ダイアログで、新しいテンプレートを保存するフォルダ（[マイ テンプレート（My Templates）] 内のフォルダ）を指定し、[OK] をクリックします。

たとえば、**[CLIテンプレート（CLI Templates）] > [システムテンプレート-CLI（System Templates - CLI）]** の下にあるテンプレートをコピーすると、そのテンプレートはデフォルトで **[マイテンプレート（My**

Templates）] > [CLIテンプレート（CLI Templates）] > [システムテンプレート-CLI（ユーザ定義）（System Templates - CLI (User Defined)）][マイテンプレート（My Templates）] > [CLIテンプレート（ユーザ定義）（CLI Templates (User Defined)）] > [システムテンプレート-CLI（ユーザ定義）（System Templates - CLI (User Defined)）] の下に保存されます。

ステップ 5 「空白テンプレートを使用した新しい CLI 設定テンプレートの作成」で説明されている手順に従って検証基準と CLI コンテンツを追加します。

例：CLI テンプレートを使用したパスワードの更新

これらの地域のデバイスには、ロケーション属性が割り当てられている必要があります。

ステップ 1 4 つグループ（North Region、South Region、East Region、および West Region）が作成されていない場合は、次の手順を実行します。

a) **[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ネットワーク デバイス（Network Devices）]（歯車アイコン）** を選択し、マウスのカーソルを [ユーザ定義（User Defined）] の上に合わせて、[サブグループを追加（Add SubGroup）] をクリックします。

b) [Create Sub-Group] 領域で、以下のように入力します。

- グループ名：North Region
- グループの説明：North Region のデバイスのリスト
- フィルタ：**[ロケーション（Location）] > [次を含む（Contains）] > [SJC-N]**

  デバイスのロケーションを決定するには、**[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ネットワーク デバイス（Network Devices）]（歯車アイコン）> [列（Columns）] > [ロケーション（Location）]** を選択します。

新しいグループのデバイスが [デバイス ワーク センター（Device Work Center）] > [ユーザ定義（User Defined）] > [ノース（North）] の下に表示されます。

c) South、East、および West 地域についても同じ手順を実行します。

ステップ 2 パスワード テンプレートを展開するには、次の手順を実行します。

a) [Configuration] > [Templates] > [Features and Technologies] > [CLI Templates] > [System Templates-CLI] の順に選択します。

b) [Enable Password-IOS] テンプレートを選択し、[Deploy] をクリックします。

c) [Device Selection] 領域で、ユーザ定義グループを開き、[North Region] および [South Region] グループを選択します。

d) [Value Selection] 領域で、新しいイネーブル パスワードを入力して確認し、[Apply] をクリックします。

e) [スケジュール（Schedule）] 領域で、ジョブの名前、新しいテンプレートを適用する日時を入力（または [現在（Now）] をクリック）し、[OK] をクリックします。

ステップ 3 ジョブの実行後、**[管理（Administration）] > [ダッシュボード（Dashboards）] > [ジョブ ダッシュボード（Job Dashboard）]** を選択し、ジョブのステータスを表示します。

テンプレートへの変数の入力

次のトピックでは、テンプレートに変数を入力する場合に役立つ情報を提供します。

- データ型 （509 ページ）
- CLI テンプレートのデータベース変数の管理 （510 ページ）
- 検証式の使用 （511 ページ）
- マルチライン コマンドの追加 （511 ページ）
- イネーブル モード コマンドの追加 （512 ページ）
- インタラクティブ コマンドの追加 （520 ページ）

データ型

表 1 に、[変数の管理（Manage Variables）] ページで設定できるデータ型を示します。

データ タイプ	説明
文字列	CLIテンプレートのテキストボックスを作成できます。検証式とデフォルト値を指定するには、行を展開して [Default Value] および [Validation Expression] フィールドを設定します。
整数	数値のみを受け入れるテキストボックスを作成できます。整数の範囲を指定する場合は、行を展開して [Range From] および [To] フィールドを設定します。検証式とデフォルト値を指定するには、行を展開して [Default Value] および [Validation Expression] フィールドを設定します。
DB	データベースタイプを指定できます。CLIテンプレートのデータベース変数の管理 （510 ページ）を参照してください。
DB_Dropdown	DB クエリに基づいたデバイス固有の値を一覧表示できます。値を指定するには、行を展開して [値（Value）] フィールドを設定します（UI に表示される複数のリストにはコンマ区切り値を使用）。
IPv4 アドレス（IPv4 Address）	CLI テンプレートに IPv4 アドレスのみを受け入れるテキスト ボックスを作成できます。検証式とデフォルト値を指定するには、行を展開して [Default Value] および [Validation Expression] フィールドを設定します。

Drop-down	CLI テンプレートのリストを作成できます。検証式とデフォルト値を指定するには、行を展開して [デフォルト値（Default Value）] フィールドを設定します（UI に表示される複数のリストにはコンマ区切り値を使用）。値を指定するには、行を展開して [値（Value）] フィールドを設定します（UI に表示される複数のリストにはコンマ区切り値を使用）。
チェックボックス（Check box）	CLI テンプレートのチェックボックスを作成できます。 検証式とデフォルト値を指定するには、行を展開して[デフォルト値（Default Value）] フィールドを設定します。デフォルト値を指定するには、行を展開して [デフォルト値（Default Value）] フィールドを設定します。
オプション ボタン（Radio Button）	CLIテンプレートのオプションボタンを作成できます。検証式とデフォルト値を指定するには、行を展開して [デフォルト値（Default Value）] フィールドを設定します。値を指定するには、行を展開して [値（Value）] フィールドを設定します（UIに表示される複数のリストにはコンマ区切り値を使用）。
テキスト領域	CLI テンプレートに複数の値を許可するテキスト領域を作成できます。検証式とデフォルト値を指定するには、行を展開して [デフォルト値（Default Value）] および [検証式（Validation Expression）] フィールドを設定します。

CLI テンプレートのデータベース変数の管理

次のような場合は、データベース（DB）変数を使用できます。

- DB 変数が CLI テンプレートでデータ型の 1 つである場合。デバイス固有のコマンドを生成するために DB 変数を使用できます。
- DB 変数が事前定義された変数である場合。事前定義された DB 変数の一覧を表示するには、場所 folder/opt/CSCOlumos/conf/ifm/template/inventoryTagsInTemplate にある CLITemplateDbVariablesQuery.properties ファイルを参照します。
- たとえば、SysObjectID、IPAddress、ProductSeries、ImageVersion は DB 変数です。デバイスが Prime Infrastructure に追加されると、デバイスの完全な詳細が DB 変数に収集されます。つまり、デバイスの OID は SysObjectID に、製品シリーズは ProductSeries に、デバイスのイメージ バージョンは ImageVersion にというように収集されます。
- DB 変数によって収集されたデータを使用して、正確なコマンドをデバイスに生成できます。
- [Type] フィールドで DB 変数を選択できます（[Managed Variables] ページを使用）。名前フィールドを展開して、使用する DB 変数のいずれかをデフォルト値のフィールドに入力します。
- デバイスが検出され、Prime Infrastructure に追加された際に、インベントリ収集中に集められたデータベース値を使用して、CLI テンプレートを作成できます。

（注） Enterprise JavaBeans クエリ言語（EJB QL）を使用してカスタマイズされたクエリを作成することができますが、これを試行できるのは高度な開発者のみです。CLITemplateDbVariablesQuery.properties ファイルで定義された変数のみを使用することを推奨します。

検証式の使用

[検証式（Validation Expression）] で定義した値は、関連付けられているコンポーネント値で検証されます。たとえば、設計フローでデフォルト値と検証式の値を入力した場合、設計フロー中に検証されます。つまり、デフォルト値が検証式に入力された値と一致しない場合、設計フローで取得エラーが発生します。

（注） 検証式の値は、文字列データ型フィールドにのみ機能します。

たとえば、**[設定（Configuration）]** > **[テンプレート（Templates）]** > **[機能およびテクノロジー（Features and Technologies）]** の順に選択し、**[CLI テンプレート（CLI Templates）]** > **[CLI]** を選択します。[テンプレートの詳細（Template Detail）] 領域で、[変数の追加（Add Variable）] タブをクリックして変数のリストを表示します。[変数の追加（Add Variable）] タブで追加のプラス記号（+）をクリックし、CLI テンプレートに行を追加します。[タイプ（Type）] フィールドで [文字列（String）] を選択し、残りの値を入力して、[保存（Save）] をクリックします。変数のリストで、この新しい変数の詳細を展開し、正規表現を設定します。そのテキストボックスではスペースは許可されません。[検証式（Validation Expression）] フィールドに、次の式を入力します。

```
^[\S]+$
```

デフォルト値（オプション）：ncs

この値は、[検証式（Validation Expression）] フィールドの正規表現と一致する必要があります。

テンプレートを保存してからデバイスを選択します。テキストフィールドにスペースを入力してみてください。正規表現のエラーが発生するはずです。

マルチライン コマンドの追加

[CLI コンテンツ（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>
```

引数の説明

- <MLTCMD> および </MLTCMD> タグは大文字と小文字が区別され、大文字で入力される必要があります。
- マルチライン コマンドは、<MLTCMD> タグと </MLTCMD> タグで囲む必要があります。
- タグの先頭にはスペースを使用できません。
- <MLTCMD> と </MLTCMD> タグは単一行では使用できません。

例 1：

```
<MLTCMD>banner_motd Welcome to
Cisco. You are using
Multi-line commands.
</MLTCMD>
```

例 2：

```
<MLTCMD>banner motd ~ ${message}
</MLTCMD>
```

{message} はマルチライン入力変数です。

マルチライン バナー コマンドを使用する場合の制限事項

Prime Infrastructure はマルチライン バナー コマンドをサポートしていません。次の例に示すように、*banner file xyz format* 形式を使用できます。

```
#conf t
Enter configuration commands, one per line. End with Ctrl-Z.
(config)#parameter-map type webauth global
(config-params-parameter-map)# type webauth
(config-params-parameter-map)#banner file tftp://209.165.202.10/banner.txt
(config-params-parameter-map)#^Z
#more tftp://192.168.0.0/banner.txt
Disclaimer:
Usage of this wireless network is restricted to authorized users only.
Unauthorized access is strictly forbidden.
All accesses are logged and can be monitored.
#
```

イネーブル モード コマンドの追加

CLI テンプレートにイネーブル モード コマンドを追加する場合は、次の構文を使用します。

```
#MODE_ENABLE<<commands >>#MODE_END_ENABLE
```

CLI 設定テンプレートのインポートとエクスポート

次の項目で、設定テンプレートのエクスポート方法とインポート方法を説明します。テンプレートはエクスポートでき、テンプレートには .xml ファイル名が付けられます。また、テンプレートが複数ある場合は zip ファイルとしてエクスポートされます。

- 複数の設定テンプレートをエクスポートする場合は、.xml ファイルが zip ファイルに配置され、**Exported Templates** というプレフィックス名が付与されます。
- 単一のファイルのエクスポートとインポートは .xml ファイルとして実行されます。
- 個別のファイルを選択するか、または zip ファイルをインポートすることで、複数の .xml ファイルをインポートできます。
- CLI テンプレートをインポートする場合、ファイルに含まれているユーザ定義のグローバル関数は自動的にはインポートされません。これらの変数は CLI テンプレートに手動で追加する必要があります。

ステップ 1 [設定（Configuration）]>[テンプレート（Templates）]>[機能およびテクノロジー（Features & Technologies）]の順に選択します。>[テンプレート（Templates）]>[機能およびテクノロジー（Features & Technologies）]の順に選択します。

ステップ 2 [CLIテンプレート（CLI Templates）] フォルダを展開してから、[システムテンプレート（System Templates）]をクリックします。

ステップ 3 設定テンプレートをエクスポートするには、次の手順を実行します。

a) 右側のパネルでエクスポートするテンプレートを選択し、[エクスポート（Export）] をクリックします。

b) 目的の場所にファイルを保存します。

ステップ 4 設定テンプレートをインポートするには、次の手順を実行します。

a) [CLI テンプレート（CLI Templates）] フォルダで、**CLI** の横にある [i] の上にマウス カーソルを合わせます。

b) [すべてのテンプレートの表示（Show All Templates）] をクリックし、[インポート（Import）] をクリックします。

c) [テンプレートのインポート（Import Templates）] ダイアログボックスで、テンプレートのインポート先の [マイテンプレート（My Templates）] フォルダを選択し、[テンプレートの選択（Select Templates）]をクリックしてインポートするファイルまで移動します。

d) 選択したテンプレートを確認し、[OK] をクリックします。

（注） デフォルトでは、インポートされたテンプレートの作成者名はログイン中のユーザと同じではありません。

新規複合テンプレートの作成

事前に設定したテンプレートやユーザが作成したテンプレートのすべてを単一の複合テンプレートに追加できます。このテンプレートは、必要としている個々の機能テンプレートすべてを集約します。また、複合テンプレートを作成すると、メンバーテンプレートを実行する順序も指定できます。複合テンプレートを使用して、単一のデバイスまたはデバイスのグループに変更を加えることができます。

ステップ 1 **[設定（Configuration）] > [テンプレート（Templates）] > [機能およびテクノロジー（Features & Technologies）]** の順に選択します。

ステップ 2 [複合テンプレート（Composite Templates）] フォルダを展開し、[複合テンプレート（Composite Templates）] を選択します。

ステップ 3 [テンプレートの基本設定（Template Basic）] 領域に、テンプレートの名前を入力します。

ステップ 4 [テンプレートの詳細（Template Detail）] 領域で、複合テンプレートに含めるテンプレートを選択します。矢印を使用し、デバイスに展開する順序でテンプレートを配置します。たとえば、ACL を作成し、インターフェイスに関連付けるには、まずACLテンプレートを配置し、その後にインターフェイステンプレートを続けます。

ステップ 5 [新しいテンプレートとして保存（Save as New Template）] をクリックします。テンプレートを保存した後にデバイスに適用します（「ウィザードを使用した複合テンプレートの展開フロー」を参照してください）。

タグを使用したテンプレートへのショートカットの作成

タグをテンプレートに適用すると、そのテンプレートは [マイ タグ（My Tags）] フォルダのリストに表示されます。設定テンプレートにタグ付けすることで、以下を行う際に役立ちます。

- 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

既存のテンプレートにタグ付けするには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [テンプレート（Templates）] > [機能およびテクノロジー（Features & Technologies）]** の順に選択します。

ステップ 2 [マイ テンプレート（My Templates）] フォルダを展開し、タグを付けるテンプレートを選択します。

ステップ 3 [次のタグを使用（Tag as）] テキスト ボックスにタグ名を入力し、[保存（Save）] をクリックします。

デバイスへのテンプレートの展開

ここでは、構成テンプレートを使用してデバイスにコマンドグループを展開（実行）する方法について説明します。

- デバイスのグループにテンプレートを展開するための設定グループの作成
- ウィザードを使用した設定グループの展開フロー
- ウィザードを使用した CLI テンプレートの展開フロー
- ウィザードを使用した複合テンプレートの展開フロー
- 設定グループを使用しないデバイスへのテンプレートの展開

デバイスのグループにテンプレートを展開するための設定グループの作成

複数のデバイスに同じ設定が必要な場合、それらのデバイスとデバイスに共通して適用できるテンプレートを含む設定グループを作成できます。設定グループを作成することで、新しいテンプレートを展開するデバイスを覚えていなくても、新しいテンプレートをすぐに適用できます。

複合テンプレートではサイズの小さい複数のテンプレートを1つにグループ化できる一方、設定グループは、テンプレートとデバイスのグループとの「関係」およびコマンドの実行順を指定します。

ステップ 1 **[構成（Configuration）] > [テンプレート（Templates）] > [設定グループ（Configuration Groups）]** の順に選択します。

ステップ 2 [設定グループの基本（Configuration Group Basic）] 領域で、名前を入力します。

ステップ 3 選択可能なデバイスを表示するには、[テンプレートの選択（Template Selection）] 領域で [追加（Add）] をクリックし、テンプレートを選択して1つ以上のテンプレートを追加します。これにより、[デバイスタイプ（Device Type）] フィールドにも値が取り込まれます。

ステップ 4 さらにテンプレートを追加するには、[テンプレートの選択（Template Selection）] 領域で [追加（Add）] をクリックします。相互に排他的なテンプレート（たとえば、Add-Host-Name-IOS と Add-Host-Name-IOS-XR）を同時に選択することはできません。

ステップ 5 テンプレートを展開するデバイスを選択し、[次へ（Next）] をクリックして入力オプションを選択します。[選択（Select）] トグル ボタンをクリックして、デバイスの [グループ別（By Group）] オプションからデバイスを選択できます。

ステップ 6 [デバイスの選択（Device Selection）] 領域で、設定グループに追加するデバイスを選択します。

ステップ 7 複数のテンプレートを使用する場合、テンプレートを選択して上矢印または下矢印をクリックすることで、テンプレートがリストされる順序を変更できます。

ステップ 8 [新しい設定グループとして保存（Save as New Configuration Group）] をクリックします。

ウィザードを使用した設定グループの展開フロー

（注） この展開フローは、コントローラ ベースのテンプレートには適用されません。

ステップ 1 設定グループを作成したら、[展開（Deploy）] をクリックします。[テンプレートの展開 - 準備とスケジュール（Template Deployment -Prepare and Schedule）] ウィザード ページが開きます。

ステップ 2 [テンプレート（Templates）] 領域で、設定グループに追加するテンプレートを表示します。

ステップ 3 [デバイスに展開（Deployed on Devices）] 領域および設定グループの作成中に、設定グループの作成時に選択したデバイスを表示します。

ステップ 4 [値の割り当て（Value Assignment）] 領域で、[テンプレートの選択（Select Template）] ドロップダウン リストから、CLIテンプレートと適切なデバイスを選択します。テンプレートを展開するデバイスの詳細や、CLI プレビューの詳細などを表示できます。[適用（Apply）] をクリックします。

ステップ 5 （任意）[スケジュール（Schedule）] 領域で展開ジョブをスケジュールします。

- わかりやすい展開ジョブ名を付けてから、ただちに実行するか、後で実行するかを指定します。
- また、時間単位、日次、週次、月次、または年次単位で定期的にジョブを実行するようにスケジュールできます。
- 次のジョブ オプションを設定できます。

  失敗ポリシー（Failure Policy）：

  - [失敗を無視して続行（Ignore failure and continue）]：これはデフォルトのオプションです。 デバイスは、テンプレートの展開にランダムに選択されます。ジョブを実行できないデバイスがあった場合、そのデバイスをスキップし、引き続き残りのデバイスでジョブを実行します。ジョブ結果には、選択したすべてのデバイスの成功/失敗情報が表示されます。
  - [失敗で停止（Stop on failure）]：ジョブがデバイスでの実行に失敗した場合、そのジョブは停止します。 ジョブ結果は、ジョブが正常に実行されたデバイスと、テンプレートの展開が行われなかった他のデバイスについてのみ更新されます。「Not Attempted」メッセージが表示されます。展開のために選択されたデバイスの順序は、[Value assignment] ペインのデバイスの順序と同じです。
  - [実行コンフィギュレーションをスタートアップにコピー（Copy Running Config to Startup）]：テンプレートの展開ジョブが成功すると、デバイスの実行コンフィギュレーションがスタートアップ コンフィギュレーションにコピーされます。
  - [展開後にコンフィギュレーションをアーカイブ（Archive Config after deploy）]：新しい設定アーカイブ ジョブを作成し、テンプレートを正常に展開した後で、デバイスのコンフィギュレーションをアーカイブします。

ステップ 6 [概要（Summary）] 領域で、展開の概要を表示します。

ステップ 7 [OK] をクリックしてテンプレートを展開します。

ステップ 8 ジョブのステータスを表示するには、ポップアップ ダイアログボックスで [ジョブのステータス（Job Status）] をクリックして [ジョブ ダッシュボード（Job Dashboard）] を起動します。

ウィザードを使用した CLI テンプレートの展開フロー

ステップ 1 CLI テンプレートを作成した後、[展開（Deploy）] をクリックします。[展開（Deployment）] ウィザード ページが開きます。

ステップ 2 [デバイスの追加（Add devices）] テーブルから、テンプレートを展開するデバイスを選択します。選択したデバイスが [展開するデバイス（Devices to deploy）] テーブルに表示されます。[選択（Select）] トグル ボタンをクリックして、デバイスの [グループ別（By Group）] オプションからデバイスを選択できます。

ステップ 3 ポート ベースの設定の場合は、[次へ（Next）] をクリックしてポートを選択します。

（注） [ポートの選択（Select Ports）] オプションは、テンプレート ページでテンプレート タイプとして [ポート（Port）] を選択している場合のみ、展開ウィザードで使用可能になります。

ステップ 4 [選択（Select）] トグル ボタンをクリックすると、[ポート別（By Ports）] オプションまたは [ポートグループ別（By Port Groups）] オプションからポートを選択できます。選択したデバイスごとに、少なくとも 1 つのポートを選択する必要があります。

ステップ 5 [次へ（Next）] をクリックして入力オプションを選択します。

ステップ 6 テンプレートを展開するモードを選択します。オプションは、[ワークフロー（Work Flow）] および [CSV のエクスポート（Export CSV）]/[CSV のインポート（Import CSV）] です。

ステップ 7 [ワークフロー（Work Flow）] オプションをクリックし、[次へ（Next）] をクリックします。ステップ *8* を参照してください。

ステップ 8 または、[CSV のエクスポート（Export CSV）]/[CSV のインポート（Import CSV）] オプションをクリックし、CSV のエクスポート/インポート メカニズムを使用して選択したデバイスのテンプレート プロパティをすべて更新します。

a) CSV ファイル内の設定値の入力時に省略可能フィールドをスキップする場合は、[省略可能パラメータも必要ですか（Do you want Optional Parameters）] チェックボックスをオフにします。
b) [CSV のエクスポート（Export CSV）] をクリックし、ローカル システムに CSV テンプレートをダウンロードします。
c) ダウンロードした CSV テンプレートで個々のデバイスの設定値を入力します。
d) [CSV のインポート（Import CSV）] をクリックし、更新された CSV ファイルをアップロードします。入力値は自動的に更新されます。
e) [次へ（Next）] をクリックして値を入力します。

ステップ 9 [入力値（Input Values）] タブでは、[フォーム（Form）] ビューと [CLI] ビューを切り替えることができます。[入力値（Input Values）] タブで以下を設定します。

a) 各テンプレートのすべての必須フィールドに入力してから、[適用（Apply）] をクリックします。

検証が成功すると、選択したテンプレートの周囲の円の境界が緑色に変わります。

（注） 検証メッセージが正常に表示された場合は、変更がワークフロー内の選択したデバイスにのみ適用されたことを意味します。設定を完了するには、手順の残りのステップを実行します。

ステップ 10 必要な設定値を入力したら、[次へ（Next）] または [CLI] をクリックして、デバイスおよびテンプレートの設定値を確認します。

ステップ 11 必要に応じて、[展開のスケジュール設定（Schedule Deployment）] タブを使用して展開ジョブをスケジュール設定します。

- わかりやすい展開ジョブ名を付けてから、ただちに実行するか、後で実行するかを指定します。
- また、時間単位、日次、週次、月次、または年次単位で定期的にジョブを実行するようにスケジュールできます。
- 次のジョブ オプションを設定できます。

  失敗ポリシー（Failure Policy）：

  - [失敗を無視して続行（Ignore failure and continue）]：これはデフォルトのオプションです。 デバイスは、テンプレートの展開にランダムに選択されます。ジョブを実行できないデバイスがあった場合、そのデバイスをスキップし、引き続き残りのデバイスでジョブを実行します。ジョブ結果には、選択したすべてのデバイスの成功/失敗情報が表示されます。
  - [失敗で停止（Stop on failure）]：ジョブがデバイスでの実行に失敗した場合、そのジョブは停止します。 ジョブ結果は、ジョブが正常に実行されたデバイスと、テンプレートの展開が行われなかった他のデバイスについてのみ更新されます。「Not Attempted」メッセージが表示されます。展開のために選択されたデバイスの順序は、[Value assignment] ペインのデバイスの順序と同じです。
  - [実行コンフィギュレーションをスタートアップにコピー（Copy Running Config to Startup）]：テンプレートの展開ジョブが成功すると、デバイスの実行コンフィギュレーションがスタートアップ コンフィギュレーションにコピーされます。
  - [展開後にコンフィギュレーションをアーカイブ（Archive Config after deploy）]：新しい設定アーカイブ ジョブを作成し、テンプレートを正常に展開した後で、デバイスのコンフィギュレーションをアーカイブします。

ステップ 12 [次へ（Next）] をクリックしてジョブ展開サマリーを表示します。

ステップ 13 [展開サマリー（Deployment Summary）] タブに、各デバイスの CLI ビューが表示されます。

ステップ 14 [終了（Finish）] をクリックしてテンプレートを展開します。

ステップ 15 ジョブのステータスを表示するには、ポップアップ ダイアログボックスで [ジョブのステータス（Job Status）] をクリックして [ジョブ ダッシュボード（Job Dashboard）] を起動します。

（注） SG220 デバイスは設定テンプレートの展開をサポートしませんが、SG300 および SG500 デバイスは CLI テンプレート展開をサポートします。ただし、SG300 デバイスおよび SG500 デバイスはどちらも、次のシステム CLI テンプレートのみサポートします。

- APIC ブートストラップ
- バナー構成 - IOS（Banner Configuration-IOS）
- Best_Practice_Access_3k
- Best_Practice_Access_4k
- Best_Practice_Global
- 認証局 - IOS（Certificate Authority-IOS）
- SNMPv3 の設定
- VLAN の設定
- Configure_Access_Port
- クリプト マップの設定
- DNS の設定
- EEM Environmental Variables
- イネーブルパスワード - IOS（Enable Password-IOS）
- EtherChannel
- HTTP SWIM イメージ アップグレード テンプレート
- HTTP-HTTPSサーバおよびWSMAの構成 - IOS（HTTP-HTTPS Server and WSMA Configuration-IOS）
- ローカル管理ユーザー
- プラグアンドプレイ ブートストラップ
- RADIUS_AUTH
- Radius Acct. サーバ
- Radius 設定-IOS
- リロード構成 - IOS（Reload Configuration-IOS）
- TACACS サーバ
- TACACS-POST-PNP
- トラップ受信者
- stp

インタラクティブ コマンドの追加

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。

[CLI Content] 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
```

<IQ> および <R> タグは大文字と小文字が区別され、大文字で入力する必要があります。

次に例を示します。

```
#INTERACTIVE
crypto key generate rsa general-keys <IQ>yes/no<R> no
#ENDS_INTERACTIVE
```

（注） 対話型の質問ではすべて、<IQNONEWLINE> タグを <IQNONEWLINE> タグに置き換える必要があります。これらの質問では、どのコントローラー デバイスでもコマンドでデフォルトの <return> または改行文字は必要ありません。たとえば、

```
#INTERACTIVE
transfer download start <IQNONEWLINE>y/N<R>y<IQNONEWLINE>y/N<R>y
#ENDS_INTERACTIVE
```

（注） <IQ> タグは、対話型の質問に正規表現を使用します。パターンを照合するには、有効な正規表現を使用する必要があります。

Format

```
#INTERACTIVE
commands<IQ>interactive question<R>response
#ENDS_INTERACTIVE
```

Example for invalid content used in interactive question

```
#INTERACTIVE
save config<IQ>Are you sure you want to save? (y/n)<R>y
#ENDS_INTERACTIVE
```

間に質問マーク「?」を使用すると無効になり、パターンと一致しません。

Example for valid content used in interactive question

```
#INTERACTIVE
save config<IQ>(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

インタラクティブ イネーブル モード コマンドを組み合わせるには、次の構文を使用します。

```
#MODE_ENABLE
#INTERACTIVE
commands<IQ>interactive question<R>response
#ENDS_INTERACTIVE
#MODE_END_ENABLE
```

次に例を示します。

```
#MODE_ENABLE
#INTERACTIVE
mkdir <IQ>Create directory<R>XXX
#ENDS_INTERACTIVE
#MODE_END_ENABLE
```

インタラクティブ マルチライン コマンドの追加

以下は、複数行を含むインタラクティブ コマンドの例です。

```
#INTERACTIVE
macro name EgressQoS<IQ>Enter macro<R><MLTCMD>mls qos trust dscp
wrr-queue queue-limit 10 25 10 10 10 10 10
wrr-queue bandwidth 1 25 4 10 10 10 10
priority-queue queue-limit 15
wrr-queue random-detect 1
wrr-queue random-detect 2
wrr-queue random-detect 3
wrr-queue random-detect 4
wrr-queue random-detect 5
wrr-queue random-detect 6
wrr-queue random-detect 7
wrr-queue random-detect max-threshold 1 100 100 100 100
wrr-queue random-detect min-threshold 1 80 100 100 100
wrr-queue random-detect max-threshold 2 100 100 100 100
wrr-queue random-detect min-threshold 2 80 100 100 100
wrr-queue random-detect max-threshold 3 80 90 100 100
wrr-queue random-detect min-threshold 3 70 80 90 100
wrr-queue random-detect min-threshold 4 70 80 90 100
wrr-queue random-detect max-threshold 4 80 90 100 100
wrr-queue random-detect min-threshold 5 70 80 90 100
wrr-queue random-detect max-threshold 5 80 90 100 100
wrr-queue random-detect min-threshold 6 70 80 90 100
wrr-queue random-detect max-threshold 6 80 90 100 100
wrr-queue random-detect min-threshold 7 60 70 80 90
wrr-queue random-detect max-threshold 7 70 80 90 100
@</MLTCMD>
#ENDS_INTERACTIVE
```

ウィザードを使用した複合テンプレートの展開フロー

ステップ 1 [設定（Configuration）] > [テンプレート（Templates）] > [機能およびテクノロジー（Features & Technologies）] > [複合テンプレート（Composite Templates）] > [複合テンプレート（Composite Templates）] の順に選択します。

ステップ 2 [テンプレートの基本設定（Template Basic）] セクションに、必要な情報を入力します。

ステップ 3 [テンプレートの詳細（Template Detail）] 領域で、複合テンプレートに含めるテンプレートを選択し、[新しいテンプレートとして保存（Save as New Template）] をクリックします。

ステップ 4 複合テンプレートを作成した後、[展開（Deploy）] をクリックします。[展開（Deployment）] ウィザードページが開きます。

ステップ 5 テンプレートを展開するデバイスを選択します。[選択（Select）] トグル ボタンをクリックすると、[グループ別（By Group）] オプションからデバイスを選択できます。[次へ（Next）] をクリックします。

ステップ 6 ポート ベースの設定の場合は、[次へ（Next）] をクリックしてポートを選択します。

（注） [ポートの選択（Select Ports）] オプションは、[テンプレートの詳細（Template Details）] セクションでポート ベースのテンプレートを選択している場合のみ、展開ウィザードで使用可能になります。

ステップ 7 [選択（Select）] トグル ボタンをクリックすると、[ポート別（By Ports）] オプションまたは [ポートグループ別（By Port Groups）] オプションからポートを選択できます。選択したデバイスごとに、少なくとも 1 つのポートを選択する必要があります。

ステップ 8 [次へ（Next）] をクリックして入力オプションを選択します。

ステップ 9 テンプレートを展開するモードを選択します。オプションは、[ワークフロー（Work Flow）] および [CSV のエクスポート（Export CSV）]/[CSV のインポート（Import CSV）] です。

ステップ 10 [ワークフロー（Work Flow）] オプションをクリックし、[次へ（Next）] をクリックします。ステップ *11* を参照してください。

ステップ 11 または、[CSV のエクスポート（Export CSV）]/[CSV のインポート（Import CSV）] オプションをクリックし、CSV のエクスポート/インポート メカニズムを使用して選択したデバイスのテンプレート プロパティをすべて更新します。

a) CSV ファイル内の設定値の入力時に省略可能フィールドをスキップする場合は、[省略可能パラメータも必要ですか（Do you want Optional Parameters）] チェックボックスをオフにします。
b) [CSV のエクスポート（Export CSV）] をクリックし、ローカル システムに CSV テンプレートをダウンロードします。
c) ダウンロードした CSV テンプレートで個々のデバイスの設定値を入力します。
d) [CSV のインポート（Import CSV）] をクリックし、更新された CSV ファイルをアップロードします。入力値は自動的に更新されます。
e) [次へ（Next）] をクリックして値を入力します。

ステップ 12 [入力値（Input Values）] タブでは、[フォーム（Form）] ビューと [CLI] ビューを切り替えることができます。[入力値（Input Values）] タブで以下を設定します。

a) ナビゲーション ウィジェットでデバイスのテンプレートを選択します。テンプレートを選択するには、右上隅の円（T1、T2、T3、T4、T5、...）をクリックします。テンプレートが 5 個より多い場合

は、3 つのドットをクリックします。使用可能なすべてのテンプレートがあるドロップダウン リストが表示されます。

b) 各テンプレートのすべての必須フィールドに入力してから、[適用（Apply）] をクリックします。

検証が成功すると、選択したテンプレートの周りの輪郭線が緑色に変わり、ポップアップで使用可能なテンプレートとして選択されたテンプレートの隣に緑色のチェックマークが表示されます。

ステップ 13 必要な設定値を入力したら、[次へ（Next）] または [CLI] をクリックして、デバイスおよびテンプレートの設定値を確認します。

ステップ 14 必要に応じて、[展開のスケジュール設定（Schedule Deployment）] タブを使用して展開ジョブをスケジュール設定します。

- わかりやすい展開ジョブ名を付けてから、ただちに実行するか、後で実行するかを指定します。
- また、時間単位、日次、週次、月次、または年次単位で定期的にジョブを実行するようにスケジュールできます。
- 次のジョブ オプションを設定できます。

  失敗ポリシー（Failure Policy）：

  - [失敗を無視して続行（Ignore failure and continue）]：これはデフォルトのオプションです。 デバイスは、テンプレートの展開にランダムに選択されます。ジョブを実行できないデバイスがあった場合、そのデバイスをスキップし、引き続き残りのデバイスでジョブを実行します。ジョブ結果には、選択したすべてのデバイスの成功/失敗情報が表示されます。
  - [失敗で停止（Stop on failure）]：ジョブがデバイスでの実行に失敗した場合、そのジョブは停止します。 ジョブ結果は、ジョブが正常に実行されたデバイスと、テンプレートの展開が行われなかった他のデバイスについてのみ更新されます。「Not Attempted」メッセージが表示されます。展開のために選択されたデバイスの順序は、[Value assignment] ペインのデバイスの順序と同じです。
  - [実行コンフィギュレーションをスタートアップにコピー（Copy Running Config to Startup）]：テンプレートの展開ジョブが成功すると、デバイスの実行コンフィギュレーションがスタートアップ コンフィギュレーションにコピーされます。
  - [展開後にコンフィギュレーションをアーカイブ（Archive Config after deploy）]：新しい設定アーカイブ ジョブを作成し、テンプレートを正常に展開した後で、デバイスのコンフィギュレーションをアーカイブします。

ステップ 15 [次へ（Next）] をクリックしてジョブ展開サマリーを表示します。

ステップ 16 [展開サマリー（Deployment Summary）] タブに、各デバイスの CLI ビューが表示されます。

ステップ 17 [終了（Finish）] をクリックしてテンプレートを展開します。

ステップ 18 ジョブのステータスを表示するには、ポップアップ ダイアログボックスで [ジョブのステータス（Job Status）] をクリックして [ジョブ ダッシュボード（Job Dashboard）] を起動します。

設定グループを使用しないデバイスへのテンプレートの展開

テンプレートを保存すると、デバイスで展開（実行）できるようになります。テンプレートは、**[構成（Configuration）]** > **[テンプレート（Templates）]** > **[機能およびテクノロジー（Features & Technologies）]** ナビゲーション領域から、または **[構成（Configuration）]** > **[テンプレート（Templates）]** > **[設定グループ（Configuration Groups）]** から起動できる [設定グループ（Configuration Groups）] を使用して展開できます（デバイスのグループにテンプレートを展開するための設定グループの作成 （515 ページ） を参照）。

[機能およびテクノロジー（Features & Technologies）] ナビゲーション領域からカスタマイズされたテンプレートまたはシステム テンプレートを展開するには、次の手順を実行します。

ステップ 1 **[構成（Configuration）]** > **[テンプレート（Templates）]** > **[機能およびテクノロジー（Features & Technologies）]** の順に選択します。

ステップ 2 展開するテンプレートが含まれているドロワーを展開します。

ステップ 3 展開するテンプレートを選択し、[展開（Deploy）] をクリックします。

ステップ 4 [テンプレートの展開（Template Deployment）] ウィンドウで、設定とスケジュールを確認し、**OK** をクリックします。

設定テンプレートを使用したコントローラの設定

この項では、ワイヤレステンプレートを追加および適用する方法を説明します。テンプレートを利用すると、複数のデバイスにパラメータを適用するときに共通の情報を再入力する必要がなくなります。

コントローラ テンプレートでは、1 つのページからすべての Prime Infrastructure テンプレートにアクセスできます。コントローラテンプレートを追加および適用、テンプレートを表示、または既存のテンプレートを変更できます。この項では、コントローラテンプレートの適用と削除、およびアクセス ポイント テンプレートの作成や変更の手順についても説明します。

コントローラ テンプレートにアクセスするには、[構成（Configuration）] > [テンプレート（Templates）] > [機能およびテクノロジー（Features & Technologies）] > [機能およびテクノロジー（Features and Technologies）] > [コントローラ（Controller）] の順に選択します。

「コントローラ テンプレートおよびフィールドの説明」を参照してください。

関連トピック

コントローラ テンプレートの作成 （525 ページ）
コントローラ テンプレートの追加 （525 ページ）
コントローラ テンプレートの削除 （526 ページ）
コントローラ テンプレートの適用 （526 ページ）
コントローラ WLAN クライアント プロファイルの設定 （528 ページ）
モバイル コンシェルジュ（802.11u）を使用するようにコントローラを設定する （529 ページ）

AP グループを使用した WLAN 構成と展開の管理 （530 ページ）
WLAN AP グループ テンプレートの作成 （530 ページ）
設定テンプレートを使用した Lightweight AP の設定 （583 ページ）
テンプレートを使用したスイッチの場所情報の設定 （567 ページ）
AP 移行テンプレートを使用した Autonomous アクセス ポイントから Lightweight アクセス ポイントへの移行 （568 ページ）

コントローラ テンプレートの作成

機能およびテクノロジー テンプレートを作成するには、次の手順を実行します。

ステップ 1 [構成（Configuration）]>[テンプレート（Templates）]>[機能およびテクノロジー（Features & Technologies）] > [コントローラ（Controller）] > [コントローラテンプレート（Controller Template）] の順に選択します。

ステップ 2 テンプレート タイプの横にあるツール チップにマウスのカーソルを合わせ、[新規（New）] をクリックしてテンプレートを作成します。

ステップ 3 必要なフィールドに入力します。

特定のデバイス タイプだけに適用する機能テンプレートを作成している場合は、[デバイス タイプ（Device Type）] フィールドには、該当するデバイス タイプだけがリストされ、選択を変更することはできません。デバイス タイプを指定することで、不一致を防止できます。つまり、設定を作成して、間違ったデバイスにその設定を適用することはできません。

ステップ 4 [新しいテンプレートとして保存（Save as New Template）] をクリックします。テンプレートを保存した後、デバイスに適用します。

ステップ 5 テンプレートの展開のステータスを確認するには、[Administration] > [Dashboard] > [Jobs Dashboard] の順に選択します。

後続の設定テンプレートの導入に関する導入パラメータを変更するには、コンフィギュレーション ジョブを選択し、[スケジュールの編集（Edit Schedule）] をクリックします。

コントローラ テンプレートの追加

新しいコントローラ テンプレートを追加するには、次の手順を実行します。

ステップ 1 [Configuration] > [Features & Technologies] > [Controller] の順に選択します。

ステップ 2 追加するテンプレートを選択します。

ステップ 3 テンプレート名を入力します。

テンプレート名は、テンプレートを特定するために使用される一意のキーです。同じキー属性を持つ 2 つのテンプレートを区別するため、テンプレート名は必須です。

ステップ 4 テンプレートの説明を入力します。

ステップ 5 [Save] をクリックします。

関連トピック

コントローラ テンプレートの削除 （526 ページ）
コントローラ テンプレートの適用 （526 ページ）

コントローラ テンプレートの削除

コントローラ テンプレートを削除するには、次の手順を実行します。

ステップ 1 **[構成（Configuration）] > [機能およびテクノロジー（Features & Technologies）] > [マイテンプレート（My Templates）]** の順に選択します。

ステップ 2 削除するテンプレートを選択し、[Delete] をクリックします。

ステップ 3 [OK] をクリックして、削除を実行します。このテンプレートがコントローラにされている場合には、[Remove Template Confirmation] ページが開き、このテンプレートを現在適用しているすべてのコントローラがリストされます。

ステップ 4 テンプレートを削除する各コントローラのチェックボックスをオンにします。

ステップ 5 [OK] をクリックして削除操作を確定するか、または [Cancel] をクリックしてテンプレートを削除せずにこのページを閉じます。

関連トピック

コントローラ テンプレートの追加 （525 ページ）
コントローラ テンプレートの適用 （526 ページ）

コントローラ テンプレートの適用

コントローラ テンプレートは、選択した設定グループの 1 つ以上のコントローラに直接適用できます。

コントローラ テンプレートを適用するには、次の手順を実行します。

ステップ 1 [Configuration] > [Features & Technologies] > [Controller] の順に選択します。

ステップ 2 左側のサイドバーのメニューを使用して、適用するテンプレートのカテゴリを選択します。

ステップ 3 コントローラに適用するテンプレートのテンプレート名をクリックします。

ステップ 4 [Apply to Controllers] をクリックして、[Apply to Controllers] ページを開きます。

ステップ 5 テンプレートを適用する各コントローラのチェックボックスをオンにします。

すべてのコントローラを選択するには、コントローラ テーブルの左隅に表示されるチェックボックスをオンにします。

[Ignore errors on Apply template to Controllers] チェックボックスをオンにすると、エラーを無視して、テンプレートのすべてのコマンドをコントローラに適用できます。このチェックボックスがオフの場合、テンプレートのコマンドをコントローラに適用するときにエラーが発生すると、残りのコマンドは適用されません。

ステップ 6 テンプレートを直接適用する対象として、選択した設定グループの 1 つまたはすべてのコントローラより選択ください。

テンプレートを 1 つのコントローラ（もしくは、すべてのコントローラ）に直接適用するには、次の手順を実行します。

a) [選択したコントローラに直接適用（Apply to controllers selected directly）] オプション ボタンを選択します。[Apply to Controllers] ページに、コントローラ名および設定グループ名（該当する場合）とともに、使用できる各コントローラの IP アドレスがリストされます。

b) テンプレートを適用する各コントローラのチェックボックスをオンにします。

[Ignore errors on Apply template to Controllers] チェックボックスをオンにすると、エラーを無視して、テンプレートのすべてのコマンドをコントローラに適用できます。このチェックボックスがオフの場合、テンプレートのコマンドをコントローラに適用するときにエラーが発生すると、残りのコマンドは適用されません。

選択した設定グループのすべてのコントローラにテンプレートを適用するには、次の手順を実行します。

a) [選択した設定グループでコントローラを適用（Apply to controllers in the selected Config Groups）] オプション ボタンを選択します。[コントローラに適用（Apply to Controllers）] ページに、モビリティ グループ名および含まれるコントローラ数とともに、各設定グループの名前がリストされます。

b) テンプレートを適用する各設定グループのチェックボックスをオンにします。

コントローラのない設定グループには、テンプレートを適用できません。

ステップ 7 次の追加操作を実行できます。

- [Save Config to Flash after apply] チェックボックスをオンにした場合は、テンプレートが正常に適用されると、save config to Flash コマンドが実行されます。
- [Reboot Controller after apply] チェックボックスをオンにした場合は、テンプレートが正常に適用されると、コントローラがリブートします。

この設定結果は、[View Save Config / Reboot Results] オプションを有効にして、[Template Results] ページで表示できます。

ステップ 8 [Save] をクリックします。

[Template List] ページから直接、テンプレートを適用できます。適用するテンプレートのチェックボックスをオンにし、[Select a command] ドロップダウン リストから [Apply Templates] を選択し、[Go] をクリックして、[Apply to Controllers] ページを開きます。このテンプレートを適用するコントローラのチェックボックスをオンにして、[OK] をクリックします。

関連トピック

コントローラ テンプレートの追加 （525 ページ）

コントローラ WLAN クライアント プロファイルの設定

クライアントが WLAN にアソシエートしようとする場合、プロセスで受信した情報からクライアントタイプを決定することができます。コントローラは情報のコレクタとして機能し、必要なデータとともに最適な形式で ISE を送信します。

クライアント プロファイルを設定する場合、次のガイドラインに従います。

デフォルトで、クライアントのプロファイルはすべての WLAN 上で無効です。

- クライアント プロファイルは、ローカル モードと FlexConnect モードのアクセス ポイントでサポートされます。
- プロファイルは、次のシナリオのクライアントではサポートされません。
  - スタンドアロン モードで FlexConnect モード AP とアソシエートしているクライアント。
  - ローカル スイッチングが有効な状態でローカル認証が行われる場合に FlexConnect モード AP とアソシエートしているクライアント。
- コントローラでは DHCP プロキシと DHCP ブリッジ モードの両方がサポートされます。
- WLAN のアカウンティング サーバの設定は、1.1 MnR 以降のリリースを実行する ISE を指している必要があります。Cisco の ACS では、クライアント プロファイルはサポートされていません。
- 使用されている DHCP サーバのタイプは、クライアントのプロファイルに影響しません。
- DHCP_REQUEST のパケットに ISE プロファイル済みデバイス リストで見つかった文字列が含まれている場合、クライアントは自動的にプロファイルされます。
- クライアントは、Accounting request パケットで送信される MAC アドレスに基づいて識別されます。
- プロファイルが有効になると MAC アドレスだけがアカウンティング パケットの発信側ステーション ID として送信されます。
- ローカル スイッチングの FlexConnect モードの AP でプロファイルが有効である場合、VLAN オーバーライドだけが AAA Override 属性としてサポートされます。

クライアント プロファイルを設定するには、次の手順に従います。

ステップ 1 [Configuration] > [Templates] > [Features & Technologies] > [Controller] > [WLANs] > [WLAN Configuration] の順に選択します。

ステップ 2 [Advanced] タブをクリックします。

ステップ 3 DHCP プロファイルを有効にするには、[DHCP Profiling] チェックボックスをオンにします。

ステップ 4 HTTP プロファイルを有効にするには、[HTTP Profiling] チェックボックスをオンにします。

HTTP クライアント プロファイルは、コントローラ バージョン 7.3.1.31 以降でサポートされます。

ステップ 5 [Save] をクリックします。

『Cisco Prime Infrastructure Reference Guide』の「*Controller* > *WLANs* > *WLAN Configuration* > *Advanced*」の項を参照してください。

モバイルコンシェルジュ（802.11u）を使用するようにコントローラを設定する

モバイル コンシェルジュは、外部ネットワークで相互運用できるように 802.1X 対応クライアントを有効にするソリューションです。モバイルコンシェルジュ機能は、クライアントにサービスのアベイラビリティに関する情報を提供し、使用可能なネットワークをアソシエートするのに役立ちます。

ネットワークから提供されるサービスは、次の 2 つのプロトコルに大きく分類できます。

- 802.11u MSAP
- 802.11u HotSpot 2.0

モバイル コンシェルジュには、次のガイドラインと制限事項が適用されます。

- モバイル コンシェルジュは FlexConnect アクセス ポイントではサポートされません。
- 802.11u 設定アップロードはサポートされません。設定のアップグレードを実行し、設定をコントローラにアップロードすると、WLAN の HotSpot の設定は失われます。

モバイル コンシェルジュ（802.11u）グループを設定するには、次の手順を実行します。

ステップ 1 [Configuration] > [Templates] > [Features & Technologies] > [Controller] > [WLANs] > [WLAN Configuration] の順に選択します。

ステップ 2 [Hot Spot] タブをクリックします。

ステップ 3 次のタブの必須フィールドに入力します。

- [802.11u 設定（802.11u Configuration）]
- [その他（Others）]
- レルム
- [サービス アドバタイズメント（Service Advertisements）]
- [ホットスポット 2.0（Hotspot 2.0）]

ステップ 4 [新しいテンプレートとして保存（Save as New Template）] をクリックします。

『Cisco Prime Infrastructure Reference Guide』の「*Controller* > *WLANs* > *WLAN Configuration*」の項を参照してください。

AP グループを使用した WLAN 構成と展開の管理

- AP グループを使用して WLAN 設定を管理する場合は、次の点に注意してください。
- [AP Groups]（コントローラ リリース 5.2 以降）は、リリース 5.2 よりも前のコントローラでは [AP Group VLANs] です。
- 使用可能なすべての WLAN プロファイル名を表示するには、テキスト ボックスから現在の WLAN プロファイル名を削除します。テキスト ボックスから現在の WLAN プロファイルの名前を削除すると、使用可能なすべての WLAN プロファイルがドロップダウン リストに表示されます。
- 各アクセス ポイントは 16 個の WLAN プロファイルに限定されます。各アクセス ポイントは、WLAN override 機能が有効にされない限り、すべての WLAN プロファイルをブロードキャストします。WLAN override 機能によって、アクセス ポイントごとに 16 個の任意の WLAN プロファイルを無効にできます。
- WLAN override 機能は、512 WLAN 機能をサポートしていない（最大 512 個の WLAN プロファイルをサポートできる）古いコントローラのみに適用されます。

関連トピック

WLAN AP グループ テンプレートの作成 （530 ページ）
WLAN AP グループの追加 （531 ページ）
WLAN AP グループの削除 （531 ページ）

WLAN AP グループ テンプレートの作成

サイト固有の VLAN または AP グループは、WLAN を異なるブロードキャスト ドメインにセグメント化することで、ブロードキャスト ドメインを最小に制限します。このようにすることで、ロードバランシングおよび帯域幅割り当てを効果的に管理できるというメリットがあります。

WLAN AP グループを設定するには、次の手順を実行します。

ステップ 1 **[構成（Configuration）] > [テンプレート（Templates）] > [機能およびテクノロジー（Features & Technologies）] > [コントローラ（Controller）] > [WLAN（WLANs）] > [APグループ（AP Groups）]** の順に選択します。

[WLAN] > [APグループ（AP Groups）] ページが表示され、テンプレートが適用されるコントローラおよび仮想ドメインの数が自動的に読み込まれます。最後の列は、テンプレートがいつ最後に保存されたかを示します。

[Applied to Controllers] の数字はリンクになっています。数字をクリックすると、[Applied to Controllers] ページが開きます。このページには、そのテンプレートが適用されているコントローラ名と IP アドレス、および適用された時刻とステータスが表示されます。[Applied to Virtual Domains] の数字もリンクになっています。このリンクをクリックすると、すべてのパーティション名が表示された [Applied to Virtual Domains] ページが開きます。

ステップ 2 新しいテンプレートを追加する場合は、[Select a command] ドロップダウン リストから [Add Template] を選択し、[Go] をクリックします。既存のテンプレートを変更するには、テンプレート名をクリックします。[AP Groups template] ページが表示されます。

このページには、ネットワーク上に設定されている AP グループのサマリーが表示されます。このページで、AP グループの詳細を追加、削除、編集または表示できます。[Edit] 列をクリックして、そのアクセスポイントを編集します。[WLAN Profile Name] 列のチェックボックスをオンにし、[Remove] をクリックして、WLAN プロファイルを削除します。

（注）
- [Description] テキスト ボックスに入力できる最大数は 256 文字です。
- バージョン 8.7 以降の ME に適用されます。

関連トピック

AP グループを使用した WLAN 構成と展開の管理 （530 ページ）
WLAN AP グループの追加 （531 ページ）
WLAN AP グループの削除 （531 ページ）

WLAN AP グループの削除

アクセス ポイント グループを削除するには、次の手順を実行します。

ステップ 1 [Configuration] > [Templates] > [Features & Technologies] の順に選択します。
左側のサイドバー メニューから、[コントローラ（Controller）] > [WLAN（WLANs）] > [APグループ（AP Groups）] の順に選択します。

ステップ 2 [削除] をクリックします。

関連トピック

AP グループを使用した WLAN 構成と展開の管理 （530 ページ）
WLAN AP グループの追加 （531 ページ）
WLAN AP グループ テンプレートの作成 （530 ページ）

WLAN AP グループの追加

WLAN プロファイルを AP グループに分割するテンプレートを作成または変更できます。

ステップ 1 [Configuration] > [Templates] > [Features & Technologies] > [Controller] > [WLANs] > [AP Groups] の順に選択します。

ステップ 2 [Select a command] ドロップダウン リストから [Add Template] を選択し、[Go] をクリックします。

ステップ 3 アクセス ポイント グループの名前およびグループの説明を入力します。グループの説明はオプションです。

ステップ 4 WLAN プロファイルを追加する場合は、[WLAN Profiles] タブをクリックし、次のフィールドを設定します。

a) [Add] をクリックします。

b) WLAN プロファイル名を入力するか、[WLAN Profile Name] ドロップダウン リストからいずれか 1 つを選択します。

c) インターフェイス/インターフェイス グループを入力するか、[Interface/Interface Group] ドロップダウン リストからいずれか 1 つを選択します。

使用できるすべてのインターフェイスを表示するには、[Interface] テキスト ボックスから現在のインターフェイスを削除します。[Interface] テキスト ボックスから現在のインターフェイスを削除すると、使用可能なすべてのインターフェイスがドロップダウン リストに表示されます。

d) 該当する場合は、[NAC Override] チェックボックスをオンにします。NAC の上書き機能は、デフォルトでは無効です。

e) [Add/Edit] リンクをクリックして、ポリシー設定パラメータを指定します。

- • [Policy Name]：ポリシーの名前。
  • [Policy Priority]：1 ～ 16 のポリシー プライオリティを設定します。2 個のポリシーが同じプライオリティを持つことはできません。WLAN 1 つあたり 16 のポリシー マッピングのみが許可されます。マッピングに選択されたポリシー テンプレートは、コントローラにポリシーがない場合に最初に適用されます。

f) アクセス ポイントおよび WLAN プロファイルを追加したら、[Save] をクリックします。

ステップ 5 RF プロファイルを追加する場合は、[RF Profiles] タブをクリックし、次のフィールドを設定します。

- [802.11a]：ドロップダウン リストから、802.11a 無線 AP の RF プロファイルを選択できます。
- [802.11b]：ドロップダウン リストから、802.11b 無線 AP の RF プロファイルを選択できます。
- RF プロファイルを追加したら、[Save] をクリックします。

『Cisco Prime Infrastructure Reference Guide』の「*Controller* > *802.11* > *RF Profiles*」の項を参照してください。

リモート LAN（RLAN）テンプレートの作成

ステップ 1 **[設定（Configuration）]** > **[機能およびテクノロジー（Features and Technologies）]** > **[コントローラ（Controller）]** > **[WLAN（WLANs）]** > **[WLANの設定（WLAN Configuration）]** の順に選択します。

ステップ 2 [テンプレートの基本設定（Template Basic）] 領域に、必要な詳細情報を入力します。

ステップ 3 [テンプレートの詳細（Template Detail）] 領域の [全般（General）] タブで、[有線LAN（Wired LAN）] チェックボックスをオンにして有効にします。

ステップ 4 [LANタイプ（LAN Type）] ドロップダウン メニューから [リモートLAN（Remote LAN）] を選択します。

ステップ 5 **プロファイル名**を入力します。

ステップ 6 [管理ステータス（Admin Status）] チェックボックスを選択して有効にします。

（注）　これは、RLAN を AP グループにマッピングし、ポートを有効にする場合に必要です。

ステップ 7 設定を保存します。

ステップ 8 テンプレートを [展開（Deploy）] します。

（注）　バージョン 8.7 以降の ME のみに適用されます。

AP グループへのリモート LAN（RLAN）のマッピング

ステップ 1 **[設定（Configuration）] > [機能およびテクノロジー（Features and Technologies）] > [コントローラ（Controller）] > [WLAN（WLANs）] > [APグループ（AP Groups）]** の順に選択します。

あるいは、[マイテンプレート（My Templates）] で同じフォルダ構造を探し、使用可能な AP グループを表示します。

ステップ 2 [テンプレートの基本設定（Template Basic）] 領域で、必要な詳細情報を入力します（新しいテンプレートを作成する場合）。

ステップ 3 [WLANプロファイル（WLAN Profile）] をクリックし、次に [追加（Add）] をクリックします。

ステップ 4 [WLANプロファイル（WLAN Profile）] を選択し、それぞれのドロップダウン メニューからインターフェイスまたはインターフェイス グループを選択します。

ステップ 5 [保存（Save）] をクリックします。

ステップ 6 [ポート（Ports）] をクリックします。

ステップ 7 ポート番号の横にあるドロップダウン メニューから、RLAN を選択します。

ステップ 8 テンプレートを [展開（Deploy）] します。

（注）　バージョン 8.7 以降の ME のみに適用されます。

FlexConnect AP グループでの FlexConnect ユーザの構成

FlexConnect の [ローカル認証（Local Authentication）] チェックボックスが有効な場合に表示される [グループで構成されるユーザ（Users configured in the group）] リンクをクリックして、FlexConnect ユーザのリストを表示できます。FlexConnect ユーザを作成できるのは、FlexConnect AP グループを保存した後のみです。最大 100 の FlexConnect ユーザがコントローラのリリース 5.2.x.x 以降でサポートされています。コントローラ リリース 5.2.0.0 以前では、20 の FlexConnect ユーザのみサポートされます。

FlexConnect ユーザを削除するには、[FlexConnect ユーザ（FlexConnect Users）] リストからユーザを選択して、[削除（Delete）] をクリックします。

FlexConnect ユーザを設定するには、次の手順を実行します。

ステップ 1 [構成（Configuration）]>[機能およびテクノロジー（Features & Technologies）]>[コントローラ（Controller）] > [FlexConnect] > [FlexConnect AP グループ（FlexConnect AP Groups）] を選択します。

ステップ 2 [FlexConnect AP グループ（FlexConnect AP Groups）] の上にマウスを移動して、[すべてのテンプレートの表示（Show All Templates）] を選択します。

ステップ 3 **[ローカル認証（Local Authentication）]** タブをクリックして、**[FlexConnect ローカル認証（FlexConnect Local Authentication）]** チェックボックスをオンにし、この FlexConnect グループのローカル認証を有効にします。

ステップ 4 [グループで構成されるユーザ（Users configured in the group）] リンクをクリックします。[FlexConnect ユーザ（FlexConnect Users）] ページが表示されます。

ステップ 5 新しいユーザを追加する場合は、[Select a command] ドロップダウン リストから [Add User] を選択し、[Go] をクリックします。[Add User] ページが表示されます。

ステップ 6 [ユーザ名（User Name）] テキスト ボックスに、FlexConnect のユーザ名を入力します。

ステップ 7 [Password] テキスト ボックスに、パスワードを入力します。

ステップ 8 [Confirm Password] テキスト ボックスにパスワードを再入力します。

ステップ 9 [Save] をクリックします。

『Cisco Prime Infrastructure Reference Guide』の「*Controller* > *FlexConnect* > *FlexConnect AP Groups*」の項を参照してください。

デバイスベースおよびユーザベースのコントローラ ポリシーの設定

[Policy Configuration Templates] ページでは、コントローラにデバイス ベースのポリシーを設定することができます。ネットワーク上のユーザまたはデバイス用のポリシーを設定できます。設定できるポリシーの最大数は 64 です。AAA オーバーライドがコントローラに設定されている場合は、ポリシーは WLAN および AP グループに適用されません。

ポリシー設定テンプレートを設定するには、次の手順を実行します。

ステップ 1 [Configuration] > [Templates] > [Features & Technologies] > [Controller] > [WLANs] > [Policy Configuration] の順に選択します。

ステップ 2 新しいテンプレートを追加する場合は、[Select a command] ドロップダウン リストから [Add Template] を選択し、[Go] をクリックします。

ステップ 3 必要なフィールドを設定します。

ステップ 4 [Save as New Template] をクリックします。

設定テンプレートを使用したコントローラでの AAA の設定

コントローラの汎用セキュリティ情報を含む新しいテンプレートを追加するには、次の手順を実行します。

ステップ 1 [Configuration] > [Templates] > [Features & Technologies] > [Controller] > [Security] の順に選択します。

ステップ 2 左側のサイドバーのメニューから [AAA] > [汎用 AAA（General-AAA）] を選択します。

ステップ 3 追加するテンプレートの横にある [新規（New）] をクリックします。

ステップ 4 次のフィールドを設定します。

- [テンプレート名（Template Name）]：テンプレート名は、テンプレートを特定するために使用される一意のキーです。同じキー属性を持つ 2 つのテンプレートを区別するため、テンプレート名は必須です。
- [ローカル データベース エントリの最大数（次の再起動時）（Maximum Local Database Entries (on next reboot)）]：許可されるデータベース エントリの最大数を入力します。これは、次回リブート時に有効になります。
- [管理ユーザの再認証の間隔（Mgmt User Re-auth Interval）]：管理ユーザの終了の間隔を入力します。

ステップ 5 [Save] をクリックします。

ステップ 6 テンプレートが [Template List] ページに表示されます。[Template List] ページで、このテンプレートをコントローラに適用できます。

関連トピック

コントローラ テンプレートの追加 （525 ページ）
コントローラ テンプレートの削除 （526 ページ）
コントローラ テンプレートの適用 （526 ページ）

コントローラへのユーザ アクセスを制御するための RADIUS 認証サーバの設定

RADIUS 認証テンプレートを追加したり、既存のテンプレートを変更したりすることができます。これらのサーバ テンプレートを設定した後、CLI または GUI を経由してコントローラにログインしているコントローラ ユーザが認証されます。

『Cisco Prime Infrastructure Reference Guide』の「*Controller* > *Security* > *AAA* > *RADIUS Auth Servers*」の項を参照してください。

コントローラでの RADIUS および TACACS サーバ フォールバック設定の構成

RADIUS TACACS フォールバック テンプレートを追加および設定したり、既存のテンプレートを変更するには、次の手順を実行します。

ステップ 1 [設定（Configuration）]>[テンプレート（Templates）]>[機能およびテクノロジー（Features & Technologies）]>[コントローラ（Controller）]>[セキュリティ（Security）]>[AAA]>[RADIUS TACACS+ フォールバック（RADIUS TACACS+ Fallback）] を選択します。

ステップ 2 [RADIUS フォールバック（Radius Fallback）] グループ ボックスで、以下を設定します。

- [RADIUS フォールバック モード（Radius Fallback Mode）] ドロップダウン リストから、次のいずれかを選択します。
  - [オフ（Off）]：フォールバックを無効にします。
  - [パッシブ（Passive）]：時間間隔を入力する必要があります。
  - [アクティブ（Active）]：ユーザ名および時間間隔を入力する必要があります。

ステップ 3 [TACACS フォールバック（TACACS Fallback）] グループ ボックスで、以下を設定します。

- [フォールバック モード（Fallback Mode）] ドロップダウン リストから [有効（Enable）] または [無効（Disable）] を選択します。
- [時間間隔（Time Interval）] テキスト ボックスに、TACACS フォールバック テスト間隔の値を秒単位で入力します。

ステップ 4 [新しいテンプレートとして保存（Save as New Template）] をクリックします。

関連トピック

コントローラ テンプレートの追加 （525 ページ）
コントローラ テンプレートの削除 （526 ページ）
コントローラ テンプレートの適用 （526 ページ）

ローカル EAP タイムアウト設定の構成

このページでは、ローカルEAPのタイムアウト値を指定できます。次に、既存のローカルEAP汎用テンプレートに変更を追加すること、またはこのテンプレートを変更することができます。

コントローラ上でRADIUSサーバが設定されている場合は、コントローラはまずRADIUSサーバを使用してワイヤレス クライアントを認証しようとします。ローカルEAPは、RADIUSサーバがタイムアウトしていたり、RADIUSサーバが設定されていない場合など、RADIUSサーバが見つからない場合にのみ試行されます。4 台の RADIUS サーバが設定されている場合、コントローラは最初の RADIUS サーバを使用してクライアントの認証を試行し、次に 2 番めの RADIUS サーバ、その次にローカル EAP を試行します。その後クライアントが手動で再認証を試みると、コントローラは 3 番めの RADIUS サーバを試行し、次に 4 番めの RADIUS サーバ、その次にローカル EAP を試行します。

関連トピック

LDAP とローカル データベースを使用してコントローラへのユーザ アクセスを制御する場合の認証順序の設定 （537 ページ）

LDAP とローカル データベースを使用してコントローラへのユーザ アクセスを制御する場合の認証順序の設定

LDAP とローカル データベースがユーザ クレデンシャル情報を取得するために使用する順序を指定できます。このページでは、ネットワーク ユーザ クレデンシャル取得優先度テンプレートを追加、または既存のテンプレートを変更できます。

ステップ 1 [Configuration] > [Templates] > [Features & Technologies] > [Controller] > [Security] > [Local EAP] > [Network Users Priority] の順に選択します。

ステップ 2 左右の矢印キーを使用して、右側のページにネットワーク ユーザ クレデンシャルを含めたり、除外したりすることができます。

ステップ 3 上下のキーを使用してクレデンシャルを試行する順序を指定します。

ステップ 4 [Save] をクリックします。

関連トピック

コントローラ テンプレートの追加 （525 ページ）
コントローラ テンプレートの削除 （526 ページ）
コントローラ テンプレートの適用 （526 ページ）

コントローラのユーザ認証に使用するクレデンシャルの設定（ローカル ネットワーク テンプレート）

このテンプレートでは、ローカル ネットワーク ユーザ全員のクレデンシャル（ユーザ名とパスワード）を保存できます。これらの資格情報は、ユーザの認証に使用されます。たとえば、ローカル EAP では、ユーザ クレデンシャルを取得するために、バックエンド データベースとしてローカル ユーザ データベースを使用する場合があります。このページでは、ローカル ネットワーク ユーザ テンプレートを追加、または既存のテンプレートを変更できます。Web 認証クライアントとしてログインする際は、ローカル ネット ユーザを作成し、パスワードを定義する必要があります。

ローカル ネットワーク ユーザ テンプレートを設定するには、次の手順を実行します。

ステップ 1 [Configuration] > [Templates] > [Features & Technologies] > [Controller] > [Security] > [AAA] > [Local Net Users] の順に選択します。

ステップ 2 [Import CSV] をクリックしてファイルからインポートし、[Browse] をクリックしてファイルに移動します。次にステップ 6 に進みます。インポートを無効にする場合はステップ 3 に進みます。

CSV ファイル形式だけがサポートされます。

Prime Infrastructure は 2 行目以降のデータを読み取ります。ファイルの最初の行はヘッダーとして扱われ、データは Prime Infrastructure によって読み取られません。ヘッダーは空白でも入力してもかまいません。

ステップ 3 次の詳細を入力します。

- [ユーザ名（Username）]
- パスワード
- Profile
- Description

[Profile] 列が空白（または「**Any Profile**」と表示）の場合、任意のプロファイルのクライアントがこのアカウントを使用できることを示します。

ステップ 4 ドロップダウン リストを使用してこのローカル ユーザに適用される SSID を選択するか、[any SSID] オプションを選択します。

ステップ 5 ユーザが定義したこのインターフェイスの説明を入力します。

ステップ 6 [保存（Save）] をクリックします。

関連トピック

コントローラ テンプレートの追加 （525 ページ）
コントローラ テンプレートの削除 （526 ページ）
コントローラ テンプレートの適用 （526 ページ）

ユーザが同時に実行できるログイン セッション数の制御

ユーザ 1 人あたりの同時ログインの最大数を設定できます。

ユーザ ログイン テンプレートを追加する、または既存のテンプレートを変更するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [テンプレート（Templates）] > [機能およびテクノロジー（Features & Technologies）] > [コントローラ（Controller）] > [セキュリティ（Security）] > [ユーザ ログイン ポリシー（User Login Policies）]** を選択します。

ステップ 2 単一の各ユーザが同時にログインできる最大数を入力します。

ステップ 3 [新しいテンプレートとして保存（Save as New Template）] をクリックします。

関連トピック

コントローラ テンプレートの追加 （525 ページ）
コントローラ テンプレートの削除 （526 ページ）
コントローラ テンプレートの適用 （526 ページ）

MAC アドレスでフィルタするための AP の設定

MAC フィルタ テンプレートを追加する、または既存のテンプレートを変更するには、次の手順を実行します。

ステップ 1 [設定（Configuration）]>[テンプレート（Templates）]>[機能およびテクノロジー（Features & Technologies）]>[コントローラ（Controller）]>[セキュリティ（Security）]>[AAA]>[MAC フィルタリング（MAC Filtering）] の順、または [セキュリティ（Security）]>[MAC フィルタリング（MAC Filtering）] を選択します。

ステップ 2 [Import CSV] をクリックして、アクセス ポイント MAC アドレスを含むファイルをインポートします。

ステップ 3 目的のファイルのパスを入力するか、または [Browse] をクリックしてファイルをインポートします。

インポート ファイルは MAC アドレス、プロファイル名、インターフェイス、および説明を示した CSV ファイルである必要があります（例：00:11:22:33:44:55,Profile1,management,test filter）。[ファイルからインポート（Import from File）] チェックボックスを無効にした場合は、ステップ 4 に進みます。

クライアントの MAC アドレスが表示されます。

ステップ 4 この MAC フィルタが適用されるプロファイル名を選択するか、または [任意のプロファイル（Any Profile）] オプションを選択します。

ステップ 5 ドロップダウン リストを使用して、使用可能なインターフェイス名から選択します。

ステップ 6 ユーザが定義したこのインターフェイスの説明を入力します。

ステップ 7 [新しいテンプレートとして保存（Save as New Template）] をクリックします。

ブロードキャスト範囲では MAC アドレスを使用できません。

関連トピック

コントローラ テンプレートの追加 （525 ページ）
コントローラ テンプレートの削除 （526 ページ）
コントローラ テンプレートの適用 （526 ページ）

AP または MSE コントローラ認証の設定

これらのテンプレートは、Cisco IOS から Lightweight アクセス ポイントに変換された Cisco 11xx/12xx シリーズのアクセス ポイント、またはブリッジ モードで接続される 1030 アクセス ポイント用に考案されています。詳細については、『Cisco Mobility Services Engine Configuration Guide』を参照してください。

MSE 認可テンプレートを追加する、または既存のテンプレートを変更するには、次の手順を実行します。

ステップ 1 [Configuration] > [Templates] > [Features & Technologies] > [Controller] > [Security] > [AAA] > [AP or MSE Authorization] の順に選択します。

ステップ 2 [Import CSV] をクリックして、アクセス ポイント MAC アドレスを含むファイルをインポートします。

インポートできるのは CSV ファイルだけです。ファイル形式は GUI のフィールドに対応しており、したがってアクセス ポイントのベース無線 MAC、種類、証明書タイプ（MIC または SSC）、およびキー ハッ

シュが含まれます（例：00:00:00:00:00:00, AP, SSC, xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx）。その他のファイル形式はサポートされていません。

ステップ 3 目的のファイルのパスを入力するか、または [Browse] をクリックしてファイルをインポートします。

ステップ 4 [Save As New Template] をクリックします。

ブロードキャスト用の MAC アドレスを使用できません。

関連トピック

コントローラ テンプレートの追加 （525 ページ）
コントローラ テンプレートの削除 （526 ページ）
コントローラ テンプレートの適用 （526 ページ）

MACアドレスでクライアントを手動で無効化するためのコントローラの設定

このページでは、手動で無効にしたクライアント テンプレートを追加したり、既存の無効になっているクライアント テンプレートに変更を加えることができます。

ステップ 1 [Configuration] > [Templates] > [Features & Technologies] > [Controller] > [Security] > [Manually Disable Clients] の順に選択します。

ステップ 2 無効にするクライアントの MAC アドレスを入力します。

ステップ 3 無効に設定するクライアントの説明を入力します。

ステップ 4 [Save as New Template] をクリックします。

ブロードキャスト範囲では MAC アドレスを使用できません。

関連トピック

コントローラ テンプレートの追加 （525 ページ）
コントローラ テンプレートの削除 （526 ページ）
コントローラ テンプレートの適用 （526 ページ）

コントローラのクライアント除外ポリシーの設定

クライアント除外ポリシー テンプレートを追加するか、既存のクライアント除外ポリシー テンプレートを変更するには、次の手順を実行します。

ステップ 1 [Configuration] > [Templates] > [Features & Technologies] > [Controller] > [Security] > [Wireless Protection Policies] > [Client Exclusion Policies] の順に選択します。

ステップ 2 次のフィールドに入力します。

- [Template Name]：クライアント除外ポリシーの名前を入力します。
- [Excessive 802.11 Association Failures]：過剰な 802.11 のアソシエーションの失敗によるクライアントの除外を有効にします。
- [Excessive 802.11 Authentication Failures]：過剰な 802.11 認証の失敗によるクライアントの除外を有効にします。
- [Excessive 802.1X Authentication Failures]：過剰な 802.1X 認証の失敗によるクライアントの除外を有効にします。
- [Excessive 802.11 Web Authentication Failures]：過剰な 802.11 Web 認証の失敗によるクライアントの除外を有効にします。
- [IP Theft or Reuse]：IP の盗難または再使用の症状を示すクライアントの除外を有効にします。

ステップ 3 [新しいテンプレートとして保存（Save as New Template）] をクリックします。

関連トピック

コントローラ テンプレートの追加 （525 ページ）
コントローラ テンプレートの削除 （526 ページ）
コントローラ テンプレートの適用 （526 ページ）

MFP を使用した AP 認証の設定

Management Frame Protection（MFP）は、ワイヤレス ネットワーク インフラストラクチャによる 802.11 管理フレームの認証を提供します。DoS 攻撃を引き起こし、アソシエーションおよびプローブでネットワークをフラッディングさせ、不正アクセス ポイントをさしはさみ、QoS および無線測定フレームの攻撃によりネットワーク パフォーマンスに影響を与える敵対者を検出するため、管理フレームを保護できます。

有効にすると、アクセス ポイントは Message Integrity Check Information Element（MIC IE; メッセージ完全性チェック情報エレメント）を各フレームに追加して、送信する管理フレームを保護します。フレームのコピー、変更、再送が試みられた場合、MIC は無効となり、MFP フレームを検出するよう設定された受信アクセス ポイントは不具合を報告します。MFP フレームを送信するには、アクセス ポイントは WDS のメンバーであることが必要です。

MFP 検出が有効な場合、アクセス ポイントは、ネットワーク内の他のアクセス ポイントから受信するすべての管理フレームを検証します。MIC IE が存在しており（送信側が MFP フレームを送信するよう設定されている場合）、管理フレームの中身に一致していることを確認します。MFP フレームを送信するよう設定されているアクセス ポイントに属する BSSID からの正当な MIC IE が含まれていないフレームを受信した場合、不具合をネットワーク管理システムに報告します。

アクセス ポイント認可および管理フレーム保護（MFP）テンプレートを追加または変更するには、次の手順を実行します。

ステップ 1 [Configuration] > [Templates] > [Features & Technologies] > [Controller] > [Security] > [Wireless Protection Policies] > [AP Authentication and MFP] の順に選択します。

ステップ 2 [保護タイプ（Protection Type）] ドロップダウン リストから、次の認証ポリシーのいずれかを選択します。

- [None]：アクセス ポイント認可ポリシーなし。
- [AP Authentication]：認証ポリシーを適用します。
- [MFP]：管理フレーム保護を適用します。

アラームが生成される閾値は、保護の種類として AP 認証が選択されている場合にだけ表示されます。アラームを発生させるまでに無視する、未知のアクセス ポイントからのヒット数を設定します。

有効な範囲は 1 ～ 255 です。デフォルト値は 255 です。

ステップ 3 [Save as New Template] をクリックします。

関連トピック

コントローラ テンプレートの追加 （525 ページ）
コントローラ テンプレートの削除 （526 ページ）
コントローラ テンプレートの適用 （526 ページ）

コントローラ WLAN の Web 認証の認証タイプを設定する

Web 認証により、ゲストはブラウザを起動すると自動的に Web 認証ページにリダイレクトされます。ゲストは、この Web ポータルから WLAN にアクセスできます。この認証メカニズムを使用している無線 LAN 管理者は、ゲスト ユーザによるアクセスに対して、暗号化通信と非暗号化通信のどちらを設定するかを選択できます。ゲストユーザは、SSL で暗号化される有効なユーザ名とパスワードを使用して無線ネットワークにログインできます。Web 認証アカウントはローカルに作成するか、RADIUS サーバで管理できます。Cisco Wireless LAN Controller は Web 認証クライアントをサポートするように設定できます。このテンプレートを使用して、コントローラで提供される Web 認証ページを置き換えることができます。

Web 認証テンプレートを追加、または既存の Web 認証テンプレートを変更するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [テンプレート（Templates）] > [機能およびテクノロジー（Features & Technologies）] > [セキュリティ（Security）] > [AAA] > [Web 認証設定（Web Auth Configuration）]** を選択します。

ステップ 2 ドロップダウン リストから、次の Web 認証タイプのうち 1 つを選択します。

- [default internal]：引き続き、ページ タイトル、メッセージ、リダイレクト URL、およびロゴを表示するかどうかを変更できます。ステップ 5 に進みます。
- [customized web authentication]：[Save] をクリックしてこのテンプレートをコントローラに適用します。Web 認証バンドルをダウンロードするプロンプトが表示されます。
- カスタマイズされた Web 認証を選択する前に、まず **[設定（Config）] > [コントローラ（Controller）]** に移動し、[コマンドの選択（Select a command）] ドロップダウン リストから [カスタマイズされた Web 認証のダウンロード（Download Customized Web Authentication）] を選択して [実行（Go）] をクリックしてバンドルをダウンロードする必要があります。

- [external]：認証に成功した後でリダイレクトする URL を入力する必要があります。たとえば、このテキスト ボックスに入力した値が http://www.example.com の場合、ユーザはこの会社のホーム ページに接続されます。

ステップ 3 会社のロゴを表示する場合は、[Logo Display] チェックボックスをオンにします。

ステップ 4 Web 認証ページに表示するタイトルを入力します。

ステップ 5 Web 認証ページに表示するメッセージを入力します。

ステップ 6 認証に成功した後でユーザがリダイレクトされる URL を指定します。たとえば、このテキスト ボックスに入力した値が http://www.example.com の場合、ユーザはこの会社のホーム ページに接続されます。

ステップ 7 [Save as New Template] をクリックします。

関連トピック

コントローラへのカスタマイズされた Web 認証ページのダウンロード （543 ページ）

コントローラへのカスタマイズされた Web 認証ページのダウンロード

始める前に、次の手順を実行します。

カスタマイズされた Web 認証ページをコントローラにダウンロードできます。カスタマイズ Web ページでは、ユーザ Web アクセス用のユーザ名とパスワードを設定できます。

カスタマイズ Web 認証をダウンロードするときは、次のガイドラインに従う必要があります。

- ユーザ名を提供する。
- パスワードを提供する。
- リダイレクト URL は、元の URL から引用した後、非表示の入力項目として保持する。
- 操作 URL は、元の URL から引用および設定する。

リターン ステータス コードをデコードするスクリプトを提供する。

ステップ 1 サーバからサンプルの login.html バンドル ファイルをダウンロードします。次の図は .html ファイルを示しています。Web 認証がオンの場合、最初に WLAN にアクセスすると、ログイン ページが Web ユーザに表示されます。

図 *11 : Login.html*

ステップ 2 Login.html を編集し、これを .tar または .zip ファイルとして保存します。

[Submit] ボタンのテキストを「Accept terms and conditions and Submit」（条件を承諾して送信）と変更できます。

ステップ 3 ダウンロードに Trivial File Transfer Protocol（TFTP）サーバを使用できることを確認します。TFTP サーバをセットアップする際の注意事項は次のとおりです。

- サービス ポート経由でダウンロードする場合、サービス ポートはルーティングできないため、TFTP サーバはサービス ポートと同じサブネット上になければなりません。ただし、管理ポートがダウンしている間、TFTP サーバを別のネットワークに配置する場合は、サービス ポートのあるサブネットにゲートウェイがあれば、スタティック ルートを追加します（config route add *IP address of TFTP server*）。
- ディストリビューション システム ネットワーク ポートを経由してダウンロードする場合、ディストリビューション システム ポートはルーティング可能なので、TFTP サーバは同じサブネット上にあっても、別のサブネット上にあってもかまいません。
- Prime Infrastructure の組み込み TFTP サーバとサードパーティの TFTP サーバは同じ通信ポートを使用するため、サードパーティの TFTP サーバを Prime Infrastructure と同じコンピュータ上で実行することはできません。

ステップ 4 .tar または .zip ファイルをコントローラにダウンロードします。

コントローラでは、Web 認証の表示に必要なページおよびイメージ ファイルを含む、1 MB までの .tar ファイルをダウンロードできます。1MB の制限には、バンドル内の圧縮されていないファイルの合計サイズが含まれます。

これでダウンロードを続行できます。

ステップ 5 ファイルを TFTP サーバ上のデフォルト ディレクトリにコピーします。

ステップ 6 [Configuration] > [Network] > [Network Devices] > [Wireless Controller] の順に選択します。

ステップ 7 デバイス名をクリックします。複数のデバイスを選択すると、カスタマイズされた Web 認証ページが複数のコントローラにダウンロードされます。

ステップ 8 左側のサイドバーのメニューから、[System] > [Commands] の順に選択します。

ステップ 9 [Upload/Download Commands] ドロップダウン リストから、[Download Customized Web Auth] を選択し、[Go] をクリックします。

ステップ 10 バンドルを受信するコントローラの IP アドレスとその現在のステータスが表示されます。

ステップ 11 [File is Located On] フィールドから [local machine] を選択します。ファイル名および、サーバのルート ディレクトリに対して相対的なパスがわかる場合は、TFTP サーバを選択することもできます。

ローカル マシンのダウンロードには、.zip または .tar のファイル オプションがありますが、Prime Infrastructure では自動的に .zip を .tar に変換します。TFTP サーバのダウンロードを選択した場合は、.tar ファイルだけを指定します。

ステップ 12 [Maximum Retries] フィールドに、コントローラがファイルのダウンロードを試みる最大回数を入力します。

ステップ 13 [Timeout] フィールドに、ファイルをダウンロードする際、コントローラがタイムアウトするまでの最大時間を秒単位で入力します。

ステップ 14 ファイルは c:\tftp ディレクトリにアップロードされます。そのディレクトリ内のローカル ファイル名を指定するか、[Browse] をクリックしてナビゲートします。

ステップ 15 [OK] をクリックします。

転送がタイムアウトした場合には、[File Is Located On] フィールドの TFTP サーバ オプションを選択すると、サーバ ファイル名が読み込まれます。ローカル マシン オプションでは 2 段階の動作が起動されます。最初に、ローカル ファイルが管理者のワークステーションから Prime Infrastructure の組み込み TFTP サーバにコピーされます。次にコントローラがそのファイルを取得します。後の操作では、ファイルはすでに Prime Infrastructure サーバの TFTP ディレクトリにあるため、[Web のダウンロード（download web）] ページには、自動的にファイル名が入力されます。

ステップ 16 [Click here to download a sample tar file] リンクをクリックし、login.tar ファイルを開くか、保存するオプションを選択します。

ステップ 17 ダウンロードが完了すると、新しいページに接続され、認証できます。

関連トピック

コントローラ テンプレートの追加 （525 ページ）
コントローラ テンプレートの削除 （526 ページ）
コントローラ テンプレートの適用 （526 ページ）
コントローラ WLAN の Web 認証の認証タイプを設定する （542 ページ）

コントローラの外部 Web 認証サーバの設定

外部 Web 認証サーバ テンプレートを作成するか、既存の外部 Web 認証サーバ テンプレートを変更するには、次の手順を実行します。

ステップ 1 [Configuration] > [Templates] > [Features & Technologies] > [Controller] > [Security] > [External Web Auth Server] の順、または [Security] > [External Web Auth Server] の順に選択します。

ステップ 2 外部 Web 認証サーバのサーバ アドレスを入力します。

ステップ 3 [Save as New Template] をクリックします。

関連トピック

コントローラ テンプレートの追加 （525 ページ）
コントローラ テンプレートの削除 （526 ページ）
コントローラ テンプレートの適用 （526 ページ）

コントローラのパスワード ポリシーの設定

パスワード ポリシー テンプレートを追加、または既存のパスワード ポリシー テンプレートを変更するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [テンプレート（Templates）] > [機能およびテクノロジー（Features & Technologies）] > [コントローラ（Controller）] > [セキュリティ（Security）] > [パスワード ポリシー（Password Policy）]** を選択します。

ステップ 2 次の設定を有効または無効にできます。

- パスワードには、大文字、小文字、数字、特殊文字など、少なくとも 3 つのクラスの文字を含める必要があります。
- 同じ文字を 4 回以上連続して使用することはできません。
- パスワードには、cisco や admin などのデフォルトの単語は使用できません。
- パスワードに「cisco」、「ocsic」、「admin」、「nimda」を使用することはできません。また、これらの文字のいくつかを大文字にしたり、i を「1」、「|」、または「!」に、「o」を「0」に、または「s」を「$」に置き換たりすることもできません。
- パスワードには、ユーザ名やユーザ名を逆にしたものを使用できません。

ステップ 3 [Save] をクリックします。

関連トピック

コントローラ テンプレートの追加 （525 ページ）
コントローラ テンプレートの削除 （526 ページ）
コントローラ テンプレートの適用 （526 ページ）

コントローラ テンプレートの適用

コントローラ テンプレートは、選択した設定グループの 1 つ以上のコントローラに直接適用できます。

コントローラ テンプレートを適用するには、次の手順を実行します。

ステップ 1 [Configuration] > [Features & Technologies] > [Controller] の順に選択します。

ステップ 2 左側のサイドバーのメニューを使用して、適用するテンプレートのカテゴリを選択します。

ステップ 3 コントローラに適用するテンプレートのテンプレート名をクリックします。

ステップ 4 [Apply to Controllers] をクリックして、[Apply to Controllers] ページを開きます。

ステップ 5 テンプレートを適用する各コントローラのチェックボックスをオンにします。

すべてのコントローラを選択するには、コントローラ テーブルの左隅に表示されるチェックボックスをオンにします。

[Ignore errors on Apply template to Controllers] チェックボックスをオンにすると、エラーを無視して、テンプレートのすべてのコマンドをコントローラに適用できます。このチェックボックスがオフの場合、テンプレートのコマンドをコントローラに適用するときにエラーが発生すると、残りのコマンドは適用されません。

ステップ 6 テンプレートを直接適用する対象として、選択した設定グループの 1 つまたはすべてのコントローラより選択ください。

テンプレートを 1 つのコントローラ（もしくは、すべてのコントローラ）に直接適用するには、次の手順を実行します。

a) [選択したコントローラに直接適用（Apply to controllers selected directly）] オプション ボタンを選択します。[Apply to Controllers] ページに、コントローラ名および設定グループ名（該当する場合）とともに、使用できる各コントローラの IP アドレスがリストされます。
b) テンプレートを適用する各コントローラのチェックボックスをオンにします。

[Ignore errors on Apply template to Controllers] チェックボックスをオンにすると、エラーを無視して、テンプレートのすべてのコマンドをコントローラに適用できます。このチェックボックスがオフの場合、テンプレートのコマンドをコントローラに適用するときにエラーが発生すると、残りのコマンドは適用されません。

選択した設定グループのすべてのコントローラにテンプレートを適用するには、次の手順を実行します。

a) [選択した設定グループでコントローラを適用（Apply to controllers in the selected Config Groups）] オプション ボタンを選択します。[コントローラに適用（Apply to Controllers）] ページに、モビリティ グループ名および含まれるコントローラ数とともに、各設定グループの名前がリストされます。
b) テンプレートを適用する各設定グループのチェックボックスをオンにします。

コントローラのない設定グループには、テンプレートを適用できません。

ステップ 7 次の追加操作を実行できます。

- [Save Config to Flash after apply] チェックボックスをオンにした場合は、テンプレートが正常に適用されると、save config to Flash コマンドが実行されます。
- [Reboot Controller after apply] チェックボックスをオンにした場合は、テンプレートが正常に適用されると、コントローラがリブートします。

この設定結果は、[View Save Config / Reboot Results] オプションを有効にして、[Template Results] ページで表示できます。

ステップ 8 [Save] をクリックします。

[Template List] ページから直接、テンプレートを適用できます。適用するテンプレートのチェックボックスをオンにし、[Select a command] ドロップダウン リストから [Apply Templates] を選択し、[Go] をクリックして、[Apply to Controllers] ページを開きます。このテンプレートを適用するコントローラのチェックボックスをオンにして、[OK] をクリックします。

関連トピック

コントローラ テンプレートの追加 （525 ページ）

コントローラのアクセス コントロール リストの設定

アクセス コントロール リスト（ACL）は、特定のインターフェイスへのアクセスを制限するために使用される一連のルールです（たとえば、無線クライアントからコントローラの管理イ

ンターフェイスに ping が実行されるのを制限する場合などに使用されます）。ACL は無線クライアントとのデータ トラフィックとコントローラの中央処理装置（CPU）へのすべてのトラフィックに適用でき、再使用可能な IP アドレス グループと再使用可能なプロトコルをサポートできるようになりました。テンプレートでACLが設定された後、これらを管理インターフェイス、AP-manager インターフェイス、またはクライアント データ トラフィックのための任意の動的インターフェイス、コントローラ CPU へのトラフィックのためのネットワーク処理装置（NPU）インターフェイス、または WAN に適用できます。

プロトコル、方向、トラフィックの送信元や宛先ごとに ACL テンプレートを作成または変更できます。

ここで、定義済みの IP アドレス グループとプロトコル グループから新しいマッピングを作成できます。また、作成したルール マッピングから自動的にルールを生成できます。これらのルールは、連続した順序で生成されます。つまり、すでにルール 1 ～ 4 が定義されている場合は、最大 29 のルールを追加します。

既存の ACL テンプレートは新しい ACL テンプレートに複製されます。この複製は、ソース ACL テンプレートで定義した ACL ルールとマッピングをすべてコピーします。

このリリースの Prime Infrastructure は、IPv6 ACL をサポートします。

ACL テンプレートを追加、または既存の ACL テンプレートを変更するには、次の手順を実行します。

ステップ 1 [Configuration] > [Templates] > [Features & Technologies] > [Controller] > [Security] > [Access Control Lists] の順に選択します。

ステップ 2 次のフィールドに入力します。

- [Access Control List Name]：テンプレートのユーザ定義名。
- [ACL Type]：[IPv4] または [IPv6] を選択します。IPv6 ACL は、コントローラ リリース 7.2.x からサポートされます。

ステップ 3 左側のサイドバー メニューから [IP Groups] を選択し、再利用可能なグループ化された IP アドレスおよびプロトコルを作成します。

ステップ 4 [Select a command] ドロップダウン リストから [Add IP Group] を選択し、[Go] をクリックして新しい IP アドレス グループを定義します。

IP アドレス グループ 1 つで最高 128 の IP アドレスとネットマスクの組み合わせを格納できます。既存の IP アドレス グループを表示または変更するには、IP アドレス グループの URL をクリックします。[IP アドレス グループ（IP address group）]ページが開きます。IP アドレスが任意の場合用に、「任意（any）」グループが事前定義されています。

ステップ 5 必要に応じて、[ACL IP グループ（ACL IP Groups）] 詳細ページで次の現在の IP グループ フィールドを編集します。

- IP Group Name
- [IPアドレス（IP Address）]
- [ネットマスクまたは CIDR 表記（Netmask OR CIDR Notation）]

- ネットマスクまたは CIDR 表記を入力して、[追加（Add）] をクリックします。IP アドレスまたはネットマスクのリストが、[IP アドレス/ネットマスク（IP Address/Netmasks）] テキスト ボックスに表示されます。
- CIDR（クラスレス ドメイン間ルーティング）は、複数の連続するブロックでのクラス C IP アドレスの割り当てを可能にするプロトコルです。CIDR 表記を入力すると、1 つのクライアント オブジェクトを設定するだけで、サブネット範囲に存在する大量のクライアントを追加できます。
- ネットマスクを入力すると、IP アドレス プロパティの CIDR 表記ではなく、ドット区切り 10 進数表記でサブネット マスクを設定できます。
- BroadCast/Network
- List of IP Addresses/Netmasks
- [Move Up] ボタンおよび [Move Down] ボタンを使用して、リスト項目の順序を変更します。[Delete] ボタンを使用すると、IP アドレスまたはネットマスクを削除できます。

ステップ 6 左側のサイドバー メニューから [Access Control] > [Protocol Groups] の順に選択して、標準の事前定義済みプロトコルではない追加のプロトコルを定義します。

プロトコル グループとその送信元ポートおよび宛先ポートと DSCP の一覧が表示されます。

ステップ 7 [Select a command] ドロップダウン リストから [Add Protocol Group] を選択し、[Go] をクリックして新しいプロトコル グループを作成します。既存のプロトコル グループを表示または変更するには、グループの URL をクリックします。

[Protocol Groups] ページが表示されます。

ステップ 8 新しいルールの名前を入力します。ルールを定義するために ACL は必要ありません。パケットがルールのすべてのパラメータに一致すると、このルールに対する動作が実行されます。

ステップ 9 ドロップダウン リストから、次のいずれかのプロトコルを選択します。

- [Any]：すべてのプロトコル
- [TCP]：トランスミッション コントロール プロトコル
- [UDP]：ユーザ データグラム プロトコル
- [ICMP]：インターネット制御メッセージ プロトコル
- [ESP]：IP Encapsulating Security Payload
- [AH]：認証ヘッダー
- [GRE]：Generic Routing Encapsulation
- [IP]：インターネット プロトコル
- [Eth Over IP]：Ethernet over Internet Protocol
- [Other Port OSPF]：Open Shortest Path First
- [Other]：その他の任意の IANA プロトコル（http://www.iana.org/）

一部のプロトコル（TCP または UDP など）を選択すると、追加の送信元ポートおよび宛先ポート GUI エレメントが表示されます。

- [Source Port]：この ACL が適用されるパケットの送信元を指定します。[Any]、[HTTP]、[HTTPS]、[Telnet]、[RADIUS]、[DHCP Server]、[DHCP Client]、[DNS]、[L2TP]、[PPTP control]、[FTP control]、[SMTP]、[SNMP]、[LDAP]、[Kerberos]、[NetBIOS NS]、[NetBIOS DS]、[NetBIOS SS]、[MS Dir Server]、[Other]、[Port Range] を選択できます。

- [Dest Port]：この ACL が適用されるパケットの宛先を指定します。[Any]、[HTTP]、[HTTPS]、[Telnet]、[RADIUS]、[DHCP Server]、[DHCP Client]、[DNS]、[L2TP]、[PPTP control]、[FTP control]、[SMTP]、[SNMP]、[LDAP]、[Kerberos]、[NetBIOS NS]、[NetBIOS DS]、[NetBIOS SS]、[MS Dir Server]、[Other]、[Port Range] を選択できます。

ステップ 10 [DSCP (Differentiated Services Code Point)] ドロップダウン リストから、[any] または [specific] を選択します。[specific] を選択した、DSCP（0 ～ 255）を入力します。

DSCP は、インターネットでのサービスの質を定義するために使用できるパケット ヘッダー コードです。

ステップ 11 [Save] をクリックします。

ステップ 12 新しいマッピングを定義するために新しいグループをマップする ACL テンプレートを選択します。すべての ACL マッピングがページの最上部に表示され、すべての ACL ルールが下部に表示されます。

ステップ 13 [Select a command] ドロップダウン リストから [Add Rule Mappings] を選択します。[Add Rule Mapping] ページが表示されます。

ステップ 14 次のフィールドを設定します。

- [Source IP Group]：IPv4 および IPv6 の事前定義グループ。
- [Destination IP Group]：IPv4 および IPv6 の事前定義グループ。
- [Protocol Group]：ACL で使用するプロトコル グループ。
- [Direction]：[Any]、[Inbound (from client)]、または[Outbound (to client)]。
- [Action]：[Deny] または [Permit]。デフォルトのフィルタでは、ルールで明示的に許可されていない限り、すべてのアクセスを拒否します。

ステップ 15 [Add] をクリックします。新しいマッピングによって下部のテーブルにデータが表示されます。

ステップ 16 [Save] をクリックします。

ステップ 17 ルールを生成するマッピングを選択して、[Generate] をクリックします。これによって、ルールが自動的に作成されます。

関連トピック

コントローラ テンプレートの追加 （525 ページ）
コントローラ テンプレートの削除 （526 ページ）
コントローラ テンプレートの適用 （526 ページ）

コントローラでのトラフィックを制御するための FlexConnect アクセス コントロール リストの設定

許可されるトラフィックのタイプを、プロトコル、トラフィックの送信元や宛先により設定する FlexConnect ACL ACL テンプレートを作成または変更できます。FlexConnect ACL は、IPv6 アドレスをサポートしません。

アクセス コントロール リスト テンプレートを設定およびコントローラに適用するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [テンプレート（Templates）] > [機能およびテクノロジー（Features & Technologies）] > [コントローラ（Controller）] > [セキュリティ（Security）] > [FlexConnect ACL（FlexConnect ACLs）]** を選択します。

ステップ 2 新しい FlexConnect ACL の名前を入力します。

ステップ 3 [Save as New Template] をクリックします。

FlexConnect ACL テンプレートが作成されます。ここで、定義済みの IP アドレス グループとプロトコル グループから新しいマッピングを作成できます。新しいマッピングを定義するには、新しいグループをマップする ACL テンプレートを選択します。すべての FlexConnect ACL マッピングがページ上部に表示され、すべての FlexConnect ACL ルールがページ下部に表示されます。

ステップ 4 [Add Rule Mappings] をクリックして、[FlexConnect ACL IP Protocol Map] ページで次のフィールドを設定します。

- [Source IP Group]：IPv4 および IPv6 の事前定義グループ。
- [Destination IP Group]：IPv4 および IPv6 の事前定義グループ。
- [Protocol Group]：ACL で使用するプロトコル グループ。
- [Action]：[Deny] または [Permit]。デフォルトのフィルタでは、ルールで明示的に許可されていない限り、すべてのアクセスを拒否します。

ステップ 5 [Add] をクリックします。新しいマッピングによって下部のテーブルにデータが表示されます。

ステップ 6 [Save] をクリックします。

ステップ 7 ルールを生成するマッピングを選択して、[Generate] をクリックします。これによって、ルールが自動的に作成されます。

ステップ 8 [FlexConnect ACL] ページの [Select a command] ドロップダウン リストから、[Apply Templates] を選択します。

[Apply to Controllers] ページが表示されます。

ステップ 9 [Save Config to Flash after apply] チェックボックスをオンにして、FlexConnect ACL をコントローラに適用した後で設定を Flash に保存します。

ステップ 10 [Reboot Controller after apply] チェックボックスをオンにして、FlexConnect ACL が適用された後でコントローラをリブートします。このチェックボックスを使用できるのは、[Save Config to Flash after apply] チェックボックスをオンにしている場合だけです。

ステップ 11 1 つ以上のコントローラを選択し、[OK] をクリックして、FlexConnect ACL テンプレートを適用します。

作成した FlexConnect ACL は、**[設定（Configure）] > [コントローラ テンプレート起動パッド（Controller Template Launch Pad）] > [IP アドレス（IP Address）] > [セキュリティ（Security）] > [アクセス コントロール（Access Control）] > [FlexConnect ACL（FlexConnect ACLs）]** に表示されます。

関連トピック

コントローラ テンプレートの追加 （525 ページ）
コントローラ テンプレートの削除 （526 ページ）
コントローラ テンプレートの適用 （526 ページ）

FlexConnect グループの一括更新の管理

FlexConnect グループの一括作成

インポート ファイルに指定されているように、複数の FlexConnect グループにまとめて作成するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [テンプレート（Templates）] > [機能およびテクノロジー（Features & Technologies）]** をクリックします。

ステップ 2 左側の **[テンプレート（Templates）]** ペインで、**[機能およびテクノロジー（Features and Technologies）] > [コントローラ（Controller）] > [FlexConnect] > [FlexConnect 一括更新（FlexConnect Bulk Update）]** をクリックします。

ステップ 3 **[テンプレートの詳細（Template Detail）]** 領域で、**[一括オペレーション タイプ（Bulk Operation Type）]** ドロップダウン メニューから **[FlexConnect グループの作成（Create FlexConnect Group）]** を選択します。

ステップ 4 (オプション) **[上書き（Overwrite）]** チェックボックスをオンにして有効にします。

（注） 上書きを有効にすると、*.csv* ファイル内のソース設定を含む FlexConnect グループ テンプレートは、Prime Infrastructure データベース内の既存の重複テンプレートをすべて上書きします。

ステップ 5 **[ファイルの選択（Choose File）]** ボタンをクリックして、*.csv* file.

ステップ 6 **.csv**ファイルをロードしてプロセスをトリガーするには、*[アップロード (Upload)]* をクリックします。

重要

- ソースからコピーすると、AP を除く残りのすべての設定をコピーします。

選択したパラメータに基づいています。次の表に、シナリオとその期待される結果を示します。

上書きが有効	指定されたソース	既存のテンプレート	結果
対応	対応	非対応	**成功** ソーステンプレート値を使用して新しいテンプレートを作成します
対応	非対応	非対応	**成功** デフォルト値を使用して新しいテンプレートを作成します

上書きが有効	指定されたソース	既存のテンプレート	結果
対応	対応	対応	**成功** ソーステンプレート値を使用して既存のテンプレートを上書きします
対応	非対応	対応	**Failure** ソーステンプレートが指定されていないため上書きされません
非対応	対応	非対応	**成功** ソーステンプレート値を使用して既存のテンプレートを上書きします
非対応	非対応	非対応	**成功** デフォルト値を使用して新しいテンプレートを作成します
非対応	対応	対応	**Failure** テンプレートがすでに存在しており、上書きが有効になっていないため、テンプレートを作成しません
非対応	非対応	対応	**Failure** テンプレートがすでに存在しており、上書きが有効になっていないため、テンプレートを作成しません

一括で FlexConnect グループへのユーザーの追加

インポート ファイルに指定されているように、複数のユーザーを FlexConnect グループにまとめて追加するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [テンプレート（Templates）] > [機能およびテクノロジー（Features & Technologies）]** をクリックします。

ステップ 2 左側の **[テンプレート（Templates）]** ペインで、**[機能およびテクノロジー（Features and Technologies）] > [コントローラ（Controller）] > [FlexConnect] > [FlexConnect 一括更新（FlexConnect Bulk Update）]** をクリックします。

ステップ 3 **[テンプレートの詳細（Template Detail）]** 領域で、**[ユーザーを FlexConnect ユーザーに追加（Add Users to FlexConnect users）]** を選択します。

ステップ 4 (オプション) **[既存ユーザーの置き換え（Replace Existing Users）]** チェックボックスをオンにして有効にします。

（注） これを有効にすると、インポートファイルで指定されているように、既存のすべてのユーザーが新しいユーザーに置き換えられます。

ステップ 5 **[ファイルの選択（Choose File）]** ボタンをクリックして、*.csv* file.

ステップ 6 **.csv**ファイルをロードしてプロセスをトリガーするには、*[アップロード (Upload)]* をクリックします。

選択したパラメータに基づいています。次の表に、シナリオとその期待される結果を示します。

重要

既存ユーザーの置き換え	すでに存在するユーザー	結果
Disabled	いいえ	**成功** 指定された FlexConnect グループに新しいユーザーを追加します
Disabled	はい	**Failure** ユーザーがすでに存在しているため追加されません
イネーブル	×	**成功** 指定した FlexConnect グループに新しいユーザーを追加します。
イネーブル	対応	**成功** 既存ユーザー (存在する場合) を、*.csv* ファイルで指定されたものと同じユーザー名で置き換えます。

一括で FlexConnect グループへの AP の追加

インポート ファイルに指定されているように、複数のアクセス ポイントを FlexConnect グループにまとめて追加するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [テンプレート（Templates）] > [機能およびテクノロジー（Features & Technologies）]** をクリックします。

ステップ 2 左側の **[テンプレート（Templates）]** ペインで、**[機能およびテクノロジー（Features and Technologies）] > [コントローラ（Controller）] > [FlexConnect] > [FlexConnect 一括更新（FlexConnect Bulk Update）]** をクリックします。

ステップ 3 **[テンプレートの詳細（Template Detail）]** 領域で、**[一括オペレーション タイプ（Bulk Operation Type）]** ドロップダウン メニューから **[AP を FlexConnect グループに追加（Add APs to FlexConnect Groups）]** を選択します。

ステップ 4 (オプション) **[上書き（Overwrite）]** チェックボックスをオンにして有効にします。

（注） 上書きを有効にすると、.csv ファイル内のソース設定を含む FlexConnect グループ テンプレートは、Prime Infrastructure データベース内の既存の重複テンプレートをすべて上書きします。

ステップ 5 **[ファイルの選択（Choose File）]** ボタンをクリックして、*.csv* ファイルを選択します。

ステップ 6 **.csv**ファイルをロードしてプロセスをトリガーするには、*[アップロード (Upload)]* をクリックします。

選択したパラメータに基づいています。次の表に、シナリオとその期待される結果を示します。

重要

Overwrite	関連付けられている AP	結果
無効	同じ FlexConnect グループ	**成功** 同じ FlexConnect グループ内の AP を保持します。
無効	異なる FlexConnect グループ	**Failure** 別の FlexConnect グループに関連付けられているため、AP を追加しません。
無効	グループなし	**成功** AP を FlexConnect グループに追加します。
イネーブル	同じ FlexConnect グループ	**成功** 同じ FlexConnect グループ内の AP を保持します。
イネーブル	異なる FlexConnect グループ	**成功** 指定された FlexConnect グループに AP を追加し、それを古い FlexConnect グループから削除します。
イネーブル	グループなし	**成功** AP を FlexConnect グループに追加します。

コントローラ CPU と NPU 間のアクセス コントロール リスト トラフィック制御の設定

IPv6 での CPU ACL 設定は、このリリースではサポートされません。これは、仮想インターフェイスを除き、インターフェイスのコントローラのすべての IP アドレスが IPv4 を使用するためです。既存の ACL は、中央処理装置（CPU）とネットワーク プロセッサ ユニット（NPU）間のトラフィック制御を設定するために使用されます。

既存の CPU ACL テンプレートを追加または変更するには、次の手順を実行します。

ステップ 1 [Configuration] > [Templates] > [Features & Technologies] > [Controller] > [Security] > [CPU Access Control List] の順に選択します。

ステップ 2 CPU ACL を有効にするには、このチェックボックスをオンにします。CPU ACL が有効になり、コントローラに適用されると、Prime Infrastructure はそのコントローラに対する CPU ACL の詳細を表示します。

ステップ 3 [ACL Name] ドロップダウン リストから、定義済みの名前のリストから名前を選択します。

ステップ 4 [CPU ACL Mode] ドロップダウン リストから、この CPU ACL リストが制御するデータ トラフィックの方向を選択します。選択肢は、データ トラフィックの有線サイド、データ トラフィックの無線サイド、または有線と無線の両方です。

ステップ 5 [Save as New Template] をクリックします。

関連トピック

コントローラ テンプレートの追加 （525 ページ）
コントローラ テンプレートの削除 （526 ページ）
コントローラ テンプレートの適用 （526 ページ）

コントローラでの不正 AP およびクライアント セキュリティ ポリシーの設定

不正テンプレートでは、コントローラに適用される（アクセス ポイントとクライアントに対する）不正ポリシーを設定できます。また、不正ロケーション検出プロトコル（RLDP）が企業の有線ネットワークに接続されているかどうかも判断されます。RLDP を使用すると、コントローラは管理対象のアクセス ポイントに対して、不正アクセス ポイントをアソシエートし、特殊なパケットをコントローラへ送信するよう指示します。コントローラがこのパケットを受信すると、不正アクセス ポイントが企業ネットワークに接続されます。この方法は、暗号化を有効にしていない不正アクセス ポイントに対して機能します。

非常に RSSI 値が低く、不正解析にとって有益な情報とならない不正が多く存在する可能性があります。そのため、このオプションを使用して AP が不正を検出する最小 RSSI 値を指定することで、不正をフィルタできます。

不正アクセス ポイントのルールを使用すると、不正アクセス ポイントを自動的に分類するルールを定義できます。Cisco Prime Infrastructure はコントローラに不正なアクセス ポイントの分類ルールを適用します。これらのルールでは、RSSI レベル（それよりも弱い不正アクセス ポイントは無視）、または時間制限（指定された時間内に表示されない不正アクセス ポイントにはフラグを立てない）に基づいて、マップ上の不正表示を制限できます。不正アクセス ポイントのルールは、誤アラームを減らすのにも役立ちます。

ロール分類ルールへの新しい拡張機能は、Cisco WLC 7.4 以降に適用されます。この拡張は、Catalyst 3850、Catalyst 3650、Catalyst 4500 スイッチ、および Cisco 5760 WLAN コントローラ（WLC）には適用されません。

現在の分類ルールテンプレート、ルールの種類、適用されているコントローラ数を表示するには、[設定（Configuration）]>[テンプレート（Templates）]>[機能およびテクノロジー（Features & Technologies）]>[コントローラ（Controller）]>[セキュリティ（Security）]>[ワイヤレス保護ポリシー（Wireless Protection Policies）]>[不正APルール（Rogue AP Rules）] の順に選択します。

不正クラスには以下の種類があります。

- Malicious Rogue：検出されたアクセス ポイントのうち、ユーザが定義した Malicious ルールに一致したアクセス ポイント、または危険性のない AP カテゴリから手動で移動されたアクセス ポイント。
- Friendly Rogue：既知、認識済み、または信頼できるアクセス ポイント、または検出されたアクセス ポイントのうち、ユーザが定義した Friendly ルールに該当するアクセス ポイント。
- Unclassified Rogue：検出されたアクセス ポイントのうち、Malicious ルールまたは Friendly ルールに該当しないアクセス ポイント。

詳細については、「不正 AP ルール グループでの複数のコントローラ不正 AP ルールの組み合わせ」および『Cisco Prime Infrastructure Reference Guide』の次のトピックを参照してください。

- [コントローラ（Controller）]>[セキュリティ（Security）]>[ワイヤレス保護ポリシー（Wireless Protection Policies）]>[不正ポリシー（Rogue Policies）]
- [コントローラ（Controller）]>[セキュリティ（Security）]>[ワイヤレス保護ポリシー（Wireless Protection Policies）]>[不正APルール（Rogue AP Rules）]
- [コントローラ（Controller）]>[セキュリティ（Security）]>[ワイヤレス保護ポリシー（Wireless Protection Policies）]>[無視された不正AP（Ignored Rogue AP）]

コントローラの不正 AP 分類ルールの定義

Cisco Prime Infrastructure で不正ルールを設定するには、次の手順を実行します。

1. 不正 AP ルールを作成する
2. 適用するすべてのルールを含む不正 AP ルール グループを作成する
3. コントローラに不正 AP ルール グループを展開する

参照してください コント ローラー > セキュリティ > ワイヤレス保護ポリシー > 不正な *AP* 規則 の シスコ総理インフラストラクチャ参照ガイド 。

関連項目

- 不正 AP ルール グループでの複数のコントローラ不正 AP ルールの組み合わせ

不正 AP ルール グループでの複数のコントローラ不正 AP ルールの組み合わせ

不正アクセス ポイント ルール グループ テンプレートを使用すると、複数の不正アクセス ポイント ルールをコントローラに統合できます。現在の不正アクセス ポイント ルール グループ テンプレートを表示するか、新しいルール グループを作成するには、次の手順を実行します。

ステップ 1 [構成（Configuration）]>[テンプレート（Templates）]>[機能およびテクノロジー（Features & Technologies）]>[コントローラ（Controller）]>[セキュリティ（Security）]>[ワイヤレス保護ポリシー（Wireless Protection Policies）]>[不正 AP ルール グループ（Rogue AP Rule Groups）] を選択します。

ステップ 2 テンプレート名を入力します。

ステップ 3 Rogue AP ルールを追加するには、左の列のルールをクリックして強調表示します。[Add] をクリックして、強調表示したルールを右側の列に移動します。

不正アクセス ポイント ルールは、[Rogue Access Point Rules] セクションから追加できます。

ステップ 4 不正アクセス ポイント ルールを削除するには、右の列のルールをクリックして強調表示します。[Remove] をクリックして、強調表示したルールを左側の列に移動します。

ステップ 5 [Move Up]/[Move Down] ボタンをクリックして、ルールが適用される順序を指定します。任意のルールを強調表示し、[Move Up] または [Move Down] をクリックして、現在のリストで上下に移動させます。

ステップ 6 不正アクセス ポイント ルール リストを保存するには、[Save] をクリックします。

ステップ 7 [Deploy] をクリックして、コントローラにルール グループを適用します。

「展開された不正 AP ルールの表示」および [コントローラ（*Controller*）] > [セキュリティ（*Security*）] > [ワイヤレス保護ポリシー（*Wireless Protection Policies*）] で『Cisco Prime Infrastructure Reference Guide』の「Rogue AP Rules」の項を参照してください。

展開された不正 AP ルールの表示

以前に展開した不正 AP ルールを表示および編集できます。

ステップ 1 [Monitor] > [Network] > [Network Devices] > [Wireless Controllers] の順に選択します。

ステップ 2 デバイス名をクリックし、[Security] > [Wireless Protection Policies] > [Rogue AP Rules] の順に選択します。

ステップ 3 ルールを編集する不正 AP ルールの名前をクリックします。

ステップ 4 不正 AP アラームを表示するには、ページの右上にある [Alarm Summary] をクリックし、[Rogue AP] を選択します。また、[Dashboard] > [Wireless] > [Security] の順に選択して、不正 AP 情報を表示することもできます。

コントローラの SIP スヌーピングの設定

SIP スヌーピングを使用する際は、次のガイドラインを考慮します。

- SIP は、Cisco 5500 シリーズ コントローラ、1240、1130、および 11n アクセス ポイント上でのみ使用できます。
- SIP CAC は、ステータス コード 17 をサポートし、TSPEC ベースのアドミッション制御をサポートしない電話に対してのみ使用してください。
- SIP CAC は、SIP スヌーピングが有効になっている場合にのみサポートされます。

コントローラの SIP スヌーピングを設定するには、次の手順を実行します。

ステップ 1 [Configuration] > [Templates] > [Features & Technologies] > [Controller] > [802.11] > [SIP Snooping] の順に選択します。

ステップ 2 次のフィールドを設定します。

- **Port Start**
- **Port End**

単一ポートを使用する場合は、開始ポートおよび終了ポートのフィールドを同じ番号で設定します。

ステップ 3 [Save as New Template] をクリックします。

「Cisco Prime Infrastructure Reference Guide」の次の項を参照してください。

- Controller > 802.11 > Load Balancing
- Controller > 802.11 > Band Select
- Controller > 802.11 > Preferred Call
- Controller > 802.11 RF Profiles

管理テンプレートの作成

コントローラの次の管理パラメータに対するテンプレートを作成または変更できます。

- トラップ レシーバ
- トラップ コントロール
- Telnet および SSH
- 複数の Syslog サーバ
- ローカル管理ユーザ
- 認証優先度

詳細については、コントローラの管理パラメータの設定 （734ページ）を参照してください。

Cisco Prime Infrastructure で Microsoft LyncSDN を使用する

LyncSDN の設定は、仮想および Cisco 2500 シリーズおよび仮想コントローラではサポートされません。

次の LyncSDN テンプレートを作成できます。

- LyncSDN グローバル設定機能テンプレート
- LyncSDN PolicyFeature テンプレート
- LyncSDN ProfileFeature テンプレート

関連トピック

Microsoft LyncSDN 診断を使用するためのコントローラの設定 （561 ページ）
ネットワーク トラフィックの QoS をモニタする Microsoft LyncSDN ポリシーを使用するためのコントローラの設定 （562 ページ）
Microsoft LyncSDN WLAN プロファイルを使用するためのコントローラの設定 （562 ページ）

Microsoft LyncSDN 診断を使用するためのコントローラの設定

パラメータを作成して、LyncSDN グローバル設定機能を使用してデバイスに適用するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [機能およびテクノロジー（Features & Technologies）] > [コントローラ（Controller）] > [LyncSDN] > [LyncSDN グローバル設定（LyncSDN Global Config）]** を選択します。

ステップ 2 [Template Basic] 領域で、該当するテキスト ボックスにテンプレートの名前、説明、およびタグを入力します。

ステップ 3 [Validation Criteria] 領域で、ドロップダウン リストからデバイス タイプを選択し、OS バージョンを入力します。

ステップ 4 [Template Detail] 領域で、次の情報を設定します。

- [LyncServer] チェックボックスを選択して、Prime Infrastructure の LYNC アプリケーションを有効または無効にします。
- ポート番号を入力します。
- LYNC サーバの Prime Infrastructure での HTTP/HTTPS 通信へのサポートを設定できます。Prime Infrastructure は http のみをサポートします。HTTPS 証明書の場合は、Prime Infrastructure からの Lync サービスの準備が整ったら取得する Lync サーバを提供し、承認しておく必要があります。

ステップ 5 終了したら、[テンプレートとして保存（Save as Template）] をクリックします。

関連トピック

ネットワーク トラフィックの QoS をモニタする Microsoft LyncSDN ポリシーを使用するためのコントローラの設定 （562 ページ）
Microsoft LyncSDN WLAN プロファイルを使用するためのコントローラの設定 （562 ページ）

ネットワーク トラフィックの QoS をモニタする Microsoft LyncSDN ポリシーを使用するためのコントローラの設定

パラメータを作成して、LyncSDN ポリシー機能を使用してデバイスに適用するには、次の手順を実行します。

ステップ 1 [Configuration] > [Features & Technologies] > [Controller] > [LyncSDN] > [LyncSDN Policy] の順に選択します。

ステップ 2 [Template Basic] 領域で、該当するテキスト ボックスにテンプレートの名前、説明、およびタグを入力します。

ステップ 3 [Validation Criteria] 領域で、ドロップダウン リストからデバイス タイプを選択し、OS バージョンを入力します。

ステップ 4 [Template Detail] 領域で、次の情報を設定します。

- [Audio] ドロップダウン リストから、WLAN での音声 lync コールのポリシーを選択します。選択可能なポリシー タイプは、[Silver]、[Gold]、[Platinum]、または [Bronze] です。
- [Video] ドロップダウン リストから、WLAN でのビデオ lync コールのポリシーを選択します。選択可能なポリシー タイプは、[Silver]、[Gold]、[Platinum]、または [Bronze] です。
- [Application-Sharing] ドロップダウン リストから、WLAN でのデスクトップ共有 lync コールのポリシーを選択します。選択可能なポリシー タイプは、[Silver]、[Gold]、[Platinum]、または [Bronze] です。
- [File-Transfer] ドロップダウン リストから、WLAN でのファイル転送 lync コールのポリシーを選択します。選択可能なポリシー タイプは、[Silver]、[Gold]、[Platinum]、または [Bronze] です。

ステップ 5 終了したら、[Save as Template] をクリックします。

関連トピック

Microsoft LyncSDN 診断を使用するためのコントローラの設定 （561 ページ）
Microsoft LyncSDN WLAN プロファイルを使用するためのコントローラの設定 （562 ページ）

Microsoft LyncSDN WLAN プロファイルを使用するためのコントローラの設定

パラメータを作成して、LyncSDN プロファイル機能を使用してデバイスに適用するには、次の手順を実行します。

ステップ 1 [Configuration] > [Features & Technologies] > [Controller] > [LyncSDN] > [LyncSDN Policy] の順に選択します。

ステップ 2 [Template Basic] 領域で、該当するテキスト ボックスにテンプレートの名前、説明、およびタグを入力します。

ステップ 3 [Validation Criteria] 領域で、ドロップダウン リストからデバイス タイプを選択し、OS バージョンを入力します。

ステップ 4 [Template Detail] 領域で、[Wlan Profile] チェックボックスをクリックし、[LyncSDN Policy] ドロップダウン リストからポリシーを選択します。

ステップ 5 終了したら、[Save as Template] をクリックします。

関連トピック

Microsoft LyncSDN 診断を使用するためのコントローラの設定 （561 ページ）
ネットワーク トラフィックの QoS をモニタする Microsoft LyncSDN ポリシーを使用するためのコントローラの設定 （562 ページ）

コントローラでのアプリケーション分類用 AVC プロファイルの設定

Application Visibility and Control（AVC）は、Network Based Application Recognition（NBAR）ディープ パケット インスペクション テクノロジーを使用して、使用するプロトコルに基づいてアプリケーションを分類します。AVC を使用して、コントローラはレイヤ 4 ～レイヤ 7 の 1400 を超えるプロトコルを検出できます。AVC により、リアルタイム分析を実施し、ネットワークの輻輳、コストの掛かるネットワーク リンクの使用、およびインフラストラクチャの更新を削減するためのポリシーを作成することができるようになります。

AVC は次のコントローラでのみサポートされます。

- Cisco 2500 および 5500 シリーズ コントローラ
- WiSM 2 コントローラ
- Cisco FLEX 7500 および Cisco 8500 シリーズ コントローラ

AVC プロファイル テンプレートを設定するには、次の手順を実行します。

ステップ 1 [Configuration] > [Features & Technologies] > [Controller] > [Application Visibility And Control] > [AVC Profiles] の順に選択します。

ステップ 2 新しいテンプレートを追加する場合は、[AVC プロファイル（AVC Profiles）] の上にマウスを移動して、[新規（New）] を選択するか、または [AVC プロファイル（AVC Profiles）] をクリックします。既存のテンプレートを変更するには、テンプレート名をクリックします。

ステップ 3 [AVC Profile Name] テキストボックスに、AVC プロファイル名を入力します。

（注） 1 つの WLAN には AVC プロファイルを 1 つだけ設定できます。また各 AVC プロファイルに最大 32 のルールを設定できます。各ルールでは、アプリケーションのマーキング アクションまたはドロップ アクションを示します。これにより、WLAN ごとに最大 32 のアプリケーション アクションを設定できます。コントローラ 1 台に最大 16 の AVC プロファイルを設定し、AVC プロファイル 1 つを複数の WLAN に関連付けることができます。

ステップ 4 [AVC Rule List] で、[Add Row] をクリックして AVC ルールを作成します。

- [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。
- [Application Group Name] フィールドに、アプリケーションが属するアプリケーション グループの名前を入力します。
- [Action] ドロップダウン リストから、次のいずれかを選択します。
  - [Drop]：選択されたアプリケーションに対応するアップストリームおよびダウンストリーム パケットをドロップします。

- [Mark]：[Differentiated Services Code Point (DSCP)] ドロップダウン リストで指定する DSCP 値と選択されたアプリケーションに対応するアップストリームおよびダウンストリーム パケットをマークします。DSCP 値を使用して、QoS レベルに基づいて Differentiated Services を提供できます。
- [Rate Limit]：アクションとして [Rate Limit] を選択すると、クライアント 1 人あたりの平均レート制限とバースト データ レート制限を指定できます。レート制限アプリケーションの数は 3 に制限されています。

デフォルト アクションは、すべてのアプリケーションの許可です。

- アクションとして [マーキング（Mark）] を選択した場合は、[DSCP] ドロップダウン リストから QoS レベルを選択します。DSCP は、インターネットでの QoS を定義するために使用されるパケット ヘッダー コードです。DSCP 値は次の QoS レベルにマッピングされます。
  - [Platinum (Voice)]：Voice over Wireless の高い QoS を保証します。
  - [Gold (Video)]：高品質のビデオ アプリケーションをサポートします。
  - [Silver (Best Effort)]：クライアントの通常の帯域幅をサポートします。
  - [Bronze (Background)]：ゲスト サービス用の最小の帯域幅を提供します。
  - [Custom]：DSCP 値を指定します。範囲は 0 ～ 63 です。
- [DSCP Value] フィールドに、[Custom] が [DSCP] ドロップダウン リストで選択されている場合のみ入力できる値を入力します。
- アクションとして **[Rate Limit（レート制限）]** を選択した場合、**[平均（Avg）] に値を指定できます。レート制限 (in Kbps)** は、そのアプリケーションの平均帯域幅の制限です。
- アクションとして [Rate Limit] を選択した場合は、そのアプリケーションの最大制限である [Burst Rate Limit (in Kbps)] を指定できます。

ステップ 5 [Save as New Template] をクリックします。

関連トピック

コントローラ テンプレートの追加 （525 ページ）
コントローラ テンプレートの削除 （526 ページ）
コントローラ テンプレートの適用 （526 ページ）

NetFlow を使用するためのデバイスの設定

NetFlowは、ネットワーク ユーザとアプリケーション、ピーク時の使用時間、およびトラフィック ルーティングに関する貴重な情報を提供するプロトコルです。このプロトコルは、トラフィックをモニタするためにネットワーク デバイスからIP トラフィック情報を収集します。NetFlow アーキテクチャは、次のコンポーネントで構成されています。

- コレクタ：さまざまなネットワーク要素から IP トラフィック情報をすべて収集するエンティティ。
- エクスポータ：IP トラフィック情報を使用してテンプレートをエクスポートするネットワーク エンティティ。コントローラは、エクスポータとして機能します。

NetFlow モニタ テンプレートまたはエクスポータ テンプレートを作成するには、次の手順を実行します。

ステップ 1 [設定（Configuration）]>[テンプレート（Templates）]>[機能およびテクノロジー（Features & Technologies）]>[コントローラ（Controller）]>[NetFlow] を選択します。

ステップ 2 新しいモニタ テンプレートを作成するには、[モニタ（Monitor）] テンプレート タイプの横にあるツールチップの上にマウスのカーソルを合わせ、[新規（New）] をクリックします。

ステップ 3 必須フィールドに値を入力し、[新しいテンプレートとして保存（Save as New Template）] をクリックします。

ステップ 4 新しい**エクスポータ** テンプレートを作成するには、[エクスポータ（Exporter）] テンプレート タイプの横にあるツールチップの上にマウスのカーソルを合わせ、[新規（New）] をクリックします。

ステップ 5 必須フィールドに値を入力し、[新しいテンプレートとして保存（Save as New Template）] をクリックします。

コントローラでの Ethernet over GRE（EoGRE）トンネルの設定

Ethernet over GRE（EoGRE）により、EoGRE トンネルを使用した Cisco WLC または Cisco AP からモバイル パケット コアへのデータ トラフィックのトンネリングが可能になります。

EoGRE トンネリング テンプレートを追加または変更するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [機能およびテクノロジー（Features & Technologies）] > [コントローラ（Controller）] > [トンネリング（Tunneling）] > [EoGRE]** を選択します。

ステップ 2 テンプレート タイプの横にあるツール チップにマウスのカーソルを合わせ、[新規（New）] をクリックして作成します。

ステップ 3 必要なフィールドに入力して、[新しいテンプレートとして保存（Save As New Template）] をクリックし、テンプレートを保存するフォルダを指定して、[保存（Save）] をクリックします。

ステップ 4 [展開（Deploy）] をクリックして、関連するコントローラにテンプレートを保存および展開します。

ステップ 5 テンプレート展開のステータスを確認するには、**[管理（Administration）] > [ダッシュボード（Dashboards）] > [ジョブ ダッシュボード（Job Dashboard）]** を選択します。

ステップ 6 後続の設定テンプレートの導入に関する導入パラメータを変更するには、コンフィギュレーション ジョブを選択し、[編集（Edit）] をクリックします。

関連トピック

コントローラ テンプレートの追加 （525 ページ）
コントローラ テンプレートの削除 （526 ページ）
コントローラ テンプレートの適用 （526 ページ）

テンプレートを使用した Lightweight AP の設定

新しい Lightweight アクセス ポイント テンプレートを設定するには、次の手順を実行します。

ステップ 1 [Configuration] > [Templates] > [Lightweight Access Points] の順に選択します。

ステップ 2 [Select a command] ドロップダウン リストから [Add Template] を選択し、[Go] をクリックします。

ステップ 3 テキスト ボックスにテンプレート名を入力します。

ステップ 4 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 5 [Save as New Template] をクリックします。

[Lightweight AP Template Detail] ページには次のタブがあります。

- AP Parameters
- Mesh
- 802.11a/n/ac
- 802.11a SubBand
- 802.11b/g/n
- [802.11a/b/g/n]
- CDP
- FlexConnect

Lightweight AP テンプレートでは、次の無線間でアンテナ方向の情報を共有できます。

- [802.11a/n/ac]
- [802.11b/g/n]
- [802.11a/b/g/n]

（注）
- 軽量 AP テンプレートでは、**外部**としてのみ**アンテナ タイプ**を選択できます。
- [他の無線に以下のパラメータをコピーする（Copy below parameters to other radios）] をクリックして、アンテナ方向の情報を現在の無線から他の無線にコピーします。この機能は、選択された [アンテナ名（Antenna Name）] が他の無線にも使用可能である場合のみ使用できます。

関連トピック

AP テンプレート展開のための AP ソースの選択 （566 ページ）

AP テンプレート展開のための AP ソースの選択

AP ソースの選択に基づいて、[AP の選択（AP Selection）] タブに適切な可視化設定がロードされます。

AP ソースを選択するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [テンプレート（Templates）] > [Lightweight アクセス ポイント（Lightweight Access Points）]** を選択します。

ステップ 2 [Lightweight アクセス ポイント（Lightweight Access Point）] ページで、該当するテンプレート名のリンクをクリックします。

ステップ 3 [AP ソース（AP Source）] タブをクリックし、可視化を選択します。

- **手動での AP の選択**：このオプションを選択すると、LWAP テンプレート設定を AP に適用するときに手動で AP を選択する必要があります。
- [サイト マップ（Site Maps）]：このオプションを選択すると、LWAP テンプレート設定の展開のために動的ロケーション ベースのサイト マップを選択できます。

テンプレートを使用した自律 AP の設定

新しい Autonomous アクセス ポイント テンプレートを設定するには、次の手順を実行します。

ステップ 1 [Configuration] > [Templates] > [Autonomous Access Points] の順に選択します。

ステップ 2 [Select a command] ドロップダウン リストから、[Add Template] を選択します。

ステップ 3 [Go] をクリックします。

ステップ 4 テンプレート名を入力します。

ステップ 5 該当する CLI コマンドを入力します。

show コマンドは [CLI commands] テキスト ボックスに含めないでください。show コマンドはサポートされていません。

ステップ 6 **[保存（Save）]** をクリックします。

テンプレートを使用したスイッチの場所情報の設定

スイッチ位置設定テンプレートを使用して、スイッチの位置テンプレートを設定できます。

スイッチの位置テンプレートを設定するには、次の手順を実行します。

ステップ 1 [Configuration] > [Templates] > [Switch Location] の順に選択します。

[Switch Location Configuration template] ページが表示されます。

ステップ 2 [Select a command] ドロップダウン リストから、[Add Template] を選択し、[Go] をクリックします。

ステップ 3 [New Template] ページの必須フィールドに値を入力します。

AP 移行テンプレートを使用した Autonomous アクセス ポイントから Lightweight アクセス ポイントへの移行

すでに管理されている Autonomous アクセス ポイントを LWAPP へ移行する場合には、その位置とアンテナの情報も移行されます。情報を再入力する必要はありません。Cisco Prime Infrastructure では、移行後に Autonomous アクセス ポイントが自動的に削除されます。

[Migration Analysis] オプションは、デフォルトでは、検出中に実行されません。検出中に移行分析を実行する場合、[Administration] > [Settings] > [CLI Session] の順に選択して、このオプションを有効にします。

Cisco Prime Infrastructure は、CAPWAP アクセス ポイントへの Autonomous アクセス ポイントの移行もサポートしています。

このページにアクセスするには、[構成（Configuration）] > [テンプレート（Templates）] > [自律型APの移行（Autonomous AP Migration）] の順に選択します。Autonomous ソリューションから Unified アーキテクチャへ移行するには、Autonomous アクセス ポイントを Lightweight アクセス ポイントへ変換する必要があります。アクセス ポイントを Lightweight に変換した後は、アクセス ポイントの前のステータスまたは設定は保持されません。

Autonomous AP 移行テンプレートを作成するには、次の手順を実行します。

- [構成（Configuration）] > [自律型APの移行（Autonomous AP Migration）] の順に選択します。
- **[コマンドの選択（Select a command）]** ドロップダウン リストから、**[テンプレートの追加（Add Template）]** を選択し、**[実行（Go）]** をクリックします。既存のテンプレートを更新している場合は、[テンプレート名（Template Name）] 列の該当するテンプレートをクリックします。
- 移行分析の概要を表示するには、[モニタ（Monitor）] > [ツール（Tools）] > [自律型AP移行分析（Autonomous AP Migration Analysis）] の順に選択します。

フィールド説明の詳細については、『Cisco Prime Infrastructure Reference Guide』を参照してください。

自律 AP 移行の影響の分析

移行分析の概要を表示するには、次の手順を実行します。

ステップ 1 [Configuration] > [Templates] > [Autonomous AP Migration] の順に選択します。

ステップ 2 [Select a Command] ドロップダウン リストから [View Migration Analysis Summary] を選択し、[Go] をクリックします。[Migration Analysis Summary] ページが表示されます。

Autonomous アクセス ポイントは、すべての基準が成功ステータスの場合だけ移行できます。赤の X マークは移行できないことを示し、緑のチェックマークは移行できることを示します。これらの列は次のものを表しています。

- [Privilege 15 Criteria]：Autonomous アクセス ポイントの検出の一部として指定された Telnet クレデンシャルは、特権 15 であることが必要です。
- [Software Version Criteria]：変換は、12.3(11)JA、12.3(11)JA1、12.3(11)JA2 および 12.3(11)JA3 を除く Cisco IOS リリース 12.3(7)JA だけでサポートされます。
- [Role Criteria]：アソシエーション要求を送信するには、アクセス ポイントとコントローラの間の有線接続が必要です。そのため、次の Autonomous アクセス ポイント ロールが必要です。
  - root
  - root access point
  - root fallback repeater
  - root fallback shutdown
  - root access point only
- [Radio Criteria]：デュアル無線アクセス ポイントの場合、1 つの無線の種類のみがサポートされている場合でも変換を実行できます。
- 変換できないことを示すラベルが付いている Autonomous アクセス ポイントは無効にすることができます。

関連トピック

AP 移行テンプレートを使用した Autonomous アクセス ポイントから Lightweight アクセス ポイントへの移行 （568 ページ）

設定テンプレートの展開

設定テンプレートを作成したら、[展開（Deploy）] をクリックします。次の表に、さまざまな展開オプションを示します。

表 47 : テンプレート展開オプション

オプション	説明
Device Selection	テンプレートを適用するデバイスのリストを表示します。 [デバイスごと（By Device）]：すべてのサポート対象デバイスを表示します。 [グループごと（By Group）]（デバイス タイプ）：サポート対象デバイスのサポート対象デバイス グループのみを表示します。 [グループごと（By Group）]（場所、定義ユーザ）サポート対象デバイスがない場合でも、すべてのデバイス グループを表示します。ただし、グループごとにサポート対象デバイスのみが表示されます。 （注） [グループごとの検索（Search for By Group）] オプションでは、サポート対象デバイスを含むグループのみが表示されます。

オプション	説明
Value Assignment	コンフィギュレーション テンプレートで事前に定義された変数以外の変数を指定できます。名前をクリックすると、事前に定義された変数が表示されます。いずれかの値を変更するには、変更する変数をクリックし、新しい値を入力して、[Apply] をクリックします。 選択したすべてのデバイスで変数を更新することもできます。選択したすべてのデバイスで同時に変更を適用するには、[All Selected Devices] をクリックして変数を更新します。他のデバイスに適用される必要がないリスト内の特定のデバイスの変数を更新する場合は、デバイスを選択し、その変数を更新します。変数が更新されたデバイスを除き、他のすべてのデバイスは、以前に定義された変数を引き続き使用します。 （注） 変更は、展開する特定の設定だけに適用されます。今後のすべての展開に対して設定テンプレートを変更するには、[Configuration] > [Templates] > [Features & Technologies] の順に選択して、テンプレートを変更します。
スケジュール	わかりやすい展開ジョブ名を付けてから、ただちにジョブを実行するか、後で実行するかを指定できます。 また、時間単位、日次、週次、月次、または年次単位で定期的にジョブを実行するようにスケジュールできます。
Job Option	次のジョブ オプションを使用できます。 • 失敗ポリシー（Failure Policy）： • [Ignore failure and continue]：これはデフォルトのオプションです。デバイスは、テンプレートの展開にランダムに選択されます。ジョブを実行できないデバイスがあった場合、そのデバイスをスキップし、引き続き残りのデバイスでジョブを実行します。ジョブ結果には、選択したすべてのデバイスの成功/失敗情報が表示されます。 • [Stop on failure]：ジョブがデバイスでの実行に失敗した場合、そのジョブは停止します。ジョブ結果は、ジョブが正常に実行されたデバイスと、テンプレートの展開が行われなかった他のデバイスについてのみ更新されます。「Not Attempted」メッセージが表示されます。展開のために選択されたデバイスの順序は、[Value assignment] ペインのデバイスの順序と同じです。 • [Copy Running Config to Startup]：テンプレートの展開ジョブが成功すると、デバイスの実行コンフィギュレーションがスタートアップ コンフィギュレーションにコピーされます。 • [Archive Config after deploy]：新しい設定アーカイブ ジョブを作成し、テンプレートを正常に展開した後で、デバイスのコンフィギュレーションをアーカイブします。
Summary	ユーザが選択した展開オプションを要約します。

モデルベースの設定テンプレートの展開フロー

（注） この展開フローは、コントローラ ベースのテンプレートには適用されません。

ステップ 1 設定テンプレートを作成したら、[展開（Deploy）] をクリックします。[展開（Deployment）] ウィザード ページが開きます。

ステップ 2 テンプレートを展開するデバイスを選択し、[次へ（Next）] をクリックして入力値を選択します。

ステップ 3 [入力値（Input Values）] タブでは、[フォーム（Form）] ビューと [CLI] ビューを切り替えることができます。

ステップ 4 必要な設定値を入力したら、[次へ（Next）] をクリックするか、または [CLI] をクリックして、デバイスおよびテンプレートの設定値を確認します。

ステップ 5 必要に応じて、[展開のスケジュール設定（Schedule Deployment）] タブを使用して展開ジョブをスケジュール設定します。

- わかりやすい展開ジョブ名を付けてから、ただちに実行するか、後で実行するかを指定します。
- また、時間単位、日次、週次、月次、または年次単位で定期的にジョブを実行するようにスケジュールできます。
- 次のジョブ オプションを設定できます。

失敗ポリシー（Failure Policy）

- **失敗を無視して続行**：これはデフォルトのオプションです。デバイスは、テンプレートの展開にランダムに選択されます。ジョブを実行できないデバイスがあった場合、そのデバイスをスキップし、引き続き残りのデバイスでジョブを実行します。ジョブ結果には、選択したすべてのデバイスの成功/失敗情報が表示されます。
- **失敗で停止**：ジョブがデバイスでの実行に失敗した場合、そのジョブは停止します。ジョブ結果は、ジョブが正常に実行されたデバイスと、テンプレートの展開が行われなかった他のデバイスについてのみ更新されます。「未試行（Not Attempted）」メッセージが表示されます。展開のために選択されたデバイスの順序は、[Value assignment] ペインのデバイスの順序と同じです。
- [実行コンフィギュレーションをスタートアップにコピー（Copy Running Config to Startup）]：テンプレートの展開ジョブが成功すると、デバイスの実行コンフィギュレーションがスタートアップ コンフィギュレーションにコピーされます。
- **展開後に設定をアーカイブ**：新しい設定アーカイブ ジョブを作成し、テンプレートを正常に展開した後で、デバイスのコンフィギュレーションをアーカイブします。

ステップ 6 [次へ（Next）] をクリックしてジョブ展開サマリーを表示します。

ステップ 7 [展開サマリー（Deployment Summary）] タブに、各デバイスの CLI ビューが表示されます。

ステップ 8 [終了（Finish）] をクリックしてテンプレートを展開します。

ステップ 9 ジョブのステータスを表示するには、ポップアップ ダイアログボックスで [ジョブのステータス（Job Status）] をクリックして [ジョブ ダッシュボード（Job Dashboard）] を起動します。

グローバル変数

グローバルユーザ変数はすべてスクリプトでアクセス可能な変数です。各ユーザ変数には、*gv* で始まる名前が必要です。名前はアルファベットで開始する必要があります。許容される特殊文字は、gv に付加されたドット、ハイフン、およびアンダースコアです。

グローバル変数を作成、削除、または編集することができます。

ステップ 1 **[設定（Configuration）] > [テンプレート（Templates）] > [グローバル変数（Global Variable）]** を選択します。

ステップ 2 [グローバル変数の定義（Define Global Variable）] ページから、[行の追加（Add Row）] をクリックします。

ステップ 3 名前、説明、タイプ、および表示ラベルを指定します。

ステップ 4 [保存（Save）] をクリックして新しい変数を保存します。

ここで作成したグローバル変数は、CLI テンプレートおよび機能およびテクノロジー テンプレートを作成する際に適用できます。

関連項目

- 既存のテンプレートを使用した新機能およびテクノロジー テンプレートの作成

共有ポリシー オブジェクト

ポリシー オブジェクトを使用すると、要素の論理集合を定義できます。ポリシー オブジェクトは再利用可能な名前付きコンポーネントであり、他のオブジェクトやポリシーで使用できます。また、ポリシーを定義するたびにコンポーネントを定義する必要がなくなります。

オブジェクトはグローバルに定義されます。つまり、オブジェクトの定義は、そのオブジェクトを参照しているすべてのオブジェクトおよびポリシーで同じになります。ただし、多くのオブジェクト タイプ（インターフェイス ロールなど）は、デバイス レベルで上書きできます。これは、ほとんどのデバイスに対して有効なオブジェクトを作成し、要件が若干異なる特定のデバイスの設定にあうようにオブジェクトをカスタマイズできることを意味します。

設定テンプレートの効率性と精度を向上させるために、設定テンプレートに含める共有ポリシー オブジェクトを作成できます。インターフェイス ロールまたはネットワーク オブジェクトを作成し、設定テンプレートに追加できます。

関連トピック

インターフェイス ロールの定義 （573 ページ）
ネットワーク オブジェクトの定義 （573 ページ）
セキュリティ ルール パラメータ マップの作成 （574 ページ）
セキュリティ サービス グループの作成 （575 ページ）
セキュリティ ゾーンの作成 （575 ページ）

インターフェイス ロールの定義

インターフェイス ロールを使用すると、各インターフェイスの名前を手動で定義することなく、複数のデバイス上の特定のインターフェイスにポリシーを定義できます。インターフェイス ロールは、デバイス上の実際のインターフェイスのいずれかを参照できます。インターフェイスには、物理インターフェイス、サブインターフェイス、仮想インターフェイス（ループバック インターフェイスなど）があります。

All-Ethernets インターフェイス ロールを作成する場合は、1 つの定義だけでデバイス上のあらゆるイーサネット インターフェイスに対して同じ高度な設定を定義できます。設定テンプレートにこのインターフェイス ロールを追加し、選択したデバイスにテンプレートを展開して、イーサネット インターフェイスを設定します。

インターフェイス ロールは、新しいデバイスにポリシーを適用するときに特に役立ちます。追加するデバイスが既存のデバイスと同じインターフェイス命名方式を共有しているかぎり、インターフェイス ロールを含む必要な設定テンプレートを新しいデバイスにすばやく展開できます。

たとえば、インターフェイス ロールを使用して、ゾーン ベースのファイアウォール設定テンプレートでゾーンを定義できます。DMZ* という命名パターンでインターフェイス ロールを定義できます。このインターフェイス ロールをテンプレートに含めると、その設定は、選択したデバイス上の名前が「DMZ」で始まるすべてのインターフェイスに適用されます。その結果、すべての DMZ インターフェイスでアンチ スプーフィング チェックをイネーブルにするポリシーを、関連するすべてのデバイス インターフェイスに 1 回のアクションで適用できます。

ステップ 1 **[設定（Configuration）] > [テンプレート（Templates）] > [共有ポリシーオブジェクト（Shared Policy Objects）]** の順に選択します。

ステップ 2 [共有ポリシー オブジェクト（Shared Policy Objects）] ペインで、**[共有（Shared）] > [インターフェイス ロール（Interface Role）]** を選択します。

ステップ 3 [Interface Role] ページから、[Add Object] をクリックします。

ステップ 4 [Add Interface Role] ページから、インターフェイス ロールに対する一致ルールを作成します。

たとえば、ゾーン ベースのテンプレートを定義すると、指定されたルールに一致するデバイス上のすべてのインターフェイスがこのインターフェイス ロールによって表されるセキュリティ ゾーンのメンバーになります。名前、説明、タイプおよび速度に応じてインターフェイスを照合できます。

ステップ 5 [OK] をクリックして、設定を保存します。

関連トピック

共有ポリシー オブジェクト （572 ページ）

ネットワーク オブジェクトの定義

ネットワーク オブジェクトは、ネットワークを表す IP アドレスまたはサブネットの論理集合です。ネットワーク オブジェクトによって、ポリシーの管理が簡単になります。

IPv4 および IPv6 アドレス用の別個のオブジェクトがあり、IPv4 オブジェクトは「ネットワーク/ホスト」と呼ばれ、IPv6 オブジェクトは「ネットワーク/ホスト IPv6」と呼ばれます。アドレス表記を除き、これらのオブジェクトは機能的に同じであり、多くの場合、名前のネットワーク/ホストはどちらかのオブジェクトのタイプに適用されます。特定のポリシーでは、ポリシーで想定されているアドレス タイプによって、いずれか 1 つのオブジェクト タイプの選択が必須になります。

次の設定テンプレートで使用される共有ポリシー オブジェクトを作成できます。

- ゾーンベース ファイアウォール テンプレート（Zone-based firewall template）
- アプリケーションの表示（Application Visibility）

ステップ 1 **[設定（Configuration）] > [テンプレート（Templates）] > [共有ポリシー オブジェクト（Shared Policy Objects）] > [共有（Shared）] > [IPv4 ネットワーク オブジェクト（IPv4 Network Object）]** を選択します。

ステップ 2 [Network Object] ページから、[Add Object] をクリックして、IP アドレスまたはサブネットのグループを追加します。

ステップ 3 [OK] をクリックして、設定を保存します。

関連トピック

共有ポリシー オブジェクト （572 ページ）

セキュリティ ルール パラメータ マップの作成

ファイアウォール ルールにパラメータ マップ オブジェクトのセットを作成して使用するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [テンプレート（Templates）] > [共有ポリシーオブジェクト（Shared Policy Objects）]** の順に選択します。

ステップ 2 [共有ポリシー オブジェクト（Shared Policy Objects）] ペインで、**[共有（Shared）] > [セキュリティ ルール パラメータ マップ（Security Rule Parameter Map）]** を選択します。

ステップ 3 [Security Rule Parameter Map] ページから、[Add Object] をクリックします。

ステップ 4 作成中のパラメータ マップの名前と説明を指定します。

ステップ 5 パラメータ リストから、それぞれに対し値を適用して指定するパラメータを選択します。

ステップ 6 デバイス レベルのオーバーライドを指定するには、**[デバイス レベルのオーバーライド（Device Level Override）] > [デバイスの追加（Add Device）]** の順に選択します。

ステップ 7 追加するデバイスを選択し、[OK] をクリックします。

ステップ 8 [OK] をクリックして、設定を保存します。

関連トピック

共有ポリシー オブジェクト （572 ページ）

セキュリティ サービス グループの作成

ファイアウォールルールにパラメータ マップ オブジェクトのセットを作成して使用するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [テンプレート（Templates）] > [共有ポリシーオブジェクト（Shared Policy Objects）]** の順に選択します。

ステップ 2 [共有ポリシー オブジェクト（Shared Policy Objects）] ペインで、**[共有（Shared）] > [セキュリティ サービス（Security Service）]** を選択します。

ステップ 3 [Security Service] ページから、[Add Object] をクリックします。

ステップ 4 作成中のサービスの名前と説明を指定します。

ステップ 5 使用可能なリストからサービス データを選択します。[TCP] または [UDP] を選択した場合は、ポート番号またはポート範囲のリストを提供します（カンマで区切る）。

ステップ 6 デバイス レベルのオーバーライドを指定するには、**[デバイス レベルのオーバーライド（Device Level Override）] > [デバイスの追加（Add Device）]** を選択します。

ステップ 7 追加するデバイスを選択し、[OK] をクリックします。

ステップ 8 [OK] をクリックして、設定を保存します。

関連トピック

共有ポリシー オブジェクト （572 ページ）

セキュリティ ゾーンの作成

ステップ 1 **[設定（Configuration）] > [テンプレート（Templates）] > [共有ポリシーオブジェクト（Shared Policy Objects）]** の順に選択します。

ステップ 2 [共有ポリシー オブジェクト（Shared Policy Objects）] ペインで、**[共有（Shared）] > [セキュリティ ゾーン（Security Zone）]** を選択します。

ステップ 3 [Security Zone] ページから、[Add Object] をクリックします。

ステップ 4 作成中のセキュリティ ゾーンの名前と説明を指定します。

ステップ 5 ゾーンにアタッチする必要があるインターフェイスを定義するルールのセットを指定します。

ステップ 6 デバイス レベルのオーバーライドを指定するには、**[デバイスレベルのオーバーライド（Device Level Override）] > [デバイスの追加（Add Device）]** の順に選択します。

ステップ 7 追加するデバイスを選択し、[OK] をクリックします。

ステップ 8 [OK] をクリックして、設定を保存します。

関連トピック

共有ポリシー オブジェクト （572 ページ）

設定グループとは

設定テンプレートのセットを特定のデバイスに関連付けることをお勧めします。同じ設定を必要とするデバイスがある場合、設定テンプレートをデバイスに関連付ける設定グループを作成できます。設定グループを作成することで、新しいテンプレートを展開するデバイスを覚えていなくても、新しいテンプレートをすぐに適用できます。

複合テンプレートを使用すると、小規模のテンプレートを一つにグループ化できますが、テンプレートとそのテンプレートが適用されるデバイスのグループとの関係を指定するのは設定グループだけです。また、設定グループ内のテンプレートがデバイスに展開される順序を指定することもできます。

設定グループを作成する前に、以下を実行する必要があります。

- 設定グループでデバイス用の設定テンプレートを作成します。
- 設定グループに含めるデバイスを決定します。

関連項目

- 既存のテンプレートを使用した新機能およびテクノロジー テンプレートの作成
- ユーザ定義グループを使用した NE グループへの変更の適用

ユーザ定義グループを使用した NE グループへの変更の適用

ステップ 1 [Configuration] > [Templates] > [Configuration Groups] の順に選択します。

ステップ 2 必須フィールドに値を入力します。表示されるデバイス タイプは、[Device Type] フィールドの選択内容によって異なります。

ステップ 3 必要に応じて、テンプレートを選択して上矢印または下矢印をクリックしてグループ内での順序を変更します。

ステップ 4 [Save as a New Configuration Group] をクリックします。可能な設定グループは次のとおりです。

- 成功（Success）：設定グループが正常に作成されたことを示します。
- 保留中（Pending）：設定グループ内の 1 つ以上のデバイスに、まだ展開されていない変更があります。たとえば、設定グループに新しいデバイスを追加した場合、新しいデバイスのステータスは [Pending] となります。設定グループが関連付けられている設定テンプレートを変更した場合、設定グループ内のすべてのデバイスのステータスは [Pending] となります。
- スケジュール済み（Scheduled）：設定グループの展開が予定されていることを示します。設定グループが [Scheduled] の場合、グループ内の [Pending] または [Failed] のデバイスは [Scheduled] に変更されます。デバイスが [Deployed] の場合、そのデバイスは [Deployed] のままとなり、そのステータスは [Scheduled] に変更されません。
- 失敗（Failure）：展開が設定グループ内の 1 つ以上のデバイスで失敗しました。

関連トピック

既存のテンプレートを使用した新機能およびテクノロジーテンプレートの作成（505 ページ）
設定グループとは（576 ページ）

WLAN コントローラ設定グループとは

設定グループを作成することで、同じモビリティグループ名および類似する設定を持つ必要のあるコントローラをグループ化できます。テンプレートをグループに割り当てて、テンプレートをグループ内のすべてのコントローラに適用できます。設定グループを追加、削除、または解除することができ、ソフトウェア、IDS シグニチャ、またはカスタマイズした Web 認証ページを、選択した設定グループのコントローラにダウンロードできます。また、現在の設定を、選択した設定グループのコントローラの不揮発性（フラッシュ）メモリに保存することもできます。

（注） コントローラは、複数のモビリティグループのメンバーにはできません。コントローラをあるモビリティ グループに追加すると、すでにメンバーとなっている別のモビリティ グループからそのコントローラが削除されます。

[設定（Configuration）] > [テンプレート（Templates）] > [WLAN コントローラ設定グループ（WLAN Controller Configuration Groups）] を選択すると、Prime Infrastructure データベースのすべての設定グループの概要を表示できます。[コマンドの選択（Select a command）] ドロップダウン リストから [設定グループの追加（Add Configuration Groups）] を選択すると、次の列を持つ表が表示されます。

- [Group Name]：設定グループの名前。
- [Templates]：設定グループに適用するテンプレートの数。

関連項目

- コントローラ設定グループを作成し、それらに設定テンプレートを適用する

コントローラ設定グループを作成し、それらに設定テンプレートを適用する

設定グループを作成するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [テンプレート（Templates）] > [WLANコントローラ設定グループ（WLAN Controller Configuration Groups）]** の順に選択します。

ステップ 2 [コマンドの選択（Select a command）] ドロップダウン リストから、[設定グループの追加（Add Config Group）] を選択し、[実行（Go）] をクリックします。

ステップ 3 新しい設定グループ名を入力します。これは全グループで一意である必要があります。

- [バックグラウンド監査の有効化（Enable Background Audit）] を選択すると、この設定グループのネットワークとコントローラの監査が実行されます。
- [適用の有効化（Enable Enforcement）] を選択すると、何らかの矛盾が見つかった場合、監査中にテンプレートが自動的に適用されます。

ステップ 4 Prime Infrastructure で作成されたその他のテンプレートを、設定グループに割り当てることができます。同じ WLAN テンプレートを、複数の設定グループに割り当てることができます。次の中から選択します。

- [Select and add later]：後でテンプレートを追加するにはクリックします。
- [Copy templates from a controller]：別のコントローラからテンプレートをコピーするにはクリックします。現在のコントローラ一覧からコントローラを選択して、それに適用されているテンプレートを新しい設定グループにコピーします。テンプレートだけがコピーされます。

（注） 無線テンプレートを使用する場合、テンプレートの順序が重要になります。たとえば、テンプレートリストに無線テンプレートが含まれ、無線パラメータを適用する前に無線ネットワークを無効にする必要がある場合、まず無線ネットワークを無効にするテンプレートをテンプレートに追加する必要があります。

ステップ 5 [Save] をクリックします。[Configuration Groups] ページが表示されます。

- 設定グループの作成後、Prime Infrastructure で、コントローラのグループに適用するテンプレートを選択することで、複数のコントローラを選択して設定することができます。
- [一般（General）]：モビリティ グループを有効にできます。
- [バックグラウンド監査（Background Audit）] オプションを有効にするには、**[管理（Administration）] > [システム（System）] > [監査の設定（Audit Settings）]** でテンプレートベースの監査を設定します。
- [コントローラ（Controllers）]
- [国/DCA（Country/DCA）]
- [テンプレート（Templates）]：作成済みの設定テンプレートを選択できます。
- [適用/スケジュール（Apply/Schedule）]
- 監査（Audit）
- 再起動
- [レポート（Report）]：このグループの最新のレポートを表示できます。

関連トピック

WLAN コントローラ設定グループとは （577 ページ）
コントローラ設定グループでのコントローラの追加または削除 （579 ページ）
コントローラ設定グループへの DCA チャネルの設定 （579 ページ）
コントローラ設定グループへのテンプレート展開のスケジュール設定 （580 ページ）
コンプライアンスを確保するためのコントローラ設定グループの監査 （581 ページ）
設定グループのリブート （582 ページ）
コントローラ設定グループへのテンプレート展開ステータスの表示 （582 ページ）

コントローラ設定グループでのコントローラの追加または削除

設定グループのコントローラを追加または削除するには、次の手順を実行します。

ステップ 1 [設定（Configuration）]>[テンプレート（Templates）]>[WLAN コントローラ設定グループ（WLAN Controller Configuration Groups）] の順に選択します。

ステップ 2 [Group Name] 列のグループ名をクリックして、[Audit] タブをクリックします。

このテーブルの列にはコントローラの IP アドレス、コントローラが含まれる設定グループの名前、コントローラのモビリティ グループ名が表示されます。

ステップ 3 グループに追加したいコントローラの行をクリックして強調表示させ、[Add] をクリックします。

ステップ 4 グループからコントローラを削除するには、[Group Controllers] 領域のコントローラを強調表示させ、[Remove] をクリックします。

ステップ 5 [Apply/Schedule] タブをクリックし、[Apply] をクリックして、設定グループでコントローラを追加または削除し、[Save Selection] をクリックします。

関連トピック

WLAN コントローラ設定グループとは （577 ページ）
コントローラ設定グループへの DCA チャネルの設定 （579 ページ）
コントローラ設定グループへのテンプレート展開のスケジュール設定 （580 ページ）
コンプライアンスを確保するためのコントローラ設定グループの監査 （581 ページ）
コントローラ設定グループへのテンプレート展開ステータスの表示 （582 ページ）

コントローラ設定グループへの DCA チャネルの設定

1 つまたは複数の国をコントローラに設定できます。国をコントローラに設定すると、対応する 802.11a/n DCA チャネルが選択可能になります。少なくとも 1 つの DCA チャネルを、802.11a/n ネットワークに対して選択する必要があります。国コードが変更されると、DCA チャネルも連携して自動的に変更されます。

（注） コントローラの 802.11a/n および 802.11b/n のネットワークとアクセス ポイントを無効にしてから、コントローラ上で国を設定してください。802.11a/n または 802.11b/n のネットワークを無効にするには、[Configure]>[Controllers] の順に選択し、無効にする目的のコントローラを選択し、[802.11a/n] または [802.11b/g/n] を左側のサイドバー メニューから選択して、[Parameters] を選択します。[Network Status] が最初のチェックボックスです。

設定グループで定義された複数のコントローラを追加して DCA チャネルを設定するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [テンプレート（Templates）] > [WLANコントローラ設定グループ（WLAN Controller Configuration Groups）]** の順に選択します。

ステップ 2 [Select a command] ドロップダウン リストから、[Add Config Groups] を選択し、[Go] をクリックします。

ステップ 3 グループ名およびモビリティ グループ名を入力して、設定グループを作成します。

ステップ 4 [Save] をクリックしてから、[Controllers] タブをクリックします。

ステップ 5 追加するコントローラを強調表示して、[Add] をクリックします。コントローラが [Group Controllers] ページに追加されます。

ステップ 6 [Country/DCA] タブをクリックします。[Country/DCA] ページが表示されます。DCA により、コントローラに接続された管理対象デバイスの中から妥当なチャネルの割り当てが自動的に選択されます。

ステップ 7 [Update Country/DCA] チェックボックスをオンにして、選択する国の一覧を表示します。

ステップ 8 同じモビリティ グループのコントローラ上で現在設定されている DCA チャネルが、[Select Country Codes] ページに表示されます。選択した国に割り当て可能な対応チャネル（802.11a/n および 802.11b/n）も表示されます。一覧に記載されているチャネルを追加または削除するには、チャネルを選択または選択解除して、[Save Selection] をクリックします。

最低 1 か国および最高 20 か国を、1 つのコントローラに設定できます。

関連トピック

WLAN コントローラ設定グループとは （577 ページ）
コントローラ設定グループへのテンプレート展開のスケジュール設定 （580 ページ）
コンプライアンスを確保するためのコントローラ設定グループの監査 （581 ページ）
コントローラ設定グループへのテンプレート展開ステータスの表示 （582 ページ）

コントローラ設定グループへのテンプレート展開のスケジュール設定

スケジューリング機能を使用して、プロビジョニングの開始日および開始時刻をスケジューリングできます。

モビリティ グループ、モビリティ メンバー、およびテンプレートを設定グループのすべてのコントローラに適用するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [テンプレート（Templates）] > [WLANコントローラ設定グループ（WLAN Controller Configuration Groups）]** の順に選択します。

ステップ 2 [Group Name] 列のグループ名をクリックして、[Apply/Schedule] タブを選択します。

ステップ 3 [Apply] をクリックして、モビリティ グループ、モビリティ メンバー、およびテンプレートのプロビジョニングを、設定グループのすべてのコントローラに対して開始します。適用後は、このページから移動するか、またはPrime Infrastructure からログアウトできます。プロセスは続行されるため、後でこのページに戻り、レポートを表示することができます。

（注） プロビジョニング プロセス中は、他の設定グループの機能は実行しないでください。

レポートが生成され、[Recent Apply Report] ページに表示されます。コントローラのそれぞれに正常に適用されたモビリティ グループ、モビリティ メンバー、またはテンプレートが表示されます。

ステップ 4 テキスト ボックスに開始日を入力するか、カレンダーのアイコンを使用して開始日を選択します。

ステップ 5 開始時刻を、[hours] および [minutes] ドロップダウン リストを使用して選択します。

ステップ 6 [Schedule] をクリックして、スケジューリングした時間にプロビジョニングを開始します。

関連トピック

WLAN コントローラ設定グループとは （577 ページ）
コントローラ設定グループでのコントローラの追加または削除 （579 ページ）
コントローラ設定グループへの DCA チャネルの設定 （579 ページ）
コントローラ設定グループへのテンプレート展開ステータスの表示 （582 ページ）

コンプライアンスを確保するためのコントローラ設定グループの監査

[コンフィギュレーション グループの監査（Configuration Groups Audit）] ページでは、コントローラの設定がグループ テンプレートとモビリティ グループに適合しているかどうかを確認できます。監査時に、このウィンドウから離れたり、Prime Infrastructure からログアウトすることができます。プロセスは継続され、後でこのページに戻りレポートを表示できます。

監査中は、その他の設定グループの機能は実行しないでください。

設定グループ監査を実行するには、次の手順を実行します。

ステップ 1 [設定（Configuration）]>[テンプレート（Templates）]>[WLAN コントローラ設定グループ（WLAN Controller Configuration Groups）] の順に選択します。

ステップ 2 [Group Name] 列のグループ名をクリックして、[Audit] タブをクリックします。

ステップ 3 [Controllers] タブでコントローラをクリックして強調表示し、[>> (Add)] および [Save Selection] を選択します。

ステップ 4 [Templates] タブでテンプレートをクリックして強調表示し、[>> (Add)] および [Save Selection] を選択します。

ステップ 5 [Audit] をクリックして、監査プロセスを開始します。

レポートが生成され、各コントローラの現在の設定が設定グループのテンプレートと比較されます。レポートには監査ステータス、同期テンプレートの数、非同期テンプレートの数が表示されます。

この監査では、デバイスに対して Prime Infrastructure 設定は強制されません。矛盾の識別だけを行います。

ステップ 6 [Details] をクリックして、コントローラ監査レポートの詳細を表示します。

ステップ 7 項目をダブルクリックして、[Attribute Differences] ページを開きます。このページには属性、Prime Infrastructure の属性値、コントローラの属性値が表示されます。

ステップ 8 [Prime Infrastructure 値の保持（Retain Prime Infrastructure Value）] をクリックして、[属性の違い（Attribute Differences）] ページのすべての属性をデバイスにプッシュします。

ステップ 9 [閉じる（Close）] をクリックして、[コントローラ監査レポート（Controller Audit Report）] ページに戻ります。

関連トピック

WLAN コントローラ設定グループとは （577 ページ）
コントローラ設定グループでのコントローラの追加または削除 （579 ページ）
コントローラ設定グループへのテンプレート展開のスケジュール設定 （580 ページ）
コントローラ設定グループへのテンプレート展開ステータスの表示 （582 ページ）

設定グループのリブート

ステップ 1 [設定（Configuration）]>[テンプレート（Templates）]>[WLAN コントローラ設定グループ（WLAN Controller Configuration Groups）] の順に選択します。

ステップ 2 [グループ名（Group Name）] 列のグループ名をクリックし、[再起動（Reboot）] タブをクリックします。

ステップ 3 一度に1つのコントローラをリブートして、そのコントローラが起動されるまで待ってから次のコントローラをリブートする場合は、[カスケード リブート（Cascade Reboot）] チェックボックスをオンにします。

ステップ 4 [Reboot] をクリックして、設定グループのすべてのコントローラを一度にリブートします。リブート中は、このページを離れたり、Prime Infrastructure からログアウトしたりできます。プロセスは継続され、後でこのページに戻りレポートを表示できます。

[Recent Reboot Report] ページに、各コントローラがリブートされた時間、リブート後のコントローラのステータスが表示されます。Prime Infrastructure がコントローラをリブートできない場合は、失敗が表示されます。

コントローラ設定グループへのテンプレート展開ステータスの表示

指定のグループ名で最近適用されたすべてのレポートを表示するには、次の手順を実行します。

ステップ 1 [設定（Configuration）]>[テンプレート（Templates）]>[WLAN コントローラ設定グループ（WLAN Controller Configuration Groups）] の順に選択します。

ステップ 2 [Group Name] 列のグループ名をクリックし、[Report] タブをクリックします。[Recent Apply Report] ページには、適用ステータス、適用が開始された日時、テンプレート数などを示す、最近適用されたレポートがすべて表示されます。各 IP アドレスに関する次の情報が表示されます。

- [Apply Status]：Success（成功）、Partial Success（一部成功）、Failure（失敗）、Not Initiated（未開始）を示します。
- [Successful Templates]：該当する IP アドレスに関連する正常なテンプレートの数を示します。

- [Failures]：コントローラに対するモビリティ グループ、モビリティ メンバー、およびテンプレートのプロビジョニングの失敗数を示します。
- [詳細（Details）]：クリックすると、それぞれの失敗と関連するエラー メッセージが表示されます。

ステップ 3 スケジューリングされたタスク レポートを表示するには、ページ下部の [ここをクリック（click here）] リンクをクリックします。

関連トピック

WLAN コントローラ設定グループとは （577 ページ）
コントローラ設定グループでのコントローラの追加または削除 （579 ページ）
コントローラ設定グループへの DCA チャネルの設定 （579 ページ）
コントローラ設定グループへのテンプレート展開のスケジュール設定 （580 ページ）

ワイヤレス設定テンプレートの作成

次の各項では、以下に対しワイヤレス設定テンプレートを作成する方法について説明します。

- Lightweight アクセス ポイント
- Autonomous アクセス ポイント
- スイッチ
- Autonomous アクセス ポイントの Lightweight アクセス ポイントへの変換

関連項目

- 設定テンプレートを使用した Lightweight AP の設定
- AP 移行テンプレートを使用した Autonomous アクセス ポイントから Lightweight アクセス ポイントへの移行
- テンプレートを使用したスイッチの場所情報の設定

設定テンプレートを使用した Lightweight AP の設定

Lightweight アクセス ポイントのテンプレートを作成するには、次の手順を実行します。

ステップ 1 [Configuration] > [Templates] > [Lightweight Access Points] の順に選択します。
ステップ 2 [Select a command] ドロップダウン リストから、[Add Template] を選択し、[Go] をクリックします。
ステップ 3 テンプレートの名前と説明を入力し、[Save] をクリックします。既存のテンプレートを更新している場合は、[Template Name] 列の該当するテンプレートをクリックします。
ステップ 4 各タブをクリックして、必須フィールドに値を入力します。

関連トピック

AP 移行テンプレートを使用した Autonomous アクセス ポイントから Lightweight アクセス ポイントへの移行 （568 ページ）

AP へのデバイス ベース ポリシーの設定

[Policy Configuration Templates] ページでは、コントローラにデバイス ベースのポリシーを設定することができます。ネットワーク上のユーザまたはデバイス用のポリシーを設定できます。

設定できるポリシーの最大数は 64 です。AAA オーバーライドがコントローラに設定されている場合は、ポリシーは WLAN および AP グループに適用されません。

ステップ 1 [設定（Configuration）]>[テンプレート（Templates）]>[機能およびテクノロジー（Features & Technologies）] を選択します。

ステップ 2 左側のサイドバーのメニューから、[機能およびテクノロジー（Features and Technologies）]>[コントローラ（Controller）]>[WLAN（WLANs）]>[ポリシー設定（Policy Configuration）] を選択します。[Policy Configuration Template] ページが表示されます。

ステップ 3 次のフィールドに入力します。

- [Name]：ポリシー テンプレートの名前
- [Description]：ポリシー テンプレートの説明。
- [Tags]：このテンプレートに適用する検索キーワード。
- [Device Type]（検証基準）：テンプレートを検証するのに使用されるデバイス製品ファミリ、シリーズまたはタイプ（Cisco Unified Wireless Network の場合は CUWN がデフォルトです）。
- [Policy Name]：ポリシーの名前。
- [Policy Role]：ユーザの属するユーザ タイプまたはユーザ グループ。たとえば、学生、従業員など。
- [EAP Type]：クライアントが使用する EAP 認証方式。使用可能なタイプは次のとおりです。
  - LEAP
  - EAP-FAST
  - EAP-TLS
  - PEAP
- [Device Type]：このポリシーが適用されるデバイス タイプを選択します（たとえば、Apple Laptop）。
- [VLAN ID]：ポリシーに関連付けられる VLAN。
- [IPv4 ACL]：リストからポリシーの IPv4 ACL を選択します。
- [QoS]：リストからポリシーの Quality of Service レベルを選択します。次のいずれかを選択できます。
  - [Platinum (Voice)]：Voice over Wireless の高い QoS を保証します。
  - [Gold (Video)]：高品質のビデオ アプリケーションをサポートします。
  - [Silver (Best Effort)]：クライアントの通常の帯域幅をサポートします。
  - [Bronze (Background)]：ゲスト サービス用の最小の帯域幅を提供します。
- [Session Timeout]：クライアントが強制的に再認証されるまでの最大時間数（秒単位）。デフォルト値は 0 秒です。

- [Sleeping Client Timeout]：ゲスト クライアントが強制的に再認証されるまでの最大時間数（時間単位）。デフォルト値は 12 時間です。範囲は 1 ～ 720 時間です。

ステップ 4 終了したら、[新規テンプレートとして保存（Save as new template）] をクリックします。

第 26 章

ワイヤレス デバイスの設定

- Cisco Prime Infrastructure でのコントローラの表示 （589 ページ）
- 設定テンプレートの展開のためのコントローラ固有のコマンド （590 ページ）
- コントローラで使用されている設定テンプレートの確認と関連付けの削除 （592 ページ）
- インポートした CSV ファイルを使用したコントローラ クレデンシャルの変更 （594 ページ）
- 再起動によるコントローラ変更の適用 （595 ページ）
- コントローラへのソフトウェアのダウンロード （595 ページ）
- FTP/TFTP サーバへのコントローラ設定とログ ファイルのアップロード （597 ページ）
- コントローラへの IDS シグネチャのダウンロード （597 ページ）
- コントローラへの圧縮された Web 認証ログイン ページ情報のダウンロード （598 ページ）
- コントローラへのベンダー デバイス証明書のダウンロード （599 ページ）
- コントローラへの CA 証明書のダウンロード （600 ページ）
- ネットワーク アシュアランスの設定 （601 ページ）
- デバイス フラッシュへのコントローラ設定の保存 （605 ページ）
- データベースへのコントローラ設定の保存（同期） （606 ページ）
- コントローラの既存のテンプレートを検出 （606 ページ）
- コントローラに適用されているテンプレートの表示 （607 ページ）
- IP アドレスを保持したままのコントローラ交換 （608 ページ）
- コントローラ プロパティの変更 （608 ページ）
- [ネットワークデバイス（Network Devices）]テーブルからコントローラの一般システム プロパティを変更する （608 ページ）
- コントローラの設定ファイルおよびログ ファイルを TFTP サーバにアップロードする （613 ページ）
- コントローラへのソフトウェアのダウンロード （613 ページ）
- 単一コントローラでのインターフェイスの設定 （614 ページ）
- コントローラでのインターフェイスの表示 （615 ページ）
- コントローラ システム インターフェイス グループを使用したコントローラ グループへのインターフェイス変更の適用 （616 ページ）
- NAC アプライアンスを使用したコントローラへのユーザ アクセスの制御 （617 ページ）
- SNMP NAC の使用時の前提条件 （618 ページ）

- RADIUS NAC の使用時の前提条件 （619 ページ）
- コントローラでの SNMP NAC の設定 （619 ページ）
- 有線コントローラへのゲスト アカウント アクセスの設定 （621 ページ）
- 有線ゲスト ユーザ アクセスの設定と有効化：ワークフロー （622 ページ）
- コントローラでのゲスト LAN 入力インターフェイスの設定 （624 ページ）
- コントローラでのゲスト LAN 出力インターフェイスの設定 （625 ページ）
- コントローラ サービス ポートでのネットワーク ルートの設定 （626 ページ）
- コントローラの STP パラメータの表示 （627 ページ）
- モビリティとは （628 ページ）
- モビリティ グループとは （632 ページ）
- メッシュ ネットワーク バック グラウンド スキャン用のコント ローラーを構成します。（638 ページ）
- コントローラ QoS プロファイルの設定 （641 ページ）
- 内部 DHCP サーバに関する情報 （642 ページ）
- コントローラのユーザ認証に使用されるコントローラのローカル ネットワーク テンプレートの表示 （646 ページ）
- コントローラのユーザ認証に使用されるコントローラのローカル ネットワーク テンプレートの設定 （646 ページ）
- コントローラに接続する AP のコントローラ ユーザ名とパスワードの設定 （647 ページ）
- コントローラでの CDP の設定 （647 ページ）
- コントローラへの 802.1X 認証の設定 （648 ページ）
- コントローラへの 802.1X 認証の設定 （649 ページ）
- コントローラでの DHCP の設定 （650 ページ）
- 障害検出時間を短縮するコントローラの拡張タイマーの設定 （651 ページ）
- コントローラでの WLAN の作成 （652 ページ）
- コントローラで構成されている WLAN の表示 （652 ページ）
- コントローラ上の WLAN へのセキュリティ ポリシーの追加 （653 ページ）
- コントローラでのモバイル コンシェルジュ（802.11u）の設定 （654 ページ）
- コントローラへの WLAN の追加 （657 ページ）
- コントローラからの WLAN の削除 （657 ページ）
- コントローラの WLAN の管理ステータスを変更する （658 ページ）
- コントローラ WLAN のモビリティ アンカーの表示 （659 ページ）
- 802.11r 高速移行の設定 （660 ページ）
- Fastlane QoS の設定 （662 ページ）
- Fastlane QoS の無効化 （662 ページ）
- コントローラの WLAN AP グループの設定 （663 ページ）
- コントローラの WLAN AP グループの作成 （664 ページ）
- コントローラの WLAN AP グループの削除 （666 ページ）
- 構成の違いを特定するためのコントローラ WLAN AP グループの監査 （666 ページ）
- キャプティブ ポータル バイパスに関する情報 （667 ページ）
- FlexConnect を使用した AP の設定とモニタ （669 ページ）

• デフォルト FlexConnect グループ （683 ページ）
• コントローラまたはデバイスのセキュリティ設定の構成 （685 ページ）
• サードパーティ製コントローラまたはアクセス ポイントの設定 （757 ページ）
• ユニファイド AP の設定 （768 ページ）
• コントローラ冗長性の設定 （771 ページ）
• 脅威からコントローラを保護するための Cisco Adaptive wIPS の設定 （771 ページ）
• MSE サーバの高可用性の設定 （778 ページ）
• プラグ アンド プレイを使用したコントローラの設定 （783 ページ）

Cisco Prime Infrastructure でのコントローラの表示

Prime Infrastructure データベースのすべてのコントローラの概要を表示できます。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 ページ上部のコマンド ボタンを使用するには、1 つ以上の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。次の表に、このページで使用できるフィールドについて説明します。

表 *48 :* ワイヤレス コントローラのサマリー情報

フィールド	説明
[管理ステータス（Admin Status）]	ワイヤレス コントローラの管理ステータス。
[DNS 名（DNS Name）]	ワイヤレス コントローラの DNS 名。
[最終インベントリ収集ステータス（Last Inventory Collection Status）]	最後のインベントリ収集のステータス。
[前回正常終了した収集の時間（Last Successful Collection Time）]	前回正常終了した収集の時間。
[クライアント カウント（Client Count）]	現在コントローラに関連付けられているクライアントの合計数を表示します。
[ソフトウェア タイプ（Software Type）]	すべての管理対象デバイスのソフトウェア タイプを表示します。
参照先	ロケーション情報を表示します。
デバイス名（Device Name）	コントローラの名前。デバイスの詳細の表示、コントローラの設定、テンプレートの適用、設定アーカイブの表示およびスケジュール設定、コントローラ ソフトウェア イメージの表示および更新を行うには、デバイス名をクリックします。

フィールド	説明
Reachability	デバイス ステータスのバックグラウンドタスクの最後の実行情報に基づいて、到達可能性ステータスが更新されます。
[IP アドレス/DNS（IP Address/DNS）]	コントローラ管理インターフェイスのローカルネットワーク IP アドレス。IP アドレスの下のアイコンをクリックすると、コントローラの Web ユーザ インターフェイスが新しいブラウザ ウィンドウで表示されます。
Device Type	デバイス タイプは、シリーズでグループ化されています。次に例を示します。 • [WLC2100]：21xx シリーズ ワイヤレス LAN コントローラ • [2500]：25xx シリーズ ワイヤレス LAN コントローラ • [4400]：44xx シリーズ ワイヤレス LAN コントローラ • [5500]：55xx シリーズ ワイヤレス LAN コントローラ • [7500]：75xx シリーズ ワイヤレス LAN コントローラ • [WiSM]：WiSM（スロット番号、ポート番号） • [WiSM2]：WiSM2（スロット番号、ポート番号）
AP Discovery Status	AP ディスカバリが完了したかどうかを示します。
ソフトウェア バージョン（Software Version）	コントローラで現在実行しているコードのオペレーティング システム リリースのバージョンとメンテナンス番号。
[モビリティ グループ名（Mobility Group Name）]	モビリティ グループまたは WPS グループの名前。

ステップ 3 コントローラに関する特定の情報を表示するには、デバイス名をクリックします。

関連トピック

設定テンプレートの展開のためのコントローラ固有のコマンド （590 ページ）

設定テンプレートの展開のためのコントローラ固有のコマンド

[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）] を選択してから、左側の [デバイスグループ（Device Groups）] メニューで [デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）] を選択し、1 つ以上のデバイスのチェックボックスをオンにすると、ページ上部に次のボタンが表示されます。

- [Delete]：コントローラを削除できます。
- [Edit]：一般パラメータ、SNMP パラメータ、Telnet/SSH パラメータ、HTTP パラメータ、および IPSec パラメータを編集できます。

- [Sync]：
- [Groups & Sites]：場所グループおよびサイトとの間でコントローラを追加または削除できます。
- [再起動（Reboot）]：設定変更を保存した後にコントローラを再起動するように設定できます。選択できるリブート オプションは次のとおりです。
  - [Save Config to Flash]：データはコントローラの不揮発性 RAM（NVRAM）に保存され、電源の再投入時にも保持されます。コントローラをリブートした場合、設定が保存されていないと、適用した変更はすべて失われます。
  - Reboot APs（AP のリブート）
  - Swap AP Image
- [ダウンロード（Download）]：次のオプションを選択して、コントローラにソフトウェアをダウンロードできます。
  - [Download Software]：[TFTP]、[FTP]、[SFTP] のいずれかを選択して、選択したコントローラ、または設定グループの構築後に選択したグループのすべてのコントローラにソフトウェアをダウンロードします。
  - Download IDS Signatures
  - Download Customized Web Auth
  - Download Vendor Device Certificate
  - Download Vendor CA Certificate
  - Bulk Update Controllers
- Configure
  - Save Config to Flash
  - Discover Templates from Controller
  - [コントローラに適用されているテンプレート（Templates Applied to Controller）]
  - Audit Now
  - 資格情報の更新

関連トピック

Cisco Prime Infrastructure でのコントローラの表示 （589 ページ）
コントローラで使用されている設定テンプレートの確認と関連付けの削除 （592 ページ）
インポートした CSV ファイルを使用したコントローラ クレデンシャルの変更 （594 ページ）
再起動によるコントローラ変更の適用 （595 ページ）
コントローラへのソフトウェアのダウンロード （595 ページ）

コントローラで使用されている設定テンプレートの確認と関連付けの削除

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）] を選択します。

ステップ 2 該当するコントローラのチェックボックスをオンにします。

ステップ 3 [Configure] > [Audit Now] をクリックします。

ステップ 4 ポップアップ ダイアログボックスで [OK] をクリックすると、データベース内の設定オブジェクトからテンプレートの関連付けが削除され、関連付けられている設定グループからもこのコントローラのテンプレートの関連付けが削除されます。

テンプレートを関連付ける Prime Infrastructure 設定を指定できます。

検出されたテンプレートは、管理またはローカルまたはゲスト ユーザー パスワードを取得しません。

テンプレート検出には次のルールが適用されます。

- テンプレート検出では、Prime Infrastructure で見つからないテンプレートが検出されます。
- 既存のテンプレートは検出されません。
- テンプレート検出では、コントローラの動的インターフェイスの設定を取得しません。コントローラで動的インターフェイスの設定を適用するには、新しいテンプレートを作成する必要があります。

関連トピック

レポートでのコントローラ監査結果の表示 （593 ページ）
コントローラに適用されているテンプレートの表示 （607 ページ）
コントローラの既存のテンプレートを検出 （606 ページ）
再起動によるコントローラ変更の適用 （595 ページ）
コントローラへのソフトウェアのダウンロード （595 ページ）
IP アドレスを保持したままのコントローラ交換 （608 ページ）

[ネットワークデバイス（NetworkDevices）]テーブルからのコントローラ クレデンシャルの変更

SNMP と Telnet のクレデンシャルを更新するには、各コントローラで変更を行う必要があります。複数のコントローラの SNMP または Telnet のクレデンシャルの詳細は同時に更新することはできません。

コントローラの設定を変更するには、SNMP 書き込みアクセス パラメータが必要です。読み取り専用アクセス パラメータを使用して設定を表示できますが、変更することはできません。

SNMP/Telnet クレデンシャルをアップデートするには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、**[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのチェックボックスをオンにします。

ステップ 3 [Configure] > [Update Credentials] をクリックします。

ステップ 4 必須フィールドに入力して [OK] をクリックします。

関連トピック

インポートした CSV ファイルを使用したコントローラ クレデンシャルの変更 （594 ページ）

レポートでのコントローラ監査結果の表示

コントローラで監査を実行すると、監査レポートに次の情報が表示されます。

- デバイス名
- 監査の時刻
- 監査ステータス
- 適用テンプレートと設定グループ テンプレートの矛盾の情報には、次の内容が含まれます。
  - テンプレートの種類（テンプレート名）
  - テンプレート適用方法
  - 監査ステータス（不一致、同一など）
  - テンプレートの属性
  - Cisco Prime Infrastructure の値
  - コントローラの値
  - その他の Cisco Prime Infrastructure の矛盾には、次の内容が含まれます。
  - 設定の種類（名前）
  - 監査ステータス（不一致、同一など）
  - 属性（Attribute）
  - コントローラの値
  - バックグラウンド監査が有効な設定グループの合計施行数。バックグラウンド監査が有効な設定グループに関する監査で矛盾が検出され、施行が有効である場合、このセクションにコントローラの監査中に行われた施行のリストが表示されます。全体の施行数が 0 より大きい場合、この数値はリンクとして表示されます。このリンクをクリックすると、Cisco Prime Infrastructure から行われた施行のリストが表示されます。
- [Failed Enforcements for Configuration Groups with background audit enabled]：失敗した施行数が 0 より大きい場合、この数値はリンクとして表示されます。このリンクをクリックすると、デバイスによって返された失敗の詳細（失敗の理由など）のリストが表示されます。

- [コントローラへのCisco Prime Infrastructure値の復元（Restore Cisco Prime Infrastructure Values to Controller）] または [コントローラからの設定の更新（Refresh Configuration from Controller）]：監査の結果として設定の相違が見つかった場合は、[コントローラへのPrime Infrastructure値の復元（Restore Prime Infrastructure Values to Controller）] または [コントローラからの設定の更新（Refresh Configuration from Controller）] をクリックして、Cisco Prime Infrastructure 設定をコントローラと同期することができます。
  - 矛盾をデバイスにプッシュする場合は、[Restore Prime Infrastructure Values to Controller] を選択します。
  - [Refresh Config from Controller] を選択して、デバイスからこの設定を取得します。[Refresh Config from Controller] をクリックしても、テンプレートはリフレッシュされません。

関連トピック

コントローラで使用されている設定テンプレートの確認と関連付けの削除（592ページ）

インポートしたCSVファイルを使用したコントローラ クレデンシャルの変更

CSVファイルをインポートすることで、複数のコントローラのクレデンシャルをアップデートできます。

コントローラの情報を一括アップデートするには、次の手順を実行します。

ステップ 1 [Configuration] > [Network] > [Network Devices] を選択し、[Wireless Controllers] を選択します。

ステップ 2 該当するコントローラのチェックボックスをオンにします。

ステップ 3 [Download] > [Bulk Update Controllers] をクリックします。

ステップ 4 [Select CSV File] テキスト ボックスに CSV ファイル名を入力するか、または [Browse] をクリックして目的のファイルを特定します。

ステップ 5 [Update and Sync] をクリックします。

関連トピック

[ネットワークデバイス（Network Devices）]テーブルからのコントローラ クレデンシャルの変更（592 ページ）
再起動によるコントローラ変更の適用（595 ページ）
IP アドレスを保持したままのコントローラ交換（608 ページ）

再起動によるコントローラ変更の適用

リブートする前に、現在のコントローラの設定を保存する必要があります。コントローラをリブートするには、次の手順を実行します。

ステップ 1 **[設定（Configuration）]** > **[ネットワーク（Network）]** > **[ネットワーク デバイス（Network Devices）]** を選択し、[ワイヤレス コントローラ（Wireless Controller）] を選択して、[再起動（Reboot）] > [コントローラの再起動（Reboot Controllers）] をクリックします。

ステップ 2 必要な [Reboot Controller] オプションを選択します。

- [Save Config to Flash]：データはコントローラの不揮発性 RAM（NVRAM）に保存され、電源の再投入時にも保持されます。コントローラをリブートした場合、設定が保存されていないと、適用した変更はすべて失われます。
- [Reboot APs]：何らかのアップデートが実行された後、アクセス ポイントがリブートされるようにするには、このチェックボックスをオンにします。
- [Swap AP Image]：AP イメージをスワップした際に、コントローラおよび AP をリブートするかどうかを示します。[Yes] または [No] のいずれかになります。

ステップ 3 [OK] をクリックします。

関連トピック

[ネットワークデバイス（Network Devices）]テーブルからのコントローラ クレデンシャルの変更 （592 ページ）
IP アドレスを保持したままのコントローラ交換 （608 ページ）

コントローラへのソフトウェアのダウンロード

コントローラにソフトウェアをダウンロードするには、次の手順を実行します。

ステップ 1 **[設定（Configuration）]** > **[ネットワーク（Network）]** > **[ネットワーク デバイス（Network Devices）]** を選択し、[デバイス タイプ（Device Type）] > [ワイヤレス コントローラ（Wireless Controllers）] を選択します。

ステップ 2 該当するコントローラのチェックボックスをオンにします。

ステップ 3 [Download] をクリックし、次のいずれかのオプションを選択します。

- **Download Software TFTP**
- **Download Software FTP**
- **Download Software SFTP**

ステップ 4 必須フィールドに値を入力します。

ステップ 5 ダウンロードタイプを選択します。事前ダウンロードオプションは、選択したすべてのコントローラがリリース 7.0.x.x 以降を使用している場合のみ表示されます。

- [Now]：ソフトウェアのダウンロードをただちに開始します。このオプションを選択した場合は、ステップ 7 に進みます。
- [Scheduled]：スケジュール設定するダウンロードオプションを指定します。
  - [Schedule download to controller]：ソフトウェアをコントローラにダウンロードするようにスケジュール設定するには、このチェックボックスをオンにします。
  - [Pre-download software to APs]：ソフトウェアを AP に事前ダウンロードするようにスケジュール設定するには、このチェックボックスをオンにします。AP にイメージがダウンロードされ、コントローラのリブート時に、AP もリブートされます。AP ごとの [イメージの事前ダウンロード（Image Predownload）] ステータスを確認するには、**[管理（Administration）] > [ダッシュボード（Dashboards）] > [ジョブ ダッシュボード（Job Dashboard）] > [システム ジョブ（System Jobs）] > [ワイヤレス ポーラー（Wireless Poller）] > [AP イメージの事前ダウンロード ステータス（AP Image Pre-Download Status）]** でタスクを有効にし、[レポート起動パッド（Report Launch Pad）] から [AP イメージ事前ダウンロード（AP Image Predownload）] レポートを実行します。
  - [FlexConnect AP Upgrade]：ローカル ネットワークのモデルごとに 1 つのアクセス ポイントでイメージをダウンロードできるようにするには、このオプションを選択します。残りのアクセス ポイントは、ローカル ネットワークを介してプリイメージダウンロード機能を使用して、マスター アクセス ポイントからイメージをダウンロードします。これにより、WAN の遅延時間が短縮されます。

ステップ 6 [Schedule] オプションを選択します。

すべての AP がソフトウェアの事前ダウンロードを完了できるように、ダウンロードとリブートの間に十分な時間（少なくとも 30 分）をスケジュール設定します。スケジュール設定されたリブート時刻に、いずれかの AP で事前ダウンロードが進行中の場合、コントローラはリブートしません。すべての AP の事前ダウンロードが終了するまで待って、コントローラを手動でリブートする必要があります。

ステップ 7 ユーザ名、パスワード、およびポートを含めて、FTP クレデンシャルを入力します。

特殊文字の @、#、^、*、~、_、-、+、=、{、}、[、]、:、.、および / をパスワードに使用できます。$、'、\、%、&、(、)、;、"、<、>、,、?、および | のような特殊文字は FTP パスワードに使用できません。特殊文字「!」（感嘆符）は、パスワード ポリシーが無効の場合に使用できます。

ステップ 8 ファイルの格納場所として [Local machine] または [FTP Server] を選択します。[FTP Server] を選択すると、インストール中に指定した FTP ディレクトリにソフトウェア ファイルがアップロードされます。

ステップ 9 [Download] をクリックします。

転送がタイムアウトした場合は、[ファイルの格納場所（File is located on）] フィールドで [FTP サーバ（FTP Server）] オプションを選択すると、サーバ ファイル名が読み込まれて Cisco Prime Infrastructure によって再試行されます。

FTP/TFTP サーバへのコントローラ設定とログ ファイルのアップロード

指定した TFP または TFTP サーバに、コントローラ システム設定をファイルとしてアップロードできます。Prime Infrastructure では、ファイルのアップロードおよびダウンロードに、ファイル FTP および TFTP の両方がサポートされています。コントローラからファイルをアップロードするには、次の手順を実行します。

ステップ 1 **[設定（Configuration）]** > **[ネットワーク（Network）]** > **[ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）]** > **[ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 デバイス名をクリックして [Configuration] タブをクリックします。

ステップ 3 左側のサイドバーのメニューから、**[システム（System）]** > **[コマンド（Commands）]** の順に選択します。

ステップ 4 [FTP] または [TFTP] オプション ボタンを選択し、[コントローラからファイルをアップロード（Upload File from ）] を選択して [実行（Go）] をクリックします。

ステップ 5 必要なフィールドに入力します。

Prime Infrastructure は統合 TFTP および FTP サーバを使用します。これは、サードパーティ製の TFTP および FTP サーバを Prime Infrastructure と同じワークステーション上で実行できないことを意味します。Prime Infrastructure とサードパーティ製サーバが、同一の通信ポートを使用するためです。

ステップ 6 [OK] をクリックします。選択したファイルが、[File Name] テキスト ボックスに入力した名前で TFTP または FTP サーバにアップロードされます。

コントローラへの IDS シグネチャのダウンロード

Prime Infrastructure では、コントローラに侵入検知システム（IDS）シグニチャ ファイルをダウンロードできます。ローカル マシンから IDS シグニチャ ファイルをダウンロードするように指定すると、Prime Infrastructure は次の 2 段階動作を開始します。

1. 管理者ワークステーションから Prime Infrastructure の組み込み TFTP サーバにローカル ファイルがコピーされます。
2. コントローラがそのファイルを取得します。

IDS シグニチャ ファイルが、すでに Prime Infrastructure サーバの TFTP ディレクトリにある場合、ダウンロードした Web ページで自動的にそのファイル名が読み込まれます。

ステップ 1 **[設定（Configuration）]** > **[ネットワーク（Network）]** > **[ネットワーク デバイス（Network Devices）]** を選択し、**[デバイス タイプ（Device Type）]** > **[ワイヤレス コントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのチェックボックスをオンにします。

ステップ 3 **[ダウンロード（Download）] > [IDS シグニチャのダウンロード（Download IDS Signatures）]** をクリックします。

ステップ 4 必須フィールドに値を入力します。

ステップ 5 [Download] をクリックします。

転送がタイムアウトした場合は、[File is located on] フィールドで [FTP server] オプションを選択すると、サーバ ファイル名が読み込まれて Prime Infrastructure によって再試行されます。

関連トピック

Cisco Prime Infrastructure でのコントローラの表示 （589 ページ）
再起動によるコントローラ変更の適用 （595 ページ）
コントローラへのソフトウェアのダウンロード （595 ページ）
IP アドレスを保持したままのコントローラ交換 （608 ページ）

コントローラへの圧縮された Web 認証ログイン ページ情報のダウンロード

Web 認証ログイン ページに使用するページおよびイメージ ファイルを圧縮して、Web 認証バンドルと呼ばれるファイルをコントローラにダウンロードできます。

コントローラでは、サイズが 1 MB 以下の .tar または .zip ファイルを受け入れます。1MB の制限には、バンドル内の圧縮されていないファイルの合計サイズが含まれます。

カスタマイズ Web 認証バンドルをコントローラにダウンロードするには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）] を選択します。

ステップ 2 該当するコントローラのチェックボックスをオンにします。

ステップ 3 **[ダウンロード（Download）] > [カスタマイズされた WebAuth のダウンロード（Download Customized WebAuth）]** をクリックします。

ステップ 4 サンプルの login.tar バンドル ファイルをダウンロードするには、表示されたプレビュー イメージをクリックして login.html ファイルを編集し、.tar または .zip ファイルとして保存します。このファイルには、Web 認証の表示に必要なページおよびイメージ ファイルが含まれています。

ステップ 5 .tar または .zip ファイルをコントローラにダウンロードします。

ステップ 6 ファイルが置かれている場所を選択します。

ローカル マシンを選択した場合は、.zip または .tar のファイル タイプでアップロードできます。Prime Infrastructure は .zip ファイルを .tar ファイルに変換します。TFTP サーバのダウンロードを選択した場合は、.tar ファイル以外は指定できません。

ステップ 7 必須フィールドに入力して [Download] をクリックします。

転送がタイムアウトした場合は、[File is located on] フィールドで [FTP server] オプションを選択すると、サーバ ファイル名が読み込まれて Prime Infrastructure によって再試行されます。

Prime Infrastructure によってダウンロードが完了すると、新しいページが表示され、認証が可能になります。

関連トピック

Cisco Prime Infrastructure でのコントローラの表示 （589 ページ）
コントローラへのソフトウェアのダウンロード （595 ページ）
IP アドレスを保持したままのコントローラ交換 （608 ページ）

コントローラへのベンダーデバイス証明書のダウンロード

各無線デバイス（コントローラ、アクセスポイント、およびクライアント）には独自のデバイスの証明書があります。ご自身のベンダー固有のデバイス証明書を使用する場合は、その証明書をコントローラにダウンロードする必要があります。

ベンダー デバイス証明書をコントローラにダウンロードするには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ネットワーク デバイス（Network Devices）]** の順に選択します。	
ステップ 2	**[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** の順に選択します（[ワイヤレスコントローラ（Wireless Controller）] を展開し、特定のコントローラ シリーズを選択します）。	
ステップ 3	目的のコントローラの [デバイス名（Device Name）] をクリックします。	
ステップ 4	[設定（Configuration）] タブをクリックします。	
ステップ 5	**[システム（System）] > [コマンド（Commands）]** の順に選択します。	
ステップ 6	[アップロード/ダウンロードコマンド（Upload/Download Commands）] で、転送プロトコルを選択します。	

	コマンドまたはアクション	目的
ステップ 7	インストールする証明書を選択し、[実行（Go）] をクリックします。	
ステップ 8	必要な詳細情報を入力し、[OK] をクリックします。	

関連トピック

コントローラへのソフトウェアのダウンロード （595 ページ）
IP アドレスを保持したままのコントローラ交換 （608 ページ）
コントローラへの CA 証明書のダウンロード （600 ページ）

TFTP を介したコントローラへのベンダー デバイス証明書のダウンロード

ベンダーデバイス証明書を TFTP のみを介してコントローラにダウンロードするには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）]** を選択し、[デバイス タイプ（Device Type）] > [ワイヤレス コントローラ（Wireless Controller）] を選択します。

ステップ 2 該当するコントローラのチェックボックスをオンにします。

ステップ 3 [Download] > [Download Vendor Device Certificate] をクリックします。

ステップ 4 必須フィールドに入力して [Download] をクリックします。

コントローラへの CA 証明書のダウンロード

コントローラとアクセス ポイントには、デバイス証明書の署名と確認に使用される認証局（CA）証明書があります。コントローラには、シスコによりインストールされた CA 証明書が付属しています。この証明書は、ローカル EAP 認証時にワイヤレス クライアントを認証するために、（PAC を使用していない場合）EAP-TLS と EAP-FAST により使用される場合があります。ただし、ご自身のベンダー固有の CA 証明書を使用する場合は、その証明書をコントローラにダウンロードする必要があります。

ベンダー CA 証明書をコントローラにダウンロードするには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）] を選択します。

ステップ 2 該当するコントローラのチェックボックスをオンにします。

ステップ 3 **[ダウンロード（Download）] > [ベンダー デバイス証明書のダウンロード（Download Vendor Device Certificate）]** をクリックします。

ステップ 4 必須フィールドに入力して [ダウンロード（Download）] をクリックします。

関連トピック

再起動によるコントローラ変更の適用 （595 ページ）
コントローラへのソフトウェアのダウンロード （595 ページ）
IP アドレスを保持したままのコントローラ交換 （608 ページ）
Cisco Prime Infrastructure でのコントローラの表示 （589 ページ）

ネットワーク アシュアランスの設定

デバイス公開証明書のダウンロードおよびインストール

シスコ ワイヤレス サービス アシュアランスに使用されるデバイス公開証明書は、シスコの CA サーバによって署名された CA 署名付き証明書です。

（注） cmca2.cer 証明書は、Prime Infrastructure 3.4 でプレインストールとして提供されています。この証明書は、ダウンロードおよびインストールが不要な場合もあります。

ステップ 1 1.https://www.cisco.com/security/pki/ にアクセスし、シスコの CA とその公開証明書の一覧を確認します。

ステップ 2 FTP サーバ上でネットワーク アシュアランスを有効化する WLC に必要なすべての .cer ファイルをダウンロードします。

例：ftp.abc.com

ステップ 3 Prime Infrastructure コマンド シェルに管理者ユーザとしてログインします。

ステップ 4 FTP サーバからデフォルト リポジトリに証明書をコピーします。

例：次のコマンドを使用して、cmca2 証明書をコピーします。

```
CLI admin# copy ftp://ftp.abc.com/cmac2.cer disk:/defaultRepo
```

ステップ 5 すべての証明書について、Prime Infrastructure サーバに CA 証明書信頼をインストールします。

例：次のコマンドを使用して、cmca2.cer をインストールします。

```
CLI admin# ncs key importcacert cmca2 cmca2.cer repository defaultRepo
The NCS server is running. 変更は次回のサーバの再起動時に反映されます。
Importing certificate to trust store
```

ステップ 6 Prime Infrastructure サーバにすべての証明書をインストールしたら、証明書を有効にするため、サーバを再起動する必要があります。

（注） ネットワーク アシュアランス処理によってデバイス処理エラーが報告される場合は、ifm_sam.log ファイルを
デバイスの公開証明書を取得してください。

例：次に、 `ifm_sam.log` ファイルのサンプルを示します。

```
2017-10-30 21:34:01,890 [https-jsse-nio-443-exec-1] ERROR logging - IFM-SAM-ERROR: Sensor device X.50
 mentioned below is not properly signed:
**********START******************************

MIIEdDCCA1ygAwIBAgIKG3upVgAAAA32cTANBgkqhkiG9w0BAQsFADA2MQ4wDAYDVQQKEwVDaXNjbzEkMCIGA1UEAxMbQ2lzY28gT
Y3R1cmluZyBDQSBTSEEyMB4XDTE1MTAwNzIzMDg1OFoXDTI1MTAwNzIzMTg1OFowgZQxCzAJBgNVBAYTAlVTMRMwEQYDVQQIEwpDY
ybmlhMREwDwYDVQQHEwhTYW4gSm9zZTEWMBQGA1UEChMNQ2lzY28gU3lzdGVtczEjMCEGA1UEAxMaQUlSLUNUODUxMC1LOS1mNGNm
wYTI3MDAxIDAeBgkqhkiG9w0BCQEWEXN1cHBvcnRAY2lzY28uY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA3pBr
23KzNGSGB1bAV71Y+YmPt+oJR7fVpZI/Vv39ncFcRGCpP0RH6ics9l20j0O/9BLQOwkRJ19d91GoPvCGc9hfU9W9ctRikg3ZPIOa1
23KzNGSGB1bAV71Y+YmPt+oJR7fVpZI/Vv39ncFcRGCpP0RH6ics9l20j0O/9BLQOwkRJ19d91GoPvCGc9hfU9W9ctRikg3ZPIOa1
VUjWI/l12zfEAuP9dsXdy29h5I0x19QfTCCjqJUtgTcoDx4QL2WjerZopCmCBlGL5ICFm+SeXADCh9OpZn1lbp4lQIDAQABo4IBIz
AQDAgWgMB0GA1UdDgQWBBQsA0phzTpk5VNFflYOK2mU8OZnmjAfBgNVHSMEGDAWgBR613mVyrtIK7hVFP2jwA+8pw+WGTBABgNVHR
3MDWgM6Axhi9odHRwOi8vd3d3LmNpc2NvLmNvbS9zZWN1cml0eS9wa2kvY3JsL2NtY2EyLmNybDBNBggrBgEFBQcBAQRBMD8wPQYI
HMAKGMWh0dHA6Ly93d3cuY2lzY28uY29tL3NlY3VyaXR5L3BraS9jZXJ0cy9jbWNhMi5jZXIwPwYJKwYBBAGCNxQCBDIeMABJAFAA
BuAHQAZQByAG0AZQBkAGkAYQB0AGUATwBmAGYAbABpAG4AZTANBgkqhkiG9w0BAQsFAAOCAQEANOilUIBV7mk3H/rhLGCW7acwiPx
WOfSZdy0EukZ8gCoKScZyLHp7IEkDGueb4CMJnPi4oJOeDw2xrxS/AkSLWUw5aQ585Qi2J2JXlLAXQ9pgaatyZ0yjm+jkkISwB18k
by2ApXdI2HqpNateGZvB0NJ4ww6xnJMIUaSdGl+50CrKWLoCssH2DHp6Qo9a8oTZtM6cG/c5wsjDn0tSfFbt4+3JzUPLnPlAff1Sl
a8pODdVe3BFe44pyMdgGCnVZnqJcevZiWtHMCG5OjaggbBhC0RObGJBxKOAGRgNlUej8hg1hWw==

**********END******************************

Check the CA Server for device X.509 Certificate is in Prime: 'ncs key listcacerts'.
```

証明書の詳細を確認し、CA サーバを特定するには、ツールを使用して証明書を Base64 フォーマットから .ce
換する必要があります。上記の例では、使用されている CA サーバは `Cisco Manufacturing CA (cmca2)` です。

関連トピック

コントローラへの NA サーバ CA 証明書のダウンロード （604 ページ）
ネットワーク アシュアランスの自己署名付き証明書を生成 （602 ページ）

ネットワーク アシュアランスの自己署名付き証明書を生成

Cisco Prime Infrastructure では、管理対象 WLC のワイヤレス クライアント情報のコレクション
と関連するイベントをサポートしています。このデータ収集には、WLC から各プロセスに
HTTPS 要求をルーティングする Prime Infrastructure サーバで実行する Apache HTTPD が必要です。WLC と Prime Infrastructure 間の通信は HTTPS 経由で行われます。つまり、WLC との通信には、PI サーバの秘密キー、証明書ファイル、CA 証明書が必要です。

1. Prime Infrastructure 3.4 をインストールすると、WSA コレクタに対して秘密キーと X.509 自己署名付き証明書のセットが自動的に生成され、次の場所にコピーされます。
   - **秘密キーの場所**：`/opt/CSCOlumos/wsa/apache/cert/server.key`
   - **自己署名付き証明書ファイル（X.509 形式）の場所**：`/localdisk/tftp` または `/localdisk/ftp`
   - **CA 証明書ファイルの場所**：`/opt/CSCOlumos/conf/certs/server_rootcacert.pem`

上記の場所にある各ファイルをコピーすると、独自の秘密キー、証明書、CA 署名付き証明書を使用できます。

例：https://[prime_server_ip]:8080

2. 自己署名付き証明書は、共通名（CN）として Prime Infrastructure サーバの eth0 インターフェイスの IP アドレスを使用します。自動的に生成された証明書の使用を続ける場合は、eth0 インターフェイスの IP アドレスを Prime Infrastructure サーバで使用する WLC の NA サーバ URL を設定する必要があります（手順 4 を参照）。例：
https://[prime_server_ip]:8080

3. WLC との通信には自動的に生成された証明書で十分です。この使用を続ける場合は、以下の証明書を使用して WLC を設定する方法を参照してください。Prime サーバのホスト名または別の IP アドレスを使用して別の証明書セットを生成する場合は、次のコマンドを使用できます。

IP アドレスを使用した証明書の生成

- TFTP の使用：

```
/usr/bin/openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout
/opt/CSCOlumos/wsa/apache/cert/server.key -out
/localdisk/tftp/prime-wsa-apache-server.crt -subj
"/C=US/ST=CA/L=CA/O=CISCO/OU=PRIME/CN=${IP_ADDR}"
```

- FTP の使用：

```
/usr/bin/openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout
/opt/CSCOlumos/wsa/apache/cert/server.key -out
/localdisk/ftp/prime-wsa-apache-server.crt -subj
"/C=US/ST=CA/L=CA/O=CISCO/OU=PRIME/CN=${IP_ADDR}"
```

ここで、IP_ADDR は、キーおよび証明書を生成するための Prime Infrastructure サーバの IP アドレスです。

ホスト名を使用した証明書の生成

- TFTP の使用：

```
usr/bin/openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout
/opt/CSCOlumos/wsa/apache/cert/server.key -out
/localdisk/tftp/prime-wsa-apache-server.crt -subj
"/C=US/ST=CA/L=CA/O=CISCO/OU=PRIME/CN=${PI_FQDN}
```

- FTP の使用：

```
usr/bin/openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout
/opt/CSCOlumos/wsa/apache/cert/server.key -out
/localdisk/ftp/prime-wsa-apache-server.crt -subj
"/C=US/ST=CA/L=CA/O=CISCO/OU=PRIME/CN=${PI_FQDN}
```

ここで、PI_FQDN は Prime Infrastructure サーバの完全修飾ホスト名です。

（注） 証明書で指定された共通名（CN）が Prime Infrastructure サーバのホスト名の場合は、DNS が解決可能である必要があります。それ以外の場合は、共通名で Prime サーバの IP アドレスを指定する必要があります。

4. 証明書の生成後、`/localdisk/tftp/prime-wsa-apache-server.crt` または `/localdisk/ftp/prime-wsa-apache-server.crt` のファイルを Prime Infrastucture にワイヤレス クライアント情報を送信する各 WLC にアップロードする必要があります。

（注） TFTP/SFTP/FTP サーバを使用して証明書ファイルをプッシュする場合は、そのサーバで指定されたファイルをコピーする必要があります。

関連トピック

コントローラへの NA サーバ CA 証明書のダウンロード （604 ページ）

コントローラへの NA サーバ CA 証明書のダウンロード

WLC が Prime Infrastructure と通信するためには、認証のため、NA サーバ CA 証明書が必要です。

証明書をダウンロードする前に、証明書のセットを生成するか、独自の証明書を特定の場所にアップロードして Prime Infrastructure がそこから取得できるようにすることが必要になる場合があります。詳細については、関連するリンクを参照してください。

（注） HA セットアップでは、WLC に証明書を適用するときは、**[管理（Administration）] > [サーバ（Servers）] > [TFTP/FTP/SFTPサーバ（TFTP/FTP/SFTP Servers）]** で、セカンダリ サーバの IP アドレスを手動で追加する必要があります。証明書をアップロードするときも、ドロップダウン リストからセカンダリ サーバの IP アドレスを選択する必要があります。そうしないと、セカンダリ サーバでのフェールオーバー後に、デフォルトの IP アドレスが プライマリとしてリストされます。

TFTP ロケーションのローカル ディスクからコントローラに CA 証明書をダウンロードするには、次の手順に従います。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）] を選択します。

ステップ 2 該当するコントローラのチェックボックスをオンにします。

ステップ 3 **[ダウンロード（Download）] > [NAサーバCA証明書のダウンロード（Download NA Server CA Certificate）]** の順にクリックします。

ステップ 4 ファイルの場所を選択し、必須フィールドに入力して、[ダウンロード（Download）] をクリックします。

コントローラへの NA サーバ CA 証明書のダウンロード

TFTP ロケーション、FTP ロケーション、SFTP ロケーション、または USB ロケーションからコントローラに CA 証明書をダウンロードするには、次の手順に従います。

（注） HA セットアップでは、WLC に証明書を適用するときは、**[管理（Administration）] > [サーバ（Servers）] > [TFTP/FTP/SFTPサーバ（TFTP/FTP/SFTP Servers）]** で、セカンダリ サーバの IP アドレスを手動で追加する必要があります。証明書をアップロードするときも、ドロップダウン リストからセカンダリ サーバの IP アドレスを選択する必要があります。そうしないと、セカンダリ サーバでのフェールオーバー後に、デフォルトの IP アドレスが プライマリとしてリストされます。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）] を選択します。

ステップ 2 証明書をダウンロードするコントローラをクリックします。

ステップ 3 [設定（Configuration）] タブをクリックします。

ステップ 4 左サイドバーのメニューで、**[システム（System）] > [コマンド（Commands）]** の順にクリックします。

ステップ 5 ファイルの場所を選択し、ドロップダウン メニューから [NAサーバCA証明書のダウンロード（Download NA Server CA Certificate）] を選択します。

（注） このオプションは、AireOS 8.6、8.7、8.8 を実行している WLC の場合のみ使用可能です。

ステップ 6 [移動（Go）] をクリックします。

ステップ 7 必要な詳細情報を入力し、[OK] をクリックします。

関連トピック

ネットワーク アシュアランスの自己署名付き証明書を生成 （602 ページ）
ネットワーク アシュアランスの設定 （739 ページ）
再起動によるコントローラ変更の適用 （595 ページ）
コントローラへのソフトウェアのダウンロード （595 ページ）
IP アドレスを保持したままのコントローラ交換 （608 ページ）
Cisco Prime Infrastructure でのコントローラの表示 （589 ページ）

デバイス フラッシュへのコントローラ設定の保存

設定をフラッシュ メモリに保存するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのチェックボックスをオンにします。

ステップ 3 **[設定（Configure）] > [フラッシュへの設定の保存（Save Config to Flash）]** をクリックします。

関連トピック

データベースへのコントローラ設定の保存（同期） （606 ページ）
コントローラへのソフトウェアのダウンロード （595 ページ）
IP アドレスを保持したままのコントローラ交換 （608 ページ）
再起動によるコントローラ変更の適用 （595 ページ）

データベースへのコントローラ設定の保存（同期）

コントローラから設定を同期するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのチェックボックスをオンにします。

ステップ 3 [同期（Sync）] をクリックし、[はい（Yes）] をクリックして続行します

関連トピック

デバイス フラッシュへのコントローラ設定の保存 （605 ページ）
コントローラへのソフトウェアのダウンロード （595 ページ）
IP アドレスを保持したままのコントローラ交換 （608 ページ）
再起動によるコントローラ変更の適用 （595 ページ）

コントローラの既存のテンプレートを検出

現在のテンプレートを検出するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）] を選択します。

ステップ 2 該当するコントローラのチェックボックスをオンにします。

ステップ 3 **[設定（Configure）] > [コントローラからのテンプレートの検出（Discover Templates from Controller）]** をクリックします。

[テンプレートの検出（Discover Templates）] ページには、検出されたテンプレートの数、各テンプレートのタイプ、および各テンプレートの名前が表示されます。テンプレート検出ツールでは、テンプレートをサポートしており、Cisco WLC 上で検出可能なすべての機能が検出されます。

ステップ 4 [Enabling this option will create association between discovered templates and the device listed above] チェックボックスをオンにすると、検出されたテンプレートがデバイスの設定に関連付けられ、当該のコントローラに適用されていることが表示されます。

テンプレートの検出を実行した場合、実際に検出が実行される前に、コントローラから設定が更新されます。

ステップ 5 検出を続行するには、警告ダイアログボックスで [OK] をクリックします。

TACACS+ サーバテンプレートの場合、サーバ IP アドレスおよびポート番号が同じで、サーバ タイプが異なるコントローラの設定は、単一のテンプレートに集約されます。このとき、対応するサーバ タイプが検出されたテンプレートに設定されます。TACACS+ サーバ テンプレートの場合、検出されたテンプレートの管理ステータスには、最初に見つかったサーバ IP アドレスおよびポート番号が同じコントローラの設定の管理ステータスが反映されます。

コントローラに適用されているテンプレートの表示

特定のコントローラに現在適用されているすべてのテンプレートを表示できます。Prime Infrastructure は、パーティションに適用されているテンプレートのみを表示します。

適用されているテンプレートを表示するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのチェックボックスをオンにします。

ステップ 3 [Configure] > [Templates Applied to a Controller] をクリックします。

このページに、適用されている各テンプレート名、テンプレート タイプ、テンプレートの最終保存日、およびテンプレートの最終適用日が表示されます。

ステップ 4 テンプレート名のリンクをクリックして、テンプレートの詳細を表示します。詳細については、「コントローラで使用されている設定テンプレートの確認と関連付けの削除」を参照してください。

関連トピック

コントローラで使用されている設定テンプレートの確認と関連付けの削除 （592 ページ）
IP アドレスを保持したままのコントローラ交換 （608 ページ）

IP アドレスを保持したままのコントローラ交換

IP アドレスを変更せずに古いコントローラ モデルを新しいモデルに置き換える場合は、次の手順を実行します。

1. Cisco Prime Infrastructure から古いコントローラを削除して、デバイスが削除されたことを示す確認メッセージを待ちます。
2. 同じ IP アドレスの設定でコントローラを新しいモデルに置き換えます。
3. IP アドレスを Cisco Prime Infrastructure に再度追加します。

関連トピック

デバイス パラメータの編集 （55 ページ）

コントローラ プロパティの変更

デバイス名、場所、SNMP パラメータ、Telnet/SSH パラメータなどのコントローラ プロパティを変更するには、次の手順を実行します。

ステップ 1 [Configuration] > [Network] > [Network Devices] を選択し、[Device Type] > [Wireless Controller] を選択します。

ステップ 2 ワイヤレス コントローラを選択して [Edit] をクリックします。

ステップ 3 必要に応じてフィールドを変更し、次のいずれかのボタンをクリックします。

- **更新**
- **Update & Sync**
- **Verify Credentials**
- Cancel（以前またはデフォルトの設定に戻す場合）

[ネットワークデバイス（Network Devices）] テーブルからコントローラの一般システム プロパティを変更する

現在のコントローラの一般システム パラメータを表示するには、次の手順を実行します。

ステップ 1 [Configuration] > [Network] > [Network Devices] を選択し、[Device Type] > [Wireless Controller] を選択します。

ステップ 2 デバイス名をクリックして [Configuration] タブをクリックします。

ステップ 3 左側のサイドバーのメニューから、[System] > [General - System] の順に選択します。一般システム パラメータが表示されます。『*Cisco Prime Infrastructure Reference Guide*』を参照してください。

ステップ 4 必要な変更を行い、[保存（Save）] をクリックします。

コントローラで障害が発生した場合の AP への優先順位の割り当て

コントローラに障害が発生した場合、アクセスポイントに設定されたバックアップ コントローラがすぐに多くの検出と接続要求を受信します。コントローラが過負荷になった場合、一部のアクセス ポイントが拒否される場合があります。

フェールオーバー優先順位をアクセスポイントに割り当てることによって、拒否されるアクセス ポイントを制御します。バックアップ コントローラが過負荷になった場合、優先度が高く設定されているアクセス ポイントの接続リクエストの方が、優先度の低いアクセス ポイントよりも優先されます。

アクセス ポイントのフェールオーバー優先度設定を設定するには、まず AP Failover Priority 機能を有効にする必要があります。

AP Failover Priority 機能を有効にする手順は、次のとおりです。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）] を選択します。

ステップ 2 デバイス名をクリックして [Configuration] タブをクリックします。

ステップ 3 左側のサイドバーのメニューから、[General - System] を選択します。

ステップ 4 [AP Failover Priority] ドロップダウン リストから、[Enabled] を選択します。

ステップ 5 アクセス ポイントのフェールオーバー プライオリティを設定するには、次の手順を実行します。

a) [Configuration] > [Network] > [Network Devices] を選択し、AP 名を選択します。

b) [AP Failover Priority] ドロップダウン リストから、適切な優先度（[Low]、[Medium]、[High]、[Critical]）を選択します。デフォルトの優先度は [Low] です。

コントローラでの 802.3 ブリッジングの設定

コントローラは、一般的にレジやレジサーバで使用されるような 802.3 フレームおよびそれらを使用するアプリケーションをサポートしています。ただし、これらのアプリケーションをコントローラとともに使用するには、802.3 のフレームがコントローラ上でブリッジされている必要があります。

未加工の 802.3 フレームのサポートにより、コントローラを、IP 上で実行していないアプリケーション用の IP 以外のフレームにブリッジできるようになります。この未加工の 802.3 フレームの形式だけが、現在サポートされています。

Prime Infrastructure を使用して 802.3 ブリッジを設定するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）] を選択します。

ステップ 2 デバイス名をクリックして [Configuration] タブをクリックします。

ステップ 3 [System] > [General - System] の順に選択して、[General] ページにアクセスします。

ステップ 4 802.3 ブリッジをコントローラ上で有効にする場合は、[802.3 Bridging] ドロップダウン リストから [Enable] を選択し、無効にする場合は [Disable] を選択します。デフォルト値は [Disable] です。

ステップ 5 [Save] をクリックして変更を確定します。

コントローラでの 802.3 フロー制御の設定

フロー制御は、モデムなどの送信エンティティにより、データを持つ受信エンティティが過負荷にならないようにする手法です。受信側デバイスのバッファに空きがない場合、メッセージが送信側デバイスに送信され、バッファ内のデータが処理されるまで伝送は一時停止されます。

デフォルトでは、フロー制御は無効に設定されています。ポーズフレームを受信しても送信できないように Cisco スイッチを設定できるだけです。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）] を選択します。

ステップ 2 デバイス名をクリックして [Configuration] タブをクリックします。

ステップ 3 [System] > [General - System] の順に選択して、[General] ページにアクセスします。

ステップ 4 [802.3x Flow Control] フィールドで [Enable] をクリックします。

[ネットワークデバイス（NetworkDevices）]テーブルからのLightweight AP Protocol 転送モードの設定

Lightweight Access Point Protocol 転送モードは、コントローラとアクセス ポイント間の通信レイヤを示します。Cisco IOS ベースの Lightweight アクセス ポイントは、レイヤ 2 Lightweight アクセス ポイント モードはサポートしていません。このようなアクセス ポイントは、レイヤ 3 でしか実行できません。

Prime Infrastructure ユーザ インターフェイスを使用して Cisco Unified Wireless Network ソリューションをレイヤ 3 からレイヤ 2 Lightweight アクセス ポイント転送モードに変換するには、次の手順を実行します。この手順を実行すると、コントローラがリブートしてアクセスポイントがコントローラと再アソシエートするまで、アクセス ポイントはオフラインになります。

ステップ 1 コントローラとアクセス ポイントはすべて同じサブネット上に配置するようにします。

変換を実行する前に、コントローラおよびアソシエートしているアクセス ポイントをレイヤ 2 モードで動作するように設定する必要があります。

ステップ 2 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、**[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 3 デバイス名をクリックし、[設定（Configuration）] タブをクリックしてから、**[システム（System）] > [一般 - システム（General - System）]** を選択して [一般（General）] ページにアクセスします。

a) Lightweight アクセス ポイント転送モードを [レイヤ 2（Layer2）] に変更し、[保存（Save）] をクリックします。

b) Prime Infrastructure に次のメッセージが表示された場合は、[OK] をクリックします。

例：

```
Please reboot the system for the CAPWAP Mode change to take effect.
```

ステップ 4 コントローラを選択し、**[再起動（Reboot）] > [コントローラの再起動（Reboot Controllers）]** をクリックします。

ステップ 5 [フラッシュへの設定の保存（Save Config to Flash）] オプションを選択します。

ステップ 6 コントローラがリブートしたら、次の手順に従って CAPWAP 転送モードがレイヤ 2 になっていることを確認します。

a) **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、**[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

b) 該当するコントローラのデバイス名をクリックします。

c) **[システム（System）] > [一般 - システム（General - System）]** ページで、現在の CAPWAP 転送モードが [レイヤ 2（Layer2）] であることを確認します。

これで、レイヤ 3 からレイヤ 2 への CAPWAP 転送モードの変換が完了しました。オペレーティング システムのソフトウェアによって、同じサブネット上のコントローラとアクセス ポイントとの間におけるすべての通信が制御されます。

アグレッシブ ロード バランシングとは

ルーティングでは、ロード バランシングは、宛先アドレスからの距離が同じすべてのネットワーク ポートでトラフィックを分配するルータの機能を示します。優れたロードバランシング アルゴリズムでは、回線速度と信頼性の両方の情報を使用します。ロードバランシングを行うと、ネットワーク セグメントの使用が増加するため、効率的なネットワーク帯域幅が増加します。

アグレッシブ ロード バランシングは、モバイル クライアントとアソシエートされたアクセス ポイントの間で負荷をアクティブに分散させます。

リンク アグリゲーションとは

リンク集約によって、物理ポートをすべてグループ化してリンク集約グループ（LAG）を作成し、コントローラ上のポートを構成するために必要な IP アドレスの数を削減できます。4402 モデルでは、LAG を形成するために 2 つのポートが組み合わされます。4404 モデルでは、4 つのポートすべてが LAG を形成するため組み合わされます。

コントローラ上では、複数の LAG を作成できません。

LAG がコントローラ上で有効な場合、次の設定が変更されます。

- インターフェイス データベース内での設定の矛盾を避けるため、作成した動的インターフェイスが削除されます。
- インターフェイスは「Dynamic AP Manager」フラグを設定した状態では作成できません。

LAG の作成には、次のようなメリットがあります。

- リンクの 1 つがダウンした場合に、常にトラフィックが LAG 内の他のリンクに移動します。物理ポートの 1 つが動作している限り、システムは機能し続けます。
- 各インターフェイスに対して個別にバックアップ ポートを設定する必要がありません。
- アプリケーションは論理ポートを 1 つしか認識しないため、複数の AP-manager インターフェイスは必要ありません。

LAG 設定に変更を加えると、変更を有効にするためにコントローラをリブートする必要があります。

ワイヤレス管理の前提条件

IPsec 動作により、ワイヤレスによる管理は WPA、静的 WEP、または VPN パススルー WLAN でログインしているオペレータのみが実行できます。ワイヤレス管理は、IPsec WLAN を経由してログインしようとしているクライアントは実行できません。

モビリティ アンカー キープアライブ間隔とは

クライアントが別のアクセス ポイントへの接続を試みるまでの遅延時間を指定できます。この機能を使用することで、エラーがすばやく特定され、クライアントが問題発生のコントローラから移動し、別のコントローラに接続されるため、コントローラのエラー後にクライアントが別のアクセス ポイントに接続するためにかかる時間が短縮されます。

関連トピック

コントローラへのソフトウェアのダウンロード （595 ページ）
コントローラの工場出荷時設定の復元
コントローラでの日時の設定

コントローラの設定ファイルおよびログファイルをTFTPサーバにアップロードする

コントローラからローカル TFTP（Trivial File Transfer Protocol）サーバにファイルをアップロードできます。**[管理（Administration）]** > **[システム設定（System Settings）]** > **[サーバ設定（Server Settings）]** ページで、TFTP を有効にして [デフォルト サーバ（Default Server）] オプションを使用する必要があります。

Prime Infrastructure では統合 TFTP サーバを使用しています。これは、サードパーティ製の TFTP サーバが Prime Infrastructure と同じワークステーション上では実行できないことを意味します。Prime Infrastructure とサードパーティ製の TFTP サーバが、同一の通信ポートを使用するためです。

ステップ 1 **[設定（Configuration）]** > **[ネットワーク（Network）]** > **[ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）]** > **[ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 デバイス名をクリックして [Configuration] タブをクリックします。

ステップ 3 左側のサイドバーのメニューから、**[システム（System）]** > **[コマンド（Commands）]** の順に選択します。

ステップ 4 [アップロード/ダウンロード コマンド（Upload/Download Commands）] ドロップダウン リストから、[コントローラからファイルをアップロード（Upload File from Controller）] を選択して [実行（Go）] をクリックします。

デフォルトでは、コンフィギュレーション ファイルの暗号化は無効になっています。コンフィギュレーション ファイルは暗号化なしでアップロードされるため、安全ではありません。

ステップ 5 ファイルをアップロードする前に暗号化を有効にするには、[Upload File from Controller] ページの下部にあるリンクをクリックします。

ステップ 6 必須フィールドに入力して [OK] をクリックします。選択したファイルが指定した名前の TFTP サーバにアップロードされます。

関連トピック

コントローラでの日時の設定
コントローラへのソフトウェアのダウンロード （595 ページ）
コントローラの工場出荷時設定の復元

コントローラへのソフトウェアのダウンロード

ローカル TFTP（Trivial File Transfer Protocol）サーバからコントローラにコンフィギュレーション ファイルをダウンロードできます。

Prime Infrastructure は統合 TFTP サーバを使用します。これは、サードパーティ製の TFTP サーバは Prime Infrastructure と同じワークステーション上では実行できないことを意味します。Cisco Prime Infrastructure とサードパーティ製 TFTP サーバが、同一の通信ポートを使用するためです。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）] を選択します。

ステップ 2 デバイス名をクリックして [Configuration] タブをクリックします。

ステップ 3 左側のサイドバーのメニューから、[System] > [Commands] の順に選択します。

ステップ 4 [Upload/Download Commands] ドロップダウン リストから、[Download Config] を選択して [Go] をクリックします。

ステップ 5 必須フィールドに入力して [OK] をクリックします。

関連トピック

コントローラでの日時の設定

コントローラの設定ファイルおよびログ ファイルを TFTP サーバにアップロードする （613 ページ）

コントローラの工場出荷時設定の復元

単一コントローラでのインターフェイスの設定

インターフェイスを追加するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）]** を選択し、[デバイス タイプ（Device Type）] > [ワイヤレス コントローラ（Wireless Controller）] を選択します。

ステップ 2 デバイス名をクリックして [Configuration] タブをクリックします。

ステップ 3 左側のサイドバーのメニューから、[System] > [Interfaces] の順に選択します。

ステップ 4 [コマンドの選択（Select a command）] ドロップダウン リストから、**[インターフェイスの追加（Add Interface）] > [実行（Go）]** を選択します。

ステップ 5 必要なフィールドに入力したら、[保存（Save）] をクリックします。

関連トピック

コントローラでのインターフェイスの表示 （615 ページ）

コントローラからの動的インターフェイスの削除 （615 ページ）

NAC アプライアンスを使用したコントローラへのユーザ アクセスの制御 （617 ページ）

有線コントローラへのゲスト アカウント アクセスの設定 （621 ページ）

コントローラでのインターフェイスの表示

既存のインターフェイスを表示するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）]** を選択し、左側の [デバイス グループ（Device Groups）] メニューから **[デバイス タイプ（Device Type）] > [ワイヤレス コントローラ（Wireless Controller）]** を選択します。

ステップ 2 デバイス名をクリックして [設定（Configuration）] タブをクリックします。

ステップ 3 左側のサイドバーのメニューから、**[システム（System）] > [インターフェイス（Interfaces）]** の順に選択します。次のパラメータが表示されます。

- [Check box]：削除する動的インターフェイスを選択するチェックボックス。[Select a command] ドロップダウン リストから [Delete Dynamic Interfaces] を選択します。
- [Interface Name]：インターフェイスのユーザ定義名（例：Management、Service-Port、Virtual）。
- [VLAN Id]：0（タグなし）～ 4096 の VLAN 識別子、または [N/A]。
- [Quarantine]：インターフェイスに検疫 VLAN ID が設定されている場合は、このチェックボックスをオンにします。
- [IP Address]：インターフェイスの IP アドレス。
- [Interface Type]：[Static]（管理、AP-Manager、サービス ポート、および仮想インターフェイス）または [Dynamic]（オペレータ定義インターフェイス）。
- [AP Management Status]：AP 管理インターフェイスのステータス。パラメータには [Enabled]、[Disabled]、および [N/A] があります。管理ポートだけがリダンダンシー マネジメント インターフェイスのポートとして設定できます。

関連トピック

コントローラ インターフェイス グループの表示と管理 （616 ページ）

コントローラからの動的インターフェイスの削除

インターフェイス グループに割り当てられている動的インターフェイスは削除できません。動的インターフェイスを削除するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）]** を選択し、左側の [デバイス グループ（Devices Groups）] メニューから **[デバイス タイプ（Device Type）] > [ワイヤレス コントローラ（Wireless Controller）]** を選択します。

ステップ 2 デバイス名をクリックして [Configuration] タブをクリックします。

ステップ 3 左側のサイドバーのメニューから、**[システム（System）] > [インターフェイス（Interfaces）]** の順に選択します。

ステップ 4 削除する動的インターフェイスのチェックボックスをオンにして、[コマンドの選択（Select a command）] ドロップダウン リストから [動的インターフェイスの削除（Delete Dynamic Interfaces）] を選択します。

ステップ 5 [OK] をクリックして削除を実行します。

関連トピック

コントローラ インターフェイス グループの表示と管理 （616 ページ）
コントローラでのインターフェイスの表示 （615 ページ）

コントローラ システム インターフェイス グループを使用したコントローラグループへのインターフェイス変更の適用

インターフェイス グループは、インターフェイスの論理的なグループです。インターフェイス グループを使用すると、同じインターフェイス グループを複数の WLAN で設定するユーザ設定や、AP グループごとに WLAN インターフェイスを上書きすることが容易になります。インターフェイス グループには検疫済みまたは検疫済みでないインターフェイスを排他的に含めることができます。1 つのインターフェイスを複数のインターフェイス グループに含めることができます。

コントローラ システム インターフェイス グループを設定する場合は、次の推奨事項に従ってください。

- インターフェイス グループ名とインターフェイス名が異なることを確認します。
- ゲスト LAN インターフェイスは、インターフェイス グループに含めることはできません。

インターフェイス グループ機能は、シスコ ワイヤレス コントローラ ソフトウェア リリース 7.0.116.0 以降でサポートされます。

関連トピック

コントローラ インターフェイス グループの表示と管理 （616 ページ）
NAC アプライアンスを使用したコントローラへのユーザ アクセスの制御 （617 ページ）

コントローラ インターフェイス グループの表示と管理

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 デバイス名をクリックして [Controller] タブをクリックします。

ステップ 3 左側のサイドバーのメニューから、**[システム（System）]> [インターフェイス グループ（Interface Groups）]** を選択します。

次のパラメータが表示されます。

- [Name]：インターフェイス グループのユーザ定義名（例：group1、group2）。
- [Description]：（任意）インターフェイス グループの説明。
- [Interfaces]：グループに属しているインターフェイスの数。

ステップ 4 既存のインターフェイス グループを表示するには、[インターフェイス グループ名（Interface Group Name）] リンクをクリックします。

[インターフェイス グループの詳細（Interface Groups Details）] ページが表示され、インターフェイス グループの詳細と、特定のインターフェイス グループの一部を構成するインターフェイスの詳細が示されます。

ステップ 5 インターフェイス グループを追加するには、次の手順を実行します。

a) [Select a Command] ドロップダウン リストから、[Add Interface Group] を選択し、[Go] をクリックします。
b) 必須フィールドに入力し、[Add] をクリックします。
c) [Interface] ダイアログボックスが表示されます。
d) グループに追加するインターフェイスを選択して、[Select] をクリックします。

ステップ 6 インターフェイス グループを削除するには、次のようにします。

a) [コマンドの選択（Select a command）] ドロップダウン リストから、[インターフェイス グループの削除（Delete Interface Group）] を選択し、[実行（Go）] をクリックします。

（注） WLAN、AP グループ、WLAN の外部コントローラ マッピング、WLAN テンプレート、および AP グループ テンプレートに割り当てられているインターフェイス グループを削除できます。

b) [OK] をクリックして削除を実行します。

ステップ 7 [Interface Group] ページからインターフェイスを削除するには、インターフェイスを選択して [Remove] をクリックします。

ステップ 8 [Save] をクリックして、変更を確定します。

関連トピック

コントローラ システム インターフェイス グループを使用したコントローラ グループへのインターフェイス変更の適用 （616 ページ）
NAC アプライアンスを使用したコントローラへのユーザ アクセスの制御 （617 ページ）

NAC アプライアンスを使用したコントローラへのユーザ アクセスの制御

Cisco Network Admission Control（NAC）アプライアンス（Cisco Clean Access（CCA）とも呼ばれます）は、ネットワーク管理者がユーザにネットワークへの接続を許可する前に、有線、無線、およびリモート ユーザとそのマシンを認証、承認、評価、修復できる、ネットワーク アドミッション コントロール（NAC）製品です。Cisco NAC アプライアンスは、マシンがセキュ

リティポリシーに準拠しているかどうかを判別し、脆弱性を修復してから、ネットワークへのアクセスを許可します。NAC アプライアンスは、インバンド モードとアウトオブバンド モードの2つのモードで利用できます。顧客は、必要に応じて特定の種類のアクセスを対象にし、2 つのモードを展開できます（例：無線ユーザをサポートする場合はインバンド、有線ユーザをサポートする場合はアウトオブバンド）。

関連トピック

SNMP NAC の使用時の前提条件 （618 ページ）
コントローラでの SNMP NAC の設定 （619 ページ）

SNMP NAC の使用時の前提条件

SNMP NAC アウトオブバンド統合を使用する場合は、次のガイドラインに従ってください。

- NAC アプライアンスは最大 3,500 のユーザをサポートし、コントローラは最大 5,000 のユーザをサポートします。したがって、複数の NAC アプライアンスの導入を必要とする場合があります。
- NACアプライアンスでは静的なVLANマッピングがサポートされているため、コントローラ上で設定されているインターフェイスごとに一意の検疫 VLAN を設定する必要があります。たとえば、コントローラ 1 で 110 という検疫 VLAN を設定し、コントローラ 2 で 120 という検疫 VLAN を設定します。ただし、2 つの WLAN またはゲスト LAN が、コントローラのダイナミック インタフェースとして同一の VLAN を使用している場合、ネットワーク内に導入された NAC アプライアンスが 1 つならば、同じ検疫 VLAN を使用する必要があります。NAC アプライアンスは、一意の検疫 - アクセス VLAN マッピングをサポートします。
- セッションの失効に基づくポスチャ再評価の場合、NAC アプライアンスと WLAN の両方にセッション タイムアウトを設定し、WLAN でのセッションの失効が NAC アプライアンスでの失効より大きいことを確認します。
- オープン WLAN でセッション タイムアウトが設定されると、Quarantine 状態にあるクライアントのタイムアウトは NAC アプライアンスのタイマーによって判定されます。Web 認証を使用する WLAN においてセッションがタイムアウトすると、クライアントはコントローラから認証解除されるので、ポスチャ検証を再度実行する必要があります。
- NACアウトオブバンド統合がサポートされるのは、WLANがFlexConnectの中央スイッチングを行うように設定されている場合だけです。FlexConnect のローカル スイッチングを行うように設定されている WLAN での使用はサポートされていません。
- アクセス ポイント グループ VLAN 上で NAC を有効にする場合は、WLAN で NAC をまず有効にする必要があります。アクセス ポイント グループ VLAN では、NAC を有効または無効にすることができます。WLAN で NAC を無効にすることに決めた場合は、アクセス ポイント グループ VLAN でも NAC を必ず無効にします。
- NAC アウトオブバンド統合は、WLAN AAA Override 機能では使用できません。
- レイヤ 2 およびレイヤ 3 認証はすべて、検疫 VLAN で実行されます。外部 Web 認証を使用するには、外部 Web サーバからの HTTP トラフィックおよび外部 Web サーバへの HTTP トラフィックを許可するとともに、検疫 VLAN でのリダイレクト URL を許可するように NAC アプライアンスを設定する必要があります。

詳細については、「Cisco NAC Appliance Configuration」を参照してください。

RADIUS NAC の使用時の前提条件

RADIUS NAC を使用する場合には、次のガイドラインに従ってください。

- RADIUS NAC は、802.1x/WPA/WPA2 レイヤ 2 セキュリティを備えた WLAN のみが使用できます。
- RADIUS NAC は、FlexConnect ローカル スイッチングが有効の場合は有効にできません。
- RADIUS NAC を設定する場合は、AAA オーバーライドを有効にしてください。

関連トピック

NAC アプライアンスを使用したコントローラへのユーザ アクセスの制御 （617 ページ）

コントローラでの SNMP NAC の設定

SNMP NAC アウトオブバンド統合を設定するには、次のワークフローを実行します。

1. 動的インターフェイスに対して隔離 VLAN を設定します。NAC アプライアンスでは静的な VLAN マッピングがサポートされているため、コントローラ上で設定されているインターフェイスごとに一意の隔離 VLAN を設定する必要があります。
2. WLAN またはゲスト LAN に NAC アウトオブバンド サポートを設定します。アクセス ポイント グループ VLAN で NAC サポートを有効にする場合は、先に WLAN またはゲスト LAN で NAC を有効にする必要があります。
3. 特定の AP グループに対して NAC アウトオブバンド サポートを設定します。特定のアクセス ポイント グループに NAC アウトオブバンド サポートを設定するには。

関連トピック

検疫 VLAN の設定（SNMP NAC） （619 ページ）
WLAN またはゲスト LAN での NAC の有効化（SNMP NAC） （620 ページ）
AP グループの NAC アウトオブバンド サポートの設定（SNMP NAC）

検疫 VLAN の設定（SNMP NAC）

動的インターフェイスに対して検疫 VLAN を設定するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）]** > **[ネットワーク（Network）]** > **[ネットワーク デバイス（Network Devices）]** を選択し、左側の [デバイス グループ（Devices Groups）] メニューから [デバイス タイプ（Device Type）] > [ワイヤレス コントローラ（Wireless Controller）] を選択します。

ステップ 2 [IP Address] 列でアウトオブバンド統合の設定を行うコントローラをクリックして選択します。

ステップ 3 左側のサイドバーのメニューから、**[システム（System）]** > **[インターフェイス（Interfaces）]** を選択します。

ステップ 4 [インターフェイス名（Interface Name）] をクリックします。

ステップ 5 [コマンドの選択（Select a command）] ドロップダウン リストから [インターフェイスの追加（Add Interface）] を選択し、[実行（Go）] をクリックします。

ステップ 6 [インターフェイス名（Interface Name）] テキスト ボックスに、「quarantine」など、このインターフェイスの名前を入力します。

ステップ 7 [VLAN ID] テキスト ボックスに、アクセス VLAN ID としてゼロ以外の値（「10」など）を入力します。

ステップ 8 インターフェイスに検疫 VLAN ID が設定されている場合は、[Quarantine] チェックボックスをオンにします。

ステップ 9 このインターフェイスの残りのフィールド（IP アドレス、ネットマスク、デフォルト ゲートウェイなど）を設定します。

（注） ワイヤレス コントローラを Prime Infrastructure に追加する際の問題を避けるため、動的インターフェイスを Prime Infrastructure と同じサブネットに配置しないでください。

ステップ 10 プライマリおよびセカンダリ DHCP サーバの IP アドレスを入力します。

ステップ 11 [Save] をクリックします。

関連トピック

WLAN またはゲスト LAN での NAC の有効化（SNMP NAC） （620 ページ）
AP グループの NAC アウトオブバンド サポートの設定（SNMP NAC）

WLAN またはゲスト LAN での NAC の有効化（SNMP NAC）

WLAN またはゲスト LAN で NAC アウトオブバンド サポートを設定するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 デバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、[WLANs] > [WLAN] の順に選択します。

ステップ 4 [コマンドの選択（Select a command）] ドロップダウン リストから [WLAN の追加（Add a WLAN）] を選択し、[実行（Go）] をクリックします。

ステップ 5 このコントローラに適用する作成済みのテンプレートがある場合には、ドロップダウン リストからゲスト LAN テンプレート名を選択します。そうでない場合には、[click here] リンクをクリックして新しいテンプレートを作成します。

ステップ 6 [Advanced] タブをクリックします。

ステップ 7 この WLAN またはゲスト LAN に SNMP NAC サポートを設定するには、[] ドロップダウン リストから [SNMP NAC] を選択します。SNMP NAC サポートを無効にするには、[NAC ステージ（NAC Stage）] ドロップダウン リストから [なし（None）]（デフォルト値）を選択します。

ステップ 8 [適用（Apply）] をクリックして、変更を確定します。

関連トピック

AP グループの NAC アウトオブバンド サポートの設定（SNMP NAC）
有線コントローラへのゲスト アカウント アクセスの設定 （621 ページ）

ネットワーク クライアントまたはユーザの NAC 状態の表示

クライアントの現在の状態（[検疫（Quarantine）] または [アクセス（Access）]）を表示するには、次の手順を実行します。

ステップ 1 **[モニタ（Monitor）] > [モニタリング ツール（Monitoring Tools）] > [クライアントおよびユーザ（Clients and Users）]** を選択して、[クライアント（Clients）] を開きます。クライアントの検索を実行します。

ステップ 2 目的のクライアントの MAC アドレスをクリックして、[Clients > Detail] ページを開きます。[Security Information] セクションの下に NAC ステートが [Access]、[Invalid]、または [Quarantine] と表示されます。

関連トピック

コントローラでの SNMP NAC の設定 （619 ページ）

有線コントローラへのゲストアカウントアクセスの設定

有線ゲストアクセスでは、ゲストユーザがゲストアクセス用に指定および設定された有線イーサネット接続からゲスト アクセス ネットワークへ接続できます。有線ゲスト アクセス ポートは、ゲストのオフィスまたは会議室の特定のポートで使用できます。

無線ゲスト ユーザ アカウントのように、有線ゲスト アクセス ポートが Lobby Ambassador 機能を使用するネットワークに追加されます。有線ゲストアクセスは、スタンドアロン設定、またはアンカーおよび外部のコントローラを配置したデュアル コントローラ設定で設定することができます。この後者の設定は、有線ゲスト アクセス トラフィックをさらに隔離するために使用されますが、有線ゲスト アクセスの展開には必須ではありません。

有線ゲスト アクセス ポートは、最初、レイヤ 2 アクセス スイッチか、有線ゲストのアクセス トラフィック用 VLAN インターフェイスで設定されたスイッチ ポートで終端します。有線ゲスト トラフィックは、その後、アクセス スイッチから無線 LAN コントローラへトランキングされます。このコントローラは、アクセス スイッチ上で有線ゲスト アクセス VLAN にマップされているインターフェイスを使用して設定されます。

2 つのコントローラが使用されている場合、外部コントローラがスイッチから有線ゲスト トラフィックを受信し、次に有線ゲスト トラフィックをアンカー コントローラへ転送します。アンカー コントローラも有線ゲストのアクセスに対して設定されています。有線ゲスト トラフィックがアンカー コントローラへ正常に渡されると、外部コントローラとアンカー コントローラ間に双方向の Ethernet over IP（EoIP）トンネルが確立され、このトラフィックを処理します。

2つのコントローラが展開されるとき、有線ゲストアクセスはアンカーと外部アンカーによって管理されますが、有線ゲスト アクセス クライアントではモビリティがサポートされていません。この場合、DHCP およびクライアントの Web 認証は、アンカー コントローラによって処理されます。

ロールと帯域幅コントラクトを設定して割り当てることで、ネットワーク内の有線ゲストユーザに割り当てる帯域幅の量を指定できます。

関連項目

- 有線ゲスト ユーザ アクセスの設定と有効化：ワークフロー

有線ゲスト ユーザ アクセスの設定と有効化：ワークフロー

有線ゲスト ユーザ アクセスを設定して有効化するには、次のワークフローを実行します。

1. 有線ゲスト アクセス用の動的インターフェイス（VLAN）を設定する：動的インターフェイスを作成して、有線ゲスト ユーザ アクセスを有効にします。
2. ゲスト ユーザ アクセス用の有線 LAN を設定する：新しい LAN（ゲスト LAN）を設定します。

関連トピック

有線ゲスト ユーザ アクセス用の動的インターフェイスの設定 （622 ページ）
ゲスト ユーザ アクセス用の有線 LAN の設定 （623 ページ）

有線ゲスト ユーザ アクセス用の動的インターフェイスの設定

ネットワークの有線ゲスト ユーザ アクセス用に動的インターフェイス（VLAN）を設定して有効にするには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）]** を選択し、左側の [デバイス グループ（Device Groups）] メニューから **[デバイス タイプ（Device Type）] > [ワイヤレス コントローラ（Wireless Controller）]** を選択します。

ステップ 2 デバイス名をクリックして [コントローラ（Controller）] タブをクリックします。

ステップ 3 左側のサイドバーのメニューから、[System] > [Interfaces] の順に選択します。

ステップ 4 [Select a command] ドロップダウン リストから [Add Interface] を選択し、[Go] をクリックします。

ステップ 5 必須フィールドに値を入力します。

ステップ 6 [Save] をクリックします。

関連トピック

有線ゲスト ユーザ アクセスの設定と有効化：ワークフロー （622 ページ）

ゲスト ユーザ アクセス用の有線 LAN の設定

ゲスト ユーザ アクセス用の有線 LAN を設定するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）]** を選択し、左側の [デバイス グループ（Devices Groups）] メニューから [デバイス タイプ（Device Type）] > [ワイヤレス コントローラ（Wireless Controller）] を選択します。

ステップ 2 デバイス名をクリックします。

ステップ 3 ゲスト ユーザ アクセス用の有線 LAN を設定するには、左側のサイドバーのメニューから [WLANs] > [WLAN configuration] の順に選択します。

ステップ 4 [Select a command] ドロップダウン リストから [Add a WLAN] を選択し、[Go] をクリックします。

ステップ 5 このコントローラに適用する作成済みのテンプレートがある場合には、ドロップダウン リストからゲスト LAN テンプレート名を選択します。そうでない場合には、[click here] リンクをクリックして新しいテンプレートを作成します。

ステップ 6 [WLAN] > [新規テンプレート（New Template）] の [一般（General）] ページで、[プロファイル名（Profile Name）] テキスト ボックスにゲスト LAN を示す名前を入力します。入力する名前には、スペースを使用しないでください。

ステップ 7 [WLAN Status] フィールドの [Enabled] チェックボックスをオンにします。

ステップ 8 [入力インターフェイス（Ingress Interface）] ドロップダウン リストから、ステップ 3 で作成した VLAN を選択します。この VLAN は、レイヤ 2 アクセス スイッチを経由して、有線ゲスト クライアントとコントローラとの間のパスを提供します。

ステップ 9 [出力インターフェイス（Egress Interface）] ドロップダウン リストから、インターフェイスの名前を選択します。この WLAN は、有線ゲスト クライアント トラフィック用にコントローラから外部へのパスを提供します。設定にコントローラが 1 つしかない場合は、[出力インターフェイス（Egress Interface）] ドロップダウン リストから [管理（management）] を選択します。

ステップ 10 [Security] > [Layer 3] タブをクリックして、デフォルトのセキュリティ ポリシー（Web 認証）を変更するか、または WLAN 固有の Web 認証（ログイン、ログアウト、ログイン失敗）ページとサーバ ソースを割り当てます。

a) セキュリティ ポリシーをパススルーに変更するには、[Web Policy] チェックボックスをオンにして、[Passthrough] オプション ボタンを選択します。これでユーザは、ユーザ名やパスワードを入力しなくてもネットワークにアクセスできます。

[Email Input] チェックボックスが表示されます。ユーザがネットワークに接続しようとしたとき、電子メール アドレスの入力を求める場合は、このチェックボックスをオンにします。

b) カスタムな Web 認証ページを指定するには、[Global WebAuth Configuration] の [Enabled] チェックボックスをオフにします。

[Web Auth Type] ドロップダウン リストが表示されたら、次のいずれかのオプションを選択して、無線ゲスト ユーザ用の Web ログイン ページを定義します。

[Default Internal]：コントローラのデフォルト Web ログイン ページを表示します。これはデフォルト値です。

[Customized Web Auth]：カスタム Web ログイン ページ、ログイン失敗ページ、およびログアウト ページを表示します。[Customized] オプションを選択した場合は、ログイン ページ、ログイン失敗ページ、およびログアウト ページを選択するための 3 つのドロップダウン リストが表示されます。これらすべてのオプションについてカスタマイズしたページを定義する必要はありません。カスタマイズしたページを表示しないオプションに対しては、該当するドロップダウン リストで [None] を選択します。

[External]：認証のためにユーザを外部サーバにリダイレクトします。このオプションを選択する場合、[URL] テキスト ボックスに外部サーバの URL も入力する必要があります。

外部認証を行う場合は、[Security] > [AAA] ペインで RADIUS サーバまたは LDAP サーバを選択できます。[Security] > [AAA] ペインで選択できるように、RADIUS 外部サーバと LDAP 外部サーバを事前に設定しておく必要があります。[RADIUS Authentication Servers]、[TACACS+ Authentication Servers]、および [LDAP Servers] ページでこれらのサーバを設定できます。

ステップ 11 [Web Authentication Type] で [External] を選択した場合は、[Security] > [AAA] を選択し、ドロップダウン リストから RADIUS サーバと LDAP サーバを 3 つまで選択します。

ステップ 12 [Save] をクリックします。

ステップ 13 2 番めの（アンカー）コントローラがネットワークで使用中の場合は、このプロセスを繰り返します。

関連トピック

有線ゲスト ユーザ アクセスの設定と有効化：ワークフロー （622 ページ）

コントローラでのゲスト LAN 入力インターフェイスの設定

入力インターフェイスを作成するには、次の手順を実行します。

ステップ 1 [設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）] を選択し、左側の [デバイスグループ（Devices Groups）] メニューから [デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）] を選択します。

ステップ 2 デバイス名をクリックして [コントローラ（Controller）] タブをクリックします。

ステップ 3 左側のサイドバーのメニューから、[System] > [Interfaces] の順に選択します。

ステップ 4 [Select a command] ドロップダウン リストから [Add Interface] を選択し、[Go] をクリックします。

ステップ 5 [インターフェイス名（Interface Name）] テキスト ボックスに、guestinterface など、このインターフェイスの名前を入力します。

ステップ 6 新しいインターフェイスの VLAN ID を入力します。

ステップ 7 [Guest LAN] チェックボックスをオンにします。

ステップ 8 プライマリ ポート番号とセカンダリ ポート番号を入力します。

ステップ 9 [Save] をクリックします。

関連トピック

コントローラでのゲスト LAN 出力インターフェイスの設定 （625 ページ）

コントローラでのゲスト LAN 出力インターフェイスの設定

出力インターフェイスを作成するには、次の手順を実行します。

ステップ 1 [設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）] を選択し、左側の [デバイスグループ（Devices Groups）] メニューから [デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）] を選択します。

ステップ 2 デバイス名をクリックして [コントローラ（Controller）] タブをクリックします。

ステップ 3 左側のサイドバーのメニューから、[System] > [Interfaces] の順に選択します。

ステップ 4 [Select a command] ドロップダウン リストから [Add Interface] を選択し、[Go] をクリックします。

ステップ 5 [インターフェイス名（Interface Name）] テキスト ボックスに、quarantine など、このインターフェイスの名前を入力します。

ステップ 6 [vlan Id] テキスト ボックスに、アクセス VLAN ID としてゼロ以外の値（「10」など）を入力します。

ステップ 7 [Quarantine] チェックボックスをオンにして、隔離 VLAN 識別子としてゼロ以外の値（「110」など）を入力します。

[Quarantine] が有効なインターフェイスの場合、[WLAN or guest WLAN template Advanced] タブで NAC サポートを有効にできます。

ステップ 8 IP アドレス、ネットマスク、およびゲートウェイの情報を入力します。

ステップ 9 プライマリ ポート番号とセカンダリ ポート番号を入力します。

ステップ 10 プライマリおよびセカンダリ DHCP サーバの IP アドレスを入力します。

ステップ 11 インターフェイスの残りのフィールドを設定し、[Save] をクリックします。

これで、ゲスト アクセス用の有線 LAN を作成できるようになりました。

関連トピック

コントローラでのゲスト LAN 入力インターフェイスの設定 （624 ページ）

コントローラ サービス ポートでのネットワーク ルートの設定

[ネットワーク ルート（Network Route）] ページでは、コントローラのサービス ポートにルートを追加できます。このルートを使用することで、すべてのサービス ポート トラフィックを指定した管理 IP アドレスに送ることができます。

関連トピック

既存のコントローラ ネットワーク ルートの表示 （626 ページ）
コントローラへのネットワーク ルートの追加 （626 ページ）

既存のコントローラ ネットワーク ルートの表示

既存のネットワーク ルートを表示するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。.

ステップ 2 デバイス名をクリックして [コントローラ（Controller）] タブをクリックします。

ステップ 3 左側のサイドバーのメニューから、**[システム（System）] > [ネットワーク ルート（Network Route）]** を選択します。次のパラメータが表示されます。

- [IP Address]：ネットワーク ルートの IP アドレス。
- [IP Netmask]：ルートのネットワーク マスク。
- [Gateway IP Address]：ネットワーク ルートのゲートウェイ IP アドレス。

関連トピック

コントローラ サービス ポートでのネットワーク ルートの設定 （626 ページ）

コントローラへのネットワーク ルートの追加

ネットワーク ルートを追加するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 デバイス名をクリックして [コントローラ（Controller）] タブをクリックします。

ステップ 3 左側のサイドバーのメニューから、[System] > [Network Route] の順に選択します。

ステップ 4 [Select a command] ドロップダウン リストから、[Add Network Route] を選択します。

ステップ 5 [Go] をクリックします。

ステップ 6 必須フィールドに入力して [Save] をクリックします。

関連トピック

コントローラ サービス ポートでのネットワーク ルートの設定 （626 ページ）
コントローラでの日時の設定

コントローラの STP パラメータの表示

スパニング ツリー プロトコル（STP）は、ネットワーク内の有害なループを防止しながら、パスの冗長性を実現するリンク管理プロトコルです。

現在の STP パラメータを表示または管理するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）]** を選択し、左側の [デバイス グループ（Device Groups）] メニューから **[デバイス タイプ（Device Type）] > [ワイヤレス コントローラ（Wireless Controller）]** を選択します。

ステップ 2 デバイス名をクリックして [Controller] タブをクリックします。

ステップ 3 左側のサイドバーのメニューから、**[システム（System）] > [スパニング ツリー プロトコル（Spanning Tree Protocol）]** を選択します。[Spanning Tree Protocol] ページに、次のパラメータが表示されます。

- [Protocol Spec]：現在のプロトコル仕様。
- [Admin Status]：有効にする場合は、このチェックボックスをオンにします。
- [Priority]：最適なスイッチのプライオリティ番号。
- [Maximum Age (seconds)]：ポートに対して記録された受信プロトコル情報が廃棄されるまでの時間（秒単位）。
- [Hello Time (seconds)]：スイッチが hello メッセージをその他のスイッチにブロードキャストする頻度（秒単位）を特定します。
- [Forward Delay (seconds)]：スイッチのポートがラーニング/リスニング ステートでの経過時間（秒単位）。

関連トピック

コントローラ サービス ポートでのネットワーク ルートの設定 （626 ページ）
[ネットワークデバイス（Network Devices）]テーブルからコントローラの一般システム プロパティを変更する （608 ページ）

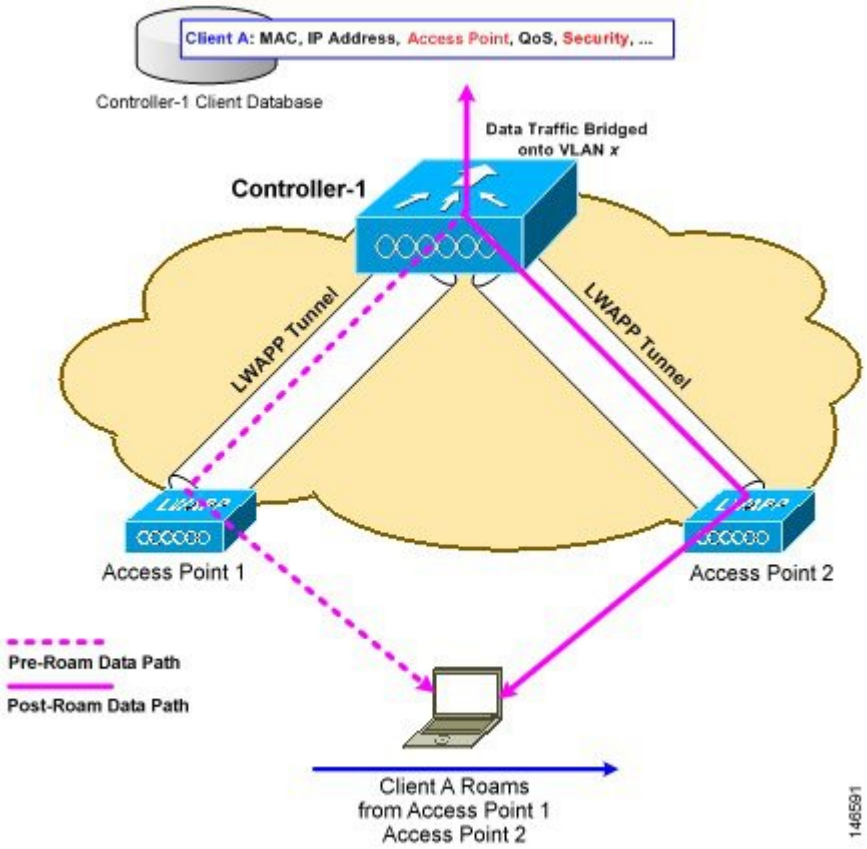
モビリティとは

モビリティ（ローミング）は、ワイヤレス ネットワークにおいて、できるだけ遅れることなく、確実かつスムーズに、あるアクセス ポイントから別のアクセス ポイントへアソシエーションを維持するワイヤレス クライアントの機能です。あるワイヤレス クライアントがアクセス ポイントによってアソシエートされ認証されると、コントローラは、クライアント データベースにそのクライアントに対するエントリを設定します。このエントリにはクライアントのMACアドレスとIPアドレス、セキュリティ コンテキストおよびアソシエーション、Quality of Service（QoS）コンテキスト、WLAN、アソシエートされているアクセス ポイントなどが含まれます。コントローラはこの情報を使用してフレームを転送し、ワイヤレス クライアントで送受信されるトラフィックを管理します。

コントローラ内ローミングとは

ワイヤレス クライアントがそのアソシエーションをあるアクセス ポイントから別のアクセス ポイントへ移動する場合、コントローラはクライアントのデータベースを新たにアソシエートするアクセス ポイントでアップデートするだけです。必要に応じて、新たなセキュリティ コンテキストとアソシエーションも確立されます。次の図には、2つのアクセス ポイントが同じコントローラに接続されている場合の両アクセス ポイント間における無線クライアント ローミングが示されています。図 146591

図 *12* : コントローラ内ローミング



関連トピック

モビリティとは （628 ページ）
モビリティ グループとは （632 ページ）
コントローラ間ローミングとは （629 ページ）

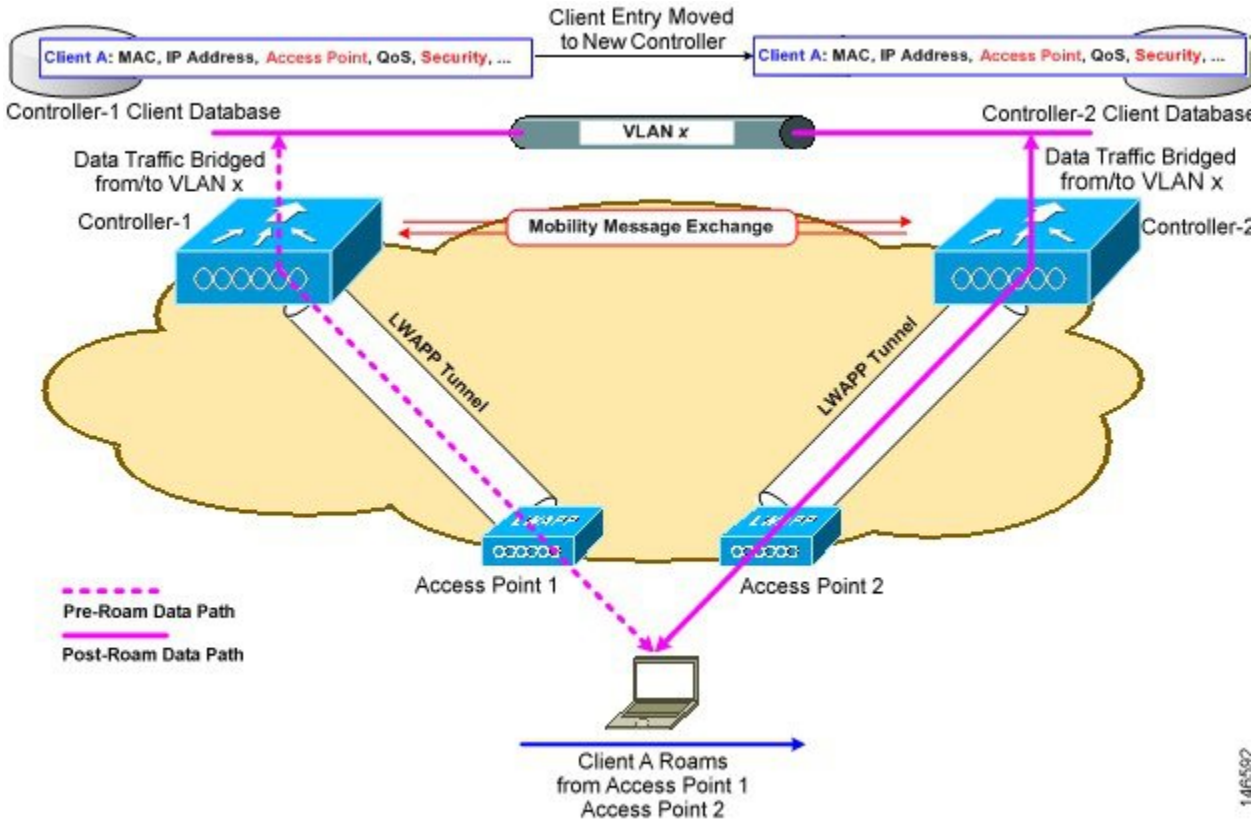
コントローラ間ローミングとは

1 つのコントローラに接続されているアクセス ポイントから別のコントローラに接続されているアクセス ポイントにクライアントがローミングする際のプロセスは、同じサブネットでコントローラが動作しているかどうかによっても異なります。次の図は、コントローラの無線LANインターフェイスが同じ IP サブネット上に存在する場合に発生するコントローラ間ローミングを表しています。

クライアントが新たなコントローラに接続されたアクセス ポイントにアソシエートされている場合、新たなコントローラはモビリティ メッセージを元のコントローラと交換し、クライアントのデータベース エントリは新たなコントローラに移動されます。新たなセキュリティ コンテキストとアソシエーションが必要に応じて確立され、クライアントのデータベース エントリは新たなアクセス ポイントに対してアップデートされます。このプロセスはユーザには見えません。

802.1X/Wi-Fi Protected Access（WPA）セキュリティで設定したすべてのクライアントは、IEEE 標準に準拠するために完全な認証を行います。

図 *13 :* コントローラ間ローミング



関連トピック

モビリティとは （628 ページ）
モビリティ グループとは （632 ページ）
コントローラ内ローミングとは （628 ページ）
コントローラをモビリティ グループに追加するための前提条件 （634 ページ）

サブネット間ローミングとは

サブネット間ローミングは、クライアント ローミング方法に関するモビリティ メッセージをコントローラが交換するという点で、コントローラ間ローミングと似ています。ただし、クライアントのデータベース エントリを新しいコントローラに移動するのではなく、元のコントローラのクライアントデータベース内で該当クライアントに「アンカー」エントリのマークが付けられます。このデータベース エントリが新しいコントローラのクライアント データベースにコピーされ、新しいコントローラ内で「外部」エントリのマークが付けられます。ローミングは無線クライアントには見えません。また、クライアントはその元の IP アドレスを保持します。

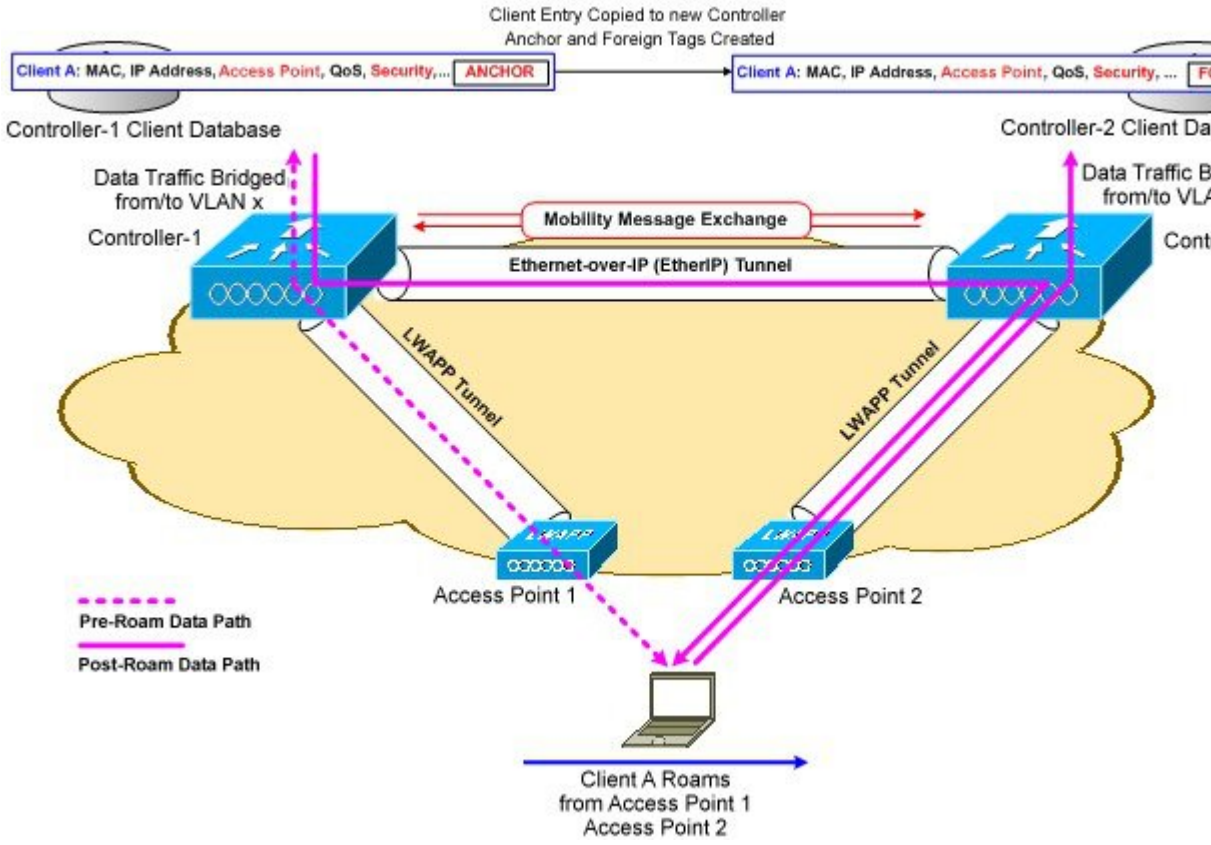
サブネット間ローミングの後は、データは無線クライアントとの間で非対称のトラフィック パスで転送されます。クライアントからネットワークへのトラフィックは、外部コントローラによってネットワークへ直接転送されます。クライアントへのトラフィックはアンカー コントローラに到達し、ここでEtherIP トンネルで外部コントローラへ転送されます。外部コントローラは、そのデータをクライアントへ転送します。無線クライアントが新しい外部コントローラへローミングする場合は、クライアントのデータベース エントリは元の外部コントローラから新しい外部コントローラへ移動されますが、元のアンカー コントローラは常に保持されます。クライアントは元のコントローラに戻ると、再びローカルになります。

サブネット間ローミングでは、アンカーと外部の両コントローラのWLANに同一のネットワーク アクセス権限を設定し、ソースベースのルーティングやソースベースのファイアウォールを設定しないでおく必要があります。そうしないと、ハンドオフ後にクライアントにネットワーク接続の問題が発生する場合があります。

サブネット間ローミングは、マルチキャスト トラフィックをサポートしていません（プッシュ ツートークの使用中に Spectralink 電話によって使用されるトラフィックなど）。

次の図 146593 は、コントローラの無線 LAN インターフェイスが異なる IP サブネット上に存在する場合に発生するサブネット間ローミングを表しています。

図 *14 :*



関連トピック

モビリティとは （628 ページ）

モビリティ グループとは （632 ページ）
コントローラ内ローミングとは （628 ページ）
コントローラ間ローミングとは （629 ページ）
コントローラをモビリティ グループに追加するための前提条件 （634 ページ）

対称トンネリングとは

シンメトリック モビリティ トンネリングを使用すると、コントローラでは 1 つのアクセス ポイントから無線 LAN 内の別のアクセス ポイントへローミングするクライアントに対して、サブネット間のモビリティが提供されます。有線ネットワーク上のクライアント トラフィックは、外部コントローラによって直接ルーティングされます。ルータでリバース パス フィルタリング（RPF）が有効になっている場合、着信パケットで追加確認が実行され、通信はブロックされます。RPF が有効になっている場合でも、シンメトリック モビリティ トンネリングによって、アンカーとして指定されたコントローラにクライアント トラフィックが到達できるようになります。モビリティ グループのすべてのコントローラは、同一のシンメトリック トンネリング モードを備えている必要があります。

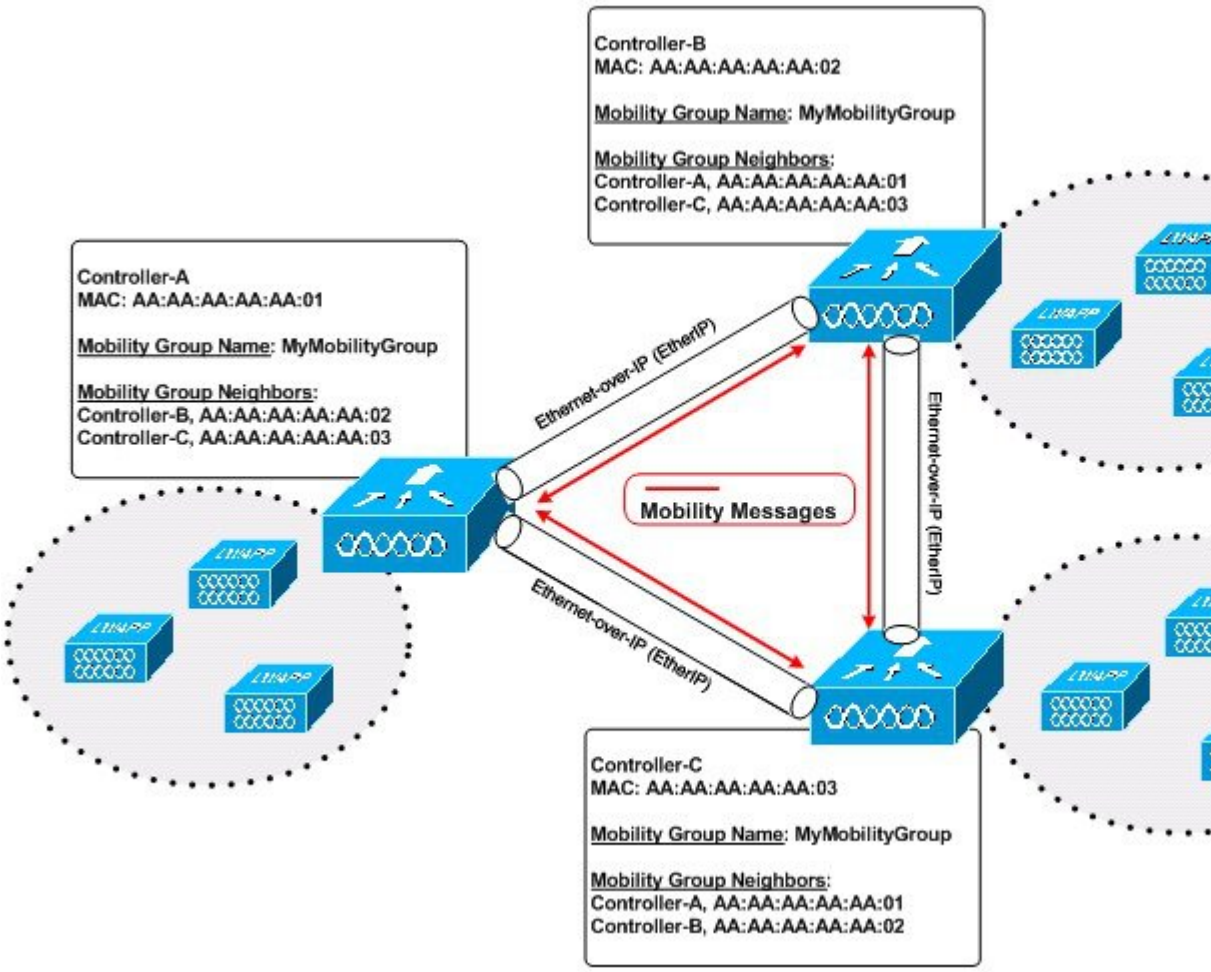
この機能を使用すると、コントローラの障害後にクライアントが別のアクセス ポイントに接続するための時間が短縮されます。障害がすばやく特定され、問題のあるコントローラからクライアントが移動し、別のコントローラに関連付けられるためです。

モビリティ グループとは

コントローラのセットをモビリティ グループとして設定すると、コントローラのグループ内でクライアントのローミングをスムーズに実行できるようになります。これにより、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、複数のコントローラが動的に情報を共有してデータ トラフィックを転送できるようになります。コントローラは、クライアントおよびコントローラのロード情報のコンテキストおよび状態を共有できます。この情報を使用して、ネットワークはコントローラ間無線 LAN ローミングとコントローラの冗長性をサポートできます。クライアントは、モビリティ グループ間のローミングは行いません。

次の図は、モビリティ グループの例を示します。

図 *15* : シングル モビリティ グループ



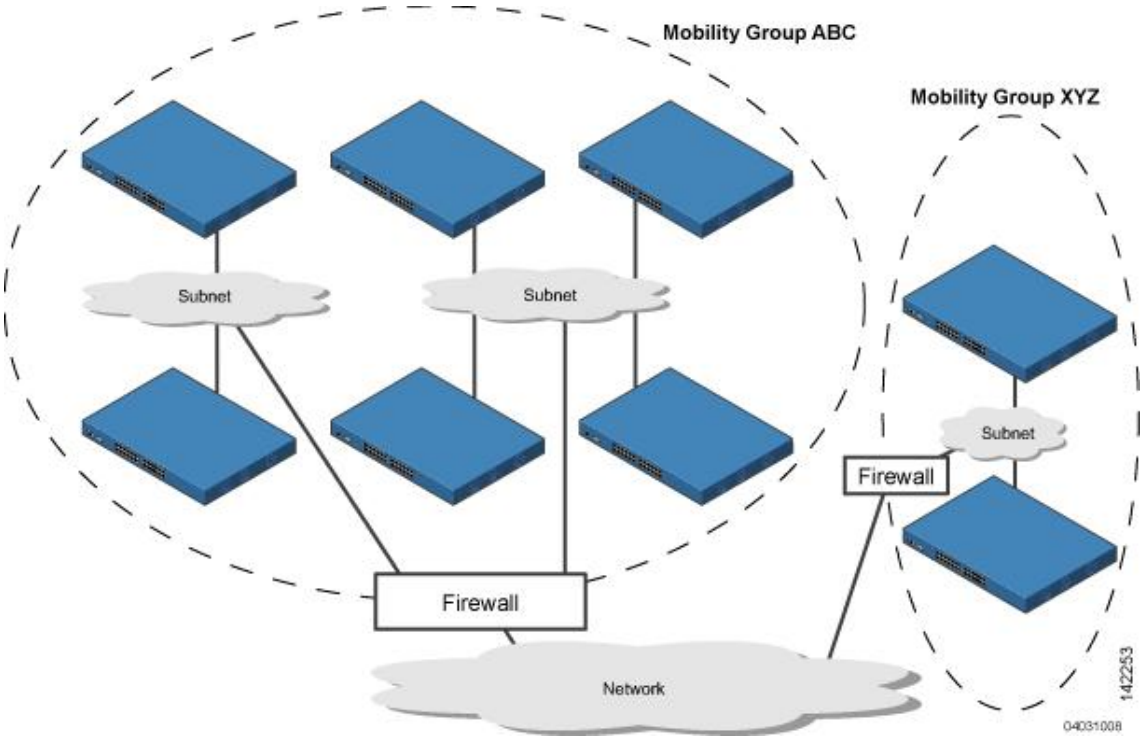
上の図に示すように、各コントローラはモビリティ グループの別メンバーのリストを使用して設定されています。新たなクライアントがコントローラに追加されると、コントローラはユニキャスト メッセージをそのモビリティ グループの全コントローラに送信します。クライアントが以前に接続されていたコントローラは、クライアントのステータスを送信します。コントローラ間のすべてのモビリティ交換トラフィックが CAPWAP トンネルで実行されます。

例：

1. 4404-100 コントローラは、最大 100 台のアクセス ポイントをサポートします。したがって、24 個の 4404-100 コントローラで構成されているモビリティ グループは、最大 2400 個のアクセス ポイント（24 * 100 = 2400 アクセス ポイント）をサポートします。
2. 4402-25 コントローラは最大 25 台のアクセス ポイントをサポートし、4402-50 コントローラは最大 50 台のアクセス ポイントをサポートします。したがって、12 個の 4402-25 コントローラと 12 個の 4402-50 コントローラで構成されたモビリティ グループは最大 900 個のアクセス ポイント（12 * 25 + 12 * 50 = 300 + 600 = 900 アクセス ポイント）をサポートします。

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。次の図には、2つのコントローラ グループに異なるモビリティ グループ名を作成した結果が示されています。

図 *16 : 2* つのモビリティ グループ



ABC モビリティ グループのコントローラは、アクセス ポイントと共有サブネットを使用して相互に認識しあい、通信します。ABC モビリティ グループのコントローラは、異なるモビリティ グループの XYZ コントローラを認識せず、通信を行いません。同様に、XYZ モビリティ グループのコントローラは、ABC モビリティ グループのコントローラを認識せず、通信を行いません。この機能により、ネットワークでのモビリティ グループの切り離しが確実に行われます。クライアントは、異なるモビリティ グループのアクセス ポイントを検出できる場合は、そのアクセス ポイント間のローミングを行う場合があります。ただし、そのセッション情報は異なるモビリティ グループのコントローラ間では伝送されません。

関連トピック

コントローラをモビリティ グループに追加するための前提条件 （634 ページ）
コントローラのモビリティ グループ メッセージングの仕組み （635 ページ）

コントローラをモビリティ グループに追加するための前提条件

モビリティ グループにコントローラを追加する前に、そのグループに含めるすべてのコントローラに対して、次の前提条件が満たされていることを確認する必要があります。

- すべてのコントローラには同じ CAPWAP モードを設定する必要があります（レイヤ 2 またはレイヤ 3）。
- すべてのコントローラの管理インターフェイス間に IP 接続が存在する必要があります。
- すべてのコントローラは、同じモビリティ グループ名で設定する必要があります。
- すべてのコントローラは、同じ仮想インターフェイス IP アドレスで設定する必要があります。
- モビリティ グループに追加するコントローラごとに、MAC アドレスと IP アドレスを収集しておく必要があります。この情報が必要となるのは、他の全モビリティ グループ メンバの MAC アドレスと IP アドレスを使用してすべてのコントローラを設定するからです。
- ネットワーク内のワイヤレス クライアントをあるコントローラに接続されたアクセス ポイントから別のコントローラに接続されたアクセス ポイントにローミング可能な場合は、両方のコントローラは同じモビリティ グループ内に存在する必要があります。

関連トピック

モビリティ グループとは （632 ページ）
コントローラのモビリティ グループ メッセージングの仕組み （635 ページ）

コントローラのモビリティ グループ メッセージングの仕組み

コントローラでは、モビリティ メッセージをその他のメンバー コントローラに送信することにより、クライアントに対してサブネット間のモビリティが提供されます。モビリティ リストで最大 72 のメンバーをサポートします（同じモビリティ グループでは最大 24 まで）。Cisco Prime Infrastructure Prime Infrastructure およびコントローラ ソフトウェア リリース 5.0 では、モビリティ メッセージングに対して次の 2 つの改良が行われました。いずれも、モビリティ メンバーの全リストにメッセージを送信する場合に役立ちます。

- Mobile Announce メッセージを、まず同じグループ内に送信してから、リスト内の他のグループに送信する

コントローラは、新しいクライアントがアソシエートされるたびに、モビリティ リスト内のメンバに Mobile Announce メッセージを送信します。5.0 より前のソフトウェア リリースでは、コントローラは所属グループに関係なく、このメッセージをリスト内のすべてのメンバに送信します。しかし、ソフトウェア リリース 5.0 では、コントローラは自分と同じグループに属するメンバーに対してだけメッセージを送信し、その後、再試行を送信しながら、他のメンバーをすべて加えます。

- ユニキャストではなくマルチキャストを使用して Mobile Annouce メッセージを送信する

Cisco Prime Infrastructure および 5.0 よりも前のコントローラ ソフトウェア リリースでは、コントローラはマルチキャストを使用して、Mobile Announce メッセージを送信するように設定される場合がありますが、これには、すべてのモビリティ メンバにメッセージのコピーを送信する必要があります。多くのメッセージ（Mobile Announce、ペアワイズ マスター キー（PMK）更新、AP リスト更新、侵入検知システム（IDS）Shun など）がグループ内のすべてのメンバー向けであるため、この動作は効率的ではありません。Cisco Prime Infrastructure およびコントローラ ソフトウェア リリース 5.0 では、コントローラでマルチキャスト モードを使用して Mobile Announce メッセージを送信します。これにより、コントローラからネットワークに送られるメッセージは 1 コピーのみになります。このコピーはモビリティ メンバすべてを含むマ

ルチキャスト グループに宛てて送られます。マルチキャスト メッセージングを最大限生かすには、グループ メンバすべてに対してこの機能を有効または無効にすることを推奨します。

関連トピック

モビリティ グループとは （632 ページ）
コントローラをモビリティ グループに追加するための前提条件 （634 ページ）
モビリティ グループの設定：ワークフロー （636 ページ）

モビリティ グループの設定：ワークフロー

モビリティ グループを設定する際は、次のワークフローに従います。

1. コントローラをモビリティ グループに追加するための前提条件（634ページ） で説明されているように、必要な情報を収集し、参加するコントローラが適切に構成されていることを確認してください。
2. モビリティ グループに個々のコントローラを追加します。モビリティ グループが存在しない場合は、場合によって手動で追加する必要があります。また、**[設定（Configuration）]** > **[ネットワーク（Network）]** > **[ネットワークデバイス（Network Devices）]** ページから追加しようとするとコントローラが表示されない場合があります。
3. モビリティ グループの規模およびメッセージング パラメータを設定します。

コントローラをモビリティ グループに追加するための前提条件

モビリティ グループにコントローラを追加する前に、そのグループに含めるすべてのコントローラに対して、次の前提条件が満たされていることを確認する必要があります。

- すべてのコントローラには同じ CAPWAP モードを設定する必要があります（レイヤ 2 またはレイヤ 3）。
- すべてのコントローラの管理インターフェイス間に IP 接続が存在する必要があります。
- すべてのコントローラは、同じモビリティ グループ名で設定する必要があります。
- すべてのコントローラは、同じ仮想インターフェイス IP アドレスで設定する必要があります。
- モビリティ グループに追加するコントローラごとに、MAC アドレスと IP アドレスを収集しておく必要があります。この情報が必要となるのは、他の全モビリティ グループ メンバの MAC アドレスと IP アドレスを使用してすべてのコントローラを設定するからです。
- ネットワーク内のワイヤレス クライアントをあるコントローラに接続されたアクセス ポイントから別のコントローラに接続されたアクセス ポイントにローミング可能な場合は、両方のコントローラは同じモビリティ グループ内に存在する必要があります。

関連トピック

モビリティ グループとは （632 ページ）
コントローラのモビリティ グループ メッセージングの仕組み （635 ページ）

モビリティ グループに属しているコントローラの表示

現在のモビリティ グループ メンバーを表示するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 デバイス名をクリックして [コントローラ（Controller）] タブをクリックします。

ステップ 3 左側のサイドバーのメニューから、**[システム（System）] > [モビリティ グループ（Mobility Groups）]** を選択します。

関連トピック

[ネットワークデバイス（Network Devices）] テーブルからコントローラをモビリティ グループに追加する （637 ページ）

[ネットワークデバイス（Network Devices）] テーブルからコントローラをモビリティ グループに追加する

既存のコントローラのリストからモビリティ グループ メンバーを追加するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Devices Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 デバイス名をクリックして [コントローラ（Controller）] タブをクリックします。

ステップ 3 左側のサイドバーのメニューから、**[システム（System）] > [モビリティグループ（Mobility Groups）]** の順に選択します。

ステップ 4 [Select a command] ドロップダウン リストから [Add Group Members] を選択します。

ステップ 5 [Go] をクリックします。

ステップ 6 モビリティ グループに追加するコントローラのチェックボックスをオンにします。

ステップ 7 [Save] をクリックします。

ステップ 8 手順 6 でコントローラの一覧が表示されない場合は、次の操作を実行して手動で追加できます。

a) [モビリティ グループ メンバーの詳細（Mobility Group Member details）] ページで [ここをクリック（click here）] リンクをクリックします。

b) [メンバーの MAC アドレス（Member MAC Address）] テキスト ボックスに、追加するコントローラの MAC アドレスを入力します。

c) [メンバーの IP アドレス（Member IP Address）] テキスト ボックスに、追加するコントローラの管理インターフェイス IP アドレスを入力します。

ネットワーク アドレス変換（NAT）が有効になっているネットワークのモビリティ グループを設定する場合は、コントローラの管理インターフェイス IP アドレスではなく、NAT デバイスからコントローラに送信される IP アドレスを入力します。そうしないと、モビリティ グループ内のコントローラ間でモビリティが失敗します。

d) マルチキャスト モビリティ メッセージに使用するマルチキャスト グループ IP アドレスを [Multicast Address] テキスト ボックスに入力します。ローカル モビリティ メンバのグループ アドレスは、ローカル コントローラのグループ アドレスと同じである必要があります。
e) [グループ名（Group Name）] テキスト ボックスに、モビリティ グループ名を入力します。
f) [保存（Save）] をクリックします。

残りのシスコ ワイヤレス コントローラ デバイスに対して上記の手順を繰り返します。

関連トピック

モビリティ グループに属しているコントローラの表示 （637 ページ）

コントローラへの NTP サーバの追加

新しい NTP サーバを追加するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Devices Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。
ステップ 2 該当するコントローラのデバイス名をクリックします。
ステップ 3 左側のサイドバーのメニューから、[System] > [Network Time Protocol] の順に選択します。
ステップ 4 [Select a command] ドロップダウン リストから [Add NTP Server] を選択します。
ステップ 5 [Go] をクリックします。
ステップ 6 [このコントローラに適用するテンプレートを選択する（Select a template to apply to this controller）] ドロップダウン リストから、このコントローラに適用する適切なテンプレートを選択します。

関連トピック

[ネットワークデバイス（Network Devices）]テーブルからコントローラの一般システム プロパティを変更する （608 ページ）

メッシュ ネットワーク バック グラウンド スキャン用のコント ローラーを構成します。

バックグラウンド スキャンにより、Cisco Aironet 1510 アクセス ポイントは、より最適なパスと親を探すために、能動的に連続してネイバー チャネルをモニタできます。アクセス ポイン

トは現在のチャネルだけでなくネイバーチャネル上でも検索を実行するため、最適な代替パスおよび親のリストは大きくなります。

親を喪失する前にこの情報を特定すると、より高速な転送速度およびそのアクセス ポイントにとって最適なリンクが実現します。さらに、新しいチャネル上のリンクが、ホップの少なさ、信号対雑音比（SNR）の強さなどの点で、現在のチャネルよりも良好であると判明した場合は、アクセス ポイントはそのチャネルに切り替わる場合があります。

その他のチャネル上でのバックグラウンドスキャンおよびそれらのチャネル上のネイバーからのデータ収集は、2 つのアクセス ポイント間のプライマリ バックホール上で実行されます。

1510 のプライマリ バックホールは、802.11a リンク上で動作します。

バックグラウンド スキャンは、アクセス ポイントのアソシエートされたコントローラ上でグローバルに有効化されます。音声コールが新しいチャネルに切り替わると、遅延が大きくなる場合があります。

EMEA 規制区域では、DFS 要件が前提となるため、その他のチャネル上でのネイバーの検索に時間がかかる場合があります。

関連トピック

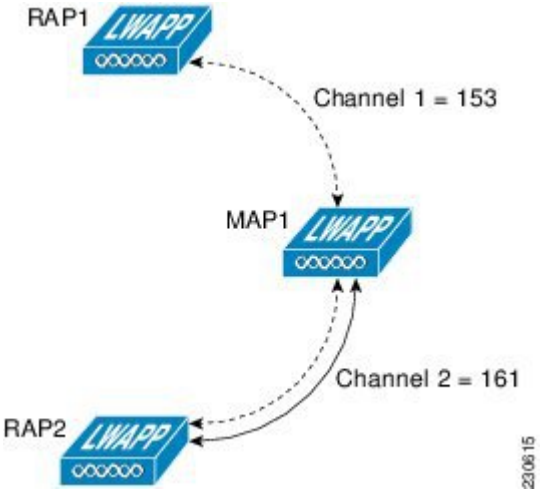
メッシュ ネットワーク バックグラウンド スキャンのシナリオ （639 ページ）
コントローラでのメッシュ ネットワーク バックグラウンド スキャンの有効化 （641 ページ）

メッシュ ネットワーク バックグラウンド スキャンのシナリオ

バックグラウンドスキャンの動作をより詳しく説明するために、いくつかのシナリオを示します。

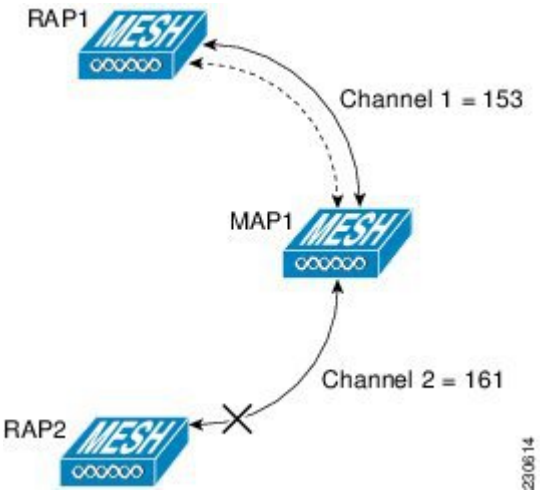
次の図では、メッシュ アクセス ポイント（MAP1）は、初回のアップ時に、ルート アクセス ポイント（RAP1 および RAP2）の両方が親になる可能性があると認識しています。ここでは、ホップ、SNR などの点で RAP2 を経由したルートの方が良好であるため、RAP2 が親として選択されています。リンクの確立後、バックグラウンドスキャン（有効にした場合）は、すべてのチャネルを継続的にモニタし、より最適なパスおよび親を検索します。RAP2 は、リンクがダウンするか、より最適なパスが別のチャネルで見つかるまで、MAP1 の親としての動作を継続し、チャネル 2 上で通信を続けます。

図 *17 :* メッシュ アクセス ポイント（*MAP1*）による親の選択



次の図 230614 では、MAP1 と RAP2 間のリンクが失われています。現在実行中のバックグラウンド スキャンからのデータにより、RAP1 と Channel 1 が、MAP1 にとって 2 番めに最適な親および通信パスであると識別されるため、RAP2 とのリンクがダウンした後に、追加のスキャンなしでリンクがただちに確立されます。

図 *18 :* バックグラウンド スキャンによる新しい親の識別



関連トピック

コントローラでのメッシュ ネットワーク バックグラウンド スキャンの有効化 （641 ページ）

コントローラでのメッシュ ネットワーク バックグラウンド スキャンの有効化

AP1510 RAP または MAP でバックグラウンド スキャンを有効にするには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）]** を選択し、左側の [デバイス グループ（Devices Groups）] メニューから **[デバイス タイプ（Device Type）] > [ワイヤレス コントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラの IP アドレスをクリックします。

ステップ 3 左側のサイドバーのメニューから、**[メッシュ（Mesh）] > [メッシュ設定（Mesh Settings）]** を選択します。

ステップ 4 バックグラウンドスキャンを有効にする場合は[バックグラウンドスキャン（Background Scanning）]チェックボックスをオンにし、この機能を無効にする場合はオフにします。デフォルトでは、無効に設定されています。

ステップ 5 この機能により、すべてのチャネルをスキャンすることによりチャネル全体にわたって親を検索するという時間のかかるタスクが削減されます。オフチャネル手順は、選択したチャネルでブロードキャスト パケットを送信し（3 秒間隔、オフチャネルあたり最大 50 ミリ秒）、すべての「到達可能」ネイバーからパケットを受信します。これにより、子 MAP はチャネル全体にわたるネイバー情報で更新され、新しいネイバーに「切り替え」てアップリンクの親として使用することができます。「切り替え」は、親損失の検出でトリガーされる必要はありませんが、より良い親の識別時にトリガーされます。ただし、子 MAP では現在の親アップリンクがアクティブなままとなります。

ステップ 6 [保存（Save）] をクリックします。

関連トピック

メッシュ ネットワーク バックグラウンド スキャンのシナリオ （639 ページ）

コントローラ QoS プロファイルの設定

QoS プロファイルを変更するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Devices Groups）] メニューから [デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）] を選択します。

ステップ 2 該当するコントローラの IP アドレスをクリックします。

ステップ 3 左側のサイドバーのメニューから、[System] > [QoS Profiles] の順に選択します。次のパラメータが表示されます。

- [Bronze]：バックグラウンド用
- [Gold]：ビデオ アプリケーション用

- [Platinum]：音声アプリケーション用
- [Silver]：ベスト エフォート用

ステップ 4 該当するプロファイルをクリックして、プロファイル パラメータを表示または編集します。

ステップ 5 [Save] をクリックします。

関連トピック

[ネットワークデバイス（Network Devices）]テーブルからコントローラの一般システム プロパティを変更する （608 ページ）

内部 DHCP サーバに関する情報

Cisco コントローラには、DHCP（Dynamic Host Configuration Protocol）リレー エージェントが組み込まれています。ただし、別個の DHCP サーバを持たないネットワーク セグメントを求められる場合、コントローラに IP アドレスとサブネット マスクを無線クライアントに割り当てる組み込みの DHCP スコープを設定できます。一般に、1 つのコントローラには、それぞれある範囲の IP アドレスを指定する複数の DHCP スコープを設定できます。

（注） この機能は、Cisco Mobility Express リリース 8.3 以降に適用されます。

現在の DHCP スコープの表示

現在の DHCP（Dynamic Host Configuration Protocol）スコープを表示するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[システム（System）] > [DHCPスコープ（DHCP Scopes）]** の順に選択します。次のパラメータが表示されます。

- スコープ名
- プール アドレス
- リース時間
- プール使用率。これは、Cisco Mobility Express DHCP スコープにのみ表示されます。

DHCP スコープの設定

新しい DHCP スコープを追加するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**[設定（Configuration）]** > **[ネットワーク（Network）]** > **[ネットワーク デバイス（Network Devices）]** > **[デバイス タイプ（Device Type）]** > **[ワイヤレス コントローラ（Wireless Controller）]** を選択します。	
ステップ 2	該当するコントローラのデバイス名をクリックします。	
ステップ 3	左側のサイドバーのメニューから、**[システム（System）]** > **[DHCPスコープ（DHCP Scopes）]** の順に選択します。	
ステップ 4	[コマンドの選択（Select a command）] ドロップダウン リストから、[DHCP スコープの追加（Add DHCP Scope）] を選択して新しい DHCP スコープを追加し、[実行（Go）] をクリックします。	
ステップ 5	[スコープ名（Scope Name）]テキストボックスに、新しい DHCP スコープの名前を入力します。	
ステップ 6	[VLAN-ID] テキストボックスに VLAN ID を入力します。	
ステップ 7	[リース時間（Lease Time）]テキストボックスに、IP アドレスをクライアントに対して許可する時間（0 ～ 65,536 秒）を入力します。	
ステップ 8	[Network] テキストボックスに、この DHCP スコープの対象となるネットワークを入力します。この IP アドレスは、[Interfaces] ページで設定されている、ネットマスクが適用された管理インターフェイスによって使用されます。	
ステップ 9	[ネットマスク（Netmask）] テキストボックスに、すべての無線クライアントに割り当てられたサブネット マスクを入力します。	
ステップ 10	[Pool Start Address] テキストボックスに、クライアントに割り当てられた範囲の開始 IP アドレスを入力します。このプールは、各 DHCP スコープで一意でなければならず、ルータまたは他のサーバの固定 IP アドレスを含めることはできません。	

	コマンドまたはアクション	目的
ステップ 11	[プール終了アドレス（Pool End Address）] テキスト ボックスに、クライアントに割り当てられた範囲の終了IPアドレスを入力します。このプールは、各 DHCP スコープで一意でなければならず、ルータまたは他のサーバの固定 IP アドレスを含めることはできません。	
ステップ 12	[デフォルト ゲートウェイ（Default Gateway）] テキスト ボックスに、オプションのゲートウェイの IP アドレスを入力します。	
ステップ 13	[DNS ドメイン名（DNS Domain Name）] テキスト ボックスに、1 つまたは複数の DNS サーバで使用する、この DHCP スコープのオプションの DNS 名を入力します。	
ステップ 14	[DNS Servers] テキストボックスに、オプションの DNS サーバの IP アドレスを入力します。各 DNS サーバは、この DHCP スコープで割り当てられた IPアドレスと一致するように、クライアントのDNS エントリを更新できる必要があります。	
ステップ 15	**[保存（Save）]** をクリックします。	

DHCP スコープの削除

（注） DHCP スコープを削除するのには、最初にその管理状態を無効にする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**[設定（Configuration）]** > **[ネットワーク（Network）]** > **[ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）]** > **[ワイヤレスコントローラ（Wireless Controller）]** を選択します。	
ステップ 2	該当するコントローラのデバイス名をクリックします。	

	コマンドまたはアクション	目的
ステップ 3	左側のサイドバーのメニューから、**[システム（System）] > [DHCPスコープ（DHCP Scopes）]** の順に選択します。	
ステップ 4	削除する DHCP スコープのチェックボックスをオンにします。	
ステップ 5	[コマンドの選択（Select a command）] ドロップダウンリストから、[DHCP スコープの削除（Delete DHCP Scope）] を選択し、[実行（Go）] をクリックします。	

DHCP スコープの詳細のエクスポート

手順

	コマンドまたはアクション	目的
ステップ 1	**[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。	
ステップ 2	該当するコントローラのデバイス名をクリックします。	
ステップ 3	左側のサイドバーのメニューから、**[システム（System）] > [DHCPスコープ（DHCP Scopes）]** の順に選択します。	
ステップ 4	[コマンドの選択（Select a command）] ドロップダウン リストから、[DHCPLeases] を選択し、[実行（Go）] をクリックします。	
ステップ 5	[MAC アドレス（MAC Address）] の横にあるチェックボックスをオンにし、[エクスポート（Export）] をクリックして DHCP スコープの詳細を csv ファイルとしてエクスポートします。	

コントローラのユーザ認証に使用されるコントローラのローカル ネットワーク テンプレートの表示

コントローラの現在のローカルネットユーザ ロールを表示するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[システム（System）] > [ユーザ ロール（User Roles）]** を選択します。

ローカル ネット ユーザ ロールのパラメータが表示されます。

ステップ 4 テンプレート名をクリックして、ユーザ ロールの詳細を表示します。

関連トピック

コントローラのユーザ認証に使用されるコントローラのローカルネットワーク テンプレートの設定 （646 ページ）

コントローラのユーザ認証に使用されるコントローラのローカル ネットワーク テンプレートの設定

新しいローカルネットユーザ ロールをコントローラに追加するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Devices Groups）] メニューから [デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）] を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、[System] > [User Roles] の順に選択します。

ステップ 4 [Select a command] ドロップダウン リストから、[Add User Role] を選択します。

ステップ 5 [Select a template to apply to this controller] ドロップダウン リストからテンプレートを選択します。

ステップ 6 [Apply] をクリックします。

関連トピック

コントローラのユーザ認証に使用されるコントローラのローカルネットワーク テンプレートの表示 （646 ページ）

[ネットワークデバイス（Network Devices）]テーブルからコントローラの一般システム プロパティを変更する （608 ページ）

コントローラに接続する AP のコントローラ ユーザ名とパスワードの設定

[AP Username Password] ページでは、すべてのアクセス ポイントがコントローラに接続する際に継承する、グローバル パスワードを設定できます。また、アクセス ポイントを追加するときに、このグローバル ユーザ名およびパスワードを受け入れるか、アクセス ポイント単位で上書きするかを選択できます。

さらにコントローラ ソフトウェア リリース 5.0 では、アクセス ポイントをコントローラに接続すると、そのアクセス ポイントのコンソール ポート セキュリティが有効になり、アクセス ポイントのコンソール ポートへログインするたびにユーザ名とパスワードの入力を要求されます。ログインした時点では非特権モードのため、特権モードを使用するには、イネーブル パスワードを入力する必要があります。

グローバル ユーザ名とパスワードを設定するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Devices Groups）] メニューから [デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）] を選択します。

ステップ 2 リリース 5.0 以降のコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、[System] > [AP Username Password] の順に選択します。

ステップ 4 コントローラに接続するアクセス ポイントで継承されるユーザ名およびパスワードを入力します。

Cisco IOS アクセス ポイントの場合は、イネーブル パスワードも入力して確認する必要があります。

ステップ 5 **[保存（Save）]** をクリックします。

コントローラでの CDP の設定

Cisco Discovery Protocol（CDP）は、すべてのシスコ製ネットワーク機器で実行されるデバイス検出プロトコルです。各デバイスはマルチキャスト アドレスに識別メッセージを送信し、他のデバイスから送信されたメッセージをモニタします。

CDP は、イーサネット ポートおよび無線ポート上で、デフォルトで有効になっています。

グローバル インターフェイス CDP 設定は、AP レベルで CDP を有効にした AP のみに適用されます。

グローバル CDP を設定するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Devices Groups）] メニューから [デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）] を選択します。

ステップ 2 目的のコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、[System] > [Global CDP Configuration] の順に選択します。[Global CDP Configuration] ページが表示されます。

ステップ 4 [グローバル CDP 設定（Global CDP Configuration）] ページで必要なフィールドを設定します。[Global CDP] グループ ボックスで、次のパラメータを設定します。

- [CDP on controller]：コントローラで CDP を有効にするか、無効にするかを選択します。この設定は、WiSM2 コントローラには適用できません。
- [Global CDP on APs]：アクセス ポイントで CDP を有効にするか、無効にするかを選択します。
- [Refresh-time Interval (seconds)]：[Refresh Time Interval] フィールドに、CDP メッセージが生成される時間を秒単位で入力します。デフォルトは 60 です。
- [Holdtime (seconds)]：CDP ネイバー エントリの期限が切れるまでの時間を秒単位で入力します。デフォルトは 180 です。
- [CDP Advertisement Version]：使用する CDP プロトコルのバージョンを入力します。デフォルトは v1 です。

ステップ 5 [CDP for Ethernet Interfaces] グループ ボックスで、CDP を有効にするイーサネット インターフェイスのスロットを選択します。

[CDP for Ethernet Interfaces] フィールドは、リリース 7.0.110.2 以降のコントローラでサポートされています。

ステップ 6 [CDP for Radio Interfaces] グループ ボックスで、CDP を有効にする無線インターフェイスのスロットを選択します。

[CDP for Radio Interfaces] フィールドは、リリース 7.0.110.2 以降のコントローラでサポートされています。

ステップ 7 [Save] をクリックします。

関連トピック

[ネットワークデバイス（Network Devices）]テーブルからコントローラの一般システム プロパティを変更する （608 ページ）

コントローラへの 802.1X 認証の設定

Lightweight アクセス ポイントとスイッチ間の 802.1X 認証を設定できます。アクセス ポイントは 802.1X サプリカントとして動作し、EAP-FAST と匿名 PAC プロビジョニングを使用してスイッチにより認証されます。すべてのアクセス ポイントがコントローラ接続時に継承するグ

ローバル認証を設定できます。これには、コントローラに現在接続されているすべてのアクセス ポイント、および今後接続されるすべてのアクセス ポイントが含まれます。

必要に応じて、このグローバル認証設定よりも優先される、独自の認証設定を特定のアクセスポイントに割り当てることができます。

グローバル サプリカント クレデンシャルを有効にするには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）]** を選択し、左側の [デバイス グループ（Devices Groups）] メニューから [デバイス タイプ（Device Type）] > [ワイヤレス コントローラ（Wireless Controller）] を選択します。

ステップ 2 目的のコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、[System] > [AP 802.1X Supplicant Credentials] の順に選択します。

ステップ 4 [Global Supplicant Credentials] チェックボックスをオンにします。

ステップ 5 サプリカント ユーザ名を入力します。

ステップ 6 適切なパスワードを入力して確定します。

ステップ 7 ドロップダウン メニューから [サプリカントEAPタイプ（Supplicant EAP Type）] を選択します。

（注） バージョン 8.7 以降のコントローラおよび ME に適用されます。

関連トピック

[ネットワークデバイス（Network Devices）]テーブルからコントローラの一般システム プロパティを変更する （608 ページ）
デバイスの 802.11 パラメータの設定 （720 ページ）

コントローラへの 802.1X 認証の設定

Lightweight アクセス ポイントとスイッチ間の 802.1X 認証を設定できます。アクセス ポイントは 802.1X サプリカントとして動作し、EAP-FAST と匿名 PAC プロビジョニングを使用してスイッチにより認証されます。すべてのアクセス ポイントがコントローラ接続時に継承するグローバル認証を設定できます。これには、コントローラに現在接続されているすべてのアクセス ポイント、および今後接続されるすべてのアクセス ポイントが含まれます。

必要に応じて、このグローバル認証設定よりも優先される、独自の認証設定を特定のアクセスポイントに割り当てることができます。

グローバル サプリカント クレデンシャルを有効にするには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）]** を選択し、左側の [デバイス グループ（Devices Groups）] メニューから [デバイス タイプ（Device Type）] > [ワイヤレス コントローラ（Wireless Controller）] を選択します。

ステップ 2 目的のコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、[System] > [AP 802.1X Supplicant Credentials] の順に選択します。

ステップ 4 [Global Supplicant Credentials] チェックボックスをオンにします。

ステップ 5 サプリカント ユーザ名を入力します。

ステップ 6 適切なパスワードを入力して確定します。

ステップ 7 ドロップダウン メニューから [サプリカントEAPタイプ（Supplicant EAP Type）] を選択します。

（注） バージョン 8.7 以降のコントローラおよび ME に適用されます。

関連トピック

[ネットワークデバイス（Network Devices）]テーブルからコントローラの一般システム プロパティを変更する （608 ページ）
デバイスの 802.11 パラメータの設定 （720 ページ）

コントローラでの DHCP の設定

コントローラの DHCP（Dynamic Host Configuration Protocol）情報を設定するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Devices Groups）] メニューから [デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）] を選択します。

ステップ 2 目的のコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、[System] > [DHCP] の順に選択します。

ステップ 4 次のパラメータを追加または変更します。

- [DHCP オプション 82 リモート ID フィールドのフォーマット（DHCP Option 82 Remote Id Field Format）]：ドロップダウン リストから [AP-MAC]、[AP-MAC-SSID]、[AP-ETHMAC]、または [AP-NAME-SSID] を選択します。

Ap-Mac を選択した場合に [DHCP オプション 82（DHCP option 82）] の [RemoteID] フィールドにフォーマットを設定するには、RemoteID フォーマットを *AP-Mac* として設定します。Ap-Mac-ssid を選択した場合、RemoteID フォーマットは [*AP-Mac:SSID*] に設定します。

- [DHCP Proxy]：プロキシで DHCP を有効にする場合は、このチェックボックスをオンにします。

DHCP プロキシがコントローラ上で有効になっている場合は、コントローラによってクライアントから設定済みサーバへDHCP要求がユニキャストされます。そのため、少なくとも1つのDHCPサーバが、WLANにアソシエートされたインターフェイスか WLAN 自体で設定されている必要があります。

ステップ 5 [DHCP Timeout] を秒単位で入力します。この時間を過ぎると DHCP 要求がタイムアウトします。デフォルト設定は 5 です。有効値の範囲は 5 ～ 120 秒です。DHCP タイムアウトは、リリース 7.0.114.74 以降のコントローラで適用されます。

ステップ 6 [Save] をクリックします。

保存後に、[監査（Audit）] をクリックして、このコントローラで監査を実行できます。

関連トピック

[ネットワークデバイス（Network Devices）]テーブルからコントローラの一般システム プロパティを変更する （608 ページ）

障害検出時間を短縮するコントローラの拡張タイマーの設定

Prime Infrastructure のコントローラには、FlexConnect およびローカル モード用の拡張タイマー設定を使用できます。

この機能は、リリース 6.0 以降のコントローラのみでサポートされています。

拡張タイマーを設定するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）]** を選択し、左側の [デバイス グループ（Devices Groups）] メニューから [デバイス タイプ（Device Type）] > [ワイヤレス コントローラ（Wireless Controller）] を選択します。

ステップ 2 タイマーを設定するコントローラを選択します。

ステップ 3 左側のサイドバーのメニューから、[System] > [AP Timers] の順に選択します。

ステップ 4 [AP タイマー（AP Timers）] ページで、該当するアクセス ポイント モードのリンク（[ローカル モード（Local Mode）] または [FlexConnect モード（FlexConnect Mode）]）をクリックします。

ステップ 5 この選択に応じて、[Local Mode AP Timer Settings] ページまたは [FlexConnect Mode AP Timer Settings] ページで必要なパラメータを設定します。

- ローカルモードの AP タイマー設定の場合、障害検出時間を短縮するには、高速ハートビート間隔（コントローラとアクセス ポイントの間）に設定するタイムアウト値をより小さくします。高速ハートビート タイマーの期限（ハートビート間隔ごとの）を過ぎると、アクセス ポイントは最後のインターバルでコントローラからデータ パケットを受信したかどうかを判断します。パケットが何も受信されていない場合、アクセス ポイントは高速エコー要求をコントローラへ送信します。この場合、10 ～ 15 秒の値を入力できます。
- [FlexConnect 用の AP タイマー設定（AP timer settings for FlexConnect）] : 選択すると、FlexConnect タイムアウト値を設定できます。[AP Primary Discovery Timeout] チェックボックスをオンにして、タイムアウト値を有効にします。30 ～ 3600 秒の値を入力します。5500 シリーズ コントローラは、1 ～ 10 の範囲のアクセス ポイント高速ハートビート タイマー値を受け入れます。

ステップ 6 [Save] をクリックします。

関連トピック

コントローラでの WLAN の作成 （652 ページ）

コントローラでの WLAN の作成

コントローラは 512 WLAN 設定をサポートできるため、Prime Infrastructure は、特定のコントローラに対して、指定した時刻に複数の WLAN を有効または無効にする効率的な方法を提供します。

ネットワーク上に設定した Wireless Local Access Network（WLAN）のサマリーを表示するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、**[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[WLAN（WLANs）] > [WLANの設定（WLAN Configuration）]** を選択します。

ステップ 4 [WLAN サマリーの設定（Configure WLAN Summary）] ページの必須フィールドを設定します。

関連トピック

コントローラで構成されている WLAN の表示 （652 ページ）
コントローラ上の WLAN へのセキュリティ ポリシーの追加 （653 ページ）
コントローラでのモバイル コンシェルジュ（802.11u）の設定 （654 ページ）
コントローラへの WLAN の追加 （657 ページ）
コントローラからの WLAN の削除 （657 ページ）
コントローラの WLAN の管理ステータスを変更する （658 ページ）
コントローラ WLAN のモビリティ アンカーの表示 （659 ページ）
コントローラの WLAN AP グループの設定 （663 ページ）

コントローラで構成されている WLAN の表示

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 WLAN 設定を表示するワイヤレス コントローラのデバイス名をクリックします。

ステップ 3 [Configuration] タブをクリックします。

ステップ 4 [機能（Features）] で **[WLAN（WLANs）] > [WLAN の設定（WLAN Configuration）]** を選択します。[WLAN Configuration] 要約ページに、コントローラで現在設定されている WLAN のリストが表示されます。リストには次の各項目が含まれます。

- WLAN ID

- WLAN 設定プロファイルの名前
- WLAN SSID
- アクティブなセキュリティ ポリシーの名前
- WLAN の現在の管理ステータス（有効または無効）
- 現在スケジュール設定されているすべての WLAN 設定タスクのリストへのリンク

ステップ 5 WLAN 設定の詳細を表示するには、**WLAN ID** をクリックします。[WLAN Configuration] 詳細ページが表示されます。

ステップ 6 タブ（[General]、[Security]、[QoS]、[Advanced]）を使用して、WLAN のパラメータを表示または編集します。パラメータを変更した場合は、[保存（Save）] をクリックします。

関連トピック

コントローラ上の WLAN へのセキュリティ ポリシーの追加 （653 ページ）
コントローラでのモバイル コンシェルジュ（802.11u）の設定 （654 ページ）
コントローラへの WLAN の追加 （657 ページ）
コントローラからの WLAN の削除 （657 ページ）
コントローラの WLAN の管理ステータスを変更する （658 ページ）
コントローラ WLAN のモビリティ アンカーの表示 （659 ページ）

コントローラ上の WLAN へのセキュリティ ポリシーの追加

ステップ 1 「コントローラで構成されている WLAN の表示」で説明されているように、[WLANの設定（WLAN Configuration）] 詳細ページに移動します。

ステップ 2 [ポリシーマッピング（Policy Mappings）] タブをクリックします。

ステップ 3 [行の追加（Add Row）] 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、WLAN にマッピングするポリシー名を選択します。

ステップ 5 プライオリティを入力します。プライオリティの範囲は、1 ～ 16 です。

2 つのポリシーに同じプライオリティを設定することはできません。

ステップ 6 [Save] をクリックします。

ポリシーを削除するには、削除するポリシーに対応するチェックボックスをオンにして [Delete] をクリックします。

関連トピック

コントローラで構成されている WLAN の表示 （652 ページ）
コントローラでのモバイル コンシェルジュ（802.11u）の設定 （654 ページ）
コントローラへの WLAN の追加 （657 ページ）

コントローラからの WLAN の削除 （657 ページ）
コントローラの WLAN の管理ステータスを変更する （658 ページ）
コントローラ WLAN のモビリティ アンカーの表示 （659 ページ）

コントローラでのモバイルコンシェルジュ（802.11u）の設定

シスコ モバイル コンシェルジュは、事前認証を行わずに外部ネットワークで相互運用できるように 802.1X 対応クライアントを有効にするソリューションです。モバイル コンシェルジュは、クライアントにサービスのアベイラビリティに関する情報を提供します。これにより、クライアントは使用可能なネットワークに、よりすばやく、簡単かつ安全にアソシエートできます。

ネットワークから提供されるサービスは、次の 2 つのプロトコルに大きく分類できます。

- 802.11u MSAP
- 802.11u HotSpot 2.0

モバイル コンシェルジュには、次のガイドラインと制限事項が適用されます。

- モバイル コンシェルジュは FlexConnect アクセス ポイントではサポートされません。
- 802.11u 設定アップロードはサポートされません。設定のアップグレードを実行し、設定をコントローラにアップロードすると、WLAN の HotSpot の設定は失われます。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、**[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 モバイル コンシェルジュを設定するワイヤレス コントローラのデバイス名をクリックします。

ステップ 3 [Configuration] タブをクリックします。

ステップ 4 [機能（Features）] で **[WLAN（WLANs）] > [WLAN の設定（WLAN Configuration）]>** を選択します。[WLAN Configuration] 要約ページに、コントローラで現在設定されている WLAN のリストが表示されます。

ステップ 5 モバイル コンシェルジュを設定する WLAN の WLAN ID をクリックします。

ステップ 6 [Hot Spot] タブをクリックします。

ステップ 7 [802.11u Configuration] サブタブをクリックし、次のようにフィールドを設定します。

a) [802.11u Status] チェックボックスをオンにして WLAN の 802.11u を有効にします。

b) [Internet Access] チェックボックスをオンにして、この WLAN からインターネット サービスを提供できるようにします。

c) [Network Type] ドロップダウン リストから、この WLAN に設定する 802.11u サービスに適した説明を選択します。次のオプションを使用できます。

- **Private Network**
- **Private Network with Guest Access**

- **Chargeable Public Network**
- **Free Public Network**
- **Emergency Services Only Network**
- **Personal Device Network**
- **Test or Experimental**
- **Wildcard**

d) このネットワークの 802.11u パラメータ用に設定する認証タイプを選択します。

- Not configured
- Acceptance of Terms and Conditions
- Online Enrollment
- DNS Redirection
- HTTP/HTTPS Redirection

e) [HESSID] フィールドに、Homogeneous Extended Service Set Identifier 値を入力します。HESSID は、HESS を識別する 6 オクテットの MAC アドレスです。

f) [IPv4 Address Type] フィールドで、IPv4 アドレスの割り当て方式を選択します。

- **Not Available**
- **パブリック**
- **Port Restricted**
- **Single NAT Private**
- **Double NAT Private**
- **Port Restricted and Single NAT Private**
- **Port Restricted and Double NAT Private**
- **不明**

g) [IPv6 Address Type] フィールドで、IPv6 アドレスの割り当て方式を選択します。

- **Not Available**
- **応対可**
- **不明**

ステップ 8 [Others] サブタブをクリックし、次のようにフィールドを設定します。

a) [OUI List] グループ ボックスで、[Add Row] をクリックして次の詳細情報を入力します。

- OUI name
- Is Beacon
- [OUI インデックス（OUI Index）]

[Save] をクリックすると、OUI（組織固有識別子）エントリがこの WLAN に追加されます。

b) [Domain List] グループ ボックスで、[Add Row] をクリックして次の詳細情報を入力します。

- [Domain Name]：802.11 アクセス ネットワークで稼働するドメイン名。
- [Domain Index]：ドロップダウン リストからドメイン インデックスを選択します。

[Save] をクリックすると、ドメイン エントリがこの WLAN に追加されます。

c) [Cellular] セクションで、[Add Row] をクリックして次の詳細情報を入力します。

- [Country Code]：3 文字のセルラー国コード。
- [Network Code]：3 文字のセルラー ネットワーク コード。

[Save] をクリックすると、セルラー エントリがこの WLAN に追加されます。

ステップ 9 [Realm] サブタブをクリックし、次のようにフィールドを設定します。

a) [Add Row] をクリックしてレルム名を入力します。
b) [Save] をクリックすると、レルム エントリがこの WLAN に追加されます。

ステップ 10 [Service Advertisements] サブタブをクリックし、次のようにフィールドを設定します。

a) [MSAP Enable] チェックボックスをオンにし、サービス アドバタイズメントを有効にします。
b) MSAP を有効にする場合は、この WLAN のサーバインデックスを入力します。サーバのインデックス フィールドによって、BSSID を使用して到達可能である場所を提供する MSAP サーバインスタンスを一意に識別します。

MSAP（Mobility Services Advertisement Protocol）は、ネットワーク接続を確立するためのポリシー セットを使用して設定されたモバイル デバイスで主に使用するために設計されています。これらのサービスは、上位層サービスを提供するデバイス、つまりサービス プロバイダー経由で有効にされるネットワーク サービス向けです。サービス アドバタイズメントは、MSAP を使用して、Wi-Fi アクセス ネットワークへのアソシエーションの前にサービスをモバイル デバイスに提供します。この情報はサービス アドバタイズメントで伝送されます。シングルモードまたはデュアルモード モバイル デバイスは、アソシエーションの前にサービス ネットワークをネットワークにクエリーします。デバイスによるネットワークの検出および選択機能では、ネットワークに join する判断においてサービス アドバタイズメントを使用する場合があります。

ステップ 11 [Hotspot 2.0] サブタブをクリックし、次のようにフィールドを設定します。

a) [HotSpot2 Enable] ドロップダウン リストから [Enable] オプションを選択します。
b) [WAM Metrics] グループ ボックスで、次の項目を指定します。

- [WAN Link Status]：リンク ステータス。有効な範囲は 1 ～ 3 です。
- [WAN SIM Link Status]：対称リンク ステータス。たとえば、アップリンクとダウンリンクに異なる速度または同じ速度を設定できます。
- [Up Link Speed]：アップリンク速度。最大値は 4,194,304 kbps です。
- [Down Link Speed]：ダウンリンク速度。最大値は 4,194,304 kbps です。

c) [Operator Name List] で、[Add Row] をクリックして次の詳細情報を入力します。

- [Operator Name]：802.11 オペレータの名前を指定します。
- [Operator Index]：オペレータ インデックスを選択します。指定できる範囲は 1 ～ 32 です。
- [Language Code]：言語を定義する ISO-14962-1997 エンコード文字列。この文字列は 3 文字の言語コードです。

[Save] をクリックすると、オペレータがリストに追加されます。

d) [Port Config List] で、[Add Row] をクリックして次の詳細情報を入力します。

- [IP Protocol]：有効にしたい IP プロトコル。次のオプションは、ESP、FTP、ICMP、および IKEV2 です。

- [Port No]：この WLAN で有効になっているポート番号。
- [Status]：ポートのステータス。

[Save] をクリックすると、ポート設定がリストに追加されます。

ステップ 12 [Save] をクリックして、モバイル コンシェルジュ設定を保存します。

関連トピック

コントローラで構成されている WLAN の表示 （652 ページ）
コントローラへの WLAN の追加 （657 ページ）
コントローラからの WLAN の削除 （657 ページ）
コントローラの WLAN の管理ステータスを変更する （658 ページ）
コントローラ上の WLAN へのセキュリティ ポリシーの追加 （653 ページ）
コントローラ WLAN のモビリティ アンカーの表示 （659 ページ）

コントローラへの WLAN の追加

ステップ 1 **[設定（Configuration）] > [テンプレート（Templates）] > [機能およびテクノロジー（Features & Technologies）] > [コントローラ（Controller）] > [WLAN（WLANs）]** [WLANの設定（WLAN Configuration）] の順に選択します。

ステップ 2 テンプレート タイプの横にあるツール チップにマウスのカーソルを合わせ、[New] をクリックします。

ステップ 3 [General]、[Security]、[QoS]、[Advanced]、[HotSpot]、[Policy Mappings] タブで必須フィールドに値を入力し、[Save as New Template] をクリックします。

ステップ 4 [展開（Deploy）] をクリックして、テンプレートの展開を続行します。

関連トピック

コントローラで構成されている WLAN の表示 （652 ページ）
コントローラでのモバイル コンシェルジュ（802.11u）の設定 （654 ページ）
コントローラからの WLAN の削除 （657 ページ）
コントローラの WLAN の管理ステータスを変更する （658 ページ）
コントローラ上の WLAN へのセキュリティ ポリシーの追加 （653 ページ）
コントローラ WLAN のモビリティ アンカーの表示 （659 ページ）
コントローラの WLAN AP グループの設定 （663 ページ）

コントローラからの WLAN の削除

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）] を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバー メニューから、**[WLAN（WLANs）] > [WLANの設定（WLAN Configuration）]** の順に選択します。

ステップ 4 削除する WLAN のチェックボックスをオンにします。

ステップ 5 **[コマンドの選択（Select a Command）] > [WLAN の削除（Delete a WLAN）] > [実行（Go）]** を選択します。

ステップ 6 [OK] をクリックして削除を実行します。

関連トピック

コントローラで構成されている WLAN の表示 （652 ページ）
コントローラでのモバイル コンシェルジュ（802.11u）の設定 （654 ページ）
コントローラへの WLAN の追加 （657 ページ）
コントローラの WLAN の管理ステータスを変更する （658 ページ）
コントローラ上の WLAN へのセキュリティ ポリシーの追加 （653 ページ）
コントローラ WLAN のモビリティ アンカーの表示 （659 ページ）

コントローラの WLAN の管理ステータスを変更する

Prime Infrastructure では、特定のコントローラ上で、複数の WLAN のステータスを一度に変更できます。複数の WLAN を選択して、そのステータスが変更される日時を選択できます。

ステップ 1 [Configuration] > [Network] > [Network Devices] を選択し、[Device Type] > [Wireless Controller] を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、[WLANs] > [WLAN Configuration] の順に選択します。

ステップ 4 ステータス変更をスケジュールする WLAN のチェックボックスをオンにします。

ステップ 5 [Select a command] ドロップダウン リストから、[Schedule Status] を選択して [WLAN Schedule Task Detail] ページを開きます。

選択した WLAN は、ページの上部にリストされます。

ステップ 6 スケジュール設定済みタスク名を入力して、このステータス変更スケジュールを特定します。

ステップ 7 ドロップダウン リストから、新しい管理ステータス（[Enabled] または [Disabled]）を選択します。

ステップ 8 スケジュール時刻を、[hours] および [minutes] ドロップダウン リストを使用して選択します。

ステップ 9 カレンダーアイコンをクリックしてスケジュール日を選択するか、テキストボックスに日付を入力します（MM/DD/YYYY 形式）。

ステップ 10 適切な [Recurrence] オプション ボタンを選択して、ステータス変更の頻度を決めます（[Daily]、[Weekly]、または [No Recurrence]）。

ステップ 11 [Submit] をクリックしてステータス変更スケジュールを開始します。

関連トピック

コントローラで構成されている WLAN の表示 （652 ページ）
コントローラでのモバイル コンシェルジュ（802.11u）の設定 （654 ページ）
コントローラへの WLAN の追加 （657 ページ）
コントローラからの WLAN の削除 （657 ページ）
コントローラ上の WLAN へのセキュリティ ポリシーの追加 （653 ページ）
コントローラ WLAN のモビリティ アンカーの表示 （659 ページ）

コントローラ WLAN のモビリティ アンカーの表示

モビリティ アンカーは WLAN のアンカーとして定義されたコントローラです。クライアント（ラップトップなどの 802.11 モバイル ステーション）は、常にいずれかのアンカーに接続しています。

モビリティ アンカーを使用すると、クライアントのネットワーク エントリ ポイントに関係なく、WLAN を単一のサブネットに制限できます。ユーザは企業全体にわたりパブリック WLAN やゲスト WLAN にアクセスできますが、引き続き特定のサブネットに制限されます。また、WLAN は建物の特定のセクション（ロビー、レストランなど）を表すことができるため、ゲスト WLAN で地理的ロード バランシングを実現できます。

クライアントが、WLAN のモビリティ アンカーとして事前設定されているモビリティ グループのコントローラに最初にアソシエートすると、クライアントはローカルでそのコントローラにアソシエートし、クライアントのローカル セッションが作成されます。クライアントは、WLAN の事前設定されたアンカー コントローラにのみアンカーできます。指定された WLAN の場合、モビリティ グループのすべてのコントローラ上で同じセットのアンカー コントローラを設定する必要があります。

クライアントが、WLAN のモビリティ アンカーとして設定されていないモビリティ グループのコントローラに最初にアソシエートすると、クライアントはローカルでそのコントローラにアソシエートし、ローカルセッションがクライアントのために作成され、コントローラは同じモビリティ グループの別のコントローラへ通知されます。その通知に対する回答がない場合、コントローラは WLAN に設定されたいずれかのアンカー コントローラに連絡をとり、ローカルスイッチ上のクライアントに対する外部セッションを作成します。クライアントからのパケットは暗号化され、有線ネットワークに配信されます。クライアントへのパケットは、アンカー コントローラで受信され、EtherIP を使用してモビリティ トンネルを介して外部コントローラへ転送されます。外部コントローラはパケットをカプセル化してクライアントへ転送します。

2000 シリーズ コントローラを WLAN のアンカーとして指定できません。ただし、2000 シリーズ コントローラ上に作成された WLAN に 4100 シリーズ コントローラまたは 4400 シリーズ コントローラをアンカーとして指定できます。

L2TP レイヤ 3 セキュリティ ポリシーは、モビリティ アンカーで設定された WLAN には使用できません。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバー メニューから、**[WLAN（WLANs）] > [WLANの設定（WLAN Configuration）]** の順に選択します。

ステップ 4 [WLAN ID] をクリックして、特定の WLAN のパラメータを表示します。

ステップ 5 [Advanced] タブをクリックします。

ステップ 6 **[モビリティ アンカー（Mobility Anchors）]** リンクをクリックします。Prime Infrastructure に各アンカーの IP アドレスおよび現在のステータス（到達可能など）が表示されます。

関連トピック

コントローラで構成されている WLAN の表示 （652 ページ）
コントローラでのモバイル コンシェルジュ（802.11u）の設定 （654 ページ）
コントローラへの WLAN の追加 （657 ページ）
コントローラからの WLAN の削除 （657 ページ）
コントローラの WLAN の管理ステータスを変更する （658 ページ）
コントローラ上の WLAN へのセキュリティ ポリシーの追加 （653 ページ）

802.11r 高速移行の設定

802.11r 対応の WLAN は、ワイヤレス クライアント デバイスに迅速かつ効果的なローミング環境を提供します。ただし、堅牢で安全なネットワーク情報交換（ビーコンまたはプローブでの応答）における Fast Transition（FT）認証キー管理（AKM）を認識しない従来のデバイスは、802.11r 対応 WLAN に接続できません。

手順

	コマンドまたはアクション	目的
ステップ 1	すべてのワイヤレスコントローラを表示するには、**[設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）]** を選択し、次に **[デバイス タイプ（Device Type）] > [ワイヤレス コントローラ（Wireless Controller）]** を選択します。	
ステップ 2	対応するコントローラの名前をクリックします。	
ステップ 3	左側のサイドバーのメニューから、**[WLAN（WLANs）] > [WLAN 設定（WLAN**	

	コマンドまたはアクション	目的
	configuration）] を選択して [WLAN 設定（WLAN Configuration）] ページにアクセスします。	
ステップ 4	対応する WLAN ID をクリックして、その特定の WLAN のパラメータを表示します。	
ステップ 5	**[セキュリティ（Security）]** > **[レイヤ 2（Layer 2）]** タブをクリックします。	
ステップ 6	[レイヤ 2 セキュリティ（Layer 2 Security）] ドロップダウン リストから、[WPA+WPA2] を選択します。	Fast Transition の認証キー管理パラメータが表示されます。
ステップ 7	[Fast Transition] チェックボックスをオンまたはオフにして、Fast Transition を有効または無効にします。Fast Transition は、Cisco WLC リリース 8.3 以降から新しい WLAN を作成する場合、デフォルトで有効になります。ただし、既存の WLAN は以前のリリースからリリース 8.3 へ Cisco WLC をアップグレードする場合に現在の設定を保持します。	
ステップ 8	[Over the DS] チェックボックスをオンまたはオフにして、分散システム経由の Fast Transition を有効または無効にします。このオプションは、Fast Transition を有効にしたとき、または Fast Transition が適応型の場合のみ指定できます。	
ステップ 9	[再アソシエーション タイムアウト（Reassociation Timeout）] フィールドに、AP へのクライアントの再関連付けの試行がタイムアウトになる秒数を入力します。有効範囲は 1 ～ 100 秒です。	このオプションは、高速移行を有効にした場合だけ使用できます。
ステップ 10	[認証キーの管理（Authentication Key Management）] で、[FT 802.1X] または [FT PSK] を選択します。キーを有効または無効にするには、対応するチェックボックスをオンまたはオフにします。[FT PSK] チェックボックスをオンにした場合は、[PSK 形式（PSK Format）] ドロップダウン リストから [ASCII] または [HEX] を選択して、キー値を入力します。	適応型 Fast Transition が有効になっている場合は、[802.1X] および [PSK] のみを使用できます。
ステップ 11	[保存（Save）] をクリックして設定を保存します。	

Fastlane QoS の設定

Fastlane QoS 機能は、Apple クライアントの場合に、その他のワイヤレス クライアントと比較して Quality of Service（QoS）処理が優れています。この機能は、デフォルトではディセーブルになっています。

（注） この機能は、少数のクライアントが接続されているときのメンテナンス時間にのみ有効または無効にできます。これは、すべての WLAN とネットワークが無効または有効に戻る時にサービスが中断されるためです。

手順

	コマンドまたはアクション	目的
ステップ 1	**[設定（Configuration）]** > **[ネットワーク（Network）]** > **[ネットワークデバイス（Network Devices）]** を選択し、**[デバイスタイプ（Device Type）]** > **[ワイヤレスコントローラ（Wireless Controller）]** を選択します。	
ステップ 2	対応するコントローラの名前をクリックします。	
ステップ 3	左側のサイドバー メニューから、**[WLAN（WLANs）]** > **[WLANの設定（WLAN Configuration）]** の順に選択します。	
ステップ 4	対応する WLAN ID をクリックして、その特定の WLAN のパラメータを表示します。	
ステップ 5	[QoS] タブをクリックします。	
ステップ 6	Fastlane QoS を有効にするには、[Fastlane] チェックボックスをオンにします。	
ステップ 7	[保存（Save）] をクリックして設定を保存します。	

Fastlane QoS の無効化

（注） Fastlane QoS を無効にする前に、すべての WLAN で Fastlane を無効にする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、**[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。	
ステップ 2	該当するコントローラの [デバイス名（Device Name）] をクリックします。	
ステップ 3	左側のサイドバー メニューから、**[WLAN（WLANs）] > [WLANの設定（WLAN Configuration）]** の順に選択します。	
ステップ 4	[コマンドの選択（Select a command）] ドロップダウン リストから [Fastlane の無効化（Disable Fastlane）] を選択します。	
ステップ 5	[保存（Save）] をクリックして設定を保存します。	

コントローラの WLAN AP グループの設定

サイト固有の VLAN または AP（アクセス ポイント）グループを使用すると、WLAN を異なるブロードキャスト ドメインにセグメント化することができます。これにより、ブロードキャスト ドメインの総数を最小限に抑えられ、より効率的なロード バランシングおよび帯域幅割り当てが可能になります。

ステップ 1 [Configuration] > [Network] > [Network Devices] を選択し、[Device Type] > [Wireless Controller] を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、[WLAN] > [AP Groups] の順に選択します。AP グループの要約ページが表示されます。

このページには、ネットワーク上に設定されている AP グループのサマリーが表示されます。

このページから、AP グループの削除または詳細の表示ができます。

ステップ 4 [Access Points] タブで AP グループ名をクリックして、そのアクセス ポイントを表示または編集します。

ステップ 5 [WLAN Profiles] タブをクリックして、WLAN プロファイルを表示、編集、追加、または削除します。

関連トピック

コントローラの WLAN AP グループの作成 （664 ページ）
コントローラの WLAN AP グループの削除 （666 ページ）
コントローラでの WLAN の作成 （652 ページ）

構成の違いを特定するためのコントローラ WLAN AP グループの監査 （666 ページ）

コントローラの WLAN AP グループの作成

AP（アクセス ポイント）グループを追加するには、[AP グループの詳細（AP Groups detail）] ページを使用します。バージョン 5.2 より前のターゲット コントローラでは、*AP* グループが *AP* グループ *VLAN* と呼ばれることに注意してください。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）] を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[WLAN] > [AP グループ（AP Groups）]** を選択します。

ステップ 4 **[コマンドの選択（Select a command）] > [AP グループの追加（Add AP Groups）] > [実行（Go）]** を選択します。[AP グループの詳細（AP Groups detail）] ページが表示されます。

ステップ 5 次のように、新しい AP グループを作成します。

a) AP グループの名前を入力します。
b) 新しい AP グループの説明を入力します（このグループの説明は任意です）。

ステップ 6 次のように、新しい AP グループにアクセス ポイントを追加します。

a) [Access Points] タブをクリックします。
b) [Add] をクリックします。[Access Point] ページに、使用できるアクセス ポイントのリストが表示されます。
c) 追加するアクセス ポイントのチェックボックスをオンにします。
d) [Select] をクリックします。

ステップ 7 次のように、WLAN プロファイルを追加します。

a) [WLAN Profiles] タブをクリックします。
b) [Add] をクリックします。

使用可能なすべての WLAN プロファイル名を表示するには、テキスト ボックスから現在の WLAN プロファイル名を削除します。テキスト ボックスから現在の WLAN プロファイルの名前を削除すると、使用可能なすべての WLAN プロファイルがドロップダウン リストに表示されます。

各アクセス ポイントは 16 個の WLAN プロファイルに限定されます。各アクセス ポイントは、WLAN override 機能が有効にされない限り、すべての WLAN プロファイルをブロードキャストします。WLAN override 機能によって、アクセス ポイントごとに 16 個の任意の WLAN プロファイルを無効にできます。

WLAN override 機能は、512 WLAN 機能をサポートしていない（最大 512 個の WLAN プロファイルをサポートできる）古いコントローラのみに適用されます。

c) WLAN プロファイル名を入力するか、[WLAN Profile Name] ドロップダウン リストからいずれか 1 つを選択します。

d) インターフェイス/インターフェイス グループを入力するか、[Interface/Interface Group] ドロップダウン リストからいずれか 1 つを選択します。

使用できるすべてのインターフェイスを表示するには、[Interface] テキスト ボックスから現在のインターフェイスを削除します。[Interface] テキスト ボックスから現在のインターフェイスを削除すると、使用可能なすべてのインターフェイスがドロップダウン リストに表示されます。

e) 該当する場合は、[NAC Override] チェックボックスをオンにします。デフォルトでは、NAC の上書きは無効になっています。

f) [Add/Edit] リンクをクリックして、ポリシー設定パラメータを指定します。

- [Policy Name]：ポリシーの名前。
- [Policy Priority]：1 ～ 16 のポリシー プライオリティを設定します。2 個のポリシーが同じプライオリティを持つことはできません。

WLAN 1 つあたり 16 のポリシー マッピングのみが許可されます。マッピングに選択されたポリシー テンプレートは、コントローラにポリシーがない場合に最初に適用されます。

g) アクセス ポイントおよび WLAN プロファイルを追加したら、[Save] をクリックします。

ステップ 8 （任意）次のように、RF プロファイルを追加します。

a) [RF Profiles] タブをクリックします。

b) 次のようにフィールドを設定します。

- [802.11a]：802.11a 無線の AP 用の RF プロファイルを選択します。
- [802.11b]：802.11b 無線の AP 用の RF プロファイルを選択します。

ステップ 9 Hyperlocation 設定パラメータは、次のように追加します。

- [ロケーション設定（Location Settings）] タブをクリックし、次の項目を設定します。
  - [Hyperlocation]：このオプションを有効にすると、そのコントローラに関連付けられた Hyperlocation モジュールがあるすべての AP が有効になります。
  - [Packet Detection RSSI Minimum]：この値を調整して、位置計算から精度の低い RSSI 測定値を除外します。
  - [Scan Count Threshold for Idle Client Detection]：スキャン中に検出されるアイドル クライアントの最大許容数。
  - [NTP Server IP Address]：有効な NTP サーバの IP アドレスを入力します。この IP アドレスは、時刻同期のためにすべての AP で使用されます。

ステップ 10 新しい AP グループへの AP、WLAN プロファイル、RF プロファイルの追加が終了したら、[保存（Save）] をクリックします。

AP グループの WLAN インターフェイス マッピングを変更すると、このグループの FlexConnect AP のローカル VLAN マッピングが削除されます。これらのマッピングは、この変更を適用した後に再度設定する必要があります。

関連トピック

コントローラの WLAN AP グループの設定 （663 ページ）

コントローラの WLAN AP グループの削除 （666 ページ）
構成の違いを特定するためのコントローラ WLAN AP グループの監査 （666 ページ）

コントローラの WLAN AP グループの削除

ステップ 1 [Configuration] > [Network] > [Network Devices] を選択し、[Device Type] > [Wireless Controller] を選択します。
ステップ 2 該当するコントローラのデバイス名をクリックします。
ステップ 3 左側のサイドバーのメニューから、[WLAN] > [AP Groups] の順に選択します。
ステップ 4 削除する AP グループのチェックボックスをオンにします。
ステップ 5 [Select a command] > [Delete AP Groups] > [Go] の順に選択します。
ステップ 6 [OK] をクリックして、削除を実行します。

関連トピック

コントローラの WLAN AP グループの設定 （663 ページ）
コントローラの WLAN AP グループの作成 （664 ページ）
構成の違いを特定するためのコントローラ WLAN AP グループの監査 （666 ページ）

構成の違いを特定するためのコントローラ WLAN AP グループの監査

Prime Infrastructure が AP グループについて保存した値と、現在のコントローラおよびアクセスポイントのデバイス設定に保存されている実際の値の間で違いが生じる可能性があります。AP グループを監査することで、相違が生じているかどうかを特定して解決することができます。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）] を選択します。
ステップ 2 該当するコントローラのデバイス名をクリックします。
ステップ 3 左側のサイドバーのメニューから、[WLAN] > [AP Groups] の順に選択します。
ステップ 4 監査するアクセス ポイント グループの名前をクリックします。
ステップ 5 [Audit] をクリックします。

[Audit] ボタンは、ページ下部の [Save] ボタンと [Cancel] ボタンの横にあります。

関連トピック

コントローラの WLAN AP グループの作成 （664 ページ）
コントローラの WLAN AP グループの削除 （666 ページ）

コントローラでの WLAN の作成 （652 ページ）

キャプティブ ポータル バイパスに関する情報

キャプティブ ポータルは、ユーザがネットワークに接続したときにリダイレクトされる Web ページです。通常は、利用規約に関する情報が表示され、ログインにも使用されます。認証 WISPr は、ユーザが異なるワイヤレス サービス プロバイダー間をローミングできるようにするドラフト プロトコルです。一部のデバイス（Apple iOS デバイスなど）には、指定の URL に対する HTTP WISPr 要求に基づいて、デバイスがインターネットに接続するかどうかを決定するときに使用するメカニズムが搭載されています。このメカニズムは、インターネットへの直接接続が不可能なときにデバイスが自動的に Web ブラウザを開くために使用されます。これにより、ユーザがインターネットにアクセスするために、自身の認証情報を提供することが可能となります。実際の認証は、デバイスが新しい SSID に接続するたびにバックグラウンドで実行されます。

クライアント デバイス（Apple IOS デバイス）は、WISPr 要求をコントローラに送信します。コントローラはユーザ エージェントの詳細をチェックし、コントローラでの Web 認証代行受信により HTTP 要求をトリガーします。ユーザ エージェントによって提供される IOS バージョンおよびブラウザの詳細の確認後に、コントローラによってクライアントはキャプティブ ポータル設定のバイパスを許可され、インターネットにアクセスできます。

この HTTP 要求は、他のページ要求がワイヤレス クライアントによって実行されると、コントローラでの Web 認証代行受信をトリガーします。この代行受信によって Web 認証プロセスが発生し、プロセスは正常に完了します。Web 認証がいずれかのコントローラ スプラッシュ ページ機能で使用されていると（設定された RADIUS サーバが URL を指定）、WISPr 要求が非常に短い間隔で発信されるので、スプラッシュ ページが表示されることはなく、いずれかのクエリーが指定のサーバに到達できるとただちに、バックグラウンドで実行されている Web リダイレクションまたはスプラッシュ ページ表示プロセスが中断されます。そして、デバイスによってページ要求が処理され、スプラッシュ ページ機能は中断されます。たとえば、Apple は iOS 機能を導入して、キャプティブ ポータルがある場合のネットワーク アクセスを容易にしました。この機能では、ワイヤレス ネットワークへの接続に関する Web 要求を送信することにより、キャプティブ ポータルの存在を検出します。この要求は、Apple IOS バージョン 6 以前の場合は http://www.apple.com/library/test/success.html に、Apple IOS バージョン 7 以降の場合は複数の該当するターゲット URL に送られます。応答が受信されると、インターネット アクセスが使用可能であると見なされ、それ以上の操作は必要ありません。応答が受信されない場合、インターネット アクセスはキャプティブ ポータルによってブロックされたと見なされ、Apple の Captive Network Assistant（CNA）が疑似ブラウザを自動起動して管理ウィンドウでポータル ログインを要求します。ISE キャプティブ ポータルへのリダイレクト中に、CNA が切断される場合があります。コントローラは、この疑似ブラウザがポップアップ表示されないようにします。

現在、WISPr 検出プロセスをバイパスするようにコントローラを設定できるようになりました。それによって、ユーザが、ユーザ コンテキストでスプラッシュ ページ ロードを引き起こす Web ページを要求したときに、バックグラウンドで WISPr 検出を実行せずに、Web 認証代行受信だけが行われるようにすることができます。

キャプティブ ネットワーク ポータル バイパスの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**[設定（Configuration）]** > **[ネットワーク（Network）]** > **[ネットワークデバイス（Network Devices）]** を選択し、**[デバイスタイプ（Device Type）]** > **[ワイヤレスコントローラ（Wireless Controller）]** を選択します。	
ステップ 2	デバイス名をクリックして [Configuration] タブをクリックします。	
ステップ 3	**[システム（System）]** > **[一般 - システム（General - System）]** を選択して、[一般（General）] ページにアクセスします。	
ステップ 4	[キャプティブネットワークアシスタント（Captive Network Assistant）]バイパス ドロップダウンリストから、[有効（Enable）] を選択します。	

WLAN ごとのキャプティブ ネットワーク ポータル バイパスの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**[設定（Configuration）]** > **[ネットワーク（Network）]** > **[ネットワークデバイス（Network Devices）]** を選択し、**[デバイスタイプ（Device Type）]** > **[ワイヤレスコントローラ（Wireless Controller）]** を選択します。	
ステップ 2	デバイス名をクリックします。	
ステップ 3	左側のサイドバーのメニューから、**[WLAN（WLANs）]** > **[WLAN 設定（WLAN Configuration）]** を選択します。	
ステップ 4	[WLAN ID] をクリックします。	
ステップ 5	**[セキュリティ（Security）]** > **[レイヤ 3（Layer 3）]** タブをクリックしてデフォルトのセキュリティ ポリシーを変更します。	
ステップ 6	[キャプティブネットワークアシスタント（Captive Network Assistant）]バイパス ドロップダウンリストから、[有効（Enable）] を選択します。	

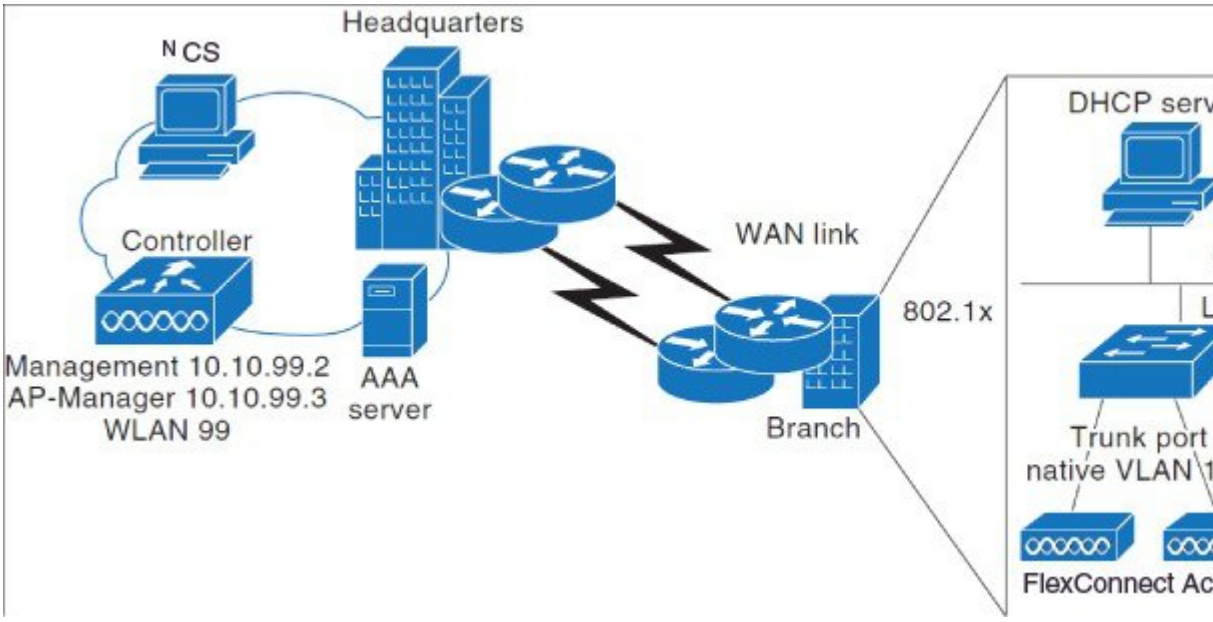
	コマンドまたはアクション	目的
ステップ 7	[保存（Save）] をクリックします。	

FlexConnect を使用した AP の設定とモニタ

FlexConnect により、各オフィスにコントローラを導入しなくても、本社オフィスからワイド エリア ネットワーク（WAN）リンク経由で、リモート ロケーションの AP を設定および制御できるようになります。FlexConnect AP は、コントローラへの接続を失うと、クライアント データ トラフィックを切り替えてクライアント認証をローカルで実行します。コントローラに接続されているときには、トラフィックをコントローラに送り返すこともできます。

次の図に、一般的な FlexConnect の導入を示します。

図 *19 : FlexConnect* の導入



関連トピック

FlexConnect がサポートされるデバイス （669 ページ）
FlexConnect の使用時の前提条件 （670 ページ）
FlexConnect が認証を実行する仕組み （671 ページ）
FlexConnect 動作モード：[接続中（Connected）] および [スタンドアロン（Standalone）] （671 ページ）
FlexConnect の状態 （672 ページ）

FlexConnect がサポートされるデバイス

FlexConnect は次のコンポーネントでのみサポートされます。

- 1130AG、1240AG、1142、および 1252 の AP
- Cisco 2000 および 4400 シリーズ コントローラ
- Catalyst 3750G Integrated Wireless LAN Controller スイッチ
- Cisco Wireless Services Module（WiSM）
- サービス統合型ルータ用のコントローラ ネットワーク モジュール

関連トピック

FlexConnect の使用時の前提条件 （670 ページ）
FlexConnect が認証を実行する仕組み （671 ページ）
FlexConnect 動作モード：[接続中（Connected）]および[スタンドアロン（Standalone）]（671 ページ）
FlexConnect の状態 （672 ページ）

FlexConnect の使用時の前提条件

FlexConnect の設定時は、次のガイドラインに従います。

- 静的 IP アドレスまたは DHCP アドレスのいずれかを持つ FlexConnect を導入することができます。DHCP サーバがローカルで使用可能になっており、ブート時に AP に IP アドレスを提供できる必要があります。
- 最大伝送単位（MTU）は、少なくとも 500 バイトにする必要があります。
- ラウンドトリップ遅延は、AP とコントローラ間で 300 ミリ秒を超えないようにする必要があります。ラウンドトリップ遅延を 300 ミリ秒以下に抑えられない場合は、ローカル認証を実行するよう AP を設定します。
- コントローラは、ユニキャスト パケットまたはマルチキャスト パケットの形式でマルチキャスト パケットを AP に送信できます。FlexConnect モードでは、AP はユニキャスト形式でのみマルチキャスト パケットを受信できます。
- FlexConnect は CCKM 完全認証をサポートしますが、CCKM 高速ローミングをサポートしません。
- FlexConnect は、真のマルチキャストを除くすべての機能に対して、1 対 1 ネットワーク アドレス変換（NAT）設定とポート アドレス変換（PAT）をサポートします。NAT 境界を越えるマルチキャストもサポートされます（ユニキャスト オプションを使用して設定されている場合）。
- VPN、IPsec、L2TP、PPTP、Fortress 認証、および Cranite 認証は、これらのセキュリティ タイプが AP でローカルにアクセス可能である場合、ローカル スイッチングのトラフィックに対してサポートされます。
- NAC アウトオブバンド統合がサポートされるのは、WLAN が FlexConnect の中央スイッチングを行うように設定されている場合だけです。FlexConnect のローカル スイッチングを行うように設定されている WLAN での使用はサポートされていません。
- FlexConnect AP の場合、FlexConnect ローカル スイッチングが設定されている WLAN のコントローラでのインターフェイス マッピングは、デフォルト VLAN タギングとして AP で継承されます。これは SSID ごと、FlexConnect AP ごとに簡単に変更できます。FlexConnect 以外の AP では、すべてのトラフィックがトンネルを通じてコントローラに戻され、VLAN タギングは WLAN の各インターフェイス マッピングによって決定されます。

- デフォルトでは、FlexConnect AP で VLAN は有効化されていません。FlexConnect を有効にすると、AP は WLAN に関連付けられた VLAN ID を継承します。この設定は AP で保存され、join response が成功した後に受信されます。デフォルトでは、ネイティブ VLAN は 1 です。VLAN が有効化されているドメインの FlexConnect AP ごとに、ネイティブ VLAN を 1 つ設定する必要があります。設定しないと、AP はコントローラとパケットを送受信できません。クライアントが RADIUS サーバから VLAN を割り当てられている場合、その VLAN はローカル スイッチングの WLAN にアソシエートされます。

関連トピック

FlexConnect が認証を実行する仕組み （671 ページ）

FlexConnect が認証を実行する仕組み

FlexConnect AP は、ブート時にコントローラを検索します。AP はそのコントローラに接続し、コントローラから最新のソフトウェア イメージと設定情報をダウンロードして、無線を初期化します。スタンドアロン モードで使用するために、ダウンロードした設定を不揮発性メモリに保存します。

FlexConnect AP は、次のいずれかの方法でコントローラの IP アドレスを識別します。

- AP が IP アドレスを DHCP サーバから割り当てられている場合、通常の CAPWAP 検出プロセス（レイヤ 3 ブロードキャスト、無線プロビジョニング（OTAP）、DNS、または DHCP オプション 43）によりコントローラを検出します。OTAP は AP の初回ブート時には動作しません。
- AP が静的 IP アドレスを割り当てられている場合、DHCP オプション 43 を除く CAPWAP 検出プロセスのいずれかのメソッドを使用してコントローラを検出します。AP がレイヤ 3 ブロードキャストでも OTAP でもコントローラを検出できない場合は、DNS 解決を使用することを推奨します。DNS を使用すれば、静的 IP アドレスを持ち DNS サーバを認識している AP は、最低 1 つのコントローラを見つけることができます。
- AP で CAPWAP 検出メカニズムを使用できないリモート ネットワークからコントローラを検出させる場合には、プライミングを使用できます。この方法を使用すると、AP の接続先のコントローラを（AP のコマンドライン インターフェイスにより）指定できます。

関連トピック

FlexConnect がサポートされるデバイス （669 ページ）
FlexConnect の使用時の前提条件 （670 ページ）
FlexConnect 動作モード：[接続中（Connected）] および [スタンドアロン（Standalone）] （671 ページ）
FlexConnect の状態 （672 ページ）

FlexConnect 動作モード：[接続中（Connected）] および [スタンドアロン（Standalone）]

FlexConnect AP の動作モードは次の 2 種類です。

- 接続モード：このモードでは、FlexConnect AP とコントローラが CAPWAP 接続されます。

- スタンドアロン モード：コントローラが到達不能な場合、FlexConnect AP はスタンドアロン モードになり、独自にクライアントを認証します。

FlexConnect AP がスタンドアロン モードになると、以下が実行されます。

-
  - 中央でスイッチされる WLAN 上のすべてのクライアントが関連付けを解除されます。
  - 802.1X または Web 認証 WLAN の場合、既存クライアントは関連付けを解除されませんが、FlexConnect AP は関連付けされたクライアントの数がゼロになると、ビーコンの送信を停止します。
  - 802.1X または Web 認証 WLAN にアソシエートしている新規クライアントにアソシエート解除のメッセージが送信されます。
  - 802.1X 認証、NAC、および Web 認証（ゲスト アクセス）などのコントローラ依存アクティビティが無効になり、AP はコントローラに侵入検知システム（IDS）レポートを送信しません。
  - 無線リソース管理（RRM）機能（ネイバー ディスカバリ、ノイズ、干渉、ロード、およびカバレッジ測定、ネイバー リストの使用、不正阻止および検出など）が無効化されます。ただし、FlexConnect AP ではスタンドアロン モードで動的周波数選択がサポートされています。

FlexConnect AP は、スタンドアロン モードになった後も、クライアントの接続を維持します。ただし、AP がコントローラとの接続を再確立すると、すべてのクライアントを関連付け解除して、コントローラからの新しい設定情報を適用し、クライアントの接続を再度許可します。

AP 上の LED は、デバイスが異なる FlexConnect モードになると変化します。

関連トピック

FlexConnect がサポートされるデバイス （669 ページ）
FlexConnect の使用時の前提条件 （670 ページ）
FlexConnect が認証を実行する仕組み （671 ページ）
FlexConnect の状態 （672 ページ）

FlexConnect の状態

FlexConnect WLAN は、コントローラ接続の設定と状態に応じて、次のいずれかの状態になります。

- **中央認証、中央スイッチング**：この状態では、コントローラがクライアント認証を処理し、すべてのクライアント データはトンネルを通じてコントローラに戻されます。この状態は、接続済みモードの場合にだけ有効です。
- **中央認証、ローカル スイッチング**：この状態では、コントローラがクライアント認証を処理し、FlexConnect AP がデータ パケットをローカルにスイッチします。この状態は、FlexConnect AP が接続モードの場合にのみサポートされます。
- **ローカル認証、ローカル スイッチング**：この状態では、FlexConnect AP がクライアント認証を処理し、クライアント データ パケットをローカルにスイッチします。AP 自体で認証できるため、遅延要件が軽減されます。ローカル認証は、ローカル スイッチング モード

の FlexConnect AP の WLAN でのみ有効にできます。この状態はスタンドアロン モードおよび接続モードで有効です。

ローカル認証は、次の条件を満たすことができない場合に役立ちます。

- • 128 kbps の最小帯域幅。
  • 100 ms 以下のラウンドトリップ遅延。
  • 500 バイト以上の最大伝送単位（MTU）。

ローカル認証は次をサポートしません。

- • ゲスト認証。
  • RRM 情報。
  • ローカル RADIUS。
  • グループ内の WLC およびその他の FlexConnect AP でクライアント情報が更新される前のローミング。

- **認証ダウン、スイッチング ダウン**：この状態になると、WLAN は既存クライアントのアソシエートを解除し、ビーコン応答とプローブ応答の送信を停止します。この状態はスタンドアロン モードでのみ有効です。
- **認証ダウン、ローカル スイッチング**：この状態では、WLAN は新しいクライアントからの認証の試行をすべて拒否しますが、既存クライアントを保持するために、ビーコン応答とプローブ応答の送信は続けます。この状態はスタンドアロン モードでのみ有効です。

FlexConnect AP がスタンドアロン モードになると、WLAN は次の状態になります。

- WLAN がオープン、共有、WPA-PSK、または WPA2-PSK 認証として設定されており、新しいクライアントの認証を続行する場合は、ローカル認証、ローカル スイッチングの状態。
- WLANが中央スイッチングを行うように設定されている場合は、認証ダウン、スイッチング ダウンの状態。
- WLAN がローカル スイッチングを行うように設定されている場合は、認証ダウン、ローカル スイッチングの状態。

関連トピック

FlexConnect がサポートされるデバイス （669 ページ）
FlexConnect の使用時の前提条件 （670 ページ）
FlexConnect が認証を実行する仕組み （671 ページ）
FlexConnect 動作モード：[接続中（Connected）]および[スタンドアロン（Standalone）]（671 ページ）
FlexConnect の設定方法と使用方法：ワークフロー （673 ページ）

FlexConnect の設定方法と使用方法：ワークフロー

FlexConnect を設定するには、この項の手順を次の順序で実行する必要があります。

1. FlexConnect のリモート スイッチの設定

2. FlexConnect 用の中央でスイッチングされる WLAN コントローラの設定
3. FlexConnect 用のローカルでスイッチングされる WLAN コントローラの設定
4. ゲスト アクセス用の中央でスイッチングされる WLAN コントローラの設定
5. AP での FlexConnect の設定
6. クライアント デバイスの WLAN への接続（FlexConnect）

FlexConnect のリモート スイッチの設定

リモート サイトでスイッチを準備するには、次の手順を実行します。

ステップ 1 FlexConnect に有効な AP をトランクに接続するか、またはスイッチ上のポートにアクセスします。

ステップ 2 FlexConnect AP をサポートするようにスイッチを設定します。

関連トピック

例：リモート サイトでスイッチに FlexConnect を設定する （674 ページ）
FlexConnect 用の中央でスイッチングされる WLAN コントローラの設定 （675 ページ）
FlexConnect 用のローカルでスイッチングされる WLAN コントローラの設定 （676 ページ）
ゲスト アクセス用の中央でスイッチングされる WLAN コントローラの設定 （676 ページ）

例：リモート サイトでスイッチに FlexConnect を設定する

この設定例の場合：

- FlexConnect AP は、トランク インターフェイス FastEthernet 1/0/2 に接続され、ネイティブ VLAN 100 を使用します。AP は、このネイティブ VLAN 上での IP 接続を必要とします。
- リモート サイトのローカル サーバとリソースは、VLAN 101 上にあります。
- DHCP プールがスイッチの両 VLAN のローカル スイッチ内に作成されます。
- 最初の DHCP プール（ネイティブ）は FlexConnect AP により使用され、2 つ目の DHCP プール（ローカル スイッチング）は、クライアントがローカルでスイッチされる WLAN に関連付ける場合、クライアントにより使用されます。

この設定例のアドレスは、図示のみを目的としています。使用するアドレスは、アップストリーム ネットワークに適合している必要があります。

```
ip dhcp pool NATIVE
   network 10.10.100.0 255.255.255.0
   default-router 10.10.100.1

!
ip dhcp pool LOCAL-SWITCH
   network 10.10.101.0 255.255.255.0
   default-router 10.10.101.1

!
interface FastEthernet1/0/1
 description Uplink port
 no switchport
 ip address 10.10.98.2 255.255.255.0
```

```
 spanning-tree portfast
!
interface FastEthernet1/0/2
 description the Access Point port
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 100
 switchport trunk allowed vlan 100,101
switchport mode trunk
 spanning-tree portfast
!
interface Vlan100
 ip address 10.10.100.1 255.255.255.0
 ip helper-address 10.10.100.1
!
interface Vlan101
 ip address 10.10.101.1 255.255.255.0
 ip helper-address 10.10.101.1
end
```

関連トピック

FlexConnect のリモート スイッチの設定 （674 ページ）
FlexConnect 用の中央でスイッチングされる WLAN コントローラの設定 （675 ページ）
FlexConnect用のローカルでスイッチングされるWLANコントローラの設定 （676ページ）
ゲストアクセス用の中央でスイッチングされるWLANコントローラの設定 （676ページ）

FlexConnect 用の中央でスイッチングされる WLAN コントローラの設定

中央でスイッチされる WLAN を作成するには、次の手順を実行します。

ステップ 1 [Configuration] > [Network] > [Network Devices] > [Wireless Controllers] を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、[WLAN] > [WLAN Configuration] を選択して [WLAN Configuration] ページにアクセスします。

ステップ 4 [コマンドの選択（Select a command）] ドロップダウン リストから [WLAN の追加（Add a WLAN）] を選択し、[実行（Go）] をクリックします。

Cisco AP はコントローラごとに最大 16 の WLAN をサポートできます。ただし Cisco AP の中には、WLAN ID が 9 以上の WLAN をサポートしないものがあります。この場合、WLAN を作成しようとすると次のメッセージが表示されます。

「*AP* のすべてのタイプが *8* 個より多い *WLAN ID* をサポートするとは限りませんが、続行しますか。（*Not all types of AP support WLAN ID greater than 8, do you wish to continue?*）」

[OK] をクリックすると、次に使用可能な WLAN ID を持つ WLAN が作成されます。

WLAN ID が 8 未満の WLAN が削除されている場合、次に作成する WLAN にその ID が適用されます。

ステップ 5 コントローラに適用するテンプレートをドロップダウン リストから選択します。

新しい WLAN テンプレートを作成する場合は、[Click here] リンクをクリックするとテンプレート作成ページにリダイレクトされます。

ステップ 6 [Layer 2 Security] ドロップダウン リストから [WPA1+WPA2] を選択します。

ステップ 7 [General Policies] の下にある [Status] チェックボックスをオンにして WLAN を有効にします。

NAC が有効で、これで使用する検疫 VLAN を作成済みである場合は、[一般ポリシー（General Policies）] の下にある [インターフェイス（Interface）] ドロップダウン リストから選択してください。また、[AAA オーバーライドを許可する（Allow AAA Override）] チェックボックスをオンにして、コントローラが確実に検疫 VLAN 割り当てを検証するようにします。

ステップ 8 [Save] をクリックします。

関連トピック

FlexConnect のリモート スイッチの設定 （674 ページ）
FlexConnect 用のローカルでスイッチングされる WLAN コントローラの設定 （676 ページ）
ゲスト アクセス用の中央でスイッチングされる WLAN コントローラの設定 （676 ページ）

FlexConnect 用のローカルでスイッチングされる WLAN コントローラの設定

ローカルでスイッチされる WLAN を作成するには、次の手順を実行します。

ステップ 1 「FlexConnect 用の中央でスイッチングされる WLAN コントローラの設定」のステップ 1 ～ 5 の説明に従って、新しい WLAN を作成します。

ステップ 2 WLAN ID をクリックして設定パラメータを変更します。

[Layer 2 Security] ドロップダウン リストから [WPA1+WPA2] を選択します。PSK 認証キー管理を選択し、事前共有キーを入力してください。

ステップ 3 この WLAN の [管理ステータス（Admin Status）] チェックボックスをオンにします。

ステップ 4 [FlexConnect ローカル スイッチング（FlexConnect Local Switching）] チェックボックスをオンにし、ローカル スイッチングを有効にします。

ステップ 5 [保存（Save）] をクリックして変更を確定します。

関連トピック

FlexConnect のリモート スイッチの設定 （674 ページ）
FlexConnect 用の中央でスイッチングされる WLAN コントローラの設定 （675 ページ）
ゲスト アクセス用の中央でスイッチングされる WLAN コントローラの設定 （676 ページ）

ゲスト アクセス用の中央でスイッチングされる WLAN コントローラの設定

ゲスト アクセス用に中央でスイッチされる WLAN を作成し、トンネルを通じてゲスト トラフィックがコントローラに渡されるようにするには、次の手順を実行します。

ステップ 1 「*FlexConnect* 用の中央でスイッチングされる *WLAN* コントローラの設定」のステップ 1 ～ 5 の説明に従って、新しい WLAN を作成します。

ステップ 2 WLAN をクリックして次の設定パラメータを変更します。

a) [セキュリティ（Security）] タブの [レイヤ 2 セキュリティ（Layer 2 Security）] および [レイヤ 3 セキュリティ（Layer 3 Security）] ドロップダウン リストから [なし（None）] を選択します。
b) [Web Policy] チェックボックスをオンにします。
c) [Authentication] を選択します。
d) 外部 Web サーバを使用する場合は、WLAN で事前認証アクセス コントロール リスト（ACL）を設定し、WLAN 事前認証 ACL としてこの ACL を選択します。

ステップ 3 [General Policies] の下にある [Status] チェックボックスをオンにして WLAN を有効にします。

ステップ 4 [Save] をクリックして変更をコミットします。

次のタスク

関連項目

- FlexConnect のリモート スイッチの設定
- FlexConnect 用の中央でスイッチングされる WLAN コントローラの設定
- FlexConnect 用のローカルでスイッチングされる WLAN コントローラの設定
- ゲスト アクセス用の中央でスイッチングされる WLAN コントローラの設定
- （テンプレートの章）

関連トピック

FlexConnect のリモート スイッチの設定 （674 ページ）
FlexConnect 用の中央でスイッチングされる WLAN コントローラの設定 （675 ページ）
FlexConnect用のローカルでスイッチングされるWLANコントローラの設定（676ページ）
コントローラ WLAN の Web 認証の認証タイプを設定する （542 ページ）

中央でスイッチングされる WLAN へのゲストの追加（FlexConnect）

ローカル ユーザを追加するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [テンプレート（Templates）] > [機能およびテクノロジー（Features & Technologies）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 左側のサイドバーのメニューから、**[セキュリティ（Security）] > [AAA] > [ローカルネットユーザ（Local Net Users）]** を選択します。

ステップ 3 必要なフィールドに入力します。

ステップ 4 [プロファイル（Profile）] ドロップダウン リストから、適切な SSID を選択します。

ステップ 5 ゲスト ユーザ アカウントの説明を入力します。

ステップ 6 [新しいテンプレートとして保存（Save as New Template）] をクリックします。

関連トピック

ゲストアクセス用の中央でスイッチングされるWLANコントローラの設定（676ページ）

AP での FlexConnect の設定

FlexConnect に AP を設定するには、次の手順を実行します。

ステップ 1 AP をネットワークに物理的に追加します。

ステップ 2 [設定（Configuration）] > [ワイヤレス テクノロジー（Wireless Technologies）] > [アクセスポイントの無線（Access Point Radios）] を選択します。

ステップ 3 [AP 名（AP Name）] リストから、AP を選択します。

ステップ 4 [設定（Configuration）] > [テンプレート（Templates）] > [Lightweight アクセス ポイント（Lightweight Acess Points）]、または [AP モード（AP Mode）] フィールドに FlexConnect が表示されない場合は [自律型アクセスポイント（Autonomous Access Points）] を選択します。

[AP Mode] フィールドに [FlexConnect] が表示される場合は、ステップ 8 に進みます。

ステップ 5 [AP Name] リストから、AP を選択します。[Lightweight AP Template Detail] ページが表示されます。

ステップ 6 [FlexConnect Mode supported] チェックボックスをオンにして、すべてのプロファイル マッピングを表示します。

モードを FlexConnect に変更する際に、AP がまだ FlexConnect モードでない場合、他のすべての FlexConnect パラメータはその AP に適用されません。

ステップ 7 [VLAN Support] チェックボックスをオンにして、[Native VLAN ID] テキスト ボックスにリモート ネットワーク上のネイティブ VLAN の番号を入力します。

ステップ 8 [Apply/Schedule] タブをクリックして変更を保存します。

ステップ 9 [Locally Switched VLANs] セクションの [Edit] リンクをクリックして、クライアント IP アドレスの取得元となる VLAN の数を変更します。

ステップ 10 [Save] をクリックして変更を保存します。

リモート サイトで FlexConnect に設定する必要があるすべての追加 AP にこの手順を繰り返します。

関連トピック

FlexConnect のリモート スイッチの設定 （674 ページ）
FlexConnect 用の中央でスイッチングされる WLAN コントローラの設定 （675 ページ）
FlexConnect 用のローカルでスイッチングされる WLAN コントローラの設定 （676 ページ）

クライアント デバイスの WLAN への接続（FlexConnect）

次の指示に従って、クライアント デバイスでコントローラの設定時に作成した WLAN に接続するプロファイルを作成します。

例では、クライアント上で 3 つのプロファイルを作成します。

1. 中央でスイッチされる WLAN に接続するには、WPA/WPA2 と PEAP-MSCHAPV2 認証を使用するクライアントプロファイルを作成します。クライアントが認証されると、コントローラの管理 VLAN から IP アドレスが取得されます。

2. ローカルでスイッチされる WLAN に接続するには、WPA/WPA2 認証を使用するクライアント プロファイルを作成します。クライアントが認証されると、ローカル スイッチの VLAN 101 から IP アドレスが取得されます。
3. ゲスト アクセス用の中央でスイッチされる WLAN に接続するには、オープン認証を使用するプロファイルを作成します。クライアントが認証されると、APへのネットワーク ローカル上の VLAN 101 から IP アドレスが取得されます。クライアントが接続されると、ローカル ユーザは任意の HTTP アドレスを Web ブラウザに入力します。Web 認証プロセスを完了するため、コントローラに自動的に誘導されます。Web ログイン ページが表示されたら、ユーザ名とパスワードを入力します。

クライアントのデータ トラフィックがローカル スイッチングか中央スイッチングかを確認するには、[Monitor] > [Devices] > [Clients] の順に選択します。

関連トピック

FlexConnect のリモート スイッチの設定 （674 ページ）
FlexConnect 用の中央でスイッチングされる WLAN コントローラの設定 （675 ページ）
FlexConnect用のローカルでスイッチングされるWLANコントローラの設定 （676ページ）
ゲストアクセス用の中央でスイッチングされるWLANコントローラの設定 （676ページ）

FlexConnect で使用する AP グループの作成

FlexConnect により、各ロケーションにコントローラを導入しなくても、ワイドエリア ネットワーク（WAN）リンク経由で、リモート ロケーションの AP を設定および制御できるようになります。ロケーションごとの FlexConnect AP の数に関する導入制限はありませんが、AP を整理してグループ化できます。

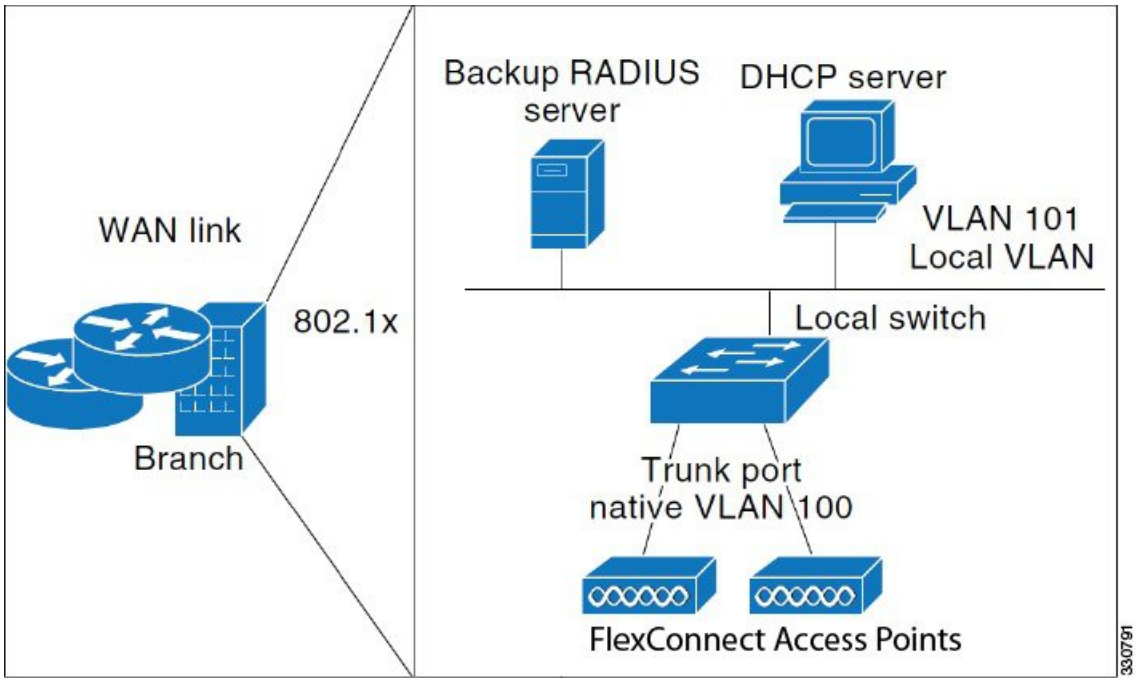
同じ設定で AP グループを作成することによって、個別にコントローラにアクセスするよりも CCKM 高速ローミングなどをより速く処理できます。

たとえば、CCKM 高速ローミングをアクティブにするには、FlexConnect AP が関連付ける可能性のあるすべてのデバイスの CCKM キャッシュを認識している必要があります。300 個の AP と 1000 台のデバイスが接続可能なコントローラを使用している場合は、1000 台のすべてのデバイスにではなく、FlexConnect グループに対して CCKM キャッシュを処理して送信する方が迅速かつ実用的です。ある特定の FlexConnect グループを少数の AP に集中させ、そのグループ内のデバイスがそれらの少数の AP に接続してローミングできるようにすることができます。確立されたグループでは、CCKM キャッシュやバックアップ RADIUS などの機能が各 AP で設定されるのではなく、FlexConnect グループ全体に設定されます。

グループ内のすべての FlexConnect AP は、同じ WLAN、バックアップ RADIUS サーバ、CCKM、およびローカル認証設定情報を共有します。この機能は、複数の FlexConnect AP がリモート オフィスやビルディングのフロアにあり、すべてを一度に設定する場合に役立ちます。たとえば、各 AP に同じサーバを設定する必要なく、FlexConnect グループのバックアップ RADIUS サーバを設定できます。

次の図に、ブランチ オフィスでのバックアップ RADIUS サーバを備えた一般的な FlexConnect グループの展開を示します。

図 *20 : FlexConnect* グループの導入



関連項目

- FlexConnect グループおよびバックアップ RADIUS サーバ
- FlexConnect グループおよび CCKM
- FlexConnect グループおよびローカル認証
- 構成の違いを特定するためのコントローラ FlexConnect AP グループの監査

FlexConnect グループおよびバックアップ RADIUS サーバ

スタンドアロン モードの FlexConnect AP がバックアップ RADIUS サーバに対して完全な 802.1x 認証を実行できるように、コントローラを設定することができます。プライマリ RADIUS サーバを設定することも、プライマリとセカンダリの両方の RADIUS サーバを設定することもできます。

関連項目

- FlexConnect グループおよび CCKM
- FlexConnect グループおよびローカル認証
- 構成の違いを特定するためのコントローラ FlexConnect AP グループの監査

FlexConnect グループおよび CCKM

CCKM 高速ローミングには FlexConnect グループが必要です。CCKM 高速セキュア ローミング用に WLAN を設定した場合、EAP が有効になっているクライアントは、RADIUS サーバで再認証せずに、あるアクセス ポイントから別のアクセス ポイントに安全にローミングを行いま

す。CCKM を使用すると、アクセス ポイントは高速キー再生成技術を使用します。これによりシスコのクライアント デバイスは、アクセス ポイント間のローミングを通常 150 ミリ秒未満で行えます。CCKM 高速セキュア ローミングでは、遅延に敏感なアプリケーションで認識できるほどの遅延が発生しません。FlexConnect アクセス ポイントは、アソシエートする可能性のあるすべてのクライアントに対する CCKM キャッシュ情報を取得します。それにより、CCKM キャッシュ情報をコントローラに送り返さずに、すばやく処理できます。

たとえば、APが300あるコントローラで、アソシエートする可能性のあるクライアントが100台ある場合、100台すべてのクライアントに対してCCKMキャッシュを送信することは現実的ではありません。限られた数の AP で構成される FlexConnect グループを作成すると、クライアントは 4 つの AP 間でのみローミングし、クライアントがそれらのいずれかに関連付けられている場合にのみ、4 つの AP 間で CCKM キャッシュが分散されます。

FlexConnect AP と非 FlexConnect AP 間の CCKM 高速ローミングはサポートされていません。

関連項目

- FlexConnect グループおよびバックアップ RADIUS サーバ
- FlexConnect グループおよびローカル認証
- 構成の違いを特定するためのコントローラ FlexConnect AP グループの監査

FlexConnect グループおよびローカル認証

スタンドアロン モードの FlexConnect AP が、最大 20 人の静的に設定されたユーザに対して LEAP または EAP-FAST 認証を実行できるように、コントローラを設定できます。コントローラは、各FlexConnect APがコントローラに接続した際に、ユーザ名とパスワードの静的リストをその AP に送信します。グループ内の各 AP は、そのアクセス ポイントに関連付けられたクライアントのみを認証します。

この機能は、Autonomous APネットワークからLightweight FlexConnect APネットワークに移行する際に、大きなユーザデータベースを保持したくない場合や、Autonomous APで利用可能なRADIUSサーバ機能を置き換える際に別のハードウェア デバイスを追加したくない場合に適しています。

LEAP または EAP-FAST 認証は、FlexConnect バックアップ RADIUS サーバと組み合わせて使用できます。FlexConnect グループがバックアップ RADIUS サーバとローカル認証の両方で設定されている場合、FlexConnect AP は常に、まずプライマリ バックアップ RADIUS サーバを使用してクライアントの認証を試行します。その後、セカンダリ バックアップ RADIUS サーバで試行し（プライマリに到達できない場合）、最後にFlexConnect AP自身で試行します（プライマリおよびセカンダリの RADIUS サーバに到達できない場合）。

関連項目

- FlexConnect グループおよびバックアップ RADIUS サーバ
- FlexConnect グループおよび CCKM
- 構成の違いを特定するためのコントローラ FlexConnect AP グループの監査

既存の FlexConnect AP グループの表示

既存の FlexConnect AP グループのリストを表示できます。個々の AP が FlexConnect グループに属していることを確認するには、[グループで設定されているユーザ（Users configured in the group）] リンクをクリックします。[FlexConnect AP グループ（FlexConnect AP Group）] ページが開き、グループの名前と、そのグループに属している AP が表示されます。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[FlexConnect] > [FlexConnect APグループ（FlexConnect AP Groups）]** の順に選択します。[FlexConnect AP グループ（FlexConnect AP Groups）] ページが開きます。

ステップ 4 グループ名をクリックして FlexConnect AP グループに関する詳細を表示します。

関連トピック

構成の違いを特定するためのコントローラ WLAN AP グループの監査 （666 ページ）

FlexConnect AP グループの設定

FlexConnect AP グループを設定するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）]** を選択し、左側の [デバイス グループ（Devices Groups）] メニューから [デバイス タイプ（Device Type）] > [ワイヤレス コントローラ（Wireless Controller）] を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[FlexConnect] > [FlexConnect APグループ（FlexConnect AP Groups）]** の順に選択します。

ステップ 4 [コマンドの選択（Select a command）] ドロップダウン リストで、[FlexConnect AP グループの追加（Add FlexConnect AP Group）] をクリックし、[FlexConnect AP グループ（FlexConnect AP Group）] > [テンプレートから追加（Add From Template）] ペインを開きます。

ステップ 5 **[このコントローラに適用するテンプレートを選択する（Select a template to apply to this controller）]** ドロップダウン リストからテンプレートを選択します。

ステップ 6 [Apply] をクリックします。

ステップ 7 必要な FlexConnect AP グループ パラメータを設定します。必要なタブをクリックして、次のマッピングを追加、編集、または削除できます。

- [VLAN-ACL Mapping]：有効な VLAN ID の範囲は 1 ～ 4094 です。
- [WLAN-ACL Mapping]：外部 Web 認証用の FlexConnect アクセス コントロール リストを選択します。最大 16 個の WebAuth ACL を追加できます。

- [WebPolicy ACL]：Web ポリシーとして追加する FlexConnect アクセス コントロール リストを選択します。最大 16 個の Web-Policy ACL を追加できます。
- Local Split
- Central DHCP
  - [Central DHCP]：この機能を有効にすると、AP から受信した DHCP パケットは、コントローラに中央でスイッチされ、AP および SSID に基づいて対応する VLAN に転送されます。
  - [Override DNS]：ローカルでスイッチされる WLAN に割り当てられたインターフェイス上での DNS サーバ アドレスのオーバーライドを有効または無効にできます。中央でスイッチされる WLAN 上で DNS をオーバーライドすると、クライアントは、コントローラからではなく AP から DNS サーバの IP アドレスを取得します。
  - [NAT-PAT]：ローカルでスイッチされる WLAN 上でのネットワーク アドレス変換（NAT）およびポート アドレス変換（PAT）を有効または無効にできます。NAT および PAT を有効にするには、[Central DHCP Processing] を有効にする必要があります。

ステップ 8 個々のアクセス ポイントが FlexConnect グループに属していることを確認するには、[グループに設定されているユーザ（Users configured in the group）] リンクをクリックします。[FlexConnect AP グループ（FlexConnect AP Group）] ページに、グループの名前と、そのグループに属しているアクセス ポイントが表示されます。

ステップ 9 [保存（Save）] をクリックします。

ステップ 10 既存の FlexConnect AP グループを削除するには、削除するグループのチェックボックスをオンにし、[コマンドの選択（Select a command）] ドロップダウン リストから [FlexConnect AP グループの削除（Delete FlexConnect AP Group）] を選択します。

関連トピック

既存の FlexConnect AP グループの表示 （682 ページ）

構成の違いを特定するためのコントローラ FlexConnect AP グループの監査

FlexConnect 設定が Cisco Prime Infrastructure またはコントローラ上で時間とともに変化した場合は、設定を監査できます。変化は、後続の画面に表示されます。Cisco Prime Infrastructure またはコントローラを更新して、設定の同期を選択できます。

関連トピック

FlexConnect AP グループの設定 （682 ページ）
既存の FlexConnect AP グループの表示 （682 ページ）

デフォルト FlexConnect グループ

デフォルト FlexConnect グループは、管理者が設定した FlexConnect グループの一部ではない FlexConnect AP がコントローラに加わると自動的に追加されるコンテナです。デフォルト FlexConnect グループは、コントローラの起動時（以前のリリースからアップグレードした後）

に作成され、保存されます。このグループを手動で追加または削除することはできません。また、デフォルト FlexConnect グループでアクセス ポイントを手動で追加または削除することはできません。デフォルト FlexConnect グループ内の AP は、グループの共通設定を継承します。グループの設定のどれかを変更すると、その変更は、グループ内のすべての AP に反映されます。

管理者が作成したグループが削除されると、そのグループからのすべての AP がデフォルト FlexConnect グループに移動され、このグループの設定を継承します。同様に、他のグループから手動で削除された AP もデフォルト FlexConnect グループに追加されます。

デフォルト FlexConnect グループからの AP がカスタマイズされたグループに追加されると、（デフォルト FlexConnect グループからの）既存の設定が削除され、カスタマイズされたグループの設定が AP にプッシュされます。スタンバイ コントローラがある場合は、デフォルト FlexConnect グループとその設定も同期化されます。

AP がローカルから FlexConnect モードに変換され、管理者が設定した FlexConnect グループの一部でない場合、AP はデフォルト FlexConnect グループの一部になります。

（注） AP イメージを効率的にアップグレードする機能は、デフォルト FlexConnect AP グループではサポートされません。

関連項目

- デフォルトの FlexConnect AP グループから別の FlexConnect グループへの AP の移動
- デフォルト FlexConnect グループ

デフォルトの FlexConnect AP グループから別の FlexConnect グループへの AP の移動

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[FlexConnect] > [FlexConnect APグループ（FlexConnect AP Groups）]** の順に選択します。

ステップ 4 [FlexConnect AP グループ（FlexConnect AP Groups）] からグループ名をクリックします。

ステップ 5 [FlexConnect AP] タブで、[AP の追加（+ Add AP）] をクリックします。[FlexConnect AP の追加（Add FlexConnect AP）] ページに、デフォルト FlexConnect グループの AP が表示されます。

ステップ 6 任意の AP 名を選択し、[追加（Add）] をクリックします。

選択した AP は、自動的に新しいグループに追加され、デフォルト FlexConnect グループから削除されます。

ステップ 7 [保存（Save）] をクリックします。

関連トピック

デフォルト FlexConnect グループ （683 ページ）

FlexConnect AP グループの削除

（注） デフォルト FlexConnect グループは削除できません。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[FlexConnect] > [FlexConnect APグループ（FlexConnect AP Groups）]** の順に選択します。

ステップ 4 グループ名をクリックしてから、[コマンドの選択（Select a Command）] ドロップダウン リストから [FlexConnect AP グループの削除（Delete FlexConnect AP Group）] を選択します。

ステップ 5 [OK] をクリックして削除を実行します。

関連トピック

デフォルト FlexConnect グループ （683 ページ）
FlexConnect を使用した AP の設定とモニタ （669 ページ）

コントローラまたはデバイスのセキュリティ設定の構成

- コントローラの TFTP ファイル暗号化の設定
- コントローラへの AAA セキュリティの設定
- コントローラでのローカル EAP の設定
- コントローラの Web 認証証明書の設定
- コントローラのユーザ ログイン ポリシーの設定
- デバイスの手動で無効化されるクライアントの設定
- コントローラのアクセス コントロール リスト（ACL）の設定
- コントローラ CPU 用の ACL セキュリティの追加
- コントローラの設定済み IDS セキュリティ センサーの表示
- コントローラでの IP Sec CA 証明書の設定
- コントローラでのネットワーク アイデンティティ（ID）証明書の設定
- コントローラでのワイヤレス保護ポリシーの設定

- コントローラでの不正 AP ポリシーの設定
- コントローラでの不正 AP ポリシーの表示
- コントローラでのクライアント除外ポリシーの設定
- コントローラに適用されるシスコが提供する IDS 署名の表示
- カスタム IDS 署名の作成
- コントローラの AP 認証と管理フレーム保護の設定
- アクセス コントロール リストの設定

コントローラへの AAA セキュリティの設定

ここでは、コントローラのセキュリティ AAA パラメータの設定方法について説明します。内容は次のとおりです。

- コントローラの AAA 一般パラメータの設定
- コントローラの AAA RADIUS 認証サーバの表示
- コントローラの AAA RADIUS アカウンティング サーバの表示
- コントローラでの AAA RADIUS フォールバック パラメータの設定
- コントローラでの AAA LDAP サーバの設定
- コントローラでの AAA TACACS サーバの設定 （691 ページ）
- コントローラの AAA ローカル ネット ユーザの表示
- コントローラでの AAA MAC フィルタリングの設定
- コントローラでの AAA AP/MSE 認証の設定
- コントローラでの AAA Web 認証の設定

コントローラの AAA 一般パラメータの設定

[一般（General）] ページでは、コントローラ上のローカル データベース エントリを設定できます。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）]** を選択し、左側の [デバイス グループ（Device Groups）] メニューから [デバイス タイプ（Device Type）] > [ワイヤレス コントローラ（Wireless Controller）] を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[セキュリティ（Security）] > [AAA] > [一般 - AAA（General - AAA）]** を選択します。

ステップ 4 許可されるデータベース エントリの最大数を入力します。有効な範囲は 512 ～ 2048 です。

ステップ 5 [管理ユーザの再認証間隔（Mgmt User Re-auth Interval）] で、管理ユーザを停止する間隔を設定します。

ステップ 6 サーバを再起動して変更を適用します。

関連トピック

コントローラへの AAA セキュリティの設定 （686 ページ）

コントローラの AAA RADIUS 認証サーバの表示

既存の RADIUS 認証サーバのサマリーを表示できます。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[セキュリティ（Security）] > [AAA] > [RADIUS 認証サーバ（RADIUS Auth Servers）]** を選択します。次の RADIUS Auth Servers パラメータが表示されます。

- [Server Index]：RADIUS サーバのアクセス プライオリティ番号（表示のみ）。[Configure IPaddr] > [RADIUS Authentication Server] の順にクリックして移動します。
- [Server Address]：RADIUS サーバの IP アドレス（読み取り専用）。
- [ポート番号（Port Number）]：コントローラのポート番号（読み取り専用）。
- [Admin Status]：[Enabled] または [Disabled]。
- [Network User]：[Enabled] または [Disabled]。
- [Management User]：[Enabled] または [Disabled]。

関連トピック

コントローラへの AAA セキュリティの設定 （686 ページ）
コントローラへの AAA 認証サーバの追加 （687 ページ）

コントローラへの AAA 認証サーバの追加

認証サーバを追加するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[セキュリティ（Security）] > [AAA] > [RADIUS認証サーバ（RADIUS Auth Servers）]** の順に選択します。

ステップ 4 [Select a command] ドロップダウン リストから [Add Auth Server] 選択して、[Radius Authentication Server] > [Add From Template] ページを開きます。

ステップ 5 [Select a template to apply to this controller] ドロップダウン リストからテンプレートを選択します。

ステップ 6 [Apply] をクリックします。

Radius 認証サーバの新しいテンプレートを作成するには、**[設定（Configuration）] > [テンプレート（Templates）] > [機能およびテクノロジー（Features and Technologies）]** を選択します。

関連トピック

コントローラへの AAA セキュリティの設定 （686 ページ）
コントローラの AAA RADIUS アカウンティング サーバの表示 （688 ページ）

コントローラの AAA RADIUS アカウンティング サーバの表示

既存の RADIUS アカウンティング サーバのサマリーを表示するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[セキュリティ（Security）] > [AAA] > [RADIUSアカウンティングサーバ（RADIUS Acct Servers）]** の順に選択します。RADIUS Acct Server パラメータには、次のようなものがあります。

- [Server Index]：RADIUS サーバのアクセス プライオリティ番号（読み取り専用）。クリックして [Radius Acct Servers Details] ページを開きます。
- 現在のアカウンティング サーバのパラメータを編集または監査するには、該当するアカウンティング サーバのサーバ インデックスをクリックします。
- [Server Address]：RADIUS サーバの IP アドレス（読み取り専用）。
- [ポート番号（Port Number）]：コントローラのポート番号（読み取り専用）。
- [Admin Status]：[Enabled] または [Disabled]。
- [Network User]：[Enabled] または [Disabled]。

関連トピック

コントローラへの AAA セキュリティの設定 （686 ページ）
コントローラへの AAA アカウンティング サーバの追加 （688 ページ）

コントローラへの AAA アカウンティング サーバの追加

アカウンティング サーバを追加するには、次の手順を実行します。

ステップ 1 [Configuration] > [Network] > [Network Devices] を選択し、左側の [Device Groups] メニューから [Device Type] > [Wireless Controller] を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、[Security] > [AAA] > [RADIUS Acct Servers] の順に選択します。

ステップ 4 [コマンドの選択（Select a command）] ドロップダウン リストから [アカウンティング サーバの追加（Add Acct Server）] 選択して、[RADIUS アカウンティング サーバの詳細（Radius Acct Servers Details）] > [テンプレートから追加（Add From Template）] ページを開きます。

ステップ 5 [Select a template to apply to this controller] ドロップダウン リストからテンプレートを選択します。

ステップ 6 ドロップダウン リストから、このテンプレートに適用するコントローラを選択します。

ステップ 7 [Apply] をクリックします。

RADIUS アカウンティング サーバの新しいテンプレートを作成するには、[Configuration] > [Templates] > [Features and Technologies] > [Controller] > [Security] > [AAA] > [RADIUS Acct Servers] を選択します。

関連トピック

コントローラへの AAA セキュリティの設定 （686 ページ）
コントローラの AAA RADIUS アカウンティング サーバの表示 （688 ページ）

コントローラからの AAA アカウンティング サーバの削除

アカウンティング サーバを削除するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから [デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）] を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[セキュリティ（Security）] > [AAA] > [RADIUSアカウンティングサーバ（RADIUS Acct Servers）]** の順に選択します。

ステップ 4 該当するアカウンティング サーバのチェックボックスをオンにします。

ステップ 5 [コマンドの選択（Select a command）] ドロップダウン リストから [アカウンティング サーバの削除（Delete Acct Server）] を選択します。

ステップ 6 [Go] をクリックします。

ステップ 7 ポップアップ ダイアログボックスで [OK] をクリックして、削除を確定します。

関連トピック

コントローラへの AAA セキュリティの設定 （686 ページ）
コントローラの AAA RADIUS アカウンティング サーバの表示 （688 ページ）

コントローラでの AAA RADIUS フォールバック パラメータの設定

RADIUS フォールバック パラメータを設定するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから [デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）] を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[セキュリティ（Security）] > [AAA] > [RADIUS フォールバック（RADIUS Fallback）]** を選択します。

ステップ 4 必要な変更を行い、[保存（Save）] をクリックします。

ステップ 5 [監査（Audit）] をクリックして、Cisco Prime Infrastructure およびコントローラの現在の設定ステータスを確認します。

関連トピック

コントローラへの AAA セキュリティの設定 （686 ページ）

コントローラでの AAA LDAP サーバの設定

LDAP サーバをコントローラに追加して削除できます。Prime Infrastructure は、匿名バインドおよび認証済みバインドの両方の LDAP 設定をサポートします。

[LDAP Servers] ページにアクセスするには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから [デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）] を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[セキュリティ（Security）] > [AAA] > [LDAPサーバ（LDAP Servers）]** の順に選択します。

このページには、現在このコントローラが使用している LDAP サーバが表示されます。次のパラメータが含まれます。

- [Check box]：チェックボックスをオンにして、削除する LDAP サーバを選択します。
- [Server Index]：LDAP サーバを識別するために割り当てられた番号。LDAP サーバの設定ページに移動するには、インデックス番号をクリックします。
- [Server Address]：LDAP サーバの IP アドレス。
- [Port Number]：LDAP サーバとの通信に使用されるポート番号。
- [Admin Status]：サーバ テンプレートのステータス。
- LDAP サーバ テンプレートの使用が有効か無効かを示します。

ステップ 4 情報を昇順または降順に並べ替えるには、列のタイトルをクリックします。

関連トピック

コントローラへの AAA セキュリティの設定 （686 ページ）
コントローラでの新しい AAA LDAP バインド要求の設定

コントローラへの AAA LDAP サーバの追加

LDAP サーバを追加するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[セキュリティ（Security）] > [AAA] > [LDAPサーバ（LDAP Servers）]** の順に選択します。

ステップ 4 [Select a command] ドロップダウン リストから [Add LDAP Server] を選択します。

ステップ 5 [Go] をクリックします。

関連トピック

コントローラへの AAA セキュリティの設定 （686 ページ）

コントローラからの AAA LDAP サーバの削除

LDAP サーバを削除するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[セキュリティ（Security）] > [AAA] > [LDAPサーバ（LDAP Servers）]** の順に選択します。

ステップ 4 削除する LDAP サーバのチェックボックスをオンにします。

ステップ 5 [コマンドの選択（Select a command）] ドロップダウン リストから [LDAP サーバの削除（Delete LDAP Servers）] を選択します。

ステップ 6 [移動（Go）] をクリックします。

関連トピック

コントローラへの AAA セキュリティの設定 （686 ページ）

コントローラでの AAA TACACS サーバの設定

コントローラから TACACS+ サーバを削除できます。[TACACS+ サーバ（TACACS+ Servers）] ページにアクセスするには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）]** を選択し、左側の [デバイス グループ（Devices Groups）] メニューから [デバイス タイプ（Device Type）] > [ワイヤレス コントローラ（Wireless Controller）] を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[セキュリティ（Security）] > [TACACS+サーバ（TACACS+ Servers）]** を選択します。

このページには、現在このコントローラが使用している TACACS+ サーバが表示されます。次のパラメータが含まれます。

- [Check box]：チェックボックスをオンにして、削除する TACACS+ サーバを選択します。
- [Server Type]：TACACS+ のサーバ タイプ（アカウンティング、許可、または認証）。
- [Server Index]：TACACS+ サーバを識別し、使用プライオリティを設定するために割り当てられた番号。TACACS+ サーバの設定ページに移動するには、インデックス番号をクリックします。
- [Server Address]：TACACS+ サーバの IP アドレス。
- [Port Number]：TACACS+ サーバとの通信に使用されるポート番号。
- [Admin Status]：サーバ テンプレートのステータス。TACACS+ サーバ テンプレートの使用が有効かを示します。

ステップ 4 [コマンドの選択（Select a command）] ドロップダウン リストから [TACACS+ サーバの削除（Delete TACACS+ Servers）] を選択し、[実行（Go）] をクリックして、選択したチェックボックスのすべての TACACS+ サーバをコントローラから削除します。

ステップ 5 情報を昇順または降順に並べ替えるには、列のタイトルをクリックします。

関連トピック

コントローラへの AAA セキュリティの設定 （686 ページ）

コントローラの AAA ローカル ネット ユーザの表示

特定の WLAN へのアクセスが許可されているクライアントの、既存のローカル ネットワーク ユーザ コントローラのサマリーを表示できます。これは、RADIUS 認証プロセスの管理バイパスです。レイヤ 3 Web 認証を有効にする必要があります。クライアント情報は、まず RADIUS 認証サーバに渡され、クライアント情報が RADIUS データベースのエントリと一致しない場合は、ローカル データベースに対してポーリングが実行されます。RADIUS 認証が失敗した場合、または存在しない場合は、このデータベースで見つかったクライアントがネットワーク サービスへのアクセスを付与されます。

既存のローカル ネットワーク ユーザを表示するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[セキュリティ（Security）] > [AAA] > [ローカル ネット ユーザ（Local Net Users）]** を選択します。[Local Net Users] ページには、次のローカル ネット ユーザ パラメータが表示されます。

- [Username]：ユーザ定義の ID。
- [WLAN ID]：任意の WLAN ID（1 ～ 16）。すべての WLAN の場合は 0、このローカル ネット ユーザがアクセスできるサードパーティ製 WLAN の場合は 17。
- [Description]：オプションのユーザが定義した説明。

関連トピック

コントローラでのローカル EAP の設定 （697 ページ）
コントローラからの AAA ローカル ネット ユーザの削除 （693 ページ）

コントローラからの AAA ローカル ネット ユーザの削除

ローカル ネット ユーザを削除するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから [デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）] を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[セキュリティ（Security）] > [AAA] > [ローカル ネット ユーザ（Local Net Users）]** を選択します。

ステップ 4 該当するローカル ネット ユーザのチェックボックスを選択します。

ステップ 5 [Select a command] ドロップダウン リストから、[Delete Local Net Users] を選択します。

ステップ 6 [Go] をクリックします。

ステップ 7 ダイアログボックスで [OK] をクリックして、削除を確定します。

関連トピック

コントローラへの AAA セキュリティの設定 （686 ページ）

コントローラでの AAA MAC フィルタリングの設定

MAC フィルタ情報を表示できます。ブロードキャスト用の MAC アドレスを使用できません。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから [デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）] を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[セキュリティ（Security）] > [AAA] > [MAC フィルタリング（MAC Filtering）]** を選択します。[MAC Filtering] ページには、次のパラメータが表示されます。

- MAC Filter Parameters
  - [RADIUS Compatibility Mode]：ユーザ定義の RADIUS サーバの互換性（[Cisco ACS]、[FreeRADIUS]、または [Other]）。
  - [MAC Delimiter]：MAC デリミタは、RADIUS サーバの要件に応じて、コロン（xx:xx:xx:xx:xx:xx）、ハイフン（xx-xx-xx-xx-xx-xx）、シングル ハイフン（xxxxxx-xxxxxx）、またはデリミタなし（xxxxxxxxxxxx）に設定できます。
- MAC Filters

- [MAC Address]：クライアント MAC アドレス。クリックして [Configure *IPaddr*] > [MAC Filter] を開きます。
- [WLAN ID]：1 ～ 16。17 = サードパーティ製 AP WLAN、0 = すべての WLAN。
- [Interface]：アソシエートされたインターフェイス名を表示します。
- [Description]：オプションのユーザ定義の説明を表示します。

ステップ 4 [Select a command] ドロップダウン リストから [Add MAC Filters] を選択して MAC フィルタを追加するか、[Delete MAC Filters] を選択してテンプレートを削除するか、[Edit MAC Filter Parameters] を選択して MAC フィルタを編集します。

ステップ 5 [Go] をクリックします。

関連トピック

コントローラへの AAA セキュリティの設定 （686 ページ）

コントローラでの AAA AP/MSE 認証の設定

[AP/MSE Authorization] ページには、アクセス ポイント ポリシーおよび認可されたアクセス ポイントのリストが表示されます。このリストには、アクセスポイントで認可に使用する証明書のタイプも示されます。

ブロードキャスト用の MAC アドレスを使用できません。

[AP/MSE Authorization] ページにアクセスするには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから [デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）] を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[セキュリティ（Security）] > [AAA] > [AP または MSE 認証（AP or MSE Authorization）]** を選択します。[AP/MSE Authorization] ページに次のパラメータが表示されます。

- AP Policies
  - [Authorize APs]：有効または無効。
  - [Accept SSC-APs]：有効または無効。
- AP/MSE Authorization
  - [AP/MSE Base Radio MAC Address]：認可されたアクセス ポイントの MAC アドレス。[AP/MSE Base Radio MAC Address] をクリックすると、AP/MSE 認可の詳細が表示されます。
  - タイプ
  - [Certificate Type]：MIC または SSC。
  - [Key Hash]：40 文字の長さの 16 進数 SHA1 キー ハッシュ。キー ハッシュは、証明書のタイプが SSC の場合のみ表示されます。

関連トピック

コントローラへの AAA セキュリティの設定 （686 ページ）
コントローラでの AAA AP/MSE ポリシーの編集 （695 ページ）

コントローラでの AAA AP/MSE ポリシーの編集

AP/MSE 認可アクセス ポイント ポリシーを編集するには、次の手順を実行します。

ステップ 1 [設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）] を選択し、左側の [デバイスグループ（Device Groups）] メニューから [デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）] を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[セキュリティ（Security）] > [AAA] > [AP または MSE 認証（AP or MSE Authorization）]** を選択します。

ステップ 4 [コマンドの選択（Select a command）] ドロップダウン リストから [AP ポリシーの編集（Edit AP Policies）] を選択し、[実行（Go）] をクリックします。

ステップ 5 必要に応じて、次のパラメータを編集します。

- [AP の認可（Authorize APs）]：アクセス ポイント認可を有効にする場合は、このチェックボックスをオンにします。
- [SSC-AP の受け入れ（Accept SSC-APs）]：SSE アクセス ポイントの承認を有効にする場合は、このチェックボックスをオンにします。

ステップ 6 [保存（Save）] をクリックして変更を確定するか、[監査（Audit）] をクリックしてこれらのデバイス値の監査を実行するか、[キャンセル（Cancel）] をクリックしてこのページを変更せずに閉じます。

関連トピック

コントローラへの AAA セキュリティの設定 （686 ページ）

コントローラでの AAA Web 認証の設定

[Web Auth Configuration] ページでは、Web 認証の設定タイプを設定できます。このタイプをカスタマイズに設定した場合は、コントローラにより提供された内部 Web 認証ページが、ユーザのダウンロードした Web 認証に置き換わります。

[Web Auth Configuration] ページにアクセスするには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから [デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）] を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[セキュリティ（Security）] > [AAA] > [Web 認証設定（Web Auth Configuration）]** を選択します。

ステップ 4 ドロップダウンリストから Web 認証タイプを選択します。

ステップ 5 選択したタイプに応じて、Web 認証パラメータを設定します。

- Default Internal
  - [Custom Redirect URL]：認証が成功した後にユーザがリダイレクトされる URL。たとえば、このテキストボックスに入力した値が http://www.example.com の場合、ユーザはこの会社のホームページに接続されます。
  - [Logo Display]：ロゴの表示を有効または無効にします。
  - [Web Auth Page Title]：Web 認証ページに表示されるタイトル。
  - [Web Auth Page Message]：認証ページに表示されるメッセージ。
- Customized Web Auth

  サンプルのログイン ページをダウンロードして、そのページをカスタマイズできます。カスタマイズ Web 認証ページを使用する場合は、サーバからサンプルの login.tar バンドル ファイルをダウンロードし、login.html ファイルを編集して .tar または .zip ファイルとして保存してから、.tar または .zip ファイルをコントローラにダウンロードする必要があります。

  プレビュー イメージをクリックして、このサンプル ログイン ページを TAR としてダウンロードします。HTML の編集後にここをクリックすると [Download Web Auth] ページにリダイレクトされます。詳細については、「コントローラへの圧縮された Web認証ログイン ページ情報のダウンロード」を参照してください。
- External
  - [External Redirect URL]：ネットワーク上の外部サーバにある login.html の場所。

    外部 Web 認証サーバが設定されていない場合は、外部 Web 認証サーバを設定するオプションがあります。

コントローラでの AAA パスワード ポリシーの設定

このページでは、パスワード ポリシーを決定できます。

既存のパスワード ポリシーを変更するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Devices Groups）] メニューから [デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）] を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[セキュリティ（Security）] > [AAA] > [パスワードポリシー（Password Policy）]** を選択します。

ステップ 4 パスワード ポリシーのパラメータを必要に応じて変更します。

ステップ 5 [Save] をクリックします。

パスワード ポリシー オプションを無効にすると、「Disabling the strong password check(s) will be a security risk as it allows weak passwords」というメッセージが表示されます。

関連トピック

コントローラへの AAA セキュリティの設定 （686 ページ）

コントローラでのローカル EAP の設定

ローカル EAP は、ユーザおよびワイヤレス クライアントのローカル認証を可能にする認証方式です。この方式は、バックエンドシステムが妨害されたり、外部認証サーバがダウンした場合でも、ワイヤレス クライアントへの接続を維持できるように、リモート オフィスで使用する目的で設計されています。

ローカル EAP を有効にすると、コントローラは認証サーバおよびローカル ユーザ データベースとして機能するため、外部認証サーバから独立します。ローカル EAP は、ローカル ユーザ データベースまたはLDAPバックエンドデータベースからユーザの資格情報を取得して、ユーザを認証します。

関連トピック

コントローラでのローカル EAP 一般パラメータの設定 （697 ページ）
コントローラで使用されるローカル EAP プロファイルの表示 （698 ページ）
コントローラでのローカル EAP 一般 EAP-Fast パラメータの設定
コントローラでのローカル EAP 一般ネットワーク ユーザ優先度の設定 （700 ページ）

コントローラでのローカル EAP 一般パラメータの設定

ローカル EAP のタイムアウト値を指定できます。その後、このタイムアウト値を持つテンプレートを追加したり、既存のテンプレートを変更できます。

コントローラ上でRADIUSサーバが設定されている場合は、コントローラはまずRADIUSサーバを使用してワイヤレスクライアントを認証しようとします。ローカルEAPは、RADIUSサーバがタイムアウトしていたり、RADIUSサーバが設定されていない場合など、RADIUSサーバが見つからない場合にのみ試行されます。4台のRADIUSサーバが設定されている場合、コントローラは最初の RADIUS サーバを使用してクライアントの認証を試行し、次に 2 番めの RADIUS サーバ、その次にローカル EAP を試行します。その後クライアントが手動で再認証を試みると、コントローラは 3 番めの RADIUS サーバを試行し、次に 4 番めの RADIUS サーバ、その次にローカル EAP を試行します。

ローカル EAP のタイムアウト値を指定するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）]** を選択し、左側の [デバイス グループ（Devices Groups）] メニューから [デバイス タイプ（Device Type）] > [ワイヤレス コントローラ（Wireless Controller）] を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[セキュリティ（Security）]** > **[ローカル EAP（Local EAP）]** > **[一般 - ローカル EAP(General - Local EAP)]** を選択します。

ステップ 4 [Local Auth Active Timeout] テキスト ボックスにローカル認証アクティブ タイムアウトを入力します（秒単位）。ローカル認証アクティブ タイムアウトは、すべての RADIUS サーバが失敗した後、ローカル EAP が必ず使用されるタイムアウト時間を指します。

ステップ 5 EAP-FAST、手動パスワード入力、ワンタイム パスワード、または 7920/7921 電話を使用する際は、次の値を調整する必要があります。

自動プロビジョニングを使用している PAC をクライアントで取得する場合、コントローラで 802.1x のタイムアウト値を大きくする必要があります（デフォルトは 2 秒）。Cisco ACS サーバでは、デフォルトの 20 秒を推奨します。

- Local EAP Identify Request Timeout =1（秒単位）
- Local EAP Identity Request Maximum Retries=20（秒単位）
- Local EAP Dynamic Wep Key Index=0
- Local EAP Request Timeout=20（秒単位）
- Local EAP Request Maximum Retries=2
- EAPOL-Key Timeout=1000（ミリ秒単位）
- EAPOL-Key Max Retries=2
- Max-Login Ignore Identity Response

複数のコントローラで次の値が同じに設定されていないと、ローミングが失敗します。

ステップ 6 [Save] をクリックします。

関連トピック

コントローラでのローカル EAP の設定 （697 ページ）
コントローラで使用されるローカル EAP プロファイルの表示 （698 ページ）
コントローラでのローカル EAP 一般 EAP-Fast パラメータの設定
コントローラでのローカル EAP 一般ネットワーク ユーザ優先度の設定 （700 ページ）

コントローラで使用されるローカル EAP プロファイルの表示

ローカル EAP プロファイルのテンプレートを適用したり、既存のテンプレートを変更したりすることができます。

LDAP バックエンド データベースは、次のローカル EAP メソッドだけをサポートします。証明書による EAP-TLS および EAP-FAST。LDAP バックエンド データベースでは、LEAP および PAC による EAP-FAST はサポートされません。

既存のローカル EAP プロファイルを表示するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）]** > **[ネットワーク（Network）]** > **[ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）]** > **[ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[セキュリティ（Security）] > [ローカル EAP（Local EAP）] > [ローカル EAP プロファイル（Local EAP Profiles）]** を選択します。[Local EAP Profiles] ページには、次のパラメータが表示されます。

- [EAP Profile Name]：ユーザ定義の ID。
- [LEAP]：Cisco Key Integrity Protocol（CKIP）と MMH Message Integrity Check（MIC）を使用してデータを保護する認証タイプ。ユーザ名とパスワードを使用し、アクセス ポイントを介して RADIUS サーバと相互認証を行います。
- [EAP-FAST]：3 段階のトンネル認証プロセスを使用して高度な 802.1x EAP 相互認証を実行する認証タイプ（Flexible Authentication via Secure Tunneling）。ユーザ名、パスワード、および PAC（保護されたアクセス クレデンシャル）を使用し、アクセス ポイントを介して RADIUS サーバと相互認証を行います。
- [TLS]：クライアント アダプタおよび RADIUS サーバの動的セッション ベースの暗号鍵を使用してデータを暗号化する認証タイプ。認証のためには、クライアント証明書が必要です。
- [PEAP]：保護拡張認証プロトコル。

関連トピック

コントローラでのローカル EAP の設定 （697 ページ）
コントローラへのローカル EAP プロファイルの追加 （699 ページ）

コントローラへのローカル EAP プロファイルの追加

ローカル EAP プロファイルを追加するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[セキュリティ（Security）] > [ローカルEAP（Local EAP）] > [ローカルEAPプロファイル（Local EAP Profile）]** の順に選択します。

ステップ 4 [Select a command] ドロップダウン リストから [Add Local EAP Profile] を選択します。

ステップ 5 [Select a template to apply to this controller] ドロップダウン リストからテンプレートを選択します。

ステップ 6 [Apply] をクリックします。

関連トピック

コントローラでのローカル EAP の設定 （697 ページ）
コントローラでのローカル EAP 一般パラメータの設定 （697 ページ）
コントローラで使用されるローカル EAP プロファイルの表示 （698 ページ）
コントローラでのローカル EAP 一般 EAP-Fast パラメータの設定
コントローラでのローカル EAP 一般ネットワーク ユーザ優先度の設定 （700 ページ）

コントローラでのローカル EAP 一般ネットワーク ユーザ優先度の設定

LDAP とローカル データベースがユーザ クレデンシャル情報を取得するために使用する順序を指定するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Devices Groups）] メニューから [デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）] を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから **[セキュリティ（Security）] > [ローカル EAP（Local EAP）] > [ネットワーク ユーザの優先度（Network Users Priority）]** を選択します。

ステップ 4 左右の矢印を使用して、右端のリストにネットワーク クレデンシャルを入れたり、除外することができます。

ステップ 5 上下のボタンを使用してクレデンシャルを試行する順序を指定します。

ステップ 6 [Save] をクリックします。

関連トピック

コントローラでのローカル EAP の設定 （697 ページ）
コントローラでのローカル EAP 一般パラメータの設定 （697 ページ）
コントローラの Web 認証証明書の設定 （700 ページ）
コントローラでの IP Sec CA 証明書の設定 （705 ページ）

コントローラの Web 認証証明書の設定

Web 認証証明書をダウンロードしたり、内部生成 Web 認証証明書を再生成したりすることができます。

注意 各証明書には、可変長 RSA キーが組み込まれています。RSA キーは、比較的に安全性が低い 512 ビットから、安全性がかなり高い数千ビットまでさまざまです。認証局（Microsoft CA など）から新しい証明書を取得する場合は、証明書に組み込まれている RSA キーが 768 ビット以上であることを確認してください。

ステップ 1 [Configuration] > [Network] > [Network Devices] を選択し、左側の [Device Groups] メニューから [Device Type] > [Wireless Controller] を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、[Security] > [Web Auth Certificate] の順に選択します。

ステップ 4 [Download Web Auth Certificate] をクリックして [Download Web Auth Certificate to Controller] ページにアクセスします。

関連トピック

コントローラでのローカル EAP 一般パラメータの設定 （697 ページ）
コントローラでのローカル EAP の設定 （697 ページ）

コントローラのユーザ ログイン ポリシーの設定

コントローラにユーザ ログイン ポリシーを設定するには、次の手順を実行します。

ステップ 1 [Configuration] > [Network] > [Network Devices] を選択し、左側の [Device Groups] メニューから [Device Type] > [Wireless Controller] を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、[セキュリティ（Security）] > [ユーザ ログイン ポリシー（User Login Policies）] を選択します。

ステップ 4 1 つのユーザ名で同時にログインできる最大数を入力します。

ステップ 5 **[保存（Save）]** をクリックします。

デバイスの手動で無効化されるクライアントの設定

[Disabled Clients] ページでは、除外された（ブラックリストに掲載された）クライアントの情報を表示できます。

アソシエートを試行した際に、3 回認証に失敗したクライアントはオペレータが定義したタイムアウトの間、再度アソシエートを試行できないように、自動的にブロック（または除外）されます。除外タイムアウトが経過すると、クライアントは認証の再試行を許可され、アソシエートすることができます。このとき、認証に失敗すると再び除外されます。

ブロードキャスト用の MAC アドレスを使用できません。

[Manually Disabled Clients] ページにアクセスするには、次の手順を実行します。

ステップ 1 [設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）] を選択し、左側の [デバイスグループ（Device Groups）] メニューから [デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）] を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、[Security] > [Manually Disabled Clients] の順に選択します。[Manually Disabled Clients] ページには、次のパラメータが表示されます。

- [MAC Address]：無効にされたクライアントの MAC アドレス。リスト項目をクリックして、無効にされたクライアントの説明を編集します。

• [Description]：無効にされたクライアントのオプションの説明。

コントローラのアクセス コントロール リスト（ACL）の設定

コントローラの新しいアクセス コントロール リスト（ACL）を表示、編集、または追加できます。

ステップ 1 [Configuration] > [Network] > [Network Devices] を選択し、左側の [Device Groups] メニューから [Device Type] > [Wireless Controller] を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、[セキュリティ（Security）] > [アクセス コントロール リスト（Access Control Lists）] を選択します。

a) チェックボックスをオンにして、1 つ以上の ACL を削除します。

または

b) ACL 項目をクリックすると、そのパラメータを表示できます。

コントローラ ACL ルールの設定 （702 ページ）
コントローラ CPU 用の ACL セキュリティの追加 （704 ページ）

コントローラ ACL ルールの設定

コントローラに適用するアクセス コントロール リスト（ACL）のルールを作成および変更できます。

ステップ 1 [Configuration] > [Network] > [Network Devices] を選択し、左側の [Device Groups] メニューから [Device Type] > [Wireless Controller] を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、[Security] > [Access Control Lists] の順に選択します。

ステップ 4 ACL 名をクリックし、パラメータを表示して変更します。

ステップ 5 必要に応じて、アクセス コントロール リスト ルールのチェックボックスをオンします。

新しいコントローラの ACL ルールの作成

ステップ 1 **[デバイス タイプ（Device Type）] > [ワイヤレス コントローラ（Wireless Controller）]** を選択し、左側の [デバイス グループ（Device Groups）] メニューから **[デバイス タイプ（Device Type）] > [ワイヤレス コントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[セキュリティ（Security）] > [アクセス コントロール リスト（Access Control Lists）]** を選択します。

ステップ 4 ACL 名をクリックします。

ステップ 5 該当する [Seq#] をクリックするか、[Add New Rule] を選択してこのページにアクセスします。

コントローラ ACL ルールの設定 （702 ページ）
コントローラ CPU 用の ACL セキュリティの追加 （704 ページ）

コントローラの FlexConnect ACL セキュリティの設定

FlexConnect 上の ACL は、ローカルでスイッチされた、アクセス ポイントからのデータ トラフィックの保護および完全性のために、FlexConnect アクセス ポイントで必要とされるアクセス コントロールを提供するメカニズムを提供します。

コントローラでの FlexConnect ACL の追加 （703 ページ）
コントローラの FlexConnect ACL の削除 （704 ページ）

コントローラでの FlexConnect ACL の追加

FlexConnect アクセス ポイントのアクセス コントロール リストを追加するには、次の手順を実行します。

ステップ 1 [Configuration] > [Network] > [Network Devices] を選択し、左側の [Device Groups] メニューから [Device Type] > [Wireless Controller] を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、[Security] > [FlexConnect ACLs] の順に選択します。

ステップ 4 [Select a command] ドロップダウン リストから、[Add FlexConnect ACLs] を選択します。

ステップ 5 [Go] をクリックします。

テンプレートが作成されていない場合は、FlexConnect ACL は追加できません。使用できるテンプレートが存在しない状態で FlexConnect ACL の作成を試行した場合は、[New Controller Templates] ページにリダイレクトされます。ここで、FlexConnect ACL 用のテンプレートを作成できます。

ステップ 6 ドロップダウン リストからコントローラに適用するテンプレートを選択して、[Apply] をクリックします。

作成した FlexConnect ACL が、[Configure] > [Controllers] > [*IP Address*] > [Security] > [FlexConnect ACLs] に表示されます。

コントローラの FlexConnect ACL セキュリティの設定 （703 ページ）

コントローラの FlexConnect ACL の削除

FlexConnect ACL を削除するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）]** を選択し、左側の [デバイス グループ（Device Groups）] メニューから **[デバイス タイプ（Device Type）] > [ワイヤレス コントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[セキュリティ（Security）] > [FlexConnect ACL（FlexConnect ACLs）]** を選択します。

ステップ 4 [FlexConnect ACLs] ページから、削除する FlexConnect ACL を 1 つ以上選択します。

ステップ 5 [Select a command] ドロップダウン リストから [Delete FlexConnect ACLs] を選択します。

ステップ 6 [Go] をクリックします。

コントローラの FlexConnect ACL セキュリティの設定 （703 ページ）

コントローラ CPU 用の ACL セキュリティの追加

アクセス コントロール リスト（ACL）は、コントローラの CPU に適用して、その CPU へのトラフィックを制御できます。

ステップ 1 [Configuration] > [Network] > [Network Devices] を選択し、左側の [Device Groups] メニューから [Device Type] > [Wireless Controller] を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、[Security] > [CPU Access Control Lists] の順に選択します。

ステップ 4 [Enable CPU ACL] チェックボックスをオンにして、CPU ACL を有効にします。次のパラメータを使用できます。

- [ACL Name]：[ACL Name] ドロップダウン リストから使用する ACL を選択します。
- [CPU ACL Mode]：この CPU ACL リストで制御するデータ トラフィックの方向を選択します。

コントローラの FlexConnect ACL セキュリティの設定 （703 ページ）
コントローラのアクセス コントロール リスト（ACL）の設定 （702 ページ）
コントローラ ACL ルールの設定 （702 ページ）

コントローラの設定済み IDS セキュリティ センサーの表示

センサーが攻撃を識別した場合は、攻撃しているクライアントを回避するようにコントローラに警告します。新しい IDS（侵入検知システム）センサーを追加した場合は、回避したクライアントのレポートをセンサーがコントローラに送信できるように、コントローラをその IDS センサーに登録します。また、コントローラは定期的にセンサーをポーリングします。

IDS センサーを表示する手順は、次のとおりです。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから **[セキュリティ（Security）] > [IDS センサー リスト（IDS Sensor Lists）]** を選択します。

[IDS Sensor] ページには、このコントローラに設定されているすべての IDS センサーのリストが表示されます。IP アドレスをクリックして、特定の IDS センサーの詳細を表示します。

コントローラでの IP Sec CA 証明書の設定

認証局（CA）の証明書は、ある認証局（CA）が別の認定 CA に対して発行したデジタル証明書です。

コントローラへの IP Sec 証明書のインポート （705 ページ）
コントローラへの IP Sec 証明書の貼り付け （705 ページ）

コントローラへの IP Sec 証明書のインポート

ファイルから CA 証明書をインポートするには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[セキュリティ（Security）] > [IP Sec 証明書（IP Sec Certificates）] > [CA 証明書（CA Certificate）]** を選択します。

ステップ 4 [Browse] をクリックして該当する証明書ファイルにナビゲートします。

ステップ 5 [Open] をクリックしてから [Save] をクリックします。

コントローラでの IP Sec CA 証明書の設定 （705 ページ）

コントローラへの IP Sec 証明書の貼り付け

CA 証明書を直接貼り付けるには、次の手順を実行します。

ステップ 1 コンピュータのクリップボードに CA 証明書をコピーします。

ステップ 2 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 3 該当するコントローラのデバイス名をクリックします。

ステップ 4 左側のサイドバーのメニューから、**[セキュリティ（Security）] > [IP Sec 証明書（IP Sec Certificates）] > [CA 証明書（CA Certificate）]** を選択します。

ステップ 5 [Paste] チェックボックスをオンにします。

ステップ 6 証明書をテキスト ボックスに直接貼り付けます。

ステップ 7 [Save] をクリックします。

コントローラでの IP Sec CA 証明書の設定 （705 ページ）
コントローラでのネットワーク アイデンティティ（ID）証明書の設定 （706 ページ）
コントローラの Web 認証証明書の設定 （700 ページ）

コントローラでのネットワーク アイデンティティ（ID）証明書の設定

このページには、既存のネットワーク アイデンティティ（ID）証明書が証明書名別に一覧表示されます。ID 証明書は、Web サーバのオペレータが、安全なサーバの動作を確保するために使用します。ID 証明書は、コントローラが Cisco Unified Wireless Network のソフトウェア バージョン 3.2 以降を実行している場合のみ、使用できます。

コントローラへの IP Sec 証明書のインポート （705 ページ）
コントローラへの IP Sec 証明書の貼り付け （705 ページ）

コントローラへの ID 証明書のインポート

ファイルから ID 証明書をインポートするには、次の手順を実行します。

ステップ 1 [設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）] を選択し、左側の [デバイス グループ（Device Groups）] メニューから **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[セキュリティ（Security）] > [IP Sec証明書（IP Sec Certificates）] > [ID証明書（ID Certificate）]** の順に選択します。

ステップ 4 [Select a command] ドロップダウン リストから [Add Certificate] を選択します。

ステップ 5 [Go] をクリックします。

ステップ 6 名前とパスワードを入力します。

ステップ 7 [Browse] をクリックして該当する証明書ファイルにナビゲートします。

ステップ 8 [Open] をクリックしてから [Save] をクリックします。

コントローラでのネットワーク アイデンティティ（ID）証明書の設定 （706 ページ）

コントローラへの ID 証明書の貼り付け

ID 証明書を直接貼り付けるには、次の手順を実行します。

ステップ 1 コンピュータのクリップボードに ID 証明書をコピーします。

ステップ 2 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 3 該当するコントローラのデバイス名をクリックします。

ステップ 4 左側のサイドバーのメニューから、**[セキュリティ（Security）] > [IP Sec証明書（IP Sec Certificates）] > [ID証明書（ID Certificate）]** の順に選択します。

ステップ 5 [Select a command] ドロップダウン リストから [Add Certificate] を選択します。

ステップ 6 [Go] をクリックします。

ステップ 7 名前とパスワードを入力します。

ステップ 8 [Paste] チェックボックスをオンにします。

ステップ 9 証明書をテキスト ボックスに直接貼り付けます。

ステップ 10 [Save] をクリックします。

コントローラでの IP Sec CA 証明書の設定 （705 ページ）
コントローラでのネットワーク アイデンティティ（ID）証明書の設定 （706 ページ）

コントローラでのワイヤレス保護ポリシーの設定

ここでは、ワイヤレス保護ポリシーの設定について説明します。内容は次のとおりです。

- コントローラでの不正 AP ポリシーの設定
- コントローラでの不正 AP ポリシーの表示
- コントローラでのクライアント除外ポリシーの設定
- コントローラに適用されるシスコが提供する IDS 署名の表示
- カスタム IDS 署名の作成
- コントローラの AP 認証と管理フレーム保護の設定

コントローラでの不正 AP ポリシーの設定

不正アクセス ポイントのポリシーを設定できます。必要なアクセス ポイントで不正検出が有効になっていることを確認します。コントローラに接続されたすべてのアクセスポイントに対し、不正の検出がデフォルトで有効化されます（OfficeExtend アクセス ポイントを除く）。ただし、Cisco Prime Infrastructure ソフトウェア リリース 6.0 以降では、[アクセス ポイントの詳細（Access Point Details）] ページで [不正検出（Rogue Detection）] チェックボックスをオンまたはオフにすることにより、アクセスポイントごとに不正検出を有効または無効にできます。

家庭の環境で展開されるアクセス ポイントは大量の不正デバイスを検出する可能性が高いため、OfficeExtend アクセス ポイントでは不正検出はデフォルトでは無効です。

[Rogue Policies] ページにアクセスするには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）][コントローラ（Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[セキュリティ（Security）] > [ワイヤレス保護ポリシー（Wireless Protection Policies）] > [不正ポリシー（Rogue Policies）]** を選択します。次のパラメータが表示されます。

- [Rogue Location Discovery Protocol]：RLDP は、企業の有線ネットワークへの不正な接続の有無を判断します。ドロップダウン リストから、次のいずれかのオプションを選択します。
  - [Disable]：すべてのアクセス ポイント上で RLDP を無効にします。これはデフォルト値です。
  - [All APs]：すべてのアクセス ポイント上で RLDP を有効にします。
  - [Monitor Mode APs]：モニタ モードのアクセス ポイント上でのみ RLDP を有効にします。
- Rogue APs
  - [Expiration Timeout for Rogue AP and Rogue Client Entries (seconds)]：不正なアクセス ポイントおよびクライアントのエントリがリストから削除されるまでの秒数を入力します。有効な範囲は 240 ～ 3600 秒で、デフォルト値は 1200 秒です。

    不正なアクセス ポイントまたはクライアントのエントリがタイムアウトすると、その不正の状態がいずれの分類タイプに対しても Alert または Threat である場合には、コントローラから削除されます。
  - [Rogue Detection Report Interval]：AP からコントローラに不正検出レポートを送信する間隔を秒数で入力します。有効な範囲は 10 ～ 300 秒で、デフォルト値は 10 秒です。この機能は、モニタ モードの AP のみに適用されます。
  - [Rogue Detection Minimum RSSI]：AP で検出するために不正に必要であり、かつコントローラで不正エントリが作成されるために必要な最小 RSSI 値を入力します。有効な範囲は -70 ～ -128 dBm で、デフォルト値は -128 dBm です。この機能は、すべての AP モードに適用できます。

    非常に RSSI 値が低く、不正解析にとって有益な情報とならない不正が多く存在する可能性があります。そのため、このオプションを使用して AP が不正を検出する最小 RSSI 値を指定することで、不正をフィルタできます。
  - [Rogue Detection Transient Interval]：最初に不正がスキャンされた後、AP が継続的に不正をスキャンする必要のある間隔を入力します。一時的な間隔を入力することで、AP が不正をスキャンする間隔を制御できます。AP は、一時的な間隔の値に基づいて、不正をフィルタできます。有効な範囲は 120 ～ 1800 秒で、デフォルト値は 0 です。この機能は、モニタ モードの AP のみに適用されます。
- Rogue Clients

- [AAA に対する不正クライアントの検証（Validate rogue clients against AAA）]：AAA サーバまたはローカル データベースを使用して、不正なクライアントが有効なクライアントかどうかを検証するには、このチェックボックスをオンにします。デフォルト値はオフです。
- [アドホック ネットワークの検出とレポート（Detect and report Adhoc networks）]：アドホック不正検出およびレポートを有効にするには、このチェックボックスをオンにします。デフォルト値はオンです。

コントローラでの不正 AP ポリシーの表示 （709 ページ）
コントローラでのクライアント除外ポリシーの設定 （709 ページ）
コントローラに適用されるシスコが提供する IDS 署名の表示 （711 ページ）
カスタム IDS 署名の作成 （715 ページ）
コントローラの AP 認証と管理フレーム保護の設定 （716 ページ）
コントローラでのワイヤレス保護ポリシーの設定 （707 ページ）

コントローラでの不正 AP ポリシーの表示

このページでは、現在の不正 AP ルールを表示および編集できます。

[不正 AP ルール（Rogue AP Rules）] ページにアクセスするには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[セキュリティ（Security）] > [ワイヤレス保護ポリシー（Wireless Protection Policies）] > [不正 AP ルール（Rogue AP Rules）]** を選択します。[Rogue AP Rules] に、不正 AP ルール、ルール タイプ（[Malicious] または [Friendly]）、およびルールの順序が表示されます。

ステップ 4 ルールの詳細を表示または編集するには、[Rogue AP Rule] をクリックします。

コントローラでのクライアント除外ポリシーの設定 （709 ページ）
コントローラに適用されるシスコが提供する IDS 署名の表示 （711 ページ）
カスタム IDS 署名の作成 （715 ページ）
コントローラの AP 認証と管理フレーム保護の設定 （716 ページ）
コントローラでのワイヤレス保護ポリシーの設定 （707 ページ）

コントローラでのクライアント除外ポリシーの設定

このページでは、コントローラに適用されているクライアント除外ポリシーを設定、有効化、または無効化できます。

[Client Exclusion Policies] ページにアクセスするには、次の手順を実行します。

ステップ 1 [Configuration] > [Network] > [Network Devices] を選択し、左側の [Device Groups] メニューから [Device Type] > [Wireless Controller] を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、[Security] > [Wireless Protection Policies] > [Client Exclusion Policies] の順に選択します。次のパラメータが表示されます。

- [Excessive 802.11a Association Failures]：有効にした場合、クライアントは 802.11 アソシエーションの試行に 5 回連続して失敗すると、6 回目の試行で除外されます。
- [802.11a 認証の過剰な失敗（Excessive 802.11a Authentication Failures）]：有効にした場合、クライアントは 802.11 認証の試行に 5 回連続して失敗すると、6 回目の試行で除外されます。
- [802.11x 認証の過剰な失敗（Excessive 802.11x Authentication Failures）]：有効にした場合、クライアントは 802.1X 認証の試行に 3 回連続して失敗すると、4 回目の試行で除外されます。
- [802.11 Web 認証の過剰な失敗（Excessive 802.11 Web Authentication Failures）]：有効にした場合、クライアントは Web 認証の試行に 3 回連続して失敗すると、4 回目の試行で除外されます。
- [IP の盗難または再使用（IP Theft Or Reuse）]：有効にした場合、IP アドレスがすでに別のデバイスに割り当てられていると、クライアントが除外されます。

ステップ 4 [保存（Save）] をクリックし、クライアント除外ポリシーに対する変更を保存して前のページに戻るか、[監査（Audit）] をクリックしてコントローラで使用された値と Prime Infrastructure の値を比較します。

コントローラでの不正 AP ポリシーの表示 （709 ページ）
コントローラに適用されるシスコが提供する IDS 署名の表示 （711 ページ）
カスタム IDS 署名の作成 （715 ページ）
コントローラの AP 認証と管理フレーム保護の設定 （716 ページ）
コントローラでのワイヤレス保護ポリシーの設定 （707 ページ）

デバイスの IDS 署名の設定

コントローラ上で、IDS シグニチャ、つまり、受信 802.11 パケットにおけるさまざまなタイプの攻撃を特定するのに使用されるビット パターンのマッチング ルールを設定することができます。シグニチャが有効化されると、コントローラに接続されたアクセス ポイントでは、受信した 802.11 データまたは管理フレームに対してシグニチャ分析が行われ、整合性がない場合はコントローラに報告されます。攻撃が検出されると、適切な緩和措置が取られます。

シスコではコントローラの 17 の標準シグニチャをサポートしています。

コントローラに適用されるシスコが提供する IDS 署名の表示 （711 ページ）
カスタム IDS 署名の作成 （715 ページ）
コントローラの AP 認証と管理フレーム保護の設定 （716 ページ）

コントローラに適用されるシスコが提供する IDS 署名の表示

[Standard Signature Parameters] ページには、現在コントローラ上にあるシスコ提供のシグニチャの一覧が表示されます。

[Standard Signatures] ページにアクセスするには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）]** を選択し、左側の [デバイス グループ（Device Groups）] メニューから **[デバイス タイプ（Device Type）] > [ワイヤレス コントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[セキュリティ（Security）] > [ワイヤレス保護ポリシー（Wireless Protection Policies）] > [標準シグネチャ（Standard Signatures）]** を選択します。このページには、次のパラメータが表示されます。

- [Precedence]：コントローラがシグニチャ チェックを実行する順序。
- [Name]：シグニチャによって検出を試みる攻撃の種類。
- [Frame Type]：シグニチャによってセキュリティ攻撃の調査が行われる管理フレームまたはデータフレームの種類。
- [Action]：シグニチャによって攻撃が検出されたときに実行する、コントローラへの指示。次に例を示します。
  - [None]：アクションが実行されません。
  - [Report]：検出をレポートします。
- [State]：有効または無効。
- [Description]：シグニチャによって検出を試みる攻撃の種類の詳細説明。

ステップ 4 シグネチャの名前をクリックして個々のパラメータを表示し、シグネチャを有効または無効にします。

関連トピック

デバイスの IDS 署名の設定 （710 ページ）
コントローラからの IDS 署名ファイルのアップロード （712 ページ）
コントローラ上のすべての IDS 署名の有効化と無効化 （713 ページ）

コントローラへの IDS 署名ファイルのダウンロード

シグネチャ ファイルをダウンロードするには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）][コントローラ（Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[セキュリティ（Security）] > [ワイヤレス保護ポリシー（Wireless Protection Policies）] > [標準シグネチャ（Standard Signatures）]** または **[セキュリティ（Security）] > [ワイヤレス保護ポリシー（Wireless Protection Policies）] > [カスタムシグネチャ（Custom Signatures）]** の順に選択します。

ステップ 4 [Select a command] ドロップダウン リストから、[Download Signature Files] を選択します。

ステップ 5 [Go] をクリックします。

ステップ 6 シグニチャ ファイル（*.sig）を TFTP サーバ上のデフォルト ディレクトリにコピーします。

ステップ 7 [File is Located On] から [Local Machine] を選択します。ファイル名および、サーバのルート ディレクトリに対して相対的なパスがわかる場合は、[TFTP server] を選択することもできます。

ステップ 8 [Maximum Retries] に、コントローラがシグニチャ ファイルのダウンロードを試みる最大回数を入力します。

ステップ 9 [Timeout] に、シグニチャ ファイルのダウンロードを試行する際、コントローラがタイムアウトになるまでの最大時間を秒単位で入力します。

ステップ 10 ファイルは /localdisk/tftp ディレクトリにアップロードされます。そのディレクトリ内のローカル ファイル名を指定するか、[Browse] をクリックしてナビゲートします。シグニチャ ファイルの「revision」行で、ファイルがシスコ提供の標準のシグニチャ ファイルか、またはサイトに合わせたカスタム シグニチャ ファイルかを指定します（カスタム シグニチャ ファイルには revision=custom が必須）。

何らかの理由で転送がタイムアウトになった場合、[File Is Located On] フィールドで [TFTP server] オプションを選択すると、サーバ ファイル名が自動的に入力され、再試行されます。ローカル マシン オプションでは 2 段階の動作が起動されます。最初に、ローカル ファイルが管理者のワークステーションから Prime Infrastructure 独自の組み込みの TFTP サーバにコピーされます。次にコントローラがそのファイルを取得します。後の操作では、ファイルはすでに Prime Infrastructure サーバの TFTP ディレクトリにあるため、ダウンロードした Web ページで自動的にそのファイル名が読み込まれます。

ステップ 11 [OK] をクリックします。

関連トピック

デバイスの IDS 署名の設定 （710 ページ）

コントローラからの IDS 署名ファイルのアップロード

コントローラからシグニチャ ファイルをアップロードできます。シグニチャのダウンロードに Trivial File Transfer Protocol（TFTP; 簡易ファイル転送プロトコル）サーバを使用できることを確認します。TFTP サーバをセットアップする際の注意事項は次のとおりです。

- サービス ポート経由でダウンロードする場合、サービス ポートはルーティングできないため、TFTP サーバはサービス ポートと同じサブネット上になければなりません。
- ディストリビューション システム ネットワーク ポートを経由してダウンロードする場合、ディストリビューション システム ポートはルーティングできないため、TFTP サーバは同じサブネット上にあっても、別のサブネット上にあってもかまいません。

- Prime Infrastructure の組み込み TFTP サーバとサードパーティの TFTP サーバは同じ通信ポートを使用するため、サードパーティの TFTP サーバを Prime Infrastructure と同じコンピュータ上で実行することはできません。

ステップ 1 シスコからシグネチャ ファイルを入手します（標準シグネチャ ファイル）。

ステップ 2 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 3 該当するコントローラのデバイス名をクリックします。

ステップ 4 左側のサイドバーのメニューから、**[セキュリティ（Security）] > [ワイヤレス保護ポリシー（Wireless Protection Policies）] > [標準シグネチャ（Standard Signatures）]** または **[セキュリティ（Security）] > [ワイヤレス保護ポリシー（Wireless Protection Policies）] > [カスタムシグネチャ（Custom Signatures）]** の順に選択します。

ステップ 5 [Select a Command] ドロップダウン リストから、[Upload Signature Files from controller] を選択します。

ステップ 6 転送に使用している TFTP サーバ名を指定します。

ステップ 7 TFTP サーバが新しい場合は、[Server IP Address] フィールドで TFTP IP アドレスを入力します。

ステップ 8 [File Type] ドロップダウン リストから [Signature Files] を選択します。

このシグニチャ ファイルは、TFTP サーバによる使用に対して設定されたルート ディレクトリにアップロードされます。[Upload to File] フィールドで別のディレクトリに変更できます（このフィールドは、[Server Name] がデフォルト サーバの場合のみ表示）。コントローラはベース ネームとしてこのローカル ファイル名を使用し、標準シグニチャ ファイルのサフィクスとして _std.sig を、カスタム シグニチャ ファイルのサフィクスとして _custom.sig を追加します。

ステップ 9 [OK] をクリックします。

デバイスの IDS 署名の設定 （710 ページ）
コントローラへの IDS シグネチャのダウンロード （597 ページ）

コントローラ上のすべての IDS 署名の有効化と無効化

このコマンドは、個々に選択して有効にしたシグニチャすべてを有効にします。このチェックボックスをオフのままにすると、以前に有効にしていても、すべてのファイルは無効になります。シグニチャが有効化されると、コントローラに接続されたアクセス ポイントでは、受信した 802.11 データまたは管理フレームに対してシグニチャ分析が行われ、整合性がない場合はコントローラに報告されます。

現在コントローラ上にあるすべての標準シグネチャおよびカスタム シグネチャを有効にするには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 [Select a command] ドロップダウン リストから [Edit Signature Parameters] を選択します。

ステップ 4 [Go] をクリックします。

ステップ 5 [Enable Check for All Standard and Custom Signatures] チェックボックスをオンにします。

ステップ 6 [Save] をクリックします。

デバイスの IDS 署名の設定 （710 ページ）

コントローラでの単一の IDS シグニチャの有効化と無効化

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 [Select a command] ドロップダウン リストから [Edit Signature Parameters] を選択します。

ステップ 4 有効または無効にする攻撃のタイプの、該当する名前をクリックします。

[Standard Signature parameters] ページには、現在コントローラ上にあるシスコ提供のシグニチャの一覧が表示されます。[Custom Signatures] ページには、現在コントローラ上に存在する、ユーザ提供のシグニチャのリストが表示されます。次のパラメータは、両方のシグニチャ ページおよび詳細シグニチャ ページに表示されます。

- [Precedence]：コントローラがシグニチャ チェックを行う順序、または優先順位。
- [Name]：シグニチャによって検出を試みる攻撃の種類。
- [Description]：シグニチャによって検出を試みる攻撃の種類の詳細説明。
- [Frame Type]：シグニチャによってセキュリティ攻撃の調査が行われる管理フレームまたはデータフレームの種類。
- [Action]：シグニチャによって攻撃が検出されたときに実行する、コントローラへの指示。アクションを実行しない場合は [なし（None）]、検出を報告する場合は [レポート（Report）] となります。
- [Frequency]：シグニチャの頻度。攻撃が検出される前に、アクセス ポイント レベルの検出において識別する必要のある、間隔ごとのシグニチャと一致するパケット数です。有効な範囲は間隔あたり 1 ～ 32,000 パケットです。デフォルト値は間隔あたり 50 パケットです。
- [Quiet Time]：各アクセス ポイント レベルで攻撃が検出されなくなってから、アラームを停止するまでの時間の長さ（秒単位）。この設定は、次項の [MAC Information] の設定が [all] もしくは [both] の場合にだけ表示されます。有効な範囲は 60 ～ 32,000 秒で、デフォルト値は 300 秒です。
- [MAC Information]：アクセス ポイント レベルの検出においてシグニチャをネットワークごとまたは MAC アドレスごと、または両方で追跡するどうか。

- [MAC Frequency]：シグニチャ MAC の頻度。攻撃が検出される前に、コントローラ レベルにおいて識別する必要のある、間隔ごとのシグニチャと一致するパケット数です。有効な範囲は間隔あたり 1 ～ 32,000 パケットです。デフォルト値は間隔あたり 30 パケットです。
- [Interval]：シグニチャの検出頻度がしきい値に達したかどうかをチェックする間隔（秒単位）を入力します。有効な範囲は 1 ～ 3600 秒で、デフォルト値は 1 秒です。
- [Enable]：このシグニチャによりセキュリティ攻撃が検出されるようにする場合はこのチェックボックスをオンにし、このシグニチャを無効にする場合はオフにします。
- [Signature Patterns]：セキュリティ攻撃の検出に使用されるパターン。

ステップ 5 [Enable] ドロップダウン リストから、[Yes] を選択します。カスタマイズされたシグニチャをダウンロードしているため、_custom.sgi という名前の付いたファイルを有効にし、同じ名前で異なる拡張子を持つ標準シグニチャを無効にする必要があります。たとえば、ブロードキャストプローブ フラッドをカスタマイズしている場合に、ブロードキャスト プローブ フラッドを標準シグニチャでは無効にし、カスタム シグニチャでは有効にする場合です。

ステップ 6 [Save] をクリックします。

デバイスの IDS 署名の設定 （710 ページ）
コントローラでの不正 AP ポリシーの設定 （707 ページ）
コントローラでの不正 AP ポリシーの表示 （709 ページ）
カスタム IDS 署名の作成 （715 ページ）
コントローラでのクライアント除外ポリシーの設定 （709 ページ）
コントローラの AP 認証と管理フレーム保護の設定 （716 ページ）

カスタム IDS 署名の作成

[Custom Signature] ページには、現在コントローラ上に存在する、ユーザ提供のシグニチャのリストが表示されます。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[セキュリティ（Security）] > [ワイヤレス保護ポリシー（Wireless Protection Policies）] > [カスタム シグネチャ（Custom Signatures）]** を選択します。このページには、次のパラメータが表示されます。

- [Precedence]：コントローラがシグニチャ チェックを実行する順序。
- [Name]：シグニチャによって検出を試みる攻撃の種類。
- [Frame Type]：シグニチャによってセキュリティ攻撃の調査が行われる管理フレームまたはデータフレームの種類。

- [Action]：シグニチャによって攻撃が検出されたときに実行する、コントローラへの指示。次に例を示します。
  - [None]：アクションが実行されません。
  - [Report]：検出をレポートします。
- [State]：有効または無効。
- [Description]：シグニチャによって検出を試みる攻撃の種類の詳細説明。

ステップ 4 シグニチャの名前をクリックして各パラメータを表示し、シグニチャを有効または無効にします。

デバイスの IDS 署名の設定 （710 ページ）
コントローラでの不正 AP ポリシーの設定 （707 ページ）
コントローラでの不正 AP ポリシーの表示 （709 ページ）
コントローラの AP 認証と管理フレーム保護の設定 （716 ページ）

コントローラの AP 認証と管理フレーム保護の設定

アクセス ポイント認証ポリシーと管理フレーム保護（MFP）を設定できます。

ステップ 1 [Configuration] > [Network] > [Network Devices] を選択し、左側の [Device Groups] メニューから [Device Type] > [Wireless Controller] を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、[Security] > [Wireless Protection Policies] > [AP Authentication and MFP] の順に選択します。

このページには、次のフィールドが表示されます。

- [RF Network Name]：このテキスト ボックスは編集できません。[一般パラメータ（General parameters）] ページに入力した RF ネットワーク名がここに表示されます。
- [Protection Type]：ドロップダウン リストから、次のいずれかの認証ポリシーを選択します。
  - [None]：アクセス ポイント認可ポリシーなし。
  - [AP Authentication]：認証ポリシーを適用します。
  - [MFP]：管理フレーム保護を適用します。
  - [Alarm Trigger Threshold]：（[Protection Type] で [AP Authentication] を選択した場合のみ表示）。アラームを発生させるまでに無視する、未知のアクセス ポイントからのヒット数を設定します。

有効な範囲は 1 ～ 255 です。デフォルト値は 255 です。

デバイスの IDS 署名の設定 （710 ページ）
コントローラでの不正 AP ポリシーの設定 （707 ページ）
コントローラでの不正 AP ポリシーの表示 （709 ページ）

カスタム IDS 署名の作成 （715 ページ）
コントローラに適用されるシスコが提供する IDS 署名の表示 （711 ページ）

URL ACL の構成

URL フィルタリング機能により、インターネットの Web サイトへのアクセスを制御できます。URL フィルタリング機能は、URL アクセス コントロール リスト（ACL）の情報に基づいて特定の Web サイトへのアクセスを許可または拒否して制御します。URL フィルタリングは、ACL リストに基づいてアクセスを制限します。

ロケーション ベースのフィルタリングで、AP はさまざまな AP グループに分けられ、WLAN のプロファイルが、同じ SSID 内でクライアントを信頼できるクライアントと、信頼できないクライアントに分類します。信頼できるクライアントが信頼できない AP に移動した場合や、その逆の場合、この分類に従って、新しい VLAN で再認証が実行されます。

ワイヤレス コントローラ（WLC）は、最大で 64 個の ACL をサポートします。各 ACL では最大 100 個の URL を指定できます。これらの ACL では、要求を許可または拒否するよう設定できます。また、これらの ACL を各種のインターフェイス（WLAN や LAN など）に関連付けて、フィルタリングを効果性を高めることができます。ポリシーは、適用されたグローバルポリシーとは異なる WLAN または AP グループでローカルで実装することができます。

各 ACL でサポートされるルール（URL）の数は WLC ごとに異なります。

- Cisco 5508 WLC および WiSM2 は URL ACL ごとに 64 件のルールをサポートできます。
- Cisco 5520、8510、8540 WLC は URL ACL ごとに 100 件のルールをサポートできます。

URL フィルタリングと NAT の制限

- Cisco 2504 WLC、vWLC、Mobility Express ではサポートされていません。
- WLAN 中央スイッチングはサポートされますが、ローカル スイッチングはサポートされていません。
- ローカル スイッチングを使用したフレックス モードではサポートされていません。
- URL 名の長さは 32 文字に制限されています。
- 一致した URL の AVC プロファイルはありません。一致した URL の ACL アクション サポート。
- ホワイト リストとブラックリストのリストを、ACL の「*」暗黙ルールを使用して作成し、要求を個別に許可または拒否することができます。
- HTTPS URL はサポートされていません。
- 次の状況では ACL はフィルタできない場合があります。
  - URL がフラグメント化されたパケットにまたがっている。
  - IP パケットがフラグメント化されている。
  - URL の代わりに直接 IP アドレスまたはプロキシ設定が使用されている。
- これらは現在サポートされていません。次の条件と一致する URL は、フィルタリングの対象になりません。
  - ワイルドカードの URL（例：www.uresour*loc.com）

- サブ URL（例：www.uresour* loc.com/support）
- サブドメイン（例：reach.url.com や sub1.url.com）

- テンプレートの作成時に、重複する URL がある場合、重複 URL ルールは考慮されません。

アクセス コントロール リストの設定

ステップ 1 [設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）] を選択し、左側の [デバイス グループ（Device Groups）] メニューから [デバイス タイプ（Device Type）] > [ワイヤレス コントローラ（Wireless Controller）] を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、[セキュリティ（Security）] > [URL ACLs] を選択します。

このページには、次のフィールドが表示されます。

- [チェックボックス（Check box）]：チェックボックスを使用して、削除する URL ACL を 1 つ以上選択します。
- [URL ACL 名（URL ACL 名）]：このテンプレートのユーザ定義名。URL ACL 項目をクリックし、説明を表示します。

ステップ 4 URL ACL をクリックします。

ステップ 5 [ルール（Rules）] の下にある [行の追加（Add Row）] をクリックして URL ACL ルールを追加します。

- [URL] テキスト ボックスに URL ACL の名前を入力します。
- [ルール アクション（Rule Action）] ドロップダウン リストから、[許可（Allow）] または [拒否（Deny）] を選択します。

ステップ 6 [保存（Save）] をクリックします。

コントローラまたはデバイスのセキュリティ設定の構成 （685 ページ）
URL ACL の削除 （718 ページ）

URL ACL の削除

URL ACL を削除するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）]** の順に選択します。

ステップ 2 コントローラ デバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[セキュリティ（Security）] > [URL ACLs]** を選択します。

ステップ 4 [URL ACLs] ページから、削除する URL ACL を 1 つ以上選択します。

ステップ 5 [コマンドの選択（Select a command）] ドロップダウン リストから [URL ACL の削除（Delete URL ACLs）] を選択します。

ステップ 6 [移動（Go）] をクリックします。

（注） ACL のカウンタをクリアする場合は、[コマンドの選択（Select a command）] ドロップダウン リストから [クリア（Clear）] を選択します。

関連トピック

アクセス コントロール リストの設定 （718 ページ）

フレキシブル ラジオ アサインメント

フレキシブル ラジオ アサインメント（FRA）は、Cisco Aironet 2800 および 3800 シリーズ アクセス ポイントで NDP 測定を分析し、新しいフレキシブル ラジオ（2.4 GHz、5 GHz、またはモニタ）の役割を判断するために使用するハードウェアを管理するために Radio Resource Management（RRM; 無線リソース管理）に追加された新しいコア アルゴリズムです。

FRA 機能により、対応可能な AP を手動で設定したり、これらの AP が、使用可能な RF 環境に基づいて統合無線の動作の役割をインテリジェントに決定したりできます。フレキシブル ラジオを備えた AP は、多数のデバイスがネットワークに接続しているときを自動的に検出し、アクセス ポイントのデュアル無線を 2.4 GHz/5 GHz から 5 GHz/5 GHz に変更し、より多くのクライアントにサービスを提供できます。AP は、パフォーマンスに影響を与える RF 干渉およびセキュリティ脅威に対しネットワークを監視しながら、このタスクを実行します。FRA により、高密度ネットワークのモバイル ユーザ エクスペリエンスが向上します。また、この機能によって、2.4GHz 無線の一部に冗長化のマークを付け、5GHz（クライアント側の役割）またはモニタの役割（2.4GHz および 5GHz）に切り替えることで、2.4GHz セルの輻輳が低減されます。無線の役割を設定するには、CLI または GUI を使用します。

フレキシブル ラジオを備えた AP は、次のモードで動作できます。

- デフォルトの動作モード：一方の無線では 2.4 GHz モードでクライアントにサービスを提供し、他方の無線では、5 GHz モードでサービスを提供します。
- デュアル 5 GHz モード：両方の無線が 5 GHz 帯域で動作し、802.11ac Wave 2 の利点を最大化し、クライアント デバイスのキャパシティを増やすために積極的にクライアントにサービスを提供します。
- ワイヤレス セキュリティ モニタリング：一方の無線では 5 GHz でクライアントにサービスを提供し、他方の無線では、wIPS 攻撃者、CleanAir 干渉源、不正なデバイスに対し 2.4 GHz 帯域および 5 GHz 帯域の両方でスキャンを行います。

フレキシブル ラジオ アサインメントの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network**	

	コマンドまたはアクション	目的
	Devices）] を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）]** > **[ワイヤレスコントローラ（Wireless Controller）]** を選択します。	
ステップ 2	該当するコントローラのデバイス名をクリックします。	
ステップ 3	左側のサイドバーのメニューから、**[802.11]** > **[フレキシブル ラジオ アサインメント（Flexible Radio Assignment）]** を選択します。[フレキシブル ラジオ アサインメント（Flexible Radio Assignment）] ページで次の内容を設定します。 • [フレキシブル ラジオ アサイメント（Flexible Radio Assignment）]：デフォルトでは FRA 機能は無効になっています。FRA を有効にし、 次のパラメータを設定するには、チェックボックスをオンにします。 • [感度（Sensitivity）]：FRA 感度しきい値を調整します。これにより、無線を冗長と見なす必要がある COF のパーセンテージ が設定されます。次の値をサポートしています。 • Low • 中 • 高 • [間隔（Interval）]：FRA の実行間隔を設定します。有効な範囲は 1 ～ 24 時間です。デフォルトの設定は1 時間です。FRA は DCA に依存しているため、FRA の間隔は、DCA の間隔を下回ることはできません。	

デバイスの 802.11 パラメータの設定

ここでは、次の項について説明します。

• 802.11 コントローラでの複数の国コードの設定
• どのようなときにコントローラが追加のクライアントアソシエーションを受け入れられなくなるかの指定（AP ロード バランシング）
• AP チャネル干渉を抑えるバンド選択の有効化

- MediaStream を使用した IP マルチキャスト配信の確保
- AP グループで使用できる RF プロファイルの作成

802.11 コントローラでの複数の国コードの設定

モビリティ グループに含まれていない単一のコントローラを複数の国をサポートするように設定するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[802.11] > [一般（General）]** を選択します。

ステップ 4 チェックボックスをオンにして追加する国を選択します。アクセス ポイントは規制基準の異なるさまざまな国で使用できるように設計されています。国の規制に準拠するように国コードを設定できます。

運用する国向けに設計されていない場合、アクセス ポイントは正しく動作しない可能性があります。たとえば、部品番号が AIR-AP1030-A-K9（米国の規制区域に含まれている）のアクセス ポイントは、オーストラリアでは使用できません。必ず自国の規制区域に合ったアクセス ポイントを購入するようにしてください。製品ごとのサポートされる国コードの完全なリストについては、http://www.cisco.com/warp/public/779/smbiz/wireless/approvals.html を参照してください。

ステップ 5 認証応答がタイムアウトになるまでの時間（秒単位）を入力します。

ステップ 6 [Save] をクリックします。

関連トピック

どのようなときにコントローラが追加のクライアントアソシエーションを受け入れられなくなるかの指定（AP ロード バランシング） （721 ページ）
AP チャネル干渉を抑えるバンド選択の有効化 （723 ページ）
MediaStream を使用した IP マルチキャスト配信の確保 （725 ページ）
AP グループで使用できる RF プロファイルの作成 （726 ページ）

どのようなときにコントローラが追加のクライアントアソシエーションを受け入れられなくなるかの指定（AP ロード バランシング）

コントローラ上でアグレッシブ ロード バランシングを有効にすると、Lightweight アクセス ポイント間で、アクセス ポイント全体のワイヤレス クライアントのロード バランスを行うことができます。クライアントの負荷は、同じコントローラ上のアクセス ポイント間で分散されます。別のコントローラ上のアクセス ポイントとの間では、ロード バランシングは行われません。

ワイヤレス クライアントが Lightweight アクセス ポイントへのアソシエートを試みると、アソシエーション応答パケットとともに 802.11 応答パケットがクライアントに送信されます。この 802.11 応答パケットの中にステータス コード 17 があります。このコードは、アクセス ポイン

トがそれ以上アソシエーションを受け付けることが可能かどうかを示します。アクセス ポイントへの負荷が高すぎる場合は、クライアントはそのエリア内の別のアクセス ポイントへのアソシエートを試みます。アクセス ポイントの負荷が高いかどうかは、そのクライアントからアクセス可能な、近隣の他のアクセス ポイントと比べて相対的に判断されます。

たとえば、AP1 上のクライアント数が、AP2 のクライアント数とロード バランシング ウィンドウの和を上回っている場合は、AP1 の負荷は AP2 よりも高いと判断されます。クライアントが AP1 にアソシエートしようとすると、ステータス コード 17 が含まれている 802.11 応答パケットがクライアントに送信されます。アクセス ポイントの負荷が高いことがこのステータス コードからわかるので、クライアントは別のアクセス ポイントへのアソシエーションを試みます。

10 回までクライアント アソシエーションを拒否するようコントローラを設定できます（クライアントが 11 回アソシエーションを試行した場合、11 回目の試行ではアソシエーションが許可されます）。また、特定の WLAN 上でロード バランシングを有効にするか、無効にするかも指定できます。これは、特定のクライアント グループ（遅延に敏感な音声クライアントなど）に対してロード バランシングを無効にする場合に便利です。

アグレッシブ ロード バランシングを設定するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）]** を選択し、左側の [デバイス グループ（Device Groups）] メニューから **[デバイス タイプ（Device Type）] > [ワイヤレス コントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[802.11] > [ロード バランシング（Load Balancing）]** を選択します。[Load Balancing] ページが表示されます。

ステップ 4 クライアントのウィンドウ サイズとして 1 ～ 20 までの値を入力します。このページ サイズは、アクセス ポイントの負荷が高すぎてそれ以上はクライアント アソシエーションを受け付けることができないかどうかを判断するアルゴリズムで使用されます。

ロード バランシング ページ + 最も負荷が低い AP 上のクライアント アソシエーション数 = ロード バランシングしきい値

特定のクライアント デバイスからアクセス可能なアクセス ポイントが複数ある場合に、アクセス ポイントはそれぞれ、アソシエートしているクライアントの数が異なります。クライアントの数が最も少ないアクセス ポイントは、負荷が最も低くなります。クライアントのページ サイズと、負荷が最も低いアクセス ポイント上のクライアント数の合計がしきい値となります。クライアント アソシエーションの数がこのしきい値を超えるアクセス ポイントはビジー状態であるとみなされ、クライアントがアソシエートできるのは、クライアント数がしきい値を下回るアクセス ポイントだけとなります。

ステップ 5 拒否の最大数として 0 ～ 10 までの値を入力します。拒否数は、ロード バランシング中のアソシエーション拒否の最大数を設定します。

ステップ 6 [Save] をクリックします。

ステップ 7 特定の WLAN でアグレッシブ ロード バランシングを有効または無効にするには、[WLAN Configuration] ページを参照して、[Advanced] タブをクリックします。[WLAN Configuration] ページの使用方法については、「関連項目」の「コントローラ WLAN の設定」を参照してください。

関連トピック

802.11 コントローラでの複数の国コードの設定 （721 ページ）
AP チャネル干渉を抑えるバンド選択の有効化 （723 ページ）
MediaStream を使用した IP マルチキャスト配信の確保 （725 ページ）
AP グループで使用できる RF プロファイルの作成 （726 ページ）
コントローラでの WLAN の作成 （652 ページ）

AP チャネル干渉を抑えるバンド選択の有効化

帯域選択によって、デュアルバンド（2.4 GHz および 5 GHz）動作が可能なクライアントの無線を、混雑の少ない 5 GHz アクセス ポイントに移動できます。2.4 GHz 帯域は、混雑していることがあります。この帯域のクライアントは一般に、Bluetooth デバイス、電子レンジ、およびコードレス電話機からの干渉を受けるだけでなく、他のアクセス ポイントからの同一チャネル干渉も発生します。802.11b/g では、重複しないチャネルが 3 つしかないからです。これらの干渉の原因を緩和して、ネットワーク全体のパフォーマンスを向上させるには、コントローラで帯域選択を設定できます。

帯域選択のしくみは、クライアントへのプローブ応答を規制するというものです。5 GHz チャネルへクライアントを誘導するために、2.4 GHz チャネルでのクライアントへのプローブ応答を遅らせます。

帯域選択をコントローラ上でグローバルに有効にすることも、特定の WLAN 上の帯域選択を有効または無効にすることもできます。後者は、特定のクライアントのグループ（遅延に敏感な音声クライアントなど）に対して帯域選択を無効にする場合に便利です。

帯域選択が有効になっている WLAN では、ローミングの遅延が発生するので、音声や映像のような、遅延に敏感なアプリケーションはサポートされません。

帯域選択の使用に関するガイドライン

帯域選択を使用する際には、次のガイドラインに従ってください。

- 帯域選択を使用できるのは、アクセス ポイントが Cisco Aironet 1140 または 1250 シリーズである場合だけです。
- 帯域選択が動作するのは、コントローラに接続されたアクセス ポイントに対してのみです。コントローラに接続しない FlexConnect アクセス ポイントは、リブート後に帯域選択を実行しません。
- 帯域選択アルゴリズムによるデュアル バンド クライアントの誘導は、同じアクセス ポイントの 2.4 GHz 無線から 5 GHz 無線に限られます。このアルゴリズムが機能するのは、アクセス ポイントで 2.4 GHz と 5 GHz の両方の無線が稼働している場合のみです。
- コントローラ上で帯域選択とアグレッシブ ロード バランシングの両方を有効にすることができます。これらは独立して動作し、相互に影響を与えることはありません。

帯域選択を設定するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[802.11] > [帯域選択（Band Select）]** を選択します。[帯域選択（Band Select）] ページが表示されます。

ステップ 4 プローブ サイクル回数として 1 ～ 10 までの値を入力します。サイクル回数は、新しいクライアントの抑制サイクルの回数を設定します。デフォルトのサイクル回数は 2 です。

ステップ 5 スキャン サイクル期間の閾値として 1 ～ 1000 ミリ秒までの値を入力します。この設定は、クライアントからの新しいプルーブ要求が新しいスキャン サイクルから送信される間の時間しきい値を決定します。デフォルトのサイクルしきい値は 200 ミリ秒です。

ステップ 6 [エージング アウト抑制（age out suppression）] フィールドに 10 ～ 200 秒までの値を入力します。エージング アウト抑制は、以前に認識されていた 802.11b/g クライアントをプルーニングするための期限切れ時間を設定します。デフォルト値は 20 秒です。この時間が経過すると、クライアントは新規とみなされて、プローブ応答抑制の対象となります。

ステップ 7 [エージング アウト デュアル バンド（age out dual band）] フィールドに 10 ～ 300 秒までの値を入力します。エージング アウト期間は、以前に認識されていたデュアルバンド クライアントをプルーニングするための期限切れ時間を設定します。デフォルト値は 60 秒です。この時間が経過すると、クライアントは新規とみなされて、プローブ応答抑制の対象となります。

ステップ 8 [acceptable client RSSI] フィールドに –20 ～ –90 dBm までの値を入力します。このフィールドは、クライアントがプローブに応答するための最大 RSSI を設定します。デフォルト値は -80 dBm です。

ステップ 9 [Save] をクリックします。

ステップ 10 特定の WLAN で帯域選択を有効または無効にするには、[WLAN Configuration] ページを参照して、[Advanced] タブをクリックします[WLAN Configuration] ページの使用方法については、「関連項目」の「コントローラ WLAN の設定」を参照してください。

802.11 コントローラでの複数の国コードの設定 （721 ページ）
どのようなときにコントローラが追加のクライアント アソシエーションを受け入れられなくなるかの指定（AP ロード バランシング） （721 ページ）
MediaStream を使用した IP マルチキャスト配信の確保 （725 ページ）
AP グループで使用できる RF プロファイルの作成 （726 ページ）
コントローラでの WLAN の作成 （652 ページ）

SIP コールの優先度の制御

優先コール機能を使用すると、特定の番号に対して行う SIP コールに最高の優先度を指定できます。高い優先度を設定するには、設定済みの音声プールに使用可能な音声帯域幅がない場合でも、そのような優先 SIP コールに帯域幅を割り当てます。この機能は、WCS または WLC で帯域幅割り当てに SIP ベースの CAC を使用するクライアントのみでサポートされます。

コントローラごとに最大 6 個の番号を設定できます。

優先コール サポートを設定するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[802.11] > [優先コール（Preferred Call）]** を選択します。既存の優先コールがある場合は、次のフィールドが表示されます。

- [Description]：優先コールの説明。
- [Number Id]：コントローラの固有識別子を示し、コントローラに割り当てられている 6 個の優先コール番号の 1 つを示します。
- [Preferred Number]：優先コール番号を示します。

ステップ 4 [Select a command] ドロップダウン リストから、[Add Number] を選択します。

ステップ 5 このコントローラに適用するテンプレートを選択します。

選択したコントローラに適用するテンプレートを選択する必要があります。優先コール番号用の新しいテンプレートを作成するには、「関連項目」の「優先コール テンプレートの設定」を参照してください。

ステップ 6 [Apply] をクリックします。

優先コールを削除するには、該当する優先コール番号のチェックボックスを選択して、[Select a command] ドロップダウン リストから [Delete] を選択します。[Go] をクリックし、[OK] をクリックして削除を確認します。

関連トピック

802.11 コントローラでの複数の国コードの設定 （721 ページ）
どのようなときにコントローラが追加のクライアントアソシエーションを受け入れられなくなるかの指定（AP ロード バランシング） （721 ページ）
AP チャネル干渉を抑えるバンド選択の有効化 （723 ページ）
AP グループで使用できる RF プロファイルの作成 （726 ページ）

MediaStream を使用した IP マルチキャスト配信の確保

802.11 のメディア パラメータを設定するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[802.11] > [メディア ストリーム（Media Stream）]** を選択します。

ステップ 4 [Media Stream Configuration] セクションで、次のパラメータを設定します

- Media Stream Name
- [Multicast Destination Start IP]：マルチキャストまでのメディア ストリームの開始 IP アドレス
- [Multicast Destination End IP]：マルチキャストまでのメディア ストリームの終了 IP アドレス
- [Maximum Expected Bandwidth]：メディア ストリームが使用できる最大帯域幅

ステップ 5 [Resource Reservation Control (RRC) Parameters] グループ ボックスで、次のパラメータを設定します。

- [Average Packet Size]：メディア ストリームが使用できる平均パケット サイズ。
- [RRC Periodical Update]：定期的に更新されるリソース予約コントロールの計算。無効にすると、RRC の計算は、クライアントがメディア ストリームに加入したときに、1 回のみ行われます。
- [RRC Priority]：最高が 1、最低が 8 の RRC の優先度。
- [Traffic Profile Violation]：ストリームが QoS ビデオ プロファイルに違反したときに、ストリームがドロップされるか、ベスト エフォート キューに入れられる場合に表示されます。
- [Policy]：メディア ストリームが許可されるか拒否される場合に表示されます。

ステップ 6 **[保存（Save）]** をクリックします。

AP グループで使用できる RF プロファイルの作成

[RF プロファイル（RF Profiles）] ページでは、AP グループに関連付ける RF プロファイルを作成または変更できます。

コントローラの RF プロファイルを設定するには、次の手順を実行します。

ステップ 1 [設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）] を選択し、左側の [デバイスグループ（Device Groups）] メニューから [デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）] を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 [RF Profiles] をクリックするか、左側のサイドバー メニューから [802.11] > [RF Profiles] を選択します。[RF Profiles] ページが表示されます。このページには、既存の RF プロファイル テンプレートがリストされます。

ステップ 4 RF プロファイルを追加する場合は、[Select a command] ドロップダウン リストから [Add RF Profile] を選択します。

ステップ 5 [Go] をクリックします。[New Controller Template] ページが表示されます。

ステップ 6 次の情報を設定します。

- General

- [Template Name]：テンプレートのユーザ定義の名前。[Profile Name]：現在のプロファイルのユーザ定義の名前。[Description]：テンプレートの説明。
- [Radio Type]：アクセス ポイントの無線タイプ。これは、802.11a または 802.11b 無線がある AP の RF プロファイルを選択できるドロップダウン リストです。

- TCP（送信電力制御）
  - [Minimum Power Level Assignment (-10 to 30 dBm)]：割り当てられている最小電力を示します。範囲は -10 ～ 30 dB で、デフォルト値は 30 dB です。
  - [Maximum Power Level Assignment (-10 to 30 dBm)]：割り当てられている最大電力を示します。範囲は -10 ～ 30 dB で、デフォルト値は 30 dB です。
  - [Power Threshold v1(-80 to -50 dBm)]：送信電力しきい値を示します。[Power Threshold v2(-80 to -50 dBm)]：送信電力しきい値を示します。

- [Data Rates]：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指定するには、[Data Rates] ドロップダウン リストを使用します。次のデータ レートが使用可能です。
  - [802.11a]：6、9、12、18、24、36、48、および 54 Mbps。
  - [802.11b/g]：1、2、5.5、6、9、11、12、18、24、36、48、または 54 Mbps。

  各データ レートに対して、次のオプションのいずれかを選択します。

  - [Mandatory]：このコントローラ上のアクセス ポイントに関連付けるには、クライアントがこのデータ レートをサポートしている必要があります。
  - [Supported]：関連付けられたクライアントは、このデータ レートをサポートしていれば、このレートを使用してアクセス ポイントと通信できます。ただし、クライアントがこのレートを使用できなくても、関連付けは可能です。
  - [Disabled]：通信に使用するデータ レートは、クライアントが指定します。

ステップ 7 [Save] をクリックします。

関連トピック

802.11 コントローラでの複数の国コードの設定 （721 ページ）
どのようなときにコントローラが追加のクライアントアソシエーションを受け入れられなくなるかの指定（AP ロード バランシング） （721 ページ）
AP チャネル干渉を抑えるバンド選択の有効化 （723 ページ）

デバイスの 802.11a/n パラメータの設定

特定のコントローラの 802.11a/n パラメータを表示するには、次の手順を実行します。

ステップ 1 [設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）] を選択し、左側の [デバイスグループ（Device Groups）] メニューから [デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）] を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、次のいずれかを選択します。

- [802.11a/n] > [パラメータ（Parameters）] : パラメータを表示または編集します。
- [802.11a、または n あるいは ac（802.11a or n or ac）] > [dot11a-RRM] > [RRM しきい値（RRM Thresholds）] ：802.11a/n RRM しきい値コントローラを設定します。
- [802.11a/n] > [RRM 間隔（RRM Intervals）] または [802.11b/g/n] > [RRM 間隔（RRM Intervals）] : 個々のコントローラに 802.11a/n または 802.11b/g/n の RRM しきい値を設定します。
- [802.11a/n-RRM] > [TPC] ：802.11a/n または 802.11b/g/n の RRM 伝送パワー コントロールを設定します。
- [802.11a または n あるいは ac（802.11a or n or ac）] > [dot11a-RRM] > [DCA]：RRM 動的チャネル割り当てを設定します。
- [802.11a/n] > [RRM] > [RF グループ化（RF Grouping）] ：個々のコントローラに 802.11a/n または 802.11b/g/n の RRM 無線のグループ化を設定します。
- [802.11a/n] > [メディア パラメータ（Media Parameters）] : 802.11a/n にメディア パラメータを設定します。
- [802.11a/n] > [EDCA パラメータ（EDCA Parameters）] または [802.11b/g/n] > [EDCA] : 個々のコントローラに 802.11a/n または 802.11b/g/n の EDCA パラメータを設定します。
- [802.11a/n] > [ローミング パラメータ（Roaming Parameters）] : 802.11a/n または 802.11b/g/n のローミング パラメータを設定します。
- [802.11a/n] > [802.11h] または [802.11b/g/n] > [802.11h] : 個々のコントローラに 802.11h パラメータを設定します。
- 802.11a/n または 802.11b/g/n 高スループット パラメータを設定する場合は、[802.11a/n] > [高スループット（High Throughput）] または [802.11b/g/n] > [高スループット（High Throughput）]。
- [802.11a/n] > [CleanAir] : 802.11a/n CleanAir パラメータを設定します。

ステップ 4 [保存（Save）] をクリックします。

デバイスの 802.11b/g/n パラメータの設定

特定のコントローラの 802.11b/g/n パラメータを表示するには、次の手順を実行します。

ステップ 1 [設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）] を選択し、左側の [デバイスグループ（Device Groups）] メニューから [デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）] を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、次のいずれかを選択します。

- [802.11b/g/n パラメータ（802.11b/g/n Parameters）]：パラメータを表示または編集します。
- [802.11b または g あるいは n（802.11b or g or n）] > [dot11b-RRM] > [しきい値（Tresholds）]：802.11b/g/n RRM しきい値を設定します。
- [802.11a/n] > [RRM 間隔（RRM Intervals）] または [802.11b/g/n] > [RRM 間隔（RRM Intervals）]：802.11b/g/n RRM 間隔を設定します。
- [802.11b/g/n-RRM] > [TPC]：802.11b/g/n RRM 伝送パワー コントロール パラメータを設定します。
- [802.11b または g あるいは n（802.11b or g or n）] > [dot11b-RRM] > [DCA]：個々のコントローラに 802.11a/n または 802.11b/g/n の RRM DCA チャネルを設定します。
- [802.11b/g/n] > [RRM] > [RF グループ化（RF Grouping）：個々のコントローラに 802.11a/n または 802.11b/g/n の RRM 無線グループ化を設定します。
- [802.11b/g/n] > [メディア パラメータ（Media Parameters）]：802.11b/g/n にメディア パラメータを設定します。
- [802.11a/n] > [EDCA パラメータ（EDCA Parameters）] または [802.11b/g/n] > [EDCA]：個々のコントローラに 802.11a/n または 802.11b/g/n の EDCA パラメータを設定します。
- [802.11a/n] > [ローミング パラメータ（Roaming Parameters）] または [802.11b/g/n] > [ローミング パラメータ（Roaming Parameters）]：802.11a/n または 802.11b/g/n の EDCA パラメータを設定します。
- 802.11a/n または 802.11b/g/n 高スループット パラメータを設定する場合は、[802.11a/n] > [高スループット（High Throughput）] または [802.11b/g/n] > [高スループット（High Throughput）]。
- [802.11b/g/n] > [CleanAir]：802.11b/g/n CleanAir パラメータを設定します。

ステップ 4 [保存（Save）] をクリックします。

デバイスのメッシュ パラメータの設定

個々のコントローラのメッシュ パラメータを設定するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）]** を選択し、左側の [デバイス グループ（Device Groups）] メニューから **[デバイス タイプ（Device Type）] > [ワイヤレス コントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバー メニューから、**[メッシュ（Mesh）] > [メッシュ設定（Mesh Settings）]** を選択します。

ステップ 4 次のメッシュ パラメータを表示または編集します。

- [RootAP to MeshAP Range]：デフォルトでは、この値は 12,000 フィートです。150 ～ 132,000 フィートの値を入力できます。ルートアクセスポイントとメッシュアクセスポイント間の適切な距離をフィート単位で入力します。このグローバルフィールドは、コントローラにアクセスポイントが接続される

とすべてのアクセス ポイントに適用され、ネットワーク内に存在するすべての既存のアクセス ポイントにも適用されます。

- [Client Access on Backhaul Link]：この機能を有効にすると、802.11a バックホールを介してメッシュ アクセス ポイントを 802.11a ワイヤレス クライアントに関連付けることができます。これは、ルートとメッシュ アクセス ポイント間の 802.11a バックホール上の既存の通信に追加されます。この機能は 2 つの無線のあるアクセス ポイントだけに適用されます。バックホール クライアント アクセスを変更すると、すべてのメッシュ アクセス ポイントがリブートされます。詳細については、「関連項目」の「1524SB デュアル バックホールでのクライアント アクセス」を参照してください。

  メッシュのバックグラウンド スキャンおよび自動親選択機能により、メッシュ アクセス ポイント（MAP）は全チャネルにわたってより良い潜在的親を検索して接続し、常に最良の親にアップリンクすることができます。

  この機能により、すべてのチャネルをスキャンすることによりチャネル全体にわたって親を検索するという時間のかかるタスクが削減されます。オフチャネル手順は、選択したチャネルでブロードキャスト パケットを送信し（3 秒間隔、オフチャネルあたり最大 50 ミリ秒）、すべての「到達可能」ネイバーからパケットを受信します。これにより、子 MAP はチャネル全体にわたるネイバー情報で更新され、新しいネイバーに「切り替え」てアップリンクの親として使用することができます。「切り替え」は、親損失の検出でトリガーされる必要はありませんが、より良い親の識別時にトリガーされます。ただし、子 MAP では現在の親アップリンクがアクティブなままとなります。

- [バックグラウンド スキャン（Background Scanning）]：メッシュのバックグラウンド スキャン機能を有効にするには、[バックグラウンド スキャン（Background Scanning）] チェックボックスをオンにします。デフォルトでは、無効に設定されています。

- [Mesh DCA Channels]：このオプションを有効にすると、DCA チャネル リストを使用してコントローラでバックホール チャネルを選択解除できるようになります。コントローラ DCA リスト内のチャネルに対する変更はすべて、関連付けられたアクセス ポイントに適用されます。このオプションは、1524SB メッシュ アクセス ポイントのみに適用可能です。詳細については、「関連項目」の「コントローラでのバックホール チャネル選択解除」を参照してください。
- [メッシュ RAP ダウンリンク バックホール（Mesh RAP Downlink Backhaul）]：バックホール ダウンリンク スロットを変更すると、すべてのメッシュ AP がリブートされます。
- [UNII 1 帯域チャネルの屋外アクセス（Outdoor Access For UNII 1 Band Channels）]
- [Global Public Safety]：このオプションを有効にすると、802.11a バックホール無線のチャネルを選択することで、4.9 GHz をバックホール リンクで使用できます。公共安全帯域とされる 4.9 Ghz の使用は、一部のサービス プロバイダーに限られています。この設定は、コントローラ レベルで適用されます。

- [Security Mode]：[Security Mode] ドロップダウン リストから [EAP]（拡張認証プロトコル）または [PSK]（事前共有キー）を選択します。セキュリティを変更すると、すべてのメッシュ アクセス ポイントがリブートされます。

ステップ 5 [Save] をクリックします。

関連トピック

1524 SB AP でのバックホール無線へのクライアント アクセスの無効化 （731 ページ）
コントローラでのバックホール チャネル選択解除の有効化 （732 ページ）

1524 SB AP でのバックホール無線へのクライアント アクセスの無効化

1524 シリアルバックホール（SB）アクセス ポイントは、3 つの無線スロットで構成されます。

- スロット 0 の無線は 2.4 GHz の周波数帯域で動作し、クライアント アクセスに使用されます。
- スロット 1 とスロット 2 の無線は 5.8 GHz 帯域で動作し、主にバックホールに使用されます。

2 つの 802.11a バックホール無線は、同じ MAC アドレスを使用します。同じ WLAN が複数のスロット内の同じ BSSID にマップされることがあります。

デフォルトでは、両方のバックホール無線を介したクライアントアクセスが無効になります。

無線スロットを有効または無効にする場合は、これらのガイドラインに従う必要があります。

- スロット 2 でのクライアント アクセスが無効の場合でも、スロット 1 でクライアント アクセスを有効にできます。
- スロット 1 でのクライアント アクセスが有効の場合のみ、スロット 2 でクライアント アクセスを有効にできます。
- スロット 1 でクライアント アクセスを無効にすると、スロット 2 でのクライアント アクセスは自動的に無効になります。
- クライアント アクセスを有効または無効にすると常に、すべてのメッシュ アクセス ポイントがリブートされます。

ユニバーサル クライアント アクセス機能を使用すると、スロット 1 とスロット 2 の両方の無線でクライアントアクセスが可能です。次のいずれかから、バックホール無線によるクライアント アクセスを設定できます。

- コントローラのコマンドライン インターフェイス（CLI）
- コントローラのグラフィカル ユーザ インターフェイス（GUI）
- Prime Infrastructure GUI。

2 つのバックホール無線でクライアント アクセスを設定するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）]** > **[ネットワーク（Network）]** > **[ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）]** > **[ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバー メニューから、**[メッシュ（Mesh）]** > **[メッシュ設定（Mesh Settings）]** を選択します。

ステップ 4 [Client Access on Backhaul Link] チェックボックスを選択します。

ステップ 5 [Extended Backhaul Client Access] チェックボックスをオンにします。

ステップ 6 [Save] をクリックします。

警告メッセージが表示されます。

例：

```
Enabling client access on both backhaul slots will use same BSSIDs on both the slots. Changing
Backhaul Client Access will reboot all Mesh APs.
```

ステップ 7 [OK] をクリックします。

ユニバーサル クライアント アクセスが、両方の無線で設定されます。

関連トピック

コントローラでのバックホール チャネル選択解除の有効化 （732 ページ）
デバイスのメッシュ パラメータの設定 （729 ページ）

コントローラでのバックホール チャネル選択解除の有効化

バックホール チャネルの選択解除を設定するには、次の手順を実行します。

ステップ 1 コントローラでメッシュ DCA チャネル フラグを設定します。「関連項目」の「1524 SB AP でのバックホール無線へのクライアント アクセスの無効化」を参照してください。

ステップ 2 設定グループを使用してチャネル リストを変更します。「関連項目」の「Prime Infrastructure 設定グループを使用したコントローラ チャネル リストの変更」を参照してください。

関連トピック

1524 SB AP でのバックホール無線へのクライアント アクセスの無効化 （731 ページ）
デバイスのメッシュ パラメータの設定 （729 ページ）
Cisco Prime Infrastructure 設定グループを使用したコントローラ チャネル リストの変更 （733 ページ）

コントローラから 1524 SB AP へのチャネル変更のプッシュ

1 つ以上のコントローラでの各チャネルの変更を、関連付けられたすべての 1524SB アクセス ポイントに適用するよう、メッシュ DCA チャネル フラグを設定できます。この機能を設定するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバー メニューから、**[メッシュ（Mesh）] > [メッシュ設定（Mesh Settings）]** を選択します。

ステップ 4 [Mesh DCA Channels] チェックボックスをオンにしてチャネル選択を有効にします。このオプションは、デフォルトでは選択解除されています。

コントローラでのチャネルの変更が、関連付けられた 1524SB アクセス ポイントに適用されます。

Cisco Prime Infrastructure 設定グループを使用したコントローラ チャネル リストの変更

コントローラの設定グループを使用して、バックホールチャネルの選択解除を設定できます。設定グループを作成して、必要なコントローラをグループに追加し、[Country/DCA] タブを使用してそのグループ内のコントローラのチャネルを選択または選択解除できます。

設定グループを使用してバックホールチャネルの選択解除を設定するには、次の手順を実行します。

ステップ 1 [Configuration] > [Controller Configuration Groups] を選択します。
ステップ 2 設定グループの詳細を表示する設定グループを選択します。
ステップ 3 [Configuration Group] 詳細ページで、[Country/DCA] タブをクリックします。
ステップ 4 [国/DCA の更新（Update Country/DCA）] チェックボックスをオンまたはオフにします。

関連トピック

1524 SB AP でのバックホール無線へのクライアント アクセスの無効化 （731 ページ）
コントローラでのバックホール チャネル選択解除の有効化 （732 ページ）
デバイスのメッシュ パラメータの設定 （729 ページ）
コントローラから 1524 SB AP へのチャネル変更のプッシュ （732 ページ）

デバイスのポート パラメータの設定

個々のコントローラのポート パラメータを設定するには、次の手順を実行します。

ステップ 1 [Configuration] > [Network] > [Network Devices] を選択し、[Device Type] > [Wireless Controller] を選択します。
ステップ 2 該当するデバイスをクリックします。
ステップ 3 左側のサイドバー メニューから、[Ports] > [Port Settings] を選択します。
ステップ 4 該当するポート番号をクリックして、[Port Settings Details] ページを開きます。次のようなパラメータが表示されます。

- General Parameters：
  - [Port Number]：読み取り専用。
  - [Admin Status]：ドロップダウン リストから [Enabled] または [Disabled] を選択します。
  - [Physical Mode]：自動ネゴシエーション（読み取り専用）。
  - [Physical Status]：全二重 1000 Mbps（読み取り専用）。
  - [STP Mode]：[802.1D]、[Fast]、または [Off] を選択します。
  - [Link Traps]：[Enabled] または [Disabled] を選択します。
  - Power Over Ethernet
  - [Multicast Application Mode]：[Enabled] または [Disabled] を選択します。
  - [Port Mode SFP Type]：読み取り専用。
- Spanning Tree Protocol Parameters：

- [Priority]：最適なスイッチのプライオリティ番号。
- [Path Cost]：ネットワーク管理者によって割り当てられ、インターネットワーク環境で最も望ましいパス（コストが低いほど、適したパスになります）を判別するために使用される値（通常、ホップ カウント、メディア帯域幅、またはその他の測定に基づく）。

ステップ 5 [保存（Save）] をクリックします。

関連トピック

デバイスのメッシュ パラメータの設定 （729 ページ）
コントローラの管理パラメータの設定 （734 ページ）
コントローラの IPv6 ネイバー バインドと RA パラメータの設定 （745 ページ）
コントローラのプロキシ モバイル IPv6（PMIP）パラメータの設定 （747 ページ）
コントローラのロケーション情報の設定 （743 ページ）
コントローラのマルチキャスト DNS（mDNS）設定の構成 （751 ページ）
コントローラの Application Visibility and Control（AVC）パラメータの設定 （753 ページ）
コントローラの NetFlow 設定の構成 （755 ページ）

コントローラの管理パラメータの設定

コントローラの次の管理パラメータを設定できます。

- トラップ レシーバ
- トラップ コントロール
- Telnet および SSH
- 複数の Syslog サーバ
- Web 管理
- ローカル管理ユーザ
- 認証優先度

関連トピック

コントローラ トラップの設定 （735 ページ）
コントローラでの Syslog サーバの設定 （738 ページ）
コントローラの Telnet SSH セッション パラメータの設定 （737 ページ）
コントローラでの Web 管理の設定 （740 ページ）
コントローラでのローカル管理ユーザの設定 （741 ページ）
コントローラの管理認証サーバ優先度の設定 （742 ページ）

コントローラのトラップ レシーバの設定

トラップ レシーバ パラメータは、個々のワイヤレス コントローラに設定できます。ワイヤレス コントローラに対してこのパラメータを追加および削除できます。[設定（Configuration）] > [機能およびテクノロジー（Features & Technologies）] でテンプレートを作成することで、トラップ レシーバを追加できます。

個々のコントローラのトラップ レシーバを設定するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[管理（Management）] > [トラップ レシーバ（Trap Receiver）]** を選択します。

ステップ 4 現在のトラップ レシーバについて、次のパラメータが表示されます。

- [Community Name]：トラップ レシーバの名前。
- [IP Address]：サーバの IP アドレス。
- [Admin Status]：SNMP トラップをレシーバに送信するには、ステータスを有効にする必要があります。

ステップ 5 詳細にアクセスするには、レシーバ名をクリックします。

ステップ 6 トラップ レシーバを有効にするには、[Admin Status] チェックボックスを選択します。トラップ レシーバを無効にするには、このチェックボックスを選択解除します。

ステップ 7 [Save] をクリックします。

ステップ 8 レシーバを削除するには、該当するレシーバのチェックボックス（複数可）をオンにします。

ステップ 9 [Select a command] ドロップダウン リストから [Delete Receivers] を選択します。

ステップ 10 [Go] をクリックします。

ステップ 11 確認メッセージで [OK] をクリックします。

コントローラ トラップの設定

個々のコントローラのトラップ制御パラメータを設定するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[管理（Management）] > [トラップ コントロール（Trap Control）]** を選択します。

ステップ 4 このコントローラの次のトラップを有効にできます。

- 一般的なトラップ
  - [SNMP Authentication]：SNMPv2 エンティティが、適切に認証されていないプロトコル メッセージを受信しました。SNMP V3 モードで設定されているユーザが正しくないパスワードでコント

ローラにアクセスを試みると、認証は失敗し、エラー メッセージが表示されます。ただし、認証エラーの場合、トラップ ログは生成されません。[Link (Port) Up/Down]：リンクのステータスは、アップまたはダウンから変更されます。[Multiple Users]：2 人のユーザが同じログイン ID でログインしています。[Spanning Tree]：スパニング ツリー トラップ。個々のパラメータについては、STP 仕様を参照してください。[Rogue AP]：不正 AP が検出されるたびに、このトラップが MAC アドレスとともに送信されます。以前に検出された不正 AP については、存在しなくなるとこのトラップが送信されます。[Config Save]：コントローラ設定が変更されると送信される通知。[RFID Limit Reached Threshold]：RFID 制限の最大許容値。

- クライアント関連トラップ
  - [802.11 Association]：クライアントがアソシエーション フレームを送信すると、アソシエーション通知が送信されます。[802.11 Disassociation]：クライアントがディスアソシエーション フレームを送信すると、ディスアソシエーション通知が送信されます。[802.11 Deauthentication]：クライアントが認証解除フレームを送信すると、認証解除通知が送信されます。[802.11 Failed Authentication]：クライアントが「成功」以外のステータス コードの認証フレームを送信すると、認証エラー通知が送信されます。[802.11 Failed Association]：クライアントが「成功」以外のステータス コードのアソシエーション フレームを送信すると、アソシエーション エラー通知が送信されます。[Excluded]：クライアントが除外されると、アソシエーションエラー通知が送信されます。[802.11 Authenticated]：クライアントがステータス コード「successful」で認証フレームを送信すると、認証通知が送信されます。[MaxClients Limit Reached Threshold]：許可されるクライアントの最大数。

- Cisco AP トラップ
  - [AP 登録（AP Register）]：アクセス ポイントがコントローラとアソシエートまたはアソシエート解除すると送信される通知です。[AP Interface Up/Down]：アクセス ポイント インターフェイス（802.11a または 802.11b/g）のステータスがアップまたはダウンになると送信される通知。

- 自動 RF プロファイル トラップ
  - [Load Profile]：[Load Profile] 状態が PASS と FAIL の間で変更されると送信される通知。[Noise Profile]：[Noise Profile] 状態が PASS と FAIL の間で変更されると送信される通知。[Interference Profile]：[Interference Profile] 状態が PASS と FAIL の間で変更されると送信される通知。[Coverage Profile]：[Coverage Profile] 状態が PASS と FAIL の間で変更されると送信される通知。

- 自動 RF 更新トラップ
  - [Channel Update]：アクセス ポイントの動的チャネル アルゴリズムが更新されると送信される通知。[Tx Power Update]：アクセス ポイントの動的送信電力アルゴリズムが更新されると送信される通知。

- AAA トラップ
  - [User Auth Failure]：このトラップは、クライアントの RADIUS 認証の失敗が発生したことを通知します。[RADIUS Server No Response]：このトラップは、RADIUS クライアントが送信した認証要求に応答する RADIUS サーバがないことを示します。

- 802.11 セキュリティ トラップ

- [WEP Decrypt Error]：コントローラが WEP 復号化エラーを検出すると送信される通知です。[Signature Attack]：シグニチャ攻撃が RADIUS 認証を使用するワイヤレス コントローラで検出されると送信される通知です。

ステップ 5 該当するパラメータの選択後に、[Save] をクリックします。

関連トピック

コントローラのトラップ レシーバの設定 （734 ページ）
コントローラでの Syslog サーバの設定 （738 ページ）
コントローラの Telnet SSH セッション パラメータの設定 （737 ページ）
コントローラでの Web 管理の設定 （740 ページ）
コントローラでのローカル管理ユーザの設定 （741 ページ）
コントローラの管理認証サーバ優先度の設定 （742 ページ）

コントローラの Telnet SSH セッション パラメータの設定

個々のコントローラの Telnet SSH（セキュア シェル）パラメータを設定するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）]** を選択し、左側の [デバイス グループ（Device Groups）] メニューから **[デバイス タイプ（Device Type）] > [ワイヤレス コントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[管理（Management）] > [Telnet SSH]** を選択します。

次のパラメータを設定できます。

- [Session Timeout]：ログオフされるまでに Telnet セッションが非アクティブの状態を継続できる分数を示します。0 は、タイムアウトしないことを意味します。0 ～ 160 までの数値で指定できます。工場出荷時のデフォルトは 5 です。
- [Maximum Sessions]：ドロップダウン リストから、0 ～ 5 までの値を選択します。このオブジェクトは、許可される同時 Telnet セッションの数を示します。
- [Allow New Telnet Sessions]：[no] に設定すると、DS ポートでは新しい Telnet セッションが許可されません。工場出荷時のデフォルト値は [no] です。DS（ネットワーク）ポートでの新しい Telnet セッションを許可または禁止できます。サービス ポートでは、新しい Telnet セッションは常に許可されます。
- [Allow New SSH Sessions]：[no] に設定すると、新しいセキュア シェル Telnet セッションが許可されません。工場出荷時のデフォルト値は [yes] です。

ステップ 4 該当するパラメータを設定した後、[保存（Save）] をクリックします。

関連トピック

コントローラのトラップ レシーバの設定 （734 ページ）
コントローラでの Syslog サーバの設定 （738 ページ）
コントローラでの Web 管理の設定 （740 ページ）
コントローラでのローカル管理ユーザの設定 （741 ページ）
コントローラの管理認証サーバ優先度の設定 （742 ページ）

コントローラでの Syslog サーバの設定

リリース 5.0.148.0 以降のコントローラでは、WLAN コントローラで複数（3 つまで）の Syslog サーバを設定できます。それぞれのメッセージが記録されると、メッセージの重大度が設定済みの Syslog フィルタ重大度レベル以上である場合、コントローラは、メッセージのコピーを設定済みの各 Syslog ホストに送信します。

個々のコントローラの Syslog を有効にするには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[管理（Management）] > [複数の Syslog（Multiple Syslog）]** を選択します。

適用されるテンプレートが示されます。

[Syslog Server Address]：該当する Syslog のサーバ アドレスを示します。

ステップ 4 [保存（Save）] をクリックします。

ステップ 5 syslog サーバを削除するには、syslog サーバのチェックボックスをオンにします。

ステップ 6 [コマンドの選択（Select a command）] ドロップダウン リストから [Syslog サーバの削除（Delete Syslog Servers）] を選択します。

ステップ 7 [Go] をクリックします。

ステップ 8 確認メッセージで [OK] をクリックします。

関連トピック

コントローラのトラップ レシーバの設定 （734 ページ）
コントローラ トラップの設定 （735 ページ）
コントローラの Telnet SSH セッション パラメータの設定 （737 ページ）
コントローラでの Web 管理の設定 （740 ページ）
コントローラでのローカル管理ユーザの設定 （741 ページ）
コントローラの管理認証サーバ優先度の設定 （742 ページ）

ネットワーク アシュアランスの設定

クライアントに関連するデータを Web サーバに定期的にプッシュするには、通常の WLC の機能に加え、ネットワーク アシュアランスを有効にします。このデータは、新たに導入されたアシュアランス関連のダッシュボードへのインプットとして使用されます。コントローラにネットワーク アシュアランスを設定するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[管理（Management）] > [ネットワークアシュアランス（Network Assurance）]** の順に選択します。

ステップ 4 適用されているテンプレートを表示し、次のパラメータを設定することができます。

- [アシュアランスサーバにデータをパブリッシュする（Publish Data to Assurance Server）]：ネットワーク アシュアランス機能を制御するグローバル レベルのフィールドです。
- [データの外部化（Data Externalization）]：データ モデルに関するコントローラ設定です。ネットワーク アシュアランスを有効にするには、最初に [データの外部化（Data Externalization）] を有効にする必要があります。[データの外部化（Data Externalization）] フィールドの値を変更するには、WLC の再起動が必要です。
- [NAサーバのURL（NA Server URL）]：WLC がクライアント データを定期的にポストするサーバのアドレスです。サーバ アドレスには、ホスト ベースまたは IP アドレス ベースのアドレスを指定できます。[NAサーバのURL（NA Server URL）] がホスト ベースの場合、NA サーバの CA 証明書はホスト名に対して生成する必要があります。同様に、URL が IP アドレス ベースの場合は、証明書は IP アドレスで生成する必要があります。

ステップ 5 [保存（Save）] をクリックします。

関連トピック

コントローラへの NA サーバ CA 証明書のダウンロード （604 ページ）
ネットワーク アシュアランスの自己署名付き証明書を生成 （602 ページ）
コントローラのトラップ レシーバの設定 （734 ページ）
コントローラでの Syslog サーバの設定 （738 ページ）
コントローラの Telnet SSH セッション パラメータの設定 （737 ページ）
コントローラでの Web 管理の設定 （740 ページ）
コントローラでのローカル管理ユーザの設定 （741 ページ）
コントローラの管理認証サーバ優先度の設定 （742 ページ）

コントローラでの Web 管理の設定

この項では、ディストリビューション システム ポートを Web ポート（HTTP を使用）またはセキュア Web ポート（HTTPS を使用）として有効にする手順について説明します。HTTPS を有効化すると、GUI との通信を保護できます。HTTPS は、Secure Socket Layer（SSL）プロトコルを使用して HTTP ブラウザ セッションを保護します。HTTPS を有効にすると、コントローラは独自の Web アドミニストレーション SSL 証明書を生成して、自動的に GUI に割り当てます。外部で生成された証明書をダウンロードできます。

個々のコントローラの WEB 管理パラメータを有効にするには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[管理（Management）] > [Web 管理（Web Admin）]** を選択します。

次のパラメータを設定できます。

- [WEB Mode]：ドロップダウン リストから [Enable] または [Disable] を選択します。有効にすると、ユーザは、*https://ip-address* を使用してコントローラの GUI にアクセスできます。デフォルトでは無効になっています。Web モードの接続は、セキュリティで保護されません。
- [Secure Web Mode]：ドロップダウン リストから [Enable] または [Disable] を選択します。有効にした場合、ユーザは *https://ip-address* を使用してコントローラ GUI にアクセスできます。デフォルトは [Enabled] です。
- [Certificate Type]：Web 管理証明書をダウンロードする必要があります。新しい Web 管理証明書を有効にするには、コントローラをリブートする必要があります。
  - [Download Web Admin Certificate]：[Download Web Admin Certificate to Controller] ページにアクセスする場合にクリックします。詳細については、「**コントローラへの Web 認証または Web 管理証明書のダウンロード**」を参照してください。

コントローラへの Web 認証または Web 管理証明書のダウンロード

Web 認証または Web 管理証明書をコントローラにダウンロードするには、次の手順を実行します。

ステップ 1 [Web 管理証明書のダウンロード（Download Web Admin Certificate）] リンクまたは [Web 認証証明書のダウンロード（Download Web Auth Certificate）] リンクをクリックします。

ステップ 2 [ファイルが存在する場所（File is located on）] フィールドで、ローカル マシンまたは TFTP サーバを指定します。証明書が TFTP サーバにある場合は、サーバ ファイル名を入力します。ローカル マシンにある場合は、[Browse] をクリックして、ローカル ファイル名を入力します。

ステップ 3 [Server Name] テキスト ボックスに TFTP サーバ名を入力します。デフォルトは Prime Infrastructure サーバです。

ステップ 4 サーバの IP アドレスを入力します。

ステップ 5 [最大試行回数（Maximum Retries）] テキスト ボックスに、TFTP サーバによる証明書のダウンロードの最大試行回数を入力します。

ステップ 6 [タイムアウト（Time Out）] テキスト ボックスに、TFTP サーバが証明書のダウンロードを試行する時間（秒単位）を入力します。

ステップ 7 [Local File Name] テキスト ボックスに、証明書のディレクトリ パスを入力します。

ステップ 8 [サーバ ファイル名（Server File Name）] テキスト ボックスに、証明書の名前を入力します。

ステップ 9 [証明書のパスワード（Certificate Password）] テキスト ボックスにパスワードを入力します。

ステップ 10 [パスワードの確認（Confirm Password）] テキスト ボックスに上記のパスワードを再入力します。

ステップ 11 [OK] をクリックします。

ステップ 12 [Regenerate Cert] をクリックして証明書を再生成します。

関連トピック

コントローラのトラップ レシーバの設定 （734 ページ）
コントローラ トラップの設定 （735 ページ）
コントローラの Telnet SSH セッション パラメータの設定 （737 ページ）
コントローラでの Web 管理の設定 （740 ページ）
コントローラでのローカル管理ユーザの設定 （741 ページ）
コントローラの管理認証サーバ優先度の設定 （742 ページ）

コントローラでのローカル管理ユーザの設定

このページには、ローカル管理ユーザの名前やアクセス権限の一覧が表示されます。ローカル管理ユーザを削除することもできます。

[ローカル管理ユーザ（Local Management Users）] ページにアクセスするには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、 **[管理（Management）] > [ローカル管理ユーザ（Local Management Users）]** を選択します。

ステップ 4 ユーザ名をクリックします。

- [User Name (read-only)]：ユーザの名前。
- [Access Level (read-only)]：[Read Write] または [Read Only]。

ステップ 5 ローカル管理ユーザを削除するには、ユーザのチェックボックスをオンにします。

ステップ 6 [コマンドの選択（Select a command）] ドロップリストから、[ローカル管理ユーザの削除（Delete Local Management Users）] を選択します。

ステップ 7 [移動（Go）] をクリックします。

ステップ 8 確認メッセージで [OK] をクリックします。

コントローラのトラップ レシーバの設定 （734 ページ）
コントローラ トラップの設定 （735 ページ）
コントローラの Telnet SSH セッション パラメータの設定 （737 ページ）
コントローラでの Web 管理の設定 （740 ページ）
コントローラの管理認証サーバ優先度の設定 （742 ページ）

コントローラの管理認証サーバ優先度の設定

認証の優先度を設定して、コントローラの管理ユーザの認証に使用する認証サーバの順序を制御します。

[認証の優先度（Authentication Priority）] ページにアクセスするには、次の手順を実行します。

ステップ 1 [設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）] を選択し、左側の [デバイスグループ（Device Groups）] メニューから [デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）] を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバー メニューから、[Management] > [Authentication Priority] の順に選択します。

ステップ 4 最初にローカル データベースが検索されます。RADIUS または TACACS+ のどちらかを次の検索対象に選択します。ローカル データベースを使用した認証に失敗した場合に、コントローラは次の種類のサーバを使用します。

ステップ 5 [Save] をクリックします。

関連トピック

コントローラの管理パラメータの設定 （734 ページ）
デバイスのメッシュ パラメータの設定 （729 ページ）
デバイスのポート パラメータの設定 （733 ページ）
コントローラのロケーション情報の設定 （743 ページ）
コントローラの IPv6 ネイバー バインドと RA パラメータの設定 （745 ページ）
コントローラのプロキシ モバイル IPv6（PMIP）パラメータの設定 （747 ページ）
コントローラのマルチキャスト DNS（mDNS）設定の構成 （751 ページ）
コントローラの Application Visibility and Control（AVC）パラメータの設定 （753 ページ）
コントローラの NetFlow 設定の構成 （755 ページ）

コントローラのロケーション情報の設定

Wi-Fi クライアントは、プローブによる AP の検出を軽減する傾向を示しています。スマートフォンではバッテリの電力節約のためにこれを実行します。スマートフォンのアプリケーションはプローブ要求を生成できなくても、簡単にデータ パケットを生成できるため、アプリケーションの拡張ロケーションをトリガーできます。Hyperlocation は WLC 8.1MR および Prime Infrastructure から設定します。これはビーコン、インベントリ、個人のモバイル デバイスの位置をかなり精密に特定します。一部のネットワークでは複数のアクセス ポイントを使用して精度が 5 ～ 7 m以内の位置座標を取得しますが、Hyperlocation は 1 m 以内まで位置を追跡できます。

個々のコントローラのロケーションを設定するには、次の手順を実行します。

ステップ 1 [設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）] を選択し、左側の [デバイスグループ（Device Groups）] メニューから [デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）] を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、[Location] > [Location Configuration] を選択します。

[ロケーションの設定（Location Configuration）] ページには、[一般（General）] と [詳細設定（Advanced）] の 2 つのタブが表示されます。

ステップ 4 次の [General] パラメータを追加または変更します。

- [RFID Tag Data Collection]：タグでデータの収集を有効にするには、このチェックボックスを選択します。

ロケーション サーバがコントローラからアセット タグ データを収集する前に、コントローラで CLI コマンド **config rfid status enable** を使用して、アクティブ RFID タグの検出を有効にする必要があります。

- Location Path Loss Configuration
  - [Calibrating Client]：クライアントの調整を有効にするには、このチェックボックスをオンにします。コントローラは、クライアントを調整するために、アクセス ポイントを介して（クライアントの機能に応じて）通常の S36 または S60 要求を送信します。パケットは、すべてのチャネルで送信されます。すべてのアクセス ポイントが、それぞれの場所でクライアントから RSSI データを収集します。これらの追加送信およびチャネル変更は、同時に発生する音声またはビデオ トラフィックの質が低下する場合があります。
  - [Normal Client]：非調整クライアントを使用するには、このチェックボックスをオンにします。S36 要求はクライアントに送信されません。S36 が CCXv2 以降と互換性があるのに対し、S60 は CCXv4 以降と互換性があります。
- Measurement Notification Interval (in secs)
  - [Tags, Clients, and Rogue APs/Clients]：クライアント、タグ、および不正に関する NMSP 測定通知間隔を設定できます。見つかった要素（タグ、クライアント、および不正アクセス ポイントやクライアント）が通知されるまでの秒数を指定します。

コントローラでこの値を設定すると、[Synchronize Servers] ページで表示できる同期外れ通知が生成されます。コントローラと Mobility Services Engine 間に別の測定間隔が存在する場合、2 つの設定のうち最長の間隔設定が Mobility Services Engine によって採用されます。

このコントローラが Mobility Services Engine と同期されると、Mobility Services Engine で新しい値が設定されます。測定通知間隔に変更を行う場合は、Mobility Services Engine に同期する必要があります。

- RSS Expiry Timeout (in secs)
  - [For Clients]：通常の（非調整）クライアントの RSSI 測定を廃棄するまでの秒数を入力します。
  - [For Calibrating Clients]：調整クライアントの RSSI 測定を廃棄するまでの秒数を入力します。
  - [For Tags]：タグの RSSI 測定を廃棄するまでの秒数を入力します。
  - [For Rogue APs]：不正アクセス ポイントの RSSI 測定を廃棄するまでの秒数を入力します。

ステップ 5 次の [Advanced] パラメータを追加または変更します。

- [RFID Tag Data Timeout (in secs)]：RFID タグ データ タイムアウトを設定するための値（秒単位）を入力します。
- Location Path Loss Configuration
  - [Calibrating Client Multiband]：すべてのチャネルで S36 および S60 パケット（該当する場合）を送信するには、[Enable] チェックボックスをオンにします。調整クライアントは、[general] タブでも有効にする必要があります。使用可能なすべての無線（802.11a/b/g/n）を使用するには、マルチバンドを有効にする必要があります。
- Hyperlocation Config Parameters
  - [Hyperlocation]：このオプションを有効にすると、そのコントローラに関連付けられた Hyperlocation モジュールがあるすべての AP が有効になります。
  - [Packet Detection RSSI Minimum]：この値を調整して、位置計算から精度の低い RSSI 測定値を除外します。
  - [Scan Count Threshold for Idle Client Detection]：スキャン中に検出されるアイドル クライアントの最大許容数。
  - [NTP Server IP Address]：有効な NTP サーバの IP アドレスを入力します。この IP アドレスは、時刻同期のためにすべての AP で使用されます。
  - 方位角角度：方位角の正しい値については、次の表を参照してください。

表 *49* : 方位角の値

設置位置	矢印方向	方位角（単位：度）	垂直角（単位：度）
天井設置型	South	90	0（上）
東側の壁面に設置	East	[0]	90（下）
南側の壁面に設置	South	90	90（下）
西側の壁面に設置	West	180	90（下）
北側の壁面に設置	North	270	90（下）

設置位置	矢印方向	方位角（単位：度）	垂直角（単位：度）
北側の壁面に対し 45 度	North	270	45（下）

ヒント　可能であれば、天井グリッド上に AP を設置し、AP の Hyperlocation 矢印を、すべて同じ方向を指すように合わせます。推奨事項は、デフォルトの方向に AP を設置することです。

ステップ 6　[保存（Save）] をクリックします。

関連トピック

コントローラの管理パラメータの設定　（734 ページ）
コントローラの IPv6 ネイバー バインドと RA パラメータの設定　（745 ページ）
コントローラのプロキシ モバイル IPv6（PMIP）パラメータの設定　（747 ページ）
デバイスのメッシュ パラメータの設定　（729 ページ）
デバイスのポート パラメータの設定　（733 ページ）
コントローラのマルチキャスト DNS（mDNS）設定の構成　（751 ページ）
コントローラの Application Visibility and Control（AVC）パラメータの設定　（753 ページ）
コントローラの NetFlow 設定の構成　（755 ページ）

コントローラの IPv6 ネイバー バインドと RA パラメータの設定

IPv6 はネイバーバインディング タイマーおよびルータ アドバタイズメント（RA）のパラメータを使用して設定できます。

関連トピック

コントローラのネイバー バインド タイマーの設定　（745 ページ）
コントローラでのルータ アドバタイズメント スロットリングの設定　（746 ページ）
コントローラでの RA ガードの設定　（747 ページ）

コントローラのネイバー バインド タイマーの設定

ネイバー バインディング タイマーを設定するには、次の手順を実行します。

ステップ 1　**[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2　該当するコントローラのデバイス名をクリックします。

ステップ 3　左側のサイドバーのメニューから、**[IPv6] > [ネイバーバインディング タイマー（Neighbor Binding Timers）]** を選択します。

ステップ 4　適用されるテンプレートが表示されます。次のパラメータを追加または変更します。

- [Down Lifetime Interval]：これは最大時間（秒単位）を示します。範囲は 0 ～ 86,400 秒で、デフォルト値は 0 です。

- [Reachable Lifetime Interval]：これは最大時間（秒単位）を示します。範囲は 0 ～ 86,400 秒で、デフォルト値は 0 です。
- [Stale Lifetime Interval]：これは最大時間（秒単位）を示します。範囲は 0 ～ 86,400 秒で、デフォルト値は 0 です。

ステップ 5 **[保存（Save）]** をクリックします。

コントローラでのルータ アドバタイズメント スロットリングの設定

[RA Throttle Policy] を使用すると、ワイヤレス ネットワークで循環するマルチキャスト ルータ アドバタイズメント（RA）の量を制限できます。

[RA Throttle Policy] を設定するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[IPv6] > [RA スロットル ポリシー（RA Throttle Policy）]** を選択します。

ステップ 4 RA スロットル ポリシーを有効にするには、[Enable] チェックボックスを選択し、次のパラメータを設定します。

- [Throttle Period]：スロットル期間（秒単位）。指定できる範囲は 10 ～ 86,400 秒です。
- [Max Through]：ある期間または無制限の期間にわたって通過する RA の数。[無制限（No Limit）] チェックボックスがオフになっている場合、最大パススルー数を指定できます。
- [Interval Option]：RA で間隔オプションが指定されている場合の動作を示します。
  - Ignore
  - Passthrough
  - Throttle
- [Allow At-least]：ルータ単位で抑制されない RA の最小数を示します。
- [Allow At-most]：ルータ単位で抑制されない RA の最大数または無制限数を示します。[無制限（No Limit）] チェックボックスがオフになっている場合、ルータ単位で抑制されない RA の最大数を指定できます。

ステップ 5 [保存（Save）] をクリックします。

関連トピック

コントローラのネイバー バインド タイマーの設定 （745 ページ）
コントローラでの RA ガードの設定 （747 ページ）

コントローラでの RA ガードの設定

RA ガードは、ワイヤレス クライアントから RA をドロップするための Unified Wireless のソリューションです。これはグローバルに設定され、デフォルトで有効です。[IPv6 Router Advertisement] パラメータを設定できます。

RA ガードを設定するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[IPv6] > [RA ガード（RA Guard）]** を選択します。

ステップ 4 [Router Advertisement Guard] を有効にするには、[Enable] チェックボックスを選択します。

ステップ 5 [Save] をクリックします。

関連トピック

コントローラのネイバー バインド タイマーの設定 （745 ページ）
コントローラでのルータ アドバタイズメント スロットリングの設定 （746 ページ）

コントローラのプロキシ モバイル IPv6（PMIP）パラメータの設定

プロキシ モバイル IPv6 は、任意の IP モビリティ関連シグナリングでモバイル ノードのプロキシとして動作することによってモバイル ノードをサポートする、ネットワーク ベースのモバイル管理プロトコルです。ネットワークのモビリティ エンティティは、モバイル ノードの移動を追跡し、モビリティ シグナリングを起動して必要なルーティング状態を設定します。

主要な機能エンティティは Local Mobility Anchor（LMA）とモバイル アクセス ゲートウェイ（MAG）です。LMA はモバイル ノードの到達可能性状態を維持し、モバイル ノードの IP アドレス用のトポロジ アンカー ポイントです。MAG はモバイル ノードの代わりにモビリティ管理を行います。MAG はモバイル ノードがアンカーされているアクセス リンクに存在します。コントローラは MAG 機能を実装します。

関連トピック

コントローラでの PMIP グローバル パラメータの設定 （747 ページ）
コントローラでの PMIP ローカル モビリティ アンカーの設定 （749 ページ）
コントローラでの PMIP プロファイルの設定 （749 ページ）

コントローラでの PMIP グローバル パラメータの設定

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[[PMIP] > [グローバル設定（Global Config）]** を選択します。

ステップ 4 次のフィールドを設定します。

- [Domain Name]：読み取り専用。
- [MAG Name]：読み取り専用。
- [MAG Interface]：読み取り専用。
- [Maximum Bindings Allowed]：コントローラが MAG に送信できるバインディング アップデートの最大数。有効な範囲は 0 ～ 40000 です。
- [Binding Lifetime]：コントローラのバインディング エントリのライフタイム。有効な範囲は 10 ～ 65535 秒です。デフォルト値は 65535 です。バインディング ライフタイムは 4 秒の倍数であることが必要です。
- [Binding Refresh Time]：コントローラのバインディング エントリのリフレッシュ時間。有効な範囲は 4 ～ 65535 秒です。デフォルト値は 300 秒です。バインディング リフレッシュ時間は 4 秒の倍数であることが必要です。
- [Binding Initial Retry Timeout]：コントローラがプロキシ バインディング確認（PBA）を受信しない場合のプロキシバインディング アップデート（PBU）間の初期タイムアウト。有効な範囲は 100 ～ 65535 秒です。デフォルト値は 1000 秒です。
- [Binding Maximum Retry Timeout]：コントローラがプロキシ バインディング確認（PBA）を受信しない場合のプロキシ バインディング アップデート（PBU）間の最大タイムアウト。有効な範囲は 100 ～ 65535 秒です。デフォルト値は 32000 秒です。
- [Replay Protection Timestamp]：受信したプロキシ バインディング確認のタイムスタンプと現在の日時との時間差の上限。有効範囲は 1 ～ 255 ミリ秒です。デフォルト値は 7 ミリ秒です。
- [Minimum BRI Retransmit Timeout]：コントローラが BRI メッセージを再送信するまでに待機する時間の最小値。有効な範囲は 500 ～ 65535 秒です。
- [Maximum BRI Retransmit Timeout]：コントローラが Binding Revocation Indication（BRI）メッセージを再送信するまでに待機する時間の最大値。有効な範囲は 500 ～ 65535 秒です。デフォルト値は 2000 秒です。
- [BRI Retries]：BRI の再試行回数。
- [MAG APN]：MAG のアクセス ポイント ノードの名前。

ステップ 5 [保存（Save）] をクリックします。

関連トピック

コントローラのプロキシ モバイル IPv6（PMIP）パラメータの設定 （747 ページ）
コントローラでの PMIP ローカル モビリティ アンカーの設定 （749 ページ）
コントローラでの PMIP プロファイルの設定 （749 ページ）

コントローラでの PMIP ローカル モビリティ アンカーの設定

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[PMIP] > [LMA 設定（LMA Config）]** を選択します。

ステップ 4 次のフィールドを設定します。

- [LMA Name]：コントローラに接続された LMA の名前。
- [LMA IP Address]：コントローラに接続された LMA の IP アドレス。

ステップ 5 [Save] をクリックします。

ステップ 6 LMA 設定を削除するには、該当する LMA 設定のチェックボックスをオンにします。

ステップ 7 [コマンドの選択（Select a command）] ドロップリストから、[PMIP ローカル設定の削除（Delete PMIP Local Configs）] を選択します。

ステップ 8 [Go] をクリックします。

ステップ 9 確認メッセージで [OK] をクリックします。

関連トピック

コントローラでの PMIP グローバル パラメータの設定 （747 ページ）
コントローラでの PMIP プロファイルの設定 （749 ページ）
コントローラのプロキシ モバイル IPv6（PMIP）パラメータの設定 （747 ページ）

コントローラでの PMIP プロファイルの設定

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、[PMIP] > [PMIP プロファイル（PMIP Profile）] を選択します。

ステップ 4 プロファイル名を入力します。

ステップ 5 [Add] をクリックし、次のフィールドを設定します。

- [Network Access Identifier]：プロファイルにアソシエートされたネットワーク アクセス識別子（NAI）の名前。
- [LMA Name]：プロファイルをアソシエートする LMA の名前。
- [Access Point Node]：コントローラに接続されているアクセス ポイント ノードの名前。

ステップ 6 [Save] をクリックします。

ステップ 7 PMIP プロファイルを削除するには、必要な PMIP プロファイルのチェックボックスをオンにします。

ステップ 8 [コマンドの選択（Select a command）] ドロップリストから、[PMIP ローカル設定の削除（Delete PMIP Local Configs）] を選択します。

ステップ 9 [Go] をクリックします。

ステップ 10 確認メッセージで [OK] をクリックします。

関連トピック

コントローラでの PMIP グローバル パラメータの設定 （747 ページ）
コントローラでの PMIP ローカル モビリティ アンカーの設定 （749 ページ）
コントローラのプロキシ モバイル IPv6（PMIP）パラメータの設定 （747 ページ）

コントローラの EoGRE トンネリングの設定

Ethernet over GRE（EoGRE）は、ホットスポットから Wi-Fi トラフィックを集約するためのソリューションです。このソリューションでは、顧客宅内機器（CPE）デバイスがエンドホストから着信するイーサネット トラフィックをブリッジし、そのトラフィックを IP GRE トンネルを介してイーサネット パケットにカプセル化できます。IP GRE トンネルがサービス プロバイダーのブロードバンド ネットワーク ゲートウェイで終わる場合、エンド ホストのトラフィックは終了し、サブスクライバ セッションがエンド ホスト用に開始します。

EoGRE トンネリングを設定するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）]** を選択し、左側の [デバイス グループ（Device Groups）] メニューから **[デバイス タイプ（Device Type）] > [ワイヤレス コントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから **[トンネリング（Tunneling）] > [EoGRE]** を選択します。

ステップ 4 [インターフェイス名（Interface Name）] ドロップダウン リストから、トンネルする送信元インターフェイスを選択します。

ステップ 5 トンネル ゲートウェイを作成するには、次の手順を実行します。

- [Heartbeat Interval] を設定します。デフォルト インターバルは 60 秒です。
- [最大ハートビート スキップ数（Max Heartbeat Skip Count）] を設定します。デフォルト値は 3 に設定されています。3 回のキープアライブ ping 後にトンネル ゲートウェイ（TWG）が応答しない場合、Cisco WLC はその TGW を非稼働とマークします。スキップ カウントの数値は、TGW が非稼働であると Cisco WLC が判断するまでに、TGW がスキップできる連続した応答の回数を決定します。
- [トンネル ゲートウェイ（Tunnel Gateway）] で、[行の追加（Add Row）] をクリックします。このようなゲートウェイを 10 個作成できます。

  1. [トンネル ゲートウェイ名（Tunnel Gateway Name）] フィールドにトンネル ゲートウェイの名前を入力します。

2. [トンネル IP アドレス（Tunnel IP Address）] フィールドにトンネルの IP アドレスを入力します。IPv4 および IPv6 の両方のアドレス形式がサポートされています。
3. [保存（Save）] をクリックします。

   デフォルトのトンネル タイプは EoGRE です。
4. [ステータス（Status）] は収集したトラップに応じて [アップ（UP）] または [ダウン（DOWN）] になります。

- [ドメイン（Domain）] の下にある [行の追加（Add Row）] をクリックして、ドメインを設定します（ドメインは、2 つのトンネル ゲートウェイのグループです）。
  1. [ドメイン名（Domain Name）] テキスト ボックスに、ドメイン名を入力します。
  2. [プライマリ ゲートウェイ（Primary Gateway）] ドロップダウン リストから、プライマリ トンネル ゲートウェイを選択します。
  3. [セカンダリ ゲートウェイ（Secondary Gateway）] ドロップダウン リストから、セカンダリ トンネル ゲートウェイを選択します。

ステップ 6 **[保存（Save）]** をクリックします。

コントローラのマルチキャスト DNS（mDNS）設定の構成

マルチキャスト DNS（mDNS）サービス検出では、ローカル ネットワーク上のサービスをアナウンスし、検出するための手段を提供します。mDNS は、IP マルチキャストで DNS クエリを実行し、ゼロ コンフィギュレーション IP ネットワーキングをサポートしています。

コントローラが mDNS サービスについて学習し、すべてのクライアントにこれらのサービスをアドバタイズできるように mDNS を設定できます。

mDNS には [Services] と [Profiles] の 2 つのタブがあります。

- [Services] タブ：このタブでは、グローバル mDNS パラメータを設定し、Master Services データベースを更新できます。
- [Profiles] タブ：このタブでは、コントローラに設定されている mDNS プロファイルを表示し、新しい mDNS プロファイルを作成できます。新しいプロファイルを作成した後、インターフェイス グループ、インターフェイス、または WLAN にプロファイルをマッピングする必要があります。クライアントはプロファイルに関連付けられたサービスのみのサービス アドバタイズメントを受信します。コントローラはインターフェイス グループに関連付けられたプロファイルに最高の優先順位を与えます。次にインターフェイス プロファイル、WLAN プロファイルが続きます。各クライアントは、優先順位に従ってプロファイルにマップされます。デフォルトで、コントローラには mDNSプロファイル default-mdns-profile があります。これは削除できません。

（注） WLAN ポリシー プロファイルにマッピングされている mDNS 設定を削除または置換するには、最初にマッピングを解除する必要があります。

ステップ 1 [設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）] を選択し、左側の [デバイスグループ（Device Groups）] メニューから [デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）] を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、[mDNS] > [mDNS] の順に選択します。

ステップ 4 [Services] タブで、次のパラメータを設定します。

- [Template Applied]：このコントローラに適用されるテンプレートの名前。
- [mDNS Global Snooping]：mDNS パケットのスヌーピングを有効にするチェックボックス。コントローラは mDNS スヌーピングを有効にしても、IPv6 mDNS パケットをサポートしません。
- [Query Interval]（10 ～ 120）：ユーザが設定できる mDNS クエリー間隔（分単位）。この間隔は、WLC によって、サービス アドバタイズメントを自動的に送信しないサービスに対して、そのサービスが開始された後に定期的な mDNS クエリー メッセージを送信するために使用されます。範囲は 10 ～ 120 分です。デフォルト値は 15 分です。
- [Master Services]：[Add Row] をクリックし、次のフィールドを設定します。
  - [Master Service Name]：ドロップダウン リストから、照会可能なサポートされているサービスを選択できます。新しいサービスを追加するには、サービス名を入力または選択し、そのサービス文字列を入力して、サービス ステータスを選択します。次のサービスを使用できます。
  - AirTunes
  - AirPrint
  - AppleTV
  - HP Photosmart Printer1
  - HP Photosmart Printer2
  - Apple File Sharing Protocol（AFP）
  - Scanner
  - Printer
  - FTP
  - iTunes Music Sharing
  - iTunes Home Sharing
  - iTunes Wireless Device Syncing
  - Apple Remote Desktop
  - Apple CD/DVD Sharing
  - Time Capsule Backup
- [Master Service Name]：mDNS サービスの名前。
- [Service String]：mDNS サービスに関連付けられた一意の文字列。たとえば、_airplay._tcp.local. は、AppleTV に関連付けられたサービス文字列です。

- [Query Status]：サービスの mDNS クエリーを有効にするために選択するチェックボックス。定期的な mDNS クエリー メッセージは、クエリーのステータスが有効な場合だけ、WLC によって、サービスに対して設定されたクエリー間隔で送信されます。それ以外の場合、サービスは、クエリーのステータスが無効になっているその他のサービス（たとえば AppleTV）に自動的にアドバタイズする場合があります。

ステップ 5 [Profiles] タブで、次のパラメータを設定します。

- [Profiles]：[Add Profile] をクリックし、次のフィールドを設定します。
  - [Profile Name]：mDNS プロファイルの名前。最大 16 個のプロファイルを作成できます。
  - [Services]：mDNS プロファイルにマップするサービスを選択します（チェックボックスを使用）。
- [編集（Edit）] および [削除（Delete）] をそれぞれクリックすると、既存のプロファイルを編集または削除できます。

ステップ 6 [保存（Save）] をクリックします。

次のタスク

デフォルトでは、コントローラによってアクセス ポリシー default-mdns-policy が作成されます。これは削除できません。これには、[グループ名（Group Name）] および [説明（Description）] が表示されます。[サービス グループ（Service Group）] の詳細を表示するポリシーを選択します。

フィールドを編集して、[保存（Save）] をクリックします。

コントローラの Application Visibility and Control（AVC）パラメータの設定

Application Visibility and Control（AVC）は、Network Based Application Recognition（NBAR）ディープ パケット インスペクション テクノロジーを使用して、使用するプロトコルに基づいてアプリケーションを分類します。AVC を使用して、コントローラはレイヤ 4 ～レイヤ 7 の 1400 を超えるプロトコルを検出できます。AVC により、リアルタイム分析を実施し、ネットワークの輻輳、コストの掛かるネットワーク リンクの使用、およびインフラストラクチャの更新を削減するためのポリシーを作成することができるようになります。

AVC は、Cisco 2500 および 5500 シリーズ コントローラ、Cisco Flex 7500 および Cisco 8500 シリーズ コントローラでだけサポートされています。

コントローラでの AVC プロファイルの設定

AVC プロファイルを設定するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[サービス（Services）]>[アプリケーションの可視性と制御（Application Visibility and Control）] > [AVC プロファイル（AVC Profile）]** を選択します。

ステップ 4 設定する AVC プロファイル名をクリックします。

ステップ 5 AVC ルールを作成するには、[Add] をクリックします。

ステップ 6 次のパラメータを設定します。

- [Application Name]：アプリケーションの名前。
- [Application Group Name]：アプリケーションが属するアプリケーション グループの名前。
- [Action]：ドロップダウン リストから、次の項目を選択できます。
  - [Drop]：選択されたアプリケーションに対応するアップストリームおよびダウンストリーム パケットをドロップします。
  - [Mark]：[Differentiated Services Code Point (DSCP)] ドロップダウン リストで指定する DSCP 値と選択されたアプリケーションに対応するアップストリームおよびダウンストリーム パケットをマークします。DSCP 値を使用して、QoS レベルに基づいて Differentiated Services を提供できます。
  - [Rate Limit]：アクションとして [Rate Limit] を選択すると、クライアント 1 人あたりの平均レート制限とバースト データ レート制限を指定できます。レート制限アプリケーションの数は 3 に制限されています。デフォルト アクションは、すべてのアプリケーションの許可です。
- [DSCP]：インターネットでのサービスの質を定義するために使用できるパケット ヘッダー コード。DSCP 値は次の QoS レベルにマッピングされます。
  - [Platinum (Voice)]：Voice over Wireless の高い QoS を保証します。
  - [Gold (Video)]：高品質のビデオ アプリケーションをサポートします。
  - [Silver (Best Effort)]：クライアントの通常の帯域幅をサポートします。
  - [Bronze (Background)]：ゲスト サービス用の最小の帯域幅を提供します。
  - [Custom]：DSCP 値を指定します。範囲は 0 ～ 63 です。
- [DSCP 値（DSCP Value）]：この値は、[DSCP] ドロップダウン リストで [カスタム（Custom）] を選択した場合にのみ入力できます。
- 平均Rate Limit (in Kbps)]：アクションとして [Rate Limit] を選択した場合は、そのアプリケーションの平均帯域幅制限である、クライアントごとの平均レート制限を指定できます。
- [Burst Rate Limit (in Kbps)]：アクションとして [Rate Limit] を選択した場合は、そのアプリケーションのピーク制限である、バースト レート制限を指定できます。

ステップ 7 [Save] をクリックします。

関連トピック

コントローラのマルチキャスト DNS（mDNS）設定の構成 （751 ページ）
コントローラの NetFlow 設定の構成 （755 ページ）
デバイスのメッシュ パラメータの設定 （729 ページ）
デバイスのポート パラメータの設定 （733 ページ）
コントローラの管理パラメータの設定 （734 ページ）
コントローラのロケーション情報の設定 （743 ページ）
コントローラの IPv6 ネイバー バインドと RA パラメータの設定 （745 ページ）
コントローラのプロキシ モバイル IPv6（PMIP）パラメータの設定 （747 ページ）

コントローラの NetFlow 設定の構成

NetFlow は、ネットワーク デバイスから IP トラフィック情報を収集することで、ネットワーク ユーザとアプリケーション、ピーク時の使用時間、およびトラフィック ルーティングに関する貴重な情報を提供するプロトコルです。NetFlow アーキテクチャは、次のコンポーネントで構成されています。

- コレクタ：さまざまなネットワーク要素から IP トラフィック情報をすべて収集するエンティティ。
- エクスポータ：IP トラフィック情報を使用してテンプレートをエクスポートするネットワーク エンティティ。コントローラは、エクスポータとして機能します。

コントローラでの NetFlow モニタの設定

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当するコントローラのデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[NetFlow] > [モニタ（Monitor）]** を選択します。

ステップ 4 次のパラメータを設定します。

- [Monitor Name]：NetFlow モニタの名前。モニタ名は最大 127 文字の英数字で、大文字と小文字を区別します。コントローラでは 1 つのみモニタを設定できます。
- [Record Name]：NetFlow レコードの名前。コントローラの NetFlow レコードには、特定のフロー内のトラフィックに関する次の情報が含まれます。
  - クライアント MAC アドレス
  - クライアント送信元 IP アドレス
  - WLAN ID

- アプリケーション ID
- データの着信バイト数
- データの発信バイト数
- 着信パケット
- 発信パケット
- 着信 DSCP
- 発信 DSCP
- 最後の AP の名前

ステップ 5 [Exporter Name]：エクスポータの名前。コントローラでは 1 つのみモニタを設定できます。
ステップ 6 [Exporter IP]：コレクタの IP アドレス。
ステップ 7 [Port Number]：NetFlow レコードをコントローラからエクスポートする UDP ポート。
ステップ 8 **[保存（Save）]** をクリックします。

コントローラでの NetFlow エクスポータの設定

ステップ 1 **[設定（Configuration）]** > **[ネットワーク（Network）]** > **[ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）]** > **[ワイヤレスコントローラ（Wireless Controller）]** を選択します。
ステップ 2 該当するコントローラのデバイス名をクリックします。
ステップ 3 左側のサイドバーのメニューから、**[NetFlow]** > **[エクスポータ（Exporter）]** を選択します。
ステップ 4 次のパラメータを設定します。

- [Exporter Name]：エクスポータの名前。
- [Exporter IP]：エクスポータの IP アドレス。
- [Port Number]：NetFlow レコードをコントローラからエクスポートする UDP ポート。

関連トピック

コントローラのマルチキャスト DNS（mDNS）設定の構成 （751 ページ）
コントローラの NetFlow 設定の構成 （755 ページ）
デバイスのメッシュ パラメータの設定 （729 ページ）
デバイスのポート パラメータの設定 （733 ページ）
コントローラの管理パラメータの設定 （734 ページ）
コントローラのロケーション情報の設定 （743 ページ）

コントローラの IPv6 ネイバー バインドと RA パラメータの設定 （745 ページ）
コントローラのプロキシ モバイル IPv6（PMIP）パラメータの設定 （747 ページ）

サードパーティ製コントローラまたはアクセスポイントの設定

Cisco Prime Infrastructure では、サードパーティのコントローラおよびアクセス ポイントを追加することができます。この機能の一部として、次の機能を実行できます。

- Cisco Prime Infrastructure にサードパーティのコントローラを追加します。
- サードパーティのコントローラの状態をモニタします。
- サードパーティのコントローラと、アソシエートされたアクセス ポイントのインベントリ情報を取得します。
- サードパーティのコントローラおよびアクセス ポイントの動作ステータスを表示するには、バックグラウンド タスクを使用します。

関連トピック

サードパーティ製コントローラの追加 （757 ページ）
サードパーティ製コントローラの動作ステータスの表示 （758 ページ）
サードパーティ アクセス ポイントの設定の表示 （759 ページ）
サードパーティ アクセス ポイントの削除 （759 ページ）
サードパーティ製コントローラの動作ステータスの表示 （758 ページ）

サードパーティ製コントローラの追加

サードパーティのコントローラを追加するには、次の手順を実行します。

ステップ 1 [設定（Configuration）] > [ネットワークデバイス（Network Devices）] > [サードパーティワイヤレスコントローラ（Third Party Wireless Controllers）] を選択します。

ステップ 2 [デバイスの追加（Add Device）] をクリックします。

ステップ 3 [Add Device] ページの次のタブで必須パラメータを入力します。

- General
- SNMP
- Telnet/SSH
- HTTP/HTTPS
- IPSec

ステップ 4 [追加（Add）] をクリックします。

関連トピック

サードパーティ製コントローラの動作ステータスの表示 （758 ページ）

サードパーティ アクセス ポイントの設定の表示 （759 ページ）
サードパーティ アクセス ポイントの削除 （759 ページ）
サードパーティ製コントローラの動作ステータスの表示 （758 ページ）

サードパーティ製コントローラの動作ステータスの表示

[サードパーティのコントローラの動作ステータス（Third Party Controller Operational Status）] ページを表示するには、次の手順を実行します。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [バックグラウンドタスク（Background Tasks）]** の順に選択します。

ステップ 2 このページで、次のいずれかを実行します。

- すぐにタスクを実行する。

  [サードパーティのコントローラの動作ステータス（Third Party Controller Operational Status）] チェックボックスをオンにします。[Select a command] ドロップダウン リストから、[Execute Now] を選択し、[Go] をクリックします。[Enabled] 列にステータス変更が表示されます。

- タスクを有効にする。

  [サードパーティのコントローラの動作ステータス（Third Party Controller Operational Status）] チェックボックスをオンにします。[Select a command] ドロップダウン リストから、[Enable Tasks] を選択し、[Go] をクリックします。[Enabled] 列のタスクが灰色から使用可能な状態に変わります。

- タスクを無効にする。

  [Third Party Controller Operational Status] チェックボックスをオンにします。[Select a command] ドロップダウン リストから、[Disable Tasks] を選択し、[Go] をクリックします。無効化が完了すると、[Enabled] 列のタスクが灰色になります。

ステップ 3 タスクを変更するには、[Background Tasks] 列の [Third Party Controller Operational Status] リンクをクリックします。

[サードパーティのコントローラの動作ステータス（Third Party Controller Operational Status）] ページには、最終実行情報が表示されます。

- [Start Time]。
- [End Time]。
- タスクの [Elapsed Time]（秒）。
- [Result]：成功またはエラー。
- [Message]：このタスクに関するテキスト メッセージ。

ステップ 4 [Task Details] セクションで、次の項目を表示または編集します。

- [Description]：表示のみ。タスクの名前を表示します。

- [Enabled]：チェックボックスをオンにすると、このタスクが有効になります。
- [Interval]：タスクの頻度（分）を示します。デフォルトは 3 時間です。

ステップ 5 完了したら、[Save] をクリックしてタスクの変更を確定します。

関連トピック

サードパーティ製コントローラの追加 （757 ページ）
サードパーティ アクセス ポイントの設定の表示 （759 ページ）
サードパーティ アクセス ポイントの削除 （759 ページ）

サードパーティ アクセス ポイントの設定の表示

サードパーティのアクセスポイントは、サードパーティのコントローラを追加すると検出されます。

サードパーティのアクセス ポイントの設定を表示するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク デバイス（Network Devices）] > [サードパーティのアクセス ポイント（Third Party Access Points）] を選択します。**

ステップ 2 詳細を表示する AP 名のリンクをクリックします。そのサードパーティのアクセス ポイントの [General] タブが表示されます。

関連トピック

サードパーティ製コントローラの追加 （757 ページ）
サードパーティ製コントローラの動作ステータスの表示 （758 ページ）
サードパーティ アクセス ポイントの削除 （759 ページ）
サードパーティ製コントローラの動作ステータスの表示 （758 ページ）

サードパーティ アクセス ポイントの削除

サードパーティのアクセス ポイントを削除するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク デバイス（Network Devices）] > [サードパーティのアクセス ポイント（Third Party Access Points）] を選択します。**

ステップ 2 削除するアクセス ポイントのチェックボックスを選択します。

ステップ 3 [Delete] をクリックします。

ステップ 4 確認メッセージが表示されます。

ステップ 5 [はい（Yes）] をクリックします。

関連トピック

サードパーティ製コントローラの追加 （757 ページ）
サードパーティ製コントローラの動作ステータスの表示 （758 ページ）
サードパーティ アクセス ポイントの設定の表示 （759 ページ）
サードパーティ製コントローラの動作ステータスの表示 （758 ページ）

サードパーティ アクセス ポイントの動作ステータスの表示

[サードパーティのアクセス ポイントの動作ステータス（Third Party Access Point Operational Status）] ページを表示するには、次の手順を実行します。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [バックグラウンドタスク（Background Tasks）]** の順に選択します。

ステップ 2 このページで、次のいずれかを実行します。

- すぐにタスクを実行する。

  [サードパーティのアクセス ポイントの動作ステータス（Third Party Access Point Operational Status）] チェックボックスをオンにします。[Select a command] ドロップダウン リストから、[Execute Now] を選択し、[Go] をクリックします。[Enabled] 列にステータス変更が表示されます。

- タスクを有効にする。

  [サードパーティのアクセス ポイントの動作ステータス（Third Party Access Point Operational Status）] チェックボックスをオンにします。[Select a command] ドロップダウン リストから、[Enable Tasks] を選択し、[Go] をクリックします。[Enabled] 列のタスクが灰色から使用可能な状態に変わります。

- タスクを無効にする。

  [Third Party Access Point Operational Status] チェックボックスをオンにします。[Select a command] ドロップダウン リストから、[Disable Tasks] を選択し、[Go] をクリックします。無効化が完了すると、[Enabled] 列のタスクが灰色になります。

ステップ 3 タスクを変更するには、[Background Tasks] 列の [Third Party Access Point Operational Status] リンクをクリックします。

[サードパーティのコントローラの動作ステータス（Third Party Controller Operational Status）] ページには、最終実行情報が表示されます。

- [Start Time]。
- [End Time]。
- タスクの [Elapsed Time]（秒）。
- [Result]：成功またはエラー。
- [Message]：このタスクに関するテキスト メッセージ。

ステップ 4 [Edit Task] グループ ボックスで、次の項目を表示または編集します。

- [Description]：表示のみ。タスクの名前を表示します。
- [Enabled]：チェックボックスをオンにすると、このタスクが有効になります。
- [Interval]：タスクの頻度（分）を示します。デフォルトは 3 時間です。

ステップ 5 完了したら、[Save] をクリックしてタスクの変更を確定します。

関連トピック

サードパーティ製コントローラの追加 （757 ページ）
サードパーティ製コントローラの動作ステータスの表示 （758 ページ）
サードパーティ アクセス ポイントの設定の表示 （759 ページ）
サードパーティ アクセス ポイントの削除 （759 ページ）

スイッチ設定の表示

Cisco Prime Infrastructure データベースのすべてのスイッチのサマリーを表示するには、**[設定（Configuration）]** > **[ネットワーク（Network）]** > **[ネットワークデバイス（Network Devices）]** > **[デバイスタイプ（Device Type）]** > **[スイッチおよびハブ（Switches and Hubs）]** を選択します。任意の列見出しをクリックして、その列で情報をソートします。列見出しを複数回クリックすることで、昇順のソートと降順のソートを切り替えることができます。

関連トピック

スイッチの詳細の表示 （761 ページ）

スイッチの詳細の表示

Cisco Prime Infrastructure データベースのすべてのスイッチのサマリーを表示するには、**[設定（Configuration）]** > **[ネットワーク（Network）]** > **[ネットワークデバイス（Network Devices）]** > **[デバイスタイプ（Device Type）]** > **[スイッチおよびハブ（Switches and Hubs）]** を選択します。デバイス名をクリックすると、そのスイッチの詳細情報が表示されます。

関連トピック

例：スイッチでの SNMPv3 の設定 （764 ページ）

スイッチの SNMP パラメータの変更

スイッチの SNMP パラメータを変更するには、次の手順を実行します。

ステップ 1 [Configuration] > [Network] > [Network Devices] > [Device Type] > [Switches and Hubs] を選択して、SNMP クレデンシャルを変更するスイッチの横にあるチェックボックスをクリックします。

ステップ 2 [Edit] をクリックします。

ステップ 3 必要な [SNMP Parameters] フィールドを変更して、次のいずれかをクリックします。

- [Reset]：以前に保存したパラメータを復元します。
- [Save]：行った変更を保存して適用します。
- [Cancel]：変更を保存せずに終了して、前の画面に戻ります。

関連トピック

スイッチ設定の表示 （761 ページ）
例：スイッチでの SNMPv3 の設定 （764 ページ）
スイッチの Telnet/SSH クレデンシャルの変更 （762 ページ）

スイッチの Telnet/SSH クレデンシャルの変更

スイッチの Telnet または SSH パラメータを変更するには、次の手順を実行します。

ステップ 1 [Configuration] > [Network] > [Network Devices] > [Device Type] > [Switches and Hubs] を選択して、Telnet または SSH クレデンシャルを変更するスイッチの横にあるチェックボックスをクリックします。

ステップ 2 [Edit] をクリックします。

ステップ 3 必要な [Telnet/SSH Parameters] フィールドを変更して、次のいずれかをクリックします。

- [Reset]：以前に保存したパラメータを復元します。
- [Save]：行った変更を保存して適用します。
- [Cancel]：変更を保存せずに終了して、前の画面に戻ります。

関連トピック

スイッチ設定の表示 （761 ページ）
例：スイッチでの SNMPv3 の設定 （764 ページ）
スイッチの SNMP パラメータの変更 （761 ページ）

スイッチの追加

スイッチを Prime Infrastructure データベースに追加して、全体的なスイッチ ヘルスとエンドポイントのモニタを表示し、スイッチポート トレースを実行できます。次のスイッチを設定できます。

- 3750
- 3560
- 3750E
- 3560E
- 2960

Prime Infrastructure の設定メニューにスイッチ機能が表示されますが、Prime Infrastructure を使用してスイッチ機能を設定することはできません。設定できるのは Prime Infrastructure システムのみです。

Prime Infrastructure では、次を実行できます。

- [設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）] > [デバイス タイプ（Device Type）] > [ワイヤレス コントローラ（Wireless Controller）] ページでスイッチを追加し、CLI および SNMP クレデンシャルを指定します。
- Mobility Services Engine と Prime Infrastructure によって有線クライアントを追跡するために、[設定（Configuration）]>[ネットワーク（Network）]>[ネットワークデバイス（Network Devices）] > [デバイス タイプ（Device Type）] > [ワイヤレス コントローラ（Wireless Controller）] ページでロケーション対応スイッチを追加します。
- [Monitor] > [Network Devices] を選択してスイッチをモニタします。
- [Reports] メニューを使用してスイッチ関連レポートを実行します。

Prime Infrastructure データベースにスイッチを追加すると、デフォルトでは、Prime Infrastructure はスイッチの SNMP クレデンシャルを検査します。デバイスのクレデンシャルが正しくない場合、SNMP 失敗メッセージが表示されますが、スイッチは Prime Infrastructure データベースに追加されます。

スイッチ タイプ別に使用可能な機能

Prime Infrastructure にスイッチを追加する場合は、スイッチの管理方法を指定します。これに基づいて、Prime Infrastructure は使用できる機能を判別します。

- [Monitored switches]：スイッチを追加（[Configuration] > [Network] > [Network Devices] > [Device Type] > [Wireless Controller] を選択）して、スイッチの動作をモニタ（[Monitor] > [Network Devices] を選択）できます。それぞれのスイッチは、ライセンスの合計デバイス数に対して 1 つのデバイスとしてカウントされます。ライセンス エンジンで使用可能な未使用のデバイス数がある場合は、スイッチを Prime Infrastructure に追加できます。使用可能なデバイス数が残っていない場合は、別のスイッチを Prime Infrastructure に追加できません。
- [Switch Port Tracing (SPT) only switches]：スイッチは、スイッチ ポート トレースのみを実行します。SPT 専用スイッチは、[Configuration] > [Network] > [Network Devices] > [Device Type] > [Switches and Hubs] ページとインベントリ レポートに表示されます。ライセンスは SPT スイッチには適用されません。

スイッチを Prime Infrastructure に追加するには、次の手順を実行します。

ステップ 1 [Configuration] > [Network] > [Network Devices] > [Device Type] > [Switches and Hubs] を選択し、[Add Device] をクリックします。

ステップ 2 表示されるフィールドに適切な情報を入力します。

詳細については、『Cisco Pime Infrastrucutre Reference Guide』を参照してください。

ステップ 3 [追加（Add）] をクリックしてスイッチを追加するか、[キャンセル（Cancel）] をクリックして操作をキャンセルし、スイッチのリストに戻ります。

関連トピック

CSV ファイルからのスイッチのインポート （764 ページ）
例：スイッチでの SNMPv3 の設定 （764 ページ）

例：スイッチでの SNMPv3 の設定

次に、スイッチでの SNMPv3 の設定例を示します。

snmp-server view v3default iso includedsnmp-server group v3group v3 auth write v3default
snmp-server user <username> <v3group> v3 auth <md5 or sha> <authentication password>

スイッチに VLAN がある場合、各 VLAN を設定する必要があります。設定しないと、スイッチ ポート トレーシングは失敗します。次に、スイッチに VLAN 1 および 20 がある場合の例を示します。

snmp-server group v3group v3 auth context vlan-1 write v3defaultsnmp-server group v3group v3 auth context vlan-20 write v3default

snmp-server group v3group v3 auth context vlan-20 write v3default

SNMP v3 ビューの作成時に、すべての OID を含めてください。

関連トピック

CSV ファイルからのスイッチのインポート （764 ページ）

CSV ファイルからのスイッチのインポート

CSV ファイルを使用してスイッチを Cisco Prime Infrastructure データベースにインポートできます。CSV ファイルの最初の行は、含まれている列の説明に使用されます。IP アドレス列は必須です。

次に、CSV ファイルの例を示します。

```
ip_address, network_mask, snmp_version, snmp_community, snmpv3_user_name, snmpv3_auth_type,
 snmpv3_auth_password, snmpv3_privacy_type, snmpv3_privacy_password, snmp_retries,
snmp_timeout,protocol,telnet_username,telnet_password,enable_password,telnet_timeout
16.1.1.3,255.255.255.0,v2,public,,,,,,3,10,telnet,cisco,cisco,cisco,60
16.1.1.4,255.255.255.0,v2,public,,,,,,3,10,ssh2,cisco,cisco,cisco,60
16.1.1.5,255.255.255.0,v2,public,,,,,,3,10,,cisco,cisco,cisco,60
16.1.1.6,255.255.255.0,v2,public,,,,,,3,10,telnet,cisco,cisco,cisco,60
3.3.3.3,255.255.255.0,v3,,default,HMAC-MD5,default,DES,default,3,4
4.4.4.4,255.255.255.0,v3,,default,HMAC-MD5,default,DES,default,3,4,telnet,cisco,cisco,cisco,60
```

[シビックロケーション（Civic Location）] ペインのフィールドは、シビック情報をインポートした後に読み込まれます。

詳細については、『Cisco Prime Infrastructure Reference Guide』を参照してください。

関連トピック

スイッチの追加 （762 ページ）
例：スイッチでの SNMPv3 の設定 （764 ページ）

スイッチの削除

Prime Infrastructure データベースからスイッチを削除すると、次の機能が実行されます。

- そのスイッチのインベントリ情報が、データベースから削除されます。
- スイッチのアラームは、ステータスが [Clear] のデータベース内に残ります。デフォルトでは、クリアされたアラームは Prime Infrastructure インターフェイスに表示されません。
- 保存したレポートは、レポートを実行したスイッチが削除されてもデータベースに残ります。

Prime Infrastructure からスイッチを削除するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）] > [デバイス タイプ（Device Type）] > [スイッチおよびハブ（Switches and Hubs）]** を選択して、削除するスイッチの横にあるチェックボックスをクリックします。

ステップ 2 [Delete] をクリックします。

ステップ 3 [OK] をクリックして、削除を実行します。

関連トピック

スイッチの追加 （762 ページ）

例：有線クライアントのスイッチ トラップと Syslog の設定

次の Cisco IOS の設定例では、この Cisco IOS スイッチ機能が MAC 通知用に SNMP トラップをスイッチから Prime Infrastructure サーバに転送する方法を示します（802.1x クライアントの場合）。

```
snmp-server enable traps mac-notification change move threshold
snmp-server host<IP address of Prime Infrastructure server> version 2c <community-string>
 mac-notification
mac address-table notification change interval 5
mac address-table notification change history-size 10
mac address-table notification change


interface <interface>
 description non-identity clients
 switchport access vlan <VLAN ID>
 switchport mode access
 snmp trap mac-notification change added  <- interface level config for MAC Notification

  snmp trap mac-notification change removed <- interface level config for MAC Notification
```

debug コマンドは次のとおりです。

```
debug snmp packets
```

show コマンドは次のとおりです。

```
show mac address-table notification change
```

詳細については、『Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide』を参照してください。

例：IOS を使用した Catalyst スイッチの Syslog 転送の設定

syslog 設定は、syslog メッセージを Catalyst スイッチから Prime Infrastructure サーバに転送します。この機能は ID クライアントの検出に使用されます。次の Cisco IOS の設定例は、この Cisco IOS スイッチが syslog メッセージを Catalyst スイッチから Prime Infrastructure サーバに転送する方法を示しています。

```
archive
 log config
  notify syslog contenttype plaintext
logging facility auth
logging <IP address of Prime Infrastructure server>
```

詳細については、『Catalyst 3750 Software Configuration Guide』を参照してください。

Cisco Prime Infrastructure での Cisco OfficeExtend AP の使用

OfficeExtend アクセス ポイントは、リモート ロケーションでコントローラからアクセス ポイントへの安全な通信を提供し、インターネットを通じて会社の WLAN を従業員の自宅にシームレスに拡張します。ホーム オフィスでのテレワーカーのエクスペリエンスは、本社オフィスでのエクスペリエンスとまったく同じです。アクセスポイントとコントローラの間の Datagram Transport Layer Security（DTLS; データグラム トランスポート層セキュリティ）による暗号化は、すべての通信のセキュリティを最高レベルにします。

図 25-1 **205774.jpg** に、典型的な OfficeExtend アクセス ポイントの設定を示します。

OfficeExtend アクセス ポイントは、ルータまたはネットワーク アドレス変換（NAT）を使用するその他のゲートウェイ デバイスを越えて動作するよう設計されています。NAT により、ルータなどのデバイスはインターネット（パブリック）と個人ネットワーク（プライベート）間のエージェントとして動作でき、これにより、コンピュータのグループ全体を単一の IP アドレスとすることができます。コントローラ リリース 6.0 では、単一の NAT デバイスの後方では単一の OfficeExtend アクセス ポイントのみを展開可能です。

現時点では、WPLUS ライセンスにより Cisco 5500 シリーズのコントローラに接続された Cisco Aironet 1130 シリーズおよび 1140 シリーズのアクセス ポイントだけを OfficeExtend アクセス ポイントとして設定できます。

ファイアウォールは、アクセス ポイントからの CAPWAP を使用するトラフィックを許可するよう設定されている必要があります。UDP ポート 5246 および 5247 が有効であり、アクセス ポイントがコントローラに join できないようにする可能性のある中間デバイスによりブロックされていないことを確認してください。

OfficeExtend アクセス ポイントのライセンスを購入する前に、WPlus ライセンスが 5500 シリーズ コントローラにインストールされていることを確認してください。ライセンスのインストー

ル後、1130 シリーズまたは 1140 シリーズ アクセス ポイントで OfficeExtend モードを有効にすることができます。

オペレーティング システムのソフトウェアによってアクセス ポイントが自動的に検出され、Cisco Prime Infrastructure データベース内の既存のコントローラに関連付けられると Cisco Prime Infrastructure データベースに追加されます。

AP とコントローラ間のリンクを測定するためのリンク遅延の設定

コントローラでリンク遅延を設定して、アクセスポイントおよびコントローラの間のリンクを計測できます。この機能は、コントローラに接続されたすべてのアクセスポイントで使用できますが、特に、リンクの速度が低いか、信頼性の低い WAN 接続の可能性がある FlexConnect アクセス ポイントで役立ちます。

リンク遅延は、接続モードの FlexConnect アクセス ポイントでのみサポートされます。スタンドアロン モードの FlexConnect アクセス ポイントはサポートされません。

リンク遅延は、アクセス ポイントからコントローラ、およびコントローラからアクセス ポイントにおける CAPWAP ハートビート パケット（エコー要求および応答）のラウンドトリップ時間をモニタします。この時間は、ネットワーク リンク速度およびコントローラの処理負荷によって異なります。アクセスポイントは、コントローラへの発信エコー要求およびコントローラから受信するエコー応答をタイムスタンプ記録します。アクセスポイントはこのデルタ時間をシステムのラウンドトリップ時間としてコントローラに送信します。アクセスポイントは、30 秒のデフォルト間隔でコントローラにハートビート パケットを送信します。

リンク遅延はアクセス ポイントとコントローラ間の CAPWAP 応答時間を計算します。ネットワーク遅延や ping 応答は計測しません。

コントローラにより、現在のラウンドトリップ時間および継続的な最短および最長ラウンドトリップ時間が表示されます。最短および最長時間はコントローラが動作している限り維持され、クリアして再開することもできます。

リンク遅延を設定するには、以下のステップに従います。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）] > [デバイス タイプ（Device Type）] > [統合型 AP（Unified AP）]** を選択し、デバイス名をクリックします。

ステップ 2 [Enable Link Latency] チェックボックスを選択して、このアクセス ポイントのリンク遅延を有効にするか、または選択解除して、エコー応答受信ごとにアクセス ポイントがコントローラにラウンドトリップ時間を送信しないようにします。デフォルト値はオフです。

ステップ 3 [Save] をクリックして変更を保存します。

リンク遅延の結果は、[Enable Link Latency] チェックボックスの下に表示されます。

1. [Current] : アクセス ポイントからコントローラ、およびコントローラからアクセス ポイントの間の CAPWAP ハートビート パケットの現在のラウンドトリップ時間（ミリ秒単位）。

2. [Minimum]：リンク遅延が有効になったか、またはリセットされたことが原因の、アクセス ポイントからコントローラ、およびコントローラからアクセス ポイントの間の CAPWAP ハートビート パケットの最短ラウンドトリップ時間（ミリ秒単位）。
3. [Maximum]：リンク遅延が有効になったか、またはリセットされたことが原因の、アクセス ポイントからコントローラ、およびコントローラからアクセス ポイントの間の CAPWAP ハートビート パケットの最長ラウンドトリップ時間（ミリ秒単位）。

ステップ 4 このアクセス ポイントのコントローラ上の現在、最短、および最長リンク遅延統計をクリアするには、[Reset Link Latency] をクリックします。[Minimum] フィールドおよび [Maximum] フィールドに更新された統計情報が表示されます。

ユニファイド AP の設定

[設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）] > [デバイス タイプ（Device Type）] > [統合型 AP（Unified AP）] ページを使用して、統合型アクセス ポイントを表示し、設定できます。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワークデバイス（Network Devices）]** を選択し、左側の [デバイスグループ（Device Groups）] メニューから **[デバイスタイプ（Device Type）] > [ワイヤレスコントローラ（Wireless Controller）]** を選択します。

ステップ 2 該当する IP アドレスをクリックして次のパラメータを表示します。

- [AP Name]：アクセス ポイント名をクリックして、アクセス ポイントの詳細を表示または設定します。
- Base Radio MAC
- Admin Status
- AP Mode
- Software Version
- Primary Controller Name

ステップ 3 アクセス ポイント名をクリックして、アクセス ポイントの詳細を表示または設定します。表示される情報は、アクセス ポイントのタイプに応じて異なります。

ユニファイドアクセスポイントでSniffer機能を有効にする（AiroPeek）

アクセス ポイントでスニファ機能を有効にした場合、そのアクセス ポイントはスニファとして機能し、特定チャネル上のすべてのパケットを取得して、AiroPeek を実行するリモート マシンへ転送します。これらのパケットには、タイムスタンプ、信号強度、パケット サイズなどの情報が含まれます。

スニファ機能は、データ パケットのデコードをサポートする、サードパーティ製のネットワーク分析ソフトウェアである AiroPeek を実行する場合だけ有効になります。AiroPeek の詳細は、次の URL を参照してください。www.wildpackets.com/products/airopeek/overview

はじめる前に

スニファ機能を使用する前に、次の作業を完了しておく必要があります。

- リモート サイトで、スニファ モードでアクセス ポイントを設定します。スニファ モードでアクセス ポイントを設定する方法については、「関連項目」の「Web ユーザ インターフェイスを使用したスニファ モードでの AP の設定」を参照してください。
- Windows XP マシンで AiroPeek バージョン 2.05 以降をインストールします。
  - 次の dll ファイルをダウンロードするには、WildPackets のメンテナンス メンバーである必要があります。次の URL を参照してください。
    https://wpdn.wildpackets.com/view_submission.php?id=30
- 次の dll ファイルをコピーします。
  - socket.dll ファイルを Plugins フォルダ（C:\ProgramFiles\WildPackets\AiroPeek\Plugins など）へ
  - socketres.dll ファイルを PluginRes フォルダ（C:\ProgramFiles\WildPackets\AiroPeek\1033\PluginRes など）へ

関連トピック

デバイスの 802.11 パラメータの設定 （720 ページ）

リモート マシンでの AiroPeek スニファの設定

リモート マシンで AiroPeek を設定するには、次の手順を実行します。

ステップ 1 AiroPeek アプリケーションを開始して、[Tools] タブで [Options] をクリックします。

ステップ 2 [Options] ページで [Analysis Module] をクリックします。

ステップ 3 ページ内を右クリックして、[Disable All] オプションを選択します。

ステップ 4 [Cisco remote module] 列を見つけて、有効にします。[OK] をクリックして変更を保存します。

ステップ 5 [New capture] をクリックして、[capture option] ページを表示します。

ステップ 6 アダプタ モジュールのリストからリモート Cisco アダプタを選択します。

ステップ 7 展開して、新しいリモートアダプタ オプションを見つけます。ダブルクリックして新規ページを開き、表示されるテキスト ボックスに名前を入力して、[IP address] 列にコントローラ管理インターフェイス IP を入力します。

ステップ 8 [OK] をクリックします。新しいアダプタがリモート Cisco アダプタに追加されます。

ステップ 9 アクセス ポイントを使用してリモートの airopeek キャプチャ用の新規アダプタを選択します。

ステップ 10 [capture] ページで [start socket capture] をクリックして、リモート キャプチャ プロセスを開始します。

ステップ 11 コントローラの CLI からアクセス ポイントを起動して、**config ap mode sniffer** *ap-name* コマンドを入力してスニファ モードに設定します。

アクセス ポイントがリブートし、スニファ モードでアップ状態になります。

Cisco Prime Infrastructure を使用したスニファ モードでの AP の設定

Web ユーザ インターフェイスを使用してスニッファ モードで AP を設定するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）]** > **[ネットワーク（Network）]** > **[ネットワーク デバイス（Network Devices）]** を選択し、[AP 名（AP Name）] 列の項目をクリックしてこのページに移動します。

ステップ 2 [General] グループ ボックスで、ドロップダウン リストを使用して AP モードを [Sniffer] に設定し、[Apply] をクリックします。

ステップ 3 [Radio Interfaces] グループ ボックスの [Protocol] 列でプロトコル（802.11a/802.11b/g）をクリックします。これによって、設定ページが開きます。

ステップ 4 [Sniff] パラメータを表示するには、[Sniff] チェックボックスを選択します。スニファ対象チャネルを選択し、サーバ（AiroPeek が実行されているリモート マシン）の IP アドレスを入力します。

ステップ 5 [保存（Save）] をクリックして、変更内容を保存します。

AP での Flex+Bridge モードの有効化

AP で Flex+Bridge モードを有効にするには、次の手順を実行します。

ステップ 1 **[設定（Configuration）]** > **[テンプレート（Templates）]** > **[Lightweightアクセスポイント（Lightweight Access Points）]** の順にクリックします。

ステップ 2 関連する AP テンプレートをクリックするか、新しいテンプレートを追加します。

ステップ 3 [APパラメータ（AP Parameters）] タブをクリックし、[APモード（AP Mode）] チェックボックスをオンにします。

ステップ 4 ドロップダウン リストから [Flex+Bridge] を選択し、[保存（Save）] をクリックします。

- AP モードを Flex+Bridge にまたは Flex+Bridge から切り替える場合、AP は再起動します。
- Flex+Bridge モードは API 暗号化および AP 再送信間隔をサポートしておらず、重要 AP のフェールオーバー条件のみをサポートします。
- [FlexConnect] タブおよび [メッシュ（Mesh）] タブで行われた設定は、AP モードを変更するとプロビジョニングされなくなります。まず AP モードを Flex+Bridge モードに変更し、その後で [FlexConnect] タブおよび [メッシュ（Mesh）] でパラメータを設定する必要があります。

コントローラ冗長性の設定

「コントローラの冗長性」は、コントローラに組み込まれているハイ アベイラビリティ（HA）フレームワークを指しています。ワイヤレス ネットワーク コントローラの冗長性により、ネットワークのダウンタイムを削減することができます。冗長アーキテクチャでは、1 台のコントローラがアクティブ状態となり、もう 1 台のコントローラがスタンバイ状態となります。スタンバイ コントローラは、冗長ポートを使用してアクティブ コントローラのヘルスを常時モニタします。両方のコントローラは管理インターフェイスの IP アドレスを含め、同じ設定を共有します。

コントローラのスタンバイ状態およびアクティブ状態は、製造時に付けられる固有デバイス識別子（UDI）である、冗長在庫管理単位（SKU）によって決まります。冗長 SKU UDI を持つコントローラは、起動されて永続カウントライセンスを実行するコントローラとペアになる場合、最初はスタンバイ状態です。永続カウントライセンスを持つコントローラの場合、コントローラがアクティブ状態であるか、スタンバイ状態であるかを手動で設定できます。

Cisco Prime Infrastructure は、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」ともいう）をサポートしています。AP SSO により、コントローラのスイッチオーバーが発生しても AP セッションがそのまま維持されます。コントローラの冗長性の詳細については、「関連項目」の「ワイヤレス冗長性の設定」を参照してください。

コントローラの冗長性は、Cisco Prime Infrastructure サーバのダウンタイムを削減するために使用される Cisco Prime Infrastructure HA フレームワークと似ていますが、別個のものです。詳細については、「関連項目」の「ハイ アベイラビリティの設定」を参照してください。

詳細については、『Cisco Prime Infrastructire Administrator Guide』を参照してください。

脅威からコントローラを保護するための Cisco Adaptive wIPS の設定

Cisco Prime Infrastructure は、プロファイルを使用してワイヤレス脅威保護機能をすばやくアクティブにする Cisco 適応型ワイヤレス侵入防御システム（Cisco Adaptive wIPS または wIPS）をサポートしています。

Cisco Prime Infrastructure は、顧客タイプ、建築タイプ、および「教育」、「財務」、「軍事」、「見本市」などのような業種に基づいて事前定義された wIPS プロファイルのリストを提供します。これらのプロファイルは「そのまま」使用することも、要件に合わせてカスタマイズすることもできます。そして、選択した Mobility Services Engine とコントローラにプロファイルを適用できます。

Cisco Adaptive wIPS は Cisco Prime Infrastructure パーティション分割機能をサポートしていません。

詳細については、『Cisco Wireless Intrusion Prevention System Configuration Guide』を参照してください。

関連トピック

wIPS プロファイルの表示 （772 ページ）
wIPS プロファイルの追加 （772 ページ）
wIPS プロファイルの編集 （773 ページ）
wIPS プロファイルの適用 （775 ページ）
wIPS プロファイルの削除 （776 ページ）

wIPS プロファイルの表示

Prime Infrastructure の [wIPS プロファイル リスト（wIPS Profiles List）] ページから wIPS プロファイルにアクセスできます。このページでは、現在の wIPS プロファイルを表示、編集、適用、削除したり、新しい wIPS プロファイルを作成したりすることができます。

[サービス（Services）] > [モビリティサービス（Mobility Services）] > [wIPSプロファイル（wIPS Profiles）] の順に選択します。[wIPS Profiles List] に現在の wIPS プロファイルが一覧表示されます。このリストには、既存のプロファイルごとに次の情報が表示されます。

- [Profile Name]：wIPS プロファイルのユーザ定義名。

  wIPS プロファイルを表示または編集するには、[Profile Name] をクリックします。その後、「関連項目」の「wIPS プロファイルの編集」の手順を実行します。

- [Profile ID]：プロファイルの固有識別子。
- [Version]：プロファイルのバージョン。
- [MSE(s) Applied To]：このプロファイルが適用されている Mobility Services Engine（MSE）の数を示します。MSE 番号をクリックすると、プロファイルの割り当ての詳細が表示されます。
- [Controller(s) Applied To]：このプロファイルが適用されているコントローラの数を示します。コントローラ番号をクリックすると、プロファイルの割り当ての詳細が表示されます。

関連トピック

wIPS プロファイルの追加 （772 ページ）
wIPS プロファイルの編集 （773 ページ）
wIPS プロファイルの適用 （775 ページ）
wIPS プロファイルの削除 （776 ページ）
SSID グループの作成 （777 ページ）

wIPS プロファイルの追加

デフォルト プロファイルまたは現在設定済みのプロファイルを使用して、新しい wIPS プロファイルを作成できます。

ステップ 1 [Services] > [Mobility Services] > [wIPS Profiles] を選択します。

ステップ 2 [Select a command] > [Add Profile] > [Go] の順に選択します。

ステップ 3 [Profile Parameters] ページの [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 4 ドロップダウン リストから、該当する定義済みのプロファイルを選択するか、[Default] を選択します。定義済みのプロファイルには次のものがあります。

- Education
- EnterpriseBest
- EnterpriseRogue
- Financial
- HealthCare
- HotSpotOpen
- Hotspot8021x
- Military
- Retail
- Tradeshow
- Warehouse

ステップ 5 次のいずれかをクリックします。

- 変更および割り当てを行わずに wIPS プロファイルを保存する場合は、[Save] をクリックします。プロファイルはプロファイル リストに表示されます。後で編集および割り当てを行う場合は、「関連項目」の「wIPS プロファイルへのアクセス」の説明に従ってプロファイルにアクセスできます。
- プロファイルを保存して設定を編集し、Mobility Services Engine とコントローラに割り当てる場合は、[Save and Edit] をクリックします。詳細については、「関連項目」の「wIPS プロファイルの編集」を参照してください。

関連トピック

脅威からコントローラを保護するための Cisco Adaptive wIPS の設定 （771 ページ）
wIPS プロファイルの表示 （772 ページ）
wIPS プロファイルの編集 （773 ページ）

wIPS プロファイルの編集

wIPS プロファイル エディタを使用すると、次の内容を含むプロファイルの詳細を設定できます。

- SSID グループ：wIPS プロファイルを適用する SSID グループを選択します。
- ポリシーの包含：プロファイルに含めるポリシーを決定します。

- ポリシー レベル設定：しきい値、重大度、通知の種類、ACL または SSID グループなど、プロファイルに含まれる各ポリシーの設定を行います。
- MSE およびコントローラ アプリケーション：プロファイルを適用する MSE およびコントローラを選択します。

ステップ 1 次の手順で wIPS プロファイル エディタにアクセスします。

- 新しい wIPS プロファイルを作成し、[Save and Edit] をクリックします。
- **[サービス（Services）] > [モビリティ サービス（Mobility Services）] > [wIPS プロファイル（wIPS Profiles）]** を選択し、編集する wIPS プロファイルのプロファイル名をクリックします。

  Prime Infrastructure に [SSID グループ リスト（SSID Group List）] ページが表示されます。このページを使用して、現在の SSID グループの編集および削除、または新しいグループの追加を行うことができます。SSID グループのグローバル リストから選択することもできます。詳細については、「関連項目」の「SSID グループと wIPS プロファイルの関連付け」を参照してください。

ステップ 2 wIPS プロファイルに関連付ける SSID グループを選択し、[Save] をクリックします

ステップ 3 [Next] をクリックします。[Profile Configuration] ページが表示されます。

ステップ 4 [Select Policy] ペインのポリシー ツリーで、現在のプロファイルで有効または無効にするポリシーのチェックボックスをオンにします。

該当するブランチまたはポリシーのチェックボックスをオンにすることで、ブランチ全体または個別のポリシーを有効または無効にできます。

デフォルトでは、すべてのポリシーが選択されています。

ステップ 5 [Profile Configuration] ページで、個々のポリシーをクリックしてポリシーの説明を表示したり、現在のポリシー ルール設定を表示または変更します。各ポリシーで次のオプションを使用できます。

- [Add]：このポリシーに新しいルールを作成するには、[Add] をクリックして [Policy Rule Configuration] ページにアクセスします。
- [Edit]：このルールの設定を編集するには、該当するルールのチェックボックスをオンにし、[Edit] をクリックして [Policy Rule Configuration] ページにアクセスします。
- [Delete]：削除するルールのチェックボックスをオンにし、[Delete] をクリックします。[OK] をクリックして、削除を実行します。

  1 つ以上のポリシー ルールが存在する必要があります。リスト内で唯一のポリシー ルールは削除できません。
- [Move Up]：リスト内で上に移動するルールのチェックボックスをオンにします。[Move Up] をクリックします。
- [Move Down]：リスト内で下に移動するルールのチェックボックスをオンにします。[Move Down] をクリックします。

  ポリシー レベルで次の設定を行うことができます。

- [Threshold]（すべてのポリシーに適用されるわけではありません）：選択したポリシーに関連付けられたしきい値または上限を示します。ポリシーのしきい値に達すると、アラームが生成されます。

  すべてのポリシーに 1 つ以上のしきい値が含まれている必要があるため、標準的なワイヤレス ネットワークの問題に基づいて、各ポリシーにデフォルトのしきい値が定義されています。

  しきい値オプションは、選択したポリシーに応じて異なります。

  Cisco Adaptive wIPS DoS およびセキュリティ ペネトレーション攻撃からのアラームは、セキュリティ アラームとして分類されます。これらの攻撃の概要は [Security Summary] ページにあります。このページにアクセスするには、[Monitor] > [Security] の順に選択します。wIPS の攻撃は [Threats and Attacks] セクションにあります。

- [Severity]：選択したポリシーの重大度を示します。パラメータとしては、[critical]、[major]、[info]、および [warning] があります。このフィールドの値は、ワイヤレス ネットワークに応じて変わります。
- [Notification]：閾値に関連付けられた通知の種類を示します。
- [ACL/SSID Group]：この閾値が適用される ACL または SSID グループを示します。

  選択されたグループに対してのみポリシーが適用されます。

ステップ 6 プロファイル設定が完了したら、[Save] をクリックして変更内容をプロファイルに保存します。

ステップ 7 [Next] をクリックすると [MSE/Controller(s)] ページが表示されます。

ステップ 8 [Apply Profile] ページで、現在のプロファイルを適用する MSE とコントローラのチェックボックスをオンにします。

ステップ 9 選択が完了したら、[Apply] をクリックして現在のプロファイルを選択した MSE とコントローラに適用します。

新しく作成したプロファイルを [Profile List] ページから直接適用することもできます。「関連項目」の「wIPS プロファイルの適用」を参照してください。

関連トピック

脅威からコントローラを保護するための Cisco Adaptive wIPS の設定 （771 ページ）
wIPS プロファイルの表示 （772 ページ）
wIPS プロファイルの適用 （775 ページ）
wIPS プロファイルの削除 （776 ページ）
SSID グループの作成 （777 ページ）

wIPS プロファイルの適用

ステップ 1 [Services] > [Mobility Services] > [wIPS Profiles] の順に選択します。

ステップ 2 適用する wIPS プロファイルのチェックボックスをオンにします。

ステップ 3 [Select a command] > [Apply Profile] > [Go] の順に選択します。

ステップ 4 プロファイルを適用する Mobility Services Engine とコントローラを選択します。

新しいプロファイルの割り当てが現在の割り当てと異なる場合、プロファイルを別の名前で保存するよう求められます。

ステップ 5 [Apply] をクリックします。

関連トピック

脅威からコントローラを保護するための Cisco Adaptive wIPS の設定 （771 ページ）
SSID グループの作成 （777 ページ）

wIPS プロファイルの削除

MSE とコントローラに現在適用されているプロファイルは削除できません。

ステップ 1 **[サービス（Services）] > [モビリティサービス（Mobility Services）] > [wIPSプロファイル（wIPS Profiles）]** の順に選択します。

ステップ 2 削除する wIPS プロファイルのチェックボックスをオンにします。

ステップ 3 **[コマンドの選択（Select a Command）] > [プロファイルの削除（Delete Profile）] > [実行（Go）]** を選択します。

ステップ 4 [OK] をクリックして削除を実行します。

関連トピック

脅威からコントローラを保護するための Cisco Adaptive wIPS の設定 （771 ページ）
wIPS プロファイルの追加 （772 ページ）
wIPS プロファイルの編集 （773 ページ）
wIPS プロファイルの適用 （775 ページ）

SSID グループと wIPS プロファイルの関連付け

SSID（Service Set IDentifier）は、802.11（Wi-Fi）ネットワークを識別するトークンまたはキーです。802.11 ネットワークに参加するには SSID が必要になります。

SSID を wIPS プロファイルに関連付けるには、SSID を SSID グループに追加して、その SSID グループを wIPS プロファイルに関連付けます。

関連トピック

脅威からコントローラを保護するための Cisco Adaptive wIPS の設定 （771 ページ）
wIPS プロファイルの削除 （776 ページ）
SSID グループの作成 （777 ページ）
SSID グループの編集 （777 ページ）

SSID グループの作成

ステップ 1 **[サービス（Services）] > [モビリティサービス（Mobility Services）] > [wIPSプロファイル（wIPS Profiles）]** の順に選択します。

ステップ 2 いずれかの wIPS プロファイルのプロファイル名をクリックします。Prime Infrastructure に SSID グループリストとグループが表示されます。

ステップ 3 **[コマンドの選択（Select a Command）] > [グループの追加（Add Groups）] > [実行（Go）]** を選択します。

ステップ 4 テキスト ボックスに SSID グループ名を入力します。

ステップ 5 [SSID List] テキスト ボックスに SSID を入力します。複数の SSID を入力するには、各 SSID の後に改行を入れます。

ステップ 6 [Save] をクリックします。

関連トピック

脅威からコントローラを保護するための Cisco Adaptive wIPS の設定 （771 ページ）
SSID グループと wIPS プロファイルの関連付け （776 ページ）

SSID グループの編集

ステップ 1 **[サービス（Services）] > [モビリティサービス（Mobility Services）] > [wIPSプロファイル（wIPS Profiles）]** の順に選択します。

ステップ 2 いずれかの wIPS プロファイルのプロファイル名をクリックします。Prime Infrastructure に SSID グループリストとグループが表示されます。

ステップ 3 編集する SSID グループのチェックボックスをオンにします。

ステップ 4 **[コマンドの選択（Select a Command）] > [グループの編集（Edit Group）] > [実行（Go）]** を選択します。

ステップ 5 [SSID Group Name] または [SSID List] に必要な変更を加えます。

ステップ 6 [Save] をクリックします。

関連トピック

脅威からコントローラを保護するための Cisco Adaptive wIPS の設定 （771 ページ）
wIPS プロファイルの表示 （772 ページ）

SSID グループの削除

ステップ 1 **[サービス（Services）] > [モビリティサービス（Mobility Services）] > [wIPSプロファイル（wIPS Profiles）]** の順に選択します。

ステップ 2 いずれかの wIPS プロファイルのプロファイル名をクリックします。Prime Infrastructure に SSID グループリストとグループが表示されます。

ステップ 3 削除する SSID グループのチェックボックスをオンにします。

ステップ 4 **[コマンドの選択（Select a Command）]** > **[グループの削除（Delete Group）]** > **[実行（Go）]** を選択します。

ステップ 5 [OK] をクリックして削除を実行します。

関連トピック

脅威からコントローラを保護するための Cisco Adaptive wIPS の設定 （771 ページ）
wIPS プロファイルの表示 （772 ページ）
wIPS プロファイルの編集 （773 ページ）

MSE サーバの高可用性の設定

Cisco Prime Infrastructure を使用して、MSE ハイ アベイラビリティ（HA）が設定された Cisco モビリティ サービス エンジン（MSE）デバイスをペアリングおよび管理することができます。その方法と関連タスクの実行方法については、下記の「関連項目」を参照してください。

関連トピック

MSE HA サーバのフェールオーバーとフェールバック （778 ページ）
MSE HA サーバの構成 （779 ページ）
プライマリおよびセカンダリ MSE HA サーバに関する詳細の表示 （780 ページ）
MSE サーバの HA ステータスの表示 （781 ページ）
MSE HA の手動フェールオーバーまたはフェールバックのトリガー （782 ページ）
MSE サーバでの自動 HA フェールオーバーおよびフェールバックの設定 （782 ページ）

MSE HA サーバのフェールオーバーとフェールバック

MSE HA は、プライマリ MSE に障害が発生しても MSE サービスに引き続きアクセスできるようにするための機能です。セカンダリ MSE がプライマリ MSE のデータの完全なコピーを保持して、バックアップとして機能します。ヘルス モニタおよび「ハートビート」のプロセスがプライマリとセカンダリの両方で実行されることで、各サーバは互いの状態を常に把握できます。

プライマリ MSE で障害が発生すると、必ずセカンダリ MSE への「フェールオーバー」がトリガーされます。Prime Infrastructure は、プライマリの問題が解決するまで、プライマリではなくセカンダリのモビリティ サービスを使用します。

プライマリが復旧すると「フェールバック」がトリガーされます。プライマリ MSE に制御が戻され、フェールオーバー中のネットワークの状態に関するデータがセカンダリ MSE からプライマリに複製されます。

MSE HA を設定する場合、自動または手動のどちらでフェールオーバーをトリガーするか選択できます。フェールバックについても同様の選択肢があります。

MSE HA を手動フェールオーバーまたはフェールバックに設定した場合は、プライマリに障害が発生したときや、サービスが復旧したときに送信される重大アラームに応じて、それぞれの動作をユーザがトリガーする必要があります。

自動フェールオーバーを行うように MSE HA を設定すると、ネットワーク管理者による MSE HA の管理の必要性が減少します。また、セカンダリ サーバが自動的に起動されるため、約 10 秒以内（デフォルト）でプライマリの障害が検出され、フェールオーバーの発生原因となった状況への対応に要する時間が削減されます。MSE HA が自動フェールバックに設定されている場合、システムは 1 分に 1 回送信される ping メッセージを 30 回正常に受信するまでフェールバックをトリガーしません。

関連トピック

MSE HA サーバの構成 （779 ページ）
MSE サーバでの自動 HA フェールオーバーおよびフェールバックの設定 （782 ページ）
MSE サーバの高可用性の設定 （778 ページ）

MSE HA サーバの構成

MSE デバイスのハイ アベイラビリティをアクティブ化するには、1 台の MSE サーバがプライマリ MSE デバイスとして動作し、別の 1 台がセカンダリ MSE として動作するペアリングを作成する必要があります。

ペアリングできるのは、次の状態の MSE デバイスのみです。

- 「関連項目」の「Configuring MSE High Availability」の説明に従って、MSE ハイ アベイラビリティで使用できるよう適切に設定されている。
- 「関連項目」の「Prime Infrastructure への MSE の追加」の説明に従って、Prime Infrastructure に追加されている。

はじめる前に

ペアリングを作成するには、次の情報が必要です。

- プライマリ MSE サーバのデバイス名。
- セカンダリ MSE サーバのデバイス名。これは、以前に割り当てたデバイス名か、サーバのペアリング時に割り当てる新しい名前になります。
- セカンダリ MSE HA サーバの IP アドレス。HA 用に MSE サーバを設定したときに割り当てた、HA ヘルス モニタの IP アドレスです。
- セカンダリ MSE HA サーバのパスワード。HA 用に MSE サーバを設定した際に割り当てた Prime Infrastructure 通信パスワードです。

また、手動または自動フェールバックのどちらで MSE HA サーバを設定するかを決める必要があります。ガイドラインについては、「関連項目」の「MSE HA の自動および手動のフェールオーバーとフェールバック」を参照してください。

ステップ 1 **[サービス（Services）]>[モビリティサービス（Mobility Services）]>[モビリティサービスエンジン（Mobility Services Engines）]** の順に選択します。既存の MSE のリストが表示されます。

ステップ 2 リストで、プライマリ MSE HA サーバとして動作させる MSE を見つけます。

ステップ 3 MSE リストの [Secondary Server] 列には、「N/A (Click here to configure)」というメッセージが表示されます。このリンクをクリックして、プライマリ MSE の HA 設定ページを表示します。

ステップ 4 該当するフィールドに、セカンダリ MSE のデバイス名、ヘルス モニタの IP アドレス、および Prime Infrastructure 通信パスワードを入力します。

ステップ 5 フェールオーバーおよびフェールバックのタイプを指定します。[手動（Manual）]または[自動（Automatic）]のいずれかを選択できます。

ステップ 6 [長時間のフェールオーバー待機（Long Failover Wait）] を指定します。これは、プライマリ MSE の障害が検出された後、システムが自動フェールオーバーをトリガーするまでに待機する最大時間です。デフォルトは 10 秒で、最大は 120 秒です。

ステップ 7 **[保存（Save）]** をクリックします。Prime Infrastructure は、これらの MSE のペアリングを確認するプロンプトを表示します。[OK] をクリックして確認します。

Prime Infrastructure は、ペアリングと同期を自動的に実行します。これらのプロセスは、ネットワーク帯域幅やその他の要因に応じて、完了までに最大20分かかる場合があります。これらのプロセスの進捗を確認するには、**[サービス（Services）]** > **[モビリティ サービス エンジン（Mobility Services Engine）]** > **[システム（System）]** > **[サービス高可用性（Services High Availability）]** > **[HA ステータス（HA Status）]** を選択します。

関連トピック

MSE HA サーバのフェールオーバーとフェールバック （778 ページ）
MSE サーバでの自動 HA フェールオーバーおよびフェールバックの設定 （782 ページ）
MSE サーバの高可用性の設定 （778 ページ）

プライマリおよびセカンダリ MSE HA サーバに関する詳細の表示

ステップ 1 **[サービス（Services）]** > **[モビリティサービス（Mobility Services）]** > **[モビリティサービスエンジン（Mobility Services Engines）]** の順に選択します。

ステップ 2 HA パラメータを表示する方法は次のとおりです。

- プライマリ MSE HA サーバの場合は、[Device Name] 列でサーバの名前をクリックします。
- セカンダリ MSE HA サーバの場合は、[Secondary Server] 列でサーバの名前をクリックします。

Prime Infrastructure に、選択したサーバのモビリティ サービスの設定ページが表示されます。

ステップ 3 左側のサイドバーのメニューから [HA設定（HA Configuration）] を選択します。[HA 設定（HA Configuration）] ページに次の情報が表示されます。

- [プライマリ ヘルス モニタ IP（Primary Health Monitor IP）]
- Secondary Device Name
- Secondary IP Address
- [セカンダリ パスワード（Secondary Password）]
- Secondary Platform UDI
- Secondary Activation Status

- [フェールオーバー タイプ（Failover Type）]
- Failback Type
- Long Failover Wait

関連トピック

MSE HA サーバの構成 （779 ページ）
MSE HA の手動フェールオーバーまたはフェールバックのトリガー （782 ページ）
MSE サーバの HA ステータスの表示 （781 ページ）
MSE サーバでの自動 HA フェールオーバーおよびフェールバックの設定 （782 ページ）
MSE サーバの高可用性の設定 （778 ページ）

MSE サーバの HA ステータスの表示

ステップ 1 **[サービス（Services）]>[モビリティサービス（Mobility Services）]>[モビリティサービスエンジン（Mobility Services Engines）]** の順に選択します。

ステップ 2 HA ステータスを表示する方法は次のとおりです。

- プライマリ MSE HA サーバの場合は、[Device Name] 列でサーバの名前をクリックします。
- セカンダリ MSE HA サーバの場合は、[Secondary Server] 列でサーバの名前をクリックします。

Prime Infrastructure に、選択したサーバのモビリティ サービスの設定ページが表示されます。

ステップ 3 左側のサイドバーのメニューで [HA ステータス（HA Status）] を選択します。[現在の高可用性ステータス（Current High Availability Status）] ページに、次の情報が表示されます。

- [ステータス（Status）]：MSE HA サーバがアクティブで正しく同期されているかどうかが表示されます。
- [ハートビート（Heartbeats）]：MSE HA サーバがパートナーとハートビート信号を交換しているかどうかが表示されます。
- [データ レプリケーション（Data Replication）]：MSE HA サーバがパートナーのデータを複製しているかどうかが表示されます。
- [平均ハートビート応答時間（Mean Heartbeat Response Time）]：サーバ間の平均ハートビート応答時間が表示されます。
- [イベント ログ（Events Log）]：MSE サーバが生成した直近 20 個のイベントが表示されます。

ステップ 4 MSA サーバの HA ステータス情報とイベント ログを更新するには、[ステータスの更新（Refresh Status）] をクリックします。

関連トピック

MSE HA サーバの構成 （779 ページ）
プライマリおよびセカンダリ MSE HA サーバに関する詳細の表示 （780 ページ）
MSE サーバでの自動 HA フェールオーバーおよびフェールバックの設定 （782 ページ）
MSE サーバの高可用性の設定 （778 ページ）

MSE HA の手動フェールオーバーまたはフェールバックのトリガー

手動フェールオーバーとフェールバックはデフォルトで有効になっています。手動設定の場合、システム アラームに応じて、Prime Infrastructure の管理者がフェールオーバーおよびフェールバックを手動でトリガーする必要があります。

ペアリングした MSE HA サーバを自動フェールオーバーおよびフェールバックに設定することもできます（「関連項目」を参照）。

ステップ 1 **[サービス（Services）]>[モビリティサービス（Mobility Services）]>[モビリティサービスエンジン（Mobility Services Engines）]** の順に選択します。

ステップ 2 トリガーする方法は次のとおりです。

- プライマリからセカンダリへのフェールオーバーをトリガーするには、[Device Name] 列でプライマリ MSE HA サーバの名前をクリックします。
- セカンダリからプライマリへのフェールバックをトリガーするには、[Secondary Server] 列でセカンダリ MSE HA サーバの名前をクリックします。

Prime Infrastructure に、選択したサーバのモビリティ サービスの設定ページが表示されます。

ステップ 3 左側のサイドバーのメニューから [HA設定（HA Configuration）] を選択します。[HA 設定（HA Configuration）] ページに、選択したサーバの HA 設定情報が表示されます。

ステップ 4 フェールオーバーまたはフェールバックを開始するには、[Switchover] をクリックします。

ステップ 5 [OK] をクリックして、スイッチオーバーの開始を確定します。

関連トピック

MSE HA サーバのフェールオーバーとフェールバック （778 ページ）
MSE サーバでの自動 HA フェールオーバーおよびフェールバックの設定 （782 ページ）
MSE サーバの高可用性の設定 （778 ページ）

MSE サーバでの自動 HA フェールオーバーおよびフェールバックの設定

手動フェールオーバーとフェールバックはデフォルトで有効になっています。ペアリングした MSE HA サーバを自動フェールオーバーおよびフェールバックに設定すると、次のように自動的に変更されます。

- プライマリからセカンダリへのフェールオーバー：セカンダリがプライマリの障害を検出するとすぐにトリガーされます。
- セカンダリからプライマリへのフェールバック：セカンダリからプライマリへの ping メッセージの送信が 30 回成功するとトリガーされます。ping 要求は、1 分間に 1 回送信されます。

ステップ 1 **[サービス（Services）] > [モビリティ サービス（Mobility Services）] > [MSE 高可用性（MSE High Availability）]** を選択します。

ステップ 2 [デバイス名（Device Name）] 列でプライマリ MSE HA サーバの名前をクリックします。

Prime Infrastructure にプライマリ MSE HA サーバの [HA 設定（HA Configuration）] ページが表示されます。

ステップ 3 [Failover Type] および [Failback Type] リスト ボックスで [Automatic] を選択します。

ステップ 4 必要に応じて、プライマリでの障害の検出から自動フェールオーバーまでの最大遅延を制御するには、[Long Failover Wait] の値を変更します。デフォルトは 10 秒です。

ステップ 5 [保存（Save）] をクリックして変更内容を保存します。

関連トピック

MSE HA サーバのフェールオーバーとフェールバック （778 ページ）
MSE HA の手動フェールオーバーまたはフェールバックのトリガー （782 ページ）
MSE サーバの高可用性の設定 （778 ページ）

MSE HA サーバのペアリング解除

ステップ 1 **[サービス（Services）] > [モビリティ サービス（Mobility Services）] > [MSE 高可用性（MSE High Availability）]** を選択します。

ステップ 2 [デバイス名（Device Name）] 列でプライマリ MSE HA サーバの名前をクリックします。

Prime Infrastructure にプライマリ MSE HA サーバの [HA 設定（HA Configuration）] ページが表示されます。

ステップ 3 [Delete] をクリックして、MSE HA サーバのペアリングを解除します。

ステップ 4 [OK] をクリックして、MSE HA サーバのペアリング解除を確定します。

関連トピック

MSE HA サーバの構成 （779 ページ）
MSE サーバの高可用性の設定 （778 ページ）

プラグ アンド プレイを使用したコントローラの設定

自動プロビジョニングを使用すると、Cisco Prime Infrastructure で現在のワイヤレス LAN コントローラ (WLC) を自動的に新規設定したり、交換したりすることができます。Cisco Prime

Infrastructure 自動プロビジョニング機能を使用すると、大量のコントローラがあるお客様の展開を簡素化できます。

自動プロビジョニングの権限を有効にするには、Admin、Root、または SuperUser ステータスでログインしている必要があります。

ユーザの自動プロビジョニング権限を有効または無効にするには、Cisco Prime Infrastructure の [管理設定（Administration Settings）] > [ユーザ、ロール、およびAAA（Users, Roles, and AAA）] > [ユーザグループ（User Groups）] > [グループ名（group name）] > [許可されているタスクのリスト（List of Tasks Permitted）] で、許可されているタスクを編集します。各チェックボックスをオンまたはオフにして、これらの権限の有効と無効を切り替えます。

コントローラの無線および b/g ネットワークは、Cisco Prime Infrastructure のダウンロードされたスタートアップ コンフィギュレーション ファイルで最初は無効になっています。必要に応じて、テンプレートを使用し、それらの無線ネットワークを有効にできます。テンプレートは、自動化されたテンプレートの 1 つとして含まれている必要があります。

自動プロビジョニング フィルタ コンテンツを指定するには、アプリケーションに直接詳細を入力するか、CSV ファイルから詳細をインポートします。自動プロビジョニング機能は、5500 シリーズのコントローラと 5500 シリーズ以外のコントローラをサポートしています。5500 シリーズ以外のコントローラでは、AP マネージャ インターフェイスのコンフィギュレーション情報が定義されているのに対し、5500 シリーズのコントローラにはこの情報がありません。

自動プロビジョニング機能にアクセスするには、**[設定（Configuration）] > [プラグアンドプレイ（Plug and Play）] > [WLC自動プロビジョニング（WLC Auto Provisioning）]** を選択します。

第 27 章

ワイヤレス テクノロジーの設定

- AP 上で最適化されたモニタ モードを使用したタグ付きアセットの追跡 （786 ページ）
- ワイヤレス チョークポイントの設定 （787 ページ）
- 統合 AP の管理 （788 ページ）
- Autonomous AP の管理 （792 ページ）
- アクセス ポイント XOR アンテナの設定 （799 ページ）
- AP オンボーディング プロファイルの設定 （802 ページ）
- アクセス ポイントの検索 （805 ページ）
- ワイヤレス設定グループ （807 ページ）
- メッシュ ネットワークにおけるリンクの表示 （810 ページ）
- コントローラの不正 AP 分類ルールの定義 （811 ページ）
- コントローラの自動プロビジョニングを使用した WLC の追加と置換 （811 ページ）
- AP オンボーディング プロファイルの設定 （813 ページ）
- 9800 シリーズ構成モデルに関する情報 （817 ページ）
- Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの Cisco Umbrella ポリシーのローカル ドメインの設定 （821 ページ）
- Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの Cisco Umbrella ポリシーの設定 （822 ページ）
- Cisco Catalyst 9800 シリーズ ワイヤレス コントローラに Flex Sxp プロファイルを設定します （822 ページ）
- Cisco Catalyst 9800 シリーズ ワイヤレス コントローラに Flex プロファイルを設定します （823 ページ）
- Catalyst 9800 シリーズ ワイヤレス コントローラの Airtime Fairness の設定 （823 ページ）
- Catalyst 9800 シリーズ ワイヤレス コントローラのリモート LAN（RLAN）の設定 （825 ページ）
- Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ上でルールを展開する （826 ページ）
- Cisco AireOS コントローラ設定を Cisco Catalyst 9800 シリーズ コントローラに変換する （827 ページ）

AP 上で最適化されたモニタ モードを使用したタグ付きアセットの追跡

タグのモニタリングとロケーション計算を最適化するには、アクセス ポイントの 2.4 GHz 帯（802.11b/g 無線）内で、最大 4 つのチャネルに対して Tracking Optimized Monitor Mode（TOMM）を有効にします。これによって、タグが機能するようにプログラミングされているチャネルだけを対象にチャネル スキャンを実行できます（チャネル 1、チャネル 6、チャネル 11 など）。

アクセス ポイント レベルでモニタ モードを有効にした後、TOMM を有効にして、そのアクセス ポイントの 802.11b/g 無線にモニタ チャネルを割り当てる必要があります。

アクセス ポイント無線で TOMM を有効にして、モニタ チャネルを割り当てるには、次の手順を実行します。

ステップ 1 アクセスポイント レベルでモニタ モードを有効にしたら、**[設定（Configuration）] > [ワイヤレス テクノロジー（Wireless Technologies）] > [アクセス ポイントの無線（Access Point Radios）]** を選択します。

ステップ 2 [アクセス ポイント（Access Points）] ページで、適切なアクセス ポイントの **[802.11 b/g 無線（802.11 b/g Radio）]** リンクをクリックします。

ステップ 3 [一般（General）] グループ ボックスで、チェックボックスをオフにして **[管理ステータス（Admin Status）]** を無効にします。無線が無効になります。

ステップ 4 **[TOMM]** チェックボックスをオンにします。このチェックボックスは、モニタ モードの AP の場合のみ表示されます。設定可能な 4 つのチャネルそれぞれにドロップダウン リストが表示されます。

ステップ 5 アクセス ポイントによるタグのモニタを有効にする 4 つのチャネルを選択します。

（注） モニタ対象として 4 つすべてのチャネルを選択する必要はありません。モニタリング チャネルを削除するには、チャネルのドロップダウン リストから **[なし（None）]** を選択します。

ステップ 6 **[保存（Save）]** をクリックします。チャネル選択が保存されます。

ステップ 7 [無線パラメータ（Radio parameters）] ページで、**[管理ステータス（Admin Status）]** チェックボックスをオンにして無線を再度有効にします。

ステップ 8 **[保存（Save）]** をクリックします。これで、アクセス ポイントが TOMM アクセス ポイントとして設定されました。

[モニタ（Monitor）] > [アクセス ポイント（Access Points）] ページに、AP モードが [モニタ/TOMM（Monitor/TOMM）] と表示されます。

ワイヤレス チョークポイントの設定

ワイヤレス チョークポイントの作成

チョークポイントを追加するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）]** > **[ワイヤレステクノロジー（Wireless Technologies）]** > **[チョークポイント（Chokepoints）]** の順に選択します。

ステップ 2 [コマンドの選択（Select a command）] ドロップダウン リストから **[チョーク ポイントの追加（Add Chokepoints）]** を選択し、**[実行（Go）]**をクリックします。

ステップ 3 チョークポイントの MAC アドレスと名前を入力します。

ステップ 4 これが [Entry/Exit Chokepoint] であることを示すには、チェックボックスを選択します。

ステップ 5 チョークポイントのカバレッジ範囲を入力します。

チョークポイントの範囲は、視覚的な表示のみです。これは製品固有です。実際の範囲は、該当するチョークポイント ベンダー ソフトウェアを使用して別個に設定する必要があります。

ステップ 6 **[OK]** をクリックします。

データベースにチョークポイントを追加したら、適切な Prime Infrastructure フロア マップに配置できます。

ネットワークからのワイヤレス チョークポイントの削除

チョークポイントを削除するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）]** > **[ワイヤレステクノロジー（Wireless Technologies）]** > **[チョークポイント（Chokepoints）]** の順に選択します。

ステップ 2 削除するチョークポイントのチェックボックスを選択します。

ステップ 3 [コマンドの選択（Select a command）] ドロップダウン リストから **[チョーク ポイントの削除（Remove Chokepoints）]** を選択し、**[実行（Go）]**をクリックします。

ステップ 4 [**OK**] をクリックして削除を確認します。

統合 AP の管理

コンフィギュレーション

AP をメンテナンス状態にする

アクセス ポイントをメンテナンス ステートに移行するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [アクセス ポイント無線（Access Points Radio）]** をクリックします。

[統合アクセス ポイント（Unified Access Points）] ページが表示されます。

ステップ 2 **[統合 AP 無線（Unified AP Radio）]** タブで、目的の AP デバイスを選択し、**[設定（Configure）] > [メンテナンス状態にする（Place in Maintenance State）]** をクリックします。

アクセス ポイントがメンテナンス ステートに移行されます。

アクセス ポイントがメンテナンス ステートに移行されると、アクセス ポイント ダウン アラームは、重大よりも低い重大度で処理されます。

（注） メンテナンス状態にあるアクセス ポイント ダウン アラームの重大度を下げると、アラーム通知ポリシーの状態が「重大なイベント」であった場合でも、Prime Infrastructure によりアラーム通知メールが送信されるのを防ぐことはできません。

メンテナンス状態からの AP の削除

アクセス ポイントをメンテナンス ステートから削除するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [アクセス ポイント無線（Access Points Radios）]** をクリックします。

[統合 AP ラジオ（Unified AP Radio）] ページが表示されます。

ステップ 2 **[統合 AP 無線（Unified AP Radio）]** タブで、目的の AP デバイスを選択し、**[設定（Configure）] > [メンテナンス状態から削除（Remove from Maintenance State）]** をクリックします。

アクセス ポイントがメンテナンス状態から削除されます。

スケジューリング（Scheduling）

AP 無線ステータス変更のスケジュール設定

無線ステータスの変更スケジュールを設定する手順は、次のとおりです。

ステップ 1 **[設定（Configuration）] > [アクセス ポイント無線（Access Points Radios）]** をクリックします。

ステップ 2 **[Unified AP 無線（Unified AP Radio）]** タブで、目的の AP を選択し、**[[スケジュール（Schedule）] > [無線ステータスのスケジュール（Schedule Radio Status）]** をクリックします。

ステップ 3 [管理ステータス（Admin Status）] ドロップダウン リストから、[有効（Enable）] または [無効（Disable）] を選択します。

ステップ 4 [時（Hours）]および[分（Minutes）] ドロップダウン リストを使用して、スケジュール時間を決定します。

ステップ 5 カレンダー アイコンをクリックして、ステータス変更の予定日を選択します。

ステップ 6 タスクを周期的に繰り返して実行する場合は、[毎日（Daily）] または [毎週（Weekly）] を選択します。タスクを一度だけ実行する場合は、[繰り返しなし（No Recurrence）] を選択します。

ステップ 7 [保存（Save）] を選択して、スケジュール設定したタスクを確定します。

スケジュール済み AP 無線ステータス変更の表示

現在スケジュール設定されている無線ステータス タスクを表示する手順は、次のとおりです。

ステップ 1 **[設定（Configuration）] > [アクセス ポイント無線（Access Points Radios）]** をクリックします。

ステップ 2 **[Unified AP 無線（Unified AP Radio）]** タブで、目的の AP を選択し、**[[スケジュール（Schedule）] > [View Schedule Radio Task(s)（無線タスクのスケジュールの表示）]** をクリックします。

スケジュール設定済みのタスクに関する次の情報が表示されます。

1. [スケジュール済みタスク（Scheduled Task(s)）]：そのアクセス ポイントとアクセス ポイント無線を表示するタスクを選択します。
2. [スケジュール済み無線管理ステータス（Scheduled Radio admin Status）]：ステータス変更（[有効（Enable）] または [無効（Disable）]）を示します。
3. [スケジュール時刻（Schedule Time）]：スケジュール タスクの発生時間を示します。
4. [実行ステータス（Execution status）]：タスクがスケジュール設定されているかどうかを示します。
5. [繰り返し（Recurrence）]：タスクが繰り返し実行されるようにスケジュール設定している場合は、その周期（[毎日（Daily）] または [毎週（Weekly）]）を示します。
6. [次の実行（Next Execution）]：タスクの次の実行日時を示します。
7. [最終実行日時（Last Execution）]：タスクの最後の実行日時を示します。

8. [スケジュール解除（Unschedule）]：スケジュール設定されているタスクをキャンセルする場合は、[スケジュール解除（Unschedule）] をクリックします。[OK] をクリックして、キャンセルを確定します。

メンテナンス状態における AP のアラームの表示

Prime Infrastructure は、クリティカル アラームを使用して、管理対象アクセス ポイントがダウンしているかどうかを追跡します。コントローラは、次のことが発生した場合に、3 つの異なるアラームを送信します。

- アクセス ポイントがダウンになる
- アクセス ポイントの無線 A がダウンになる
- アクセス ポイントの無線 B/G がダウンになる

リリース 7.0.172.0 以降では、これらの 3 つのアラームは単一のアラームにグループ化されます。

アクセス ポイントの技術メンテナンス中は、クリティカル アラームの優先順位付けを解除する必要があります。アクセス ポイントのアラームの重大度の優先順位付けを解除するには、**[設定（Configure）] > [アクセスポイント（Access Points）]** ページを使用します。アクセス ポイントをメンテナンス ステートに移行すると、そのアクセス ポイントのアラーム ステータスは黒色で表示されます。

AP イーサネット インターフェイスの設定

イーサネット インターフェイスを設定するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ワイヤレステクノロジー（Wireless Technologies）] > [アクセスポイントの無線（Access Point Radios）]** の順に選択します。

ステップ 2 [AP名（AP Name）] の下のリンクをクリックして、そのアクセス ポイント名についての詳細情報を表示します。[アクセス ポイントの詳細（Access Point Detail）] ページが表示されます。

（注） [アクセス ポイントの詳細（Access Point Details）] ページに、イーサネット インターフェイスのリストが表示されます。

ステップ 3 [インターフェイス（Interface）] の下のリンクをクリックすると、そのインターフェイスに関する詳細情報が表示されます。[イーサネット インターフェイス（Ethernet Interface）] ページが表示されます。

このページには、次のパラメータが表示されます。

- [AP の名前（AP Name）]：アクセス ポイントの名前。
- [スロット ID（Slot Id）]：スロット番号を示します。
- [管理ステータス（Admin Status）]：アクセス ポイントの管理状態を示します。
- [CDP ステート（CDP State）]：CDP ステートを有効にするには、[CDP ステート（CDP State）] チェックボックスをオンにします。

ステップ 4 **[保存（Save）]** をクリックします。

CSV ファイルのインポートによる AP の設定

現在のアクセス ポイントのコンフィギュレーション ファイルをインポートするには、次の手順を実行します。

（注） これを使用して、AP 名、プライマリ、セカンダリ、およびターシリア コントローラの詳細、AP ロケーションを一括で設定できます。

ステップ 1 **[設定（Configuration）]** > **[ワイヤレステクノロジー（Wireless Technologies）]** > **[アクセスポイントの無線（Access Point Radios）]** の順に選択します。

ステップ 2 **[統合 AP 無線（Unified AP Radio）]**ページで、該当する AP を選択し、**[インポート/エクスプローラー（Import / Export）]** > **[AP 設定のインポート（Import AP Config）]** をクリックします。

ステップ 3 テキスト ボックスに CSV ファイルのパスを入力するか、[参照（Browse）] をクリックして、コンピュータで CSV ファイルにナビゲートします。

CSV ファイルの最初の行は、含まれている列の説明に使用されます。[AP イーサネット MAC アドレス（AP Ethernet Mac Address）] 列は必須です。このページのパラメータは、CSV ファイルで定義されていない列に使用されます。

ファイル ヘッダーの例：

例：

```
AP Name,Ethernet MAC,Location,Primary Controller,Secondary Controller,Tertiary Controller
ap-1, 00:1c:58:74:8c:22, sjc-14-a, controller-4404-1, controller-4404-2, controller-4404-3
```

CSV ファイルには、次のフィールドを含めることができます。

- [AP イーサネット MAC アドレス（AP Ethernet MAC Address）]：必須
- [AP 名（AP Name）]：省略可能
- [ロケーション（Location）]：省略可能
- [プライマリ コントローラ（Primary Controller）]：省略可能
- [セカンダリ コントローラ（Secondary Controller）]：省略可能
- [ターシャリ コントローラ（Tertiary Controller）]：省略可能

省略可能フィールドは空のままにできます。[AP 設定のインポート（AP Config Import）] は、空の省略可能フィールド値を無視します。ただし、primaryMwar と secondaryMwar エントリが空の場合は、ユニファイド アクセス ポイントの更新は完了していません。

- [イーサネット MAC（Ethernet MAC）]：AP イーサネット MAC アドレス
- [AP 名（AP Name）]：AP 名
- [ロケーション（Location）]：AP ロケーション

- [プライマリ コントローラ（Primary Controller）]：プライマリ コントローラ名
- [セカンダリ コントローラ（Secondary Controller）]：セカンダリ コントローラ名
- [ターシャリ コントローラ（Tertiary Controller）]：ターシャリ コントローラ名

（注） 省略可能フィールドは空のままにできます。[AP 設定のインポート（AP Config Import）] は、空の省略可能フィールド値を無視します。ただし、プライマリ コントローラおよびセカンダリ コントローラのエントリが空の場合は、統合アクセス ポイントの更新は実行されません。

ステップ 4 適切な CSV ファイルのパスが [CSV ファイルの選択（Select CSV File）] テキスト ボックスに表示されたら、[OK] をクリックします。

アクセス ポイントでの CDP の設定

Cisco Discovery Protocol（CDP）は、すべてのシスコ製ネットワーク機器で実行されるデバイス検出プロトコルです。各デバイスはマルチキャスト アドレスに識別メッセージを送信し、他のデバイスから送信されたメッセージをモニタします。

（注） CDP は、デフォルトでイーサネットと、ブリッジの無線ポートで有効です。

ステップ 1 **[設定（Configuration）] > [ワイヤレステクノロジー（Wireless Technologies）] > [アクセスポイントの無線（Access Point Radios）]** の順に選択します。

ステップ 2 ソフトウェア リリース 5.0 以降のコントローラに関連付けられたアクセス ポイントを選択します。

ステップ 3 CDP を有効にする無線またはイーサネット インターフェイスのスロットをクリックします。

ステップ 4 インターフェイスで CDP を有効にするには、[CDP ステート（CDP State）] チェックボックスを選択します。

ステップ 5 **[保存（Save）]** をクリックします。

Autonomous AP の管理

Prime Infrastructure から、自律アクセス ポイントを追加するには、次の方法があります

デバイス情報を使用した自律 AP の追加

デバイス情報によって Autonomous アクセス ポイントを Prime Infrastructure に追加するには、カンマ区切りの IP アドレスとクレデンシャルを使用します。

Cisco Autonomous アクセス ポイントには、工場出荷時にデフォルトのイネーブル パスワード *Cisco* が設定されています。ユーザはこのパスワードを使用して、非特権モードにログインし、

show および debug コマンドを実行することができますが、これはセキュリティに対する脅威となります。不正アクセスを防止し、ユーザがアクセス ポイントのコンソール ポートからコンフィギュレーション コマンドを実行できるようにするには、デフォルトのイネーブル パスワードを変更する必要があります。

デバイス情報を使用して Autonomous アクセス ポイントを追加する手順は、次のとおりです。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）]** の順にクリックします。

ステップ 2 **[+]** アイコンをクリックして、ドロップダウン メニューから **[デバイスの追加（Add Device）]** を選択します。

ステップ 3 [全般（General）] タブで、Cisco アクセス ポイントの IP アドレスを入力します。DNS 名によって追加する場合は、DNS 名を追加します。

ステップ 4 [SNMP] タブで、Cisco アクセス ポイントで作成した SNMP のバージョンを選択します。

ステップ 5 SNMP v1 または v2c を使用する場合は、AP で設定された読み取り/書き込みコミュニティ ストリングを記述する必要があります。SNMP v3 を使用している場合は、以下を設定する必要があります。

- [ユーザ名（Username）]
- [モード（Mode）]
- 認証タイプ（Auth.Type）
- 認証パスワード（Auth.Password）
- Privacy タイプ
- プライバシー パスワード（Privacy Password）

ステップ 6 [Telent/SSH] タブで、Telnet/SSH パラメータを設定します。

ステップ 7 [HTTP/HTTPS] タブで HTTP クレデンシャルを指定して、Cisco Prime Infrastructure がそこからデータを収集できるようにします。

- [プロトコル（Protocol）] ドロップダウン リストから [HTTP] または [HTTPS] を選択します。TCP ポートは、選択したプロトコルのデフォルト ポートに自動的に変更されます。
- [TCPポート（TCP Port）] テキスト ボックスで、デフォルトを上書きする場合は、別の TCP ポートを入力します。
- ユーザの名前を入力します。
- パスワードを入力し、そのパスワードを確認します。
- モニタのユーザ名およびパスワードを入力し、そのパスワードを確認します。

ステップ 8 [追加（Add）] をクリックします。

AP が追加され、インベントリの収集が完了すると、Autonomous AP リスト ページ（[設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）] > [デバイス タイプ（Device Type）] > [自律 AP（Autonomous AP）]) に表示されます。Autonomous AP リストにない場合は、**[設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）] > [デバイス タイプ（Device Type）] > [不明なデバイス（Unknown Devices）]** ページを選択して、ステータスを確認します。

（注） Autonomous アクセス ポイントは、ライセンスの合計デバイス数に含まれません。

CSV ファイルを使用した自律 AP の追加

Autonomous アクセス ポイントを Prime Infrastructure に追加するには、WLSE からエクスポートした CSV ファイルを使用します。

CSV ファイルを使用して Autonomous アクセス ポイントを追加する手順は、次のとおりです。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）]** の順に選択します。

ステップ 2 **[+]** アイコンをクリックし、**[一括インポート（Bulk Import）]** オプションを選択します。

ステップ 3 [参照（Browse）] をクリックして、システムから CSV ファイルを選択します。

ステップ 4 [Import] をクリックします。

CSV ファイルを使用した自律 AP の一括更新

CSV ファイルをインポートすることで、複数の Autonomous アクセス ポイントのクレデンシャルを更新できます。

Autonomous アクセス ポイント情報を一括で更新するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ワイヤレステクノロジー（Wireless Technologies）] > [アクセスポイントの無線（Access Point Radios）]** の順に選択します。

ステップ 2 **[Autonomous AP 比率（Autonomous AP Radio）]** ページで、目的の AP のチェックボックスをオンにします。

ステップ 3 **[AP の一括更新（Bulk Update APs）]** をクリックします。
[Autonomous アクセス ポイントの一括更新（Bulk Update Autonomous Access Points）] ページが表示されます。

ステップ 4 **[ファイルの選択（Choose File）]** をクリックして CSV ファイルを選択し、インポートする CSV ファイルの場所を見つけます。

ステップ 5 [更新と同期（Update and Sync）] をクリックします。

自律 AP の一括更新用のサンプル CSV ファイル

次に、V2 デバイス用の CSV ファイルの例を示します。

```
ip_address, network_mask, snmp_version, snmp_community, snmpv3_user_name, snmpv3_auth_type,
```

```
 snmpv3_auth_password, snmpv3_privacy_type,
 snmpv3_privacy_password, snmp_retries,
snmp_timeout,telnet_username,telnet_password,telnet_retries,telnet_timeout
209.165.200.224,255.255.255.224,v2,public,,,,,3,4209.165.201.0,255.255.255.0,v2,public,,,,,3,4,Cisco,Cisco,2,10
```

（注） SNMP、telnet、または SSH クレデンシャルは必須です。

次に、V3 デバイス用の CSV ファイルの例を示します。

```
ip_address, network_mask, snmp_version, snmpv3_user_name, snmpv3_auth_type,
snmpv3_auth_password, snmpv3_privacy_type,
snmpv3_privacy_password, snmp_retries,
snmp_timeout,telnet_username,telnet_password,telnet_retries,
telnet_timeout209.165.200.224,255.255.255.224,v3,default,HMAC-MD5,default,None,,3,4209.165.201.0,255.255.255.224,v3,
default1,HMAC-MD5,default1,DES,default1,3,4,Cisco,Cisco,2,10
```

CSV ファイルには、次のフィールドを含めることができます。

- ip_address
- network_mask
- snmp_version
- snmp_community
- snmpv3_user_name
- snmpv3_auth_type
- snmpv3_auth_password
- snmpv3_privacy_type
- snmpv3_privacy_password
- snmp_retries
- snmp_timeout
- telnet_username
- telnet_password
- enable_password
- telnet_retries
- telnet_timeout

Prime Infrastructure からの自律 AP の削除

（注） 何らかの理由により、Autonomous アクセス ポイントを交換する場合は、代替のアクセス ポイントをネットワークにインストールする前に Prime Infrastructure から Autonomous アクセス ポイントを削除します。

Prime Infrastructure から Autonomous アクセス ポイントを削除するには、次の手順を実行します。

ステップ 1 削除するアクセスポイントのチェックボックスをオンにします。関連付けられていない AP を選択します。

ステップ 2 [コマンドの選択（Select a command）] ドロップダウン リストから、[AP の削除（Remove APs）] を選択します。

自律型 AP の表示

Autonomous アクセス ポイントが追加されると、[Monitor] > [Access Points] ページに表示されます。

Autonomous アクセス ポイントをクリックすると、次のような詳細が表示されます。

- アクセス ポイントの操作ステータス
- 無線情報、チャネル、電力、無線上のクライアント数などの主要な属性
- CDP 近隣情報

Autonomous アクセス ポイントは、[モニタ（Monitor）] > [マップ（Maps）] でも表示できます。

Autonomous アクセス ポイントをフロア領域に追加するには、**[モニタ（Monitor）] > [マップ（Maps）]** [フロア領域（floor area）] を選択して、[コマンドの選択（Select a command）] ドロップダウン リストから [アクセスポイントの追加（Add Access Points）] を選択します。

TFTP を介した自律 AP へのイメージのダウンロード

Lightweight アクセス ポイント イメージは、コントローラ イメージにバンドルされており、コントローラによって管理されます。Autonomous アクセス ポイント イメージは、WLSE、CiscoWorks、または Prime Infrastructure などの NMS システムで処理する必要があります。

TFTP を使用してイメージを Autonomous アクセス ポイントにダウンロードするには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ワイヤレステクノロジー（Wireless Technologies）] > [アクセスポイントの無線（Access Point Radios）]** の順に選択します。

ステップ 2 **[Autonomous AP 比率（Autonomous AP Radio）]** イメージをダウンロードする Autonomous アクセス ポイントのチェックボックスを選択します。

[AP Type] 列には、Autonomous と Lightweight のいずれのアクセス ポイントであるかが表示されます。

ステップ 3 **[ダウンロード（Download）] > [自律 AP イメージ (TFTP) のダウンロード（Download Autonomous AP Image (TFTP)）]** をクリックします。

[Autonomous AP へのイメージのダウンロード（Download images to Autonomous APs）] ページが表示されます。

ステップ 4 次のパラメータを設定します。

- [ファイルの格納場所（File is located on）] : [ローカル マシン（Local machine）] または [TFTP サーバ（TFTP server）] を選択します。
- [サーバ名（Server Name）] : デフォルト サーバを選択するか、[サーバ名（Server Name）] ドロップダウン リストから新しいサーバを追加します。
- [IP アドレス（IP address）] : TFTP サーバの IP アドレスを指定します。デフォルトのサーバを選択した場合は、これが自動的に入力されます。
- [Prime Infrastructure サーバ ファイルの場所（Prime Infrastructure Server Files In）] : Prime Infrastructure サーバ ファイルのある場所を指定します。デフォルトのサーバを選択した場合は、これが自動的に入力されます。
- [サーバ ファイル名（Server File Name）] : サーバ ファイル名を指定します。

ステップ 5 [ダウンロード（Download）] をクリックします。

ヒント 一部の TFTP サーバでは、32 MB を超えるファイルはサポートされません。

FTP を介した自律 AP へのイメージのダウンロード

イメージを自律型アクセス ポイントに（FTP を使用して）ダウンロードするには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ワイヤレステクノロジー（Wireless Technologies）] > [アクセスポイントの無線（Access Point Radios）]** の順に選択します。

ステップ 2 **[Autonomous AP 比率（Autonomous AP Radio）]** イメージをダウンロードする Autonomous アクセス ポイントのチェックボックスを選択します。[AP Type] 列には、Autonomous と Lightweight のいずれのアクセス ポイントであるかが表示されます。

ステップ 3 **[ダウンロード（Download）] > [自律 AP イメージ (FTP) のダウンロード（Download Autonomous AP Image (FTP)）]** をクリックします。

[Autonomous AP へのイメージのダウンロード（Download images to Autonomous APs）] ページが表示されます。

ステップ 4 ユーザ名とパスワードを含む FTP クレデンシャルを入力します。

ステップ 5 [Download] をクリックします。

ワークグループ ブリッジ（WGB）モードの自律 AP の表示

Workgroup Bridge（WGB）モードは、Autonomous アクセス ポイントがワイヤレス クライアントとして機能して、Lightweight アクセス ポイントに接続する特殊なモードです。AP モードが [ブリッジ（Bridge）] に設定され、アクセス ポイントがブリッジ対応である場合、WGB とその有線クライアントは、Prime Infrastructure にクライアントとしてリストされます。

WGB であるすべての Prime Infrastructure クライアントのリストを表示するには、**[モニタ（Monitor）] > [クライアント（Clients）]** を選択します。[表示（Show）] ドロップダウン リストから [WGBクライアント（WGB Clients）] を選択して、[実行（Go）] をクリックします。[クライアント（WGB として検出）（Clients (detected as WGBs)）] ページが表示されます。ユーザをクリックして、特定の WGB とその有線クライアントに関する詳細な情報を表示します。

（注） Prime Infrastructure は、Autonomous アクセス ポイントが Prime Infrastructure によって管理されているかどうかにかかわらず、Autonomous アクセス ポイントの WGB クライアント情報を提供します。WGB アクセス ポイントも Prime Infrastructure によって管理されている場合、Prime Infrastructure は他の Autonomous アクセス ポイントに類似したアクセス ポイントに対する基本的なモニタリング機能を提供します。

自律 AP の詳細のエクスポート

現在のアクセス ポイントのコンフィギュレーション ファイルをエクスポートするには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ワイヤレステクノロジー（Wireless Technologies）] > [アクセスポイントの無線（Access Point Radios）]** の順に選択します。

ステップ 2 [コマンドの選択（Select a command）] ドロップダウン リストから、[AP 設定のエクスポート（Export AP Config）] を選択します。

すべての Unified AP が CSV/EXCEL/XML ファイルにエクスポートされることを示すポップアップ アラート ボックスが表示されます。

ステップ 3 [OK] をクリックして、ポップアップ アラート ボックスを閉じます。

ステップ 4 次のものを含む現在の AP 設定を表示するには、[実行（Go）] をクリックします。

a) AP 名
b) イーサネット MAC（Ethernet MAC）
c) 参照先
d) プライマリ コントローラ（Primary Controller）
e) セカンダリ コントローラ（Secondary Controller）

f) ターシャリ コントローラ（Tertiary Controller）

ステップ 5 アクセス ポイント設定をエクスポートするには、ファイル オプション（CSV、Excel、XML）を選択します。

ステップ 6 [ファイルのダウンロード（File Download）] ウィンドウで、[保存（Save）] をクリックしてファイルを保存します。

アクセス ポイント XOR アンテナの設定

Prime Infrastructure には、特定のアンテナの使用を有効または無効にする機能があります。デフォルトでは、すべてのアンテナが有効になっています。

[設定（Configuration）] > [ワイヤレステクノロジー（Wireless Technologies）] > [アクセスポイントの無線（Access Point Radios）] の順に選択し、[無線（Radio）] 列で [XOR（2.4 GHz）（XOR (2.4GHz)）] または [XOR（5 GHz）（XOR(5GHz)）] を選択すると、次のページが表示されます。

このページには、次のフィールドがあります。

（注） いずれかのフィールドを変更すると、無線が一時的に無効になり、一部のクライアントの接続が失われる場合があります。

一般

- [AP 名（AP Name）] : アクセス ポイントのオペレータ定義名。
- [AP ベース無線 MAC（AP Base Radio MAC）] : アクセス ポイントのベース無線の MAC アドレス。
- [スロット ID（Slot ID）] : スロット ID。
- [管理ステータス（Admin Status）] : アクセス ポイントの管理状態を有効するには、このボックスを選択します。
- [CDP状態（CDP State）] : CDP を有効にするには、**[CDP状態（CDP State）]** チェックボックスをオンにします。
- [コントローラ（Controller）] : コントローラの IP アドレス。詳細については、コントローラの IP アドレスをクリックします。
- [サイト設定 ID（Site Config ID）] : サイトの識別番号。
- [CleanAir 対応（CleanAir Capable）] : アクセス ポイントが CleanAir 対応かどうかが表示されます。
- [CleanAir] : ドロップダウンで、[両方無効（Both Disabled）]、[5 GHz 有効（5GHz Enabled）]、[2.4 GHz 有効（2.4 GHz Enabled）]、および [両方有効（Both Enabled）] から任意のオプションを選択します。

無線割り当て

- [割り当て方式（Assignment Method）]：割り当て方式は、[自動（Auto）]、[運用（Serving）]、または [モニタ（Monitor）] です。

（注） [帯域選択（Band Selection）]、[RF チャネル割り当て（RF Channel Assignment）]、および [送信電力レベル割り当て（Tx Power Level Assignment）] は、[運用（Serving）] 割り当て方式の場合にのみ表示されます。

- [帯域選択（Band Selection）]：[2.4 GHz] または [5 GHz] いずれかの無線を選択できます。

アンテナ

[無線割り当て（Radio Assignment）] の選択内容に応じて、次のパラメータが表示されます。

- [アンテナ タイプ（Antenna Type）]：アンテナ タイプ [外部（External）] または [内部（Internal）] を示します。
- [XOR A アンテナ（XOR A Antenna）]：（[自動（Auto）] 割り当て方式の場合にのみ表示されます）。ドロップダウンリストから [外部アンテナ（external antenna）] または [その他（Other）] を選択します。
- [XOR B アンテナ（XOR B Antenna）]：（[自動（Auto）] 割り当て方式の場合にのみ表示されます）。ドロップダウンリストから [外部アンテナ（external antenna）] または [その他（Other）] を選択します。
- [外部アンテナ（External Antenna）]：（[運用（Serving）] および [モニタ（Monitor）] 割り当て方式の場合にのみ表示されます）。ドロップダウン リストから [外部アンテナ（external antenna）] または [その他（Other）] を選択します。ドロップダウンの値は、2.4 GHz 無線と 5 GHz 無線で異なります。
- [アンテナゲイン（Antenna Gain）]：（[運用（Serving）] および [モニタ（Monitor）] 割り当て方式の場合に表示されます）。テキスト ボックスに望ましいアンテナ ゲインを入力します。カスタム アンテナ ゲインを設定するには、[外部アンテナ（External Antenna）] オプションで [その他（Others）] を選択します。

（注） 無線ネットワーク アダプタに接続される指向性アンテナのピーク ゲイン（dBi）、および全方向性アンテナの平均ゲイン（dBi）。ゲインは 0.5dBi の倍数で表します。整数値 4 は、4 X 0.5 = 2dBi のゲインであることを意味します。

RF チャネル割り当て

次の [802.11a RF チャネル割り当て（802.11a RF Channel Assignment）] パラメータは、無線割り当て方式として [運用（Serving）] を選択した場合にのみ表示されます。

- [現在のチャネル（Current Channel）]：アクセス ポイントのチャネル番号。

- [チャネル幅（Channel Width）]：2.4 GHz 無線の場合は 20 MHz の無線のみがサポートされます。5 GHZ 無線の場合は、[チャネル幅（Channel Width）] ドロップダウン リストから [20 MHz]、[40 MHz]、[80 MHz]、または [160 MHZ] を選択します。
- [割り当て方式（Assignment Method）]：次のいずれかを選択します。
  - [グローバル（Global）]：アクセスポイントのチャネルがコントローラによってグローバルに設定される場合は、この設定を使用します。
  - [カスタム（Custom）]：アクセスポイントのチャネルがローカルで設定されている場合は、この設定を使用します。[カスタム（Custom）] ドロップダウン リストからチャネルを選択します。ドロップダウンの値は 2.4 GHz 無線と 5 GHz 無線で異なります。

11n および 11ac のパラメータ

- [11n をサポート（11n Supported）]：802.11n 無線がサポートされているかどうかを示します。
- [11ac をサポート（11ac Supported）]：802.11ac 無線がサポートされいるかどうかを示します。

パフォーマンス プロファイル

[URL] をクリックして、このアクセスポイントのインターフェイスのパフォーマンスプロファイル パラメータを表示または編集します。

- [ClientLink]：インターフェイスごとにアクセス ポイントの無線のクライアント リンクを有効または無効にします。この機能は、従来の（直交周波数分割多重）OFDM レートのみでサポートされます。インターフェイスでは ClientLink がサポートされる必要があり、OFDM レートを有効にする必要があります。また、複数のアンテナを送信可能にして、3 つすべてのアンテナを受信可能にする必要があります。

（注） サポートされるクライアントの最大数は 15 です。アンテナ設定により操作が 1 本の送信アンテナに制限されている場合、あるいは OFDM レートが無効になっている場合、ClientLink は使用できません。

送信電力レベル割り当て

- [現在の送信電力レベル（Current Tx Power Level）]：現在の送信電力レベルを示します。
- [割り当て方式（Assignment Method）]：次のいずれかを選択します。
  - [グローバル（Global）]：電力レベルがコントローラによってグローバルに設定されている場合は、この設定を使用します。
  - [カスタム（Custom）]：アクセスポイントの電力レベルがローカルで設定されている場合は、この設定を使用します。ドロップダウン リストから電力レベルを選択します。

11n アンテナ選択

Prime Infrastructure には、特定のアンテナの使用を有効または無効にする機能があります。デフォルトでは、すべてのアンテナが有効になっています。

（注） 少なくとも 1 つの送信アンテナと 1 つの受信アンテナが有効である必要があります。すべての送信アンテナおよび受信アンテナを一度に無効にできません。

次のいずれかの [11n アンテナ選択（11n Antenna Selection）] パラメータを設定します。

- Antenna A （アンテナ A）
- Antenna B （アンテナ B）
- Antenna C （アンテナ C）
- Antenna D （アンテナ D）

[11n] パラメータ

次の [11n] フィールドが表示されます。

- [11n をサポート（11n Supported）]：802.11n の無線がサポートされているかどうかを示します。
- [クライアント リンク（Client Link）]：クライアント リンクを有効または無効にするには、このオプションを使用します。ドロップダウン リストから [有効（Enable）]、[無効（Disable）]、または [該当なし（Not Applicable）] を選択します。

AP オンボーディング プロファイルの設定

AP が ME コントローラに参加し、検出されると、Prime Infrastructure では、AP を自動的にプロビジョニングできます。AP オンボーディング機能は、このように検出した AP で AP 名および AP グループを自動的に設定します。このプロセスでは、Prime Infrastructure の AP 名および他のコンフィギュレーションパラメータを設定する必要性が削除されるため、クライアントとして機能します。Prime Infrastructure は AP オンボーディング プロファイルを使用して、PI の AP を事前に設定します。

AP オンボーディング サービス プロセス

Prime Infrastructure が新しい AP を検出した場合、または既存の AP との関連性を検出した場合は、この特定の AP のアクティブなオンボーディング プロファイルが存在するかどうかをチェックします。アクティブなプロファイルが検出されると、Prime Infrastructure は次の手順を実行します。

1. プロファイル変更を [処理中（in-progress）] とマークします。
2. プロファイルの AP 名を設定します。

3. オンボーディング プロファイルに記載されている AP テンプレートを展開します。
4. すべての AP テンプレートが展開されると、プロファイルは完了とマークされ、ステータスが成功または失敗に設定されます。

関連トピック

AP オンボーディング プロファイル グループの作成 （803 ページ）
AP オンボーディング プロファイルの編集 （804 ページ）
AP オンボーディング プロファイルの削除 （805 ページ）

AP オンボーディング プロファイル グループの作成

単一の AP オンボーディング プロファイルを作成するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ワイヤレステクノロジー（Wireless Technologies）] > [APオンボーディングプロファイル（AP Onboarding Profile）]** の順にクリックします。

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 次の必要な詳細情報を入力します。

- [プロファイルグループ（Profile Group）]（デフォルトでは割り当てなし）
- **[イーサネットMACアドレス/シリアル番号（Ethernet MAC Address/ Serial Number）]**
- [AP名（AP Name）]：AP が検出されたときに AP に対して設定する名前。
- [コントローラの選択（Controller Selection）]：AP がこのコントローラに参加する場合のみ、このプロファイルを適用します。このような制限をしない場合は、[任意（Any）] を選択します。
- [APテンプレート（AP Template）]：AP にプッシュする AP テンプレートの名前。AP テンプレートは 3 つまで選択できます。
- [プロファイルモード（Profile Mode）]（デフォルトで有効）

ステップ 4 [保存（Save）] をクリックします。

AP オンボーディング プロファイルの一括作成

AP オンボーディング プロファイルを一括アップロードの .csv ファイルで作成するには、次の手順に従います。

ステップ 1 **[設定（Configuration）] > [ワイヤレステクノロジー（Wireless Technologies）] > [APオンボーディングプロファイル（AP Onboarding Profile）]** の順にクリックします。

ステップ 2 **[新規プロファイル（New Profile）] > [一括追加（Bulk Add）]** の順にクリックします。

ステップ 3 [ファイルの選択（Choose File）] をクリックしてウィザードを開きます。必要な .csv ファイルまで移動して選択します。

[サンプルCSVのダウンロード（Download Sample CSV）] をクリックして、サンプル .csv ファイルをダウンロードします。

ステップ 4 既存のエントリを上書きするには、[既存のエントリを上書き（Override Existing Entries）] チェックボックスをオンにします。

ステップ 5 **[保存（Save）]** をクリックします。

AP オンボーディング プロファイルの編集

プロファイル モードを編集、複製、展開、または変更するには、次の手順に従います。

（注） プロファイルの状態が [進行中（in-progress）] である場合、そのプロファイルは編集または変更できません。

ステップ 1 **[設定（Configuration）] > [ワイヤレステクノロジー（Wireless Technologies）] > [APオンボーディングプロファイル（AP Onboarding Profile）]** の順にクリックします。

ステップ 2 関連するプロファイル グループをクリックします。

ステップ 3 編集するプロファイル（1 つまたは複数）を選択します。

ステップ 4 [プロファイルの編集（Edit Profile）] をクリックします。

複数のプロファイルを選択している場合、[AP名（AP Name）]および[プロファイルモード（Profile Mode）]は編集できません。

ステップ 5 必須フィールドを編集して [保存（Save）] をクリックします。

AP オンボーディング プロファイルの変更

プロファイル モードを編集、複製、展開、または変更するには、次の手順に従います。

ステップ 1 **[設定（Configuration）] > [ワイヤレステクノロジー（Wireless Technologies）] > [APオンボーディングプロファイル（AP Onboarding Profile）]** の順にクリックします。

ステップ 2 関連するプロファイル グループをクリックします。

ステップ 3 変更するプロファイル（1 つまたは複数）を選択します。

ステップ 4 次のタスクから選択します。

- [プロファイルの複製（Duplicate Profile）]：プロファイルを複製します。

  （注） 複数のプロファイルを一斉に複製することはできません。

- [プロファイルの削除（Delete Profiles）]：プロファイル（1 つまたは複数）を削除します。
- [プロファイルの編集（Edit Profiles）]：プロファイル（1 つまたは複数）を編集します。

- [プロファイルモード/状態の変更（Change Profile Mode/Status）]：プロファイル モードを [有効（Enable）]、[保留中（Pending）]、または [無効（Disable）] に変更します。

  （注） プロファイル モードを [完了（Completed）] に変更することと、状態が [進行中（in-progress）] であるプロファイルのプロファイル モードを変更することはできません。

- [展開（Deploy）]：プロファイルを展開します。

AP オンボーディング プロファイルの削除

既存の AP オンボーディング プロファイル グループを削除するには、次の手順に従います。

（注） プロファイルの状態が [進行中（in-progress）] である場合、そのプロファイルは削除できません。

手順の概要

1. **[設定（Configuration）] > [ワイヤレステクノロジー（Wireless Technologies）] > [APオンボーディングプロファイル（AP Onboarding Profile）]** の順にクリックします。
2. 削除するプロファイル グループを選択します。
3. [プロファイルグループの削除（Delete Profile Groups）] をクリックします。

手順の詳細

ステップ 1 **[設定（Configuration）] > [ワイヤレステクノロジー（Wireless Technologies）] > [APオンボーディングプロファイル（AP Onboarding Profile）]** の順にクリックします。

ステップ 2 削除するプロファイル グループを選択します。

ステップ 3 [プロファイルグループの削除（Delete Profile Groups）] をクリックします。

アクセス ポイントの検索

カスタム検索を作成して保存するには、ページの右上隅にある検索オプションを使用します。

- [新規検索（New Search）]：IP アドレス、名前、SSID、または MAC を入力して、[検索（Search）] をクリックします。
- [保存した検索（Saved Searches）]：[保存した検索（Saved Search）] をクリックして、カテゴリ、保存したカスタム検索を選択するか、ドロップダウン リストから他の検索基準を選択します。

- [詳細検索（Advanced Search）]：詳細検索では、さまざまなカテゴリとフィルタに基づいてデバイスを検索できます。

[実行（Go）] をクリックすると、アクセス ポイントの検索結果が表示されます（表 50 : アクセス ポイントの検索結果 （806 ページ） を参照）。

表 *50* : アクセス ポイントの検索結果

フィールド	オプション
[IPアドレス（IP Address）]	アクセス ポイントの IP アドレス。
[イーサネット MAC（Ethernet MAC）]	アクセス ポイントの MAC アドレス。
AP 名	アクセス ポイントに割り当てられた名前。詳細を表示するには、アクセスポイント名の項目をクリックします。
[無線（Radio）]	アクセス ポイントのプロトコルは、802.11a/n または 802.11b/g/n のどちらかです。
[マップ位置（Map Location）]	キャンパス、ビルディング、またはフロアの位置。
[コントローラ（Controller）]	コントローラの IP アドレス。
[AP タイプ（AP Type）]	アクセス ポイントの無線周波数の種類。
[動作ステータス（Operational Status）]	Cisco 無線の動作ステータスを表示します（[アップ（Up）] または [ダウン（Down）]）。
[アラーム ステータス（Alarm Status）]	アラームのカラー コードは、次のとおりです。 • 透明 = アラームなし • 赤 = クリティカル アラーム • オレンジ = メジャー アラーム • 黄 = マイナー アラーム
[監査ステータス（Audit Status）]	アクセス ポイントの監査ステータス。
シリアル番号（Serial Number）	アクセス ポイントのシリアル番号。
[AP モード（AP Mode）]	ローカル、FlexConnect、モニタ、不正検出、スニファ、ブリッジ、SE 接続などのアクセス ポイント モードの役割について説明します。

ワイヤレス設定グループ

ワイヤレス設定グループ ワークフローは、Cisco Prime Infrastructure で使用できる WLAN コントローラ設定グループ機能のワークフローを改良したものです。改良されたワイヤレス設定ワークフローで実現できることは次のとおりです。

- デバイス固有のテンプレートを選択する。
- 複数のデバイスに複数のテンプレートを展開する。
- PI から複数のワイヤレス テンプレートを監査する。

（注） CLIテンプレートおよびゲストユーザはワイヤレス設定グループから展開することはできません。

新しい設定グループの作成

ステップ 1 **[設定（Configuration）]** > **[ワイヤレステクノロジー（Wireless Technologies）]** > **[ワイヤレス設定グループ（Wireless Configuration Groups）]** の順に選択します。

ステップ 2 新しい設定グループを作成するには、[作成（Create）] をクリックします。
[設定グループ ワークフロー（Configuration Group Workflow）] ウィザードが表示されます。

ステップ 3 [一般設定（General Configuration）] タブで、設定グループ名を入力して [次へ（Next）] をクリックします。
[テンプレートの選択（Select Template）] タブが表示されます。

ステップ 4 [テンプレートの選択（Select Template）] タブで、[デバイス タイプ（Device Type）] として [CUWN] または [CUWN-IOS] と [UA] を選択します。

ステップ 5 **[テンプレート（Templates）] ツリー ビュー** > **[マイ テンプレート（My Templates）]** から [選択したテンプレート（Selected Template(s)）] グループ ボックスにテンプレートまたはグループをドラッグ アンド ドロップします。

[選択したテンプレート（Selected Template(s)）] グループ ボックスに、[テンプレート（Templates）] ツリー ビューから追加したテンプレートまたはグループがリストされます。

ステップ 6 設定グループを保存してワークフローを終了するには、[保存して終了（Save and Quit）] をクリックします。

ステップ 7 設定グループを保存して選択したテンプレートを展開するには、[次へ（Next）] をクリックします。
[デバイスの選択（Select Devices）] タブが表示されます。

ステップ 8 [デバイスの選択（Select Devices）] タブに、選択したデバイス タイプに基づいてコントローラがリストされます。

ステップ 9 [デバイス名（Device Name）] チェックボックスをオンにし、[展開（Deploy）] をクリックします。

展開に成功すると、[ワイヤレス設定グループ（Wireless Configuration Groups）] リスト ページが表示されます。

[ワイヤレス設定グループ（Wireless Configuration Groups）] ページには、展開されたデバイスに関する次の詳細が表示されます。

- グループ名（Group Name）
- 最後に展開されたデバイスの数（Last Deployed Devices Count）
- [テンプレート数（Templates Count）]
- [最後の展開ステータス（Last Deploy Status）]
  - 未開始（Not Initiated）：テンプレートがいずれかのデバイスに展開されているかどうかを示します。
  - 成功（Success）：該当する IP アドレスに関連する正常なテンプレートの数を示します。
  - 一部成功/失敗（Partial Success / Failure）：該当するコントローラへのテンプレートのプロビジョニングが失敗した数を示します。失敗の理由を確認するには、[一部成功/失敗（Partial Success/Failure）] リンクをクリックします。
- [最後の展開解除ステータス（Last Undeploy status）]
- [最後の監査ステータス（Last Audit Status）]
- [バックグラウンド監査（Background Audit）] : [オン（On）]/[オフ（Off）] を切り替えてバックグラウンド監査を有効にします。これをオンにすると、このグループに含まれるすべてのテンプレートが、ネットワークとコントローラの監査中にコントローラと対照して監査されます。
- [適用（Enforcement）] : [オン（On）]/[オフ（Off）] を切り替えて適用を有効にします。[適用（Enforcement）] をオンにすると、何らかの矛盾が見つかった場合は監査中にテンプレートが自動的に適用されます。
- [最終変更日（Last Modified On）]
- [最終適用日（Last Applied On）]

ワイヤレス設定グループでのテンプレートの追加または削除

[設定グループの監査（Config Groups Audit）] ページを使用すると、コントローラ設定がグループテンプレートに従っているかどうかを確認できます。監査中は、この画面を離れたり、Cisco Prime Infrastructure からログアウトしたりできます。プロセスは継続され、後でこのページに戻りレポートを表示できます。

（注） 監査中は、その他の設定グループの機能は実行しないでください。

ステップ 1 **[設定（Configuration）] > [ワイヤレステクノロジー（Wireless Technologies）] > [ワイヤレス設定グループ（Wireless Configuration Groups）]** の順に選択します。

（注） [コントローラリスト（Controller List）] ページで、[コントローラリスト（Controller List）] 列にある情報アイコンをクリックし、次にエクスポートアイコンをクリックすると、設定グループが設定されたコントローラの詳細を含む CSV ファイルをダウンロードできます。

ステップ 2 [グループ名（Group Name）] チェック ボックスをオンにし、[編集（Edit）] をクリックします。

ステップ 3 設定グループ ワークフロー ウィザードで、[テンプレートの選択（Select Templates）] タブをクリックします。

ステップ 4 [CUWN] または [CUWN-IOS] を選択します。

- [テンプレート（Templates）] ツリー ビューから [選択したテンプレート（Selected Template(s)）] グループ ボックスに、テンプレートまたはグループをドラッグ アンド ドロップします。
- [選択したテンプレート（Selected Template(s)）] グループ ボックスに、[テンプレート（Templates）] ツリー ビューから追加した、選択したテンプレートまたはグループがリストされます。

ステップ 5 [次へ（Next）] をクリックします。

ステップ 6 [デバイスリスト（Device List）] ページで、設定グループを設定するデバイスを選択します。

ステップ 7 [展開（Deploy）] をクリックして、選択したコントローラに設定グループを展開します。または、[保存して終了（Save and Quit）] をクリックして設定します。

[最後に展開された時刻（Last Deployed Time）] 列には、グループが展開されたコントローラにはタイムスタンプが表示され、グループが設定されただけのコントローラには [展開なし（Not Deployed）] と表示されます。

ワイヤレス設定グループの監査

[設定グループの監査（Config Groups Audit）] ページを使用すると、コントローラ設定がグループテンプレートに従っているかどうかを確認できます。監査中は、この画面を離れたり、Cisco Prime Infrastructure からログアウトしたりできます。プロセスは継続され、後でこのページに戻りレポートを表示できます。

（注） 監査中は、その他の設定グループの機能は実行しないでください。

ステップ 1 **[設定（Configuration）] > [ワイヤレステクノロジー（Wireless Technologies）] > [ワイヤレス設定グループ（Wireless Configuration Groups）]** の順に選択します。

ステップ 2 [グループ名（Group Name）] チェックボックスをオンにし、[監査（Audit）] をクリックします。[デバイスの選択（Select Devices）] ページが表示されます。

ステップ 3 [デバイス名（Device Name）] チェックボックスをオンにし、[監査（Audit）] をクリックします。
レポートが生成され、各コントローラの現在の設定が設定グループのテンプレートと比較されます。レポートには監査ステータス、同期テンプレートの数、非同期テンプレートの数が表示されます。

- [監査ステータス（Audit Status）]
  - [未開始（Not Initiated）]
  - [成功（Success）]：該当する IP アドレスに関連するテンプレートの数が同期しているかどうかを示します。
  - [非同期（Not In Sync）]：該当するコントローラへのテンプレートのプロビジョニングが失敗した数を示します。[同期していない（Not In Sync）] をクリックし、詳細を確認します。

メッシュ ネットワークにおけるリンクの表示

メッシュ リンクの詳細には、次のいくつかの方法でアクセスできます。

- Prime Infrastructure ホーム ページで [メッシュ（Mesh）] ダッシュボードをクリックします。
- **[モニタ（Monitor）] > [アクセスポイント（Access Points）]** の順に選択して、[メッシュリンク（Mesh Links）] タブをクリックしてから、[詳細（Details）] リンクをクリックします
- Google Earth から KML ファイルをインポートした後で、[APメッシュ（AP Mesh）] リンクをクリックします

ページの上部に、現在の統計、その後に特定の統計の図が表示されます。

- [SNR グラフ（SNR Graph）]：[SNR Up] および [SNR Down] グラフは 1 つのグラフに結合されています。各データ セットは、別の色で表されます。
- [リンク メトリック グラフ（Link Metrics Graph）]：[調整済みリンク メトリック（Adjusted Link Metric）] と [未調整のリンク メトリック（Unadjusted Link Metric）] は 1 つのグラフに結合されています。各データ セットは、別の色で表されます。
- [パケット エラー レート グラフ（Packet Error Rate Graph）]：パケット エラー レートをグラフで表示します。
- [リンク イベント（Link Events）]：リンクの最近 5 つのイベントが表示されます。
- [メッシュのワースト SNR リンク（Mesh Worst SNR Links）]：最低信号対雑音比（SNR）リンクが表示されます。
- [AP 稼働時間（AP Uptime）]：これらの統計は、アクセス ポイントが頻繁にリブートされるかどうかを判別するために役立ちます。
- [LWAPP 接続所要時間（LWAPP Join Taken Time）]：これらの統計は、アクセス ポイントの追加に要する時間を判別します。
- [ロケーション リンク（Location Links）]：Prime Infrastructure マップまたは Google Earth のロケーションに移動できます。

コントローラの不正 AP 分類ルールの定義

単一の WLC で、不正アクセス ポイントの現在の分類ルールを表示または編集できます。

不正アクセス ポイント分類ルールにアクセスするには、次の手順を実行します。

ステップ 1 **[設定（Configure）] > [コントローラ（Controllers）]** を選択します。

ステップ 2 [IP Address] 列で IP アドレスをクリックします。

ステップ 3 左側のサイドバーのメニューから、**[セキュリティ（Security）] > [不正 AP のルール（Rogue AP Rules）]** を選択します。[不正 AP ルール（Rogue AP Rules）] 画面に、不正アクセス ポイントの分類ルール、ルール タイプ（[悪意のある（Malicious）] または [危険性のない（Friendly）]）、およびルールの順序が表示されます。

ステップ 4 ルールの詳細を表示または編集するには、[不正 AP ルール（Rogue AP Rule）] を選択します。

コントローラの自動プロビジョニングを使用したWLCの追加と置換

Prime Infrastructure では、自動プロビジョニングのサポートによって WLAN の展開を簡素化します。自動プロビジョニングを使用すると、Prime Infrastructure で現在の Cisco ワイヤレス LAN コントローラ (WLC) を自動的に新規設定したり、交換したりすることができます。Prime Infrastructure 自動プロビジョニング機能を使用すると、大量のコントローラがあるお客様の展開を簡素化できます。

（注） コントローラの無線および b/g ネットワークは、Prime Infrastructure のスタートアップ コンフィギュレーション ファイルによって当初は無効になっています。必要に応じて、自動化テンプレートの 1 つとして含まれているテンプレートを使用し、それらの無線ネットワークを有効にできます。

コントローラ自動プロビジョニング リストの表示

[自動プロビジョニングフィルタ（Auto Provision Filters）] ページでは、自動プロビジョニング フィルタを作成して編集することで、Prime Infrastructure による自動プロビジョニングや自動モニタを許可するデバイスのリストを定義できます。

自動プロビジョニングの権限を有効にするには、管理者、ルート、またはスーパー ユーザ ステータスが必要です。ユーザの自動プロビジョニング権限を有効または無効にするには、Prime Infrastructure の **[管理（Administration）] > [ユーザロールおよびAAAユーザグループ（User Roles & AAA User Groups）] > [グループ名（group name）] > [許可されているタスクのリスト**

（**List of Tasks Permitted**）] で、許可されているタスクを編集します。各チェックボックスをオンまたはオフにして、これらの権限の有効と無効を切り替えます。

フィルタ パラメータは次のとおりです。

パラメータ	説明
Filter Name	フィルタの名前を識別します。
Filter Enable	フィルタが有効かどうかを示します。 有効にしたフィルタだけを自動プロビジョニング プロセスに追加できます。
モニタのみ（Monitor Only）	選択した場合、このフィルタで定義された Cisco WLC は Prime Infrastructure で管理されますが、自動プロビジョニング処理中に Cisco WLC が Prime Infrastructure と通信する場合、Prime Infrastructure で設定されることはありません。
Filter Mode	このフィルタの検索モード（[Host Name]、[MAC Address]、または [Serial Number]）を示します。
Config Group Name	設定グループの名前を示します。 自動プロビジョニング フィルタで使用されるすべての設定グループで、コントローラが定義されていてはなりません。

コントローラの自動プロビジョニング フィルタの作成

自動プロビジョニング フィルタ コンテンツを指定するには、アプリケーションに直接詳細を入力するか、CSV ファイルから詳細をインポートします。自動プロビジョニング機能は、5500 シリーズのコントローラと 5500 シリーズ以外のコントローラをサポートしています。5500 シリーズ以外のコントローラでは、AP マネージャ インターフェイスのコンフィギュレーション情報が定義されているのに対し、5500 シリーズのコントローラにはこの情報がありません。

自動プロビジョニング フィルタを追加するには：

ステップ 1 **[設定（Configuration）] > [ワイヤレス テクノロジー（Wireless Technologies）] > [WLAN コントローラの自動プロビジョニング（WLAN Controller Auto Provisioning）]** を選択します。

ステップ 2 [コマンドの選択（Select a Command）] ドロップダウン リストから [フィルタの追加（Add Filter）] を選択し、[実行（Go）] をクリックします。

ステップ 3 必須パラメータを入力します。

動的インターフェイス コンフィギュレーションとデバイス固有コンフィギュレーションの詳細は、CSV ファイルを入力するときのみ指定します。これら 2 つは、グラフィカル ユーザ インターフェイスでは設定できません。

ステップ 4 [保存（Save）] をクリックします。

デフォルトのユーザ名とパスワードを変更するには、ステップ 5 ～ 8 の説明に従って、管理ユーザを削除してから再作成する必要があります。

ステップ 5 デフォルトのユーザ名とパスワードを変更するには、ローカル管理ユーザ テンプレートを使用して、コントローラに新規の読み取り/書き込みユーザを作成する必要があります。ステップ 6 に示すように、新しいユーザを作成し、デフォルトの管理ユーザを削除できるようにする必要があります。

ステップ 6 **[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ネットワーク デバイス（Network Devices）]** を選択し、[設定（Configuration）] タブをクリックした後、**[管理（Management）] > [ローカル管理ユーザ（Local Management User）]** を選択して管理ユーザを選択します。その後、[コマンドの選択（Select a command）] ドロップダウン リストから [ローカル管理ユーザの削除（Delete Local Management User）] を選択して [実行（Go）] をクリックします。

ステップ 7 ローカル管理ユーザ テンプレートを使用して、コントローラに新しい管理ユーザを作成します。

ステップ 8 ステップ 5 で作成したユーザを削除します。

コントローラの自動プロビジョニングに使用されるプライマリキーの検索順序の制御

[プライマリ検索キー設定（Primary Search Key Setting）] を使用して、一致条件の検索順序を設定します。

ステップ 1 **[設定（Configuration）] > [プラグ アンド プレイ（Plug and Play）] > [コントローラ自動プロビジョニング（Controller Auto Provisioning）]** を選択し、左側のサイドバーのメニューから [設定（Setting）] を選択します。

ステップ 2 該当する検索キーをクリックして強調表示し、[Move Up] または [Move Down] ボタンを使用して、検索キーの優先順位を変更します。

ステップ 3 [Save] をクリックして、変更を確定します。

AP オンボーディング プロファイルの設定

AP が ME コントローラに参加し、検出されると、Prime Infrastructure では、AP を自動的にプロビジョニングできます。AP オンボーディング機能は、このように検出した AP で AP 名および AP グループを自動的に設定します。このプロセスでは、Prime Infrastructure の AP 名および他のコンフィギュレーションパラメータを設定する必要性が削除されるため、クライアントとして機能します。Prime Infrastructure は AP オンボーディング プロファイルを使用して、PI の AP を事前に設定します。

AP オンボーディング サービス プロセス

Prime Infrastructure が新しい AP を検出した場合、または既存の AP との関連性を検出した場合は、この特定の AP のアクティブなオンボーディング プロファイルが存在するかどうかをチェックします。アクティブなプロファイルが検出されると、Prime Infrastructure は次の手順を実行します。

1. プロファイル変更を [処理中（in-progress）] とマークします。
2. プロファイルの AP 名を設定します。
3. オンボーディング プロファイルに記載されている AP テンプレートを展開します。
4. すべての AP テンプレートが展開されると、プロファイルは完了とマークされ、ステータスが成功または失敗に設定されます。

関連トピック

AP オンボーディング プロファイル グループの作成 （803 ページ）
AP オンボーディング プロファイルの編集 （804 ページ）
AP オンボーディング プロファイルの削除 （805 ページ）

AP オンボーディング プロファイル グループの作成

単一の AP オンボーディング プロファイルを作成するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ワイヤレステクノロジー（Wireless Technologies）] > [APオンボーディングプロファイル（AP Onboarding Profile）]** の順にクリックします。

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 次の必要な詳細情報を入力します。

- [プロファイルグループ（Profile Group）]（デフォルトでは割り当てなし）
- **[イーサネットMACアドレス/シリアル番号（Ethernet MAC Address/ Serial Number）]**
- [AP名（AP Name）]：AP が検出されたときに AP に対して設定する名前。
- [コントローラの選択（Controller Selection）]：AP がこのコントローラに参加する場合のみ、このプロファイルを適用します。このような制限をしない場合は、[任意（Any）] を選択します。
- [APテンプレート（AP Template）]：AP にプッシュする AP テンプレートの名前。AP テンプレートは 3 つまで選択できます。
- [プロファイルモード（Profile Mode）]（デフォルトで有効）

ステップ 4 [保存（Save）] をクリックします。

AP オンボーディング プロファイルの一括作成

AP オンボーディング プロファイルを一括アップロードの .csv ファイルで作成するには、次の手順に従います。

ステップ 1 **[設定（Configuration）] > [ワイヤレステクノロジー（Wireless Technologies）] > [APオンボーディングプロファイル（AP Onboarding Profile）]** の順にクリックします。

ステップ 2 **[新規プロファイル（New Profile）] > [一括追加（Bulk Add）]** の順にクリックします。

ステップ 3 [ファイルの選択（Choose File）] をクリックしてウィザードを開きます。必要な .csv ファイルまで移動して選択します。

[サンプルCSVのダウンロード（Download Sample CSV）] をクリックして、サンプル .csv ファイルをダウンロードします。

ステップ 4 既存のエントリを上書きするには、[既存のエントリを上書き（Override Existing Entries）] チェックボックスをオンにします。

ステップ 5 **[保存（Save）]** をクリックします。

AP オンボーディング プロファイルの編集

プロファイル モードを編集、複製、展開、または変更するには、次の手順に従います。

（注） プロファイルの状態が [進行中（in-progress）] である場合、そのプロファイルは編集または変更できません。

ステップ 1 **[設定（Configuration）] > [ワイヤレステクノロジー（Wireless Technologies）] > [APオンボーディングプロファイル（AP Onboarding Profile）]** の順にクリックします。

ステップ 2 関連するプロファイル グループをクリックします。

ステップ 3 編集するプロファイル（1 つまたは複数）を選択します。

ステップ 4 [プロファイルの編集（Edit Profile）] をクリックします。

複数のプロファイルを選択している場合、[AP名（AP Name）]および[プロファイルモード（Profile Mode）] は編集できません。

ステップ 5 必須フィールドを編集して [保存（Save）] をクリックします。

AP オンボーディング プロファイルの変更

プロファイル モードを編集、複製、展開、または変更するには、次の手順に従います。

ステップ 1 **[設定（Configuration）] > [ワイヤレステクノロジー（Wireless Technologies）] > [APオンボーディングプロファイル（AP Onboarding Profile）]** の順にクリックします。

ステップ 2 関連するプロファイル グループをクリックします。

ステップ 3 変更するプロファイル（1 つまたは複数）を選択します。

ステップ 4 次のタスクから選択します。

- [プロファイルの複製（Duplicate Profile）]：プロファイルを複製します。

  （注） 複数のプロファイルを一斉に複製することはできません。

- [プロファイルの削除（Delete Profiles）]：プロファイル（1 つまたは複数）を削除します。
- [プロファイルの編集（Edit Profiles）]：プロファイル（1 つまたは複数）を編集します。
- [プロファイルモード/状態の変更（Change Profile Mode/Status）]：プロファイル モードを [有効（Enable）]、[保留中（Pending）]、または [無効（Disable）] に変更します。

  （注） プロファイルモードを [完了（Completed）] に変更することと、状態が [進行中（in-progress）] であるプロファイルのプロファイル モードを変更することはできません。

- [展開（Deploy）]：プロファイルを展開します。

AP オンボーディング プロファイル グループの削除

既存の AP オンボーディング プロファイル グループを削除するには、次の手順に従います。

（注） プロファイルの状態が [進行中（in-progress）] である場合、そのプロファイルは削除できません。

ステップ 1 **[設定（Configuration）] > [ワイヤレステクノロジー（Wireless Technologies）] > [APオンボーディングプロファイル（AP Onboarding Profile）]** の順にクリックします。

ステップ 2 削除するプロファイル グループを選択します。

ステップ 3 [プロファイルグループの削除（Delete Profile Groups）] をクリックします。

9800 シリーズ構成モデルに関する情報

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ は、さまざまなタグ（rf タグ、ポリシー タグ、サイトタグ）を使用して、ワイヤレス コントローラの設定を簡素化します。アクセス ポイントでは、タグ内に含まれているプロファイルから設定が導出されます。

プロファイルは、特定のターゲットに適用される機能固有の属性とパラメータの集まりです。設定のターゲットとなるのは、AP、無線、および WLAN です。Rf タグには無線プロファイルが、ポリシータグには flex-profile と ap-join-profile が、ワイヤレスタグには WLAN プロファイルとポリシー プロファイルが、それぞれ含まれています。

新しい設定モデル（flexconnect モード）は、たとえば小売店舗やキャンパスなど、WLAN が同じである地理的に分散したサイトを中央のコントローラで管理するのに役に立ちます。ローカルの展開またはトポロジに基づいてネットワークと無線のプロファイルに多少の変更が生じるだけです。

表 *51 : Catalyst 9800* シリーズ設定のワークフロー

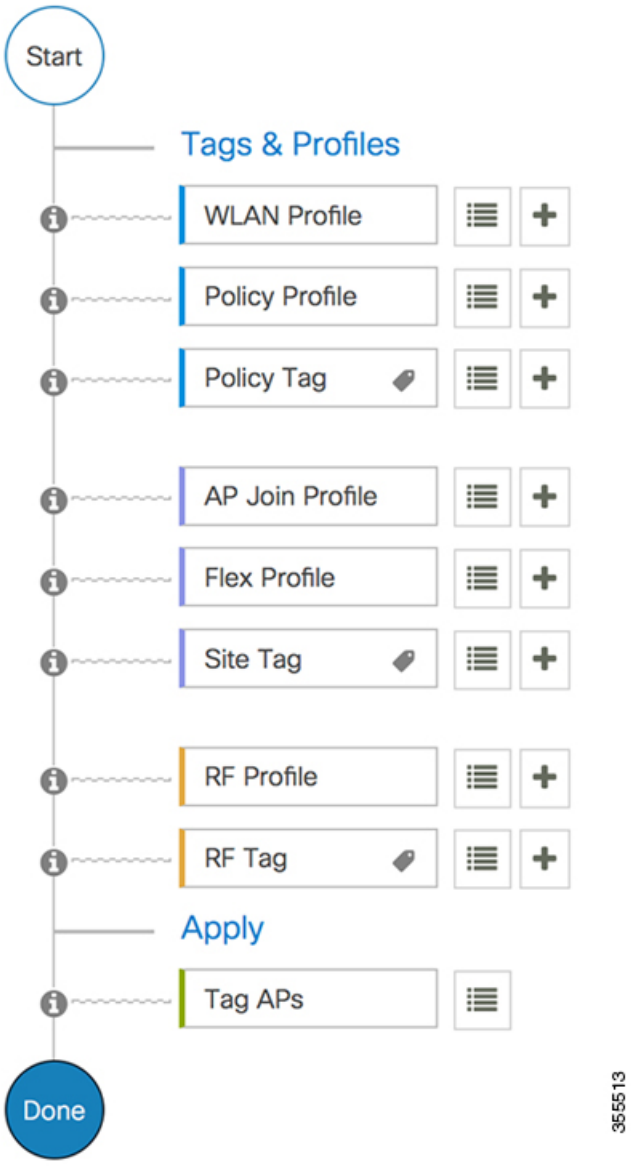
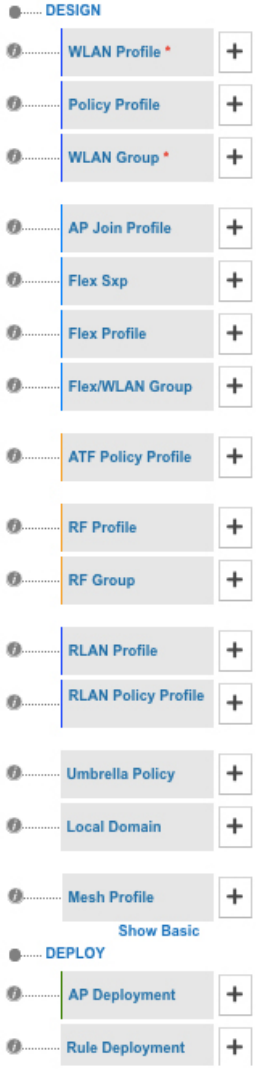
IOS XE Polaris	Prime Infrastructure
	

表 *52 : IOS XE Polaris* と *Prime Infrastructure* 間の *UI* 構造のマッピング

IOS-XE Polaris	Prime Infrastructure
ポリシー タグ	• **WLAN グループ** • **FLEX WLAN グループ**(Prime Infrastructure のみ) Flex プロファイルと WLAN プロファイルのマッピングを保存します。これは、flex ベースの展開で役立ちます。
RF タグ	**RF プロファイル**
サイト タグ	**AP 展開**と**AP 参加プロファイル** AP 展開名は、次を使用してデバイスのサイト タグを作成するために使用されます。 • Flex ベース展開の AP 参加プロファイルと Flex WLAN グループ • 非 Flex ベース展開の AP 参加プロファイルと WLAN グループ

ポリシー タグ

ポリシー タグは、WLAN プロファイルからポリシー プロファイルへのマッピングを構成します。WLAN プロファイルは、WLAN の無線特性を定義します。ポリシー プロファイルは、クライアントのネットワーク ポリシーとスイッチング ポリシーを定義します（AP ポリシーも構成する Quality of Service（QoS）は除きます）。

ポリシー タグには WLAN ポリシー プロファイルのマップが含まれています。そのようなエントリはポリシー タグごとに 16 個あります。マップ エントリの変更は、WLAN プロファイルとポリシー プロファイルのステータスに基づいて影響を受けます。たとえば、マップ（WLAN1 および Policy1）がポリシー タグに追加された場合、WLAN プロファイルとポリシー プロファイルの両方が有効になっていると、その定義がポリシー タグを使用して AP にプッシュされます。ただし、これらのいずれかが無効状態になっている場合には、定義は AP にプッシュされません。同様に、WLAN プロファイルがすでに AP によってブロードキャストされている場合は、ポリシー タグでコマンドの no 形式を使用して削除できます。

サイト タグ

サイト タグはサイトのプロパティを定義するもので、flex プロファイルと AP join プロファイルが含まれています。対応する flex またはリモート サイトに固有の属性は、flex プロファイルの一部となります。flex プロファイルとは別に、サイト タグは物理サイトに固有の属性も構成します（そのため、再利用可能なエンティティであるプロファイルの一部にすることはできま

せん）。たとえば、効率的なアップグレードのためのマスター AP のリストは、flex プロファイルの一部ではなくサイト タグの一部になります。

flexプロファイル名またはAPプロファイル名がサイトタグで変更された場合、APは、Datagram Transport Layer Security（DTLS）セッションを切断することによってコントローラへの再参加を強制されます。サイト タグが作成されると、AP プロファイルと flex プロファイルはデフォルト値（default-ap-profile と default-flex-profile）に設定されます。

RF タグ

RF タグには IEEE 802.11a および IEEE 802.11b の RF プロファイルが含まれています。デフォルトの RF タグにはグローバル設定が含まれています。どちらのプロファイルにも、それぞれの無線についてグローバル RF プロファイルの同じデフォルト値が含まれています。

プロファイル

プロファイルは、特定のターゲットに適用される機能固有の属性とパラメータの集まりです。設定のターゲットとなるのは、AP、無線、および WLAN です。プロファイルは、タグ全体で使用できる再利用可能なエンティティです。プロファイル（タグで使用されます）は、AP またはそれに関連付けられているクライアントのプロパティを定義します。

WLAN プロファイル

WLAN プロファイルは、同じまたは異なるサービスセット識別子（SSID）で設定されます。SSIDは、コントローラがアクセスするための特定の無線ネットワークを識別します。同じSSIDで WLAN を作成すると、同じ無線 LAN 内で異なるレイヤ 2 セキュリティ ポリシーを割り当てることができます。

同じ SSID を持つ WLAN を区別するには、各 WLAN に対して一意のプロファイル名を作成します。同じSSIDを持つWLANには、ビーコン応答とプローブ応答でアドバタイズされる情報に基づいてクライアントがWLANを選択できるように、一意のレイヤ2セキュリティポリシーが設定されている必要があります。スイッチング ポリシーとネットワーク ポリシーは WLAN 定義の一部ではありません。

ポリシー プロファイル

ポリシー プロファイルは、広義にはネットワーク ポリシーとスイッチング ポリシーで構成されます。ポリシー プロファイルはタグ全体にわたって再利用可能なエンティティです。AP またはコントローラに適用されるクライアントのポリシーとなっているものはすべて、ポリシープロファイルに移動されます。たとえば、VLAN、ACL、QoS、セッション タイムアウト、アイドル タイムアウト、AVC プロファイル、bonjour プロファイル、ローカル プロファイリング、デバイス分類、BSSIDQoSなどが該当します。ただし、WLANのワイヤレス関連のセキュリティ属性と機能はすべて、WLAN プロファイルの配下にグループ化されます。

flex プロファイル

flex プロファイルには、flex グループの一部となっている属性が含まれています。ただし、ポリシー属性はポリシープロファイルとともにグループ化されます。flex プロファイルにはリモート サイト固有のパラメータも含まれています。たとえば、EAP プロファイル（AP がロー

カルRADIUSサーバ情報の認証サーバとして機能する場合に使用可能）、VLANとACLのマッピング、VLAN名とIDのマッピングなどです。

AP join プロファイル

デフォルトの AP join プロファイルの値には、グローバル AP パラメータと AP グループ パラメータが設定されます。AP join プロファイルには、CAPWAP、IPv4 および IPv6、UDP Lite、ハイ アベイラビリティ、再送信設定パラメータ、グローバル AP フェールオーバー、HyperLocation 設定パラメータ、Telnet および SSH、11u パラメータなどのパラメータが含まれています。

RF プロファイル

RF プロファイルには、AP の共通の無線設定が含まれています。RF プロファイルは、AP グループに属するすべての AP に適用され、そのグループ内のすべての AP に同じプロファイルが設定されます。

AP の静的な関連付け

AP を静的に設定できるのは、ポリシータグ、サイト タグ、および RF タグを使用した場合のみです。AP はイーサネット MAC アドレスによって識別され、AP およびタグへの関連付けは設定としてコントローラに保存されます。

AP タグの変更

AP タグを変更すると、DTLS 接続がリセットされ、AP が強制的にコントローラに再参加します。設定でタグが1つだけ指定されている場合は、他のタイプにデフォルト タグが使用されます。たとえば、ポリシー タグのみが指定されている場合は、サイト タグと RF タグに対して default-site-tag と default-rf-tag が使用されます。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの Cisco Umbrella ポリシーのローカル ドメインの設定

OpenDNSは、DNSトラフィックの分割をサポートしているため、管理者は目的のDNSに希望のDNSサーバ(たとえば、企業内にあるDNSサーバ)に直接送信し、OpenDNSクラウドをバイパスすることができます。

ステップ 1 **[設定（Configuration）]** > **[ワイヤレス テクノロジー（Wireless Technologies）]** > **[Cisco Catalyst 9800 設定（Cisco Catalyst 9800 configuration）]** をクリックします。

ステップ 2 **[アドバンストの表示（Show Advanced）]** をクリックし、**[ローカル ドメイン（Local Domain）]** をクリックして使用可能なプロファイルを表示し、編集するプロファイルをクリックします。または、+ アイコンをクリックして新しいを作成します。

ステップ 3 **[Regex パターン（Regex Pattern）]** 領域で、+ アイコンをクリックして新しいローカル ドメインを作成します。

ステップ 4 URL を入力して**保存**します。

このローカル ドメインを Umbrella ポリシーに追加する必要があります。

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

Cisco Umbrella は、クラウドで提供されているネットワーク セキュリティ サービスです。マルウェアからデバイスを保護し、リアルタイムで侵害を阻止します。

ステップ 1 **[設定（Configuration）] > [ワイヤレス テクノロジー（Wireless Technologies）] > [Cisco Catalyst 9800 設定（Cisco Catalyst 9800 configuration）]** をクリックします。

ステップ 2 **[アドバンストの表示（Show Advanced）]** をクリックし、**[Umbrella ポリシー（Umbrella Policy）]** をクリックして使用可能なプロファイルを表示し、編集するプロファイルをクリックします。または、+ アイコンをクリックして新しいを作成します。

ステップ 3 必要な詳細を入力または編集し、**[ローカル ドメイン（Local domain）]** ドロップダウン メニューからローカル ドメインを選択します。

OpenDNS ダッシュボードからデバイスのトークンを取得し、WLC に適用されていることを確認する必要があります。

（注） Prime Infrastructure 3.5 は**グローバル**ポリシーのみをサポートします。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラに Flex Sxp プロファイルを設定します

ステップ 1 **[設定（Configuration）] > [ワイヤレス テクノロジー（Wireless Technologies）] > [Cisco Catalyst 9800 設定（Cisco Catalyst 9800 configuration）]** をクリックします。

ステップ 2 **[アドバンストの表示（Show Advanced）]** をクリックし、**[Flex Sxp]** をクリックして使用可能なプロファイルを表示し、編集するプロファイルをクリックします。または、+ アイコンをクリックして新しいを作成します。

ステップ 3 必要な詳細を入力または編集して**保存**します。

この Flex Sxp プロファイルを Flex プロファイルにマッピングする必要があります。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラに Flex プロファイルを設定します

ステップ 1 **[設定（Configuration）]** > **[ワイヤレス テクノロジー（Wireless Technologies）]** > **[Cisco Catalyst 9800 設定（Cisco Catalyst 9800 configuration）]** をクリックします。

ステップ 2 **[アドバンストの表示（Show Advanced）]** をクリックし、**[Flex プロファイル（Flex Profile）]** をクリックして使用可能なプロファイルを表示し、編集するプロファイルをクリックします。または、+ アイコンをクリックして新しく作成します。

ステップ 3 必要な詳細を入力または編集します。

ステップ 4 Flex Sxp プロファイルをマッピングまたは変更するには、**[アドバンスト（Advanced）]** > **全般（General）]** に移動し、**[Flex Sxp プロファイル（Flex Sxp Profile）]** ドロップダウン メニューからプロファイルを選択します。

ステップ 5 **[保存（Save）]** をクリックします。

Catalyst 9800 シリーズ ワイヤレス コントローラの Airtime Fairness の設定

Catalyst 9800 シリーズ ワイヤレス コントローラの Airtime Fairness ポリシーの作成

ステップ 1 **[設定（Configuration）]** > **[ワイヤレス テクノロジー（Wireless Technologies）]** > **[Cisco Catalyst 9800 設定（Cisco Catalyst 9800 configuration）]** をクリックします。

ステップ 2 **[アドバンストの表示（Show Advanced）]** をクリックし、**[ATF ポリシー プロファイル（ATF Policy Profile）]** をクリックして使用可能なポリシーを表示するか、+ アイコンをクリックして新しいを作成します。既存の ATF ポリシーをクリックして編集します。

ステップ 3 必要な詳細を入力または編集します。

ステップ 4 **[Save（保存）]** をクリックします。

（注） このポリシーをポリシー プロファイルにマッピングする必要があります。

ポリシー プロファイルへの Airtime Fairness ポリシーの追加

ステップ 1 **[設定（Configuration）] > [ワイヤレス テクノロジー（Wireless Technologies）] > [Cisco Catalyst 9800 設定（Cisco Catalyst 9800 configuration）]** をクリックします。

ステップ 2 **[アドバンストの表示（Show Advanced）]** をクリックし、**[ポリシー プロファイル（Policy Profile）]** をクリックして使用可能なポリシーを表示するか、+ アイコンをクリックして新しいを作成します。クリックして、既存のポリシーを編集します。

ステップ 3 **[アクセス ポリシー（Access Policies））]** をクリックします。

ステップ 4 **[電波時間正常性ポリシー（Air Time Fairness Policies）]** で、2.4 GHz および 5 GHz 帯域のポリシー プロファイルを選択します。

両方の帯域に対して個別のポリシーまたは同じポリシーを選択できます。

ステップ 5 **[保存（Save）]** をクリックします。

RF プロファイルで ATF ポリシーを有効にする

ステップ 1 **[設定（Configuration）] > [ワイヤレス テクノロジー（Wireless Technologies）] > [Cisco Catalyst 9800 設定（Cisco Catalyst 9800 configuration）]** をクリックします。

ステップ 2 **[アドバンストの表示（Show Advanced）]** をクリックし、**[RF プロファイル（RF Profile）]** をクリックして使用可能なポリシーを表示するか、+ アイコンをクリックして新しく作成します。既存のプロファイルをクリックして、編集します。

ステップ 3 **[アドバンスト（Advanced）] > [Air Time Fairness]** をクリックします。

ステップ 4 必要に応じて、動作モードを選択します。

- **無効:** WLC で ATF を無効にします。
- **適用対象:**WLC に ATF ポリシーを適用します。
- **モニタ:** ネットワークの通信時間の使用状況を監視する

（注） メッシュ AP の場合、**[通信時間割り当ての上書き（verride Airtime Allocation）]** を有効にすることによって、WLANの重量設定を上書きするように択できます。上書きを有効にする場合は、このようなシナリオの重量を入力できます。

ステップ 5 **[保存（Save）]** をクリックします。

Catalyst 9800 シリーズ ワイヤレス コントローラのリモート LAN（RLAN）の設定

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

Prime Infrastructure のリモート LAN (RLAN) 機能は、有線クライアントがワイヤレス クライアントとしてネットワークに参加するためのサポートを提供します。WLC は有線クライアントを認証します。有線クライアントが正常に参加すると、LAN ポートは設定に応じて、中央スイッチング モードまたはローカル スイッチング モードでトラフィックを切り替えることができます。

ステップ 1 **[設定（Configuration）] > [ワイヤレス テクノロジー（Wireless Technologies）] > [Cisco Catalyst 9800 設定（Cisco Catalyst 9800 configuration）]** をクリックします。

ステップ 2 **[アドバンストの表示（Show Advanced）]** をクリックし、**[RLAN プロファイル（RLAN Profile）]** をクリックして使用可能なポリシーを表示するか、+アイコンをクリックして新しいを作成します。クリックして、既存のポリシーを編集します。

ステップ 3 必要な詳細を入力または編集して **[保存（Save）]** をクリックします。

（注） このプロファイルを WLAN グループにマッピングする必要があります。

Catalyst 9800 シリーズ ワイヤレス コントローラの RLAN ポリシー プロファイルの作成

ステップ 1 **[設定（Configuration）] > [ワイヤレス テクノロジー（Wireless Technologies）] > [Cisco Catalyst 9800 設定（Cisco Catalyst 9800 configuration）]** をクリックします。

ステップ 2 **[アドバンストの表示（Show Advanced）]** をクリックし、**[RLAN ポリシー プロファイル（RLAN Policy Profile）]** をクリックして使用可能なポリシーを表示するか、+ アイコンをクリックして新しいを作成します。クリックして、既存のポリシーを編集します。

ステップ 3 必要な詳細を入力または編集して **[保存（Save）]** をクリックします。

アクセス ポリシー、QoS および AVC、および高度なパラメータを設定することもできます。

（注） このプロファイルを WLAN グループにマッピングする必要があります。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラに WLAN グループを設定します

ステップ 1 **[設定（Configuration）] > [ワイヤレス テクノロジー（Wireless Technologies）] > [Cisco Catalyst 9800 設定（Cisco Catalyst 9800 configuration）]** をクリックします。

ステップ 2 **[WLAN グループ（WLAN Group）]** をクリックして、使用可能なグループを表示し、編集するグループをクリックします。または、+ アイコンをクリックして新しいを作成します。

ステップ 3 **[WLAN マッピング（WLAN Mapping）]** タブで、それらをマッピングする WLAN プロファイルとポリシープロファイルを選択します。

ステップ 4 **[ポリシーにマップ（Map To Policy）]** をクリックします。

ステップ 5 **[RLAN マッピング（RLAN Mapping）]** タブで、プロファイルをアクティブにするポートを選択します。

（注） これらのポートが AP で有効になっていることを確認します。

軽量アクセスポイント > AP パラメータ > AP LAN ポート設定。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ上でルールを展開する

ステップ 1 **[設定（Configuration）] > [ワイヤレス テクノロジー（Wireless Technologies）] > [Cisco Catalyst 9800 設定（Cisco Catalyst 9800 configuration）]** をクリックします。

ステップ 2 **[ルール展開（Rule Deployment）]** をクリックし、使用可能なポリシーを表示するか、+ アイコンをクリックして新しく作成します。既存のルールをクリックして、編集します。

ステップ 3 必要な詳細を次のフィールドに入力します。

- **ルール名**: 展開ルールの名前を入力します。
- **AP 名に含む**: このルールが展開されている AP を選択する基準となる正規表現 (regex) を入力します。
- **展開モード**: 展開モード (flex ベースまたは非 flex ベース) を選択します。

ステップ 4 **Flex プロファイル**、**WLAN グループ**、**AP 参加プロファイル**、および **RF グループ**をそれぞれのドロップダウン メニューから選択します。

ステップ 5 **[Save（保存）]** をクリックします。

ステップ 6 **[ルールの展開（Rule Deployment）]**を再度クリックすると、使用可能なルールのリストが表示されます。

ステップ 7 展開するルールを選択し、**[展開 (Deploy)]** をクリックします。

ステップ 8 使用可能な展開オプションから選択し、**[展開 (Deploy)]** をクリックします。

Catalyst 9800 シリーズ ワイヤレス コントローラに展開されているルールを表示するには、**[設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）] > デバイス グループ（Device Groups）] > [デバイス タイプ（Device Type）] > [クラウドの Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ（Cisco Catalyst 9800 Series Wireless Controller for Cloud）] > .** Catalyst 9800 シリーズ デバイスをクリックし、**[設定（Configuration）] > [システム（System）] > [ルール展開（Rule Deployment）]** をクリックします。

Cisco AireOS コントローラ設定を Cisco Catalyst 9800 シリーズ コントローラに変換する

AireOS Config Translator を使用すると、レガシー Cisco WLC から Cisco Catalyst 9800 シリーズ ワイヤレス コントローラへのシームレスな移行が可能になります。

（注）
- この機能は、AireOS バージョン8.8 以降を実行している Cisco WLCs で動作します。
- WLC の設定が 5000CLI よりも大きい場合は、変換プロセスに時間がかかることがあります。
- AireOS 設定変換ツールを使用して AireOS 設定を変換する際に、Catalyst 9800 コントローラにすでに存在するものと同じ ID を持つ WLAN がある場合、それらは作成されません。

始める前に

次の基準が満たされていることを確認してください。

- レガシー (AireOS) WLC と Catalyst 9800 シリーズコントローラの両方が、すでにプライムインフラストラクチャで管理されている必要があります。
- 有効な SNMP および CLI クレデンシャルを使用して、両方のデバイス (AireOS および Catalyst 9800 シリーズ) をプライムインフラストラクチャに追加する必要があります。

ステップ 1 **[設定（Configuration）] > [ワイヤレス テクノロジー（Wireless Technologies）] > [AireOS Config Translator（AireOS Config Translator）]** をクリックします。

ステップ 2 **[ソースの選択（Choose source）]** ページで、**[ソース AireOS デバイスの選択（Select a Source Aireos Device）]** リストから AireOS デバイスを選択します。

ステップ 3 **[Target 9800 デバイスの選択（Select a Target 9800 Device）]** リストから適切な Catalyst 9800 シリーズ コントローラを選択します。

ステップ 4 **[設定の取得（Fetch Config）]** をクリックします。
これにより、送信元 WLC から実行設定が取得されます。

ステップ 5 **[設定の確認と更新（Verify And Update Config）]** ページで **[移行（Translate）]** をクリックします。
これにより、取得された AireOS 設定が Catalyst 9800 シリーズに変換されます。変換された設定は次のように分類されます。

1. **サポート済み** – 正常に変換されている CLI
2. **サポートされていない**: サポートされていないまたは変換されなかった CLI
3. **該当なし**: 変換が不要な CLI

ステップ 6 **サポートされている**設定 (強調表示されている) で、ホスト名、パスワード、および事前共有キーを変更します。

ステップ 7 **[承認して展開（Accept to deploy）]** チェックボックスをオンにします。

ステップ 8 [Deploy] をクリックします。

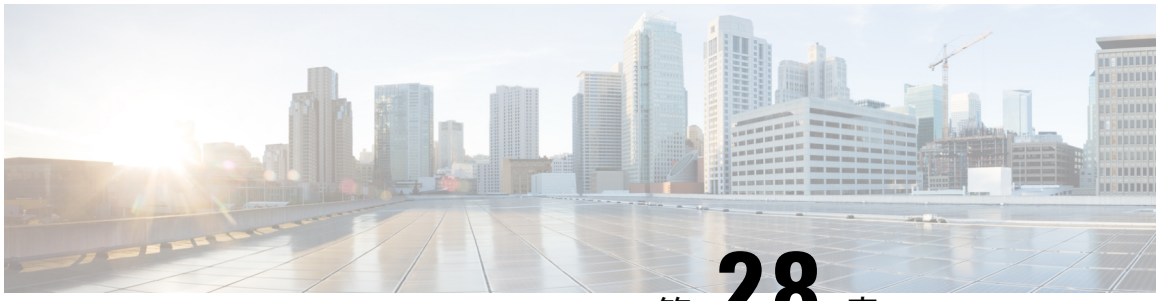
ステップ 9 移行する AP を選択し、**[移行 (Migrate)]** をクリックします。

結果：

- プライマリ コントローラの名前と IP アドレスが設定されます。
- 同期は、Prime Infrastructure で自動的にトリガーされます。

関連トピック

Prime Infrastructure へのデバイスの追加 （37 ページ）



第 28 章

ワイヤレス/データセンター設定タスクのスケジュール設定

• スケジュール設定変更の表示 （829 ページ）

スケジュール設定変更の表示

[スケジュール済み設定タスク（Scheduled Configuration Tasks）] ページでは、スケジュール済みのテンプレート、設定タスク、ソフトウェア ダウンロード タスクに移動し、それらのタスクのフィルタ ビューを使用できます。このページには、タスクに関するサマリー情報が表示されます。情報には、テンプレート名、最後にタスクが実行された時間、次回のタスク実行スケジュール、前回の実行結果を表示するリンクなどが含まれています。また、テンプレートの編集、スケジュールの変更、スケジュール済みタスクの有効化、無効化、削除を行うこともできます。

設定テンプレート、設定グループ、またはソフトウェア ダウンロード タスクを作成してスケジュールを設定すると、それらのスケジュール設定したタスクやテンプレートが [Scheduled Configuration Tasks] ページに一覧表示されます。

このページでは、新たにタスクやテンプレートを作成してスケジュールを設定できません。すでに作成されているスケジュール済みタスクまたはテンプレートの編集のみを行うことができます。

次のスケジュール済みタスクを変更、有効化、無効化、または削除できます。

- AP テンプレート
- 設定グループ
- WLAN の設定
- ソフトウェアのダウンロード

関連トピック

スケジュール済み設定変更の表示：アクセス ポイント無線 （830 ページ）

スケジュール設定変更の表示：WLAN （830 ページ）

スケジュール済み設定変更の表示：アクセス ポイント無線

[APテンプレートタスク（AP Template Tasks）] ページでは、現在のアクセス ポイント テンプレート タスクを管理できます。少なくとも 1 つの Lightweight アクセス ポイント タスクが存在することを確認します（テンプレートを使用した Lightweight AP の設定 （566 ページ） を参照）。

タスク	説明
現在のアクセス ポイント テンプレート タスクの変更	• **[設定（Configuration）] > [テンプレート（Templates）] > [スケジュール設定された設定タスク（Scheduled Configuration Task）]** を選択します。 • 該当するタスクのテンプレート名をクリックします。 • [AP無線/テンプレート（AP Radio/Template）] ページで、[適用/スケジュール（Apply/Schedule）] タブをクリックします。 • 現在のスケジュールまたはアクセス ポイント テンプレートの内容を必要に応じて変更し、[スケジュール（Schedule）] をクリックします。
現在のアクセス ポイント テンプレート タスクの有効化	• **[設定（Configuration）] > [テンプレート（Templates）] > [スケジュール設定された設定タスク（Scheduled Configuration Task）]** を選択します。 • 有効にするスケジュール済みタスクのチェックボックスをオンにします。 • [コマンドの選択（Select a command）] ドロップダウン リストから [スケジュールを有効にする（Enable Schedule）] を選択し、[実行（Go）] をクリックします。

関連トピック

スケジュール設定変更の表示 （829 ページ）
スケジュール設定変更の表示：WLAN （830 ページ）

スケジュール設定変更の表示：WLAN

すべてのスケジュール済み WLAN タスクを Prime Infrastructure で表示および管理するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [テンプレート（Template）] > [スケジュール設定された設定タスク（Scheduled Configuration Task）]** を選択します。

ステップ 2 左側のサイドバー メニューから [WLAN Configuration] を選択します。

ステップ 3 [WLAN Schedule Detail] ページを開くには、[Task Name] リンクを選択します。このページで、スケジュール設定されたタスクの日付と時刻を変更できます。

ステップ 4 スケジュール済みタスクのチェックボックスをオンにして、[Select a command] ドロップダウン リストを使用し、選択したタスクを有効化、無効化、または削除します。

関連トピック

スケジュール設定変更の表示 （829 ページ）
スケジュール済み設定変更の表示：アクセス ポイント無線 （830 ページ）

コントローラおよび AP へのソフトウェアのダウンロード

ソフトウェア ダウンロード タスクを管理するには、この機能を使用します。

• コントローラと AP へのソフトウェア ダウンロードのスケジュール設定 （831 ページ）
• スケジュール済みソフトウェア ダウンロードの変更 （833 ページ）
• ソフトウェア ダウンロードに関するコントローラのスケジュール設定 （833 ページ）

コントローラと AP へのソフトウェア ダウンロードのスケジュール設定

ソフトウェア ダウンロード タスクを追加するには：

ステップ 1 **[設定（Configuration）] > [テンプレート（Template）] > [スケジュール済み設定タスク（Scheduled Configuration Task）]** を選択し、左側のサイドバーのメニューから [ソフトウェア ダウンロード（Download Software）] を選択します。

ステップ 2 [コマンドの選択（Select a command）] ドロップダウン リストから [ソフトウェア ダウンロード タスクの追加（Add Download Software Task）] を選択し、[実行（Go）] をクリックします。

ステップ 3 次の情報を設定します。

- General
  - [Task Name]：スケジュール設定済みタスク名を入力して、当該のスケジュール設定済みソフトウェア ダウンロード タスクを特定します。
- Schedule Details
  - [Download Type]：ダウンロード タイプを選択します。[Download software to controller] チェックボックスをオンにして、コントローラへのソフトウェア ダウンロードをスケジュール設定するか、[Pre-download software APs] チェックボックスをオンにして、ソフトウェア AP の事前ダウンロードをスケジュール設定します。[Download software to controller] を選択した場合、イメージの詳細を指定します。

（注） 事前ダウンロードオプションは、選択したすべてのコントローラがリリース 7.0.x.x 以降を使用している場合のみ表示されます。

AP ごとの [イメージの事前ダウンロード（Image Predownload）] ステータスを確認するには、**[管理（Administration）] > [ダッシュボード（Dashboards）] > [ジョブ ダッシュボード（Job Dashboard）] > [システム ジョブ（System Jobs）] > [ワイヤレス ポーラー AP イメージの事前ダウンロード ステータス（Wireless Poller AP Pre-Download Image Status）]** でタスクを有効にし、[レポート起動パッド（Report Launch Pad）] から [AP イメージ事前ダウンロード（AP Image Predownload）] レポートを実行します。

- [Reboot Type]：リブート タイプが手動、自動、またはスケジュール設定済みかどうかを示します。

（注） [Reboot Type] として [Automatic] を設定できるのは、[Download software to controller] オプションが選択されている場合のみです。

- [Download date/time]：表示されるテキスト ボックスに日付を入力するか、カレンダー アイコンをクリックして、日付を選択できるカレンダーを開きます。時間と分のドロップダウン リストから時刻を選択します。
- [Reboot date/time]：このオプションは、[Reboot Type] として [Scheduled] を選択した場合にのみ表示されます。表示されるテキストボックスに日付を入力するか、カレンダーアイコンをクリックして、コントローラをリブートする日付を選択できるカレンダーを開きます。時間と分のドロップダウン リストから時刻を選択します。

すべての AP がソフトウェアの事前ダウンロードを完了できるように、ダウンロードとリブートの間に十分な時間（少なくとも 30 分）をスケジュール設定します。

スケジュール設定されたリブート時刻に、いずれかの AP で事前ダウンロードが進行中の場合、コントローラはリブートしません。そのような場合は、すべての AP の事前ダウンロードが終了するまで待機し、コントローラを手動でリブートします。

- [Notification]（任意）：電子メールで通知を送信する際の受信者の電子メール アドレスを入力します。

電子メール通知を受信するには、**[管理（Administration）] > [設定（Settings）] > [メール サーバ設定（Mail Server Configuration）]** ページで Prime Infrastructure メール サーバを設定します。

- [Image Details]：TFTP サーバまたは FTP サーバの情報を指定します。

[Schedule Details] 領域で [Download software to controller] オプションを選択した場合は、以下の詳細を入力します。

[TFTP]：TFTP サーバ情報を指定します。

- [File is Located on] ドロップダウン リストから、[Local machine] または [TFTP server] を選択します。

TFTP サーバを選択した場合は、[Default Server] を選択するか、[Server Name] ドロップダウン リストから **新しいサーバを追加**します。

- TFTP サーバの IP アドレスを指定します。これは、デフォルトのサーバを選択すると自動的に入力されます。
- ローカル ファイル名を指定するか、[Browse] をクリックして該当するファイルにナビゲートします。
- 上で [TFTP server] を選択した場合、ファイル名を指定します。

[FTP]：FTP サーバ情報を指定します。

- [FTP Credentials Information]：[FTP] オプション ボタンを選択した場合は、FTP ユーザ名、パスワード、およびポートを入力します。
- [File is Located on] ドロップダウン リストから、[Local machine] または [FTP server] を選択します。
- FTP サーバを選択した場合は、[Default Server] を選択するか、[Server Name] ドロップダウン リストから**新しいサーバを追加**します。
- FTP サーバの IP アドレスを指定します。これは、デフォルトのサーバを選択すると自動的に入力されます。
- ローカル ファイル名を指定するか、[Browse] をクリックして該当するファイルにナビゲートします。

- 上で [FTP server] を選択した場合は、ファイル名を指定します。

ステップ 4 [Save] をクリックします。

関連トピック

スケジュール済みソフトウェア ダウンロードの変更 （833 ページ）
ソフトウェア ダウンロードに関するコントローラのスケジュール設定 （833 ページ）

スケジュール済みソフトウェア ダウンロードの変更

はじめる前に

少なくとも 1 つの ソフトウェア ダウンロード タスクが存在している必要があります（「コントローラと APへのソフトウェア ダウンロードのスケジュール設定（831 ページ）」を参照）。

ソフトウェア ダウンロード タスクを変更するには：

ステップ 1 **[設定（Configuration）] > [テンプレート（Template）] > [スケジュール設定された設定タスク（Scheduled Configuration Task）]** を選択します。

ステップ 2 左側のサイドバー メニューから、[Download Software] を選択します。

ステップ 3 [Task Name] リンクをクリックして [Download Software Task] ページを開き、変更を行ってから [Save] をクリックします。

ステータスが [Enabled] になっているタスクの [Download Type]（[Download]/[Pre-download]）または [Server Type]（[FTP]/[TFTP]）を変更すると、タスクのステータスが [Disabled] になり、タスクと既存のコントローラとの関連付けがすべて解除されます。

関連トピック

コントローラと AP へのソフトウェア ダウンロードのスケジュール設定 （831 ページ）
ソフトウェア ダウンロードに関するコントローラのスケジュール設定 （833 ページ）

ソフトウェア ダウンロードに関するコントローラのスケジュール設定

このページには、スケジュール設定されたイメージのダウンロードまたは事前ダウンロードタスクで選択できる、サポートされているすべてのコントローラの一覧が表示されます。

スケジュール済みイメージのダウンロード用コントローラを選択するには：

ステップ 1 **[設定（Configuration）] > [テンプレート（Template）] > [スケジュール設定された設定タスク（Scheduled Configuration Task）]** を選択します。

ステップ 2 左側のサイドバー メニューから、[Download Software] を選択します。

ステップ 3 [Controller] をクリックして [Download Software Task] 詳細ページを開き、[Select Controller] をクリックしてコントローラ リストを表示します。

（注） タスクで事前ダウンロード オプションを選択した場合、ソフトウェア リリースが 7.0.x.x 以降のコントローラのみが表示されます。

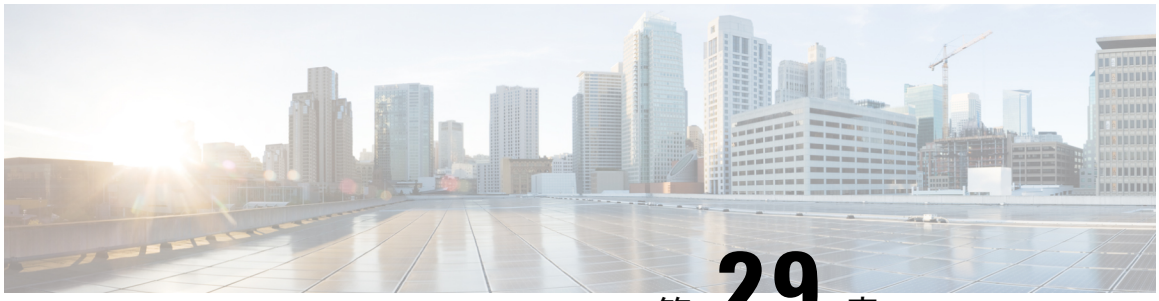
[コントローラの選択（Select Controller）] ページにアクセスする別の方法として、**[設定（Configure）]** > **[テンプレート（Template）]** > **[スケジュール済み設定タスク（Scheduled Configuration Task）]** > **[ソフトウェア ダウンロード（Download Software）]** を選択し、ステータスが [有効（Enabled）]、[無効（Disabled）]、または [期限切れ（Expired）] になっているダウンロード タスクの [コントローラの選択（Select Controller）] 列のハイパーリンクをクリックすることもできます。

[Reachability Status] が [Unreachable] のコントローラにはソフトウェアをダウンロードできません。

ステップ 4 必要な変更を行い、[Save] をクリックします。

関連トピック

スケジュール済みソフトウェア ダウンロードの変更 （833 ページ）
コントローラと AP へのソフトウェア ダウンロードのスケジュール設定 （831 ページ）



第 29 章

プラグ アンド プレイを使用した新しいデバイスの展開

- プラグ アンド プレイについて （835 ページ）
- プラグ アンド プレイの使用時の前提条件 （836 ページ）
- プラグ アンド プレイのワークフロー （836 ページ）
- [プラグアンドプレイ（Plug and Play）] ダッシュボードを使用した新しいデバイス展開のモニタ （838 ページ）
- デバイスの展開を定義するプラグ アンド プレイ プロファイルの作成 （844 ページ）
- デバイスとプラグ アンド プレイ プロファイルの関連付け （850 ページ）
- デバイスにブートストラップ コンフィギュレーションを展開するための前提条件 （860 ページ）
- プラグアンドプレイ用のブートストラップ コンフィギュレーションの作成 （861 ページ）
- ブートストラップ コンフィギュレーションをインストールする方法 （862 ページ）
- プラグ アンド プレイを使用して展開されたデバイスの確認 （868 ページ）
- プラグ アンド プレイ プロファイルの削除 （871 ページ）
- APIC-EM サーバで削除されたデバイスとプロファイルを取得する方法 （872 ページ）
- CNS プロファイルを APIC-EM プロファイルに変換する方法 （873 ページ）

プラグ アンド プレイについて

Cisco Prime Infrastructure は、新しいネットワーク デバイスで必要なソフトウェア イメージと設定を取得して適用することにより、ネットワークにおける新しいデバイスの展開の自動化をサポートします。Prime Infrastructure では、APIC-EM（Application Policy Infrastructure Controller）のコールホームと Cisco IOS の自動インストール（DHCP と TFTP を使用）機能を使用して、新しいデバイスがネットワークに参加して機能するまでの時間を短縮します。

Prime Infrastructure のプラグ アンド プレイ機能では、**[設定（Configuration）] > [テンプレート（Templates）] > [機能およびテクノロジー（Features and Technologies）]** で定義されたテンプレートを使用します。ユーザはテンプレートを再利用して新しいデバイスに適用できます。必要な初期設定を定義するブートストラップ テンプレートを作成して、デバイスが Prime

Infrastructure と通信できるようにすることで、新しいデバイスの展開を合理化できます。今後デバイスに追加するソフトウェア イメージと設定を指定（および事前展開）できます。

関連トピック

プラグ アンド プレイの使用時の前提条件 （836 ページ）
プラグ アンド プレイのワークフロー （836 ページ）

プラグ アンド プレイの使用時の前提条件

次の前提条件を完了する必要があります。

- サンプル DHCP サーバ設定 （867 ページ） の説明に従って、ネットワークに DHCP を適切に設定します。
- 新しいデバイスが接続しているブランチまたはキャンパスに、利用可能な既存のネットワーク接続（ディストリビューション/コア）がなければなりません。
- ブランチに Cisco Prime Infrastructure サーバへの直接接続があることが必要です。直接接続がない場合は、プラグ アンド プレイ外部サーバを使用して Cisco Prime Infrastructure に接続する必要があります。

関連トピック

デバイスの展開を定義するプラグ アンド プレイ プロファイルの作成 （844 ページ）

プラグ アンド プレイのワークフロー

Cisco Prime Infrastructure では、新しいデバイスに対してソフトウェア イメージと設定の初期プロビジョニングを実行できます。ネットワークへの新しいデバイスの展開を自動化するには、次のワークフローを実行します。

1. Cisco Prime Infrastructure がプラグ アンド プレイに APIC-EM サーバを使用するように指定します。APIC-EM の設定方法については、「マップ ビューと [プラグアンドプレイ（Plug and Play）] ダッシュボードの統合 （869 ページ）」を参照してください。
2. デバイスに応じたプラグアンドプレイ プロファイルを作成します。このプロファイルは、ルータ、スイッチ、ワイヤレス AP、および Nexus プロファイルとして分類されます。デバイスの展開を定義するプラグアンドプレイ プロファイルの作成 （844 ページ）を参照してください。
3. デバイスの電源を入れます。
4. デバイスにブートストラップ コンフィギュレーションを適用します。ブートストラップ コンフィギュレーションは、デバイスが Cisco Prime Infrastructure ゲートウェイ（APIC-EM）との接続を確立するために必要な最小限の設定です。プラグ アンド プレイ用のブートストラップ コンフィギュレーションの作成 （861 ページ）を参照してください。

ワイヤレス AP プロファイルの場合、プライマリ、セカンダリ、ターシャリ WLC の詳細が必要です。ワイヤレス AP のプラグ アンドプレイ プロファイルの作成 （847 ページ）を参照してください。

（注） Nexusデバイスの場合、これらのデバイスがブートストラップ コンフィギュレーションサポートしていないため、プラグアンドプレイ ワークフローが異なります。詳細については、Nexus デバイスのプラグ アンド プレイ プロファイルの作成 （848 ページ）を参照してください。

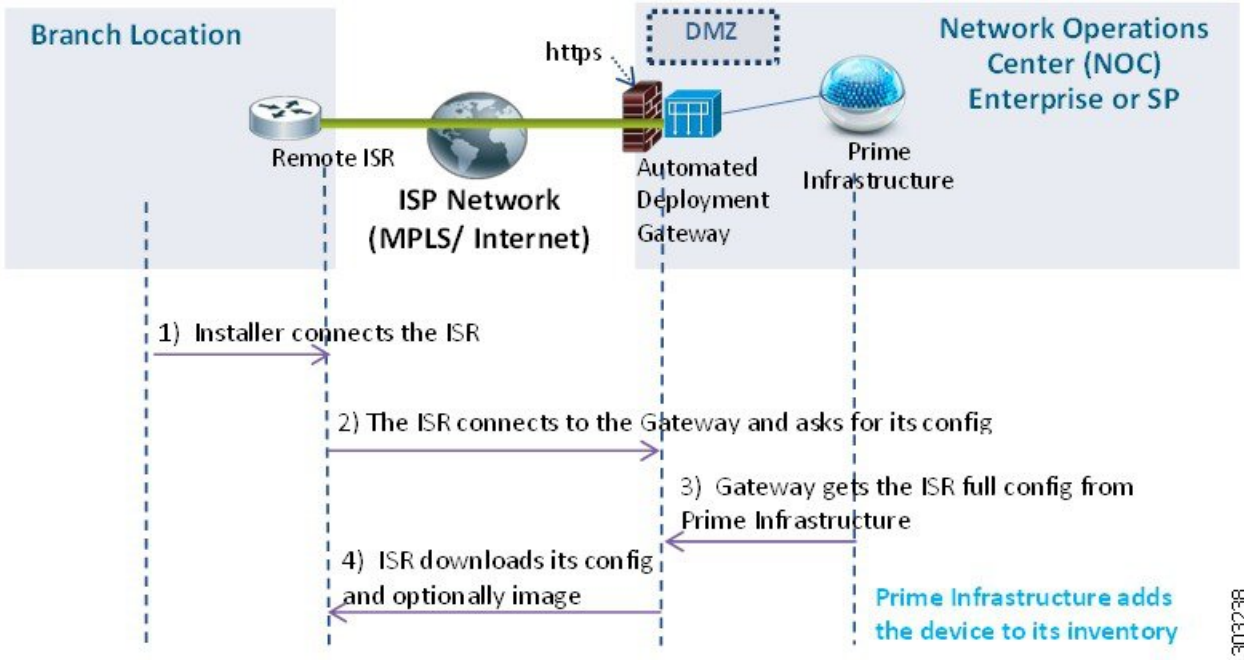
初期設定を適用すると、以下が実行されます。

1. デバイスは Cisco Prime Infrastructure サーバと通信します。
2. デバイスのプラグ アンド プレイ ID/シリアル番号に基づいて、Cisco Prime Infrastructure は、それがプラグ アンド プレイ事前プロビジョニング定義のデバイス ID と一致するかどうかを確認します。
3. 一致がある場合、Cisco Prime Infrastructure は、一致しているプラグ アンド プレイ プロファイルに指定されているアップグレード済みのソフトウェアイメージと設定をデバイスに適用します。

   デバイス ID と一致するものがない場合、Cisco Prime Infrastructure は既存のタイプベースのプラグ アンド プレイ事前プロビジョニング定義とデバイス タイプを照合します。
4. デバイスがインベントリに追加され、Cisco Prime Infrastructure で管理されます。
5. プラグ アンド プレイはインベントリ ワークフローに影響はありません。プラグ アンド プレイ プロファイルに指定されている場合、インベントリが収集された後にのみ、Cisco Prime Infrastructure はプラグ アンド プレイ後設定をデバイスに適用します。デバイスの追加と整理 （37 ページ）の章を参照してください。

デバイスにブートストラップ コンフィギュレーションが適用されると、インストーラはデバイスをリモート サイトの WAN に接続します。デバイスは、シリアル番号を使用してプラグ アンド プレイ ゲートウェイに接続し、すべての設定と（任意で）Cisco IOS イメージをダウンロードします（次のイメージを参照）。

図 *21 :* プラグ アンド プレイ ブランチの展開



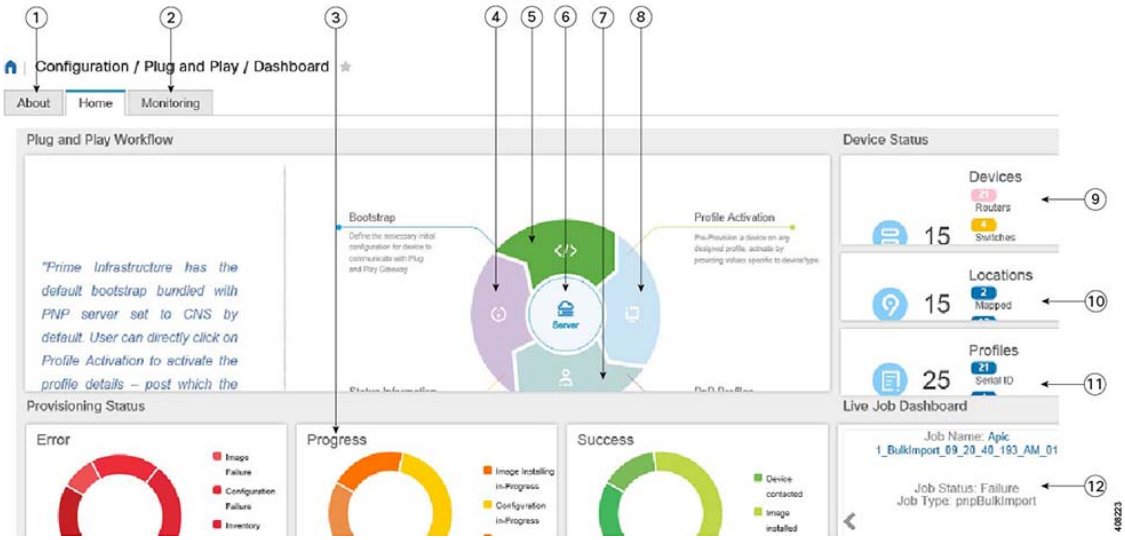
（注） 自動展開ゲートウェイは、APIC-EM コントローラです。

関連トピック

プラグアンドプレイ用のブートストラップコンフィギュレーションの作成 （861 ページ）
デバイスの展開を定義するプラグ アンド プレイ プロファイルの作成 （844 ページ）

[プラグアンドプレイ（Plug and Play）] ダッシュボードを使用した新しいデバイス展開のモニタ

[設定（Configuration）] > [プラグアンドプレイ（Plug and Play）] > [ダッシュボード（Dashboard）] の順に選択し、[ホーム（Home）] タブを選択してプラグ アンド プレイ アプリケーションのダッシュボードを表示します。



1	プラグアンドプレイ機能を理解するには、[製品情報（About）] をクリックします。プラグ アンド プレイについて （835 ページ）を参照してください。
2	マップ ビューにデバイスの詳細を表示するには、[モニタリング（Monitoring）] をクリックします。マップ ビューと [プラグアンドプレイ（Plug and Play）] ダッシュボードの統合 （869 ページ）を参照してください。
3	[デバイスのステータス（Device Status）] ページに移動するには、[エラー（Errors）]/[進捗ステータス（Progress）]/[成功（Success）] をクリックします。詳細はフィルタリングされ、適切に表示されます。
4	デバイスとそのステータスをモニタリングするには、[デバイスのステータス（Device status）] ページをクリックして移動します。
5	プロファイルのブートストラップテンプレートを作成するには、[ブートストラップ（Bootstrap）] ページをクリックして移動します。
[6]	**[管理（Administration）] > [サーバ（Servers）] > [APIC-EMコントローラ（APIC-EM Controller）]** ページをクリックして移動します。
7	デバイス タイプのプロファイルを作成するには、[プラグ アンド プレイ プロファイル（Plug and Play Profiles）] ページをクリックして移動します。
8	デバイス/タイプに固有の値を入力して有効化するには、**[プロファイルの有効化（Profile Activation）]** ページをクリックして移動します。
9	[デバイス ステータス（Device Status）] ページをクリックして移動します。
10	デバイスと設置ロケーションを表示するには、**[マップ ビュー（Map View）]**ページをクリックして移動します。

11	[プラグ アンド プレイ プロファイル（Plug and Play Profiles）] ページをクリックして移動します。
12	ジョブ ステータスを表示するには、**[管理（Administration）] > [ダッシュボード（Dashboard）] > [ジョブダッシュボード（Jobs Dashboard）]** ページをクリックして移動します。

関連トピック

マップ ビューと [プラグアンドプレイ（Plug and Play）] ダッシュボードの統合 （869 ページ）
プラグ アンド プレイへの APIC-EM ポリシー情報の統合 （842 ページ）
デバイスの展開を定義するプラグ アンド プレイ プロファイルの作成 （844 ページ）
デバイスとプラグ アンド プレイ プロファイルの関連付け （850 ページ）
プラグアンドプレイ用のブートストラップ コンフィギュレーションの作成 （861 ページ）
プラグ アンド プレイを使用して展開されたデバイスの確認 （868 ページ）

APIC-EM でプラグ アンド プレイを使用するための前提条件

Cisco Prime Infrastructure は、APIC-EM GA リリース 1.0、APIC-EM GA リリース 1.1、APIC-EM GA リリース 1.2、APIC-EM GA リリース 1.3、APIC-EM GA リリース 1.4 および APIC-EM GA リリース 2.0 をサポートしています。

（注） APIC-EM の構成または設定は、Prime Infrastructure の GUI でのみ実行し、APIC-EM では実行しないでください。

デバイスに展開される内容（設定、イメージなど）を決定するプロファイルを事前に設定する必要があります。デバイスがデバイスのシリアル番号に基づいて自宅にコールを発信すると、プロファイルが照合され、 APIC-EM のプラグ アンド プレイを使用して、デバイスが Cisco Prime Infrastructure から事前設定された同じイメージと設定でプロビジョニングされます。

APIC-EM プラグ アンドプレイ統合機能を使用すると、デバイスを http/https でプロビジョニングできます。必要に応じて、プロファイルを作成する場合、PKI（公開キー インフラストラクチャ）および SUDI（セキュアな固有デバイス識別子）をデバイスにインストールし、PKI と SUDI ベースの認証を使用することもできます。

関連トピック

プラグ アンド プレイへの APIC-EM ポリシー情報の統合 （842 ページ）
プラグ アンド プレイのワークフロー （836 ページ）

Nexus デバイスでプラグ アンド プレイを使用するための前提条件

ネットワークに Nexus デバイスを接続するには、次の前提条を満たす必要があります。

- インターフェイスの IP アドレス、ゲートウェイ アドレス、スクリプト サーバ（Cisco Prime Infrastructure 3.2）およびスクリプト ファイル（プラグ アンド プレイ）をブートストラップする DHCP サーバ。DHCP サーバの設定 （841 ページ）を参照してください。
- ソフトウェア イメージのインストールと設定のプロセスを自動化するコンフィギュレーション スクリプトが保管されている TFTP または HTTP サーバ。HTTP サーバの設定 （841 ページ）を参照してください。
- Cisco Prime Infrastructure 3. 2 サーバ（ソフトウェア イメージとコンフィギュレーション ファイルを含むプラグ アンド プレイ Nexus プロファイルが作成されている）。Nexus デバイスのプラグ アンド プレイ プロファイルの作成 （848 ページ）を参照してください。
- Cisco Prime Infrastructure のすべての Nexus 機能を管理するには、Nexus デバイスのバージョンが 6.2(12) 以降である必要があります。

DHCP サーバの設定

Nexus デバイスは、すべてのアクティブ インターフェイス（管理インターフェイスを含む）で、DHCP サーバからの DHCP オファーを要請する DHCP 検出メッセージを送信します。Nexus デバイス上の DHCP クライアントは、クライアント ID オプションにデバイスのシリアル番号または MAC アドレスを使用して、それ自体を DHCP サーバに識別させます。DHCP サーバはこの ID を使用して、IP アドレスやスクリプト ファイル名などの情報を DHCP クライアントに返します。

DHCP 検出メッセージでは、次のオプションを設定する必要があります。

- オプション 66（TFTP サーバ名）、オプション 150（TFTP サーバ アドレス）：DHCP サーバは、DHCP クライアントに TFTP サーバ名または TFTP サーバのアドレスをリレーします。DHCP クライアントはこの情報を使用して TFTP サーバに接続し、スクリプト ファイルを取得します。
- IP アドレス
- デフォルトゲートウェイ
- オプション 67（ブートファイル名）：DHCP サーバは、DHCP クライアントにブートファイル名をリレーします。ブートファイル名には、DHCP クライアントがスクリプト ファイルをダウンロードするのに使用する TFTP サーバ上にあるブートファイルのフル パスが含まれます。

関連トピック

HTTP サーバの設定 （841 ページ）
Nexus デバイスのプラグ アンド プレイ プロファイルの作成 （848 ページ）
Nexus デバイスでプラグ アンド プレイを使用するための前提条件 （840 ページ）
Nexus プラグ アンド プレイ プロファイルへのデバイス プロファイルの追加 （857 ページ）

HTTP サーバの設定

[管理（Administration）] > **[設定（Settings）]** > **[システム設定（System Settings）]** > **[全般（General）]** を選択して、左側のナビゲーション メニューから [サーバ（Server）] を選択します。

[HTTP 転送（HTTP Forward）] セクションで [有効（Enable）] をクリックすると、デバイスがプラグアンドプレイ ゲートウェイに接続し、初期設定およびイメージをダウンロードします。デフォルト ポートは 80 ですが、デバイスのポート設定も変更できます。

（注） Cisco Prime Infrastructure を再起動して変更を反映します。

関連トピック

DHCP サーバの設定 （841 ページ）
Nexus デバイスのプラグ アンド プレイ プロファイルの作成 （848 ページ）
Nexus デバイスでプラグ アンド プレイを使用するための前提条件 （840 ページ）
Nexus プラグアンドプレイ プロファイルへのデバイス プロファイルの追加 （857 ページ）

プラグ アンド プレイへの APIC-EM ポリシー情報の統合

Prime Infrastructure は、HTTPS および APIC-EM によって公開されている REST API を介して APIC-EM と通信します。

（注） Prime Infrastructure には、専用の APIC-EM サーバが必要です。そのため、APIC-EM サーバと 2 台以上の Prime Infrastructure サーバを統合しないでください。これによりデータ破損や非同期状態を防ぎます。

APIC-EM コントローラを Prime Infrastructure に統合するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [プラグ アンド プレイ（Plug and Play）] > [ダッシュボード（Dashboard）]** を選択します。

ステップ 2 **[ホーム (Home)]** タブで、**[サーバ（Server)]** をクリックして **Administration > Servers > APIC-EM Controller** ページを表示します。

ステップ 3 [追加（Add）] をクリックします。

ステップ 4 APIC-EM コントローラの IPv4 アドレスを入力します。

ステップ 5 HTTPS ポート番号を入力して APIC-EM に接続します。

ステップ 6 ユーザ名を入力します。

ステップ 7 パスワードを入力して、確認します。

ポーリング間隔は編集できません。Prime Infrastructure との接続/統合ステータスをチェックするために、APIC-EM コントローラは定期的（5 分ごと）にポーリングされます。また、デバイスのステータスも APIC-EM から 5 分ごとに更新されます。

APIC-EM コントローラを Prime Infrastructure に追加した後、同じページで APIC コントローラの到達可能性ステータスを表示できます。特定の APIC-EM コントローラを選択して、接続のポーリング ステータス

の履歴を表示することもできます。サービスを使用する前に、APIC-EMの接続が正常であることを確認してください。

[設定（Configuration）] > **[プラグ アンド プレイ（Plug and Play）]** > **[ダッシュボード（Dashboard）]** に移動するには、[プラグアンドプレイ プロファイルを作成するにはここをクリックしてください（Please Click here to create Plug and Play Profiles）] リンクをクリックします。

Prime Infrastructure に有効な APIC-EM コントローラを追加すると、**[管理（Administration）]** > **[サーバ（Servers）]** > **[APIC-EM コントローラ グローバル PnP/ZTD 設定（APIC-EM Controller Global PnP/ZTD Settings）]** にグローバル オプションが自動的に [APIC-EM] に設定されます。

APIC-EMの統合は双方向に行われません。したがって、統合するAPIC-EMに変更を加えないでください。

関連トピック

デバイスの展開を定義するプラグ アンド プレイ プロファイルの作成 （844 ページ）
プラグアンドプレイ用のブートストラップ コンフィギュレーションの作成 （861 ページ）
[プラグアンドプレイ（Plug and Play）] ダッシュボードを使用した新しいデバイス展開のモニタ （838 ページ）

APIC-EM サイトの同期

Prime Infrastructure では、そのインベントリを APIC-EM と統合して同期できます。APIC-EM と統合する Prime Infrastructure 専用インスタンスが必要です。Prime Infrastructure 専用インスタンスはネットワークのモニタリングに使用できますが、プロビジョニングには使用できません。

Prime Infrastructure 専用インスタンスから、[管理（Administration）] > [サーバ（Servers）] > [APIC-EM コントローラ（APIC-EM Controller）] ページで APIC-EM インスタンスを指定します。この Prime Infrastructure インスタンスは、サイト、デバイス、デバイスとロケーションのグループ、WAN インターフェイス ポート グループ、および APIC-EM インスタンスとのエンドポイント アソシエーションを定期的に同期します。Prime Infrastructure は同期済みデバイスのインベントリとその他のモニタリング情報を収集し、[すべてのデバイス（All Devices）] > [ロケーション（Location）] に新しいフォルダを作成して、対応するサイトにデバイスを追加します。Prime Infrastructure は、保証および syslog 情報を収集することによってデバイスをモニタします。

デフォルトでは、Prime Infrastructure は 6 時間ごとに APIC-EM 統合同期ジョブを実行します。APIC-EMからサイトやデバイスを削除すると、Prime Infrastructureからも削除されます。APIC-EMでデバイスを追加または更新した場合は、Prime Infrastructure でもそれらが追加、更新されます。

デバイスの展開を定義するプラグアンドプレイプロファイルの作成

[設定（Configuration）] > [プラグアンドプレイ（Plug and Play）] > [ダッシュボード（Dashboard）] の順に選択し、[ホーム（Home）] タブで [PnPプロファイル（PnP Profiles）] をクリックします。プラグ アンド プレイ プロファイル リストの詳細な要約が表示されます。

Cisco Prime Infrastructure は、デバイスを検出し、インベントリに追加し、設定できるように、新たに接続されたデバイスが Cisco Prime Infrastructure サーバに「call home」することを可能にするプラグ アンド プレイ プロファイルを作成するのに役立ちます。このプロファイル（ブートストラップ プロファイルとも呼ばれる）はデバイスにクレデンシャルを設定するので、デバイスごとにコンソールで設定しなくても Cisco Prime Infrastructure でデバイスを管理できるようになります。

特定のフォルダにある次のプラグ アンド プレイ プロファイルを作成できます。

- ルータ プロファイル：ルータとスイッチのプラグ アンド プレイ プロファイルへのデバイス プロファイルの追加 （853 ページ）を参照してください
- スイッチ プロファイル：ルータとスイッチのプラグ アンド プレイ プロファイルへのデバイス プロファイルの追加 （853 ページ）を参照してください
- ワイヤレス AP プロファイル：ワイヤレス AP のプラグ アンド プレイ プロファイルの作成 （847 ページ）を参照してください
- Nexus プロファイル：Nexus デバイスのプラグ アンド プレイ プロファイルの作成 （848 ページ）を参照してください
- Mobility Express WLC プロファイル：参照 Mobility Express WLC プラグ アンド プレイ プロファイルの作成 （849 ページ）

タイプに応じて、次の項目が含まれるプラグ アンド プレイ プロファイルを作成できます。

- ソフトウェア イメージのみ。
- 設定のみ。
- ソフトウェア イメージと設定の両方。
- PKI 証明書および SUDI 証明書。
- プライマリおよびセカンダリ コントローラ、AP グループと FlexConnect グループ（ワイヤレス AP 用のみ）。

プロファイルには、追加のプラグ アンド プレイ後の設定（オプション）を含めることができます。これは、デバイスが Cisco Prime Infrastructure によって管理された後にのみデバイスに適用できます。

（注） ルートの [プラグアンドプレイ（Plug and Play）] フォルダの下にプロファイルを作成することはできません。プロファイルタイプに応じて、特定のフォルダにのみプロファイル（Nexus プロファイル、スイッチ プロファイル、ルータ プロファイル、ワイヤレス AP プロファイル）を作成できます。

（注）

- PnP スケールはプロファイル全体に分散された任意の数のデバイスをサポートしますが、プロファイルは 1 つのプロファイル インスタンスでサポートできるデバイスが最大 500 個です。このスケールを増やすには、別のプロファイルを作成し、この新しいプロファイルにデバイスを追加します。
- プロファイルに関係なく、最大 50 個のデバイスが同時にプロビジョニングされます。現在の 50 個のデバイスがプロビジョニングされると、PnP エージェントは次の一連のデバイスを選択します。
- Cisco Prime Infrastructure プロファイルとプロファイル インスタンスが作成および更新される仮想ドメインの詳細を保存します。プロビジョニングされたデバイスは、個別仮想ドメインと ROOT-DOMAIN のインベントリに追加されます。
- 各プロファイル インスタンスの管理 IP アドレスが固有であることを確認します。
- デバイス プロファイルの一括インポートまたはエクスポート中のプロファイル インスタンスへのロケーション グループの追加はサポートされていません。対応するロケーション グループのルールを作成すると、管理対象デバイスを動的に追加できます。

関連トピック

Nexus デバイスでプラグ アンド プレイを使用するための前提条件 （840 ページ）
デバイスとプラグ アンド プレイ プロファイルの関連付け （850 ページ）
[プラグアンドプレイ（Plug and Play）] ダッシュボードを使用した新しいデバイス展開のモニタ （838 ページ）
プラグ アンド プレイを使用して展開されたデバイスの確認 （868 ページ）
プラグ アンド プレイ プロファイルの削除 （871 ページ）

ルータおよびスイッチのプラグ アンド プレイ プロファイルの作成

プラグ アンド プレイ プロファイルには、次の少なくとも *1* つを含める必要があります。

- ブートストラップ コンフィギュレーション：Prime Infrastructure には標準のブートストラップ コンフィギュレーションがありますが、ユーザが独自に作成することもできます。「プラグアンドプレイ用のブートストラップ コンフィギュレーションの作成（861ページ）」を参照してください。
- ソフトウェア イメージ（「インベントリ収集中にイメージ リポジトリに保存されたイメージの制御方法 （115 ページ）」を参照）。

- 設定 CLI テンプレート（PnP と PnP 後の設定）：空白テンプレートを使用した新しい CLI 設定テンプレートの作成 （506 ページ）を参照してください。

ステップ 1 **[設定（Configuration）] > [プラグ アンド プレイ（Plug and Play）] > [ダッシュボード（Dashboard）]** の順に選択し、[ホーム（Home）] タブで [PnP プロファイル（PnP Profiles）] をクリックします。

ステップ 2 左側のナビゲーション ペインから必要なプロファイル（[ルータ プロファイル（Router Profiles）] または [スイッチ プロファイル（Switch Profiles）]）を選択し、[追加（Add）] をクリックし、[プロファイルの概要（Profile Summary）] タブに詳細を表示します。

ステップ 3 [プロファイル基本情報（Profile Basic）] セクションに適切な情報を入力します。

[クレデンシャル プロファイル（Credential Profiles）] ドロップダウン リストから必要なクレデンシャル プロファイルを選択して、デバイスに共通するクレデンシャルを関連付けることができます。

ステップ 4 （任意）[プロファイルの詳細（Profile Detail）] セクションで、[ターミナル サーバの有効化（Enable Terminal Server）]チェックボックスをオンにし、デバイスをターミナル サーバ IP とポートでプロビジョニングします。

ステップ 5 （任意）[プロファイルの詳細（Profile Detail）] セクションで、[PKI の有効化（Enable PKI）]チェックボックスをオンにし、PKI 証明書でデバイスをプロビジョニングします。PKI 証明書は、イメージのプロビジョニングと設定が完了した後にデバイスにインストールされます。詳細については、『Cisco Open Plug-n-Play Agent Configuration Guide, Cisco IOS XE Release 3E』を参照してください。

[PKI の有効化（Enable PKI）] チェックボックスをオフにすると、デバイスは PKI 証明書を使ってプロビジョニングされません。

（注） [PKI を有効にする（Enable PKI）] チェックボックスはスイッチ プロファイルでは使用できません。

ステップ 6 （任意）[プロファイルの詳細（Profile Detail）] セクションで、[SUDI の有効化（Enable SUDI）]チェックボックスをオンにし、SUDI 証明書でデバイスをプロビジョニングします。このオプションを有効にする前に、APIC-EM コントローラが SUDI 証明書を検証してデバイスを認証するように指定できます。

（注） [SUDI の有効化（Enable SUDI）] を選択した場合は、デバイスが SUDI をサポートしていることを確認し、SUDI serial number.una を使用してデバイスを追加します。

ステップ 7 [ブートストラップ テンプレート（Bootstrap Template）] ドロップダウン リストから、ブートストラップ テンプレートを選択します。また、PnP ブートストラップ テンプレート（ユーザ定義）に保存されるカスタマイズ ブートストラップ テンプレートを作成することもできます。プラグ アンド プレイ用のブートストラップ コンフィギュレーションの作成 （861 ページ）を参照してください。

ステップ 8 （任意）[Software Image] ドロップダウン リストから、必要なソフトウェア イメージを選択します。この手順は、イメージを使ってデバイスをプロビジョニングする場合にのみ必要です。プラグアンドプレイ プロファイルのソフトウェア イメージのインポート （847 ページ）を参照してください。

ステップ 9 （任意）[コンフィギュレーション テンプレート（Configuration Template）] ドロップダウン リストから、以前作成した設定テンプレートを選択します。

ステップ 10 （任意）[PnP 後の設定テンプレート（Post PnP Configuration Template）] ドロップダウン リストから必要な設定テンプレートを選択します。この設定は Prime Infrastructure で管理されるようになると、デバイスに適用されます。

ステップ 11 [新しいプラグ アンド プレイ プロファイルとして保存（Save as New Plug and Play Profile）] をクリックします。

ステップ 12 プロファイルが作成され、[プロファイルの概要（Profile Summary）] タブの詳細が表示されます。詳細を編集して [保存（Save）] をクリックし、同一プロファイルの詳細を保存したり、[未開封にする（Save as New）] をクリックして新しいプロファイルを作成したりできます。

ステップ 13 [プロファイル インスタンス（Profile Instances）] タブをクリックします。

ステップ 14 [追加（Add）] をクリックし、プラグ アンド プレイ プロファイルの事前プロビジョニングの対象となるデバイスの詳細を追加します。ルータとスイッチのプラグ アンド プレイ プロファイルへのデバイス プロファイルの追加 （853 ページ）を参照してください。

関連トピック

ルータとスイッチのプラグ アンド プレイ プロファイルへのデバイス プロファイルの追加（853 ページ）
デバイス プロファイルのエクスポート、編集、およびプラグ アンド プレイ プロファイルへのインポート （854 ページ）
デバイスとプラグ アンド プレイ プロファイルの関連付け （850 ページ）
プラグ アンド プレイ用のブートストラップ コンフィギュレーションの作成 （861 ページ）

プラグ アンド プレイ プロファイルのソフトウェア イメージのインポート

ソフトウェア イメージをインポートして、プラグ アンド プレイ プロファイルの一部として含めることができます。

ステップ 1 **[インベントリ（Inventory）]>[デバイス管理ソフトウェア（Device Management Software）]>[ソフトウェア イメージ（Software Images）]** を選択します。

ステップ 2 **[インポート（Import）]**をクリックし、ソフトウェア イメージのインポート元を指定します。

ステップ 3 収集オプションと、イメージ ファイルをインポートするタイミングを指定します。ジョブをすぐに実行することも、後で実行するようにスケジュール設定することもできます。

インポート ジョブは一度だけ実行されます。

ステップ 4 [Submit] をクリックします。

ステップ 5 イメージ管理ジョブの詳細を表示するには、**[管理（Administration）]>[ダッシュボード（Dashboards）]>[ジョブ ダッシュボード（Job Dashboard）]** を選択します。

関連トピック

ルータおよびスイッチのプラグ アンド プレイ プロファイルの作成 （845 ページ）

ワイヤレス AP のプラグ アンド プレイ プロファイルの作成

ワイヤレス AP のプラグ アンド プレイ プロファイルを作成し、一度に数千台のデバイスをプロビジョニングできます。

ステップ 1 **[設定（Configuration）] > [プラグ アンド プレイ（Plug and Play）] > [ダッシュボード（Dashboard）]** を選択し、[ホーム（Home）] タブで [PnP プロファイル（PnP Profiles）] をクリックします。

ステップ 2 左側のナビゲーション ペインから [ワイヤレス AP プロファイル（Wireless AP Profiles）] を選択し、[追加（Add）] をクリックして [プロファイルの概要（Profile Summary）] タブに詳細を表示します。

ステップ 3 [プロファイル基本情報（Profile Basic）] セクションに適切な情報を入力します。

[デバイス タイプ（Device Type）] フィールドの [自立型 AP（Autonomous AP）] は自動的に入力されますが、編集することはできません。ワイヤレス AP プロファイルへの PID 値の入力は必須です。

ステップ 4 [プロファイルの詳細（Profile Detail）] セクションに適切な情報を入力します。

ステップ 5 [新しいプラグ アンド プレイ プロファイルとして保存（Save as New Plug and Play Profile）] をクリックします。

ステップ 6 プロファイルが作成され、[プロファイルの概要（Profile Summary）] タブの詳細が表示されます。詳細を編集して [保存（Save）] をクリックし、同一プロファイルの詳細を保存したり、[未開封にする（Save as New）] をクリックして新しいプロファイルを作成したりできます。

ステップ 7 [プロファイル インスタンス（Profile Instances）] タブをクリックします。

ステップ 8 [追加（Add）] をクリックし、プラグ アンド プレイ プロファイルの事前プロビジョニングの対象となるデバイスの詳細を追加します。ワイヤレス AP プラグ アンド プレイ プロファイルへのデバイス プロファイルの追加 （856 ページ）を参照してください。

関連トピック

ワイヤレス AP プラグ アンド プレイ プロファイルへのデバイス プロファイルの追加 （856 ページ）
プラグ アンド プレイ用のブートストラップ コンフィギュレーションの作成 （861 ページ）
プラグ アンド プレイを使用して展開されたデバイスの確認 （868 ページ）

Nexus デバイスのプラグ アンド プレイ プロファイルの作成

Nexus デバイス用のプラグ アンド プレイ プロファイルを作成するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [プラグ アンド プレイ（Plug and Play）] > [ダッシュボード（Dashboard）]** の順に選択し、[ホーム（Home）] タブで [PnP プロファイル（PnP Profiles）] をクリックします。

ステップ 2 左側のナビゲーション ペインから [Nexus プロファイル（Nexus Profiles）] を選択し、[追加（Add）] をクリックして [プロファイルの概要（Profile Summary）] タブで詳細を表示します。

ステップ 3 [プロファイル基本情報（Profile Basic）] セクションに適切な情報を入力します。

[クレデンシャル プロファイル（Credential Profiles）] ドロップダウン リストから必要なクレデンシャル プロファイルを選択し、デバイスに共通するクレデンシャルを関連付けます。クレデンシャル プロファイルを使用したデバイス クレデンシャルの一貫した適用 （58 ページ）を参照してください。

ステップ 4 [システム イメージ（System Image）] および [キック スタート イメージ（Kick Start Image）] ドロップダウン リストから必要なソフトウェア イメージを選択します。プラグ アンド プレイ プロファイルのソフトウェア イメージのインポート （847 ページ）を参照してください。

（注） Cisco.com からダウンロードする場合は、システム イメージとキック スタート イメージの両方が同じイメージ バージョンであることを確認します。

ステップ 5 [設定テンプレート（Configuration Template）] ドロップダウン リストから、システムで定義された Nexus POAP 設定テンプレートまたは以前に作成した設定テンプレートのいずれかを選択し、変更を追加します。

ステップ 6 [新しいプラグ アンド プレイ プロファイルとして保存（Save as New Plug and Play Profile）] をクリックします。

ステップ 7 プロファイルが作成され、[プロファイルの概要（Profile Summary）] タブの詳細が表示されます。詳細を編集して [保存（Save）] をクリックし、同一プロファイルの詳細を保存したり、[新規として保存（Save as New）] をクリックして新しいプロファイルを作成することができます。

ステップ 8 [プロファイル インスタンス（Profile Instances）] タブをクリックします。

ステップ 9 [追加（Add）] をクリックし、プラグ アンド プレイ プロファイルの事前プロビジョニングの対象となるデバイスの詳細を追加します。Nexus プラグ アンド プレイ プロファイルへのデバイス プロファイルの追加（857 ページ）を参照してください。

関連トピック

Nexus デバイスでプラグ アンド プレイを使用するための前提条件 （840 ページ）
プラグ アンド プレイ プロファイルのソフトウェア イメージのインポート （847 ページ）
[プラグアンドプレイ（Plug and Play）] ダッシュボードを使用した新しいデバイス展開のモニタ （838 ページ）
Nexus プラグ アンド プレイ プロファイルへのデバイス プロファイルの追加 （857 ページ）

Mobility Express WLC プラグ アンド プレイ プロファイルの作成

Mobility Express WLC デバイス用のプラグ アンド プレイ プロファイルを作成するには、次の手順を実行します。

始める前に

APIC-EM が Prime Infrastructure と同期されていることを確認します。

ステップ 1 **[設定（Configuration）] > [プラグ アンド プレイ（Plug and Play）] > [ダッシュボード（Dashboard）]** の順に選択し、[ホーム（Home）] タブで [PnP プロファイル（PnP Profiles）] をクリックします。

ステップ 2 左側のナビゲーション ペインから [Mobility Express WLCプロファイル（Mobility Express WLC Profiles）] を選択し、[追加（Add）] をクリックして [プロファイルの概要（Profile Summary）] タブで詳細を表示します。

ステップ 3 [プロファイル基本情報（Profile Basic）] セクションに適切な情報を入力します。

（任意）[クレデンシャルプロファイル（Credential Profiles）] ドロップダウン リストから必要なクレデンシャル プロファイルを選択し、デバイスに共通するクレデンシャルを関連付けます。

ステップ 4 [設定テンプレート（Configuration Template）] ドロップダウン リストで、Mobility Express デイ ゼロ設定テンプレートのいずれかを選択します。

raw 設定をインポートする場合は、設定テンプレートを選択しないでください。Mobility Express WLC プラグアンドプレイ プロファイルインスタンスへのデバイス プロファイルの追加（858ページ）のステップ 3 を参照してください。

ステップ 5 （任意）デバイスが Prime Infrastructure の管理対象になった後で、[Postプラグアンドプレイワイヤレス設定グループ（Post Plug and Play Wireless Configuration Groups）] 領域で、[ワイヤレス設定グループ（Wireless Configuration group）] ドロップダウン リストからデバイスにプッシュする追加の設定を選択します。

ステップ 6 （任意）[ソフトウェアイメージ（Software Image）] ドロップダウン リストから、必要なソフトウェア イメージを選択します。

（注） アップグレードされたバージョンのソフトウェア イメージを展開する場合は、[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ソフトウェアイメージ（Software Images）]ページでアップグレード後のソフトウェア 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 イメージをリポジトリに追加（インポート）する （134 ページ）を参照してください。

ステップ 7 [新しいプラグ アンド プレイ プロファイルとして保存（Save as New Plug and Play Profile）] をクリックします。

ステップ 8 プロファイルが作成され、[プロファイルの概要（Profile Summary）] タブの詳細が表示されます。詳細を編集して[保存（Save）]をクリックし、同一プロファイルの詳細を保存したり、[新規として保存（Save as New）] をクリックして新しいプロファイルを作成することができます。

ステップ 9 [プロファイル インスタンス（Profile Instances）] タブをクリックします。

ステップ 10 [追加（Add）] をクリックし、プラグ アンド プレイ プロファイルの事前プロビジョニングの対象となるデバイスの詳細を追加します。詳細については、「Mobility Express WLC プラグ アンド プレイ プロファイル インスタンスへのデバイス プロファイルの追加 （858 ページ）」を参照してください。

デバイスとプラグ アンド プレイ プロファイルの関連付け

定義したプロファイルにデバイスを事前プロビジョニングし、特定のデバイス/タイプに値を入力すると有効化できます。デバイスを一括して追加する場合は、デバイス プロファイルのエクスポート、編集、およびプラグ アンド プレイ プロファイルへのインポート （854 ページ）を参照してください。

次のいずれかを実行できます。

- 新しいプラグ アンド プレイ プロファイルを作成し、デバイス プロファイルを作成したプラグ アンド プレイ プロファイルに追加します。新しいプラグ アンド プレイ プロファイルの作成とデバイス プロファイルの追加 （851 ページ）を参照してください。

- 既存のプラグ アンドプレイ プロファイルにデバイス プロファイルを追加します。既存のプラグ アンドプレイ プロファイルへのデバイス プロファイルの追加 （852 ページ）を参照してください。

また、**[設定（Configuration）] > [プラグアンドプレイ（Plug and Play）] > [ダッシュボード（Dashboard）]** を選択し、[ホーム（Home）] タブで [PnPプロファイル（PnP Profiles）] をクリックして、新しいプラグ アンドプレイ プロファイルを作成できます。必要なプラグ アンドプレイ プロファイルを作成したら、[プロファイル インスタンス（Profile Instances）] タブで [追加（Add）] をクリックしてデバイス プロファイルを追加します。

関連トピック

ルータとスイッチのプラグ アンドプレイ プロファイルへのデバイス プロファイルの追加（853 ページ）
ワイヤレス APプラグ アンドプレイ プロファイルへのデバイス プロファイルの追加 （856 ページ）
Nexusプラグ アンドプレイ プロファイルへのデバイス プロファイルの追加 （857 ページ）

新しいプラグ アンド プレイ プロファイルの作成とデバイス プロファイルの追加

ステップ 1 **[設定（Configuration）] > [プラグアンドプレイ（Plug and Play）] > [ダッシュボード（Dashboard）]** の順に選択し、[ホーム（Home）] タブで [プロファイルの有効化（Profile Activation）] をクリックします。

ステップ 2 [PnP プロファイルの選択（Select PnP Profile）] ページで、[新しいプロファイルを作成してデバイスを追加（Add device by creating new Profile）] を選択します。

ステップ 3 [プロファイル タイプ（Profile Type）] ドロップダウン リストから作成するプロファイルのタイプを選択します。

ステップ 4 [プロファイル基本情報（Profile Basic）] および [プロファイルの詳細（Profile Detail）] セクションに必要な情報を入力します。プロファイル作成の詳細については、デバイスの展開を定義するプラグアンドプレイ プロファイルの作成 （844 ページ）を参照してください。

ステップ 5 （任意）プラグ アンド プレイ プロファイルの作成時に [ターミナル サーバの有効化（Enable Terminal Server）] チェックボックスが選択されている場合は、[ターミナル サーバ IP（Terminal Server IP）] および [ポート（Port）] を入力します。

ステップ 6 右側の矢印アイコンをクリックし、[プラグ アンド プレイ プロファイル（Plug and Play Profile）] ページに移動して、作成したプラグ アンド プレイ プロファイルにデバイス プロファイルを追加します。

ステップ 7 （任意）[ターミナル サーバの有効化（Enable Terminal Server）] チェックボックスをオンにしている場合は、次のように raw 設定をデバイスにインポートします。

1. 複数のテキスト ファイルを含む zip ファイルまたは tar ファイルをインポートします。各テキスト ファイルには、デバイスに適用する必要がある raw 設定が含まれます。また必要に応じて、1 つのテキスト ファイルをインポートすることもできます。

   テキスト ファイルには DeviceSerialID.txt または DeviceName.txt という名前を付ける必要があります。たとえば、デバイス ID が FGLABCD443f の場合に設定の詳細を含むテキスト ファイルは

FGLABCD443f.txt、デバイス名が XaaaXX の場合に設定の詳細を含むテキスト ファイルは XaaaXX.txt である必要があります。

2. ファイルが正常にアップロードされると、このファイルを処理してAPICにアップロードするために、ジョブがトリガーされます。
3. APICの特定のプロファイルに移動することで、設定がそのプロファイル内で対応するデバイスに正常に適用されていることを確認します。

関連トピック

既存のプラグアンドプレイ プロファイルへのデバイスプロファイルの追加（852ページ）
ルータとスイッチのプラグ アンド プレイ プロファイルへのデバイス プロファイルの追加（853 ページ）
ワイヤレス AP プラグアンドプレイ プロファイルへのデバイス プロファイルの追加（856 ページ）
Nexus プラグアンドプレイ プロファイルへのデバイスプロファイルの追加（857ページ）

既存のプラグ アンド プレイ プロファイルへのデバイス プロファイルの追加

ステップ 1 **[設定（Configuration）] > [プラグアンドプレイ（Plug and Play）] > [ダッシュボード（Dashboard）]** の順に選択し、[ホーム（Home）] タブで [プロファイルの有効化（Profile Activation）] をクリックします。

ステップ 2 [PnP プロファイルの選択（Select PnP Profile）] ページで、[既存のプロファイルへのデバイスの追加（Add device to an existing profile）] を選択します。

ステップ 3 [プロファイルの選択（Select Profile）] ドロップダウン リストから、デバイス プロファイルを追加するための必要なプロファイルを選択します。プロファイル作成の詳細については、デバイスの展開を定義するプラグ アンド プレイ プロファイルの作成 （844 ページ） を参照してください。

ステップ 4 選択したプロファイルの詳細は自動的に入力されますが、編集することはできません。

ステップ 5 右側の矢印アイコンをクリックし、[プラグアンドプレイプロファイル（Plug and Play Profile）] ページに移動して、作成したプラグ アンド プレイ プロファイルにデバイス プロファイルを追加します。

関連トピック

新しいプラグアンドプレイ プロファイルの作成とデバイスプロファイルの追加（851 ページ）
ルータとスイッチのプラグ アンド プレイ プロファイルへのデバイス プロファイルの追加（853 ページ）
ワイヤレス AP プラグアンドプレイ プロファイルへのデバイス プロファイルの追加（856 ページ）
Nexus プラグアンドプレイ プロファイルへのデバイスプロファイルの追加（857ページ）

ルータとスイッチのプラグ アンド プレイ プロファイルへのデバイス プロファイルの追加

必要なプラグ アンドプレイ プロファイルにデバイス プロファイルを追加するには、次の手順を実行します。

ステップ 1 [プラグ アンド プレイ デバイスのプロビジョニング プロファイル（Plug and Play Device Provisioning Profile）] ページに必要な情報を入力します。

- [ロケーション（Location）] ドロップダウン リストから、デバイスをマッピングする設置ロケーションを選択します。この詳細は [マップ（Map）] ビューに表示されます。

（注） 特定のロケーションにデバイスを追加する前に、**[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ネットワークデバイス（Network Devices）]** または **[インベントリ（Inventory）] > [グループ管理（Group Management）] > [ネットワークデバイスグループ（Network Device Groups）]** でロケーション グループを作成します。ロケーション グループの作成 （68 ページ）を参照してください。

ステップ 2 右側の矢印アイコンをクリックし、[ブートストラップの選択（Bootstrap Selection）] に移動します。

ステップ 3 [ブートストラップの選択（Bootstrap Selection）] ページで、プロファイルの作成段階に選択したブートストラップ テンプレートは自動的に入力されます。必要に応じて値を編集できます。

- プラグ アンド プレイ ゲートウェイ ロケーション：デフォルトでは、Prime Infrastructure サーバはプラグ アンドプレイ ゲートウェイ サーバとして動作します。外部プラグ アンド プレイ ゲートウェイの IP アドレスを指定することによって、サーバを変更できます。

[CLI] をクリックし、設定したブートストラップの CLI のサマリーを表示します。

ステップ 4 右側の矢印アイコンをクリックし、次のページに移動します。

（注） プロファイルの作成段階で [ソフトウェアイメージ（Software Image）] および [設定テンプレート（Configuration Template）] を選択している場合は、[ソフトウェアイメージ（Software Image）]、[設定（Configuration）]、および [PnP後の設定（Post PnP Configuration）] タブが [プロファイルの有効化（Profile Activation）] ページに表示されます。

ステップ 5 （任意）[ソフトウェアイメージ（Software Image）] ページで必要な情報を入力します。

ステップ 6 （任意）[設定（Configuration）] ページで、プロファイルの作成段階に選択した設定テンプレートは自動的に入力されます。必要な情報を入力し、次のページに移動します。

[CLI] をクリックし、CLI のサマリーを表示します。

ステップ 7 （任意）[PnP 後の設定テンプレート（Post PnP Configuration Template）] ページで、プロファイルの作成段階に選択したブートストラップテンプレートは自動的に入力されます。必要な情報を入力し、次のページに移動します。

[CLI] をクリックし、CLI のサマリーを表示します。

ステップ 8 [管理クレデンシャル（Management Credentials）] ページで必要な情報を入力します。これらのデバイスのパラメータは、プロビジョニング時にデバイスに適用されます。

（注） デバイス タイプがルータまたはスイッチの場合、[管理クレデンシャル（Management Credentials）] ページでは、プロファイルの作成段階に選択したクレデンシャル プロファイルが自動的に入力されますが、値は編集できません。

ステップ 9 [プロファイル有効化サマリー（Profile Activation Summary）] ページでは、設定されたデバイスの詳細が表示されます。

ステップ 10 [終了（Finish）] をクリックし、デバイス プロファイルをプロビジョニングします。

プロビジョニングに成功すると、デバイス プロファイルが特定のプロファイルの [プロファイルインスタンス（Profile Instances）] ページ表示されます。また、デバイスのプロビジョニング ステータスは [デバイス ステータス（Device Status）] ページに表示されます。

デバイスが正常にプロビジョニングされると、そのデバイスはPrime Infrastructureインベントリに追加され、管理できるようになります。デバイスは、プラグアンドプレイ プロファイルの管理パラメータに基づいて、Prime Infrastructure インベントリに追加されます。デバイスがインベントリに正常に追加されたら、別のプラグ アンド プレイ後の設定（必要な場合）がデバイスに適用されます。

クレデンシャルが一致しない場合、デバイスはインベントリに追加されますが、そのステータスは「管理対象（Managed）」になりません。

関連トピック

デバイス プロファイルのエクスポート、編集、およびプラグ アンド プレイ プロファイルへのインポート （854 ページ）
デバイスの展開を定義するプラグ アンド プレイ プロファイルの作成 （844 ページ）
ルータおよびスイッチのプラグ アンド プレイ プロファイルの作成 （845 ページ）
Nexus プラグアンドプレイ プロファイルへのデバイスプロファイルの追加 （857 ページ）
ワイヤレス AP プラグアンドプレイ プロファイルへのデバイス プロファイルの追加 （856 ページ）

デバイス プロファイルのエクスポート、編集、およびプラグ アンド プレイ プロファイルへのインポート

デバイスプロファイルでインポートとエクスポートの処理を一括で実行できます。デバイスを1つずつ追加して属性を指定する代わりに、すべてのデバイスと属性を含むCSVファイルをインポートできます。一括でインポートすると、既存のプロファイルを更新し、新しいプロファイルを追加できます。複数のデバイス プロファイルを一度に更新するには、一括でエクスポートすることができます。

ステップ 1 **[設定（Configuration）] > [プラグ アンド プレイ（Plug and Play）] > [ダッシュボード（Dashboard）]** を選択し、[ホーム（Home）] タブで [PnP プロファイル（PnP Profiles）] をクリックします。

ステップ 2 左側のナビゲーション メニューから必要なプラグ アンド プレイ プロファイルを選択します。[プロファイルの概要（Profile Summary）] タブに詳細が表示されます。

ステップ 3 [プロファイル インスタンス（Profile Instances）] タブをクリックします。

ステップ 4 編集するデバイスプロファイルチェックボックスを選択し、[エクスポート（Export）]をクリックします。

デバイス プロパティ付きの CSV ファイルがエクスポートされます。エクスポートされた CSV ファイルには、設定情報は含まれません。.スプレッドシートでは、デバイスを追加したり、既存のデバイスのプロパティを編集できます。スプレッドシートの編集時に属性名を変更しないでください。

Mobility Express WLC のプロファイルとしては、デバイスのシリアル番号または MAC アドレスのいずれかを入力できます。

（注） 空白の CSV ファイルをエクスポートする場合は、デバイス プロファイルを選択せずに [エクスポート（Export）] をクリックします。[プロファイルインスタンス（Profile Instances）] ページにデバイス プロファイルがなくても、空白の CSV ファイルがエクスポートされます。

ステップ 5 [インポート（Import）] をクリックし、デバイスの詳細を入力した CSV ファイルを選択します。[アップロード（Upload）] をクリックします。

CSV ファイルをアップロードすると、**[管理（Administration）] > [ダッシュボード（Dashboard）] > [ジョブ ダッシュボード（Jobs Dashboard）]** へのリンクが表示されます。

ステップ 6 [ジョブダッシュボード（Jobs Dashboard）] ページで、左側のナビゲーション メニューから [PnP一括インポート（PnP Bulk Import）]をクリックし、一括でインポートしたファイルのジョブ ステータスを表示します。

関連トピック

ルータおよびスイッチのプラグ アンド プレイ プロファイルの作成 （845 ページ）
Nexus プラグ アンド プレイ プロファイルへのデバイス プロファイルの追加 （857 ページ）
ワイヤレス AP プラグ アンド プレイ プロファイルへのデバイス プロファイルの追加 （856 ページ）
デバイス タイプに基づく展開 （855 ページ）

デバイス タイプに基づく展開

デバイス タイプに基づいてプラグ アンド プレイ プロファイルを展開するには、デバイス ID を展開プロファイルに関連付ける必要はありません。デバイス タイプに基づく展開は、主に、同じイメージと設定のセットを使用するスイッチに対して有用です。一致するプロファイルは、設計段階でプロファイルで指定された入力デバイスのタイプ（PID）によって識別されます。

デバイス タイプに基づく展開時：

1. デバイス タイプは階層的に照合されます。Cisco Prime Infrastructure は入力デバイスと同じデバイス タイプのプロファイルを検索します。プロファイルがデバイス タイプに一致しない場合、Cisco Prime Infrastructure は、階層のより上位のデバイス タイプに対して定義されているプロファイルを検索します。次に例を示します。

   - Cisco Prime Infrastructure で [Switches and Hubs] に対して 「switch_profile」 が定義されており、入力デバイスのタイプが [Switches and Hubs] > [Catalyst 2928 Series Switches] > [Catalyst 2928-24TC-C switch] である場合、および

- このスイッチ（Catalyst 2928-24TC-C または Catalyst 2928 シリーズ スイッチ）に対してプロファイルが明確に定義されていない場合は、展開において「switch_profile」が考慮されます。

2. 特定のデバイスのタイプに一致する複数の展開プロファイルが Cisco Prime Infrastructure に存在する場合、Cisco Prime Infrastructure は、作成された展開プロファイルまたは最近更新された展開プロファイルを選択します。

関連トピック

デバイス プロファイルのエクスポート、編集、およびプラグ アンド プレイ プロファイルへのインポート （854 ページ）

ワイヤレス AP プラグ アンド プレイ プロファイルへのデバイス プロファイルの追加

Cisco Prime Infrastructure は、ワイヤレス AP プロファイルの APIC-EM のみをサポートします。デバイスでプロビジョニングする必要がある、プライマリ、セカンダリ、およびターシャリ WLC の詳細を決定するプラグ アンド プレイ プロファイルを事前に設定する必要があります。ワイヤレス AP のプラグ アンド プレイ プロファイルの作成 （847 ページ）を参照してください。

AP（アクセスポイント）をネットワークに接続すると、AP はネットワークの DHCP に接続して APIC-EM の詳細を確認します。次に AP は APIC-EM に接続し、デバイスのシリアル番号および PID に基づいてプロファイルを一致させます。AP は、デバイスにイメージと設定をプッシュする WLC に接続します。

必要なプラグ アンド プレイ プロファイルにデバイス プロファイルを追加するには、次の手順を実行します。

ステップ 1 [プラグ アンド プレイ デバイスのプロビジョニング プロファイル（Plug and Play Device Provisioning Profile）] ページに必要な情報を入力します。

[ロケーション（Location）] ドロップダウン リストから、デバイスをマッピングする設置ロケーションを選択します。この詳細は [マップ（Map）] ビューに表示されます。

（注） 特定のロケーションにデバイスを追加する前に、**[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ネットワークデバイス（Network Devices）]** または **[インベントリ（Inventory）] > [グループ管理（Group Management）] > [ネットワークデバイスグループ（Network Device Groups）]** でロケーション グループを作成します。「ロケーション グループの作成」を参照してください。

ステップ 2 [プロファイル有効化サマリー（Profile Activation Summary）] ページでは、設定されたデバイスの詳細が表示されます。

ステップ 3 [終了（Finish）] をクリックし、デバイス プロファイルをプロビジョニングします。

プロビジョニングに成功すると、デバイス プロファイルが特定のプロファイルの [プロファイルインスタンス（Profile Instances）] ページ表示されます。また、デバイスのプロビジョニング ステータスは [デバイスのステータス（Device Status）] ページに表示されます。

関連トピック

デバイスとプラグ アンド プレイ プロファイルの関連付け （850 ページ）
デバイスの展開を定義するプラグ アンド プレイ プロファイルの作成 （844 ページ）
ワイヤレス AP のプラグ アンド プレイ プロファイルの作成 （847 ページ）
ルータとスイッチのプラグ アンド プレイ プロファイルへのデバイス プロファイルの追加 （853 ページ）
Nexus プラグ アンド プレイ プロファイルへのデバイス プロファイルの追加 （857 ページ）

Nexus プラグ アンド プレイ プロファイルへのデバイス プロファイルの追加

始める前に、満たすべき一連の前提条件があります。Nexus デバイスでプラグ アンド プレイを使用するための前提条件 （840 ページ）を参照してください。

Nexus デバイスをネットワークに接続する場合は、次のワークフローに従います。

1. 設定済み DHCP サーバを特定して通信を確立し、IP アドレス、ゲートウェイ、スクリプト サーバ（Prime Infrastructure 3.2）、およびスクリプト ファイル（Nexus プラグ アンド プレイ プロファイル）を取得します。
2. 次に、デバイスは Prime Infrastructure と通信し、Nexus デバイスの作成済みプラグ アンド プレイ プロファイルをダウンロードします。Nexus デバイスのプラグ アンド プレイ プロファイルの作成 （848 ページ）を参照してください。
3. さらに、デバイスは、イメージと必要な設定ファイルをダウンロードする TFTP サーバの IP アドレス、または HTTP サーバの URL を取得します。

必要なプラグ アンド プレイ プロファイルにデバイス プロファイルを追加するには、次の手順を実行します。

ステップ 1 [プラグ アンド プレイ デバイスのプロビジョニング プロファイル（Plug and Play Device Provisioning Profile）] ページに必要な情報を入力します。

[ロケーション（Location）] ドロップダウン リストから、デバイスをマッピングする設置ロケーションを選択します。この詳細は [マップ（Map）] ビューに表示されます。

（注） 特定のロケーションにデバイスを追加する前に、**[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ネットワークデバイス（Network Devices）]** または **[インベントリ（Inventory）] > [グループ管理（Group Management）] > [ネットワークデバイスグループ（Network Device Groups）]** でロケーション グループを作成します。ロケーション グループの作成 （68 ページ）を参照してください。

ステップ 2 右側の矢印アイコンをクリックし、[イメージ選択（Image Selection）] ページに移動します。

選択したシステムとキック スタートのイメージが自動的に入力されますが、編集することはできません。

ステップ 3 右側の矢印アイコンをクリックし、[設定（Configuration）] ページに移動します。

プロファイルの作成段階に選択した設定テンプレートは自動的に入力されます。管理インターフェイス IP アドレス、管理ルート IP アドレス、およびその他の必要な情報を入力する必要があります。この管理 IP アドレスは、Nexus デバイスに到達できるように設定されます。

[CLI] をクリックし、CLI のサマリーを表示します。

ステップ 4 右側の矢印アイコンをクリックし、[管理クレデンシャル（Management Credentials）] に移動します。

Nexus デバイスの場合、デバイスが管理できるように [管理IPアドレス（Management IP Address）] の指定が必須です。その他の必要な情報を入力し、次のページに移動します。これらのデバイスのパラメータは、プロビジョニング時にデバイスに適用されます。

ステップ 5 [プロファイル有効化サマリー（Profile Activation Summary）] ページでは、設定されたデバイスの詳細が表示されます。

ステップ 6 [終了（Finish）] をクリックし、デバイス プロファイルをプロビジョニングします。

プロビジョニングに成功すると、デバイス プロファイルが特定のプロファイルの [プロファイルインスタンス（Profile Instances）] ページ表示されます。また、デバイスのプロビジョニング ステータスは [デバイス ステータス（Device Status）] ページに表示されます。デバイスを管理できるように、デバイスを Prime Infrastructure のインベントリに追加します。

関連トピック

[プラグアンドプレイ（Plug and Play）] ダッシュボードを使用した新しいデバイス展開のモニタ （838 ページ）
デバイスの展開を定義するプラグ アンド プレイ プロファイルの作成 （844 ページ）
Nexus デバイスでプラグ アンド プレイを使用するための前提条件 （840 ページ）
Nexus デバイスのプラグ アンド プレイ プロファイルの作成 （848 ページ）
ルータとスイッチのプラグ アンド プレイ プロファイルへのデバイス プロファイルの追加 （853 ページ）
ワイヤレス AP プラグアンドプレイ プロファイルへのデバイス プロファイルの追加 （856 ページ）

Mobility Express WLC プラグ アンド プレイ プロファイル インスタンスへのデバイス プロファイルの追加

[Mobility Express（ME）WLCプラグアンドプレイプロファイル（Mobility Express (ME) WLC Plug and Play Profiles）] ページにある [プロファイルインスタンス（Profile Instances）] タブで [追加（Add）] アイコンをクリックし、[プロファイルの有効化（Profile Activation）] ページに進みます。

ME APデバイスは、DHCPサーバからIPアドレスを取得する必要があります。管理IPは、ME AP で設定されている IP アドレスとは異なっている必要があります。DHCP IP と管理 IP は、同じサブネット上にある必要があります。

ステップ 1 [プロファイルの有効化（Profile Activation）]ページで、[プラグアンドプレイデバイスのプロビジョニング プロファイル（Plug and Play Device Provisioning Profile）] タブに必要な情報を入力します。

ステップ 2 [設定（Configuration）] タブをクリックします。

プロファイルの作成段階に選択した設定テンプレートは自動的に入力されます。インターフェイスIPアドレスなど、必要な情報を入力する必要があります。

プロファイルの作成中に Mobility Express デイ ゼロ設定テンプレートを選択していた場合、ME AP を ME WLC に変換するのに役立ちます。

[CLI] をクリックし、CLI のサマリーを表示します。

（注） この [設定（Configuration）] タブは、プロファイルの作成中に設定テンプレートを選択しなかった場合は表示されません。デバイスのraw設定をインポートする場合は、[プロファイルインスタンス（Profile Instances）] タブにある [raw設定のインポート（Import Raw Config）] をクリックし、ローカル システムからコンフィギュレーション ファイルをインポートします。raw 設定は、プロファイル インスタンスが 1 つ作成されるとインポートできるようになります。raw 設定ファイルの名前がデバイスのシリアル番号またはベース イーサネット MAC アドレスと同じであることを確認します。MAC アドレスをファイルの名前として指定する場合は、必ず「:」記号の代わりに「-」記号を指定してください。

ステップ 3 [管理クレデンシャル（Management Credentials）] タブをクリックします。

管理 IP アドレスは、事前ロード済みのコンフィギュレーション ファイルを選択している場合は [設定（Configuration）] タブから編集不可の状態で自動入力されます。自動入力されない場合は、デバイスが Prime Infrastructure インベントリに追加されるよう、管理 IP アドレスを入力する必要があります。SNMP パラメータおよび CLI パラメータを入力します。これらのパラメータは、デバイスにプッシュされる追加コマンドとして追加されます。

ステップ 4 [プロファイル有効化サマリー（Profile Activation Summary）] ページでは、設定されたデバイスの詳細が表示されます。

ステップ 5 [終了（Finish）] をクリックし、デバイス プロファイルをプロビジョニングします。

プロビジョニングに成功すると、デバイス プロファイルが特定のプロファイルの [プロファイルインスタンス（Profile Instances）] ページ表示されます。また、デバイスのプロビジョニング ステータスは [デバイス ステータス（Device Status）] ページに表示されます。イメージのアップグレード状態を確認するには、[Post PNPステータス（Post PNP Status）]の横にある情報アイコンをクリックします。デバイスを管理できるように、デバイスを Prime Infrastructure のインベントリに追加します。Mobility Express WLC が管理対象の状態になると、WLC に接続されているすべての AP がインベントリに追加されます。デバイスが管理対象の状態になると、イメージのアップグレードが開始されます。

[インフラストラクチャ（Infrastructure）] にあるシステム ジョブ [Post PnPイメージのアップグレード（Post PnP Image Upgrade）] は、Mobility Express コントローラの Post PnP 設定からオンデマンドで実行され、ソフトウェア イメージの配信と有効化を実行します。このジョブは、Mobility Express コントローラのインベントリ収集が完了すると、必要な場合のみトリガーされます。各デバイスのイメージのアップグレードの状態は、[ジョブの詳細（Job Details）] で確認できます。

プラグアンドプレイでサポートされるデバイスとソフトウェアイメージ

APIC-EM を使用している場合、Prime Infrastructure プラグ アンド プレイは APIC-EM によってサポートされているデバイスのみをサポートします。

APIC-EM でサポートされているデバイスおよび対応するソフトウェア イメージについては、Cisco Network Plug and Play のリリース ノートを参照してください。

サポートされているすべてのデバイスおよび対応する sysObjectID については、Cisco Prime Infrastructure サポート対象デバイスを参照してください。

関連トピック

デバイスの展開を定義するプラグ アンド プレイ プロファイルの作成 （844 ページ）
プラグ アンド プレイのワークフロー （836 ページ）

デバイスにブートストラップコンフィギュレーションを展開するための前提条件

ブートストラップ コンフィギュレーションを Cisco Prime Infrastructure サーバのデバイスに展開するには、次の手順を実行します。

- 次のコマンドを入力して、サーバの Cipher in Admin モードを有効にします。

ncs run pnp-ciphers enable

- **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** ページの [HTTP転送（HTTP Forward）] セクションで、[有効化（Enable）] をクリックします。
- ブートストラップ コンフィギュレーションや PIN を電子メールを使用して配信する場合は、**[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] > [メールサーバ設定（Mail Server Configuration）]** で、事前にメール サーバを設定しておく必要があります。
- **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] > [サーバ（Server）]** を選択し、TFTP の [有効化（Enable）] をクリックして、Cisco Prime Infrastructure サーバで TFTP が有効になっていることを確認します。TFTP はデフォルトで有効になっています。

関連トピック

プラグアンドプレイ用のブートストラップ コンフィギュレーションの作成（861 ページ）

プラグアンドプレイ用のブートストラップコンフィギュレーションの作成

ブートストラップ コンフィギュレーションは、デバイスが Prime Infrastructure ゲートウェイ（APIC-EM）との接続を確立するために必要な最小限の設定です。Prime Infrastructure は、使用可能な標準ブートストラップ設定を提供します。

DHCP オプションを使用する場合は、ブートストラップ コンフィギュレーションを作成する必要はありません。DHCP を使用したブートストラップ コンフィギュレーションのエクスポート（867 ページ）を参照してください。

ユーザ定義ブートストラップ テンプレートを作成するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [プラグ アンド プレイ（Plug and Play）] > [ダッシュボード（Dashboard）]** を選択し、[ホーム（Home）] タブで [ブートストラップ（Bootstrap）] をクリックします。

デフォルトでは、APIC ブートストラップおよびプラグアンドプレイ ブートストラップ テンプレートが表示されます。これらのテンプレートは削除できません。

ステップ 2 特定のブートストラップ チェックボックスを選択し、[複製（Clone）] をクリックして同様のテンプレートを複製します。この新しいテンプレートは、複製したブートストラップに応じて、APIC Bootstrap_1、APIC Bootstrap_1_1、Plug and Play Bootstrap_1、Plug and Play Bootstrap_1_1 などと表示されます。

（注）
- 複製したテンプレートの名前を変更することができます。名前を変更すると、テンプレート名を再び変更することはできません。
- カスタマイズしたブートストラップ テンプレートの作成に [設定（Configuration）] > [テンプレート（Templates）] > [機能およびテクノロジー（Features & Technologies）] > [CLI テンプレート（CLI Templates）] > [システム テンプレート-CLI（System Templates-CLI）]> [プラグ アンド プレイ ブートストラップ（Plug And Play Bootstrap）] を使用しないでください。

ステップ 3 [保存（Save）] をクリックします。

ステップ 4 ブートストラップ テンプレートの横にあるポインタをクリックし、詳細を表示または編集します。

ステップ 5 [更新（Update）] をクリックして変更を保存します。[CLI] をクリックし、CLI のサマリーを表示します。

ステップ 6 ブートストラップ テンプレートを削除するには、特定のブートストラップ テンプレートを選択して [削除（Delete）] をクリックします。

作成するこれらのテンプレートは、[PnP ブートストラップ テンプレート（ユーザ定義）（PnP Bootstrap Templates (User Defined)）] に保存されます。

プロファイル インスタンスの新たに作成したこのブートストラップ テンプレートは、プロファイル インスタンスの追加時に [PnP ブートストラップ テンプレート（ユーザ定義）（PnP Bootstrap Templates (User

Defined)）]から特定のブートストラップテンプレートを選択することで選択できます。詳細は自動的に表示され、編集することができます。

Prime Infrastructure が提供するブートストラップ設定の内容は次のとおりです。

- APIC-EM HTTP ブートストラップ

```
pnp profile network-pnp
transport http ipv4 <APIC-EM server IP>
```

- APIC-EM HTTPS ブートストラップ

```
crypto ca trustpoint <APIC-EM Server IP>.cisco.com
enrollment mode ra
enrollment terminal
usage ssl-client
exit
crypto ca authenticate <APIC-EM Server IP>.cisco.com
-----BEGIN CERTIFICATE-----
Certificate detail
-----END CERTIFICATE-----
pnp profile network-pnp
transport https ipv4 <APIC-EM Server IP> port 443
!
```

関連トピック

ブートストラップ コンフィギュレーションをインストールする方法 （862 ページ）
[プラグアンドプレイ（Plug and Play）] ダッシュボードを使用した新しいデバイス展開のモニタ （838 ページ）
デバイスの展開を定義するプラグ アンド プレイ プロファイルの作成 （844 ページ）
デバイスとプラグ アンド プレイ プロファイルの関連付け （850 ページ）
デバイスにブートストラップ コンフィギュレーションを展開するための前提条件 （860 ページ）

ブートストラップコンフィギュレーションをインストールする方法

ブートストラップ コンフィギュレーションは、デバイスが Cisco Prime Infrastructure ゲートウェイ（APIC-EM）との接続を確立するために必要な最小限の設定です。Cisco Prime Infrastructure がサポートしているブートストラップ配布方法のいずれかを使用して、ブートストラップ コンフィギュレーションをデバイスにインストールできます。

- ブートストラップをエクスポートしてダウンロードする：デバイス コンソールへのアクセス権限がある場合は、ブートストラップをエクスポートし、ブートストラップ コンフィギュレーションをデバイスにコピー アンド ペーストできます。エクスポートを参照してください。

- ターミナル サーバを介したブートストラップ コンフィギュレーションの展開。関連項目の「ターミナル サーバを使用したブートストラップ コンフィギュレーションの展開」を参照してください。
- USB フラッシュ ドライブにブートストラップをエクスポートして保存する：*ciscortr.cfg* というファイル名でブートストラップ コンフィギュレーションを USB ドライブに保存できます。USB ドライブをデバイスに接続して、デバイスをブートします。デバイスは USB ドライブからブートストラップ コンフィギュレーションを取得します。関連項目の「TFTP を使用したブートストラップ コンフィギュレーションのエクスポート」を参照してください。
- ブートストラップを電子メールで送信する。関連項目の「電子メール ブートストラップ コンフィギュレーション」を参照してください。
- 指定されたサーバに基づく DHCP オプション。関連項目の「DHCP を使用したブートストラップ コンフィギュレーションのエクスポート」を参照してください。
  - [DHCP設定（DHCP Configuration）] の下で APIC-EM サーバ IP に DHCP オプション 43 を設定できます。デバイスは DHCP から IP アドレスを取得するときに、ブートストラップ コンフィギュレーションも取得します。
- モバイル アプリケーション：Cisco Network Plug and Play モバイル アプリケーションを使用できます。

関連トピック

デバイスにブートストラップ コンフィギュレーションを展開するための前提条件 （860 ページ）
プラグアンドプレイ用のブートストラップ コンフィギュレーションの作成 （861 ページ）
ターミナルサーバを使用したブートストラップ コンフィギュレーションの展開 （864 ページ）
ブートストラップ コンフィギュレーションのエクスポート （863 ページ）
DHCP を使用したブートストラップ コンフィギュレーションのエクスポート （867 ページ）
TFTP によるブートストラップ コンフィギュレーションのエクスポート （864 ページ）
電子メール ブートストラップ コンフィギュレーション （865 ページ）

ブートストラップ コンフィギュレーションのエクスポート

ブートストラップ コンフィギュレーションをエクスポートして、手動でデバイスにブートストラップを適用できます。ブートストラップ コンフィギュレーションが適用された後、プラグアンド プレイの展開が開始され、管理者は Prime Infrastructure 上の設定ステータスを表示できます。

ステップ 1 **[設定（Configuration）]** > **[プラグ アンド プレイ（Plug and Play）]** > **[ダッシュボード（Dashboard）]** を選択し、[ホーム（Home）] タブで [PnP プロファイル（PnP Profiles）] をクリックします。

ステップ 2 [プラグ アンド プレイ プロファイル（Plug and Play Profiles）] ページで、リストからプロファイルを選択します。

ステップ 3 [プロファイル インスタンス（Profile Instances）] をクリックします。

ステップ 4 [ブートストラップのエクスポート（Export Bootstrap）] > [ブートストラップのダウンロード（Download Bootstrap）] をクリックし、[OK] をクリックします。

ステップ 5 ブートストラップ コンフィギュレーションがダウンロードされ適用された後、プラグ アンド プレイ導入が開始されます。

関連トピック

TFTP によるブートストラップ コンフィギュレーションのエクスポート （864 ページ）
電子メール ブートストラップ コンフィギュレーション （865 ページ）
DHCP を使用したブートストラップ コンフィギュレーションのエクスポート （867 ページ）
プラグ アンド プレイ用のブートストラップ コンフィギュレーションの作成（861 ページ）

ターミナルサーバを使用したブートストラップコンフィギュレーションの展開

プラグ アンド プレイ プロファイルの作成時に [ターミナル サーバの有効化（Enable Terminal Server）] チェックボックスをオンにすると、次のようにブートストラップ コンフィギュレーションを展開できます。

ステップ 1 プラグ アンド プレイ プロファイルからデバイスを選択します。

ステップ 2 [展開（Deploy）] ボタンをクリックします。

ステップ 3 ポップアップ ダイアログボックスの [OK] をクリックして、ジョブをトリガーし、ターミナル サーバを使用してデバイスにブートストラップを直接実行します。

[ジョブ（Job）] ダッシュボードで [PnP ターミナル サーバ（PnP Terminal Server）] のステータスを確認できます。

ジョブが正常に実行されると、APIC がデバイスをプロビジョニングします。デバイスがプロビジョニングされると、Prime Infrastructure のインベントリにデバイスが追加されます。

関連トピック

デバイスの展開を定義するプラグ アンド プレイ プロファイルの作成 （844 ページ）

TFTP によるブートストラップ コンフィギュレーションのエクスポート

TFTP プロトコルを使用して、ブートストラップ コンフィギュレーションを Prime Infrastructure TFTP サーバに配布できます。TFTP サーバに作成するファイル名を指定できます。このファイルは、自動インストール対応のデバイスが DHCP を介して IP アドレスとその他の Prime Infrastructure の詳細情報を取得するために使用されます。DHCP サーバでは、TFTP サーバを

Prime Infrastructure TFTP サーバとして設定する必要があります。詳細については、『Cisco Open Plug-n-Play Agent Configuration Guide, Cisco IOS XE Release 3E』を参照してください。

ステップ 1 **[設定（Configuration）] > [プラグアンドプレイ（Plug and Play）] > [ダッシュボード（Dashboard）]** の順に選択し、[ホーム（Home）] タブで [PnPプロファイル（PnP Profiles）] をクリックします。

ステップ 2 [プラグアンドプレイプロファイル（Plug and Play Profiles）] ページで、リストからプロファイルを選択します。

ステップ 3 [プロファイル インスタンス（Profile Instances）] をクリックします。

ステップ 4 [ブートストラップをエクスポート（Export Bootstrap）] > [TFTP] をクリックします。

ステップ 5 ブートストラップ コンフィギュレーションがダウンロードされ適用された後、プラグ アンド プレイ導入が開始されます。

関連トピック

電子メール ブートストラップ コンフィギュレーション （865 ページ）
プラグアンドプレイ用のブートストラップ コンフィギュレーションの作成 （861 ページ）
DHCP を使用したブートストラップ コンフィギュレーションのエクスポート （867 ページ）

電子メール ブートストラップ コンフィギュレーション

ブートストラップ コンフィギュレーションを電子メールで送信し、手動でデバイスにブートストラップを適用できます。ブートストラップ設定が適用された後、自動導入が開始されます。管理者は Prime Infrastructure で設定ステータスを表示できます。

（注） ブートストラップ コンフィギュレーションを電子メールで送信する前に、**[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] > [メールと通知（Mail and Notification）] > [メール サーバ設定（Mail Server Configuration）]** で電子メールを設定する必要があります。

オペレータにブートストラップ コンフィギュレーションをメール送信するには：

ステップ 1 **[設定（Configuration）] > [プラグアンドプレイ（Plug and Play）] > [ダッシュボード（Dashboard）]** の順に選択し、[ホーム（Home）] タブで [PnPプロファイル（PnP Profiles）] をクリックします。

ステップ 2 [プラグアンドプレイプロファイル（Plug and Play Profiles）] ページで、リストからプロファイルを選択します。

ステップ 3 [プロファイル インスタンス（Profile Instances）] をクリックします。

ステップ 4 [ブートストラップをエクスポート（Export Bootstrap）] > [ブートストラップをダウンロード（Download Bootstrap）] をクリックします。

ステップ 5 ブートストラップ コンフィギュレーションの送信先メールアドレスを入力し、[OK] をクリックします。

ステップ 6 ブートストラップ コンフィギュレーションがダウンロードされ適用された後、プラグ アンド プレイ導入が開始されます。

関連トピック

プラグアンドプレイ用のブートストラップ コンフィギュレーションの作成（861 ページ）
DHCP を使用したブートストラップ コンフィギュレーションのエクスポート（867 ページ）
ブートストラップ コンフィギュレーションのエクスポート（863 ページ）
TFTP によるブートストラップ コンフィギュレーションのエクスポート（864 ページ）

ブートストラップ コンフィギュレーションの PIN のメール送信

Prime Infrastructure は、デバイスごとにランダムな個人識別番号（PIN）を生成します。この PIN を使用して、PIN に関連付けられているデバイスとプラグ アンド プレイ プロファイル（ブートストラップ コンフィギュレーション）を識別できます。事前プロビジョニング タスクが完了したら、管理者は、[PIN を電子メールで送信（Email PIN）] オプション（Prime Infrastructure の事前プロビジョニング タスクで使用可能）を使用して、展開エンジニアに一意の PIN をメール送信する必要があります。インストール時、展開エンジニアはこの PIN を使用して、サーバからブートストラップ コンフィギュレーションをダウンロードします。

ブートストラップ コンフィギュレーションの PIN を配信するには：

ステップ 1 **[設定（Configuration）] > [プラグ アンド プレイ（Plug and Play）] > [ダッシュボード（Dashboard）]** の順に選択し、[ホーム（Home）] タブで [PnP プロファイル（PnP Profiles）] をクリックします。

ステップ 2 [プラグ アンド プレイ プロファイル（Plug and Play Profiles）] ページで、リストからプロファイルを選択します。

ステップ 3 [プロファイル インスタンス（Profile Instances）] タブをクリックします。

ステップ 4 [PIN を電子メールで送信（Email PIN）] をクリックします。

ステップ 5 PIN の送信先電子メール アドレスを指定し、[OK] をクリックします。

ステップ 6 次のいずれかの方法でブートストラップ コンフィギュレーションを適用します。

- 展開アプリケーションを使用してブートストラップ コンフィギュレーションを適用する場合は、Prime Infrastructure プラグ アンド プレイ展開アプリケーションが Prime Infrastructure と通信して、デバイスにブートストラップ コンフィギュレーションを適用します。
- PIN を使用して手動でブートストラップ コンフィギュレーションを適用する場合は、以下を実行します。
  - PIN を使用して、Prime Infrastructure プラグ アンド プレイ ゲートウェイ（https://%3Cpnp-gateway-server%3E/cns/PnpBootstrap.html）からブートストラップ コンフィギュレーションをダウンロードします。このプロセス中に ISR のシリアル番号も登録できます。
  - コンソールまたは USB フラッシュを使用して、手動でブートストラップ コンフィギュレーションをデバイスに適用します。

プラグ アンド プレイの展開の詳細については、『Cisco Plug and Play Application User Guide』を参照してください。

ステップ 7 ブートストラップ コンフィギュレーションが適用された後、プラグ アンド プレイの展開が開始されます。

関連トピック

電子メール ブートストラップ コンフィギュレーション （865 ページ）
プラグアンドプレイ用のブートストラップ コンフィギュレーションの作成 （861 ページ）
DHCP を使用したブートストラップ コンフィギュレーションのエクスポート （867 ページ）
ブートストラップ コンフィギュレーションのエクスポート （863 ページ）
TFTP によるブートストラップ コンフィギュレーションのエクスポート （864 ページ）

DHCP を使用したブートストラップ コンフィギュレーションのエクスポート

DHCP オプションを使用してブートストラップ コンフィギュレーションをエクスポートするには、デバイスで以下の設定を行う必要があります。

- APIC-EM の場合：DHCP オプション 43

```
ip dhcp pool <DHCP pool name>
network <subnet> <subnet mask>
default-router <default gateway>
option 43 ascii "5A1D;B2;K4;I<APIC-EM_server_IP>;J80"
```

関連トピック

ブートストラップ コンフィギュレーションのエクスポート （863 ページ）
サンプル DHCP サーバ設定 （867 ページ）
[プラグアンドプレイ（Plug and Play）] ダッシュボードを使用した新しいデバイス展開のモニタ （838 ページ）
デバイスの展開を定義するプラグ アンド プレイ プロファイルの作成 （844 ページ）
プラグアンドプレイ用のブートストラップ コンフィギュレーションの作成 （861 ページ）
ブートストラップ コンフィギュレーションをインストールする方法 （862 ページ）

サンプル DHCP サーバ設定

DHCP ベースの方式を選択してプラグ アンド プレイ プロファイルを配信する場合は、次の表で説明されているコマンドを入力して、スイッチを TFTP サーバにリダイレクトするように DHCP サーバを設定する必要があります。

DHCP ベースの方式は、次の手順で実行されます。

1. 新しいスイッチが DHCP サーバと通信します。スイッチを TFTP サーバにリダイレクトするように DHCP サーバを設定する必要があります。詳細については、以下の表を参照してください。

2. DHCP サーバは、スイッチをプラグ アンド プレイ ブートストラップ プロファイルがある新しい TFTP サーバに向けます。
3. スイッチはブートストラップ コンフィギュレーション ファイルをロードして起動し、プラグ アンド プレイ ゲートウェイにアクセスします。

表 *53 : DHCP* サーバの設定項目

入力するコマンド	説明
`ip dhcp pool PNP`	PNP という名前の DHCP プールを作成します。
`network 10.106.190.0 255.255.255.224`	ネットワーク 10.106.190.0 とサブネット マスク 255.255.255.224 を定義します。DHCP はこの IP アドレス プールを使用して、新しいデバイスに IP アドレスを割り当てます。
`default-router 10.106.190.17`	新しいデバイスにデフォルト ルート 10.106.190.17 を設定します。
`option 150 ip 10.77.240.224`	TFTP サーバの IP アドレス 10.77.240.224 が Cisco Prime Infrastructure サーバの IP アドレスであることを指定します。

関連トピック

ブートストラップ コンフィギュレーションのエクスポート （863 ページ）
DHCP を使用したブートストラップ コンフィギュレーションのエクスポート （867 ページ）
[プラグアンドプレイ（Plug and Play）] ダッシュボードを使用した新しいデバイス展開のモニタ （838 ページ）
デバイスの展開を定義するプラグ アンド プレイ プロファイルの作成 （844 ページ）
プラグアンドプレイ用のブートストラップコンフィギュレーションの作成 （861 ページ）
ブートストラップ コンフィギュレーションをインストールする方法 （862 ページ）

プラグアンドプレイを使用して展開されたデバイスの確認

[設定（Configuration）] > [プラグアンドプレイ（Plug and Play）] > [ダッシュボード（Dashboard）] の順に選択し、[ホーム（Home）] タブで **[ステータス情報（Status Information）]** をクリックします。

デバイスの詳細（シリアルID、ホスト名、IPアドレス、タイプ、プロファイル名、ロケーション）、最新のプラグ アンド プレイとプラグ アンド プレイ後のステータス、プロビジョニング ステータスのグラフィック表示が、[リスト（List）] ビューに表示されます。

右上隅にある [マップ（Map）] をクリックし、デバイスの詳細とそのステータスを [マップ（Map）] ビューに表示します。関連項目を参照してください。

[管理（Administration）] > [ダッシュボード（Dashboard）] > [ジョブダッシュボード（Jobs Dashboard）] > [ユーザジョブ（User Jobs）] > [PnP後のステータス（Post PnP Status）] を選択すると、デバイスでプラグ アンド プレイ後の設定ジョブのステータスを表示できます。

リストからデバイスを選択して、[リセット（Reset）] ボタンをクリックすると、デバイス プロファイルを再びプロビジョニングできます。**[設定（Configuration）] > [プラグアンドプレイ（Plug and Play）] > [ダッシュボード（Dashboard）] > [デバイスのステータス（Device status）]** の順に選択します。[リセット（Reset）] ボタンは、正常にプロビジョニングされたデバイスでのみ有効になります。または、プロビジョニングが失敗した場合にも有効になります。プロビジョニングのステータスが保留を示すデバイスでは有効になりません。

また、**[設定（Configuration）] > [プラグアンドプレイ（Plug and Play）] > [ダッシュボード（Dashboard）] > [プロファイル（Profiles）] > [ルータポリシー（Router Policies）]** の順に選択すると、プロファイル インスタンスのページでデバイス プロファイルをリセットすることもできます。

デバイスのリセット時、プロビジョニングのステータスは保留にリセットされます。

これよりも前にプロビジョニングが失敗している場合、Cisco Prime Infrastructure を APIC-EM GA リリース 1.2.0.x 以降のバージョンの APIC-EM と統合すると、デバイスのリセット時にデバイスが最初にリロードされます。

関連トピック

マップ ビューと [プラグアンドプレイ（Plug and Play）] ダッシュボードの統合 （869 ページ）
プラグ アンド プレイ プロファイルの削除 （871 ページ）
[プラグアンドプレイ（Plug and Play）] ダッシュボードを使用した新しいデバイス展開のモニタ （838 ページ）
デバイスの展開を定義するプラグ アンド プレイ プロファイルの作成 （844 ページ）
デバイスとプラグ アンド プレイ プロファイルの関連付け （850 ページ）
プラグアンドプレイ用のブートストラップ コンフィギュレーションの作成 （861 ページ）

マップ ビューと [プラグアンドプレイ（Plug and Play）] ダッシュボードの統合

次のいずれかの方法でマップ ビューで詳細を表示できます。

- **[設定（Configuration）] > [プラグアンドプレイ（Plug and Play）] > [ダッシュボード（Dashboard）]** の順に選択し、[モニタリング（Monitoring）] タブをクリックします。
- **[設定（Configuration）] > [プラグアンドプレイ（Plug and Play）] > [ダッシュボード（Dashboard）]** の順に選択し、[ホーム（Home）] タブをクリックします。[デバイスのステータス（Device Status）] ページの右上隅から [ステータス情報（Status Information）] および [マップ（Map）] をクリックします。
- **[設定（Configuration）] > [プラグアンドプレイ（Plug and Play）] > [ダッシュボード（Dashboard）]** の順に選択し、[ホーム（Home）] タブをクリックします。[ロケーション（Locations）] をクリックします。

1	クリックすると、全画面でマップが表示されます。
2	マウスまたはキーボードを使用してズーム操作を実行できます。キーボードでは、[+] または [-] 記号を押してズームインまたはズームアウトします。マウスの場合は、マウスのスクロール ホイールを使用してズームインまたはズームアウトします。または、ダブルクリックしてズームインします。
3	クリックすると、デバイスのプロビジョニング ステータスが詳細に表示されます。
4	クリックすると、地理座標が指定されていない場所が表示されます。
5	クリックすると、どのロケーションにもマッピングされていないデバイスが表示されます。マップ内のロケーションにデバイスをドラッグ アンド ドロップします。デバイスがこのロケーション グループに自動的にマッピングされます。
[6]	ボタンを切り替えると、編集モードが有効になります。有効になると、マップ内のロケーションにマッピングされていないデバイスをドラッグ アンド ドロップできます。ロケーションにデバイスをマッピングする前に、ロケーション グループを作成します。ロケーション グループの作成 （68 ページ）を参照してください。
7	リストからロケーションを選択します。
8	クリックすると、クラスタの詳細が表示されます。クラスタは、地理的領域内の複数のロケーションを表します。この場所にマウスを重ねると、マッピングされているデバイスの数が表示されます。ハイパーリンクの番号をクリックすると、デバイスの詳細が表示されます。
9	リストをクリックすると、[デバイスのステータス（Device status）] ページが表示されます。

関連トピック

プラグ アンド プレイを使用して展開されたデバイスの確認 （868 ページ）

プラグ アンド プレイ プロファイルの削除 （871 ページ）
[プラグアンドプレイ（Plug and Play）] ダッシュボードを使用した新しいデバイス展開のモニタ （838 ページ）
デバイスの展開を定義するプラグ アンド プレイ プロファイルの作成 （844 ページ）
デバイスとプラグ アンド プレイ プロファイルの関連付け （850 ページ）
プラグアンドプレイ用のブートストラップ コンフィギュレーションの作成 （861 ページ）

プラグ アンド プレイ プロファイルの削除

プラグ アンド プレイに APIC-EM を使用している場合は、不適切なまたは古いプラグ アンド プレイ プロファイルの削除が必要になることがあります。

（注）

- Prime Infrastructure プラグ アンド プレイからデバイスを削除すると APIC-EM からそのデバイスが削除されるのに対し、APIC-EM からデバイスを削除しても Prime Infrastructure にはそのデバイスが残ります。
- APIC-EM が Prime Infrastructure と統合されている場合は、APIC-EM にプロファイルを作成しないでください。
- プラグ アンド プレイからデバイスを削除した場合は、その後すぐにそのデバイスをプラグ アンド プレイに追加できます。

ステップ 1 ルータの CLI で次のコマンドを実行して、ルータからプラグ アンド プレイ プロファイルを削除します。
no pnp profile*plug_and_play_profile_name*.

ステップ 2 **[設定（Configuration）] > [プラグ アンド プレイ（Plug and Play）] > [ダッシュボード（Dashboard）]** を選択し、[PnP プロファイル（PnP Profiles）] をクリックして、プロビジョニング プロファイルを削除します。プラグ アンド プレイ プロファイルを選択して、[プロファイル インスタンス（Profile Instances）] をクリックし、必要なプロビジョニング プロファイルを削除します。

ステップ 3 **[設定（Configuration）] > [プラグ アンド プレイ（Plug and Play）] > [ダッシュボード（Dashboard）]** を選択し、[PnP プロファイル（PnP Profiles）] をクリックします。削除するプラグ アンド プレイ プロファイルを選択し、**[削除（Delete）]** をクリックします。

（注） 統合された APIC-EM の PnP プロファイルを [プラグ アンド プレイ（Plug and Play）] ダッシュボードから削除すると、Prime Infrastructure はワイプ コマンドを APIC-EM に送信し、PnP プロファイルに関連付けられているデバイスをリセットしてプロビジョニング済みデバイスのリストから削除します。

関連トピック

プラグ アンド プレイを使用して展開されたデバイスの確認 （868 ページ）

[プラグアンドプレイ（Plug and Play）] ダッシュボードを使用した新しいデバイス展開のモニタ （838 ページ）
デバイスの展開を定義するプラグ アンド プレイ プロファイルの作成 （844 ページ）
デバイスとプラグ アンド プレイ プロファイルの関連付け （850 ページ）
プラグアンドプレイ用のブートストラップ コンフィギュレーションの作成 （861 ページ）

APIC-EM サーバで削除されたデバイスとプロファイルを取得する方法

Prime Infrastructure では、APIC-EM サーバのダウン時に誤ってシステムから削除または消去されたデバイスやプロファイルを取得できます。

Prime Infrastructure で削除されたデバイスやプロファイルを取得するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [プラグアンドプレイ（Plug and Play）] > [ダッシュボード（Dashboard）]** の順に選択し、[ホーム（Home）] タブで [プラグアンドプレイプロファイル（Plug and Play Profiles）] をクリックします。
すべてのプラグ アンド プレイ プロファイルの詳細サマリーのリストが表示されます。

ステップ 2 [プラグ アンド プレイのプロファイル（Plug and Play Profiles）] タブの [PNP から APIC EM への同期（PNP APIC EM Sync）] ボタンをクリックします。
確認を求めるプロンプトが表示されたら、[OK] をクリックし、同期を開始します。

ステップ 3 [PNP から APIC EM への同期（PNP APIC-EM Sync）] ポップアップ ウィンドウで [ジョブ ダッシュボード（Job Dashboard）] リンクをクリックして、新たにスケジュールを設定した APIC-EM の同期ジョブのステータスを表示します。
ジョブがトリガーされ、[PNP から APIC EM への同期ジョブ（PNP APIC-EM SYNC JOB）] ページで使用できるようになります

ステップ 4 プロファイル名の横にある [i] アイコンをクリックして、ジョブに関する詳細を表示します。
同期が成功すると、[new_apic_profile の同期済みデバイス（Synced Devices for new_apic_profile）] ウィンドウの [プロファイル インスタンス名（Profile Instance Name）] の横にステータスとして [成功（SUCCESS）] と表示されます。

同期が成功しなかった場合は、ステータスに [Failure（失敗）] と表示され、エラーの詳細がジョブの概要に表示されます。デバイスが削除されていない場合は、ステータスに [すでに同期済み（Already Synced）] が表示されます。

（注） [プロファイル インスタンス（Profiles Instances）] タブで [保留中（PENDING）] ステータスのデバイスのみが APIC EM で作成または同期されます。成功状態または失敗状態のデバイスは、すでに正常にプロビジョニングされているため、APIC-EM で作成/同期されず、PnP が再度必要になることはありません。

CNS プロファイルを APIC-EM プロファイルに変換する方法

Prime Infrastructure 3.2 以降、CNS でのプラグ アンド プレイのサポートは廃止されています。既存のすべての CNS プロファイルは APIC-EM プロファイルに変換できます。

（注） 次の操作を実行するには、ルート ドメイン ユーザである必要があります。それ以外の場合、操作は失敗します。

- CNS から APIC-EM への変換
- PnP CNS から APIC-EM への同期

CNS プロファイルを APIC-EM プロファイルに変換するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [プラグアンドプレイ（Plug and Play）] > [ダッシュボード（Dashboard）]** の順に選択し、[ホーム（Home）] タブで [プラグアンドプレイプロファイル（Plug and Play Profiles）] をクリックします。
すべてのプラグ アンド プレイ プロファイルの詳細サマリーのリストが表示されます。

ステップ 2 [プラグ アンド プレイのプロファイル（Plug and Play Profiles）] ページで [CNS から APIC-EM への変換（Convert CNS to APIC-EM）] ボタンをクリックします。
確認を求めるプロンプトが表示されたら [OK] をクリックし、変換を開始します。

ステップ 3 [CNS から APIC-EM への変換（Convert CNS to APIC-EM）] ポップアップ ウィンドウで [ジョブ ダッシュボード（Job Dashboard）] リンクをクリックして、新たにスケジュールを設定した APIC-EM 変換ジョブのステータスを表示します。
ジョブがトリガーされ、[PNP CNS から APIC-EM への同期ジョブ（PNP CNS TO APIC-EM SYNC JOB）] ページで使用できるようになります

ステップ 4 プロファイル名の横にある [i] アイコンをクリックして、ジョブに関する詳細を表示します。

変換が成功しなかった場合、ステータスには [失敗（Failure）] と表示され、エラーの詳細がジョブの概要に表示されます。

（注） [プロファイル インスタンス（Profiles Instances）] タブで [保留中（PENDING）] ステータスのデバイスのみが APIC EM に変換され、APIC-EM で作成されます。成功状態または失敗状態のデバイスは、成功状態にすでにプロビジョニングされているため、APIC EM で作成/同期されません。

デバイス タイプに基づいて作成された CNS プロファイルは APIC-EM に変換されません。これは、APIC-EM がデバイス タイプに基づいて作成されたプロファイルをサポートしていないためです。

第 VI 部

ネットワーク サービスの確保

- Trustsec を使用したネットワーク サービスの確保 （877 ページ）
- IWAN を使用したアプリケーション パフォーマンスの向上 （881 ページ）
- 統合アクセス導入テンプレートを使用したキャンパスおよびブランチ ネットワーク向けのデバイスの設定 （887 ページ）
- Branch Threat Defense の設定 （913 ページ）
- アクセス ネットワーク ワークフロー （917 ページ）
- Application Visibility and Control（AVC）によるアプリケーション パフォーマンスの向上 （921 ページ）
- Prime Infrastructure によって、WAN エンド ユーザの一貫したアプリケーション エクスペリエンスが確保される仕組み。 （975 ページ）
- Microsoft Lync トラフィックのモニタ （987 ページ）
- Mediatrace を使用した RTP および TCP フローのトラブルシューティング （991 ページ）
- Cisco モビリティ サービス エンジンおよびサービス （999 ページ）
- Cisco AppNav を使用した WAN の最適化 （1083 ページ）
- Cisco WAAS コンテナを使用した WAN の最適化 （1091 ページ）
- ワイヤレス モビリティの使用 （1101 ページ）

第 30 章

Trustsec を使用したネットワーク サービスの確保

- Cisco TrustSec の概要 （877 ページ）
- Trustsec 準備状況評価レポートの生成 （878 ページ）

Cisco TrustSec の概要

Cisco TrustSec テクノロジーは、ソフトウェアで定義したセグメンテーションを使用してセキュリティ ポリシーのプロビジョニングを簡素化し、セキュリティ処理を高速化して、ネットワーク全体に一貫したポリシーを適用します。TrustSec は、シスコのスイッチ、ルータ、ワイヤレス、およびセキュリティ デバイスに組み込まれているテクノロジーです。Cisco TrustSec テクノロジーは、キャンパス、ブランチ、データセンターを接続するネットワーク全体にセキュリティを拡張する、セキュアなネットワーク アーキテクチャです。TrustSec は、「エンフォーサーとしてのネットワーク」を使用する際の基盤であり、攻撃対象を減らしてリスクを軽減するとともに、運用効率を高め、コンプライアンス目標を簡単に達成できるようにします。

Cisco Prime Infrastructure では TrustSec ネットワーク サービス設計により、TrustSec 対応デバイスに 802.1X や他の TrustSec 機能を有効にする設定をプロビジョニングするための優先オプションを選択できます。TrustSec モデルベースの設定テンプレートを作成し、次のナビゲーション パスのいずれかを選択して、有線の 802_1x デバイスを設定できます。

- **[サービス（Services）] > [TrustSec]**
- **[設定（Configuration）] > [テンプレート（Templates）] > [機能およびテクノロジー（Features & Technologies）] > [セキュリティ（Security）] > [TrustSec] > [有線 802_1x（Wired 802_1x）]**

（注） TrustSec 5.3 プラットフォームのサポート リストについては、『Cisco TrustSec Release 5.3 System Bulletin』を参照してください。

TrustSec モデルベースの設定テンプレートの設定に関する詳細については、「既存のテンプレートを使用した新機能およびテクノロジーテンプレートの作成（505 ページ）」を参照してください。

関連トピック

Trustsec 準備状況評価レポートの生成 （878 ページ）

Trustsec 準備状況評価レポートの生成

TrustSec 準備状況の評価には、TrustSec 機能分類などの TrustSec ベースのデバイスの詳細が表示されます。

デバイスの分類は次のように行われます。

- 分類とは、ID またはコンテキストに応じてセキュリティ グループ タグを割り当てるプロセスです（802.1x、MAB、Web 認証を使用して動的に、または IP、サブネット、VLAN、インターフェイスに静的にマッピング）。これらのセキュリティ グループ タグは、インラインのタグ付けまたはセキュリティ グループ タグ交換プロトコル（SXP）を使用してデバイスに送信されます。
- 適用とは、セキュリティ グループ ACL（スイッチとルータ上の SGACL）またはセキュリティ グループ ファイアウォール（SGFW）を経由し、セキュリティ グループ タグに応じてトラフィック ポリシーを適用するプロセスです。
- TrustSec 非対応とは、分類機能、伝播機能、または適用機能を持たないデバイスのことをいいます。

TrustSec 準備状況の評価レポートを生成するには、次の手順を実行します。

ステップ 1 [サービス（Services）] > [TrustSec] > [準備状況の評価（Readiness Assessment）] を選択します。

ステップ 2 [TrustSec 準備状況（TrustSec Readiness）] タブをクリックします。TrustSec のテーブルに、次のタイプのデバイスが表示されます。

- 分類デバイス
- 適用デバイス
- TrustSec 非対応デバイス

ステップ 3 さまざまなデバイス カテゴリをクリックし、選択した TrustSec ベースのデバイス タイプの詳細を表示します。各カテゴリは、色分けされた円を使用してデバイス数を割合で表示します。各カテゴリの色分けは次のとおりです。

分類、適用、および TrustSec 非対応デバイス：

- 赤：TrustSec 非対応デバイスの数。
- 薄い緑：分類対応デバイスの数。
- 濃い緑：適用対応デバイスの数。

ステップ 4 [表示（Show）] ドロップダウンリストから適切なフィルタを選択し、各カテゴリでデバイスをフィルタリングします。

ステップ 5 [エクスポート（Export）] アイコンをクリックし、デバイスの詳細を CSV または PDF ファイルとしてダウンロードします。

第 31 章

IWAN を使用したアプリケーション パフォーマンスの向上

- シスコ インテリジェント WAN（IWAN）の概要 （881 ページ）
- IWAN サービスをイネーブルにするための前提条件 （882 ページ）
- IWAN ウィザードを使用した IWAN サービスの設定 （884 ページ）
- IWAN（APIC-EM）を使用したデバイス上での PKI 証明書ベースの認証設定 （885 ページ）

シスコ インテリジェント WAN（IWAN）の概要

Cisco IWAN は、WAN の運用コストを削減しながら、コラボレーションおよびクラウド アプリケーションのパフォーマンスを向上させるシステムです。このシステムでは、低コストで高帯域幅のインターネット サービスを利用して、クラウドベースのアプリケーションのパフォーマンス、可用性、またはセキュリティの質を落とすことなく、帯域幅容量を向上させます。組織は IWAN を使用して、インターネットを WAN トランスポートとしてや、パブリック クラウド アプリケーションへのダイレクト アクセスのために利用できます。詳細については、『Cisco Intelligent WAN (IWAN) Design Guide』を参照してください。

Prime Infrastructure は、主に IWAN サービスを初めて有効にする必要があるグリーン フィールド顧客のために、IWAN ウィザード ワークフローを配置しています。有効になっている IWAN サービスは、ブラウンフィールドの顧客に対して変更できません。しかし、必要なサイトでこれらのサービスのいずれかを書き換えることで、顧客は最後に設定したサービスをいつでも上書きできます。

Prime Infrastructure を使用して、企業の IWAN サービスを設計、構成、およびモニタすることができます。Cisco IWAN には、異なるデバイスで IWAN サービスを有効化する一部として、DMVPN、PFR、AVC および QOS の設定が必要です。

関連トピック

IWAN サービスをイネーブルにするための前提条件 （882 ページ）
IWAN ウィザードを使用した IWAN サービスの設定 （884 ページ）

IWAN サービスをイネーブルにするための前提条件

IWAN サービスを設計または展開する場合は、構成を決定する必要があります。ネットワーク管理者は、IWAN を有効化または再設定する必要があるブランチを計画する必要があります。Cisco Prime Infrastructure では、**[設定（Configuration）] > [テンプレート（Templates）] > [機能およびテクノロジー（Features & Technologies）] > [機能テンプレート（Feature Templates）]** の順に移動して、CVD により検証済みのアウトオブボックスの IWAN テンプレートのセットにアクセスできます。この **[機能テンプレート（Feature Templates）]** フォルダの下にあるすべてのテンプレートは「IWAN」というプレフィックスがついており、ユーザーが作成した新しいテンプレートには自動的に IWAN プレフィックスが適用され、IWAN ワークフローに表示されます。

テンプレートに自動的に使用されるタグは次のとおりです。

- DMVPN：IWAN-DMVPN
- PFR：IWAN-PFR
- QOS：IWAN-QOS
- AVC：IWAN-AVC
- ZBFW: DIA_ZBFW
- CWS：DIA-CWS

（注） テンプレートに必要な最小ソフトウェア バージョンは次のとおりです。

- IWAN-DMVPN：Cisco IOS リリース 15.4 以降
- IWAN-DMVPN：Cisco IOS リリース 15.4 以降
- IWAN-QOS–Cisco IOS リリース 15.4 以降
- DIA-ZBFW–Cisco IOS リリース 15.4 以降
- WAN-AVC：「AVC とは」を参照してください
- DIA-CWS
  - Cisco Validated Design（CVD）：Cisco IOS リリース 15.2(1)T1 以降からクラウド Web セキュリティ（CWS）サービス統合型ルータ G2 プラットフォーム
  - CVD-CWS：Cisco IOS リリース 15.5(3)S1 以降からサービス統合型ルータ 4000 プラットフォーム

デバイス ロールに基づいて IWAN ハブと IWAN ブランチのカテゴリに使用されるタグは次のとおりです。

- ハブ カテゴリ：
  - マスター コントローラ：IWAN-HUB-Master-Controller

- MPLS ハブ：IWAN-HUB-MPLS
- インターネット ハブ：IWAN-HUB-Internet

- ブランチ カテゴリ：
  - 単一ルータ ブランチ：IWAN-Branch-Single-Router
  - デュアル ルータ ブランチ -MPLS：IWAN-Branch-Dual-MPLS
  - デュアル ルータ ブランチ - インターネット：IWAN-Branch-Dual-Internet

ユーザは、バンドル テンプレートから独自のテンプレートを作成するか、または、CVD テンプレートから作り直し、IWAN ワークフローに表示できるアウトオブボックスのデザインテンプレートを変更できます。

（注） ワークフローでユーザ定義の IWAN DMVPN テンプレートを使用する場合は、次のタグを使用してテンプレートを作成する必要があります。

1. IWAN-DMVPN
2. デバイス ロールとカテゴリに基づいたデバイス ロール タグ
3. IWAN ワークフローで DHCP オプションを有効/無効にするかどうかに応じて DHCP または STATIC
4. オーバーレイ プロトコルに応じて EIGRP または BGP

したがって、Cisco Prime Infrastructure を介した IWAN サービスの完全な有効化は、2 つのカテゴリ SITE および ROLE に基づいて行われます。SITE は HUB または SPOKE にすることができ、ROLE は X、Y、Z などにすることができます。この選択に応じて、テンプレートはユーザが値を入力する順に整理され表示されます。ワークフローの最後に、ネットワークに展開される設定の概要が表示されます。[Deploy] ボタンをクリックすると、設定がネットワークにプッシュされます。

特記事項

- 展開前に、インターフェイスのループバック 0 IP アドレスがすべてのマスターコントローラで設定されていることを確認します。
- マスター コントローラのループバック IP は、境界ルーターが MC に到達できるように、HUB-Border-MPLS および HUB-Border-Internet ルータの DC-LOCAL-ROUTES プレフィックス リストに許可される必要があります。

例：

```
ip prefix-list DC-LOCAL-ROUTES seq 40 permit <MC loopback0 ip>/32
```

- CVD-DMVPN-MPLS および CVD-DMVPN-Internet テンプレートの [DC_Prefix1] フィールドは、DC サブネットと一致する必要があります。DC に複数のサブネットがある場合は、サフィクス「le 32」を使用してすべてのサブネットを含めることができます。

例：

- • サブネット A：172.29.10.0/30
  • サブネット B：172.29.10.4/30
  • サブネット C：172.29.10.8/30
  • DC_Prefix1(x.x.x.x/x)：172.29.10.0/24 le 32
- CVD-DMVPN、CVD-DMVPN-Dual-Internet、および CVD-DMVPN-Dual-MPLS テンプレートでは、ループバック インターフェイスのサブネット マスクを [Loopback-Subnet] フィールドに入力する必要があります。
- %IPSEC-3-REPLAY_ERROR：IPSec SA はアンチリプレイ エラーを受信します。

このエラー メッセージが HUB-Border-MPLS ルータで表示された場合は、ウィンドウ サイズを増やすことで解決できる場合があります。

例：

```
crypto ipsec security-association replay window-size 1024
```

関連トピック

シスコ インテリジェント WAN（IWAN）の概要 （881 ページ）
IWAN ウィザードを使用した IWAN サービスの設定 （884 ページ）

IWAN ウィザードを使用した IWAN サービスの設定

Cisco Prime Infrastructure では、IWAN サービスを設計して展開するのに役立つウィザードが提供されます。

ステップ 1 **[サービス（Services）] > [ネットワーク サービス（Network Services）] > [IWAN の有効化（IWAN Enablement）]** を選択します。

ステップ 2 [次へ（Next）] をクリックして設定を選択します。

ステップ 3 カテゴリ、デバイス ロール、オーバーレイ プロトコル、およびこのワークフローで有効にするテクノロジー（DMVPN、PFR、QoS、AVC、DIA-ZBFW、CWS）を選択します。

CWS テクノロジーは、単一ルータ ブランチおよびデュアル ルータ ブランチ - インターネットの場合にのみ有効になります。

ステップ 4 （任意）IWAN 展開後に必要な設定のプッシュに使用できるポスト IWAN テンプレートを選択します。

ステップ 5 [次へ（Next）] をクリックし、指定した機能を設定するデバイスを選択します。複数のブランチで IWAN を同時に設定するには、複数のデバイスを選択して、各変数の値を入力します。

ステップ 6 [次へ（Next）] をクリックして入力オプションを選択します。

ステップ 7 [ワークフロー（Work Flow）] オプションをクリックすると、ウィザードが表示され、選択した設定に必要な値を入力します。

ステップ 8 または、[CSV のエクスポート（Export CSV）]/[CSV のインポート（Import CSV）] オプションをクリックし、CSV のエクスポート/インポート メカニズムを使用して選択したデバイスのテンプレート プロパティをすべて更新します。

a) CSV ファイル内の設定値の入力時に省略可能フィールドをスキップする場合は、[省略可能パラメータも必要ですか（Do you want Optional Parameters）] チェックボックスをオフにします。
b) [CSV のエクスポート（Export CSV）] をクリックし、ローカル システムに CSV テンプレートをダウンロードします。
c) ダウンロードした CSV テンプレートの設定値を入力します。
d) [CSV のインポート（Import CSV）] をクリックし、更新した CSV ファイルをアップロードします。

ステップ 9 必要な設定値を入力したら、[次へ（Next）] をクリックするか、または [CLI のサマリ（CLI Summary）] をクリックして、デバイスおよびテンプレートの設定値を確認します。

ステップ 10 必要に応じて、[準備およびスケジュール（Prepare and Schedule）] タブを使用して展開ジョブをスケジューリングします。

ステップ 11 [Next] をクリックするか、または [Confirmation] タブをクリックしてテンプレートを展開します。

展開後は、マスター コントローラとハブの境界ルータ間でルーティングをイネーブルにし、ルーティング ドメインの一部としてループバック 0 インターフェイスのサブネットを含めてください。

関連トピック

シスコ インテリジェント WAN（IWAN）の概要 （881 ページ）
IWAN サービスをイネーブルにするための前提条件 （882 ページ）
IWAN（APIC-EM）を使用したデバイス上での PKI 証明書ベースの認証設定 （885 ページ）

IWAN（APIC-EM）を使用したデバイス上での PKI 証明書ベースの認証設定

IWAN ワークフローで PKI 証明書（DMVPN の場合のみ）を使用するには、最初に Prime Infrastructure に有効な APIC-EM コントローラを追加する必要があります。「プラグ アンド プレイへの APIC-EM ポリシー情報の統合」を参照してください。CNS ゲートウェイが [グローバル PnP/ZTD 設定（Global PnP/ZTD Settings）]（**[管理（Administration）]** > **[サーバ（Servers）]** > **[APIC-EMコントローラ（APIC-EM Controller）]** > **[グローバル PnP/ZTD 設定（Global PnP/ZTD Settings）]**）で選択されている場合は、[PKI] オプションを有効にできません。これは、IWAN DMVPN に事前共有キーを使用する場合のオプションです。

IWAN ワークフローで、[PKI] オプションが有効な場合、バックエンドでは、デバイスが APIC-EM インベントリに追加され、PKI サービスがデバイスに PKI 認定をインストールするためにトリガーされます。デバイスは HTTP で証明書をダウンロードできます。

デバイスが管理対象ステートにある場合は、IWAN のプロビジョニングに使用できます。ここで、PKI 証明書ベースの認証が事前共有キーを使用する代わりに実行されます。

ステップ 1 **[サービス（Services）] > [ネットワーク サービス（Network Services）] > [IWAN の有効化（IWAN Enablement）]** を選択します。

ステップ 2 [始める前に（Before You Begin）] セクションで、[次へ（Next）] をクリックします。

ステップ 3 [設定の選択（Choose Configuration）] セクションで、ドロップダウン リストからカテゴリ、デバイス ロールを選択します。デバイス ロールを選択すると、DMVPN、PFR、QOS、および AVC 値が自動的に入力されます。ただし、これらの値は編集できます。DMVPN は PKI 証明書用のみです。

ステップ 4 ユーザが DMVPN トンネルに PKI 証明書ベースの認証を有効にできるように、[PKI の展開（Deploy PKI）] チェックボックスをオンにします。[次へ（Next）] をクリックします。

ステップ 5 [デバイスの選択（Select Devices）] セクションで、デバイスを選択し、[次へ（Next）] をクリックします。

ステップ 6 [Demo_DMVPN_TEMP] セクションで、[ループバック（Loopback）]、[MPLS トンネル（MPLS Tunnel）]、および [EDGRP] の下のフィールドに値を入力します。[適用（Apply）] をクリックし、[次へ（Next）] をクリックします。

ステップ 7 [CLI Summary] セクションに、DMVPN テンプレートの CLI コマンドが [Demo_DMVPN_TEMP] セクションでユーザが入力した値とともに表示されます。[次へ（Next）] をクリックします。

ステップ 8 ジョブをすぐに開始し繰り返さない場合は、[準備およびスケジュール（Prepare and Schedule）] セクションで、[次へ（Next）] をクリックします。IWAN ジョブを繰り返しパターンで後で実行するには、[スケジュール（Schedule）] で時間と繰り返しを指定します。必要に応じて、[ジョブ オプション（Job Option）] を指定します。

ステップ 9 [確認（Confirmation）] セクションで、[展開（Deploy）] をクリックしてデバイスを設定します。

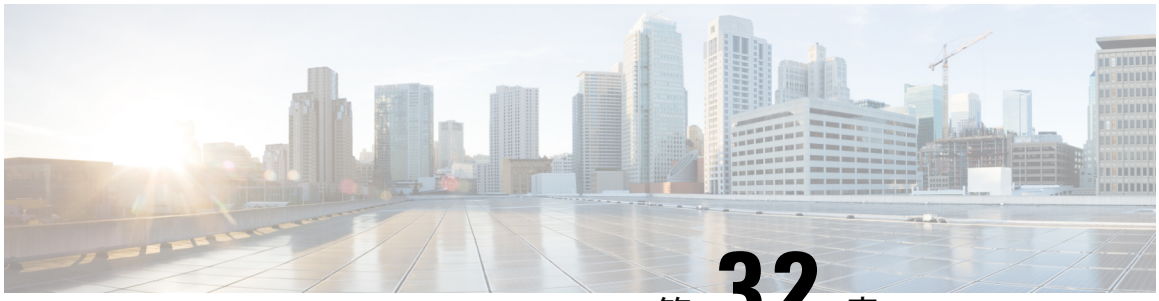
ステップ 10 確認メッセージが表示されます。[OK] をクリックします。[Administration / Jobs] の下に [User Jobs] ペインが表示されます。デバイス上の IWAN DMVNP 設定と PKI 証明書のプロビジョニングのステータスを [Job] ダッシュボードで追跡できます。

IWAN DMVPN 設定または PKI が失敗すると、IWAN プロビジョニングの全体のステータスが「Failed」と表示され、詳細に IWAN DMVPN 設定または PKI が失敗したことが表示されます。

たとえば、PKI IWAN サービスに障害があると、エラー メッセージ「Failed to install PKI certificate on device」が IWAN の [Job] ページに表示されます。PKI サービスが失敗すると、すべてのジョブが失敗します。

関連トピック

シスコ インテリジェント WAN（IWAN）の概要 （881 ページ）
IWAN ウィザードを使用した IWAN サービスの設定 （884 ページ）
プラグ アンド プレイへの APIC-EM ポリシー情報の統合 （842 ページ）



第 32 章

統合アクセス導入テンプレートを使用したキャンパスおよびブランチ ネットワーク向けのデバイスの設定

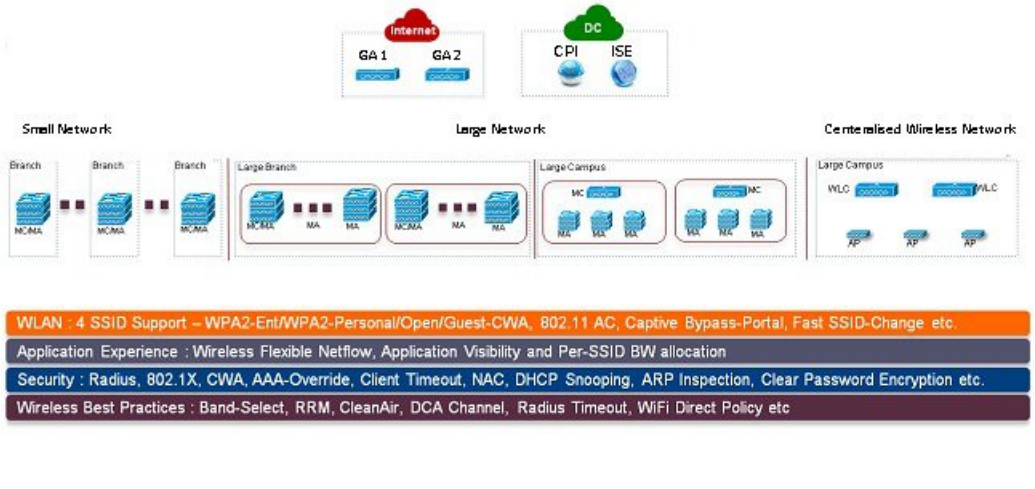
- 統合アクセス ワークフローとは （887 ページ）
- サポート対象の Cisco IOS-XE プラットフォーム （889 ページ）
- 統合アクセス導入の前提条件 （890 ページ）
- 統合アクセス テンプレートを使用したデバイスの設定 （895 ページ）
- 設定値入力のガイドライン （897 ページ）

統合アクセス ワークフローとは

コンバージドアクセス ワークフローは、キャンパス およびブランチ ネットワーク向けのさまざまなエンタープライズクラスの次世代ワイヤレス展開モデルの導入を簡素化、自動化、最適化します。Cisco Prime Infrastructure は、Catalyst 3650、3850、4500 SUP 8-E スイッチ、Cisco 5760 ワイヤレス LAN コントローラ（WLC）などのコンバージド アクセス コンポーネントを使用して、ワイヤレス ネットワークのコンバージド アクセス展開を自動化できます。Catalyst スイッチは、モビリティ エージェント（MA）、モビリティ コントローラ（MC）、およびゲスト アンカー コントローラ（GA）として導入できます。

次の図に、ワイヤレス統合アクセス展開モードを示します。

図 *22* : 統合アクセス ワークフローの概要



単一スイッチの小規模ネットワーク導入モデル

この導入モデルは、MA と MC ロールの組み合わせでアクセス レイヤに導入された単一の Catalyst 3650、3850 または 4500 SUP 8-E スイッチを仮定しています。Catalyst スイッチは、個別のスタンドアロン システム モードまたは StackWise 冗長スーパバイザ モードで導入できます。

コントローラのない単一もしくはマルチドメイン導入モデル

この導入モデルは、複数のサブドメインで構成され、サブドメイン間のエンドツーエンドのシームレスなローミングのためにドメイン間 MC ピアリングを許可します。MA スイッチはアクセス レイヤに導入でき、MC スイッチはディストリビューション レイヤに配置できます。

コントローラベースの単一もしくはマルチドメイン導入モデル

大規模なコンバージド アクセス キャンパスのビルディングは、MC として外部 5760 WLC により展開されます。アクセス レイヤ スイッチは、集中型 5760 MC により複数のビルディングにまたがる MA として導入されます。このような大規模ネットワークでは、よりよいロードバランシングおよび冗長性のために複数の 5760 WLC が共存する場合があります。異なるビルディング間のローミングの要件に応じて、5760 WLC 間でドメイン間モビリティ ピアリングを確立できます。

中央集中型ワイヤレス キャンパス導入モデル

この導入モデルでは、アクセス レイヤ内のスイッチは従来のスイッチング モードのままで、アクセス ポイント（AP）と WLC 間のワイヤレス通信はオーバーレイ ネットワークとして構築されます。大規模なキャンパス導入環境では、よりよいロードバランシングおよび冗長性のために複数の 5760 WLC を導入できます。シームレスで大規模なモビリティ ドメインを提供するために、ドメイン間モビリティ ピアリングの 5760 WLC を確立できます。

主なメリット

- 簡易な導入の自動化：デバイス設定のプロセスの自動化により統合アクセス導入を簡素化します。ネットワーク管理者による導入に関するわずかな入力だけで、完全な統合アクセス設定がネットワーク デバイスにプッシュされます。
- エラーのない導入：Cisco Prime Infrastructure によって使用されるテンプレート ベースの設定では、手動による設定ミスが回避され、ネットワーク管理者によく理解されている企業全体の標準化された設定の構築や保守が容易になります。
- 最適化された導入：Cisco Prime Infrastructure によって使用される設定テンプレートには、多数のシスコのベスト プラクティス ガイドラインが組み込まれており、導入の品質を向上させることができます。テンプレートに自動的に含まれているベストプラクティスの無線テクノロジー/機能には、帯域選択、無線リソース管理（RRM）、高速 SSID 変更、CleanAir およびワイヤレス QoS などがあります。
- 高い拡張性：何千もの支社を持つ大企業をサポートします。新規支社を展開する労力を減らせるだけでなく、統合アクセス ブランチへの従来のイーサネット ベースのブランチ ネットワークの大規模な変換がエラーのない方法で簡略化できます。

関連トピック

サポート対象の Cisco IOS-XE プラットフォーム （889 ページ）
統合アクセス導入の前提条件 （890 ページ）
統合アクセス テンプレートを使用したデバイスの設定 （895 ページ）
フィールド参照：統合アクセス テンプレート （897 ページ）
例：コントローラなしの単一スイッチ ネットワーク （901 ページ）
例：コントローラなしの単一/マルチドメイン ワイヤレス ネットワーク （906 ページ）
例：コントローラベースの単一/マルチドメイン ワイヤレス ネットワーク （908 ページ）
例：集中型ワイヤレス キャンパス （910 ページ）

サポート対象の Cisco IOS-XE プラットフォーム

次の表では、小規模、大規模、および集中型ネットワーク導入モデルでサポートされる Cisco IOS-XE プラットフォームについて説明します。

表 *54 :* 小規模ネットワーク導入モードでサポートされる *Cisco IOS-XE*

デバイス ロール	Cisco IOS-XE プラットフォーム	システム モード	ソフトウェア バージョン
モビリティ エージェント/モビリティ コントローラ（単一スイッチ）	Catalyst 3650	シングルまたは StackWise	3.6.0 以降
	Catalyst 3850	シングルまたは StackWise	3.6.0 以降
	Catalyst 4500 SUP 8-E	シングルまたは Dual-SUP	3.7.0 以降
ゲスト アンカー WLC	CT5760 WLC	シングルまたは StackWise	3.6.0 以降

表 *55 :* 大規模ネットワーク導入モデルでサポートされる *Cisco IOS-XE*

デバイス ロール	Cisco IOS-XE プラットフォーム	システム モード	ソフトウェア バージョン
モビリティ エージェント	Catalyst 3650	シングルまたは StackWise	3.6.0 以降
	Catalyst 3850	シングルまたは StackWise	3.6.0 以降
	Catalyst 4500 SUP 8-E	シングルまたは Dual-SUP	3.7.0 以降
モビリティ コントローラ	Catalyst 3650	シングルまたは StackWise	3.6.0 以降
	Catalyst 3850	シングルまたは StackWise	3.6.0 以降
	Catalyst 4500 SUP 8-E	シングルまたは Dual-SUP	3.7.0 以降
	CT5760 WLC	シングルまたは StackWise	3.6.0 以降
ゲスト アンカー コントローラ	CT5760 WLC	シングルまたは StackWise	3.6.0 以降

表 *56 :* 中央集中型ワイヤレス導入モードでサポートされる *Cisco IOS-XE*

デバイス ロール	Cisco IOS-XE プラットフォーム	システム モード	Software Version
モビリティ コントローラ	CT5760 WLC	シングルまたは StackWise	3.6.0 以降
ゲスト アンカー WLC	CT5760 WLC	シングルまたは StackWise	3.6.0 以降

関連トピック

統合アクセス ワークフローとは （887 ページ）
統合アクセス導入の前提条件 （890 ページ）
統合アクセス テンプレートを使用したデバイスの設定 （895 ページ）
フィールド参照：統合アクセス テンプレート （897 ページ）
例：コントローラなしの単一スイッチ ネットワーク （901 ページ）
例：コントローラなしの単一/マルチドメイン ワイヤレス ネットワーク （906 ページ）
例：コントローラベースの単一/マルチドメイン ワイヤレス ネットワーク （908 ページ）
例：集中型ワイヤレス キャンパス （910 ページ）

統合アクセス導入の前提条件

統合アクセス ワークフローを使用して統合アクセス ソリューションを正常に導入するには、ネットワークの有線インフラストラクチャを統合アクセスに必要なその他の構成に設定する必

要があります。ここでは、統合アクセス ワークフロー ベースの導入に必要な設定について説明します。

前提条件は、統合アクセス ワークフローの [はじめる前に（Before you Begin）] ページの [ここをクリック（click here）] リンクを使用して表示できます（**[サービス（Services）]** > **[ネットワークサービス（Network Services）]** > **[統合アクセス（Converged Access）]**）。

関連トピック

レイヤ 2 およびレイヤ 3 の前提条件 （891 ページ）
サーバの構成の前提条件 （894 ページ）

レイヤ 2 およびレイヤ 3 の前提条件

次の表では、レイヤ 2 およびレイヤ 3 の前提条件、および統合アクセス ワークフローのサンプル構成について説明します。設定例では、MA および MC のさまざまなワイヤレス管理 VLAN を表すために次の名称が使用されます。

- WM_VLAN：ワイヤレス管理 VLAN の名前
- WM_VLAN_id：ワイヤレス管理 VLAN の ID
- WLAN1_Client_VLAN_Name：WLAN 1 の VLAN 名
- WLAN2_Client_VLAN_Name：WLAN 2 の VLAN 名
- WLAN3_Client_VLAN_Name：WLAN 3 の VLAN 名
- WLAN1_Client_VLAN_id：WLAN 1 の VLAN ID
- WLAN2_Client_VLAN_id：WLAN 2 の VLAN ID
- WLAN3_Client_VLAN_id：WLAN 3 の VLAN ID

（注） WLANx_Client_VLAN_id は 3 つのクライアントすべての VLAN ID を表します。

表 *57*：デバイス ロール *MA* および *MC* 用の統合アクセス スイッチのレイヤ *2* およびレイヤ *3* の前提条件

統合アクセス スイッチのタスク	設定例
ワイヤレス管理 VLAN • ネットワーク全体の一意の名前でワイヤレス管理 VLAN を作成します。 • この VLAN の下に AP に接続されたアクセス ポートを設定します。	! Mgmt VLAN on Access Switch vlan <WM_VLAN_id> name <WM_VLAN> ! Apply VLAN to access ports connected to Access Points interface GigabitEthernet 1/0/x description Connected to Access-Points switchport mode access switchport access vlan <WM_VLAN_id>

統合アクセス スイッチのタスク	設定例
ワイヤレス クライアント VLAN の作成 • VLAN データベースでワイヤレス クライアント VLAN を作成します。VLAN 名は、キャンパスおよびブランチで共通です。	! Create the wireless Client VLANs on Access Switch vlan <WLAN1_Client_VLAN_id> name <WLAN1_Client_VLAN_Name> vlan <WLAN2_Client_VLAN_id> name <WLAN2_Client_VLAN_Name> vlan <WLAN3_Client_VLAN_id> name <WLAN3_Client_VLAN_Name>
DHCP スヌーピング/ARP インスペクション • アクセス スイッチ（スタティックまたはダイナミック VLAN 用）の各 WLAN クライアント VLAN で DHCP スヌーピングと ARP インスペクションをイネーブルにします。 • ARP インスペクションおよび DHCP スヌーピング用に信頼されているアップストリーム レイヤ 2 トランクを設定します。	! Enable DHCP Snooping & ARP Inspection on all WLAN ! Client VLANs (Static or Dynamic) ip dhcp snooping ip dhcp snooping vlan name <WLANx_Client_VLAN_id> no ip dhcp snooping information option ip arp inspection vlan <WLANx_Client_VLAN_id> ip arp inspection validate source destination allow-zeros interface Port-Channel <id> description L2 Trunk to Upstream Router/Switch ip dhcp snooping trust ip arp inspection trust
トランク ポートの切り替え • WAN ルータにトランク ポートを設定します。トランクは WM_VLAN とクライアント VLAN を許可する必要があり、DHCP スヌーピングまたは ARP インスペクション用の信頼できるポートである必要があります。 • トランク ポートのもう一方の端が正しく設定されていることを確認します（表示されていません）。	! Configure trunk port to other connected switches/router interface Port-channel1 description Connected to Upstream System switchport trunk allowed vlan add <WM_VLAN_id>, <WLAN1_Client_VLAN_id>,<WLAN2_Client_VLAN_id>, <WLAN3_Client_VLAN_id>, ip arp inspection trust ip dhcp snooping trust
デフォルト ゲートウェイ • デフォルト ゲートウェイが設定されていることを確認します。	! Configure default-gateway <*ip default-gateway*> >
ワイヤレス モビリティ コントローラ • Catalyst 3650、3850、および 4500 SUP 8-E スイッチを MC として導入する場合は、それらのスイッチを MC として設定し、リロードして設定を有効にします。	wireless mobility controller write memory reload

統合アクセス スイッチのタスク	設定例
AP ライセンス • MC には、サブドメイン内のすべての AP をサポートするのに十分な AP ライセンスが必要で、そのライセンスを AP でアクティブにする必要があります。アクティブ化に再起動は不要です。 • GA には AP ライセンスは不要です。	`! Activate AP license on branch converged access switch` `license right-to-use activate ap-count <count> slot <ID> acceptEULA`
セキュリティ • アクセス スイッチの関連する認証コマンドをクラスベースのポリシー言語（CPL）相当に変換します。	`authentication convert-to new-style` このコマンドは、スイッチのレガシー設定を ID ベースのネットワーキング サービスに完全に変換します。このコマンドを入力すると、続行する許可を求めるメッセージが表示されます。変換を許可します。

AP インターフェイス テンプレートの更新
• AP インターフェイス テンプレート LAP_INTERFACE_TEMPLATE にワイヤレス管理 VLAN を追加します。
• AP に接続されている各スイッチ ポートに更新されたテンプレートを適用します。
• 次のコマンドを使用して、VLAN が適用されたことを確認します。
 	
`show derived-config interface <interface id>`
 	
autoconf enable コマンドがグローバルに設定されている場合は、この手順は必要ありません。この場合、スイッチは接続されたデバイスのデバイス タイプを自動的に検出し、適切なインターフェイス テンプレートを適用します。
	`template LAP_INTERFACE_TEMPLATE`
	`switchport access vlan <Wireless_Mgmt_VLAN_id>`
	`! Associate the LAP_INTERFACE_TEMPLATE to switch`
	`! ports connected to APs. This puts the interface`
	`! in shutdown state; so issue a “no shut” command`
	`interface Gig 1/0/x`
	`source template LAP_INTERFACE_TEMPLATE`
	`no shutdown`

以下では、レイヤ 2 およびレイヤ 3 の前提条件、および GA のサンプル構成について説明します。設定例では、GA のワイヤレス管理 VLAN およびゲスト VLAN の詳細を表すために次の名称が使用されます。

- WM_VLAN：ワイヤレス管理 VLAN の名前
- WM_VLAN_id：ワイヤレス管理 VLAN の ID
- GUEST_VLAN_Name：ゲスト アンカー コントローラの VLAN 名
- GUEST_VLAN_id：ゲスト アンカー コントローラの VLAN ID

表 *58* : ゲスト アンカー コントローラのレイヤ *2* およびレイヤ *3* の前提条件

ゲスト アンカー コントローラのタスク	ゲスト アクセス コントローラの設定例

ワイヤレス管理 VLAN
• ネットワーク全体の一意の名前でワイヤレス管理VLANを作成します。
	`! Mgmt VLAN on Access Switch`
	`vlan <WM_VLAN_id>`
	`name <WM_VLAN>`

ワイヤレス ゲスト VLAN の作成
• VLAN データベースでワイヤレス ゲスト VLAN を作成します。VLAN名はすべてのGAで共通である必要があります。
	`! Create the wireless guest VLANS on Access Switch`
	`vlan <GUEST_VLAN_id>`
	`name <GUEST_VLAN_Name>`

DHCP スヌーピング/ARP インスペクション
• ゲスト VLAN で DHCP スヌーピングおよび ARP インスペクションをイネーブルにします。
• ネットワークに接続されたレイヤ2トランクを、ARPインスペクションおよびDHCPスヌーピング用に信頼されるように設定します。
	`! Enable DHCP Snooping & ARP Inspection on Guest`
	`! VLAN`
	`ip dhcp snooping`
	`ip dhcp snooping vlan name <GUEST_VLAN_Name>`
	`no ip dhcp snooping information option`
	`ip arp inspection vlan <GUEST_VLAN_id>`
	`ip arp inspection validate source destination allow-zeros`
	`interface Port-Channel <id>`
	`description L2 Trunk to network`
	`ip dhcp snooping trust`
	`ip arp inspection trust`

デフォルト ゲートウェイ • デフォルト ゲートウェイが設定されていることを確認します。	`ip default-gateway <ip address>`
セキュリティ • アクセス スイッチの関連する認証コマンドをクラスベースのポリシー言語（CPL）相当に変換します。	`authentication convert-to new-style` このコマンドは、スイッチのレガシー設定を ID ベースのネットワーキング サービスに完全に変換します。このコマンドを入力すると、続行する許可を求めるメッセージが表示されます。変換を許可します。

関連トピック

統合アクセス導入の前提条件 （890 ページ）
サーバの構成の前提条件 （894 ページ）

サーバの構成の前提条件

- Cisco Prime Infrastructure
  - すべてのネットワーク全体の Catalyst スイッチおよび 5760 WLC は、SNMP で設定する必要があります。

- 統合アクセス スイッチは、Cisco Prime Infrastructure のインベントリに追加する必要があります。デバイスをインベントリに追加するには、SNMP および Telnet のクレデンシャルを指定する必要があります。
- エンドツーエンドのクライアント接続とポリシー適用の詳細を一元的に監視するため、外部サーバとして Cisco ISE エンジンに Cisco Prime Infrastructure をリンクします。

- Cisco ISE/ACS
  - 中央集中型のポリシー エンジン機能を有効にするには、Catalyst スイッチおよびゲスト アンカー WLC を含むすべてのネットワーク デバイスを Cisco ISE/ACS に設定する必要があります。
  - AAA 設定は、統合アクセス ワークフローによって自動的に生成されるので、個々のネットワーク デバイスの統合アクセスには必要ありません。
- DHCP サーバ：内部または外部の DHCP サーバは、ワイヤレス クライアント用の適切なプール設定によってあらかじめ設定しておく必要があります。
- DNS サーバ：ネットワークに正常に接続するように、適切な名前ルックアップ プロセスで事前に設定しておく必要があります。

関連トピック

統合アクセス導入の前提条件 （890 ページ）
レイヤ 2 およびレイヤ 3 の前提条件 （891 ページ）

統合アクセス テンプレートを使用したデバイスの設定

Prime Infrastructure は、さまざな導入モデルに異なるテンプレートを使用します。次の表で説明するように、ネットワーク トポロジに基づいて適切なテンプレート ベースを選択する必要があります。

ネットワーク トポロジ	設定テンプレート
単一スイッチの小規模ネットワーク	IOS-XE Controller - Small Network
コントローラのない単一もしくはマルチドメイン ブランチ	IOS-XE Controller - Large Network
コントローラ ベースの単一もしくはマルチドメイン ブランチ	IOS-XE Controller - Large Network
中央集中型ワイヤレス キャンパス	IOS-XE Centralized Wireless Network

統合アクセス テンプレートを展開するには、次の手順を実行します。

ステップ 1 **[サービス（Services）]** > **[統合型アクセス（Converged Access）]** を選択します。

ステップ 2 [次へ（Next）] をクリックして導入モデルを選択します。

ステップ 3 [導入モデルの選択（Select Deployment Model）] ドロップダウン リストから、次のいずれかのオプションを選択します。

- IOS-XE Controller - Small Network
- IOS-XE Controller - Large Network
- IOS-XE Centralized Wireless Network

ステップ 4 [Next] をクリックして展開するデバイスを選択します。

ステップ 5 デバイスを選択し、[次へ（Next）] をクリックして、選択したネットワーク構成を適用します。

選択したデバイスは左側のペインに表示され、右側のペインでは、ワイヤレス管理、WLAN、ゲスト WLAN、モビリティ、セキュリティ、Application Visibility and Control（AVC）、および Quality of Service（QoS）の値を入力してテンプレートを設定できます。

ステップ 6 デバイスを個別に選択し、[ワイヤレス管理（Wireless Management）] の設定値を入力します。

ステップ 7 [適用（Apply）] をクリックし、次に [次へ（Next）] をクリックします。

ステップ 8 選択したすべてのデバイスに共通の [WLAN（WLANs）] の設定値を入力します。

デフォルトでは、[選択したすべてのデバイス（All Selected Devices）] チェックボックスはオンになっています。すべてのデバイスの WLAN の設定値を同時に入力できます。

ステップ 9 [適用（Apply）] をクリックし、次に [次へ（Next）] をクリックします。

ステップ 10 （オプション）選択したすべてのデバイスに共通の、[無線（Radio）] の設定値を入力します。デフォルトでは、[**All Selected Devices**] チェックボックスは有効になっています。

ステップ 11 [適用（Apply）] をクリックし、次に [次へ（Next）] をクリックします。

ステップ 12 （オプション）選択したすべてのデバイスに共通の、[ゲスト WLAN（Guest WLAN）] の設定値を入力します。

デフォルトでは、[選択したすべてのデバイス（All Selected Devices）] チェックボックスはオンになっています。

ステップ 13 [適用（Apply）] をクリックします。

ステップ 14 デバイスを個別に選択し、[ゲストコントローラ（Guest Controller）] の設定値を入力します。

ステップ 15 [適用（Apply）] をクリックし、次に [次へ（Next）] をクリックします。

ステップ 16 デバイスを個別に選択し、[モビリティ（Mobility）] の設定値を入力します。[コンバージドアクセス（Converged Access）] ウィザードで [モビリティ（Mobility）] 設定フィールドを利用できるのは、大規模な集中型ネットワークのみです。

ステップ 17 [適用（Apply）] をクリックし、次に [次へ（Next）] をクリックします。

ステップ 18 （オプション）選択したすべてのデバイスに共通の、[セキュリティ（Securiy）] の設定値を入力します。デフォルトでは、[選択したすべてのデバイス（All Selected Devices）] チェックボックスはオンになっています。

ステップ 19 [適用（Apply）] をクリックし、次に [次へ（Next）] をクリックします。

ステップ 20 （任意）選択したすべてのデバイスに共通の [AVC] および [QoS] の設定値を入力します。デフォルトでは、[**All Selected Devices**] チェックボックスは有効になっています。

ステップ 21 [適用（Apply）] をクリックし、次に [次へ（Next）] をクリックすると、確認画面が表示されます。

導入前に、確認画面でデバイス設定情報を確認できます。

ステップ 22 （オプション）ジョブ名を入力後、[日付（Date）] オプション ボタンをクリックし、展開ジョブをスケジュールします。

ステップ 23 [展開（Deploy）] をクリックします。

関連トピック

統合アクセス導入の前提条件 （890 ページ）
フィールド参照：統合アクセス テンプレート （897 ページ）
例：コントローラなしの単一スイッチ ネットワーク （901 ページ）
例：コントローラなしの単一/マルチドメイン ワイヤレス ネットワーク （906 ページ）
例：コントローラベースの単一/マルチドメイン ワイヤレス ネットワーク （908 ページ）
例：集中型ワイヤレス キャンパス （910 ページ）

設定値入力のガイドライン

ここでは、統合アクセステンプレートのフィールドの説明と、次の導入モデルに対するグローバルおよびローカルの設定値の入力に関するガイドラインを具体的な例とともに説明します。

- コントローラのない単一スイッチ導入モデル
- コントローラのない単一もしくはマルチドメイン導入モデル
- コントローラベースの単一もしくはマルチドメイン導入モデル
- 中央集中型ワイヤレス キャンパス導入モデル

フィールド参照：統合アクセス テンプレート

ここでは、コンバージド アクセス テンプレートのフィールドについて説明します。

表 *59 :* ワイヤレス管理フィールドの説明

Field Name	Description
VLAN ID（Admin. VLAN ID）	選択したデバイスの VLAN ID。
[IPアドレス（IP Address）]	選択したデバイスのワイヤレス管理 IP。
Subnet mask	選択したデバイスに割り当てられたサブネット マスク。

表 *60 : WLAN* フィールドの説明

フィールド	説明
SSID	無線 LAN の名前。

フィールド	説明
ID	無線 LAN の ID。SSID が 16 より大きい場合は、AP グループ名を手動で入力する必要があります。
セキュリティ	ISE などの外部 Web サーバを設定するためのログイン ウィンドウをカスタマイズできます。WLAN では次のセキュリティ オプションを使用できます。 • [WPA2 エンタープライズ（WPA2-Enterprise）] • [WPA2 パーソナル（WPA2-Personal）] • [オープン（OPEN）] ゲスト WLAN では、WebAuth（外部）オプションのみが使用可能です。
[事前共有キー（Pre-Shared Key）]	[WPA2 パーソナル（WPA2-Personal）] が選択されている場合、このフィールドは必須です。この値は英数字で、8 文字以上である必要があります。
[クライアント VLAN 名（Client VLAN Name）]	クライアント VLAN の名前。英数字を使用できます。
[AP グループ（AP Group）]	AP グループ名は、WLAN とクライアント VLAN に関連付けられた AP にグループ名を割り当てるために使用されます。
[DHCP が必要です（DHCP Required）]	これはオプションのフィールドです。WLAN の **DHCP Required** チェックボックスをオンにします。これはワイヤレス クライアントに、IP アドレスを取得するために DHCP を使用することを強制します。スタティック アドレスのクライアントはネットワークにアクセスできません。
[無線（Radio）]	WLAN で使用される無線帯域。
[デバイスの分類（Device Classification）]	OUI と DHCP を使用して、スイッチのデバイス分類のオン/オフを切り替えることができます。
[デバイスプロファイリング（Device Profiling）]	デバイス プロファイリングのオン/オフを切り替えることができます。デバイス プロファイリングでは次の 2 種類のオプションを使用できます。 • HTTP 属性に基づくローカル プロファイリング • HTTP 属性に基づく RADIUS プロファイリング
[クライアント除外（Client Exclusion）]	WLAN のクライアント除外のオン/オフを切り替えます。オンにすると、正常に動作していないクライアントが、タイムアウトになるまでネットワークにアクセスできないように、除外リストに追加されます。認証を過剰な回数試行したり、別のクライアントの IP アドレスを使用したりすると、クライアントが除外リストに追加される可能性があります。
[クライアント除外のタイムアウト(秒)（Client Exclusion Timeout (sec)）]	クライアント除外のタイムアウト時間。
[セッションのタイムアウト(秒)（Session Timeout (sec)）]	クライアントセッションのタイムアウト時間。タイムアウト時間が終了する前に、クライアントが再認証されます。

表 *61 :* ワイヤレス無線フィールドの説明

フィールド	説明
[RF グループ名（RF Group Name）]	RF グループの名前。グローバルに最適化された方法で RRM を実行し、無線単位でネットワークの計算を実行するために、複数の MC が単一の RF グループの下に配置することが可能です。
[無線 2 GHz（Radio 2 GHz）]	これはオプションのチェックボックスです。
[無線 5 GHz（Radio 5 GHz）]	このチェックボックスは、デフォルトでオンになっており、必須です。このチェックボックスをオフにすることはできません。
[レートの無効化（Disable Rates）]	このデータ レートが無効になります。クライアントはこのデータ レートを使用して、アクセス ポイントに接続することはできません。
[必須レート（Mandatory Rates）]	クライアントはサポートされているデータ レートを使用してアクセス ポイントに接続する可能性がありますが、アクセス ポイントに関連付けるには、クライアントがこのデータ レートをサポートしている必要があります。
[サポートされるレート（Supported Rates）]	このデータ レートをサポートするクライアントは、このレートを使用してアクセス ポイントと通信できます。ただし、クライアントはアクセス ポイントとの関連付けにこのデータ レートを使用する必要はありません。
国コード（Country Code）	特定の運用国を国コードで指定できます。国コードを設定すると、各無線のブロードキャスト周波数帯域、インターフェイス、チャネル、および送信電力レベルが国別の規制に準拠していることを確認できます。

表 *62 :* ゲスト サービスのフィールドの説明

フィールド	説明
Anchor Controller IP	ゲスト アンカー デバイスのワイヤレス管理 IP。
Anchor Group Name	アンカー デバイスのグループ名。
Foreign Controller	ゲスト アンカー デバイスが関連付けられた MC のワイヤレス管理 IP。

表 *63 :* セキュリティ フィールドの説明

フィールド	説明
[Radius サーバ（IP）（Radius Server (IPs)）]	Remote Authentication Dial In User Service（RADIUS）サーバの IP アドレス。
キー（Key）	RADIUS サーバのパスワード。

フィールド	説明
[デバイス HTTP TACACS 認証（Device HTTP TACACS Authentication）]	TACACS ベースのデバイス認証を有効にして、コンバージド アクセス デバイスにアクセスするには、ここを選択します。
[TACACS+ サーバの IP（TACACS+ Server IP(s)）]	TACACS サーバの IP アドレス。
キー（Key）	TACACS サーバのパスワード。

表 *64*：アプリケーション サービスのフィールドの説明

フィールド名	説明
Netflow Collectors (IP:Port)	[IP]：Prime Infrastructure サーバの IP アドレス。 [ポート（Port）]：NetFlow モニタがエクスポートされたデータを受信するポート。Prime Infrastructure の場合、デフォルト ポートは 9991 です。 例：172.20.114.251:9991
WLAN-1 SSID Bandwidth(%)	最初の WLAN に許可される最大帯域幅の割合を指定します。
WLAN-2 SSID Bandwidth(%)	2 番目の WLAN に許可される最大帯域幅の割合を指定します。
WLAN-3 SSID Bandwidth(%)	3 番目の WLAN に許可される最大帯域幅の割合を指定します。
Guest SSID Bandwidth(%)	ゲスト WLAN に許可される最大帯域幅の割合を指定します。

表 *65*：ワイヤレス モビリティのフィールドの説明

フィールド名	説明
ロール	モビリティ コントローラまたはモビリティ エージェント。
Controller IP	コントローラ デバイスのワイヤレス管理 IP。
Switch Peer Group Name	エージェントが追加されるピア グループ名。
Mobility Agent IP(s)	モビリティ エージェントのデバイスのワイヤレス管理 IP。複数の IP アドレスを入力する場合は、セミコロンを使用して IP アドレスを区切ります。
Peer Controller IP(s)	ピア コントローラ デバイスのワイヤレス管理 IP。複数の IP アドレスを入力する場合は、セミコロンを使用して IP アドレスを区切ります。

関連トピック

統合アクセス導入の前提条件 （890 ページ）
統合アクセス テンプレートを使用したデバイスの設定 （895 ページ）
例：コントローラなしの単一スイッチ ネットワーク （901 ページ）
例：コントローラなしの単一/マルチドメイン ワイヤレス ネットワーク （906 ページ）

例：コントローラベースの単一/マルチドメイン ワイヤレス ネットワーク （908 ページ）
例：集中型ワイヤレス キャンパス （910 ページ）

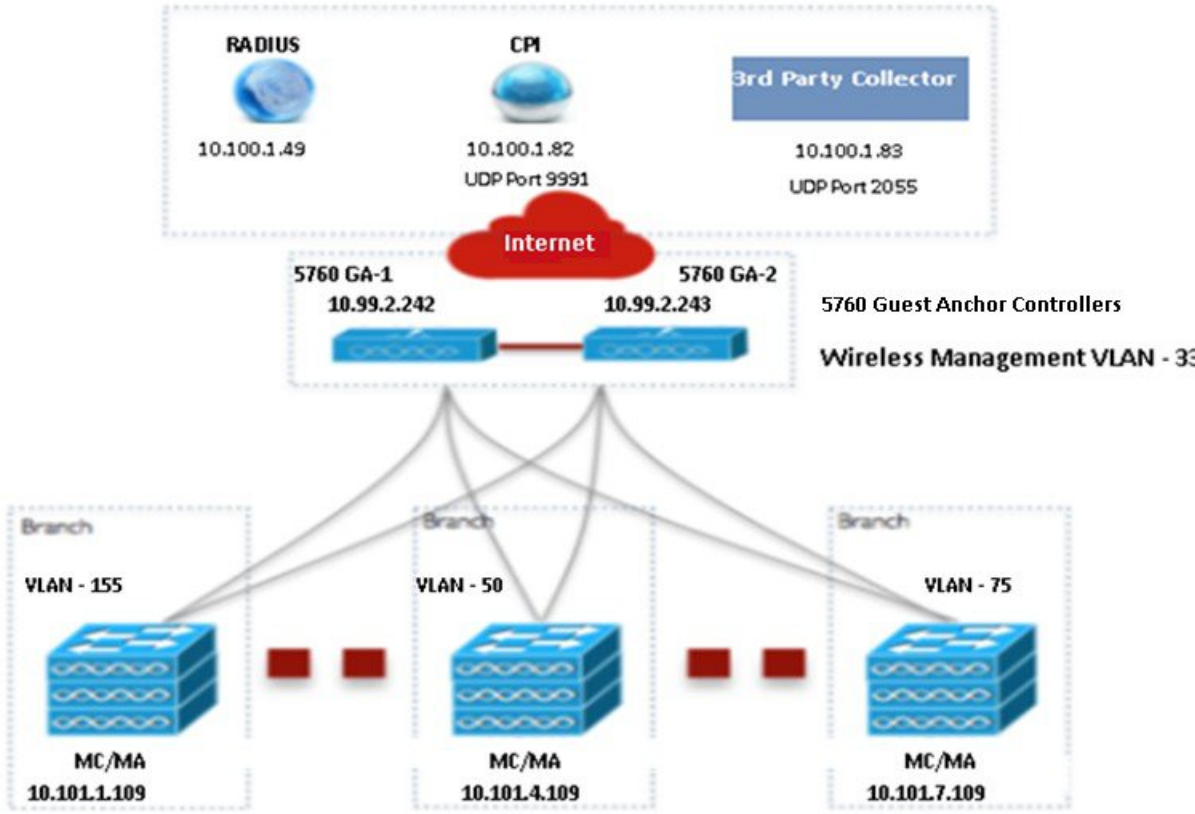
例：コントローラなしの単一スイッチ ネットワーク

小規模のリモート ブランチ オフィスまたは小売店は、有線および無線ユーザにネットワーク接続を提供するために単一の統合アクセス スイッチ（スタンドアロンまたはスタック）で構成されている場合があります。

このようなネットワーク設計の場合、スイッチはMCおよびMA両方の機能を統合します。これらのネットワークでは、ゲスト ワイヤレス サービスと、展開されたすべてのサイトで共通のセキュリティおよびネットワーク アクセス ポリシーの適用が必要になる場合があります。

ネットワーク管理者は、Prime Infrastructure IOS-XE コントローラの小規模ネットワーク テンプレートを使用して、コンバージド アクセスを展開することができます。次の図 405448 に、3 つのブランチ オフィスを示す単一スイッチの小規模ネットワークのリファレンス ネットワークを示します。各サイトは、ワークフローを使用して個別に展開できます。また、1 つの導入ワークフローは複数のサイトを展開できます。Prime Infrastructure では、5 個の WLAN でデバイスを設定できます。次の図に、単一スイッチの小規模ネットワーク トポロジでの WLAN 設定シナリオを示します。

図 *23 :* コントローラのない単一スイッチの小規模ネットワーク モデル



	SSID	Security	Client VLAN Name	Guest VLAN Na
WLAN 1	ABCCorp_802.1X	WPA2-Enterprise	8021x-WiFi_VLAN	
WLAN 2	ABCCorp_PSK	WPA2-Personal	PSK-WiFi_VLAN	
WLAN 3	ABCCorp-OPEN	OPEN	OPEN_WiFi-VLAN	
Guest WLAN	ABCCorp_Guest	WebAuth-External		Guest_WiFi-VLA

デバイスごとに別々にワイヤレス管理の設定値を入力する必要があります。次の表に、上の図に示す単一スイッチの小規模ネットワーク トポロジ内の MA/MC（10.100.1.109）およびゲストアンカー（10.99.2.242）に対するワイヤレス管理の設定値を示します。

表 *66 : MA/MC*（*10.100.1.109*）および *GA*（*10.99.2.242*）に対するサンプルのワイヤレス管理の設定値

データ フィールド	MA/MC	GA
VLAN ID	155	33
IP	10.101.1.109	10.99.2.242

データ フィールド	MA/MC	GA
Subnet Mask	255.255.255.240	255.255.255.240

ワイヤレス管理の設定値を適用した後、少なくとも 1 つの WLAN 設定値を入力する必要があります。次の表に、上の図に示す単一スイッチ小規模ネットワーク トポロジにおける 3 つの WLAN の設定例を示します。

表 *67 : MC/MA*、および *GA* に対するサンプルの *WLAN* 設定値

データ フィールド	WLAN 1	WLAN 2	WLAN 3
SSID	ABCCorp_802.1x	ABCCorp_PSK	ABCCorp_OPEN
ID	1	2	3
セキュリティ	[WPA2 エンタープライズ（WPA2-Enterprise）]	[WPA2 パーソナル（WPA2-Personal）]	[オープン（OPEN）]
Pre-Shared Key; 事前共有キー	—	CISCO123	—
[クライアント VLAN 名（Client VLAN Name）]	8021X-WiFi_VLAN	PSK-WiFi_VLAN	OPEN_WiFi_VLAN
[AP グループ（AP Group）]	Ap-group-1		Ap-group-HR
DHCP			はい（[DHCP] チェックボックスをオンにします）。
[無線（Radio）]	すべて（All）	802.11g	802.11a/g
[デバイスの分類（Device Classification）]		はい（[デバイスの分類（Device Classification）] チェックボックスをオンにします）。	
[デバイスプロファイリング（Device Profiling）]	[なし（None）]	[ローカル（Local）]	両方
[クライアント除外（Client Exclusion）]	はい（[クライアント除外（Client Exclusion）] チェックボックスをオンにします）。	はい（[クライアント除外（Client Exclusion）]チェックボックスをオンにします）。	はい（[クライアント除外（Client Exclusion）] チェックボックスをオンにします）。
[タイムアウト(秒)（Timeout (sec)）]	60	100	100
[セッションのタイムアウト(秒)（Session Timeout (sec)）]	1800	2000	300

WLANの設定値を適用した後、すべてのデバイスのワイヤレス設定値を同時に入力します。次の表に、上の図に示す単一スイッチの小規模ネットワーク トポロジ内の MC/MA、および GA に対するワイヤレス無線設定値を示します。

表 *68 : MC/MA*、および *GA* に対するサンプルのワイヤレス無線設定値

データ フィールド	サンプルの設定値
[RF グループ名（RF Group Name）]	CA-RF
[無線 5 GHz（Radio 5 GHz）]	はい（このチェックボックスは、デフォルトでオンになっており、必須です。このチェックボックスをオフにすることはできません）。
[レートの無効化（Disable Rates）]	[RATE_6M]、[RATE_18M]、[RATE_54M]
[必須レート（Mandatory Rates）]	[RATE_6M]、[RATE_18M]、[RATE_54M]
[サポートされるレート（Supported Rates）]	[RATE_6M]、[RATE_18M]、[RATE_54M]
[無線 2 GHz（Radio 2 GHz）]	いいえ（これはオプションのチェックボックスです）。
[レートの無効化（Disable Rates）]	—
[必須レート（Mandatory Rates）]	—
[サポートされるレート（Supported Rates）]	—
国コード（Country Code）	[アメリカ合衆国（UNITED STATES）]

ワイヤレス設定値を適用した後、すべてのデバイスのゲストサービスの設定値を同時に入力します。次の表に、上の図に示す単一スイッチの小規模ネットワークトポロジ内のすべてのデバイスに対するゲスト WLAN 設定値を示します。

表 *69 : MC/MA*、および *GA* に対するサンプルのゲスト *WLAN* 設定値

データ フィールド	サンプルの設定値
SSID	ABCCorp_Guest
ID	15
セキュリティ	WebAuth-External
Pre-Shared Key; 事前共有キー	—
[クライアント VLAN 名（Client VLAN Name）]	Guest_WiFi_VLAN
[AP グループ（AP Group）]	AP-group-guest
DHCP	はい（[DHCP] チェックボックスをオンにします）。

データ フィールド	サンプルの設定値
[無線（Radio）]	[802.11a]（もしくは[802.11a/g]、[802.11b/g]、[802.11g]、[すべて（All）]）
[デバイスの分類（Device Classification）]	はい（[デバイスの分類（Device Classification）] チェックボックスをオンにします）。
[デバイスプロファイリング（Device Profiling）]	両方
[クライアント除外（Client Exclusion）]	オン
[タイムアウト(秒)（Timeout (sec)）]	100
[セッションのタイムアウト(秒)（Session Timeout (sec)）]	[5000]

次の表に、上の図に示す単一スイッチの小規模ネットワーク トポロジ内の MC/MA（10.100.1.109）、およびGAに対する、サンプルのゲスト コントローラの設定値を示します。

表 *70 : MA/MC*（*10.100.1.109*）、および *GA* に対するサンプルのゲスト コントローラの設定値

データ フィールド	MC/MA	GA
Anchor Controller IP	10.99.2.242; 10.99.2.243	10.99.2.242; 10.99.2.243
Anchor Group Name	CA-Mobility-SubDomain-3	CA-Mobility-SubDomain-3
Foreign Controllers	10.101.4.109	10.101.1. 109; 10.101.4.109; 10.101.7.109

ゲスト サービスの設定値を適用した後、すべてのデバイスのセキュリティの設定値を同時に入力します。次の表に、上の図に示す単一スイッチの小規模ネットワーク トポロジ内のMC/MA、およびGA に対するサンプルのセキュリティ設定値を示します。

表 *71 : MC/MA*、および *GA* に対するサンプルのセキュリティの設定値

データ フィールド	サンプルの設定値
[Radius サーバ（IP）（Radius Server (IPs)）]	10.100.1.49
キー（Key）	CISCO
[デバイス HTTP TACACS 認証（Device HTTP TACACS Authentication）]	はい（[デバイス HTTP TACACS 認証（Device HTTP TACACS Authentication）] チェックボックスをオンにします）。
[TACACS+ サーバの IP（TACACS+ Server IP(s)）]	10.100.1.51
キー（Key）	cisco

セキュリティの設定値を適用した後、すべてのデバイスの AVC および QoS の設定値を同時に入力します。次の表に、上の図に示す単一スイッチの小規模ネットワーク トポロジ内の MC/MA、および GA に対するサンプルの設定値を示します。

表 *72 : MC/MA*、および *GA* に対するサンプルの *AVC* および *QoS* 設定値

データ フィールド	サンプルの設定値
[NetFlow コレクタ(IP: ポート)（Netflow Collectors (IP:Port)）]	10.100.1.02:9991; 10.100.1.03:2055
[WLAN-1 SSID 帯域幅(%)（WLAN-1 SSID Bandwidth(%)）]	40
[WLAN-2 SSID 帯域幅(%)（WLAN-2 SSID Bandwidth(%)）]	30
[WLAN-3 SSID 帯域幅(%)（WLAN-3 SSID Bandwidth(%)）]	20
[ゲスト SSID 帯域幅(%)（Guest SSID Bandwidth(%)）]	10

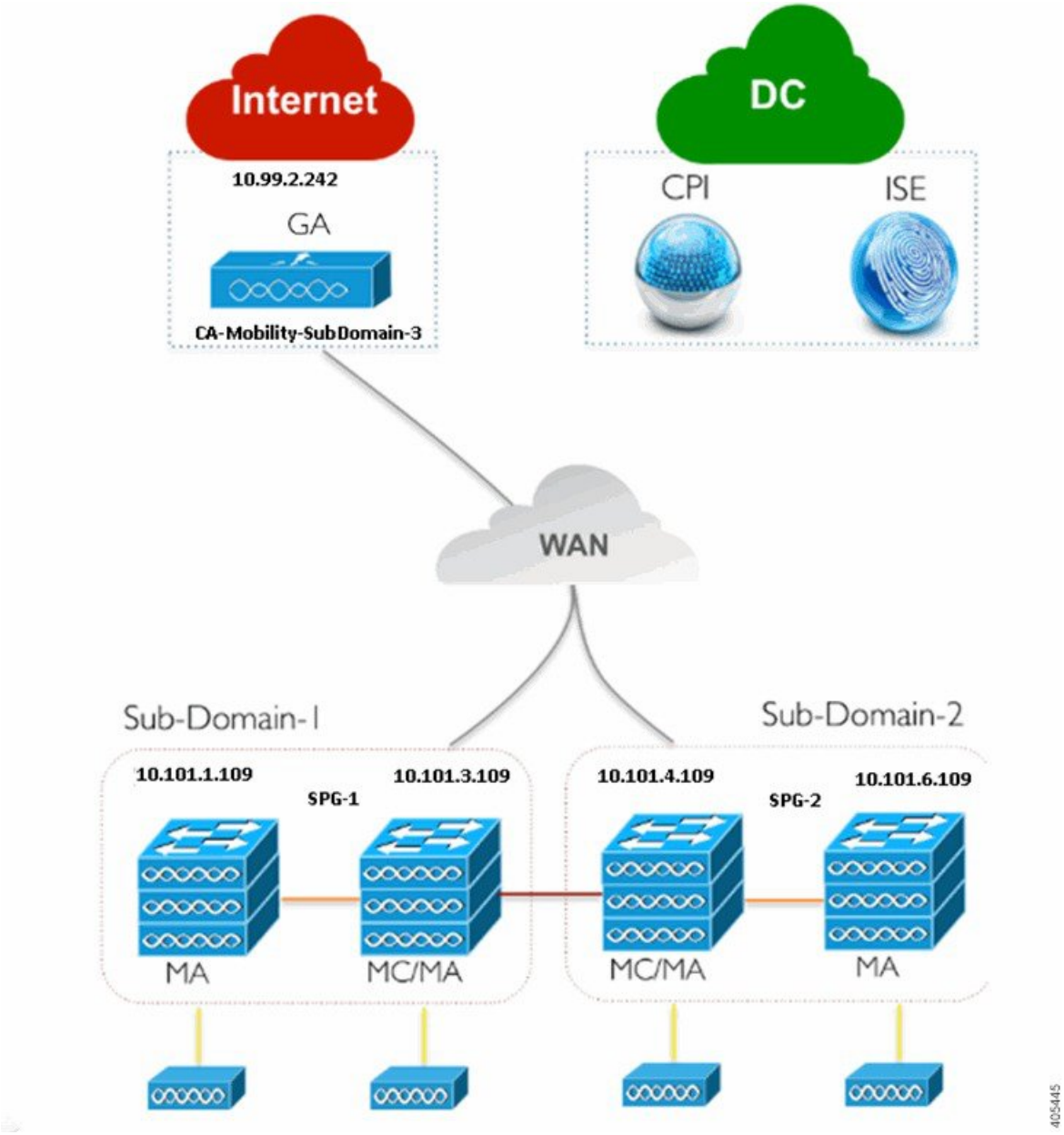
関連トピック

統合アクセス導入の前提条件 （890 ページ）
統合アクセス テンプレートを使用したデバイスの設定 （895 ページ）
フィールド参照：統合アクセス テンプレート （897 ページ）
例：コントローラなしの単一/マルチドメイン ワイヤレス ネットワーク （906 ページ）
例：コントローラベースの単一/マルチドメイン ワイヤレス ネットワーク （908 ページ）
例：集中型ワイヤレス キャンパス （910 ページ）

例：コントローラなしの単一/マルチドメイン ワイヤレス ネットワーク

次の図に、外部 WLC に依存せず MA および MC ロールに Catalyst スイッチを活用するコントローラのない導入モデルを示します。このコンバージドアクセス導入モデルは、大規模ブランチやキャンパスに適しており、Prime Infrastructure IOS-XE コントローラの大規模ネットワーク テンプレートを使用して実装できます。

図 *24 :* コントローラのない大規模ブランチ ネットワークのモデル



単一スイッチの小規模ネットワーク導入モデルで説明したように、すべてのデバイスに対するワイヤレス管理、WLAN、ワイヤレス ラジオ、およびゲスト WLAN の設定値を入力します。上の図に示すように、トポロジの MA、MC および GA に対する、ゲスト コントローラ設定値およびモビリティ設定値を示します。

表 *73 : MA*、*MC*、および *GA* に対するゲスト コントローラ設定値の例

データ フィールド	**MA**	**MC**	**GA**
Anchor Controller IP	10.99.2.242	10.99.2.242	10.99.2.242

データ フィールド	MA	MC	GA
Anchor Group Name	CA-Mobility-SubDomain-3	CA-Mobility-SubDomain-3	CA-Mobility-SubDomain-3
Foreign Controller	10.101.4.109	10.101.3.109	10.101.3.109

次の表に、上の図に示す SPG-1 での MA、MC、および GA のモビリティ設定値を示します。

表 *74 : MA*、*MC*、および *GA* に対するサンプルのモビリティ設定値

データ フィールド	MA	MC	GA
Role	Agent	Controller	Controller
Controller IP	10.101.3.109	10.101.3.109	—
Switch Peer Group Name	SPG-1	SPG-1	—
Mobility Agent IP(s)	—	10.101.1.109	—
Peer Controller IP(s)	—	10.101.4.109	—

上の図に示すように、SPG-2 の MA および MC に対し同じ手順を繰り返します。

モビリティ設定値を適用した後、単一スイッチの小規模ネットワーク導入モデルで説明したように、セキュリティ、AVC および QoS の設定値を入力します。

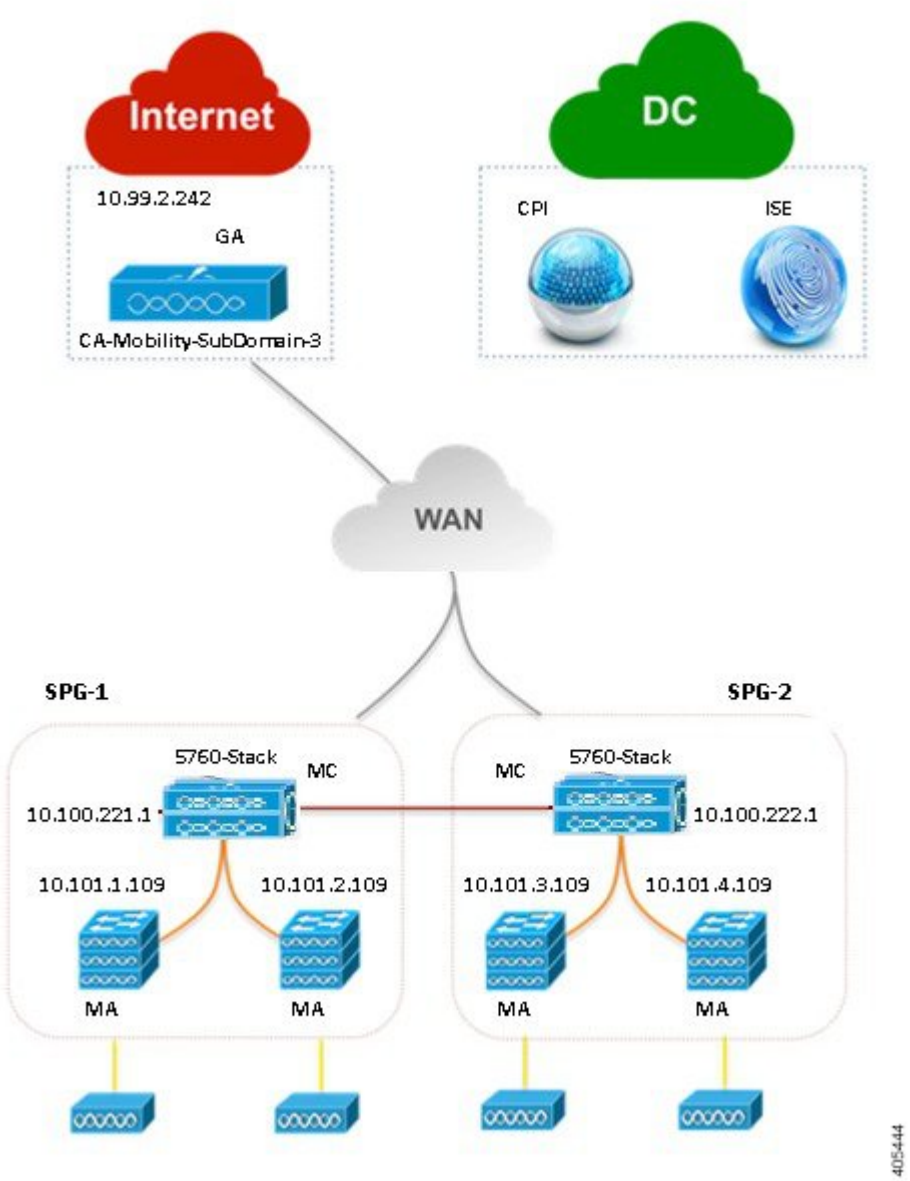
関連トピック

統合アクセス導入の前提条件 （890 ページ）
統合アクセス テンプレートを使用したデバイスの設定 （895 ページ）
フィールド参照：統合アクセス テンプレート （897 ページ）
例：コントローラなしの単一スイッチ ネットワーク （901 ページ）
例：コントローラベースの単一/マルチドメイン ワイヤレス ネットワーク （908 ページ）
例：集中型ワイヤレス キャンパス （910 ページ）

例：コントローラベースの単一/マルチドメインワイヤレスネットワーク

次の図に、MC として外部 5760 WLC を使用してコンバージドアクセスを展開するために同じ IOS-XE コントローラの大規模ネットワーク テンプレートを活用するコントローラベースの単一もしくはマルチドメイン導入モデルを示します。

図 *25 :* コントローラベースの大規模キャンパス モデル



コントローラのない単一もしくはマルチドメイン ワイヤレス導入モデルで説明したように、設定値を入力します。

関連トピック

統合アクセス導入の前提条件 （890 ページ）
統合アクセス テンプレートを使用したデバイスの設定 （895 ページ）
フィールド参照：統合アクセス テンプレート （897 ページ）
例：コントローラなしの単一スイッチ ネットワーク （901 ページ）

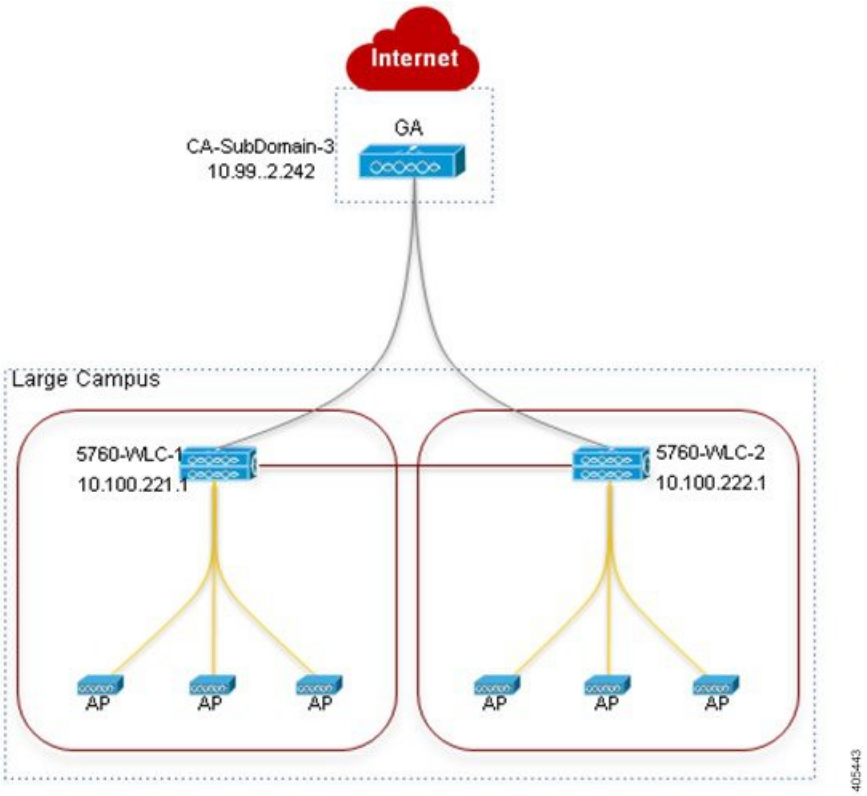
例：コントローラなしの単一/マルチドメイン ワイヤレス ネットワーク （906 ページ）
例：集中型ワイヤレス キャンパス （910 ページ）

例：集中型ワイヤレス キャンパス

Prime Infrastructure IOS-XE 中央集中型ワイヤレス テンプレートは、次世代 5760-WLC を使用して従来の無線導入モデルをサポートします。このモデルでは、ジェネレーション アクセス レイヤ スイッチは従来のイーサネット スイッチ モードで展開され、WLC および AP はこのモードで CAPWAP トンネリング メカニズムを使用してオーバーレイ ネットワークを構築します。

次の図に、IOS-XE 中央集中型テンプレートを使用する 5760-WLC ベースの中央集中型ワイヤレス展開を示します。

図 *26 :* 中央集中型キャンパス ネットワーク モデル



単一スイッチの小規模ネットワーク導入モデルで説明したように、すべてのデバイスに対するワイヤレス管理、WLAN、ワイヤレス ラジオ、およびゲスト WLAN の設定値を入力します。上の図に示すように、トポロジの SPG-1 の 5760 WLC および GA に対する、ゲスト コントローラ設定値およびモビリティ設定値を入力します。

表 *75 : 5760 WLC* および *GA* に対するサンプルのゲスト コントローラ設定値

データ フィールド	5760 WLC	GA
Anchor Controller IP	10.99.2.242	10.99.2.242
Anchor Group Name	CA-Mobility-SubDomain-3	CA-Mobility-SubDomain-3
Foreign Controllers	10.100.222.1	10.100.221.1; 10.100.222.1

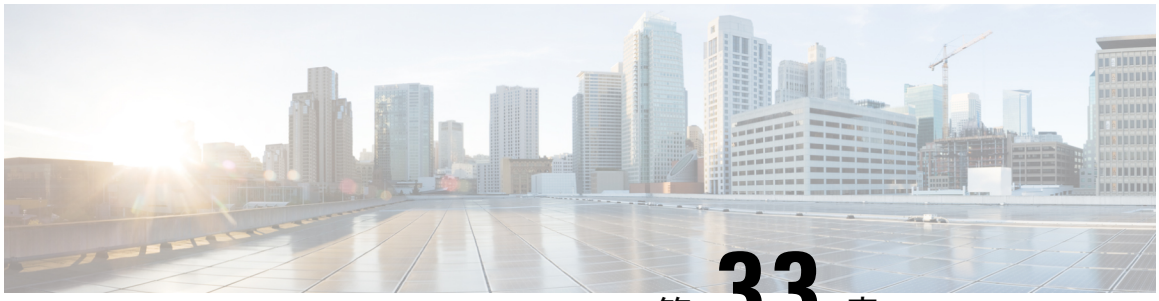
表 *76 : 5760 WLC* および *GA* に対するサンプルのモビリティ設定値

データ フィールド	5760 WLC	GA
Peer Controller IP(s)	10.100.222.1	—

上の図に示す、SPG-2 の 5760 WLC に対し同じ手順を繰り返します。モビリティ設定値を適用した後、単一スイッチの小規模ネットワーク導入モデルで説明したように、セキュリティ、AVC および QoS の設定値を入力します。

関連トピック

統合アクセス導入の前提条件 （890 ページ）
統合アクセス テンプレートを使用したデバイスの設定 （895 ページ）
フィールド参照：統合アクセス テンプレート （897 ページ）
例：コントローラなしの単一スイッチ ネットワーク （901 ページ）
例：コントローラなしの単一/マルチドメイン ワイヤレス ネットワーク （906 ページ）
例：コントローラベースの単一/マルチドメイン ワイヤレス ネットワーク （908 ページ）



第 33 章

Branch Threat Defense の設定

- Cisco Branch Threat Defense の概要 （913 ページ）
- サポート対象の IOS-XE プラットフォーム （913 ページ）
- サポート対象の IOS-XE バージョン （914 ページ）
- Branch Threat Defense を有効にするための前提条件 （914 ページ）
- Branch Threat Defense ウィザードの使用 （914 ページ）

Cisco Branch Threat Defense の概要

Cisco Branch Threat Defense は、保護を強化し、セキュリティ製品を重複して導入する必要がないことで時間と資金を節約するルータ セキュリティ テクノロジーです。このテクノロジーは、直接インターネット接続を使用してデータ センターをバイパスするブランチ オフィスにおけるセキュリティの脆弱性を軽減し、企業の支社、本社、およびデータ センターの間の通信を暗号化します。『Cisco Branch Threat Defense Guide』を参照してください。

Cisco Prime Infrastructure を使用して、規制コンプライアンスの使用例から開始して、Branch Threat Defense を設定し、ゾーンベースのファイアウォール（ZBFW）、Snort 侵入防御システム（IPS）、クラウド Web セキュリティ（CWS）、OpenDNS などのテクノロジーを設定できます。

関連トピック

サポート対象の IOS-XE プラットフォーム （913 ページ）
サポート対象の IOS-XE バージョン （914 ページ）
Branch Threat Defense を有効にするための前提条件 （914 ページ）
Branch Threat Defense ウィザードの使用 （914 ページ）

サポート対象の IOS-XE プラットフォーム

Branch Threat Defense 機能は、Cisco 4000 シリーズ サービス統合型ルータ（ISR）でサポートされます。

サポート対象の IOS-XE バージョン

Branch Threat Defense 機能は、Cisco IOS-XE リリース 15.5(3)S1（OpenDNS が設定されている場合は 16.3.1）および以降のリリースでサポートされます。

Branch Threat Defense を有効にするための前提条件

- この機能は、セキュリティ ライセンスを必要とするセキュリティ パッケージでのみ使用できます。ライセンスの取得については、シスコ サポートにお問い合わせください。
- Cisco 4000 シリーズ ISR に少なくとも 8 GB の RAM があることを確認してください。詳細については、『Security Configuration Guide for Branch Threat Defense』の「Virtual Service Resource Profile」の項を参照してください。
- プロビジョニング対象の各ルータには、ファイル システム上の同じ場所に Snort IPS OVA がすでに存在している必要があります。先に進む前に、「Copy OVA to Device」CLI テンプレートを使用して Snort IPS OVA をプロビジョニング対象の各デバイスに配布します。

関連トピック

サポート対象の IOS-XE プラットフォーム （913 ページ）
サポート対象の IOS-XE バージョン （914 ページ）
Branch Threat Defense ウィザードの使用 （914 ページ）

Branch Threat Defense ウィザードの使用

ステップ 1 **[サービス（Services）] > [ネットワーク サービス（Network Services）] > [Branch Threat Defense]** を選択します。

ステップ 2 [次へ（Next）] をクリックして設定を選択します。

ステップ 3 [設定の選択（Choose Configuration）] ページの説明を読み、[使用例の選択（Select a Use Case）] ドロップダウン リストから必要な使用例を選択します。

設定オプションは、選択した使用例によって異なります。

ステップ 4 必要な設定オプションを選択し、[次へ（Next）] をクリックします。

ステップ 5 設定するデバイスを選択し、[次へ（Next）] をクリックします。

ステップ 6 設定値を入力するか、または選択した使用例に応じて、インポート/エクスポート アイコンを使用して、**ZBFW**、**Snort IPS CLI**、**CWS**、および **OpenDNS** を設定します。

ステップ 7 [適用（Apply）] をクリックし、[次へ（Next）] をクリックして [CLI サマリー（CLI Summary）] タブに移動すると、デバイスおよびテンプレートの設定値を確認できます。

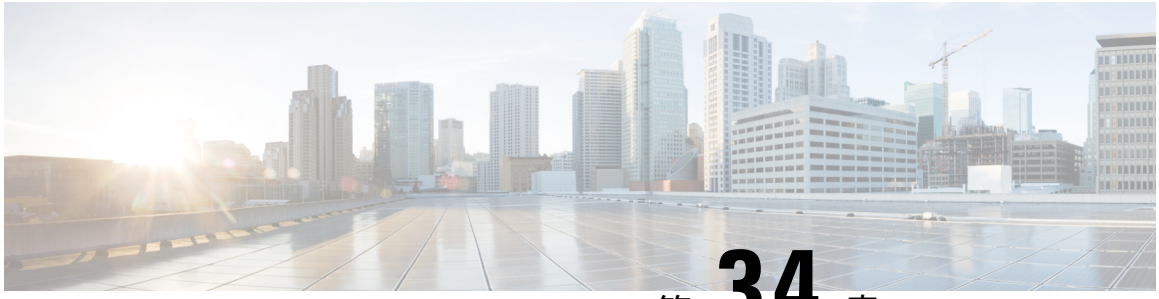
ステップ 8 [準備およびスケジュール（Prepare and Schedule）] タブを使用して導入ジョブのスケジュールを設定します。

ステップ 9 [次へ（Next）] をクリックし、[確認（Confirmation）] タブで [展開（Deploy）] をクリックして、Branch Threat Defense を導入します。

ステップ 10 [ジョブ ステータス（Job Status）] をクリックして [ジョブ ダッシュボード（Job Dashboard）] にジョブの詳細を表示します。

関連トピック

Cisco Branch Threat Defense の概要 （913 ページ）
サポート対象の IOS-XE プラットフォーム （913 ページ）
サポート対象の IOS-XE バージョン （914 ページ）
Branch Threat Defense を有効にするための前提条件 （914 ページ）



第 34 章

アクセス ネットワーク ワークフロー

- 概要 （917 ページ）
- Cisco アクセス ネットワーク ワークフローを使用するための前提条件 （918 ページ）
- サポートされるデバイス （918 ページ）

概要

Cisco Prime Infrastructure でのアクセス ネットワーク ワークフローは、企業の支社またはキャンパス ネットワーク内のルーティングされたアクセス ネットワークにおけるアクセス スイッチの展開を自動化します。これには、アクセス VLAN データベースの作成と管理、インターフェイス テンプレート管理、およびアクセス ポート設定が含まれます。アクセス ネットワーク ワークフローは、Cisco Catalyst 4500、3850、3650、2960XR、および 2960X の各シリーズのスイッチを使用したアクセス ネットワークの導入を完全に自動化します。さらに、自動デバイス検出に基づいたアクセス ポートの静的または動的なプロビジョニングも自動化されます。このワークフローは、該当するシスコのベスト プラクティス設定を自動的に展開することで労力と時間を削減し、管理を目的とした一元化されたネットワーク表示を提供します。

アクセス ネットワーク ワークフローは、次のタスクを自動化します。

- 複数のアクセス スイッチの同時設定：管理者が複数のアクセス スイッチを同時にプロビジョニングすることが可能で、これによりネットワーク プロビジョニングの労力が削減されます。シード デバイスからアクセス スイッチを自動的に検出できるため、ディストリビューション スイッチに接続しているすべてのアクセス スイッチを検出するための労力を最小限に抑えることができます。
- VLAN 管理：Cisco Prime Infrastructure は、アクセス レイヤで使用されるアクセス VLAN と音声 VLAN のデータベースを作成して維持できます。このデータベースはアクセス スイッチを設定するために使用され、VLAN 名の統一性を確保することにより VLAN の名称および ID の不一致エラーが回避されます。
- アクセス ポイントのプロビジョニング：テンプレートおよび VLAN を作成して適用し、以下の目的でアクセス ポートを自動的にプロビジョニングします。
  - 動的に検出可能なシスコ デバイスの受け入れ（Cisco IP Phone、Cisco アクセス ポイント、Cisco ビデオ監視カメラ、Cisco TelePresence、Cisco Digital Media Player など）。

- OUI または MAC アドレスに基づいて動的に検出できるシスコ以外のデバイスの検出。
- 動的に検出できないラップトップなどのデバイスのサポート。

- 適用可能なシスコのベスト プラクティス設定の自動的導入。

Cisco アクセス ネットワーク ワークフローを使用するための前提条件

Cisco アクセス ネットワーク ワークフローを正常に使用するには、ネットワーク デバイスおよびCisco Prime Infrastructure システムに関して次の前提条件が満たされていることを確認する必要があります。

- ルーティングされたアクセス ネットワーク：アクセス スイッチがレイヤ 3 インターフェイス経由でディストリビューション レイヤに接続されていることを確認します。
- 初期デバイス セットアップ：設定されている SSH/Telnet および SNMP を使用して Cisco Prime Infrastructure からデバイスに到達できる。
- デバイス オンボーディング：デバイスが Cisco Prime Infrastructure インベントリに追加されている。
- IOS ソフトウェア：デバイスが推奨されるソフトウェア バージョンを使用している（「サポートされるデバイス」を参照）。
- サポートされるプラットフォーム：デバイスは、サポートされる製品ファミリに属している必要があります（「サポートされるデバイス」を参照）。

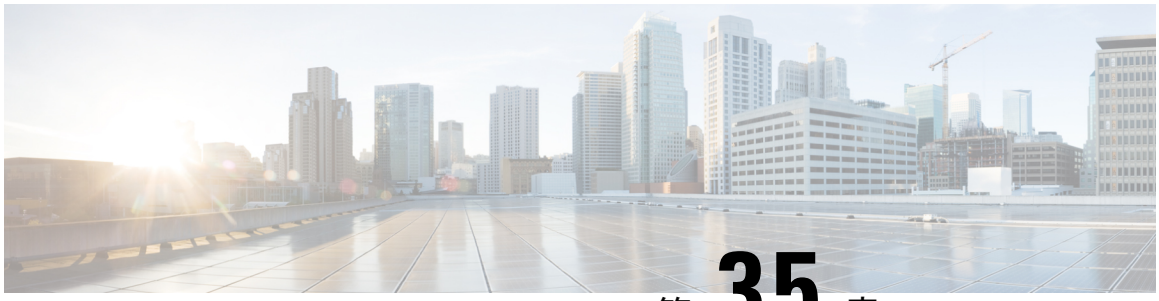
サポートされるデバイス

次の表は、アクセス ネットワーク ワークフローでサポートされるスイッチを示しています。

表 77 : サポートされるスイッチ

製品	SKU タイプ	モード	モジュール	最小ソフトウェア バージョン	最小ソフトウェア ライセンス
WS-C2960X	Copper/POE	スタンドアロン（Standalone）	-	IOS 15.2.2E	LANbase
WS-C2960X	Copper/POE	FlexStack	-	IOS 15.2.2E	LANbase
WS-C2960XR	Copper/POE	スタンドアロン（Standalone）	-	IOS 15.2.2E	IP Lite
WS-C2960XR	Copper/POE	FlexStack	-	IOS 15.2.2E	IP Lite

製品	SKU タイプ	モード	モジュール	最小ソフトウェア バージョン	最小ソフトウェア ライセンス
WS-C3650	Copper/POE	スタンドアロン（Standalone）	-	IOS-XE 3.7.3	IPBase
WS-C3650	Copper/POE	StackWise	-	IOS-XE 3.7.3	IPBase
WS-C3850	Copper/POE/mGig	スタンドアロン（Standalone）	-	IOS-XE 3.7.3	IPBase
WS-C3850	Copper/POE/mGig	StackWise	-	IOS-XE 3.7.3	IPBase
WS-C45xx-E	Copper/POE/mGig	スタンドアロン（Standalone）	47xx シリーズと 46xx シリーズのライン カードを搭載した、シングルおよびデュアル SUP（SUP7E または SUP8E）	IOS-XE 3.6.4 以降	IPServices
WS-C45xx-R+E	Copper/POE/mGig	スタンドアロン（Standalone）	47xx シリーズと 46xx シリーズのライン カードを搭載した、シングルおよびデュアル SUP（SUP7E または SUP8E）	IOS-XE 3.6.4 以降	IPServices



第 35 章

Application Visibility and Control（AVC）によるアプリケーション パフォーマンスの向上

• Application Visibility and Control（AVC）によるアプリケーション パフォーマンスの向上（921 ページ）

Application Visibility and Control（AVC）によるアプリケーション パフォーマンスの向上

デバイス ワーク センターからデバイスの機能設定を変更したり、ブランチのデバイスをセットアップしたりするために必要な一連のデバイス コンフィギュレーションを設計するには、Cisco Prime Infrastructure の設定テンプレートを使用します。

WSMA で AVC 機能を使用するためのデバイスの設定 （921 ページ）
AVC で使用するデータ ソースの設定 （933 ページ）
AVC データ重複除去の設定 （935 ページ）
Easy VPN サーバとは （938 ページ）
ScanSafe を使用した HTTP および HTTPS トラフィックのスキャンの有効化 （943 ページ）
DMVPN を使用した IPSec トポロジの設定 （949 ページ）
GETVPN を使用した IPSec トポロジの設定 （954 ページ）
ゾーンベースのファイアウォールを使用したインターフェイス グループ間のファイアウォール ポリシーの制御 （962 ページ）

WSMA で AVC 機能を使用するためのデバイスの設定

Prime Infrastructure では、主に Telnet または SSHv2 を介した CLI 方式を使用してデバイスを設定します。ASR および ISR デバイスの特定の機能の設定に WSMA （SSHv2 経由）を使用できます。Cisco Web サービス管理エージェントは、より効率的かつ堅牢な方法でデバイスを設定

できます。Prime Infrastructure は、ASR および ISR デバイスで、WSMA によるゾーン ベース ファイアウォールおよびアプリケーションの可視性の設定をサポートしています。

WSMA を介してゾーンベース ファイアウォールまたはアプリケーション可視性を設定するには、次の手順を実行します。

ステップ 1 管理トランスポート プロトコルとして Telnet ではなく SSHv2 を使用するために、Prime Infrastructure でデバイスを追加または編集します。

a) 自動検出を使用してデバイスを追加する場合は、SSH クレデンシャルを入力します。
b) デバイスを手動で追加する場合は、ステップ 2 でプロトコルとして SSH2 を選択します。

ステップ 2 デバイスが（SSH2 を使用するよう設定されていない）Prime Infrastructure によっても管理される場合は、デバイス クレデンシャルを次のように編集します。

a) [Inventory] > [Device Management] > [Network Devices] を選択します。
b) デバイスを選択して [Edit] をクリックします。
c) プロトコルを [SSH2] に変更します。
d) [Update] をクリックします。

ステップ 3 WSMA の設定プロファイルを次のように設定して、デバイスの WSMA プロファイルをアクティブ化します。

例：

```
#configure terminal
wsma agent config profile PIwsmaConfigServiceSSH
#exit
#wsma profile listener PIwsmaConfigServiceSSH
no wsse authorization level 15
transport ssh subsys wsma-config
#exit
```

ステップ 4 デバイスで次の CLI コマンドを使用して、設定アーカイブを設定します。これは WSMA でトランザクションの設定とロールバックの処理に使用されます。

例：

```
#configure terminal
archive
log config
hidekeys
path flash:roll
maximum 5
#end
```

詳細については、次のガイドを参照してください。

- 『WSMA Configuration Guide』
- 『Cisco IOS Configuration Fundamentals Command Reference Guide』

AVC とは

アプリケーション可視性（アプリケーションの表示）機能を使用すると、特定のインターフェイスでトラフィックをモニタし、パフォーマンスおよび帯域幅統計情報のレポートを生成できます。この情報はCisco Prime Infrastructure のさまざまなダッシュレットとレポートに使用されます。デバイスはこれらのレポートCisco Prime Infrastructureをに送信し、各レポートはCisco Prime Infrastructureダッシュレットおよびレポートのサブセットに情報を提供します。Cisco Prime Infrastructure CLI (Telnet または SSH 経由) または WSMA を使用して、アプリケーションの可視性を設定できます。WSMA を使用すると、より効率的かつ堅牢な方法でアプリケーションの可視性を設定できます。したがって、アプリケーションの可視性の設定には WSMA プロトコルを使用することを推奨します。Cisco Prime Infrastructure での WSMA の使用に関する詳細を参照してください。

設定を簡素化するため、アプリケーションの可視性機能は、4 種類のメトリックおよびNetFlow レポートに分割されます。

レポート	説明
Traffic Statistics	ユーザ単位およびインターフェイス単位で、NBAR で認識された各アプリケーションが消費する帯域幅の統計情報を送信します。このレポートの情報が、「上位 N 個のアプリケーション」、「アプリケーション帯域幅レポート」、「上位 N 個のクライアント」などの形で Cisco Prime Infrastructure のさまざまなアプリケーション帯域幅ダッシュレットおよびレポートに表示されます。
HTTP URL 可視性（HTTP URL Visibility）	HTTP ベースのトラフィックのパフォーマンスおよび帯域幅レポートを送信します。このレポートの情報は、「ヒット件数の上位 N 個の URL」および「応答時間の上位 N 個の URL」として Cisco Prime Infrastructure のさまざまな URL ダッシュレットおよびレポートに表示されます。 （注） HTTP URL の可視性ツールは ISR-G2 デバイスではサポートされません。
Application Response Time	TCP トラフィックのパフォーマンス関連情報を送信します。このレポートの情報は、「アプリケーション ART 分析」、「トランザクション時間の下位 N 個のクライアント」などの形で Cisco Prime Infrastructure のさまざまな応答時間ダッシュレットおよびレポートに表示されます。
音声/ビデオ メトリック（Voice/Video Metrics）	RTP ベースの音声/ビデオ トラフィックのさまざまな RTP 主要パフォーマンス評価指標を送信し、その情報が音声/ビデオ カテゴリの「パケット損失の下位 N 個の RTP ストリーム」として Cisco Prime Infrastructure のダッシュレットおよびレポートに表示されます。

WSMA で AVC 機能を使用するためのデバイスの設定 （921 ページ）
NBAR プロトコル パックとは （927 ページ）

アプリケーションの可視性テンプレートの作成 （928 ページ）
インターフェイスでデフォルトのアプリケーションの可視性を有効にする （929ページ）

AVC がサポートされるデバイス

アプリケーションの可視性機能は次のプラットフォームでサポートされています。

- Cisco IOS-XE Release 15.3(1)S1 以降の ASR 1000 シリーズ プラットフォーム
- 次に示す、Cisco IOS リリース 15.2(4)M2 以降の ISR G2 プラットフォーム
  - Cisco 1900 シリーズ サービス統合型ルータ
  - Cisco MWR 1900 モバイル ワイヤレス ルータ
  - Cisco 2900 シリーズ サービス統合型ルータ
  - Cisco 3900 シリーズ サービス統合型ルータ
  - Cisco 812 CiFi サービス統合型ルータ
  - Cisco 819 Non-Hardened サービス統合型ルータ
  - Cisco 819 Hardened サービス統合型ルータ
  - Cisco 819 Hardened 3G - Dual Radio 802.11n WiFi ISR
  - Cisco 861、861W サービス統合型ルータ G2
  - Cisco 867、867W サービス統合型ルータ G2
  - Cisco 866VAE サービス統合型ルータ
  - Cisco 880 3G サービス統合型ルータ G2
  - Cisco 881、881W サービス統合型ルータ G2
  - Cisco 881SRST、881SRSTW サービス統合型ルータ G2
  - Cisco 881W、881WD サービス統合型ルータ
  - Cisco 886、886W サービス統合型ルータ G2
  - Cisco 886SRST、886SRSTW サービス統合型ルータ G2
  - Cisco 886VA、886VAG サービス統合型ルータ G2
  - Cisco 886VA-W サービス統合型ルータ G2
  - Cisco 887、887W サービス統合型ルータ G2
  - Cisco 887V サービス統合型ルータ G2
  - Cisco 886VA サービス統合型ルータ G2
  - Cisco 887VA M サービス統合型ルータ G2
  - Cisco 887VA-W サービス統合型ルータ G2
  - Cisco 888、888W、888GW サービス統合型ルータ G2
  - Cisco 888ESRST、888ESRSTW サービス統合型ルータ G2
  - Cisco 888E、888EW サービス統合型ルータ G2
  - Cisco 888EA サービス統合型ルータ G2
  - Cisco 888SRST、888SRSTW サービス統合型ルータ G2
  - Cisco 891、891W サービス統合型ルータ G2
  - Cisco 892、892W サービス統合型ルータ G2
  - Cisco 892F、892FW サービス統合型ルータ
  - Cisco C892FSP サービス統合型ルータ

- Cisco C897VA サービス統合型ルータ
- Cisco C897VAW サービス統合型ルータ
- Cisco C891F サービス統合型ルータ
- Cisco C881 サービス統合型ルータ
- マルチモード 4G LTE ルータ搭載 Cisco C899 セキュア ギガビット イーサネット
- 4 ポート LAN サービス統合型ルータ搭載 Cisco 800M
- 8 ポート LAN サービス統合型ルータ搭載 Cisco 800M
- Cisco C896VA サービス統合型ルータ

- Cisco IOS-XE リリース 16.3 以降のシスコ サービス統合型仮想ルータ（ISRv）プラットフォーム
- Cisco IOS-XE リリース 16.6.1 以降の Cisco ISR 1000 プラットフォーム
- Cisco IOS-XE Release 15.3(2)S 以降の Cisco ISR 4200 および 4400 シリーズ プラットフォーム
- Cisco IOS-XE Release 15.3(2)S 以降の CSR プラットフォーム

Application Visibility and Control の使用時の前提条件

アプリケーションの可視性機能をアクティブ化すると、デバイスのパフォーマンスに影響を与える場合があります。潜在的影響を最小限に抑えるため、テンプレートではモニタするトラフィック インターフェイスと生成するレポートを選択できます。

アプリケーションの可視性を設定する方法は、プラットフォームおよびIOSリリースによって異なります。新しい IOS リリースでは、Application Visibility and Control（AVC）の設定に、よりパフォーマンスの高い新しいメカニズムを使用できます。したがって、15.4(1)S より前の IOS-XE リリースを実行する ASR 1000、CSR または ISR 4400 のプラットフォームを IOS-XE リリース 15.4(1)S 以降にアップグレードする場合、または 15.4(1)T より前の IOS リリースを実行する ISR-G2 プラットフォームを IOS リリース 15.4(1)T 以降にアップグレードする場合は、デバイスで AVC を再設定することを推奨します。

ネットワークでのアプリケーションの可視性を設定する方法は次のとおりです。

1. （任意）CLI ではなく WSMA プロトコルを使用してデバイスが設定されるようにするには、デバイスで WSMA を設定します。WSMA はより堅牢な設定メカニズムを提供します。
2. デバイスで最新の NBAR プロトコル パックが実行されていることを確認します。
3. デバイスでアプリケーションの可視性をアクティブ化する前に、デバイスへのリソース（CPU とメモリ）の潜在的な影響を推測します。

テンプレートを作成してネットワーク全体にプッシュするか、デバイス ワーク センターからインターフェイスの AVC を有効化することによって、デバイスでアプリケーションの可視性をアクティブ化します。

（注） アプリケーション トラフィック フローの可視性を確認するには、次を参照してください。
https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Aug2014/CVD-ApplicationMonitoringUsingNetFlowDesignGuide-AUG14.pdf

ASR デバイス上の CPU、メモリ、およびネットワーク リソースの推測

ASR デバイスでアプリケーションの可視性機能を展開する場合は、レディネス アセスメント機能を使用すると、CPU 消費量、メモリ使用量、および NetFlow エクスポート トラフィックを推測することができます。ASR デバイスのこれらのリソースの需要を、一般的な定義済みトラフィック プロファイルおよびデバイスのインターフェイス速度に基づいて分析する際は、DRE が役立ちます。

DRE は、次のモジュールが 1 つ以上インストールされた、Cisco IOS-XE Release 15.3(1)S1 以降を実行するすべての ASR でサポートされます。

- cevModuleASR1000ESP5
- cevModuleASR1000ESP10
- cevModuleASR1000ESP20
- cevModuleASR1001ESP
- cevModuleASR1002FESP

特定のデバイス上のリソース使用率を推測するには、次の手順を実行します。

ステップ 1 [サービス（Services）] > [アプリケーションの可視性と制御（Application Visibility and Control）] > [レディネス アセスメント（Readiness Assessment）] を選択します。

ステップ 2 推測するデバイスの [Interface] 列で、下矢印アイコンをクリックします。

アプリケーションの可視性機能をサポートするインターフェイスのみがリストに表示されます。

ステップ 3 [インターネット プロファイル（Internet Profile）] または [エンタープライズ プロファイル（Enterprise Profile）] を選択します。デバイス リソースの推測は、一般的なトラフィック プロファイルに基づきます。一般的なサービスプロバイダー トラフィックの場合は [Internet Profile]、一般的な企業トラフィックの場合は [Enterprise Profile] を選択してください。

ステップ 4 リソース使用率を推測するインターフェイスを選択します。

表示される速度は、各インターフェイスに対して現在設定されている速度です。別の速度を推測のベースにする場合は、[Speed (Mbps)] をクリックして別の値を入力します。

ステップ 5 [Get Estimates] をクリックします。

[Estimated Resource Usage] グラフに、CPU およびメモリの現在の使用率、追加使用率、および総使用率に加えて、これらのリソースのしきい値制限が表示されます。推測される最大 NetFlow エクスポート トラフィックも表示されます。AVC がすでに有効になっているデバイスについては、現在および追加の使用率のみが表示されます。

リソース使用率がしきい値制限を超えている場合は、次の方法で問題のデバイスを最適化してください。

- 現在の CPU 使用率を減らす
- 設定メモリを増やす
- 設定されたインターフェイス速度を低減する
- 別のデバイスにトラフィックをリダイレクトする

ルータの DMVPN 詳細の表示

ルータの DMVPN 詳細を表示するには、次の手順を実行します。

ステップ 1 **[サービス（Services）] > [アプリケーションの可視性と制御（Application Visibility and Control）] > [DMVPN モニタ ホーム（DMVPN Monitor Home）]** を選択し、DMVPN とアクティブなスポーク カウントをサポートするルータの詳細を表示します。

ステップ 2 デバイス名をクリックし、VRF、ローカル トンネル IP、トンネル インターフェイス番号、およびスポーク カウントを含めたハブの詳細を表示します。

ステップ 3 [スポークの詳細の表示（Show Spoke Details）] ボタンをクリックし、選択したハブのスポークの詳細を表示します。

NBAR プロトコル パックとは

アプリケーションの可視性レポートを作成するデバイスの機能は、NBAR テクノロジーに基づきます。Network-Based Application Recognition（NBAR）とは、多種多様なプロトコルおよびアプリケーション（動的な TCP/ユーザ データグラム プロトコル（UDP）ポート割り当てを使用する Web ベースなどの分類困難なアプリケーションおよびプロトコルを含む）を認識し、分類する分類エンジンです。

NBAR は新しいアプリケーションとプロトコルをサポートするように頻繁に更新され、NBAR のソフトウェア アップデートはプロトコル パックと呼ばれます。

NBAR プロトコル パックの詳細とそのアップグレード方法の詳細。

デバイスで NBAR プロトコル パックをアップグレードする際には、対応する Prime Infrastructure のアップデートを実行することで、デバイスでのサポート対象プロトコルおよびアプリケーションによって Prime Infrastructure を更新する必要があります。

これを行うために、新しいプロトコル パックがリリースされると、定期的な Prime Infrastructure のソフトウェア アップデート（UBF ファイル）が発行されます。デバイスで NBAR プロトコル パックをアップグレードした後、Prime Infrastructure もまた最新のプロトコルで更新されるように、Prime Infrastructure のソフトウェア アップグレードを使用する必要があります。

ネットワークには常に、さまざまな Cisco IOS ソフトウェア リリースおよびさまざまなプロトコル パック リリースを実行しているプラットフォーム（ISR-G2/ASR）が含まる可能性があります。アプリケーション可視性レポートを生成するさまざまなデバイスで、別々のプロトコル

パック リリースを同時に使用することは推奨されません。ただし、異なるバージョンのNBARプロトコルパックを実行する複数のデバイスにアプリケーション可視性テンプレートを展開する際に、各デバイスでテンプレートのフィルタリング条件として定義されたサポート対象プロトコル/アプリケーションのサブセットのみを設定することで、Prime Infrastructure はこれに対応できます。

詳細については、『NBAR Configuration Guide』を参照してください。

アプリケーションの可視性テンプレートの作成

アプリケーションの可視性モニタリング ポリシーは、選択したインターフェイス グループで定義されます。テンプレートを定義する場合は、定義したインターフェイスロール オブジェクトが、トラフィックをモニタしてNetFlow レポートを生成するインターフェイス グループに一致していることを確認します。

アプリケーションの可視性テンプレートを作成するには、次の手順を実行します。

ステップ 1 [設定（Configuration）]>[テンプレート（Templates）]>[機能およびテクノロジー（Features & Technologies）]>[アプリケーションの可視性（Application Visibility）]>[AVC 設定（AVC Configuration）] を選択します。

ステップ 2 [Template Basic] 領域で、適切なフィールドに一意の名前と説明を入力します。

ステップ 3 [Validation Criteria] 領域で、リストからデバイス タイプを選択し、OS バージョンを入力します。

ステップ 4 [Template Detail] 領域で、ドロップダウン リストからインターフェイス ロールを選択します。インターフェイス ロールは、トラフィックをモニタしてアプリケーションの可視性レポートを作成する対象のインターフェイス グループを示します。

ステップ 5 [Traffic Statistics] 領域では、トラフィック統計情報のレポートを作成するためにモニタするトラフィックを決定できます。データ パケットの統計情報を収集しない場合は [Off] オプション ボタンを選択します。

a) IP アドレス/サブネットを選択します。IPv4 トラフィックに対してのみレポートを生成できます。必要最小限のフィルタ セットを設定することを推奨します。

ステップ 6 [HTTP URL Visibility] 領域で、レポートを作成するためにモニタするトラフィックを選択できます。URLの統計情報を収集しない場合は、[オフ（Off）] オプション ボタンをオンにします。

a) IP アドレス/サブネットを選択します。モニタする特定の IPv4 アドレスまたはサブネットのセットを選択できます。

b) 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。モニタする特定のアプリケーション群を選択できます（モニタ可能なアプリケーションは最大で 32 個です）。デフォルトでは、すべてのエンタープライズ関連の HTTP ベースのアプリケーションがリストに含まれます。

ステップ 7 [Application Response Time] 領域では、アプリケーション応答時間レポートを作成するためにモニタするトラフィックを決定できます。また、レポートのサンプリング オプションを設定することもできます。ART メトリックを収集しない場合は、[Off] オプション ボタンを選択します。

a) IP アドレス/サブネットを選択します。モニタする特定の IPv4 アドレスまたはサブネットのセットを選択できます。

b) 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。モニタする特定のアプリケーション群を選択できます（モニタ可能なアプリケーションは最大で 32 個です）。デフォルトでは、すべての TCP トラフィックがモニタされます。

c) [Advanced Options] で、ドロップダウン リストからサンプリング レートを選択します。大規模な環境で、すべての TCP カンバセーションのパフォーマンス評価指標を収集すると、デバイス上のリソース消費量が大きくなることがあります。サンプリング オプションでは、「n」ごとに「1」の TCP カンバセーションでパフォーマンス評価指標を収集することで、リソース消費量をさらに最適化できます。この拡張オプションは、サンプリングのアクティブ化とツールのサンプリング レートの選択に使用できます。サンプリングのアクティブ化は結果の精度を低下させる原因となるため、サンプリングをアクティブ化することは推奨されません。サンプリングは、デバイス上のリソース消費量を制限する必要がある場合に使用してください。

（注） サンプリング オプションは ISR-G2 ルータには適用されません。ISR-G2 ではこのオプションは無視されます。

ステップ 8 [Voice/Video metrics] 領域では、音声/ビデオ レポートを作成するためにモニタするトラフィックを決定できます。音声/ビデオ メトリックを収集しない場合は、[Off] オプション ボタンを選択します。

a) IP アドレス/サブネットを選択します。モニタする特定の IPv4 アドレスまたはサブネットのセットを選択できます。

（注） すべての UDP トラフィックがモニタされない限り、ISR-G2 ルータでは IP フィルタリングがサポートされません。

b) ドロップダウン リストから音声/ビデオアプリケーションを選択します。モニタする特定のアプリケーション群を選択できます（モニタ可能なアプリケーションは最大で 32 個です）。デフォルトでは、RTP のエンタープライズ関連アプリケーションがすべてモニタされます。

ステップ 9 [Save as New Template] をクリックします。

インターフェイスでデフォルトのアプリケーションの可視性を有効にする

デバイス ワーク センターから、各インターフェイスで生成されたレポートを表示し、選択したインターフェイスでアプリケーションの可視性のデフォルト設定を有効または無効にすることができます。

デバイスにアプリケーションの可視性の設定が展開されていない場合や、アプリケーションの可視性のデフォルト設定が展開されている場合（一連のデフォルト パラメータですべてのメトリックが収集される場合）は、デバイス ワーク センターを使用すると、デバイスのインターフェイスを選択して、そのインターフェイスのデフォルト設定を有効または無効にすることで、デバイスでアプリケーションの可視性のデフォルト設定を有効または無効にすることができます。

（注） デバイスにアプリケーションの可視性テンプレートを導入すると、デバイス ワーク センターから有効化したアプリケーションの可視性のデフォルト設定は、アプリケーションの可視性テンプレートの設定によって上書きされます。

デフォルト設定では、該当するすべての IPv4 トラフィックで収集可能な可視性メトリックをすべて収集します。

アプリケーションの可視性機能は次のプラットフォームでサポートされています。

- Cisco IOS-XE Release 15.3(1)S1 以降の ASR プラットフォーム
- Cisco IOS Release 15.2(4)M2 以降の ISR G2 プラットフォーム
- Cisco IOS-XE Release 15.3(2)S 以降の ISR G3 プラットフォーム
- Cisco IOS-XE Release 15.3(2)S 以降の CSR プラットフォーム
- Cisco IOS-XE リリース 16.3 以降のシスコ サービス統合型仮想ルータ（ISRv）プラットフォーム
- Cisco IOS-XE リリース 16.6.1 以降の Cisco ISR 1000 プラットフォーム

（注） Cisco IOS-XE15.3(1)S1 を実行する ASR プラットフォームでのアプリケーションの可視性の設定は、Cisco IOS-XE15.3(2)S 以降のリリースでの設定とは異なります。ASR プラットフォームの Cisco IOS リリースを、Cisco IOS-XE15.3(1)S1 から Cisco IOS-XE Releases 15.3(2)S 以降にアップグレードした後は、デバイスでアプリケーションの可視性を再設定することを推奨します。

デバイスに設定されたアプリケーションの可視性のデフォルト設定プロファイルを変更するには、最初にすべてのインターフェイスでアプリケーションの可視性ポリシーを無効にしてから、選択したインターフェイスで新しいプロファイルを使って再度有効化します。

特定のインターフェイスでアプリケーションの可視性のデフォルト設定を有効または無効にするには、次の手順を実行します。

ステップ 1 [インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ネットワーク デバイス（Network Devices）] を選択します。

ステップ 2 リストからデバイスを選択したら、[Configuration] をクリックします。[Feature Configuration] ペインが表示されます。

ステップ 3 [アプリの可視性と制御（App Visibility & control）] フォルダを展開して、[アプリの可視性（App Visibility）] を選択します。

ステップ 4 次のいずれかを実行します。

- インターフェイスで設定済みの AVC プロファイルをアクティブ化するには、1 つ以上のインターフェイスを選択し、[Enable App Visibility] をクリックして必要なプロファイルを選択します。選択されていない 1 つ以上のインターフェイスに別のプロファイルが適用されている場合、警告メッセージが表示され、別のプロファイルが適用されている未選択のすべてのインターフェイスでプロファイルの適用が解除されます。
- デバイスの現在のアプリケーションの可視性設定を確認するには、インターフェイス リストを使用します。[App Visibility Policy] 列に、インターフェイスに現在適用されているプロファイルとポリシーが表示されます。

  （注） アプリケーションの可視性機能では、アプリケーションの可視性インターフェイスにユーザ定義の AVC ポリシーがインターフェイスごとに表示されます。

表示されるオプションは複数あります。

- アプリケーションの可視性テンプレートを使用するインターフェイスにアプリケーションの可視性制御が設定されている場合は、テンプレート名が表示されます。
- 「ワンクリック」オプションを使用するインターフェイスにアプリケーションの可視性制御が設定されている場合は、設定済みの AVC プロファイル名が表示されます。
- アプリケーションの可視性制御が、CLI を使用して手動でアウトオブバンドに設定されている場合は、設定済みのポリシーマップ名または Performance Monitor のコンテキスト名前が表示されます。

（注） 視覚的に表示される列（[App Visibility Status]）は、AVC がインターフェイスで現在アクティブかどうかを示します。また、インターフェイスで AVC を実行できない場合や、インターフェイスで AVC が誤って設定されている場合（NetFlow を Prime Infrastructure 以外のサーバに送信するように設定されている AVC など）も、この列に示されます。

- 選択したインターフェイスでアクティブ化した任意の AVC プロファイルを無効にするには、[アプリの可視性の無効化（Disable App Visibility）] をクリックします。

（注） AVC の有効化または無効化時には、実際のプロビジョニングの実行前にポップアップ メッセージが表示されます。ポップアップ メッセージの [CLI preview] タブを選択すると、デバイスにプッシュされる CLI のリストが生成されます。

（注） または、**[サービス（Services）]** > **[アプリケーションの可視性と制御（Application Visibility & Control）]** > **[インターフェイスの設定（Interfaces Configuration）]** から、デバイスの AVC を有効または無効にすることもできます。

HA が IPv4 仮想 IP アドレスを使用して設定されている場合、AVC がデバイスまたはインターフェイスで有効になっている際に、同じ仮想 IP アドレスが設定で自動的に取得されます。

AVC を使用したトラフィック フローのトラブルシューティング

モニタ対象インターフェイスを通過するすべてのフローでアプリケーションの可視性データを収集できます。ただし、これはデバイスのパフォーマンスに大きな影響を与える可能性があるため、アプリケーションの可視性データは集約されて収集されます。特定フローの詳細なトラブルシューティングを行う場合は、デバイスでアプリケーションの可視性のトラブルシューティングセッションをアクティブ化できます。セッションは、特定のインターフェイスと特定のトラフィックでアクティブ化されます。これによりフローに基づくレベルで非集約情報を収集でき、Prime Infrastructure に Raw NetFlow レポートが提供されます。この情報は、後で特定のフローを分析する際に使用できます。

アプリケーションの可視性トラブルシューティング機能では次のことが可能です。

- 特定のインターフェイスのトラブルシューティングセッションの作成およびアクティブ化
- 特定のインターフェイスのトラブルシューティングセッションの非アクティブ化および削除

注意 サーバのオーバーロードを回避するため、設定するアクティブなトラブルシューティングセッションは10以下にすることを推奨します。ISR-G2プラットフォームではアプリケーション トラブルシューティングはサポートされません。

（注） Cisco IOS-XE Release 15.3(1)S1 を実行する ASR プラットフォームでのトラブルシューティングセッションの設定は、Cisco IOS-XE Release15.3(2)S 以降のリリースでの設定とは異なります。設定後に ASR プラットフォームの Cisco IOS リリースを、Cisco IOS-XE Release 15.3(1)S1 から Cisco IOS-XE Release 15.3(2)S 以降にアップグレードした場合は、デバイスでアクティブなトラブルシューティングセッションを非アクティブ化してから再度アクティブ化することを推奨します。

アプリケーションの可視性のトラブルシューティングを行うには、次の手順を実行します。

ステップ 1 [Services] > [Application Visibility & Control] > [Application Troubleshooting] の順に選択します。

ステップ 2 [AVC トラブルシューティング セッション（AVC Troubleshooting Session）] ページで、[追加（Add）] をクリックしてセッション名を入力します。

ステップ 3 [送信元/宛先 IP（Source/Destination IPs）] フィールドで [編集（Edit）] をクリックし、ドロップダウン リストから送信元および宛先の IP アドレスを選択します。IP トラフィックを選択して、その特定の IP トラフィックのアプリケーションの可視性のトラブルシューティング情報を収集できます。すべての IPv6 トラフィック、すべての IPv4 トラフィック、または特定の IPv4 アドレス/サブネットを選択できます。IP 制約ペアのリストを選択することもできます。この場合、各ペアによってトラフィックの送信元と宛先 IP の双方向の対称条件が指定されます。たとえば、Any IPv4 <=> IPv4 subnet 192.168.0.0/16 ペアは、192.168.0.0/16 から他の IP へのフローおよびその逆のフロー（任意の IP アドレスから 192.168.0.0/16）のすべてに一致します。複数のペア条件を追加できます。

ステップ 4 IP 制約を IP 送信元/宛先ペアの形式でさらに追加するには、[Select Source Destination] ダイアログボックスの [+] アイコンをクリックします。

（注） ペアになっている IP アドレスは両方が同じ IP バージョンである必要があります。

ステップ 5 [OK] をクリックします。

ステップ 6 [Device Table] リストからデバイスを選択します。

ステップ 7 [Interface Table] リストからインターフェイスを選択します。

ステップ 8 オブジェクトセレクタ ダイアログボックスからアプリケーションを選択します。アプリケーションを選択する際に、使用可能なリストのカテゴリ、サブカテゴリ、暗号化アプリケーション、およびトンネル アプリケーションを組み合わせることができます。アプリケーション、カテゴリ、または属性を32個まで選択できます。

ステップ 9 [Save] をクリックすると、セッションが自動的にアクティブ化されます。

ステップ 10 トラブルシューティング セッションをアクティブ化したら、[Launch Report] をクリックして Raw NetFlow レポートを生成します。

AVC トラブルシューティング セッションのアクティブ化

非アクティブなトラブルシューティング セッションをアクティブ化したり、既存のトラブルシューティング セッションを非アクティブ化したりすることができます。

トラブルシューティングセッションをアクティブ化または非アクティブ化するには、次の手順を実行します。

ステップ 1 [Services] > [Application Visibility & Control] > [Application Troubleshooting] の順に選択します。

ステップ 2 リストからトラブルシューティング セッションを選択し、[アクティブ化（Activate）] または [非アクティブ化（Deactivate）] をクリックします。

ステップ 3 **[保存（Save）]** をクリックします。

AVC トラブルシューティング セッションの編集

非アクティブなトラブルシューティングセッションを編集または削除できます。（アクティブなセッションは、編集または削除する前に非アクティブ化する必要があります）。

トラブルシューティング セッションを編集または削除するには、次の手順を実行します。

ステップ 1 [Services] > [Application Visibility & Control] > [Application Troubleshooting] の順に選択します。

ステップ 2 次のいずれかを実行します。

a) リストからセッションを選択して [Edit] をクリックします。

注意 サーバのオーバーロードを回避するため、設定するアクティブなトラブルシューティングセッションは 10 以下にすることを推奨します。

b) トラブルシューティング セッションを編集および保存して、[Activate] をクリックします。

c) トラブルシューティング セッションを削除するには、リストからセッションを選択して [Delete] をクリックします。

AVC で使用するデータ ソースの設定

Prime Infrastructure は、デバイス、パフォーマンス、保証データを正確に収集およびレポート作成するうえで、さまざまなソースに依存しています。これらのソースとしては、NAM などの専門モニタリング デバイスのほか、Cisco Medianet、NetFlow、Network Based Application Recognition（NBAR）、Performance Monitoring（PerfMon）、Performance Agent などの通常デバイス上で実行されるプロトコルなどもあります。

アクティブなソースから正確なデータのみが収集されるようにするには、これらのソースの管理が必要となります。[Data Sources] ページを使用すれば、現在のデータ ソースを確認し、無効になったデータ ソースを削除することができます。

[データ ソース（Data Sources）] ページを使用することにより、Prime Infrastructure の現在のデータ ソースを表示できます。

ステップ 1 **[サービス（Services）] > [アプリケーションの可視性と制御（Application Visibility & Control）] > [データ ソース（Data Sources）]**の順に選択します。Prime Infrastructure は各データ ソースを一覧表示するサマリ ページを表示します。

- [デバイス名（Device Name）]：データ ソースのホスト名
- [データ ソース（Data Source）]：データ ソースの IP アドレス
- [タイプ（Type）]：ソースが Prime Infrastructure に送信しているデータのタイプ（「NetFlow」など）
- [エクスポートするデバイス（Exporting Device）]：データを Prime Infrastructure にエクスポートするデバイスの IP アドレス
- [直近の 5 分間の読み取りフロー レート（Last 5 min Flow Read Rate）]：直近の 5 分間に Prime Infrastructure がこのソースから受け取ったデータのフロー レートハイパーリンクをクリックすると、上位 5 つのフロー データ ソースのフロー レートとフロー数を表形式またはグラフィック形式で表示できます。また、特定のデータ ソースに対応するハイパーリンクをクリックすると、そのデータのフロー レートとフロー数を表形式またはグラフィック形式で表示することもできます。
- [前回のアクティブ時間（Last Active Time）]：このソースから最後にデータを受け取った日付と時刻

ステップ 2 データ ソースの設定テンプレート、またはエクスポート元デバイスのデバイス 360 度ビューの詳細を確認するには、リストのデータ ソースまたはエクスポート元デバイスの横に表示される [i] アイコンをクリックします。

ステップ 3 非アクティブな Prime Infrastructure のデータ ソースを削除するには、削除する非アクティブ データ ソースの隣にあるチェックボックスをオンにします。

ステップ 4 [Delete] をクリックします。

ステップ 5 [OK] をクリックして、削除を実行します。

NetFlow データ ソースは、そのソースから最後にデータを受け取った日から丸 7 日が経過するまでは削除できません。この時間差により、NetFlow データ ソースが不使用になったことをネットワーク オペレータが確認する時間（丸 1 週間）が確保されるため、NetFlow データ（ソースに従って Prime Infrastructure が識別および集約するデータ）の整合性を保護するのに役立ちます。その 7 日間のいずれかの時点でソースが再度アクティブになると、データは引き続き同じソースからの他のデータと共に適切に識別および集約されます。ソースが 7 日後に削除され、再度アクティブになると、そのすべてのデータは新しいソースからのデータとして識別および集約されます。

AVC データ重複除去の設定

データ重複除去を使用すると、対応するロケーション グループに対する信頼できるデータ ソースを識別できます。

Prime Infrastructure は、すべてのソースから受信したネットワーク使用率に関するすべてのデータを保存します。これには、複数のソースから受信した重複データも含まれます。正式なデータ ソースを指定した場合、特定のサイトを表示した際に、指定したソースからのデータだけが表示されます。

データ重複除去ページを使用すれば、特定のサイトのデータ ソースを指定することができます。たとえば、ブランチ（支社）オフィスのネットワーク解析モジュール（NAM）に加えて、同じブランチから送信される NetFlow データも存在する場合、信頼できるデータ ソースを使用した NAM または NetFlow データで報告されたときにサイト情報を表示することを選択できます。

2 つの信頼できるデータ ソースは、次のとおりです。

- システムで検出：管理対象デバイス製品ファミリに基づきます。デバイス ファミリの選択の優先順位を変更できます。優先順位を変更するには、設定アイコンをクリックして、デバイス ファミリをドラッグ アンド ドロップします。この手順に従って、信頼できるデータ ソースが選択されます。
- カスタマイズ：管理対象データ ソースから選択できます。

ステップ 1 [サービス（Services）] > [アプリケーションの可視性と制御（Application Visibility & Control）] > [データ重複除去（Data Deduplication）] の順に選択します。[データ重複除去（Data Deduplication）] ページが表示されます。

ステップ 2 [システムで検出（System Detected）] をクリックしてロケーション グループ内のデータ ソースを特定するか、または [カスタマイズ（Customized）] を選択してデータ ソースを選択します。

ステップ 3 **[Save（保存）]** をクリックします。

ステップ 4 [Apply] をクリックします。

設定テンプレートを使用した VPN IKE ポリシーと設定の構成

IKE ポリシー テンプレートを作成するには、次の手順を実行します。

ステップ 1 [設定（Configuration）] > [テンプレート（Templates）] > [機能およびテクノロジー（Features & Technologies）] > [セキュリティ（Security）] > [VPN コンポーネント（VPN Components）] > [IKE ポリシー（IKE Policies）] を選択します。

ステップ 2 [Template Basic] 領域で、該当するテキスト ボックスにテンプレートの名前、説明、およびタグを入力します。

ステップ 3 [Validation Criteria] 領域で、ドロップダウン リストからデバイス タイプを選択し、OS バージョンを入力します。必須フィールドの詳しい説明については、『Cisco Prime Infrastructure Reference Guide』を参照してください。

ステップ 4 [新しいテンプレートとして保存（Save as New Template）] をクリックします。

設定テンプレートを使用した VPN IPSec プロファイルの設定

IPsec プロファイル テンプレートを作成するには、次の手順を実行します。

ステップ 1 [設定（Configuration）] > [テンプレート（Templates）] > [機能およびテクノロジー（Features & Technologies）] > [セキュリティ（Security）] > [VPN コンポーネント（VPN Components）] > [IPSec プロファイル（IPSec Profile）] を選択します。

ステップ 2 [Template Basic] 領域で、該当するテキスト ボックスにテンプレートの名前、説明、およびタグを入力します。

ステップ 3 [Validation Criteria] 領域で、ドロップダウン リストからデバイス タイプを選択し、OS バージョンを入力します。

ステップ 4 [Template Detail] 領域で、[Add Row] をクリックして必要な情報を入力します。トランスフォーム セットは、特定のセキュリティ プロトコルとアルゴリズムを組み合わせたものです。IPsec のネゴシエーション中に、ピアは、特定のトランスフォームセットを使用して特定のデータ フローを保護することに合意します。トランスフォームセットには、特定のセキュリティプロトコルとそれに対応するアルゴリズムが記述されます。必須フィールドの詳しい説明については、『Cisco Prime Infrastructure Reference Guide』を参照してください。

ステップ 5 [新しいテンプレートとして保存（Save as New Template）] をクリックします。

設定テンプレートを使用した VPN 事前共有キーの設定

事前共有キー テンプレートを作成するには、次の手順を実行します。

ステップ 1 [設定（Configuration）] > [テンプレート（Templates）] > [機能およびテクノロジー（Features & Technologies）] > [セキュリティ（Security）] > [VPN コンポーネント（VPN Components）] > [事前共有キー（Preshared Keys）] を選択します。

ステップ 2 [Template Basic] 領域で、該当するテキスト ボックスにテンプレートの名前、説明、およびタグを入力します。

ステップ 3 [Validation Criteria] 領域で、ドロップダウン リストからデバイス タイプを選択し、OS バージョンを入力します。

ステップ 4 [Template Detail] 領域で、[Add Row] をクリックして必要な情報を入力します。

ステップ 5 [Save as New Template] をクリックします。

設定テンプレートを使用した VPN RSA キーの設定

RSA キー テンプレートを作成するには、次の手順を実行します。

ステップ 1 [設定（Configuration）]>[テンプレート（Templates）]>[機能およびテクノロジー（Features & Technologies）]>[セキュリティ（Security）]>[VPN コンポーネント（VPN Components）]>[RSA キー（RSA Keys）] を選択します。

ステップ 2 [Template Basic] 領域で、該当するテキスト ボックスにテンプレートの名前、説明、およびタグを入力します。

ステップ 3 [Validation Criteria] 領域で、ドロップダウン リストからデバイス タイプを選択し、OS バージョンを入力します。

ステップ 4 [Template Detail] 領域で、[Add] をクリックして必要な情報を入力します。

ステップ 5 エクスポート可能キーとして RSA を生成するには、[エクスポート可能（Exportable）] ボックスをオンにして [OK] をクリックします。

ステップ 6 [新しいテンプレートとして保存（Save as New Template）] をクリックします。

設定テンプレートを使用した VPN トランスフォーム セットの設定

トランスフォーム セット テンプレートを作成するには、次の手順を実行します。

ステップ 1 [設定（Configuration）]>[テンプレート（Templates）]>[機能およびテクノロジー（Features & Technologies）]>[セキュリティ（Security）]>[VPN コンポーネント（VPN Components）]>[トランスフォーム セット（Transform Sets）] を選択します。

ステップ 2 [Template Basic] 領域で、該当するテキスト ボックスにテンプレートの名前、説明、およびタグを入力します。

ステップ 3 [Validation Criteria] 領域で、ドロップダウン リストからデバイス タイプを選択し、OS バージョンを入力します。

ステップ 4 [Template Detail] 領域で、[Add Row] をクリックして必要な情報を入力します。

（注） ESP 暗号化アルゴリズムがペイロードの暗号化に使用され、ペイロードの整合性の確認には整合性アルゴリズムが使用されます。

ステップ 5 [Save as New Template] をクリックします。

エンドポイント アソシエーションを使用した NetFlow データの分類

Prime Infrastructure は、NetFlow データをサイトごとに分類し、[ネットワークヘルスとサービスヘルス（Network Health and Service Health）] ページに表示します。エンドポイント アソシエーションを使用すると、着信クライアント/サーバ IP をそれらのサブネットやデータ ソースに応じて分類するルールを作成するのに役立ちます。

（注） デバイスまたはクライアント/サーバ IP を特定のロケーション グループに割り当てるには、**[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ネットワークデバイス（Network Devices）]** で、ロケーション グループを定義する必要があります。

ルールを作成するには、次の手順を実行します。

ステップ 1 **[サービス（Services）] > [アプリケーションの可視性と制御（Application Visibility & Control）] > [エンドポイントアソシエーション（Endpoint Association）]** に移動します。

ステップ 2 [+]（行の追加）アイコンをクリックし、新しいルールを作成します。

ステップ 3 [ロケーショングループ（Location Group）] ドロップダウン リストから必要なロケーション グループを選択します。

ステップ 4 [サブネット（Subnet）] フィールドで有効なサブネットを指定します。

ステップ 5 （任意）[データソース（Data Source）] ドロップダウン リストで、必要なデータ ソースを選択します。

ステップ 6 [保存（Save）] をクリックします。ルールが作成されます。Netflow があるときは常に、UDP ペイロードのクライアント/サーバ IP は、作成されたルールに従って分類されます。

（注） 保存されたルールのリストは、CSV ファイルとしてインポート/エクスポートできます。

NetFlow テンプレートの表示

Netflow テンプレートでは、受信 UDP パケットの処理に使用されるメタデータ/構造を定義します。このテンプレートでは、デバイスから収集するメトリックを指定します。Prime Infrastructure では、**[サービス（Services）] > [アプリケーションの可視性と制御（Application Visibility & Control）] > [NetFlowテンプレート（NetFlow Templates）]** から定義したテンプレートを表示できます。[アプリケーション制御（Application Control）] ページの AVC プロファイルまたは CLI のいずれかを介してテンプレートを手動で設定することができます。

[NetFlow テンプレート（NetFlow Templates）] ページの [カスタム レポート（Custom Reports）] オプションは、ディスク領域の使用率が高いため Cisco Prime Infrastructure リリース3.2 では廃止されています。レポートは、**[レポート（Reports）] > [レポート起動パッド（Reports Launchpad）] > [Raw NetFlow]** ページから生成できます。

Easy VPN サーバとは

ケーブル モデムや xDSL ルータなど、インターネットへの接続性能が高いブロードバンド アクセスにはさまざまな形式がありますが、多くのアプリケーションでは、高度な認証を実行したり、2 つのエンドポイント間のデータを暗号化したりするなど、VPN 接続に対するセキュリティが必要です。また、2 つのルータ間に VPN 接続を確立するには、複雑な作業が伴う場合がありますし、2 つのルータの VPN パラメータを設定するには普通、ネットワーク管理者間で面倒な調整が必要です。

Cisco Easy VPN Remote 機能を使い、Cisco Unity Client プロトコルを実装することで、ほとんどの VPN パラメータが Cisco IOS Easy VPN サーバで定義できるようになるため、こうした面倒な作業が大幅に軽減されます。このサーバには、たとえば次のいずれかの専用 VPN デバイスを使用できます。

- Cisco VPN 3000 コンセントレータ
- Cisco PIX Firewall
- Cisco Unity Client プロトコルをサポートする Cisco IOS ルータ

Cisco Easy VPN サーバを設定すると、Cisco 800 シリーズ ルータや Cisco 2800 シリーズ ルータなどの Easy VPN Remote 上で最小限の設定を行うだけで、VPN 接続を構成できます。Easy VPN Remote による VPN トンネル接続が開始すると、Cisco Easy VPN サーバでは、IPsec ポリシーが Easy VPN Remote にプッシュされ、それに対応する VPN トンネル接続が構成されます。

設定テンプレートを使用した Easy VPN サーバの Web ブラウザ プロキシ設定

Easy VPN サーバ プロキシ機能を使用して、Easy VPN クライアントの設定を指定できます。この機能を使用すると、Cisco IOS VPN クライアントを使用して社内ネットワークに接続する際に Web ブラウザのプロキシ設定を手動で変更する必要はありません。また、ネットワークから切断する際にプロキシ設定を手動で元に戻す必要もありません。

Easy VPN サーバ プロキシ テンプレートを作成するには、次の手順を実行します。

ステップ 1 [設定（Configuration）]>[テンプレート（Templates）]>[機能およびテクノロジー（Features & Technologies）]>[セキュリティ（Security）]>[Easy VPN サーバ プロキシ設定（Easy VPN Server Proxy Setting）] を選択します。

ステップ 2 基本的なテンプレート情報を入力します。

ステップ 3 [Device Type] ドロップダウン リストから、[Routers] を選択します。

ステップ 4 [Template Detail] 領域に名前を入力して、グループに関連付ける設定を選択します。

ステップ 5 [No Proxy Server] オプションまたは [Automatically Detect Proxy Settings] オプション（このグループのクライアントが VPN トンネルを使用する際にプロキシ サーバを自動的に検出するようにする場合）を選択します。

ステップ 6 このグループのクライアントにプロキシ サーバを手動で設定するには、[Manual Configuration] オプションを選択します。このオプションを選択した場合は、手動でプロキシ サーバを設定する必要があります。

ステップ 7 クライアントがローカル（LAN）アドレスにプロキシサーバを使用しないように設定するには、[ローカル アドレスのプロキシ サーバをバイパス（Bypass proxy server for local addresses）] チェックボックスをオンにします。

ステップ 8 [新しいテンプレートとして保存（Save as New Template）] をクリックします。

設定テンプレートを使用した Easy VPN Remote の設定

Cisco Easy VPN Remote 機能を使い、Cisco Unity Client プロトコルを実装することで、ほとんどの VPN パラメータが Cisco IOS Easy VPN サーバで定義できるようになるため、こうした面倒な作業が大幅に軽減されます。

はじめる前に

ACL テンプレートを作成および公開します。

Easy VPN Remote テンプレートを作成するには、次の手順を実行します。

手順の概要

1. [設定（Configuration）]>[テンプレート（Templates）]>[機能およびテクノロジー（Features & Technologies）]>[セキュリティ（Security）]>[Easy VPN Remote] を選択します。
2. 基本的なテンプレート情報を入力します。
3. [Device Type] ドロップダウン リストから、[Routers] を選択します。
4. [Easy VPN Remote インターフェイスの設定（Easy VPN Remote Interface Configuration）] 領域に必要な情報を入力します。必須フィールドの詳しい説明については、『Cisco Prime Infrastructure Reference Guide』を参照してください。
5. [Remote Authentication Mechanisms] 領域で、認証方式を選択します。
6. [Remote Firewall Settings] 領域で、Easy VPN Remote 接続のファイアウォール設定を行います。
7. [新規テンプレートとして保存（Save as New Template）] をクリックします。
8. My Templates フォルダに移動し、保存したテンプレートを選択します。
9. 右上隅の **[発行（Publish）]** アイコンをクリックして、**OK** をクリックします。
10. 複合テンプレートを作成して ACL テンプレートと Easy VPN Remote テンプレートを複合テンプレートに追加します。
11. 矢印ボタンを使用し、テンプレートをデバイスに展開する順序に並べ替えます。たとえば、ACL を作成してインターフェイスに関連付けるには、Easy VPN Remote テンプレートの前に ACL テンプレートを配置します。
12. [Save as New Template] をクリックします。

手順の詳細

ステップ 1 [設定（Configuration）]>[テンプレート（Templates）]>[機能およびテクノロジー（Features & Technologies）]>[セキュリティ（Security）]>[Easy VPN Remote] を選択します。

ステップ 2 基本的なテンプレート情報を入力します。

ステップ 3 [Device Type] ドロップダウン リストから、[Routers] を選択します。

ステップ 4 [Easy VPN Remote インターフェイスの設定（Easy VPN Remote Interface Configuration）] 領域に必要な情報を入力します。必須フィールドの詳しい説明については、『Cisco Prime Infrastructure Reference Guide』を参照してください。

ステップ 5 [Remote Authentication Mechanisms] 領域で、認証方式を選択します。

ステップ 6 [Remote Firewall Settings] 領域で、Easy VPN Remote 接続のファイアウォール設定を行います。

ステップ 7 [新規テンプレートとして保存（Save as New Template）] をクリックします。

ステップ 8 My Templates フォルダに移動し、保存したテンプレートを選択します。

ステップ 9 右上隅の **[発行（Publish）]** アイコンをクリックして、**OK** をクリックします。

ステップ 10 複合テンプレートを作成して ACL テンプレートと Easy VPN Remote テンプレートを複合テンプレートに追加します。

ステップ 11 矢印ボタンを使用し、テンプレートをデバイスに展開する順序に並べ替えます。たとえば、ACL を作成してインターフェイスに関連付けるには、Easy VPN Remote テンプレートの前に ACL テンプレートを配置します。

ステップ 12 [Save as New Template] をクリックします。

設定テンプレートを使用した Easy VPN サーバの設定

Easy VPN サーバ機能により、新たに Cisco VPN ソフトウェア クライアントのリリース 3.x 以降および Cisco VPN ハードウェア クライアント（Cisco 800、Cisco 900、Cisco 1700、VPN 3002、および PIX 501 の各デバイス）がサーバのサポート対象となりました。IP セキュリティ（IPsec）を使用すると、リモート エンド ユーザは Easy VPN サーバによって Cisco IOS バーチャル プライベート ネットワーク（VPN）ゲートウェイと通信できます。また、集中管理された IPsec ポリシーがサーバによってクライアント デバイスにプッシュされることで、エンド ユーザによる設定を最小限に抑えることができます。

はじめる前に

次の手順を実行します。

- CLI テンプレートを使用して、グループおよびユーザの AAA メソッド リストを作成します。
- IPsec プロファイル テンプレートを作成します。
- 暗号マップを使用する場合は、トランスフォーム セット テンプレートを作成します。
- （任意）RADIUS サーバ グループ作成用の CLI テンプレートを作成するか、AAA メソッド リストの作成時に RADIUS サーバを設定します。
- （任意）ISAKMP グループ設定でスプリット トンネル ACL 用の ACL テンプレートを作成します。
- ISAKMP グループ設定用のブラウザ プロキシ テンプレートを作成します。

Easy VPN Remote テンプレートを作成するには、次の手順を実行します。

ステップ 1 [設定（Configuration）] > [テンプレート（Templates）] > [機能およびテクノロジー（Features & Technologies）] > [セキュリティ（Security）] > [Easy VPN サーバ（Easy VPN Server）] を選択します。

ステップ 2 基本的なテンプレート情報を入力します。

ステップ 3 [Device Type] ドロップダウン リストから、[Routers] を選択します。

ステップ 4 [Interface Configuration] 領域で、設定方法を選択し、デバイスに設定されたインターフェイスのフィールドに入力します。

ステップ 5 [VPN コンポーネント アセンブリ（VPN Components Assembly）] 領域で、トランスフォーム セット テンプレートで作成したトランスフォーム セット プロファイル名を入力し（「VPN トランスフォーム セットの設定」）、この領域内のフィールドに入力します。

ステップ 6 [Group Authorization] 領域で、CLI テンプレートで作成した メソッド リスト プロファイル名を入力し、領域内のフィールドに入力します。

ステップ 7 [User Authorization] 領域で、CLI テンプレートで作成した同じメソッド リスト プロファイル名を入力し、領域内のフィールドに入力します。

ステップ 8 [ISAKMP グループ設定（ISAKMP Group configuration）] 領域で、[行を追加（Add Row）] をクリックして ISAKMP グループ設定を追加します。

ステップ 9 [ISAKMP Group configuration] ダイアログボックスで、ACL テンプレートで作成した ACL プロファイル名、およびブラウザ プロキシ テンプレートで作成したブラウザ プロキシ プロファイル名を入力し、この領域内のフィールドに入力します。

ステップ 10 [Save as New Template] をクリックします。

ステップ 11 複合テンプレートを作成し（「VPN トランスフォーム セットの設定」）、AAA メソッド リストと RADIUS サーバ、IPsec プロファイル（「設定テンプレートを使用した VPN IPSec プロファイルの設定」）、ACL ブラウザ プロキシ（「Easy VPN サーバとは」）、および Easy VPN_ Remote テンプレートを複合テンプレートに追加します。

ステップ 12 矢印アイコンを使用して、テンプレートをデバイスに展開する順序に並べ替えます。たとえば、ACL を作成してインターフェイスに関連付けるには、Easy VPN Remote テンプレートの前に ACL テンプレートを配置します。

ステップ 13 [Save as New Template] をクリックします。

設定テンプレートを使用した GSM プロファイルの設定

GSM プロファイル テンプレートを作成するには、次の手順を実行します。

ステップ 1 [設定（Configuration）]>[テンプレート（Templates）]>[機能およびテクノロジー（Features & Technologies）]>[インターフェイス（Interfaces）]>[セルラー（Cellular）]>[GSM プロファイル（GSM Profile）] をクリックします。

ステップ 2 基本的なテンプレート情報を入力します。

ステップ 3 [Device Type] ドロップダウン リストから、[Routers] を選択します。

ステップ 4 [Template Detail] 領域で、アクセス ポイント名を入力し、ドロップダウン リストからプロファイル番号を選択します。

ステップ 5 サービス プロバイダーが使用する認証のタイプを選択します（CHAP 認証は PAP 認証よりもセキュアです）。

ステップ 6 ISP またはネットワーク管理者から付与されたユーザ名を入力し、パスワードを入力します。

ステップ 7 [Save as New Template] をクリックします。

ステップ 8 [OK] をクリックします。

設定テンプレートを使用した セルラー プロファイルの設定

セルラー プロファイル テンプレートを作成するには、次の手順を実行します。

（注） セルラー プロファイル テンプレートを GSM HSPA、HSPA+R7、および LTE-Verizon モデムに展開するには、ルータ上に GSM プロファイルを作成しておく必要があります（「設定テンプレートを使用した GSM プロファイルの設定」）。

ステップ 1 [設定（Configuration）]>[テンプレート（Templates）]>[機能およびテクノロジー（Features & Technologies）]>[インターフェイス（Interfaces）]>[セルラー（Cellular）]>[セルラー プロファイル（Cellular Profile）]を選択します。

ステップ 2 基本的なテンプレート情報を入力します。

ステップ 3 [Device Type] ドロップダウン リストから、[Routers] を選択します。

ステップ 4 [Template Detail] 領域で、インターフェイスをプライマリ WAN インターフェイスまたはバックアップ WAN インターフェイスとして定義し、フィールドに入力します。

ステップ 5 [Dialer Configuration] 領域で、[Yes] を選択して永続的データ接続を有効化し、フィールドに入力します。

ステップ 6 [Save as New Template] をクリックします。

ステップ 7 [OK] をクリックします。

ScanSafe を使用した HTTP および HTTPS トラフィックのスキャンの有効化

ScanSafe の Software as a Service（SaaS）Web セキュリティを使用すると、HTTP および HTTPS トラフィックのコンテンツをスキャンできます。ScanSafe Web セキュリティとルータを統合すると、コンテンツ スキャンおよびマルウェア検出のために、選択した HTTP トラフィックと HTTPS トラフィックが ScanSafe クラウドにリダイレクトされます。

Cisco ScanSafe による Cisco サービス統合型ルータ（ISR）Web セキュリティを有効にして、Web トラフィックを ScanSafe にリダイレクトするように ISR を設定すると、サービス統合型ルータ（ISR）は IP アドレスとポートに基づいて HTTP および HTTPS のトラフィックを ScanSafe のプロキシ サーバに透過的にリダイレクトします。ScanSafe でスキャンせずに、最初に要求された Web サーバに Web トラフィックを直接リレーするように ISR を設定できます。

トラフィックのホワイトリスト

承認された Web トラフィックがスキャン用に ScanSafe にリダイレクトされないように ISR を設定できます。ScanSafe スキャンをバイパスすると、ISR は ScanSafe に接続せず、最初に要求された Web サーバからコンテンツを直接取得します。ISR は Web サーバから応答を受け取ると、データをクライアントに送信します。これをトラフィックのホワイトリストといいます。

ScanSafe の詳細については、『Cisco ISR Web Security with Cisco ScanSafe Solution Guide』を参照してください。

ScanSafe テンプレートの作成

ScanSafe テンプレートを作成するには、次の内容を指定する必要があります。

- ScanSafe サーバおよびインターフェイス情報
- ホワイトリスト情報

ScanSafe テンプレートを作成するには、次の手順を実行します。

ステップ 1 [設定（Configuration）]>[テンプレート（Templates）]>[機能およびテクノロジー（Features & Technologies）]>[セキュリティ（Security）]>[ScanSafe] を選択します。

ステップ 2 [Template Basic] 領域で、適切なフィールドに名前と説明を入力します。

ステップ 3 [Validation Criteria] 領域で、リストからデバイス タイプを選択し、OS バージョンを入力します。

ステップ 4 [Template Detail] 領域で、必要な情報を入力します。必須フィールドの詳しい説明については、『Cisco Prime Infrastructure Reference Guide』を参照してください。

ステップ 5 [新しいテンプレートとして保存（Save as New Template）] をクリックします。

CDMA セルラー WAN インターフェイスの設定

CDMA インターフェイスを設定するには、次の手順を実行します。

ステップ 1 [Inventory] > [Device Management] > [Network Devices] を選択します。

ステップ 2 リストからデバイスを選択してから、[Configuration] をクリックします。[Feature Configuration] ペインが表示されます。

ステップ 3 [Feature Configuration] ペインで、[Interface] フォルダを展開して [Cellular WAN Interfaces] をクリックします。

ステップ 4 CDMA Sprint モデムの場合は次の手順を実行します。

a) CDMA Sprint モデムのセルラー インターフェイスを選択し、[モデムの管理（Manage Modem）] をクリックします。

b) [モデムの管理（Manage Modem）] ダイアログボックスで、[OMA-DM] または [手動（Manual）] オプション ボタンを選択します。[手動（Manual）] オプションを選択した場合は、フィールドに入力して手動で CDMA Sprint モデムを設定し、[OK] をクリックします。

ステップ 5 CDMA Verizon モデムの場合は次の手順を実行します。

a) CDMA Verizon モデムのセルラー インターフェイスを選択し、[モデムの管理（Manage Modem）] をクリックします。

b) [Manage Modem] ダイアログボックスで、[Account Activation Information] に入力し、[OK] をクリックします。

ステップ 6 CDMA Generic モデムの場合は次の手順を実行します。

a) CDMA Generic モデムのセルラー インターフェイスを選択し、[モデムの管理（Manage Modem）] をクリックします。

b) [モデムの管理（Manage Modem）] ダイアログボックスで、フィールドに入力して CDMA Generic モデムを設定し、[OK] をクリックします。

GSM セルラー WAN インターフェイスの設定

GSM インターフェイスを設定するには、次の手順を実行します。

ステップ 1 [Inventory] > [Device Management] > [Network Devices] を選択します。

ステップ 2 リストからデバイスを選択するか、[Add] をクリックして新しいデバイスを追加してから、デバイスを設定します。

ステップ 3 デバイスを選択後、[Configuration] をクリックします。[Feature Configuration] ペインが表示されます。

ステップ 4 [Interface] フォルダを展開して、[Cellular WAN Interfaces] を選択します。

ステップ 5 GSM インターフェイスを選択し、[Manage Modem] をクリックします。

ステップ 6 [モデムの管理（Manage Modem）] ダイアログボックスで、[行を追加（Add Row）] をクリックします。

ステップ 7 ドロップダウン リストからプロファイル番号を選択し、アクセス ポイント名を入力して [OK] をクリックします。

ネットワーク アドレス変換（NAT）の設定

ネットワーク アドレス変換（NAT）とは、ネットワーク デバイス（通常はファイアウォール）がプライベート ネットワーク内のコンピュータ（またはコンピュータのグループ）にパブリック アドレスを割り当てるプロセスのことです。NAT は、経済性とセキュリティの両方の目的で、組織または会社で使用されるパブリック IP アドレスの数を制限するために役立ちます。

組織が NAT 機能を使用すると、既存のネットワークを持っていてインターネットにアクセスする必要がある場合に、IP アドレスが枯渇する問題を解決できます。組織の IP ネットワークで NAT を使用することにより、外部のネットワークに異なる IP アドレス空間を使用できます。したがって、NAT を使用すると、グローバルなルーティングが可能なアドレスを持たない組織でも、そのアドレスをグローバルにルーティング可能なアドレス空間に変換して、インターネットに接続できるようになります。また、サービス プロバイダーの変更や、Classless Inter Domain Routing（CIDR）ブロックへの自発的な再番号割り当てを行う組織は、NAT を使用して、より適切に番号を割り当て直せるようになります。NAT は RFC 1631 に記述されています。

NAT が設定されたルータには、少なくとも内部ネットワークに対して 1 つ、外部ネットワークに対して 1 つのインターフェイスがあります。標準的な環境では、NAT はサブドメインとバックボーンの間の出口ルータに設定します。パケットがドメインから出て行くとき、NAT はローカルで意味のある送信元アドレスをグローバルで一意のアドレスに変換します。パケットがドメインに入ってくる際は、NAT はグローバルで一意の宛先アドレスをローカル アドレスに変換します。出力点が複数存在する場合、個々の NAT は同一の変換テーブルを持っていなければなりません。アドレスが足りなくなって、パケットにアドレスを割り当てられなくなった場合、NAT はそのパケットをドロップし、Internet Control Message Protocol（ICMP）ホスト到達不能パケットを送信します。

NAT の詳細については、『IP Addressing: NAT Configuration Guide, Cisco IOS XE Release 3S』を参照してください。

NAT タイプ

NAT はルータ（通常、2 つのネットワークどうしを接続するもの）で動作し、パケットが別のネットワークに転送される前に、内部ネットワークのプライベート（内部ローカル）アドレスをパブリック（内部グローバル）アドレスに変換します。この機能により、ネットワーク全体を表す 1 つのアドレスのみを外部にアドバタイズするように NAT を設定できるようになります。これにより、内部ネットワークを外部から効果的に隠すことができるため、セキュリティがさらに強化されます。

NAT には次のタイプがあります。

- スタティック アドレス変換（SAT）：ローカル アドレスとグローバル アドレスを 1 対 1 でマッピングできます。
- ダイナミック アドレス変換（DAT）：未登録の IP アドレスを、登録済み IP アドレスのプールから取得した登録済み IP アドレスにマップします。
- オーバーロード：複数の未登録 IP アドレスを、複数の異なるポートを使用して、1 つの登録済み IP アドレスにマップ（多対 1）するダイナミック NAT の一形式。この方法は、ポート アドレス変換（PAT）とも呼ばれます。PAT を使用することにより、使用できる正規のグローバル IP アドレスが 1 つのみでも、数千のユーザをインターネットに接続することができます。

IP アドレス節約のための NAT 設定

NAT を設定する手順は、次のとおりです。

1. NAT IP プールの作成 （946 ページ）（ダイナミック NAT に必要）
2. ACL テンプレートの作成と ACL の設定
3. NAT44 ルールの作成 （947 ページ）
4. インターフェイスの設定 （948 ページ）およびルールの割り当て
5. NAT MAX 変換を使用したルータでの同時 NAT 操作数の制限 （948 ページ）（任意）

（注） NAT 機能は Cisco IOS Release 3.5 以降の ASR プラットフォーム、および Cisco IOS Release 12.4(24)T 以降の ISR プラットフォームでサポートされます。

注意 「EMS_」で始まる CLI 変更はサポートされないため、予期しない動作を引き起こす可能性があります。

NAT IP プールの作成

IP プールは、ダイナミック NAT で使われる IP の範囲を表すデバイス オブジェクトです。NAT の IP プール機能を使用すると、ダイナミック NAT で使用できる新しいプールの作成、既存のプールの変更、デバイスからのプールの削除が可能です。

IP プールを作成するには、次の手順を実行します。

ステップ 1 [インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ネットワークデバイス（Network Devices）] を選択します。

ステップ 2 リストからデバイスを選択してから、[設定（Configuration）] をクリックします。[機能設定（Feature Configuration）] ペインが表示されます。

ステップ 3 [機能設定（Feature Configuration）] ペインで [セキュリティ（Security）] を展開し、[NAT] サブフォルダを展開して [IP プール（IP Pools）] をクリックします。[NAT プール（NAT Pools）] ページが表示されます。

ステップ 4 [IP プールの追加（Add IP Pool）] > [IP + プレフィックス（IP+Prefix）] または [IP 範囲 + プレフィックス（IP Range + Prefix）] をクリックし、[名前（Name）]、[IP アドレス/範囲（IP Address/Range）]、[プレフィックス長（Prefix Length）]、および [説明（Description）] に入力します。プールの作成後に、プール名を変更することはできません。

（注） 有効な IPv4 アドレスは、ピリオド（.）で区切られた 4 つのオクテットから構成されます。

ステップ 5 デバイスに IP プールを展開するには [保存（Save）]、編集をキャンセルする場合は [キャンセル（Cancel）] をクリックします。

ステップ 6 既存の IP プールを編集するには、[NAT IP Pools] ページで次のようにします。

a) 選択した IP プールのパラメータの行をクリックしてパラメータを編集します。または

b) IP プールを選択して [編集（Edit）] をクリックします。選択した IP プールが編集用に開かれます。プール名を除くすべてのパラメータを編集できます。

ステップ 7 [保存（Save）] をクリックして、デバイスに変更を展開します。

NAT44 ルールの作成

NAT44 機能を使用すると、NAT44 ルールを作成、削除、および変更できます。

NAT ルールには、次の 3 つのタイプがあります。

- スタティック
- ダイナミック
- ダイナミック PAT

NAT44 ルールを作成するには、次の手順を実行します。

ステップ 1 [インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ネットワークデバイス（Network Devices）] を選択します。

ステップ 2 リストからデバイスを選択してから、[設定（Configuration）] をクリックします。[機能設定（Feature Configuration）] ペインが表示されます。

ステップ 3 [機能設定（Feature Configuration）] ペインで [セキュリティ（Security）] を展開し、[NAT] サブフォルダを展開して [NAT44 ルール（NAT44 Rules）] をクリックします。

ステップ 4 [NAT 44] ページで、[NAT ルールを追加（Add NAT Rule）] ボタンの横の下矢印アイコンをクリックします。

- スタティック ルールを作成するには、[スタティック（Static）]をクリックします。要素の説明については、『Cisco Prime Infrastructure Reference Guide』を参照してください。
- ダイナミック NAT ルールを作成するには、[Dynamic] をクリックします。要素の説明については、『Cisco Prime Infrastructure Reference Guide』を参照してください。
- ダイナミック PAT ルールを作成するには、[Dynamic PAT] をクリックします。要素の説明については、『Cisco Prime Infrastructure Reference Guide』を参照してください。

ステップ 5 [保存（Save）] をクリックして変更を保存し、デバイスに展開します。

ステップ 6 既存の NAT44 ルールを編集するには、[NAT44] ページで次のいずれかを実行します。

- 選択した NAT44 ルールのパラメータ行をクリックし、パラメータを編集します。
- NAT44 ルールを選択して [編集（Edit）] をクリックします。選択した NAT44 ルールが編集用に開かれます。すべてのパラメータを編集できます。

ステップ 7 作成ルールに従って、発信元と送信先を変更できます。また、[Options] の選択も作成ルールに従って変更できます。

ステップ 8 [保存（Save）] をクリックして、変更をサーバに保存します。

インターフェイスの設定

仮想インターフェイスは、特定の目的または特定のユーザ向けの汎用情報とルータ依存情報を使用して設定された論理インターフェイスです。

仮想インターフェイスを設定するには、次の手順を実行します。

ステップ 1 [インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ネットワーク デバイス（Network Devices）] を選択します。

ステップ 2 リストからデバイスを選択したら、[Configuration] をクリックします。[Feature Configuration] ペインが表示されます。

ステップ 3 [機能設定（Feature Configuration）] ペインで [セキュリティ（Security）] を展開し、[NAT] サブフォルダを展開して [インターフェイス（Interfaces）] をクリックします。

[Interface] ページで、変更するインターフェイスを選択し、ドロップダウン リストからアソシエーションを選択します。選択できる項目は、[Inside]、[Outside]、および [None] です。

ステップ 4 [Save] をクリックして、変更をサーバに保存します。

NAT MAX 変換を使用したルータでの同時 NAT 操作数の制限

NAT MAX 変換機能によって、ルータ上で同時に処理される NAT の数を制限できます。さらに、NAT MAX 機能では、NAT アドレスの使用を詳細に制御できます。NAT 変換のレート制限機能を使用して、ウイルスやワーム、サービス拒絶攻撃の影響を制限することができます。NAT 変換のレート制限機能の設定の詳細については、『*IP Addressing: NAT Configuration Guide,*

Cisco IOS XE Release 3S』の「Configuring NAT for IP Address Conservation」を参照してください。

NAT MAX 変換機能を使用すると、グローバル変換の属性値をリセットできます。

MAX 変換を設定するには、次の手順を実行します。

ステップ 1 [Inventory] > [Device Management] > [Network Devices] を選択します。

ステップ 2 リストからデバイスを選択するか、[Add] をクリックして新しいデバイスを作成してから、デバイスを設定します。

ステップ 3 デバイスを選択後、[Configuration] をクリックします。[Feature Configuration] ペインが表示されます。

ステップ 4 [セキュリティ（Security）] を展開し、[NAT] サブフォルダを展開して [詳細設定（Advanced Settings）] > [変換の最大数（Max Translation）] をクリックします。

ステップ 5 パラメータ値をリセットします。すべてのパラメータに許可されるNATエントリの最大数を設定します。一般的な NAT レート制限の範囲は、100 ～ 300 エントリです。

ステップ 6 [保存（Save）] をクリックして、変更をサーバに保存します。

DMVPN を使用した IPSec トポロジの設定

DMVPN 機能により、総称ルーティング カプセル化（GRE）トンネル、IP Security（IPSec）暗号化、および Next Hop Resolution Protocol（NHRP）を組み合わせて、大小さまざまな規模の IPSec VPN を構築できます。

一般的な VPN 接続は、2 台のルータを接続するポイントツーポイント IPsec トンネルです。DMVPN を使用すると、中央ハブから IPsec トンネル経由で GRE を使用して他のリモート ルータ（スポークと呼ばれる）を接続するネットワークを作成できます。IPsec トラフィックは、ハブを通じてネットワーク内のスポークにルーティングされます。

DMVPN の詳細については、『Dynamic Multipoint IPsec VPNs (Using Multipoint GRE/NHRP to Scale IPsec VPNs)』を参照してください（Cisco.com ログイン ID が必要です）。

Cisco Network Control System では、ルータを DMVPN ハブ、DMVPN スポークまたはクラスタとして設定できます。ルータは次のように設定できます。

関連トピック

DMVPN ハブ アンド スポーク トポロジの設定 （951 ページ）
DMVPN フルメッシュ トポロジの設定 （951 ページ）
DMVPN クラスタ トポロジの設定 （952 ページ）

DMVPN トンネルの作成

DMVPN トンネルを作成するには、次の手順を実行します。

ステップ 1 [Inventory] > [Device Management] > [Network Devices] を選択します。

ステップ 2 リストからデバイスを選択してから、[Configuration] をクリックします。[Feature Configuration] ペインが表示されます。

ステップ 3 [機能設定（Feature Configuration）] ペインで、[セキュリティ（Security）] フォルダを展開して [DMVPN] をクリックします。[Add] をクリックして DMVPN を作成します。

ステップ 4 [Device Role and Topology Type] 領域で、トポロジとデバイス ロールを選択します。オプションは [Spoke]、[Hub]、および [Dynamic Connection between Spokes] です。

ステップ 5 [マルチポイント GRE インターフェイス情報（Multipoint GRE Interface Information）] 領域で、インターネットに接続する WAN インターフェイスをドロップダウン リストから選択します。

ステップ 6 トンネル インターフェイスの IP アドレスとサブネット マスクを入力します。

ステップ 7 [NHRP and Tunnel Parameters] 領域のフィールドに入力します。

（注） ネットワーク ID は、非ブロードキャスト マルチアクセス（NBMA）ネットワークの一意の 32 ビット ネットワーク ID です。トンネル キーは、特定のトンネル インターフェイスに対してキー ID を有効にするために使用されます。特定のインターフェイスで送信される IP パケットの MTU サイズ。

（注） イーサネットとシリアル インターフェイスに対するデフォルトの MTU 値は 1500 です。デフォルト値は、メディア タイプによって異なります。トンネルのスループット遅延は、特定のインターフェイスの遅延値を設定するために使用されます。

ステップ 8 [暗号化ポリシー（Encryption policy）] フィールドで、プラス（+）のアンカー ボタンをクリックし、トランスフォーム セット プロファイルを追加します（『Cisco Prime Infrastructure Reference Guide』の「Security > VPN Components > Transform Sets」を参照）。

ステップ 9 [Transform Set Profile] ダイアログボックスで [Name] に入力し、ドロップダウン リストからセキュリティ プロトコルとアルゴリズムの許容される組み合わせを選択して、トランスフォーム セットを設定します。

ステップ 10 [IP Compression] チェックボックスをオンにして、トランスフォーム セットの IP 圧縮を有効にします。

ステップ 11 トランスフォーム セットのモードを選択します。オプションは [Tunnel] モードまたは [Transport] モードです。

ステップ 12 [NHS Server Information] 領域で、ハブとトンネルの物理インターフェイスの IP アドレス、および [Fallback Time] を入力します。デバイスがクラスタをサポートしている場合は、[Cluster ID]、[Max Connection]、[Hub IP address]、および [Priority] などのネクスト ホップ サーバ情報を追加します。

（注） NHS サーバ情報は、スポークの設定だけに必要です。[Use Cluster for NHS] チェックボックスをオンにした場合は、[Cluster ID]、[Max Connection]、および [Next Hub Server] などの情報を追加します。NHS クラスタ設定があるテンプレートは、Cisco IOS ソフトウェア リリース 15.1(2)T 以降を実行しているデバイスだけに適用されます。

ステップ 13 [Routing Information] 領域では、ルーティング情報を選択します。オプションは [EIGR]、[RIPV2]、および [Other] です。

（注） このルーティング情報は、ハブ設定だけに必要です。

ステップ 14 ドロップダウン リストから既存の EIGRP 番号を選択するか、EIGRP 番号を入力します。その他のプロトコルを設定するには、[Other] オプションを使用します。

ステップ 15 [保存（Save）] をクリックすると、単一の NHS サーバ エントリの詳細とそのサーバのプライオリティ、サーバ グループ全体、および NHS クラスタ情報が保存されます。NHS クラスタ情報を保存すると、NHS サーバが編集不可フィールドに入力されます。

ステップ 16 [OK] をクリックして、設定をデバイスに保存します。

DMVPN ハブ アンド スポーク トポロジの設定

ハブ アンド スポーク トポロジを設定するには、次の手順を実行します。

ステップ 1 [Inventory] > [Device Management] > [Network Devices] を選択します。

ステップ 2 リストからデバイスを選択してから、[Configuration] をクリックします。[Feature Configuration] ペインが表示されます。

ステップ 3 [機能設定（Feature Configuration）] ペインで、[セキュリティ（Security）] フォルダを展開して [DMVPN] をクリックします。[追加（Add）] ボタンをクリックして **DMVPN** トンネルを作成します。

ステップ 4 [Device Type and Topology] 領域で、トポロジとして [Hub and Spoke] を選択し、デバイス ロールとして [Hub] または [Spoke] のいずれかを選択します。

ステップ 5 ドロップダウン リストから WAN インターフェイスを選択後、トンネル インターフェイスのマルチポイント GRE IP アドレスとサブネット マスクを設定します。

ステップ 6 NHRP およびトンネル インターフェイスのパラメータ、たとえば、IP アドレス、NHRP パラメータおよびマップ、MTU 値、トンネルの送信元、トンネル モード、トンネル キーなどを設定します。

ステップ 7 デバイス間のデータ フローを保護するためのトランスフォーム セットを作成します。1 つの認証ヘッダー（AH）、1 つのカプセル化セキュリティ ペイロード（ESP）暗号化、1 つの ESP 認証、および 1 つの圧縮という、最大 4 つのトランスフォームを指定できます。これらのトランスフォームは、IPsec プロトコルとアルゴリズムを定義します。

ステップ 8 使用するルーティング プロトコルを設定します。

ステップ 9 [Save] をクリックして、コンフィギュレーションをデバイスに保存します。

DMVPN フルメッシュ トポロジの設定

ダイナミック スポークツースポーク オプションを使用すると、DMVPN フルメッシュ トポロジを設定できます。このトポロジでは、ネットワーク内の他のスポークに直接 IPsec トンネルを確立できるスポークとして、ルータを設定できます。

DMVPN フルメッシュ トポロジを設定するには、次の手順を実行します。

ステップ 1 [Inventory] > [Device Management] > [Network Devices] を選択します。

ステップ 2 リストからデバイスを選択するか、[Add] をクリックして新しいデバイスを作成してから、デバイスを設定します。

ステップ 3 デバイスを選択後、[Configuration] をクリックします。[Feature Configuration] ペインが表示されます。

ステップ 4 [Security] フォルダを展開して [DMVPN] をクリックします。[追加（Add）] をクリックして、フルメッシュ トポロジで DMVPN トンネルを作成します。

ステップ 5 [DMVPN トンネルの作成（Create DMVPN Tunnel）] 設定ページで [フル メッシュ（Full Mesh）] オプション ボタンを選択して、ネットワーク タイプをフルメッシュ トポロジとして設定します。

ステップ 6 「DMVPN ハブ アンド スポーク トポロジの設定」の項にあるステップ 6 ～ 8 を繰り返します。

ステップ 7 フルメッシュ スポーク トポロジでは、[NHS Server Information] 領域に、ハブの物理インターフェイスの IP アドレスやハブのトンネル インターフェイスの IP アドレスなど、次のハブのサーバ情報を追加します。

ステップ 8 [Save] をクリックして、コンフィギュレーションをデバイスに保存します。

DMVPN クラスタ トポロジの設定

クラスタ トポロジを設定するには、次の手順を実行します。

ステップ 1 [Inventory] > [Device Management] > [Network Devices] を選択します。

ステップ 2 リストからデバイスを選択してから、[Configuration] をクリックします。[Feature Configuration] ペインが表示されます。

ステップ 3 [機能設定（Feature Configuration）] ペインで、[セキュリティ（Security）] フォルダを展開して [DMVPN] をクリックします。[追加（Add）] をクリックして DMVPN トンネルを作成します。

ステップ 4 [DMVPN トンネルの作成（Create DMVPN Tunnel）] 設定ページで、[スポーク（Spoke）] オプション ボタンを選択して、デバイス ロールをスポークとして設定します。

ステップ 5 「DMVPN ハブ アンド スポーク トポロジの設定」の項にあるステップ 6 ～ 8 を繰り返します。

（注） デバイスで IOS のバージョン 15.1(2)T 以降を実行している必要があります。

ステップ 6 [行を追加（Add Row）] をクリックしてクラスタ関連情報を設定し、[クラスタ ID（Cluster-ID）] と [最大接続（Maximum Connection）] の値を追加します。

ステップ 7 （オプション ボタンの横にある）[行を展開（Expand Row）] をクリックし、[行を追加（Add Row）] をクリックして NHS サーバ情報を追加します。

ステップ 8 NHS サーバ、GRE トンネル IP アドレス、およびこの NHS サーバの優先度を入力します。[保存（Save）] をクリックして、NHS サーバ エントリの設定を保存します。

ステップ 9 [保存（Save）] をクリックして、NHS サーバ グループ情報を保存します。

ステップ 10 再び [保存（Save）] をクリックして、クラスタ設定を含む NHS グループ情報を保存します。これにより、テーブルに NHS サーバ IP アドレスが自動的に入力されます。

デバイスからの DMVPN トンネルの削除

DMVPN トンネルを削除するには、次の手順を実行します。

ステップ 1 [Inventory] > [Device Management] > [Network Devices] を選択します。

ステップ 2 DMVPN トンネルを削除するデバイスをリストから選択します。デバイスが追加されていない場合は、[Add] をクリックしてデバイスを追加します。

ステップ 3 デバイスを選択後、[Configuration] をクリックします。[Feature Configuration] ペインが表示されます。

ステップ 4 [セキュリティ（Security）] フォルダを展開して [DMVPN] をクリックします。使用可能なトンネルが表示されます。

ステップ 5 トンネルを選択して [削除（Delete）] をクリックします。

ステップ 6 警告メッセージに対して [Yes] をクリックし、選択したトンネルを削除します。

ステップ 7 選択したトンネルを削除しない場合は、警告メッセージに対して [No] をクリックします。

ステップ 8 加えた変更をルータへ送信せずに、すべての変更を取り消すには、[Cancel] をクリックします。

デバイスの QoS 設定

デバイスに QoS を有効または無効にするには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [ネットワーク（Network）] > [ネットワーク デバイス（Network Devices）]** の順に選択します。

ステップ 2 QoS を有効にするデバイス名をクリックし、**[アプリケーションの可視性と制御（App Visibility & Control）] > [QoS]** を選択します。

ステップ 3 QoS 対応のインターフェイスを選択し、[QoS の有効化（Enable QoS）] をクリックします。

ステップ 4 要件に応じて、[入力時に QoS を有効化（Enable QoS on Ingress）] チェックボックスまたは [出力時に QoS を有効化（Enable QoS on Egress）] チェックボックスをオンにするか、あるいはその両方をオンにします。

ステップ 5 [入力時に QoS を有効化（Enable QoS on Ingress）] をオンにした場合は、[プロファイルの選択（Select Profile）] ドロップダウン リストからプロファイルを選択して [OK] をクリックします。

ステップ 6 [出力時に QoS を有効化（Enable QoS on Egress）] をオンにした場合は、次の手順を実行します。

a) [プロファイルに基づいて分類（Classify based on profile）] オプション ボタンをクリックし、[プロファイルの選択（Select Profile）] ドロップダウン リストからプロファイルを選択します。

b) [QoS のスケジューリング（QoS scheduling）] では、[プロファイルの選択（Select Profile）] ドロップダウン リストからプロファイルに基づくスケジューリング アクションを選択します。

（注） ステップ 4 で [入力時に QoS を有効化（Enable QoS on Ingress）] と [出力時に QoS を有効化（Enable QoS on Egress）] の両方を選択した場合は、同じプロファイルを選択する必要があります。

ステップ 7 展開する前に [CLI プレビュー（CLI Preview）] タブをクリックし、QoS 設定をプレビューします。

ステップ 8 [展開（Deploy）] をクリックします。

ステップ 9 デバイスの QoS を無効にするには、次の手順を実行します。

a) [QoS の無効化（Disable QoS）] をクリックし、QoS 設定をデバイスから削除する方向（[入力（Ingress）] または [出力（Egress）]）を選択します。

b) [展開（Deploy）] をクリックします。

また、**[サービス（Services）] > [インターフェイスの設定（Interface Configuration）]** からデバイスの QoS を有効または無効にすることもできます。

GETVPN を使用した IPSec トポロジの設定

Group Encrypted Transport VPN（GETVPN）展開には、グループ メンバ、キー サーバ、およびグループ ドメイン オブ インタープリテーション プロトコルという、3 つの主要コンポーネントがあります。グループ メンバはトラフィックを暗号化および復号化し、キー サーバはすべてのグループ メンバに暗号キーを配布します。キー サーバは、ある一定期間において 1 つのデータ暗号化キーを決定します。すべてのグループ メンバが同じキーを使用するため、どのグループ メンバも他のすべてのグループ メンバによって暗号化されたトラフィックを復号化することができます。GDOI プロトコルは、グループ メンバとキー サーバの間でグループ キーおよびグループのセキュリティ アソシエーション（SA）管理に使用されます。GETVPN 展開には、最小 1 つのキー サーバが必要です。

従来の IPsec 暗号化ソリューションとは異なり、GETVPN ではグループ SA の概念が使用されます。GETVPN グループ内のすべてのメンバは、共通の暗号化ポリシーと共有 SA を使用して互いに通信することができます。したがって、グループ メンバ間でピアツーピア ベースの IPsec のネゴシエーションを行う必要はなく、これによってグループ メンバ ルータにかかるリソースの負荷が軽減されます。

グループ メンバー

グループ メンバは、グループ内のデータ トラフィックを暗号化するために必要な IPsec SA を取得するために、キー サーバに登録します。グループ メンバはキー サーバにグループ識別番号を提供し、そのグループの個別のポリシーおよびキーを取得します。これらのキーは、トラフィックのロスがないよう、現在の IPsec SA が期限切れになる前にキー サーバによって定期的に更新されます。

キー サーバ

キー サーバは、セキュリティ ポリシーの保守、グループ メンバの認証、トラフィック暗号化用のセッション キーの提供を行います。キー サーバは個々のグループ メンバを登録時に認証します。グループ メンバは登録が成功した場合のみ、グループ SA に参加できます。

グループ メンバはいつでも登録可能で、最新のポリシーおよびキーを受信できます。グループ メンバがキー サーバに登録する際に、キー サーバはグループ メンバのグループ識別番号を検証します。この識別番号が有効で、グループ メンバが有効なインターネット キー エクスチェンジ（IKE）クレデンシャルを提供した場合、キー サーバは SA ポリシーとキーをグループ メンバに送信します。

グループ メンバに送信されるキーは、キー暗号キー（KEK）とトラフィック暗号キーの 2 種類です。TEK は、同じグループ内のグループ メンバがデータの暗号化に使用する IPsec SA の一部になります。KEK は、キー サーバとグループ メンバ間でキー再生成メッセージを保護するために使用されます。

キー サーバは、近々 IPsec SA の期限が切れる場合や、キー サーバでセキュリティ ポリシーが変更された場合に、キー再生成メッセージを送信します。キーの配布は、マルチキャストまた

はユニキャストトランスポートを使用して、キーの再生成中に行われます。マルチキャスト方式は、キーを各グループ メンバに個別に送信する必要がないため、拡張性に優れています。ユニキャストとは異なり、キー サーバは、マルチキャスト キー再生成方式を使用して成功したキー再生成の受信に関する確認応答をグループ メンバーから受信しません。ユニキャストのキー再生成方式を使用すると、グループ メンバが 3 回連続でキー再生成の確認応答を行わなかった場合、キー サーバはそのグループ メンバをデータベースから削除します。

グループ ドメイン オブ インタープリテーション

グループ ドメイン オブ インタープリテーション プロトコルは、グループ キーとグループ SA の管理に使用されます。グループ ドメイン オブ インタープリテーションでは、グループ メンバおよびキー サーバの認証に Internet Security Association Key Management Protocol（ISAKMP）を使用します。GETVPN には、RSA 署名（証明書）や事前共有キーなど、標準的なすべての ISAKMP 認証スキームを使用できます。

GETVPN の詳細については、
http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6635/ps7180/deployment_guide_c07_554713.html
を参照してください。

GETVPN グループ メンバーの設定

[Add GroupMember] 設定ページを使用して、GETVPN グループ メンバを設定します。

GETVPN グループ メンバを作成するには、次の手順を実行します。

ステップ 1 [Inventory] > [Device Management] > [Network Devices] を選択します。

ステップ 2 リストからデバイスを選択してから、[Configuration] をクリックします。[Feature Configuration] ペインが表示されます。

ステップ 3 [機能設定（Feature Configuration）] ペインで、[セキュリティ（Security）] フォルダを展開して [GETVPN-GroupMember] をクリックします。[追加（Add）] をクリックして、GET VPN のグループ メンバーを作成します。

ステップ 4 [Add GroupMember] ダイアログボックスで [General] タブを選択し、[Group Name] および [Group Identity] を入力します。ドロップダウン リストから [Registration Interface] を選択します。

ステップ 5 プライマリ キー サーバとセカンダリ キー サーバの IP アドレスを入力します。セカンダリ キー サーバの IP アドレスを追加または削除するには、[Add Row] または [Delete] をクリックします。

（注） プライマリ キー サーバは、グループ ポリシーを作成してすべてのグループ メンバに配布する処理、およびセカンダリ キー サーバと定期的に同期する処理を担当します。プライオリティが最も高いサーバが、プライマリ キー サーバとして選択されます。

ステップ 6 [行（row）] または [フィールド（field）] をクリックして、セカンダリ キー サーバの IP アドレスを編集します。

ステップ 7 [保存（Save）] をクリックして、設定を保存します。

ステップ 8 [Add Group Member] ダイアログボックスで [Advanced] タブを選択し、ドロップダウン リストから [Local Exception ACL] および [Fail Close ACL] を選択します。

フェールクローズ機能を設定した場合、グループ メンバを通過するすべてのトラフィックは、グループ メンバが正常に登録されるまでドロップされます。グループ メンバが正常に登録され、SAがダウンロードされた後、この機能は自動的にオフになります。

ステップ 9 [Migration] タブを選択し、[Enable Passive SA] チェックボックスをオンにして、パッシブ SA を有効にします。このグループ メンバでパッシブ SA モードをオンにするには、このオプションを使用します。

ステップ 10 [OK] をクリックしてテーブルにグループ メンバーを追加します。コマンドを表示するには、[CLI] プレビューをクリックします。スケジュールした展開が完了すると、設定がデバイスに適用されます。

GETVPN キー サーバの設定

[Add KeyServer] 設定ページを使用して、GETVPN キー サーバを設定します。

GETVPN キー サーバを作成するには、次の手順を実行します。

手順の概要

1. [Inventory] > [Device Management] > [Network Devices] を選択します。
2. リストからデバイスを選択してから、[設定（Configuration）] をクリックします。[機能設定（Feature Configuration）] ペインが表示されます。
3. [機能設定（Feature Configuration）] ペインで、[セキュリティ（Security）] フォルダを展開して [GETVPN-KeyServer] をクリックします。[追加（Add）] をクリックして GETVPN キー サーバを作成します。
4. [Add Key Server] ダイアログボックスで [General] タブを選択し、このキー サーバの [Group Name]、[Group Identity]、[WAN IP address]、および [Priority] を入力します。
5. [Co-operative Key Server] の IP アドレスを入力します。共同キー サーバの IP アドレスを追加または削除するには、[行を追加（Add Row）] または [削除（Delete）] をクリックします。[行（row）] または [フィールド（field）] をクリックして、IP アドレスを編集します。
6. [Add KeyServer] ダイアログボックスで [Rekey] タブを選択し、ドロップダウン リストから配布方法を選択します。
7. [Add KeyServer] ダイアログボックスで [GETVPN Traffic] タブを選択し、暗号化するトラフィック、暗号化ポリシー、およびアンチリプレイを入力します。
8. [OK] をクリックしてテーブルにグループ メンバーを追加します。コマンドを表示するには、[CLI] プレビューをクリックします。スケジュールした展開が完了すると、コンフィギュレーションがデバイスに適用されます。

手順の詳細

ステップ 1 [Inventory] > [Device Management] > [Network Devices] を選択します。

ステップ 2 リストからデバイスを選択してから、[設定（Configuration）] をクリックします。[機能設定（Feature Configuration）] ペインが表示されます。

ステップ 3 [機能設定（Feature Configuration）] ペインで、[セキュリティ（Security）] フォルダを展開して [GETVPN-KeyServer] をクリックします。[追加（Add）] をクリックして GETVPN キー サーバを作成します。

ステップ 4 [Add Key Server] ダイアログボックスで [General] タブを選択し、このキー サーバの [Group Name]、[Group Identity]、[WAN IP address]、および [Priority] を入力します。

ステップ 5 [Co-operative Key Server] の IP アドレスを入力します。共同キー サーバの IP アドレスを追加または削除するには、[行を追加（Add Row）] または [削除（Delete）] をクリックします。[行（row）] または [フィールド（field）] をクリックして、IP アドレスを編集します。

ステップ 6 [Add KeyServer] ダイアログボックスで [Rekey] タブを選択し、ドロップダウン リストから配布方法を選択します。

この配布方法は、キー サーバからグループ メンバにキー再生成情報を送信するために使用されます。配布方法としてマルチキャストを選択した場合は、キー再生成を送信する必要があるマルチキャスト アドレスを指定します。

ステップ 7 [Add KeyServer] ダイアログボックスで [GETVPN Traffic] タブを選択し、暗号化するトラフィック、暗号化ポリシー、およびアンチリプレイを入力します。

このアクセス リストでは、暗号化するトラフィックが定義されます。「permit」行と一致するトラフィックだけが、暗号化されます。暗号化セッションが非アクティブな場合も常に許可する必要がある特定のトラフィックは、暗号化しないでください。

ステップ 8 [OK] をクリックしてテーブルにグループ メンバーを追加します。コマンドを表示するには、[CLI] プレビューをクリックします。スケジュールした展開が完了すると、コンフィギュレーションがデバイスに適用されます。

VPN のコンポーネント

インターネット キーエクスチェンジ（IKE）は、セキュアな認証された通信を設定するための標準的な方式です。IKE では、ネットワークを介した 2 つのホストの間にセッション キー（およびそれに関連した暗号とネットワークの設定）が確立されます。IKE ポリシーは、認証の際にピアの識別情報を保護します。

IKE ネゴシエーションは保護される必要があります。このため、それぞれの IKE ネゴシエーションは、共通する（共有されている）IKE ポリシーに各ピアが同意することで開始されます。このポリシーは、後続の IKE ネゴシエーションを保護するために使用されるセキュリティ パラメータを示します。ピアがポリシーに同意した後、そのポリシーのセキュリティ パラメータが、ピアごとに確立されたセキュリティ アソシエーションによって識別されます。それらのセキュリティ アソシエーションは、ネゴシエーションの間、後続のすべての IKE トラフィックに適用されます。

ネゴシエーションが開始されると、IKE は、両ピア上で同一の IKE ポリシーを検索します。ネゴシエーションを開始したピアは、そのすべてのポリシーをリモート ピアに送信します。リモート ピアは、相手側ピアから受信したすべてのポリシーと自身の最優先ポリシーを比較することにより、一致しているポリシーを検索します。2 つのピアのポリシーが一致するのは、暗号化、ハッシュ、認証、Diffie-Hellman（D-H）パラメータの各値が同じで、リモート ピアのポ

リシーに指定されているライフタイムが、比較しているポリシーのライフタイム以下の場合です。ライフタイムが同一でない場合は、より短い、リモート ピアのポリシーのライフタイムが使用されます。

関連トピック

VPN IKE ポリシーの設定 （958 ページ）
VPN IPSec プロファイルの設定 （958 ページ）
VPN 事前共有キーの設定 （959 ページ）
VPN RSA キーの設定 （960 ページ）
VPN トランスフォーム セットの設定 （961 ページ）

VPN IKE ポリシーの設定

IKE ポリシーを設定するには、次の手順を実行します。

ステップ 1 [Inventory] > [Device Management] > [Network Devices] を選択します。

ステップ 2 リストからデバイスを選択してから、[Configuration] をクリックします。[Feature Configuration] ペインが表示されます。

ステップ 3 [機能設定（Feature Configuration）] ペインで、[セキュリティ（Security）] フォルダを展開して [VPN コンポーネント（VPN Components）] > [IKE ポリシー（IKE Policies）] を選択します。

ステップ 4 [行を追加（Add Row）] をクリックして IKE ポリシーを作成します。

ステップ 5 [IKE ポリシー（IKE Policies）] ページで、優先度、認証、D-H グループ、暗号化、ハッシュ、およびライフタイムを入力します。

[IKE ポリシー（IKE Policies）] ページの要素の説明については、『Cisco Prime Infrastructure Reference Guide』の「Security > VPN Components > IKE Policies」を参照してください。

ステップ 6 [IKE の有効化（Enable IKE）] と [アグレッシブ モードの有効化（Enable Aggressive Mode）] チェックボックスをオンにし、ピア ルータとアグレッシブ モードの IKE ポリシーをグローバルに有効にします。

ステップ 7 ドロップダウン リストから [IKE Identity] を選択します。

ステップ 8 [Dead Peer Detection Keepalive] および [Dead Peer Detection Retry] の時間を秒単位で入力します。

[IKE ポリシー（IKE Policies）] ページの要素の説明については、『**Cisco Prime Infrastructure 参照ガイド**』の「セキュリティ > VPN コンポーネント > IKE ポリシー.」を参照してください。

ステップ 9 [保存（Save）] をクリックして設定を保存し、再び [保存（Save）] をクリックして CLI コマンドを生成します。

VPN IPSec プロファイルの設定

IPsec プロファイルは ISAKMP プロファイルとも呼ばれ、これを使用すると、一連の IKE パラメータを定義して 1 つ以上の IPsec トンネルに関連付けることができます。IPsec プロファイルは、その一致識別基準の概念によって一意に識別された着信 IPsec 接続に、パラメータを適用します。これらの基準は、着信 IKE 接続によって提示された IKE 識別情報に基づいており、

この識別情報には、IP アドレス、完全修飾ドメイン名（FQDN）、およびグループ（VPN リモート クライアント グループ）が含まれます。

IKE プロファイル機能を使用すると、IPsec プロファイルを作成できます。

ステップ 1 [Inventory] > [Device Management] > [Network Devices] を選択します。

ステップ 2 リストからデバイスを選択してから、[Configuration] をクリックします。[Feature Configuration] ペインが表示されます。

ステップ 3 [機能設定（Feature Configuration）] ペインで、[セキュリティ（Security）] フォルダを展開して [VPN コンポーネント（VPN Components）] > [IPsec プロファイル（IPsec Profile）] を選択します。

ステップ 4 [行を追加（Add Row）] をクリックして IPsec プロファイルを作成します。

ステップ 5 [IPsec Profile] ページで、[Name]、[Description]、[Transform Set]、[IPsec SA Lifetime] などの情報を入力します。

（注） プロファイルを編集する場合、IPsecプロファイルの名前を編集することはできません。トランスフォーム セットは、特定のセキュリティ プロトコルとアルゴリズムを組み合わせたものです。IPSec SA のネゴシエーション中に、ピアは特定のトランスフォーム セットを使用して特定のデータ フローを保護することに合意します。トランスフォームには、特定のセキュリティ プロトコルとそれに対応するアルゴリズムが記述されます。

ステップ 6 設定した期間が経過した後に新しい SA を確立するための、[IPsec SA Lifetime] を秒単位で入力します。

ステップ 7 IPsecプロファイルのパラメータを編集するには、[Field] をクリックし、そのIPsecプロファイルのパラメータを編集します。

ステップ 8 IPSec プロファイルを削除するには、リストから [IPSec プロファイル（IPsec Profile）] を選択し、[削除（Delete）] をクリックします。

ステップ 9 [保存（Save）] をクリックして設定を保存し、再び [保存（Save）] をクリックして CLI コマンドを生成します。

VPN 事前共有キーの設定

事前共有キー機能を使用すると、2 つのピア間で秘密キーを共有できます。このキーは、IKE が認証フェーズで使用します。

事前共有キーを作成するには、次の手順を実行します。

ステップ 1 [Inventory] > [Device Management] > [Network Devices] を選択します。

ステップ 2 リストからデバイスを選択してから、[Configuration] をクリックします。[Feature Configuration] ペインが表示されます。

ステップ 3 [機能設定（Feature Configuration）] ペインで、[セキュリティ（Security）] フォルダを展開して [VPN コンポーネント（VPN Components）] > [事前共有キー（Preshared Keys）] を選択します。

ステップ 4 [Add Row] をクリックして事前共有キーを作成します。

ステップ 5 [Preshared Keys] ページで、[IP Address]、[Host Name]、[Subnet Mask]、および [Preshared Keys] を入力します。

ステップ 6 事前共有キーのパラメータを編集するには、[Field] をクリックし、その事前共有キーのパラメータを編集します。

ステップ 7 事前共有キーを削除するには、リストから事前共有キーを選択して [Delete] をクリックします。

ステップ 8 [保存（Save）] をクリックして設定を保存し、再び [保存（Save）] をクリックして CLI コマンドを生成します。

VPN RSA キーの設定

RSA キーペアは、公開キーと秘密キーで構成されます。公開キーインフラストラクチャ（PKI）を設定する場合、証明書登録要求に公開キーを含める必要があります。証明書が付与された後、ピアが公開キーを使用して、ルータに送信されるデータを暗号化できるように、公開キーが証明書に組み込まれます。秘密キーはルータに保持され、ピアによって送信されたデータの復号化と、ピアとネゴシエーションする際の、トランザクションのデジタル署名に使用されます。

RSA キーペアには、キーのモジュラス値が含まれています。モジュラス値に応じて、RSA キーのサイズが決まります。モジュラス値が大きいほど、RSA キーの安全性が高まります。ただしモジュラス値が大きいと、キーの生成、暗号化、および復号化にかかる時間が長くなります。

RSA キーを作成するには、次の手順を実行します。

ステップ 1 [Inventory] > [Device Management] > [Network Devices] を選択します。

ステップ 2 リストからデバイスを選択してから、[Configuration] をクリックします。[Feature Configuration] ペインが表示されます。

ステップ 3 [機能設定（Feature Configuration）] ペインで、[セキュリティ（Security）] フォルダを展開して [VPN コンポーネント（VPN Components）] > [RSA キー（RSA Keys）] を選択します。

ステップ 4 [行を追加（Add Row）] をクリックして RSA キーを作成します。

ステップ 5 [Add RSA Keys] ダイアログボックスが表示されます。

ステップ 6 [Add RSA Keys] ダイアログボックスで、[Label]、[Modulus]、および [Type] を入力します。

（注） モジュラス値が 512 ～ 1024 の範囲内の場合は、64 の倍数（整数値）を入力します。1024 よりも大きい値が必要な場合は、1536 または 2048 を入力できます。512 よりも大きい値を入力すると、キー生成に 1 分以上かかる場合があります。モジュラス値に応じて、キーのサイズが決まります。モジュラスが大きいほどキーの安全性は高くなりますが、大きなモジュラスのキーは生成に要する時間が長くなり、大きなキーほど暗号化/復号化の処理にかかる時間が長くなります。

ステップ 7 RSA をエクスポート可能キーとして生成するには、[Make the Key exportable] チェックボックスをオンにします。

ステップ 8 [OK] をクリックして、設定を保存します。

ステップ 9 RSA キーをインポートするには、[Import] をクリックします。[Import RSA Key] ダイアログボックスが表示されます。

ステップ 10 [Import RSA Key] ダイアログボックスで、RSA キーのラベル、キー タイプ、およびキーを復号化するためのパスワードを入力します。キータイプが汎用キー、署名、または暗号の場合は、保存された公開キーと秘密キーのデータをコピーして貼り付けます。

ステップ 11 用途キーをインポートするには、署名キーと暗号キーの両方の公開および秘密キーデータを入力します。

ステップ 12 [Import] をクリックして、RSA キーをインポートします。

ステップ 13 RSA キーをエクスポートするには、リストから RSA キーを選択して [Export] をクリックします。[Export RSA Key Pair] ダイアログボックスが表示されます。

ステップ 14 [Export RSA Key Pair] ダイアログボックスで、RSA キーを暗号化するためのパスワードを入力し、ドロップダウン リストから暗号化アルゴリズムを選択します。

ステップ 15 [OK] をクリックして、エクスポートしたキーを表示します。

ステップ 16 RSA キーを削除するには、リストから RSA キーを選択して [削除（Delete）] をクリックします。

VPN トランスフォーム セットの設定

トランスフォーム セットを定義するには、1 ～ 3 個のトランスフォームを指定します。各トランスフォームは、使用するアルゴリズムと IPsec セキュリティ プロトコル（AH または ESP）を表します。IPsec セキュリティ アソシエーションのネゴシエーション中に特定のトランスフォーム セットを使用する場合は、トランスフォーム セット全体（プロトコル、アルゴリズム、およびその他の設定値の組み合わせ）が、リモート ピアのトランスフォーム セットと一致している必要があります。

トランスフォーム セットを設定する手順は、次のとおりです。

ステップ 1 [Inventory] > [Device Management] > [Network Devices] を選択します。

ステップ 2 リストからデバイスを選択してから、[Configuration] をクリックします。[Feature Configuration] ペインが表示されます。

ステップ 3 [機能設定（Feature Configuration）] ペインで、[セキュリティ（Security）] フォルダを展開して [VPN コンポーネント（VPN Components）] > [トランスフォーム セット（Transform Sets）] を選択します。

ステップ 4 [行の追加（Add Row）] をクリックしてトランスフォーム セットを作成します。

ステップ 5 [Transform Sets] ページで、[Name] を入力し、トランスフォーム セットを設定するために有効なセキュリティ プロトコルとアルゴリズムの組み合わせを選択します。

（注） ESP 暗号化アルゴリズムがペイロードの暗号化に使用され、ペイロードの整合性の確認には整合性アルゴリズムが使用されます。

ステップ 6 トランスフォーム セットのモードを指定します。

- [Transport]：データだけを暗号化します。トランスポート モードは、両方のエンドポイントが IPsec をサポートしている場合に使用されます。トランスポート モードでは、認証ヘッダーまたはカプセル化されたセキュリティ ペイロードが元の IP ヘッダーの後に置かれます。これにより、IP ペイロードだ

けが暗号化されます。この方式を使用すると、暗号化されたパケットに Quality of Service（QoS）制御などのネットワーク サービスを適用できます。

- [Tunnel]：データと IP ヘッダーを暗号化します。トンネル モードはトランスポート モードよりも強力な保護を提供します。IP パケット全体が AH または ESP 内にカプセル化されるため、新しい IP ヘッダーが付加され、データグラム全体を暗号化できます。トンネル モードを使用すると、ルータなどのネットワーク デバイスを複数の VPN ユーザ用の IPsec プロキシとして機能させることができます。トンネル モードは、そのような設定で使用してください。

ステップ 7 [保存（Save）] をクリックして設定を保存し、再び [保存（Save）] をクリックして設定の変更を保存します。

ゾーンベースのファイアウォールを使用したインターフェイスグループ間のファイアウォール ポリシーの制御

ゾーンベース ファイアウォール機能を使用すると、ゾーンと呼ばれるインターフェイス グループの間で Cisco IOS 単方向ファイアウォール ポリシーを簡単に管理できます。

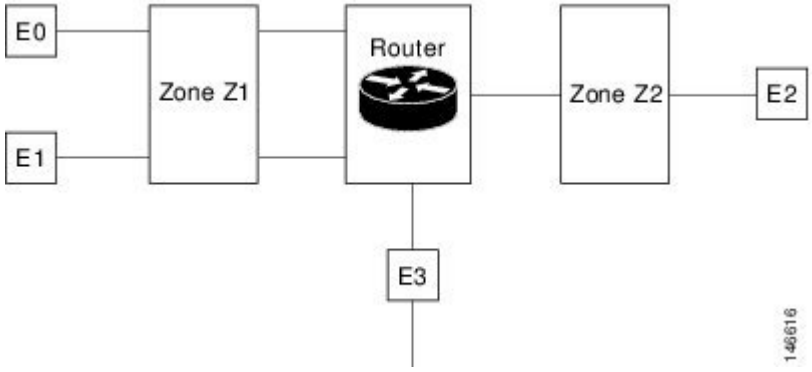
ゾーンとは、同様の機能を果たすインターフェイスのグループです。たとえばルータで、ギガビット イーサネット インターフェイス 0/0/0 とギガビット イーサネット インターフェイス 0/0/1 を LAN に接続するとします。これら 2 つのインターフェイスは、内部ネットワークを表している点で同類です。したがって、ファイアウォール設定でゾーンとしてグループ化できます。

デフォルトでは、同じゾーン内のインターフェイス間のトラフィックはポリシーの制約を受けません。トラフィックは自由に通過します。

インターフェイスがセキュリティ ゾーンのメンバである場合、そのインターフェイスで送受信されるトラフィックはすべて（ルータ宛または同じゾーンの別のインターフェイス宛のトラフィックを除く）ドロップされます。

別のゾーンに属するインターフェイス間のトラフィックを許可するには、具体的なルールを含むファイアウォール ポリシーをデバイスにプッシュする必要があります。ポリシーで（inspect または pass アクションによって）これら 2 つのゾーン間のトラフィックが許可されると、トラフィックはゾーンを通過できます。図 48-1 では、セキュリティ ゾーンについて説明します。

図 *27*：セキュリティ ゾーンの図



上の図に示したインターフェイスとセキュリティ ゾーンの関係について、以下で説明します。

- インターフェイス E0 と E1 はセキュリティ ゾーン Z1 のメンバです。
- インターフェイス E2 はセキュリティ ゾーン Z2 のメンバです。
- インターフェイス E3 は、どのセキュリティ ゾーンのメンバでもありません。

このシナリオでは、次のような状況になっています。

- インターフェイス E0 と E1 は同じセキュリティ ゾーン（Z1）のメンバーなので、2 つのインターフェイス間のトラフィックは自由に流れます。
- ポリシーが設定されていない場合、ゾーン間（たとえば、E0 と E2 の間、E1 と E2 の間、E3 と E1 の間、および E3 と E2 の間）でトラフィックは流れません。
- E0 または E1 と E2 のインターフェイス間でトラフィックを流すことができるのは、ゾーン Z1 とゾーン Z2 の間のトラフィックを許可する明示的なポリシーが設定されている場合だけです。

E3 は、どのセキュリティ ゾーンにも属していないため、E3 と E0、E1、または E2 のインターフェイス間をトラフィックが流れることはありません。

Cisco Prime Infrastructure は、Cisco ASR、ISR、CSR ルータでのゾーンベース ファイアウォール機能をサポートしています。Cisco Prime Infrastructure を使用して、ゾーンベース ファイアウォール ポリシーテンプレートを設定し、複数のデバイスにそれを展開できます。ゾーンベースの設定を展開した後、デバイス ワーク センターに移動して、特定のデバイスに展開されたファイアウォールの設定を確認できます。

ゾーンベース ファイアウォールをモニタするには、デバイス ワーク センターまたは（ゾーンベース ファイアウォールの syslog メッセージをサポートする）Cisco Prime Infrastructure の syslog 機能で、Zone-Based Firewall Monitor Hits 機能を確認します。

Cisco Prime Infrastructure では、（Telnet または SSH を介した）CLI または WSMA を使用してゾーンベース ファイアウォールを設定できます。WSMA を使用すると、より効率的かつ堅牢な方法でゾーンベース ファイアウォールを設定できます。したがって、ゾーンベース ファイアウォールの設定には WSMA プロトコルを使用することを推奨します。Cisco Prime Infrastructure での WSMA の使用の詳細については、「WSMA で AVC 機能を使用するためのデバイスの設定」を参照してください。

ゾーンベース ファイアウォールの設定：ワークフロー

複数のデバイスでゾーンベース ファイアウォールを設定するには、ゾーンベース テンプレートを使用して変更を行います。ゾーンベース ファイアウォール テンプレートを使用するために、まずはネットワークのゾーンを定義してネットワークにゾーンベース ファイアウォールを設計する必要があります。Cisco Prime Infrastructure では、ゾーンはインターフェイス ロールのグローバル オブジェクトで表され、ゾーンに属するインターフェイスのリストが動的に選択されます。次に、ファイアウォール環境でネットワーク オブジェクトを定義して作成します。ゾーンベース ファイアウォールの機能は、Cisco Prime Infrastructure で IPv4 ネットワークのみをサポートしています。（IPv6 はサポートされていません）。

（注） ゾーンベース ファイアウォール機能は、Cisco IOS-XE Release 15.2(2)S 以降の ASR プラットフォーム、Cisco IOS Release 15.0(1)M 以降の ISR G2 プラットフォーム、Cisco IOS-XE 15.3(2)S Release 以降の ISR G3 プラットフォーム、Cisco IOS-XE 15.3(1)S Release 以降の CSR プラットフォーム、Cisco IOS-XE Release 16.3 以降の Cisco ISRv プラットフォーム、および Cisco IOS-XE Release 16.6.1 以降の Cisco ISR 1000 プラットフォームでサポートされます。

ゾーンベース ファイアウォール テンプレートを設定する手順は、次のとおりです。

1. ゾーンを定義します。セキュリティ ゾーンはインターフェイス ロールとして定義されます。
2. IPv4 ネットワーク オブジェクトを定義します。

（注） Cisco Prime Infrastructure 2.0 は、IPv4 ネットワーク オブジェクトのみをサポートしています。

3. ファイアウォール ポリシーを設計し、複数のデバイスに展開します（詳細については、「単一デバイスのゾーンベース ファイアウォール用のポリシー ルールを作成する」を参照）。
4. 特定のデバイスの設定を検証します（「ゾーンベースのファイアウォールを使用したインターフェイス グループ間のファイアウォール ポリシーの制御」を参照）。
5. グローバル オブジェクトとテンプレートの設定を変更します（「ゾーンベース ファイアウォールのポリシー ルールの設定」を参照）。
6. ポリシー ルールをモニタします（単一デバイスのゾーンベース ファイアウォールに関するポリシー ルールのモニタとトラブルシューティング （969 ページ） を参照）。
7. Syslog メッセージをモニタします。

セキュリティ ゾーン、IPv4 ネットワーク オブジェクト、およびファイアウォール ポリシーを変更するには、ファイアウォール ポリシーを編集して、該当するデバイスに再び展開します。

ゾーンベース ファイアウォールのポリシー ルールの設定

共有ポリシー オブジェクトの作成後に、ゾーンベース ファイアウォールのポリシー ルール テンプレートを作成します。

ゾーンベース ファイアウォールのポリシー ルール テンプレートを作成するには、次の手順を実行します。

ステップ 1 [設定（Configuration）]>[テンプレート（Templates）]>[機能およびテクノロジー（Features & Technologies）]>[セキュリティ（Security）]>[ゾーンベース ファイアウォール（Zone Based Firewall）]>[ポリシー ルール（Policy Rules）] を選択します。

ステップ 2 [Template Basic] 領域で、適切なフィールドに名前と説明を入力します。

ステップ 3 [Validation Criteria] 領域で、リストからデバイス タイプを選択し、OS バージョンを入力します。

ステップ 4 必須フィールドに入力します。テンプレート パラメータの説明については、『Cisco Prime Infrastructure Reference Guide』を参照してください。

ステップ 5 [新しいテンプレートとして保存（Save as New Template）] をクリックします。

CLI を使用したゾーンベース ファイアウォール設定の削除

ユーザーは次の手順を実行することによって、CLIテンプレートを使用してデバイスからゾーン ベース ファイアウォール設定を削除できます。

ステップ 1 **[設定（Configuration）] > [テンプレート（Templates）] > [機能およびテクノロジー（Features & Technologies）]** の順に移動します。

ステップ 2 **[CLI テンプレート（CLI Templates）]** ツリーを展開し、**[SYSTEM Template-cli]** オプションを選択します。

ステップ 3 **Delete_ZBFW_Configuration** テンプレートを選択します。

ステップ 4 ゾーンベースのファイアウォール設定を削除するデバイスを同期させる必要があります。**[展開（Deploy）]** ボタンをクリックします。

ステップ 5 ゾーンベースのファイアウォール設定を削除するデバイスを選択します。

ゾーンベースのファイアウォールを使用して設定されたデバイスのリストが、**[CLI プレビュー（CLI Preview）]** ペインに表示されます。

ステップ 6 ゾーンベースのファイアウォール設定を削除するには、デバイスを再同期する必要があります。

単一デバイスのゾーン ベースのファイアウォールのポリシー ルールを構成します。

単一のデバイスでゾーンベース ファイアウォールを設定するには、デバイス ワーク センターのゾーンベースの設定を使用して変更を行います。

単一デバイスのゾーンベース ファイアウォール用のセキュリティ ゾーンを作成する

セキュリティ ゾーンを作成するには、次の手順を実行します。

（注） ゾーンベース ファイアウォール機能は、Cisco IOS-XE Release 15.2 (2)S 以降の ASR プラットフォーム、Cisco IOS リリース 15.0 (1) M 以降の ISR G2 プラットフォーム、Cisco IOS-XE Release 15.3(2)S 以降の ISR G3 プラットフォーム、および Cisco IOS-XE Release 15.3(1)S の CSR プラットフォームでサポートされます。

ステップ 1 [インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ネットワーク デバイス（Network Devices）] を選択してから、デバイスをクリックします。

ステップ 2 [設定（Configuration）] タブで [セキュリティ（Security）] サブフォルダを展開します。

ステップ 3 [セキュリティ（Security）] サブフォルダで、[ゾーンベース ファイアウォール（Zone Based Firewall）] > [共通のビルディング ブロック（Common Building Blocks）] を展開して [ゾーン（Zones）] をクリックします。

ステップ 4 [Add Zone] をクリックしてセキュリティ ゾーンを作成します。

ステップ 5 **ゾーン名**を選択します。

ステップ 6 （Cisco ASR デバイスのみ）これを Cisco ASR デバイスのデフォルト ゾーンにするには、[デフォルトの有効化（Enable Default）] をクリックします。デフォルト ゾーンは、どのゾーンにも関連付けられていないすべてのインターフェイスをホスティングします。

ステップ 7 [OK] をクリックして、設定を保存します。

ステップ 8 ゾーンの VRF を選択します。

a) VRF は、インターフェイスをセキュリティ ゾーンに割り当てる前に選択します。ゾーンに割り当てることができるのは、選択した VRF に割り当てられたインターフェイスのみです。

b) 「グローバル VRF」を選択した場合、どの VRF にも割り当てられていないインターフェイスのみゾーンに割り当てることができます。

ステップ 9 インターフェイスをセキュリティ ゾーンに割り当てるには、下矢印アイコンをクリックします。[Interface Object Selector] ダイアログボックスが表示されます。

a) [Interface selector] ダイアログボックスで、[Interface] チェックボックスをオンにして、リストからインターフェイスを選択します（複数を選択可能）。

b) 設定を保存する場合は [OK] をクリックします。変更内容をルータに送信せずにすべての変更を取り消す場合は [キャンセル（Cancel）] をクリックします。

ステップ 10 [Advanced options] 列で [Configure] をクリックします。[Advanced Parameters Configuration] ダイアログボックスが表示されます。

ステップ 11 ゾーンに属するインターフェイスを通過する検査対象トラフィックに適用される、一連の詳細パラメータを定義します。パラメータごとに、デフォルト値を上書きするパラメータ名の左にあるチェックボックスをオンにして、そのパラメータの新しい値を選択します。（任意）[Advanced Parameters Configuration] ダイアログボックスで、次の手順を実行します。

（注） [Advanced Parameters] オプションは、ASR1K シリーズのデバイスでのみサポートされます。

a) [Alert] チェックボックスをオンにして [On] オプション ボタンを選択し、アラートを設定します。

b) [Maximum Destination] チェックボックスをオンにして最大接続数を設定します。

c) [接続先ごとの TCP SYN フラッディング レート（TCP SYN-Flood Rate per Destination）] チェックボックスをオンにし、TCP フラッディング レートを設定します。
d) [基本的な脅威検出パラメータ（Basic Threat Detection Parameters）] チェックボックスをオンにして、[オン（On）] オプション ボタンを選択し、FW ドロップ脅威検出レート、FW 検査脅威検出レート、および FW SYN 攻撃脅威検出レートを設定します。

ステップ 12 次をクリックします。

- コンフィギュレーションを保存するには [OK]。
- 保存しないで終了するには [Cancel]。

ステップ 13 既存のセキュリティ ゾーン パラメータを編集するには、ゾーンを選択し、[Advance options] 列で [Edit] をクリックします。[Advanced Parameters Configuration] ダイアログボックスが表示されます。

ステップ 14 [高度なパラメータ設定（Advanced Parameters Configuration）] ダイアログボックスで値を編集し、[保存（Save）] をクリックして変更を保存します。[Advanced Options] アイコンにマウス カーソルを合わせると、設定されたパラメータがクイック ビュー ウィンドウに表示されます。

ステップ 15 ゾーンの説明を入力してから、[Save] をクリックします。

単一デバイスのゾーンベース ファイアウォール用のポリシー ルールを作成する

ポリシー ルール（規則）を作成するには、次の手順を実行します。

ステップ 1 [インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ネットワークデバイス（Network Devices）] を選択してから、デバイスを選択します。

ステップ 2 [機能設定（Feature Configuration）] ペインで [セキュリティ（Security）] サブフォルダを展開します。

ステップ 3 [セキュリティ（Security）] サブフォルダで、[ゾーンベース ファイアウォール（Zone Based Firewall）] を展開して [ポリシー ルール（Policy Rules）] をクリックします。[ポリシー ルール（Policy Rules）] ページが表示されます。

ステップ 4 既存のポリシー ルールを編集するには、次のオプションのいずれかを選択します。

- 規則のパラメータ行をクリックし、パラメータを編集します。
- チェックボックスをオンにして規則を選択し、[Edit] をクリックします。選択した規則が編集用に開かれます。ポリシー規則の名前は編集できません。

  （注） ファイアウォール規則サービスで、伝送制御プロトコル（TCP）またはユーザ データグラム プロトコル（UDP）のポート範囲を指定できます。[Service] 列で新しい規則を追加したり、既存の規則を編集したりする場合に、TCP または UDP を割り当てるには、オブジェクト セレクタをクリックして [OK] をクリックします。プロトコル アイコンの近くに表示されるテキスト ボックスでポート番号を定義できます。また、<start-port-number>-<end-port-number> の形式でポート範囲を定義して、この範囲を特定のプロトコル（TCP または UDP）に設定することができます。

- 規則をドラッグして別の場所にドロップすると、ファイアウォール規則の順序を変更できます。

ステップ 5 [ポリシー ルール（Policy Rules）] ページから、[ルールの追加（Add Rule）] をクリックし、フィールドに入力します。規則を追加する際は、ポリシーの上部か下部、または既存の規則の前後に規則を配置できます。□ファイアウォール規則は、それぞれの順序に従って処理されます。規則の順序を制御するには、テーブルで規則の場所を選択し、[Add Top] または [Add Bottom] オプションを使用して規則をテーブルの上部または下部に追加します。ルールを選択し、[後ろに追加（Add After）] または [前に追加（Add Before）] オプションを使用してルールを既存のルールの前または後ろに追加します。所定の場所にルールを配置して後でドラッグ アンド ドロップを使用することでその場所を変更できます。

ステップ 6 （任意）□ファイアウォール規則名を入力します。ファイアウォール規則の名前を指定しなかった場合は、システムでファイアウォール規則の名前が生成されます。たとえば rule_1 のように、rule_<number> または EMS_rule_<number> の形式を使用してファイアウォール規則名を作成することはできません。これらは、システムで予約済みの形式です。

ステップ 7 規則の送信元および宛先のゾーンを選択します。規則は送信元ゾーンから宛先ゾーンに流れるトラフィックにのみ適用されます。送信元ゾーンと宛先ゾーンを同一にすることはできません。

ステップ 8 送信元および宛先 IP アドレスを追加するには、[add] アイコンをクリックします。[Source/Destination IP address] ダイアログボックスが表示されます。

a) [Source/Destination IP address] ダイアログボックスで、値を any に設定するには、[Any] チェックボックスをオンにします。
b) 送信元および宛先 IP アドレスを入力します。
c) [+] ボタンをクリックして新しい IP アドレスとサブネットを追加します。
d) [-] ボタンをクリックして IP/サブネットを削除します。
e) [OK] をクリックして設定を保存するか、または [キャンセル（Cancel）] をクリックし、これまでに加えた変更をルータに送信せずに、すべての変更を取り消します。

ステップ 9 （任意）[Service] の値を設定します。サービスを追加または削除するには、下矢印アイコンをクリックします。[Firewall Service] ダイアログボックスが表示されます。定義済みのサービスを選択することもできます。サービスの作成については、「単一デバイスのゾーンベース ファイアウォール用のポリシー ルールを作成する」を参照してください。

a) [Firewall Service] ダイアログボックスで、サービスまたはポートベースのアプリケーションのチェックボックスをオンにして、規則用のアプリケーションまたはサービスを選択します。
b) [TCP] または [UDP] を選択して特定の TCP/UDP ポートを選択し、ウィンドウを閉じて、[TCP] または [UDP] アイコンの横に表示されるテキスト ボックスに、使用するポートのリストを入力します。ポートベース アプリケーションの表示については、「単一デバイスのゾーンベース ファイアウォール用のアプリケーション TCP/UDP ポートを割り当てる」を参照してください。
c) 前に戻るには、ナビゲーション用矢印ボタンを使用します。
d) [OK] をクリックして、コンフィギュレーションを保存します。

ステップ 10 適切なアクションを選択します。オプションは、[ドロップ（Drop）]、[ドロップして記録（Drop and Log）]、[検査（Inspect）]、[通過（Pass）]、および [通過させて記録（Pass and Log）] です。

ステップ 11 検査アクションを選択した場合は、[Advance options] 列で [Configure] をクリックします。[Advanced Parameters Configuration] ダイアログボックスが表示されます。

ステップ 12 [Advanced Parameters Configuration] ダイアログボックスで、次のようにします。

a) デバイスのデフォルト値をカスタマイズするには、[Parameter] チェックボックスをオンにして新しい値を設定します。
b) デバイスのデフォルト値を適用するには、[Parameter] チェックボックスをオフにします。

c) ファイアウォール ルールのデフォルト パラメータを表示するには、「単一 Cisco ISR デバイスのゾーンベース ファイアウォール用にデフォルトのパラメータを設定する」を参照してください。

d) [高度なオプション（Advanced Options）] アイコンの上にマウス カーソルを移動させると、設定されたパラメータがクイック ビュー ウィンドウに表示されます。

ステップ 13 [保存（Save）] をクリックして、ルールをデバイスに適用します。要素の説明については、『Cisco Prime Infrastructure Reference Guide』を参照してください。

単一デバイスのゾーンベース ファイアウォールに関するポリシー ルールのモニタとトラブルシューティング

モニタリング機能を使用すると、ポリシー規則をモニタすることができます。最も使用された規則の特定、特定の規則のトラブルシューティング、選択した規則のヒットの確認を行うことができます。

ポリシー規則をモニタするには、次の手順を実行します。

ステップ 1 [インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ネットワーク デバイス（Network Devices）] を選択してデバイスを選択します。

ステップ 2 [機能設定（Feature Configuration）] ペインで [セキュリティ（Security）] フォルダを展開します。

ステップ 3 [セキュリティ（Security）] サブフォルダで、[ゾーンベース ファイアウォール（Zone Based Firewall）] を展開して [ポリシー ルール（Policy Rules）] をクリックします。[ファイアウォール ルール（Firewall Rules）] ページが表示されます。

ステップ 4 [ファイアウォール ルール（Firewall Rules）] ページで [ヒット カウンタ（Hit Counters）] をクリックし、次のいずれかのオプションを使用して、ファイアウォール ルールのセッションおよびパケットのヒット カウンタを分析します。

ステップ 5 ファイアウォール ルールのパケットおよびセッション カウンタを表示するには、[すべて表示（Show all）] オプションをクリックします。パケットおよびセッション カウンタは 2 つの別々の列に表示されます。

（注） [Show All] オプションを選択すると、この操作の完了に時間がかかる可能性があることを示す警告メッセージが表示されます。セッションのヒット カウンタはドロップおよびパス規則には適用されません。同様に、パケットのヒット カウンタは検査規則に適用されません。

ステップ 6 ルールの最終更新時刻を確認するには、列名にマウス カーソルを合わせるか、[ヒット カウンタ（Hit Counters）] の [最終更新時刻（Last Update Time）] オプションをクリックします。

ステップ 7 特定のルールまたは選択した複数のルールのヒット カウンタを表示するには、[選択したルールについて表示（Show for selected rules）] オプションをクリックします。ヒット カウントがポップアップ ダイアログ ボックスに表示され、データを即座に更新できるボタンも一緒に表示されます。

ステップ 8 パケット/セッション数に基づいた上位または下位の規則を表示するには、テーブルの右上隅に表示される定義済みフィルタ オプションを使用します。

ステップ 9 デバイスのすべての規則カウンタを廃棄するには、[Reset All Counters] をクリックします。アプリケーションは、規則カウンタをリセットする前に警告メッセージを表示します。

単一デバイスのゾーンベース ファイアウォール用のサービス グループを作成する

サービス グループを作成、更新、または削除することができます。サービス グループには、複数のポートベースのアプリケーションをファイアウォール ポリシーで使用できる論理グループにグループ化するオプションがあります。

たとえば、参照サービスグループ オブジェクトを定義して、HTTP と HTTPS の両方のアプリケーションを割り当てることができます。次に、この参照サービスグループをファイアウォール規則で使用して、トラフィックの参照を許可または拒否できます。規則の HTTP と HTTPS を両方選択する必要はありません。

サービス グループを作成するには、次の手順を実行します。

ステップ 1 [インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ネットワークデバイス（Network Devices）] を選択してから、デバイスを選択します。

ステップ 2 [機能設定（Feature Configuration）] ペインで [セキュリティ（Security）] サブフォルダを展開します。

ステップ 3 [セキュリティ（Security）] サブフォルダで、[ゾーンベース ファイアウォール（Zone Based Firewall）] > [共通のビルディング ブロック（Common Building Blocks）] を展開して [サービス グループ（Service Groups）] をクリックします。[Service Groups] ページが表示されます。

ステップ 4 次の手順でサービス グループを作成します。

a) [サービス グループ（Service Group）] ページで、[サービス グループの追加（Add Service Group）] をクリックしてサービス グループ名を入力します。サービス グループの作成後に、この名前を変更することはできません。また、アプリケーションを使用しないと、サービス グループを作成することもできません（「パフォーマンスをモニタするカスタム アプリケーションの作成」を参照してください）。

b) アプリケーションを割り当てるには、下矢印アイコンをクリックします。

c) [Applications] ダイアログボックスで、[Applications] チェックボックスをオンにしてリストからアプリケーションを 1 つ以上選択し、[OK] をクリックします。

ステップ 5 既存のサービス グループを編集するには、次のいずれかを実行します。

- [Service Groups] ページで、サービス グループのパラメータ行をクリックしてパラメータを編集します。
- サービス グループを選択して [Edit] をクリックします。新しいアプリケーションを追加したり、選択済みのアプリケーションを削除することができます。
- 選択したリストからアプリケーションを削除するには、アプリケーション名の上にカーソルを置き、[X] をクリックします。

ステップ 6 [Save] をクリックして、変更をデバイスに適用します。

単一デバイスのゾーンベース ファイアウォール用のアプリケーション TCP/UDP ポートを割り当てる

伝送制御プロトコル（TCP）またはユーザ データグラム プロトコル（UDP）ポートをアプリケーションに割り当てたり、割り当てを解除したりすることができます。

（注） 次の手順で[保存（Save）]をクリックすると、デバイスに変更が展開されます。要求済みの操作を確認したり、保留中の変更キューから要求を削除したりすることはできません。

アプリケーションに TCP/UDP ポートを割り当てるか、その割り当てを解除するには、次の手順を実行します。

手順の概要

1. [インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ネットワークデバイス（Network Devices）] を選択してから、デバイスを選択します。
2. [機能設定（Feature Configuration）] ペインで [セキュリティ（Security）] サブフォルダを展開します。
3. [セキュリティ（Security）] サブフォルダで、[ゾーンベース ファイアウォール（Zone Based Firewall）] > [共通のビルディング ブロック（Common Building Blocks）] を展開して [ポート マッピング（Port Mappings）] をクリックします。[ポート アプリケーション マッピング（Port Application Mapping）] ページが表示されます。
4. アプリケーションに TCP/UDP ポートを割り当てるか、その割り当てを解除するには、アプリケーションをクリックし、その TCP/UDP ポート値を更新します。TCP/UDP ポート値が特定のアプリケーションに割り当てられます。
5. [保存（Save）] をクリックして、設定を保存します。

手順の詳細

ステップ 1 [インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ネットワークデバイス（Network Devices）] を選択してから、デバイスを選択します。

ステップ 2 [機能設定（Feature Configuration）] ペインで [セキュリティ（Security）] サブフォルダを展開します。

ステップ 3 [セキュリティ（Security）] サブフォルダで、[ゾーンベース ファイアウォール（Zone Based Firewall）] > [共通のビルディング ブロック（Common Building Blocks）] を展開して [ポート マッピング（Port Mappings）] をクリックします。[ポート アプリケーション マッピング（Port Application Mapping）] ページが表示されます。

（注） [ポート アプリケーション マッピング（Port Application Mapping）] ページには、デバイスから稼働されるアプリケーションの名前が表示されます。

ステップ 4 アプリケーションに TCP/UDP ポートを割り当てるか、その割り当てを解除するには、アプリケーションをクリックし、その TCP/UDP ポート値を更新します。TCP/UDP ポート値が特定のアプリケーションに割り当てられます。

a) 1 つ以上のポートをコンマで区切って定義することにより、ポートを割り当てます（例：1234, 2222 など）。
b) ポート範囲を定義することにより、ポートを割り当てます（例：1111-1118）。ポートの組み合わせおよびポート範囲を割り当てることもできます。
c) 既存のポート値を削除することにより、ポートの割り当てを解除します。

ステップ 5 [保存（Save）] をクリックして、設定を保存します。

単一 Cisco ISR デバイスのゾーンベース ファイアウォール用にデフォルトのパラメータを設定する

デフォルト パラメータを設定するには、次の手順を実行します。

ステップ 1 [インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ネットワークデバイス（Network Devices）] を選択してから、デバイスを選択します。

ステップ 2 [機能設定（Feature Configuration）] ペインで [セキュリティ（Security）] サブフォルダを展開します。

ステップ 3 [セキュリティ（Security）] サブフォルダで、[ゾーンベース ファイアウォール（Zone Based Firewall）] を展開して [デフォルト パラメータ（Default Parameters）] をクリックします。[Default Parameters] ページが表示されます。

ステップ 4 [Default Parameters] ページで、パラメータ値を変更します。

（注） デフォルト パラメータを変更できるのは ISR デバイスだけです。

ステップ 5 [保存（Save）] をクリックして、設定を保存します。

単一デバイスのゾーンベース ファイアウォール内の別のゾーンへのインターフェイスの割り当て

インターフェイス ビューには、ファイアウォール インスペクションに該当するデバイスのインターフェイスの概要が表示されます。ビューでは、インターフェイスのセキュリティ ゾーンへの割り当てを確認および変更できます。

ゾーンに対してインターフェイスの割り当てまたは割り当て解除を行うには、次の手順を実行します。

ステップ 1 [インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ネットワークデバイス（Network Devices）] を選択してから、デバイスを選択します。

ステップ 2 [機能設定（Feature Configuration）] ペインで [セキュリティ（Security）] サブフォルダを展開します。

ステップ 3 [セキュリティ（Security）] サブフォルダで、[ゾーンベース ファイアウォール（Zone Based Firewall）] を展開して [インターフェイス（Interfaces）] をクリックします。

ステップ 4 [Interface] ページで、変更するインターフェイスを選択し、下矢印アイコンをクリックします。[Zone] ダイアログボックスが表示されます。

ステップ 5 [Zone] ダイアログボックスで、インターフェイスの新しいセキュリティ ゾーンを選択します。選択したインターフェイスがすでにゾーンに割り当てられている場合は、警告メッセージが表示されます。

ステップ 6 そのインターフェイスの割り当てを変更する場合は、警告メッセージに対して [Yes] をクリックします。

ステップ 7 特定のゾーンからインターフェイスの割り当てを解除するには、そのインターフェイスを選択し、ゾーン情報を削除します。

ステップ 8 [Save] をクリックして、変更を保存および適用します。

データ ソースとしての NAM アプリケーション サーバの追加

Prime Infrastructure では、さまざまな機能をリモートで NAM に設定できます。NAM アプリケーション サーバ機能を使用すると、アプリケーション サーバを使用して NAM デバイスを設定することができます。

アプリケーション サーバのパラメータを設定するには、NAM デバイスで次の手順を実行します。

ステップ 1 [インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ネットワークデバイス（Network Devices）] を選択してから、デバイスを選択します。

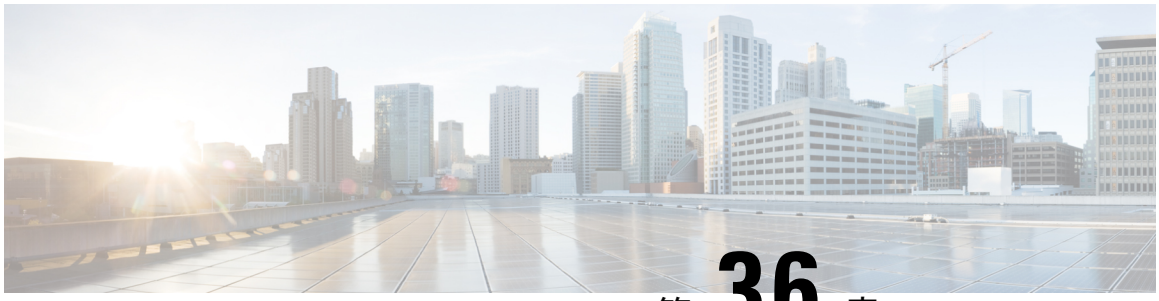
ステップ 2 [追加（Add）] をクリックします。

ステップ 3 [サーバを追加（Add Servers）] ダイアログボックスにサーバの IP アドレスを入力し、ダイアログボックス内の [追加（Add）] ボタンをクリックします。サーバの IP アドレスのリストが [IPアドレス（IP address）] 列の下に表示されます。

ステップ 4 NAM デバイスに展開するサーバの IP アドレスを選択して、[NAMサーバリストに追加（Add to NAM Server lists）] をクリックします。

ステップ 5 [NAMサーバリストにサーバを追加（Add Server(s) to NAM Server List）] ダイアログボックスで、1 つ以上の NAM デバイスの IP アドレスを選択し、ダイアログボックス内の [追加（Add）] ボタンをクリックします。

選択したデバイス IP アドレスが [NAM サーバ リストの一部（Part of NAM Server List on）] 列の下に表示され、選択した NAM デバイスにサーバ パラメータが設定されます。



第 36 章

Prime Infrastructure によって、WAN エンドユーザの一貫したアプリケーション エクスペリエンスが確保される仕組み。

- WAN エンド ユーザの一貫したアプリケーション エクスペリエンスの確保 （975 ページ）

WAN エンド ユーザの一貫したアプリケーション エクスペリエンスの確保

Cisco Prime Infrastructure によって、複数のサイトでアプリケーション間の高品質な WAN エンドユーザ エクスペリエンスを実現できます。

- サイトのアプリケーション主要パフォーマンス評価指標の表示
- WAN 最適化のためのアプリケーション パフォーマンス ダッシュボードの設定
- パフォーマンスの低い WAN アプリケーション、クライアント、サーバ、およびリンクの識別
- WAN 最適化の結果の表示
- WAN クライアント/サーバおよびサイト間最適化トラフィック フローの表示

（注） この機能を使用するには、Cisco Prime Infrastructure の実装に保証ライセンスを含める必要があります。

ネットワーク運用スタッフは共通のデータ リソースを共有する必要があります。これにより、次のような最適化サイクルの各段階を通じてネットワークのパフォーマンス データをすべて把握できます。

- アプリケーションの最適化が必須な場所をネットワーク設計者が計画できるようにするための、最適化の候補となるサイトおよびアプリケーションの識別（「サイトのアプリケーション主要パフォーマンス評価指標の表示」を参照）。

- サイトおよびアプリケーションのパフォーマンス ベースラインの確立（「WAN 最適化のためのアプリケーション パフォーマンス ダッシュボードの設定」を参照）。

Cisco Prime Infrastructure は、重要なパフォーマンス メトリックのベースライン化を実行し、ベースライン値の異常な逸脱を検出します。重要なパフォーマンス メトリックには次のものがあります。

- サーバの応答時間
- クライアントのトランザクション時間
- ネットワーク ラウンドトリップ時間
- MOS スコア
- ジッター
- パケット損失
- 送受信バイト
- インターフェイス使用率
- CPU 使用率
- メモリ使用率

Cisco Prime Infrastructure は、過去 30 日間のメトリックの平均値を取って、各メトリックのベースライン（平均）を決定します。平均値は、各監視対象のエンティティ（インターフェイス、ホスト、サイト、またはアプリケーションなど）で 1 時間ごとに個別に計算されます。たとえば、本日 9 AM ～ 10 AM の特定のサーバの HTTP 応答時間のベースラインは、昨日の 7 PM ～ 8 PM の同じサーバのベースラインとは異なります。

また、Cisco Prime Infrastructure は、過去 30 日のデータを使用してメトリックの標準偏差も計算します。平均値と同様に、標準偏差は各監視対象のエンティティで 1 時間ごとに個別に計算されます。

- WAN のパフォーマンスとアプリケーションの安定性が実際に向上したかどうかを実装後に検証します（「WAN 最適化の結果の表示」を参照）。

各メトリックの平均と標準の偏差は時間とともに変化するため、Cisco Prime Infrastructure はヘルス スコア（適応型しきい値）の計算に使用されるしきい値を継続的に再計算します。Cisco Prime Infrastructure は、1 時間ごとに基準としきい値を計算し、5 分ごとに正常性スコアを評価します。各間隔ごとに、以下のようになります。

1. ヘルス スコアは、アプリケーション サイトの組み合わせごとに計算されます。
2. これらのヘルス スコアは、（すべてのサイト間の）各ビジネス クリティカルなアプリケーションの全体的な健全性と、（すべてのビジネス クリティカルなアプリケーション間の）各サイトの全体的な健全性を得るために集約されます。

サイトまたはアプリケーションにわたって集約する場合は、最も低いスコアが使用されます。たとえば、特定のサイトのビジネス クリティカルなアプリケーションが「赤色」と評価されると、そのサイトもまたその間隔で「赤色」と評価されます。詳細については、「アプリケーション パフォーマンスのサービス ヘルス ルールのカスタマイズ」を参照してください。

- 最適化されたフローの継続的なモニタリングとトラブルシューティング（「WAN クライアント/サーバおよびサイト間最適化トラフィック フローの表示」を参照）。

ベースラインの平均および標準偏差を使用して、Cisco Prime Infrastructure はベースライン値からキーメトリックの異常な偏差を検出することでアプリケーションおよびサービスの健全性の問題をモニタし、モニタリング間隔ごとに各アプリケーションおよびサイトにヘルス スコア（赤色、黄色、または緑色）を割り当てることができます。

- 赤色のスコアは、ベースラインからの非常に異常な偏差（0.1% 未満と思われるベースラインからの偏差）を示します。
- 黄色のスコアは、軽度の異常な偏差（1% 未満と思われる偏差）を示します。
- 緑色のスコアは、メトリックが正常範囲内であることを示します。
- 灰色のスコアは、サイトまたはアプリケーションに不十分なデータがあることを示します。

Cisco Prime Infrastructure は、パフォーマンスの最適化におけるこれらの各段階で一貫したデータ リソースを提供します。

サイトのアプリケーション主要パフォーマンス評価指標の表示

サイトおよびそのサイトのビジネスクリティカルなアプリケーションを表示するには、[Services] > [Application Visibility & Control] > [Service Health] の順に選択します。サイトの各アプリケーションには、システムで使用できる KPI（重要業績評価指標）ごとにスコアが与えられます。

- **トラフィック**（メガビット/秒）
- **クライアント エクスペリエンス**（アプリケーション タイプに基づいて異なります。HTTP などのトランザクション ベース アプリケーションの場合は平均トランザクション時間、RTP などのリアルタイム アプリケーションの場合は MOS コードです。）
- **ネットワーク パフォーマンス**（HTTP の場合は平均ネットワーク時間、RTP の場合はジッターおよびパケット損失）
- **アプリケーション応答**（HTTP などのトランザクション ベースのアプリケーションにのみ適用可能）

KPI スコアは複数のデータ ソースから取得できます。スコアはすべての KPI のすべてのデータ ソースで計算され、メイン ダッシュボードの全体スコアはこれらのスコアの合計です。スコアには、[Health rules] ページに割り当てられた警告と重大しきい値に基づいて、赤色、黄色、または緑色が割り当てられます。このページに移動するには、**[サービス（Services）] > [アプリケーションの可視性と制御（Application Visibility & Control）] > [サービスヘルス（Service Health）]** ページの **[ヘルスルールの起動（Launch Health Rules）]** をクリックします。このオプションを使用して、新しい標準偏差値またはカスタム値を指定することによって、任意のサイト レベルでヘルス ルールの設定を追加または変更できます。

[Service Health] に表示されるデータは、少なくとも 1 時間分のデータでなければなりません。最初の 1 時間の後、前の 1 時間分のデータは次の 1 時間の履歴データとしてデータ ラインでオーバーレイされます。初日の後、標準偏差と平均は、前日の時間単位のデータに基づきます。

これらのスコアは7日間保存されます。前日のデータを表示する場合、最大の移動時間間隔は 6 時間です（最大 6 時間分のデータを同時に確認できます）。

パフォーマンスをモニタするカスタム アプリケーションの作成

カスタム アプリケーションおよびサービスを作成および管理するには、**[サービス（Services）] >[アプリケーションの可視性と制御（Application Visibility & Control）] > [アプリケーションとサービス（Applications and Services）]** を選択します。サービスはアプリケーションのグループです。Prime Infrastructure によって、Cisco NBAR 標準規格と一致したアプリケーションおよびサービスのデフォルト セットが提供されます。（詳細については、NBAR のホーム ページを参照。）

[すべてのアプリケーション（All Applications）] テーブルに、事前定義アプリケーションとユーザ定義アプリケーションがすべて表示されます。一部のアプリケーションを **[ビジネス クリティカルなアプリケーション（Business Critical applications）]** として設定できます。

必要な定義を含み、（デバイスまたは Prime Infrastructure から）使用できないカスタム アプリケーションを作成できます。アプリケーションを作成後、サポート対象デバイスにアプリケーションを展開できます。デバイスにアプリケーション定義を展開すると、NetFlow でエクスポートされたデータが Prime Infrastructure および他の管理ツールに一致します。

デバイスにカスタム アプリケーションを展開し、後にそのアプリケーションを削除する場合は、**[アプリケーションとサービス（Applications and Services）]** オプションを使用してアプリケーションの展開を解除する必要があります。カスタム アプリケーションを Prime Infrastructure からのみ削除すると、カスタム アプリケーションはデバイスでアクティブのままになります。

定義のないアプリケーションは「Unknown」として表示されます。

カスタム アプリケーションはサービスの下に構成されます。サービスは、Cisco NBAR 標準規格に合わせるためにカテゴリおよびサブカテゴリごとに編成されます。詳細については、NBAR のホーム ページを参照してください。

カスタム アプリケーションを作成するには、次の手順に従ってください。

ステップ 1 **[サービス（Services）] > [アプリケーションの可視性と制御（Application Visibility & Control）] > [アプリケーションとサービス（Applications and Services）]** を選択します。

ステップ 2 [作成（Create）]**Create**をクリックします。

ステップ 3 必須の **[一般（General）]** フィールドと **[属性（Attributes）]** フィールドに入力します。

ステップ 4 **[ルール（Rule）]** ドロップダウン リストからトラフィック分類ルールを選択します。

（注） プロトコルは、NAM および NBAR2 をサポートする IOS デバイスに適用できます。

サーバ/DSCP は、NBAR2 をサポートする IOS デバイス バージョン 15.5(2) 以降に適用可能です。

[URL]：NAM バージョン 6.0(2) 以降および NBAR2 をサポートする IOS デバイスに適用可能です。

[NAM サーバ IP アドレス（NAM Server IP Address）]：NAM 6.0(2) と上記のデバイスにのみ適用されます。

[RTP ペイロード タイプ（RTP Payload Type）]：Prime Infrastructure にのみ適用されます。

ステップ 5 **[条件（Condition）]** ドロップダウン リストをクリックし、選択したルールに応じて該当するフィールドに必要な値を入力します。

ステップ 6 より多くのトラフィック ルールおよび条件を追加するには、[+] アイコンをクリックします。

ステップ 7 [作成（Create）] をクリックします。

新しく作成されたアプリケーションが **[すべてのアプリケーション（All Applications）]** に表示されます。

ステップ 8 新しく作成されたアプリケーションを選択し、**[展開（Deploy）]** をクリックします。

（注） 既存のアプリケーションの展開を解除することができます。展開を解除するには、[アプリケーションとサービス（Applications and Services）] を選択し、[展開の解除（Undeploy）] をクリックします。

ステップ 9 このアプリケーションを展開するデバイスを選択し、**[送信（Submit）]** をクリックします。

ステップ 10 **[ジョブの表示（View Jobs）]** をクリックし、展開ジョブのステータスを表示します。

[AVCサービスヘルス（AVC Service Health）] ウィンドウを使用したサービス ヘルスの表示

[サービス（Services）][アプリケーションの可視性と制御（Application Visibility & Control）][サービスヘルス（Service Health）] の順に選択し、**[ヘルスの概要（Health Summary）]** をクリックします。Cisco Prime Infrastructure はタイムラインのヘルス情報を表示するために変更します。

[サービスヘルス（Service Health）] ウィンドウでは、次の図に示す情報を確認できます。

[サービスアプリケーションの表示およびコントロールサービスヘルス（Service Application Visibility and Control Service Health）] ウィンドウに表示される情報は、次のとおりです。

表 *78 : [*サービスアプリケーションの表示およびコントロールサービスヘルス（*Service Application Visibility and Control Service Health***）*]* ウィンドウの説明**

1	選択したフィルタのロケーション グループがリストされます。
2	クリックして [Health Summary] と [Health Timeline] を切り替えます。
3	次の項目へのクイック リンクが提供されます。 • **[ヘルスルール（Health Rules）]** ページ。このページでは、必要に応じて、ネットワークのヘルス ルール設定を変更できます。 • 現在定義されているビジネス クリティカルなアプリケーションを表示および変更します。
4	現在表示しているフィルタが示されます。任意のフィルタをクリックして削除し、ウィンドウを更新できます。
5	ビジネス クリティカルなアプリケーションがリストされます。
6	色付きの記号は、**[ヘルスルール（Health Rules）]** ページで指定したヘルス ルールの設定に基づく、良好、警告、およびクリティカルの各しきい値を示します。
7	スライダを移動して、サービス ヘルス情報を表示する時間範囲を指定します。

アプリケーション パフォーマンスのサービス ヘルス ルールのカスタマイズ

[サービス（Services）] > [アプリケーションの可視性と制御（Application Visibility & Control）] > [サービスヘルス（Service Health）] に表示されるデータは、ヘルス ルールを使用して算出されます。目的の行をクリックし、クリティカル値と警告値を編集することで、ヘルス ルールをカスタマイズできます。

- [Critical]：データ値が指定されたクリティカル値を超えると赤色に変わります。
- [Warning]：データ値が警告値を超えると黄色に変わります。

ヘルス ルールが指定したクリティカル値または警告値を超えない場合は、緑色です。

たとえば、トラフィック レートの場合、T1 を指定して、特定のサイト、アプリケーション、およびデータソースに対しベースライン値 100 Mbps を指定し、標準偏差値を 20 Mbps に指定したとします。

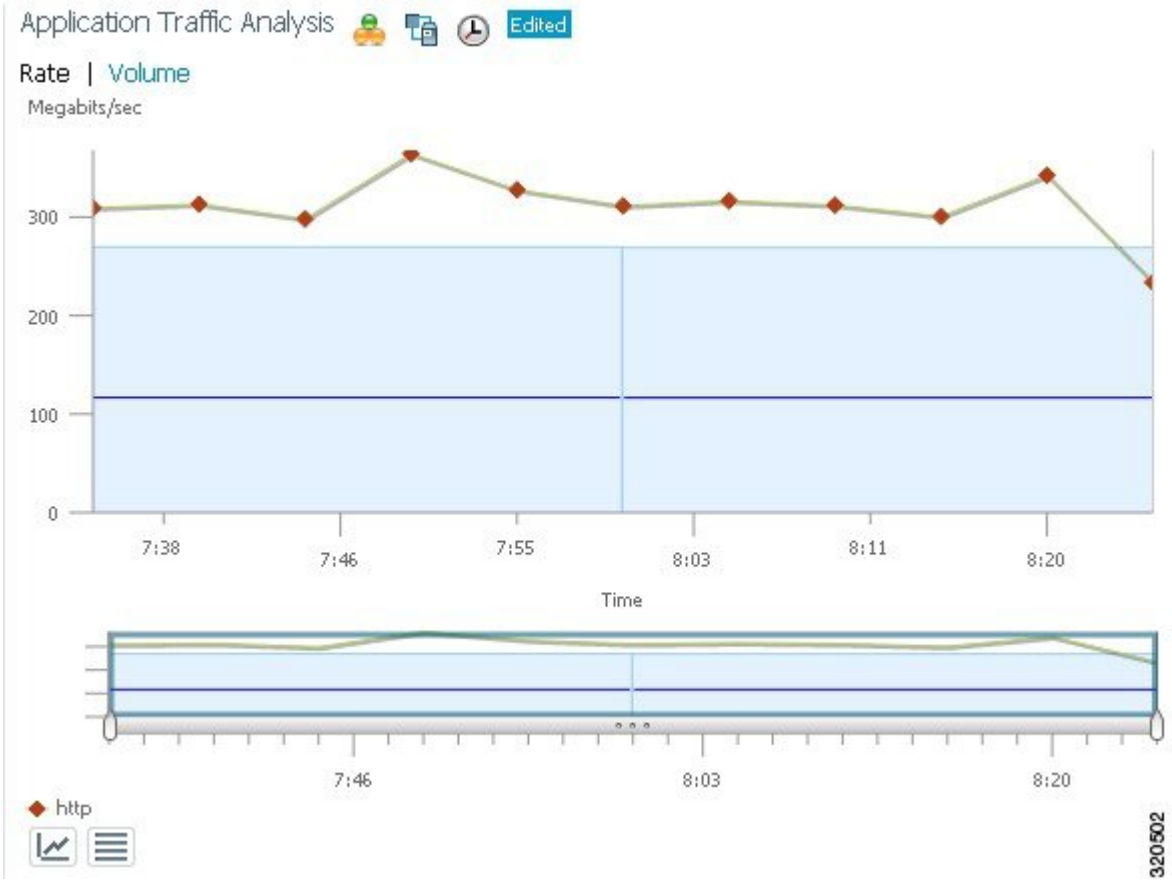
トラフィック レートが 161.8 Mbps（100+(3.09 x 20)）を超えた場合、クリティカルな警告を示す赤色のバーが表示されます。

色付きのバーをクリックすると詳細情報を取得できます。

アプリケーション パフォーマンスを計算するためのベースラインの有効化

標準偏差値および平均値は、[Service Health] でスコアを計算するために使用されます。ベースライン化は、デフォルトではイネーブルにされていません。ベースライン化がイネーブルの場合は次のようになります。

- 青色のボックスは標準偏差を示します。
- 青色の線は、その時間の平均値を示します。



ベースライン化を有効にするには、次の手順に従います。

ステップ 1 [ダッシュボード（Dashboard）]>[パフォーマンス（Performance）]>[アプリケーション（Application）]の順に選択します。

ベースライン化は次のダッシュレットでサポートされています。

1. [Application Traffic Analysis]：サイト/企業の 1 つのアプリケーション、サービス、またはアプリケーションのセットの集約帯域幅率/量を示します。
2. [Application ART Analysis]：トランザクションの応答時間を示します。

ステップ 2 アプリケーション トラフィック分析のベースライン化を有効にするには、次の手順を実行します。

a) **[アプリケーション トラフィックの分析（Application Traffic Analysis）]** ダッシュレットを開き、カーソルをダッシュレット アイコンの上に合わせて、**[ダッシュレット オプション（Dashlet Options）]** をクリックします。

b) [ベースライン（Baseline）] チェックボックスを選択して変更を保存します。

ステップ 3 アプリケーション応答時間分析のベースライン化を有効にするには、次の手順を実行します。

a) **[アプリケーション ART 分析（Application ART Analysis）]** ダッシュレットを開き、カーソルをダッシュレット アイコンの上に合わせて、**[ダッシュレット オプション（Dashlet Options）]** をクリックします。

b) **[メトリック タイプ（Metric Type）]** ドロップダウンリストからメトリックを選択します。

[サーバ応答時間（Server Response Time）] メトリックを選択すると、個々のアプリケーション サーバを選択して、そのサーバの応答時間が過去にどうであったかを確認できます。

c) [ベースライン（Baseline）] チェックボックスを選択して変更を保存します。

WAN 最適化のためのアプリケーション パフォーマンス ダッシュボードの設定

WAN の最適化を実行する前に、次の手順を実行して、対象のアプリケーションとサイトの標準パフォーマンス特性を確立します。

ステップ 1 [ダッシュボード（Dashboard）]>[パフォーマンス（Performance）]>[アプリケーション（Application）] の順に選択します。

ステップ 2 このページに次のダッシュレットを追加します（「ダッシュボードへのダッシュレットの追加 （15 ページ）」を参照）。

- Worst N Clients by ART Metrics
- Worst N Sites by ART Metrics
- Application Server Performance
- Application Traffic Analysis

ステップ 3 これらのダッシュレットを使用して、現在設定されているように最適化候補のパフォーマンス特性を確立します。

- **[ART メトリックがワースト N のクライアント（Worst N Clients by ART Metrics）]**：パフォーマンスが最も低いクライアントとアプリケーション：最大および平均トランザクション時間、24時間パフォーマンス トレンド。
- **[ART メトリックがワースト N のサイト（Worst N Sites by ART Metrics）]**：パフォーマンスが最も低いサイトおよびアプリケーションに関する同じ情報。
- **[アプリケーション サーバのパフォーマンス（Application Server Performance）]**：すべてのアプリケーション サーバ：最大および平均サーバ応答時間、24 時間パフォーマンス トレンド。
- **[アプリケーション トラフィックの分析（Application Traffic Analysis）]**：24 時間のアプリケーション トラフィック メトリック（バイト/秒）と1秒当たりのパケット数が提供されます。期間中の統計情報の平均値、最小値、最大値、中央値と、第 1 および第 2 標準偏差が計算されます。

任意のダッシュレットの列ヘッダーをクリックすることで列ごとにソートできます。また、ダッシュレットのデータは、**[タイム フレーム（Time Frame）]**、**[サイト（Site）]**、および **[アプリケーション（Application）]** でフィルタリングできます。

ステップ 4 **[サイト（Site）]** タブをクリックし、ステップ 3 と同様に、**[トップ N のアプリケーション（Top N Applications）]** **[アラーム数がトップ N のデバイス（Top N Devices with Most Alarms）]**、**[トップ N のクライアント（Top N Clients）]** および **[ART メトリックがワースト N のクライアント（Worst N Clients by ART Metrics）]** を使用します。

パフォーマンスの低い WAN アプリケーション、クライアント、サーバ、およびリンクの識別

次の手順に従い、ネットワークでパフォーマンスが最も低いアプリケーション、クライアント、サーバ、およびネットワーク リンクを特定します。

ステップ 1 **[ダッシュボード（Dashboard）]** > **[パフォーマンス（Performance）]** > **[WAN 最適化（WAN Optimization）]** を選択します。

ステップ 2 このダッシュボードに次のダッシュレットを追加します（「ダッシュレットの追加」を参照）。

- Application Traffic
- Server Traffic
- Client Traffic
- Network Links

ステップ 3 これらのダッシュレットを使用して、最適化の候補を特定します。

- すべてのダッシュレットには、アプリケーション、クライアント、サーバ、またはネットワーク リンクごとに現在のトラフィック レート（バイト/秒）、同時接続の平均数、および平均トランザクション時間（ミリ秒）が表示されます。
- **[ネットワーク リンク（Network Links）]** には、各リンクのクライアントおよびサーバのエンドポイントのサイト、ならびにリンクが存在する時間の長さの平均が表示されます。
- **[サーバのトラフィック（Server Traffic）]** には、サーバの IP アドレスとそのサーバにより処理されるアプリケーションの両方が表示されます。

ステップ 4 必要に応じてパフォーマンス データをソートおよびフィルタリングします。

- 任意のダッシュレットの任意の列のソートするには、列ヘッダーをクリックします。
- **[タイム フレーム（Time Frame）]** **[サイト（Site）]**、または **[アプリケーション（Application）]** 別にすべてのダッシュレットに表示されるデータをフィルタリングするには、**[フィルタ（Filters）]** 行で使用するフィルタ基準を入力または選択し、**[実行（Go）]** をクリックします。

- ダッシュレット内でフィルタリングするには、その[Filter]アイコンをクリックして、クイック フィルタまたは高度なフィルタを指定するか、またはプリセット フィルタを使用します。

ステップ 5 同じデータのクイック レポートの場合：

a) **[レポート（Reports）] > [レポート起動パッド（Report Launch Pad）]** を選択します。
b) レポートに対してフィルタとその他の基準を指定し、**[実行（Run）]** をクリックします。

WAN 最適化の結果の表示

候補サイトで変更を展開した後、次の手順を実行して、最適化の投資利益率を検証します。

ステップ 1 [Dashboard] > [Performance] > [WAN Optimization] の順に選択します。

このページのダッシュレットには、次のものが表示されます。

- **トランザクション時間（クライアント エクスペリエンス）**：過去 24 時間の平均クライアント トランザクション時間（ミリ秒単位）がグラフ表示されます。最適化されたトラフィックとパススルー トラフィック（最適化がオフ）で行が分かれています。最適化が有効になっている場合は、パススルー時間と比較して、最適化されたトラフィック時間の方が短くなっているはずです。
- **平均同時接続数（最適化とパススルーの比較）**：指定された期間の同時クライアントおよびパススルー接続数の平均がグラフ表示されます。
- **トラフィックのボリュームと圧縮率**：圧縮前のバイト数と圧縮後のバイト数の帯域幅減少率がグラフ表示されます。
- **マルチセグメント ネットワーク時間（クライアント LAN-WAN - サーバ LAN）**：複数のセグメント間のネットワーク時間がグラフ表示されます。

ステップ 2 ダッシュレットのデータは、**タイム フレーム**、**クライアント サイト**、**サーバ サイト**、**アプリケーション**でフィルタリングできます。

ステップ 3 レポートを作成するには、次の手順を実行します。

a) [Tools] > [Reports] > [Report Launch Pad] の順に選択し、[Performance] > [WAN Application Performance Analysis Summary] の順に選択します。
b) フィルタと他のレポートの設定を指定し、[Run] をクリックします。

WAN クライアント/サーバおよびサイト間最適化トラフィック フローの表示

最適化された WAN トラフィックをモニタするには、次の手順を実行します。

ステップ 1 **[ダッシュボード（Dashboard）] > [パフォーマンス（Performance）] > [WAN 最適化（WAN Optimization）]** を選択します。

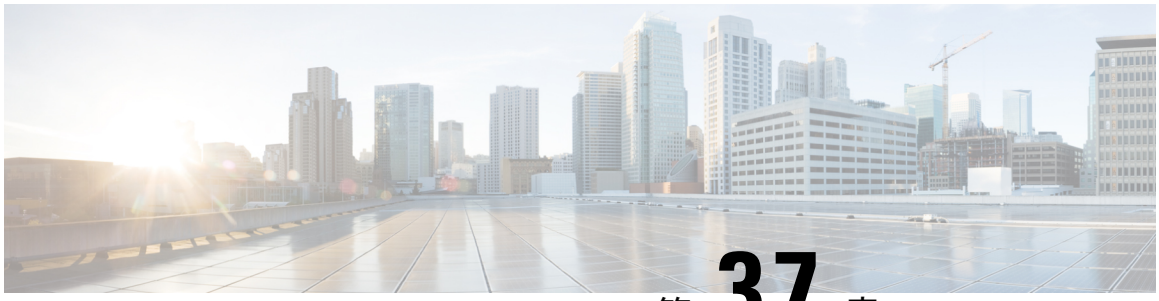
ステップ 2 **[マルチセグメント分析（Multi-Segment Analysis）]** ダッシュレットで、**[マルチセグメント分析の表示（View Multi-Segment Analysis）]** をクリックします。

ステップ 3 個々のクライアント/サーバセッションを表示するには **[カンバセーション（Conversations）]** タブをクリックし、集約されたサイト トラフィックを表示するには **[サイト間（Site to Site）]** タブをクリックします。各クライアント（またはクライアント サイト）とサーバ（またはサーバ サイト）のペアおよび使用中のアプリケーションについて、これらのページには次のものが表示されます。

- 平均および最大トランザクション時間：クライアント要求が行われてから、サーバから最後の応答パケットを受け取るまでの時間。トランザクション時間は、クライアントの使用とアプリケーション タイプ、およびネットワーク遅延によって異なります。トランザクション時間は、クライアント エクスペリエンスをモニタし、アプリケーション パフォーマンスの問題を検出するときの、主要なインジケータです。
- 平均クライアント ネットワーク時間：クライアントとローカル スイッチやローカル ルータとの間のネットワーク時間。Wide Area Application Services（WAAS）モニタリングでは、WAE クライアント データ ソースからのクライアント ネットワーク時間は、クライアントとそのエッジ WAE との間のネットワーク RTT を表し、WAE サーバ データ ソースからのクライアント ネットワーク時間は、（エッジ WAE とコア WAE との間の）WAN RTT を表します。
- 平均 WAN ネットワーク時間：WAN セグメント全体の時間（クライアントの場所とサーバの場所のエッジ ルータ間）。
- 平均サーバ ネットワーク時間：サーバと NAM プローブ ポイントとの間のネットワーク時間。WAAS モニタリングでは、サーバ データ ソースからのサーバ ネットワーク時間は、サーバとそのコア WAE との間のネットワーク時間を表します。
- 平均サーバ応答時間：アプリケーション サーバが要求に応答するのに要する平均時間。これは、サーバに到達したクライアント要求と、サーバによって返された最初の応答パケットとの間の時間です。通常、サーバ応答時間の増加は、CPU、メモリ、ディスク、または I/O などのアプリケーション サーバ リソースに問題があることを示します。
- トラフィック量：クライアント、WAN、サーバの各セグメントにおける毎秒のバイト量。

ステップ 4 必要に応じてパフォーマンス データをソートおよびフィルタリングします。

- 任意の列をソートするには、列ヘッダーをクリックします。
- **[タイム フレーム（Time Frame）]** に表示されるデータをフィルタリングしたり、[フィルタ（Filter）] アイコンをクリックして、クイック フィルタまたは高度なフィルタを指定するか、またはプリセット フィルタを使用できます。



第 37 章

Microsoft Lync トラフィックのモニタ

• Microsoft Lync トラフィックをモニタする方法 （987 ページ）

Microsoft Lync トラフィックをモニタする方法

Prime Infrastructure を使用して、ネットワーク内の Microsoft Lync トラフィックをモニタすることができます。Microsoft Lync Software Defined Network（SDN）API に備わっているインターフェイスを使用すると、ネットワーク管理システムは Microsoft Lync ネットワーク診断データにアクセスして、Lync ネットワーク トラフィックの監視と Microsoft Lync の Quality of Service の最適化を行うことができます。Prime Infrastructure は、Microsoft Lync の品質アップデート メッセージを処理およびフィルタリングし、Microsoft Lync コールを集約します。ボリュームの傾向を時系列で表示でき、時間および場所のグループに基づくフィルタリングなどの、コール タイプの概要を取得できます。また、個々のコールを表示したり、個々のコール ストリームをトラブルシューティングできます。

（注） Prime Infrastructure は、SDN 2.2 以降のバージョンをサポートしていません。

Lync モニタリングのセットアップ （987 ページ）
Microsoft Lync の一般データの表示 （988 ページ）
ユーザの Microsoft Lync コールの問題のトラブルシューティング （989 ページ）
サイト間 Microsoft Lync データの表示 （989 ページ）

Lync モニタリングのセットアップ

Microsoft Lync がネットワーク内でどのように展開されているかをモニタして集中型ビューを提供するには、Microsoft Lync データの受信側として Prime Infrastructure を登録する必要があります。

SDN サーバで、次の行を追加するには LyncDialogListener.exe ファイルを編集します。LyncDialogListener.exe.config ファイルは、次のデフォルトの場所の Lync SCN API インストール ディレクトリにあります：C:\Program Files\Microsoft Lync Server\Microsoft Lync SDN API

<add key=“submituri” value=“https://PI_server_name/webacs/lyncData”/>

https://PI_server_name は、信頼されたルート証明機関の証明書で指定されている Prime Infrastructure の名前です。

<add key= “clientcertificateid” value=“value”/>

value は、信頼されたルート証明機関の証明書で指定されている Prime Infrastructure サーバの証明書の値です。

または、Microsoft SDN インターフェイスを使用して Prime Infrastructure サーバの詳細を入力する場合は、セキュア HTTP 経由での XML 通信を可能にするために SSL 証明書を受け入れる必要があります。

Prime Infrastructure を Microsoft Lync データの受信側として登録すると、Microsoft Lync の全詳細が Prime Infrastructure に送信されます。

Microsoft Lync の一般データの表示

Prime Infrastructure を Microsoft Lync データの受信側として登録すると、Microsoft Lync の全詳細が Prime Infrastructure に送信されます。Microsoft Lync データをモニタするには、次の手順を実行します。

ステップ 1 [Services] > [Application Visibility & Control] > [Lync Monitoring] の順に選択します。

ステップ 2 さまざまなコール タイプと、指定した時間帯にわたるそれぞれのコール量を表す色付きバーのいずれかをクリックして、追加の詳細を表示します。[Lync Conversations] テーブルには、選択したコール タイプの集約されたカンバセーションがリストされます。

ステップ 3 [Lync Conversations] テーブルから、発信者の横にある矢印をクリックして、発信者から呼び出し先へのそのカンバセーションの詳細を展開して表示します。たとえば、ビデオ会話を展開する場合は、次の詳細を示す 4 つの行があります。

1. 発信側から着信側へのオーディオの詳細
2. 着信側から発信側へのオーディオの詳細
3. 発信側から着信側へのビデオの詳細
4. 着信側から発信側へのビデオの詳細

ステップ 4 [Filter] アイコンをクリックして、特定の発信者サイトから、または特定の呼び出し先サイトからの、選択した時間内のカンバセーションのリストを表示します。

Lync モニタリングのセットアップ （987 ページ）
ユーザの Microsoft Lync コールの問題のトラブルシューティング （989 ページ）
サイト間 Microsoft Lync データの表示 （989 ページ）

ユーザの Microsoft Lync コールの問題のトラブルシューティング

エンドユーザがコールの問題を抱えていることを示すコールを受信した場合は、Prime Infrastructure を使用して、特定のユーザの Microsoft Lync コールを表示し、ジッターが最も多い（またはパケット損失が最も著しい）コールのリストを表示できます。

ステップ 1 [Services] > [Application Visibility & Control] > [Lync Monitoring] の順に選択します。

ステップ 2 [Filter] アイコンをクリックし、エンドユーザが属するサイトを選択します。

Prime Infrastructure に、過去 6 時間におけるコール量が表示されます。

ステップ 3 エンドユーザでコールの問題が発生していた時間がわかっている場合は、[Filter] アイコンをクリックし、[Time Filter] に目的の時間のパラメータを入力します。

ステップ 4 問題が発生した期間の音声コールに対応する色付きバーをクリックします。[Lync Conversations] テーブルには、選択したコール タイプの集約されたカンバセーションがリストされます。

ステップ 5 [Lync Conversations] テーブルから、コール問題を経験したエンドユーザの横にある矢印をクリックして、発信者から呼び出し先へのそのカンバセーションの詳細を展開して表示します。たとえば、ビデオ会話を展開する場合は、次の詳細を示す 4 つの行があります。

1. 発信側から着信側へのオーディオの詳細
2. 着信側から発信側へのオーディオの詳細
3. 発信側から着信側へのビデオの詳細
4. 着信側から発信側へのビデオの詳細

Prime Infrastructure に、メッセージ交換（カンバセーション）のコール メトリックが表示されます。

関連トピック

Lync モニタリングのセットアップ （987 ページ）
Microsoft Lync の一般データの表示 （988 ページ）
サイト間 Microsoft Lync データの表示 （989 ページ）

サイト間 Microsoft Lync データの表示

Prime Infrastructure を使用して、サイト間の Microsoft Lync データを表示できます。たとえば、特定のサイトから特定のサイトに発信されるすべての Microsoft Lync コールをモニタできます。

ステップ 1 [Services] > [Application Visibility & Control] > [Lync Monitoring] の順に選択します。

ステップ 2 [Filter] アイコンをクリックし、[Caller Site] で Microsoft Lync コールの発信元となるサイトを選択します。

ステップ 3 [Filter] アイコンから、[Callee Site] で、Microsoft Lync コールが受信されるサイトを選択します。

Prime Infrastructure に、選択したサイト間の各タイプのすべてのコール（ビデオ、音声およびアプリケーション共有）について、過去 6 時間のコール量が 5 分刻みで表示されます。

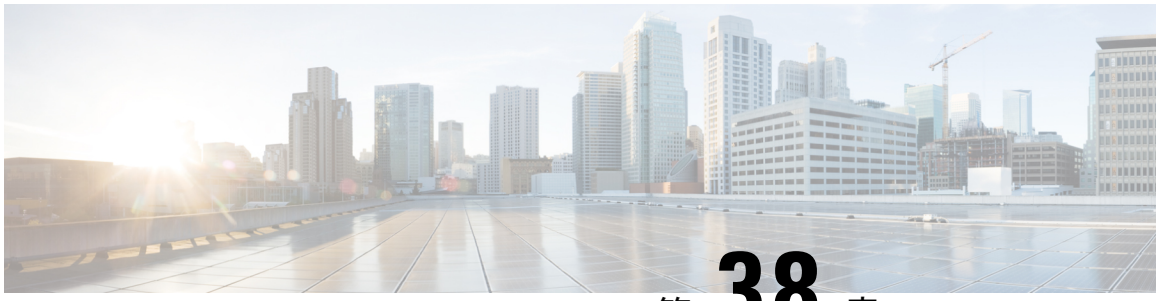
ステップ 4 [サービス（Services）] > [アプリケーションの可視性と制御（Application Visibility & Control）] > [Lync モニタリング（Lync Monitoring）] > [コール タイプ（Call type）]（[音声（audio）]、[ビデオ（video）]、または [アプリケーション共有（application sharing）]）を選択してコール メトリックを表示します。

音声通話の詳細には平均オピニオン評点（MOS）の数値が含まれています。Prime Infrastructure はこの値に対して、次の表に示すエンドユーザに提供されるエクスペリエンスの音声品質を表す値を割り当てます。

MOS 値	Prime Infrastructure 値
3.5 より多い	Good
2 ～ 3.5	Fair
2 未満	不良

関連トピック

Lync モニタリングのセットアップ （987 ページ）
Microsoft Lync の一般データの表示 （988 ページ）
ユーザの Microsoft Lync コールの問題のトラブルシューティング （989 ページ）



第 38 章

Mediatrace を使用した RTP および TCP フローのトラブルシューティング

• Mediatrace とは （991 ページ）

Mediatrace とは

Mediatrace トラブルシューティング ツールは、現在アクティブな RTP ストリームまたは TCP セッションが一覧表示されたテーブルを生成します。これらの Mediatrace テーブルおよび関連オプションを使用すると、次の操作が可能です。

- 問題のある RTP または TCP フローの識別と選択。
- RTP または TCP フローに関する問題のトラブルシューティング。
- 2 つの任意のエンドポイント間の RTP または TCP フローに関する問題のトラブルシューティング。
- [RTP Conversations] ダッシュレットから開始する RTP フローに関する問題のトラブルシューティング。
- フロー パフォーマンス インジケータとデータ ソースの識別と比較。

Mediatrace を使用した現在アクティブな RTP ストリームと TCP セッションの表示 （991 ページ）

RTP または TCP フローからの Mediatrace の起動 （993 ページ）

エンドポイントからの Mediatrace の起動 （994 ページ）

Mediatrace で報告された最も悪い RTP エンドポイントのトラブルシューティング （996 ページ）

Mediatrace を使用した複数のソースからのフロー データの比較 （998 ページ）

Mediatrace を使用した現在アクティブな RTP ストリームと TCP セッションの表示

[RTP Streams] および [TCP Sessions] テーブルに表示されるフロー情報は、ネットワーク全体にわたって生成される NAM および NetFlow データから収集され集約されます。

[RTP Streams] テーブルの多くの行は、ツリー階層で配置されています。これは、1 つの RTP アプリケーション フローが複数のデータ ストリームに関与するときに発生します。この場合、2 つのアプリケーション エンドポイント間のフローは三角形のアイコンが付いている単一行に集約されます。

デフォルトでは、[RTP ストリーム（RTP Streams）] テーブルのデータが Prime Infrastructure で 60 秒ごとに自動的に更新されます。また、いずれかのプリセット フィルタを使用することもできます。

[TCP セッション（TCP Sessions）] のデータは Prime Infrastructure によって 300 秒間（5 分）に一度更新されます。[アプリケーション別にフィルタ（Filter by Application）] フィルタリング オプションを使用すると、リスト内のアプリケーションを追加したり除外したりできます。

また、どちらかのテーブルの [Refresh] ボタンをいつでもクリックすることができます。[Enable auto refresh] チェックボックスをオフにすることで、自動更新をオフにすることができます。

Mediatrace テーブルを使用するには、次の手順を実行します。

ステップ 1 [サービス（Services）] > [Application Visibility and Control] > [Mediatrace] の順に選択します。

ステップ 2 **[アプリケーション（Application）]** ドロップダウン リストから、**[RTP]** または **TCP** を選択します。ページに対応するテーブル [RTP Streams] または [TCP Sessions] が表示されます。

ステップ 3 トラブルシューティング対象のフローを探します。

- 特定のタイプの問題があるすべてのフローを確認するには、適切な列ヘッダーをクリックしてその列でソートします。

  たとえば、ネットワーク全体の RTP パフォーマンスをモニタしていて、ジッター/パケット損失が最も著しいストリームを確認する場合は、[Jitter] または [Packet Loss] の列ヘッダーをクリックして、これらのパフォーマンス インジケータでストリームをソートします。その後、トラブルシューティングのためにストリームのいずれかを選択できます。

- 問題のある特定のフローを検索するには、[クイック フィルタ（Quick Filter）] アイコンをクリックし、1 つ以上の行見出しの下にフィルタ基準を入力します。

  たとえば、アプリケーションへのアクセスに問題があるエンドユーザは、IP アドレスとそのアプリケーションの名前を報告する場合があります。クライアント IP アドレスまたはアプリケーション ID の TCP テーブルでクイック フィルタを実行し、そのセッションをトラブルシューティングのために選択できます。

- RTP サブフローの問題を発見するには、集約された RTP フローの横にある三角形のアイコンをクリックします。

  たとえば、任意の 2 つのエンドポイント間の RTP 音声/ビデオ フローは、三角形のアイコンとともに単一フローとして [RTP Streams] テーブルに表示されます。アイコンをクリックすると、4 つのサブフロー（着信および発信ビデオ サブフローと着信および発信音声サブフロー）が表示されます。

ステップ 4 フローをトラブルシューティングするには、「選択した RTP または TCP フローからの Mediatrace の実行」を参照してください。

関連トピック

RTP または TCP フローからの Mediatrace の起動 （993 ページ）
エンドポイントからの Mediatrace の起動 （994 ページ）
Mediatrace で報告された最も悪い RTP エンドポイントのトラブルシューティング （996 ページ）
Mediatrace を使用した複数のソースからのフロー データの比較 （998 ページ）

RTP または TCP フローからの Mediatrace の起動

Mediatrace を使用して RTP フローまたは TCP フローをトラブルシューティングするには、次の手順を実行します。

ステップ 1 [サービス（Services）] > [Application Visibility and Control] > [Mediatrace] の順に選択します。[アプリケーション（Application）] ドロップダウン リストで [RTP] または [TCP] を選択し、「Mediatrace を使用した現在アクティブな RTP ストリームと TCP セッションの表示」のステップに使用するフローを見つけます。

ステップ 2 フローを選択して [サービス パスのトレース（Trace Service Path）] をクリックします。Prime Infrastructure には、選択したフローの [RTP ストリームの詳細（RTP Stream Details）] または [TCP ストリームの詳細（TCP Stream Details）] ページが表示されます。[トラブルシューティングの状態（Troubleshooting Status）] テーブルに、フローのパス内のすべてのルータがフローの送信元エンドポイントからの距離の順に表示されます。Medianet 対応ルータは、フィルムストリップ（映画）アイコンで示されます。

ステップ 3 フローのパス内のルータから Mediatrace または Traceroute を実行するには、テーブルでそのルータの横にある [Mediatraceの開始（Start Mediatrace）] または [tracerouteの開始（Start Traceroute）] リンクをクリックします。

デバイスが Mediatrace に対応している場合は [Mediatrace の開始（Start Mediatrace）] リンクが表示され、デバイスが Mediatrace に対応していない場合は [traceroute の開始（Start Traceroute）] リンクが表示されます。

Mediatrace が開始するまでに 1 分以上かかる場合があり、その時間はトラフィック、輻輳、およびフローエンドポイント間のホップの総数によって異なります。

Mediatrace または Traceroute の実行中に [ログ（Logs）] タブをクリックすると、次のような役立つ情報を確認できます。

- 操作の進行状況。
- ルータの応答タイムアウトや完了しなかった他の手順など、操作中に発生したエラー。
- 非 Medianet 対応ルータのある場所、発生した場所、およびどのように処理されたか。
- Medianet が設定されていない Medianet 対応ルータ。

ステップ 4 操作が完了すると、[Troubleshooting] タブにフローの 2 つのエンドポイント間のすべてのデバイスのトポロジ マップが表示されます。マップ内のデバイス アイコンは以下で構成されます。

- [Alarm Severity]：現在デバイスに記録されている最も重大なアラーム。
- [フラグ（Flag）]：Mediatrace または Traceroute が開始されたデバイス。
- [Filmstrip]：デバイスは Medianet に対応しています。

- 赤色の背景のマイナス記号：デバイスは Medianet に対応していますが、Medianet レスポンダとして設定されていません。RTP/TCP のパフォーマンス統計情報は、そのデバイスで使用できません。この状況を解決するには、「Mediatrace で報告された最も悪い RTP エンドポイントのトラブルシューティング」の説明に従って、Medianet としてデバイスを設定する必要があります。
- マイナス記号：デバイスは管理対象外です。

ステップ 5 RTP または TCP フローのパス内のすべての Medianet 対応デバイスについて、CPU およびメモリ使用率、ジッター、パケット損失などの重要なパフォーマンス メトリックを確認するには、[Medianet Path View] タブをクリックします。パフォーマンス メトリックを数値またはグラフ形式で表示するには、[Medianet Path View] ペインのサブタブをクリックします。

（注） [Medianetパスビュー（Medianet Path View）] タブは、[トラブルシューティングの状態（Troubleshooting Status）] テーブルから Mediatrace の操作を開始できる場合にのみ使用可能です。Traceroute 操作をトリガーできるだけの場合は、表示されません。

ステップ 6 次の操作を実行するには、[Troubleshooting Status] テーブルの適切なリンクを使用します。

- 別のルータで Mediatrace または Traceroute 操作を開始する。
- 完了した Mediatrace または Traceroute 操作を再起動する、または進行中の操作を停止する。

関連トピック

Mediatrace を使用した現在アクティブな RTP ストリームと TCP セッションの表示 （991 ページ）
エンドポイントからの Mediatrace の起動 （994 ページ）
Mediatrace で報告された最も悪い RTP エンドポイントのトラブルシューティング （996 ページ）
Mediatrace を使用した複数のソースからのフロー データの比較 （998 ページ）

エンドポイントからの Mediatrace の起動

ネットワークの任意の 2 つのエンドポイント間のすべての RTP フローまたは TCP フローに対して、Mediatrace をすばやく起動できます。これには、同一または異なるサイトでの任意の 2 つのエンドポイント間、または2つの異なるサイトでのルータのペア間で動作している特定のフローを含めることができます。

これは、ネットワークに NAM モニタリング機能がない場合、または急いでいて RTP または TCP フローの 2 つのエンドポイントの IP アドレスしか分からない場合に役立ちます。ただしこの場合も、適切な RTP または TCP の Mediatrace テーブルからトレースに移動して開始する必要があります。

2 つのエンドポイントからアドホック Mediatrace を起動するには、次の手順を実行します。

ステップ 1 [サービス（Services）] > [Application Visibility and Control] > [Mediatrace] の順に選択します。[アプリケーション（Application）] ドロップダウン リストから、[RTP] または [TCP] を選択します。

ステップ 2 [Mediatrace のセッションの指定（Specify Session for ）] をクリックします。

ステップ 3 必要な情報を入力します。

- RTP フローの場合：
  - 送信元サイトを選択します。
  - 送信元のエンドポイント IP アドレスを入力します。
  - 宛先のエンドポイント IP アドレスを入力します。
- TCP フローの場合：
  - クライアント サイトを選択します。
  - クライアントのエンドポイント IP アドレスを入力します。
  - サーバ エンドポイント IP アドレスを入力します。

ステップ 4 分かっている追加のエンドポイント情報を提供します。

- RTP フローの場合は、送信元エンドポイント ポートと宛先エンドポイント ポートを選択するか、または入力します。
- TCP フローの場合は、サーバのエンドポイント ポートを選択するか、または入力します。

ステップ 5 [Trace Service Path]（RTP フローの場合）または [OK]（TCP フローの場合）をクリックします。Prime Infrastructure には、指定したフローの [RTP ストリームの詳細（RTP Stream Details）] または [TCP ストリームの詳細（TCP Stream Details）] ページが表示されます。[トラブルシューティングの状態（Troubleshooting Status）] テーブルに、フローのパス内のすべてのルータがフローの送信元またはクライアント エンドポイントからの距離の順に表示されます。横に [映画（filmstrip）] アイコンがあるルータは Medianet に対応しています。

ステップ 6 フローのパス内のルータから Mediatrace または Traceroute を実行するには、テーブルでそのルータの横にある [Mediatraceの開始（Start Mediatrace）] または [tracerouteの開始（Start Traceroute）] リンクをクリックします。

Mediatrace が開始するまでに 1 分以上かかる場合があり、その時間はトラフィック、輻輳、およびフローエンドポイント間のホップの総数によって異なります。

Mediatrace または Traceroute の実行中に [ログ（Logs）] タブをクリックすると、次のような役立つ情報を確認できます。

- 操作の進行状況。
- ルータの応答タイムアウトや完了しなかった他の手順など、操作中に発生したエラー。
- 非 Medianet 対応ルータが検出されて処理された場所とその状況。
- Medianet が設定されていない Medianet 対応ルータ。

ステップ 7 操作が完了すると、[Troubleshooting] タブにフローの 2 つのエンドポイント間のすべてのデバイスのトポロジ マップが表示されます。マップ内のデバイス アイコンは次のような形をしています。

- [Alarm Severity]：現在デバイスに記録されている最も重大なアラーム。
- [フラグ（Flag）]：Mediatrace または Traceroute が開始されたデバイス。
- [Filmstrip]：デバイスは Medianet に対応しています。
- 赤色の背景のマイナス記号：デバイスは Medianet に対応していますが、Medianet レスポンダとして設定されていません。RTP/TCP のパフォーマンス統計情報は、そのデバイスで使用できません。この状況に対処するには、Medianet レスポンダとしてデバイスを設定する必要があります。
- マイナス記号：デバイスは管理対象外です。

ステップ 8 フローのパス内のすべての Medianet 対応デバイスについて重要なパフォーマンス メトリックを確認するには、[Medianet Path View] タブをクリックします。パフォーマンス メトリックを数値またはグラフ形式で表示するには、[Medianet Path View] ペインのサブタブをクリックします。

（注） [Medianetパスビュー（Medianet Path View）] タブは、[トラブルシューティングの状態（Troubleshooting Status）] テーブルから Mediatrace の操作を開始できる場合にのみ使用可能です。単に Traceroute 操作をトリガーできるだけの場合は、これが表示されません。

ステップ 9 別のルータで Mediatrace または Traceroute 操作を起動する場合、完了した Mediatrace または Traceroute 操作を再起動する場合、または進行中の操作を停止する場合には、[トラブルシューティングの状態（Troubleshooting Status）] テーブルの適切なリンクを使用します。

関連トピック

Mediatrace を使用した現在アクティブな RTP ストリームと TCP セッションの表示 （991 ページ）
RTP または TCP フローからの Mediatrace の起動 （993 ページ）
Mediatrace で報告された最も悪い RTP エンドポイントのトラブルシューティング （996 ページ）
Mediatrace を使用した複数のソースからのフロー データの比較 （998 ページ）

Mediatraceで報告された最も悪いRTPエンドポイントのトラブルシューティング

[ワースト N 個の RTP エンド ポイント ペア（Worst N RTP End Point Pairs.）] および [RTP メッセージ交換（RTP Conversation）] ダッシュレットを使用すると、ネットワーク内の最も効率の良くない RTP フローに対して Mediatrace をすぐに開始できます。これは、RTP フローでのみ機能します。

[RTP Conversations] ダッシュレットに、アクティブでなくなったフローを含む、送信元エンドポイントの完全な履歴が表示されます。最新のフローのみを選択できます。そのような非アクティブなフローで Mediatrace を起動すると、この事実を知らせるエラー メッセージが表示されます。

ステップ 1 [ダッシュボード（Dashboard）]>[パフォーマンス（Performance）]>[エンドユーザ エクスペリエンス（End User Experience）] の順に選択します。

ステップ 2 [ワースト N 個の RTP エンド ポイント ペア（Worst N RTP End Point Pairs）] ダッシュレットで、最も効率の良くない RTP フローの送信元アドレスをメモします（このダッシュレットがダッシュボードにない場合は「ダッシュボードへのダッシュレットの追加 （15 ページ）」を参照）。

ステップ 3 同じページの [RTP Conversations] ダッシュレットで、同じ送信元アドレスの最新のカンバセーションを検索します。

ステップ 4 [RTP Conversations] ダッシュレットでそのカンバセーションを選択し、[Troubleshoot] > [Trace Service] パスの順に選択します。Prime Infrastructure には、選択したフローの [RTP ストリームの詳細（RTP Stream Details）] ページが表示されます。[トラブルシューティングの状態（Troubleshooting Status）] テーブルに、フローのパス内のすべてのルータがフローの送信元エンドポイントからの距離の順に表示されます。Medianet 対応ルータは、フィルムストリップ（映画）アイコンで示されます。

ステップ 5 フローのパス内のルータから Mediatrace または Traceroute を実行するには、テーブルでそのルータの横にある [Mediatrace の開始（Start Mediatrace）] または [Traceroute の開始（Start Traceroute）] リンクをクリックします。

（注） デバイスが Mediatrace に対応している場合は [Mediatrace の開始（Start Mediatrace）] リンクが表示され、デバイスが Mediatrace に対応していない場合は [traceroute の開始（Start Traceroute）] リンクが表示されます。

Mediatrace が開始するまでに 1 分以上かかる場合があり、その時間はトラフィック、輻輳、およびフローエンドポイント間のホップの総数によって異なります。

Mediatrace または Traceroute の実行中に [ログ（Logs）] タブをクリックすると、次のような役立つ情報を確認できます。

- 操作の進行状況。
- ルータの応答タイムアウトや完了しなかった他の手順など、操作中に発生したエラー。
- 非 Medianet 対応ルータが検出されて処理された場所とその状況。
- Medianet が設定されていない Medianet 対応ルータ。

ステップ 6 操作が完了すると、[Troubleshooting] タブにフローの 2 つのエンドポイント間のすべてのデバイスのトポロジ マップが表示されます。マップ内のデバイス アイコンは次のような形をしています。

- [フラグ（Flag）]：Mediatrace または Traceroute が開始されたデバイス。
- [Filmstrip]：デバイスは Medianet に対応しています。
- マイナス記号：デバイスは管理対象外です。

ステップ 7 フローのパス内のすべての Medianet 対応デバイスについて重要なパフォーマンス メトリックを確認するには、[Medianet Path View] タブをクリックします。パフォーマンス メトリックを数値またはグラフ形式で表示するには、[Medianet Path View] ペインのサブタブをクリックします。

（注） [Medianetパスビュー（Medianet Path View）] タブは、[トラブルシューティングの状態（Troubleshooting Status）] テーブルから Mediatrace の操作を開始できる場合にのみ使用可能です。Traceroute 操作をトリガーできるだけの場合は、表示されません。

ステップ 8 次の操作を実行するには、[Troubleshooting Status] テーブルの適切なリンクを使用します。

- 別のルータで Mediatrace または Traceroute 操作を開始する。
- 完了した Mediatrace または Traceroute 操作を再起動する、または進行中の操作を停止する。

関連トピック

Mediatrace を使用した現在アクティブな RTP ストリームと TCP セッションの表示 （991 ページ）
RTP または TCP フローからの Mediatrace の起動 （993 ページ）
エンドポイントからの Mediatrace の起動 （994 ページ）
Mediatrace を使用した複数のソースからのフロー データの比較 （998 ページ）

Mediatrace を使用した複数のソースからのフロー データの比較

Mediatrace パフォーマンス データを解釈する際には、次の操作が役立つことがあります。

- NAM、NetFlow、およびこのパフォーマンス データを報告する他のソースの識別。
- 複数の NAM または NetFlow データ ソースがある場合は、それらのソースが特定のフローに対して重要業績評価指標をどのように報告しているかを比較します。

複数のソースからフロー データを比較するには、次の手順を実行します。

ステップ 1 [サービス（Services）] > [Application Visibility and Control] > [Mediatrace] の順に選択します。

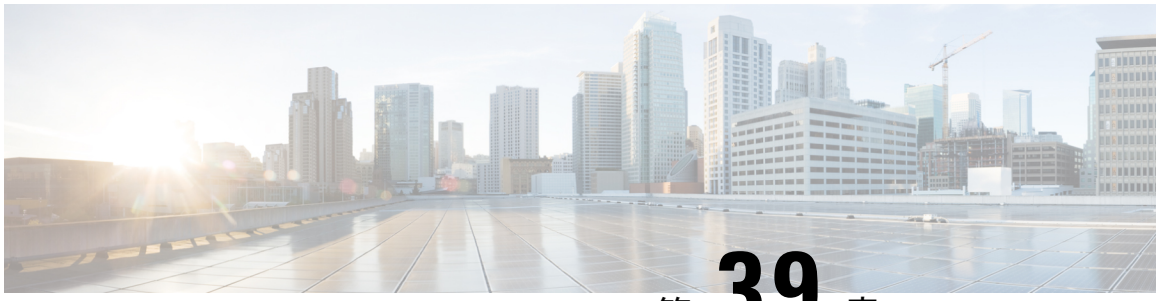
ステップ 2 [アプリケーション（Application）] ドロップダウン リストから [RTP] または [TCP] を選択し、「Mediatrace を使用した現在アクティブな RTP ストリームと TCP セッションの表示」のステップに使用するフローを見つけます。

ステップ 3 （RTP または TCP フローに関する）行を展開すると、各インジケータ セットに関して、選択したフローとデータ ソースに該当する重要業績評価指標の詳細が表示されます。

ステップ 4 操作が終了したら、[OK] をクリックします。

関連トピック

Mediatrace を使用した現在アクティブな RTP ストリームと TCP セッションの表示 （991 ページ）
RTP または TCP フローからの Mediatrace の起動 （993 ページ）
エンドポイントからの Mediatrace の起動 （994 ページ）
Mediatrace で報告された最も悪い RTP エンドポイントのトラブルシューティング （996 ページ）



第 39 章

Cisco モビリティ サービス エンジンおよびサービス

- Cisco モビリティ サービス エンジン（MSE）の概要 （999 ページ）
- Cisco Prime Infrastructure への MSE の追加 （1000 ページ）
- MSE ライセンス （1005 ページ）
- MSE の表示 （1007 ページ）
- MSE と同期される Cisco Prime Infrastructure データ （1008 ページ）
- MSE に関する通知統計情報の表示 （1017 ページ）
- MSE サーバの基本プロパティの変更 （1018 ページ）
- MSE ユーザ アカウントの設定 （1028 ページ）
- 読み取り/書き込みアクセスを制御する MSE ユーザ グループの設定 （1029 ページ）
- MSE と製品サーバのモニタ （1030 ページ）
- MSE コンテキスト認識型サービス（ロケーション サービス）によるトラッキングの向上 （1039 ページ）
- MSE モバイル コンシェルジュ アドバタイズメントの表示 （1060 ページ）
- MSE イベント グループとは （1061 ページ）
- MSE を使用したモバイル コンシェルジュの設定 （1071 ページ）
- MSE ワイヤレス セキュリティ構成ウィザードを使用した wIPS の設定 （1076 ページ）
- Connected Mobile Experience の設定 （1079 ページ）

Cisco モビリティ サービス エンジン（MSE）の概要

Cisco MSE は、Cisco Unified Wireless Network（CUWN）全体でさまざまなサービスをサポートしています。

Cisco MSE では現在、次のサービスがサポートされています。

- ロケーション サービス：コンテキスト認識型サービス（CAS）とも呼ばれます。これは、Wi-Fi クライアント追跡およびロケーション API 機能をオンにする MSE のコア サービスです。プレゼンス、ロケーション、テレメトリ データ、履歴情報などのコンテキスト情報

を取得することで、MSE は数千のモバイル アセットとクライアントを同時に追跡できます。

- ワイヤレス侵入防御サービス：CUWNインフラストラクチャ内の悪意のある攻撃、セキュリティの脆弱性、およびパフォーマンス阻害のソースに対してワイヤレス特有のネットワークへの脅威の検出と緩和を行うことができます。wIPS は、ワイヤレスの脅威を可視化、分析、および識別し、シスコのモニタ モードおよび拡張ローカル モード（ELM）のアクセス ポイントを使用して、セキュリティとパフォーマンスの問題の緩和と解決を一元管理します。予防的な脅威防御は、ほとんどのワイヤレス攻撃を寄せ付けない強固なワイヤレス ネットワークのコアを作成するためにもサポートされます。
- モバイル コンシェルジュ：モバイル コンシェルジュはCisco Mobility Services Advertisement Protocol（MSAP）をイネーブルにします。このプロトコルによって、MSE とモバイル デバイス間の直接的な通信が可能になり、コンテンツをモバイルデバイスのプリアソシエーションに直接プッシュできるようになります。この機能は、802.11uおよびMSAPをサポートするモバイル デバイスに依存します。
- CMX 分析サービス：CMX 分析サービスは、特定のネットワーク内のワイヤレス デバイスのロケーション情報を分析します。CMX 分析サービスは、MSE が提供するデータを使用して、ワイヤレス ローカルエリア ネットワーク（WLAN）内のWi-Fiデバイスのロケーションを計算します。また、FastLocate 機能では、データ パケットの RSSI の強度に関する情報が Cisco WLC に送信され、ロケーションの計算に使用できます。

ネットワーク内でワイヤレス デバイスが有効化されている場合、そのワイヤレス デバイスはプローブ要求パケットを送信して、その近隣のワイヤレス ネットワークを識別します。WLAN のアクセス ポイントに接続した後でも、クライアント デバイスはより良い QoS のために、その他のアクセス ポイントを特定するためのプローブ要求パケットの送信を続けます。アクセス ポイントは、各種のワイヤレス デバイスからこれらの要求と関連する RSSI を収集し、それらをワイヤレス LAN コントローラ（WLC）に送信します。コントローラは、この情報を MSE に送信します。

さまざまな AP から収集された基本データを分析することにより、建物内で Wi-Fi デバイスを使用するユーザの移動と行動のパターンについて情報や知識を得ることができます。建物には、たとえば空港、ショッピング モール、都市中心部などがあります。CMX Analytics サービスは、空港局や建物の所有者が自分の建物内の通行人または顧客の動向を認識できます。これは、これらの所有者が建物内の標示を改善したり、使用率の低い場所に変更を加えたりするのに役立ちます。

関連トピック

Cisco Prime Infrastructure への MSE の追加 （1000 ページ）
MSE と同期される Cisco Prime Infrastructure データ （1008 ページ）
MSE を使用したモバイル コンシェルジュの設定 （1071 ページ）

Cisco Prime Infrastructure への MSE の追加

[モビリティサービス（Mobility Service）] ページの [モビリティサービスエンジンの追加（Add Mobility Services Engine）] ダイアログボックスを使用して MSE を追加できます。このダイアログボックスでは、ライセンス ファイルと追跡パラメータを追加し、マップを MSE に割り当

てることができます。設定のために既存の MSE でウィザードを起動する場合、[Add MSE] オプションの代わりに [Edit MSE Details] として表示されます。

MSE を Prime Infrastructure に追加するには、Prime Infrastructure にログインして次の手順に従います。

始める前に

- Cisco Adaptive wIPS の特性と機能の詳細については、https://www.cisco.com/ にアクセスして、マルチメディア プレゼンテーションをご覧ください。Prime Infrastructure に関するさまざまなトピックについての学習モジュールがあります。今後のリリースに合わせて、学習を強化する概要プレゼンテーションおよび技術プレゼンテーションが追加されていく予定です。
- Prime Infrastructure は、MSE 3355 を適切に認識してサポートします。MSE のインストレーション ガイドには、https://www.cisco.com/c/en/us/td/docs/wireless/mse/3355/user/guide/mse3355_qsg/mse_qsgmain.html からアクセスできます。
- [サービス（Services）] > [モビリティサービス（Mobility Services）] > [モビリティサービスエンジン（Mobility Services Engines）] ページは、root 仮想ドメインでのみ使用可能です。

ステップ 1 追加する Mobility Service Engine に対して Prime Infrastructure から ping を実行できることを確認します。

ステップ 2 **[サービス（Services）] > [モビリティサービス（Mobility Services）] > [モビリティサービスエンジン（Mobility Services Engines）]** の順に選択し、[モビリティサービス（Mobility Services）] ページを表示します。

ステップ 3 [Select a command] ドロップダウン リストから、[Add Mobility Services Engine] を選択し、[Go] をクリックします。

[Add Mobility Services Engine] ページが表示されます。

ステップ 4 次の情報を入力します。

- [Device Name]：MSE のユーザ割り当て名。
- [IP Address]：Mobility Services Engine の IP アドレス。

有効な IP アドレスが入力された場合にだけ、MSE が追加されます。デバイス名は、複数のモビリティサービス エンジンを含む複数の Prime Infrastructure がある場合にデバイスを区別するのに役立ちますが、MSE を検証する際には考慮されません。

- [Contact Name]（任意）：Mobility Services Engine 管理者。
- [Username]：デフォルトのユーザ名は admin です。これは、MSE に対して設定されているPrime Infrastructure 通信ユーザ名です。
- [パスワード（Password）]：デフォルトのパスワードは admin です。これは、MSE 用に設定される Prime Infrastructure 通信パスワードです。

自動インストール スクリプトの実行中にユーザ名とパスワードを変更した場合は、変更後の値をここに入力してください。デフォルト パスワードを変更しなかった場合は、自動インストール スクリプトを再実行してユーザ名とパスワードを変更することを推奨します。

- MSE からすべてのサービス割り当てを永久に削除するには、[Delete synchronized service assignments] チェックボックスをオンにします。

このオプションは、ネットワーク設計、有線スイッチ、コントローラ、およびイベント定義に適用されます。既存のロケーション履歴データは維持されますが、今後ロケーション計算を実行するときには手動サービス割り当てを使用する必要があります。

ステップ 5 [次へ（Next）] をクリックします。Prime Infrastructure により、選択されている要素と MSE が自動的に同期されます。

同期完了後、[MSE License Summary] ページが表示されます。[MSE License Summary] ページから、ライセンスのインストール、ライセンスの追加、ライセンスの削除、アクティベーション ライセンスのインストール、サービス ライセンスのインストールを実行します。

MSE のサービスの設定

ステップ 6 MSE 上のサービスを有効にするには、サービスの横にあるチェックボックスをオンにします。サービスのタイプは次のとおりです。

- [Context Aware Service]：[Context Aware Service] チェックボックスをオンにすると、ロケーション計算を実行するためにロケーション エンジンを選択する必要があります。CAS を選択すると、クライアント、不正、干渉、およびタグを追跡できます。[Cisco Context-Aware Engine for Clients and Tag] を選択してタグを追跡することができます。
- [WIPS]：[Wireless Intrusion Prevention System] チェックボックス。無線およびパフォーマンスの脅威が検出されます。
- [Mobile Concierge Service]：[Mobile Concierge Service] チェックボックス。モバイル デバイスで使用可能なサービスが記述されるサービス アドバタイズメントが提供されます。
- [CMX Analytics Service]：[CMX Analytics Service] チェックボックス。MSE からの Wi-Fi デバイス位置データを分析するためにパッケージされた各種データ分析ツールを利用できます。
- [CMX Connect & Engage]：CMX Connect and Engage サービスでは、ゲスト Wi-Fi オンボーディング ソリューションと、CMX ソフトウェア開発キット（SDK）のゾーンおよびメッセージの設定が提供されます。
- [HTTP Proxy Service]：MSE 上の HTTP プロキシ サービスはポリシーベース ルーティング（PBR）を使用して代行受信されたすべての HTTP トラフィックを終端し、ワイヤレス クライアントの代わりにコンテンツを引き出すことでフォワード プロキシとして機能します。

リリース 7.5 以降、wIPS サービスは同じ MSE 上の CAS および wIPS をサポートしないため、wIPS サービスには専用の MSE が必要になります。

MSE 追跡パラメータおよび履歴パラメータの設定

ステップ 7 MSE でサービスを有効にすると、[Select Tracking & History Parameters] ページが表示されます。

追跡パラメータの設定を省略すると、デフォルト値が選択されます。

ステップ 8 追跡するクライアントを選択するには、対応する [Tracking] チェックボックスをオンにします。追跡パラメータを以下に示します。

- Wired Clients
- Wireless Clients
- Rogue Access Points
  - Exclude Adhoc Rogue APs
- Rogue Clients
- Interferers
- Active RFID Tags

ステップ 9 デバイスの履歴トラッキングを有効にするには、対応するデバイスのチェックボックスをオンにします。履歴パラメータを以下に示します。

- Wired Stations
- Client Stations
- Rogue Access Points
- Rogue Clients
- Interferers
- Asset Tags

ステップ 10 [Next] をクリックして MSE にマップを割り当てます。

MSE へのマップの割り当て

[Assigning Maps] ページは、MSE で有効にするサービスの 1 つとして CAS を選択する場合にだけ使用可能です。

ステップ 11 MSE 追跡パラメータおよび履歴パラメータを設定すると、[Assigning Maps] ページが表示されます。

[Assign Maps] ページには以下の情報が表示されます。

- Name
- Type（ビルディング、フロア、キャンパス）
- Status

ステップ 12 必要なマップ タイプを確認するには、ページで使用可能な [Filter] オプションから [All]、[Campus]、[Building]、[Floor Area]、または [Outdoor Area] を選択します。

ステップ 13 マップを同期するには、[名前（Name）] チェックボックスをオンにし、[同期（Synchronize）] をクリックします。

ネットワーク設計の同期が完了すると、特定のネットワーク設計で AP が割り当てられている適切なコントローラが MSE と自動的に同期されます。

ステップ 14 [次へ（Next）] をクリックして、モバイル アプリケーションの有効化を設定します。

モバイル アプリケーションの有効化

この統合を有効にすると、MSE はフロア マップおよびワイヤレス クライアントの位置通知を Meridian に送信できます。Meridian は、この情報を使用して、ロケーション ベースのサービスをユーザに提供します。このとき、ユーザは、ネットワークに接続し、MSEに直接アクセスする必要はありません。Meridian を有効にした後、アカウントをアクティブにする方法、および組織内の他のユーザとアクセスを共有する方法についての指示を含む電子メールを受信します。Meridianモバイルアプリケーションまたは Android および iOS 向けのモバイル SDK を使用した独自のアプリケーションのいずれかを介してビジターにロケーション サービスを提供するために Meridians プラットフォームを使用できます。MSE から Meridian への各ワイヤレス クライアント位置通知またはゾーン通知のデータ帯域幅は最大 1 MB/秒です。

MSE にマップを割り当てると、[モバイル アプリケーションの有効化（Mobile App Enablement）] ページが表示されます。

ステップ 15 [モバイルアプリケーション統合を有効にする（Enable Mobile App Integration）] チェックボックスを選択してモバイル アプリケーション統合を有効にします。アイコンをクリックすると [モバイル アプリケーション有効化のヘルプ（Mobile App Enablement Help）] ページが開きます。

ステップ 16 [ロケーション名（Location Name）] テキスト ボックスにロケーションの名前を入力します。ここに入力する名前が Meridian アプリケーションで表示されるため、各自のデバイスでロケーション サービスをテストできます。

ステップ 17 Meridian オンライン エディタおよびSDK にアクセスするには、[電子メールアドレス（E-mail Address）] テキスト ボックスに電子メール アドレスを入力します。Meridian は、これらのアドレスに、アカウントへのアクセス方法、および組織内の他のユーザとのアカウント共有方法についての指示を含む電子メールを送信します。

ステップ 18 MSE が UDI を登録して MSE に同期されるマップを送信できるサーバを、[登録エンドポイント（Registration Endpoint）] テキスト ボックスに入力します。

ステップ 19 [通知エンドポイント（Notifications Endpoint）] テキスト ボックスで、指定したデータ形式で MSE がロケーション更新通知を送信できるサーバの詳細を入力します。

ステップ 20 [通知データ形式（Notifications Data Format）] オプション ボタンを選択します。これは、MSE から送信される通知のデータ形式です。データ形式には、レガシー SOAP/XML、XML、JSON およびプロトコル バッファがあります。

ステップ 21 [番地（Street Address）] テキスト ボックスに、ロケーションの住所を入力します。

ステップ 22 [電話番号（Phone Number）] テキスト ボックスに、Meridian からの連絡用の電話番号を入力します。

ステップ 23 [詳細設定（Advanced）] をクリックすると [詳細設定（Advanced）] ペインが開きます。

ステップ 24 選択したゾーンにワイヤレス クライアントが入った場合に MSE でリアルタイム通知を Meridian に送信するには、[ゾーンに関するゾーン通知を有効にする（Enable Zone Notifications for zones）] チェックボックスをオンにし、ドロップダウン リストからフロアおよびゾーンを選択します。

[ゾーンに関するゾーン通知を有効にする（Enable zone notifications for zones）] ドロップダウン リストには、Prime Infrastructure に追加され、MSE と同期されるすべてのフロアとゾーンが表示されます。

ステップ 25 ゾーンとフロアを選択した後、[OK] をクリックします。

ステップ 26 [Save] をクリックします。

ステップ 27 [Done] をクリックして MSE 設定を保存します。

（注） CMX は次に示す MSE の機能をサポートしていません。

- CMX ハイ アベイラビリティの管理
- Synchronization History
- コンテキスト認識型通知
- モバイル コンシェルジュ
- wIPS およびワイヤレスのセキュリティ
- 位置精度

関連トピック

MSE の表示 （1007 ページ）
MSE ライセンス ファイルの削除 （1006 ページ）
Prime Infrastructure からの MSE の削除 （1007 ページ）

MSE ライセンス

Cisco MSE は、さまざまなロケーション ベースのサービスを提供します。これらのサービスをイネーブルにするには、以下のものが必要です。

- Cisco MSE のハードウェアまたはソフトウェア アプライアンス
  - 物理アプライアンス：アクティベーション ライセンスは不要です。
  - 仮想アプライアンス：仮想アプライアンスのインスタンスでは、MSE Virtual Appliance Activation ライセンス（L-MSE-7.0-K9）が必要です。MSE 仮想アプライアンス上にサービス/機能ライセンスがあるだけでは不十分です。
- ライセンス
- サポート
- 詳細については、『Cisco Prime Infrastructure Administrator Guide』の「*Licenses and Software Updates*」の章を参照してください。

ライセンスの発注およびダウンロードの詳細については、次の URL で『*Cisco Mobility Services Engine Licensing and Ordering Guide*』を参照してください。http://www.cisco.com/en/US/prod/collateral/wireless/ps9733/ps9742/data_sheet_c07-473865.html

MSE ライセンス ファイルの削除

MSE ライセンス ファイルを削除するには、次の手順に従います。

手順の概要

1. **[サービス（Services）] > [モビリティ サービス（Mobility Services）] > [モビリティ サービス エンジン（Mobility Service Engine）]** を選択します。
2. 削除する Mobility Services Engine ライセンスを選択するため、対応する [Device Name] チェックボックスをオンにします。
3. [コマンドの選択（Select a command）] ドロップダウン リストから [構成の編集（Edit Configuration）] を選択します。
4. [Edit Mobility Services Engine] ダイアログボックスの [Next] をクリックします。
5. [MSE License Summary] ページで削除する MSE ライセンス ファイルを選択します。
6. [Remove License] をクリックします。
7. [OK] をクリックして削除操作を確定するか、または [Cancel] をクリックしてライセンスを削除せずにこのページを閉じます。
8. [Next] をクリックして MSE でサービスを有効にします。

手順の詳細

ステップ 1 **[サービス（Services）] > [モビリティ サービス（Mobility Services）] > [モビリティ サービス エンジン（Mobility Service Engine）]** を選択します。

[Mobility Services] ページが表示されます。

ステップ 2 削除する Mobility Services Engine ライセンスを選択するため、対応する [Device Name] チェックボックスをオンにします。

ステップ 3 [コマンドの選択（Select a command）] ドロップダウン リストから [構成の編集（Edit Configuration）] を選択します。

ステップ 4 [Edit Mobility Services Engine] ダイアログボックスの [Next] をクリックします。

[MSE License Summary] ページが表示されます。

ステップ 5 [MSE License Summary] ページで削除する MSE ライセンス ファイルを選択します。

ステップ 6 [Remove License] をクリックします。

ステップ 7 [OK] をクリックして削除操作を確定するか、または [Cancel] をクリックしてライセンスを削除せずにこのページを閉じます。

ステップ 8 [Next] をクリックして MSE でサービスを有効にします。

関連トピック

MSE の表示 （1007 ページ）
Cisco Prime Infrastructure への MSE の追加 （1000 ページ）
Prime Infrastructure からの MSE の削除 （1007 ページ）

MSE と同期される Cisco Prime Infrastructure データ （1008 ページ）

MSE の表示

現在のモビリティ サービスのリストを表示するには、**[サービス（Services）] > [モビリティ サービス（Mobility Services）] > [モビリティサービスエンジン（Mobility Services Engines）]** の順に選択します。

[モビリティサービスエンジン（Mobility Services Engines）] ページには、各デバイスのデバイス情報と機能、および [コマンドの選択（Select a command）] ドロップダウン リストが表示されます。

Cisco Prime Infrastructure のロケーション機能および MSE 機能では、パーティショニングがサポートされていません。

関連トピック

Cisco Prime Infrastructure への MSE の追加 （1000 ページ）
MSE ライセンス ファイルの削除 （1006 ページ）
Prime Infrastructure からの MSE の削除 （1007 ページ）
MSE と同期される Cisco Prime Infrastructure データ （1008 ページ）

Prime Infrastructure からの MSE の削除

Prime Infrastructure データベースから MSE を削除するには、次の手順に従います。

ステップ 1 **[サービス（Services）] > [モビリティ サービス（Mobility Services）] > [モビリティ サービス エンジン（Mobility Services Engines）]** を選択します。

[Mobility Services] ページが表示されます。

ステップ 2 対応する [Device Name] チェックボックスをオンにして、削除する MSE を選択します。

ステップ 3 [Select a command] ドロップダウン リストから [Delete Service(s)] を選択します。

ステップ 4 [Go] をクリックします。

ステップ 5 選択した MSE を Prime Infrastructure データベースから削除することを確定するには、[OK] をクリックします。

ステップ 6 削除を中止するには、[Cancel] をクリックします。

関連トピック

MSE の表示 （1007 ページ）
Cisco Prime Infrastructure への MSE の追加 （1000 ページ）

MSE と同期される Cisco Prime Infrastructure データ

ここでは、Cisco Prime Infrastructure と MSE を手動でスマートに同期させる方法について説明します。

Cisco Prime Infrastructure に MSE を追加した後、ネットワーク設計（キャンパス、ビルディング、フロア、および屋外マップ）、コントローラ（名前と IP アドレス）、特定の Catalyst 3000 シリーズおよび 4000 シリーズ スイッチ、およびイベント グループを MSE と同期できます。

- ネットワーク設計：施設全体でのアクセス ポイントの物理的配置の論理マッピング。1 つのネットワーク設計は、1 つのキャンパス、そのキャンパスを構成するビルディング、および各ビルディングを構成するフロアという階層構造で構成されます。
- コントローラ：MSE に関連付けられている選択されたコントローラ。MSE と定期的にロケーション情報を交換します。定期的な同期により、正確なロケーション情報を維持できます。
- イベント グループ：イベントを生成するトリガーを定義する事前定義イベントのグループ。定期的な同期により、最新の定義イベントが追跡されます。
- 有線スイッチ：ネットワーク上の有線クライアントへのインターフェイスを提供する有線 Catalyst スイッチ。定期的な同期によって、ネットワーク上の有線クライアントのロケーションが正確に追跡されます。
  - MSE は、Catalyst スタッカブル スイッチ（3750、3750-E、3560、2960、IE-3000 スイッチ）、スイッチ ブレード（3110、3120、3130、3040、3030、3020）、およびスイッチ ポートと同期できます。
  - また、MSE は Catalyst 4000 シリーズ スイッチ WS-C4948、WS-C4948-10GE、ME-4924-10GE、WS-4928-10GE、WS-C4900M、WS-X4515、WS-X4516、WS-X4013+、WS-X4013+TS、WS-X4516-10GE、WS-X4013+10GE、WS-X45-SUP6-E、および WS-X45-SUP6-LE とも同期できます。
- サードパーティ要素：要素を MSE と同期する場合、サードパーティ アプリケーションにより MSE にイベント グループが作成されていることがあります。未使用の要素を削除するか、または未使用の要素をサードパーティ要素としてマークすることができます。
- サービス アドバタイズメント：モバイル コンシェルジュ サービスは、モバイル デバイスにサービス アドバタイズメントを提供します。これにより、MSE と同期されたサービス アドバタイズメントが示されます。

同期を実行する前に、コントローラ、Cisco Prime Infrastructure、および MSE 間のソフトウェア互換性を確認してください。

MSE、Cisco Prime Infrastructure、およびコントローラ間の通信は、協定世界時（UTC）で実行されます。各システムで NTP を設定すると、デバイスに UTC 時刻が提供されます。MSE とその関連コントローラは、同じ NTP サーバおよび同じ Cisco Prime Infrastructure サーバにマップされる必要があります。NTP サーバは、コントローラ、Cisco Prime Infrastructure、および MSE の間で自動的に時刻を同期する必要があります。

関連トピック

MSE の表示 （1007 ページ）

製品データと MSE の同期 （1009 ページ）
ワイヤレス コントローラの MSE 割り当ての変更 （1010 ページ）
サードパーティ NE と MSE の同期 （1012 ページ）
MSE データベースと製品データベース間の同期のセットアップ （1014 ページ）
MSE データベースと製品データベースの同期の履歴表示 （1017 ページ）

製品データと MSE の同期

Prime Infrastructure ネットワーク設計、コントローラ、有線スイッチ、またはイベント グループを MSE と同期させるには、次の手順に従います。

手順の概要

1. **[サービス（Services）] > [モビリティサービス（Mobility Services）] > [サービスの同期（Synchronize Services）]** の順に選択します。
2. 左側のサイドバーのメニューから、適切なメニュー オプション（[ネットワーク設計（Network Designs）]、[コントローラ（Controllers）]、[イベント グループ（Event Groups）]、[有線スイッチ（Wired Switches）]、[サードパーティ要素（Third Party Elements）]、または [サービス アドバタイズメント（Service Advertisements）]）を選択します。
3. MSE にネットワーク設計を割り当てるには、左側のサイドバーのメニューから [ネットワーク設計（Network Designs）] を選択します。
4. 対応する [Name] チェックボックスをオンにして、MSE と同期させるすべてのマップを選択します。
5. [Change MSE Assignment] をクリックします。
6. マップと同期する MSE を選択します。
7. [MSE Assignment] ダイアログボックスで次のいずれかをクリックします。
8. [同期（Synchronize）] をクリックし、MSE データベースを更新します。

手順の詳細

ステップ 1 **[サービス（Services）] > [モビリティサービス（Mobility Services）] > [サービスの同期（Synchronize Services）]** の順に選択します。

ステップ 2 左側のサイドバーのメニューから、適切なメニュー オプション（[ネットワーク設計（Network Designs）]、[コントローラ（Controllers）]、[イベント グループ（Event Groups）]、[有線スイッチ（Wired Switches）]、[サードパーティ要素（Third Party Elements）]、または [サービス アドバタイズメント（Service Advertisements）]）を選択します。

ステップ 3 MSE にネットワーク設計を割り当てるには、左側のサイドバーのメニューから [ネットワーク設計（Network Designs）] を選択します。

ステップ 4 対応する [Name] チェックボックスをオンにして、MSE と同期させるすべてのマップを選択します。

6.0 では、MSE に割り当てることができる最も詳細なレベルはキャンパス レベルです。7.0 以降では、このオプションはフロア レベルまで拡大されました。たとえば、floor1 を MSE 1 に、floor2 を MSE 2 に、floor3 を MSE 3 に割り当てることを選択できます。

ステップ 5 [Change MSE Assignment] をクリックします。

ステップ 6 マップと同期する MSE を選択します。

ネットワーク設計には、キャンパス内のフロアや、複数のビルディングが含まれている大規模キャンパス（各ビルディングが異なる MSE によりモニタされる）などがあります。このため、単一ネットワーク設計を複数の MSE に割り当てる必要があります。

ステップ 7 [MSE Assignment] ダイアログボックスで次のいずれかをクリックします。

- **[保存（Save）]**—MSE 割り当てを保存します。次のメッセージが [Network Designs] ページの [Messages] 列に黄色の矢印アイコンとともに表示されます。

  「割り当て予定 — 同期してください（To be assigned - Please synchronize）」

- [キャンセル（Cancel）]：MSE 割り当ての変更内容を取り消し、[ネットワーク設計（Network Designs）] ページに戻ります。
- また、[リセット（Reset）] をクリックして **MSE** の割り当てを元に戻すこともできます。

ネットワーク設計には、キャンパス内のフロアや、複数のビルディングが含まれている大規模キャンパス（各ビルディングが異なる MSE によりモニタされる）などがあります。このため、単一ネットワーク設計を複数の MSE に割り当てる必要があります。

ネットワーク設計割り当てでは、同期対象のコントローラが自動的に選択されます。

ステップ 8 [同期（Synchronize）] をクリックし、MSE データベースを更新します。

項目が同期されると、同期済みエントリの [Sync.

有線スイッチまたはイベント グループを MSE に割り当てるときにも同じ手順を使用できます。

関連トピック

MSE と同期される Cisco Prime Infrastructure データ （1008 ページ）
MSE データベースと製品データベースの同期の履歴表示 （1017 ページ）
ワイヤレス コントローラの MSE 割り当ての変更 （1010 ページ）
MSE データベースと製品データベース間の同期のセットアップ （1014 ページ）
MSE 製品の Out-of-Sync アラームの検索とトラブルシューティング （1031 ページ）

ワイヤレス コントローラの MSE 割り当ての変更

サービス単位（CAS または wIPS）で MSE を任意のワイヤレス コントローラに割り当てることができます。

MSE サービスをワイヤレス コントローラに割り当てるには、次の手順に従います。

ステップ 1 同期ページで [Controllers] を選択します。

ステップ 2 MSE に割り当てるコントローラを選択します。

ステップ 3 **Change MSE Assignment** をクリックします。

ステップ 4 コントローラと同期する必要がある MSE を選択します。

ステップ 5 ダイアログボックスで次のいずれかをクリックします。

- [保存（Save）]：**MSE の割り当て**を保存します。[コントローラ（Controllers）] ページの [メッセージ（Messages）] 列に次のメッセージが表示されます。

「割り当て予定 — 同期してください（To be assigned - Please synchronize）」

- [キャンセル（Cancel）]：MSE 割り当ての変更内容を取り消し、[コントローラ（Controllers）] ページに戻ります。
- また、[リセット（Reset）] をクリックして黄色ボタンの割り当てを元に戻すこともできます。

ステップ 6 [Synchronize] をクリックし、同期プロセスを実行します。

ステップ 7 MSE が、選択されているサービスの各コントローラ間だけで通信していることを確認します。これは、ステータス ページの [NMSP status] リンクをクリックして確認できます。詳細については、NMSP 接続ステータスのトラブルシューティング （1011 ページ）を参照してください。

コントローラの同期後、関連付けられているコントローラでタイムゾーンが設定されていることを確認します。MSE と同期するコントローラの名前は一意でなければなりません。同じ名前のコントローラが 2 つある場合は 1 つのコントローラだけが同期されます。

ステップ 8 ネットワークネットワーク設計、コントローラ、有線スイッチ、またはイベント グループの割り当てを MSE から解除する場合は、次の手順を実行します。

a) 該当するタブで 1 つ以上の要素をクリックし、[MSE 割り当ての変更（Change MSE Assignment）] をクリックします。[MSE の選択（Choose MSE）] ダイアログボックスが表示されます。

b) その MSE に要素を関連付けないようにするには、[モビリティ サービス エンジン（Mobility Services Engines）] チェックボックスをオフにします。

c) [保存（Save）] をクリックし、割り当ての変更内容を保存します。

d) **[同期（Synchronize）]** をクリックします。[同期ステータス（Sync Status）] 列に 2 つの矢印のアイコンが表示されます。

関連トピック

NMSP 接続ステータスのトラブルシューティング （1011 ページ）
MSE の表示 （1007 ページ）
MSE と同期される Cisco Prime Infrastructure データ （1008 ページ）
MSE データベースと製品データベースの同期の履歴表示 （1017 ページ）
MSE データベースと製品データベース間の同期のセットアップ （1014 ページ）

NMSP 接続ステータスのトラブルシューティング

最新のコントローラにアップグレードし、**[サービス（Services）]** > **[モビリティ サービス（Mobility Services）]** > **[サービスの同期（Synchronize Services）]** > **[コントローラ（Controllers）]** ページで NMSP ステータスが非アクティブの場合には、Prime Infrastructure がアップグレードしたコントローラ情報を受信できるようにインベントリ収集をトリガーする必要があります。

ステップ 1 **[管理（Administration）] > [ダッシュボード（Dashboards）] > [ジョブ ダッシュボード（Job Dashboard）]** の順に選択します。

ステップ 2 **[システム ジョブ（System Jobs）] > [インベントリ（Inventory）]** を選択し、[ワイヤレス コントローラ インベントリ（Wireless Controller Inventory）] を選択します。

ステップ 3 [実行（Run）] をクリックします。

ジョブが完了したら、NMSP ステータスが更新されます。

関連トピック

ワイヤレス コントローラの MSE 割り当ての変更 （1010 ページ）

サード パーティ NE と MSE の同期

要素を MSE と同期する場合、MSE にサードパーティ アプリケーションによって作成されたイベント グループがあることがあります。未使用の要素を削除するか、または未使用の要素をサードパーティ要素としてマークすることができます。

要素を削除またはサード パーティ要素としてマークするには、次の手順に従います。

手順の概要

1. **[サービス（Services）] > [モビリティ サービス（Mobility Services）] > [サービスの同期（Synchronize Services）]** の順に選択します。
2. 1 つ以上の要素を選択します。
3. 次のいずれかのボタンをクリックします。

手順の詳細

ステップ 1 **[サービス（Services）] > [モビリティ サービス（Mobility Services）] > [サービスの同期（Synchronize Services）]** の順に選択します。

[ネットワーク設計（Network Design）] ページが表示されます。

[ネットワーク設計（Network Design）] ページで、左側のサイドバーのメニューから [サードパーティ要素（Third Party Elements）] を選択します。

[Third Party Elements] ページが表示されます。

ステップ 2 1 つ以上の要素を選択します。

ステップ 3 次のいずれかのボタンをクリックします。

- [Delete Event Groups]：選択されているイベント グループを削除します。

- [Mark as 3rd Party Event Group(s)]：選択されているイベント グループをサードパーティ イベント グループとしてマークします。

関連トピック

MSE の表示 （1007 ページ）
MSE と同期される Cisco Prime Infrastructure データ （1008 ページ）
MSE データベースと製品データベースの同期の履歴表示 （1017 ページ）
MSE データベースと製品データベース間の同期のセットアップ （1014 ページ）
ワイヤレス コントローラの MSE 割り当ての変更 （1010 ページ）
MSE 製品の Out-of-Sync アラームの検索とトラブルシューティング （1031 ページ）

MSEとの適切な同期を実現するためのコントローラのタイムゾーンの設定

リリース4.2以上のコントローラでは、MSE（リリース5.1以上）がネットワークにインストールされている場合、2つのシステム間で同期が適切に実行されるようにするため、コントローラでタイムゾーンを設定する必要があります。

コントローラのタイムゾーン システム時刻を設定する際の基準として、グリニッジ標準時（GMT）が使用されます。

コントローラの初期システムセットアップ時にタイムゾーンを自動的に設定するか、またはすでにネットワークに導入されているコントローラで手動でタイムゾーンを設定することができます。

ネットワークの既存のコントローラ上でCLIを使用して時刻とタイムゾーンを手動で設定するには、次の手順に従います。

ステップ 1 コントローラ上で現在の現地時間を GMT で設定するため、次のコマンドを入力します。

例：

```
(Cisco Controller) >config time manual 09/07/07 16:00:00
(Cisco Controller) >config end
```

時刻を設定するときは、現在の現地時間を GMT で表した時間を 00:00 ～ 24:00 の範囲内の値として入力します。たとえば、米国の太平洋標準時（PST）で 8 AM の場合、PST タイムゾーンは GMT よりも 8 時間遅れているため、16:00（4 PM PST）と入力します。

ステップ 2 次のコマンドを入力し、現在の現地時間が GMT で表した時間として設定されていることを確認します。

例：

```
(Cisco Controller) >show time
Time..................................... Fri Sep 7 16:00:02 2007
Timezone delta........................... 0:0
```

ステップ 3 次のコマンドを入力し、システムの現地時間のタイムゾーンを設定します。

タイムゾーンを設定するときは、GMT を基準とした現地時間の時間帯との時差を +/- を付けて入力します。たとえば米国（US）の太平洋標準時（PST）は、GMT（UTC）時間よりも 8 時間遅れています。したがって、-8 と入力します。

例：

```
(Cisco Controller) >config time timezone -8
(Cisco Controller) >config end
```

ステップ 4 次のコマンドを入力すると、コントローラで GMT ではなく現地のタイムゾーンに基づいて現在の現地時刻が表示されることを確認できます。

例：

```
(Cisco Controller) >show time
Time..................................... Fri Sep 7 08:00:26 2007
Timezone delta........................... -8:0
```

show time コマンドの time zone delta パラメータは、現地のタイムゾーンと GMT の時差（8 時間）を示します。設定前にはこのパラメータが 0.0 に設定されています。

関連トピック

MSE の表示 （1007 ページ）
MSE と同期される Cisco Prime Infrastructure データ （1008 ページ）
MSE データベースと製品データベースの同期の履歴表示 （1017 ページ）
MSE データベースと製品データベース間の同期のセットアップ （1014 ページ）
ワイヤレス コントローラの MSE 割り当ての変更 （1010 ページ）
MSE 製品の Out-of-Sync アラームの検索とトラブルシューティング （1031 ページ）
サード パーティ NE と MSE の同期 （1012 ページ）

MSE データベースと製品データベース間の同期のセットアップ

Prime Infrastructure と MSE データベースの手動同期では、ただちに同期が実行されます。ただし、将来のデプロイメントの変更（マップやアクセス ポイントの位置の変更など）が原因で、再同期を再び実行するまでの間、ロケーションの計算やアセットの追跡が正しく行われないことがあります。

同期していない状態が発生しないようにするため、Prime Infrastructure を使用して同期を実行します。この手法により、Prime Infrastructure と MSE データベースの間の同期が定期的に実行され、関連アラームがすべてクリアされます。

1 つ以上の同期コンポーネントに対する変更は、MSE と自動的に同期されます。たとえば、アクセス ポイントが設置されているフロアを特定の MSE と同期し、その後 1 つのアクセス ポイントが同じフロアの新しいロケーション、または別のフロア（MSE と同期されるフロア）に移動すると、アクセス ポイントの変更後のロケーションが自動的に伝達されます。

Prime Infrastructure と MSE が同期されるようにするため、バックグラウンドでスマート同期が実行されます。

スマート同期を設定するには、次の手順に従います。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [バックグラウンド タスク（Background Tasks）]** を選択します。

[Background Tasks summary] ページが表示されます。

ステップ 2 [Mobility Service Synchronization] チェックボックスをオンにします。

ステップ 3 [Mobility Services Synchronization] ページが表示されます。

ステップ 4 MSE が同期外れアラートを送信するように設定するには、[Out of Sync Alerts] グループ ボックスの [Enabled] チェックボックスをオンにします。

ステップ 5 スマート同期を有効にするには、[Smart Synchronization] の [Enabled] チェックボックスをオンにします。

スマート同期は、MSE に割り当てられていない要素（ネットワーク設計、コントローラ、またはイベント グループ）には適用されません。ただし、これらの未割り当て要素に関する out-of-sync アラームは生成されます。スマート同期をこれらの要素に適用するには、これらの要素を MSE に手動で割り当てる必要があります。

Prime Infrastructure に MSE が追加されると、Prime Infrastructure 内のデータは常に、MSE との間で同期されるプライマリ コピーとして扱われます。MSE に含まれていても Prime Infrastructure には含まれていない同期対象のネットワーク設計、コントローラ、イベント グループ、および有線スイッチはすべて、MSE から自動的に削除されます。

ステップ 6 スマート同期の実行間隔を分数単位で入力します。

デフォルトでは、スマート同期は無効化されています。

ステップ 7 [送信（Submit）] をクリックします。

関連トピック

MSE との適切な同期を実現するためのコントローラのタイム ゾーンの設定（1013 ページ）

例：MSEとの製品データの同期時におけるスマートコントローラの選択方法

シナリオ 1

[Synchronization] ページの [Network Designs] セクションで、コントローラからのアクセス ポイントが 1 つ以上存在するフロアを MSE と同期することを選択した場合、アクセス ポイントに接続しているコントローラが、CAS サービスの MSE への割り当て対象として自動的に選択されます。

シナリオ 2

コントローラからの 1 つ以上のアクセス ポイントが、MSE と同期されるフロアに配置されている場合、アクセス ポイントに接続するコントローラは、CAS サービスの同じ MSE に自動的に割り当てられます。

シナリオ 3

アクセス ポイントがフロアに追加され、MSE に割り当てられます。このアクセス ポイントをコントローラ A からコントローラ B に移動すると、コントローラ B が MSE と自動的に同期されます。

シナリオ 4

MSE と同期するフロアに配置されているすべてのアクセス ポイントが削除されると、そのコントローラは自動的に MSE 割り当てから削除されるか、または同期されなくなります。

関連トピック

MSE と同期される Cisco Prime Infrastructure データ （1008 ページ）
MSE データベースと製品データベースの同期の履歴表示 （1017 ページ）
ワイヤレス コントローラの MSE 割り当ての変更 （1010 ページ）
MSE 製品の Out-of-Sync アラームの検索とトラブルシューティング （1031 ページ）
サード パーティ NE と MSE の同期 （1012 ページ）

MSE データベースと製品データベースの同期ステータスの表示

Prime Infrastructure で Synchronize Servers コマンドを使用して、ネットワーク設計、コントローラ、およびイベント グループと MSE との同期のステータスを表示できます。

同期ステータスを表示するには、次の手順に従います。

ステップ 1 **[サービス（Services）] > [モビリティ サービス（Mobility Services）] > [サービスの同期（Synchronize Services）]** を選択します。

ステップ 2 左側のサイドバーのメニューから、[ネットワーク設計（Network Designs）]、[コントローラ（Controllers）]、[イベント グループ（Event Groups）]、[有線スイッチ サードパーティ要素（Wired Switches Third Party Elements）]、または [サービス アドバタイズメント（Service Advertisements）] を選択します。

各要素の [Sync. Status] 列に、同期ステータスが表示されます。緑の 2 つの矢印アイコンは、その対応する要素が、MSE などの指定されたサーバと同期していることを示します。灰色の 2 つの矢印と赤い円のアイコンは、対応する項目が指定のサーバと同期していないことを示します。

緑色の 2 つの矢印のアイコンは、コントローラの NMSP 接続状態は示しません。

[モニタ（Monitor）] > [マップ（Maps）] > [システム キャンパス（System Campus）] > [ビルディング（Building）] > [フロア（Floor）] を選択して、同期ステータスを表示することもできます。

このビルディングはキャンパス内のビルディング、フロアはキャンパス ビルディング内の特定のフロアです。

左側のサイドバーのメニューの [MSE Assignment] オプションに、フロアが現在割り当てられている MSE が表示されます。このページから MSE 割り当てを変更することもできます。

関連トピック

MSE の表示 （1007 ページ）
Cisco Prime Infrastructure への MSE の追加 （1000 ページ）
MSE と同期される Cisco Prime Infrastructure データ （1008 ページ）
MSE データベースと製品データベースの同期の履歴表示 （1017 ページ）
ワイヤレス コントローラの MSE 割り当ての変更 （1010 ページ）
MSE 製品の Out-of-Sync アラームの検索とトラブルシューティング （1031 ページ）

MSE データベースと製品データベースの同期の履歴表示

MSE の過去 30 日間の同期履歴を表示できます。アラームが自動的にクリアされるため、これは特に自動同期が有効な場合に便利です。[Synchronization History] には、クリアされたアラームの要約が表示されます。

[Services] タブの [Synchronization History] ページは、リリース 7.3 の root 仮想ドメインでのみ使用可能です。

同期履歴を表示するには、**[サービス（Services）] > [同期化履歴（Synchronization History）]** の順に選択し、列ヘッダーをクリックしてエントリをソートします。

関連トピック

MSE の表示 （1007 ページ）
サード パーティ NE と MSE の同期 （1012 ページ）
MSE と同期される Cisco Prime Infrastructure データ （1008 ページ）
ワイヤレス コントローラの MSE 割り当ての変更 （1010 ページ）
MSE 製品の Out-of-Sync アラームの検索とトラブルシューティング （1031 ページ）
MSE データベースと製品データベース間の同期のセットアップ （1014 ページ）
MSE データベースと製品データベースの同期ステータスの表示 （1016 ページ）

MSE に関する通知統計情報の表示

特定の MSE の通知統計情報を表示できます。特定の MSE の通知統計情報を表示するには、次の手順を実行します。

[サービス（Services）] > [モビリティサービス（Mobility Services）] > [モビリティサービスエンジン（Mobility Services Engines）] > [MSE-name] [コンテキスト認識型サービス（Context Aware Service）] > [通知統計情報（Notification Statistics）] の順に選択します（[MSE-name] は MSE の名前）。

次の表は、[通知統計情報（Notification statistics）] ページのフィールドの説明を示しています。

表 *79 : [Notification Statistics]* のフィールド

フィールド	説明
要約	
Destinations	
Total	宛先の合計数。
Unreachable	到達不能宛先の数。
Notification Statistics Summary	
Destination Address	通知送信先の宛先アドレス。
Destination Port	通知送信先の宛先ポート。
Destination Type	宛先のタイプ。例：SOAP_XML
Destination Status	トラック定義のステータス。トラック通知ステータスは[有効（Enabled）] または [無効（Disabled）] のいずれかです。
Last Sent	最終通知が宛先デバイスに送信された日時。
Last Failed	通知が失敗した日時。
Track Definition (Status)	
Total Count	宛先に送信された通知の合計数。宛先デバイスの通知統計詳細情報を表示するには、カウント リンクをクリックします。

MSE サーバの基本プロパティの変更

Prime Infrastructure を使用して、Prime Infrastructure データベースに登録されている MSE の一般プロパティを編集できます。一般プロパティには、連絡担当者名、ユーザ名、パスワード、HTTP などがあります。

MSE の一般プロパティを編集するには、次の手順に従います。

ステップ 1 **[サービス（Services）] > [モビリティ サービス（Mobility Services）] > [モビリティ サービス エンジン（Mobility Services Engines）]** を選択し、[モビリティ サービス（Mobility Services）] ページを表示します。

ステップ 2 編集する MSE の名前をクリックします。[General Properties] ページが表示されます（[General] タブと [Performance] タブがあります）。

ステップ 3 [General Properties] ページで以下のサーバ詳細情報を必要に応じて変更します。

- [Contact Name]：モビリティ サービスの連絡先の名前を入力します。

- [ユーザ名（Username）]：モビリティ サービスを管理する Prime Infrastructure サーバのログイン ユーザ名を入力します。
- [パスワード（Password）]：モビリティ サービスを管理する Prime Infrastructure サーバのログイン パスワードを入力します。
- [HTTP]：HTTP を有効にするには、[HTTP enable] チェックボックスをオンにします。デフォルト以外のポートを使用しているか、またはHTTPSがオンになっている場合、コマンドを使用して正しい情報を受け渡す必要があります。たとえば、*getserverinfo* には *-port<<port>> -protocol<<HTTP/HTTPS>>* を含める必要があります。同様に、サーバを停止するには、*stoplocserver - port <<port>> -protocol <HTTP/HTTPS>>* を使用します。
- [Legacy Port]：8001
- [Legacy HTTPS]：レガシー HTTPS を有効にするには、このチェックボックスをオンにします。
- [Delete synchronized service assignments and enable synchronization]：MSE からすべてのサービス割り当てを永久に削除するには、[Delete synchronized service assignments] チェックボックスをオンにします。このオプションが表示されるのは、MSE を追加するときに [Delete synchronized service assignments] チェックボックスをオフにした場合のみです。

Prime Infrastructure は MSE との通信に常に HTTPS を使用します。

リリース 6.0 の MSE で使用される TCP ポートは、tcp 22（MSE SSH ポート）、tcp 80（MSE HTTP ポート）、tcp 443（MSE HTTPS ポート）、tcp 1411（AeroScout）、tcp 1999（AeroScout 内部ポート）、tcp 4096（AeroScout 通知ポート）、tcp 5900X（AeroScout）（X は 1 ～ 10）、tcp 8001（レガシー ポート）です。ロケーション API に使用されます。

リリース 6.0 の MSE で使用される UDP ポートは、udp 123（NTPD ポート、NTP 設定の後に開きます）、udp 162（AeroScout SNMP）、udp/tcp 4000X（AeroScout プロキシ、X は 1 ～ 5）、udp 12091（AeroScout デバイス）（TDOA Wi-Fi レシーバ、チョークポイント）、udp 12092（AeroScout デバイス）（TDOA Wi-Fi レシーバ、チョークポイント）、udp 32768（ロケーション内部ポート）、udp 32769（AeroScout 内部ポート）、udp 37008（AeroScout 内部ポート）です。

ステップ 4 [Mobility Services] ダイアログボックスで [Admin Status] チェックボックスをオンにし、該当するサービス（Context Aware Service、WIPS、Mobile Concierge Service、Location Analytics Service、Billboard service）を有効にします。

[Context Aware Service] を選択する場合は、ロケーション計算を実行するロケーション エンジンを選択する必要があります。

次のいずれかを選択します。

- Cisco Tag Engine

または

- Partner Tag Engine

（注） MSE 6.0 では、複数のサービス（CAS と wIPS）を同時に有効にできます。6.0 よりも前のバージョンでは、MSE では一度に 1 つのアクティブ サービスしかサポートできませんでした。

[Mobility Services] ダイアログボックスには次の情報が表示されます。

- Service Name
- Service Version

- Service Status
- License Type

MSE のライセンスの詳細については、[Click here] リンクを使用してください。

ステップ 5 [保存（Save）] をクリックして Prime Infrastructure とモビリティ サービスのデータベースを更新します。

ステップ 6 [パフォーマンス（Performance）] タブをクリックし、CPU とメモリの使用率グラフを表示します。

MSE の NMSP プロトコル プロパティの変更

ネットワーク モビリティ サービス プロトコル（NMSP）は、モビリティ サービスとコントローラ間の通信を管理します。モバイル サービスとコントローラの間でのテレメトリ、緊急事態、RSSI の値の転送はこのプロトコルにより管理されます。

（注） リリース 3.0 ～ 7.0.105.0 でインストールされたモビリティ サービスでは、NMSP パラメータがサポートされています。7.0.105.0 より後のリリースではサポートされていません。

- NMSP は、リリース 3.0 で導入された LOCP の条件に置き換わるものです。
- テレメトリおよび緊急事態情報は、リリース 4.1 以降のソフトウェアでインストールされた Prime Infrastructure およびコントローラと、リリース 3.0 以降のソフトウェアを実行するモビリティ サービス エンジンでのみ表示されます。
- コントローラとモビリティ サービスとの通信には、TCP ポート 16113 が使用されます。コントローラとモビリティ サービスの間にファイアウォールがある場合、NMSP を機能させるにはこのポートが開いている（ブロックされていない）必要があります。

Prime Infrastructure の [NMSP パラメータ（NMSP Parameters）] ダイアログボックスでは、エコー間隔、ネイバー デッド間隔、応答期間、再送信期間などの NMSP パラメータを変更できます。

NMSP パラメータを設定するには、次の手順に従います。

ステップ 1 **[サービス（Services）]** > **[モビリティ サービス（Mobility Services）]** > **[モビリティ サービス エンジン（Mobility Services Engines）]** の順に選択します。

ステップ 2 プロパティを編集する MSE の名前をクリックします。

ステップ 3 左側のサイドバーのメニューから **[ステータス（Status）]** > **[NMSP パラメータ（NMSP Parameters）]** を選択します。

ステップ 4 必要に応じて、NMSP パラメータを変更します。

（注） ネットワークの応答が遅くなっている場合や大幅な遅延が発生している場合を除き、デフォルトのパラメータ値は変更しないことを推奨します。

NMSP パラメータには、次のものがあります。

- [Echo Interval]：モビリティ サービスからコントローラにエコー要求を送信する頻度を定義します。デフォルト値は 15 秒です。有効値の範囲は 1 ～ 120 秒です。
- ネットワークの応答が遅くなっている場合は、[エコー間隔（Echo Interval）]、[ネイバー デッド間隔（Neighbor Dead Interval）]、[応答タイムアウト（Response Timeout）] の値を大きくして、エコー確認の失敗回数を制限できます。
- [Neighbor Dead Interval]：Mobility Services Engine がネイバー デッドを宣言するまでに、コントローラから正常なエコー応答の受信を待機する時間（秒数）です。この時間は、エコー要求が送信された時点から始まります。
- デフォルト値は 30 秒です。有効値の範囲は 1 ～ 240 秒です。この値はエコー間隔値の 2 倍以上でなければなりません。
- [Response Timeout]：モビリティ サービスが、保留要求をタイムアウトと見なすまでに待機する時間を示します。デフォルト値は 1 秒です。最小値は 1 です。最大値はありません。
- [Retransmit Interval]：モビリティ サービスが、応答タイムアウトの通知を受け取ってから要求再送信を開始するまで待機する時間です。デフォルト設定は 3 秒です。有効値の範囲は 1 ～ 120 秒です。
- [Maximum Retransmits]：要求に対する応答がない場合に実行される再送信の最大回数を定義します。デフォルト設定は 5 です。有効な最小値は 0 です。最大値はありません。

ステップ 5 [保存（Save）] をクリックして Prime Infrastructure とモビリティ サービスのデータベースを更新します。

MSE アクティブ セッションの表示

Prime Infrastructure の [アクティブ セッション（Active Sessions）] ダイアログボックスでは、MSE でのアクティブなユーザ セッションを表示できます。

ステップ 1 **[サービス（Services）]** > **[モビリティサービス（Mobility Services）]** > **[モビリティサービスエンジン（Mobility Services Engines）]** の順に選択します。

ステップ 2 MSE の名前をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[システム（System）]** > **[アクティブ セッション（Active Sessions）]** を選択します。

Prime Infrastructure により、アクティブなモビリティ サービス セッションのリストが表示されます。Prime Infrastructure は各セッションに関する次の情報を表示します。

- セッション ID
- モビリティ サービス アクセス元の IP アドレス
- 接続ユーザのユーザ名
- セッションが開始された日時
- モビリティ サービスが最後にアクセスされた日時
- 最終アクセス以降セッションがアイドルになっていた期間

MSE トラップ接続先の表示

Prime Infrastructure の [トラップ宛先（Trap Destinations）] ダイアログボックスでは、MSE により生成される SNMP トラップを、どの Prime Infrastructure または Cisco Security Monitoring Analysis and Response System（CS-MARS）ネットワーク管理プラットフォームが受信するかを指定できます。

MSE のトラップ宛先を表示するには、次の手順に従います。

ステップ 1 **[サービス（Services）]** > **[モビリティサービス（Mobility Services）]** > **[モビリティサービスエンジン（Mobility Services Engines）]** の順に選択します。

ステップ 2 MSE の名前をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[システム（System）]** > **[トラップ宛先（Trap Destinations）]** の順に選択します。

Prime Infrastructure には現在のトラップ宛先のリストが表示されます。これには、次の情報が含まれます。

- IP アドレス
- ポート番号
- コミュニティ
- 宛先タイプ
- SNMP バージョン

[Select a command] ドロップダウン リストを使用してトラップ宛先を追加または削除します。

関連トピック

MSE トラップ接続先の設定 （1022 ページ）

MSE トラップ接続先の設定

トラップ宛先を追加するには、次の手順に従います。

ステップ 1 **[サービス（Services）]** > **[モビリティサービス（Mobility Services）]** > **[モビリティサービスエンジン（Mobility Services Engines）]** の順に選択します。

ステップ 2 モビリティ サービスの名前をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[システム（System）]** > **[トラップ宛先（Trap Destinations）]** の順に選択します。

ステップ 4 [コマンドの選択（Select a command）] ドロップダウン リストから [トラップ宛先の追加（Add Trap Destination）] を選択し、[実行（Go）] をクリックします。

[新しいトラップ宛先（New Trap Destination）] ページが表示されます。

ステップ 5 次の詳細を入力します（次の表を参照）。

表 *80 : [*トラップ宛先の追加（***Add Trap Destination***）*]* ページ

フィールド	説明
IPアドレス	トラップ宛先の IP アドレス。
[ポート番号（Port No.）]	トラップ宛先のポート番号。デフォルト ポート番号は、162 です。
Destination Type	このフィールドは編集できず、値 [Other] が表示されます。
Snmp Version	[v2c] または [v3] を選択します
SNMP バージョンとして v3 を選択した場合にだけ表示されるフィールドを以下に示します。	
User Name	SNMP バージョン 3 のユーザ名。
Security Name	SNMP バージョン 3 のセキュリティ名。
Authentication Type	次のいずれかを選択します。 HMAC-MD5 HMAC-SHA
Authentication Password	SNMP バージョン 3 の認証パスワード。
Privacy Type	次のいずれかを選択します。 CBC-DES CFB-AES-128 CFB-AES-192 CFB-AES-256
Privacy Password	SNMP バージョン 3 のプライバシー パスワード。

ステップ 6 [Save] をクリックして変更内容を保存するか、または [Cancel] をクリックして変更内容を取り消します。

関連トピック

MSE トラップ接続先の表示 （1022 ページ）

MSE サーバの詳細設定

Prime Infrastructure の [詳細パラメータ（Advanced Parameters）] ダイアログボックスでは、イベントを保持する日数、セッション タイムアウト値、データが存在しない間隔のクリーンアップ間隔を設定することができます。また、[拡張デバグ（Advanced Debug）] を有効または無効にすることができます。Prime Infrastructure を使用して、MSE のトラブルシューティング パラメータを変更できます。

MSE の詳細パラメータを編集するには、次の手順に従います。

ステップ 1 **[サービス（Services）]** > **[モビリティサービス（Mobility Services）]** > **[モビリティサービスエンジン（Mobility Services Engines）]** の順に選択します。

ステップ 2 プロパティを編集するモビリティ サービスの名前をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[システム（System）]** > **[詳細パラメータ（Advanced Parameters）]** を選択します。

ステップ 4 必要に応じて詳細パラメータを確認または変更します。

- General Information
- Advanced Parameters

  注意 詳細デバッグを実行するとモビリティ サービスの処理速度が低下するため、詳細デバッグは Cisco TAC 担当者の指示がある場合に限り有効にしてください。

  - [Number of Days to keep Events]：ログを維持する日数を入力します。モニタリングとトラブルシューティングで変更する必要がある場合に、この値を変更します。
  - [Session Timeout]：セッションがタイムアウトになるまでの分数を入力します。モニタリングとトラブルシューティングで変更する必要がある場合に、この値を変更します。現時点では、このオプションは淡色表示されます。
- Cisco UDI
  - [Product Identifier (PID)]：MSE の製品 ID。
  - [Version Identifier (VID)]：MSE のバージョン番号。
  - [Serial Number (SN)]：MSE のシリアル番号。
- Advanced Commands
  - [Reboot Hardware]：モビリティ サービス ハードウェアをリブートする場合にクリックします。詳細については、MSE サーバの再起動 （1025 ページ）を参照してください。
  - [ハードウェアのシャットダウン（Shutdown Hardware）]：モビリティ サービス ハードウェアをオフにする場合にクリックします。詳細については、「MSE サーバのシャット ダウン （1025 ページ）MSE サーバのシャットダウン」を参照してください。
  - [データベースのクリア（Clear Database）]：モビリティ サービス データベースをクリアする場合にクリックします。[Prime InfrastructurePrime Infrastructure の現在のサービス割り当てを保持（Retain current service assignments in the Prime Infrastructure）] チェックボックスをオフにし、Prime Infrastructure と MSE から既存のすべてのサービス割り当てを削除します。リソースは **[サービス（Services）]** > **[サービスの同期（Synchronize Services）]** ページから再度割り当てる必要があります。このオプションは、デフォルトで選択されます。

ステップ 5 [保存（Save）] をクリックして Prime Infrastructure とモビリティ サービスのデータベースを更新します。

MSE サーバの再起動

MSE を再起動する必要がある場合は、次の手順を実行します。

ステップ 1 **[サービス（Services）] > [モビリティ サービス（Mobility Services）] > [モビリティ サービス エンジン（Mobility Services Engines）]** を選択します。
ステップ 2 再起動する MSE の名前をクリックします。
ステップ 3 [System] をクリックします。
ステップ 4 [Advanced Parameters] をクリックします。
ステップ 5 [Advanced Commands] ダイアログボックスで [Reboot Hardware] をクリックします。
ステップ 6 [OK] をクリックして、MSE ハードウェアのリブートを確認します。

リブート プロセスが完了するには数分間かかります。

MSE サーバのシャット ダウン

MSE をシャット ダウンする必要がある場合には、次の手順に従います。

ステップ 1 **[サービス（Services）] > [モビリティ サービス（Mobility Services）] > [モビリティ サービス エンジン（Mobility Services Engines）]** を選択します。
ステップ 2 シャット ダウンする MSE の名前をクリックします。
ステップ 3 [System] をクリックします。
ステップ 4 [Advanced Parameters] をクリックします。
ステップ 5 [Advanced Commands] ダイアログボックスで [Shutdown Hardware] をクリックします。
ステップ 6 [OK] をクリックして、MSE をシャット ダウンすることを確認します。

MSE データベースの工場出荷時設定の復元（クリア）

MSE 設定をクリアし、工場出荷時の初期状態に戻すには、次の手順を実行します。

ステップ 1 **[サービス（Services）]>[モビリティサービス（Mobility Services）]>[モビリティサービスエンジン（Mobility Services Engines）]** の順に選択します。
ステップ 2 設定する MSE の名前をクリックします。
ステップ 3 [System] をクリックします。
ステップ 4 [Advanced Parameters] をクリックします。

ステップ 5 Prime Infrastructure と MSE から既存のサービス割り当てをすべて削除するには、[高度なコマンド（Advanced Commands）] ダイアログボックスの [Prime InfrastructurePrime Infrastructure での現在のサービス割り当てを保持（Retain current service assignments in the Prime Infrastructure）] チェックボックスをオフにします。

[サービス（Services）] > > [モビリティ サービス（Mobility Services）] > [サービスの同期（Synchronize Services）] ページでリソースの再割り当てを行う必要があります。デフォルトでは、このオプションが選択されています。

ステップ 6 [詳細コマンド（Advanced Commands）] ダイアログボックスで [データベースのクリア（Clear Database）] をクリックします

ステップ 7 [OK] をクリックすると、MSE データベースが消去されます。

MSE ロギング レベルの設定

Prime Infrastructure を使用して、ログに記録するメッセージのロギング レベルとタイプを指定できます。

ロギング オプションを設定するには、次の手順に従います。

ステップ 1 **[サービス（Services）] > [モビリティサービス（Mobility Services）] > [モビリティサービスエンジン（Mobility Services Engines）]** の順に選択します。

ステップ 2 設定する MSE の名前をクリックします。

ステップ 3 **[システム（System）] > [ログ（Logs）]** を選択します。選択されている MSE の詳細パラメータが表示されます。

ステップ 4 [Logging Level] ドロップダウン リストから適切なオプションを選択します。

ロギング オプションは、[Off]、[Error]、[Information]、および [Trace] の 4 つです。

ログ レベルを [Error] またはこれよりも前のレベルに設定した場合、ログ レコードはすべて、新しいエラー ログ ファイル locserver-error-%u-%g.log に記録されます。これは、ロケーション サーバの locserver-%u-%g.log ログ ファイルとともに維持される追加のログ ファイルです。このエラー ログ ファイルには、[Error] レベルのログとそのコンテキスト情報が記録されます。コンテキスト情報には、当該エラーよりも前の 25 ログ レコードが含まれています。最大 10 のエラー ログ ファイルを維持できます。各ログ ファイルの最大許容サイズは 10 MB です。

注意 [エラー（Error）] と [トレース（Trace）] は、Cisco TAC 担当者の指示があった場合にのみ使用してください。

ステップ 5 イベントのロギングを開始する各要素の横の [Enabled] チェックボックスをオンにします。

ステップ 6 [Advanced Parameters] ダイアログボックスの [Enable] チェックボックスをオンにし、詳細デバッグを有効にします。デフォルトでは、このオプションは無効になっています。

ステップ 7 サーバからログ ファイルをダウンロードするには、[Download Logs] をクリックします。詳細については、MSE ログ ファイルのダウンロード （1027 ページ）を参照してください。

ステップ 8 [Log File] グループ ボックスに、以下の情報を入力します。

- MSE で維持するログ ファイルの数。MSE で維持できるログ ファイルの数は 5 ～ 20 です。
- 最大ログ ファイル サイズ（MB 単位）。ログ ファイルのサイズは 10 ～ 50 MB です。

ステップ 9 [MAC Address Based Logging] グループ ボックスで、次の手順を実行します。

- [Enable] チェックボックスをオンにし、MAC アドレス ロギングを有効にします。デフォルトでは、このオプションは無効になっています。
- ロギングを有効にする 1 つ以上の MAC アドレスを追加します。また、以前に追加した MAC アドレスを削除できます。削除するには、リストから MAC アドレスを選択して [Remove] をクリックします。

MAC アドレス ベースのロギングの詳細については、「MSE MAC アドレス指定ベースのロギングの仕組み」MSE MAC アドレス指定ベースのロギングの仕組み （1027 ページ）を参照してください。

ステップ 10 [保存（save）] をクリックして変更を適用します。

MSE MAC アドレス指定ベースのロギングの仕組み

この機能では、指定されている MAC アドレスのエンティティ固有のログ ファイルを作成できます。ログ ファイルは次に示すパスの locserver ディレクトリ内に作成されます。

/opt/mse/logs/locserver

一度に最大で 5 つの MAC アドレスをログに記録できます。MAC アドレス aa:bb:cc:dd:ee:ff のログ ファイルの形式は macaddress-debug-aa-bb-cc-dd-ee-ff.log です。

1 つの MAC アドレスに対して最大で 2 つのログ ファイルを作成できます。2 つのログ ファイルのうち、1 つがメインのログファイルであり、もう 1 つがバックアップまたはロールオーバー ログ ファイルです。

MAC ログ ファイルの最小サイズは 10 MB です。最大許容サイズは、MAC アドレスあたり 20 MB です。MAC ログ ファイルの未更新時間が 24 を超えると、この MAC ログ ファイルはプルーニングされます。

MSE ログ ファイルのダウンロード

MSE ログ ファイルを解析する必要がある場合は、Prime Infrastructure を使用してログ ファイルをシステムにダウンロードできます。Prime Infrastructure は、ログ ファイルを含む zip ファイルをダウンロードします。

ログ ファイルが含まれている .zip ファイルをダウンロードするには、以下のステップに従います。

ステップ 1 **[サービス（Services）]>[モビリティ サービス（Mobility Services）]>[モビリティ サービス エンジン（Mobility Services Engines）]** の順に選択します。

ステップ 2 ステータスを表示する MSE の名前をクリックします。

ステップ 3 左側のサイドバーのメニューから、[Logs] を選択します。

ステップ 4 [Download Logs] をクリックします。

ステップ 5 [File Download] ダイアログボックスの指示に従い、ファイルを開くかまたは zip ファイルをシステムに保存します。

MSE ユーザ アカウントの設定

MSE ユーザ アカウントを設定するには、次の手順を実行します。

手順の概要

1. **[サービス（Services）] > [モビリティサービス（Mobility Services）] > [モビリティサービスエンジン（Mobility Services Engines）]** の順に選択します。
2. 編集する MSE のデバイス名をクリックします。
3. 左側のサイドバーのメニューから **[システム（Systems）] > [アカウント（Accounts）] > [ユーザ（Users）]** を選択します。
4. ユーザを MSE に追加するには、次の手順を実行します。
5. ユーザを MSE から削除するには、次の手順を実行します。
6. ユーザ プロパティを変更するには、次の手順を実行します。

手順の詳細

ステップ 1 **[サービス（Services）] > [モビリティサービス（Mobility Services）] > [モビリティサービスエンジン（Mobility Services Engines）]** の順に選択します。

ステップ 2 編集する MSE のデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから **[システム（Systems）] > [アカウント（Accounts）] > [ユーザ（Users）]** を選択します。

ステップ 4 ユーザを MSE に追加するには、次の手順を実行します。

a) [コマンドの選択（Select a command）] ドロップダウン リストから、[ユーザの追加（Add User）] を選択します。
b) [Go] をクリックします。
c) [Username] テキストボックスにユーザ名を入力します。
d) [Password] テキストボックスにパスワードを入力します。
e) [Group Name] テキストボックスにユーザが属するグループの名前を入力します。
f) [Permission] ドロップダウン リストから権限レベルを選択します。
g) 選択できる権限レベルには、[読み取りアクセス（Read Access）]、[書き込みアクセス（Write Access）]、および [フル アクセス（Full Access）]（Prime Infrastructure が MSE にアクセスするために必要な権限）の 3 つがあります。

注意 グループ権限は個々のユーザの権限を上書きします。たとえば、ユーザにフル アクセス権限を付与し、読み取りアクセス権限が付与されているグループにそのユーザを追加すると、そのユーザは MSE を設定できなくなります。

h) [Save] をクリックして新しいユーザを MSE に追加します。

ステップ 5 ユーザを MSE から削除するには、次の手順を実行します。

a) 左側のサイドバー メニューから [Systems] > [Accounts] > [Users] の順に選択します。
b) 削除するユーザのチェックボックスをオンにします。
c) [Select a command] ドロップダウン リストから [Delete User] を選択します。
d) [Go] をクリックします。
e) [OK] をクリックして、選択したユーザを削除することを確定します。

ステップ 6 ユーザ プロパティを変更するには、次の手順を実行します。

a) 編集するユーザのユーザ名をクリックします。
b) [Password]、[Group Name]、および [Permission] テキストボックスで必要な変更を行います。
c) [Save] をクリックして変更を適用します。

読み取り/書き込みアクセスを制御するMSEユーザグループの設定

次の手順を使用すると、MSE ユーザ グループの読み取り/書き込みアクセスを制御できます。

ステップ 1 **[サービス（Services）]>[モビリティサービス（Mobility Services）]>[モビリティサービスエンジン（Mobility Services Engines）]** の順に選択します。

ステップ 2 編集する MSE のデバイス名をクリックします。

ステップ 3 左側のサイドバーのメニューから **[システム（Systems）]>[アカウント（Accounts）]>[グループ（Groups）]** を選択します。

ステップ 4 ユーザ グループを MSE に追加するには、次の手順を実行します。

a) [Select a command] ドロップダウン リストから [Add Group] を選択します。
b) [Go] をクリックします。
c) [Group Name] テキストボックスにグループ名を入力します。
d) [Permission] ドロップダウン リストから権限レベルを選択します。

次の 3 つの権限レベルのいずれかを選択できます。

- **Read Access**
- **Write Access**
- **フル アクセス（Full Access）**（Prime Infrastructure がモビリティ サービス エンジンにアクセスするのに必要）

e) [Save] をクリックして新しいグループを MSE に追加します。

注意 グループ権限は個々のユーザの権限を上書きします。たとえば、ユーザにフルアクセス権限を付与し、読み取りアクセス権限が付与されているグループにそのユーザを追加すると、そのユーザは MSE を設定できなくなります。

ステップ 5 MSE からユーザ グループを削除するには、次の手順を実行します。

a) 削除するグループのチェックボックスをオンにします。
b) [コマンドの選択（Select a command）] ドロップダウン リストから [グループの削除（Delete Group）] を選択します。
c) [Go] をクリックします。
d) [OK] をクリックして、選択したユーザを削除することを確定します。

ステップ 6 ユーザ グループの権限を変更するには、次の手順を実行します。

a) 編集するグループのグループ名をクリックします。
b) [Permission] ドロップダウン リストから権限レベルを選択します。
c) [Save] をクリックして変更を適用します。

注意 グループ権限は個々のユーザの権限を上書きします。たとえば、ユーザにフル アクセス権限を付与し、読み取りアクセス権限が付与されているグループにそのユーザを追加すると、そのユーザは MSE を設定できなくなります。

MSE と製品サーバのモニタ

[システム（System）]>[ステータス（Status）]ページでは、サーバイベント、Prime Infrastructure アラームとイベント、および MSE の NMSP 接続ステータスをモニタできます。

サーバ イベントのリストを表示するには、次の手順を実行します。

ステップ 1 **[サービス（Services）]>[モビリティサービス（Mobility Services）]>[モビリティサービスエンジン（Mobility Services Engines）]** の順に選択します。

ステップ 2 該当する MSE の名前をクリックします。

ステップ 3 左側のサイドバー メニューから、**[システム（System）]>[ステータス（Status）]>[サーバイベント（Server Events）]** を選択します。

[Status] > [Server Events] ページに、次の情報が表示されます。

- [Timestamp]：サーバ イベントの時刻。
- [Severity]：サーバ イベントのシビリティ。
- [Event]：イベントの詳細な説明。
- [Facility]：イベントが発生した機能。

製品関連 MSE アラームの表示

MSE で使用可能な [Audit Logs] オプションを使用して、ユーザが実行した操作の監査ログを表示できます。監査ログを表示するには、次の手順に従います。

ステップ 1 **[サービス（Services）]** > **[モビリティサービス（Mobility Services）]** > **[モビリティサービスエンジン（Mobility Services Engines）]** の順に選択します。

ステップ 2 該当する MSE の名前をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[システム（System）]** > **[ステータス（Status）]** > **[監査ログ（Audit Logs）]** を選択します。

[ステータス（Status）] > **[監査ログ（Audit Logs）]** ページに、次の情報が表示されます。

- [Username]：監査ログを生成したユーザのユーザ名。
- [Operation]：ユーザが実行した操作。
- [Operation Status]：操作のステータス。これは [SUCCESSFUL] または [FAILED] です。
- [Invocation Time]：示されている操作について監査ログが記録された日時。

MSE アラームとイベントの表示

Prime Infrastructure アラームおよびイベントのリストを表示するには、次の手順を実行します。

ステップ 1 **[サービス（Services）]** > **[モビリティサービス（Mobility Services）]** > **[モビリティサービスエンジン（Mobility Services Engines）]** の順に選択します。

ステップ 2 該当するモビリティ サービスの名前をクリックします。

ステップ 3 左側のサイドバーのメニューから、次の手順を実行します。

- **[システム（System）]** > **[ステータス（Status）]** > **[Prime Infrastructure アラーム（Prime Infrastructure Alarms）]** Prime Infrastructure を選択し、アラームを表示します。
- **[システム（System）]** > **[ステータス（Status）]** > **[Prime Infrastructure イベント（Prime Infrastructure Events）]**Prime Infrastructure を選択し、アラームを表示します。

MSE 製品の Out-of-Sync アラームの検索とトラブルシューティング

Out-of-Sync アラームは、重大度が Minor（黄色）のアラームであり、次の条件に対して出されます。

- Cisco Prime Infrastructure で要素が変更された（自動同期ポリシーはこれらの要素をプッシュします）。
- MSE で要素が変更された。
- コントローラ以外の要素が MSE データベースに存在するが、Cisco Prime Infrastructure には存在しない。
- 要素が MSE に割り当てられていない（自動同期ポリシーは適用されません）。

Out-of-Sync アラームは、次の条件が発生するとクリアされます。

- MSE が削除される

MSE を削除すると、そのシステムの Out-of-Sync アラームも削除されます。また、使用可能な最後の MSE を削除すると、「どのサーバにも割り当てられていない要素」のアラームも削除されます。

- 要素が手動または自動で同期される
- ユーザがアラームを手動でクリアする（ただしスケジュールされているタスクが次回実行されるときに、アラームが再び表示される可能性があります）。

デフォルトでは、Out-of-Sync アラームは有効に設定されています。**[管理（Administration）]** > **[システム設定（System Settings）]** > **[アラームおよびイベント（Alarms and Events）]** を選択し、[モビリティサービスの同期（Mobility Service Synchronization）] をクリックし、[自動同期（Auto Synchronization）] チェックボックスの選択を解除して [送信（Submit）] をクリックすると、Cisco Prime Infrastructure でこれらを無効にできます。

コントローラと MSE 間の接続ステータスのモニタ

[NMSP Connection Status] ページでは、MSE と、この MSE が割り当てられているシスコ コントローラ間の NMSP 接続を確認できます。

ネットワーク モビリティ サービス プロトコル（NMSP）は、モビリティ サービスとコントローラ間の通信を管理するプロトコルです。

ステップ 1 **[サービス（Services）]** > **[モビリティサービス（Mobility Services）]** > **[モビリティサービスエンジン（Mobility Services Engines）]** の順に選択します。

ステップ 2 該当するモビリティ サービスの名前をクリックします。

ステップ 3 左側のサイドバー メニューから、**[システム（System）]** > **[ステータス（Status）]** > **[NMSP接続ステータス（NMSP Connection Status）]** の順に選択します。

[NMSP Connection Status] ページに、次の情報が表示されます。

- [Summary]：[Summary] セクションには、各デバイス タイプ、接続の合計数、非アクティブな接続の数が表示されます。
- [NMSP Connection Status]：このグループ ボックスには以下が表示されます。

[IP address]：デバイスの IP アドレスをクリックすると、そのデバイスの NMSP 接続ステータスの詳細が表示されます。追加情報については、特定のデバイスと MSE 間の接続ステータスのモニタ （1033 ページ）を参照してください。

- [Target Type]：NMSP 接続の接続先デバイスを示します。
- [Version]：デバイスの現在のソフトウェア バージョンを示します。
- [NMSP Status]：接続がアクティブまたは非アクティブのいずれであるかを示します。
- [Echo Request Count]：送信されたエコー要求の数を示します。
- [Echo Response Count]：受信したエコー応答の数を示します。
- [Last Message Received]：最新メッセージの受信日時を示します。

ステップ 4 [NMSP Status] が [ACTIVE] であることを確認します。

- アクティブである場合は、有線スイッチ、コントローラ、および有線クライアントの詳細情報を表示できます。
- アクティブでない場合は、Prime Infrastructure デバイスと MSE を再同期してください。

非アクティブな接続に対して NMSP トラブルシューティング ツールを起動できます。

関連トピック

NMSP 接続ステータスのトラブルシューティング （1011 ページ）

特定のデバイスと MSE 間の接続ステータスのモニタ

NMSP の接続ステータスの詳細を表示するには、次の手順に従います。

ステップ 1 **[サービス（Services）]>[モビリティサービス（Mobility Services）]>[モビリティサービスエンジン（Mobility Services Engines）]** の順に選択します。

ステップ 2 該当するモビリティ サービスの名前をクリックします。

ステップ 3 左側のサイドバー メニューから、**[システム（System）]>[ステータス（Status）]>[NMSP接続ステータス（NMSP Connection Status）]** の順に選択します。

ステップ 4 デバイスの IP アドレスをクリックします。[NMSP Connection Status Details] ページが開きます。[Details] ページには次の情報が表示されます。

- Summary
  - IP Address
  - [Version]：デバイスの現在のソフトウェア バージョン。
  - [Target Type]：NMSP 接続の接続先デバイス。
  - [NMSP Status]：接続がアクティブまたは非アクティブのいずれであるかを示します。
  - [Echo Request Count]：送信されたエコー要求の数。
  - [Echo Response Count]：受信したエコー応答の数。
  - [Last Activity Time]：デバイスと MSE 間での最終メッセージ アクティビティの日時。
  - [Last Echo Request Message Received At]：最新のエコー要求を受信した日時。
  - [Last Echo Response Message Received At]：最新のエコー応答を受信した日時。
  - [Model]：デバイスのモデル。
  - [MAC Address]：デバイスの MAC アドレス（該当する場合）。
  - [Capable NMSP Services]：このデバイスの NMSP 対応サービス（ATTACHMENT、LOCATION など）。
- [Subscribed Services]：サブスクライブしている各 NMSP サービスのサブサービスを示します。たとえば、MOBILE_STATION_ATTACHMENT は ATTACHMENT のサブサービスです。
- Messages
  - [Message Type]：メッセージ タイプには、ATTACHMENT_NOTIFICATION、ATTACHMENT_REQUEST、ATTACHMENT_RESPONSE、CAPABILITY_NOTIFICATION、ECHO_REQUEST、ECHO_RESPONSE、LOCATION_NOTIFICATION、LOCATION_REQUEST、SERVICE_SUBSCRIBE_REQUEST、SERVICE_SUBSCRIBE_RESPONSE などがあります。

- [In/Out]：メッセージが着信メッセージと発信メッセージのいずれであるかを示します。
- [Count]：着信メッセージまたは発信メッセージの数を示します。
- [Last Activity Time]：最新のアクティビティまたはメッセージの日時。
- [Bytes]：メッセージのサイズ（バイト単位）。

MSE データベース バックアップの設定

モビリティ サービス バックアップ パラメータを表示または編集するには、次の手順に従います。

ステップ 1 **[サービス（Services）]** > **[モビリティサービス（Mobility Services）]** > **[モビリティサービスエンジン（Mobility Services Engines）]** の順に選択します。

ステップ 2 プロパティを編集するモビリティ サービスの名前をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[メンテナンス（Maintenance）]** > **[バックアップ（Backup）]** の順に選択します。

- [Backups located at]：バックアップ ファイルの場所を示します。
- [Enter a name for the Backup]：バックアップ ファイル名を入力または編集します。
- [Timeout (in secs)]：ファイル バックアップ試行操作がタイムアウトになるまでの時間（秒単位）を示します。

製品サーバへの MSE 履歴データのバックアップ

Prime Infrastructure には、MSE のデータをバックアップするための機能が搭載されています。

ステップ 1 **[サービス（Services）]** > **[モビリティサービス（Mobility Services）]** > **[モビリティサービスエンジン（Mobility Services Engines）]** の順に選択します。

ステップ 2 バックアップする MSE の名前をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[メンテナンス（Maintenance）]** > **[バックアップ（Backup）]** の順に選択します。

ステップ 4 バックアップの名前を入力します。

ステップ 5 バックアップがタイムアウトになるまでの時間（秒単位）を入力します。

ステップ 6 [送信（Submit）] をクリックし、Prime Infrastructure が実行しているサーバのハード ドライブに履歴データをバックアップします。

バックアップ処理中に、このページでバックアップのステータスを確認できます。バックアップ処理中に、このページには 3 つの項目が表示されます。（1）[Last Status] フィールドには、バックアップのステータ

スを示すメッセージが表示され、（2）[Progress] フィールドには、バックアップの完了率が表示され、（3）[Started at] フィールドには、バックアップの開始日時が示されます。

別の Prime Infrastructure ページで他の MSE 操作を実行しながら、バックアップ プロセスをバックグラウンドで実行できます。

バックアップは、Prime Infrastructure のインストール時に指定した FTP ディレクトリに保存されます。ただし、Prime Infrastructure のインストールでは、FTP ディレクトリは指定されません。場合によっては、FTP ルートのフル パスを指定する必要があります。

製品サーバからの MSE 履歴データの復元

ファイルをモビリティ サービス エンジンに復元するには、次の手順を実行します。

ステップ 1 **[サービス（Services）]** > **[モビリティサービス（Mobility Services）]** > **[モビリティサービスエンジン（Mobility Services Engines）]** の順に選択します。

ステップ 2 プロパティを編集するモビリティ サービスの名前をクリックします。

ステップ 3 左側のサイドバーのメニューから、[Maintenance] > [Restore] の順に選択します。

ステップ 4 ドロップダウン リストから、復元するファイルを選択します。

ステップ 5 MSE からすべてのサービス割り当てを永久に削除するには、[Delete synchronized service assignments] チェックボックスをオンにします。

このオプションは、ネットワーク設計、有線スイッチ、コントローラ、およびイベント定義に適用されます。既存のロケーション履歴データは維持されますが、今後ロケーション計算を実行するときには手動サービス割り当てを使用する必要があります。

ステップ 6 [Submit] をクリックして復元プロセスを開始します。

ステップ 7 [OK] をクリックし、Prime Infrastructure サーバのハード ドライブからデータを復元することを確定します。

復元が完了すると、Prime Infrastructure にそのことを示すメッセージが表示されます。

別の Prime Infrastructure ページで他の MSE 操作を実行しながら、復元プロセスをバックグラウンドで実行できます。

MSE へのソフトウェアのダウンロード

Prime Infrastructure を使用して、MSE にソフトウェアをダウンロードするには、次の手順を実行します。

ステップ 1 アプリケーション コードのダウンロードに使用する Prime Infrastructure または外部 FTP サーバから、ロケーション アプライアンスに対して ping を実行できることを確認します。

ステップ 2 **[サービス（Services）] > [モビリティサービス（Mobility Services）] > [モビリティサービスエンジン（Mobility Services Engines）]** の順に選択します。

ステップ 3 ソフトウェアのダウンロード先となる MSE の名前をクリックします。

ステップ 4 左側のサイドバーのメニューから、[メンテナンス（Maintenance）] を選択します。

ステップ 5 [ソフトウェアのダウンロード（Download Software）] をクリックして、次のいずれかを実行します。

- Prime Infrastructure ディレクトリにリストされているソフトウェアをダウンロードするには、[サーバに転送するアップロード済みイメージを選択（Select from uploaded images to transfer into the Server）] チェックボックスを選択します。次に、ドロップダウン リストからバイナリ イメージを選択します。

  Prime Infrastructure により、ドロップダウン リストにリストされているバイナリ イメージが、Prime Infrastructure インストール時に指定した FTP サーバ ディレクトリにダウンロードされます。

  Prime Infrastructure のインストール時に FTP ディレクトリが指定されていません。FTP ルートのフルパスを指定する必要が生じることがあります。

- ローカルまたはネットワーク経由で入手可能なダウンロード済みソフトウェアを使用するには、[サーバに転送する新しいソフトウェア イメージを参照（Browse a new software image to transfer into the Server）] チェックボックスをオンにし、[参照（Browse）] をクリックします。ファイルを見つけ、[Open] をクリックします。

ステップ 6 ソフトウェア ダウンロードがタイムアウトになるまでの時間（秒単位、1 ～ 1800）を入力します。

ステップ 7 [ダウンロード（Download）] をクリックし、ソフトウェアを MSE 上の /opt/installers ディレクトリにダウンロードします。

モバイルデバイスのナビゲーションを向上するための**MSE**パートナーシステムの設定（**Qualcomm PDS**）

[システム（System）] > [パートナーシステム（Partner Systems）] ページでは、MSE-Qualcomm PDS を設定できます。この設定の目的は、モバイル デバイスのナビゲーション機能を向上させることです。パートナー検出サーバ（PDS）は、MSE によって提供されるフロア プランと AP データを使用して暗号化されたサポート データを生成します。PDS は Qualcomm スマートフォンで使用される最適化された形式にこの情報を変換します。

MSE を使用するための Qualcomm PDS の設定

MSE の Qualcomm PDS を設定するには、次の手順に従います。

ステップ 1 **[サービス（Services）] > [モビリティサービス（Mobility Services）] > [モビリティサービスエンジン（Mobility Services Engines）]** の順に選択します。

ステップ 2 モビリティ サービスの名前をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[システム（System）] > [パートナー システム（Partner Systems）]** を選択します。

[MSE 用の Qualcomm PDS 設定（Qualcomm PDS Configuration for MSE）] ページが表示されます。

ステップ 4 MSE-Qualcomm 通信を有効にするには、[Qualcomm の有効化（Enable Qualcomm）] チェックボックスをオンにします。

ステップ 5 [Qualcomm PDS Endpoint] テキスト ボックスに、Qualcomm PDS サーバの URL を入力します。これは、データ サポートをフェッチできる PDS の URL です。デフォルトの URL は http://207.114.133.174:8000/AssistanceDataMgr/AssistanceDataMgrSOAP?wsdl です。

ステップ 6 [MSE URL to request assistance data] テキスト ボックスに MSE URL を入力します。これは、場所においてデバイスがアクセスできる MSE の URL です。

ステップ 7 [Cisco Mobile Concierge SSID] テキスト ボックスに、モバイル クライアントを接続させる先のモバイル コンシェルジュ SSID 情報を入力します。Qualcomm のスマート フォンがこの SSID を関連付けられ、MSE と通信します。

ステップ 8 [Venue Description] テキスト ボックスに場所の説明を入力します。

ステップ 9 [Refresh time period for assistance data on MSE] テキスト ボックスに、MSE のサポート データの更新間隔を入力します。

ステップ 10 [Refresh time period for assistance data on mobile clients] テキスト ボックスに、モバイル クライアントのサポート データの更新間隔を入力します。

ステップ 11 メッセージ/サポート データを Qualcomm PDS サーバに送信し、モバイル クライアントが著作権で保護される必要がある場合は、[Include Copyright Information] チェックボックスを選択します。

ステップ 12 含める必要がある著作権所有者情報を [著作権所有者（Copyright Owner）] テキスト ボックスに入力します。

ステップ 13 [Copyright Year] テキスト ボックスに、含める必要のある著作権年を入力します。

ステップ 14 設定を保存する場合は [Save] を、元に戻る場合は [Cancel] をクリックします。

Qualcomm PDS が MSE を使用する仕組み

MSE-Qualcomm の設定には、次の手順が含まれます。

- CAD ファイルからの Map Extraction Tool（MET）の出力の生成
- MET の出力を Prime Infrastructure に入力する
- GPS マーカーを追加する
- フロアを MSE に同期する
- Qualcomm QUIPS/PDS および著作権情報を提供する
- MSE で Qualcomm PDS サーバに対する F2 インターフェイス要求を実行する

Qualcomm の MET アプリケーションを使用すると、マップ ファイル（DXF ファイル）からさまざまなレイヤをカスタマイズおよび選択し、以下の項目を含む zip ファイルを生成することができます。

- Prime Infrastructure でフロア マップとして使用されるイメージ ファイル（.PNG 形式）。
- メートル単位でのフロア面積（水平および垂直）を含む Span.xml ファイル。
- 壁、扉、関心のあるポイントなどに関連する幾何機能情報を含む Qualcomm 固有のマップ XML ファイル。

（注） MET アプリケーションは Prime Infrastructure および MSE には依存せず、任意のホスト マシンに常駐させることができます。MET の出力のみが Prime Infrastructure でマップ関連の入力情報として使用されます。

ステップ 1 [MET Tool] フォルダ内の ReadMe.txt ファイルにある手順に従って、Qualcomm MET ツールを起動します。

ステップ 2 Map Extraction Tool に DXF ファイルを入力します。

ステップ 3 左側のサイド バーのメニューから必要な階層を選択します。

ステップ 4 Map Extraction Tool のユーザ インターフェイスで目的の場所に Map Extraction Tool の出力を保存します。

MSE wIPS サービス管理設定の構成

[wIPS サービス（wIPS Service）] ページでは、wIPS サービス管理設定を表示または管理できます。

（注） 非ルート パーティション ユーザに対しては Cisco Adaptive wIPS 機能がサポートされていません。

wIPS サービス管理設定を表示または管理するには、次の手順に従います。

ステップ 1 **[サービス（Services）] > [モビリティサービス（Mobility Services）] > [モビリティサービスエンジン（Mobility Services Engines）]** の順に選択します。

ステップ 2 該当する MSE のデバイス名を選択します。

ステップ 3 左側のサイドバー メニューから [wIPS Service] を選択します。

ステップ 4 次のパラメータを表示または編集します。

- [Log level]：ドロップダウン リストから適切なログ レベルを選択します。ログ レベルには、[デバッグ（Debug）]、[エラー（Error）]、[重要イベント（Important Event）]、[メジャー デバッグ（Major Debug）]、[なし（None）]、および [警告（Warning）] があります。
- [Forensic size limit (GB)]：フォレンジック ファイルの最大許容サイズを入力します。
- [Alarm ageout (hours)]：各アラームの有効期間を時間単位で入力します。
- [Device ageout (days)]：デバイスによるアラーム送信の有効期間を日単位で入力します。

ステップ 5 [Save] をクリックして変更を確定するか、または [Cancel] をクリックして変更を適用せずにページを閉じます。

MSEコンテキスト認識型サービス（ロケーションサービス）によるトラッキングの向上

コンテキスト認識型サービス（CAS）ソフトウェアにより、シスコ アクセス ポイントからクライアントまたはタグ（Cisco CX バージョン以降）に関する状況依存情報（ロケーション、温度、アセット可用性など）を取得することで、MSE は数千のモバイル アセットとクライアントを同時に追跡できます。

CAS は、受信した状況依存情報を処理する際に 2 つのエンジンを使用します。*Context-Aware Engine for Clients* は Wi-Fi クライアントから受信したデータを処理し、*Context-Aware Engine for Tags* は Wi-Fi タグから受信したデータを処理します。業務上のニーズに応じてこれらのエンジンを一緒に導入することも、個別に導入することもできます。

Mobility Services Engine は Cisco CX 以外のタグの追跡とマッピングは行いません。

CAS は、以前は Cisco ロケーションベース サービスと呼ばれていました。

追跡対象のクライアントまたはタグの数とタイプに関する コンテキスト認識型サービス ソフトウェアのプロパティと、クライアントまたはタグのロケーションを計算するかどうかの設定を変更できます。

クライアントとタグのロケーション計算（受信信号強度インジケータ（RSSI）測定など）に影響するパラメータも変更できます。

インストールと初期設定が完了した後、MSE は複数の Cisco ワイヤレス LAN コントローラと通信して、オペレータが定義したコンテキスト情報を収集できます。その後、関連付けられた Cisco Prime Infrastructure を使用して各 MSE と通信し、選択したデータの送信や表示を行えます。

クライアント、不正アクセス ポイント、不正クライアント、モバイル ステーション、干渉源、およびアクティブ RFID アセット タグに関するデータを収集するように MSE を設定できます。

MSE CAS の使用時の前提条件、MSE コンテキスト認識型サービス（ロケーション サービス）によるトラッキングの向上

Cisco Prime Infrastructure を使用して状況依存情報を表示するには、その前に、コマンドライン インターフェイス（CLI）コンソール セッションを使用して MSE の初期設定を行う必要があります。http://www.cisco.com/en/US/products/ps9742/tsd_products_support_series_home.html で『*Cisco 3355 Mobility Services Engine Getting Started Guide*』および『*Cisco 3100 MSE Getting Started Guide*』を参照してください。

クライアントおよびタグのライセンス

アクセス ポイントからタグおよびクライアントに関する状況依存情報を取得するには、シスコからライセンスを購入する必要があります。

- タグとクライアントのライセンスはそれぞれ個別に提供されます。

- クライアント ライセンスには、不正クライアント、不正アクセス ポイント、および干渉（有効に設定されている場合）の追跡機能も含まれています。
- タグとクライアントのライセンスは、さまざまな数量（1,000 ～ 12,000 ユニット）で提供されます。

AeroScout Context-Aware Engine for Tags では、100 の永久タグ ライセンスがサポートされています。Context-Aware Services は永久タグ ライセンスで構成されています。

（注） タグおよびクライアント ライセンスの詳細については、http://www.cisco.com/en/US/products/ps9742/tsd_products_support_series_home.html で『*Release Notes for Cisco 3300 Series Mobility Services Engine for Software Release 6.0*』を参照してください。

コンテキスト認識型サービスの一般パラメータ

[コンテキスト認識型サービス（Context Aware Service）] > [一般（General）] ページにアクセスするには、次の手順を実行します。

ステップ 1 **[サービス（Services）] > [モビリティサービス（Mobility Services）] > [モビリティサービスエンジン（Mobility Services Engines）]** の順に選択します。

ステップ 2 左側のサイドバーのメニューから、**[全般（General）]** を選択します。

このページには、次の情報が表示されます。

- バージョン
- 動作ステータス
- 追跡対象有線クライアントの数
- トレース対象タグの数
- 追跡対象不正 AP の数
- 追跡対象不正クライアントの数
- 追跡対象干渉源の数
- 追跡対象有線クライアントの数
- 追跡対象の要素の合計数
- 追跡対象の要素（ワイヤレス クライアント、不正 AP、不正クライアント、干渉源、および有線クライアント）の制限
- 追跡対象のタグの制限

[Clients] は 15 分ごとのクライアント数のスナップショットを表します。[Peak Clients] は、その 15 分間の最大数です。たとえば、15 分の期間では、クライアント数は 100 ～ 300 まで変動します。Prime Infrastructure が MSE をポーリングすると、MSE はその正確な時点での数値としてクライアント数を返します。これは 100 ～ 300 の範囲になり、クライアント最大数は 300 です。

MSE でのコンテキスト認識型サービスの有効化と設定

MSE では、最大 25,000 クライアントまたは 25,000 タグを追跡できます（適切なライセンスを購入している場合）。追跡中の要素の位置のアップデート内容は、シスコ ワイヤレス LAN コントローラから MSE に送信されます。

このうち、コントローラから追跡対象として指定した要素だけを、Prime Infrastructure マップ、クエリ、およびレポートで表示できます。追跡対象外の要素のイベントとアラームは一切収集されず、クライアントまたはタグの 25,000 個の要素上限にはカウントされません。

Prime Infrastructure を使用して次の追跡パラメータを変更できます。

- アクティブに追跡する要素ロケーション（クライアント ステーション、アクティブなアセット タグ、干渉、有線クライアント、不正クライアント、不正アクセス ポイント）の有効化および無効化。
  - 有線クライアント ロケーションの追跡により、データセンターのサーバはネットワーク上の有線クライアントを容易に検出できるようになります。サーバにはネットワーク上の有線スイッチ ポートが関連付けられています。
- 追跡対象とする特定要素の個数上限を設定します。

たとえば、12,000 の追跡対象ユニットのクライアント ライセンスで、追跡できるクライアント ステーションの数の上限として 8,000 を設定できます（この場合残りの 4,000 ユニット分は、不正クライアントと不正アクセス ポイントの追跡に使用できます）。特定の要素の追跡上限に達すると、追跡されていない要素の合計数が [Tracking Parameters] ページに表示されます。

- アドホックの不正クライアントと不正アクセス ポイントの追跡解除とレポート解除。

MSE の追跡パラメータを設定するには、次の手順に従います。

ステップ 1 **Services > Mobility Services > Mobility Services Engines** を選択して、モビリティ サービス ページを開きます。

ステップ 2 プロパティを編集する MSE の名前をクリックします。[General Properties] ページが表示されます。

ステップ 3 [管理（Administration）] サブヘッダーから [コンテキスト認識型のソフトウェア（Context-Aware Software）] > [追跡パラメータ（Tracking Parameters）] を選択して、設定オプションを表示します。

ステップ 4 次に示す追跡パラメータを適切に変更します（次の表を参照）。

表 *81* : 追跡パラメータ（*Tracking Parameters*）

フィールド	設定オプション
Tracking Parameters	

フィールド	設定オプション
Wired Clients	**1.** MSE によるクライアント ステーションの追跡を有効にするには、[**Enable**] チェックボックスをオンにします。 7.0 では、クライアント ライセンスはすべてのネットワーク ロケーション サービス要素を対象としており、有線クライアント、ワイヤレス クライアント、不正クライアント、不正アクセス ポイント、および干渉の間で共有されます。 有線クライアント数の上限は、MSE 7.0 および Prime Infrastructure 1.0 からサポートされています。つまり、有線クライアントの数を一定数（例：500）に制限できます。この上限を設定することで、ライセンスで許可されているデバイスの数が有線クライアントによって使い切ることがなく、一部のライセンスが他のデバイスに対して使用可能になります。 **注意** MSE を 6.0 から 7.0 にアップグレードすると、ワイヤレス クライアントまたは不正クライアント/アクセス ポイントの上限が設定されている場合、この上限はリセットされます。これは、7.0 では有線クライアントの上限が変更されているためです。 （注） [Active Value]（表示のみ）：現在追跡されている有線クライアント ステーションの数を示します。 （注） [Not Tracked]（表示のみ）：上限を超えている有線クライアント ステーションの数を示します。
Wireless Clients	**1.** MSE によるクライアント ステーションの追跡を有効にするには、[**Enable**] チェックボックスをオンにします。 **2.** 追跡するクライアント ステーションの上限数を設定するには、**Enable Limiting** チェックボックスをオンにします。 **3.** 上限が有効になっている場合は、上限値を入力します。入力できる上限値は、25,000（MSE で追跡できるクライアントの最大数）までの正の値です。 （注） 追跡対象クライアントの実際の数は、購入ライセンスによって決まります。 （注） [Active Value]（表示のみ）：現在追跡されているクライアント ステーションの数を示します。 （注） [Not Tracked]（表示のみ）：上限を超えているクライアント ステーションの数を示します。

フィールド	設定オプション
Rogue Access Points	1. MSEによる不正クライアントおよび不正アクセス ポイントの追跡を有効にするには、**Enable** チェックボックスをオンにします。 2. 追跡する不正クライアントおよびアクセス タグ ステーションの数を設定するには、**Enable Limiting** チェックボックスをオンにします。 3. 上限が有効になっている場合は、上限値を入力します。入力できる上限値は、25,000（MSEで追跡できる不正クライアントおよび不正アクセス ポイントの最大数）までの正の値です。 （注） 追跡対象不正クライアント/アクセス ポイントの実際の数は、購入したクライアントライセンスによって決まります。クライアント、不正クライアント、および不正アクセス ポイントには同一ライセンスが適用されるため、不正クライアントと不正アクセス ポイントの追跡のために割り当て可能な数量を決定する際には、追跡されているクライアントの数を考慮する必要があります。 （注） [Active Value]（表示のみ）：現在追跡している不正クライアントと不正アクセス ポイントの数を示します。 （注） [Not Tracked]（表示のみ）：上限を超えた不正クライアントと不正アクセス ポイントの数を示します。
Exclude Ad-Hoc Rogues	ネットワーク内のアドホックの不正クライアント/アクセス ポイントの追跡と報告を無効にするには、このチェックボックスをオンにします。このように設定すると、Prime Infrastructure マップにアドホック不正クライアント/アクセス ポイントが表示されず、イベントとアラームが報告されません。
Rogue Clients	1. MSEによる不正クライアントの追跡を有効にするには、**Enable** チェックボックスをオンにします。 2. 追跡するクライアント ステーションの数の上限を設定するには、**Enable Limiting** チェックボックスをオンにします。 3. 上限が有効になっている場合は、上限値を入力します。入力できる上限値は、25,000（MSEで追跡できる不正クライアントの最大数）までの正の値です。 （注） 追跡対象不正クライアント/アクセス ポイントの実際の数は、購入したクライアントライセンスによって決まります。クライアント、不正クライアント、および不正アクセス ポイントには同一ライセンスが適用されるため、不正クライアントと不正アクセス ポイントの追跡のために割り当て可能な数量を決定する際には、追跡されているクライアントの数を考慮する必要があります。 （注） [Active Value]（表示のみ）：追跡されている不正クライアントの数を示します。 （注） [Not Tracked]（表示のみ）：上限を超えている不正クライアントの数を示します。

フィールド	設定オプション
Interferers	**1.** MSE による干渉源の追跡を有効にするには、**Enable** チェックボックスをオンにします。 7.0 では、クライアント ライセンスはすべてのネットワーク ロケーション サービス要素を対象としており、有線クライアント、ワイヤレス クライアント、不正クライアント、不正アクセス ポイント、および干渉の間で共有されます。 （注） [Active Value]（表示のみ）：現在追跡されている干渉の数を示します。 （注） [Not Tracked]（表示のみ）：上限を超えている干渉の数を示します。
Asset Tracking Elements	
Active RFID Tags	**1.** MSE によるアクティブな RFID タグの追跡を有効にするには、**Enable** チェックボックスをオンにします。 （注） 追跡対象のアクティブ RFID タグの実際の数は、購入ライセンスによって決まります。 （注） [Active Value]（表示のみ）：現在追跡されているアクティブ RFID タグの数を示します。これは、選択されたタグ エンジンによって異なります。 （注） [Not Tracked]（表示のみ）：上限を超えているアクティブ RFID タグの数を示します。
SNMP Parameters 7.0.105.0 以降のモビリティ サービスには適用されません。	
SNMP Retry Count	ポーリング サイクルの再試行回数を入力します。デフォルト値は 3 です。有効値は 1 ～ 99999 です。（リリース 4.1 以前のコントローラでのみ設定可能。）
SNMP Timeout	ポーリング サイクルがタイムアウトになるまでの時間を秒数で入力します。デフォルト値は 5 です。有効値は 1 ～ 99999 です。（リリース 4.1 以前のコントローラでのみ設定可能。）
SNMP Polling Interval	
Client Stations	クライアント ステーションのポーリングを有効にし、ポーリング間隔（秒数）を入力するには、**Enable** チェックボックスをオンにします。デフォルト値は 300 です。有効値は 1 ～ 99999 です。（リリース 4.1 以前のコントローラでのみ設定可能。）
Active RFID Tags	アクティブ RFID タグのポーリングを有効にし、ポーリング間隔（秒数）を入力するには、**Enable** チェックボックスをオンにします。有効値は 1 ～ 99999 です。 （注） モビリティ サービスでコントローラからアセット タグ データを収集できるようにするには、その前に、コントローラで CLI コマンド **config rfid status enable** を使用して、アクティブ RFID タグの検出を有効にする必要があります。

フィールド	設定オプション
Rogue Clients and Access Points	不正アクセス ポイントのポーリングを有効にし、ポーリング間隔（秒数）を入力するには、**Enable** チェックボックスをオンにします。デフォルト値は 600 です。有効値は 1 ～ 99999 です。（リリース 4.1 以前のコントローラでのみ設定可能）。
Statistics	モビリティ サービスの統計ポーリングを有効にし、ポーリング間隔（秒数）を入力するには、**Enable** チェックボックスをオンにします。デフォルト値は 900 です。有効値は 1 ～ 99999 です。（リリース 4.1 以前のコントローラでのみ設定可能）。

ステップ 5 [Save] をクリックし、MSE データベースに新しい設定を保存します。

コンテキスト認識型サービスフィルタを使用して追跡するMSEアセットのカスタマイズ

以下の項目をフィルタリングすることで、ロケーションが追跡されるアセットタグ、有線クライアント、不正クライアント、干渉源、およびアクセス ポイントの数を制限できます。

- MAC アドレス

特定の MAC アドレスを入力し、ロケーション追跡での許可または不許可を設定できます。許可または不許可にする MAC アドレスを記述したファイルをインポートするか、または Prime Infrastructure GUI ページに個々の MAC アドレスを入力することができます。

MAC アドレスの入力形式は xx:xx:xx:xx:xx:xx です。MAC アドレスのファイルをインポートする場合、ファイルは次の形式に従っている必要があります。

- 各 MAC アドレスを 1 行ずつ記述する必要があります。
- 許可される MAC アドレスを最初にリストする必要があり、その前に [Allowed] 行項目を含めます。「[Disallowed]」の後に不許可 MAC アドレスをリストする必要があります。
- ワイルドカードを使用して MAC アドレスの範囲を指定できます。たとえば、以下の [Allowed] リストの 1 番めのエントリ「00:11:22:33:*」はワイルドカードです。

（注） 許可 MAC アドレスの形式は、[Filtering Parameters] 設定ページに表示されます。詳細については、次の表を参照してください。

ファイルの記述例：

[Allowed]00:11:22:33:*22:cd:34:ae:56:4502:23:23:34:*[Disallowed]00:10:*ae:bc:de:ea:45:23

- プローブ クライアント

プローブ クライアントとは、別のコントローラに関連付けられているが、プロービング アクティビティによって別のコントローラから認識され、そのプライマリ コントローラとともに「プローブ済み」コントローラによって要素としてカウントされるクライアントです。

MSE のフィルタリング パラメータを設定するには、次の手順に従います。

ステップ 1 **[サービス（Services）]>[モビリティサービス（Mobility Services）]>[モビリティサービスエンジン（Mobility Services Engines）]** の順に選択します。[Mobility Services] ページが表示されます。

ステップ 2 プロパティを編集する MSE の名前をクリックします。[General Properties] ページが表示されます。

ステップ 3 [Context-Aware Software] メニューの [Administration] サブヘッダーから [Filtering Parameters] を選択します。設定オプションが表示されます。

ステップ 4 次に示すフィルタリング パラメータを適切に変更します（次の表を参照）。

表 82 : Filtering Parameters

フィールド	設定オプション
Advanced Filtering Parameters	
Duty Cycle Cutoff Interferers	指定した制限を満たすデューティ サイクルのある干渉のみ追跡され、基本ロケーション ライセンスに対してカウントされるように、干渉のデューティ サイクルのカットオフ値を入力します。 [Duty Cycle Cutoff Interferers] のデフォルト値は 0% で、設定可能な範囲は 0% ～ 100% です。 ロケーション ライセンスをより適切に使用するために、干渉源のデューティ サイクルに基づいて干渉源のフィルタを指定することもできます。
MAC Filtering Parameters	
Exclude Probing Clients	プローブ クライアントのロケーション計算を実行しないようにするには、このチェックボックスをオンにします。

フィールド	設定オプション
Enable Location MAC Filtering	**1.** MAC アドレスによる特定要素の MAC フィルタリングを有効にするには、このチェックボックスをオンにします。 **2.** MAC アドレスのファイルをインポートするには（[Upload a file for Location MAC Filtering] フィールド）、ファイル名を検索して選択し、[Save] をクリックしてファイルをロードします。インポートされた MAC アドレスのリストは、ファイルでの指定に基づいて [Allowed List] と [Disallowed List] に自動的に読み込まれます。 （注） 許可 MAC アドレスの形式を表示するには、[*Upload a file for Location MAC Filtering*] フィールドの横にある赤色の疑問符をクリックします。 **1.** 個々の MAC アドレスを追加するには、MAC アドレス（形式：xx:xx:xx:xx:xx:xx）を入力して [Allow] または [Disallow] をクリックします。該当する列にアドレスが表示されます。 （注） [Allow] 列と [Disallow] 列の間でアドレスを移動するには、MAC アドレス項目を選択し、該当する列の下にあるボタンをクリックします。 （注） 複数のアドレスを移動するには、1 番めの MAC アドレスをクリックし、Ctrl キーを押しながら他の MAC アドレスを選択します。追加先の列に基づいて [Allow] または [Disallow] をクリックします。 （注） MAC アドレスが [Allow] 列と [Disallow] 列のいずれにもリストされていない場合、デフォルトでは [Blocked MACs] 列に表示されます。[Unblock] ボタンをクリックすると、MAC アドレスは自動的に [Allow] 列に移動します。[Disallow] 列に移動するには、[Allow] 列の下にある [Disallow] ボタンを選択します。

ステップ 5 [保存（Save）] をクリックし、MSE データベースに新しい設定を保存します。

クライアント ステーション、不正クライアント、およびアセット タグの履歴情報を保存するための設定

Prime Infrastructure を使用して、クライアント ステーション、不正クライアント、およびアセット タグに関する履歴の保存（アーカイブ）期間を指定できます。履歴は、モビリティ サービスに関連付けられているコントローラから受信します。

また、ハード ドライブに保存するデータの量を削減するため、履歴ファイルから重複データを定期的に削除（プルーニング）するようにモビリティ サービスをプログラミングできます。

Mobility Services Engine の履歴設定を設定するには、次の手順に従います。

ステップ 1 **[サービス（Services）]>[モビリティ サービス（Mobility Services）]>[モビリティ サービス エンジン（Mobility Services Engines）]** の順に選択します。

ステップ 2 プロパティを編集するモビリティ サービスの名前をクリックします。

ステップ 3 左側のサイドバーのメニューから **[コンテキスト認識型サービス（Context Aware Service）] > [履歴パラメータ（History Parameters）]** を選択します。

ステップ 4 次に示す履歴パラメータを適切に変更します（次の表を参照）。

表 83 : History Parameters

フィールド	説明
Archive for	ロケーション アプライアンスで有効な各カテゴリの履歴を維持する日数を入力します。デフォルト値は 30 です。有効値は 1 ～ 99999 です。
Prune data starting at	ロケーション アプライアンスがデータ プルーニングを開始する時刻（時間と分）を入力します（時間は 0 ～ 23、分は 1 ～ 59）。 データ プルーニングを再び開始するまでの間隔を入力します（0 ～ 99900000、0 はプルーニングを実行しないことを意味します）。デフォルトの開始時刻は 23 時間 50 分、デフォルトの間隔は 1440 分です。
Enable History Logging of Location Transitions for	ロケーション遷移の履歴ロギングを有効にするには、次に示す項目を 1 つ以上選択します。 • Client Stations • Wired Stations • Asset Tags • Rogue Clients • Rogue Access Points • Interferers （注） モビリティ サービスがコントローラからアセット タグ データを収集する前に、CLI コマンド **config rfid status enable** を使用して、RFID タグの検出を有効にする必要があります。

ステップ 5 [保存（Save）] をクリックして、選択内容をロケーション アプライアンス データベースに保存します。

ロケーション情報を強化するための MSE ロケーション プレゼンスの有効化

MSE でロケーション表示を有効にすると、シスコのデフォルト設定（キャンパス、ビルディング、フロア、XY 座標）以外の拡張都市ロケーション情報（市町村、州、郵便番号、国）および GEO ロケーション情報（経度、緯度）を表示できます。ワイヤレス クライアントと有線クライアントは、ロケーションベースのサービスとアプリケーションで使用するためにオンデマンド ベースでこの情報を要求できます。

また、拡張ロケーション情報（有線クライアントの MAC アドレス、有線クライアントが接続している有線スイッチのスロットおよびポートなど）をインポートできます。

新しいキャンパス、ビルディング、フロア、または屋外領域が後で追加または設定されるときに、ロケーション表示を設定できます。

有効にすると、MSE はロケーションを要求する Cisco CX v5 クライアントに対してそのロケーションを提供できます。

（注） この機能を有効にする前に、MSE を同期化します。

MSE でロケーション表示を有効化および設定するには、次の手順に従います。

ステップ 1 **[サービス（Services）] > [モビリティサービス（Mobility Services）] > [モビリティサービスエンジン（Mobility Services Engines）]** の順に選択します。

ステップ 2 キャンパス、ビルディング、またはフロアが割り当てられている MSE を選択します。

ステップ 3 左側のサイドバーのメニューから、**[コンテキスト認識型サービス（Context Aware Services）] > [管理（Administration）] > [表示パラメータ（Presence Parameters）]** を選択します。

ステップ 4 [Service Type On Demand] チェックボックスをオンにし、Cisco CX クライアント v5 のロケーション表示を有効にします。

ステップ 5 次のロケーション解決オプションのいずれかを選択します。

a) [Building] を選択した場合、MSE は要求クライアントに対して、ビルディングによってその位置を示します。

たとえば、Building A に配置されているクライアントがその位置を要求している場合、MSE は *Building A* というクライアント アドレスを返します。

b) [AP] を選択すると、MSE は要求クライアントに対して、アソシエートされたアクセス ポイントによってその位置を示します。アクセス ポイントの MAC アドレスが表示されます。

たとえば、クライアントがその位置を要求しており、そのクライアントが MAC アドレス 3034:00hh:0adg のアクセス ポイントにアソシエートされている場合、MSE はクライアントにアドレス *3034:00hh:0adg* を返します。

c) [X,Y] が選択されている場合、MSE は要求クライアントに対し、そのクライアントのロケーションを XY 座標で示します。

たとえば、（50, 200）に位置しているクライアントがそのロケーションを要求している場合、MSE はクライアントにアドレス *50, 200* を返します。

ステップ 6 必要なロケーション形式のチェックボックスをオンにします。

a) [Cisco] チェックボックスをオンにすると、ロケーションがキャンパス、ビルディング、フロア、および XY 座標で示されます。デフォルト設定

b) [Civic] チェックボックスをオンにすると、キャンパス、ビルディング、フロア、または屋外領域の名前とアドレス（通り、市、州、郵便番号、国）が示されます。

c) [GEO] チェックボックスをオンにすると、緯度と経度による座標が示されます。

ステップ 7 デフォルトでは、[Location Response Encoding] チェックボックスはオンになっています。これは、クライアントが受信する情報の形式を示しています。この設定を変更する必要はありません。

ステップ 8 受信側クライアントが受信した情報を別の相手へ再送信できるようにするには、[Retransmission Rule] チェックボックスをオンにします。

ステップ 9 [Retention Expiration] 値を分単位で入力します。これにより、クライアントで格納される受信情報が上書きされるまでの時間を決定します。デフォルト値は 24 時間（1440 分）です。

ステップ 10 **[保存（Save）]** をクリックします。

MSE への MSE アセット、チョークポイント、TDOA レシーバ情報のインポートとエクスポート

Prime Infrastructure を使用して MSE のアセット、チェックポイント、および TDOA レシーバ情報をインポートするには、次の手順を実行します。

ステップ 1 **[サービス（Services）] > [モビリティサービス（Mobility Services）] > [モビリティサービスエンジン（Mobility Services Engines）]** の順に選択します。

ステップ 2 MSE の情報をインポートするには、次の手順を実行します。

a) 情報をインポートする MSE の名前をクリックします。

b) [コンテキスト認識型サービス（Context Aware Service）] > [管理（Administration）] > [アセット情報のインポート（Import Asset Information）] を選択します。

c) テキスト ファイル名を入力するか、ファイル名を参照して選択します。

インポート ファイルの情報を次の形式で指定します。

- タグ形式 : # タグ、00:00:00:00:00:00、カテゴリ名、グループ名、アセット名
- ステーション形式 : # ステーション、00:00:00:00:00:00、カテゴリ名、グループ名、アセット名

d) インポート ファイル名が [Browse] テキストボックスに表示されたら、[Import] をクリックします。

ステップ 3 Prime Infrastructure を使用してアセット、チェックポイント、および TDOA レシーバ情報を MSE からファイルにエクスポートするには、次の手順に従います。

a) 情報をエクスポートする MSE の名前をクリックします。

b) **[コンテキスト認識型サービス（Context Aware Services）] > [管理（Administration）] > [アセット情報のエクスポート（Export Asset Information）]** を選択します。

エクスポート ファイルの情報を次の形式で指定します。

- タグ形式 : # タグ、00:00:00:00:00:00、カテゴリ名、グループ名、アセット名
- ステーション形式 : # ステーション、00:00:00:00:00:00、カテゴリ名、グループ名、アセット名

c) [エクスポート（Export）] をクリックします。

画面に表示するには [開く（Open）] を、外部 PC またはサーバに保存するには [保存（Save）] を、要求を取り消すには [キャンセル（Cancel）] をクリックします。

[Save] を選択すると、アセットファイルの保存先とアセットファイル名を選択するよう求められます。デフォルトのファイル名は *assets.out* です。ダウンロードが完了したら、ダイアログボックスの [Close] をクリックします。

MSE への都市アドレス情報のインポート

Prime Infrastructure を使用して MSE の都市情報をインポートするには、次の手順に従います。

ステップ 1 **[サービス（Services）] > [モビリティサービス（Mobility Services）] > [モビリティサービスエンジン（Mobility Services Engines）]** の順に選択します。

ステップ 2 アセット情報をインポートする MSE の名前をクリックします。

ステップ 3 左側のサイドバー メニューから、[Context Aware Software] を選択します。

ステップ 4 左側のサイドバー メニューの [Administration] から、[Import Civic Information] を選択します。

ステップ 5 テキスト ファイル名を入力するか、ファイル名を参照して選択します。

インポート ファイルの情報は、次のいずれかの形式でなければなりません。

スイッチ IP アドレス、スロット番号、ポート番号、拡張親都市アドレス、X、Y、フロア ID、ビルディング ID、ネットワーク設計 ID、ELIN:"ELIN"、PIDF-Lo-Tag:"Civic Address Element Value"

各エントリをそれぞれ個別の行に指定する必要があります。

ステップ 6 [Import] をクリックします。

MSEと同期されている有線スイッチおよびクライアントに関する詳細の表示

ここでは、[コンテキスト認識型サービス（Context Aware Service）] > [有線（Wired）] ドロップダウン リストのパラメータについて説明します。

MSE と同期される有線スイッチの表示（CAS）

有線スイッチの詳細情報（IP アドレス、MAC アドレス、シリアル番号、ソフトウェア バージョン、ELIN）と、有線スイッチのポート、有線クライアント（カウントとステータス）、および都市情報についての詳細を確認できます。

（[サービス（Services）] > [サービスの同期（Synchronize Services）] > [スイッチ（Switches）] で）イーサネット スイッチと MSE が同期されると、Prime Infrastructure を介して有線スイッチ データが MSE にダウンロードされます。ロケーション対応スイッチと MSE は、NMSP 経由で通信します。Prime Infrastructure および MSE は XML で通信します。

有線スイッチの詳細を表示するには、次の手順に従います。

ステップ 1 **[サービス（Services）]>[モビリティサービス（Mobility Services）]>[モビリティサービスエンジン（Mobility Services Engines）]** の順に選択します。

ステップ 2 該当する有線ロケーション スイッチのデバイス名リンクをクリックします。

ステップ 3 **[コンテキスト認識型サービス（Context Aware Service）] > [有線（Wired）] > [有線スイッチ（Wired Switches）]** を選択します。MSE と同期された有線スイッチの概要が表示されます。

ステップ 4 該当する有線スイッチの IP アドレス リンクをクリックします。[Wired Switch Details] ページが表示されます。

[Wired Switch Details] ページには、[Switch Information]、[Switch Ports]、[Civic]、および [Advanced] の 4 つのタブがあります。

スイッチから都市情報をエクスポートするには、[Select a command] ドロップダウン リストからそのオプションを選択します。このオプションは、[Wired Switches] ページの 4 つのダッシュレットすべてで使用可能です。

[Wired Switch Details] のタブには次の情報が表示されます。

- [Switch Information]：スイッチに接続している有線クライアントの合計数の要約とクライアントの状態（接続、未接続、不明）が表示されます。
  - [Connected clients]：有線スイッチに接続しているクライアント。
  - [Disconnected clients]：有線スイッチから接続が解除されたクライアント。
  - [Unknown clients]：有線スイッチとの NMSP 接続が失われた時点で、クライアントは不明としてマークされます。

有線クライアントの詳細情報を表示するには、クライアント カウント リンク（合計クライアント数、接続、未接続、不明）のいずれかをクリックします。詳細については、MSE と同期される有線クライアントの表示（CAS） （1052 ページ）を参照してください。

- [Switch Ports]：スイッチのポートの詳細なリストを表示します。

ポート IP アドレス、スロット番号、モジュール番号、ポート タイプ、ポート番号のリストの順序（昇順、降順）を変更できます。変更するには、該当する列見出しをクリックします。

- [Civic]：有線スイッチの都市情報の詳細なリストを表示します。
- [Advanced]：有線スイッチの追加都市情報の詳細なリストを表示します。

MSE と同期される有線クライアントの表示（CAS）

有線クライアントの詳細情報（MAC アドレス、IP アドレス、ユーザ名、シリアル番号、UDI、モデル番号、ソフトウェア バージョン、VLAN ID）、ポートの関連付け、都市情報を表示することができます。

（[サービス（Services）] > [サービスの同期（Synchronize Services）] > [スイッチ（Switches）] で）スイッチと MSE が同期されると、Cisco Prime Infrastructure を介して有線クライアント データが MSE にダウンロードされます。

Cisco Prime Infrastructure と MSE は XML を介して通信します。

有線クライアントの詳細は、有線スイッチのページ（[Context Aware Service] > [Wired] > [Wired Switches]）または有線クライアントのページ（[Context Aware Service] > [Wired] > [Wired Clients]）に表示されます。

- IP アドレス、MAC アドレス、VLAN ID、シリアル番号、またはユーザ名が判明している場合は、有線クライアントのページの検索フィールドを使用できます。
- 特定のスイッチに関連する有線クライアントを調べるには、有線スイッチのページでその情報を確認できます。詳細については、MSE と同期される有線スイッチの表示（CAS）（1051 ページ）を参照してください。

有線クライアントの詳細情報を表示するには、次の手順に従います。

ステップ 1 **[サービス（Services）] > [モビリティサービス（Mobility Services）] > [モビリティサービスエンジン（Mobility Services Engines）]** の順に選択します。

ステップ 2 該当する MSE のデバイス名リンクをクリックします。

ステップ 3 **[コンテキスト認識型サービス（Context Aware Service）] > [有線（Wired）] > [有線クライアント（Wired Clients）]** を選択します。

[Wired Clients] 要約ページでは、クライアントがスイッチ別にグループ化されています。

クライアント ステータスは接続、未接続、不明として示されます。

- [Connected clients]：有線スイッチに接続しているアクティブなクライアント。
- [Disconnected clients]：有線スイッチから接続が解除されたクライアント。
- [Unknown clients]：有線スイッチとの NMSP 接続が失われた時点で、不明としてマークされたクライアント。NMSP 接続の詳細については、コントローラと MSE 間の接続ステータスのモニタ（1032 ページ）を参照してください。

有線クライアントの MAC アドレスがわかっている場合は、そのリンクをクリックしてクライアントの詳細ページを表示するか、または検索フィールドを使用することができます。

有線クライアントを IP アドレス、ユーザ名、または VLAN ID で検索することもできます。

スイッチの IP アドレスをクリックすると、スイッチの詳細ページが表示されます。詳細については、MSE と同期される有線スイッチの表示（CAS）（1051 ページ）を参照してください。

ステップ 4 該当する有線クライアントの MAC アドレス リンクをクリックします。[Wired Client Details] ページが表示されます。

[Wired Client Details] ページには、[Device Information]、[Port Association]、[Civic Address]、および [Advanced] の 4 つのタブがあります。

[Wired Switch Details] のタブには次の情報が表示されます。

- [Device Information]：MAC アドレス、IP アドレス、ユーザ名、シリアル番号、モデル番号、UDI、ソフトウェア バージョン、VLAN ID、および VLAN 名が表示されます。

- [Port Association]：有線クライアントが終端するスイッチポート、スロット、またはモジュールの物理的なロケーション、クライアントのステータス（接続、未接続、不明）、およびスイッチ IP アドレスが表示されます。
- [Civic Address]：都市アドレス情報が表示されます。
- [Advanced]：有線クライアントの拡張物理アドレス詳細情報が表示されます（該当する場合）。

クライアントは、クライアントが終端するポートに対して設定されている都市アドレス情報と拡張ロケーション情報を使用します。ポート（ポート、スロット、モジュール）に対して都市情報と拡張情報が定義されていない場合、ロケーション データは表示されません。

サードパーティ（ノースバウンド）アプリケーションにタグ通知を送信するための MSE CAS の設定

ノースバウンド通知により、MSE がサードパーティ アプリケーションに送信するタグ通知が定義されます。

ノースバウンド パラメータを設定するには、次の手順に従います。

ステップ 1 **[サービス（Services）] > [モビリティ サービス（Mobility Services）] > [モビリティ サービス エンジン（Mobility Services Engines）]** を選択します。

ステップ 2 設定する MSE の名前をクリックします。

ステップ 3 **[コンテキスト認識型サービス（Context Aware Service）] > [詳細（Advanced）] > [通知パラメータ（Notification Parameters）]** を選択して、設定オプションを表示します。

ステップ 4 [ノースバウンド通知を有効にする（Enable Northbound Notifications）] チェックボックスをオンにし、この機能を有効にします。

ステップ 5 通知をサードパーティ アプリケーションに送信（ノースバウンド）するには、[通知コンテンツ（Notification Contents）] チェックボックスをオンにします。

ステップ 6 1 つ以上の [通知コンテンツ（Notification Contents）] チェックボックスをオンにします。

ステップ 7 [通知トリガー（Notification Triggers）] チェックボックスをオンにします。

ステップ 8 1 つ以上の [通知トリガー（Notification Triggers）] チェックボックスをオンにします。

ステップ 9 ノースバウンド通知を受信するシステムの IP アドレスまたはホスト名およびポートを入力します。

ステップ 10 ドロップダウン リストからトランスポート タイプを選択します。

ステップ 11 宛先システムに安全にアクセスするために HTTPS プロトコルを使用する場合は、[HTTPS] チェックボックスをオンにします。

ステップ 12 通知パラメータの設定を変更するには、このページの [Advanced] タブの該当するテキスト ボックスに新しい値を入力します。次の表を参照してください。

表 *84 :* ユーザが設定可能な条件付き通知とノースバウンド通知のフィールド

フィールド	設定オプション
Rate Limit	MSEが通知を生成するレートをミリ秒単位で入力します。値0（デフォルト）を指定すると、MSE は可能な限り迅速に通知を生成します（ノースバウンド通知のみ）。
Queue Limit	通知送信のイベント キュー制限を入力します。MSE は、この制限を超過するイベントをすべてドロップします。
Retry Count	リフレッシュ時間の終わりまでにイベント通知を生成する回数を入力します。このパラメータは非同期トランスポートタイプの場合にだけ使用されます。非同期トランスポート タイプでは通知受信が確認されないため、通知が送信中に失われる可能性があります。デフォルト値は 1 です。 （注） MSE データベースにイベントが保存されません。
Refresh Time	通知を再送信するまで待機する必要がある時間を分単位で入力します。たとえば、In Coverage Area 通知の対象としてデバイスが設定されており、このデバイスがカバレッジ エリア内で頻繁に検出されるとします。この通知は、リフレッシュ時間ごとに 1 回送信されます。デフォルト値は 0 分です。
Drop Oldest Entry on Queue Overflow	（読み取り専用）。起動時以降にキューからドロップされたイベント通知の数。
Serialize Events per Mac address per Destination	同じ MAC アドレスの連続するイベントを、連続して 1 つの宛先に送信するには、このオプションを選択します。

ステップ 13 **[保存（Save）]** をクリックします。

MSE CAS ロケーション パラメータの設定

Prime Infrastructure を使用して、モビリティ サービスで計算回数を維持するかどうかと、モビリティ サービスが収集したレシーバ信号強度インジケータ（RSSI）の測定回数を削除するまでの期間を指定できます。要素のロケーション移動を管理するため、さまざまなスムージング レートを適用できます。

ロケーション パラメータを設定するには、次の手順に従います。

ステップ 1 **[サービス（Services）]** > **[モビリティサービス（Mobility Services）]** > **[モビリティサービスエンジン（Mobility Services Engines）]** の順に選択します。

ステップ 2 プロパティを編集するモビリティ サービスの名前をクリックします。

ステップ 3 左側のサイドバーのメニューから、**[コンテキスト認識型サービス（Context Aware Service）]** > **[ロケーション パラメータ（Location Parameters）]** を選択します。

ステップ 4 必要に応じて、ロケーション パラメータを変更します（『*Cisco Prime Infrastructure 3.2 Reference Guide*』を参照）。

ステップ 5 [保存（Save）] をクリックし、選択内容を Prime Infrastructure およびモビリティ サービスのデータベースに保存します。

MSE CAS イベント通知の設定

Prime Infrastructure を使用して、MSE のイベント通知パラメータを設定できます。これらのパラメータで MSE による通知の生成または再送信の頻度などの項目を定義します。

通知パラメータを変更するのは、MSE が大量の通知を送信する場合、または通知を受信しない場合だけにしてください。

タグのノースバウンド通知をサードパーティ アプリケーションに転送できるようにも設定できます。

MSE が送信するノースバウンド通知の形式は、次の URL のシスコ開発者向けサポート ポータルで参照できます。

http://www.cisco.com/en/US/products/svcs/ps3034/ps5408/ps5418/serv_home.html

通知パラメータを設定するには、次の手順に従います。

ステップ 1 **[サービス（Services）] > [モビリティサービス（Mobility Services）] > [モビリティサービスエンジン（Mobility Services Engines）]** の順に選択します。

ステップ 2 設定する MSE の名前をクリックします。

ステップ 3 [Context Aware Software] メニューの [Advanced] サブヘッダーから [Notification Parameters] を選択します。設定オプションが表示されます。

ステップ 4 [Enable Northbound Notifications] チェックボックスをオンにし、この機能を有効にします。

ステップ 5 通知をサードパーティアプリケーションに送信するため（ノースバウンド）、[Notification Contents] チェックボックスをオンにします。

ステップ 6 通知コンテンツ オプションを 1 つ以上選択します。

ステップ 7 [Notification Triggers] チェックボックスをオンにします。

ステップ 8 通知トリガー オプションを 1 つ以上選択します。

ステップ 9 ノースバウンド通知を受信するシステムの IP アドレスとポートを入力します。

ステップ 10 ドロップダウン リストからトランスポート タイプを選択します。

ステップ 11 宛先システムに安全にアクセスするために HTTPS プロトコルを使用する場合は、[HTTPS] を選択します。

ステップ 12 通知パラメータの設定を変更するには、このページの [Advanced] タブの該当するテキスト ボックスに新しい値を入力します。（『*Cisco Prime Infrastructure 3.2 Reference Guide*』を参照。）

ステップ 13 **[保存（Save）]** をクリックします。

MSE のコンテキスト認識型パートナーとタグ エンジン ステータスの表示

[パートナーエンジンステータス（Partner Engine Status）] ページにアクセスするには、**[サービス（Services）] > [モビリティサービス（Mobility Services）] > [モビリティサービスエンジン（Mobility Services Engines）]** > [MSE名（MSE Name）] > [コンテキスト認識型サービス（Context Aware Service）] > [パートナーエンジン（Partner Engine）] > [ステータス（Status）] の順に選択します。

タグ ライセンスが使用可能な場合は、Aeroscout Tag Engine が有効になっています。または、デフォルトで Cisco Partner Engine が有効になっています。

評価ライセンスだけが使用可能な場合は、デフォルトで Cisco Partner Engine が有効になっています。Partner Engine のステータス ページでは、Partner Engine が Aeroscout Tag Engine または Cisco Tag Engine のいずれであるかに基づいてステータスが表示されます。『*Cisco Prime Infrastructure 3.2 Reference Guide*』を選択してください。

（注） Cisco Prime Infrastructure マップ名に特殊文字（「&」など）が含まれていると、Aeroscout エンジンは MSE で開始できません。

MSE によって送信される通知の表示（CAS）

通知の概要を表示するには、**[サービス（Services）] > [モビリティサービス（Mobility Services）] > [コンテキスト認識型サービス（Context Aware Service）] > [通知の概要（Notification Summary）]** の順に選択します。

モビリティ サービスはイベント通知を送信しますが、保存しません（ファイア アンド フォーゲット）。ただし、通知イベントの宛先が Cisco Prime Infrastructure の場合は、受信した通知を保存し、次に示す 7 つのカテゴリに分類します。

- [Absence (Missing)]：Mobility Services Engine が、指定された時間内に WLAN 上のアセットを認識できない場合に生成されます。
- [Location Change Events]：クライアント ステーション、アセット タグ、不正クライアント、および不正アクセスポイントが前のロケーションから移動した場合に生成されます。
- [Chokepoint Notifications]：チョークポイントによってタグが確認（スティミュレート）されたときに生成されます。この情報は、CCX v.1 準拠のタグについてのみ、報告および表示されます。
- [Battery Level]：追跡対象のアセット タグが指定した電池残量になったときに生成されます。
- [In/Out Area]：アセットが指定エリア内外に移動したときに生成されます。

Cisco Prime Infrastructure の [マップ（Maps）] セクションで Containment 領域（キャンパス、ビルディング、またはフロア）を定義します。カバレッジエリアを定義するには、Map Editor を使用します。

- [Movement from Marker]：マップ上に定義する指定マーカーから指定の距離を超えてアセットが移動したときに生成されます。

- [Emergency]：タグのパニック ボタンが生成されたか、タグが削除、改ざん、非アクティブになった、または不明な状態が報告されたときに、CCX v.1 準拠のアセット タグについて生成されます。この情報は、CCX v.1 準拠のタグについてのみ、報告および表示されます。

概要の詳細には、次の情報が含まれます。

- All Notifications
- Client Stations
- Asset Tags
- Rogue Clients
- Rogue Access Points

各通知の詳細を表示するには、[Last Hour]、[Last 24 Hours]、または [Total Active] 列の数値をクリックし、該当する通知の詳細ページを開きます。

MSE 通知のクリア方法（CAS）

モビリティ サービスでは、次のいずれかの状況でイベント条件をクリアしたときに、イベント通知を送信します。

- [Missing (Absence)]：要素が再び表示される。
- [In/Out Area (Containment)]：要素が封じ込むエリア内に戻るか、このエリアから外に出る。
- [Distance]：要素がマーカーから指定された距離以内に戻る。
- [Location Changes]：クリアの状態はこの条件には適用されません。
- [Battery Level]：普通の電池残量で動作しているタグが再検出される。
- Emergency
- Chokepoint

Cisco Prime Infrastructure で、[通知の概要（Notifications Summary）] ページには、クリアされたイベント条件の通知が受信されたかどうかが反映されます。

MSE 通知に関する現在の定義の表示（CAS）

通知の定義を表示するには、**[サービス（Services）] > [モビリティ サービス（Mobility Services）] > [コンテキスト認識型通知（Context Aware Notifications）] > [通知定義（Notifications Definition）]** の順に選択します。このページのグループにイベント グループおよびイベント定義を追加できます。どのグループも、イベント通知を編成するのに役立ちます。イベント定義は、特定のグループに属さなければなりません。

イベント グループおよびイベント定義の追加の詳細については、MSE 通知に関するイベント グループの設定（1061 ページ）およびイベント グループへの MSE イベント定義の追加（1065 ページ）を参照してください。

イベント グループおよびイベント定義を追加した後でのみ、[Notification Definition] ページに次のパラメータが表示されます。

次の表は、[通知定義（Notification Definition）] ページのフィールドのリストおよび説明を示しています。

表 *85 : [Notification Definition]* ページ

フィールド	説明
Group Name	イベント定義を追加する先のグループの名前。
Event Definitions	イベント グループの既存のイベント定義。
Created On	イベント グループの作成日。

特定の MSE に関する通知統計情報の表示（CAS）

特定の MSE の通知統計情報を表示できます。特定の MSE の通知統計情報を表示するには、**[サービス（Services）]** > **[モビリティサービス（Mobility Services）]** > [MSE-name] > **[コンテキスト認識型サービス（Context Aware Service）]** > **[通知統計情報（Notification Statistics）]** の順に選択します（[MSE-name] は MSE の名前）。

次の表は、[通知統計情報（Notification statistics）] ページのフィールドのリストおよび説明を示しています。

表 *86 : [*通知統計情報（*Notification Statistics*）*]* のフィールド

フィールド	説明
要約	
Destinations	
Total	宛先の合計数。
Unreachable	到達不能な宛先の数。
Notification Statistics Summary	
Track Definition Status	トラック定義のステータス。トラック通知ステータスは [Enabled] または [Disabled] のいずれかです。
Track Definition	トラック定義は、Northbound または CAS イベント通知です。
Destination IP Address	通知送信先の宛先 IP アドレス。
宛先ポート	通知送信先の宛先ポート。
Destination Type	宛先のタイプ。たとえば、SOAP_XML です
Destination Status	宛先デバイスのステータス。ステータスは [Up] または [Down] です。
Last Sent	最終通知が宛先デバイスに送信された日時。
Last Failed	通知に失敗した日時。

フィールド	説明
Total Count	宛先に送信された通知の合計数。宛先デバイスの通知統計詳細情報を表示するには、カウント リンクをクリックします。

MSE モバイル コンシェルジュ アドバタイズメントの表示

設定済みのサービス アドバタイズメントを表示するには、次の手順に従います。

ステップ 1 **[サービス（Services）]** > **[モビリティサービス（Mobility Services）]** > **[モビリティサービスエンジン（Mobility Services Engines）]** の順に選択します。

ステップ 2 [Device Name] をクリックして、そのプロパティを表示します。

ステップ 3 左側のサイドバーのメニューから、**[モバイル コンシェルジュ サービス（Mobile Concierge Service）]** > **[アドバタイズメント（Advertisements）]** を選択します。

[Mobile Concierge Service] ページに次の情報が表示されます。

- [Icon]：サービス プロバイダーに関連付けられたアイコンを表示します。
- [Provide Name]：サービス プロバイダー名を表示します。
- [Venue Name]：場所の名前を表示します。
- Advertisements
  - [Friendly Name]：ヘッドセットに表示されるわかりやすい名前。
  - [Advertisement Type]：ヘッドセットに表示されるアドバタイズメントのタイプ。

MSE モバイル コンシェルジュ統計情報の表示

モバイル コンシェルジュ サービスの統計情報を表示するには、次の手順に従います。

ステップ 1 **[サービス（Services）]** > **[モビリティサービス（Mobility Services）]** > **[モビリティサービスエンジン（Mobility Services Engines）]** の順に選択します。

ステップ 2 [Device Name] をクリックして、そのプロパティを表示します。

ステップ 3 左側のサイドバーのメニューから **[モバイル コンシェルジュ サービス（Mobile Concierge service）]** > **[統計情報（Statistics）]** を選択します。

[モバイル コンシェルジュ サービス（Mobile Concierge Service）] ページに次の情報が表示されます。

- [Top 5 Active Mobile MAC addresses]：特定の場所で最もアクティブなモバイルについての情報を表示します。

- [Top 5 Service URIs]：特定の場所またはプロバイダー上でサービスの使用量についての情報を表示します。

MSE イベント グループとは

イベントをより効率的に管理するために、Cisco Prime Infrastructure を使用してイベント グループを作成できます。イベント グループを使用すると、イベント定義を編成しやすくなります。

MSE 通知に関するイベント グループの設定

イベント グループを追加するには、次の手順に従います。

手順の概要

1. **[サービス（Services）] > [モビリティ サービス（Mobility Services）] > [コンテキスト認識型通知（Context Aware Notifications）]** の順に選択します。
2. 左側のサイドバーのメニューから [Notification Definitions] を選択します。
3. [Select a command] ドロップダウン リストから、[Add Event Group] を選択します。
4. [Go] をクリックします。
5. [Group Name] テキストボックスにグループ名を入力します。
6. [Save] をクリックします。

手順の詳細

ステップ 1 **[サービス（Services）] > [モビリティ サービス（Mobility Services）] > [コンテキスト認識型通知（Context Aware Notifications）]** の順に選択します。

ステップ 2 左側のサイドバーのメニューから [Notification Definitions] を選択します。

ステップ 3 [Select a command] ドロップダウン リストから、[Add Event Group] を選択します。

ステップ 4 [Go] をクリックします。

ステップ 5 [Group Name] テキストボックスにグループ名を入力します。

ステップ 6 [Save] をクリックします。

[Event Settings] ページに新しいイベント グループが表示されます。

MSE 通知に関するイベント グループの削除

イベント グループを削除するには、次の手順に従います。

ステップ 1 **[サービス（Services）] > [モビリティサービス（Mobility Services）] > [コンテキスト認識型通知（Context Aware Notifications）]** の順に選択します。

ステップ 2 左側のサイドバーのメニューから [Notification Definitions] を選択します。

ステップ 3 削除するイベント グループのチェックボックスをオンにします。

ステップ 4 [Select a command] ドロップダウン リストから、[Delete Event Group(s)] を選択します。

ステップ 5 [Go] をクリックします。

ステップ 6 [OK] をクリックして、削除を実行します。

ステップ 7 **[保存（Save）]** をクリックします。

新しい MSE イベントの設定（イベント定義）

イベント定義には、イベントを発生させた条件、イベントが適用されるアセット、イベント通知の宛先に関する情報が含まれます。この項では、イベント定義の追加、削除、およびテストの方法について説明します。

Prime Infrastructure では、グループ単位に定義を追加できます。新しいイベント定義はいずれも、特定のグループに属さなれければなりません。

イベント定義を追加するには、次の手順を実行します。

ステップ 1 **[サービス（Services）] > [モビリティサービス（Mobility Services）] > [コンテキスト認識型通知（Context Aware Notifications）]** の順に選択します。

ステップ 2 左側のサイドバーのメニューから、[Notification Definitions] を選択します。

ステップ 3 イベントを追加するグループの名前をクリックします。選択したイベント グループのイベント定義の概要ページが表示されます。

ステップ 4 [Select a command] ドロップダウン リストから、[Add Event Definition] を選択します。

ステップ 5 [Go] をクリックします。

ステップ 6 [Event Definition Name] テキスト ボックスにイベント定義の名前を入力します。

イベント定義名は、イベント グループ内で一意である必要があります。

ステップ 7 [Save] をクリックします。

ステップ 8 [General] タブで、次のパラメータを管理します。

- [Admin Status]：[Enabled] チェックボックスをオンにして、イベントの生成を有効にします（デフォルトは無効）。
- [Priority]：ドロップダウン リストから数値を選択して、イベントの優先順位を設定します。ゼロが最も高い優先順位です。
- 優先順位の高いイベント定義は、優先順位の低いイベント定義よりも先に処理されます。

- [Activate]：継続してイベントをレポートするには [All the Time] チェックボックスを選択します。アクティベーションを特定の日時に指定するには、[All the Time] チェックボックスをオフにし、適用する日付および開始時刻と終了時刻を選択します。[Save] をクリックします。

ステップ 9 [Conditions] タブで、1 つ以上の条件を追加します。条件ごとに、イベント通知を生成するためのルールを指定します。条件を追加するには、次の手順を実行します。

a) [Add] をクリックして、[Add/Edit Condition] ページを開きます。

b) [条件タイプ（Condition Type）] ドロップダウン リストから条件タイプを選択し、それに関連付ける [トリガー条件（Trigger If）] パラメータを設定します（次の表を参照）。

表 *87 : [*条件タイプ（*Condition Type***）*]/[*トリガー条件（***Trigger If***）*] *パラメータ***

Condition Type	Trigger If
Missing	[Missing for Time (mins)]：不明なアセット イベントが生成されてから経過した時間（分）を入力します。 たとえば、このテキスト ボックスに 10 と入力した場合、MSE は、10 分経過してもアセットが見つからないときに、不明なアセット イベントを生成します。
In/Out	[Inside of] または [Outside of]：[Select Area] をクリックし、[Select] ページからエリア パラメータを選択します。[Select] をクリックします。モニタするエリアは、キャンパス全体、キャンパス内のビルディング、ビルディング内のフロア、またはカバレッジ エリアになります（Map Editor を使用してカバレッジ エリアを定義できます）。
Distance	[マーカーからの *x* の距離（フィート）（In the distance of x (feet) from Marker）] テキスト ボックス：距離（フィート単位）を入力します。モニタ対象アセットが指定した距離を超えて指定マーカーから移動した場合にイベント通知がトリガーされます。[Select Marker] をクリックし、[Select] ページでマーカー パラメータを選択します。[Select] をクリックします。
Battery Level	[Battery Level Is]：Low（低）、Medium（中）、Normal（普通）。イベントを生成する適切な電池残量を選択します。
Location Change	アセットの位置が変わったときにイベントが生成されます。
緊急（Emergency）	[すべて（Any）]、[パニック ボタン（Panic Button）]、[改ざん（Tampered）]、または [削除（Detached）] チェックボックスを選択します。
Chokepoint	[In the range of Chokepoints]：[Select Chokepoint] チェックボックスをオンにし、[Select] ページでチョークポイント パラメータを選択します。[Select] をクリックします。

c) [適用先（Apply To）] ドロップダウン リストで、トリガー条件を満たしたときにイベントを生成する対象となるアセットのタイプ（[すべて（Any）]、[クライアント（Clients）]、[タグ（Tags）]、[不正アクセス ポイント（Rogue APs）]、[不正クライアント（Rogue Clients）]、または [干渉源（Interferers）]）を選択します。

d) 緊急イベントおよびチョークポイント イベントは、（CCXv.1 準拠の）タグにのみ適用できます。

e) [一致基準（Match By）] ドロップダウン リストから一致基準（[MAC アドレス（MAC Address）]、[アセット名（Asset Name）]、[アセット グループ（Asset Group）]、または [アセット カタログ（Asset

Category）]）、演算子（[等しい（Equals）] または [類似（Like）]）を選択し、選択した [一致基準（Match By）] 要素に適切なテキストを入力します。

f) [追加（Add）] をクリックします。

ステップ 10 [Destination and Transport] タブで、次の手順を実行して、イベント通知を受信する 1 つ以上の宛先を追加し、転送設定を行います。

a) [Add] をクリックして、[Add/Edit Destination and Transport] ページを開きます。

b) 1 つ以上の新しい宛先を追加するには、[Add New] をクリックし、該当する IP アドレスを入力して [OK] をクリックします。

c) 受信者のシステムのイベント リスナーが通知を処理するように動作している必要があります。イベント定義を作成する場合はデフォルトで、Prime Infrastructure により、その IP アドレスが宛先として追加されます。

d) 通知を受信する宛先を選択するには、右側のボックスで 1 つ以上の IP アドレスをクリックして強調表示させ、[Select] をクリックして、左側のボックスに IP アドレスを追加します。

e) [Message Format field] ドロップダウン リストから、[XML] または [Plain Text] を選択します。

f) Prime Infrastructure を宛先として選択する場合は、XML 形式を選択する必要があります。

g) [トランスポート タイプ（Transport Type）] ドロップダウン リストから次のいずれかの転送（トランスポート）タイプを選択します。

- [SOAP]：Simple Object Access Protocol。通知は、SOAP を使用して、HTTP/HTTPS を介して送信され、宛先の Web サービスによって処理されます。
- HTTPS を介して通知を送信するかどうかを、対応するチェックボックスをオンにして指定します。[Port Number] テキスト ボックスに宛先のポート番号を入力します。
- [メール（Mail）]：このオプションを使用すると、電子メールで通知を送信します。
- [Mail Type] ドロップダウン リストから、メールを送信するためのプロトコルを選択します。必要に応じて、ユーザ名とパスワード（認証が有効な場合）、送信者の名前、件名行に追加するプレフィックス、受信者の電子メール アドレス、およびポート番号を入力します。
- [SNMP]：Simple Network Management Protocol。このオプションを使用すると、SNMP 対応デバイスに通知を送信します。
- SNMP バージョン v2c を選択した場合は、[SNMP Community] テキスト ボックスに SNMP コミュニティ ストリングを、[Port Number] テキスト ボックスに該当するポート番号を入力するように指示されます。
- SNMP バージョン v3 を選択した場合は、ユーザ名、セキュリティ名を入力し、ドロップダウン リストから認証タイプを選択して認証パスワードを入力し、ドロップダウン リストからプライバシー タイプを選択してプライバシー パスワードを入力するように指示されます。
- [SysLog]：イベント通知の受信者である宛先システム上のシステム ログを指定します。
- [Priority] テキスト ボックスに通知の優先順位を入力し、ファシリティの名前、および宛先システムのポート番号を入力します。

h) [追加（Add）] をクリックします。

イベント グループへの MSE イベント定義の追加

イベント定義には、イベントを発生させた条件、イベントが適用されるアセット、イベント通知の宛先についての情報が含まれます。

Prime Infrastructure では、グループごとに定義を追加できます。イベント定義は、特定のグループに属さなければなりません。イベント定義を削除またはテストする方法の詳細については、『Cisco Content-Aware Software Configuration Guide』を参照してください。

イベント定義を追加するには、次の手順を実行します。

手順の概要

1. **[サービス（Services）] > [モビリティサービス（Mobility Services）] > [コンテキスト認識型通知（Context Aware Notifications）]** の順に選択します。
2. 左側のサイドバーのメニューから [Notification Definitions] を選択します。
3. イベントに追加するグループの名前をクリックします。選択したイベント グループのイベント定義の概要ページが表示されます。
4. [Select a command] ドロップダウン リストから、[Add Event Definition] を選択し、[Go] をクリックします。
5. [Conditions] タブで、1 つ以上の条件を追加します。追加する条件ごとに、イベント通知をトリガーするためのルールを指定します。
6. [Destination and Transport] タブで、次の手順を実行して、イベント通知を受信する 1 つ以上の宛先を追加し、転送設定を行います。
7. [General] タブで、次の手順を実行します。
8. イベント グループに新しいイベント通知がリストされたことを確認します（[Mobility] > [Notifications] > [Settings] > [Event Group Name]）。

手順の詳細

ステップ 1 **[サービス（Services）] > [モビリティサービス（Mobility Services）] > [コンテキスト認識型通知（Context Aware Notifications）]** の順に選択します。

ステップ 2 左側のサイドバーのメニューから [Notification Definitions] を選択します。

ステップ 3 イベントに追加するグループの名前をクリックします。選択したイベント グループのイベント定義の概要ページが表示されます。

ステップ 4 [Select a command] ドロップダウン リストから、[Add Event Definition] を選択し、[Go] をクリックします。

ステップ 5 [Conditions] タブで、1 つ以上の条件を追加します。追加する条件ごとに、イベント通知をトリガーするためのルールを指定します。

ヒント たとえば、病院で心臓モニタによる経過観察を行う場合、心臓モニタを見失ってから 1 時間経過したとき、心臓モニタがその割り当てられたフロアから移動したとき、心臓モニタがフロア内の特定のカバレッジ エリアに入ったときなどにイベント通知を生成するルールを追加します。

条件を追加するには、次の手順を実行します。

a) [Add] をクリックして、このイベントを生成する条件を追加します。
b) [Add/Edit Condition] ダイアログ ボックスで、次の手順を実行します。

1. [Condition Type] ドロップダウン リストから条件タイプを選択します。

[条件タイプ（Condition Type）] ドロップダウン リストから [見つかりません（Missing）] を選択した場合は、欠落アセット イベントが生成されるまでの経過時間（分）を入力します。たとえば、このテキスト ボックスに 10 と入力した場合、Mobility Services Engine は、10 分経過してもアセットが見つからないときに、不明なアセット イベントを生成します。手順 c に進みます。

[条件タイプ（Condition Type）] ドロップダウン リストから [内外（In/Out）] を選択した場合は、[次の内部（Inside of）] または [次の外部（Outside of）] を選択してから [エリアの選択（Select Area）] を選択し、アセットが出入りする対象エリアを選択します。[Select] ダイアログボックスで、モニタするエリアを選択し [Select] をクリックします。モニタするエリアは、キャンパス全体、キャンパス内のビルディング、ビルディング内のフロア、またはカバレッジ エリアになります（Map Editor を使用してカバレッジエリアを定義できます）。たとえば、ビルディング内のフロア部分をモニタするには、[Campus] ドロップダウン リストからキャンパスを、[Building] ドロップダウン リストからビルディングを、[Floor Area] ドロップダウン リストからモニタするエリアを選択します。次に、[Select] をクリックします。手順 c に進みます。

[条件タイプ（Condition Type）] ドロップダウン リストから [距離（Distance）] を選択した場合は、モニタ対象アセットが指定の距離を超えて指定マーカーから移動した場合にイベント通知をトリガーする距離（フィート単位）を入力し、[マーカーの選択（Select Marker）] をクリックします。[Select] ダイアログボックスで、キャンパス、ビルディング、フロア、およびマーカーを、対応するドロップダウンリストから選択し、[Select] をクリックします。たとえば、マーカーをフロア図面に追加し、トリガーに距離を設定する場合などです。テキストボックスに 60 フィートと設定した場合、モニタ対象アセットがマーカーから 60 フィートを超えて離れたときにイベント通知が生成されます。手順 c に進みます。

Map Editor を使用して、マーカーおよびカバレッジ エリアを作成できます。マーカー名を作成する場合は、システム全体で一意になるようにします。

[条件タイプ（Condition Type）] ドロップダウン リストから [電池残量（Battery Level）] を選択した場合は、イベントをトリガーする電池残量（低、中、正常）の横にあるチェックボックスをオンにします。ステップ c に進みます。

[条件タイプ（Condition Type）] ドロップダウン リストから [ロケーション変更（Location Change）] を選択した場合は、ステップ c に進みます。

[条件タイプ（Condition Type）] ドロップダウン リストから [緊急（Emergency）] を選択した場合は、イベントをトリガーする緊急事態（すべて、パニック ボタン、改ざん、削除）の横にあるボタンをクリックします。ステップ c に進みます。

[条件タイプ（Condition Type）] ドロップダウン リストから [チョークポイント（Chokepoint）] を選択した場合は、ステップ c に進みます。トリガー条件は 1 つのみ存在し、それがデフォルトで表示されます。設定は必要ありません。

c) [Apply To] ドロップダウン リストから、生成条件を満たした場合にイベントを生成するアセットのタイプ（[Any]、[Clients]、[Tags]、[Rogue APs]、[Rogue Clients]、または [Interferers]）を選択します。

[Apply to] ドロップダウン リストから [any] オプションを選択した場合は、タグ、クライアント、不正アクセス ポイント、および不正クライアントのすべてに電池の条件が適用されます。

Emergency イベントおよび Chokepoint イベントは、Cisco Compatible Extensions のタグのバージョン 1（以降）だけに適用されます。

d) [一致基準（Match By）] ドロップダウン リストから一致基準（[MAC アドレス（MAC Address）]、[アセット名（Asset Name）]、[アセット グループ（Asset Group）]、または [アセット カタログ（Asset Category）]）を、ドロップダウン リストから演算子（[等しい（Equals）] または [類似（Like）]）を選択し、選択した [一致基準（Match By）] 要素に適切なテキストを入力します。

次に、指定可能なアセットの一致基準の例をいくつか示します。

- [Match By] ドロップダウン リストから [MAC Address] を選択し、[Operator] ドロップダウン リストから [Equals] を選択して、MAC アドレス（たとえば、12:12:12:12:12:12）を入力した場合、MAC アドレスが 12:12:12:12:12:12（完全一致）の要素にイベント条件が提供されます。
- [Match By] ドロップダウン リストから [MAC Address] を選択し、[Operator] ドロップダウン リストから [Like] を選択して、**12:12** を入力した場合、MAC アドレスが 12:12 で始まる要素にイベント条件が適用されます。

e) [Add] をクリックして、定義済みの条件を追加します。

チョークポイントを定義している場合は、条件を追加した後にチョークポイントを選択する必要があります。

チョークポイントを選択するには、次の手順を実行します。

1. [Select Chokepoint] をクリックします。入力ページが表示されます。
2. [Campus]、[Building]、および [Floor] を該当するドロップダウン リストから選択します。
3. 表示されるメニューから [Chokepoint] を選択します。

[Add/Edit Condition] ページに戻ると、[Select Checkpoint] ボタンの横にあるテキスト領域にチョークポイントのロケーション パス（[Campus] > [Building] > [Floor]）が自動的に読み込まれます。

ステップ 6 [Destination and Transport] タブで、次の手順を実行して、イベント通知を受信する 1 つ以上の宛先を追加し、転送設定を行います。

a) 新しい宛先を追加する場合は、[Add] をクリックします。[Add/Edit Destination configuration] ページが表示されます。
b) [Add New] をクリックします。
c) イベント通知を受信するシステムの IP アドレスを入力し、[OK] をクリックします。
d) 受信者のシステムのイベント リスナーが通知を処理するように動作している必要があります。イベント定義を作成する場合はデフォルトで、Cisco Prime Infrastructure により、その IP アドレスが宛先として追加されます。
e) イベント通知を送信する宛先を選択する場合は、右側のボックスで 1 つ以上の IP アドレスを強調表示し、[Select] をクリックして左側のボックスに IP アドレスを追加します。
f) [XML] または [Plain Text] を選択して、メッセージ形式を指定します。
g) [トランスポート タイプ（Transport Type）] ドロップダウン リストから次のいずれかの転送（トランスポート）タイプを選択します。

- [SOAP]：イベント通知を送信するための転送タイプとして、簡易 XML プロトコルである Simple Object Access Protocol を指定します。SOAP を使用すると通知は HTTP/HTTPS を介して送信され、宛先の Web サービスによって処理されます。
- [SOAP] を選択した場合は、HTTPS を介して通知を送信するかどうかを、対応するチェックボックスをオンにして指定します。選択しない場合は HTTP が使用されます。また、[Port Number] テキスト ボックスに宛先のポート番号を入力します。
- [メール（Mail）]：このオプションを使用すると、電子メールで通知を送信します。
- [Mail] を選択した場合は、[Mail Type] ドロップダウン リストから電子メールを送信するためのプロトコルを選択する必要があります。必要に応じて、ユーザ名とパスワード（認証が有効な場合）、送信者の名前、件名行に追加するプレフィックス、受信者の電子メール アドレス、およびポート番号を入力する必要もあります。
- [SNMP]：SNMP 対応デバイスに通知を送信するために使用され、ネットワークのモニタリングに広く使用されている技術である Simple Network Management Protocol を使用します。
- [SNMP] を選択した場合は、[SNMP コミュニティ（SNMP Community）] テキスト ボックスに SNMP コミュニティ ストリングを、[ポート番号（Port Number）] テキスト ボックスに通知の送信先のポート番号を入力します。
- [SysLog]：イベント通知の受信者である宛先システム上のシステム ログを指定します。
- [SysLog] を選択した場合は、[Priority] テキスト ボックスに通知の優先順位を、[Facility] テキスト ボックスにファシリティの名前を、[Port Number] テキスト ボックスに宛先システムのポート番号を入力します。

h) HTTPS を有効にするには、その横にある [Enable] チェックボックスをオンにします。

ポート番号が自動的に読み込まれます。

i) [Save] をクリックします。

ステップ 7 [General] タブで、次の手順を実行します。

a) [Admin Status] の [Enabled] チェックボックスをオンにして、イベントの生成を有効にします（デフォルトは無効）。

b) [優先順位（Priority）] ドロップダウン リストから数値を選択して、イベントの優先度を設定します。ゼロが最も高い優先順位です。

c) 優先順位の高いイベント通知は、優先順位の低いイベント定義よりも先に処理されます。

d) イベント通知の送信頻度を選択するには、次の手順を実行します。

e) イベントを継続的に報告する場合は、[All the Time] チェックボックスをオンにします。手順 g に進みます。

f) イベント通知を送信する曜日と時刻を選択する場合は、[All the Time] チェックボックスをオフにします。曜日と時刻のフィールドが表示され、選択できるようになります。手順 d に進みます。

g) イベント通知を送信する各日の横にあるチェックボックスをオンにします。

h) [Apply From] 見出しから適切な時、分、AM/PM のオプションを選択して、イベント通知を開始する時刻を選択します。

i) [Apply Until] 見出しから適切な時、分、AM/PM のオプションを選択して、イベント通知を終了する時刻を選択します。

j) [Save] をクリックします。

ステップ 8 イベント グループに新しいイベント通知がリストされたことを確認します（[Mobility] > [Notifications] > [Settings] > [Event Group Name]）。

MSE 通知に関するイベント定義の削除

Prime Infrastructure から 1 つ以上のイベント定義を削除するには、次の手順を実行します。

ステップ 1 [Services] > [Mobility Services] > [Context Aware Notifications] の順に選択します。
ステップ 2 左側のサイドバーのメニューから、[Settings] を選択します。
ステップ 3 イベント定義を削除するグループの名前をクリックします。
ステップ 4 削除するイベント定義を、対応するチェックボックスをオンにして選択します。
ステップ 5 [Select a command] ドロップダウン リストから、[Delete Event Definition(s)] を選択します。
ステップ 6 [Go] をクリックします。
ステップ 7 [OK] をクリックして、選択したイベント定義を削除することを確認します。

特定の MSE ワイヤレス クライアントの検索（IPv6）

（注） このリリースでは、ワイヤレス クライアントだけが IPv6 アドレスを使用します。

Prime Infrastructure の [詳細検索（Advanced Search）] 機能を使用して、MSE の配置されたクライアントを検索するには、次の手順を実行します。

ステップ 1 [Advanced Search] をクリックします。
ステップ 2 [New Search] ダイアログで、[Search Category] ドロップダウン リストから検索カテゴリとして [Clients] を選択します。
ステップ 3 [Media Type] ドロップダウン リストから、[Wireless Clients] を選択します。

メディア タイプとして [Wireless Clients] を選択した場合だけ、[Wireless Type] ドロップダウン リストが表示されます。

ステップ 4 [Wireless Type] ドロップダウン リストから、[All]、[Lightweight]、または [Autonomous Clients] のうちいずれかのタイプを選択します。
ステップ 5 [Search By] ドロップダウン リストから、[IP Address] を選択します。

IP アドレスによるクライアントの検索は、IP アドレス全体または一部を対象にできます。各クライアントは、最大 16 個の IPv6 アドレスと 4 個の IPv4 アドレスを持つことができます。

ステップ 6 [Clients Detected By] ドロップダウン リストから、クライアント検出の実行を MSE として選択します。

これは、コントローラと直接通信することで、MSE の Context-Aware Service で検索したクライアントが表示されます。

ステップ 7 [Last detected within] ドロップダウン リストから、クライアントが検出された時間帯を選択します。

ステップ 8 [Client IP Address] テキスト ボックスにクライアント IP アドレスを入力します。IPv6 アドレスの一部または全体を入力できます。

IPv4 アドレスを使用して、MSE 上で Prime Infrastructure のクライアントを検索する場合は、[クライアント IP アドレス（Client IP address）] テキスト ボックスに IPv4 アドレスを入力します。

ステップ 9 [Client States] ドロップダウン リストから、クライアントの状態を選択します。ワイヤレス クライアントに指定できる値は、[All States]、[Idle]、[Authenticated]、[Associated]、[Probing]、または [Excused] です。有線クライアントに指定できる値は、[All States]、[Authenticated]、および [Associated] です。

ステップ 10 [Posture Status] ドロップダウン リストからポスチャ ステータスを選択すると、デバイスがクリーンであるかどうかを判別します。指定できる値は、**[すべて（All）]**、**[不明（unknown）]**、**[合格（Passed）]** および **[失敗（Failed）]** です。

ステップ 11 [CCX Compatible] チェックボックスをオンにすると、Cisco Client Extensions と互換性のあるクライアントを検索します。指定できる値は、[All Versions]、[V1]、[V2]、[V3]、[V4]、[V5]、および [V6] です。

ステップ 12 [E2E Compatible] チェックボックスをオンにして、エンドツーエンドの互換性のあるクライアントを検索します。指定できる値は、[All Versions]、[V1]、および [V2] です。

ステップ 13 [NAC State] チェックボックスをオンにすると、特定のネットワーク アドミッション コントロール（NAC）の状態で特定されるクライアントを検索します。指定可能な値は、[Quarantine]、[Access]、[Invalid]、および [Not Applicable] です。

ステップ 14 [関連付け解除を含む（Include Disassociated）] チェックボックスをオンにすると、ネットワーク上には存在しなくなったものの、Prime Infrastructure には履歴レコードが残っているクライアントが含まれます。

ステップ 15 [Items per page] ドロップダウン リストから、検索結果ページに表示するレコードの数を選択します。

ステップ 16 [Save Search] チェックボックスをオンにして、選択した検索オプションを保存します。

ステップ 17 [移動（Go）] をクリックします。

[クライアントおよびユーザ（Clients and Users）] ページに、MSE で検出されたすべてのクライアントが表示されます。

すべての MSE クライアントの表示

Cisco WLC で 2.4 GHz のプローブ状態にあるクライアントを確認できますが、「a」無線のみのプローブ状態にあるクライアントのみです（[モニタ（Monitor）]>[クライアントおよびユーザ（Clients and Users）]>[MSE で検出されたクライアント（Client detected by MSE）] ページ）。「b/g」無線のプローブ状態にあるクライアントは表示されません。これは、クライアントがプローブ状態にあるとき、Prime Infrastructure はプロトコルの詳細を取得せず、デフォルトでこれらが 5 GHz チャネルと表示されるためです。これらが関連付けられた後、プロトコルおよびチャネルの詳細を含む INFO メッセージがコントローラから受信されます。しかし、それらが測定メッセージでプローブしている場合、Prime Infrastructure にはこの情報がなく、デフォルトで 5 GHz に設定します。

MSE で検出されたすべてのクライアントを表示するには、次の手順を実行します。

ステップ 1 [Monitor] > [Monitoring Tools] > [Clients and Users] の順に選択して、有線クライアントとワイヤレス クライアントの両方の情報を表示します。

[Clients and Users] 表にはデフォルトでいくつかの列が表示されます。使用可能な列を追加して表示するには、330159 イメージをクリックし、[列（Columns）] をクリックします。使用可能な列が表示されます。[Clients and Users] 表に表示する列を選択します。列内の任意の場所をクリックすると、その列が選択され、クライアントの詳細が表示されます。

ステップ 2 [表示（Show）] ドロップダウン リストから [MSE で検出されたクライアント（Clients detected by MSE）] を選択すると、現在のリストをフィルタリングし、MSEによって検出されたクライアントをすべて選択できます。

有線およびワイヤレスを含め、MSE によって検出されたすべてのクライアントが表示されます。

MSEテーブルで検出したクライアントで利用可能なさまざまなパラメータの詳細については、『Cisco Prime Infrastructure 3.2 Reference Guide』を参照してください。

ステップ 3 [クライアントおよびユーザ（Client and User）] ページの MAC アドレスの横にあるオプション ボタンを選択すると、アソシエートされたクライアント情報を表示できます。

ステップ 4 特定の MSE のアラームの詳細にアクセスするには、次の手順を実行します。

a) [モニタ（Monitor ）] > [モニタリング ツール（Monitoring Tools）] > [アラームおよびイベント（Alarms and Events）] を選択し、[障害の発生源（Failure Source）] 列の MSE 項目をクリックします。

または

b) [サービス（Services）] > [モビリティ サービス エンジン（Mobility Services Engines）] > [MSE 名（MSE Name）] > [システム（System）] > [ステータス（Status）] > [Prime Infrastructure アラーム（Prime Infrastructure Alarms）] を選択し、[障害の発生源（Failure Source）] 列で特定の MSE 項目をクリックします。

[アラームの詳細（Alarm Detail）] ページのフィールドの説明については、『Cisco Prime Infrastructure 3.2 Reference Guide』を参照してください。

MSE を使用したモバイル コンシェルジュの設定

モバイル コンシェルジュ サービスにより、場所所有者とサービス プロバイダーはWLAN をモニタできます。このソリューションは、スマートフォンを使用している顧客に固有のストア内エクスペリエンスを提供します。

モバイル コンシェルジュ サービスは、ネットワーク接続を確立するための一連のポリシーを使用して設定されたワイヤレス スマート フォンを使用します。モバイル コンシェルジュ サービスにより、使用できるネットワークベース サービスをスマート フォンで簡単に検出できます。ストアの Wi-Fi ネットワークに接続した後、ストアのワイヤレス ゲスト ネットワークに

参加して、電子クーポン、プロモーション オファー、顧客ロイヤルティ データ、製品提案など、さまざまなサービスにアクセスすること、ショッピング リストを編成すること、およびショッピング設定に基づき固有のデジタル署名を受け取ることができます。

関連トピック

モバイル コンシェルジュ（MSE）の場所の設定 （1072 ページ）
モバイル コンシェルジュ（MSE）のプロバイダーの設定 （1073 ページ）
モバイル コンシェルジュ ポリシー（MSE）の設定 （1074 ページ）

モバイル コンシェルジュ（MSE）の場所の設定

場所を定義するには、次の手順に従います。

ステップ 1 **[サービス（Services）] > [モビリティ サービス（Mobility Services）] > [モバイル コンシェルジュ（Mobile Concierge）]** を選択します。

ステップ 2 左側のサイドバーのメニューから [モバイル コンシェルジュ サービス（Mobile Concierge Services）] > [場所（Venues）] を選択します。

[場所（Venues）] ページが表示されます。

ステップ 3 [コマンドの選択（Select a command）] ドロップダウン リストから [新しい場所の定義（Define New Venue）] を選択し、[実行（Go）] をクリックします。

[Venue Wizard] ページが表示されます。

ステップ 4 [Venue Name] テキスト ボックスに場所の名前を入力し、[Next] をクリックします。

ステップ 5 [Floor/Outdoor Association] グループ ボックスで、以下を設定できます。

- [Area Type] ドロップダウン リストから、サービス アドバタイズメントを表示するエリア タイプを選択します。指定できる値は、[フロア領域（Floor Area）] と [屋外領域（Outdoor Area）] です。

（注） エリア タイプとして [フロア領域（Floor Area）] を選択した場合に限り、[ビルディング（Building）]、[フロア領域（Floor Area）]、および [カバレッジ領域（Coverage Area）] のドロップダウン リストが表示されます。

- [キャンパス（Campus）] ドロップダウン リストから、サービス アドバタイズメントを表示させるキャンパス名を選択します。
- [ビルディング（Building）] ドロップダウン リストから、アドバタイズメントを表示させるビルディング名を選択します。
- [Floor] ドロップダウン リストから、フロア タイプを選択します。
- [Coverage Area] ドロップダウン リストから、フロア内のカバレッジ領域を選択します。
- [Outdoor Area] ドロップダウン リストから、サービス アドバタイズメントを表示する屋外領域を選択します。このフィールドは、エリア タイプとして [Outdoor Area] を選択した場合にのみ表示されます。

ステップ 6 **[次へ（Next）]** をクリックします。[オーディオ（Audio）] グループ ボックスが表示されます。

ステップ 7 [オーディオ（Audio）] グループ ボックスから [ファイルの選択（Choose File）] をクリックし、オーディオ通知を再生するためのオーディオ ファイルを参照して選択します。

ステップ 8 [次へ（Next）] をクリックします。[Icons] グループ ボックスが表示されます。

ステップ 9 **[アイコン（Icons）]** グループ ボックスから **[ファイルの選択（Choose File）]** をクリックし、クライアント ハンドセットに表示するアイコンを参照して選択します。

ステップ 10 [Next] をクリックします。[Venue Apps] グループ ボックスが表示されます。

ステップ 11 [場所アプリ（Venue Apps）] グループ ボックスの [Web アプリ（Web App）] ドロップダウン リストから、サービス アドバタイズメントを表示する場所アプリケーションを選択します。

ステップ 12 **[次へ（Next）]** をクリックします。[追加の場所情報（Additional Venue Information）] グループ ボックスが表示されます。

ステップ 13 [追加情報（Additional Information）] グループ ボックスから、場所でモバイル アプリケーションに提供する追加情報を指定できます。次の設定を行えます。

- [ロケーションの詳細（Location Detail）] テキスト ボックスに場所の詳細情報を入力します。ここでは、場所のストア アドレス、郵便番号、住所などの詳細を指定します。
- [Latitude and Longitude] テキスト ボックスに、場所の GPS 緯度および経度を入力します。これにより、アプリケーションが場所を正確に特定しやすくなります。
- [Additional Information] テキスト ボックスに、場所でモバイル アプリケーションに提供する追加情報を入力します。

ステップ 14 [Save] をクリックします。この情報は MSE に適用され、自動的に同期されます。

ステップ 15 任意の場所を削除する場合は、[場所（Venue）] ページで次の手順を実行します。

a) 削除する場所のチェックボックスをオンにします。

b) [コマンドの選択（Select a command）] ドロップダウン リストから、[場所の削除（Delete Venue）] を選択して [実行（Go）] をクリックします。

c) [OK] をクリックして削除を実行します。

関連トピック

MSE を使用したモバイル コンシェルジュの設定 （1071 ページ）
モバイル コンシェルジュ（MSE）のプロバイダーの設定 （1073 ページ）
モバイル コンシェルジュ ポリシー（MSE）の設定 （1074 ページ）

モバイル コンシェルジュ（MSE）のプロバイダーの設定

ステップ 1 **[サービス（Services）] > [モビリティ サービス（Mobility Services）] > [モバイル コンシェルジュ（Mobile Concierge）]** を選択します。

ステップ 2 左側のサイドバーのメニューから**[モバイル コンシェルジュ サービス（Mobile Concierge Services）] > [プロバイダー（Providers）]** を選択します。

[プロバイダー（Providers）] ページが表示されます。

ステップ 3 [コマンドの選択（Select a command）] ドロップダウン リストから、[新しいプロバイダーの定義（Define New Provider）] を選択し、[実行（Go）] をクリックします。

[Provider Wizard] ページが表示されます。

ステップ 4 [Provider Name] テキスト ボックスにプロバイダーの場所の名前を入力します。

ステップ 5 [Next] をクリックします。[アイコン（Icons）] グループ ボックスが表示されます。

ステップ 6 [Icons] グループ ボックスから [Choose File] をクリックして、クライアント無線端末に表示するアイコンを参照して選択します。

ステップ 7 [次へ（Next）] をクリックします。[ローカル サービス（Local Services）] グループ ボックスが表示されます。

ステップ 8 [ローカル サービス（Local Services）] グループ ボックスから、次の手順を実行します。

- [Local Service # name] の左側にある逆三角形アイコンをクリックして [Local Service] を展開し、以下を設定します。
  - [Service Type] ドロップダウン リストからサービス タイプを選択します。選択可能なオプションは、[Directory Info]、[Sign Up]、[Discount Coupon]、[Network Help]、および [Other] です。
  - [Display Name] テキスト ボックスに表示名を入力します。
  - [Description] テキスト ボックスに説明を入力します。
  - [サービス URI（Service URIs）] ドロップダウン リストから URI を選択します。
  - [推奨アプリ（Recommended Apps）] テキスト ボックスにその場所に推奨するアプリケーションを入力します。

ステップ 9 [保存（Save）] をクリックします。

ステップ 10 プロバイダーを削除する場合は、[プロバイダー（Providers）] ページで次の手順を実行します。

a) 削除する場所のチェックボックスをオンにします。

b) [コマンドの選択（Select a command）] ドロップダウンリストから、[プロバイダーの削除（Delete Provider）] を選択して [実行（Go）] をクリックします。

c) [OK] をクリックして削除を実行します。

関連トピック

モバイル コンシェルジュ（MSE）の場所の設定 （1072 ページ）
MSE を使用したモバイル コンシェルジュの設定 （1071 ページ）
モバイル コンシェルジュ ポリシー（MSE）の設定 （1074 ページ）

モバイル コンシェルジュ ポリシー（MSE）の設定

ポリシーを設定するには、次の手順を実行します。

ステップ 1 **[サービス（Services）] > [モビリティ サービス（Mobility Services）] > [モバイルコンシェルジュ（Mobile Concierge）]** の順に選択します。

ステップ 2 左側のサイドバーのメニューから **[モバイル コンシェルジュ サービス（Mobile Concierge Services）]** > **[ポリシー（Policies）]** を選択します。

[ポリシー（Policies）] ページが表示されます。

ステップ 3 [Select a command] ドロップダウン リストから [Define New Policy] を選択し、[Go] をクリックします。

[Policy Wizard] ページが表示されます。

ステップ 4 [Venue] ドロップダウン リストから、ポリシーを適用する場所を選択します。

ステップ 5 [Next] をクリックします。[Provider] グループ ボックスが表示されます。

ステップ 6 [プロバイダー（Provider）] ドロップダウン リストからプロバイダーを選択します。

ステップ 7 [次へ（Next）] をクリックします。[SSID] グループ ボックスが表示されます。

ステップ 8 ドロップダウン リストから、サービス アドバタイズメントをブロードキャストする SSID を選択し、[OK] をクリックします。複数の SSID を選択できます。

ステップ 9 [Next] をクリックします。[表示ルール（Display Rule）] グループ ボックスが表示されます。

ステップ 10 [Display Rule] グループ ボックスでは、次の操作を実行できます。

- [Display Rule] オプション ボタンを選択します。[Everywhere] または [Near selected APs] オプション ボタンを選択できます。デフォルトでは、[Display everywhere] が選択されています。

[Display everywhere] を選択した場合、これらの SSID を提供するすべてのモバイル コンシェルジュ対応コントローラが検索され、それらのコントローラが MSE に割り当てられます。

[選択した AS に近い AP の表示（Display near selected APs）] を選択した場合は、次のパラメータを設定できます。

- [AP]：アドバタイズメントをブロードキャストする AP を選択します。
- [Radio]：アドバタイズメントをブロードキャストする無線周波数を選択します。選択した無線帯域の近くにモバイルデバイスがある場合、サービス アドバタイズメントが表示されます。指定できる値は 2.4 GHz または 5 GHz です。
  - [最小 RSSI（min RSSI）]：サービス アドバタイズメントをユーザ インターフェイスに
  - 表示する RSSI の値を入力します。

ステップ 11 [終了（Finish）] をクリックします。

ステップ 12 ポリシーを削除する場合は、[ポリシー（Policy）] ページで次の手順を実行します。

a) 削除するポリシーのチェックボックスをオンにします。

b) [コマンドの選択（Select a command）] ドロップダウンリストから、[プロバイダーの削除（Delete Provider）] を選択して [実行（Go）] をクリックします。

c) [OK] をクリックして削除を実行します。

関連トピック

MSE を使用したモバイル コンシェルジュの設定 （1071 ページ）
モバイル コンシェルジュ（MSE）の場所の設定 （1072 ページ）
モバイル コンシェルジュ（MSE）のプロバイダーの設定 （1073 ページ）

MSEワイヤレスセキュリティ構成ウィザードを使用したwIPSの設定

Wireless Security ウィザードのページが表示され、次の wIPS 関連の設定を行うことができます。

- 不正ポリシーによって、アドホック ネットワークを検出およびレポートできます。
- 不正ルールによって、不正アクセス ポイントを自動的に分類するルールを定義できます。
- 新しい wIPS プロファイルを追加できます。

ステップ 1 **[サービス（Services）] > [モビリティ サービス（Mobility Services）] > [ワイヤレス セキュリティ（Wireless Security）]** を選択します。

デフォルトでは、[始める前に（Before You Begin）] タブが開きます。[始める前に（Before You Begin）] ウィザード ページには、[ワイヤレス セキュリティ（Wireless Security）] ウィザード の使用方法の情報が表示され、さらに次の情報が含まれています。

- [Rogue Policy]：[Rogue Policy] ページでは、不正ポリシーを設定できます。このページには、不正アクセス検出と封じ込めのための 3 つの不正ポリシー事前設定があります。
- [Rogue Rules]：[Rogue Rules] ページでは、認証タイプ、一致条件設定済みの SSID、クライアント数、RSSI 値などの基準に基づいて、不正アクセス ポイントを自動的に分類できます。不正アクセスのルールは、不正アクセスを [Malicious] または [Friendly] として分類するように作成できます。
- [wIPS Profile]：[wIPS Profile] ページでは、いくつかの定義済みプロファイルからプロファイルを選択できます。これらのプロファイルによって、Cisco Adaptive wIPS を通じて使用可能な追加のワイヤレスの脅威保護をすばやくアクティブにできます。プロファイルは、検出して封じ込める wIPS シグニチャを選択することでさらにカスタマイズできます。
- [Devices]：[Devices]ページでは、不正ポリシー、不正アクセス ルール、wIPS プロファイルをコントローラに適用できます。

ステップ 2 [次へ（Next）] をクリックして、アドホック ネットワークを検出およびレポートする不正ポリシーを設定します。このページでは、コントローラに適用される（アクセス ポイントとクライアントに対する）不正ポリシーを設定できます。

- ポリシー設定は、[低（Low）]、[High（高）]、または [クリティカル（Critical）] のいずれかに設定できます。これを行うには、[不正ポリシー設定値の設定（Configure the rogue policy settings）] スライディング バーをマウスを使用して移動するか、または [カスタム（Custom）] チェックボックスをオンにしてポリシー設定値を設定します。
- [General] グループ ボックスで、次のフィールドを設定します。
  - [Rogue Location Discovery Protocol]：Rogue Location Discovery Protocol（RLDP）が企業の有線ネットワークに接続されているかどうかを判断します。ドロップダウン リストから、次のいずれかのオプションを選択します。
  - [Disable]：すべてのアクセス ポイント上で RLDP を無効にします。
  - [All APs]：すべてのアクセス ポイント上で RLDP を有効にします。

- [Monitor Mode APs]：モニタ モードのアクセス ポイント上でのみ RLDP を有効にします。

- [不正 AP および不正クライアント エントリの有効期限タイムアウト（Expiration Timeout for Rogue AP and Rogue Client Entries）]：不正アクセス ポイント エントリの失効タイムアウトを秒単位で設定します。有効な値の範囲は 240 ～ 3600 秒です。
- [不正クライアントの AAA の検証（Validate rogue clients against AAA）]：[不正クライアントの AAA の検証（Validate rogue clients against AAA）] チェックボックスをオンにして、不正クライアントの AAA 検証を有効にします。
- [アドホック ネットワーキングの検出とレポート（Detect and report Adhoc networks）]：[アドホック ネットワーキングの検出とレポート（Detect and report Adhoc networks）] チェックボックスをオンにして、アドホック ネットワーキングに参加している不正クライアントの検出とレポートを有効にします。
- [不正検出レポート間隔（Rogue Detection Report Interval）]：[不正検出レポート間隔（Rogue Detection Report Interval）] テキスト ボックスに、AP が不正検出レポートをコントローラに送信するまでの時間間隔を秒数で入力します。有効な範囲は 10 ～ 300 秒で、デフォルト値は 10 秒です。この機能は、モニタ モードの AP のみに適用されます。
- [Rogue Detection Minimum RSSI]：[Rogue Detection Minimum RSSI] テキスト ボックスに、AP により検出され、不正エントリがコントローラに作成する RSSI の最小値を入力します。有効な範囲は -70 dBM ～ -128 dBm です。この機能は、すべての AP モードに適用できます。
- [Rogue Detection Transient Interval]：[Rogue Detection Transient Interval] テキスト ボックスに、不正が AP により最初にスキャンされてから、必ずスキャンされる時間間隔を入力します。一時的な間隔を入力することで、AP が不正をスキャンする間隔を制御できます。AP は、一時的な間隔の値に基づいて、不正をフィルタできます。有効な範囲は 120 ～ 1800 秒で、デフォルト値は 0 です。この機能は、モニタ モードの AP のみに適用されます。
- [自動封じ込み（Auto Contain）] グループ ボックスで、次のフィールドを設定します。

  - [有線の不正（Rogue on Wire）]：[有線の不正（Rogue on Wire）] チェックボックスをオンにして、有線ネットワークで検出された AP を自動的に封じ込めます。
  - [SSID の使用（Using our SSID）]：[SSID の使用（Using our SSID）] チェックボックスをオンにします。
  - [不正 AP 上の有効なクライアント（Valid Client on Rogue AP）]：[不正 AP 上の有効なクライアント（Valid Client on Rogue AP）] チェックボックスをオンにして、有効なクライアントを不正 AP への接続から封じ込めます。
  - [アドホック不正（AdHoc Rogue）]：[アドホック不正（AdHoc Rogue）] チェックボックスをオンにして、アドホック不正 APs を自動的に封じ込めます。

- [適用（Apply）] をクリックして、コントローラに現在のルールを適用します。[デバイス（Devices）] ウィザードのページで、該当するコントローラを選択し、[コントローラに適用（Apply to Controllers）] をクリックします。

ステップ 3 [次へ（Next）] をクリックして不正ルールを設定します。このページでは、不正アクセス ポイントを自動的に分類するルールを定義できます。Prime Infrastructure はコントローラに不正なアクセス ポイントの分類ルールを適用します。これらのルールでは、RSSI レベル（それよりも弱い不正アクセス ポイントは無視）、または時間制限（指定された時間内に表示されない不正アクセス ポイントにはフラグを立てない）に基づいて、マップ上の不正表示を制限できます。

ステップ 4 [新規作成（Create New）]をクリックして新しい不正ルールを作成します。[不正ルールの追加/編集（Add/Edit Rogue Rule）] ウィンドウが表示されます。

- [一般（General）] グループ ボックスで、次のフィールドを設定します。
  - [ルール名（Rule Name）] : テキスト ボックスにルールの名前を入力します。
  - [ルール タイプ（Rule Type）] : ドロップダウン リストから [悪意がある（Malicious）] または [フレンドリ（Friendly）] を選択します。

（注） [Malicious Rogue]：検出されたアクセス ポイントのうち、ユーザが定義した Malicious ルールに一致したアクセス ポイント、または危険性のない AP カテゴリから手動で移動されたアクセス ポイント。[Friendly Rogue]：既知、認識済み、または信頼できるアクセス ポイント、または検出されたアクセス ポイントのうち、ユーザが定義した Friendly ルールに該当するアクセス ポイント。

- [一致の種類（Match Type）] : ドロップダウン リストから [すべての条件に一致（Match All Conditions）] または [いずれかの条件に一致（Match Any Condition）] を選択します。
- [不正分類ルール（Rogue Classification Rule）] グループ ボックスで、次のフィールドを設定します。
  - [オープン認証（Open Authentication）] : オープン認証を有効にするには、[オープン認証（Open Authentication）] チェックボックスをオンにします。
  - [管理対象 AP SSID の照合（Match Managed AP SSID）] : 管理対象 AP SSID のルール条件との一致を有効にするには、[管理対象 AP SSID の照合（Match Managed AP SSID）] チェックボックスをオンにします。

    （注） 管理対象 SSID は、WLAN に対して設定された SSID で、システムが既知のものです。

  - [ユーザ設定 SSID の照合（Match User Configured SSID）]（1 行に 1 つずつ入力）：ユーザ設定の SSID のルール条件との一致を有効にするには、[ユーザ設定 SSID の照合（Match User Configured SSID）] チェックボックスをオンにします。

    （注） ユーザ設定の SSID は、手動で追加された SSID です。[ユーザ設定の SSID に一致（Match User Configured SSID）] テキスト ボックスに、ユーザ設定の SSID を（1 行に 1 つずつ）入力します。

  - [最小 RSSI（Minimum RSSI）] : 最小 RSSI しきい値制限を有効にするには、[最小 RSSI（Minimum RSSI）] チェックボックスをオンにします。

    （注） テキスト ボックスに RSSI 閾値の最小レベル（dB 単位）を入力します。検出されたアクセス ポイントがここで指定した RSSI 閾値を超えていると、そのアクセス ポイントは悪意のあるものとして分類されます。

  - [期間（Time Duration）] : 時間制限を有効にするには、[期間（Time Duration）] チェックボックスをオンにします。

    （注） テキストボックスに制限時間（秒単位）を入力します。検出されたアクセスポイントが指定した制限時間よりも長く表示されているとき、そのアクセス ポイントは悪意のあるものとして分類されます。

  - [不正クライアントの最小数（Minimum Number Rogue Clients）] : 悪意のあるクライアントの最小数の制限を有効にするには、[不正クライアントの最小数（Minimum Number Rogue Clients）] チェックボックスをオンにします。

（注） 悪意のあるクライアントを許可する最小数を入力します。検出されたアクセス ポイントにアソシエートされたクライアントの数が指定した値以上になると、そのアクセス ポイントは悪意のあるものとして分類されます。

- [OK] をクリックしてルールを保存するか、または [キャンセル（Cancel）] をクリックして現在のルールの作成または変更をキャンセルします。[不正ルール（Rogue Rules）] ページに戻り、新しく追加された不正ルールが表示されます。
- [適用（Apply）] をクリックして、コントローラに現在のルールを適用します。[デバイス（Devices）] ウィザードのページで、該当するコントローラを選択し、[コントローラに適用（Apply to Controllers）] をクリックします。

ステップ 5 **[次へ（Next）]** をクリックして、wIPS プロファイルを設定します。Prime Infrastructure は、選択可能なものからいくつかの事前定義ポリシーを提供します。これらのプロファイル（カスタマー タイプ、ビルディング タイプ、業界タイプなどに基づきます）を使用すると、Cisco Adaptive wIPS を通じて使用可能な追加のワイヤレスの脅威保護をすばやくアクティブにできます。プロファイルは「そのまま」使用することも、要件に合わせてカスタマイズすることもできます。

ステップ 6 wIPS プロファイル設定の詳細については、「Configuring wIPS and Profiles」を参照してください。

ステップ 7 wIPS プロファイルを設定したら、[次へ（Next）] をクリックして [デバイス（Devices）] ページを開き、設定を適用するコントローラを選択できます。

Connected Mobile Experience の設定

Cisco Connected Mobile Experience（CMX）は、ワイヤレス インフラストラクチャを使用してユーザのモバイルデバイスを検出して特定するスマート Wi-Fi ソリューションです。これを使用して、ユーザの好みに合わせてカスタマイズされたコンテンツをスマートフォンやタブレットに直接配信できます。Cisco CMX は、ロケーション識別用の Cisco モビリティ サービス エンジン（MSE）や、モバイル アプリの開発、配布、管理用の Cisco Enterprise Mobility Services Platform（EMSP）などの他のコンポーネントと統合するソフトウェア ソリューションです。

重要

- Prime Infrastructure 3.2 は、CMX 10.3 との統合をサポートしています。以下のクエリを使用して CMX をクエリします。
  - /api/config/v1/version/image（CMX バージョンの取得用）
  - /api/config/v1/campuses/import（CMX へのマップ ファイルのインポート用）
- プライム Infrstructure 3.5 は、CMX バージョン10.3 および10.4 をサポートしていません。したがって、プライムインフラストラクチャをバージョン3.5 にアップグレードする場合は、CMX を10.5 にアップグレードする必要もあります。
- CMXにマップをインポートする際のファイルストレージ制限はマップエクスポートファイル 10 個です。さらにファイルをインポートしようとすると、既存のファイルのいずれかの削除を求めるメッセージが表示されます。
- Prime Infrastructure で CMX クライアントを表示する前に、CMX をロケーション モードで設定し、Prime Infrastructure からマップをロードする必要があります
- Prime Infrastructure 3.4 以降、CMX 10.4 以降と同期化されたサイト マップには、RFID タグ、不正クライアント、不正 AP、クライアント（関連する、関連しない）の位置が表示されます。
- Prime Infrastructure に MSE と CMX の両方が追加されている場合、フロア マップを同期できるのはそのいずれかのみです。そのため、このフロアで対応するクライアントを追跡できるのは、このいずれかのクライアントのみです。
- 情報を更新するための定期的なタスクがないため、Prime Infrastructure のマップに対する変更は CMX と同期されません。更新した情報を取得するには、マップを CMX に再びインポートする必要があります。
- マップ ページが開いて、設定したマップ更新間隔で更新されると、Prime Infrastructure は CMX に対して API クエリを実行します。

関連トピック

Prime Infrastructure での CMX の管理 （1080 ページ）

Prime Infrastructure での CMX の管理

CMX デバイスを追加、編集、削除し、サイト マップを Prime Infrastructure から CMX にインポートするには、次の手順を実行します。

ステップ 1 デバイスを追加するには、**[サービス（Services）]** > **[モビリティサービス（Mobility Services）]** > **[Connected Mobile Experiences]** を選択します。

または、**[サービス（Services）]** > **[モビリティ サービス（Mobility Services）]** > **[モビリティ サービス エンジン（Mobility Service Engine）]** ページで [CMXの管理（Manage CMX）] リンクをクリックできます。

ステップ 2 [Add] をクリックします。

ステップ 3 次の詳細を入力します。

- IP アドレス
- デバイス名（Device Name）
- CMX ユーザ名（GUI クレデンシャル）
- CMX パスワード（GUI クレデンシャル）
- SSH ユーザー (オプション)
- SSH パスワード（オプション）
- 所有者の名前（オプション）

ステップ 4 [Save] をクリックして、デバイスを追加します。

ステップ 5 デバイスパラメータを編集するには、**[サービス（Services）]** > **[モビリティサービス（Mobility Services）]** > **[Connected Mobile Experiences]** を選択します。

ステップ 6 [編集（Edit）] をクリックします。

ステップ 7 次のパラメータのいずれかまたはすべてを編集します。

- CMX ユーザ名（GUI クレデンシャル）
- CMX パスワード（GUI クレデンシャル）
- SSH ユーザー (オプション)
- SSH パスワード（オプション）
- 所有者の名前（必須ではありません）

ステップ 8 [更新（Update）]をクリックして新しいパラメータを保存するか、または前のパラメータに戻るには[キャンセル（Cancel）] をクリックします。

ステップ 9 デバイスを削除するには、**[サービス（Services）]** > **[モビリティサービス（Mobility Services）]** > **[Connected Mobile Experiences]** を選択します。

ステップ 10 [削除（Delete）] をクリックします。

ステップ 11 削除するデバイスを選択し、**[削除（Delete）]** > **[Ok]** をクリックします。

ステップ 12 サイト マップを CMX にインポートするには、**[サービス（Services）]** > **[モビリティサービス（Mobility Services）]** > **[Connected Mobile Experiences]** を選択し、CMX を選択して [マップをCMXにインポート（Import Map to CMX）] をクリックします。

（注） CMX がプレゼンス モードの場合、マップは CMX では表示されませんが、ロケーション モードでは表示されます。

ステップ 13 マップを選択し、[マップをCMXにインポート（Import Map to CMX）] をクリックします。

（注） [CMXのリスト（List CMX）] ページの [PIからマップをエクスポート（Export Map from PI）] ボタンを使用してマップ ファイルを Prime Infrastructure に追加することもできます。

ステップ 14 新しいマップ ファイルを作成するには、[マップをCMXにインポート（Import Map to CMX）] ウィンドウで [PIからエクスポート（Export From PI）] をクリックします。

ステップ 15 [マップ（Maps）] ページで、マップを選択して Prime Infrastructure に保存します。

同期されると、CMX は次のパラメータを追跡できるようになります。

- クライアント
- 干渉
- [不正 AP（Rogue APs）]
- 不正クライアント（Rogue Clients）
- RFID タグ

第 40 章

Cisco AppNav を使用した WAN の最適化

- Cisco AppNav とは （1083 ページ）
- Cisco AppNav 設定の前提条件 （1085 ページ）
- Cisco AppNav の設定方法 （1085 ページ）
- 単一デバイスでの Cisco AppNav の設定 （1086 ページ）
- Cisco Prime Infrastructure のインターフェイス ロールと Cisco AppNav ソリューション （1087 ページ）
- テンプレートを使用した複数デバイス上での Cisco AppNav の設定 （1088 ページ）
- Cisco AppNav テンプレートの展開 （1089 ページ）
- ISR-WAAS コンテナで作成する場合の Cisco AppNav の設定方法 （1090 ページ）

Cisco AppNav とは

Cisco AppNav は WAN 最適化のネットワーク統合を簡素化するハードウェアおよびソフトウェア ソリューションです。さらに、プロビジョニング、可視性、拡張性、非対称性、およびハイ アベイラビリティに関する課題を解決します。

Cisco AppNav ソリューションは、強力なクラスおよびポリシー メカニズムを使用し、Cisco WAAS デバイス間でトラフィックを分散して最適化することで、代行受信スイッチやルータへの依存を低減します。ISR-WAAS を使用し、サイトやアプリケーションに基づいてトラフィックを最適化できます。これにはデバイス レベルおよびテンプレートベースの設定が含まれます。

Cisco IOS-XE ソフトウェアのインテリジェント ロードバランシング メカニズムによって、Cisco WAAS および OneFirewall（Cisco WAAS を初期ターゲットとする）を含むさまざまな製品への TCP トラフィックの転送が可能です。ルータ管理は、Cisco Prime Infrastructure ネットワーク管理アプリケーションによって実行されます。

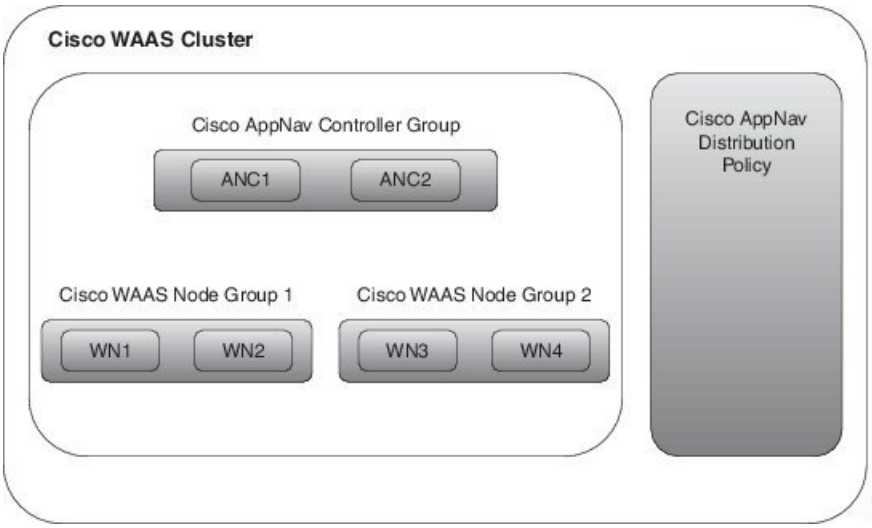
Cisco AppNav ソリューションは、Cisco AppNav コントローラ（AC）と呼ばれる配信ユニットと WAAS サービス ノード（SN）で構成されます。Cisco AppNav コントローラはフローを配信し、サービス ノードはフローを処理します。最大 4 台の Cisco AppNav-XE（ルータ）をグループ化して Cisco AppNav コントローラ グループ（ACG）を形成し、非対称フローとハイ アベイラビリティに対応できます。ただし、ACG 内のすべてのルータは同じプラットフォームにあり、メモリ容量が同じである必要があります。

Cisco AppNav ソリューションのコンポーネントは、次の機能を実行します。

- AppNav コントローラ：ルータからサービス ノードにインテリジェントにトラフィックを配信するコンポーネントです。Cisco AppNav コントローラは、Cisco ISR-4400、Cisco CSR、および Cisco ASR 1K プラットフォーム上の Cisco IOS-XE Release 3.10 の一部です。
- Cisco WAAS サービス ノード：トラフィック フローを最適化します。Cisco IOS-XE コンテナで稼働するスタンドアロン アプライアンスや仮想化 ISR-WAAS などのさまざまなフォーム ファクタで利用できます。
- Cisco WAAS Central Manager：ISR-WAAS のモニタリングおよび設定に使用されます。
- この章では、ルータでの Cisco AppNav コントローラ機能の設定について説明します。

次の図は、Cisco AppNav のコンポーネントについて説明しています。

図 *28 : Cisco AppNav* のコンポーネント



Cisco AppNav コンポーネントを使用する利点は次のとおりです。

- 各サービス ノードの負荷に基づいて、インテリジェントに新しいフローをリダイレクトできます。これには、個々のアプリケーション アクセラレータの負荷が含まれます。
- 最適化を必要としないフローの場合、サービス ノードがパケットを直接渡すよう Cisco AppNav コントローラに通知するため、遅延やリソース使用量が最小化されます。
- サービス ノードを追加または除去する際のトラフィックへの影響が最小限になります。
- Cisco AppNav コンポーネントは VRF をサポートします。トラフィックがサービス ノードから戻るときに VRF 情報が維持されます。しかし、Cisco Prime Infrastructure では VRF はサポートされていません。
- Messaging Application Programming Interface（MAPI）や仮想デスクトップ インフラストラクチャ（VDI）などの特定のアプリケーションの場合、コンポーネントを使用することで一連のフローが同じサービス ノードにリダイレクトされます。
- 1 方向のトラフィックが Cisco AppNav コントローラを通過し、リターン トラフィックが別の Cisco AppNav コントローラを通過する状況で、非対称フローを最適化できます。ただし、どちらも同じ ISR-WAAS にトラフィックをリダイレクトします。これは、Cisco AppNav コントローラ グループを使用して行います。

Cisco AppNav テクノロジーにより、IP フローをルータで代行受信し、一連の Cisco WAAS サービス ノードに送信して処理できます。Cisco IOS-XE Release 3.10 でサポートされる Cisco AppNav の初期アプリケーションは Cisco WAAS に含まれます。

関連項目

- Cisco AppNav 設定の前提条件
- Cisco AppNav の設定方法

Cisco AppNav 設定の前提条件

Cisco AppNav を設定する際の前提条件は次のとおりです。

- プラットフォームは、Cisco 4451-X ISR、Cisco ASR 1000 シリーズ アグリゲーション サービス ルータ、またはシスコ クラウド サービス ルータである必要があります。
- 上記プラットフォームのソフトウェア バージョンは、バージョン 3.10 以降である必要があります。
- 有効な appxk9 ライセンスをルータで有効にする必要があります。
- Cisco WAAS サービス ノードが使用可能である必要があります。

Cisco AppNav の設定方法

トラフィックを Cisco WAAS サービス ノードにリダイレクトするには、ルータでいくつかのパラメータを設定する必要があります。Cisco WAAS 仮想アプライアンスのインストールの一環として Cisco AppNav 設定が生成される場合、これは対応するユーザに対して透過的です。テンプレートまたはデバイス ワーク センターを使用して設定する場合は、ユーザがより直接的に関与します。

次の 3 とおりの方法で Cisco AppNav を設定できます。

- 単一デバイスでの Cisco AppNav の設定 （1086 ページ）
- テンプレートを使用した複数デバイス上での Cisco AppNav の設定 （1088 ページ）
- ISR-WAAS コンテナで作成する場合の Cisco AppNav の設定方法 （1090 ページ）

Cisco AppNav 設定には次のいずれかを使用します。

- コントローラ：共同でトラフィックをリダイレクトするルータのリスト。これは IP アドレスのリストです。この内のいずれか 1 つが Cisco AppNav を設定するルータに属している必要があります。
- Cisco WAAS サービス ノード グループ（SNG）：リダイレクトするトラフィックのターゲットで、一連の IP アドレスとして定義された 1 つ以上の SNG が含まれます。
- クラスマップ：着信および発信トラフィックを分類する一連のクラスマップ。クラスマップは一連の一致条件で構成され、これらを組み合わせて対象トラフィックを指定します。次の 3 種類の条件に基づいてトラフィックを照合できます。

- 送信元および宛先の IP アドレスとポートに基づいてトラフィックを選択するアクセス コントロール リスト（ACL）。
- 固定ポート番号に依存せずに、Microsoft のポート マッパー サービスを使用するトラフィックを選択するためのプロトコル。MAPI、および他の Microsoft プロトコルのホストを含みます。
- リモート エンドの特定の Cisco WAAS サービス ノードを通過したトラフィックを照合するリモート デバイス。リモート デバイスは MAC アドレスで識別されます。

- ポリシー マップ：Cisco AppNav ポリシー マップはルールの番号付きリストです。各ルールで特定のタイプのトラフィックに対する処理を指定します。したがって、ルールはクラス マップとアクションで構成されます。このアクションは、サービス ノード グループへのリダイレクトかパス スルーのいずれかになります。
- クラスタ：Cisco WAAS クラスタとは、ポリシー マップ、コントローラ グループ、およびポリシー マップが使用する一連のサービス ノード グループを組み合わせたものです。クラスタは有効化または無効化できます。Cisco Prime Infrastructure では複数のクラスタを定義できますが、一度に有効にできるのは 1 つのみです。クラスタのコントローラとノード間の通信を保護するため、認証キーが使用されます。
- Cisco WAAS インターフェイス：Cisco WAAS が有効になっているインターフェイスでのみトラフィックを最適化できます。

WAN 最適化テンプレートとデバイス ワーク センターの両方にデフォルト ポリシーがあります。デフォルト ポリシーを構成する複数のクラス マップは、Cisco ISR-WAAS によって最適化されるさまざまなタイプのトラフィック（HTTP、CIFS、TCP など）を照合します。テンプレートにも、これらの各クラス マップのルールから成るポリシー マップが含まれます。デフォルトでは、一致したすべてのトラフィックは単一のサービス ノード グループにリダイレクトされます。

単一デバイスでの Cisco AppNav の設定

管理者はデバイス ワーク センターを使用して、個々のデバイスの設定を表示および変更できます。ユーザが所有するデバイスが 1 つまたは少数である場合は、デバイス ワーク センターを使用して Cisco AppNav を設定できます。デバイスでテンプレートを使用して展開された設定を個別に編集することができます。

デバイス ワーク センターから Cisco AppNav を設定するには、次の手順を実行します。

ステップ 1 **[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ネットワーク デバイス（Network Devices）]** の順に選択します。

ステップ 2 設定するデバイスを選択します。

ステップ 3 下部ペインの [Configuration] タブで [WAN Optimization] をクリックします。

Cisco AppNav 設定は次のセクションに分かれています。

- AppNav コントローラ：[Controllers] ページには、そのルータと同じクラスタに属しているルータの IP アドレスが表示されます。アドレスの 1 つを、現在選択されているルータのいずれかのインターフェ

イスに割り当てる必要があります。各ルータのIPアドレスはドロップダウン リストに表示されます。同じクラスタ内の他のルータの IP アドレスは個別のテーブルに表示されます。

- Cisco WAAS クラスタ：[Cisco WAAS クラスタ（Cisco WAAS Clusters）] ページは Cisco AppNav のメインのページです。デバイスに設定された Cisco WAAS クラスタが一覧表示され、新規の作成が可能です。ポリシーマップなど、クラスタの詳細設定を表示するには、クラスタを選択して [Edit] をクリックします。
  - このページで、クラスタ設定およびポリシーを編集できます。3 列目の矢印をクリックすると、個々のルールが展開されます。これにより、該当するルールを編集したり、クラス マップおよび Cisco WAAS サービス ノード グループを表示、変更、作成したりすることができます。新しいルールを追加するには、[Add Policy] をクリックします。ポリシー マップ内のルールの順序は重要です。順序は、テーブルで行をドラッグするか、隣接する複数の行を選択し、メニュー バーにある上下の矢印を使用して変更できます。
  - 新しいクラスタを作成するには、[Cisco WAAS Cluster Overview] タブで [Add WAAS Cluster] を選択します。ウィザードが起動し、コントローラ、Cisco WAAS サービス ノード、代行受信インターフェイス、およびクラスタの一般パラメータの入力を求めるプロンプトが表示されます。必要な情報を入力して [Finish] をクリックすると、設定が有効になります。ウィザードによって、最小限のインストールで機能するデフォルト ポリシーを含むクラスタが作成されます。すべての TCP フローは単一のノード グループにリダイレクトされ、そのノード グループは過負荷条件についてモニタされます。

（注） Prime Infrastructure は VRF をサポートしていません。そのため、一度に有効にできる Cisco WAAS クラスタは 1 つのみです。

- 代行受信：管理者は [Interception] ページを使用して、着信および発信トラフィックをリダイレクトする（ポリシーの対象）インターフェイスを選択できます。ルータ上のすべての WAN インターフェイスで Cisco WAAS を有効にする必要があります。
- 詳細設定：[Advanced Settings] フォルダには、Cisco WAAS サービス ノード グループ、クラス マップ、およびポリシー マップのページが含まれます。この情報のほとんどは [Cisco WAAS Clusters] ページでも利用できますが、これらのオブジェクトの定義を直接表示できるので便利です。
  - Cisco WAAS ノード グループ：[Cisco WAAS Node Groups] ページでは、既存の Cisco WAAS ノード グループの編集、および新規の作成が可能です。
  - クラス マップとポリシー マップ：[Class Maps] ページと [Policy Maps] ページは同様に機能します。

Cisco Prime Infrastructure のインターフェイス ロールと Cisco AppNav ソリューション

Cisco AppNav ソリューションが明示的に有効にされているインターフェイスでのみトラフィックが再ルーティングされます。インターフェイス ロールと論理オブジェクトを使用すると、各インターフェイスの名前を手動で定義することなく、複数のデバイス上の特定のインターフェ

イスにポリシーを定義できます。テンプレートをデバイスに導入すると、インターフェイス ロールは一連の実際のインターフェイスに解決されます。

デバイスごとのテンプレート導入中に、Cisco WAAS が有効になっているインターフェイスの設定を上書きできます。ただし、テンプレート導入プロセスを簡素化するためには、インターフェイス ロールを 1 つ以上定義してテンプレートの一部として保存することをお勧めします。また、**[設定（Configuration）] > [テンプレート（Templates）] > [共有ポリシーオブジェクト（Shared Policy Objects）] > [インターフェイスロール（Interface Role）]** でインターフェイス ロールを定義することもできます。

テンプレートを使用した複数デバイス上でのCiscoAppNavの設定

Prime Infrastructure のテンプレートには、任意の数のデバイスに展開できる再利用可能な複数の設定が含まれています。WAN 最適化テンプレートは、AppNav ルータ全体に適用できるポリシーおよびその他の情報を定義します。

デザイン ビューでテンプレートを定義して、後で 1 つ以上のデバイスに導入できます。導入プロセスの一環として、設定をデバイスに適用する前に、デバイス固有のパラメータを入力して最終的な CLI を確認できます。テンプレートを変更した場合は、デバイスに再導入して変更を適用する必要があります。

複数のデバイスで類似した Cisco AppNav 設定が必要な場合に、この設定方法を使用します。同様の設定で一部の値を若干カスタマイズした単一のテンプレートを、導入オプションを使用して同じタイプの複数のデバイスに導入できます。

テンプレートを使用して Cisco AppNav を設定するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [テンプレート（Templates）] > [機能およびテクノロジー（Features & Technologies）] > [WAN 最適化（WAN Optimization）]** を選択します。

ステップ 2 **AppNav クラスタ** を選択します。

ステップ 3 次のタブで設定の詳細情報を入力します。

- [Controller IP addresses]：コントローラのリストはここで設定することも、導入時に設定することもできます。たとえば、支社などの複数のサイトにテンプレートを使用する場合は、このフィールドを空のままにしてください。ただし、導入時に値を指定できます。
- [Service nodes]：Cisco WAAS サービス ノード グループはポリシー マップによって使用されます。デフォルトでは、WNG-Default というサービス ノード グループが 1 つ含まれます。テンプレートを複数のサイトに使用する場合は、サービス ノード グループを空のままにして、導入時に実際の IP アドレスを追加します。次の詳細を入力します。
  - サービス ノードの名前
  - 説明
  - Cisco WAAS サービス ノードの IP アドレス

- [Interception]：Cisco WAAS を有効にする必要があるインターフェイス ロール。導入時に、インターフェイスの実際のリストが表示されます。デバイスに属する実際のインターフェイスを、デバイスごとに選択できます。インターフェイス ロールの目的は、選択内容をデフォルトによって初期化することです。したがって、テンプレートのデザイン ビューで有効なインターフェイス ロールのリストが空になっている可能性があります。次の操作を実行できます。
  - [Enable WAAS] チェックボックスをオンまたはオフにします。
- [General]：有効なクラスタ ID の範囲は 1 ～ 32 です。チェックボックスを使ってクラスタを有効または無効にします。次の詳細を入力します。
  - Cluster ID
  - Authentication Key
  - この後、[分散の有効化（Enable Distribution）] チェックボックスをオンまたはオフにします。
- [Traffic redirection]：これは、ポリシー関連の設定、ポリシーマップ、クラスマップ、およびそれらと ISR-WAAS グループとの関係です。単純な設定によって、すべての TCP トラフィックを 1 つのノード グループにリダイレクトするデフォルト ポリシーを作成します。カスタム ポリシーを作成して各種の TCP トラフィックを別の ISR-WAAS にリダイレクトするには、[エキスパート モード（Expert Mode）] を選択します。

ステップ 4 [Save as Template] をクリックします。

ステップ 5 [Finish] をクリックします。

[設定（Configuration）] > [テンプレート（Templates）] > [機能およびテクノロジー（Features & Technologies）] > [マイ テンプレート（My Templates）] を選択して、設定したテンプレートを表示できます。

Cisco AppNav テンプレートの展開

作成した Cisco AppNav テンプレートを適用して、トラフィック分散を開始できます。

Cisco AppNav テンプレートを導入するには、次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [テンプレート（Templates）] > [機能およびテクノロジー（Features and Technologies）]** を選択します。

ステップ 2 左側のウィンドウ ペインで [My Templates] フォルダを選択します。

ステップ 3 導入する Cisco WAAS テンプレートを選択し、[Deploy] をクリックします。

1 つまたは複数のデバイスを選択して必要な設定を変更できます。

ステップ 4 [Value Assignment] パネルで各ターゲット デバイスを選択し、1 つずつそのルータのすべてのフィールドに入力します。

- [Basic Parameters]：クラスタが有効であるかどうかを示します。

- [Controllers]：コントローラの IP アドレスのリスト。デバイス自体に割り当てられている IP アドレスを含める必要があります。
- [Node Groups]：ポリシーで使用される各 ISR-WAAS グループに属する IP アドレスを入力します。
- [Interception]：Cisco WAAS 代行受信が有効になっている一連の WAN インターフェイス。

ステップ 5 [Apply] をクリックします。

ステップ 6 [OK] をクリックします。

Cisco AppNav が複数のデバイスに導入されます。

（注） テンプレートを 1 つ以上のデバイスに導入すると、ジョブが作成されます。テンプレートの展開のステータスを確認し、失敗、成功、または警告に関する詳細なステータス情報を表示するには、**[管理（Administration）] > [ダッシュボード（Dashboards）] > [ジョブ ダッシュボード（Job Dashboard）]** を選択します。テンプレートの作成後は、必要に応じて何度でも編集できます。

ISR-WAAS コンテナで作成する場合の Cisco AppNav の設定方法

Cisco AppNav は、Cisco 4451-X ISR デバイスまたはプラットフォームでのみ設定できます。また、ISR-WAAS アクティベーションの必須ソフトウェア バージョンが、バージョン 3.10 以降である必要があります。この方法では、Cisco WAAS 仮想アプライアンス ノード（ISR4451X-WAAS）のインストールの一環として、自動的に設定が行われます。

- 単一のサービス ノード グループに、新しく作成された ISR-WAAS が含まれます。
- Cisco WAAS サービス ノードによって最適化される各種のトラフィックに対して、クラスマップが作成されます。
- すべての TCP トラフィックを Cisco WAAS サービス ノードにリダイレクトするデフォルト ポリシー マップが作成されます。
- Cisco WAAS クラスタが作成されます。
- インターフェイス ロール（コンテナ アクティベーション時に指定）で表されたインターフェイスで Cisco WAAS が有効化されます。

この方式で Cisco AppNav を設定する方法については、「Cisco WAAS コンテナの作成」を参照してください。

第 41 章

Cisco WAAS コンテナを使用した WAN の最適化

- Cisco WAAS コンテナを使用して WAN を最適化する方法 （1091 ページ）
- Cisco WAAS コンテナをインストールするための前提条件 （1092 ページ）
- Cisco Prime Infrastructure と Cisco WAAS Central Manager の統合 （1092 ページ）
- Cisco WAAS Central Manager ユーザの作成 （1094 ページ）
- Cisco Prime Infrastructure から Cisco WAAS Central Manager を起動する方法 （1094 ページ）
- Cisco WAAS コンテナの OVA イメージのインポート （1095 ページ）
- アクティブ化時に Cisco WAAS コンテナを自動的に設定する （1096 ページ）
- Cisco WAAS コンテナの作成 （1096 ページ）
- Cisco WAAS コンテナをアンインストールおよび非アクティブ化する方法 （1098 ページ）
- Cisco WAAS コンテナを非アクティブ化する方法 （1099 ページ）

Cisco WAAS コンテナを使用して WAN を最適化する方法

Cisco Wide Area Application Services（Cisco WAAS）コンテナは、強力な WAN 最適化アクセラレーション ソリューションです。

（注） この章では、Cisco WAAS デバイスをルータと呼び、Cisco WAAS コンテナをコンテナと呼びます。

- Cisco WAAS コンテナをインストールするための前提条件 （1092 ページ）
- 単一デバイスでの Cisco WAAS コンテナのインストール （1097 ページ）
- 複数デバイスでの Cisco WAAS コンテナのインストール （1097 ページ）
- 単一デバイスでの Cisco WAAS コンテナのアンインストール （1098 ページ）
- Cisco WAAS コンテナを非アクティブ化する方法 （1099 ページ）

CiscoWAASコンテナをインストールするための前提条件

Cisco WAAS コンテナをインストールする前に、Cisco Prime Infrastructure で次の設定を行う必要があります。

- Cisco Prime Infrastructure と Cisco WAAS Central Manager の統合
- Cisco WAAS コンテナの OVA イメージのインポート

（注） Cisco WAAS コンテナの名前が 22 文字を超えないようにしてください。

Cisco Prime Infrastructure と Cisco WAAS Central Manager の統合

Cisco WAAS Central Manager で Cisco-WAAS を管理するには、Cisco WAAS Central Manager に登録する必要があります。Cisco WAAS Central Manager への Cisco WAAS の登録は、Cisco WAAS の CLI か Cisco WAAS Central Manager GUI、または Prime Infrastructure を通じて Cisco WAAS をアクティブ化する際に行うことができます。WCM は定期的に Cisco 4451-X サービス統合型ルータ（ISR）をポーリングし、現在のステータス情報を取得して設定を同期させます。

一般的な Cisco WAAS の展開は、Prime Infrastructure と Cisco WAAS Central Manager の両方のアプリケーションから構成されます。Cisco WAAS Central Manager の IP が Cisco WAAS の有効化時に使用されます。Cisco WAAS を有効にした後で Cisco WAAS Central Manager に登録されます。Prime Infrastructure は、次の理由で WCM の IP アドレスとサーバ名が必要です。

- Cisco WAAS Central Manager に新しい Cisco WAAS を通知する
- モニタリングのために Cisco WAAS Central Manager GUI を相互起動する

（注） Cisco WAAS Central Manager の設定はワンタイム設定です。Cisco WAAS Central Manager で Prime Infrastructure を認証するには Cisco WAAS Central Manager の IP アドレスが必要であり、Prime Infrastructure の [設定（Settings）] メニューを使ってこれを設定します。

（注） Cisco WAAS Central Manager の IP を Prime Infrastructure に設定しないと、新たにアクティブ化された Cisco WAAS が Cisco WAAS Central Manager に登録されません。

Prime Infrastructure で Cisco WAAS Central Manager の IP アドレスとサーバ名を設定するには、次の手順を実行します。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** を選択します。

ステップ 2 [サービス コンテナの管理（Service Container Management）] をクリックします。

ステップ 3 WCM IP アドレスと WCM サーバ名を入力します。

ステップ 4 [保存（Save）] をクリックします。

WCM は次の条件下で展開できます。

Prime Infrastructure は、Prime Infrastructure で設定されているアクティブな Cisco WAAS Central Manager とのみ連携します。

Cisco WAAS Central Manager のフェールオーバー後は、Prime Infrastructure と Cisco WAAS Central Manager のインターワーキングを再び正常に動作させるために、次のいずれかを実行する必要があります。

- Prime Infrastructure で新しい Cisco WAAS Central Manager の IP アドレスを再設定する。
- 障害が発生した Cisco WAAS Central Manager をアクティブにする。

Cisco Prime Infrastructure から Cisco WAAS Central Manager を起動するためのシングル サイオンの設定

シングル サインオン（SSO）機能を設定すると、既存の シングル サインオン機能を使用して Prime Infrastructure からシームレスに Cisco WAAS Central Manager を起動できます。

SSO を設定するには：

ステップ 1 **[管理（Administration）] > [ユーザ、ロール、および AAA（User, Roles & AAA）] > [SSO サーバ（SSO Servers）]** を選択します。

ステップ 2 [コマンドの選択（Select a command）] ドロップダウン リストから [SSO サーバの追加（Add SSO Server）] を選択します。

ステップ 3 SSO サーバで使用する SSL/TLS 証明書のタイプを選択します。自己署名証明書または認証局（CA）の証明書タイプから選択します。

ステップ 4 自己署名証明書タイプを使用している場合は、SSO サーバとして機能している Prime Infrastructure の IP アドレスを入力します。CA 証明書を使用している場合は、SSO サーバとなる Prime Infrastructure サーバの IP アドレスまたは FQDN のいずれかを入力します。

（注） シングル サインオン機能を提供するブラウザ Cookie は、ここで指定した IP アドレスまたは FQDN に従ってブラウザに保存されます。したがって、すべてのクライアントにわたって一貫性がある IP アドレスまたは FQDN を SSO サーバに入力する必要があります。

ステップ 5 [実行（Go）] をクリックします。

ステップ 6 [Save] をクリックします。

ステップ 7 [AAA Mode Settings] を選択します。

ステップ 8 [SSO] オプション ボタンを選択します。

ステップ 9 [保存（Save）] をクリックします。

ステップ 10 WCM IP アドレスを設定します。WCM IP アドレスの設定方法については、「Cisco Prime Infrastructure と Cisco WAAS Central Manager の統合」を参照してください。

ステップ 11 IP アドレスを設定した後、Prime Infrastructure からログアウトし、WCM にログインしてユーザ名を作成します。

Cisco WAAS Central Manager ユーザの作成

ステップ 1 WCM にログインします。

ステップ 2 **[ホーム（Home）] > [管理（Admin）] > [AAA] > [ユーザ（Users）]** を選択します。

ステップ 3 [作成（Create）] をクリックします。

ステップ 4 Prime Infrastructure のユーザ名と一致するユーザ名を入力します。

ステップ 5 **[ロール管理（Role Management）]** を選択し、**[管理（admin）]** をクリックして RBAC ロールを割り当て、ユーザ アカウントを作成します。

ステップ 6 **[ドメイン管理（Domain Management）]** を選択してロールとドメインを割り当てます。

ステップ 7 [送信（Submit）] をクリックします。

ステップ 8 **[デバイス（Devices）] > [設定（Configure）] > [AAA] > [NCS シングル サインオン（NCS Single Sign-On）]** を選択します。

ステップ 9 [Enable NCS Single Sign-On] チェックボックスをオンにして、CAS/SSO サーバの URL を入力します。

ステップ 10 [Submit] をクリックして、証明書を作成します。

ステップ 11 証明書が作成された後、**[実行（Submit）]** をクリックします。

Cisco Prime Infrastructure から Cisco WAAS Central Manager を起動する方法

次の方法で Cisco WAAS Central Manager をクロス起動できます。

- 単一デバイスからの Cisco WAAS Central Manager の起動
- 複数のデバイスからの Cisco WAAS Central Manager の起動

単一デバイスからの Cisco WAAS Central Manager の起動

Device Work Center から Cisco WAAS Central Manager をクロス起動するには：

ステップ 1 **[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ネットワーク デバイス（Network Devices）]** の順に選択します。

ステップ 2 Cisco WAAS デバイスを選択します。

下のペインにデバイスの詳細が表示されます。

ステップ 3 [Service Container] タブをクリックします。

ステップ 4 対応する Cisco WAAS コンテナを選択して、[WCM の起動（Launch WCM）] をクリックします。

複数のデバイスからの Cisco WAAS Central Manager の起動

[導入済みサービス（Deployed Services）] からクロス起動するには：

ステップ 1 **[運用（Operate）] > [導入済みサービス（Deployed Services）]** を選択します。

ステップ 2 対応する Cisco WAAS コンテナを選択して、[WCM の起動（Launch WCM）] をクリックします。

（注） Cisco WAAS Container Lifecycle を使用すると、ユーザはサービス コンテナをインストール、アンインストール、アクティブ化、または非アクティブ化することができます。

Cisco WAAS コンテナの OVA イメージのインポート

Cisco WAAS コンテナの OVA イメージをインポートするには、次の手順を実行します。

ステップ 1 **[サービス（Services）] > [ルータ仮想コンテナ（Router Virtual Containers）] > [WAAS-XE]** を選択します。

ステップ 2 次のいずれかの場所から OVA イメージを選択します。

- Device
- URL
- Protocol
- File

ステップ 3 [送信（Submit）] をクリックして Prime Infrastructure にイメージをインポートします。

ステップ 4 [更新（Refresh）] をクリックし、**[サービス（Services）] > [ルータ仮想コンテナ（Router Virtual Containers）] > [WAAS-XE] > [サービス カタログ（Services Catalogue）]** フォルダ内のインポートされたイメージを表示します。

アクティブ化時に Cisco WAAS コンテナを自動的に設定する

Cisco WAAS コンテナは、単一のルータに設定するか（単一デバイスでの Cisco WAAS コンテナのインストール）、または複数のルータに設定するか（複数デバイスでの Cisco WAAS コンテナのインストール）によって、2 つの異なる方法で設定できます。

Cisco WAAS コンテナのインストールは、2 つの方法で実行できます。コンテナをインストールした後でアクティブ化するか、インストールとアクティブ化を同時に行うことができます。

（注） Cisco WAAS コンテナの名前が 22 文字を超えないようにしてください。

Cisco WAAS コンテナの作成

Cisco WAAS コンテナをインストールするには、次の手順を実行します。

始める前に

- Cisco WAAS をインストールし、アクティブ化するには、各リソース プロファイルに十分なメモリがあることを確認します。次のメモリが必要です。
  - Cisco WAAS-750 の場合は 4194304 KB メモリおよび 2 個のCPU
  - Cisco WAAS-1300 の場合は 6291456 KB メモリおよび 4 個の CPU
  - Cisco WAAS-2500 の場合は 8388608 KB メモリおよび 6 個の CPU
- Cisco WAAS をインストールしてアクティブ化するには、750 リソース プロファイルの場合、ルータに 8 GB の RAM が必要です。
- Cisco WAAS がインストールされてアクティブになると、Cisco AppNav が自動的に設定されます。

ステップ 1 **[サービス（Services）] > [ルータ仮想コンテナ（Router Virtual Containers）] > [WAAS-XE] > [サービス カタログ（Services Catalogue）]** を選択し、OVA イメージをインポートします。OVA イメージのインポート方法については、「Cisco WAAS コンテナの OVA イメージのインポート」を参照してください。

ステップ 2 インポート後、[更新（Refresh）] をクリックして、インポートしたイメージを表示します。

ステップ 3 [展開（Deploy）] をクリックします。

ステップ 4 [ネットワーク ウィザード（Network Wizard）] ページで、コンテナを設定する Cisco WAAS デバイスを選択します。

ステップ 5 [インストール（Install）] オプション、または [インストールおよび有効化（Install and Activate）] を選択し、ドロップダウン リストからリソース プロファイルを選択します。

（注） Cisco WAAS デバイスは、複数選択できます。[デバイスの選択（Device Selection）] 領域で同じ Cisco WAAS デバイスが選択されている場合は、[リソースプロファイル（Resource Profile）] ドロップダウンリストを使用してプロファイルを選択できます。[デバイスの選択（Device Selection）] 領域で異なる Cisco WAAS デバイスが選択されている場合は、[リソースプロファイル（Resource Profile）] ドロップダウン リストは [サービスコンテナパラメータ（Service Container Parameter）] 領域に表示されません。[サービスコンテナパラメータ（Service Container Parameter）] 領域で、選択されているデバイスのそれぞれにプロファイルを選択し、[保存（Save）] をクリックする必要があります。

ステップ 6 [OK] をクリックして、Cisco WAAS コンテナをインストールします。

ステップ 7 [WAAS-XE with AppNav-XE へのトラフィックのリダイレクト（Redirect Traffic to WAAS-XE with AppNav-XE）] チェックボックスをオンにしてインストールし、アクティブにします。

ステップ 8 [OK] をクリックし、Cisco WAAS コンテナをインストールしてアクティブにします。

単一デバイスでの Cisco WAAS コンテナのインストール

Cisco WAAS コンテナを単一のルータにインストールするには、次の手順を実行します。

ステップ 1 **[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ネットワーク デバイス（Network Devices）]** の順に選択します。

ステップ 2 表示されたリストから、Cisco WAAS コンテナをインストールするルータを選択します。

ステップ 3 [Service Container] タブをクリックします。

ステップ 4 [Add] をクリックし、各フィールドに設定の詳細の入力します。

ステップ 5 [OK] をクリックします。

複数デバイスでの Cisco WAAS コンテナのインストール

Cisco WAAS コンテナを複数のルータにインストールするには、次の手順を実行します。

ステップ 1 **[サービス（Services）] > [ルータ仮想コンテナ（Router Virtual Containers）]** を選択します。

ステップ 2 インポートした OVA イメージが含まれている Cisco WAAS フォルダを選択します。

ステップ 3 [展開（Deploy）] をクリックします。

表示されたリストから、Cisco WAAS コンテナをインストールするルータを選択します。

展開後、[インストール（Install）] または [インストールおよび有効化（Install and Activate）] のいずれかをクリックします（「Cisco WAAS コンテナの作成」）。

ステップ 4 [インストールおよび有効化（Install and Activate）] を選択した場合は、[値割り当て（Value Assignment）] 領域で次の詳細を入力します。

- Cisco WAAS の IP アドレス/マスクを入力します
- ルータの IP/マスクを入力します
- サービス コンテナ名を入力します
- リソース プロファイルを選択します

ステップ 5 [OK] をクリックします。

Cisco WAAS コンテナをアンインストールおよび非アクティブ化する方法

[デバイス ワーク センター（Device Work Center）] または [導入済みサービス（Deployed Services）] から Cisco WAAS コンテナを非アクティブ化できます。デバイス ワーク センターでは単一の Cisco WAAS コンテナを非アクティブ化できますが、[導入済みサービス（Deployed Services）] では複数の Cisco WAAS コンテナを非アクティブ化できます。

単一デバイスでの Cisco WAAS コンテナのアンインストール

[デバイス ワーク センター（Device Work Center）] から単一の Cisco WAAS コンテナをアンインストールするには、次の手順を実行します。

ステップ 1 **[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ネットワーク デバイス（Network Devices）]** の順に選択します。

ステップ 2 表示されたリストで、Cisco WAAS コンテナをアンインストールするルータをクリックして選択します。

ステップ 3 下部ペインで [Service Container] タブをクリックします。

ステップ 4 [Uninstall] をクリックします。

ステップ 5 [OK] をクリックします。

複数デバイスでの Cisco WAAS コンテナのアンインストール

[導入済みサービス（Deployed Services）] から複数の Cisco WAAS コンテナをアンインストールするには、次の手順を実行します。

ステップ 1 **[サービス（Services）] > [ルータ仮想コンテナ（Router Virtual Containers）] > [WAAS-XE] > [導入済みサービス（Deployed Services）]** を選択します。

ステップ 2 表示されたリストで、Cisco WAAS コンテナをアンインストールする複数のルータをクリックして選択します。

ステップ 3 [Uninstall] をクリックします。

ステップ 4 [OK] をクリックします。

（注） Prime Infrastructure を介して Cisco WAAS 仮想アプライアンスをアンインストールすると、対応する Cisco AppNav の設定も削除されます。

Cisco WAAS コンテナを非アクティブ化する方法

次の 2 つの方法で Cisco WAAS コンテナを非アクティブ化できます。

- 単一の Cisco WAAS コンテナの非アクティブ化
- 複数の Cisco WAAS コンテナの非アクティブ化

単一の Cisco WAAS コンテナの非アクティブ化

[デバイス ワーク センター（Device Work Center）] の単一の Cisco WAAS コンテナを非アクティブ化するには、次の手順を実行します。

ステップ 1 **[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ネットワーク デバイス（Network Devices）]** の順に選択します。

ステップ 2 デバイス グループ リストから Cisco WAAS デバイス名を選択します。

ステップ 3 [Service Container] タブをクリックします。

ステップ 4 [Deactivate] をクリックします。

複数の Cisco WAAS コンテナの非アクティブ化

[導入済みサービス（Deployed Services）] の複数の Cisco ISR-WAAS コンテナを非アクティブ化するには：

ステップ 1 **[サービス（Services）] > [ルータ仮想コンテナ（Router Virtual Containers）] > [WAAS-XE] > [導入済みサービス（Deployed Services）]** を選択します。

ステップ 2 リストから複数の Cisco WAAS デバイス名を選択します。

ステップ 3 [非アクティブ化（Deactivate）] をクリックします。

第 42 章

ワイヤレス モビリティの使用

- モビリティとは （1101 ページ）
- WLAN 階層型モビリティとは （1102 ページ）
- モビリティ ワーク センターを使用したモビリティ ドメインの表示 （1103 ページ）
- コントローラ グループからのモビリティ ドメインの作成 （1104 ページ）
- モビリティ アンカーとは （1106 ページ）
- Spectrum Expert とは （1108 ページ）
- モビリティ ネットワークにおける脅威からの保護を目的とした Cisco Adaptive wIPS プロファイルの使用 （1109 ページ）

モビリティとは

モビリティ（ローミング）とは、安全かつ最小限の遅延で、あるアクセス ポイントから別のアクセス ポイントへアソシエーションをシームレスに維持するワイヤレス クライアントの機能です。より柔軟なローミングを可能にし、トラフィックのトンネル カプセル化の必要性を最小限にするために、Prime Infrastructure は、ネットワーク デバイス全体にモビリティ機能を提供する堅固なモビリティ アーキテクチャを用意しています。

モビリティ アーキテクチャの主要要素は次のとおりです。

- モビリティ コントローラ（MC）：MC（Cisco 5700 シリーズ ワイヤレス コントローラなど）は1つ以上のMAまたはスイッチ ピア グループを受け持ち、その制御範囲内でのローミングと、MA 間または MC 間（または MA と MC 間）を移動するトラフィックを処理します。
- モビリティ エージェント（MA）：MA（Catalyst 3650 や Catalyst 3850 スイッチなど）は、WAP が直接接続されるアクセス スイッチまたはエッジ スイッチに配置され、WAP との通信用 CAPWAP トンネルの終端となります。
- モビリティ オラクル（MO）：MO は大規模展開において複数の MC またはモビリティ サブドメインを接続する最上位のコントロールエンティティであり、非常に大きな物理領域でのローミングを可能にします。
- モビリティ ドメイン（ローミング ドメイン）：モバイル ユーザは、このドメイン（WAP とそれに関連するすべての制御エンティティ）のデバイス全体をローミングできます。通

常、これには MA と MC が含まれますが、MO が含まれる場合もあります（複数のサブドメインを結合するため）。

- モビリティ サブドメイン：WAP とそれに関連する複数の MA および 1 つの MC。大規模なモビリティ ドメインの一部を担います（複数のサブ ドメイン間のローミングは MO によって調整されます）。
- スイッチ ピア グループ（SPG）：スイッチのグループ（MA として機能）。SPG は、グループ メンバー間にフル メッシュのモビリティ トンネルを確立し、グループ内のスイッチに関連する WAP 全体にわたって効率的なローミングをサポートします。また、SPG は、ハンドオフ中のスイッチ間のインタラクションの範囲を制限するためにも使用されます。SPG はモビリティ コントローラによって設定され、スイッチ ピア グループ内のすべてのスイッチがメンバーシップに対して同一のビューを持ちます。SPG 内のスイッチは、一連のダイレクト トンネルによって相互接続される場合もあります。同じスイッチ ピア グループ内であるスイッチから別のスイッチにステーションがローミングするときに、Point of Presence が元のスイッチまたはアンカー スイッチにとどまる場合は、MTE を使用せずに、トラフィックを直接トンネリングしてアンカー スイッチに戻すことができます。この直接トンネリング メカニズムはデータ パスの最適化であり、オプションです。
- モビリティ グループ：モビリティ グループは一連の MC（および関連する MA/スイッチ ピア グループ）です。
- モビリティ トンネル エンドポイント：モビリティ トンネル エンドポイント（MTE）は、トンネリングを使用してモバイル デバイスにデータ プレーン サービスを提供します。これにより、ネットワーク上のユーザの Point of Presence を一定に保ち、ローミング イベントのネットワークへの影響を最小化します。ローミング対象のクライアントの VLAN またはサブネットを MTE で使用可能な場合、MTE は Point of Presence となることができます。使用できない場合、MTE は単なるトンネル スイッチング エンティティとして機能し、Point of Presence であるアクセス スイッチまたは MTE にローミング対象のクライアントを接続します。

関連トピック

モビリティ ワーク センターを使用したモビリティ ドメインの表示 （1103 ページ）
コントローラ グループからのモビリティ ドメインの作成 （1104 ページ）

WLAN 階層型モビリティとは

階層型モビリティは、ワイヤレス LAN コントローラ構成において新しいモビリティと呼ばれます。Cisco Prime Infrastructure 2.0 は、Cisco WLC 7.6 を実行している Cisco 5508 と WiSM2 プラットフォームに新しいモビリティ機能を提供します。

Prime Infrastructure の新しいモビリティ機能の主要機能は、次のとおりです。

- Mobility Work Center は、Cisco WLC 7.6 を実行している Cisco 5508 と WiSM 2 プラットフォームを検出し、階層型モビリティ アーキテクチャの構築に必要な操作を提供します。このアーキテクチャには、2 つのデバイス タイプ（Cisco 5508 と WiSM2）とモビリティ エージェントとして展開されている Cisco 3650/3850 が含まれます。

- 階層型モビリティアーキテクチャを展開するときに、LifeCycleビューを使用して、WLAN、VLAN、セキュリティ、ゲスト アンカーなどの無線機能を Cisco 5508 と WiSM2 に設定できます。
- Cisco 5508 および WiSM2 でのフラット モビリティ アーキテクチャの展開は、クラシックビューでのみサポートされ、ワイヤレス設定全体はクラシックおよび LifeCycle ビューのままになります。
- Prime Infrastructure 2.0 の場合、IOS ベースのデバイス（3850 と 5760）では、一部の無線機能（VLANインターフェイスの作成など）は引き続き CLI テンプレートを使用して設定されます。

新しいモビリティ機能の詳細については、『Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points for Release 7.3.112.0』の「Hierarchical Mobility (New Mobility)」の項を参照してください。

モビリティ ワーク センターを使用したモビリティ ドメインの表示

Mobility Work Center を使用するには、**[サービス（Services）]** > **[モビリティサービス（Mobility Services）]** > **[モビリティドメイン（Mobility Domains）]** を選択します。

次の情報が表示されます。

- [Device Name]：MC の名前。
- [Management IP]：MC の管理 IP アドレス。
- [Wireless Interface IP]：モビリティ プロトコルで使用される MC の IP アドレス。
- [Mobility Group]：MC が属しているモビリティ グループの名前。
- [Mobility Role]：管理および動作のモビリティ モードを表示します。[Admin] と [Operational] の値が異なる場合は、管理モードを有効にするためにデバイスをリブートする必要があります。モビリティ オラクルが有効な場合は、モビリティ モードに加えて MO が表示されます。

このページでは、次のタスクを実行できます。

- モビリティ ドメインの作成。
- スイッチ ピア グループの作成：MC にスイッチ ピア グループを作成します。
- モビリティ ロールの変更：MA から MC にコントローラを変更します。
- ドメインの削除：ドメインのみを削除します。コントローラは Prime Infrastructure から削除されません。
- メンバーの削除：選択したドメインから選択した MC を削除します。

- モビリティ オラクルとして設定：MC をドメイン全体の MO として動作させる場合は、選択した MC で MO を有効にします。ドメインごとに 1 つの MO のみが存在できます。Cisco 5760 シリーズのコントローラだけが MO 機能をサポートしています。
- スイッチ ピア グループへのメンバーの追加：スイッチ ピア グループにメンバーを追加します。
- スイッチ ピア グループからのメンバーの削除：スイッチ ピア グループからメンバーを削除します。

（注） デフォルトでは、[Mobility Work Center] ページには、管理対象ネットワークに設定されているすべてのモビリティ ドメインが表示されます。モバイル デバイスのリストを表示するには、左側のサイドバーから [All Mobility Devices] を選択します。

関連トピック

モビリティとは （1101 ページ）
コントローラ グループからのモビリティ ドメインの作成 （1104 ページ）

コントローラグループからのモビリティドメインの作成

モビリティ ドメインは互いの IP アドレスが設定されたコントローラの集合であり、クライアントはモビリティ ドメイン内のコントローラ間でローミングできます。

[Mobility Work Center] には、Prime Infrastructure によって管理対象ネットワーク内に設定されたすべてのモビリティ ドメインが表示されます。

左側のサイドバー メニューからノードを選択すると、右側のペインに詳細が表示されます。左側のサイドバー メニューからドメイン ノードを選択すると、右側のペインにドメイン内の MC が表示されます。

モビリティ ドメインを作成するには：

ステップ 1 **[サービス（Services）] > [モビリティ サービス（Mobility Services）] > [モビリティ ドメイン（Mobility Domains）]** を選択します。

ステップ 2 左側のサイドバー メニューをクリックします。

ステップ 3 グループ化する一連の MC のモビリティ ドメインの名前を入力します。

選択した MC が別のドメインに存在している場合、MC はそのドメインから削除され、新しいドメインに追加されます。

ステップ 4 モビリティ ドメインのメンバー デバイスを選択します。

デバイスは 1 つのドメインまたは SPG にのみ属することができます。

ステップ 5 [Apply] をクリックします。

スイッチ グループからのモビリティ スイッチ ピア グループの作成

MC にはスイッチ ピア グループ（SPG）を含めることができ、スイッチ ピア グループには MA を含めることができます。管理対象ネットワークの MA は [Switch Peer Group] ページに表示されます。すでに存在しているスイッチ ピア グループを作成すると、古いスイッチ ピア グループから新しいスイッチ ピア グループに MC が移動され、すべての MA に MC ワイヤレス インターフェイスの IP アドレスが設定されます。

スイッチ ピア グループを作成するには、次の手順を実行します。

ステップ 1 **[サービス（Services）] > [モビリティサービス（Mobility Services）] > [モビリティドメイン（Mobility Domains）]** の順に選択します。

ステップ 2 左側のサイドバーから MC を選択します。

ステップ 3 [Create Switch Peer Group] をクリックします。

ステップ 4 選択した MC にグループ化する、一連の MA を含めるスイッチ ピア グループの名前を入力します。

選択した MA が別のスイッチ ピア グループに存在している場合、MA はそのグループから削除され、新しいグループ追加されます。MC に複数のスイッチ ピア グループを作成できます。

ステップ 5 モビリティ エージェントを選択します。

デバイスは 1 つのドメインまたは SPG にのみ属することができます。

ステップ 6 [Apply] をクリックします。

作成した SPG が左側のサイド バーに表示されます。そこに移動して、選択したスイッチ ピア グループのモビリティ エージェントを表示できます。

デバイスのモビリティ ロールの変更

デフォルトでは、Cisco 3850 コントローラは MA として動作します。ネットワーク で MC が必要な場合は、これらの コントローラを MC に変換できます。

モビリティ ロールを変更するには：

ステップ 1 **[サービス（Services）] > [モビリティサービス（Mobility Services）] > [モビリティドメイン（Mobility Domains）]** の順に選択します。

ステップ 2 [All Mobility Devices] を選択します。

ステップ 3 変更先のロールとデバイスを選択します。

- [Change Role To Mobility Controller]：選択したコントローラでモビリティ コントローラ機能を有効にします。
- [Change Role To Mobility Agent]：選択したコントローラでモビリティ エージェント機能を有効にします。これを実行すると、MC 機能が無効化されます。
- MA から MC（またその逆）への変換は、3850 デバイスでのみ行うことができます。ロールの変更を有効にするには、デバイスをリブートする必要があります。
- [Assign Mobility Group]：選択したデバイスの新しいモビリティ グループ名を入力します。

ステップ 4 [Apply] をクリックします。

モビリティ アンカーとは

モビリティ アンカーは、WLAN のアンカー コントローラとして指定されるモビリティ グループのサブセットです。この機能は、クライアントのネットワークへのエントリ ポイントに関係なく、WLAN を 1 つのサブネットに制限する際に使用されます。これによって、ユーザは企業全体にわたりパブリック WLAN やゲスト WLAN にアクセスできますが、引き続き特定のサブネットに制限されます。また、WLAN は建物の特定のセクション（ロビー、レストランなど）を表すことができるため、ゲスト WLAN で地理的ロード バランシングを実現できます。

クライアントが、WLAN のモビリティ アンカーとして事前設定されているモビリティ グループのコントローラに最初にアソシエートすると、クライアントはローカルでそのコントローラにアソシエートし、クライアントのローカル セッションが作成されます。クライアントは、WLAN の事前設定されたアンカー コントローラにのみアンカーできます。指定された WLAN の場合、モビリティ グループのすべてのコントローラ上で同じセットのアンカー コントローラを設定する必要があります。

クライアントが、WLAN のモビリティ アンカーとして設定されていないモビリティ グループのコントローラに最初にアソシエートすると、クライアントはローカルでそのコントローラにアソシエートし、ローカルセッションがクライアントのために作成され、コントローラは同じモビリティ グループの別のコントローラへ通知されます。その通知に対する回答がない場合、コントローラは WLAN に設定されたいずれかのアンカー コントローラに連絡をとり、ローカルスイッチ上のクライアントに対する外部セッションを作成します。クライアントからのパケットは EtherIP を使用してモビリティ トンネルを介してカプセル化され、アンカー コントローラに送信されます。ここでカプセルを解除されて有線ネットワークへ配信されます。クライアントへのパケットは、アンカー コントローラで受信され、EtherIP を使用してモビリティ トンネルを介して外部コントローラへ転送されます。外部コントローラはパケットのカプセルを解除し、クライアントへ転送します。

WLAN のモビリティ ゲスト アンカー コントローラの設定

ゲスト アンカー コントローラはゲスト トラフィック専用のコントローラであり、非武装地帯（DMZ）とも呼ばれる非保護ネットワーク領域に配置されます。トラフィック発信元の他の内部 WLAN コントローラは、エンタープライズ LAN に配置されます。

（注） Cisco 5760 コントローラはゲスト アンカーとして指定できますが、Catalyst 3850 スイッチはゲスト アンカーとして指定できません。ただし、外部コントローラとして指定できます。

ロードバランシングのために WLAN のモビリティ アンカーとしてゲスト コントローラを設定できます。

はじめる前に

- Prime Infrastructure にワイヤレス デバイスが設定されていることを確認します。ワイヤレス デバイスの設定方法については、「*Configuring Wireless Features*」を参照してください。
- WLAN のモビリティ アンカーとして設定するワイヤレス デバイスが、同じモビリティ ドメイン内にあることを確認します。

WLAN のゲスト アンカー コントローラを設定するには：

手順の概要

1. [Inventory] > [Device Management] > [Network Devices] の順に選択します。
2. [Device Group] 領域で、[Device Type] を展開し、次に [Wireless Controller] を展開します。
3. ゲスト モビリティ アンカーとして指定するコントローラを選択します。デバイスの詳細が、ページの下部に表示されます。
4. [Configuration] タブをクリックします。
5. 左側のサイドバーのメニューから、[WLANs] > [WLAN 設定（WLAN Configuration）] の順に選択します。[WLAN Configuration] ページが表示されます。
6. 必要な WLAN ID の URL を選択します。タブ付きのページが表示されます。
7. [Advanced] タブをクリックし、ページ下部にある [Mobility Anchors] リンクをクリックします。[Mobility Anchors] ページが表示されます。
8. モビリティ アンカーとして指定するコントローラの [IP address] チェックボックスをオンにして、[Save] をクリックします。

手順の詳細

ステップ 1 [Inventory] > [Device Management] > [Network Devices] の順に選択します。

ステップ 2 [Device Group] 領域で、[Device Type] を展開し、次に [Wireless Controller] を展開します。

ステップ 3 ゲストモビリティ アンカーとして指定するコントローラを選択します。デバイスの詳細が、ページの下部に表示されます。

ステップ 4 [Configuration] タブをクリックします。

ステップ 5 左側のサイドバーのメニューから、[WLANs] > [WLAN 設定（WLAN Configuration）] の順に選択します。[WLAN Configuration] ページが表示されます。

（注） クラシック ビューを使用している場合は、[Configure] >[Controllers] > [Ctrl IP addr] > [WLANs] > [WLAN Configuration] の順に選択して、[WLAN Configuration] 詳細ページにアクセスします。

ステップ 6 必要な WLAN ID の URL を選択します。タブ付きのページが表示されます。

ステップ 7 [Advanced] タブをクリックし、ページ下部にある [Mobility Anchors] リンクをクリックします。[Mobility Anchors] ページが表示されます。

（注） また、[WLAN Configuration] ページから [Mobility Anchors] ページにアクセスすることもできます。目的の WLAN ID のチェックボックスをオンにします。[Select a command] ドロップダウン リストから、[Mobility Anchors] を選択し、[Go] をクリックします。[Mobility Anchors] ページが表示されます。

ステップ 8 モビリティ アンカーとして指定するコントローラの [IP address] チェックボックスをオンにして、[Save] をクリックします。

Spectrum Expert とは

Spectrum Expert クライアントは、リモート干渉センサーとして機能し、動的な干渉データを Prime Infrastructure に送信します。この機能により、Prime Infrastructure はネットワーク内の Spectrum Expert から詳細な干渉データを収集、モニタ、およびアーカイブできます。

Spectrum Expert を設定するには、[サービス（Services）] > [モビリティ サービス（Mobility Services）] > [Spectrum Experts] の順に選択します。このページには、次の項目を含むすべての Spectrum Expert の一覧が表示されます。

- [Hostname]：Spectrum Expert ラップトップのホスト名または IP アドレス。
- [MAC Address]：ラップトップのスペクトラム センサー カードの MAC アドレス。
- [到達可能性ステータス（Reachability Status）]：Spectrum Expert が正常に稼働し、情報を Prime Infrastructure に送信しているかどうかを示します。ステータスは、[到達可能（Reachable）] または [到達不能（Unreachable）] と表示されます。

[Spectrum Expert] ページのフィールドの説明については、『Cisco Prime Infrastructure Reference Guide』の「*Mobility Services*」の項を参照してください。

干渉源データを収集するためのモビリティ Spectrum Expert の設定

Spectrum Expert を追加する手順は、次のとおりです。

手順の概要

1. [Services] > [Mobility Services] > [Spectrum Experts] の順に選択します。
2. [Select a command] ドロップダウン リストから、[Add Spectrum Expert] を選択します。このリンクは、Spectrum Expert が 1 つも追加されていない場合にだけ表示されます。[Select a command] ドロップダウン リストから [Add a Spectrum Expert] を選択しても、[Add a Spectrum Expert] ページにアクセスできます。
3. Spectrum Expert のホスト名または IP アドレスを入力します。ホスト名を使用する場合、Spectrum Expert を Prime Infrastructure に追加するには DNS に登録する必要があります。

手順の詳細

ステップ 1 [Services] > [Mobility Services] > [Spectrum Experts] の順に選択します。

ステップ 2 [Select a command] ドロップダウン リストから、[Add Spectrum Expert] を選択します。このリンクは、Spectrum Expert が 1 つも追加されていない場合にだけ表示されます。[Select a command] ドロップダウン リストから [Add a Spectrum Expert] を選択しても、[Add a Spectrum Expert] ページにアクセスできます。

ステップ 3 Spectrum Expert のホスト名または IP アドレスを入力します。ホスト名を使用する場合、Spectrum Expert を Prime Infrastructure に追加するには DNS に登録する必要があります。

Spectrum Expert として正しく追加するには、Spectrum Expert クライアントが稼働しており、Prime Infrastructure に通信するように設定されていなければなりません。

詳細については、『Cisco Prime Infrastructure Reference Guide』の「*Mobility Services*」の項を参照してください。

モビリティネットワークにおける脅威からの保護を目的とした Cisco Adaptive wIPS プロファイルの使用

Prime Infrastructure にはいくつかの定義済みプロファイルが用意されており、そこから選択できます。これらのプロファイル（カスタマー タイプ、ビルディング タイプ、業界タイプなどに基づきます）を使用すると、Cisco Adaptive wIPS を通じて使用可能な追加のワイヤレスの脅威保護をすばやくアクティブにできます。プロファイルは「そのまま」使用することも、要件に合わせてカスタマイズすることもできます。

定義済みプロファイルには次のものがあります。

- Education
- EnterpriseBest
- EnterpriseRogue
- Financial
- HealthCare
- HotSpotOpen
- Hotspot8021x

- Military
- Retail
- Tradeshow
- Warehouse

[wIPS プロファイル（wIPS Profiles）] > [プロファイル リスト（Profile List）] ページでは、現在の wIPS プロファイルの表示、編集、適用、削除を行ったり、新しいプロファイルを追加したりできます。[プロファイル リスト（Profile List）] には、各プロファイルの次の情報が表示されます。

- [Profile Name]：現在のプロファイルのユーザ定義名を示します。プロファイルの詳細を表示または編集するには、プロファイル名をクリックします。

マウス カーソルをプロファイル名に移動すると、プロファイル ID とバージョンが表示されます。

- [MSE(s) Applied To]：このプロファイルが適用されている Mobility Services Engine（MSE）の数を示します。MSE 番号をクリックすると、プロファイルの割り当ての詳細が表示されます。
- [Controller(s) Applied To]：このプロファイルが適用されているコントローラの数を示します。コントローラ番号をクリックすると、プロファイルの割り当ての詳細が表示されます。

wIPS プロファイルを作成するには、次の手順を実行します。

手順の概要

1. [Services] > [Mobility Services] > [wIPS Profiles] の順に選択します。
2. [Select a command] ドロップダウン リストから、[Add Profile] を選択し、[Go] をクリックします。
3. [Profile Parameters] ページの [Profile Name] テキスト ボックスにプロファイル名を入力します。
4. ドロップダウン リストから該当する定義済みのプロファイルを選択するか、[Default] を選択します。
5. [Save] > [Next] を選択します。
6. 既存グループを編集または削除したり、新しいグループを追加するには：
7. 現在のプロファイルに含めるポリシーを指定するには、[Profile Configuration] を選択します。ポリシー ツリーのチェックボックス（左側の [Select Policy] ペインにあります）は、現在のプロファイルで有効または無効になっているポリシーを示します。このページでは次の操作を実行できます。
8. プロファイル設定が完了したら、[Next] を選択して [MSE/Controller] ページに進みます。
9. [Apply Profile] ページで、現在のプロファイルを適用するモビリティ サービス エンジンとコントローラを選択し、[Apply] をクリックして、選択したモビリティ サービス エンジン/コントローラに現在のプロファイルを適用します。

手順の詳細

ステップ 1 [Services] > [Mobility Services] > [wIPS Profiles] の順に選択します。

ステップ 2 [Select a command]ドロップダウン リストから、[Add Profile] を選択し、[Go] をクリックします。

ステップ 3 [Profile Parameters] ページの [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 4 ドロップダウン リストから該当する定義済みのプロファイルを選択するか、[Default] を選択します。

ステップ 5 [Save] > [Next] を選択します。

[Save] を選択すると、モビリティ サービス エンジンまたはコントローラの割り当てや変更なしで、プロファイルが Prime Infrastructure データベースに保存されます。プロファイルはプロファイル リストに表示されます。

ステップ 6 既存グループを編集または削除したり、新しいグループを追加するには：

a) [SSID Group List] ページの [Select a command] ドロップダウン リストから、[Add Group] または [Add Groups from Global List] を選択し、[Go] をクリックします。

b) グループ名と 1 つ以上の SSID グループを入力し、[Save] をクリックします。

ステップ 7 現在のプロファイルに含めるポリシーを指定するには、[Profile Configuration] を選択します。ポリシー ツリーのチェックボックス（左側の [Select Policy] ペインにあります）は、現在のプロファイルで有効または無効になっているポリシーを示します。このページでは次の操作を実行できます。

- 該当するブランチまたはポリシーのチェックボックスをオン/オフすることで、ブランチ全体や個別のポリシーを有効化または無効化することができます。

デフォルトでは、すべてのポリシーが選択されています。

- ポリシーの説明を表示するには、個々のポリシーをクリックします。[Policy Rules] ページを使用して、現在のポリシー ルールの設定を追加、編集、削除、並べ替えることができます。

（注） 1 つ以上のポリシー ルールが存在する必要があります。リスト内で唯一のポリシー ルールは削除できません。

（注） プロファイルがコントローラに適用されている場合、そのプロファイルは削除できません。

- 次の設定を行います。
  - [Threshold]（すべてのポリシーに適用されるわけではありません）：選択したポリシーに関連付けられたしきい値または上限を示します。すべてのポリシーに 1 つ以上のしきい値が含まれている必要があるため、標準的なワイヤレス ネットワークの問題に基づいて、各ポリシーにデフォルトのしきい値が定義されています。しきい値オプションは、選択したポリシーに応じて異なります。
  - ポリシーのしきい値に達すると、アラームが生成されます。Cisco Adaptive wIPS DoS およびセキュリティ ペネトレーション攻撃からのアラームは、セキュリティ アラームとして分類されます。これらの攻撃の要約は [Security Summary] ページに表示されます。このページにアクセスするには [Monitor] > [Security] を選択します。wIPS の攻撃は [Threats and Attacks] セクションにあります。
  - [Severity]：選択したポリシーの重大度を示します。パラメータとしては、[critical]、[major]、[info]、および [warning] があります。このフィールドの値は、ワイヤレス ネットワークに応じて変わります。

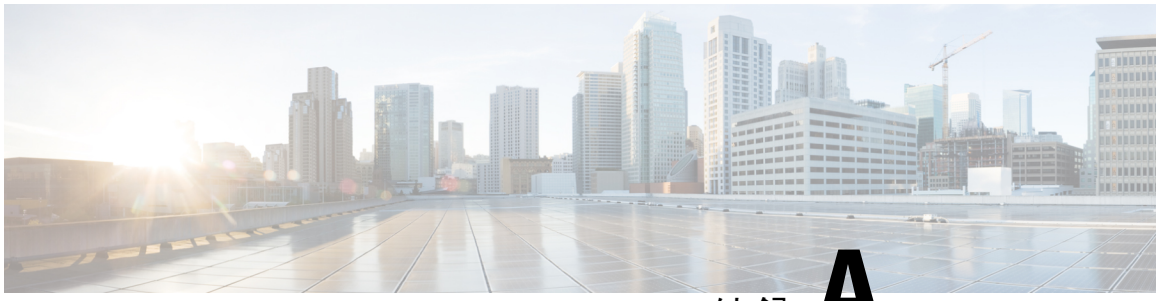
- [Notification]：閾値に関連付けられた通知の種類を示します。
- [ACL/SSID Group]：この閾値が適用される ACL または SSID グループを示します。

（注） 選択されたグループに対してのみポリシーが適用されます。

ステップ 8 プロファイル設定が完了したら、[Next] を選択して [MSE/Controller] ページに進みます。

ステップ 9 [Apply Profile] ページで、現在のプロファイルを適用するモビリティ サービス エンジンとコントローラを選択し、[Apply] をクリックして、選択したモビリティ サービス エンジン/コントローラに現在のプロファイルを適用します。

また、プロファイル リストから直接プロファイルを適用することもできます。[Profile List] ページで、適用するプロファイルを選択し、[Select a command] ドロップダウン リストで [Apply Profile] をクリックします。次に、[Go] をクリックして [Apply Profile] ページにアクセスします。



付録 A

Cisco Prime Infrastructure ユーザ インターフェイスの参照

• Cisco Prime Infrastructure ユーザ インターフェイスの参照 （1113 ページ）

Cisco Prime Infrastructure ユーザ インターフェイスの参照

Cisco Prime Infrastructureは Web ベースのアプリケーションです。

インストール済みの Cisco Prime 製品のいずれかがライセンスによって有効化されていない場合、それらの機能のメニュー項目やオプションは Web インターフェイスに表示されません。

• Cisco Prime Infrastructure ユーザ インターフェイスについて
• 一般的な UI タスク
• 検索方法

Cisco Prime Infrastructure ユーザ インターフェイスについて

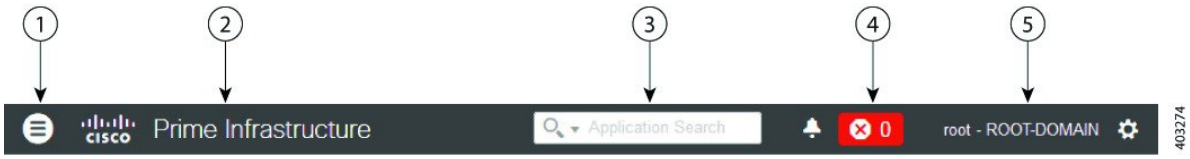
Cisco Prime Infrastructureは Web ベースのアプリケーションです。

インストール済みの Cisco Prime 製品のいずれかがライセンスによって有効化されていない場合、それらの機能のメニュー項目やオプションは Web インターフェイスに表示されません。

初めて Prime Infrastructure にログインした際に、オーバーレイ ウィンドウにグラフィカル インターフェイスの主要コンポーネントが表示されます。このオーバーレイ ウィンドウを再度表示するには、画面の右上にあるログイン名をクリックし、**[ヘルプ（Help）]>[はじめに（Getting Started）]** を選択します。

図 58-1 に表示されているツールバーは、各ページの上部にあります。

図 *29 : Prime Infrastructure* のツールバー



1	クリックすると、メニューが開きます。
2	クリックすると、cisco.com の Prime Infrastructure 製品ページに移動します。
3	Prime Infrastructure 内のデータを検索するときに入力します。IP アドレス、ユーザー名、アプリケーション名、または設定アーカイブの一部またはすべてなど、テキスト文字列を入力できます。uration archives. 検索結果には、アクセス ポイント、アラーム、変更監査、設定アーカイブ、デバイスなどの情報が表示されます。検索結果を CSV 形式および PDF 形式でエクスポートするには、右隅にあるエクスポート アイコンをクリックします。
4	アラームの数が表示されます。色は使用しているネットワーク内の最も重大度が高いアラームに対応しています。クリックすると、アラーム概要ウィンドウにすべてのアラームが表示され、重大度別（クリティカル、メジャー、マイナー）にアラームの数が示されます。
5	割り当てられているログイン名と仮想ドメインが表示されます。ユーザ設定の変更、パスワードの変更、ログアウト、ヘルプへのアクセス、製品フィードバックの送信を行う際にクリックします。

関連トピック

検索方法 （1129 ページ）

[ドック（Dock）] ウィンドウ

通常、Cisco Prime Infrastructure 内のサブセクション ページを閲覧する場合、[ドック（Dock）] ウィンドウにそのページに簡単に移動できる方法が表示されます。Cisco Prime Infrastructure の任意のページから、[ドック（Dock）] アイコン（右上隅）をクリックすることができます。

- 現在のページに関連するビデオへのリンク
- 最近アクセスしたページへのリンク（最大 15 個）
- お気に入りとしてマークされたページへのリンク（最大 15 個）
- ピン止めした項目

[ドック（Dock）] ウィンドウは閉じるまで開いた状態を維持します。

関連トピック

[ドック（Dock）] ウィンドウへのデバイスのピン止め （1115 ページ）

[ドック（Dock）] ウィンドウへのデバイスのピン止め

特定のデバイスを詳細に確認する場合は、[ドック（Dock）] ウィンドウにデバイスをピン止めできます。最大 15 個の項目をピン止めできます。

ステップ 1 [デバイスの 360 度ビュー（Device 360° View）] で [ドックへの追加（Add to Doc）] アイコンをクリックします。

デバイスは、[ドック（Dock）] ウィンドウの [ピン止めした項目（Pinned Items）] セクションに表示されます。

ステップ 2 Prime Infrastructure の任意の場所にある [ドック（Dock）] ウィンドウのデバイスのリンクをクリックすると、[デバイスの 360 度ビュー（Device 360° View）] に更新済み情報が表示されます。

ステップ 3 [ドック（Dock）] ウィンドウから項目を削除するには、項目の横にある [ごみ箱（Trash）] アイコンをクリックします。[ピン止めした項目（Pinned Items）] から削除されます。

Filters

フィルタ機能を使用すると、Cisco Prime Infrastructure インターフェイスに関する特定の情報を表示できます。データが表形式で表示されるときは常に [Filter] アイコンが表示されます。次のタイプのフィルタを使用できます。

- クイック フィルター-を参照してください クイック フィルタ 。
- フィルター オプションの設定-を参照してください 詳細フィルタ 。
- ダッシュ ボード フィルター-を参照してください ダッシュボード フィルタ 。

クイック フィルタ

このフィルタを使用すると、フィルタを特定のテーブル列に適用することで、テーブル内のデータを絞り込むことができます。さまざまな演算子を適用するには、[高度なフィルタ（Advanced Filter）] オプションを使用します（「詳細フィルタ」を参照）。

クイック フィルタを起動するには、[フィルタ（Filter）] ドロップダウン リストから [クイック フィルタ（Quick Filter）] を選択します。

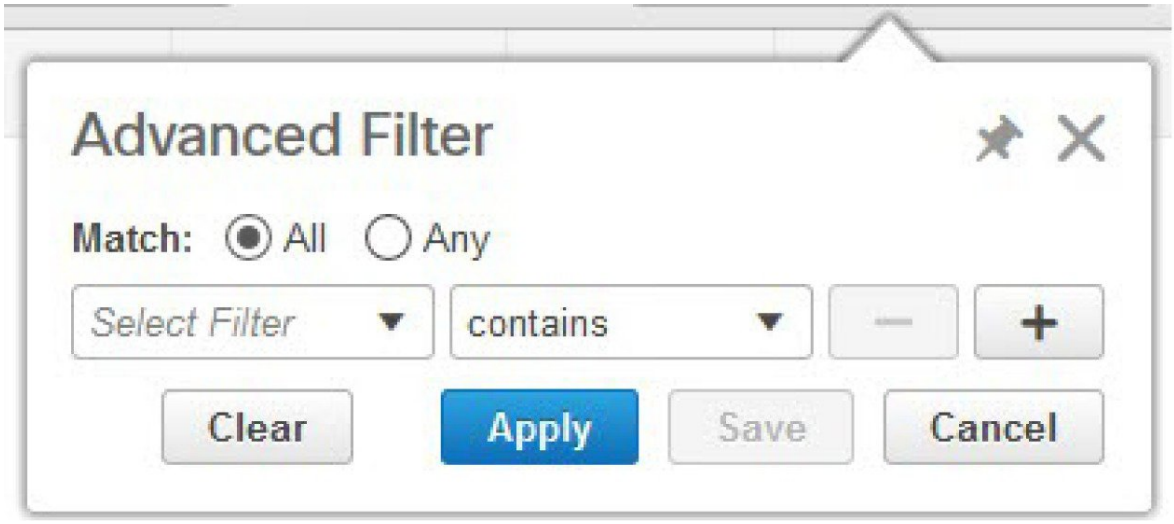
クイック フィルタをクリアするには、[フィルタ（Filter）] をクリックします。

詳細フィルタ

このフィルタを使用すると、Does not contain、Does not equal、Ends with、Is empty など、複数の演算子を使用してフィルタを適用することによって、表内のデータを絞り込むことができます。たとえば、ドロップダウン リストからフィルタ パターン（テーブル列名ごと）と演算子を選択できます。さらに、Prime Infrastructureデータベースで使用可能なデータに基づいて、フィルタ基準を入力する必要があります。

拡張フィルタ機能を起動するには、[フィルタ（Filter）] ドロップダウン リストから [拡張フィルタ（Advanced Filters）] を選択します。

図 *30* : 拡張フィルタ



拡張フィルタで使用するフィルタ基準を保存するには、次の手順を実行します。

ステップ 1 拡張フィルタの基準を入力して、[Go] をクリックします。フィルタ基準に基づいて、データがフィルタリングされます。

ステップ 2 データがフィルタリングされたら、[保存（Save）] アイコンをクリックします。

ステップ 3 [プリセットフィルタの保存（Save Preset Filter）] ダイアログボックスで、プリセット フィルタの名前を入力して、[保存（Save）] をクリックします。

ダッシュボード フィルタ

[Filters] ツールバーを使用すると、ダッシュボードのすべてのダッシュレットに表示するデータを絞り込むことができます。このツールバーを使用し、以下の基準によってダッシュレットのデータをフィルタリングできます。

- [Time frame]：いずれかのプリセット オプションを選択するか、カスタムのタイム フレームを作成します。
- クライアント —クライアント属性を選択または入力します。

（注） クライアント ユーザー名フィールドは、"（二重引用符）以外の特殊文字をサポートしています。

"（二重引用符）以外の特殊文字を使用することもできます。

- [Applications]：1 つのサービス、最大 10 個のアプリケーション、またはすべてのアプリケーションを選択します。
- [Network Aware]：有線、ワイヤレス、またはすべてのネットワークを選択します。

• [Site]：1 つのサイト、未割り当てサイト、またはすべてのサイトを選択します。

図 *31* : ダッシュボードの *[Filters]* ツールバー

ダッシュボードのすべてのダッシュレット向けにデータをフィルタリングするには、次の手順を実行します。

ステップ 1 ダッシュボードを開きます（例：**[ダッシュボードの概要（Dashboard Overview）] > [概要（Overview）] > [一般（General）]** を選択）。

ステップ 2 [フィルタ（Filters）] ツールバーで任意のオプションの設定を変更し、[実行（Go）] をクリックします。

データ入力機能

大部分のユーザ インターフェイスには、チェックボックスに加えて、ドロップダウン リストとデータ入力フィールドがあり、Cisco Prime Infrastructure ではいくつかの専用データ入力機能が使用されます。これらの機能の目的はネットワークのビューを可能な限り整えることですが、ユーザは、必要に応じて、独自の設定を追加、更新、保存することができます。これらの専用データ入力機能は、次のとおりです。

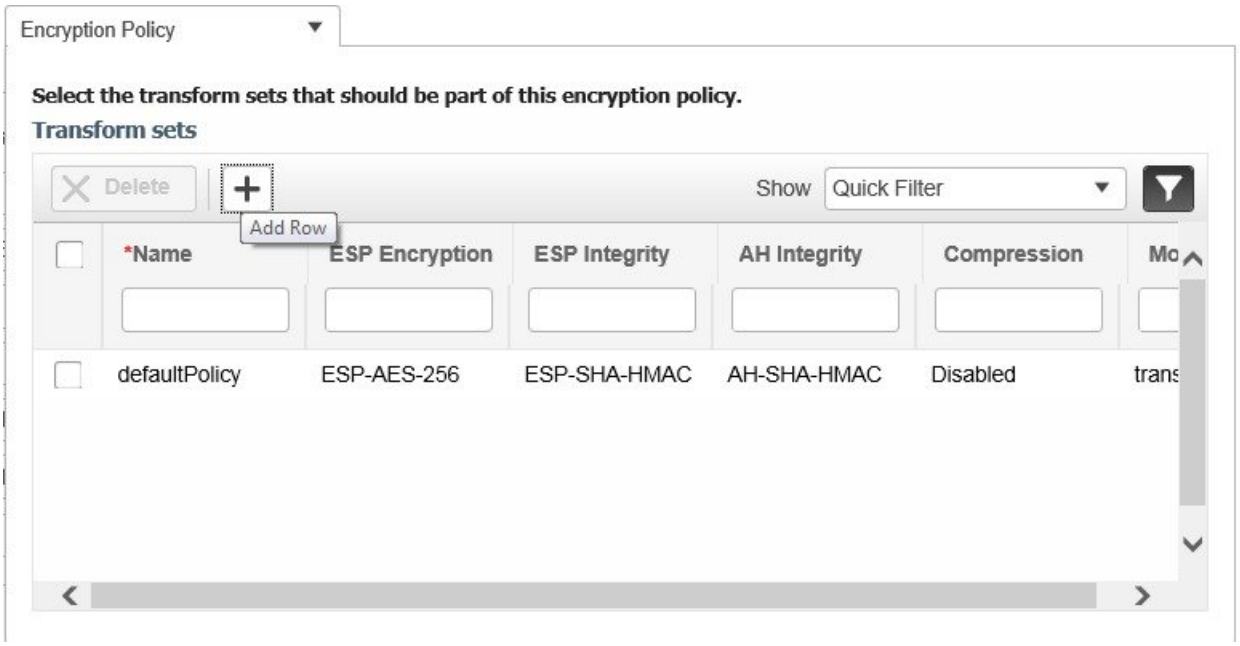
- 編集テーブル
- データ ポップアップ

編集テーブル

Cisco Prime Infrastructure では、サイト、デバイス、イベントのリストなど、テーブルを使用してさまざまな種類のデータが表示されます。スプレッドシートと同様に、データは行と列に配置されます。

編集テーブルは他のテーブルとは異なり、そこに含まれているデータを追加、編集、削除することができます。一部の編集テーブルでは、フィルタにアクセスすることもできます（「Filters」を参照）。通常、編集テーブルは、チェックボックスをオンにすると開くデータ ポップアップに表示されます。

図 *32* : 編集テーブル



編集テーブルの使用方法：

- 編集テーブルに新規行を追加するには：

[+] アイコンをクリックし、新しい行のフィールドに入力して [Save] をクリックします。

- 編集テーブルから 1 つ以上の既存の行を削除するには：

行ヘッダーのチェックボックス（各行の左端）をオンにして、[Delete] をクリックします。

- 編集テーブルの行でフィールドのエントリを更新するには：

行ヘッダーまたはフィールドをクリックし、内容を編集して [Save] をクリックます。

データのポップアップ

データ ポップアップは、チェックボックス、固定フィールド、その他のデータ入力機能に関連するウィンドウです。機能を選択すると自動的に表示されるので、機能に関連するデータを表示したり更新することができます。データ ポップアップには、チェックボックス、ドロップダウンリスト、データ入力フィールドに加えて、編集テーブルが含まれていることがあります。

データ ポップアップを使用するには：

1. データ ポップアップを開く機能（固定フィールドやチェックボックスなど）を選択します。
2. 関連するポップアップが表示されるので、必要に応じてフィールドを表示または更新します。
3. 作業が完了したら、データ ポップアップの外側をクリックします。新しい情報を入力したり、既存の情報を変更した場合は、変更内容が自動的に保存されます。

インタラクティブ グラフ

Cisco Prime Infrastructure は、時間ベースと非時間ベースの両方のデータのインタラクティブな折れ線、面積、円、積み積み重ね棒グラフを提供します。インタラクティブ グラフには次の機能が含まれています。

- 自動更新のサポート：グラフは事前に定義された間隔で自動的に更新されます。
- 次の 2 つのグラフ ビューがあります。
  - グラフ（チャート）ビュー（デフォルト）
  - テーブル（グリッド）ビュー
- グラフの拡大

関連項目

- インタラクティブ グラフの使用方法
- 時間ベースのグラフ

インタラクティブ グラフの使用方法

次の表は、インタラクティブ グラフの使用方法の要約を示しています。

表 *88* : インタラクティブ グラフの使用

目的	操作
グラフボタンを使ってヘルプを参照する	マウス カーソルをボタンの上に置きます。Cisco Prime Infrastructure には、ボタンを説明するポップアップ ツールチップが表示されます。
データをグラフまたはチャートとして表示する	[View in Chart] をクリックします。
グリッドまたは表形式でデータを表示する	[View in Grid] をクリックします。
グラフを拡大する	グラフの右下にあるボタンをクリックします。Cisco Prime Infrastructure は別のページのかグラフの拡大バージョンが表示されます。新しいページでは [View in Chart] と [View in Grid] 切り替えボタンを使用できるので、表示する拡大グラフの種類を変更できます。

関連項目

- インタラクティブ グラフ
- 時間ベースのグラフ

時間ベースのグラフ

一部のグラフには時間ベースのデータが表示されます。時間ベースのグラフの場合、Cisco Prime Infrastructure ではグラフの上にリンク バーが表示されます。リンク バーには、チャートのデータ タイプに応じた標準のタイムフレーム（直近 6 時間、1 日など）を示す一連のリンクが含まれています。これらのタイムフレーム リンクのいずれかを選択すると、そのタイム フレームのデータが取得され、グラフが更新されてそのタイムフレームのデータだけが表示されます。

時間ベースのグラフに表示されるタイムフレーム リンクには、以下のオプションがあります。

- [6h]：現在の時刻から最近の 6 時間分のデータを表します。データは、現在のデータベース テーブルから収集されます。
- [1d]：現在の時刻から最近の 1 日（24 時間）分のデータを表します。データは、現在のデータベース テーブルから収集されます。
- [1w]：現在の時刻から最近の 1 週間（7 日間）分のデータを表します。データは、時間単位で集積したテーブルから収集されます。
- [2w]：現在の時刻から最近の 2 週間分のデータを表します。データは、時間単位で集積したテーブルから収集されます。
- [4w]：現在の時刻から最近の 4 週間分のデータを表します。データは、時間単位で集積したテーブルから収集されます。
- [3m]：現在の時刻から最近の 3 ヵ月間分のデータを表します。データは、日単位で集積したテーブルから収集されます。
- [6m]：現在の時刻から最近の 6 ヵ月間分のデータを表します。データは、週単位で集積したテーブルから収集されます。
- [1y]：現在の時刻から最近の 1 年間（12 ヵ月間）分のデータを表します。データは、週単位で集積したテーブルから収集されます。
- [Custom]：ユーザが選択した期間。開始日時と終了日時を設定できます。現在のデータを使用するのか、または時間単位、日単位、週単位で集積したデータ元を使用するのかは、選択した開始日によって変わります。

時間ベースのグラフに表示される集約データのデフォルトの最大および最小保持期間は、Cisco Prime Infrastructure の管理者によって制御されます。詳細については、関連項目の「履歴データの保持について」を参照してください。

関連項目

- インタラクティブ グラフ
- インタラクティブ グラフの使用方法
- 履歴データの保持について

一般的な UI タスク

Cisco Prime Infrastructure のほぼすべてのウィンドウから、次のアクションを実行できます。

- [デバイス360度ビュー（Device 360° View）] からのデバイス詳細の取得 （1121 ページ）
- [ユーザ360度ビュー（User 360° View）] からのユーザ詳細の取得
- [ルータ360度ビュー（Router 360° View）] からの VRF 詳細の取得

[デバイス360度ビュー（Device 360° View）] からのデバイス詳細の取得

[デバイス 360 度ビュー（Device 360°View）] には、デバイス ステータス、インターフェイス ステータス、関連するデバイス情報など、詳細なデバイス情報が表示されます。デバイスの IP アドレスが表示されるほぼすべての画面で [Device 360°View] を表示できます。

デバイスの 360 度ビューを起動するには、デバイスの IP アドレスの横にある情報アイコンをクリックします。

図 58-5 は [デバイス360度ビュー（Device 360° View）] の一例を示しています。

（注） [デバイス 360 度ビュー（Device 360°View）] に表示される機能は、デバイス タイプによって異なります。

Cisco Prime Infrastructure ユーザ インターフェイスの参照

図 *33 : [*デバイス*360*度ビュー（*Device 360° View*）*]* の例

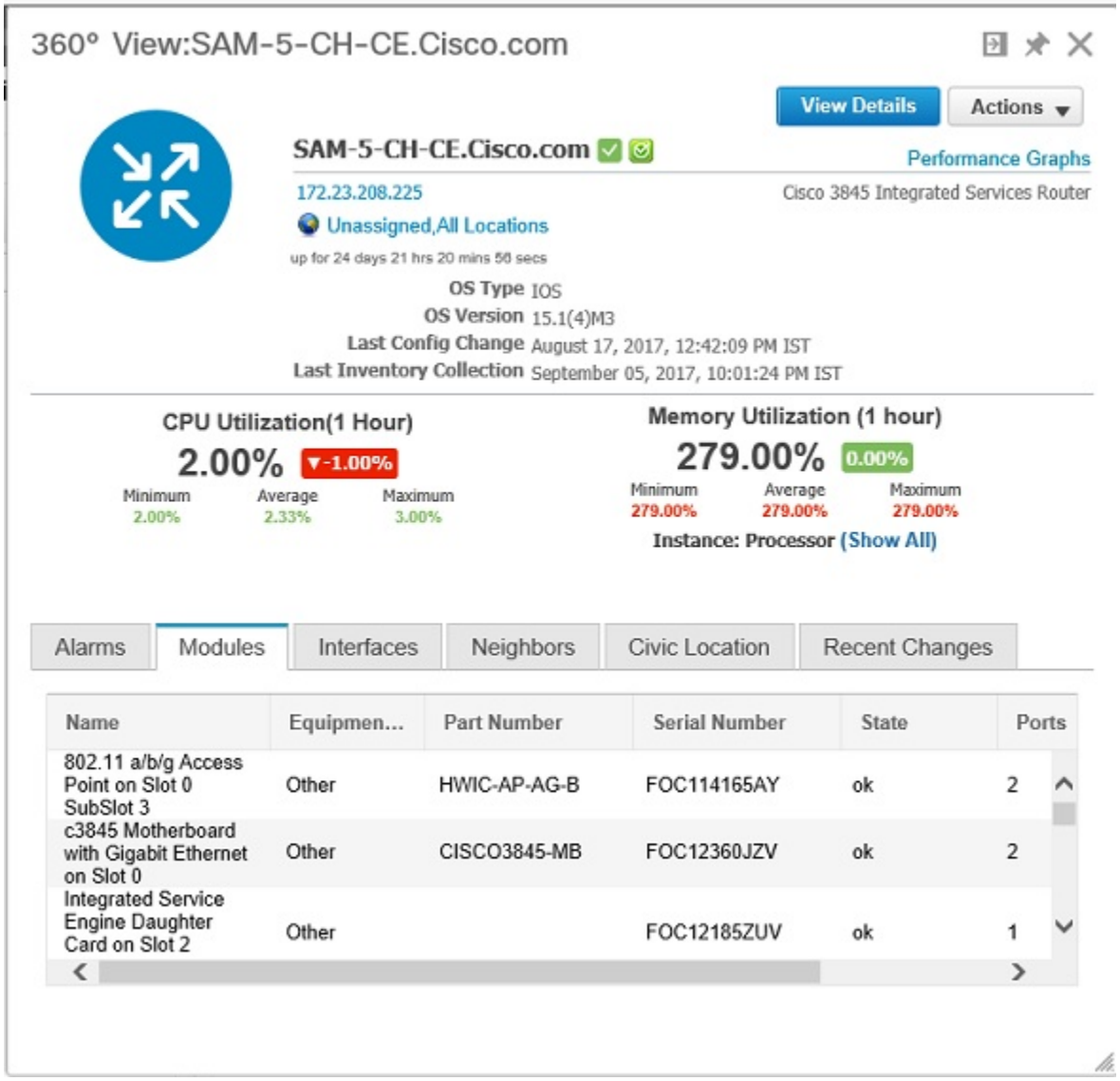


表 *89 : [*デバイス *360* 度ビュー（*Device 360°View*）*]* の機能

[Device 360°View] の機能	説明
デバイスのステータス	デバイスが到達可能かどうか、管理されているかどうか、および Cisco Prime Infrastructure データベース、CPU使用率、メモリ使用率が同期されているかどうかを示します。[すべて表示（Show All）] をクリックすると、デバイスのメモリ使用率のインスタンスがすべて表示されます。

Cisco Prime Infrastructure ユーザ インターフェイスの参照

[Device 360°View] の機能	説明
[アクション（Action）] ドロップダウン リスト	[Device 360°View] の右上にある [Action] ドロップダウン リストから、次のいずれかのオプションを選択します。 • [アラームブラウザ（Alarm Browser）]：アラーム ブラウザを起動します。詳細については、「アラームとイベントのモニタリング」を参照してください。 • [デバイスの詳細（Device Details）]：デバイスの詳細を表示します。 • [サポートコミュニティ（Support Community）]：シスコ サポート コミュニティを起動します。「シスコ サポート コミュニティとテクニカル アシスタンス センター（TAC）から支援を受ける」を参照してください。 • [サポート要求（Support Request）]：サポート ケースを開くことができます。詳細については、「シスコ サポート ケースの登録」を参照してください。 • [Ping]：デバイスを ping できます。 • [Traceroute]：デバイスに対して traceroute を実行できます。 • [デバイスへの接続（Connect to Device）]：Telnet、SSH、HTTP、および HTTPS プロトコルを使用してデバイスに接続できます。 • [今すぐ同期（Sync Now）]：デバイスを Cisco Prime Infrastructure データベース内に保存された設定と同期できます。 • [ルーティングテーブル情報（Routing Table Info）]：ルータおよび Nexus デバイスの VRF の詳細を示します。 （注） 360 度ビューの Telnet や SSH をクライアント ブラウザで動作させるには、いくつかの前提条件があります。 • Firefox：外部アプリケーション（Putty for Telnet、SSH 用 FireSSH アドオンなど）を使用します。 • Internet Explorer（IE）および Google Chrome：Telnet および SSH の Regedit エントリを追加します「関連項目」を参照してください。
アラーム	アラーム ステータス、タイム スタンプ、およびカテゴリなど、デバイスのアラームがリストされます。
Modules	デバイス モジュールと、それらの名前、タイプ、状態、およびポートがリストされます。
Interfaces	デバイス インターフェイスと、各インターフェイスの上位 3 つのアプリケーションがリストされます。設定済みの VRF を表示します（ルータおよび Nexus デバイスの場合のみ）。
ネイバー	ネイバーのインデックス、ポート、デュプレックス ステータス、および IP アドレスなど、デバイスのネイバーがリストされます。このタブでは、[タイプ（Type）]列にデバイス タイプ（CDP や LLDP など）も表示されます。近接デバイスが Cisco Prime Infrastructure で管理されている場合、デバイス名にはデバイスの詳細ページへのリンクが含まれ、情報アイコンを使用してデバイス 360 度ビューを起動できます。
シビック ロケーション	デバイスのネットワーク モビリティ サービス プロトコル（NMSP）ステータス、都市アドレス、およびロケーションの詳細が表示されます。

[Device 360°View] の機能	説明
ワイヤレスインターフェイス	インターフェイス名、関連する WLAN、VLAN ID、IP アドレスを一覧表示します。
WLAN	WLAN 名、SSID、セキュリティ ポリシー、およびクライアント数がリストされます。
最近の変更	選択したデバイスのユーザが行った最新の監査変更が 5 つ表示されます。これらの変更は次のように分類されます。 • インベントリ • 設定（Configuration） • ソフトウェア イメージの管理
仮想ドメイン	このタブには、特定のデバイスがメンバーになっている仮想ドメインの名前が一覧表示されます。

関連項目

- Internet Explorer と Google Chrome で Telnet と SSH を使用してデバイスに接続する

Internet Explorer と Google Chrome で Telnet と SSH を使用してデバイスに接続する

はじめる前に

Internet Explorer および Chrome に Telnet と SSH のブラウザ プラグインがインストールされていることを確認します。

Internet Explorer での Telnet クライアント機能の有効化

32 ビット Internet Explorer を搭載した 64 ビット Windows オペレーティング システムで Telnet クライアント機能を有効にするには、次の手順を実行します。

ステップ 1 コントロール パネルで Telnet クライアントを開きます。

- [コントロール パネル] に移動します。
- [Programs and Features] をクリックします。
- 左側のペインで [Windows の機能の有効化または無効化（Turn Windows features on or off）] をクリックします。
- [Telnet Client] チェックボックスをオンにします。
- [OK] をクリックします。

ステップ 2 Windows ディレクトリの System32 から同じディレクトリの SysWOW64 に、telnet.exe の 64 ビット バージョンをコピーします。

ステップ 3 32 ビット版 Internet Explorer の次のレジストリ キーを追加します。

- regedit.exe を開き、次のレジストリキーに移動します。

例：

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet
Explorer\MAIN\FeatureControl\FEATURE_DISABLE_TELNET_PROTOCOL
```

- キーをバックアップする場合は、FEATURE_DISABLE_TELNET_PROTOCOL を右クリックし、[export] を選択します。復元が必要になったときに簡単に検索できる場所にキーを保存します。

  （注） このキーが存在していない場合は、上記で指定されているキーを追加してください。

- FEATURE_DISABLE_TELNET_PROTOCOL を再び右クリックして [New] を選択し、ドロップダウンリストから [DWORD (32-bit) Value] を選択します。
- 右側のペインで、New Value を iexplore.exe に名前変更します。
- iexplore.exe の値が「0x00000000」であることを確認し、regedit.exe を終了します。

ステップ 4 System32\en-US\telnet.exe.mui ファイルを SysWOW64 \ en-US フォルダにコピーします。

SSH の有効化

Internet Explorer で SSH セッションを開始するには、次の手順を実行します。

ステップ 1 以下の内容を含む ssh.reg というファイルを作成します。

例：

```
REGEDIT4
[HKEY_CLASSES_ROOT\ssh]
@="URL:ssh Protocol"
"URL Protocol"=""
[HKEY_CLASSES_ROOT\ssh\shell]
[HKEY_CLASSES_ROOT\ssh\shell\open]
[HKEY_CLASSES_ROOT\ssh\shell\open\command]
@="\"C:\\Program Files\\putty\\putty.exe\" \"%1\""
```

ステップ 2 このファイルを実行して Windows レジストリに情報を追加します。

（注） Internet Explorer での Telnet クライアント機能の有効化と SSH の有効化を実行した場合は、その変更内容が Google Chrome にも反映されます。

関連トピック

[デバイス360度ビュー（Device 360° View）] からのデバイス詳細の取得 （1121 ページ）

[ユーザ360度ビュー（User 360° View）] からのユーザ詳細の取得

[User 360°View] には、エンド ユーザに関する以下の詳細情報が表示されます。

- エンド ユーザのネットワーク接続とアソシエーション
- 認証と認可
- ユーザのネットワーク接続に関連するネットワーク デバイスの潜在的な問題
- アプリケーション関連の問題
- 広範囲のネットワークにおけるその他の問題

ユーザの 360°ビューにアクセスするには、次の手順を実行します。

ステップ 1 **[モニタ（Monitor）] > [モニタリングツール（Monitoring Tools）] > [クライアントおよびユーザ（Clients and Users）]** を選択します。

ステップ 2 [ユーザ名（User Name）] 列の下のユーザ名の横にある展開アイコンをクリックします。[ユーザ 360 度ビュー（User 360°View）] を表示できます。

次の図に [ユーザ 360 度ビュー（User 360° View）] の例を示します。

Cisco Prime Infrastructure ユーザ インターフェイスの参照

図 *34 : [*ユーザ *360* 度ビュー（*User 360° View*）*]* の例

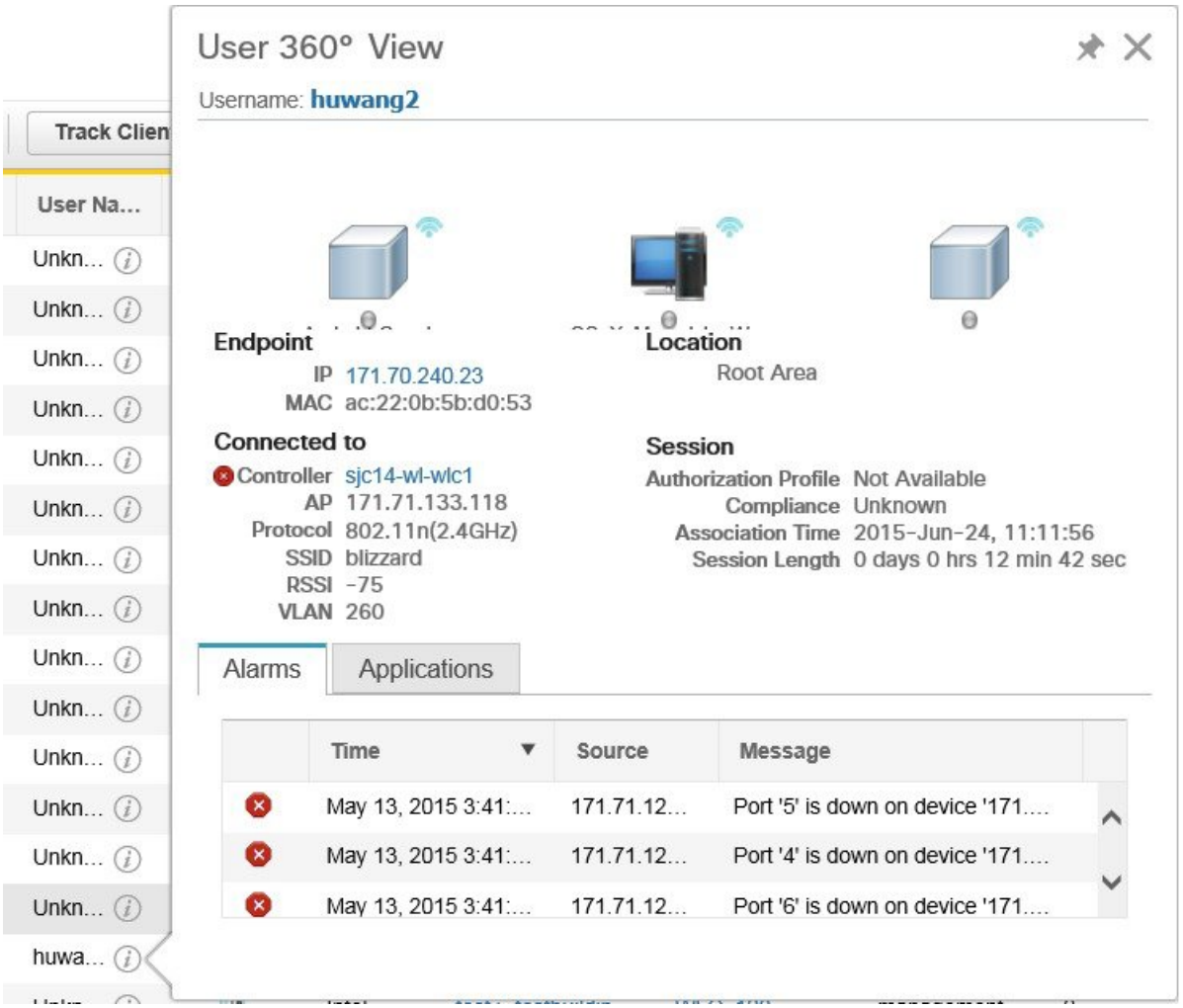


表 *90 : [User 360°View]* の機能

[User 360°View] の機能	説明
User information	エンド ユーザに関する重要な情報を表示します。
Endpoint	エンドポイント情報を表示します。この機能を使用するには、ISE サーバと統合する必要があります。
Connected To	ネットワーク接続情報を表示します。 • ネットワーク デバイス（アクセス スイッチまたは AP + コントローラ）：デバイスに関連するアクティブ アラームの発生と重大度を視覚的に表示します。 • 接続ポート：ポートに関連するアクティブ アラームの発生と重大度を視覚的に表示します。

[User 360°View] の機能	説明
LocationSession	ネットワーク セッション情報を表示します。 • ロケーションは Prime Infrastructure 階層での位置です。 • 認証プロファイル：認証に関連するエラーの発生を視覚的に表示します。この機能を使用するには、ISE サーバと統合する必要があります。 • エンドポイントのコンプライアンス ステータス。この機能を使用するには、ISE サーバと統合する必要があります。 • セッションの開始時刻と終了時刻
Alarms	ネットワーク セッションに関連するアラームと統計情報のリストを表示するには、[Alarms] タブをクリックします。
Applications	ネットワーク セッションに関連するアプリケーションと統計情報のリストを表示するには、[Applications] タブをクリックします。セッション情報（Netflow/NAM データ、保証ライセンス）が使用可能である必要があります。

[ルータ360度ビュー（Router 360° View）] からの VRF 詳細の取得

ルータの 360 度ビューには、次のルーティング プロトコルの VRF の詳細が表示されます。

- BGP ルーティング
- BGP ネイバー
- EIGRP ルーティング
- EIGRP ネイバー

ルータの 360 度ビューを使用して VRF 詳細を表示するには、次の手順を実行します。

ステップ 1 **[インベントリ デバイス管理（Inventory Device Management）] > [ネットワーク デバイス（Network Devices）]** を選択します。

ステップ 2 [デバイス グループ（Device Groups）] ペインで **[デバイス タイプ（Device Type）] > [ルータ（Routers）]** を選択します。

ステップ 3 詳細を表示するルータを選択します。

ルータの詳細が右側のペインに表形式で表示されます。

ステップ 4 ルータの IP アドレスの横にある情報アイコンをクリックします。

ステップ 5 ルータの 360 度ビューで、**[アクション（Actions）] > [ルーティング テーブル情報（Routing Table Info）]** を選択します。

ステップ 6 [VRF の選択（Select a VRF）] ドロップダウン リストから VRF を選択し、ルーティングの詳細を表示するプロトコルを選択します。

検索方法

Cisco Prime Infrastructure には次の検索方法が用意されています。

- アプリケーション検索：「アプリケーション検索機能の使用」を参照してください。
- 詳細検索：「アプリケーション検索機能の使用」を参照してください。
- 保存した検索：「保存した検索の使用」を参照してください。

検索オプションには、Cisco Prime Infrastructure 内のどのページからもアクセスできます。

アプリケーション検索機能の使用

Prime Infrastructure 内ですばやくデータを検索するために、任意のテキスト文字列を入力できます。たとえば、クライアントを検索する場合は、IP アドレスやユーザ名の一部またはすべてを入力できます。

ステップ 1 画面右下の [Search] アイコンをクリックします。

ステップ 2 [検索（Search）]テキスト ボックスで、検索文字列を入力し、**[検索（Search）]**Prime Infrastructure をクリックします。

[アプリケーション検索 (Application Search)] テキスト ボックスに複数の文字列を入力すると、指定されたすべてのキーワードに一致するすべての結果が返されます。また、管理対象デバイス、クライアント、アラーム、設定アーカイブ、変更監査、およびマップをアプリケーションから分離して検索することもできます。

（注） 検索テキストに特殊文字が含まれている場合、検索では正確な結果が返されません。[検索 (search)] テキスト ボックスにプレーン テキストを入力すると、特殊文字を含むすべての関連する結果が返されます。

ステップ 3 [リストの表示（View List）] をクリックして、[モニタ（Monitor）] ページまたは [設定（Configuration）] ページから一致するデバイスを表示します。

詳細検索機能の使用

ステップ 1 画面右下の [Search] アイコンをクリックします。

ステップ 2 [Search] プルダウン メニューから、[Advanced Search] を選択します。

ステップ 3 [Advanced Search] ダイアログ ボックスで、[Search Category] ドロップダウン リストからカテゴリを選択します。

ステップ 4 検索に適用できるすべてのフィルタまたはパラメータを選択します。

（注） 検索パラメータは、選択したカテゴリによって異なります。

ステップ 5 検索を保存するには、[検索の保存（Save Search）] チェックボックスを選択して、テキストボックスに検索の一意の名前を入力し、[実行（Go）] をクリックします。

（注）　検索結果ページに表示する情報を指定できます。

検索カテゴリは以下のとおりです。

- [アクセス ポイント（Access Points）]：「アクセス ポイントの検索」を参照してください。
- [アラーム（Alarms）]：「アラームの検索」を参照してください。
- [クライアント（Clients）]：「アラームの検索」を参照してください。
- [監査の変更（Change Audit）]：次を参照してください。 監査変更の詳細検索 （1137 ページ）
- [チョークポイント（Chokepoints）]：「チョークポイントの検索」を参照してください。
- [設定バージョン（Configuration Versions）]：「設定バージョンの検索」を参照してください。
- [コントローラ ライセンス（Controller Licenses）]：「コントローラ ライセンスの検索」を参照してください。
- [コントローラ（Controllers）]：「コントローラの検索」を参照してください。
- [デバイス タイプ（Device Type）]：「デバイス タイプの検索」を参照してください。
- [イベント（Events）]：「イベントの検索」を参照してください。
- [インターフェイス（Interferers）]：「干渉源の検索」を参照してください。
- [ジョブ（Jobs）]：「ジョブの検索」を参照してください。
- [マップ（Maps）]：「マップの検索」を参照してください。
- [不正クライアント（Rogue Client）]：「不正クライアントの検索」を参照してください。
- [孤立クライアント（Shunned Client）]：「回避クライアントの検索」を参照してください。
- [スイッチ（Switches）]：「スイッチの検索」を参照してください。
- [タグ（Tags）]：「タグの検索」を参照してください。
- [Wi-Fi TDOA レシーバ（Wi-Fi TDOA Receivers）]：Wi-Fi TDOA レシーバの検索」を参照してください。

アラームの検索

アラームの高度な検索を実行する際に、次のパラメータを設定できます。

表 *91* : アラーム検索フィールド

フィールド	Options
重大度（Severity）	[すべての重大度（All Severities）]、[CriticalMajor]、[メジャー（Major）]、[マイナー（Minor）]、[警告（Warning）]、または [クリア（Clear）] を選択します。

フィールド	Options
[アラームカテゴリ（Alarm Category）]	[すべてのタイプ（All Types）]、[システム（System）]、[アクセスポイント（Access Points）]、[コントローラ（Controllers）]、[カバレッジホール（Coverage Hole）]、[設定監査（Config Audit）]、[モビリティサービス（Mobility Service）]、[コンテキスト認識型通知（Context Aware Notifications）]、[SEにより検出された干渉（SE Detected Interferers）]、[メッシュリンク（Mesh Links）]、[不正AP（Rogue AP）]、[アドホック不正（Adhoc Rogue）]、[セキュリティ（Security）]、[パフォーマンス（Performance）]、[アプリケーションパフォーマンス（Application Performance）]、[ルータ（Routers）]、[スイッチとハブ（Switches and Hubs）] または [Ciscoインターフェイスおよびモジュール（Cisco Interfaces and Modules）] を選択します。
Condition	ドロップダウンリストを使用し、条件を選択します。また、このドロップダウンリストに入力して、条件を入力することもできます。 （注） アラーム カテゴリを選択した場合は、このドロップダウン リストには、そのカテゴリで使用可能な条件が含まれています。
Time Period	[Any Time] から [Last 7 days] までの時間増分を選択します。デフォルトは [Any Time] です。
Acknowledged State	承認済みステートまたは未承認ステートのアラームを検索するには、このチェックボックスを選択します。このチェックボックスを選択しない場合、承認済みステートは検索基準の考慮に入れられません。
Assigned State	割り当て済みステートまたは未割り当てステートのアラームを検索するか、所有者名によってアラームを検索するには、このチェックボックスを選択します。このチェックボックスを選択しない場合は、割り当て済みステートは検索基準に含まれません。 （注） [Assigned State] > [Owner Name] を選択する場合は、使用可能なテキスト ボックスに所有者名を入力します。

ジョブの検索

ジョブの高度な検索を実行する際に、次のパラメータを設定できます（表 58-5 を参照）。

表 *92 :* ジョブの検索フィールド

フィールド	オプション
Job Name	検索するジョブの名前を入力します。
Job Type	検索するジョブのタイプを入力します。
ジョブのステータス（Job Status）	[すべてのステータス（All Status）]、[電源（Power）]、または [スケジュール済み（Scheduled）] を選択します。

（注） [ジョブ名（Job Name）] と [ジョブタイプ（Job Type）] テキスト ボックスでは、ワイルドカード（*、? など）を使用して検索を絞り込んだり、検索範囲を広げたりすることができます。

アクセス ポイントの検索

アクセス ポイントの高度な検索を実行する際に、次のパラメータを設定できます（次の表を参照）。

表 *93* : アクセス ポイントの検索フィールド

フィールド	オプション
検索方法（Search By）	[すべてのAP（All APs）]、[基礎無線MAC（Base Radio MAC）]、[イーサネットMAC（Ethernet MAC）]、[AP名（AP Name）]、[APモデル（AP Model）]、[APロケーション（AP Location）]、[IPアドレス（IP Address）]、[デバイス名（Device Name）]、[コントローラIP（Controller IP）]、[すべての関連付けられていないAP（All Unassociated APs）]、[床面積（Floor Area）]、[屋外区域（Outdoor Area）]、[未割り当てAP（Unassigned APs）]、または [アラーム（Alarms）] を選択します。 （注） 検索パラメータは、選択したカテゴリによって変わることがあります。適用可能な場合は、[Search By] カテゴリの特定に役立つよう、追加のパラメータまたはフィルタ情報を入力します。たとえば、[Floor Area] を選択した場合は、キャンパスとビルディングも特定する必要があります。または、[Alarms] を選択した場合は、アラームのシビリティに基づいてアクセス ポイントを検索できます。
AP Type	[All Types]、[LWAPP]、または [Autonomous] を選択します。
AP Mode	[すべてのモード（All Modes）]、[ローカル（Local）]、[モニタ（Monitor）]、[FlexConnect]、[不正検出（Rogue Detector）]、[スニファ（Sniffer）]、[ブリッジ（Bridge）]、または [SE接続（SE-Connect）] を選択します。
Radio Type	[All Radios]、[802.11a]、または [802.11b/g] を選択します。
802.11n Support	802.11n がサポートされるアクセス ポイントを検索するには、このチェックボックスを選択します。
OfficeExtend AP Enabled	Office Extend アクセス ポイントを検索するには、このチェックボックスをオンにします。
CleanAir Support	CleanAir をサポートするアクセス ポイントを検索するには、このチェックボックスを選択します。
CleanAir Enabled	CleanAir がサポートされ、有効になっているアクセス ポイントを検索するには、このチェックボックスを選択します。
Items per page	検索結果ページに表示するレコードの数を設定します。

コントローラ ライセンスの検索

コントローラ ライセンスの高度な検索を実行する際に、次のパラメータを設定できます。

表 *94 :* コントローラ ライセンスの検索フィールド

フィールド	オプション
Controller Name	ライセンス検索に関連付けられたコントローラ名を入力します。
機能名（Feature Name）	ライセンス階層に応じて、[すべて（All）]、[プラス（Plus）]、[基本（Base）] から選択します。
タイプ（Type）	[すべて（All）]、[評価（Evaluation）]、[拡張（Extension）]、[猶予期間（Grace Period）]、または [無期限（Permanent）] を選択します。
% Used or Greater	このドロップダウン リストからライセンスの使用パーセンテージを選択します。0 ～ 100 の範囲のパーセント値を使用します。
Items per page	検索結果ページに表示するレコードの数を設定します。

コントローラの検索

コントローラの高度な検索を実行する際に、次のパラメータを設定できます。

表 *95 :* コントローラの検索フィールド

フィールド	オプション
Search for controller by	[すべてのコントローラ（All Controllers）]、[IPアドレス（IP Address）]、および [コントローラ名（Controller Name）] を選択します。 （注） 検索パラメータは、選択したカテゴリによって変わることがあります。適用可能な場合は、[Search By] カテゴリの特定に役立つよう、追加のパラメータまたはフィルタ情報を入力します。
Enter Controller IP Address	このテキスト ボックスは、[Search for controller by] ドロップダウン リストから [IP Address] を選択した場合のみ表示されます。
Enter Controller Name	このテキスト ボックスは、[Search for controller by] ドロップダウン リストから [Controller Name] を選択した場合のみ表示されます。
Audit Status	ドロップダウン リストから、次のいずれかのオプションを選択します。 • **All Status** • [不一致（Mismatch）]：最新の監査で、Cisco Prime Infrastructure とコントローラ間の設定の相違が検出された。 • [Identical]：最新の監査で、設定の相違は検出されなかった。 • [Not Available]：監査ステータスは使用できない。

フィールド	オプション
Items per page	検索結果ページに表示するレコードの数を設定します。

スイッチの検索

スイッチの高度な検索を実行する際に、次のパラメータを設定できます。

表 *96* : スイッチの検索フィールド

フィールド	オプション
Search for Switches by	[All Switches]、[IP Address]、または [Switch Name] を選択します。ワイルドカード（*）を使用できます。たとえば、[IPアドレス（IP Address）] を選択して **172*** と入力すると、Cisco Prime Infrastructure は IP アドレスが 172 で始まるすべてのスイッチを返します。
Items per page	検索結果ページに表示するレコードの数を設定します。

クライアントの検索

クライアントの高度な検索を実行する際に、次のパラメータを設定できます（表 58-10 を参照）。

表 *97* : クライアントの検索フィールド

フィールド	オプション
[メディア タイプ（Media Type）]	[すべて（All）]、[ワイヤレスクライアント（Wireless Clients）]、または [有線クライアント（Wired Clients）] を選択します。
[ワイヤレスタイプ（Wireless Type）]	[メディアタイプ（Media Type）] リストから [ワイヤレスクライアント（Wireless Clients）] を選択した場合は、[すべて（All）]、[Lightweight]、または [自律型クライアント（Autonomous Clients）] を選択します。

Cisco Prime Infrastructure ユーザ インターフェイスの参照

フィールド	オプション
検索方法（Search By）	[すべてのクライアント（All Clients）]、[除外されたすべてのクライアント（All Excluded Clients）]、[すべての有線クライアント（All Wired Clients）]、[すべてのログインゲスト（All Logged in Guests）]、[IPアドレス（IP Address）]、[ユーザ名（User Name）]、[MACアドレス（MAC Address）]、[アセット名（Asset Name）]、[アセットカテゴリ（Asset Category）]、[アセットグループ（Asset Group）]、[AP名（AP Name）]、[コントローラ名（Controller Name）]、[コントローラIP（Controller IP）]、[MSE IP]、[床面積（Floor Area）]、[屋外区域（Outdoor Area）]、[スイッチ名（Switch Name）]、または [スイッチタイプ（Switch Type）] を選択します。 （注） 検索パラメータは、選択したカテゴリによって変わることがあります。適用可能な場合は、[Search By] カテゴリの特定に役立つよう、追加のパラメータまたはフィルタ情報を入力します。たとえば、[IP address] を選択した場合は、この検索の特定のIPアドレスを入力する必要があります。
Clients Detected By	[Prime Infrastructure] または [MSEs] を選択します。 [Cisco Prime Infrastructureにより検出されたクライアント（Clients detected by Cisco Prime Infrastructure）]：Cisco Prime Infrastructure データベースに保存されたクライアント。 [Clients detected by MSE]：コントローラと直接通信する MSE で Context Aware Service によって検索されるクライアント。
[クライアント状態（Client States）]	[すべての状態（All States）]、[アイドル（Idle）]、[認証（Authenticated）]、[関連付けられました（Associated）]、[プローブ中（Probing）]、または [除外（Excluded）] を選択します。
[ポスチャ ステータス（Posture Status）]	デバイスがクリーンであるかどうかを確認するには、[すべて（All）]、[不明（Unknown）]、[合格（Passed）]、[失敗（Failed）] を選択します。
[無線帯域による制限（Restrict By Radio Band）]	特定の無線帯域を示すには、このチェックボックスを選択します。ドロップダウンリストから [5 GHz] または [2.4 GHz] を選択します。

Cisco Prime Infrastructure ユーザ インターフェイスの参照

フィールド	オプション
Restrict By Protocol	特定のプロトコルを示すには、このチェックボックスを選択します。ドロップダウンリストから [802.11a]、[802.11b]、[802.11g]、[802.11n]、または [モバイル（Mobile）] を選択します。
SSID	このチェックボックスを選択して、ドロップダウン リストから適切な SSID を選択します。
Profile	選択したプロファイルに関連するすべてのクライアントを一覧表示するには、このチェックボックスを選択します。 （注） チェックボックスの選択後に、ドロップダウンリストから適切なプロファイルを選択します。
CCX Compatible	Cisco Client Extensions との互換性があるクライアントを検索するには、このチェックボックスを選択します。 （注） チェックボックスの選択後に、ドロップダウンリストから、適切なバージョンとして [All Versions] または [Not Supported] を選択します。
E2E Compatible	エンドツーエンドの互換性のあるクライアントを検索するには、このチェックボックスを選択します。 （注） チェックボックスの選択後に、ドロップダウンリストから、適切なバージョンとして [すべてのバージョン（All Versions）] または [サポート対象外（Not Supported）] を選択します。
[NAC 状態（NAC State）]	特定のネットワーク アドミッション コントロール（NAC）ステートによって識別されたクライアントを検索するには、このチェックボックスを選択します。 （注） チェックボックスの選択後に、ドロップダウンリストから [隔離（Quarantine）]、[アクセス（Access）]、[無効（Invalid）]、および [該当なし（Not Applicable）] のうち適切なステートを選択します。
[関連付けなしを含む（Include Disassociated）]	ネットワークに存在しないが、Cisco Prime Infrastructure に履歴レコードが保持されているクライアントを含めるには、このチェックボックスを選択します。
[ページあたりの項目数（Items per page）]	検索結果ページに表示するレコードの数を設定します。

チョークポイントの検索

チョークポイントの高度な検索を実行する際に、次のパラメータを設定できます。

表 *98* : チョークポイントの検索フィールド

フィールド	オプション
Search By	[MAC Address] または [Chokepoint Name] を選択します。 （注） 検索パラメータは、選択したカテゴリによって変わることがあります。適用可能な場合は、[Search By] カテゴリの特定に役立つよう、追加のパラメータまたはフィルタ情報を入力します。たとえば、[MAC address] を選択した場合は、この検索の特定の MAC アドレスを入力する必要があります。

監査変更の詳細検索

監査変更の詳細な検索を実行する際に、次のパラメータを設定できます。

表 *99* : 監査変更のフィールド検索

フィールド	オプション
[監査コンポーネント（Audit Component）]	検索する監査コンポーネントの名前を入力します。
[監査の説明（Audit Description）]	検索する監査説明の名前を入力します。
[IPアドレス（IP Address）]	検索する IP アドレスの名前を入力します。
[ユーザ名（User Name）]	検索するユーザ名を入力します。

イベントの検索

イベントの高度な検索を実行する際に、次のパラメータを設定できます。

表 *100* : イベントの検索フィールド

フィールド	**Options**
Severity	**[すべての重大度（All Severities）]**、**[クリティカル（Critical）]**、**[メジャー（Major）]**、**[マイナー（Minor）]**、**[警告（Warning）]**、**[クリア（Clear）]**、または **色分け**
[イベントカテゴリ（Event Category）]	[すべてのタイプ（All Types）]、[アクセスポイント（Access Points）]、[コントローラ（Controller）]、[セキュリティ（Security）]、[カバレッジホール（Coverage Hole）]、[不正 AP（Rogue AP）]、[アドホック不正（Adhoc Rogue）]、[干渉（Interference）]、[メッシュリンク（Mesh Links）]、[クライアント（Client）]、[モビリティサービス（Mobility Service）]、[モビリティサービス（Mobility Service）]、[ロケーション通知（Location Notifications）]、[再カバレッジホール（re Coverage Hole）]、または [Prime Infrastructure] を選択します。

フィールド	Options
条件	ドロップダウン リストを使用し、条件を選択します。また、このドロップダウン リストに入力して、条件を入力することもできます。 （注） イベント カテゴリを選択した場合は、このドロップダウン リストには、そのカテゴリで使用可能な条件が含まれています。
Search All Events	検索結果ページに表示するレコードの数を設定します。

干渉源の検索

アクセス ポイントで検出された干渉源の高度な検索を実行する際に、次のパラメータを設定できます。

表 *101 : SE* によって検出された干渉源の検索フィールド

フィールド	オプション
検索方法（Search By）	[すべての干渉源（All Interferers）]、[干渉源ID（Interferer ID）]、[干渉源カテゴリ（Interferer Category）]、[干渉源タイプ（Interferer Type）]、[影響を受けるチャネル（Affected Channel）]、[影響を受けるAP（Affected AP）]、[重要度（Severity）]、[電源（Power）]、または [デューティサイクル（Duty Cycle）] を選択します。 （注） 検索パラメータは、選択したカテゴリによって変わることがあります。適用可能な場合は、[Search By] カテゴリの特定に役立つよう、追加のパラメータまたはフィルタ情報を入力します。
Detected By	[All Spectrum Experts] を選択するか、ドロップダウン リストから特定の Spectrum Expert を選択します。
Detected within the last	干渉検出の時間範囲を選択します。時間範囲は、5 分～ 24 時間または [All History] です。
Interferer Status	ドロップダウンリストから、[すべて（All）]、[アクティブ（Active）]、または [非アクティブ（Inactive）] を選択します。
Restrict by Radio Bands/Channels	無線帯域またはチャネルによる検索を設定します。
Items per page	検索結果ページに表示するレコードの数を設定します。

Wi-Fi TDOA レシーバの検索

Wi-Fi TDOA 受信機の高度な検索を実行する際に、次のパラメータを設定できます。

表 *102 : Wi-Fi TDOA* 受信機検索フィールド

フィールド	オプション
Search By	[MAC Address] または [Wi-Fi TDOA Receivers Name] を選択します。 （注） 検索パラメータは、選択したカテゴリによって変わることがあります。適用可能な場合は、[Search By] カテゴリの特定に役立つよう、追加のパラメータまたはフィルタ情報を入力します。

マップの検索

マップの高度な検索を実行する際に、次のパラメータを設定できます。

表 *103 :* マップの検索フィールド

フィールド	オプション
Search for	[All Maps]、[Campuses]、[Buildings]、[Floor Areas]、または [Outdoor Areas] を選択します。
Map Name	マップ名で検索します。テキスト ボックスにマップ名を入力します。
Items per page	検索結果ページに表示するレコードの数を設定します。

不正クライアントの検索

不正クライアントの高度な検索を実行する際に、次のパラメータを設定できます。

表 *104 :* 不正クライアントの検索フィールド

フィールド	オプション
Search for clients by	[すべての不正クライアント（All Rogue Clients）]、[MACアドレス（MAC Address）]、[コントローラ（Controller）]、[MSE]、[床面積（Floor Area）]、または [屋外区域（Outdoor Area）] を選択します。
検索場所（Search In）	[MSEs] または [Prime Infrastructure Controllers] を選択します。
Status	チェックボックスをオンにし、ドロップダウンリストから [アラート（Alert）]、[包含（Contained）]、または [脅威（Threat）] を選択して、検索条件にステータスを含めます。

回避クライアントの検索

（注） 有線ネットワーク上の Cisco IPS センサーが不審なクライアントまたは脅威的なクライアントを検出した場合は、そのクライアントを回避するようにコントローラに警告します。

回避クライアントの高度な検索を実行する際に、次のパラメータを設定できます。

表 *105 :* 回避クライアントの検索フィールド

フィールド	オプション
Search By	[All Shunned Clients]、[Controller]、または [IP Address] を選択します。 （注） 検索パラメータは、選択したカテゴリによって変わることがあります。適用可能な場合は、[Search By] カテゴリの特定に役立つよう、追加のパラメータまたはフィルタ情報を入力します。

タグの検索

タグの高度な検索を実行する際に、次のパラメータを設定できます。

表 *106 :* タグの検索フィールド

フィールド	オプション
Search for tags by	[すべてのタグ（All Tags）]、[アセット名（Asset Name）]、[アセットカテゴリ（Asset Category）]、[アセットグループ（Asset Group）]、[MACアドレス（MAC Address）]、[コントローラ（Controller）]、 [MSE]、[床面積（Floor Area）]、または [屋外区域（Outdoor Area）] を選択します。 （注） 検索パラメータは、選択したカテゴリによって変わることがあります。適用可能な場合は、[Search By] カテゴリの特定に役立つよう、追加のパラメータまたはフィルタ情報を入力します。
検索場所（Search In）	[MSE（MSEs）] または [Prime Infrastructureコントローラ（Prime Infrastructure Controllers）] を選択します。
Last detected within	時間増分を 5 分～ 24 時間の間で選択します。デフォルト値は、15 分です。
Tag Vendor	このチェックボックスを選択して、[Aeroscout]、[G2]、[PanGo]、または [WhereNet] を選択します。
Telemetry Tags only	適宜にタグを検索するには、[テレメトリタグのみ（Telemetry Tags only）] チェックボックスを選択します。
Items per page	検索結果ページに表示するレコードの数を設定します。

デバイス タイプの検索

デバイス タイプの高度な検索を実行する際に、次のパラメータを設定できます。

表 *107* : デバイス タイプの検索フィールド

フィールド	オプション
Select Device Type	[すべてのスイッチとハブ（All Switches and Hubs）]、[ワイヤレスコントローラ（Wireless Controller）]、[ユニファイドAP（Unified AP）]、[自律AP（Autonomous AP）]、[管理対象外AP（Unmanaged AP）]、または [ルータ（Routers）] を選択します。
Enter Device IP	[Select Device Type] フィールドで選択したデバイスの IP アドレスを入力します。

設定バージョンの検索

設定バージョンの高度な検索を実行する際に、次のパラメータを設定できます。

表 *108* : 設定バージョン検索フィールド

フィールド	オプション
Enter Tag	タグ名を入力します。

保存した検索の使用

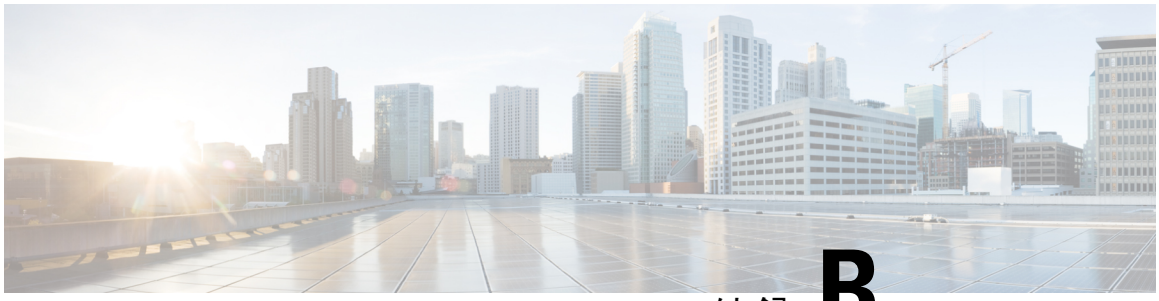
（注） Saved Search は、現在のパーティションのみに適用されます。

以前に保存した検索にアクセスして実行するには、次の手順に従います。

ステップ 1 [Application Search] ボックスのアイコンをクリックし、[Saved Search] をクリックします。

ステップ 2 [Search Category] ドロップダウン リストからカテゴリを選択し、[Saved Search List] ドロップダウン リストから保存されている検索を選択します。

ステップ 3 必要に応じて、保存されている検索の現在のパラメータを変更し、[Go] をクリックします。



付録 B

アイコンと状態の参照

ここでは、次の内容について説明します。

- デバイスの到達可能性状態と管理状態 （1143 ページ）
- ポートまたはインターフェイスの状態 （1145 ページ）
- リンクの有用性状態 （1147 ページ）
- リンクの特徴 （1147 ページ）
- 機器の動作状態（シャーシ ビュー） （1148 ページ）
- アラーム重大度アイコン （1149 ページ）
- デバイス タイプのアイコン （1149 ページ）

デバイスの到達可能性状態と管理状態

デバイスの到達可能性状態：Prime Infrastructure が設定されたすべてのプロトコルを使用してデバイスと通信できるかどうかを表します。

表 *109* : デバイスの到達可能性状態

アイコン	デバイスの到達可能性状態	説明	トラブルシューティング
✅	到達可能	Prime Infrastructure は、SNMP を使用してデバイスに、または ICMP を使用して NCS 2K デバイスにアクセスすることができます。	—

アイコンと状態の参照

	ping 到達可能	Prime Infrastructure は、ping を使用してデバイスに到達できますが、SNMP 経由では到達できません。	ICMP ping は成功しますが、SNMP 通信が失敗する原因すべてをチェックします。デバイス SNMP クレデンシャルがデバイスと Prime Infrastructure の両方で同じであること、SNMP がデバイス上で有効になっているかどうか、またはトランスポートネットワークが設定ミスなどの理由で SNMP パケットをドロップしていないかどうかをチェックします。
	到達不能	Prime Infrastructure は、ping を使用してデバイスに到達できません。	物理デバイスが動作中でネットワークに接続されていることを確認します。
	不明	Prime Infrastructure は、デバイスに接続できません。	デバイスをチェックします。

デバイスの管理状態：デバイスの設定状態を表します（たとえば、デバイスが ping によって到達できないためにダウンしている場合や、管理者が手動でデバイスをシャットダウンした場合などです）。

表 *110* : デバイスの管理状態

デバイスの管理状態	説明	トラブルシューティング
管理対象	Prime Infrastructure は、デバイスを積極的にモニタしています。	該当なし。
メンテナンス	Prime Infrastructure は、デバイスの到達可能性をチェックしていますが、トラップ、syslog、または TL1 メッセージを処理していません。	デバイスを管理対象状態に移行するには、デバイスのメンテナンス状態の切り替え （54 ページ）を参照してください。

管理対象外	Prime Infrastructure は、デバイスをモニタしていません。	[ネットワーク デバイス（Network Devices）] テーブルで、デバイスを特定し、[最新のインベントリ収集ステータス（Last Inventory Collection Status）] 列でデータの横にある [i] アイコンをクリックします。ポップアップ ウィンドウに、詳細とトラブルシューティングのヒントが表示されます。収集問題の一般的な原因は次のとおりです。 • デバイス SNMP クレデンシャルが間違っている。 • Prime Infrastructure 展開がライセンスで許可されているデバイスの数を上回っている。 • デバイスがスイッチ パス トレース専用になっている。 デバイス タイプがサポートされていない場合は、その [デバイス タイプ（Device Type）] が [不明（Unknown）] になります。そのデバイス タイプのサポートが Cisco.com で提供されているかをチェックするには、**[管理（Administration）] > [ライセンスおよびソフトウェアアップデート（Licenses and Software Updates）] > [ソフトウェアアップデート（Software Update）]** を選択してから、[更新の確認（Check for Updates）] をクリックします。
不明	Prime Infrastructure は、デバイスに接続できません。	デバイスをチェックします。

ポートまたはインターフェイスの状態

ポートまたはインターフェイスのプライマリ状態：管理者と運用状態を組み合わせることでポートまたはインターフェイスの最も重要な状態情報を伝えます。[多層トレース（Multilayer Trace）] には、ポートのプライマリ状態またはアラーム状態が表示されます。[シャーシビュー（Chassis View）] の場合は、要素が状態変化を示す色の変化をサポートしていない場合でも、生成されたアラームから状態変更情報を取得できます。

（注） ポート/インターフェイスにアラームが関連付けられている場合、アラーム アイコンが表示され、ポート アイコンは表示されません。

ポートまたはインターフェイスのプライマリ状態	アイコン	管理ステータス	動作状態

アイコンと状態の参照

不明		不明	不明
ダウン		アップ	Down
テスト		テスト	—
管理上ダウン		管理上ダウン	—
Up		Up	Up
自動アップ		アップ	自動アップ

ポートまたはインターフェイスの管理状態：ポートまたはインターフェイスの設定状態を表します（たとえば、管理者が手動でポートをシャットダウンした場合など）。

ポートまたはインターフェイスの管理状態	アイコン	説明
不明		ポートまたはインターフェイスの管理状態は不明です。デバイスからの応答（または不十分な応答）はありません。
管理上ダウン		ポートまたはインターフェイスは管理者によって手動でシャットダウンされました。
アップ		ポートまたはインターフェイスは管理者によって有効にされています。
テスト		ポートまたはインターフェイスは管理者によってテストされています。

ポートまたはインターフェイスの動作状態：ポートまたはインターフェイスの実行状態と、それが適切に動作しているかどうかを伝えます。

ポートまたはインターフェイスの動作状態	アイコン	説明
不明		ポートまたはインターフェイスの動作状態は不明です。デバイスからの応答（または不十分な応答）はありません。
ダウン		ポートまたはインターフェイスは正しく動作していません。
アップ		ポートまたはインターフェイスがデータを送受信しています。

自動アップ		ポートまたはインターフェイスがデータを送受信しています（特定のデバイスのみがこの状態をサポートしています。他のデバイスは [アップ（Up）] を使用します）。

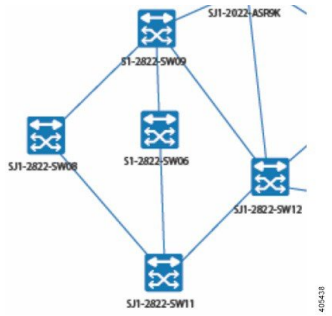
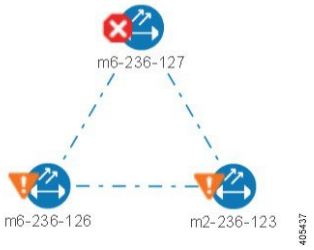
リンクの有用性状態

サービスアビリティ状態	アイコン	
管理上ダウン		リンクは意図的に管理者によってシャットダウンされました。
ダウン		リンクがダウンしています（ただしダウンは不適切な状態）。 **説明**
アップ		リンクはアップの状態で、トラフィックがリンクを通過しています。
[取得不可（Unavailable）]		リンクがまだ検出されていないか、またはステータスが取得できません。
Partial		リンクの要求、リソース、またはリソース状態に不一致があります。例： • リンクが、一部のサービス リソースをアクティブ化し、他のサービス リソースを非アクティブにする要求を処理している。 • リンクにいくつかのアクティブ リソースといくつかの非アクティブ リソースがある。 • アップしているリンク リソースとダウンしているリンク リソースがある。 • リンクのリソースのいずれかの状態が不明である。

リンクの特徴

以下の表では、Prime Infrastructure の [トポロジマップ（Topology Map）] ビューでデバイス間の接続を表すために使用されるさまざまなタイプのリンクについて説明します。

リンク タイプ	説明

	[実線（Solid Line）]：2つのデバイス間のリンクなど、物理リンク、トポロジ リンク、またはサービス リンクを示します。
	[破線（Dashed Line）]：EVC、VPLS サービス インスタンス、またはVPN コンポーネントなど、要素間の関連性またはビジネス リンクを示します。

機器の動作状態（シャーシ ビュー）

機器の動作状態はネットワーク要素の実行状態を表しています。

機器の動作状態	アイコン	説明
サービス中（In Service）	（なし）	機器が正常に動作しています。
事前プロビジョニング済み		（Cisco NCS 2000 および Cisco ONS デバイスのみ）機器は設定されていますが、シャーシには物理的に存在していません。
失敗/無効/ダウン/休止中/メンテナンス中のため休止中		機器は正常に動作していません。
不明		機器の動作状態は不明です。デバイスからの応答はありません（または不十分な応答）。

アラーム重大度アイコン

次の表に、Web GUI のさまざまな部分に表示されるアイコンのアラームの色とその重大度を示します。

重大度アイコン	説明	色
	クリティカル アラーム	赤
	メジャーアラーム	オレンジ
	マイナーアラーム	黄
	警告アラーム	ライト ブルー
	アラームはクリア済み。正常、OK	緑
	情報アラーム	青
	不確定アラーム	暗い青色

デバイス タイプのアイコン

次の表では、Prime Infrastructure の [トポロジ（Topology）] ビューと [マルチレイヤトレース（Multi-layer Trace）] ビューでさまざまなデバイス タイプを表すために使用されるアイコンを定義します。

アイコン	定義
	スイッチ（Switch）
	ルータ（Router）

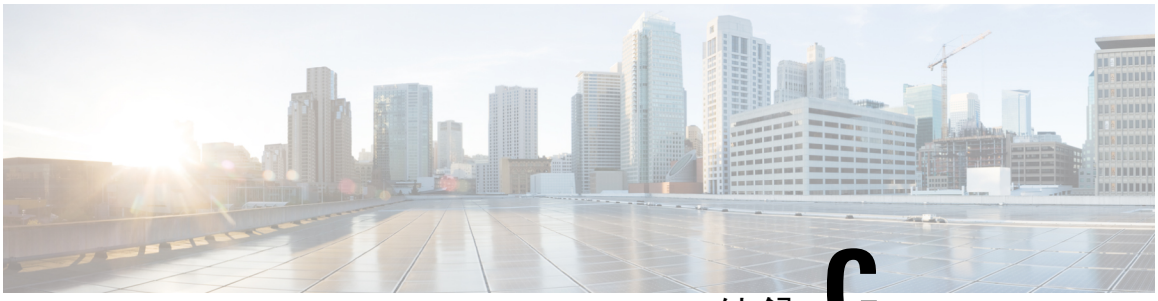
アイコンと状態の参照

アイコン	定義
	ルータ集約
	セキュア ドメイン ルータ（SDR）が搭載された Cisco NCS 6000 デバイス。SDR の名前はデバイスのアイコン上に直接表示されます。 （注） クラスタまたはユーザ定義グループに属するデバイスの SDR ラベルが表示されない場合（自動クラスタリングがデバイスのプロキシミティに基づいてデバイスに適用されるため）などがあります。
	L3VPN サービスで構成されたルータ。
	スイッチ集約
	アクセス ポイント（Access Point）
	サービス モジュール
	UCS C シリーズ
	NAM ブレード
	グループ

アイコンと状態の参照

アイコン	定義
	汎用デバイス
	仮想サーバ
	ワイヤレス LAN コントローラ
	[不明（Unknown）]
	DWDM ROADM 再生/NCS 2000

アイコンと状態の参照



付録 C

Cisco Prime Infrastructure でサポートされるタイム ゾーン

• Cisco Prime Infrastructure でサポートされるタイム ゾーン （1153 ページ）

Cisco Prime Infrastructure でサポートされるタイム ゾーン

この表に、システムのタイム ゾーンで利用可能な値を示します。

Africa/Abidjan	America/St_Johns	Etc/GMT+6
Africa/Accra	America/St_Kitts	Etc/GMT+7
Africa/Addis_Ababa	America/St_Lucia	Etc/GMT+8
Africa/Algiers	America/St_Thomas	Etc/GMT+9
Africa/Asmara	America/St_Vincent	Etc/GMT0
Africa/Asmera	America/Swift_Current	Etc/GMT-0
Africa/Bamako	America/Tegucigalpa	Etc/GMT-1
Africa/Bangui	America/Thule	Etc/GMT-10
Africa/Banjul	America/Thunder_Bay	Etc/GMT-11
Africa/Bissau	America/Tijuana	Etc/GMT-12
Africa/Blantyre	America/Toronto	Etc/GMT-13
Africa/Brazzaville	America/Tortola	Etc/GMT-14
Africa/Bujumbura	America/Vancouver	Etc/GMT-2
Africa/Cairo	America/Virgin	Etc/GMT-3
Africa/Casablanca	America/Whitehorse	Etc/GMT-4

Cisco Prime Infrastructure でサポートされるタイム ゾーン

Africa/Ceuta	America/Winnipeg	Etc/GMT-5
Africa/Conakry	America/Yakutat	Etc/GMT-6
Africa/Dakar	America/Yellowknife	Etc/GMT-7
Africa/Dar_es_Salaam	Antarctica/Casey	Etc/GMT-8
Africa/Djibouti	Antarctica/Davis	Etc/GMT-9
Africa/Douala	Antarctica/DumontDUrville	Etc/Greenwich
Africa/El_Aaiun	Antarctica/Mawson	Etc/UCT
Africa/Freetown	Antarctica/McMurdo	Etc/Universal
Africa/Gaborone	Antarctica/Palmer	Etc/UTC
Africa/Harare	Antarctica/Rothera	Etc/Zulu
Africa/Johannesburg	Antarctica/South_Pole	Europe/Amsterdam
Africa/Kampala	Antarctica/Syowa	Europe/Andorra
Africa/Khartoum	Antarctica/Vostok	Europe/Athens
Africa/Kigali	rctic/Longyearbyen	Europe/Belfast
Africa/Kinshasa	Asia/Aden	Europe/Belgrade
Africa/Lagos	Asia/Almaty	Europe/Berlin
Africa/Libreville	Asia/Amman	Europe/Bratislava
Africa/Lome	Asia/Anadyr	Europe/Brussels
Africa/Luanda	Asia/Aqtau	Europe/Bucharest
Africa/Lubumbashi	Asia/Aqtobe	Europe/Budapest
Africa/Lusaka	Asia/Ashgabat	Europe/Chisinau
Africa/Malabo	Asia/Ashkhabad	Europe/Copenhagen
Africa/Maputo	Asia/Baghdad	Europe/Dublin
Africa/Maseru	Asia/Bahrain	Europe/Gibraltar
Africa/Mbabane	Asia/Baku	Europe/Guernsey
Africa/Mogadishu	Asia/Bangkok	Europe/Helsinki
Africa/Monrovia	Asia/Beirut	Europe/Isle_of_Man
Africa/Nairobi	Asia/Bishkek	Europe/Istanbul
Africa/Ndjamena	Asia/Brunei	Europe/Jersey

Africa/Niamey	Asia/Calcutta	Europe/Kaliningrad
Africa/Nouakchott	Asia/Choibalsan	Europe/Kiev
Africa/Ouagadougou	Asia/Chongqing	Europe/Lisbon
Africa/Porto-Novo	Asia/Chungking	Europe/Ljubljana
Africa/Sao_Tome	Asia/Colombo	Europe/London
Africa/Timbuktu	Asia/Dacca	Europe/Luxembourg
Africa/Tripoli	Asia/Damascus	Europe/Madrid
Africa/Tunis	Asia/Dhaka	Europe/Malta
Africa/Windhoek	Asia/Dili	Europe/Mariehamn
America/Adak	Asia/Dubai	Europe/Minsk
America/Anchorage	Asia/Dushanbe	Europe/Monaco
America/Anguilla	Asia/Gaza	Europe/Moscow
America/Antigua	Asia/Harbin	Europe/Nicosia
America/Araguaina	Asia/Ho_Chi_Minh	Europe/Oslo
America/Argentina/	Asia/Hong_Kong	Europe/Paris
America/Argentina/	Asia/Hovd	Europe/Podgorica
America/Argentina/Catamarca	Asia/Irkutsk	Europe/Prague
America/Argentina/Cordoba	Asia/Istanbul	Europe/Riga
America/Argentina/Jujuy	Asia/Jakarta	Europe/Rome
America/Argentina/La_Rioja	Asia/Jayapura	Europe/Samara
America/Argentina/Mendoza	Asia/Jerusalem	Europe/Samara
America/Argentina/Rio_Gallegos	Asia/Kabul	Europe/Sarajevo
America/Argentina/Salta	Asia/Kamchatka	Europe/Simferopol
America/Argentina/San_Juan	Asia/Karachi	Europe/Skopje
America/Argentina/San_Luis	Asia/Kashgar	Europe/Sofia
America/Argentina/Tucuman	Asia/Kathmandu	Europe/Stockholm
America/Argentina/Ushuaia	Asia/Katmandu	Europe/Tallinn
America/Aruba	Asia/Kolkata	Europe/Tirane
America/Asuncion	Asia/Krasnoyarsk	Europe/Tiraspol

Cisco Prime Infrastructure でサポートされるタイム ゾーン

America/Atikokan	Asia/Kuala_Lumpur	Europe/Uzhgorod
America/Atka	Asia/Kuching	Europe/Vaduz
America/Bahia	Asia/Kuwait	Europe/Vatican
America/Barbados	Asia/Macao	Europe/Vienna
America/Belem	Asia/Macau	Europe/Vilnius
America/Belize	Asia/Magadan	Europe/Volgograd
America/Blanc-Sablon	Asia/Makassar	Europe/Warsaw
America/Boa_Vista	Asia/Manila	Europe/Zagreb
America/Bogota	Asia/Muscat	Europe/Zaporozhye
America/Boise	Asia/Nicosia	Europe/Zurich
America/Buenos_Aires	Asia/Novosibirsk	Factory
America/Cambridge_Bay	Asia/Omsk	GB
America/Campo_Grande	Asia/Oral	GB-Eire
America/Cancun	Asia/Phnom_Penh	GMT
America/Caracas	Asia/Pontianak	GMT+0
America/Catamarca	Asia/Pyongyang	GMT0
America/Cayenne	Asia/Qatar	GMT-0
America/Cayman	Asia/Qyzylorda	Greenwich
America/Chicago	Asia/Rangoon	Hongkong
America/Chihuahua	Asia/Riyadh	HST
America/Coral_Harbour	Asia/Riyadh87	Iceland
America/Cordoba	Asia/Riyadh88	Indian/Antananarivo
America/Costa_Rica	Asia/Riyadh89	Indian/Chagos
America/Cuiaba	Asia/Saigon	Indian/Christmas
America/Curacao	Asia/Sakhalin	Indian/Cocos
America/Danmarkshavn	Asia/Samarkand	Indian/Comoro
America/Dawson	Asia/Seoul	Indian/Kerguelen
America/Dawson_Creek	Asia/Shanghai	Indian/Mahe
America/Denver	Asia/Singapore	Indian/Maldives

America/Detroit	Asia/Taipei	Indian/Mauritius
America/Dominica	Asia/Tashkent	Indian/Mayotte
America/Edmonton	Asia/Tbilisi	Indian/Reunion
America/Eirunepe	Asia/Tehran	Iran
America/El_Salvador	Asia/Tel_Aviv	Israel
America/Ensenada	Asia/Thimbu	Jamaica
America/Fort_Wayne	Asia/Thimphu	Japan
America/Fortaleza	Asia/Tokyo	Kwajalein
America/Glace_Bay	Asia/Ujung_Pandang	Libya
America/Godthab	Asia/Ulaanbaatar	MET
America/Goose_Bay	Asia/Ulan_Bator	Mexico/BajaNorte
America/Grand_Turk	Asia/Urumqi	Mexico/BajaSur
America/Grenada	Asia/Vientiane	Mexico/General
America/Guadeloupe	Asia/Vladivostok	Mideast/Riyadh87
America/Guatemala	Asia/Yakutsk	Mideast/Riyadh88
America/Guayaquil	Asia/Yekaterinburg	Mideast/Riyadh89
America/Guyana	Asia/Yerevan	MST
America/Halifax	Atlantic/Azores	MST7MDT
America/Havana	Atlantic/Bermuda	Navajo
America/Hermosillo	Atlantic/Canary	New_Salem
America/Indiana/Indianapolis	Atlantic/Cape_Verde	NZ
America/Indiana/Knox	Atlantic/Faeroe	NZ-CHAT
America/Indiana/Marengo	Atlantic/Faroe	Pacific/Apia
America/Indiana/Petersburg	Atlantic/Jan_Mayen	Pacific/Auckland
America/Indiana/Tell_City	Atlantic/Madeira	Pacific/Chatham
America/Indiana/Vevay	Atlantic/Reykjavik	Pacific/Easter
America/Indiana/Vincennes	Atlantic/South_Georgia	Pacific/Efate
America/Indiana/Winamac	Atlantic/St_Helena	Pacific/Enderbury
America/Indianapolis	Atlantic/Stanley	Pacific/Fakaofo

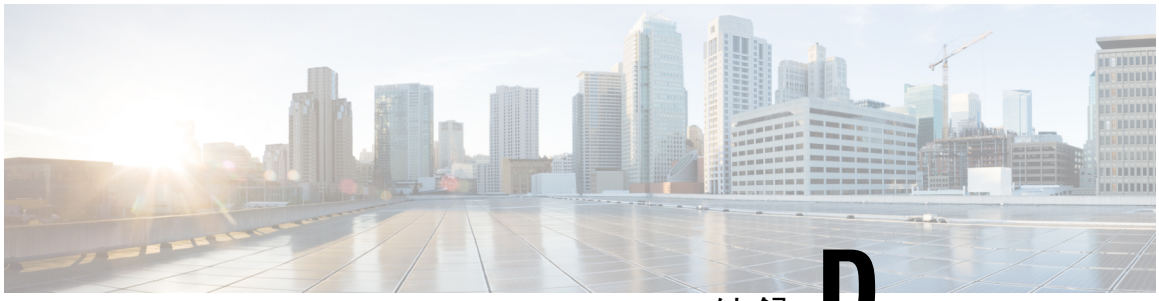
Cisco Prime Infrastructure でサポートされるタイム ゾーン

America/Inuvik	Australia/ACT	Pacific/Fiji
America/Iqaluit	Australia/Adelaide	Pacific/Funafuti
America/Jamaica	Australia/Brisbane	Pacific/Galapagos
America/Jujuy	Australia/Broken_Hill	Pacific/Gambier
America/Juneau	Australia/Canberra	Pacific/Guadalcanal
America/Kentucky/Louisville	Australia/Currie	Pacific/Guam
America/Kentucky/Monticello	Australia/Darwin	Pacific/Honolulu
America/Knox_IN	Australia/Eucla	Pacific/Johnston
America/La_Paz	Australia/Hobart	Pacific/Kiritimati
America/Lima	Australia/LHI	Pacific/Kosrae
America/Los_Angeles	Australia/Lindeman	Pacific/Kwajalein
America/Louisville	Australia/Lord_Howe	Pacific/Majuro
America/Maceio	Australia/Melbourne	Pacific/Marquesas
America/Managua	Australia/North	Pacific/Midway
America/Manaus	Australia/NSW	Pacific/Nauru
America/Marigot	Australia/Perth	Pacific/Niue
America/Martinique	Australia/Queensland	Pacific/Norfolk
America/Mazatlan	Australia/South	Pacific/Noumea
America/Mendoza	Australia/Sydney	Pacific/Pago_Pago
America/Menominee	Australia/Tasmania	Pacific/Palau
America/Merida	Australia/Victoria	Pacific/Pitcairn
America/Mexico_City	Australia/West	Pacific/Ponape
America/Miquelon	Australia/Yancowinna	Pacific/Port_Moresby
America/Moncton	Brazil/Acre	Pacific/Rarotong
America/Monterrey	Brazil/DeNoronha	Pacific/Saipan
America/Montevideo	Brazil/East	Pacific/Samoa
America/Montreal	Brazil/West	Pacific/Tahiti
America/Montserrat	Buenos_Aires	Pacific/Tarawa
America/Nassau	Canada/Atlantic	Pacific/Tongatapu

America/New_York	Canada/Central	Pacific/Truk
America/Nipigon	Canada/Eastern	Pacific/Wake
America/Nome	Canada/East-Saskatchewan	Pacific/Wallis
America/Noronha	Canada/Mountain	Pacific/Yap
America/North_Dakota/	Canada/Newfoundland	Poland
America/North_Dakota/Center	Canada/Pacific	Portugal
America/Panama	Canada/Saskatchewan	PRC
America/Pangnirtung	Canada/Yukon	PST8PDT
America/Paramaribo	CET	ROC
America/Phoenix	Chile/Continental	ROK
America/Port_of_Spain	Chile/EasterIsland	Singapore
America/Port-au-Prince	ComodRivadavia	Turkey
America/Porto_Acre	CST6CDT	UCT
America/Porto_Velho	Cuba	Universal
America/Puerto_Rico	EET	US/Alaska
America/Rainy_River	Egypt	US/Aleutian
America/Rankin_Inlet	Eire	US/Arizona
America/Recife	EST	US/Central
America/Regina	EST5EDT	US/Eastern
America/Resolute	Etc/GMT	US/East-Indiana
America/Rio_Branco	Etc/GMT+0	US/Hawaii
America/Rosario	Etc/GMT+1	US/Indiana-Starke
America/Santarem	Etc/GMT+10	US/Michigan
America/Santiago	Etc/GMT+11	US/Mountain
America/Santo_Domingo	Etc/GMT+12	US/Pacific
America/Sao_Paulo	Etc/GMT+2	US/Samoa
America/Scoresbysund	Etc/GMT+3	UTC
America/Shiprock	Etc/GMT+4	WET
America/St_Barthelemy	Etc/GMT+5	W-SU

Cisco Prime Infrastructure でサポートされるタイム ゾーン

		Zulu



付録 D

よくある質問：オペレーション センターと Prime Infrastructure

• よくある質問：オペレーション センターと Cisco Prime Infrastructure （1161 ページ）

よくある質問：オペレーション センターと Cisco Prime Infrastructure

• アラームおよびイベント
• クロス起動
• デバイス
• レポート
• その他

アラームおよびイベント

Q. オペレーション センターに表示される [アラームのまとめ（Alarm Summary）] の集計値が Cisco Prime Infrastructure の管理対象インスタンスに表示される数と一致しないのはなぜですか。

A. ユーザは、オペレーション センターとオペレーション センターが管理しているすべての Cisco Prime Infrastructure インスタンスが同じアラーム カテゴリを使用していることを確認する必要があります。

オペレーションセンターとすべてのインスタンスが同じカテゴリを使用していることを確認するには、次の手順を実行します。

1. 管理者権限を持つ ID を使用してオペレーション センターにログオンし、**[管理（Administration）] > [ユーザ設定（User Preferences）]** を選択します。
2. [アラーム（Alarms）] の下で、[アラームカテゴリの編集（Edit Alarm Categories）] をクリックします。

よくある質問：オペレーション センターと Prime Infrastructure

3. オペレーション センターで現在選択されているアラーム カテゴリをメモします。通常の状況では、次のカテゴリが選択されます。
   - アラームのまとめ
   - AP
   - コントローラ
   - カバレッジ ホール
   - メッシュ リンク
   - モビリティ サービス
   - パフォーマンス
   - 不正 AP
   - セキュリティ
   - ルータ
   - アプリケーション パフォーマンス
   - スイッチおよびハブ
   - システム
4. いずれかの選択肢を変更する必要がある場合は、選択または選択解除するアラーム カテゴリの横にあるチェックボックスをクリックして、[完了（Done）] をクリックします。
5. Cisco Prime Infrastructure の各管理対象インスタンスで上記の手順を繰り返し、各インスタンスで同じ選択を行います。

Q. オペレーションセンターに表示される合計アラーム数が管理対象インスタンスに表示される数と一致しないのはなぜですか。

A. デフォルトでは、オペレーションセンターは、合計アラーム数を計算するときにすべてのアラームをカウントしますが、Cisco Prime Infrastructure の管理対象インスタンスは、承認済みアラームとクリア済みアラームを非表示にしています。すべての管理対象インスタンスの合計アラーム数をオペレーションセンターのアラーム数と一致させる場合は、承認済みアラームとクリア済みアラームを表示するようにすべての管理対象インスタンスを設定する必要があります。

1. Cisco Prime Infrastructure の最初の管理対象インスタンスにログインします。
2. [管理（Administration）][システム設定（System Settings）][アラームおよびイベント（Alarms and Events）] を選択します。
3. [表示オプションのアラーム（Alarm Display Options）] で、[確認済みのアラームを非表示（Hide acknowledged alarms）] と [クリア済みのアラームを非表示（Hide cleared

よくある質問：オペレーション センターと Prime Infrastructure

alarms）] の横にあるチェックボックスが両方とも**オフ**になっていることを確認します。

4. [保存（Save）] をクリックして変更を保存します。
5. 他のすべての管理対象インスタンスでこれらの手順を繰り返します。

Q. オペレーション センターに表示されるイベントおよび Syslog の集計数が管理対象インスタンスに表示される数と一致しないのはなぜですか。

A. 性質上、イベントおよびsyslogは管理対象インスタンス上で常に変化しています。この変化は、5 秒ごとに更新ボタンをクリックすることで確認できます。イベントおよび Syslog の数が変化してから、対応するNBIコールでその数が更新されるまでの時間には、常にわずかなラグがあります。これは絶えず変化しているため、オペレーションセンターに表示される集計数を個々の管理対象インスタンスと比較するべきではありません。

クロス起動

Q. [ネットワークデバイスの概要（NDS）（Network Device Summary (NDS)）] ダッシュレットからワイヤレス コントローラ（WLC）の [デバイス（Devices）] ページにクロス起動するときに不一致があるのはなぜですか。

A. これは、Cisco Prime Infrastructure がダッシュレットのデータと個々のワイヤレス デバイスのデータを取得する方法の違いによる問題です。[ネットワークデバイスの概要（Network Device Summary）] のカウントを取得するために、ダッシュレットは、デバイスが到達可能なときにエントリを持つデータ構造を照会しますが、インベントリ収集ステータスはチェックしません。開いている WLC の [デバイス（Devices）] ページをクロス起動すると、そのデバイスのインベントリ収集ステータスが正常である（少なくとも一度）場合にのみ、エントリがあるテーブルからカウントが取得されます。これはオペレーションセンターではなく Cisco Prime Infrastructure の問題であることに注意してください。

Q. [ネットワークデバイス（Network Devices）]ページの特定のデバイス グループからのクロス起動に関する既知の問題はありますか。

A. オペレーション センターの [ネットワークデバイス（Network Devices）] ページ下の特定のデバイス グループから、管理対象インスタンス内の同じデバイス グループへのクロス起動に関する既知の問題があります。ユーザは管理対象インスタンスの [ネットワークデバイス（Network Devices）] ページにリダイレクトされますが、オペレーション センターで選択されたデバイス グループではなくすべてのデバイス グループが表示されます。

Q. [ネットワークデバイスの概要（Network Device Summary）] ダッシュレットのサードパーティ製 AP でクロス起動が正常に機能しないのはなぜですか。

A. オペレーションセンターのサードパーティ製APの[ネットワークデバイスの概要（Network Device Summary）] ダッシュレットからのクロス起動には既知の問題があります。オペレーションセンターからクロス起動すると、[ネットワークデバイス（Network Devices）] ページにはサードパーティ製 AP は表示されません。

Q. syslog のクロス起動が予期どおりに機能しません。

A. 現在 Cisco Prime Infrastructure では、syslog のインスタンス ID によるフィルタリングはサポートされていません。その結果、オペレーション センターは、Cisco Prime Infrastructure

よくある質問：オペレーション センターと Prime Infrastructure

の管理対象インスタンスへのクロス起動時に、syslog のフィルタリングをサポートできません。

デバイス

Q. オペレーション センターの [クライアントおよびユーザ（Clients and Users）] ページと、Cisco Prime Infrastructure 管理対象インスタンスの同じページで、VLAN ID とアソシエーション ID に違いがあるのはなぜですか。

A. これは、これらの値がすばやく更新されるために発生します。オペレーションセンターでこれらの値を更新すると、Cisco Prime Infrastructure 管理対象インスタンスで同じデータが既に変更されている可能性があります。

Q. オペレーションセンターと管理対象インスタンス間で、[デバイスの詳細（Device Details）] ページの 自律 AP の [CPU使用率（CPU Utilization）] フィールドと [メモリ使用率（Memory Utilization）] フィールドに表示される内容が異なるのはなぜですか。

A. 不一致の理由の 1 つは、これらの値が非常に迅速に変化することです。オペレーションセンターでこれらの値を更新すると、1 つ以上の Cisco Prime Infrastructure 管理対象インスタンスで同じデータが既に変更されている可能性があります。

レポート

Q. オペレーション センターと Cisco Prime Infrastructure で生成されるレポート値にわずかな差異があるのはなぜですか。

A. これは予期された動作です。Cisco Prime Infrastructure は小数値を自由に使用してレポート値を生成しますが、オペレーションセンターは丸められた数値のセットを使用してこれらの値を集約します。このため不一致が生じます。

Q. レポート データが 2.1 の Cisco Prime Infrastructure インスタンスからポーリングされないのはなぜですか。

A. 2.1 の Cisco Prime Infrastructure インスタンス上の既存のレポートと同じ名前でオペレーションセンターでレポートを生成しようとすると、そのインスタンスのデータはオペレーション センターで無視されます。この問題を回避するには、オペレーション センターとすべての管理対象 Cisco Prime Infrastructure インスタンス間で一意となるレポート名を指定します。

その他

Q. 2.1 の管理対象インスタンスからサイト情報が取得されないのはなぜですか。

A. **[パフォーマンス（Performance）] > [デバイス（Device）] > /デバイスを選択/ > [サイト（Site）]** の順に選択すると、2.1 インスタンスのサイト情報は取得されません。これは、

よくある質問：オペレーション センターと Prime Infrastructure

Cisco Prime Infrastructure バージョン 2.1 と 2.2 の間で変更された内部（IFM）API が原因です。

Q. オペレーション センターと Cisco Prime Infrastructure で、[現在関連付けられている有線クライアント（Current Associated Wired Clients）] テーブルの列が異なるのはなぜですか。

A. オペレーションセンターの [現在関連付けられている有線クライアント（Current Associated Wired Clients）] テーブルには固定列があります。Cisco Prime Infrastructure の管理対象インスタンスの同じテーブルには、カスタマイズ可能な列があります。オペレーション センターの今後のバージョンでは、これが変更される可能性があります。

よくある質問：オペレーション センターと Prime Infrastructure