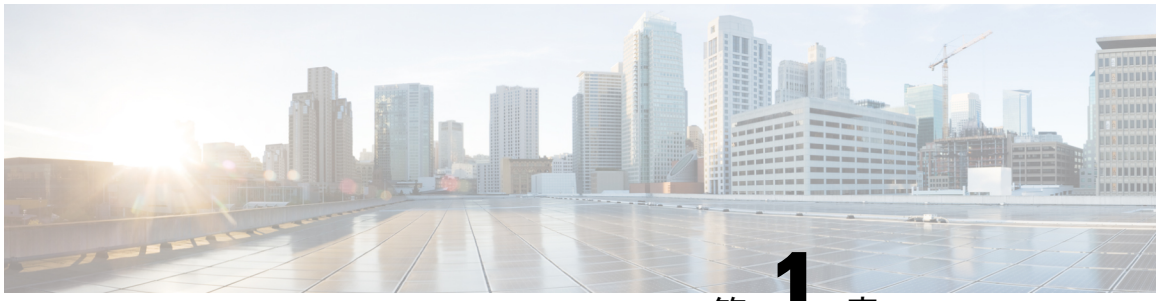
Cisco DNA Center リリース 2.3.3 ユーザーガイド

初版：2022 年 4 月 26 日

最終更新：2023 年 4 月 21 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/

目 次



第 1 章

新機能および変更された機能に関する情報

新機能および変更された機能に関する情報

次の表に、新機能および変更された機能の要約と参照先を示します。

表 *1 : Cisco DNA Center* リリース *2.3.3.7* の新機能および機能変更

機能	説明
動的チャネル割り当て（DCA）の検証	DCA チャネルのサポートは、デバイスの規制ドメインに基づきます。RF プロファイルを選択して AP をプロビジョニングする際、RF プロファイルで設定されたすべての DCA チャネルのうち、国コードに従ってサポートされているチャネルのみが考慮され、サポートされていないチャネルは無視されます。サポートされていないチャネルのリストは、AP 事前プロビジョニングの [Summary] ウィンドウで確認できます。 ワイヤレス無線周波数プロファイルの作成 （268 ページ）、AI 無線周波数プロファイルの作成 （273 ページ）、およびワイヤレスデバイスと国コードについて （421 ページ）を参照してください。

表 *2 : Cisco DNA Center* リリース *2.3.3* の新機能および機能変更

機能	説明
Cisco DNA Center Insights	製品の発表、ネットワークのハイライト、ネットワークパフォーマンスに関する情報などを含む *Cisco DNA CenterInsights* を購読できます。*Cisco DNA Center Insights* パブリケーションは、指定した電子メールアドレスに PDF 形式で送信されます。 『Cisco DNA Center インサイトへの登録 （31 ページ）』を参照してください。

新機能および変更された機能に関する情報

機能	説明
シスコデバイスのハードウェア、ソフトウェア、およびモジュールのサポート終了（EoX）ステータス	Cisco DNA Center は、EoX アラートのスキャンを実行したデバイスのアラートを表示します。[Inventory] テーブルの [EoX Status] 列には、EoX アラートの数が表示されます。 『インベントリに関する情報の表示 （85 ページ）』を参照してください。
クレデンシャルステータス	[Inventory] テーブルの [Credential Status] 列には、設定されているデバイスのデバイスクレデンシャルステータスが表示されます。クレデンシャルの詳細を表示するには、[See Details] をクリックします。 『インベントリに関する情報の表示 （85 ページ）』を参照してください。
すべてのディスカバリの表示	Cisco DNA Center の新しい [Discoveries] テーブルには、すべてのディスカバリジョブの詳細が表示され、再ディスカバリおよびディスカバリジョブ削除のオプションが提供されます。 『すべてのディスカバリの表示 （80 ページ）』を参照してください。
システムビーコンの管理	システムビーコンを使用して、Cisco DNA Center インベントリ内のスイッチを強調表示できます。 システムビーコンは、次のデバイスをサポートします。 • Cisco Catalyst 3850 シリーズ イーサネット スタッカブル スイッチ • Cisco Catalyst 9200 シリーズ スイッチ • Cisco Catalyst 9300 シリーズ スイッチ 『システムビーコンの管理 （125 ページ）』を参照してください。
Cisco AI エンドポイント分析と Talos インテリジェンスの統合	Talos インテリジェンス [英語] は、包括的な脅威検出ネットワークです。Talos は脅威をリアルタイムで検出して相関関係を示します。Cisco AI エンドポイント分析を Talos と統合することで、悪意のある IP アドレスに接続しているネットワーク内のエンドポイントにフラグを付けることができます。 『Cisco AI エンドポイント分析とTalos インテリジェンスの統合 （694 ページ）』を参照してください。
ソフトウェアイメージへのデバイスロールとタグの割り当て	ソフトウェアイメージにデバイスロールとタグを割り当て、ソフトウェアイメージがゴールデンとしてマークされていることを示すことができます。デバイスタグとデバイスロールの両方がソフトウェアイメージに割り当てられている場合、デバイスタグが優先されます。 『ソフトウェアイメージの表示 （356 ページ）』を参照してください。
ソフトウェアイメージの更新の同期	Cisco DNA Center 内のすべての管理対象デバイスについて、cisco.com からのソフトウェアイメージの情報を同期できます。 『ソフトウェアイメージの表示 （356 ページ）』を参照してください。

新機能および変更された機能に関する情報

機能	説明
FIPS 140-2 のサポート	ソフトウェアイメージは、連邦情報処理標準（FIPS）に準拠しています。Cisco DNA Center で FIPS モードが有効になっている場合、URL からイメージをインポートすることはできません。コンピュータまたは cisco.com からイメージをインポートします。 『ソフトウェア イメージのインポート （360 ページ）』を参照してください。
	FIPS モードは、Cisco DNA Center の新規インストールでのみサポートされます。以前のリリースからのアップグレードの場合は、FIPS モードはサポートされません。
	FIPS 展開では、外部認証を有効にできません。
	Cisco Wide Area Bonjour アプリケーションでは、FIPS モードはサポートされていません。FIPS 展開では、Cisco DNA Center GUI または CLI から Cisco Wide Area Bonjour アプリケーションをインストールできません。
	FIPS モードは、マップアーカイブのエクスポートとインポートに次の影響を与えます。 FIPS モードが有効な場合： • エクスポートされるマップアーカイブは暗号化されません。 • 暗号化されていないマップアーカイブのみをインポートできます。 FIPS モードが無効な場合： • エクスポートされるマップアーカイブは暗号化されます。 • 暗号化されたマップアーカイブと暗号化されていないマップアーカイブの両方をインポートできます。 既存の Cisco ネットワーク階層の使用 （156 ページ）、Cisco DNA Center からのマップアーカイブのエクスポート （164 ページ）、およびCisco DNA Center へのマップアーカイブのインポート （160 ページ）を参照してください。
エンドポイント分析の FIPS サポート	Cisco DNA Center で FIPS モードが有効になっている場合、エンドポイント分析に関連する一部の機能は Cisco DNA Center GUI で使用できません。 『FIPS Compliance （687 ページ）』を参照してください。
イメージ更新ワークフローの表示	ソフトウェアイメージの更新タスクの進行状況を表示できます。Cisco DNA Center は、配布操作とアクティブ化操作に関連付けられている各タスクのステータスと、各操作の完了にかかった時間を示します。 『イメージ更新ワークフローの表示 （374 ページ）』を参照してください。

新機能および変更された機能に関する情報

機能	説明
エンドポイント スプーフィングの制御	コントロール エンドポイント スプーフィング機能は、エンドポイントの MAC アドレス以外のネットワーク情報を提供することにより、詳細なポリシーコントロールを提供します。 『エンドポイント スプーフィングの制御 （725 ページ）』を参照してください。

3D ワイヤレスマップの機能強化	• 3D ワイヤレスマップと Cisco DNA Spaces または Cisco Connected Mobile Experiences（CMX）の間の相互作用が改善されました。
	• 3D ワイヤレスマップのその他の機能強化により、次のことが可能になります。
	  • 建物内の空き領域の 3D RF モデリングを実行する。
	  • 3D ヒートマップの計算に最大 5 フロアを含める。
	  • 信号漏れと信号反射を表示する。
	  • 関連付けられた AP へのクライアントのリンクなどのクライアント情報を表示する。
	  • 画面のサイズを変更した後も、引き続き 3D マップツールバーを表示する。
	
	3D ワイヤレスマップの表示 （210 ページ）、3D マップビューオプション （213 ページ）、および3D ワイヤレスマップツールバー （211 ページ）を参照してください。

新機能および変更された機能に関する情報

機能	説明
2D ワイヤレスマップの機能強化	• 2D ワイヤレスマップと Cisco DNA Spaces または Cisco Connected Mobile Experiences（CMX）の間の相互作用が改善されました。 • 2D ワイヤレスマップのその他の機能強化により、次のことが可能になります。 • スイッチスタックを表示して、個々のスイッチとそれらに関連付けられた AP 間のリンクを表示する。 • 関連付けられた AP へのクライアントのリンクなどのクライアント情報を表示する。 • AP アイコンで、AP 無線の状態、正常性、名前、およびモードを表示する。 • CAD ファイルを使用してフロアマップを作成するときに、グリッドパターンをオンまたはオフにする。 • 計画済み AP にデュアル無線を設定する。 • フロアに位置合わせポイントを追加して、フロアが正確に順に重なって配置されるようにする。 • Ekahau サイト調査ファイルを Cisco DNA Center にインポートする。 • 画面のサイズを変更した後も、引き続き 2D マップツールバーを表示する。 2D ワイヤレスフロアマップの表示 （195 ページ）、CAD マップファイルを使用したフロアの追加 （171 ページ）、マップへの計画済み AP の追加 （180 ページ）、AP アイコンの凡例 （205 ページ）、位置合わせポイントの追加、編集、および削除 （195 ページ）、およびEkahau サイト調査の Cisco DNA Center へのインポート （163 ページ）を参照してください。
インベントリの管理	[Inventory] ウィンドウで [Focus] ドロップダウンリストから [Default] ビューを選択した場合、[Inventory] テーブルには、リストされたデバイスの [Device Name]、[IP Address]、[Device Family]、および [MAC Address] のみが表示されます。 『インベントリに関する情報の表示 （85 ページ）』を参照してください。
LAN オートメーション サマリールートを BGP にアドバタイズする	LAN 自動化は、プライマリデバイスとピアデバイスの BGP にサマリールートをアドバタイズします。 『LAN 自動化によるネットワークのプロビジョニング （501 ページ）』を参照してください。
ファブリックサイトのボーダー優先設定オプション	必要なボーダーノードを介してトラフィックをナビゲートするには、ファブリックサイトのボーダーノードに優先順位値を割り当てます。 『ボーダーノードとしてのデバイスの追加 （515 ページ）』を参照してください。

新機能および変更された機能に関する情報

機能	説明
拡張ノードのポリシー拡張ノードへのアップグレード	ライセンスレベルを変更することにより、拡張ノードとして構成されているポリシー拡張ノード対応デバイスをアップグレードできます。 『拡張ノードのポリシー拡張ノードへのアップグレード （534 ページ）』を参照してください。
REP リングトポロジステータスの表示	[REP Ring Topology Status] オプションを使用すると、REP リング内のすべてのデバイスの現在の状態を表示できます。 『REP リングステータスの表示 （538 ページ）』を参照してください。
NAS ID の設定	エンタープライズおよびゲスト ワイヤレス ネットワークの SSID にネットワーク アクセス サーバー識別子（NAS ID）を設定できます。 エンタープライズ ワイヤレス ネットワーク用 SSID の作成 （248 ページ）およびゲスト ワイヤレス ネットワークの SSID の作成 （256 ページ）を参照してください。
ゲストワイヤレスネットワーク用の、サードパーティ AAA サーバーを使用した中央 Web 認証	ゲストワイヤレスネットワークの SSID を作成するときに、サードパーティ AAA サーバーを使用して中央 Web 認証（CWA）を設定できるようになりました。 ゲスト ワイヤレス ネットワークの SSID の作成 （256 ページ）およびゲスト ワイヤレス ネットワーク用の AAA サーバーの設定 （264 ページ）を参照してください。
グループベースのアクセス コントロール ポリシーの更新スケジュール設定	ポリシーの変更をすぐに保存することも、特定の時刻に更新をスケジュールすることもできます。**[Activities]** > **[Tasks]** で、スケジュールされたタスクのステータスを表示できます。 [Cisco DNA Center Automation Events for ITSM (ServiceNow)] バンドルが有効になっている場合、[Save Now] オプションは無効になり、グループベースのアクセス コントロール ポリシー変更に対する [Schedule Later] オプションのみが有効になります。スケジュールされたタスクは、スケジュールされた時刻の前に IT サービス管理（ITSM）で承認される必要があることに注意してください。 『グループベースのアクセス コントロール ポリシー （603 ページ）』を参照してください。

機能	説明
ワイヤレスネットワークの QoS 設定	エンタープライズおよびゲスト ワイヤレス ネットワークの SSID を作成するときに、プライマリトラフィックに対して次のいずれかの QoS 設定を選択できます。 • [VoIP (Platinum)] • [Video (Gold)] • [Best Effort (Silver)] • [Non-real Time (Bronze)] エンタープライズ ワイヤレス ネットワーク用 SSID の作成 （248 ページ）およびゲスト ワイヤレス ネットワークの SSID の作成 （256 ページ）を参照してください。
新しいデバイスの返品許可（RMA）のサポート	RMA ワークフローのサポートは、次のように拡張されています。 • Cisco Catalyst 4500e、Catalyst 6500、Catalyst 6800、および Catalyst 9000 シリーズのモジュラ型スイッチ。 • シングルエンジンおよびデュアルエンジンを搭載した、モジュラ型スイッチのスーパーバイザ。 • STP リングまたはデイジーチェーンの一部である拡張ノード。 • 産業用イーサネット（IE）スイッチのデイジーチェーンとリング。 • 外部の Simple Certificate Enrollment Protocol（SCEP）ブローカー PKI 証明書を持つデバイス。 『故障したデバイスの交換 （136 ページ）』を参照してください。
RMA サポート	PnP による交換デバイスのゼロタッチオンボーディングは、ファブリックおよび LAN 自動化デバイスでサポートされています。 故障したデバイスの交換 （136 ページ）およびCisco DNA Center での RMA ワークフローの制限事項 （141 ページ）を参照してください。
複数の シスコ ワイヤレス コントローラ にまたがる AP 更新	古い AP と新しい AP が異なる シスコ ワイヤレス コントローラに接続されている場合に AP の更新を実行できます。古い AP がプロビジョニングされていない場合でも、AP の更新を実行できます。 『AP 更新ワークフロー （781 ページ）』を参照してください。
ネットワーク階層の設計	[Site Name] と [Site Type] のフィルタ基準を使用して、ネットワーク階層を検索できるようになりました。 『ネットワーク階層の検索 （165 ページ）』を参照してください。

新機能および変更された機能に関する情報

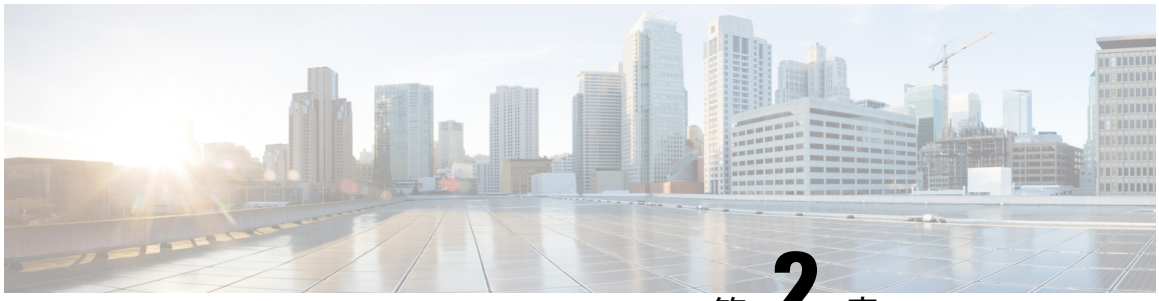
機能	説明
URL ベースのアクセスコントロールリスト	ネットワークの IP ベースおよび URL ベースの認証後アクセスコントロールリスト（ACL）を作成できます。 『IP ベースおよび URL ベースのアクセス コントロール ポリシー作成のワークフロー （812 ページ）』を参照してください。
サイトを選択しない Day 0 オンボーディング用のカスタムテンプレート	デバイスをサイトに割り当てていない場合は、テンプレートを選択してデバイスを要求する必要があります。 『スイッチまたはルータ デバイスのプロビジョニング （408 ページ）』を参照してください。
アプリケーションホスティングの機能強化	デバイスの準備状況チェック中に、デバイスに提供された HTTPS クレデンシャルを検証できます。 『Cisco Catalyst 9300 デバイスへのアプリケーションのインストール （577 ページ）』を参照してください。
AP の定期的なイベントのスケジュール	AP 設定ワークフローで、AP の定期的なイベントおよび無線パラメータをスケジュールできます。 『AP ワークフローの定期的なイベントのスケジュール （798 ページ）』を参照してください。
AP 設定ワークフローの機能強化	サイトに割り当てられていない AP も設定できます。 次の AP パラメータを設定できます。 • AP の高さ • LED の明るさレベル 次の無線パラメータを設定できます。 • CleanAir またはスペクトルインテリジェンスの設定 • アンテナの設定 Cisco DNA Center での AP 設定 （791 ページ）および AP ワークフローの設定 （791 ページ）を参照してください。
コンプライアンス監査レポートの生成	ネットワーク内のデバイスのコンプライアンスステータスを示す統合コンプライアンスレポートを取得できます。 『ネットワークデバイスのコンプライアンス監査レポートの生成 （382 ページ）』を参照してください。
ポートグループの作成	属性またはルールに基づいてデバイスポートをグループ化できます。 『ポート グループの作成 （121 ページ）』を参照してください。

機能	説明
モニター対象外デバイスのトラブルシューティング	MRE ワークフローを使用すると、モニター対象外デバイスまたは Cisco DNA アシュアランス データが表示されないデバイスのトラブルシューティングを行うことができます。 『MRE ワークフローを使用したモニター対象外のデバイスのトラブルシューティング （754 ページ）』を参照してください。
ワイヤレスクライアントに関する問題のトラブルシューティング	MRE ワークフローを使用して、ワイヤレスクライアントの問題のトラブルシューティングを行うことができます。 『MRE ワークフローを使用した無線クライアントの問題のトラブルシュート （753 ページ）』を参照してください。
カスタムポリシータグ	ワイヤレスデバイスのネットワークプロファイルを作成するときに、詳細設定を使用して Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのポリシータグを設定できます。 『ネットワークプロファイルの AP グループ、Flex グループ、サイトタグ、およびポリシータグの事前プロビジョニング （308 ページ）』を参照してください。
AP ゾーン	AP ゾーンをワイヤレスデバイス用のネットワークプロファイルに追加できます。AP ゾーンを使用すると、同じサイト上の一連の AP に異なる SSID と RF プロファイルを関連付けることができます。 ワイヤレス用のネットワークプロファイルの作成 （304 ページ）およびシスコ製 AP のプロビジョニング：Day 1 AP プロビジョニング （430 ページ）を参照してください。
SD-Access ユーザーインターフェイスの機能強化	• [Create Fabric Site] ワークフローが拡張され、有線エンドポイントデータの収集および認証テンプレート設定を構成するオプションが含まれるようになりました。 • ファブリックサイトの [Port Assignment] タブのオプションが強化されました。 • ファブリックサイトの認証テンプレートを選択するためのオプションが、[Authentication Template] タブに表示されるようになりました。 • [Create Port Channel] ワークフローが強化されました。 • エニーキャストゲートウェイ設定を構成するオプションが、[Anycast Gateway] タブに表示されるようになりました。 • [Create Layer 2 Virtual Networks] と [Create Layer 3 Virtual Networks] が強化されました。 ファブリックサイトの追加 （511 ページ）、ファブリックサイトのデバイスの構成 （512ページ）、ファブリックサイト内のポートの設定 （520ページ）、ポートチャネルの設定 （547ページ）、および仮想ネットワーク （522ページ）を参照してください。

新機能および変更された機能に関する情報

第 I 部

はじめに



第 2 章

Cisco DNA Center について

Cisco DNA Center の概要

Cisco Digital Network Architecture は、設計、プロビジョニング、ネットワーク環境全体へのポリシーの適用を迅速かつ容易にする一元化された使いやすい管理機能を備えています。Cisco DNA Center GUI はネットワークを隅々まで見ることを可能にし、ネットワーク パフォーマンスの最適化およびユーザーエクスペリエンスおよびアプリケーションエクスペリエンスの最適化のためにネットワークインサイトを利用します。

ログイン

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

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

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

https://*server-ip*

例：https://192.0.2.1

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

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

使用しているユーザー ID に SUPER-ADMIN-ROLE が割り当てられていて、同じ権限を持つ他のユーザーが先にログインしていない場合、ホームページではなく初回セットアップウィザードが表示されます。

ステップ 3 ログアウトするには、メニューアイコン（☰）をクリックし、[Sign Out] を選択します。

クイック スタート ワークフローの完了

Cisco DNA Center アプライアンスをインストールして設定した後、Web ベースの GUI にログインできます。Cisco DNA Center にアクセスする際には、互換性のある HTTPS 対応ブラウザを使用してください。

（ユーザー名 admin と SUPER-ADMIN-ROLE が割り当てられた）管理者スーパーユーザーとして初めてログインすると、クイック スタート ワークフローが自動的に開始されます。このワークフローを完了して、Cisco DNA Center がデバイスからのテレメトリの収集を管理および有効化するデバイスを検出します。

始める前に

Cisco DNA Center にログインしてクイック スタート ワークフローを完了するには、次の内容が必要です。

- Cisco DNA Center 第 2 世代アプライアンスの設置ガイドに記載されている、次のいずれかの手順を実行する際に指定した管理スーパーユーザーのユーザー名とパスワード。
  - Maglev ウィザードを使用したプライマリ ノードの設定
  - インストール構成ウィザードを使用したアプライアンスの設定（44 コアまたは 56 コアアプライアンス）
  - インストール構成ウィザードを使用したアプライアンスの設定（112 コアアプライアンス）
  - 高度なインストール構成ウィザードを使用したプライマリ ノードの設定（44 コアまたは 56 コアアプライアンス）

- 高度なインストール構成ウィザードを使用したプライマリノードの設定（112 コアアプライアンス）

- 設置ガイドの「Required First-Time Setup Information」のトピックで説明されている情報。

ステップ 1 Cisco DNA Center アプライアンスのリブートが完了したら、ブラウザを起動します。

ステップ 2 **HTTPS://** と設定プロセスの最後に表示された Cisco DNA Center GUI の IP アドレスを使用して、Cisco DNA Center GUI にアクセスするホスト IP アドレスを入力します。

IP アドレスを入力すると、次のいずれかのメッセージが表示されます（使用しているブラウザによって異なります）。

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

ステップ 3 メッセージを無視して **[詳細設定（Advanced）]** をクリックします。

次のメッセージが表示されます。

- Google Chrome：

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

- Mozilla Firefox：

```
Someone could be trying to impersonate the site and you should not continue.

Websites prove their identity via certificates. Firefox does not trust GUI-IP-address because
its certificate issuer is unknown,
the certificate is self-signed, or the server is not sending the correct intermediate
certificates.
```

こうしたメッセージが表示されるのは、コントローラが自己署名証明書を使用しているためです。Cisco DNA Center での証明書の使用方法については、『Cisco DNA Center 管理者ガイド』の「Certificate and Private Key Support」の項を参照してください。

ステップ 4 メッセージを無視し、次のいずれかを実行します。

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

Cisco DNA Center ログイン画面が表示されます。

ステップ 5 次のいずれかを実行し、[Log In] をクリックします。

- Maglev 構成ウィザードを完了し、[Start using DNAC pre manufactured cluster] オプションを選択した場合は、管理者のユーザー名（**admin**）とパスワード（**maglev1@3**）を入力します。

- Maglev 構成ウィザードを完了し、[Start configuration of DNAC in advanced mode] オプションを選択した場合は、Cisco DNA Center アプライアンスの構成時に設定した管理者のユーザー名（**admin**）とパスワードを入力します。
- インストール構成ウィザードを完了したら、管理者のユーザー名（**admin**）を入力し、ウィザードの最後の画面からコピーしたパスワード（**maglev1@3**）を貼り付けます。
- 高度なインストール構成ウィザードを完了した場合は、Cisco DNA Center アプライアンスの構成時に設定した管理者のユーザー名（**admin**）とパスワードを入力します。

次の画面で、（セキュリティ対策として）新しい管理者パスワードを指定するよう求められます。

ステップ 6 次のいずれかを実行します。

- この時点で管理者パスワードを変更しない場合は、[Skip] をクリックします。
- 新しい管理者パスワードを設定するには、次の手順を実行します。
  1. ステップ 5 で指定したのと同じパスワードを入力します。
  2. 新しい管理者パスワードを入力し、確認します。
  3. [Next] をクリックします。

ステップ 7 cisco.com のユーザー名とパスワード（ソフトウェアダウンロードの登録とシステム通信の受信に使用される）を入力し、[Next] をクリックします。

（注） 現時点でこれらのログイン情報を入力したくない場合は、代わりに [Skip] をクリックします。

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

ステップ 8 各ドキュメントを確認したら、[Next] をクリックして EULA に同意します。

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

ステップ 9 クイック スタート ワークフローを完了します。

a) [Let's Do it] をクリックします。

b) [Discover Devices: Provide IP Ranges] 画面で、次の情報を入力し、[Next] をクリックします。

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

c) [Discover Devices: Provide Credentials] 画面で、設定するログイン情報のタイプに関する情報（次の表を参照）を入力し、[Next] をクリックします。

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

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

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

d) [Create Site] 画面で、テレメトリを容易にするために検出するデバイスを 1 つのサイトにグループ化し、[Next] をクリックします。

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

e) [Enable Telemetry] 画面で、Cisco DNA Center にテレメトリを収集させるネットワークコンポーネントを選択し、[Next] をクリックします。

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

f) [Summary] 画面で、入力した設定を確認し、次のいずれかを実行します。

- 変更を加える場合は、該当する [Edit] リンクをクリックして、関連画面を開きます。
- 設定に問題がなければ、[Start Discovery and Telemetry] をクリックします。Cisco DNA Center により設定が検証され、問題が発生しないことが確認されます。検証が完了すると、画面が更新されます。

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

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

g) 次のいずれかを実行します。

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

ユーザープロファイルの役割および権限

Cisco DNA Center は、ロールベース アクセス コントロール（RBAC）をサポートします。ユーザープロファイルに割り当てられたロールは、ユーザーが実行する権限を持つ機能を定義します。Cisco DNA Center には、SUPER-ADMIN-ROLE、NETWORK-ADMIN-ROLE、および OBSERVER-ROLE の 3 つの主要なデフォルトユーザーロールがあります。

SUPER-ADMIN-ROLE は、ユーザーに幅広い機能を提供し、カスタムロールの作成やユーザープロファイルへの割り当てなど、Cisco DNA Center GUI ですべてのアクションを実行できるようにします。NETWORK-ADMIN-ROLE と OBSERVER-ROLE は、Cisco DNA Center GUI での機能が制限されます。

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

デフォルト ホームページ

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

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

アシュアランス 要約

このエリアには次が含まれています。

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

[Network Snapshot]

このエリアには次が含まれています。

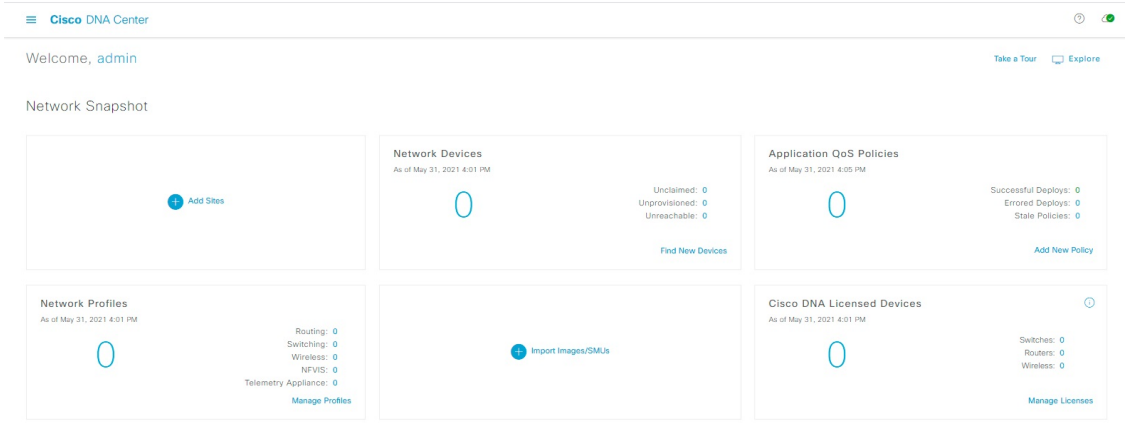
- [Sites]：ネットワーク上で検出されたサイトの数と、DNS サーバーおよびNTP サーバーの数が示されます。[Add Sites] をクリックすると、[Add Site] ウィンドウが表示されます。

- [Network Devices]：ネットワーク上で検出されたネットワーク デバイスの数と、要求されていないデバイス、プロビジョニングされていないデバイス、および到達不能なデバイスの数が示されます。[Find New Devices] をクリックすると、[New Discovery] ウィンドウが表示されます。
- [Application policies]：ネットワーク上で検出されたアプリケーション ポリシーの数と、成功およびエラーになった展開の数を表示します。[Add New Policy] をクリックすると、[Application Policies] ウィンドウが表示されます。
- [Network Profiles]：ネットワーク上で検出されたプロファイルの数を示します。[Manage Profiles] をクリックすると、[Network Profiles] ウィンドウが表示されます。
- [Images]：ネットワーク上で検出されたイメージの数と、タグなしイメージおよび未検証イメージの数が示されます。[Import Images/SMUs] をクリックすると、[Image Repository] ウィンドウが表示されます。
- [Licensed Devices]：Cisco DNA Center ライセンスを持つデバイスの数と、スイッチ、ルータ、およびアクセスポイントの数が示されます。[Manage Licenses] をクリックすると、[License Management] ウィンドウが表示されます。
- [EoX Status]：ネットワーク上で検出された EoX アラートの数を提供します。[Accept EoX EULA] をクリックすると、[Success Tracks] ウィンドウが表示されます。[Success Tracks] ウィンドウの情報を読み、[OK] をクリックしてネットワークをスキャンして EoX アラートを探します。

ツール

[Tools] エリアを使用して、ネットワークを設定および管理します。

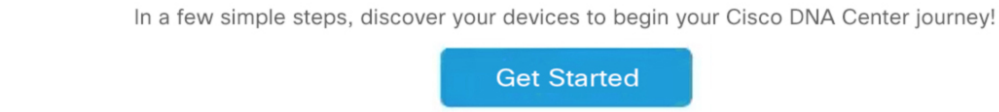
図 *1 : Cisco DNA Center* ホームページ



ホームページのさまざまなビュー

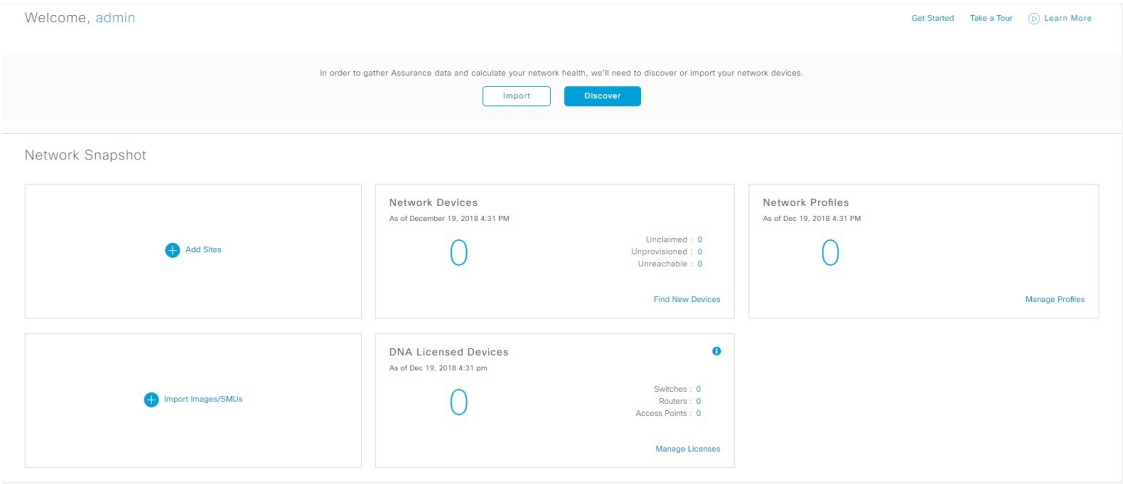
ホームページは、Cisco DNA Center のさまざまなステージやログインに使用されるロールなどの要因によって異なります。

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

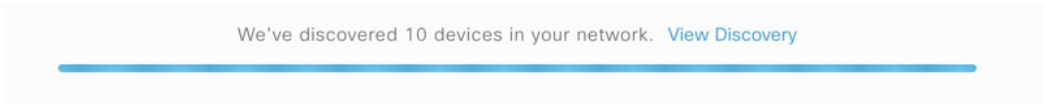


初めてオブザーバとしてCisco DNA Centerにログインすると、次のメッセージが表示されます。

- [Day 0 Home Page]：開始をスキップした場合、またはシステム内にデバイスが存在しない場合は、次のホームページが表示されます。



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



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

メニュー バー

メニューバーの左側にあるメニューアイコン（☰）をクリックして、次のメニュー項目にアクセスします。

- 設計
- ポリシー
- プロビジョニング
- 保証
- ワークフロー
- ツール
- プラットフォーム
- アクティビティ
- Reports
- システム
- 詳細

アイコン

一般的なタスクを実行するには、メニューバーの右側にあるアイコンをクリックします。

アイコン	説明
	[Search]：Cisco DNA Center データベース内の任意の場所に保存されているデバイス、ユーザー、ホスト、メニュー、およびその他の項目を検索します。

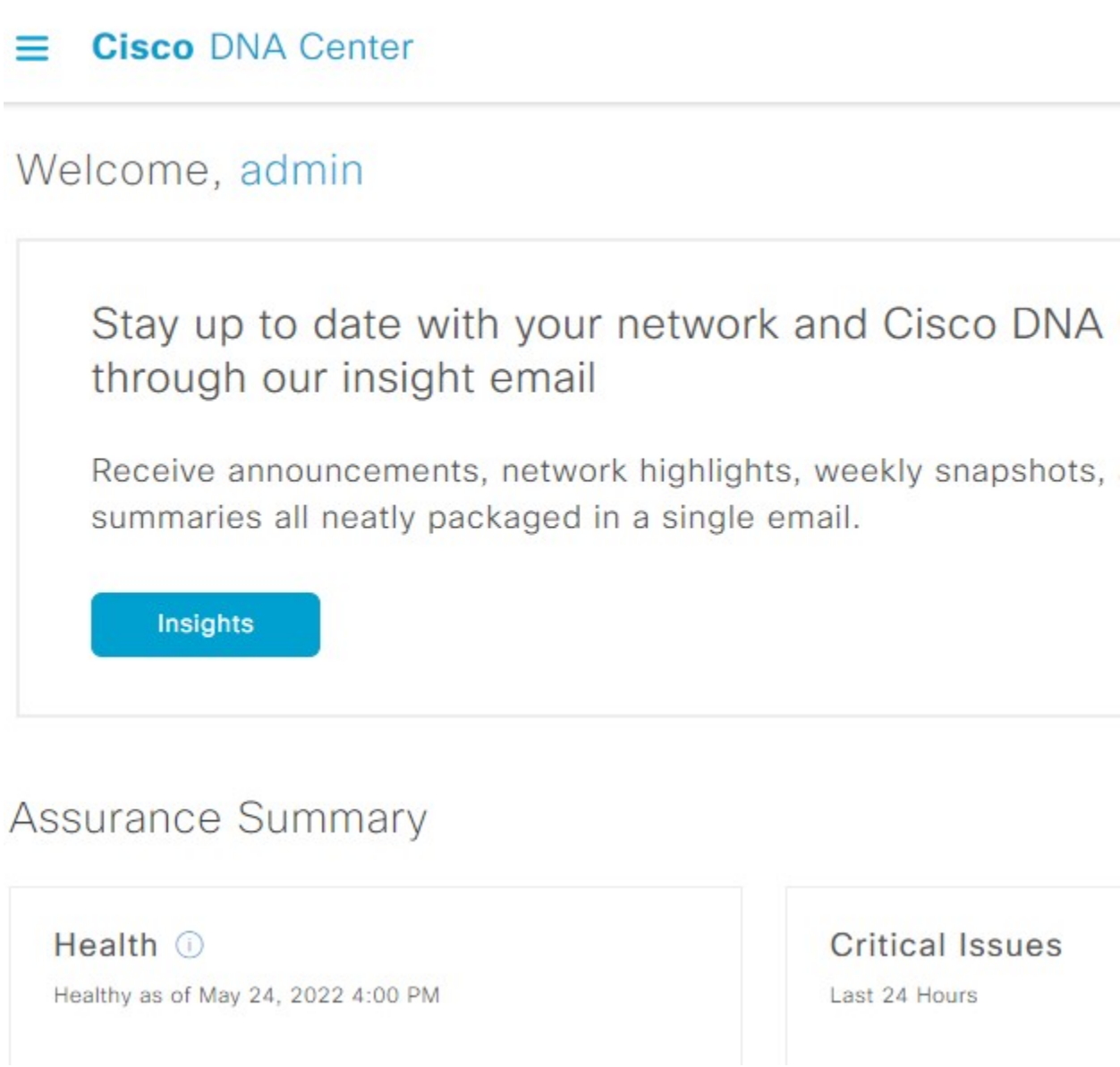
アイコン	説明
	**Help** • [About]： 現在の Cisco DNA Center のソフトウェアバージョンが表示されます。 [Release Notes] をクリックすると、別のブラウザタブでリリースノートが起動します。 [Packages] をクリックすると、システムおよびアプリケーションパッケージのバージョンが表示されます。 [Serial number] をクリックすると、Cisco DNA Center のアプライアンスのシリアル番号が表示されます。 • [API Reference]：Cisco DevNet に Cisco DNA Center プラットフォーム API のドキュメントが開きます。 • [Developer Resources]：開発者ツールにアクセスできる Cisco DevNet が開きます。 • [Contact Support]：Cisco Technical Assistance Center（TAC）でサポートケースが開きます。 • [Remote Support Authorization]：ネットワークのトラブルシューティングを行うために、シスコの専門家に Cisco DNA Center へのリモートアクセスを許可します。詳細については、リモートサポート許可ダッシュボードの表示 （26 ページ）を参照してください。 • [Help]：状況に応じたオンラインヘルプが、ブラウザの別のタブに表示されます。 • [Keyboard Shortcuts]：ショートカットグループのキーボードショートカット名、ショートカットキー、およびショートカットキーの組み合わせを表示します。 サポートされているショートカットグループは、[Global]、[Geo Maps]、[Topology] です。 • [Make a Wish]：コメントや提案事項が Cisco DNA Center 製品チームに送信されます。
	[Software Updates]：利用可能なソフトウェアアップデートのリストが表示されます。[Go to Software Updates] リンクをクリックすると、システムとアプリケーションのアップデートを表示できます。
	[Notifications]：イベント通知を表示し、通知設定を指定します。通知アイコンの横にある赤色の丸は、新しい通知があることを示しています。

インタラクティブヘルプ

[Interactive Help] には、Cisco DNA Center の特定のタスクに関するウォークスルーが含まれています。このウォークスルーでは、タスクを完了するために役立つ画面上のガイダンスが示されます。

[Interactive Help] ウィジェットは、デフォルトでは Cisco DNA Center ウィンドウの右下隅に表示されます。ウィジェットをクリックして **[Interactive Help]** のメニューを開きます。

図 *2:* インタラクティブ ヘルプ ウィジェット



インタラクティブ ヘルプ ウィジェットをデフォルトの場所から他の場所に移動することもできます。ウィジェットを、緑色の点線の長方形で示されている移動可能な場所にドラッグアンドドロップします。

リモートサポート許可ダッシュボードの表示

リモートサポートを許可することで、ネットワークのトラブルシューティングを行うために、シスコの専門家に Cisco DNA Center へのリモートアクセスを許可できます。

（注） Cisco DNA Center リモートサポートの許可は、LM コンソールバージョン 0.40.5 でのみサポートされます。

ステップ 1 Cisco DNA Center GUI で、右上隅にあるヘルプアイコンをクリックし、[Remote Support Authorization] を選択します。

[Remote Support Authorization] ダッシュボードの [SUMMARY] エリアには、リモートサポートの許可の合計、スケジュール済みリモートサポートの許可、および完了したリモートサポートの許可が表示されます。

ステップ 2 [Create New Authorization] タブをクリックして、新しい許可を作成します。詳細については、リモートサポート許可の作成 （807 ページ）を参照してください。

ステップ 3 [Current Authorization] タブをクリックして、現在のリモートサポートの許可タイルを表示します。

[Current Authorization] には、リモートサポートの許可ステータスが表示されます。

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

サポート許可タイルには、トラブルシューティングのためにシスコの専門家が Cisco DNA Center にアクセスするスケジュールと期間が表示されます。

ステップ 4 許可をキャンセルする場合は、それぞれのサポート許可タイルで [Cancel Authorization] リンクをクリックします。

ステップ 5 [View Logs] をクリックして、リモートサポートの許可ログを一覧表示する [Audit Logs] ウィンドウに移動します。

詳細については、Cisco DNA Center 管理者ガイドの「**View Audit Logs**」を参照してください。

ステップ 6 [Past Authorizations] タブをクリックして、過去の許可を表示します。

[Past Authorizations] テーブルには、[Cisco Specialist]、[Happened On]、[Session Status]、および [Log] に基づいてサポート許可が表示され、次の過去の許可ステータスが一覧表示されます。

- [All]：期限切れおよびキャンセルされたすべてのリモートサポート許可を一覧表示します。
- [Expired]：期限切れのすべてのリモートサポート許可を一覧表示します。
- [Canceled]：キャンセルされたすべてのリモートサポート許可を一覧表示します。

[Remote Support Authorization] ダッシュボードに、CX Cloud サービスの接続ステータスが表示されます。

- 右上隅にある緑色のチェックマークは、リモートサポートの許可が CX Cloud サービスに接続されていることを示します。

- 右上隅の感嘆符は、リモートサポートの許可が CX Cloud サービスに接続されていないことを示します。

グローバル検索の使用

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

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

- **ユーザー**：システム設定およびユーザーをユーザー名で検索します。大文字と小文字は区別されません。ユーザー名のサブストリング検索はサポートされていません。
- 新しいバージョンの Cisco DNA Center として別のアイテムがリリースされます。

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

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

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

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

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

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

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

- 2001:0db8:85a3:0000:0000:8a2e:0370:7334（完全な IPv6 アドレスを使用）
- 2001:db8:85a3:0:0:8a2e:0:7334（先行ゼロは切り捨て）
- 2001:db8:85a3::8a2e:0:7334（連続するゼロは二重コロンで圧縮）
- 2001:db8:85a3（IPv6 アドレスの一部を使用）

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

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

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

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

完了したら、 をクリックしてウィンドウを閉じます。

グローバル検索では、カテゴリごとに一度に 5 つの結果を表示できます。

ローカリゼーションの有効化

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

デフォルトの言語を変更するには、次のタスクを実行します。

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

- Google Chrome から、次の手順を実行します。

  1. 右上隅にある アイコンをクリックし、[Settings] を選択します。
  2. 下にスクロールして [Advanced] をクリックします。
  3. **[Languages]** > **[Language]** ドロップダウンリストから、[Add languages] を選択します。

     [Add languages] ポップアップウィンドウが表示されます。
  4. [Chinese]、[Japanese]、または [Korean] を選択して、[Add] をクリックします。

- Mozilla Firefox から、次の手順を実行します。

  1. 右上隅にある アイコンをクリックし、[Options] を選択します。
  2. **[Language and Appearance]** > **[Language]** エリアから、[Search for more languages] を選択します。

     [Firefox Language Settings] ポップアップウィンドウが表示されます。
  3. [Select a language to add] ドロップダウンリストから、[Chinese]、[Japanese]、または [Korean] を選択します。
  4. [OK] をクリックします。

ステップ 2 Cisco DNA Center にログインします。

GUI 画面は、選択した言語で表示されます。

図 *3* : ローカライズされたログイン画面の例

Cisco DNA Center インサイトへの登録

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

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

始める前に

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

ステップ 1 メニューアイコン（☰）をクリックし、表示されるユーザー名にカーソルを合わせて、**[My Profile and Settings]** > **[Communication Preferences]**の順に選択します。

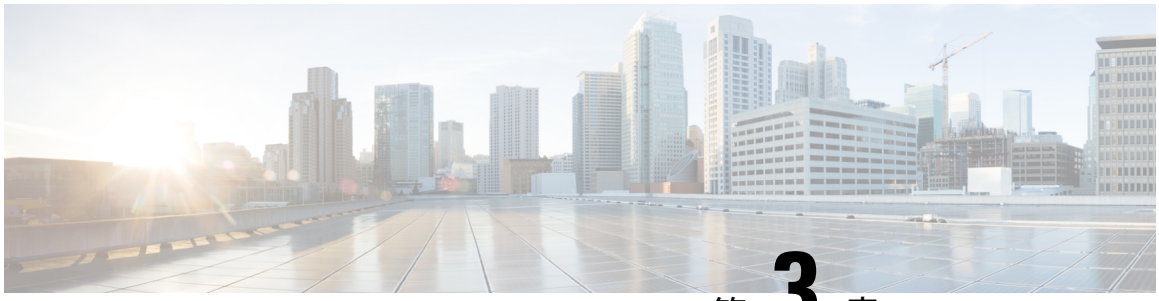
ステップ 2 [Subscription Off] ボタンを [Subscription On] に切り替えます。

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

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

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

ステップ 5 （オプション）Cisco DNA Center Insights の登録を解除するには、[Subscription On] ボタンを [Subscription Off] に切り替えます。



第 3 章

テレメトリの設定

アプリケーションテレメトリの概要

アプリケーションテレメトリを使用すると、デバイスの正常性をモニターおよび評価するためのグローバルネットワーク設定を構成できます。

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

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

始める前に

サイトを作成し、サイトにデバイスを割り当てます。『ネットワーク階層のサイトの作成（166 ページ）』を参照してください。

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

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

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

ステップ 3 [Syslogs] エリアで、次のいずれかを実行します。

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

ステップ 4 [NetFlow] エリアで、次のいずれかを実行します。

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

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

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

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

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

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

ステップ 7 [Save] をクリックします。

デバイスでのアプリケーションテレメトリ有効化の基準

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

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

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

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

プラットフォーム	従来のタギングベースのアルゴリズム	自動選択アルゴリズム

Router	• インターフェイスの説明に **lan** キーワードが含まれている。[12]
	• インターフェイスが物理インターフェイスである。
	• インターフェイスに管理 IP アドレス以外の IP アドレスがある。
		• インターフェイスに管理 IP アドレス以外の IP アドレスがある。
		• インターフェイスが次のいずれでもない。
		  • WAN
		  （注） インターフェイスにパブリック IP アドレスがあり、パブリック IP アドレスがインターフェイスを経由するルートルールがある場合、そのインターフェイスは WAN 側インターフェイスとして扱われます。
		  このコンテキストでは、パブリック IP アドレスはプライベート範囲にない（たとえば、192.168.x.x、172.16.y.y、10.z.z.z にない）か、システムの IP プールにない IP アドレスです。
		  ルートルールは動的に学習できます。このコンテキストでは、**show ip route** コマンドでこのインターフェイスを通過するパブリック IP アドレスへのルートは表示されません。
		  • ループバック
		  • 管理インターフェイス：IGABITETHERNET0、GIGABITETHERNET0/0、MGMT0、FASTETHERNET0、FASTETHERNET1

プラットフォーム	従来のタギングベースのアルゴリズム	自動選択アルゴリズム

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

Cisco AireOS コントローラ	• WLAN プロファイル名が **lan** キーワードでタグ付けされている。[1、2]	SSID が混在している場合、つまりローカルモード、フレックスモード、およびファブリックモードの場合、Wireless Service Assurance（WSA）の処理が有効になります。すべての SSID がローカルモードの場合、NetFlow が有効になります。
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ と最適化アプリケーション パフォーマンス モニタリング（APM）プロファイルおよび IOS リリース 16.12.1 以降	WLAN プロファイル名が **lan** キーワードでタグ付けされている。[1、2]	SSID が混在している場合、つまりローカルモード、フレックスモード、およびファブリックモードの場合は、Cisco Application Visibility and Control（AVC）の基本レコードが設定されます。すべての SSID がローカルモードの場合、最適化 APM レコードが設定されます。
	（注） テレメトリ設定を更新する場合は、テレメトリを無効にしてから、設定の変更後にテレメトリを有効にする必要があります。	
Cisco DNA トラフィック テレメトリ アプライアンス と最適化 APM プロファイルおよび IOS リリース 17.3 以降	• インターフェイスの説明に **lan** キーワードが含まれている。[1、2] • インターフェイスが物理インターフェイスである。	• インターフェイスが物理インターフェイスである。 • インターフェイスが管理インターフェイス（GIGABITETHERNET0、GIGABITETHERNET0/0、MGMT0、FASTETHERNET0、および FASTETHERNET1）ではない。

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

アプリケーションテレメトリ設定のプロビジョニング

テレメトリを使用した Syslog、SNMP トラップ、NetFlow コレクタサーバー、および有線クライアントデータ収集の設定 （33 ページ） の説明に従って、グローバルテレメトリ設定を構成します。

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

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

ステップ 2 プロビジョニングするデバイスを選択します。

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

（注） アプリケーションテレメトリのオプションは、Cisco DNA Center からのアプリケーションテレメトリの有効化がデバイスでサポートされている場合にのみ有効になります。

a) [Enable Application Telemetry]：選択したデバイスでアプリケーションテレメトリを設定します。

b) [Disable Application Telemetry]：選択したデバイスからアプリケーションテレメトリ設定を削除します。

ステップ 4 [Apply] をクリックします。

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

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

ワイヤレスコントローラのアプリケーションテレメトリを有効化する

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

始める前に

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

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

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

ステップ 3 [Inventory] ウィンドウで、デバイスを選択します。複数のデバイスを同時に選択できます。

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

ステップ 5 [Enable Telemetry] slide-in paneで、次の設定を完了します。

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

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

c) [Telemetry Source]：

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

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

ステップ 6 [Enable] をクリックします。

ステップ 7 [Application Telemetry] ウィンドウで、[OK] をクリックします。

今後この画面をスキップするには、[Don't show this to me again] チェックボックスをオンにします。

テレメトリステータスは、[Inventory] ウィンドウの [Application Telemetry] 列に表示されます。

新しいクラスタ仮想IPアドレスを使用するためのテレメトリ設定の更新

Cisco DNA Centerアプリケーションテレメトリを使用してデバイスデータをモニターし、Cisco DNA Center クラスタ仮想 IP アドレス（VIP）を変更する必要がある場合は、次の手順を実行して VIP を変更し、ノードテレメトリデータが新しい VIP に送信されることを確認します。

始める前に

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

- 割り当てるクラスタ VIP を特定します。クラスタ VIP は、『Cisco DNA Center Installation Guide』の「Required IP Addresses and Subnets」セクションで説明されている要件に準拠している必要があります。

ステップ 1 Cisco DNA Center GUI にアクセスし、次の手順に従ってすべてのサイトでアプリケーションテレメトリを無効にします。

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

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

b) 現在モニターしているすべてのサイトとデバイスを選択します。

c) [Actions] ドロップダウンリストから、[Telemetry] > [Disable Application Telemetry] の順に選択します。

d) サイトとデバイスでテレメトリが無効になったことが示されるまで待ちます。

ステップ 2 アプライアンス構成ウィザードを使用して、次のようにクラスタ VIP を変更します。

a) SSH クライアントを使用して、Cisco DNA Center プライマリノード上のエンタープライズ ネットワーク側の 10 GB インターフェイスに設定された VIP アドレスにログインします。ポート 2222 にログインしていることを確認します。

b) プロンプトが表示されたら、Linux のユーザー名とパスワードを入力します。

c) 次のコマンドを入力すると、プライマリノード上で構成ウィザードにアクセスできます。

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

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

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

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

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

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

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

ステップ 3 SSH プロンプトで次の一連のコマンドを入力して、必要な Cisco DNA Center サービスを再起動します。

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

ステップ 4 すべてのサービスが再起動するまで待ちます。次のコマンドを入力して、再起動の進行状況をモニターリングできます。必要に応じて、使用している Cisco DNA Center のバージョンが属するリリーストレインに適したサービス名に置き換えてください。

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

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

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

ステップ 5 Cisco DNA Center GUI にアクセスし、次の手順に従ってすべてのノードでアプリケーションテレメトリを有効にします。

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

b) モニターするすべてのサイトとデバイスを選択します。

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

d) サイトとデバイスでテレメトリが有効になったことが示されるまで待ちます。

テレメトリを使用したデバイス設定の更新

デバイスの可制御性が有効か無効かに関係なく、デバイスに設定の変更をプッシュできます。

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

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

ステップ 2 設定の変更を反映するデバイスを選択します。

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

[Update Telemetry Settings] slide-in paneが表示されます。

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

構成に変更がない場合は、既存の構成がデバイスに再度プッシュされます。

ステップ 5 [Next] をクリックします。

ステップ 6 テレメトリ設定を今すぐ更新する（[Now]）か後で更新する（[Later]）かを選択し、[Apply] をクリックします。

ステップ 7 CLI 構成をプレビューするには、[Generate Configuration Preview] オプションボタンをクリックして、次の手順を実行します。

1. [Task Name] フィールドに任意のタスク名を入力し、[Preview] をクリックします。

後で、作成した設定のプレビューを使用して、選択したデバイスに展開できます。

2. [Task Submitted] ダイアログボックスで、[View Work Items] リンクをクリックします。

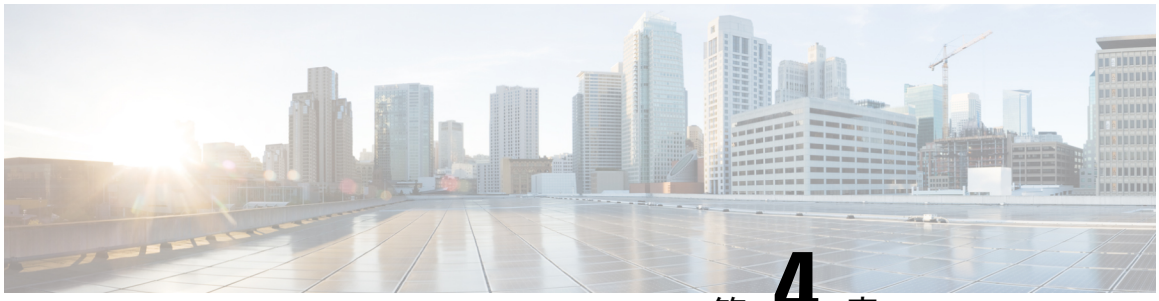
   （注） このダイアログボックスは表示されてから数秒で表示されなくなります。[Work Items] ウィンドウに移動するには、メニューアイコン（☰）をクリックして、**[Activities]** > **[Work Items]** を選択します。

3. [Work Items] ウィンドウで、設定プレビュー要求を送信した CLI プレビュータスクをクリックします。
4. CLI 設定の詳細を表示し、[Deploy] をクリックします。
5. デバイスを今すぐ展開する（[Now]）か、後でスケジュールする（[Later]）かを選択します。
6. 表示される確認ウィンドウで、[Yes] をクリックします。

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

第 II 部

ネットワークインベントリとトポロジの検出および管理



第 4 章

ネットワークの検出

検出の概要

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

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

デバイスは次の 3 つの方法で検出できます。

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

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

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

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

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

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

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

検出ダッシュボード

メニューアイコン（≡）をクリックして、**[Tools]** > **[Discovery]** の順に選択して、[Discovery Dashboard] を表示します。[Discovery Dashboard] には、インベントリの概要、最新のディスカバリ、ディスカバリタイプ、ディスカバリステータス、最近のディスカバリが表示されます。

ディスカバリの前提条件

ディスカバリを実行する前に、次の最小要件を満たしてください。

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

- Cisco DNA Center が使用できるように 1 つ以上の SNMP クレデンシャルがデバイス上で設定されていることを確認してください。少なくとも、これには SNMPv2C 読み取りクレデンシャルを使用できます。詳細については、ディスカバリ クレデンシャル （47 ページ）を参照してください。
- Cisco DNA Center に検出させ、管理委させるデバイスの SSH クレデンシャルを設定します。以下の基準のうち、少なくとも 1 つが満たされる場合、Cisco DNA Center はデバイスを検出し、そのインベントリに追加します。
  - デバイスへの SSH アクセスのために Cisco DNA Center が使用するアカウントが、特権 EXEC モード（レベル 15）である。
  - ディスカバリ ジョブで設定される CLI クレデンシャルの一部としてデバイスのイネーブルパスワードを設定している。詳細については、設定のガイドラインと制限事項のディスカバリ （50 ページ）を参照してください。

ディスカバリ クレデンシャル

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

- ネットワークデバイス：CLI と SNMP のクレデンシャル。

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

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

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

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

クレデンシャルと Cisco ISE のディスカバリ

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

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

Cisco ISE を AAA サーバーとして定義する方法については、Cisco ISE またはその他の AAA サーバーの追加 （228 ページ）を参照してください。

ディスカバリ クレデンシャルのガイドラインと制約事項

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

- ディスカバリ ジョブで使用されるデバイス クレデンシャルを変更するには、ディスカバリ ジョブを編集し、使用しなくなったクレデンシャルの選択を解除する必要があります。その後、新しいクレデンシャルを追加してディスカバリを開始する必要があります。詳細については、「ディスカバリ ジョブでクレデンシャルを変更 （75 ページ）」を参照してください。
- デバイスが正常に検出された後にデバイスのクレデンシャルを変更すると、そのデバイスのその後のポーリング サイクルは失敗します。この状況を修正するには、次のいずれかのオプションを使用します。
  - ディスカバリ ツールを使用します：
    - デバイスの新しいクレデンシャルと一致する、ジョブ固有のクレデンシャルを使用して、新しいディスカバリ ジョブを実行します。
    - 既存のディスカバリ ジョブを編集し、ディスカバリを再実行します。
  - 設計ツールを使用します：
    - 新しいグローバル クレデンシャルを作成し、適切なグローバル クレデンシャルを使用して新しいディスカバリ ジョブを実行します。

- 既存のグローバルログイン情報を編集し、[Copy & Edit] を使用してディスカバリジョブを再作成します。または、新しいディスカバリジョブを作成します。

- デバイス認証に失敗するために進行中のディスカバリ ポーリング サイクルが失敗する場合は、次のいずれかのオプションを使用して状況を修正できます。
  - ディスカバリ ツールを使用します：
    - 現在のディスカバリ ジョブを停止または削除し、デバイスのクレデンシャルと一致する、ジョブ固有のクレデンシャルを使用して、新しいディスカバリ ジョブを実行します。
    - 現在のディスカバリ ジョブを停止または削除し、既存のディスカバリ ジョブを編集して、ディスカバリを再実行します。
  - 設計ツールを使用します：
    - 新しいグローバル クレデンシャルを作成し、適切なグローバル クレデンシャルを使用して新しいディスカバリ ジョブを実行します。
    - 既存のグローバルログイン情報を編集し、[Copy & Edit] を使用してディスカバリジョブを再作成します。または、新しいディスカバリジョブを作成します。

- グローバル クレデンシャルを削除しても、以前に検出されたデバイスは影響を受けません。以前に検出されたデバイスのステータスは、認証の失敗を示しません。ただし、削除されたクレデンシャルの使用を試みる次回のディスカバリは失敗します。ディスカバリは、いずれかのデバイスへの接続を試みる前に失敗します。

ディスカバリ クレデンシャルの例

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

FIPS モードの展開の場合、ディスカバリパスワードの最小文字数は 8 です。

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

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

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

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

ステップ 4 該当するジョブ固有のクレデンシャル（クレデンシャル 1、クレデンシャル 2、クレデンシャル 3 など）を使用して、残りの 10 台のデバイスごとに 10 個の別個のディスカバリ ジョブを実行します。

ステップ 5 [Inventory] ウィンドウで結果を確認します。

優先管理 IP アドレス

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

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

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

デバイスが検出された後に、**[Inventory]** ウィンドウから管理 IP アドレスを更新できます。詳細については、デバイスの管理 IP アドレスの更新 （128 ページ）を参照してください。

設定のガイドラインと制限事項のディスカバリ

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

- CLI ユーザ名およびパスワードは特権 EXEC モード（レベル 15）で設定してください。これらのログイン情報は、ディスカバリ機能に関して Cisco DNA Center で設定する CLI ユーザー名およびパスワードと同じです。Cisco DNA Center にはデバイスへの最高レベルのアクセス権が必要です。
- 着信接続と発信接続の両方に関して、個々のインターフェイスで許可されるトランスポート プロトコルを明示的に指定してください。この設定には、**transport input** と **transport**

output コマンドを使用してください。これらのコマンドについては、各デバイス タイプ用のコマンド リファレンス ドキュメントを参照してください。

- デバイスのコンソールポートと VTY 回線のデフォルトのログイン方式を変更しないでください。デバイスがすでに AAA（TACACS）ログインで設定されている場合は、Cisco DNA Center で定義されている CLI ログイン情報が、TACACS サーバで定義されている TACACS ログイン情報と同じであることを確認してください。
- シスコ ワイヤレス コントローラは、サービスポート IP アドレスではなく、管理 IP アドレスを使用して検出する必要があります。それ以外の場合は、関連するワイヤレス コントローラ 360 および AP 360 のウィンドウでは、データが表示されません。

ディスカバリの実行

ここでは、ディスカバリの実行方法について説明します。

CDP を使用したネットワークの検出

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

（注）

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

始める前に

- ネットワークデバイスで CDP を有効にします。
- ディスカバリの前提条件 （46 ページ）で説明されているように、ネットワークデバイスを設定します。
- クライアント IP アドレスとしてネットワークデバイスのホスト IP アドレスを設定します。(A host is an end-user device, such as a laptop computer or mobile device.)

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

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

ステップ 3 [New Discovery] ウィンドウの [Discovery Name] フィールドに、名前を入力します。

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

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

  IP アドレスとサブネットをさらに除外するには、追加アイコン（⊕）をクリックします。
- [CDP Level]：スキャンするシードデバイスからのホップ数を入力します。

  有効値は 1 ～ 16 です。デフォルト値は 16 です。たとえば、CDP レベル 3 は、CDP がシード デバイスから最大 3 つのホップまでスキャンすることを意味します。
- [Preferred Management IP Address]：次のいずれかのオプションボタンをクリックします。
  - [None]：デバイスが任意の IP アドレスを使用できるようにします。
  - [Use Loopback IP]：デバイスのループバック インターフェイスの IP アドレスを指定します。

    （注） [Use Loopback IP] の使用を選択し、デバイスにループバック インターフェイスがない場合、Cisco DNA Centerは優先管理 IP アドレス （50 ページ）で説明されているロジックを使用して、管理 IP アドレスを選択します。

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

ステップ 5 [Credentials] エリアを展開し、使用するログイン情報を選択します。

すでに作成されているグローバル クレデンシャルのいずれかを選択するか、独自のディスカバリ クレデンシャルを設定します。

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

ステップ 7 新しいログイン情報を設定するには、[Add Credentials] をクリックします。

（注） 自身のログイン情報を設定する場合は、[Save as global settings] チェックボックスをオンにして、将来の検出ジョブのためにそれらを保存できます。

ステップ 8 CLI クレデンシャルの場合は、次の手順を実行します。

a) 次のフィールドを設定します。

表 *3 : CLI* クレデンシャル

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

b) これらのログイン情報を後で使用するために保存する場合は、[Save as global settings] チェックボックスをオンにします。このチェックボックスをオンにしない場合、ログイン情報は現在の検出ジョブにのみ使用できます。

c) [Save] をクリックします。

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

a) 次のフィールドを設定します。

表 *4 : SNMPv2c* のクレデンシャル

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

b) これらのログイン情報を後で使用するために保存する場合は、[Save as global settings] チェックボックスをオンにします。このチェックボックスをオンにしない場合、ログイン情報は現在の検出ジョブにのみ使用できます。

c) [Save] をクリックします。

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

a) 次のフィールドを設定します。

表 *5 : SNMPv3* のクレデンシャル

フィールド	説明
Name/Description	追加した SNMPv3 設定の名前または説明。
Username	SNMPv3 設定に関連付けられている名前。
Mode	SNMP メッセージを必要とするセキュリティ レベル。次のいずれかのモードを選択します。 • [noAuthNoPriv]：認証または暗号化を提供しません。 • [AuthNoPriv]：認証を提供しますが、暗号化は提供しません。 • [AuthPriv]：認証と暗号化の両方を提供します。

フィールド	説明
Auth Type	使用する認証タイプ（[Mode] として [AuthPriv] または [AuthNoPriv] を選択した場合に有効になります）。次のいずれかの認証タイプを選択します。 • [SHA]：HMAC-SHA に基づく認証。 • [MD5]：HMAC-MD5 に基づく認証。
Auth Password	SNMPv3 を使用するデバイスから情報にアクセスする際に使用する SNMPv3 パスワード。これらのパスワード（またはパスフレーズ）は、8 文字以上にする必要があります。 （注） • 一部のシスコ ワイヤレス コントローラでは、パスワード（あるいはパスフレーズ）は少なくとも 12 文字以上である必要があります。ワイヤレスコントローラのパスワードの最小要件を必ず確認してください。パスワードに必要な最低限の文字数が守られないと、デバイスではCisco DNA Centerによる検出、監視、管理が行われなくなります。 • パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。
Privacy Type	プライバシー タイプ。（[Mode] として [AuthPriv] を選択した場合に有効になります）。次のいずれかのプライバシー タイプを選択します。 • [AES128]：暗号化の 128 ビット CBC モード AES。 • **CISCOAES192**：シスコのデバイス上での暗号化の 192 ビット CBC モード AES。 • **CISCOAES256**：シスコのデバイス上での暗号化の 256 ビット CBC モード AES。 （注） • 検出機能とインベントリ機能の使用は、プライバシータイプ CISCOAES192 および CISCOAES256 のみでサポートされています。アシュアランス 機能はサポートされていません。 • プライバシータイプ AES128 は、検出、インベントリ、およびアシュアランスでサポートされています。

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

b) これらのログイン情報を後で使用するために保存する場合は、[Save as global settings] チェックボックスをオンにします。このチェックボックスをオンにしない場合、ログイン情報は現在の検出ジョブにのみ使用できます。

c) [Save] をクリックします。

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

a) 次のフィールドを設定します。

表 *6 : SNMP* のプロパティ

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

b) これらのログイン情報を後で使用するために保存する場合は、[Save as global settings] チェックボックスをオンにします。このチェックボックスをオンにしない場合、ログイン情報は現在の検出ジョブにのみ使用できます。

c) [Save] をクリックします。

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

a) 次のフィールドを設定します。

表 *7: HTTPS* クレデンシャル

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

b) （任意） これらのログイン情報を後で使用するために保存する場合は、[Save as global settings] チェックボックスをオンにします。このチェックボックスをオンにしない場合、ログイン情報は現在の検出ジョブにのみ使用できます。

c) [Save] をクリックします。

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

a) [Port] フィールドに、ポート番号を入力します。次のいずれかのポートを使用できます。

- ポート 830（デフォルト）
- デバイスで使用可能なその他のポート
- Cisco DNA Center で設定されたカスタムポート（デバイスの可制御性が有効な場合のみカスタムポートを使用できます。詳細については、*Cisco DNA Center* 管理者ガイド の「Device Controllability」の項を参照してください

）。

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

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

b) これらのログイン情報を後で使用するために保存する場合は、[Save as global settings] チェックボックスをオンにします。このチェックボックスをオンにしない場合、ログイン情報は現在の検出ジョブにのみ使用できます。

c) [Save] をクリックします。

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

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

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

b) 使用する順序でプロトコルをドラッグ アンド ドロップします。

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

ステップ 15 [Discover] をクリックします。

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

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

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

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

- [Daily]：[Run at Interval（Days）] フィールドに間隔を日単位で入力します。
- [Weekly]:[Run at Interval（Weeks）] フィールドに間隔を週単位で入力します。

5. 繰り返しに [Daily] または [Weekly] を選択した場合は、[Set Schedule End] チェックボックスをオンにして終了日時を定義します。

（注） 繰り返しでは、新しいデバイスのみを検出できます。上部に表示される [Discover only new devices] トグルボタンは、デフォルトで有効になっています。

6. [End Date] または [End After] をクリックします。
   - [End Date]：繰り返しを終了する月、日付、年を入力します。
   - [End After]：繰り返しを終了するまでの回数を入力します。
7. [Start] をクリックします。

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

[Discoveries] ウィンドウにスキャンの結果が表示されます。

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

IP アドレス範囲を使用したネットワークの検出

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

始める前に

ディスカバリの前提条件 （46 ページ） で説明されているように、デバイスには必須のデバイス設定が存在する必要があります。

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

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

ステップ 3 [New Discovery] ウィンドウの [Discovery Name] フィールドに、名前を入力します。

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

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

IP アドレス範囲を追加するには、追加アイコン（[+]）をクリックします。

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

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

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

- [Preferred Management IP Address]：次のいずれかのオプションボタンをクリックします。
  - [None]：デバイスが任意の IP アドレスを使用できるようにします。
  - [Use Loopback IP]：デバイスのループバック インターフェイスの IP アドレスを指定します。

    （注） [Use Loopback IP] の使用を選択し、デバイスにループバック インターフェイスがない場合、Cisco DNA Centerは優先管理 IP アドレス （50 ページ）で説明されているロジックを使用して、管理 IP アドレスを選択します。

ステップ 5 [Credentials] エリアを展開し、使用するログイン情報を選択します。

すでに作成されているグローバル クレデンシャルのいずれかを選択するか、独自のディスカバリ クレデンシャルを設定します。

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

ステップ 7 新しいログイン情報を設定するには、[Add Credentials] をクリックします。

（注） 自身のログイン情報を設定する場合は、[Save as global settings] チェックボックスをオンにして、将来の検出ジョブのためにそれらを保存できます。

ステップ 8 CLI クレデンシャルの場合は、次の手順を実行します。

a) 次のフィールドを設定します。

表 *8 : CLI* クレデンシャル

フィールド	説明
Name/Description	CLIクレデンシャルを説明する名前または語句。
Username	ネットワーク内のデバイスのCLIにログインするために使用する名前。

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

b) これらのログイン情報を後で使用するために保存する場合は、[Save as global settings] チェックボックスをオンにします。このチェックボックスをオンにしない場合、ログイン情報は現在の検出ジョブにのみ使用できます。

c) [Save] をクリックします。

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

a) 次のフィールドを設定します。

表 9 : SNMPv2c のクレデンシャル

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

b) これらのログイン情報を後で使用するために保存する場合は、[Save as global settings] チェックボックスをオンにします。このチェックボックスをオンにしない場合、ログイン情報は現在の検出ジョブにのみ使用できます。

c) [Save] をクリックします。

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

a) 次のフィールドを設定します。

表 *10 : SNMPv3* のクレデンシャル

フィールド	説明
Name/Description	追加した SNMPv3 設定の名前または説明。
Username	SNMPv3 設定に関連付けられている名前。
Mode	SNMP メッセージを必要とするセキュリティ レベル。次のいずれかのモードを選択します。 • [noAuthNoPriv]：認証または暗号化を提供しません。 • [AuthNoPriv]：認証を提供しますが、暗号化は提供しません。 • [AuthPriv]：認証と暗号化の両方を提供します。
Auth Type	使用する認証タイプ（[Mode] として [AuthPriv] または [AuthNoPriv] を選択した場合に有効になります）。次のいずれかの認証タイプを選択します。 • [SHA]：HMAC-SHA に基づく認証。 • [MD5]：HMAC-MD5 に基づく認証。
Auth Password	SNMPv3 を使用するデバイスから情報にアクセスする際に使用する SNMPv3 パスワード。これらのパスワード（またはパスフレーズ）は、8 文字以上にする必要があります。 （注） • 一部のシスコ ワイヤレス コントローラでは、パスワード（あるいはパスフレーズ）は少なくとも 12 文字以上である必要があります。ワイヤレスコントローラのパスワードの最小要件を必ず確認してください。パスワードに必要な最低限の文字数が守られないと、デバイスではCisco DNA Centerによる検出、監視、管理が行われなくなります。 • パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。

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

b) これらのログイン情報を後で使用するために保存する場合は、[Save as global settings] チェックボックスをオンにします。このチェックボックスをオンにしない場合、ログイン情報は現在の検出ジョブにのみ使用できます。

c) [Save] をクリックします。

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

a) 次のフィールドを設定します。

表 *11 : SNMP* のプロパティ

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

b) これらのログイン情報を後で使用するために保存する場合は、[Save as global settings] チェックボックスをオンにします。このチェックボックスをオンにしない場合、ログイン情報は現在の検出ジョブにのみ使用できます。

c) [Save] をクリックします。

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

a) 次のフィールドを設定します。

表 *12 : HTTPS* クレデンシャル

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

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

b) （任意）これらのログイン情報を後で使用するために保存する場合は、[Save as global settings] チェックボックスをオンにします。このチェックボックスをオンにしない場合、ログイン情報は現在の検出ジョブにのみ使用できます。

c) [Save] をクリックします。

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

a) [Port] フィールドに、ポート番号を入力します。次のいずれかのポートを使用できます。

- ポート 830（デフォルト）
- デバイスで使用可能なその他のポート
- Cisco DNA Center で設定されたカスタムポート（デバイスの可制御性が有効な場合のみカスタムポートを使用できます。詳細については、*Cisco DNA Center* 管理者ガイド の「Device Controllability」の項を参照してください

  ）。

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

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

b) これらのログイン情報を後で使用するために保存する場合は、[Save as global settings] チェックボックスをオンにします。このチェックボックスをオンにしない場合、ログイン情報は現在の検出ジョブにのみ使用できます。

c) [Save] をクリックします。

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

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

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

b) 使用する順序でプロトコルをドラッグ アンド ドロップします。

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

ステップ 15 [Discover] をクリックします。

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

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

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

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

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

7. [Start] をクリックします。

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

[Discoveries] ウィンドウにスキャンの結果が表示されます。

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

LLDP を使用したネットワークの検出

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

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

始める前に

- ネットワークデバイスで LLDP を有効にします。
- ディスカバリの前提条件 （46 ページ）で説明されているように、ネットワークデバイスを設定します。
- クライアント IP アドレスとしてネットワークデバイスのホストの IP アドレスを設定します。(A host is an end-user device, such as a laptop computer or mobile device.)

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

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

ステップ 3 [New Discovery] ウィンドウの [Discovery Name] フィールドに、名前を入力します。

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

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

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

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

- [LLDP Level]：スキャンするシードデバイスからのホップ数を入力します。

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

- [Preferred Management IP Address]：次のいずれかのオプションボタンをクリックします。
  - [None]：デバイスが任意の IP アドレスを使用できるようにします。
  - [Use Loopback IP]：デバイスのループバック インターフェイスの IP アドレスを指定します。

    （注） [Use Loopback IP] の使用を選択し、デバイスにループバック インターフェイスがない場合、Cisco DNA Centerは優先管理 IP アドレス （50 ページ）で説明されているロジックを使用して、管理 IP アドレスを選択します。

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

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

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

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

表 *13 : CLI* クレデンシャル

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

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

d) [SNMP v2c] をクリックして、次のフィールドを設定します。

表 *14 : SNMPv2c* のクレデンシャル

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

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

表 *15 : SNMPv3* のクレデンシャル

フィールド	説明
Name/Description	追加した SNMPv3 設定の名前または説明。
Username	SNMPv3 設定に関連付けられている名前。
Mode	SNMP メッセージを必要とするセキュリティ レベル。次のいずれかのモードを選択します。 • [noAuthNoPriv]：認証または暗号化を提供しません。 • [AuthNoPriv]：認証を提供しますが、暗号化は提供しません。 • [AuthPriv]：認証と暗号化の両方を提供します。

フィールド	説明
Auth Type	使用する認証タイプ（[Mode] として [AuthPriv] または [AuthNoPriv] を選択した場合に有効になります）。次のいずれかの認証タイプを選択します。 • [SHA]：HMAC-SHA に基づく認証。 • [MD5]：HMAC-MD5 に基づく認証。
Auth Password	SNMPv3 を使用するデバイスから情報にアクセスする際に使用する SNMPv3 パスワード。これらのパスワード（またはパスフレーズ）は、8 文字以上にする必要があります。 （注） • 一部のシスコ ワイヤレス コントローラでは、パスワード（あるいはパスフレーズ）は少なくとも 12 文字以上である必要があります。ワイヤレス コントローラのパスワードの最小要件を必ず確認してください。パスワードに必要な最低限の文字数が守られないと、デバイスではCisco DNA Centerによる検出、監視、管理が行われなくなります。 • パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。
Privacy Type	プライバシー タイプ。（[Mode] として [AuthPriv] を選択した場合に有効になります）。次のいずれかのプライバシー タイプを選択します。 • [AES128]：暗号化の 128 ビット CBC モード AES。 • **CISCOAES192**：シスコのデバイス上での暗号化の 192 ビット CBC モード AES。 • **CISCOAES256**：シスコのデバイス上での暗号化の 256 ビット CBC モード AES。 （注） • 検出機能とインベントリ機能の使用は、プライバシータイプ CISCOAES192 および CISCOAES256 のみでサポートされています。アシュアランス 機能はサポートされていません。 • プライバシー タイプ AES128 は、検出、インベントリ、およびアシュアランスでサポートされています。

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

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

表 *16 : SNMP* のプロパティ

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

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

表 *17 : HTTPS* クレデンシャル

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

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

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

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

a) 使用するプロトコルの名前をクリックします。緑のチェックマークはプロトコルが選択されていることを示します。有効なプロトコルは、[SSH]（デフォルト）および [Telnet] です。

b) 使用する順序でプロトコルをドラッグ アンド ドロップします。

ステップ 7 [Discover] をクリックします。

[Discover Devices] スライドインペインが表示されます。

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

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

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

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

- [Daily]：[Run at Interval（Days）] フィールドに間隔を日単位で入力します。
- [Weekly]:[Run at Interval（Weeks）] フィールドに間隔を週単位で入力します。

5. 繰り返しに [Daily] または [Weekly] を選択した場合は、[Set Schedule End] チェックボックスをオンにして終了日時を定義します。

   （注） 繰り返しでは、新しいデバイスのみを検出できます。上部に表示される [Discover only new devices] トグルボタンは、デフォルトで有効になっています。

6. [End Date] または [End After] をクリックします。
   - [End Date]：繰り返しを終了する月、日付、年を入力します。
   - [End After]：繰り返しを終了するまでの回数を入力します。

7. [Start] をクリックします。

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

[Discoveries] ウィンドウにスキャンの結果が表示されます。

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

ディスカバリ ジョブの管理

ここでは、ディスカバリジョブの管理方法について説明します。

ディスカバリ ジョブの停止および開始

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

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

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

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

b) 下部ペインの右側で、[Stop] をクリックします。

ステップ 4 非アクティブなディスカバリ ジョブを再起動するには、次の手順を実行します。

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

b) 下部ペインの右側で、[Re-discover] をクリックします。

ディスカバリ ジョブの編集

既存のディスカバリジョブを編集して、ジョブを再実行できます。

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

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

ステップ 3 **[Discovery]** ペインで、検出ジョブを選択します。

ステップ 4 [Edit] をクリックします。

ステップ 5 次のフィールドを除き、ディスカバリのタイプに応じてジョブのタイプを変更できます。

- [CDP]：ディスカバリ名、ディスカバリタイプ、IP アドレス。変更可能なフィールドの詳細については、CDP を使用したネットワークの検出 （51 ページ）を参照してください。
- [IP Range]：ディスカバリ名、タイプ、IP アドレス範囲（ただし別の IP アドレス範囲を追加できます）。変更可能なフィールドの詳細については、IP アドレス範囲を使用したネットワークの検出（59 ページ）を参照してください。
- LLDP：ディスカバリ名、タイプ、IP アドレス。変更可能なフィールドの詳細については、LLDP を使用したネットワークの検出 （67 ページ）を参照してください。

ステップ 6 [Start] をクリックします。

ディスカバリ ジョブでクレデンシャルを変更

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

始める前に

少なくとも 1 つのディスカバリ ジョブが必要です。

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

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

ステップ 3 **[Discovery]** ペインで、検出ジョブを選択します。

ステップ 4 [Edit] をクリックします。

ステップ 5 [クレデンシャル（Credentials）] エリアを展開します。

ステップ 6 使わないクレデンシャルを非選択状態にします。

ステップ 7 使用するクレデンシャルを設定します。

a) [クレデンシャルの追加（Add Credentials）] をクリックします。

b) CLI クレデンシャルを設定するには、次のフィールドを設定します。

表 *18 : CLI* クレデンシャル

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

c) [SNMP v2c] をクリックして、次のフィールドを設定します。

表 *19 : SNMPv2c* のクレデンシャル

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

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

表 *20 : SNMPv3* のクレデンシャル

フィールド	説明
Name/Description	追加した SNMPv3 設定の名前または説明。
Username	SNMPv3 設定に関連付けられている名前。
Mode	SNMP メッセージを必要とするセキュリティ レベル。次のいずれかのモードを選択します。 • [noAuthNoPriv]：認証または暗号化を提供しません。 • [AuthNoPriv]：認証を提供しますが、暗号化は提供しません。 • [AuthPriv]：認証と暗号化の両方を提供します。
Auth Type	使用する認証タイプ（[Mode] として [AuthPriv] または [AuthNoPriv] を選択した場合に有効になります）。次のいずれかの認証タイプを選択します。 • [SHA]：HMAC-SHA に基づく認証。 • [MD5]：HMAC-MD5 に基づく認証。
Auth Password	SNMPv3 を使用するデバイスから情報にアクセスする際に使用する SNMPv3 パスワード。これらのパスワード（またはパスフレーズ）は、8 文字以上にする必要があります。 （注） • 一部のシスコ ワイヤレス コントローラでは、パスワード（あるいはパスフレーズ）は少なくとも 12 文字以上である必要があります。ワイヤレス コントローラのパスワードの最小要件を必ず確認してください。パスワードに必要な最低限の文字数が守られないと、デバイスではCisco DNA Centerによる検出、監視、管理が行われなくなります。 • パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。

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

ステップ 8 [Start] をクリックします。

ディスカバリ ジョブの複製

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

始める前に

少なくとも 1 つのディスカバリ ジョブを実行する必要があります。

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

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

ステップ 3 左側の [Discoveries] ペインで、ディスカバリジョブをクリックします。

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

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

ステップ 5 （任意） ディスカバリジョブの名前を変更するには、[Discovery Name] フィールドのデフォルト名を新しい名前に置き換えます。

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

ディスカバリ ジョブの削除

アクティブまたは非アクティブに関係なく、検出ジョブを削除できます。

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

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

ステップ 3 左側の [Discoveries] ペインで、削除するディスカバリジョブをクリックします。

ステップ 4 下部ペインの右側で、[Delete] をクリックします。

ステップ 5 [OK] をクリックして確定します。

ディスカバリ ジョブ情報の表示

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

始める前に

少なくとも 1 つのディスカバリジョブを実行します。

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

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

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

ステップ 4 詳細については、次の領域のひとつの隣にある下矢印をクリックします。

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

- [Credentials]：使用されたログイン情報の名前が提供されます。
- [History]：開始された時間およびデバイスが検出されたかどうかを含め、実行された各ディスカバリジョブがリストされます。

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

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

すべてのディスカバリの表示

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

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

[Discovery] テーブルには、すべての検出ジョブの [Type]、[Status]、[IP Address List]、および [Reachable Devices] の詳細が表示されます。

ステップ 3 [Discovery] テーブルで、検索またはフィルタアイコンを使用して検出ジョブを検索します。

または、左側のペインでフィルタの [Type] を選択して、検出ジョブをフィルタ処理します。

ステップ 4 [Discovery Name] 列で検出ジョブの名前をクリックして、[Discovery Details] ページを起動します。

[Discovery Details] ページには、検出ジョブのタイプ（[Type]）、再試行回数（[Retry Count]）、プロトコルの順序（[Protocol Order]）、および合計時間（[Total Time]）の詳細が表示されます。

検出ジョブが完了すると、検出されたデバイスの数と検出されたデバイスに関する詳細が [Discovery Details] ページに表示されます。[Devices] テーブルには、検出されたデバイスの IP アドレス、デバイス名、到達可能ステータス、ICMP、SNMP、CLI、HTTP、および NETCONF の詳細が表示されます。同じ検出ジョブを使用してデバイスを再度検出する場合は、[Re-discover] をクリックします。

ステップ 5 [Discovery Details] ページで、[View all details] をクリックして、検出ジョブに関するすべての詳細を表示します。

[Discovery Details] スライドインペインには、タイプ、CDP レベル、再試行回数、タイムアウト、範囲、サブネットフィルタ、プロトコルの順序、優先管理 IP、CLI 資格情報、SNMPv2 読み取り、SNMPv2 書き込み、HTTPS 読み取り、HTTPS 書き込み、および NETCONF の詳細が表示されます。

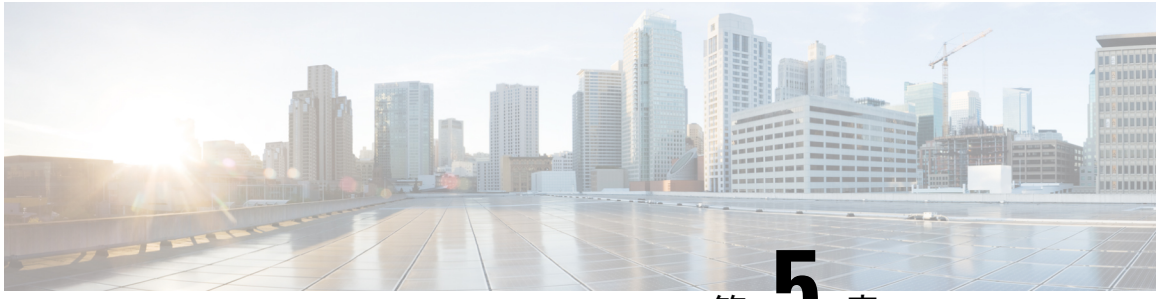
ステップ 6 デバイスを再検出するには、検出ジョブに対応する [Actions] 列の省略記号（ ••• ）アイコンの上にカーソルを置き、[Re-discover] をクリックします。

[Re-discover] スライドインペインでは、次のいずれかの操作を実行できます。

- デバイスをすぐに検出するには、[Now] オプションボタンをクリックし、[Task Name] フィールドに検出ジョブの名前を入力して、[Start] をクリックします。

- 後でデバイスを検出するには、[Later] オプションボタンをクリックし、[Task Name] フィールドに検出ジョブの名前を入力し、[Start Date/time] を定義し、ドロップダウンリストからタイムゾーンを選択して、[Start] をクリックします。

ステップ 7 検出ジョブを削除するには、検出ジョブに対応する [Actions] 列の省略記号（ ••• ）アイコンの上にカーソルを置き、[Delete] をクリックし、確認メッセージで [Delete] を再度クリックします。



第 5 章

インベントリの管理

インベントリについて

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

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

インベントリは、必要に応じて次のプロトコルを使用します。

- リンク層検出プロトコル（LLDP）
- IP デバイス トラッキング（IPDT）またはスイッチ統合セキュリティ機能（SISF）（IPDT または SISF をデバイス上で有効にする必要があります）。
- LLDP Media Endpoint Discovery（このプロトコルは IP フォンや一部のサーバーの検出に使用されます）。
- ネットワーク設定プロトコル（NETCONF）デバイスのリストについては、ディスカバリの前提条件 （46 ページ） を参照してください。

初期検出後、Cisco DNA Center は定期的にデバイスをポーリングすることでインベントリを維持します。デフォルトの間隔は 24 時間ごとです。ただし、この間隔は、ネットワーク環境の必要性に応じて変更できます。詳細については、デバイスポーリング間隔の更新（128ページ）を参照してください。また、デバイスの設定変更によって SNMP トラップがトリガーされ、次にデバイスの再同期がトリガーされます。ポーリングはデバイス、リンク、ホスト、およびインターフェイスごとに実行されます。アクティブ状態が 1 日未満のデバイスのみが表示されます。これによって、古いデバイス データが表示されないようにします。500 個のデバイスのポーリングに約 20 分かかります。

インベントリと Cisco ISE の認証

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

- ネットワークでデバイス認証に Cisco ISE を使用する場合、Cisco DNA Center で Cisco ISE を設定する必要があります。これにより、Cisco DNA Center でデバイスをプロビジョニングする際に、ユーザーが定義した Cisco ISE サーバー情報を使用してデバイスが設定されます。また、Cisco DNA Center は Cisco ISE サーバーでデバイスを設定し、後に続くデバイスの更新プログラムについても伝えます。Cisco DNA Center での Cisco ISE の設定については、グローバル ネットワーク サーバーの設定 （230 ページ）を参照してください。

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

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

Cisco DNA Center が Cisco ISE サーバーでデバイスを設定および更新する場合、トランザクションは Cisco DNA Center の監査ログでキャプチャされます。Cisco DNA Center や Cisco ISE インベントリに関する問題のトラブルシューティングに監査ログを役立てることができます。

デバイスのプロビジョニング後、Cisco DNA Center は Cisco ISE でデバイスを認証します。Cisco ISE に到達できない（RADIUS 応答がない）場合、デバイスはローカルのログイン クレデンシャルを使用します。Cisco ISE に到達できるが Cisco ISE にデバイスが存在しない場合や、そのクレデンシャルが Cisco DNA Center で設定されたクレデンシャルと一致しない場合、デバイスはローカルのログイン クレデンシャルを使用するためにフォールバックしません。代わりに、部分的な収集状態になります。

この状態を回避するには、Cisco DNA Center を使用してデバイスをプロビジョニングする前に、必ず Cisco DNA Center で使用しているのと同じデバイス クレデンシャルで Cisco ISE のデバイスを設定します。また、有効なディスカバリ クレデンシャルを設定したことも確認してください。詳細については、ディスカバリ クレデンシャル （47 ページ）を参照してください。

- 必要に応じて、Cisco ISE を使用してデバイス グループにアクセス制御を実行できます。

インベントリに関する情報の表示

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

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

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

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

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

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

始める前に

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

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

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

表 *21* : インベントリ

カラム	説明
Device Name	

カラム	説明
	デバイスの名前。 デバイス名をクリックすると、デバイスの次の詳細が表示されます。 [Details]：デバイス名、到達可能性ステータス、管理性ステータス、IPアドレス、デバイスモデル、ロール、稼働時間、サイトなどの詳細が表示されます。 • [View Assurance 360]：[Assurance 360] ウィンドウが表示されます。ウィンドウを開くには、アシュアランス アプリケーションをインストールしておく必要があります。 • **インターフェイス** • [Ethernet Ports]（すべてのデバイスが対象）：イーサネットポートの動作ステータスと管理ステータスが表示されます。 トグルボタン（  ）を使用して、[Ports] ビューと [Ports] テーブルを切り替えます。[Ports] ビューでポートをクリックするか、[Ports] テーブルでポート名をクリックして、ポートの詳細を表示します。 Cisco Catalyst 4000 シリーズ、6000 シリーズ、および 9000 シリーズ スイッチと Cisco ASR 1000 シリーズアグリゲーション サービス ルータの場合、[Ports] ビューにはラインカードとスーパーバイザカードの詳細が表示されます（使用可能な場合）。 ラインカードの詳細には、プラットフォーム、アドレス、シリアル番号、ロール、およびスタックメンバー番号に関する情報が含まれます。スーパーバイザカードの詳細には、部品番号、シリアル番号、スイッチ番号、およびスロット番号に関する情報が含まれます。 [Ports] テーブルには、動作ステータス、管理ステータス、タイプ、ネイティブ VLAN、音声 VLAN、MAC アドレス、PoE ステータス、速度、MTU およびポートの説明が表示されます。 Cisco Catalyst 2000、3000、および 9000 シリーズ スイッチの場合は、[Ports] ビューでポートをクリックするか、[Ports] テーブルのポート名をクリックして、ポートの最大割り当て電力、および消費電力の詳細を表示します。 • [Neighbor Details]： [Ports] ビューでポートをクリックするか、[Ports] テーブルでポート名をクリックして、ポートの詳細を表示します。[Port Details] ウィンドウには、ポートに接続されているデバイスの詳細が表示されます。[Neighbor Details] エリアには、デバイス名、デバイスが接続されているポートの名前、およびデバイスの機能が表示されます。 ポートには、CDP ネイバーの詳細が表示されます。CDP が存在しない場合、LLDP ネイバーの詳細が表示されます。CDP と LLDP ネイバーの両方が存在しない場合、[Port Details] ウィンドウに [Neighbor Details] が表示されません。 • [Color Code]：このドロップダウンリストには、次のビューが用意されています。

カラム	説明
	• [Status]：イーサネットポートのデフォルトビューを表示します。 • [VLANs]：特定のポートに割り当てられているVLANを表示します。[VLANs] ビューでは、最大 5 つの VLAN を選択し、ポートに関連付けられている VLAN のみを一覧表示できます。 [VLANs] ビューには、VLAN ポートマッピングの [Selected]、[Not Configured]、[Default]、および [VLAN] カラーコードが表示されます。 • [Port Channels]：デバイスで設定されている上位 5 つのポートチャネルを表示します。 [Port Channels] ビューには、デバイスで設定されているポートチャネルの [Selected] および [Port-channel] カラーコードが表示されます。 • [Port Actions]： • [Clear Mac Address]：ポートの MAC アドレスをクリアできます。[Ports] ビューでポートをクリックし、[Port Actions] ドロップダウンリストから [Clear Mac Address] を選択します。 • [Port Shut]：ポートをシャットダウンできます。[Ports] ビューでポートをクリックし、[Port Actions] ドロップダウンリストから [Port Shut] を選択します。[Okay] をクリックして確定します。ポートの管理ステータスが [Down] に変わります。 ポートの管理ステータスを [Up] に変更するには、[Port Actions] ドロップダウンリストから [Port No Shut] を選択し、[Okay] をクリックします。 error-disabled ポートは黄色で表示されます。[Ports] ビューで error-disabled ポートをクリックして、エラーの理由を表示します。error-disabled ポートをアクティブにするには、MAC アドレスをクリアして、ポートをシャットダウンします。 • [Port Description]：[PORT DESCRIPTION] の横にある [Edit] アイコンをクリックし、説明を入力して [Save] をクリックし、[Okay] をクリックしてポートに説明を追加します。説明を削除するには、[Delete] アイコンをクリックします。

カラム	説明
	• [Update Native VLAN]：[Native VLAN] の横にある [Edit] アイコンをクリックし、[Edit Native VLAN] ドロップダウンリストから VLAN を選択し、[Save] をクリックして VLAN を更新します。2 つの VLAN が事前設定されているポートの VLAN を更新することはできません。 • VLAN の更新、ポートの説明の追加、MAC アドレスのクリア、およびポートのシャットダウンを行うには、デバイスソフトウェアタイプが Cisco IOS または Cisco IOS-XE である必要があります。 • ワイヤレスコントローラ では、VLAN の更新、MAC アドレスのクリア、およびポートのシャットダウンはサポートされていません。 • VLAN の更新、MAC アドレスのクリア、およびポートのシャットダウンは、アクセスポートでのみサポートされます。 • ポートをシャットダウンすると、ポートのトラフィックが中断されます。 • [Update Voice VLAN]：[Voice VLAN] の横にある [Edit] アイコンをクリックし、[Edit Voice VLAN] ドロップダウンリストから VLAN を選択し、[Save] をクリックして VLAN を更新します。 • [Native VLAN]（スイッチとハブのみが対象）：動作ステータス、管理ステータス、VLAN タイプ、および IP アドレスが表示されます。このテーブルには、次のタイプの VLAN の ID も表示されます。 • 製造時提供のデフォルト VLAN の VLAN ID • 設定されたデフォルト VLAN の VLAN ID • 設定された VLAN の VLAN ID [Search] または [Filter] をクリックして、VLAN の詳細を表示できます。 • [Virtual Ports]（ワイヤレスデバイス、コントローラ、ルータのみが対象）：動作ステータス、管理ステータス、タイプ、MAC アドレス、PoE ステータス、速度、および MTU が表示されます。[Search] または [Filter] をクリックして、ポートの詳細を表示できます。 • [Hardware and Software]：デバイスのハードウェアとソフトウェアの詳細が表示されます。 • [Configuration]：**show running-config** コマンドの出力で表示される内容に似た詳細な構成情報が表示されます。 この機能は、AP とワイヤレスコントローラにはサポートされていません。したがって、これらのデバイス タイプの場合は設定データは返されません。

カラム	説明
	• [Power]：デバイスに割り当てられている電力、消費電力、および残りの電力に関する詳細が表示されます。[Power Supplies] テーブルに、動作ステータス、シリアル番号、およびベンダー機器タイプの詳細が表示されます。 • [Fans]：ファンの動作ステータス、シリアル番号、およびベンダー機器タイプが表示されます。 • [SFP Modules]：プラットフォーム、シリアル番号、製造元、および Small Form-Factor Pluggable（SFP）モジュールの接続先ポートの詳細を表示します。[Search] または [Filter] をクリックして、ポートの詳細を表示できます。 • [User Defined Fields]：デバイスに関連付けられているユーザー定義フィールドが表示されます。 • [Config Drift]：構成の変更を表示し、同じデバイスの任意の 2 つのバージョンを選択して、各バージョンの実行中の構成データを比較できます。 • [Wireless Info]：プライマリとセカンダリの管理対象ロケーションが表示されます。 • [Mobility]：モビリティグループ名、RF グループ名、仮想 IP、およびモビリティ MAC アドレスが表示されます。 （注） 赤で表示されているデバイス名は、インベントリがデバイスをポーリングしておらず、30 分を超える期間にわたってその情報を更新していないことを意味しています。
IP Address	デバイスの IP アドレス。

カラム	説明
Support Type	デバイスのサポートレベルが表示されます。 • [Supported]：Cisco DNA Center のすべてのアプリケーションに対してデバイスパックがテスト済みです。これらのデバイスのいずれかの Cisco DNA Center 機能が動作しない場合は、サービスリクエストを開くことができます。 • [Limited]：レガシーデバイス用のデバイスパックは、Cisco DNA Center の次の機能についてのみテストされています。 • 検出 • トポロジ • デバイスの到達可能性 • 構成変更監査 • インベントリ：デバイス名、IPアドレス、サポートタイプ、デバイスファミリ、サイト、到達可能性、MAC アドレス、デバイスロール、イメージバージョン、稼働時間、最終同期ステータス、最終更新日、シリアル番号、デバイスシリーズ、プラットフォームなどのデバイス詳細について、サポートが提供されます。 • ソフトウェアイメージ管理：ソフトウェアイメージは、cisco.com に記載の EOL デバイスでは利用できない場合があります。EOLデバイスには推奨されません。 • テンプレート プロビジョニング：スイッチにのみ適用されます。 詳細については、『Cisco DNA Center Compatibility Matrix』を参照してください。 • [Unsupported]：Cisco DNA Center でテストおよび認定されていない他のすべてのシスコデバイスとサードパーティ製デバイス。これらのデバイスについて、Cisco DNA Center でさまざまな機能をベストエフォートとして試すことができます。ただし、Cisco DNA Center の機能が期待どおりに動作しない場合 、サービスリクエストまたはバグを発生させることは求められていません。 • [Third Party]：デバイスパックは、お客様またはビジネスパートナーによって構築され、認定プロセスを経ています。サードパーティ製デバイスは、ディスカバリ、インベントリ、トポロジなどの基本自動化機能をサポートします。Cisco TAC は、これらのデバイスの初期レベルのサポートを提供します。ただし、デバイスパックに問題がある場合は、ビジネスパートナーに連絡する必要があります。

カラム	説明
Reachability	以下は、さまざまなステータスのリストです。 • [Reachable]：Cisco DNA Center から SNMP、HTTP（S）、および NETCONF ポーリングを使用してデバイスに到達できます。 • [Ping Reachable]：Cisco DNA Center から ICMP ポーリングを使用してデバイスに到達できます。SNMP、HTTP（S）、および NETCONF ポーリングでは到達できません。 • [Unreachable]：SNMP、HTTP（S）、NETCONF、ICMP のいずれのポーリングでもデバイスに到達できません。
[EoX Status]	EoX スキャンのステータスが表示されます。 • [Success]：デバイスでの EoX アラートのスキャンに成功しました。 • [Not Scanned]：デバイスは EoX アラートについてスキャンされていません。 • [Scan Failed]：Cisco DNA Center でデバイスでの EoX アラートのスキャンに失敗しました。 • [Scanning]：Cisco DNA Center でデバイスでの EoX アラートのスキャンを実行しています。 正常にスキャンされたデバイスについては、[EoX Status] 列にアラートの数が表示されます（ある場合）。 アラートの数をクリックすると、アラートの詳細が表示されます。 slide-in pane で、[Hardware]、[Software]、および [Module] タブをクリックして、ハードウェア、ソフトウェア、およびモジュールの EoX アラートを表示します。
Manageability	デバイスのステータスが示されます。 • [Managed] と緑色のチェックアイコン：デバイスに到達可能で、完全に管理されています。 • [Managed] とオレンジ色のエラーアイコン：デバイスは管理されていますが、到達不能、認証失敗、NETCONF ポートがない、内部エラーなど、何らかのエラーがあります。エラーメッセージにカーソルを合わせると、エラーおよび影響を受けるアプリケーションに関する詳細が表示されます。 • [Unmanaged]：デバイスの接続の問題が原因でデバイスに到達できず、インベントリ情報が収集されていません。
MAC Address	デバイスの MAC アドレス。
Image Version	デバイスで現在実行されている Cisco IOS ソフトウェア。
Platform	シスコ製品の部品番号。

カラム	説明
Serial Number	シスコ デバイスのシリアル番号。
Uptime	デバイスが起動してから、稼働している時間。
Device Role	スキャン プロセス中に、検出された各デバイスに割り当てられているロール。デバイス ロールは、ネットワーク内での役目と配置に従って、デバイスを識別およびグループ分けするために使用されます。Cisco DNA Center でデバイス ロールを特定できない場合、デバイス ロールは不明に設定されます。 （注） デバイス ロールを手動で変更すると、割り当ては静的のままになります。Cisco DNA Center は、後続のデバイスの再同期中に変更が検知されたとしても、デバイス ロールは更新されません。 必要に応じて、このカラムのドロップダウン リストを使用して、割り当てられたデバイス ロールを変更することができます。
Site	デバイスに割り当てられているサイト。デバイスがどのサイトにも割り当てられていない場合は、[Assign] をクリックします。[Choose a site] をクリックし、階層からサイトを選択して [Save] をクリックします。詳細については、ネットワーク階層の概要 （155 ページ）を参照してください。
Last Updated	Cisco DNA Center がデバイスをスキャンし、デバイスに関する新しい情報でデータベースを更新した最新の日付と時刻。
Device Family	ルータ、スイッチ、ハブ、またはワイヤレスコントローラなどの関連するデバイスのグループ。
Device Series	デバイスのシリーズ番号（Cisco Catalyst 4500 シリーズ スイッチなど）。
Resync Interval	デバイスのポーリング間隔。この間隔は、[Settings] でグローバルに設定するか、またはインベントリ内の特定のデバイスに対して設定できます。詳細については、Cisco DNA Center 管理者ガイドを参照してください。
Last Sync Status	デバイス最終検出のスキャン状態。 • [Managed]：デバイスは完全に管理された状態です。 • [Partial Collection Failure]：デバイスは部分的に収集された状態で、すべてのインベントリ情報は収集されていません。障害の追加情報を表示するには、[Information]（i）アイコンにマウスを合わせます。 • [Unreachable]：デバイスの接続問題のため、デバイスに到達できず、インベントリ情報は収集されませんでした。この状態は、定期的な収集が行われたときに発生します。 • [Wrong Credentials]：デバイスをインベントリに追加した後にデバイスのログイン情報が変更された場合、この状態が表示されます。 • [In Progress]：インベントリ収集が実行されています。

カラム	説明
プロビジョニング ステータス	デバイスで試行された最後のプロビジョニング操作のステータスが示されます。過去のプロビジョニング操作のステータスを確認するには、[See Details] をクリックします。 • [Success]：デバイスでの最近の操作が成功しました。 • [Success with a warning icon]：デバイスでの最近の操作が成功しました。ただし、過去のプロビジョニング操作による障害があるため、注意が必要です。 • [Failed]：デバイスでの最近の操作が失敗しました。 • [Failed] と警告アイコン：デバイスでの最近の操作が失敗しました。過去のプロビジョニング操作による障害があるため、注意が必要です。 • [Configuring]：デバイスは現在設定中です。 • [Pending]：システムは、進行中のプロビジョニング操作によってデバイスが影響を受けるかどうかを判断しようとしています。 • [Not Provisioned]：デバイスは一度もプロビジョニングされていません。 • [Out of Sync]：デバイスのネットワーク設定またはネットワークプロファイルが、最後のプロビジョニング操作の後に変更されました。
Credential Status	デバイスのクレデンシャルステータスが示されます。 • [Not Applied]：デバイスのクレデンシャルがデバイスに適用されていません。 • [Success]：デバイスのクレデンシャルがデバイスに正常に適用されました。 • [Failed]：デバイスのクレデンシャルがデバイスで失敗しました。 クレデンシャルの詳細を表示するには、[See Details] をクリックします。 [Credential Status] slide-in paneには、クレデンシャルの [Type]、[Name/Description]、[Status]、および [Details] が表示されます。 ステータスが [Failed] のデバイスの場合、[Actions] 列の省略記号アイコン（ *** ）の上にカーソルを置き、[Retry] または [Clear] を選択します。 • [Retry]：デバイスにクレデンシャルを適用します。 • [Clear]：デバイスのクレデンシャルをクリアします。
AP Ethernet Mac Address	AP イーサネット MAC アドレスに関する詳細を表示します。

カラム	説明
AP CDP Neighbors	インベントリリストページのAPに接続されているスイッチとポートに関する詳細を表示します。インベントリリストページには、接続されたアクセススイッチがCisco DNA Centerによって管理されている場合でも、AP CDPネイバーに関する情報が表示されます。

ユーザー定義フィールドの管理

ユーザー定義フィールドは、Cisco DNA Centerで作成して任意のデバイスに割り当てることができるカスタムラベルです。これらのラベルを使用すると、デバイスの詳細のページにデバイスのより多くの詳細情報を表示できます。ユーザー定義フィールドを表示するには、そのフィールドをデバイスに割り当て、それに値を追加する必要があります。

ユーザー定義フィールドの作成

Cisco DNA Centerでは、ユーザー定義フィールドを作成し、任意のデバイスに割り当てることができます。

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

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

ステップ2 [Actions] ドロップダウンリストから、**[Provision]** > **[Inventory]** > **[Manage User Defined Fields]** の順に選択します。

ステップ3 [Manage User Defined Fields] ダイアログボックスで、[Create New Field] をクリックします。

ステップ4 [Create New Field] ダイアログボックスで、[Field Name] フィールドと [Field Description] フィールドにユーザー定義フィールドの名前と説明を入力します。

（注） お客様のIPアドレスやお客様のデバイス名など、[Device Details] ページにまだ表示されていないデバイスの詳細をユーザー定義フィールドに追加できます。

ステップ5 [**保存（Save）**] をクリックします。

同様に、追加のユーザー定義フィールドを作成できます。ユーザー定義フィールドはテーブルに表示されます。

ステップ6 ユーザー定義フィールドを編集する場合は、対応する [Edit] アイコンをクリックして必要な変更を行い、[Save] をクリックします。

ステップ7 ユーザー定義フィールドを削除する場合は、対応する [delete] アイコンをクリックし、後続の警告メッセージで [Yes] をクリックします。

デバイスへのユーザー定義フィールドの追加

始める前に

[Manage User Defined Fields] ウィンドウで少なくとも 1 つのユーザー定義フィールドを作成しておく必要があります。『ユーザー定義フィールドの作成 （96 ページ）』を参照してください。

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

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

ステップ 2 ユーザー定義フィールドを追加するデバイスの名前をクリックします。

ステップ 3 左側のペインで、[User Defined Fields] をクリックします。

ステップ 4 [Add] をクリックします。

ステップ 5 [Field Name] ドロップダウンリストでユーザー定義フィールドを選択し、[Value] フィールドにその値を入力します。

たとえば、顧客の IP アドレスのユーザー定義フィールドを作成した場合、[Field Name] ドロップダウンリストでそのフィールドを選択し、[Value] フィールドに顧客の IP アドレスを入力します。

ステップ 6 デバイスからユーザー定義フィールドを削除する場合は、対応する [Delete] アイコンをクリックします。

ステップ 7 [Save] をクリックします。

インベントリからのトポロジマップの起動

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

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

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

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

Cisco DNA Center インベントリ内のデバイスのタイプ

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

- **ネットワークデバイス**：サポート対象のネットワークデバイスには、シスコルータ、スイッチ、およびワイヤレスコントローラやアクセスポイント（AP）などのワイヤレスデバイスが含まれます。
- **計算デバイス**：サポート対象の計算デバイスには、Cisco Unified Computing System（UCS）、シスコ エンタープライズ ネットワーク機能仮想化インフラストラクチャ ソフトウェア（NFVIS）を実行しているデバイス、その他のデータセンターデバイスが含まれます。
- **Meraki ダッシュボード**：Cisco Meraki 製品を管理するためのシスコクラウド管理プラットフォームのダッシュボード。
- Firepower Management Center（FMC）：シスコのネットワーク セキュリティ ソリューションを管理するための Firepower Threat Defense（FTD）デバイスを介した完全かつ統合された管理を提供します。

サポートされるデバイスの完全なリストについては、『Cisco DNA Center Compatibility Matrix』を参照してください。

ネットワークデバイスの管理

ネットワーク デバイスを追加

ネットワーク デバイスは、インベントリに手動で追加できます。

始める前に

ネットワークデバイスを設定していることを確認します。詳細については、「ディスカバリの前提条件 （46 ページ）」を参照してください。

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

[Inventory] ウィンドウには、検出プロセス中に収集されたデバイス情報が表示されます。

ステップ 2 [Add Device] をクリックします。

ステップ 3 [Type] ドロップダウン リストから、[Network Device] を選択します。

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

（注） デバイスで HSRP プロトコルを使用している場合は、仮想 IP アドレスではなく、プライマリ IP アドレスを入力する必要があります。

ステップ 5 [CLI] 領域がまだ展開されていない場合は展開し、次のいずれかを実行します。

a) すでに作成されているグローバル CLI クレデンシャルを使用する場合は、[Select global credential] オプションボタンをクリックします。

（注） 使用可能なグローバル CLI クレデンシャルがない場合は、**[Network Settings]** > **[Device Credentials]**ウィンドウでグローバル CLI クレデンシャルを作成します。「グローバル CLI クレデンシャルの設定」を参照してください。

b) [Add device specific credential] オプションボタンをクリックし、次のフィールドを設定します。

表 *22 : CLI* クレデンシャル

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

ステップ 6 [SNMP] 領域がまだ表示されていない場合は展開し、次のいずれかを実行します。

a) すでに作成されている SNMP グローバルログイン情報を使用する場合は、[Select global credential] オプションボタンをクリックします。

（注） 使用可能なグローバル SNMP クレデンシャルがない場合は、**[Network Settings]** > **[Device Credentials]**ウィンドウでグローバル SNMP クレデンシャルを作成します。「グローバル SNMPv2c クレデンシャルの設定」および「グローバル SNMPv3 クレデンシャルの設定」を参照してください。

b) [Add device specific credential] オプションボタンをクリックし、次の手順を実行します。

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

[V2C] を選択した場合、次のフィールドを設定します。

表 *23 : SNMPv2c* のクレデンシャル

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

[V3] を選択した場合、次のフィールドを設定します。

表 *24 : SNMPv3* のクレデンシャル

フィールド	説明
Name/Description	追加した SNMPv3 設定の名前または説明。
Username	SNMPv3 設定に関連付けられている名前。
Mode	SNMP メッセージを必要とするセキュリティ レベル。次のいずれかのモードを選択します。 • [noAuthNoPriv]：認証または暗号化を提供しません。 • [AuthNoPriv]：認証を提供しますが、暗号化は提供しません。 • [AuthPriv]：認証と暗号化の両方を提供します。
Auth Type	使用する認証タイプ（[Mode] として [AuthPriv] または [AuthNoPriv] を選択した場合に有効になります）。次のいずれかの認証タイプを選択します。 • [SHA]：HMAC-SHA に基づく認証。 • [MD5]：HMAC-MD5 に基づく認証。

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

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

表 *25 : SNMP* のプロパティ

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

ステップ 9 [HTTP(S)] 領域がまだ表示されていない場合は展開し、次のいずれかを実行します。

a) すでに作成されている HTTP（HTTPS）グローバルログイン情報を使用する場合は、[Select global credential] オプションボタンをクリックします。

（注） 使用可能なグローバル HTTP（HTTPS）ログイン情報がない場合は、**[Network Settings]** > **[Device Credentials]** ウィンドウでグローバル HTTP（HTTPS）ログイン情報を作成します。「グローバル HTTPS クレデンシャルの設定」を参照してください。

b) [Add device specific credential] オプションボタンをクリックし、次のフィールドを設定します。

表 *26 : HTTP*（*S*）

フィールド	説明
Username	ネットワーク内のデバイスの HTTP（HTTPS）にログインするために使用する名前。
Password	ネットワーク内のデバイスの HTTP（HTTPS）にログインするために使用するパスワード。 セキュリティ上の理由から、確認のためにパスワードを再入力します。 （注） パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。
Port	必要な HTTP（HTTPS）ポート番号を指定します。

ステップ 10 まだ展開されていない場合は **NETCONF** 領域を展開し、**ポート** フィールドを設定します。

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

ステップ 11 Cisco DNA Center とリモートデバイスとの通信を可能にするいずれかのネットワークプロトコルの [Protocol] オプションボタンを選択します。有効な値は **SSH2** または **Telnet** です。

ステップ 12 （オプション）[Credentials] の横にある [Validate] をクリックします。Cisco DNA Center により、デバイスログイン情報が検証され、有効なログイン情報には緑色のチェックマーク、無効なログイン情報には赤色の X マークが表示されます。

SNMP 書き込みログイン情報を除くすべてのログイン情報が検証されます。

ステップ 13 [Add] をクリックします。

ネットワーク デバイス クレデンシャルの更新

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

始める前に

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

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

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

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

ステップ 2 更新するネットワーク デバイスを選択します。

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

ステップ 4 [Edit Device] ダイアログボックスで、[Type] ドロップダウンフィールドから [Network Device] を選択します（まだ選択していない場合）。

ステップ 5 [CLI] 領域がまだ展開されていない場合は展開し、次のいずれかを実行します。

a) すでに作成されているグローバル CLI クレデンシャルを使用する場合は、[Select global credential] オプションボタンをクリックします。

（注） 使用可能な CLI グローバルログイン情報がない場合は、**[Network Settings]** > **[Device Credentials]** ページで作成します。「グローバル CLI クレデンシャルの設定」を参照してください。

b) [Edit device specific credential] オプションボタンをクリックし、次のフィールドを設定します。

表 *27 : CLI* クレデンシャル

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

フィールド	説明
Enable Password	CLI で高い権限レベルに移るために使用するパスワード。 セキュリティ上の理由から、有効なパスワードを再入力します。 パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。

ステップ 6 [SNMP] 領域がまだ展開されていない場合は展開し、次のいずれかを実行します。

a) すでに作成されている SNMP グローバルログイン情報を使用する場合は、[Select global credential] オプションボタンをクリックします。

（注） 使用可能な SNMP グローバルログイン情報がない場合は、**[Network Settings]** > **[Device Credentials]** ページで作成します。「グローバル SNMPv2c クレデンシャルの設定」および「グローバル SNMPv3 クレデンシャルの設定」を参照してください。

b) [Edit device specific credential] オプションボタンをクリックし、次の手順を実行します。

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

[V2C] を選択した場合、次のフィールドを設定します。

表 28 : SNMPv2c のクレデンシャル

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

[V3] を選択した場合、次のフィールドを設定します。

表 29 : SNMPv3 のクレデンシャル

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

フィールド	説明
Username	SNMPv3 設定に関連付けられている名前。
Mode	SNMP メッセージを必要とするセキュリティ レベル。次のいずれかのモードを選択します。 • [noAuthNoPriv]：認証または暗号化を提供しません。 • [AuthNoPriv]：認証を提供しますが、暗号化は提供しません。 • [AuthPriv]：認証と暗号化の両方を提供します。
Auth Type	使用する認証タイプ（[Mode] として [AuthPriv] または [AuthNoPriv] を選択した場合に有効になります）。次のいずれかの認証タイプを選択します。 • [SHA]：HMAC-SHA に基づく認証。 • [MD5]：HMAC-MD5 に基づく認証。
Auth Password	SNMPv3 を使用するデバイスから情報にアクセスする際に使用する SNMPv3 パスワード。これらのパスワード（またはパスフレーズ）は、8 文字以上にする必要があります。 （注） • 一部のシスコ ワイヤレス コントローラでは、パスワード（あるいはパスフレーズ）は少なくとも 12 文字以上である必要があります。ワイヤレス コントローラのパスワードの最小要件を必ず確認してください。パスワードに必要な最低限の文字数が守られないと、デバイスではCisco DNA Centerによる検出、監視、管理が行われなくなります。 • パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。

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

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

表 *30 : SNMP* のプロパティ

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

ステップ 9 [HTTP(S)] 領域がまだ展開されていない場合は展開し、次のいずれかを実行します。

a) すでに作成されている HTTP（HTTPS）グローバルログイン情報を使用する場合は、[Select global credential] オプションボタンをクリックします。

（注） 使用可能な HTTP（HTTPS）グローバルログイン情報がない場合は、**[Network Settings]** > **[Device Credentials]** ページで作成します。「グローバル HTTPS クレデンシャルの設定」を参照してください。

b) [Edit device specific credential] オプションボタンをクリックし、次のフィールドを設定します。

表 *31 : HTTP*（*S*）

フィールド	説明
Username	ネットワーク内のデバイスの HTTP（HTTPS）にログインするために使用する名前。
Password	ネットワーク内のデバイスの HTTP（HTTPS）にログインするために使用するパスワード。 セキュリティ上の理由から、確認のためにパスワードを再入力します。 パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。
Port	必要な HTTP（HTTPS）ポート番号を指定します。

ステップ 10 まだ展開されていない場合は **NETCONF** 領域を展開し、**ポート** フィールドを設定します。

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

ステップ 11 Cisco DNA Center とリモートデバイスとの通信を可能にするいずれかのネットワークプロトコルの [Protocol] オプションボタンを選択します。有効な値は **SSH2** または **Telnet** です。

ステップ 12 （オプション）[Credentials] の横にある [Validate] をクリックします。Cisco DNA Center により、デバイスログイン情報が検証され、有効なログイン情報には緑色のチェックマーク、無効なログイン情報には赤色の X マークが表示されます。

ログイン情報を更新する対象として複数のデバイスを選択した場合、[Validation] ボタンは無効になります。

ステップ 13 [更新（Update）] をクリックします。

ネットワークデバイスのセキュリティフォーカス

Cisco DNA Center のセキュリティフォーカスにより、デバイスでの信頼できるチェックの結果を表示できます。

使用しているシスコのデバイスが正規の製品であり、セキュリティ侵害を受けたり物理的に変更されたりしていないことを確認するために実行されるセキュリティチェックはわずかしかありません。

デバイスアイデンティティ検証の一環として、次のチェックが実行されます。

- セキュアな固有デバイス識別子（SUDI）証明書チェーンの検証。
- デバイスの SUDI 証明書応答の署名検証。
- SUDI 証明書による製品 ID 検証。
- SUDI 証明書によるシリアル番号検証。

これらのチェックは、次の状況でトリガーされます。

- Cisco DNA Center でインベントリが収集されるたび。
- デバイスの設定を変更するとき。
- デバイスでイメージをアップグレードするとき。

次の CLI コマンドを使用して、デバイスアイデンティティ検証チェックを実行します。

```
show platform sudi certificate sign nonce ${randomNonceValue}
```

整合性検証チェックの実行

この手順では、整合性検証チェックのステータスを確認する方法について説明します。

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

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

ステップ 2 [Inventory] ドロップダウンメニューから [Security] を選択します。

ステップ 3 テーブルに示されているデバイスの詳細情報を確認します。

ステップ 4 テーブルをカスタマイズするには、テーブルの端にある縦に並んだ3つのドットをクリックし、[Add] または [Delete] を選択します。
[Integrity Verification] 列に結果が表示されます。

ステップ 5 デバイスの [Integrity Verification] 列にステータスとして [Failed] と表示されている場合は、情報アイコンをクリックして理由を表示します。

整合性検証のステータスは次のとおりです。

- [Passed]：デバイスの整合性検証に合格しました。
- [Failed]：デバイスの整合性検証に合格しませんでした。
- [Unverified]：検証を実行できませんでした。

- [Not Available]：このバージョンのデバイスまたはソフトウェアイメージが検証をサポートしていません。

計算デバイスの管理

計算デバイスの追加

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

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

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

ステップ 2 [Add Device] をクリックします。

ステップ 3 [Type] ドロップダウン リストから、[Compute Device] を選択します。

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

ステップ 5 [HTTP(S)] 領域がまだ展開されていない場合は展開し、次のいずれかを実行します。

a) すでに作成されている HTTP（HTTPS）グローバルログイン情報を使用する場合は、[Select global credential] オプションボタンをクリックします。

（注） 使用可能な HTTP（HTTPS）グローバルログイン情報がない場合は、**[Network Settings]** > **[Device Credentials]** ページで作成します。「グローバル HTTPS クレデンシャルの設定」を参照してください。

b) [Add device specific credential] オプションボタンをクリックし、次のフィールドを設定します。

表 *32 : HTTP*（*S*）

フィールド	説明
Username	HTTPS 接続の認証に使用される名前。
Password	HTTPS 接続の認証に使用されるパスワード。
Port	HTTPS トラフィックに使用される TCP/UDP ポートの番号。デフォルトはポート番号 443（HTTPS の既知のポート）です。

ステップ 6 [CLI] 領域がまだ展開されていない場合は展開し、次のいずれかを実行します。

a) すでに作成されているグローバル CLI クレデンシャルを使用する場合は、[Select global credential] オプションボタンをクリックします。

（注） 使用可能な CLI グローバルログイン情報がない場合は、**[Network Settings]** > **[Device Credentials]** ページで作成します。「グローバル CLI クレデンシャルの設定」を参照してください。

b) [Add device specific credential] オプションボタンをクリックし、次のフィールドを設定します。

表 *33* : *CLI* クレデンシャル

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

ステップ 7 [SNMP] 領域がまだ展開されていない場合は展開し、次のいずれかを実行します。

a) すでに作成されている SNMP グローバルログイン情報を使用する場合は、[Select global credential] オプションボタンをクリックします。

（注） 使用可能な SNMP グローバルログイン情報がない場合は、**[Network Settings]** > **[Device Credentials]** ページで作成します。「グローバル SNMPv2c クレデンシャルの設定」および「グローバル SNMPv3 クレデンシャルの設定」を参照してください。

b) [Add device specific credential] オプションボタンをクリックし、次の手順を実行します。

ステップ 8 [Version] ドロップダウンリストから、[V2C]（SNMP バージョン 2c）または [V3]（SNMP バージョン 3）を選択します。

[V2C] を選択した場合、次のフィールドを設定します。

表 *34* : *SNMPv2c* のクレデンシャル

フィールド	説明
Read	• [Name/Description]：追加している SNMPv2c 設定の名前または説明。 • [Read Community]：デバイスに SNMP 情報を表示する目的のみに使用される読み取り専用のコミュニティ文字列パスワード。 （注） パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。

フィールド	説明
Write	• [Name/Description]：追加している SNMPv2c 設定の名前または説明。 • [Write Community]：デバイス上の SNMP 情報を変更するために使用される書き込みコミュニティ文字列。 （注） パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。

[V3] を選択した場合、次のフィールドを設定します。

表 *35 : SNMPv3* のクレデンシャル

フィールド	説明
Name/Description	追加した SNMPv3 設定の名前または説明。
Username	SNMPv3 設定に関連付けられている名前。
Mode	SNMP メッセージを必要とするセキュリティ レベル。次のいずれかのモードを選択します。 • [noAuthNoPriv]：認証または暗号化を提供しません。 • [AuthNoPriv]：認証を提供しますが、暗号化は提供しません。 • [AuthPriv]：認証と暗号化の両方を提供します。
Auth Type	使用する認証タイプ（[Mode] として [AuthPriv] または [AuthNoPriv] を選択した場合に有効になります）。次のいずれかの認証タイプを選択します。 • [SHA]：HMAC-SHA に基づく認証。 • [MD5]：HMAC-MD5 に基づく認証。
Auth Password	SNMPv3 を使用するデバイスから情報にアクセスする際に使用する SNMPv3 パスワード。これらのパスワード（またはパスフレーズ）は、8 文字以上にする必要があります。 （注） • 一部のシスコ ワイヤレス コントローラでは、パスワード（あるいはパスフレーズ）は少なくとも 12 文字以上である必要があります。ワイヤレス コントローラのパスワードの最小要件を必ず確認してください。パスワードに必要な最低限の文字数が守られないと、デバイスではCisco DNA Centerによる検出、監視、管理が行われなくなります。 • パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。

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

ステップ 9 （オプション）[Credentials] の横にある [Validate] をクリックします。Cisco DNA Center により、デバイスログイン情報が検証され、有効なログイン情報には緑色のチェックマーク、無効なログイン情報には赤色の X マークが表示されます。

SNMP 書き込みログイン情報を除くすべてのログイン情報が検証されます。

ステップ 10 [Add] をクリックします。

計算デバイス クレデンシャルの更新

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

始める前に

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

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

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

ステップ 2 更新するデバイスを選択します。

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

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

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

ステップ 6 [Username] および [Password] フィールドに、ユーザー名とパスワードを入力します。

ステップ 7 [Port] フィールドにポート番号を入力します。

ステップ 8 （オプション）[Credentials] の横にある [Validate] をクリックします。Cisco DNA Center により、デバイスログイン情報が検証され、有効なログイン情報には緑色のチェックマーク、無効なログイン情報には赤色の X マークが表示されます。

ログイン情報を更新する対象として複数のデバイスを選択した場合、[Validation] ボタンは無効になります。

ステップ 9 [更新（Update）] をクリックします。

Meraki ダッシュ ボードの管理

Meraki ダッシュボードの統合

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

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

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

ステップ 2 [Add Device] をクリックします。

ステップ 3 [デバイスの追加（Add Device）] ダイアログボックスの [タイプ（Type）] ドロップダウンリストで、[Meraki ダッシュボード（Meraki Dashboard）] を選択します。

ステップ 4 まだ展開されていない場合は、[HTTP（S）] エリアを展開します。

ステップ 5 [API Key/Password] フィールドで、API キーとパスワードのログイン情報を入力し、[Get Organization details] リンクをクリックします。

ステップ 6 [Organization] ドロップダウンリストから組織のオプションを選択するか、組織名を検索します。

ステップ 7 （オプション）[Credentials] の横にある [Validate] をクリックします。Cisco DNA Center により、デバイスログイン情報が検証され、有効なログイン情報には緑色のチェックマーク、無効なログイン情報には赤色の X マークが表示されます。

ステップ 8 [Add] をクリックします。

選択した組織のみで Cisco Meraki ダッシュボードとデバイスの収集が開始されます。

Meraki ダッシュボード クレデンシャルの更新

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

始める前に

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

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

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

ステップ 2 更新するデバイスを選択します。

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

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

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

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

ステップ 7 [Port] フィールドにポート番号を入力します。

ステップ 8 （オプション）[Credentials] の横にある [Validate] をクリックします。Cisco DNA Center により、デバイスログイン情報が検証され、有効なログイン情報には緑色のチェックマーク、無効なログイン情報には赤色の X マークが表示されます。

ログイン情報を更新する対象として複数のデバイスを選択した場合、[Validation] ボタンは無効になります。

ステップ 9 [更新（Update）] をクリックします。

Firepower Management Center の管理

Firepower Management Center の統合

Firepower Management Center（FMC）を Cisco DNA Center と統合できます。

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

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

ステップ 2 [Add Device] をクリックします。

ステップ 3 [Add Device] ダイアログボックスの [Type] ドロップダウンリストで、[Firepower Management Center] を選択します。

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

ステップ 5 [HTTP(S)] エリアを展開します（まだ展開していない場合）。

[Add device specific credential] オプションボタンは、デフォルトで選択されています。

ステップ 6 次の情報を入力します。

a) [Username]：HTTPS 接続の認証に使用される名前です。

b) [Password]：HTTPS 接続の認証に使用されるパスワードです。パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。

c) [Port]：HTTPS トラフィックで使用される TCP/UDP ポートの番号です。デフォルトのポート番号は 443 です。

ステップ 7 [Add] をクリックします。

（注） インベントリに FMC を追加すると、FMC によって管理される Firepower Threat Defense（FTD）デバイスもインベントリに自動的に追加されます。

Firepower Management Center のログイン情報の更新

Cisco DNA Center では Firepower Management Center（FMC）のログイン情報を更新できます。選択したデバイスに対しては、この更新された設定が、グローバル設定やジョブ固有の設定よりも優先されます。

始める前に

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

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

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

ステップ 2 更新する FMC デバイスを選択します。

（注） FMC によって管理されている Firepower Threat Defense（FTD）デバイスを更新、編集、または削除することはできません。インベントリ内の FMC を介して FTD デバイスを管理する必要があります。

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

[Edit Device] ダイアログボックスが表示されます。

ステップ 4 [Credentials] をクリックします。

ステップ 5 [HTTP(S)] エリアを展開します（まだ展開していない場合）。

[Add device specific credential] オプションボタンは、デフォルトで選択されています。

ステップ 6 次の情報を入力します。

a) [Username]：HTTPS 接続の認証に使用される名前です。

b) [Password]：HTTPS 接続の認証に使用されるパスワードです。パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。

c) [Port]：HTTPS トラフィックで使用される TCP/UDP ポートの番号です。デフォルトのポート番号は 443 です。

ステップ 7 [Management IP] をクリックし、[Device IP/DNS Name] フィールドにデバイスの IP アドレスまたは名前を入力します。

ステップ 8 [Resync Interval] をクリックし、再同期間隔タイプを選択します。

- [Custom]：再同期間隔を分単位で入力できます。有効な範囲は 25 ～ 1,440 分（24 時間）です。
- [Global]：デフォルトでは、再同期間隔は 1,440 分（24 時間）に設定されます。
- [Disable]：再同期間隔が無効になるかゼロに設定されます。

ステップ 9 [Role] をクリックし、[Device Role] ドロップダウンリストからロールを選択します。

ステップ 10 [更新（Update）] をクリックします。

デバイスのフィルタ

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

始める前に

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

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

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

ステップ 2 [Filter] をクリックします。

次のタイプのフィルタを使用できます。

- クイック フィルタ
- 拡張フィルタ
- 最近のフィルタ

[Quick Filter]：このフィルタでは、次の項目に基づいてデバイスの詳細を取得できます。

- **Device Family**
- **Device Role**
- **Last Sync Status**
- **Provision Status**
- **Credential Status**
- **OS Updated Status**
- **Image Needs Update**
- **Image Pre Check Status**
- **Support Type**

[Advanced Filters]：このフィルタでは、[Contains]、[Starts With]、[Ends With]、[Equals]、[Does not contains] などの演算子と正規表現を使用してフィルタ基準を設定し、その条件に基づいてデバイスの詳細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、使用可能なデータに基づいてフィルタ基準の値を入力する必要があります。

[Recent Filters]：このフィルタでは、最近使用したフィルタが表示されます。フィルタ基準を保存するには、[RECENT] から [SAVED] にフィルタをドラッグアンドドロップします。

ステップ 3 選択したフィルタのフィールドに適切な値を入力します。たとえば、[Device Name] フィルタであれば、デバイスの名前を入力します。

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

これらのフィルタにワイルドカード（アスタリスク）を使用することもできます。たとえば、文字列値の先頭、末尾、または中間にアスタリスクがある値を入力できます。その後、Enter を押します。

ステップ 4 [Apply] をクリックして情報をフィルタします。

[Devices] テーブルに表示されるデータは、フィルタ選択に従って自動的に更新されます。

（注） フィルタごとに複数のフィルタ タイプと複数の値を使用できます。

ステップ 5 （オプション）必要に応じて、フィルタを追加します。

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

インベントリ内のデバイスの管理

ここでは、[Inventory] ウィンドウを使用して、サイトにデバイスを割り当て、デバイスタグを管理する方法について説明します。

デバイスをサイトに追加する

ステップ 1 メニューアイコン（☰）をクリックして、**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。
[Inventory] ウィンドウには、**ディスカバリ**プロセス中に収集されたデバイス情報が表示されます。

ステップ 2 サイトに割り当てるデバイスのチェックボックスをオンにします。

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

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

ステップ 5 [Choose a floor] スライドインペインで、デバイスに割り当てるフロアを選択します。

ステップ 6 [Save] をクリックします。

ステップ 7 （任意） 複数のデバイスを選択して同じ場所に追加した場合は、最初のデバイスで [Apply to All] チェックボックスをオンにすると、残りのデバイスに同じ場所を割り当てることができます。

ステップ 8 [Next] をクリックします。

ステップ 9 [Task Name] フィールドに、任意のタスク名を入力します。

ステップ 10 即座にデバイスをサイトに割り当てるには、[Now] オプションボタンをクリックし、[Assign] をクリックします。

ステップ 11 将来の日付と時刻でデバイスのサイトへの割り当てをスケジュールするには、[Later] オプションボタンをクリックして展開する日時を定義し、[Assign] をクリックします。

ステップ 12 CLI 構成をプレビューするには、[Generate Configuration Preview] オプションボタンをクリックして、次の手順を実行します。

- [Task Name] フィールドに任意のタスク名を入力し、[Preview] をクリックします。

  後で、作成した構成のプレビューを使用して、選択したデバイスに展開できます。

- [Task Submitted] メッセージで、[Work Items] リンクをクリックします。

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

- [Work Items] ウィンドウで、設定プレビュー要求を送信した CLI プレビュータスクをクリックします。
- CLI 設定の詳細を表示し、[Deploy] をクリックします。
- 即座にデバイスを展開するには、[Now] オプションボタンをクリックし、[Apply] をクリックします。

- 将来の日付と時刻でデバイスの展開をスケジュールするには、[Later] オプションボタンをクリックし、展開する日時を定義します。
- 確認ウィンドウで [Yes] をクリックします。

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

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

デバイスのタグ付け

デバイス タグは属性またはルールに基づいてデバイスをグループ化することができます。単一のデバイスに複数のタグを設定できます。同様に、複数のデバイスに適用できる単一のタグもあります。

[プロビジョン（Provision）]ウィンドウのデバイスに対してタグを追加したり、削除できます。

ステップ 1 メニューアイコン（☰）をクリックして、**[Provision]**。デバイスインベントリのページには、ディスカバリ プロセス中に収集されたデバイス情報が表示されます。

ステップ 2 タグを適用するデバイスの横にあるチェックボックスをオンにして、[Tag Device] をクリックします。

ステップ 3 [タグ名（Tag Name）] フィールドにタグ名を入力します。

- 新しいタグを作成している場合は、 [新規タグの作成（Create New Tag）] をクリックします。ルールを使用して新規タグを作成することもできます。「ルールを使用してデバイスにタグ付けする（120 ページ）」を参照してください。
- 既存のタグを使用する場合は、一覧からタグを選択して、[Apply] をクリックします。

タグを適用するデバイス名の下に、タグ アイコンとタグ名が表示されます。

ステップ 4 デバイスからタグを削除するには、以下のいずれか 1 つを行います。

- Click **Create New Tag**, unselect all tags, and then click **APply**.
- タグアイコンまたはタグ名にカーソルを合わせて、[X] をクリックし、デバイスからタグの関連付けを解除します。

ルールを使用してデバイスにタグ付けする

ルールを定義するタグに基づいてデバイスをグループ化することができます。ルールを定義するとき、Cisco DNA Center は指定したルールと一致するすべてのデバイスにタグを適用します。ルールはデバイス名、デバイスファミリ、デバイスシリーズ、IP アドレス、ロケーション、またはバージョンに基づくことができます。

ステップ 1 メニューアイコン（☰）をクリックして、**[Provision]**。デバイスインベントリのページには、ディスカバリ プロセス中に収集されたデバイス情報が表示されます。

ステップ 2 タグを適用するデバイスの隣のチェックボックスをオンにして、**[デバイスのタグ付け（Tag Device）]** をクリックします。

ステップ 3 [タグ名（Tag Name）] フィールドにタグ名を入力し、[ルールによる新規タグの作成（Create New Tag with Rule）] をクリックします。

[新規 VRF の作成（Create New VRF）] ウィンドウが表示されます。

[Total Devices Tagged Count] の下にある [Manually Added] フィールドは、選択されたデバイスの数を示します。

ステップ 4 [条件の追加（Add Condition）] をクリックして、ルールに必要なフィールドに記入します。

[一致するデバイス（Matching Devices）] の数は、この条件に一致するデバイスの数に応じて、自動的に変更されます。

追加条件を作成するためには、次の 2 つのオプションがあります。

- *And* 条件：[Add Condition] リンクをクリックします。**And** が条件の上に表示されます。
- *Or* 条件：既存の条件の横にある追加アイコン (+) をクリックします。**Or** は条件の隣に表示されます。

必要に応じていくつでも条件を追加できます。ルールを変更すると、指定したルールに一致するインベントリのデバイス数を反映して一致するデバイス数が変更されます。デバイス数でクリックして、ルールと一致するデバイスを表示できます。

ステップ 5 [保存（Save）] をクリックして、定義されたルールと共にタグを保存します。

タグを適用するデバイス名の下に、タグ アイコンとタグ名が表示されます。

デバイスがインベントリに追加されると、定義したruleと一致する場合、タグは自動的にデバイスに適用されます。

デバイスタグの編集

以前に作成したデバイスタグを編集できます。

ステップ 1 メニューアイコン（☰）をクリックして、**[Provision]**。デバイスインベントリのページには、ディスカバリ プロセス中に収集されたデバイス情報が表示されます。

[デバイス名（Device Name）] 列のデバイス名の下に以前に作成したデバイスタグがありある場合はそれがリスト表示されます。

ステップ 2 デバイスを選択しないで、[デバイスのタグ付け（Tag Device）] をクリックします。

以前に作成されたタグがリストされます。

ステップ 3 編集するタグをマウスオーバーして、タグ名の隣の鉛筆アイコンをクリックします。

代わりに、**[Tag Device]** > **[View All Tags]** の順に選択してから、編集するタグの横にある鉛筆アイコンをクリックすることもできます。

ステップ 4 タグを変更し、[Save] をクリックします。

タグの削除

デバイスタグまたはテンプレートタグは、デバイスまたはテンプレートに関連付けられていない場合にのみ削除できます。

始める前に

デバイスに（ルールを使用して）静的または動的に関連付けられているタグを削除します。

テンプレートに関連付けられているタグを削除します。

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

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

ステップ 2 デバイスを選択しないで、**[Tag Device]** > **[Manage Tags]** の順に選択します。

ステップ 3 削除するタグにマウスカーソルを合わせてから、タグ名の横にある削除アイコンをクリックします。

ステップ 4 プロンプトで [Yes] をクリックします。

タグがデバイスまたはテンプレートに関連付けられている場合は、エラーメッセージが生成されます。デバイスまたはテンプレートに関連付けられているタグを除去し、タグを削除します。

ポート グループの作成

この手順を使用して、属性またはルールに基づいてポートをグループ化します。

ステップ 1 [Provision]メニューアイコン（☰）をクリックして、>[Inventory] の順に選択します。[Inventory] ウィンドウには、ディスカバリプロセス中に収集されたデバイス情報が表示されます。

ステップ 2 新しいポートタグを作成するには、[Tag] をクリックし、[Create New Tag] を選択します。

[Create New Tag] スライドインペインが表示されます。

ステップ 3 [Tag Name] フィールドに、タグ名を入力します。[Description] フィールドにタグの説明を追加できます。

（注） [WAN] タグは予約済みのタグ名です。WAN タグは自動生成されるため、*WAN* という名前の新しいポートタグは作成できません。

ステップ 4 [Tag Rule] 領域で、[Port] タブをクリックします。

ステップ 5 [Device Scope] 領域で、ドロップダウンリストをクリックし、デバイスの [Location] または [Tag Name] を選択して、フィルタを定義します。

ステップ 6 ポートにタグを付けるためのルールを追加するには、⊕アイコンをクリックします。ポートステータス、速度、タグ名、動作ステータス、および説明に基づいてポートにタグを付けることができます。ブール演算子（AND、OR）を使用して条件を追加できます。

条件を削除するには、削除アイコンをクリックします。

ステップ 7 条件が設定されると、ペインの左下隅に条件に一致するポートのリンクが表示されます。

リンクをクリックしてポートを表示します。[Matching Ports] スライドインペインが表示されます。ポートが属するデバイスとポート名を表示できます。

ステップ 8 [Save] をクリックします。

ポートへのタグの割り当て

ポートにタグを手動で割り当てることができます。たとえば、システムで生成された **WAN** タグをポートに手動で割り当てることができます。

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

ステップ 2 [Inventory] ウィンドウで、デバイス名をクリックし、[View Device Details] を選択します。

ステップ 3 左ペインで [Interfaces] を展開し、[Ethernet Ports] をクリックします。

ステップ 4 ウィンドウの右上隅で、テーブルビューに切り替えます。

ステップ 5 タグ付けするポート（1 つまたは複数）を選択し、[Tag] をクリックします。

ステップ 6 適切なタグを選択します。

ステップ 7 [Apply] をクリックします。

デバイスのメンテナンスモード

デバイスのメンテナンスのスケジュール

Cisco DNA Center で 1 つ以上のデバイスをメンテナンスモードにすることができます。デバイスがメンテナンスモードになっている場合、Cisco DNA Center ではデバイスに関連付けられているテレメトリデータは処理されません。故障したデバイスをメンテナンスモードにすることで、デバイスからの不要なアラートの受信を回避できます。

（注） メンテナンスモードのデバイスからは情報を収集できません。また、設定やポーリング操作はできません。

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

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

ステップ 2 メンテナンスをスケジュールするデバイスを選択します。

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

[Schedule Maintenance] スライドインペインが表示されます。

ステップ 4 [Reason For Maintenance] フィールドに、デバイスをメンテナンスモードにする理由を入力します。

デフォルトでは、Cisco DNA Center が理由を追加し、ユーザーがそれを変更できます。

ステップ 5 [Define Maintenance Window] 領域で、次の手順を実行します。

a) メンテナンスの開始日時を選択します。
b) メンテナンスの終了日時を選択します。
c) または、[Days/Hours] をクリックして、メンテナンスの日数と時間を入力します。

注：メンテナンスの繰り返しを選択するには、[Days/Hours] オプションを選択します。

ステップ 6 [Maintenance Recurrence] 領域で、[None]、[Daily]、または [Weekly] をクリックします。

- [None]：メンテナンスは繰り返されません。
- [Daily]：[Run at Interval（Days）] フィールドに間隔を日単位で入力します。
- [Weekly]:[Run at Interval（Weeks）] フィールドに間隔を週単位で入力します。

ステップ 7 繰り返しに [Daily] または [Weekly] を選択した場合は、[Set Schedule End]チェックボックスをオンにします。

ステップ 8 [End Date] または [End After (Occurrences)] をクリックします。

- [End Date]：メンテナンスを終了する月、日付、年を入力します。
- [End After (Occurrences)]：メンテナンスを終了するまでの回数を入力します。

ステップ 9 [Maintenance Time Zone] 領域で、メンテナンスのタイムゾーンを選択します。

ステップ 10 [送信（Submit）] をクリックします。

デバイスのメンテナンススケジュールの管理

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

ステップ 2 [Actions] ドロップダウンリストから、**[Inventory]** > **[Manage Maintenance]** の順に選択します。

[Manage Maintenance] スライドインペインが表示されます。[Status] 列には、メンテナンススケジュールの現在のステータスが表示されます。

ステップ 3 [Search] または [Filter] アイコンをクリックして、メンテナンススケジュールを検索またはフィルタします。

ステップ 4 [Actions] 列で、[Edit] アイコンをクリックして、メンテナンススケジュールを編集します。

（注） 進行中のメンテナンススケジュールの場合、メンテナンスの終了時間のみを延長できます。

ステップ 5 [Actions] 列で、[Delete] アイコンをクリックして、メンテナンススケジュールを削除します。

（注） 進行中のメンテナンススケジュールは削除できません。

インベントリインサイト

[Inventory Insights] ウィンドウには、他の直接接続されたデバイスと設定が一致しないデバイスが表示されます。また、Cisco DNA Center のベストプラクティスの推奨事項と比較して、誤って設定されたデバイスも表示されます。Cisco DNA Center では、次のインサイトと推奨されるアクションが提供されます。

- 速度/デュプレックス設定の不一致
- VLAN の不一致

速度/デュプレックス設定の不一致

Cisco DNA Center には、相互に接続されているが、デバイスリンクの両端で異なる速度とデュプレックス値が設定されているデバイスが表示されます。

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

[Inventory Insights] ウィンドウが表示されます。

ステップ 2 [Speed/Duplex settings mismatch] をクリックして、デバイスで実行できる推奨アクションを確認します。

推奨アクションが右側のペインに表示されます。

ステップ 3 インスタンスの番号をクリックして、不一致を確認します。

[Speed/Duplex settings mismatch] ウィンドウでは、速度とデュプレックスの不一致が強調表示されます。

ステップ 4 推奨アクションに従って、デバイス設定に必要な変更を加えます。

VLAN の不一致

Cisco DNA Center には、相互に接続されているが、デバイスリンクの両端で異なる VLAN が設定されているデバイスが表示されます。

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

[Inventory Insights] ウィンドウが表示されます。

ステップ 2 [VLAN Mismatch] をクリックして、デバイスで実行できる推奨アクションを確認します。

推奨アクションが右側のペインに表示されます。

ステップ 3 インスタンスの番号をクリックして、不一致を確認します。

[VLAN Mismatch] ウィンドウに、許可された VLAN とネイティブ VLAN の不一致が強調表示されます。

ステップ 4 推奨アクションに従って、デバイス設定に必要な変更を加えます。

システムビーコンの管理

システムビーコンを使用して、Cisco DNA Center インベントリ内のスイッチを強調表示できます。

システムビーコンは、次のデバイスをサポートします。

- Cisco Catalyst 9200 シリーズ スイッチ
- Cisco Catalyst 9300 シリーズ スイッチ
- Cisco Catalyst 3850 シリーズ イーサネット スタッカブル スイッチ

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

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

ステップ 2 ビーコンを有効または無効にするデバイスを選択します。

（注）
- 一度に最大 5 台のスタンドアロンデバイスでビーコンを有効にできます。
- スタックされたデバイスでビーコンを有効にする場合は、一度に 1 つのデバイスのみを選択する必要があります。スタックされたデバイスでは、1つ以上のスタックメンバーでビーコンを有効にすることができます。

ステップ 3 [Actions] ドロップダウンリストから、**[Inventory]** > **[Manage System Beacon]**を選択します。

ステップ 4 [Manage System Beacon] スライドインペインで、[System Beacon State] の下の [Enabled] オプションボタンをクリックし、[Apply] をクリックして、選択したデバイスでビーコンを有効にします。

システムビーコンが有効になると、インベントリのデバイス名の横に青いビーコン（ ）が表示されます。

ステップ 5 スタックされたデバイスを選択した場合は、[Manage System Beacon] スライドインペインで次の手順を実行します。

a) ビーコンを有効にするスタックメンバーに対応する [Update System Beacon Status?] チェックボックスをオンにします。
b) [System Beacon State] で、[Enabled] オプションボタンをオンにします。
c) [Apply] をクリックします。

ステップ 6 選択したデバイスでビーコンを無効にするには、[Manage System Beacon] スライドインペインで次の手順を実行します。

a) [System Beacon State] で、[Disabled] オプションボタンをオンにします。
b) [Apply] をクリックします。

または、[Inventory] ウィンドウで、デバイス名の横にある青いビーコン（ ）にカーソルを合わせ、[Disable] をクリックします。

デバイスのロールの変更（インベントリ）

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

表 *36 :* デバイスのロールとトポロジの位置

トポロジの位置	デバイス ロール
階層 1	インターネット（設定不可）
階層 2	[Border Router]
階層 3	コア
階層 4	Distribution
階層 5	アクセス
階層 6	不明（Unknown）

（注） **アクセス**ロールをデバイスに割り当てると、IP デバイストラッキング（IPDT）が設定されるか、サイトの IPDT 設定に基づいてデバイスから削除されます。

始める前に

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

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

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

ステップ 2 Locate the device whose role you want to change, click the pencil icon under the **Device Role** column, and choose a role from the **Update Device Role** dialog box. 有効な選択肢は、[Unknown] 、[Access] 、[Core] 、[Distribution] 、または [Border Router] です。

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

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

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

デバイスの管理 IP アドレスの更新

デバイスの管理 IP アドレスを更新することができます。

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

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

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

ステップ 2 更新するデバイスを選択します。

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

[Edit Device] ダイアログボックスが表示されます。

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

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

次のタスク

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

デバイスポーリング間隔の更新

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

デバイスにポーリングさせない場合は、ポーリングを無効にできます。

始める前に

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

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

ステップ 2 更新するデバイスを選択します。

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

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

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

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

ステップ 6 [更新（Update）] をクリックします。

デバイス情報の再同期

選択したデバイスのデバイス情報は、再同期間隔の構成にかかわらず、ただちに再同期できます。同時に最大 40 台のデバイスを再同期することができます。

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

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

ステップ 2 関連する情報を収集するデバイスを選択します。

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

ステップ 4 [OK] をクリックします。

ネットワーク デバイスの削除

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

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

始める前に

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

ステップ 1 メニューアイコン（☰）をクリックして、**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。[Inventory] ウィンドウには、**ディスカバリ**プロセス中に収集されたデバイス情報が表示されます。

ステップ 2 削除するデバイスの横にあるチェックボックスをオンにします。

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

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

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

ステップ 5 [OK] をクリックして、アクションを確認します。

コマンド ランナーを起動（インベントリ）

[Inventory] ウィンドウで選択したデバイスのコマンド ランナー アプリケーションを起動できます。

始める前に

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

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

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

ステップ 2 コマンドを実行するデバイスを選択します。

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

実行可能なコマンドの詳細、およびこれらのコマンドの実行方法については、デバイスの診断コマンドを実行 （387 ページ）を参照してください。

Run コマンドを使用したデバイスの到達可能性の問題のトラブルシューティング

[Inventory] ウィンドウから [Run Commands] ウィンドウを起動し、ping、traceroute、snmpget などのプラットフォームコマンドを実行して、デバイス到達可能性の問題をトラブルシューティングできます。

（注） Cisco DNA Center クラスタでプラットフォームコマンドを直接実行する場合は、[Run Commands] を起動する前にデバイスを選択しないでください。そうしないと、プラットフォームではなくそのデバイスに対してコマンドが実行されます。

始める前に

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

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

ステップ 2 [Actions] ドロップダウンリストから、**[Others]** > **[Run Commands]** の順に選択します。

man を入力すると、現在サポートされているコマンドおよびショートカットのリストをいつでも取得できます。

CSV ファイルを使用したデバイス設定のインポート/エクスポート

CSV ファイルのインポート

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

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

CSV ファイルでクレデンシャル プロファイルを指定し、対応する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て、CSV ファイルに手動で値も入力する場合、手動入力されたクレデンシャルが優先され、デバイスは手動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管理されます。たとえば、手動で入力した SNMP ログイン情報に加えて、SNMP および SSH または Telnet のログイン情報を含むログイン情報プロファイルが CSV ファイルに含まれている場合、デバイスは手動で入力された SNMP ログイン情報とログイン情報プロファイル内の SSH または Telnet ログイン情報に基づいて管理されます。Telnet は非推奨です。

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

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

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

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

- デバイスのIPアドレス
- SNMPバージョン
- SNMP読み取り専用コミュニティ ストリング
- SNMP書き込みコミュニティ ストリング
- SNMP再試行値
- SNMPタイムアウト値
- Protocol
- CLIユーザー名
- CLIパスワード
- CLIイネーブル パスワード
- CLIタイムアウト値

CSV ファイル エクスポート

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

CSV ファイルからのデバイス設定のインポート

CSV ファイルからデバイス設定をインポートできます。

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

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

ステップ 2 [Actions] ドロップダウンリストから、[Inventory] > [Import Inventory] > を選択してデバイスのログイン情報をインポートします。

ステップ 3 [Bulk Import] ダイアログボックスのボックスエリアに CSV ファイルをドラッグアンドドロップするか、点線のボックスエリアをクリックして CSV ファイルを参照します。

ステップ 4 **[インポート (Import)]** をクリックします。

デバイスデータのエクスポート

選択したデバイスに関する特定のデータを CSV ファイルにエクスポートできます。CSV ファイルは圧縮されます。[Export] をクリックして、フィルタ処理されたデバイスまたはすべてのデバイスのデータをエクスポートします。

⚠

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

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

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

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

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

[Export Inventory] ダイアログボックスが表示されます。

ステップ 4 **[パスワード（Password）]** フィールドに、エクスポートされた CSV ファイルを暗号化するために使用するパスワードを入力します。

（注） エクスポートしたファイルを開くには、パスワードが必要です。

ステップ 5 確認のために暗号化パスワードをもう一度入力します。

ステップ 6 [Include SSH key information] チェックボックスをオンにして、最初の SSH 鍵、最初の SSH 鍵アルゴリズム、現在の SSH 鍵、現在の SSH 鍵アルゴリズムなどの情報をエクスポートした CSV ファイルに追加します。

ステップ 7 [Export] をクリックします。

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

デバイスのクレデンシャルのエクスポート

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

⚠

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

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

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

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

ステップ 3 [Actions] ドロップダウンリストから **[Inventory]** > **[Export Inventory]** を選択します。

[Export] ダイアログボックスが表示されます。

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

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

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

（注） エクスポートしたファイルを開くには、パスワードが必要です。

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

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

デバイスの構成ドリフトの表示

デバイスで行った構成の変更は、内部 Cisco DNA Center サーバーに保存されます。外部 Cisco DNA Center からデバイスに加えられた設定変更に関する詳細情報を表示できます。

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

ステップ 2 デバイス名をクリックします。

[Device Details] ウィンドウが表示されます。

ステップ 3 左ペインで、[Config Drift] を選択します。

[Configuration Changes] ウィンドウには、保存された構成ドリフトの数が表示されます。これには、ラベル付きの設定と構成ドリフトバージョンが含まれます。

ステップ 4 [Change History] タブを展開して、次の詳細を表示します。

a) [Config drift date range]：[Start Date] と [End date] をクリックして、構成ドリフトを表示する日付範囲を選択します。デフォルトでは、開始日と終了日は、過去 15 日間の構成ドリフトを表示するように設定されています。

b) [Config drift timeline graph]：選択した日付範囲の構成ドリフトを表示します。デフォルトでは、過去 15 日間の構成ドリフトがタイムライングラフに表示されます。

タイムライングラフには、次の詳細が表示されます。

- [In-band Config Drift]：Cisco DNA Center によって行われた設定変更は、タイムライングラフに青いバブルとして表示されます。
- [Out-of-band Config Drift]：Cisco DNA Center の外で行われた設定変更は、タイムライングラフに紫色のバブルとして表示されます。
- [Labeled Config]：ラベル付きで Cisco DNA Center にアーカイブされた設定バージョンは、タイムライングラフにオレンジ色のバブルとして表示されます。詳細については、「構成ドリフトのラベル付け」を参照してください。

c) [Config Drift Version]：下矢印をクリックして、使用可能なすべての構成ドリフトバージョンを表示します。

d) [Running Config]：タイムライングラフの構成ドリフトをクリックします。比較が [Running Config] タブに表示されます。設定バージョン間の違いは、見やすくするために異なる色でマークされています。

構成ドリフトのラベル付け

将来の参照のために、時系列グラフで構成ドリフトにラベルを付けることができます。

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

ステップ 2 [Inventory] ウィンドウで、デバイス名をクリックすると、デバイスの詳細が表示されます。

ステップ 3 左側のペインから、[Config Drift] タブを選択します。[Configuration Changes] ウィンドウが表示されます。

ステップ 4 ラベルを付ける時系列グラフの構成ドリフトを選択します。選択した構成ドリフトのタイムスタンプは、時系列グラフの下の [Config Drift Version] に表示されます。

ステップ 5 選択した構成ドリフトバージョンに対応する [Label Config] をクリックします。

ステップ 6 [Label Configuration] ウィンドウで、設定バージョンの名前を入力します。ラベル設定のプレフィックスは CCA_ に固定されています。

（注） 設定バージョン名に特殊文字を使用しないでください。

ステップ 7 **[Save]** をクリックします。ラベル付きの構成ドリフトは、時系列グラフでオレンジ色で表示されます。

ラベル付けされた設定バージョンの数が選択した範囲より大きい場合は、保存される構成ドリフトの合計数を変更します。保存する構成ドリフトの数を設定する方法の詳細については、*Cisco DNA Center* 管理者ガイドの「Configure Device Configuration Backup Settings」のセクションを参照してください。

ステップ 8 ラベルを削除するには、ラベル付きの設定バージョンを選択し、[Remove label] をクリックします。

故障したデバイスの交換

ネットワーク内で障害が発生したデバイスを交換することは、デバイスのライフサイクル管理の重要な部分です。Cisco DNA Center の返品許可（RMA）ワークフローにより、障害が発生したデバイスを迅速に交換できるため、生産性が向上し、運用コストが減少します。RMA では、ルータ、スイッチ、および AP を共通のワークフローに従って交換できます。

ルータおよびスイッチで RMA ワークフローを使用すると、ソフトウェアイメージ、構成、およびライセンスが、障害が発生したデバイスから交換用デバイスに復元されます。ワイヤレス AP の場合、交換用デバイスは同じサイトに割り当てられ、プライマリワイヤレスコントローラ、RF プロファイル、および AP グループ設定でプロビジョニングされ、障害が発生した AP と同じ Cisco DNA Center のフロアマップの場所に配置されます。

（注） **デバイス交換**ワークフローを使用して、故障したデバイスを交換することもできます。詳細については、デバイスの交換ワークフロー （805 ページ）を参照してください。

始める前に

- 故障したデバイスのソフトウェア イメージ バージョンをイメージリポジトリにインポートしてから、交換するデバイスにマークを付ける必要があります。
- 故障したデバイスは到達不能な状態になっている必要があります。

- 交換用デバイスがプラグアンドプレイ（PnP）で Cisco DNA Center をオンボードしている場合は、故障したデバイスをユーザー定義のサイトに割り当てる必要があります。
- RMA ワークフローのトリガー中は、交換用デバイスがプロビジョニング状態であってはなりません。

ステップ 1 故障したデバイスを交換対象としてマークするには、次の手順を実行します。

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

[Inventory] ウィンドウには、検出プロセス中に収集されたデバイス情報が表示されます。

b) 交換する故障したデバイスを選択します。

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

d) [Mark For Replacement] ウィンドウで、[Mark] をクリックします。

（注） ファブリックデバイスのシームレスな交換を実現するために、DHCP サーバーがネイバーデバイスで設定されます。これは、PnP でデバイスを Cisco DNA Center にオンボードするために、交換用デバイスに IP アドレスを割り当てるために必要です。この DHCP サーバーは、故障したデバイスが正常に交換されると削除されます。

障害のあるデバイスからの最新の構成変更は、RMA ワークフロー中に交換後のデバイスにプッシュされます。

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

交換用としてマークされたデバイスのリストが表示されます。

f) （任意） デバイスを交換しない場合は、デバイスを選択して、**[Actions]** > **[Unmark for Replacement]** を選択します。

ステップ 2 （任意） デバイスを交換するには、次の手順を実行します。

a) 交換するデバイスを選択し、**[Actions]** > **[Replace Device]** を選択します。

b) [Choose Replace Device] ウィンドウで、[Unclaimed] タブまたは [Managed] タブから交換用デバイスを選択します。

[Unclaimed] タブには、PnP によってオンボードされたデバイスが表示されます。[Managed] タブには、インベントリまたは検出プロセスによってオンボードされたデバイスが表示されます。

c) （任意） 交換用デバイスがまだオンボードされていない場合は、次の手順を実行します。

1. [Choose Replace Device] ウィンドウで、[Add Device] をクリックします。
2. [Add New Device] ウィンドウで、デバイスの**シリアル番号**を入力し、[Add New Device] をクリックします。

または

1. [Choose Replace Device] ウィンドウで、[Sync with Smart Account] をクリックします。

2. [Sync with Smart Account] ウィンドウで、[Sync] をクリックします。

d) [Next] をクリックします。

e) [Schedule Replace] ウィンドウで、[Now] をクリックしてデバイスの交換をただちに開始するか、[Later] をクリックして特定時間でのデバイスの交換をスケジュールします。

交換用デバイスがまだオンボードされていない場合、[Now] オプションは無効になります。[Later] をクリックして特定時間でのデバイスの交換をスケジュールすることは可能です。

f) [Review] をクリックして、選択したデバイスタイプ、故障したデバイスの詳細情報、および交換用デバイスの詳細情報を確認します。

g) [Next] をクリックして [Summary] ウィンドウで詳細情報を確認します。

h) [Summary] ウィンドウで、次の手順を実行します。

1. 前の手順で選択したデバイスタイプ、故障したデバイス、または交換用デバイスを変更する場合は、[Edit] をクリックします。
2. [Replacement Device] で、[View] をクリックして、交換用デバイスの設定を確認します。
3. [置換（Replace）] をクリックします。

i) [Click Monitor Replacement Status] をクリックして [Provision] ウィンドウの [Mark for Replacement] ビューに移動します。

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

- （PnP）交換用デバイスを請求します。
- 交換用デバイスにソフトウェアイメージを配信してアクティブ化します。
- ライセンスを展開する。
- VLAN 構成をプロビジョニングします。
- スタートアップ構成をプロビジョニングします。
- 交換用デバイスをリロードします。
- 交換用デバイスの到達可能性を確認します。
- 交換用デバイスに SNMPv3 ログイン情報を展開します。
- 交換用デバイスを同期します。
- 故障したデバイスを CSSM から削除します。
- 交換用デバイスを CSSM に追加します。
- PKI 証明書を失効化して作成します。
- Cisco ISE を更新します。
- 障害のあるデバイスを削除します。

ワークフローが完了すると、[Replace Status] が [Replaced] に更新されます。

k) エラーメッセージが表示された場合は、エラーリンクをクリックします。

l) [Retry] をクリックして、故障したデバイスと交換用デバイスの同じ組み合わせを使用してワークフローを再トリガーします。

（注） [Main Inventory] ウィンドウには、故障したデバイスと交換した新しいデバイスの詳細情報が表示されます。

デバイスを交換対象としてマーキングする先行タスクと、デバイスを交換するタスクは、異なるタイミングで実行できます。

障害のあるアクセスポイントの交換

AP の RMA 機能を使用して、障害のある AP をデバイスインベントリに登録されている交換用 AP に交換できます。

始める前に

- AP の返品許可（RMA）機能では、同等の交換のみをサポートしています。モデル番号と PID が障害のある AP と同じ交換用 AP を用意する必要があります。
- 交換用 AP を障害のある AP と同じ シスコ ワイヤレス コントローラに接続しておく必要があります。
- ワイヤレスコントローラとして機能する Cisco Mobility Express AP は、交換用 AP の候補ではありません。
- 障害のある AP のソフトウェア イメージ バージョンをイメージリポジトリにインポートしてから、交換用デバイスにマークを付ける必要があります。
- 交換用デバイスがプラグアンドプレイ（PnP）で Cisco DNA Center をオンボードしている場合は、故障したデバイスをユーザー定義のサイトに割り当てる必要があります。
- RMA ワークフローのトリガー中は、交換用 AP がプロビジョニング状態であってはなりません。
- 故障したデバイスは到達不能な状態になっている必要があります。

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

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

ステップ 2 交換する故障した AP のチェックボックスをオンにします。

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

ステップ 4 [Mark For Replacement] ウィンドウで、障害のあるデバイス名の横にあるオプションボタンをクリックします。

ステップ 5 [Actions] ドロップダウンリストから、**[Replace Device]** を選択します。

ステップ 6 [Replace Device] ウィンドウで、[Start] をクリックします。

ステップ 7 [Available Replacement Devices] テーブルで、交換用デバイスの名前の横にあるオプションボタンをクリックします。

ステップ 8 **[次へ (Next)]** をクリックします。

ステップ 9 [Replacement Summary] を確認し、[Next] をクリックします。

ステップ 10 [Schedule Replacement] ウィンドウで、デバイスを今すぐ交換するか、後で交換を行うようスケジュールするかを選択し、[Submit] をクリックします。

RMA ワークフローが開始されます。

ステップ 11 交換ステータスをモニターするには、[What's Next] で [Monitor Replacement Status] をクリックします。

[Mark For Replacement] ウィンドウに、交換用としてマークされているデバイスのリストが表示されます。

[Replace Status] 列で交換のステータスを確認します。当初は [In-Progress] と表示されます。

ステップ 12 [Replace Status] 列の [In-Progress] をクリックします。

[Replace Status] タブには、デバイス交換の一環として Cisco DNA Center で実行されるさまざまな手順が表示されます。

ステップ 13 [Marked for Replacement] ウィンドウで、[Refresh] をクリックしてから [Replace Status] をクリックして交換ステータスを確認します。

故障した AP の交換が失敗すると、[Replace Status] 列にエラーメッセージとともに失敗した理由が表示されます。

故障した AP を別の新しい AP に交換するか、AP RMA 再試行機能を使用して失敗した交換を再試行できます。

ステップ 14 失敗した交換を再試行するには、デバイス名の [Replace Status] 列のエラーメッセージをクリックします。

ステップ 15 [Retry] をクリックします。

ステップ 16 [Marked for Replacement] ウィンドウで、[Replace Status] 列の [In-Progress] をクリックします。

故障した AP が正常に交換されると、[Replace Status] タブに成功と表示されます。

ステップ 17 故障したデバイスが正常に交換されると、[Replacement History] ウィンドウの [Replace Status] に [Replaced] と表示されます。

ステップ 18 （オプション）デバイスを交換しない場合は、デバイスを選択し、**[Actions]** > **[Unmark for Replacement]** の順に選択します。

Cisco DNA Center での RMA ワークフローの制限事項

- RMA は、類似デバイスの交換のみサポートしています。たとえば Cisco Catalyst 3650 スイッチは、別の Cisco Catalyst 3650 スイッチとのみ交換できます。また、故障したデバイスと交換用デバイスのプラットフォーム ID も同じである必要があります。
- RMA は、以下を除くすべてのスイッチ、ルータ、および Cisco SD-Access デバイスの交換をサポートします。
  - ワイヤレスコントローラが組み込まれたデバイス
  - シスコ ワイヤレス コントローラについて
  - シャーシベース Nexus 7700 シリーズ スイッチ
  - スイッチスタック（ハードウェアスタッキングおよび SVL スタッキング）
- RMA は、外部 SCEP ブローカ PKI 証明書を使用するデバイスをサポートします。RMA ワークフロー中に、交換デバイス用に PKI 証明書が作成および認証されます。交換した障害のあるデバイスの PKI 証明書は、証明書サーバーから手動で削除する必要があります。
- RMA ワークフローでは、次の場合にのみデバイスの交換が可能です。
  - 障害のあるデバイスと交換用デバイスの両方に同じ拡張カードが搭載されている。
  - 両方のデバイスのポート数が拡張カードによって変わらない。
  - 障害のあるデバイスは、Cisco DNA Center によって静的 IP で管理されます（RMA は、拡張ノードおよびファブリック内の AP を除く、Cisco DNA Center によって DHCP IP で管理されるデバイスではサポートされません）。
- ネイバーデバイスがファブリックの一部でない場合、ファブリックエッジの交換ではネイバーデバイスの DHCP サーバー設定はサポートされていません。中間ノードは Cisco SD-Access ファブリックの一部ではないため、オプション 43 の DHCP サーバーはプッシュされません。
- 交換用デバイスが、障害のあるデバイスが接続されていたポートと同じポートに接続されていることを確認してください。
- Cisco DNA Center レガシーライセンスの導入はサポートされていません。

  RMA ワークフローにより、Cisco SSM から障害のあるデバイスの登録が解除され、交換用デバイスが Cisco SSM に登録されます。
  - 障害のあるデバイスにインストールされているソフトウェアイメージが Cisco IOS XE 16.8 よりも前のバージョンの場合、[License Details] ウィンドウにはネットワークと機能のライセンスの詳細が表示されず、警告メッセージも表示されません。そのため、障害のあるデバイスに設定されているレガシー ネットワーク ライセンスを確認し、交換用デバイスに同じレガシー ネットワーク ライセンスを手動で適用する必要があります。

- 故障したデバイスにインストールされているソフトウェアイメージが Cisco IOS XE 16.8 以降の場合は、[License Details] ウィンドウにネットワークライセンスの詳細（**レガシー**、**ネットワーク**など）と機能ライセンス（IP Base、IP Service、LAN Base など）が表示されます。障害のあるデバイスを交換対象としてマークしている際に、次の警告メッセージが表示されます。

  ```
  Some of the faulty devices don't have a Cisco DNA license. Please
  ensure your replacement device has the same Legacy license of
  the faulty device enabled.
  ```

- 交換用デバイスと障害のあるデバイスのレガシー ネットワーク ライセンスが一致しない場合は、ライセンスの展開中に次のエラーメッセージが表示されます。

  ```
  Cisco DNA Center doesn't support legacy license deployment.
  ```
  そのため、交換用デバイスで障害のあるデバイスのライセンスを手動で更新し、再同期してから続行してください。

- Cisco DNA Center は、ファブリックネットワークでの交換デバイスの PnP オンボーディングをサポートします。ただし、次の場合を除きます。
  - 障害のあるデバイスが複数のインターフェイスを使用してアップリンクデバイスに接続されている。
  - 重複プールを使用したローカルエリアネットワーク（LAN）自動化。
- 交換用デバイスが PnP DHCP 機能によってオンボードされる場合は、リロードのたびにデバイスが同じ IP アドレスを取得し、DHCP のリースタイムアウトが 2 時間を超えていることを確認してください。

アクセス ポイントのリブート

AP の再起動機能を使用すると、トラブルシューティングとメンテナンスのために 1 つ以上の AP を再起動できます。

始める前に

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

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

ステップ 2 再起動する AP のチェックボックスをオンにします。

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

ステップ 4 [Reboot Device] スライドインペインで、AP を今すぐ再起動するか、後で再起動をスケジュールするよう求められます。

- AP を今すぐ再起動するには、[Now] オプションボタンをクリックし、再起動タスクの名前を入力します。

- 後で再起動をスケジュールするには、[Later] オプションボタンをクリックし、タスクの名前を入力して、再起動の日時を定義します。

ステップ 5 [Selected Devices] を展開して、再起動 AP の AP 名とフロアの詳細を表示します。

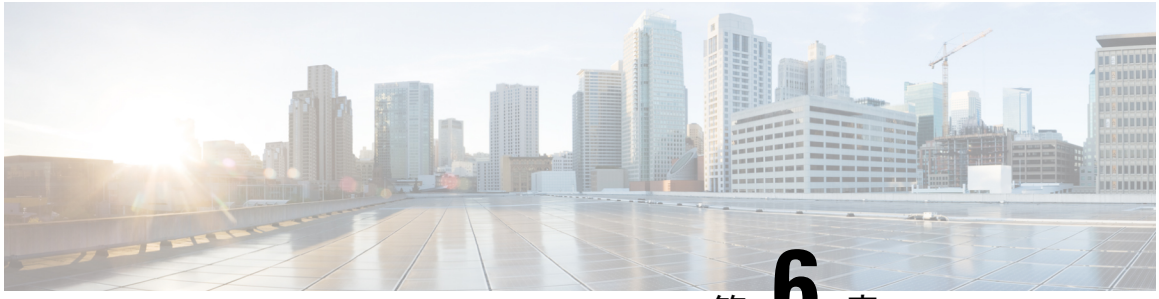
ステップ 6 [Reboot] をクリックします。

シスコ ワイヤレス コントローラ が選択した AP の再起動を開始すると、「`Reboot Initiated Successfully`」というメッセージが表示されます。

ステップ 7 [Task Submitted] ポップアップで、[Task] リンクをクリックします。

[Task Submitted] ポップアップが表示されなかった場合は、[Menu] アイコン（☰）をクリックし、**[Activities]** > **[Tasks]** の順に選択します。

ステップ 8 [AP Reboot] で、AP の再起動タスク名をクリックして、再起動の開始ステータスを表示します。



第 6 章

ネットワーク トポロジを表示

トポロジについて

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

トポロジ マップを使用すると、次のことができます。

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

- Virtual Routing and Forwarding（VRF）機能を使用してデバイスをフィルタ処理する。
- トポロジ マップにデバイスをピン留めする
- トポロジ マップ レイアウトの保存
- トポロジ マップ レイアウトを開く
- トポロジ レイアウト全体のスクリーンショットを PNG 形式でエクスポートする。

エリア、サイト、ビルディング、フロアのトポロジを表示

エリア、サイト、ビルディングまたはフロアのトポロジを表示できます。

始める前に

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

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

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

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

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

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

（注）

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

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

トポロジ マップでデバイスをフィルタリング

次のいずれかの属性に基づいてデバイスをフィルタ処理できます。

- VLAN
- Routing
- VRF
- タギング

始める前に

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

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

ステップ 2 [Filter] をクリックします。

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

ステップ 3 次のいずれかを実行します。

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

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

また、次の手順を実行して、デバイスをタグに関連付けることもできます。

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

デバイス情報の表示

Cisco DNA Center では、デバイス名、IP アドレス、およびデバイスのソフトウェアバージョンを表示できます。

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

始める前に

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

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

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

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

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

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

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

（注） ネットワークデバイスが Cisco DNA Center 内で Cisco Discovery Protocol（CDP）を使用して設定されていない場合、トポロジは Link Layer Discovery Protocol（LLDP）を使用してネイバーデバイスを決定します。

リンク情報の表示

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

始める前に

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

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

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

ステップ 3 興味のあるリンクにカーソルを合わせます。

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

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

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

（注） トポロジでは、Link Layer Discovery Protocol（LLDP）を使用して、Cisco DNA Center で LLDP を使用して検出されたデバイスのリンクが決定されます。

トポロジ マップにデバイスをピン留めする

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

始める前に

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

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

- デバイスをピン留めするには、デバイス グループをクリックして、デバイス名の左にあるピンのアイコンをクリックします。
- すべてのデバイスをピン留めするには、デバイス グループをクリックして、ダイアログボックスで、[すべてピン留め（Pin All）] をクリックします。

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

サイトへのデバイスの割り当て

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

始める前に

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

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

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

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

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

ステップ 5 [**Assign**] をクリックします。

トポロジ マップ レイアウトの保存

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

始める前に

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

ステップ 1 メニューアイコン（☰）をクリックして、[Tools] > [Topology] の順に選択します。
ステップ 2 [Custom View] をクリックします。
ステップ 3 [表示タイトルの入力（Enter View Title）] フィールドに、カスタマイズしたマップの名前を入力します。
ステップ 4 **[Save]** をクリックします。
ステップ 5 （任意） カスタマイズしたマップをデフォルトとして設定するには、[Make Default] をクリックします。

トポロジ マップ レイアウトを開く

以前に保存したトポロジ マップを開くことができます。

始める前に

トポロジ マップ レイアウトが保存済みである必要があります。

ステップ 1 メニューアイコン（☰）をクリックして、[Tools] > [Topology] の順に選択します。
ステップ 2 [Custom View] をクリックします。
ステップ 3 表示するマップの名前をクリックします。

トポロジマップレイアウトの共有

カスタマイズしたマップを他のユーザーと共有できます。

始める前に

- トポロジマップレイアウトが保存済みである必要があります。
- 少なくとも 1 つのトポロジビューが保存済みである必要があります。

ステップ 1 メニューアイコン（☰）をクリックして、[Tools] > [Topology] の順に選択します。
ステップ 2 [Custom View] をクリックします。
ステップ 3 カスタムマップの名前にマウスカーソルを合わせて、[Share Focus] アイコンをクリックします。
ステップ 4 確認ウィンドウで [Yes] をクリックします。

トポロジのレイアウトをエクスポート

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

始める前に

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

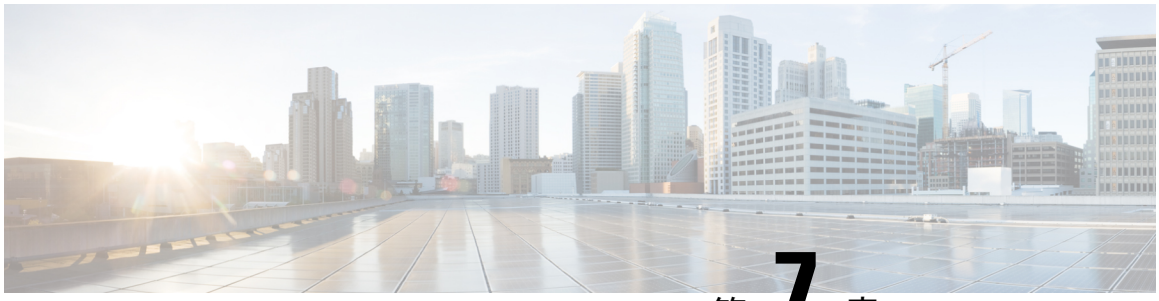
ステップ 1 メニューアイコン（≡）をクリックして、[Tools] > [Topology] の順に選択します。

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

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

第 III 部

ネットワークの設計



第 7 章

ネットワーク階層の設計

ネットワーク階層の概要

ネットワークの地理的な場所を表すネットワーク階層を作成できます。この階層構造により、デザインの設定や構成を特定の階層要素に簡単に適用できます。たとえば、デザインの設定をエリア全体に適用したり、床のみに適用したりすることができます。

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

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

- [Global]：他のすべての階層要素がその中に存在するデフォルトの要素。[Global] の直下に配置することが可能な要素は、エリアおよびサイトのみです。
- [Areas] と [Sites]：エリア（Area）とサイト（Site）は、[Global] または他のエリアやサイトに存在します。エリアとサイトには物理アドレスがありません。最大の要素として、地理的地域を識別します。エリアとサイトにより、エリアおよびサイトのグループ化が可能になります。
- [Buildings]：建物（Building）は、エリアまたはサイトに存在します。建物を作成する場合、物理アドレスまたは緯度と経度の座標を指定する必要があります。建物にエリアを含めることはできません。ただし、フロアを含めることはできます。

- [Floors]：フロア（Floor）は建物に存在します。壁や窓など、建物のさまざまなコンポーネントを含むマップの有無にかかわらず、建物にフロアを追加できます。フロアマップを使用する場合は、手動で作成するか、DXF、DWG、JPG、GIF、PNG、またはPDFを含むファイルタイプのファイルからインポートできます。次に、ワイヤレスデバイスをフロアマップに配置して、ワイヤレスネットワークのカバレッジを視覚化できます。

  プロビジョニングされていないデバイスのサイト階層は、フロアマップ上のAPの場所を維持したまま変更できます。ただし、既存のフロアを別の建物に移動できないことに注意してください。

開始するには、次のいずれかの方法を使用してネットワーク階層を構築します。

- 新しいネットワーク階層を作成する。詳細については、「新しいネットワーク階層の設計（156 ページ）」を参照してください。
- Cisco Prime Infrastructure または Ekahau Pro から既存のネットワーク階層をインポートする。詳細については、 の 既存の Cisco ネットワーク階層の使用 （156 ページ） または 既存の Ekahau ネットワーク階層の使用 （160 ページ）を参照してください。

新しいネットワーク階層の設計

[Design]領域では、ネットワーク全体のデバイスに適用可能な物理トポロジ、ネットワーク設定、デバイスのタイプやプロファイルなど、ネットワークの構造とフレームワークを作成します。既存のインフラストラクチャがない場合は、設計ワークフローを使用します。既存のインフラストラクチャがある場合は、**ディスカバリ**機能を使用します。詳細については、「検出の概要 （45 ページ）」を参照してください。

これらのタスクは、[Design] 領域で実行します。

ステップ 1 ネットワーク階層を作成します。詳細については、ネットワーク階層のサイトの作成 （166 ページ）を参照してください。

ステップ 2 グローバル ネットワーク設定を定義します。詳細については、ネットワーク設定の概要 （227 ページ）を参照してください。

ステップ 3 ネットワーク プロファイルを定義します。詳細については、ネットワークプロファイルの概要 （297 ページ）を参照してください。

既存の Cisco ネットワーク階層の使用

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

次の情報を使用して、ネットワーク階層を再作成できます。

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

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

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

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

FIPS モードは、マップアーカイブのエクスポートとインポートに次の影響を与えます。

FIPS モードが有効な場合：

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

FIPS モードが無効な場合：

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

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

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

始める前に

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

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

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

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

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

CSV ファイルがダウンロードされます。

Cisco Prime Infrastructure からのマップアーカイブのエクスポート

Cisco Prime Infrastructure からマップアーカイブファイルをエクスポートし、それらを Cisco DNA Center にインポートできます。マップアーカイブには、フロア寸法などのマップ情報と Cisco Prime Infrastructure の各フロアに適用されている無線周波数（RF）減衰モデルなどのキャリブレーション情報が含まれています。

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

ステップ 2 **[エクスポート（Export）]** ドロップダウン リストから **[マップ アーカイブ（Map Archive）]** を選択します。

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

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

ステップ 4 次のオプションの少なくとも 1 つを選択します。

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

  キャリブレーション情報を含めることを選択した場合は、次のように、選択したマップの情報を含めるか、すべての情報を含めるかを指定する必要もあります。

  - [Calibration Information for selected maps]：選択したサイトマップのキャリブレーション情報がエクスポートされます。
  - [All Calibration Information]：選択したマップに加えて、システムで使用可能なその他のキャリブレーション情報もエクスポートされます。

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

次のメッセージは、操作の進行状況を示しています。

```
Exporting data is in progress
```

TAR ファイルが作成され、ローカルマシンに保存されます。

ステップ 6 [Done] をクリックします。

Cisco DNA Center へのサイト階層のインポート

Cisco Prime Infrastructure から CSV ファイルとしてエクスポートしたサイト階層をインポートできます。サイト階層のエクスポートについては、Cisco Prime Infrastructure からのサイト階層のエクスポート （157 ページ）を参照してください。

始める前に

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

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

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

ステップ 3 ダイアログボックスで、次のいずれかのオプションボタンをクリックします。

- [Merge with Existing Sites]：ダウンロードしたサイト情報を既存のサイト情報と結合します。
- [Overwrite Existing Sites]：Cisco DNA Center に同じサイトがすでに存在する場合、既存のサイト情報はダウンロードしたサイト情報で上書きされます。

ステップ 4 ダイアログボックスで、CSV ファイルをダウンロードエリアにドラッグアンドドロップします。または、[Choose a file] をクリックして CSV ファイルの場所に移動し、[Upload] をクリックすることもできます。

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

Cisco DNA Center へのマップアーカイブのインポート

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

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

サイト階層のエクスポートについては、「Cisco Prime Infrastructure からのマップアーカイブのエクスポート （158 ページ）」を参照してください。

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

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

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

ステップ 4 [Import] をクリックします。

マップアーカイブファイルがインポートされます。

既存の Ekahau ネットワーク階層の使用

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

Ekahau プロジェクトのエクスポート

Ekahau Pro からネットワーク階層をエクスポートし、さらに計画するために Cisco DNA Center にインポートできます。

ステップ 1 Ekahau Pro ツールでフロアレイアウトを計画します。

- ビルディングとフロアを作成します。

  Ekahau Pro ツールでビルディングを作成することは必須ではありません。

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

- ビルディングの座標を追加します。
- サイト名を定義します。

  ここで指定した AP 名は、ワイヤレスコントローラ の設定中に、シスコ ワイヤレス コントローラ の AP 名を更新するために使用されます。
- 障害物を追加します。
- プロジェクトをエクスポートします。

  （注） Ekahau Cloud を使用している場合、Ekahau Cloud プロジェクトをエクスポートする前に、ローカルの変更を Ekahau Cloud に同期してください。Ekahau プロジェクトに、Ekahau Cloud プロジェクトと同期していないローカルの変更（AP やウォールの削除など）がある場合、Cisco DNA Center への Ekahau プロジェクトのインポートが失敗する可能性があります。

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

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

ステップ 3 Cisco DNA Center で、シスコ ワイヤレス コントローラを構成します。

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

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

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

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

始める前に

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

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

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

（注） 詳細については、ネットワーク階層のサイトの作成（166ページ）、建物の追加（167ページ）、および建物への基本フロアの追加（169 ページ）を参照してください。

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

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

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

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

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

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

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

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

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

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

[Assign Planned APs] パネルが表示されます。

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

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

ステップ 9 [Save] をクリックします。

Ekahau サイト調査の Cisco DNA Center へのインポート

Ekahau サイト調査をアップロードして、ネットワーク階層に建物とフロアを作成できます。サイト調査には、ワイヤレスデバイスが割り当てられているサイト、建物、フロア、およびフロアマップ上の位置など、ワイヤレスデバイスに関する情報が含まれます。ただし、AP アンテナ情報は含まれません。そのため、CSV ファイルを使用してこの情報を個別にアップロードする必要があります。

Cisco DNA Center には、ダウンロードして編集して必要な AP アンテナ情報を定義できる CSV テンプレートファイルが含まれています。CSV ファイルには、次のフィールドとデフォルトが含まれています。

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

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

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

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

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

または、左側のペインで [Global] または親サイトの横にある省略記号 ••• にカーソルを合わせ、[Add Area] を選択することもできます。詳細については、ネットワーク階層のサイトの作成 （166 ページ）を参照してください。

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

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

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

（注） CSV ファイルがない場合は、[Download AP Mapping Template] をクリックして、編集可能な CSV ファイルをダウンロードして、アップロードすることができます。

ステップ 6 [Import] をクリックします。

ファイルが正常にダウンロードされると、成功メッセージが表示されます。

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

詳細を表示するには、デバイスにカーソルを合わせます。

Cisco DNA Center からのネットワーク階層のエクスポート

サイト階層を CSV 形式のファイルにエクスポートできます。完全なネットワークマップ（グローバル階層）、またはサイト、建物、フロアの階層をエクスポートすることもできます。Cisco Prime Infrastructure または Ekahau Pro 形式のいずれかを選択できます。ネットワーク階層をこれらの形式にエクスポートすると、これらのツールでネットワーク階層を引き続き操作できます。

Cisco DNA Center からのサイト階層のエクスポート

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

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

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

ステップ 3 [Export Sites] ダイアログボックスで [OK] をクリックします。

Cisco DNA Center からのマップアーカイブのエクスポート

完全なネットワークマップ（グローバル階層）、またはサイト、建物、フロアの階層を Cisco Prime Infrastructure または Ekahau Pro 形式のいずれかにエクスポートすることができます。最大 500 のフロアをエクスポートできます。

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

FIPS モードは、マップアーカイブのエクスポートとインポートに次の影響を与えます。

FIPS モードが有効な場合：

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

FIPS モードが無効な場合：

- エクスポートされるマップアーカイブは暗号化されます。

- 暗号化されたマップアーカイブと暗号化されていないマップアーカイブの両方をインポートできます。

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

ステップ 2 完全なネットワークマップをエクスポートするには、マップツールバーの [Export] をクリックし、[Export Maps] を選択します。

あるいは、左側のペインで、サイト、建物、またはフロアの横にある省略記号（...）にカーソルを合わせ、[Export Maps] を選択します。

エクスポートされる情報は、選択内容によって異なります。

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

ステップ 3 [Export Maps] ダイアログボックスで、[Ekahau Project] または [Prime] オプションボタンのいずれかをクリックします。

ステップ 4 [Export] をクリックします。

ネットワーク階層の検索

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

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

階層は、検索フィールドに入力したテキストに基づきフィルタリングされます。

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

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

   フィルタ基準に基づいて、階層がフィルタリングされます。

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

ネットワーク階層でのサイトの管理

ネットワーク階層のサイトの作成

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

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

世界地図が右側のペインに表示されます。

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

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

ステップ 3 [Area Name] フィールドに、サイト名を入力します。

ステップ 4 [Parent] ドロップダウンリストから、親ノードを選択します。[Global] がデフォルトの親ノードです。

ステップ 5 [Add]をクリックします。

左側ペインの親ノードにサイトが作成されます。

サイトの編集

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

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

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

ステップ 4 [Update] をクリックして変更を保存します。

サイトの削除

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

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

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

ネットワーク階層でのビルディングの管理

建物の追加

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

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

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

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

a) [Building Name] フィールドに建物の名前を入力します。

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

c) [Address] フィールドにアドレスを入力します。

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

ステップ 4 [Add] をクリックします。

左側ペインの親サイトに建物が作成され、表示されます。

ビルディングの編集

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

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

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

ステップ 4 [Update] をクリックして変更を保存します。

ビルディングの削除

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

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

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

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

ネットワーク階層でのフロアの管理

フロアとフロアマップの概要

Cisco DNA Center で建物にフロアとフロアマップを追加する理由はいくつかあります。理由の 1 つは、ワイヤレスネットワークを現在の状態で表示することです。もう 1 つの理由は、将来の変更の計画と視覚化を支援するためです。

壁や窓などのさまざまな建物コンポーネントを含むフロアマップを作成またはインポートし、その上にワイヤレスデバイスを配置することで、ワイヤレスネットワークを視覚化できます。Cisco DNA Center では、フロアプランを使用して、カバレッジエリア内の RF 信号の相対強度を示す 2D および 3D ヒートマップを計算します。2D ワイヤレスマップの場合、このヒートマップは、石壁や金属の物体など、ビルディングのさまざまな素材の減衰は考慮されておらず、RF信号が障害物に跳ね返る影響も表示されないため、実際のRF信号強度の近似値に過ぎません。いずれの場合も、既存のフロアプランを含むファイルをインポートして開始することをお勧めします。

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

インタラクティブ フロア プランニングにより、次のことが可能になります。

- キャンバスとしてラスターまたは CAD フロアプランを使用してフロアレイアウトを作成する。

- 信号カバレッジ要件に基づいて、計画された AP または仮想 AP をフロアマップに配置する。これらの仮想 AP または計画された AP は、Cisco DNA Center によってまだインストールまたは検出されていません。
- アンテナのタイプと方向を割り当てる。
- 信号の減衰に影響を与える壁や棚などの障害物をフロアに描画する。
- すべての AP を順番に計画する。
- フロアマップを PDF としてエクスポートする。

建物への基本フロアの追加

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

建物に基本フロアを追加するには、次の手順を使用します。

CAD、非 CAD、または Ekahau ファイルのフロアマップを含むフロアを追加するには、次のいずれかのトピックを参照してください:

- CAD マップファイルを使用したフロアの追加 （171 ページ）
- CAD 以外のマップファイルを使用したフロアの追加 （172 ページ）
- Cisco DNA Center への Ekahau プロジェクトのインポート （161 ページ）

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

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

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

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

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

ステップ 5 [Add] をクリックします。

マップファイルを使用したフロアの追加

フロアを作成するときに、同時にフロアマップを含めることができます。次のトピックは、使用するフロアマップファイルタイプに応じたさまざまなフロア作成方法を理解するのに役立ちます。各方法の手順も記載されています。

フロアマップの作成方法

ワイヤレスマップを表示するには、まずフロアプランを作成するかインポートする必要があります。

- **フロアマップを作成する**：フロアマップを最初から作成するには、壁や棚などのすべてのフロア要素を手動で作成して、それらがワイヤレスマップに表示されるようにする必要があります。詳細については、2Dマップでのフロアマップ要素とオーバーレイの構成（177ページ）を参照してください。

- **CAD ファイルをインポートする**：CAD ファイル（DXF または DWG ファイルタイプ）を使用してフロアマップをインポートすると、Cisco DNA Center によって CAD レイヤがインポートされ、ワイヤレスマップでフロア要素として表示されるレイヤを指定できます。

  3D ヒートマップの計算にはかなりの計算能力が必要なため、ヒートマップの計算に大きく貢献する CAD レイヤーのみを含めることをお勧めします。正確なヒートマップを取得するのに十分な情報を含める必要がありますが、計算プロセスを過負荷にしてヒートマップの表示を遅らせる不必要な情報は含めないでください。

  Cisco DNA Center は、ヒートマップの生成にかかる時間を最小限に抑えるために、次の最初の手順を実行します。

  - 2D および 3D マップの壁の最大数を制限します。最適化後の 3D ヒートマップの最大壁数は 3000 です。CAD ファイルにそれ以上が含まれている場合は、Cisco DNA Center で警告が表示され、（壁の長さにその減衰を掛けたものに基づいて）最適な 3000 の壁が保持されます。

    最適化後の 2D ヒートマップの最大壁数は 300 です。CAD ファイルにそれ以上が含まれている場合は、Cisco DNA Center で警告が表示され、（壁の長さにその減衰を掛けたものに基づいて）最適な 300 の壁が保持されます。

  - 小さな障害物（0.75 フィート未満）と壁の 2 番目の側面を自動的に取り除き、壁ごとに 1 つの側面だけを残します。（Cisco DNA Center は、壁の各側面ではなく、壁ごとに減衰値を適用します。）

  インポートするレイヤーと要素を決定するときは、最も減衰が大きい障害物に注目してください。原則として、壁が長く厚くなればなるほど、減衰は大きくなります。キュービクルのような低い壁や、柱のような狭い壁では、減衰が少なく、ヒートマップへの影響はほとんどありません。障害物の材質が重い場合でも、信号は障害物の周囲を放射できるため、減衰は大きな影響を与えません。同様に、建物の外側のカバレッジに関心がない場合は、外壁や窓を含めないでください。そうすることで、建物の内部をより適切に 3D で可視化できます。

  CADファイルの特定のレイヤーに壁がないが、他の要素と混在している壁がある場合は、それらをインポート対象として選択しないでください。壁は後で手動で追加できます。詳細については、壁の追加、編集、および削除 （192 ページ）を参照してください。

  ブロック挿入とプロキシエンティティはインポートできません。インポートしたレイヤーには、ライン、ポリライン、アークなどのネイティブ要素のみが含まれるようにしてください。

手順については、CADマップファイルを使用したフロアの追加 （171 ページ）を参照してください。

- **CAD 以外の画像ファイルをインポートする**：JPG、GIF、PNG、または PDF ファイルを使用してフロアプランをインポートできます。通常、このタイプのファイルは2Dフロアマップの作成に使用されます。ただし、壁や棚などのフロア要素をワイヤレスマップに表示するには、それらを手動で作成する必要があります。手順については、CAD 以外のマップファイルを使用したフロアの追加 （172 ページ）を参照してください。
- **Ekahau Pro プロジェクトプランをインポートする**：障害物、AP などの Ekahau プロジェクトデータをインポートして、ワイヤレスマップを作成できます。手順については、Cisco DNA Center への Ekahau プロジェクトのインポート （161 ページ）を参照してください。

マップ内で使用するイメージファイルに関するガイドライン

マップイメージファイルを使用するには、次のガイドラインに従ってください。

- マップのイメージファイルを .jpg、.gif、.png、.pdf、.dxf、.dwg などの形式で保存できるグラフィカル アプリケーションを使用します。
- マップのイメージファイルのサイズはさまざまです。Cisco DNA Center は元のイメージをフル解像度でデータベースにインポートしますが、表示中は、ワークスペースに合わせてサイズが自動的に変更されます。
- インポートする前に、サイトの縦と横の寸法をフィートまたはメートル単位で取得してください。これにより、マップ インポート時にこれらの寸法を指定できます。
- 回転メタデータを持つフロアマップイメージは、CMX や Cisco DNA Spaces に同期したときに正しく表示されないことがあるため、使用しないようにします。フロアマップイメージは Cisco DNA Center でサポートされているフォーマットだとしても、特定のツールがメタデータを追加する方法によって、異なる方法でレンダリングされる可能性があります。たとえば、回転メタデータを含むイメージファイルを 3 つの異なるアプリケーションで開くと、2 つのアプリケーションでは水平にレンダリングされ、もう一方のアプリケーションでは垂直にレンダリングされる場合があります。

CAD マップファイルを使用したフロアの追加

ワイヤレスマップを表示するには、フロアマップを作成する必要があります。CAD ファイル（DXF または DWG ファイルタイプ）を使用して、フロアマップを作成できます。

2D フロアマップの場合、2D ビューに表示する CAD レイヤーを選択する必要があります。3D フロアマップの場合、Cisco DNA Center は CAD レイヤーを壁、棚、障害物、およびマップ内のその他の要素としてインポートします。

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

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

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

ステップ 4 [Type（RF Model）] ドロップダウンリストから、フロアに適用する RF モデルを選択します。RF モデルは、フロアの特性に基づいて RF を計算する方法を決定します。

ステップ 5 CAD ファイル（DXF または DWG ファイルタイプ）を [Floor Image] エリアにドラッグアンドドロップします。

（注） デフォルトでは、マップをインポートした後にオーバーレイは表示されません。そのため、フロアプランをインポートしたら、必ずオーバーレイ表示を有効にしてください。マップツールバーから、[View Options] をクリックします。右側のペインで [Overlay Objects] を展開し、表示する各オブジェクトのトグルボタンをクリックします。

ステップ 6 [Floormap] ダイアログボックスで、マップにフロア要素として表示する CAD レイヤを選択します。

a) [2D] 列で、2D ビューに表示する CAD レイヤーのチェックボックスをオンにします。

b) [3D Wall/Shelving Type] 列で、ドロップダウンリストを使用して、壁または棚のタイプを指定する CAD レイヤーを選択します。

（注） レイヤーを 3D ビューに表示するには、[3D Wall/Shelving Type] 値が必要です。壁/棚のタイプは、減衰とヒートマップの計算方法に影響します。詳細については、フロアマップの作成方法 （170 ページ）を参照してください。

c) [Use Selected Layers] をクリックします。

ステップ 7 [Width]、[Length]、および [Height] フィールドにフロアマップの寸法を入力します。

ステップ 8 [Add] をクリックします。

デフォルトでは、マップはグリッド付きで表示されます。グリッドのオンとオフを切り替えるには、マップの左下にある [Show Grid] トグルボタンを使用します。

（注） フロアプランをインポートしたら、必ずオーバーレイ表示を有効にしてください。（フロアから、[View Options] をクリックし、[Overlay Objects] でオーバーレイの切り替えを有効にします）。デフォルトでは、マップをインポートした後にオーバーレイは表示されません。

CAD 以外のマップファイルを使用したフロアの追加

CAD 以外のファイル（JPG、GIF、PNG、または PDF ファイルタイプ）を使用して、フロアマップを作成できます。ただし、CAD 以外のファイルを使用する場合、壁や棚などの 3D フロア要素はインポートできず、後で手動で追加する必要があります。詳細については、2D マップでのフロアマップ要素とオーバーレイの構成 （177 ページ）を参照してください。

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

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

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

ステップ 4 [Type（RF Model）] ドロップダウンリストから、フロアに適用する RF モデルを選択します。RF モデルは、フロアの特性に基づいて RF を計算する方法を決定します。

ステップ 5 CAD 以外のファイル（JPG、GIF、PNG、または PDF ファイルタイプ）を [Floor Image] 領域にドラッグアンドドロップします。

（注） フロアから画像の幅と高さの比率を抽出できないため、フロアの正確な寸法を PDF 形式で指定してください。

ステップ 6 [Add] をクリックします。

フロアマップが作成されます。

（注） フロアプランをインポートしたら、必ずオーバーレイ表示を有効にしてください。（フロアから、[View Options] をクリックし、[Overlay Objects] でオーバーレイの切り替えを有効にします）。デフォルトでは、マップをインポートした後にオーバーレイは表示されません。

ステップ 7 マップツールバーから、[Add/Edit] をクリックします。

ステップ 8 壁を 3D フロア要素として追加するには、次の手順を実行します。

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

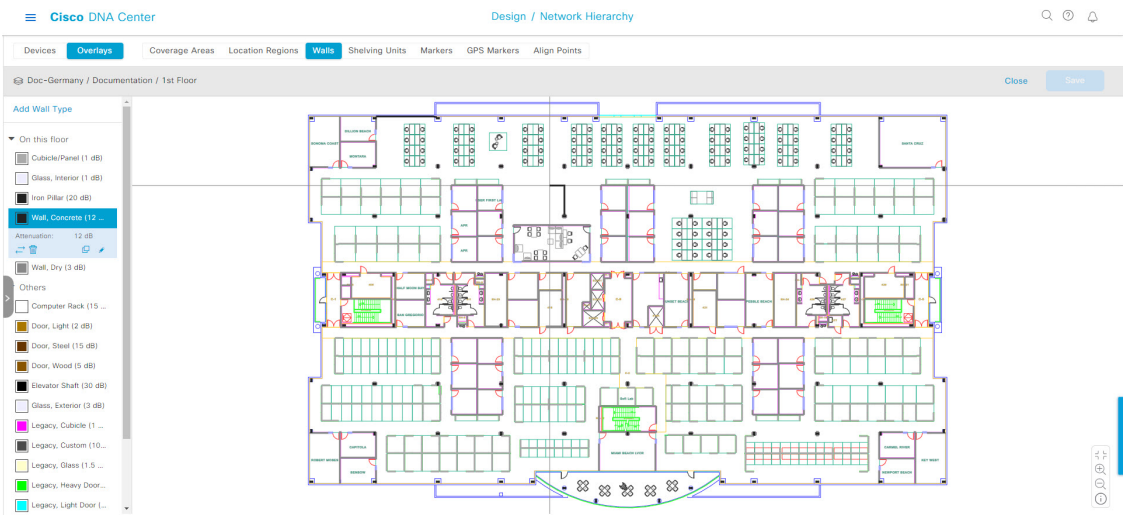
b) マップの左ペインで、追加する壁のタイプをクリックします。

壁タイプがリストにない場合は、[Add Wall Type] をクリックして新しい壁タイプを作成します。

c) 描画ツールを使用してマップ上に壁を作成します。

- マップ上の壁を開始する場所をクリックします。次に、カーソルを次のポイントに移動して、もう一度クリックします。必要な形状の壁を作成するまで、このプロセスを続けます。
- 壁を完成させるには、壁を終了する場所をダブルクリックします。描画をキャンセルするには、マップを右クリックします。
- 既存の壁のタイプを変更するには、形状を右クリックして [Change Type] を選択します。
- 既存の壁を移動するには、形状を新しい場所にドラッグアンドドロップします。
- 既存の壁を削除するには、形状を右クリックして [Delete] を選択します。

図 *4*: 描画ツールで壁を追加する



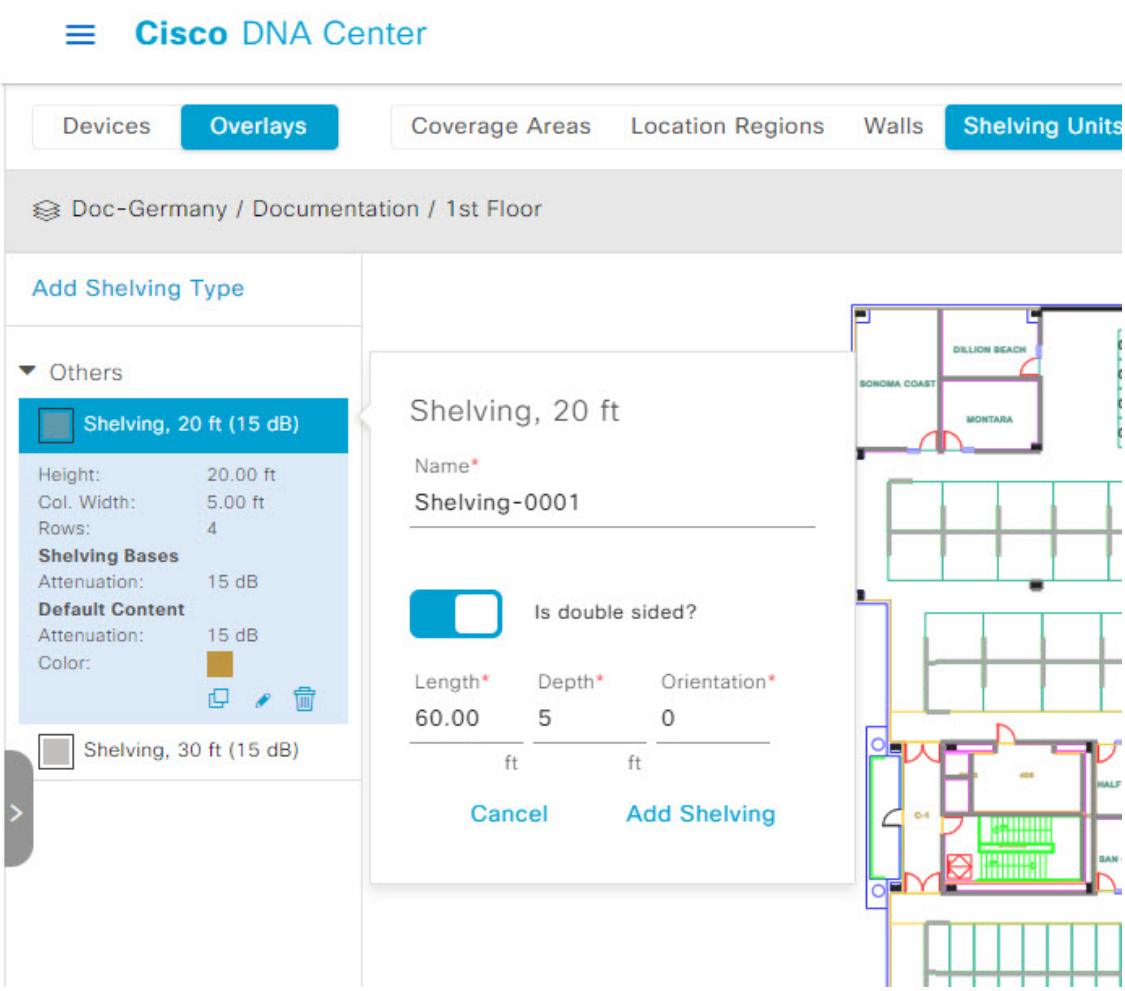
ステップ 9 シェルフユニットを 3D フロア要素として追加するには、次の手順を実行します。

a) マップツールバーで、[Shelving Units] をクリックします。

b) マップの左ペインで、追加するシェルフタイプをクリックします。

- [Shelving] ダイアログボックスでは、シェルフタイプの名前、寸法、および向きを編集できます。向きはシェルフの角度を表します。たとえば、0 はシェルフが垂直で y 軸に平行であることを意味します。
- シェルフタイプがリストにない場合は、[Add Shelving Type] をクリックして新しいシェルフタイプを作成します。

図 *5*：追加するシェルフタイプの選択



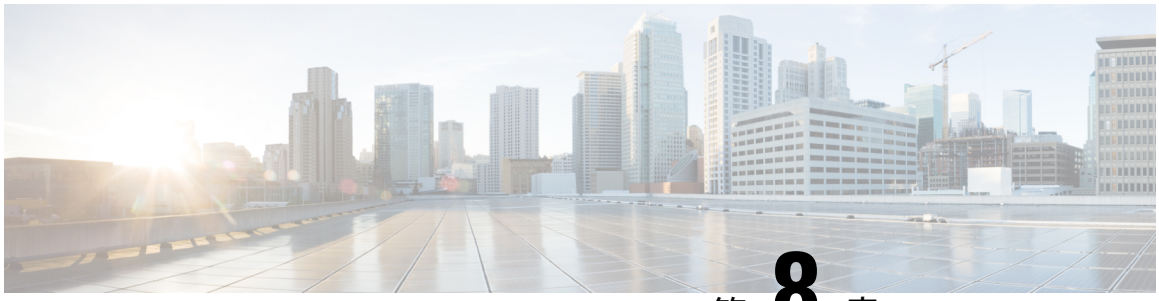
c) [Shelving] ダイアログボックスで、[Add Shelving] をクリックしてシェルフをフロアマップに追加します。

d) シェルフをドラッグアンドドロップして、フロアマップ上の場所に移動します。

e) シェルフを右クリックし、次のいずれかのアクションを選択します。

- [Edit]：シェルフの名前、寸法、および向きを編集します。
- [Clone]：シェルフのコピーを作成します。
- [Array]：シェルフの数とシェルフ間の距離を指定して、シェルフの配列を作成します。
- [Delete]：フロアマップからシェルフを削除します。

ステップ 10 完了したら、マップツールバーの [Save] をクリックします。



第 8 章

ワイヤレス 2D および 3D マップの操作

フロアマップの操作

2D と 3D の両方でワイヤレス ネットワーク ヒートマップを視覚化できます。

2D マップの操作

2D マップは、主にフロアマップ上の要素を構成し、ヒートマップを表示するために使用されます。

2D マップを使用して、フロアマップの要素とオーバーレイを追加できます。2D マップを表示しているときに、さまざまな要素とオーバーレイの表示を操作できます。デバイスデータをフィルタリングし、ワイヤレス干渉を特定することもできます。

Cisco DNA Center はワイヤレス信号の強度と品質を計算します。この RF 予測は、2D ワイヤレスカバレッジ領域マップ上で RF 信号の相対強度を示しているため、一般的にはヒートマップとして知られています。

2D マップでのフロアマップ要素とオーバーレイの構成

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

- 次のデバイスを追加、配置、および削除します。
  - アクセスポイント（AP）と計画されたアクセスポイント（PAP）
  - Sensor
- 次のオーバーレイ オブジェクトを追加、編集、および削除します。

- カバレッジエリア
- ロケーションリージョン
- 壁
- 棚ユニット
- マーカー
- \[GPS Markers\]
- ポイントの位置合わせ

フロアマップでの AP の操作

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

フロア マップに AP を配置する際は、次の注意事項を考慮してください。

- 部屋や建物の屋外の近くにデバイスが置かれるように、カバレッジ領域の境界に沿って AP を設置します。このようなカバレッジ領域の中心に設置された AP からは、場合によっては他の全 AP から等距離に見えてしまうデバイスに関しても有益なデータが得られます。
- AP 全体の密度を高め、AP をカバレッジ エリアの周辺部に近づけることにより、位置精度を向上させることができます。
- 細長いカバレッジ領域では、直線的に AP を配置しないようにします。各 AP でデバイス ロケーションのスナップショットが他と異なるように、それらを交互にずらします。
- 設計では高帯域幅アプリケーションにも十分に対応できる AP 密度が提供されますが、位置に関しては、単一デバイスの各 AP ビューが似ているという弱点があります。そのことが位置の判別を困難にしています。AP をカバレッジ領域の周辺に移動して、それらを交互にずらします。それぞれにおいてデバイスの見え方が明確に異なる可能性が高くなり、結果としてより位置精度が高まります。
- フロアマップでのヒートマップの表示を最適化するには、AP の高さを約 10 フィート （3 m）以下に設定します。

Cisco Prime Infrastructure から一括 AP をエクスポートして Cisco DNA Center にインポートする

Cisco DNA Center では、アクセスポイントのコレクションをフロアマップにインポート、割り当て、および配置できます。Cisco Prime Infrastructure にアクセスポイントの既存のコレクションがある場合は、それを Cisco DNA Center にインポートすると、フロアマップへのアクセスポイントのインポート、割り当て、および配置に費やす時間と労力を節約できます。

この手順では、Cisco Prime Infrastructure からアクセスポイントの既存のコレクションをエクスポートして Cisco DNA Center にインポートする方法について説明します。

始める前に

- 次のタスクを実行するには、**スーパー管理者**または**ネットワーク管理者**である必要があります。
- インベントリに AP があることを確認します。ない場合は、[Discovery] 機能を使用して検出します。
- フロアマップ上に AP を追加して配置します。
- サイト、ビルディング、およびフロアは、サイト階層に存在する必要があります。

ステップ 1 一括 AP 位置を CSV ファイルとして Cisco Prime Infrastructure からワークステーションにエクスポートします。

ステップ 2 メニューアイコン（☰）をクリックして、 **[Design]** > **[Network Hierarchy]**。

ステップ 3 左側の階層型ペインで、サイトの横にある省略記号 ••• にカーソルを合わせて、[Import Bulk AP] を選択します。

ステップ 4 [Import Bulk AP] ポップアップウィンドウで、AP ファイルをドラッグアンドドロップするか、[Choose a file] をクリックしてワークステーションからファイルを選択します。

（注）
- Prime テンプレートを使用して [AP Positions] CSV ファイルを手動で作成するには、[Download Prime Template] をクリックして、Prime テンプレートをワークステーションにエクスポートします。Prime テンプレートは、ネストされたファイルをサポートしていません。
- Cisco DNA テンプレートを使用して [AP Positions] CSV ファイルを手動で作成するには、[Download Template] をクリックして、Cisco DNA テンプレートをワークステーションにエクスポートします。Cisco DNA テンプレートは、ネストされたファイルをサポートしています。

CSV ファイルがダウンロードされるまで待ちます。CSV ファイルには、ネットワーク内のさまざまなサイトの AP 位置に関する情報が含まれています。

ステップ 5 [Import] をクリックします。

[Import Summary] ウィンドウが表示されます。

- [Information] タブに、正常にインポートされた AP のリストが表示されます。
- [Warning] タブをクリックすると、警告のリストが表示されます。
- [Error] タブをクリックすると、エラーのリストが表示されます。

マップへの AP の追加

AP は、一度に 1 つずつ追加することも、まとめて追加することもできます。

始める前に

インベントリにシスコの AP があることを確認してください。ない場合は、[Discovery] 機能を使用して検出します。『検出の概要 （45 ページ）』を参照してください。

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

ステップ 2 フロアを 左側の階層ツリーで、次を選択します。 します。

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

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

ステップ 5 [Add APs] スライドインペインでは、次のいずれかの操作を実行できます。

- **単一の AP を追加するには**：追加する AP の横にある [Add] をクリックします。
- **複数の AP を追加するには**：追加する AP の横にあるチェックボックスをオンにして、[Add Selected] をクリックします。

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

編集モードでは、新しく追加された AP は、マップの左ペインの [Unpositioned] カテゴリに表示されます。詳細については、AP をマップ上に配置する （182 ページ）を参照してください。

ステップ 6 AP をフロアに追加したら、[Add APs] ウィンドウを閉じます。

マップへの計画済み AP の追加

AP モデルカタログ機能を使用して、計画済み AP をフロアに追加し、そのモデル、アンテナタイプ、方位角、および仰角を設定できます。次に、その設定を、同じモデルタイプに属する計画済みの残りの AP に複製できます。

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

ステップ 2 フロアを 左側の階層ツリーで、次を選択します。 します。

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

ステップ 4 マップの左側のペインにある [AP Models] エリアで、追加する計画済み AP の AP モデルをクリックします。

（注） AP モデルがリストにない場合は、[Add Model] をクリックして、リストに追加する AP モデルを選択します。

ステップ 5 計画済み AP を配置するフロアマップ上の場所をクリックします。

選択したモデルの計画済み AP がフロアマップに追加され、右側に [Edit Planned AP] スライドインペインが表示されます。このペインには、デフォルトで AP 名が追加されます。

ステップ 6 [Edit Planned AP] スライドインペインで、[AP Name] フィールドの横にある歯車のアイコンをクリックします。

[Name pattern] ダイアログボックスが表示されます。

ステップ 7 最初の AP をフロアに追加するときは、SJC-BLD21-FL2-AP #### などの有効な名前パターンを入力してから、[Set name pattern] をクリックするようにしてください。

（注） 計画済み AP は Cisco DNA Center 内で一意である必要があるため、名前パターンでフロアを識別できるようにします。

名前パターンの #### は、[AP Name] の番号に置き換えられます（SJC-BLD21-FL2-AP0001 や SJC-BLD21-FL2-AP0002 など）。

ステップ 8 [Antenna] ドロップダウンリストから、デュアルアンテナを含む、この AP の適切なアンテナタイプを選択します。

（注） アンテナイメージは、選択されたアンテナを反映しています。

ステップ 9 アンテナタイプに応じて、[Azimuth] と [Elevation] の方向を度数で入力します。

ステップ 10 必要に応じて、次のアクションを実行します。

- 作成した計画済み AP と同じプロパティを持つ別の計画済みAP を追加するには、その新しい AP を配置するフロアマップ内の場所をクリックします。

  新しい AP アイコンがマップに表示されます。すべてのプロパティが継承され、AP 名が付加されています（例：BLD1-AP0002-TX）。

- 同じプロパティを持ち、AP 名が付加された計画済み AP をさらに追加するには、フロアマップをクリックします。
- フロアマップへの計画済み AP の追加を止めるには、**Esc** を押すか、フロアマップを右クリックします。
- 計画済み AP を再配置するには、AP をフロアマップ内の適切な場所にドラッグアンドドロップします。
- 計画済み AP を削除するには、AP のアイコンを右クリックし、[Delete] をクリックします。
- 計画済み AP を編集するには、AP のアイコンを右クリックし、[Edit] をクリックします。

ステップ 11 完了したら、マップツールバーの [Save] をクリックします。

計画 AP への実際の AP の割り当て

準備ができたら、実際の AP をマップ上の計画された AP に割り当てることができます。

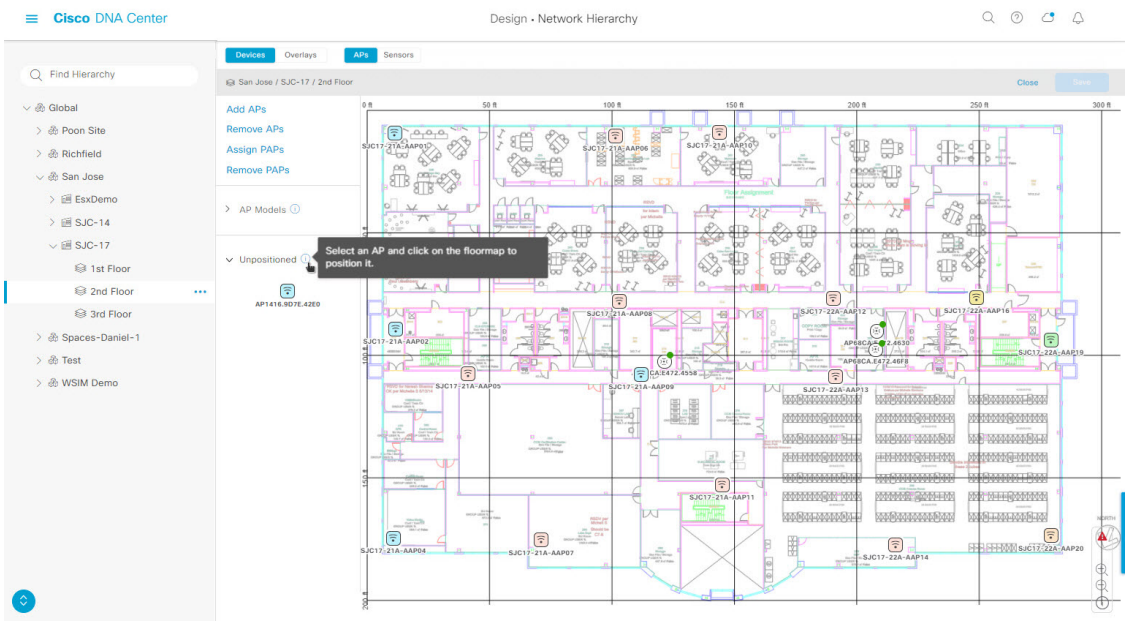
ステップ 1 メニューアイコン（☰）をクリックして、**[Design]** > **[Network Hierarchy]**。
ステップ 2 フロアを 左側の階層ツリーで、次を選択します。 します。
ステップ 3 マップツールバーから、**[2D]** > **[Add/Edit]** > **[APs]** をクリックします。
ステップ 4 マップの左側のペインで、[Assign PAPs] をクリックします。
ステップ 5 フロアマップで、計画済み AP をクリックします。
ステップ 6 [Assign Planned APs] スライドインペインで、割り当てる AP の横にあるチェックボックスをオンにします。
ステップ 7 [**Assign**] をクリックします。
ステップ 8 マップツールバーの [Save] をクリックします。

AP をマップ上に配置する

AP をフロアに追加したら、それらをマップ上に配置する必要があります。

ステップ 1 メニューアイコン（☰）をクリックして、 **[Design]** > **[Network Hierarchy]**。
ステップ 2 フロアを 左側の階層ツリーで、次を選択します。 します。
ステップ 3 マップツールバーから、**[2D]** > **[Add/Edit]** > **[APs]** をクリックします。
ステップ 4 マップの左ペインの [Unpositioned] カテゴリから、AP をクリックします。

図 *6 :* 未配置の *AP*



ステップ 5 AP を配置するには、次のいずれかを実行します。

- AP を配置するフロアマップ上の場所をクリックします。

- [Edit AP] スライドインペインから、対応するフィールドに **x** 座標と **y** 座標を入力します。
- フロアマップに 3 つの点を描き、選択した点を使用して AP を配置します。手順は次のとおりです。

  1. [Edit AP] スライドインペインで、[Position by 3 points] をクリックします。
  2. 点を定義するには、フロアマップの任意の場所をクリックして、最初の点を描画します。再度クリックすると点の描画が終了します。

     最初の点までの距離を設定するためにダイアログボックスが表示されます。
  3. 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。
  4. 2 番目と 3 番目の点を同様の方法で定義し、[保存（Save）] をクリックします。

- フロアマップに 2 つの壁を定義し、定義した壁の間に AP を配置します。この方法によって、2 つの壁の間の AP の位置を把握できるようになります。

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

     最初の壁までの距離を設定するためにダイアログボックスが開きます。
  3. 距離をメートル単位で入力し、[Set Distance] をクリックします。
  4. 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。

     壁の間の定義された距離に基づいて AP が配置されます。

ステップ 6 マップツールバーの [Save] をクリックします。

（注） Cisco Connected Mobile experience（CMX）が Cisco DNA Center と同期されている場合は、ヒートマップ上のクライアントの場所を表示できます。Cisco CMX 設定の作成 （287 ページ）を参照してください。

AP をマップ上に再配置する

いつでも、マップ上に AP を再配置できます。

（注） このタスクは、2D または 3D マップで実行できます。

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

ステップ 2 フロアを 左側の階層ツリーで、次を選択します。 します。

ステップ 3 2D の場合は、次の手順を実行します。

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

b) マップで、AP を新しい位置にドラッグアンドドロップします。

ステップ 4 3D の場合は、次の手順を実行します。

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

b) マップで AP を右クリックし、[Move] を選択します。

c) マップで、AP を新しい位置にドラッグアンドドロップします。

ステップ 5 マップツールバーの [Save] をクリックします。

AP の編集

単一の AP の設定を変更できます。複数の AP の設定を変更するには、複数の AP の編集 （185 ページ）を参照してください。

（注） このタスクは、2D または 3D マップで実行できます。

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

ステップ 2 フロアを 左側の階層ツリーで、次を選択します。 します。

ステップ 3 2D の場合は、次の手順を実行します。

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

b) マップで AP を右クリックし、[Edit] を選択します。

ステップ 4 3D の場合は、次の手順を実行します。

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

b) マップで AP を右クリックし、[Details] を選択します。

ステップ 5 [Edit AP] スライドインペインで、必要に応じて次の AP 設定のいずれかを変更します。

- [AP Name] または [Planned AP Name]：AP の名前
- [MAC Address]：選択した AP の MAC アドレス。
- [AP Model]：選択した AP のモデル。
- [x]：AP の x 軸座標。
- [y]：AP の y 軸座標。
- [AP Height]：AP の高さ。
- [Antenna]：この AP のアンテナタイプ。

（注） 外部の AP の場合は、アンテナを選択する必要があります。選択しないと、AP がマップに表示されません。

- [Azimuth]：アンテナ方位角。x 軸に対して時計回りに測定されたアンテナの角度です。方位角の範囲は 0 ー 360 です。Cisco DNA Center では、右向きは 0 度または 360 度で、下向きは 90 度です。

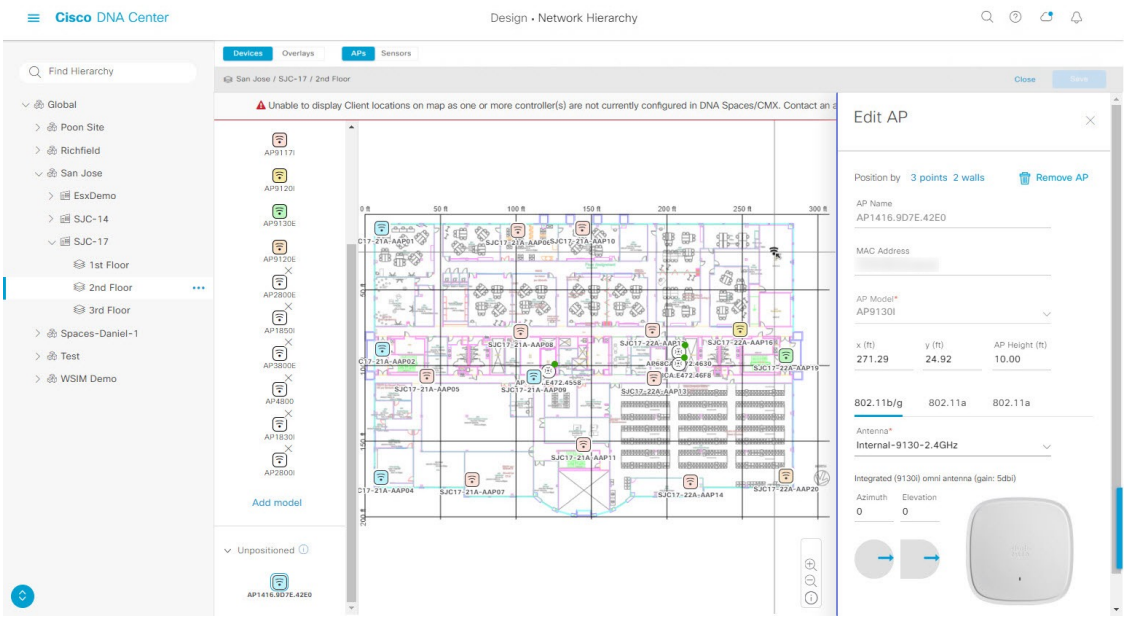
  値を手動で入力するか、フィールドの下の青色の矢印を使用して値を変更できます。

  （注）　無指向性アンテナの場合、仰角が 0 の場合、方位角は関係ありません。

- [Elevation]：仰角（度）。値を手動で入力するか、フィールドの下の青色の矢印を使用して値を変更できます。

（注）　天井に配置するように設計された AP およびアンテナモデルの場合、仰角が 0 の場合は下を向きます。壁に配置するように設計された AP およびアンテナモデルの場合、仰角が 0 の場合は水平方向を向き、負の値の場合は下を向きます。

図 *7: AP* スライドインペインの編集



ステップ 6　マップツールバーの [Save] をクリックします。

複数の AP の編集

AP を 1 つだけ選択すると、編集可能なすべての属性を変更できます。ただし、複数の AP を選択する場合は、次のガイドラインが適用されます。

- 選択したデバイスの属性値が同じ場合、その値が表示されます。それ以外の場合、値は空白です。いずれの場合も、値を変更すると、選択したすべてのデバイスに新しい値が適用されます。
- 選択した AP のモデル番号と無線（無線の数と動作帯域）が同じ場合、アンテナは編集可能です。それ以外の場合、アンテナは編集できません。

- 計画された AP のモデル番号は変更できますが、追加された AP は変更できません。そのため、AP を選択した場合、モデル番号は編集できません。
- 一括変更はより多くのデバイスに影響を与えるため、すぐには有効になりません。[Apply] をクリックして、変更内容を適用する必要があります。

（注） このタスクは、2D または 3D マップで実行できます。

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

ステップ 2 フロアを 左側の階層ツリーで、次を選択します。 します。

ステップ 3 次のいずれかを実行します。

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

ステップ 4 次のいずれかの方法を使用して、AP を選択します。

- 最初のデバイスをクリックし、Shift キーを押しながら残りのデバイスをクリックします。
- マップ ナビゲーション ツールバーで、[Select by rectangle] をクリックします。次に、マップの領域をクリックし、強調表示された長方形をドラッグして、連続した領域内の AP を選択します。長方形内で強調表示されているすべての AP が選択されています。

AP の選択を解除するには、次のいずれかの方法を使用します。

- 1 つの AP の選択を解除するには、Shift キーを押しながら AP をクリックします。
- 1 つを除くすべての AP の選択を解除するには、選択したままにする AP をクリックします。その他はすべて選択解除されます。
- すべての AP の選択を解除するには、ESC キーを押すか、[Edit] ペインを閉じます。

ステップ 5 [Edit AP] スライドインペインで、利用可能な設定を構成します。

- [AP Name] または [Planned AP Name]：AP の名前
- [MAC Address]：選択した AP の MAC アドレス。
- [AP Model]：選択した AP のモデル。
- [x]：AP の x 軸座標。値は手動で入力できます。
- [y]：AP の y 軸座標。値は手動で入力できます。
- [AP Height]：AP の高さ。値は手動で入力できます。
- [Antenna]：この AP のアンテナタイプ。

（注） 外部の AP の場合は、アンテナを選択する必要があります。選択しないと、AP がマップに表示されません。

- [Azimuth]：アンテナ方位角。x 軸に対して時計回りに測定されたアンテナの角度です。方位角の範囲は 0 ー 360 です。Cisco DNA Center では、右向きは 0 度または 360 度で、下向きは 90 度です。

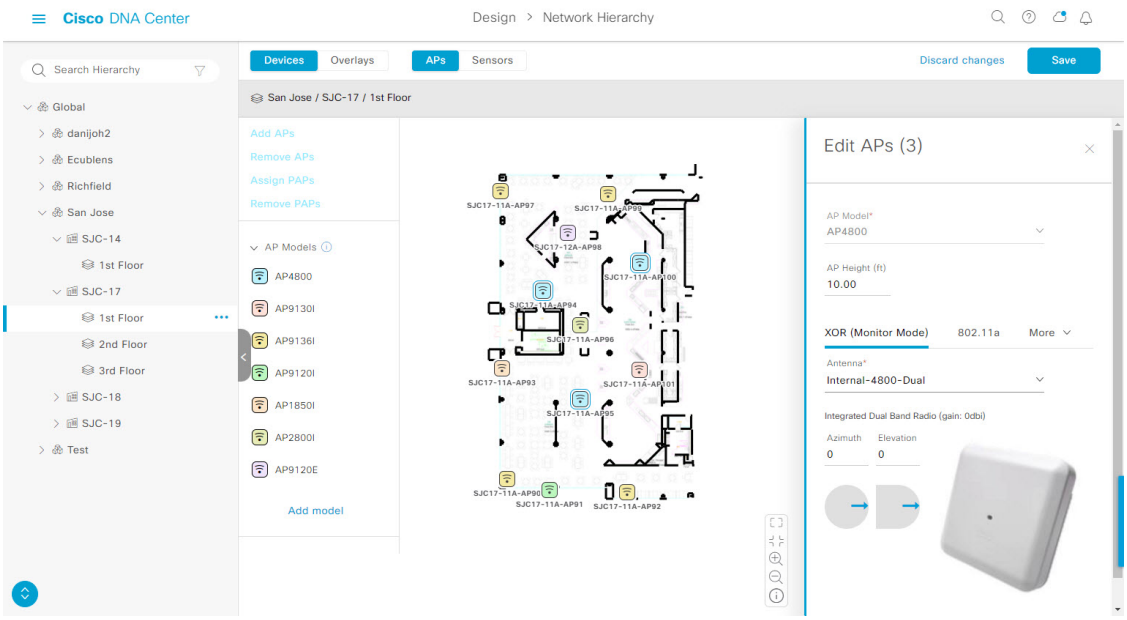
  値を手動で入力するか、フィールドの下の青色の矢印を使用して値を変更できます。

  （注） 無指向性アンテナの場合、仰角が 0 の場合、方位角は関係ありません。

- [Elevation]：仰角（度）。値を手動で入力するか、フィールドの下の青色の矢印を使用して値を変更できます。

（注） 天井に配置するように設計された AP およびアンテナモデルの場合、仰角が 0 の場合は下を向きます。壁に配置するように設計された AP およびアンテナモデルの場合、仰角が 0 の場合は水平方向を向き、負の値の場合は下を向きます。

図 *8*：複数 *AP* 編集のスライドインペイン



ステップ 6 マップツールバーの [Save] をクリックします。

AP をマップから削除する

AP および計画済み AP（PAP）をマップから削除できます。

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

ステップ 2 フロアを 左側の階層ツリーで、次を選択します。 します。

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

ステップ 4 AP（計画済み AP を含む）を削除するには、次の手順を実行します。

a) AP をクリックするか、複数の AP を選択する場合は、最初の AP をクリックし、Shift キーを押しながら残りの AP をクリックします。

b) [Edit] ペインで、[Remove] をクリックします。

ステップ 5 マップツールバーの [Save] をクリックします。

フロアマップでのセンサーの操作

次のトピックでは、フロアマップにセンサーを追加し、必要に応じてセンサーを配置、再配置、および削除する方法を説明します。

マップへのセンサーの追加

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

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

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

ステップ 2 フロアを 左側の階層ツリーで、次を選択します。 します。

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

ステップ 4 [Add Sensors] スライドインペインから、追加するセンサーのチェックボックスをオンにします。またはセンサー行の横にある [Add] をクリックします。

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

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

ステップ 5 完了したら、[Save] をクリックします。

センサーをマップ上に配置する

新しく追加されたセンサーは、編集モードのマップの左ペインの [Unpositioned] カテゴリに表示されます。この手順では、センサーを最初に追加した後にセンサーを配置する方法を示します。

始める前に

センサーは、配置する前にマップに追加する必要があります。詳細については、マップへのセンサーの追加 （188 ページ）を参照してください。

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

ステップ 2 フロアを 左側の階層ツリーで、次を選択します。 します。

ステップ 3 マップツールバーから、[2D] をクリックします。

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

ステップ 5 マップツールバーの [Sensors] をクリックします。

ステップ 6 マップの左側のペインから、[Unpositioned] カテゴリのセンサーをクリックして、センサーを配置します。

ステップ 7 センサーを配置するフロアマップ上の場所をクリックします。

[Sensor Details] スライドインペインの [x]、[y]、および [sensorHeight] フィールドを使用して、センサーの正確な x、y、および z 座標を入力できます。

ステップ 8 [Save] をクリックします。

マップ上のセンサーの再配置

いつでも、マップ上のセンサーの位置を変更できます。

（注） このタスクは、2D または 3D マップで実行できます。

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

ステップ 2 フロアを 左側の階層ツリーで、次を選択します。 します。

ステップ 3 マップツールバーから、[2D] または [3D] をクリックします。

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

ステップ 5 マップで、センサーを新しい位置にドラッグアンドドロップします。

ステップ 6 完了したら、[Save] をクリックします。

センサーをマップから削除する

フロアマップからセンサーを削除できます。

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

ステップ 2 フロアを 左側の階層ツリーで、次を選択します。 します。

ステップ 3 マップツールバーから、[2D] をクリックします。

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

ステップ 5 センサーを削除するには、次の手順を実行します。

a) センサーをクリックします。複数のセンサーを選択する場合は、最初のセンサーをクリックし、Shift キーを押しながら残りのセンサーをクリックします。

b) [Edit] ペインで、[Remove] をクリックします。

ステップ 6 完了したら、[Save] をクリックします。

カバレッジエリアの追加、編集、および削除

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

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

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

ステップ 2 フロアを 左側の階層ツリーで、次を選択します。 します。

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

ステップ 4 カバレッジエリアを追加するには、次の手順を実行します。

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

b) [Add Coverage] をクリックします。

c) マップをクリックしてポイントを作成し、描画ツールを開始します。

d) 引き続きポイントを作成して、カバレッジエリアの形状を定義します。

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

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

f) マップツールバーの [Save] をクリックします。

ステップ 5 カバレッジエリアを編集するには、次の手順を実行します。

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

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

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

d) 完了したら、マップツールバーの [Save] をクリックします。

ステップ 6 カバレッジエリアを削除するには、次の手順を実行します。

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

ロケーションリージョンの追加、編集、および削除

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

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

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

包含リージョンの追加、編集、および削除

ステップ 1 メニューアイコン（☰）をクリックして、**[Design]** > **[Network Hierarchy]**。
ステップ 2 フロアを 左側の階層ツリーで、次を選択します。 します。
ステップ 3 マップツールバーから、**[2D]** > **[Add/Edit]** > **[Overlays]** > **[Location Regions]** をクリックします。
ステップ 4 マップの左側のペインから、[Inclusion] アイコンをクリックします。
ステップ 5 包含リージョンを作成するには、描画ツールを使用します。
a) マップをクリックして、包含リージョンを開始するポイントを作成します。
b) カーソルを次のポイントに移動して、もう一度クリックします。
c) 引き続きポイントを作成して、包含リージョンの形状を定義します。
d) 形状を完成させるには、マップをダブルクリックします。

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

e) 描画ツールを終了するには、マップをもう一度ダブルクリックします。
ステップ 6 包含リージョンの場所を編集するには、その形状を新しい場所にドラッグアンドドロップします。
ステップ 7 包含リージョンを削除するには、形状を右クリックして [Delete] を選択します。
ステップ 8 マップツールバーの [Save] をクリックします。

除外リージョンの追加、編集、および削除

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

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

ステップ 2 フロアを 左側の階層ツリーで、次を選択します。 します。

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

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

ステップ 5 除外リージョンを作成するには、描画ツールを使用します。

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

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

e) 描画ツールを終了するには、マップをもう一度ダブルクリックします。

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

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

ステップ 8 マップツールバーの [Save] をクリックします。

壁の追加、編集、および削除

より正確なヒートマップを得るには、フロアに壁を追加します。壁は、信号の減衰と、ヒートマップでの RF の計算方法に影響します。

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

ステップ 2 フロアを 左側の階層ツリーで、次を選択します。 します。

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

ステップ 4 壁を追加するには、次の手順を実行します。

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

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

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

e) 壁を終了するには、マップをダブルクリックします。

または、左側のペインで壁のタイプをクリックします。

f) 描画ツールを終了するには、マップをもう一度ダブルクリックします。

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

a) 変更する壁をクリックします。

[Wall Type] ダイアログボックスが表示されます。

b) [Wall Type] ドロップダウンリストから、壁のタイプを選択します。

c) 新しい壁タイプに適したその他のパラメータを設定します。

d) [Update] をクリックします。

ステップ 6 壁を移動するには、次の操作を行います。

a) 移動する壁にカーソルを合わせます。

壁が黒くなります。これは選択されたことを意味します。

b) 壁をクリックし、新しい場所にドラッグアンドドロップします。

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

ステップ 8 マップツールバーの [Save] をクリックします。

シェルフユニットの追加、編集、および削除

シェルフユニットは、信号の減衰に影響を与える障害物です。シェルフユニットがある場所の例としては、天井が高い倉庫などがあります。

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

ステップ 2 フロアを 左側の階層ツリーで、次を選択します。 します。

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

ステップ 4 シェルフユニットを追加するには、次の手順を実行します。

a) マップの左側のペインで、追加するシェルフのタイプをクリックします。

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

棚のタイプがリストにない場合は、[Add Shelving Type] をクリックして新しい棚のタイプを作成します。

c) [Add Shellving] をクリックします。

シェルフユニットがマップに表示されます。

d) シェルフをマップ上の場所にドラッグアンドドロップします。

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

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

ステップ 5 名前、寸法、向き、および両面かどうかを編集するには、[Edit] を選択します。
ステップ 6 シェルフユニットを削除してフロアマップから削除するには、[Delete] を選択します。
ステップ 7 マップツールバーの [Save] をクリックします。

マーカーの追加、編集、および削除

ステップ 1 メニューアイコン（☰）をクリックして、**[Design]** > **[Network Hierarchy]**。
ステップ 2 フロアを 左側の階層ツリーで、次を選択します。 します。
ステップ 3 マップツールバーから、**[2D]** > **[Add/Edit]** > **[Overlays]** > **[Markers]** をクリックします。
ステップ 4 マップの左側のペインから、[Markers] アイコンをクリックします。
ステップ 5 [Place Markers] ダイアログボックスで、マーカーの名前を入力し、[Add Marker] をクリックします。
ステップ 6 マーカーを配置するには、マーカーを配置するマップをクリックします。
ステップ 7 マーカーを移動するには、マーカーが青色に変わるまでカーソルを合わせます。次に、マーカーを新しい場所にドラッグアンドドロップします。
ステップ 8 マーカーを編集するには、マーカーを右クリックして [Edit] を選択します。
ステップ 9 マーカーを削除するには、マーカーを右クリックして [Delete] を選択します。
ステップ 10 マップツールバーの [Save] をクリックします。

GPS マーカーの追加、編集、および削除

ワールドマップ上で建物の物理的な位置を特定し、クライアントの位置の精度を高めるために、2D マップ上に GPS マーカーを配置できます。

（注） GPS マーカーは、ビルディングの属性であり、ビルディングのすべてのフロアに適用できます。

ステップ 1 メニューアイコン（☰）をクリックして、**[Design]** > **[Network Hierarchy]**。
ステップ 2 フロアを 左側の階層ツリーで、次を選択します。 します。
ステップ 3 マップツールバーから、**[2D]** > **[Add/Edit]** > **[Overlays]** > **[GPS Markers]** をクリックします。
ステップ 4 GPS マーカーを追加するには、次の手順を実行します。
a) マップの左側のペインから、[GPS Markers] アイコンをクリックします。

b) GPS マーカーを配置するマップ上の場所をクリックします。
c) [Place Markers] ダイアログボックスで、適切なフィールドに名前、緯度、経度、X 座標、および Y 座標を入力します。
d) [GPS マーカーの追加（Add GPS Marker）] をクリックします。

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

ステップ 6 GPS マーカーを削除するには、右クリックして [Delete] を選択します。

ステップ 7 マップツールバーの [Save] をクリックします。

位置合わせポイントの追加、編集、および削除

3D マップでは、フロアはマップの左上隅（ポイント 0,0）に配置されます。フロアごとに独立して管理すればズレは問題ありません。ただし、一部の 3D マップの機能を使用するには、実際のフロアをそのまま配置する必要があります。このずれを補正するために、2 つ以上のフロアに 1 つ以上の位置合わせポイントを挿入して、フロアが 3D マップ内で適切に上下に配置されるようにすることができます。

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

ステップ 2 フロアを 左側の階層ツリーで、次を選択します。 します。

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

ステップ 4 位置合わせポイントを追加するには、次の手順を実行します。
a) マップの左側のペインから、[Align Points] アイコンをクリックします。
b) 位置合わせポイントを配置するマップ上の場所をクリックします。

ステップ 5 位置合わせポイントの名前を編集するには、次の手順を実行します。
a) 位置合わせポイントを右クリックし、[Edit] を選択します。
b) 名前を変更し、[Edit Marker] をクリックします。

ステップ 6 位置合わせポイントの位置を変更するには、次の手順を実行します。
a) 位置合わせポイントを右クリックし、[Edit] を選択します。
b) [Edit Marker] をクリックします。
c) 位置合わせポイントを新しい位置にドラッグアンドドロップします。

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

ステップ 8 マップツールバーの [Save] をクリックします。

2D ワイヤレスフロアマップの表示

2D ヒートマップを使用して、ワイヤレスネットワークに関する情報を表示します。

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

ステップ 2 フロアを 左側の階層ツリーで、次を選択します。 します。

ステップ 3 マップツールバーから、[2D] をクリックします。

ワイヤレス 2D マップが開きます。

ステップ 4 デバイスに関する特定の詳細を表示するには、デバイスタイプに基づいて次の手順を実行します。

- **AP**：AP アイコンは、無線の数、その周波数と正常性、デバイスの全体的な正常性スコア、および AP の名前とモードを示します。AP アイコンの解釈についてはAP アイコンの凡例 （205 ページ）を参照してください。

  デバイスの詳細を表示するには、AP アイコンの上にカーソルを置きます。AP の Rx ネイバー、クライアント、干渉源、正常性スコアなどの情報が表示されます。

  AP の詳細については、ダイアログボックスで [Device 360] リンクをクリックします。

  （注） [Device 360] を使用するには、「Assurance - Base」パッケージが必要です。

- **メッシュAP**：デバイスの詳細を表示するには、メッシュ AP アイコンの上にカーソルを置きます。メッシュ、バックホール、アクセスデータなどの情報が表示されます。
- [Clients]：関連付けられた AP へのリンクを含むクライアント情報を表示するには、カーソルをクライアントの上に置くか、クライアントをクリックします。クライアントの詳細については、ダイアログボックスで [Client 360] リンクをクリックします。
- **センサー**：センサーのステータスとテスト結果を表示するには、センサーアイコンをクリックします。
- **スイッチとスイッチスタック**：スイッチスタックのメンバースイッチを表示するには、スイッチスタックアイコンの横にある矢印をクリックします。スイッチとそれに関連付けられた AP 間の接続を表示するには、カーソルをスイッチまたはスイッチスタックアイコンの上に置きます。マップには、スイッチからそれに関連付けられた AP への接続を示す線が表示されます。スイッチと AP の関連付けを色で識別することもできます。1 つの特定のスイッチに接続されている AP には、スイッチアイコンのカラーコードと一致するラベルが付いています。

  デバイスの詳細を表示するには、スイッチまたはスイッチスタックのアイコンをクリックします。スライドインペインが開き、デバイスの詳細とヒートマップ表示のオプションが表示されます。[Select Heatmap] 見出しの下で、次のオプションボタンのいずれかをクリックできます。

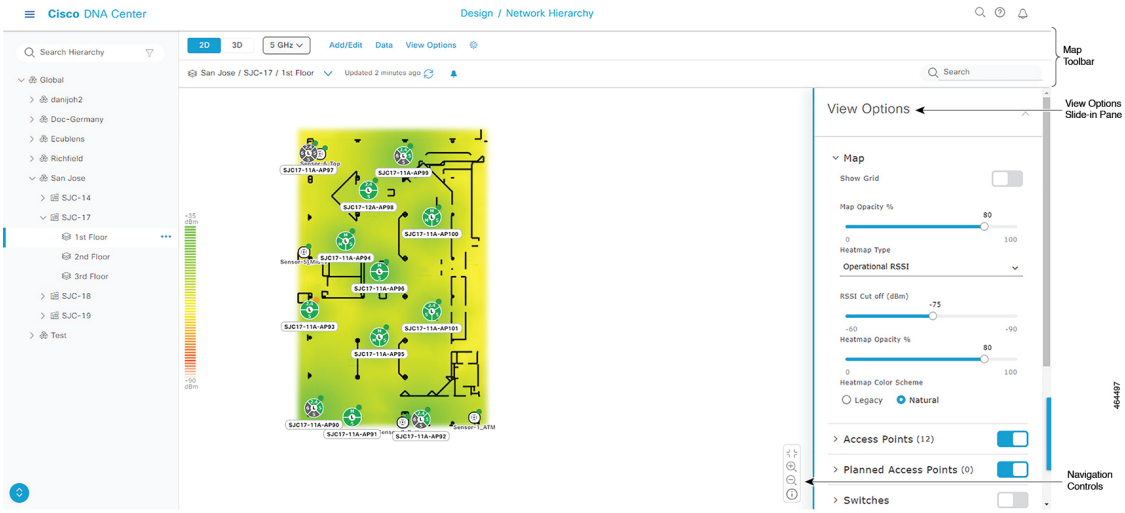
  - [All visible switches]：表示されているマップ領域内のすべてのスイッチのヒートマップを計算して表示します。
  - [This switch]：選択したスイッチのみのヒートマップを計算して表示します。
  - [Rest of visible switches]：選択したスイッチを除く、すべての可視スイッチのヒートマップを計算して表示します。
  - [None]：ヒートマップ計算にスイッチを含めず、ヒートマップ表示にスイッチを含めません。

ステップ 5 リンクに関する情報を表示するには、リンクをクリックします。リンクのタイプに応じて、リンクの状態やその他の統計などの情報が表示されます。

メッシュリンクの場合、2 つのメッシュ AP 間のリンクテストを実行できます。

ステップ 6 次の図に示すツールとオプションを使用して、ワイヤレスネットワークに関するインサイトを取得します。

図 *9*: ツールとオプションを示す *2D* ワイヤレスマップ



- **マップツールバー**：マップの上からツールバーオプションを使用して、ヒートマップに表示される内容を制御します。詳細については、2D マップツールバー （197 ページ）を参照してください。
- **[View Options] スライドインペイン**：スライドインペインで、表示オプションを使用してヒートマップ表示をカスタマイズします。詳細については、2D マップビューオプション （200 ページ）を参照してください。
- **ナビゲーションコントロール**：マップの右下隅から、マップナビゲーションコントロールを使用してヒートマップ表示を管理します。詳細については、「2D マップ ナビゲーション コントロール （204 ページ）」を参照してください。

2D マップツールバー

2D マップにアクセスするには、メニューアイコン（☰）をクリックし、**[Design]** > **[Network Hierarchy]**を選択します。左側の階層ツリーでフロアを選択し、マップツールバーから**[2D]**をクリックします。

マップツールバーは2つのバーで構成され、マップの上にあります。次のアクションおよび設定にはマップツールバーを使用します。

項目	説明
2D 3D	[2D] をクリックしてワイヤレスマップを 2D で表示するか、[3D] をクリックして 3D で表示します。

項目	説明
	**Wi-Fi 帯域フィルタ**：このフィルタを使用して、2.4 GHz および 5 GHz の Wi-Fi 帯域のヒートマップを表示します。
Add/Edit	このボタンをクリックして、次のデバイスとオーバーレイオブジェクトを追加、編集、および削除します。 • [Access points]：詳細については、フロアマップでの AP の操作（178 ページ）を参照してください。 • [Sensor]：詳細については、マップへのセンサーの追加（188 ページ）を参照してください。 • [Coverage areas]：詳細については、カバレッジエリアの追加、編集、および削除（190 ページ）を参照してください。 • [Location regions]：詳細については、ロケーションリージョンの追加、編集、および削除（191 ページ）を参照してください。 • [Walls]：詳細については、壁の追加、編集、および削除（192 ページ）を参照してください。 • [Shelving Units]：詳細については、シェルフユニットの追加、編集、および削除（193 ページ）を参照してください。 • [Markers]：詳細については、マーカーの追加、編集、および削除（194 ページ）を参照してください。 • [GPS Markers]：詳細については、GPS マーカーの追加、編集、および削除（194 ページ）を参照してください。 • [Align points]：詳細については、位置合わせポイントの追加、編集、および削除（195 ページ）を参照してください。
データ	ワイヤレスマップに表示されるアクセスポイント、センサー、およびクライアントデータにフィルタを適用します。詳細については、フロアのデバイスデータのフィルタ処理（206 ページ）を参照してください。
View Options	このボタンをクリックして、マップ、デバイス、およびオーバーレイの表示を制御するためのオプションを含む [View Options] スライドインペインを開きます。詳細については、2D マップビューオプション（200 ページ）を参照してください。

項目	説明
	歯車のアイコン：このアイコンにカーソルを合わせると、次のオプションが表示されます。 • [Recompute]：ヒートマップを再計算します。 • [Export]：フロアマップを PDF または CSV ファイル形式でエクスポートします。 • [Edit Floor]：名前などのフロアの詳細情報を変更します。 • [Set Scale]：地図上に既知の測定値を表示して、地図の縮尺を変更します。 1. マップをクリックして、測定の開始点を指定します。 2. 地図をもう一度クリックして、測定の終点を指定します。 3. [New line length (ft)] フィールドに、測定位置の長さを入力します。 4. [OK] をクリックします。 フロアマップの寸法は、新しい測定値に基づいて再計算されます。 • [Measure Distance]：フロアマップ上の距離を測定します。マップをクリックして開始点を指定します。マップをもう一度クリックして、終点を指定します。測定距離が表示されます。 • [DNA Spaces/CMX Sync History]：Cisco DNA Spaces と Cisco Connected Mobile Experiences（CMX）がいつデータを同期したかを示すログを表示します。ログエントリには、要求の受信時刻、開始時刻と終了時刻、ステータス、および失敗メッセージ（操作が失敗した場合）が含まれます。 • [Floor Health]：Cisco DNA アシュアランス、Cisco DNA Spaces コネクタ、Cisco DNA Spaces フロアサブスクリプションなど、インストールされているアプリケーションの正常性を表示します
	[Full Hierarchy Path]：フロアの完全なナビゲーションパスを表示します。関連する建物、エリアまたはサイトも含まれます。下矢印をクリックすると、別のフロアに移動します。
	[Refresh]：このアイコンをクリックすると、デバイスおよびマップデータが更新されます。アイコンの左側には、最後の更新のタイムスタンプが表示されます。

項目	説明
	[DNA Spaces Connector]：このアイコンをクリックして、Cisco DNA Spaces コネクタに関する IP アドレス、ステータス、バージョンなどの情報を表示します。
	[Map Notification]：このアイコンをクリックして、未配置の AP または計画済みの AP の数などのマップ情報を表示します。
	[Search]：この検索フィールドを使用して、AP、センサー、クライアントなどの特定のフロアマップ要素を検索します。

2D マップビューオプション

2D マップにアクセスするには、メニューアイコン（  ）をクリックし、**[Design]** > **[Network Hierarchy]**を選択します。左側の階層ツリーでフロアを選択し、マップツールバーから**[2D]** > **[View Options]**をクリックします。

[View Options] スライドインペインが開きます。カテゴリを展開して設定を表示します。

- [Map]：さまざまなフロアマップおよびヒートマップ設定が含まれています。

項目	説明
Show Grid	フロアマップのグリッドを有効または無効にするには、このトグルボタンをクリックします。このグリッドにより、フロアマップの寸法を把握できます。
Map Opacity %	フロアマップの不透明度または透明度をカスタマイズするには、このスライダを使用します。

項目	説明
ヒートマップ タイプ	ヒートマップは、変数から取得した値をマップに色として表した、無線周波数（RF）ワイヤレスデータのグラフィック表示を提供します。RSSI ヒートマップは、フロアの RSSI 予測モデル、アンテナタイプ、およびその向きに基づいて計算されます。 2D ヒートマップは、2.4 GHz では 18 dB、5 GHz では 15 dB、6 GHz では 5dB の固定送信電力を使用します。 3D ヒートマップは、稼働中の AP のリアルタイム送信電力と、計画 AP の 11 dB を使用します。 ドロップダウンリストを使用してヒートマップタイプを選択します。 • [Operational RSSI]：稼働中 AP のワイヤレス信号の強度を特定するカバレッジヒートマップ。 • [Planned Heatmap]：計画アクセスポイントがフロア上で持つであろうカバレッジを示す架空のヒートマップ。 • [Operational + Planned RSSI]：（3D のみ）稼働中 AP と計画 AP の両方を使用して作成されたカバレッジヒートマップ。2D マップは稼働中の AP カバレッジのみを表示するため、この結合カバレッジヒートマップを表示するには 3D マップに切り替える必要があります。 • [Client Density]：関連付けられたクライアントの密度。 • [IDS]：ワイヤレスクライアントに提供されるモニターモードアクセスポイントカバレッジをフロアマップ上に示すヒートマップ。
RSSI Cut off (dBm)	ヒートマップに表示される RSSI 値のしきい値を設定するには、このスライダを使用します。しきい値を満たさない RSSI 値は表示されません。
Heatmap Opacity %	ヒートマップの不透明度または透明度をカスタマイズするには、このスライダを使用します。
Heatmap Color Scheme	ヒートマップの配色をカスタマイズできます。オプションは [Legacy] と [Natural] です。

• [Access Points]：フロアマップ上の AP のアイコンを有効または無効にするには、このトグルボタンをクリックします。

このカテゴリを展開して、各 AP に表示するラベルのタイプを設定します。有効なラベルタイプは、[Name]、[AP MAC address]、[IP address]、[Bridge Group Names] などです。[Display Label] ドロップダウンリストからラベルタイプを選択します。

AP に関するその他の詳細を表示するには、2D ワイヤレスフロアマップの表示 （195 ページ）を参照してください。

- [Planned Access Points]：フロアマップ上の計画 AP のアイコンの表示を有効または無効にするには、このトグルボタンをクリックします。

  このカテゴリを展開して、計画 AP 名のラベルを表示します。[Display Label] ドロップダウンリストからラベルタイプを選択します。

- [Switches and Switch Stacks]：フロアマップ上のスイッチまたはスイッチスタックのアイコンの表示を有効または無効にするには、このトグルボタンをクリックします。

  このカテゴリを展開して、スイッチ名、MAC アドレス、または AP カウントのラベルを表示します。[Display Label] ドロップダウンリストからラベルタイプを選択します。

  スイッチに関するその他の詳細を表示するには、2D ワイヤレスフロアマップの表示 （195 ページ）を参照してください。

- [Sensors]：フロアマップ上のセンサーのアイコンの表示を有効または無効にするには、このトグルボタンをクリックします。

  このカテゴリを展開して、センサー名、MAC アドレス、または AP カウントのラベルを表示します。[Display Label] ドロップダウンリストからラベルタイプを選択します。

  センサーに関するその他の詳細を表示するには、2D ワイヤレスフロアマップの表示 （195 ページ）を参照してください。

- [Mesh]：フロアマップ上のメッシュ AP の表示を有効または無効にするには、このトグルボタンをクリックします。

  このカテゴリを展開して、メッシュ AP とルート AP のリンク関係の表示方法を制御するオプションを設定します。

  - [Link Label]：リンクラベルを無効にするには、[None] オプションボタンをクリックします。リンクの信号対雑音比のラベルを表示するには、[Link SNR] オプションボタンをクリックします。パケットエラーレートのラベルを表示するには、[Packet Error Rate] オプションボタンをクリックします。リンクのラベル設定は、ただちにマップ上に反映されます。

  - [Link Color]：リンクの色を無効にするには、[None] オプションボタンをクリックします。リンクの信号対雑音比を色で表示するには、[Link SNR] ラジオボタンをクリックします。パケットエラーレートを色で表示するには、[Packet Error Rate] オプションボタンをクリックします。

    リンクの色の設定は、ただちにマップ上に反映されます。色の定義については、次の表を参照してください。

リンクの色	リンク信号対雑音比（SNR）	パケット エラー率（PER）
🟢	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。
🟠	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。
🔴	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。

- [Mesh Parent-Child Hierarchical View]：表示するメッシュ AP を選択します。このドロップダウンリストから、[Select Only Root APs）、[Select up to 1st hops]、[Select up to 2nd hops]、[Select up to 3rd hops]、または [Select All] を選択します。

- [Overlay Objects]：このカテゴリを展開し、次のトグルボタンのいずれかをクリックして、フロアマップ上のオーバーレイオブジェクトを有効または無効にします。
  - **カバレッジ エリア**
  - **Location Regions**
  - **壁 2D および 3D**
  - **壁 3D のみ**
  - **棚**
  - **Markers**
  - **GPS マーカー**
  - **ポイントの位置合わせ**

- [Clients]：フロアマップ上のクライアントのアイコンの表示を有効または無効にするには、このトグルボタンをクリックします。

  このカテゴリを展開して、クライアント名、MAC アドレス、または AP カウントのラベルを表示します。[Display Label] ドロップダウンリストからラベルタイプを選択します。

  近接したクライアントのグループ化を有効または無効にするには、[Show Client Clusters] トグルボタンをクリックします。

- [Interferers]：フロアマップ上のクライアントのアイコンの表示を有効または無効にするには、このトグルボタンをクリックします。

  このカテゴリを展開して、干渉源からの影響ゾーンの表示を有効または無効にします。[Show Zone of Impact] トグルボタンをクリックします。

- [Map Properties]：このカテゴリを展開して、マップデータの各自動更新の間隔を指定します。[Auto Refresh] ドロップダウンリストから、間隔を選択します。

  マップに表示されるデバイスのタイプに応じて、追加情報が提供されます。たとえば、メッシュ AP の表示が選択されている場合、[Map Properties] カテゴリにメッシュ SNR および PER のカラーチャートが表示されます。メッシュ SNR および PER 値の範囲、およびそれらに対応する色を設定できます。

- [Global Map Properties]：このカテゴリを展開して、優先する測定系を変更します。[Units of Measure] ドロップダウンリストから、[Feet]（ヤードポンド法）または [Meters]（メートル法）のいずれかを選択します。

  この設定は、すべてのワイヤレスマップに適用されます。

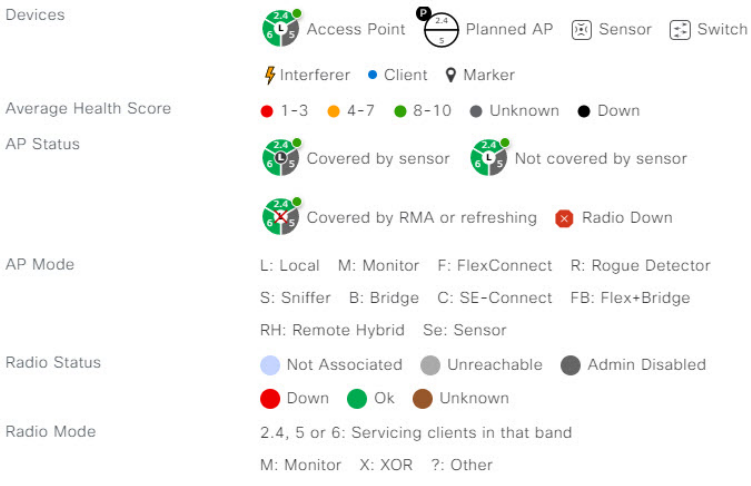
2D マップ ナビゲーション コントロール

2D マップにアクセスするには、メニューアイコン（☰）をクリックし、**[Design]** > **[Network Hierarchy]** を選択します。フロアを左側の階層ツリーで、次を選択します。、マップツールバーで [2D] をクリックします。

2D マップ ナビゲーション コントロールは、マップの右下にあります。マップの詳細については、2D ワイヤレスフロアマップの表示 （195 ページ）を参照してください。

次の機能には、マップ ナビゲーション コントロールを使用します。

マップ ナビゲーション コントロール	説明
	**デフォルトマップビュー**：クリックすると、マップビューがデフォルトにリセットされます。
	**ズームイン/ズームアウト**：ズームインおよびズームアウトのアイコンをクリックして、マップのサイズを拡大および縮小します。マウスホイールを使用して拡大/縮小することもできます。

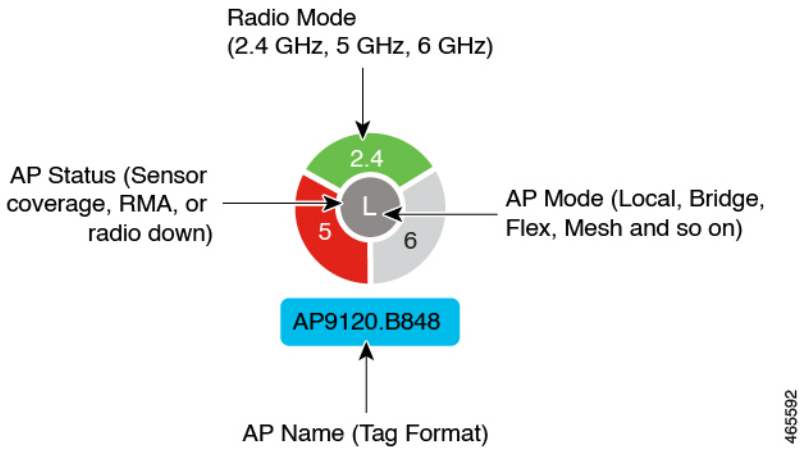
マップ ナビゲーション コントロール	説明
ⓘ	**マップ凡例**：このアイコンをクリックすると、デバイスタイプ、平均正常性スコア、AP ステータスなどのマップのアイコンを説明するマップ凡例が表示されます。 

AP アイコンの凡例

AP アイコンは、ネットワーク内の AP の設定と正常性に関する情報を提供します。円形の AP アイコンは無線帯域に分割され、無線の状態を示すために色分けされています。

- ：関連付けられていません
- ：到達不可
- ：管理者無効
- ：ダウン
- ：OK
- ：不明

次の図に、AP アイコンのすべての要素を示します。



フロアのデバイスデータのフィルタ処理

2D ワイヤレスマップの場合、アクセスポイントやセンサーなどのネットワークデバイスにさまざまなフィルタを適用できます。フィルタ条件に基づいて、検索結果がテーブルに表示されます。デバイスデータのフィルタ処理は、多数のデバイスがあるフロアの特定のデバイスを見つけるために役立ちます。

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

ステップ 2 フロアを 左側の階層ツリーで、次を選択します。 します。

ステップ 3 マップツールバーから、[2D] をクリックします。

ステップ 4 マップツールバーから、[Data] をクリックします。

ステップ 5 [Data] スライドインペインで、フィルタを適用するデバイスタイプをクリックします。

ステップ 6 ドロップダウンリストを使用してパラメータを選択することにより、フィルタルールを定義します。

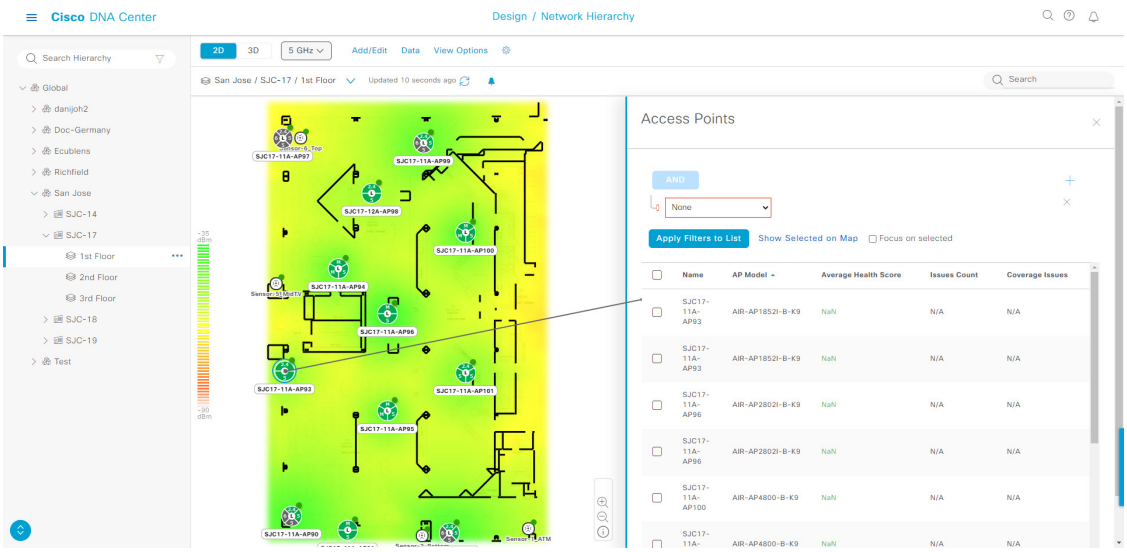
ステップ 7 フィルタルールをさらに追加するには、スライドインペインの上部近くにある [+]アイコンをクリックします。

ステップ 8 完了したら、[Apply Filters to List] をクリックします。

フィルタの結果がスライドインペインの下部にあるテーブルに表示されます。

ステップ 9 テーブル内のデバイスにカーソルを合わせると、そのデバイスのフロアマップ上の位置を確認できます。

図 *10* : フィルタ結果によるデバイスの位置の特定



ステップ 10 適用されたフィルタを削除するには、次の手順を実行します。

a) [Data] スライドインペインを閉じます。

b) マップツールバーから、[Data] をクリックします。

c) デバイスタイプの横にあるフィルタのアイコンをクリックしてフィルタを削除します。

フロアマップでのワイヤレス干渉源の特定

これは 2D マップ機能です。

Cisco DNA Center は、干渉を検出し、フロアマップ上の特定の帯域に対する干渉源を無効にします。2.4 GHz 帯域に干渉があると、802.11 ワイヤレスネットワークのネットワークトラフィックが中断します。

Cisco DNA Center は、干渉源の場所、影響範囲、および強度を特定します。

この手順では、フロアマップ上のネットワーク干渉源を特定する方法を示します。

始める前に

Cisco Connected Mobile Experiences（CMX）または Cisco DNA Spaces が Cisco DNA Center と同期されていることを確認します。

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

ステップ 2 フロアを 左側の階層ツリーで、次を選択します。 します。

ステップ 3 マップツールバーから、[2D] をクリックします。

ステップ 4 フロアの横にある省略記号のアイコン ••• にカーソルを合わせ、[Sync: DNA Spaces/CMX] を選択して、[DNA Spaces] または [CMX] をフロアと同期します。

（注） （オプション）世界地図で、フロアにカーソルを合わせ、[Sync: DNA Spaces/CMX] を選択して、[DNA Spaces] または [CMX] をフロアと同期します。

ステップ 5 [Network Hierarchy] ウィンドウで、[View Options] をクリックします。

ステップ 6 [View Options] ウィンドウで下にスクロールし、[Interferers] トグルボタンをクリックして、干渉源がフロアマップに表示されるようにします。

ステップ 7 [Interferers] カテゴリを展開し、[Show Zone of Impact] トグルボタンをクリックして、干渉源の影響ゾーンがフロアマップに表示されるようにします。

（注） デフォルトでは、[Zone of Impact] は無効になっています。

ステップ 8 フロアマップで、干渉源のアイコンにカーソルを合わせ、影響を受けるチャネルをクリックして干渉源デバイスの詳細情報を確認します。

3D マップの操作

3D マップは、主にフロア上のワイヤレスネットワークの計画と分析に使用されます。そのため、3D マップで実行できる最小限の構成および編集機能があります。

3D ワイヤレスマップを使用すると、ワイヤレスネットワークを 3D で表示できます。ほぼリアルタイムの予測モデルにより、3D マップが動的に更新され、RF カバレッジの変化が示されます。

3D ワイヤレスマップが提供する独自の機能には、次のようなものがあります。

- 3D 環境で一人称ビューまたは三人称ビューを使用してワイヤレスネットワークを移動する。
- サービスレベル契約（SLA）が満たされていないワイヤレスネットワークのエリアに関するインサイトを得る。
- さまざまな高度の RF カバレッジを表示し、**スキャナ**ツールを使用して特定の高度の RF カバレッジを表示する。
- クリッピングツールを使用して、重要業績評価指標（KPI）ヒートマップをクリッピングする。
- ピンツールを使用してフロアプラン上の特定ポイントの x、y、z 座標を予測し、AP またはセンサーの配置を適切に計画する。
- 壁などのフロアプラン要素を 3D で可視化して、RF カバレッジおよび減衰に与える影響を確認する。

- さまざまな構成でワイヤレスネットワークをシミュレートして、フロアのワイヤレスカバレッジがどのように影響を受けるかを確認する。これらのシミュレーションを保存し、後で開いてさらに変更を加えることができます。
- KPI、テレメトリ、および 3D マップ要素の設定を変更して、マップ表示をカスタマイズする。

3D マップでのフロアマップ要素とオーバーレイの構成

3D マップでは、次の構成および編集機能に制限されています。

- AP のクローンの作成 （209 ページ）
- AP の編集 （184 ページ）
- 複数の AP の編集 （185 ページ）
- AP をマップ上に再配置する （183 ページ）
- マップ上のセンサーの再配置 （189 ページ）

他のフロアマップ要素またはオーバーレイを設定するには、2D マップを使用する必要があります。詳細については、「2D マップでのフロアマップ要素とオーバーレイの構成 （177 ページ）」を参照してください。

AP のクローンの作成

AP のクローンを作成することで、その構成を使用して AP を複製できます。

始める前に

クローンを作成する実際の AP が必要です。

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

ステップ 2 フロアを 左側の階層ツリーで、次を選択します。 します。

ステップ 3 マップツールバーから、[3D] をクリックします。

ステップ 4 マップツールバーから、シミュレーションアイコン をクリックします。

ステップ 5 マップツールバーから、[Add/Edit] をクリックします。

ステップ 6 マップで、AP をクリックします。

ステップ 7 [AP Details] スライドインペインで、[Clone] をクリックします。

複製 AP が作成され、元の AP の下に表示されます。名前に **-1** が付きます。同じ AP のクローンを作成し続けると、名前は増分的に追加され続けます。たとえば、**a-floor1-ap01** の最初のクローンには **a-floor1-ap01-1** という名前が付けられ、同じ AP の 2 番目のクローンには **a-floor1-ap01-2** という名前が付けられます。

ステップ 8 マップで、複製された AP を右クリックし、[Move] を選択します。

ステップ 9 AP を新しい位置にドラッグアンドドロップします。

ステップ 10 [Save] をクリックします。

3D ワイヤレスマップの表示

この手順を使用して、3D ワイヤレスマップを表示します。

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

ステップ 2 フロアを 左側の階層ツリーで、次を選択します。 します。

ステップ 3 マップツールバーから、[3D] をクリックします。

3D ワイヤレスマップが開きます。

（注） 3D ヒートマップは、デフォルトで、フロア全体の幅と長さであるカバレッジエリアによって区切られます。ヒートマップ境界のポリゴンを指定するには、2D マップビューで [Coverage Area] フィールドの値を編集します。ただし、フロア全体の幅と長さが 2D マップビューで使用されるため、これらの境界は 2D マップビューには適用されません。

ステップ 4 デバイスに関する特定の詳細を表示するには、デバイスアイコンの上にカーソルを置きます。ダイアログボックスにデバイスに関する情報が表示されます。

（注） アシュアランス - 基本パッケージがインストールされている場合は、[Device 360] ウィンドウへのリンクもダイアログボックスに表示されます。

ステップ 5 1 つ以上の AP のヒートマップを表示するには、次のいずれかの方法を使用して AP を選択および選択解除します。

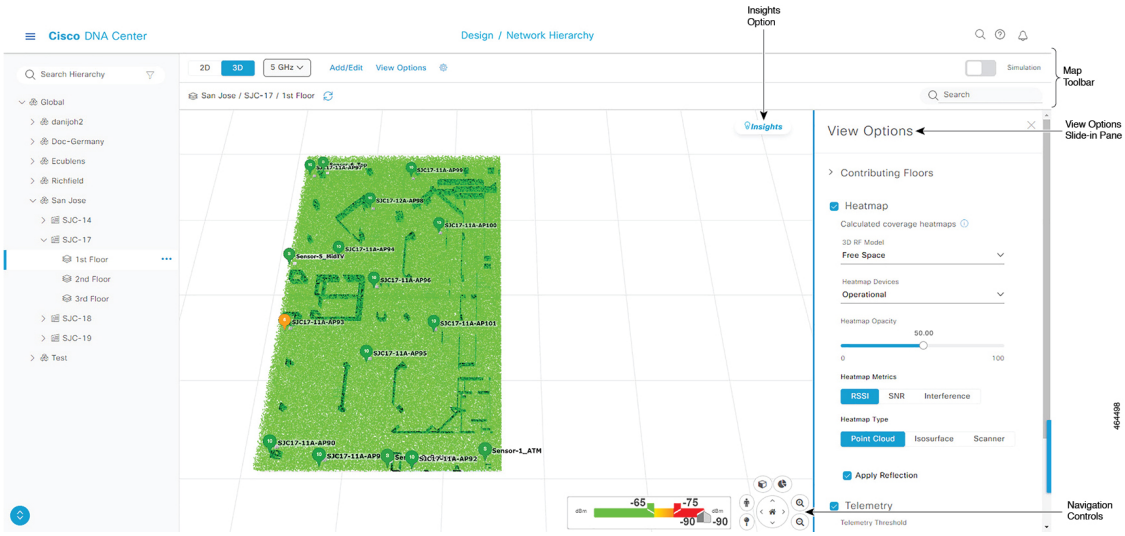
- 1 つの AP を選択するには、その AP をクリックします。
- 複数の AP を選択するには、**Shift** キーを押しながら各 AP をクリックし、**Shift** キーを放します。
- 1 つの AP の選択を解除するには、その AP をクリックします。

  （注） AP が選択されていない場合、ヒートマップにはすべての AP が含まれます。

- すべての AP の選択を解除するには、**ESC** キーを押すか、AP がないマップの領域をダブルクリックします。

ステップ 6 次の図に示すツールとオプションを使用して、ワイヤレスネットワークに関するインサイトを取得します。

図 *11* : ツールとオプションを示す *3D* ワイヤレスマップ



- **ツールバー**：マップの上で、ツールバーオプションを使用して、ヒートマップに表示される内容を制御します。詳細については、3D ワイヤレスマップツールバー （211 ページ）を参照してください。
- [Insights]：マップの右上隅にある [Insights] をクリックして、ワイヤレスネットワークの潜在的な問題を表示して確認します。詳細については、3D ワイヤレスマップからのインサイトの取得 （224 ページ）を参照してください。
- [View Options]：スライドインペインで、表示オプションを使用してヒートマップの表示を制御します。表示されるフロア、ヒートマップのカバレッジとメトリック、テレメトリのしきい値、デバイスとクライアント、オーバーレイオブジェクト、フロアと空の描写などの要素を操作できます。詳細については、3D マップビューオプション （213 ページ）を参照してください。
- **ナビゲーションコントロール**：マップの右下隅で、マップナビゲーションコントロールを使用して、さまざまな視点からヒートマップを表示します。詳細については、「3D マップ ナビゲーション コントロール （216 ページ）」を参照してください。

3D ワイヤレスマップツールバー

3D マップにアクセスするには、メニューアイコン（☰）をクリックし、**[Design]** > **[Network Hierarchy]**を選択します。左側の階層ツリーでフロアを選択し、マップツールバーから**[3D]**をクリックします。

マップツールバーは 2 つのバーで構成され、マップの上にあります。次のアクションおよび設定にはマップツールバーを使用します。

項目	説明
2D 3D	[3D] をクリックしてワイヤレスマップを 3D で表示するか、[2D] をクリックして 2D で表示します。

項目	説明
5 GHz	Wi-Fi 帯域の下矢印をクリックして、次の Wi-Fi 帯域のいずれかを選択します。 • 5 GHz • 6 GHz • 2.4 GHz
Add/Edit	[Add/Edit] をクリックして、既存の AP または計画された AP を複製して計画された AP を追加します。 詳細については、「AP のクローンの作成」を参照してください。 （注） 3D では、インベントリから使用可能な AP を追加することはできません。使用可能な AP を追加するには、2D マップから [Add/Edit] を使用します。
View Options	[3D Floormap] スライドインペインを開いて、関与しているフロア、KPI、テレメトリ、デバイスとクライアントの情報、およびフロア要素の設定を表示します。詳細については、3D マップビューオプション （213 ページ）を参照してください。
	歯車のアイコンにカーソルを合わせて [Insights Configuration] を選択し、インサイトの条件をカスタマイズします。詳細については、3D ワイヤレスマップからのインサイトの取得 （224ページ）を参照してください。
[Simulation] トグルボタン	[Simulation] トグルボタンをクリックして、シミュレーションモードでマップを表示します。デフォルトビューは、動作モードです。詳細については、3D ワイヤレスマップのシミュレーションの作成 （225 ページ）を参照してください。 （注） シミュレーションモードは3Dマップでのみ使用でき、2Dマップでは使用できません。
Area or Site / Building / Floor	[Full Hierarchy Path]：フロアの完全なナビゲーションパスを表示します。関連する建物とサイトも含まれます。下矢印をクリックすると、別のフロアに移動します。
	更新アイコンをクリックすると、デバイスおよびマップデータが更新されます。アイコンの左側には、最後の更新のタイムスタンプが表示されます。

項目	説明
Search	[Search] フィールドを使用して、AP、センサー、クライアントなどの特定のフロアマップ要素を検索します。検索結果は、[Search] フィールドの下に表示されます。 リスト内の要素にカーソルを合わせると、インジケータがマップ上の要素を指します。要素が視野角の外にある場合、インジケータは赤い破線で表示されます。マップの向きを変えて要素を確認します。

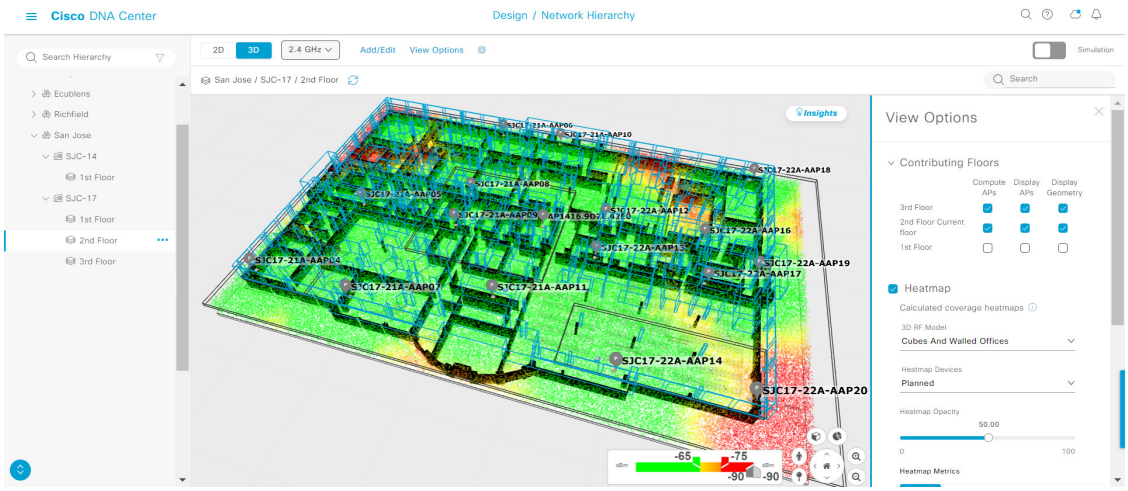
3D マップビューオプション

3D マップにアクセスするには、メニューアイコン（☰）をクリックし、**[Design]** > **[Network Hierarchy]**を選択します。 左側の階層ツリーでフロアを選択し、マップツールバーから**[3D]** > **[View Options]**をクリックします。

[View Options] スライドインペインが開きます。カテゴリを展開して設定を表示します。

- [Contributing Floors]：このオプションを展開して、ヒートマップの計算により多くのフロアを含めます。フロアを含める場合、その AP をヒートマップ計算に追加し、その AP とフロアの形状を表示することを選択できます。[Apply] をクリックして、設定を使用してヒートマップを生成します。

図 *12*：複数のフロアの *3D* マップ



項目	説明
[Compute APs] チェックボックス	ヒートマップを計算するときにフロアの AP を含めるには、このチェックボックスをオンにします。
[Display APs] チェックボックス	ヒートマップにフロアの AP を表示するには、このチェックボックスをオンにします。
[Display Geometry] チェックボックス	ヒートマップにフロアの物理属性を表示するには、このチェックボックスをオンにします。

- [Heatmap]：ヒートマップを表示し、次の表の設定を構成するには、このチェックボックスをオンにします。

項目	説明
3D RF Model	RF モデルを選択するには、このドロップダウンリストを使用します。 RF モデルは、フロアの形状に基づいて RF を計算する方法を決定します。使用可能なモデルには、乾式壁のオフィス、キューブおよび壁付きオフィス、フリースペース、屋外オープンスペース、天井の高い屋内があります。 （注） 壁を手動で配置した場合や、CAD ファイルまたは Ekahau プロジェクトからインポートした場合は、[Free Space] を選択することをお勧めします。壁を手動で配置しなかった場合は、[Free Space] 以外の RF モデルを使用します。
[Heatmap Devices]	このドロップダウンリストを使用して、稼働中のデバイス、稼働中および計画中のデバイス、または計画中のデバイスのみをヒートマップに表示するかどうかを選択します。
Heatmap Opacity	ヒートマップの不透明度または透明度をカスタマイズするには、このスライダを使用します。
Heatmap Metrics	ヒートマップに表示するメトリックのタイプを選択します。 • [RSSI]：受信信号強度表示（RSSI）の値が表示されます。 • [SNR]：信号対雑音比（SNR）の値が表示されます。 • [Interference]：同一チャネル干渉（CCI）または隣接チャネル干渉によって発生した SNR が表示されます。 • [Leakage]：フロア間の信号漏えいを表示します。このオプションを使用できるようにするには、2 つ以上のフロアを関与させてヒートマップを計算する必要があります。
ヒートマップ タイプ	ヒートマップタイプを選択します。 • [Point Cloud]：空間内のデータポイントのコレクションを提供します。各データポイントには、x、y、および z 座標があります。 • [Isosurface]：等値線または連続値線による RSSI を提供します。 • [Scanner]：特定の高度の RSSI が表示されます。

項目	説明
[Apply Reflection]	このチェックボックスをオンにすると、信号の反射が表示されます。これは、信号がガラス、ホワイトボード、プラスチックなどの素材で跳ね返ったときに発生する可能性があります。
Telemetry	このトグルボタンを使用して、テレメトリを有効または無効にします。 テレメトリが有効になっている場合は、センサーまたは AP をクリックするとテレメトリが表示されます。 • センサーのテレメトリには、センサー AP とその他の AP の間の予測される RSSI 値と測定された RSSI 値が表示されます。 • AP のテレメトリには、近接 AP 間の予測される RSSI 値と測定された RSSI 値が表示されます。

- [Telemetry]：このチェックボックスをオンにし、[Telemetry Threshold] スライダを使用して、ヒートマップに表示されるテレメトリソースのしきい値を設定します。

  予測値がしきい値を満たさないテレメトリソースは表示されません。

- [Devices and Clients]：このオプションをクリックして、次の表の設定を構成します。

項目	説明
AP	このチェックボックスをクリックすると、マップ上に AP が表示されます。
[Planned APs]	このチェックボックスをクリックすると、計画された AP がマップ上に表示されます。
Sensor	このチェックボックスをオンにすると、マップ上にセンサーが表示されます。
[Clients]	このチェックボックスをオンにすると、マップ上にクライアントが表示されます。さらに、次のことができます。 • クライアントをデフォルトの青色（[None]）で、または [RSSI]、[SNR]、または [Health Score] で表示します。RSSI、SNR、および正常性スコアの場合、クライアントは、現在の状態に応じて、青、黄、または赤に色付けされます。 • スライダを使用して、マップ上のクライアントを表すボールのサイズを変更します。

- [Overlay Objects]：このオプションをクリックして、次の表の設定を構成します。

項目	説明
Geometry	このチェックボックスをクリックすると、フロアの形状が表示されます。
[Height]	このスライダを使用して、ヒートマップ上の壁の高さを設定します。

- [Map]：このオプションをクリックして、次の表の設定を構成します。

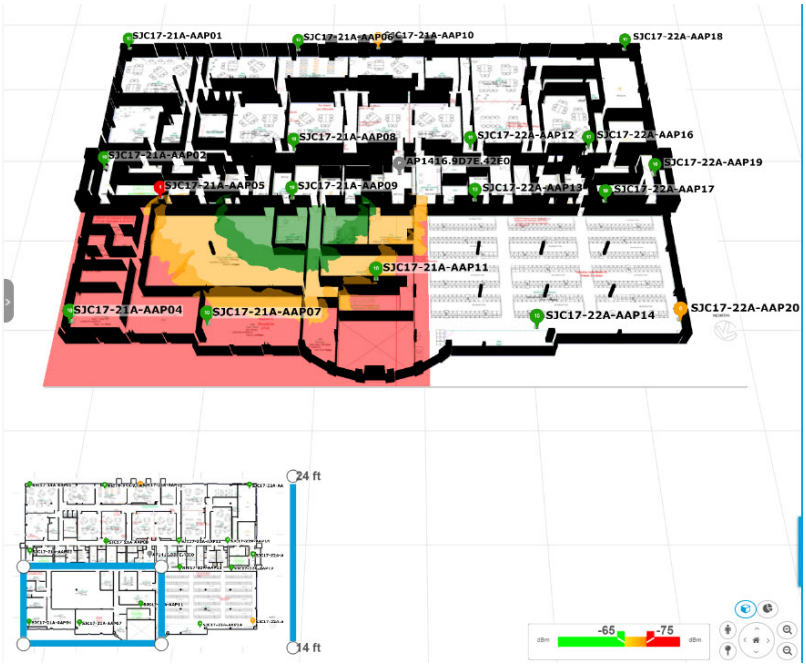
項目	説明
[Sky]	このチェックボックスをクリックすると、ヒートマップに空が表示されます。
Floor	このチェックボックスをクリックすると、ヒートマップにフロアが表示されます。

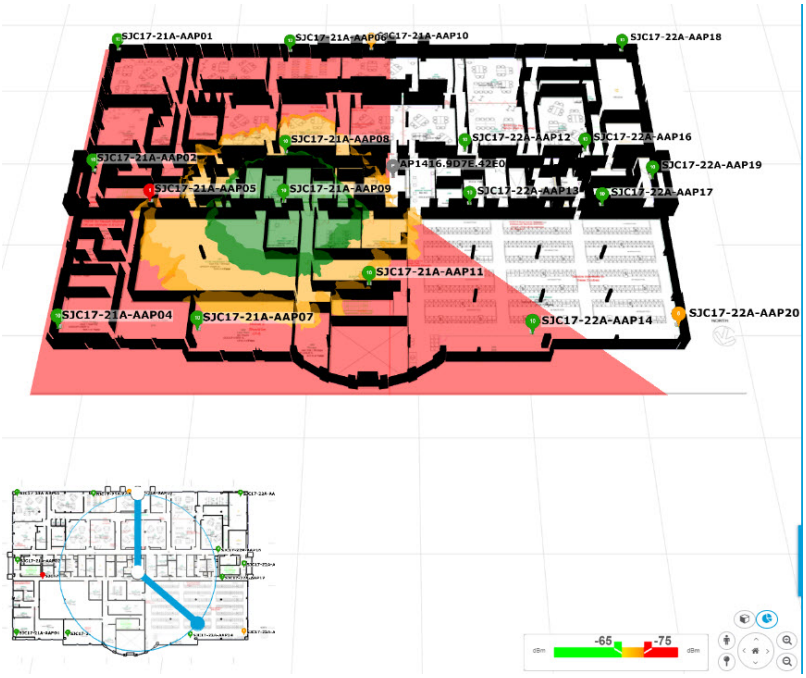
3D マップ ナビゲーション コントロール

2D マップにアクセスするには、メニューアイコン（☰）をクリックし、**[Design]** > **[Network Hierarchy]**を選択します。左側の階層ツリーでフロアを選択し、マップツールバーから [3D] をクリックします。

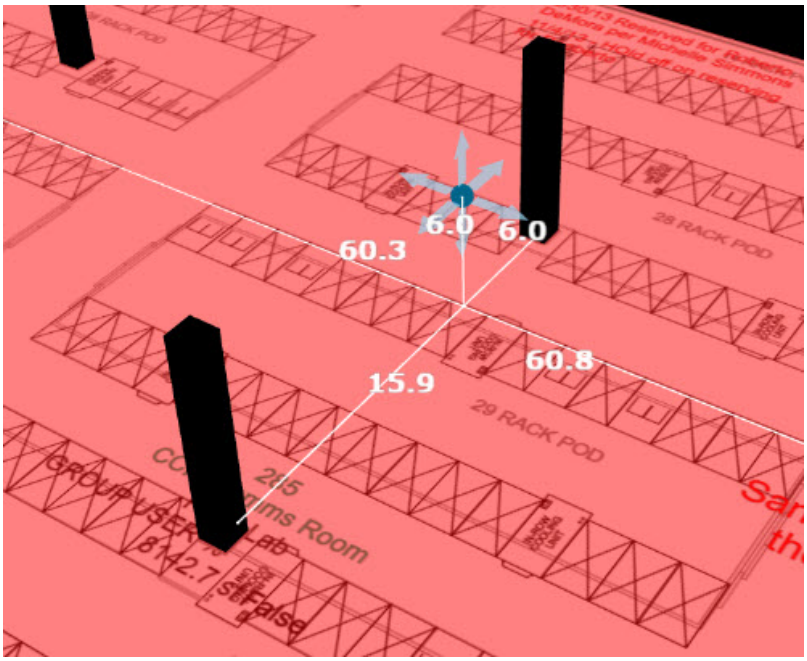
3D マップ ナビゲーション コントロールは、マップの右下にあります。マップの詳細については、3D ワイヤレスマップの表示 （210 ページ）を参照してください。

マップビューを制御するには、マップの右下にあるマップ ナビゲーション コントロールを使用します。

マップ ナビゲーション コントロール	説明
	[Use clip box]：このアイコンをクリックし、ボックス形状を使用してヒートマップをトリミングします。マップの左下隅にあるクリッパーを使用して、トリミング位置を指定します。 • トリミングのサイズを変更するには、アンカーポイントの1つをクリックしてドラッグします。 • トリミングの上下の範囲を指定するには、右側にある垂直スライダのアンカーポイントの 1 つをクリックしてドラッグします。 図 *13:* クリップボックス 

マップ ナビゲーション コントロール	説明
	[Use clip planes]：このアイコンをクリックし、ドーナツ形状を使用してヒートマップをトリミングします。マップの左下隅にあるクリッパーを使用して、トリミング位置を指定します。 • ドーナツの位置を変更するには、ドーナツの中心にあるアンカーポイントをクリックしてドラッグします。 • トリミングの形状を変更するには、外周にある 2 つのアンカーポイントをクリックしてドラッグします。 **図 *14*：使用中のクリッププレーン** 
	[First Person View]：このアイコンをクリックして、一人称ビューと三人称ビューを切り替えます。 青い球は、マップ上の自分の位置を示しています。マップ全体にわたって移動すると、視野が変化します。左下隅にあるミニマップを使用して、視野と方向を把握できます。 （注） 表示用に複数のフロアを選択している場合、[First Person View] によって現在のフロアが自動的に自分の位置となります。 ビューのコントロールなどの詳細については、3D ワイヤレスマップの一人称ビューと三人称ビューの使用 （221 ページ）を参照してください。

マップ ナビゲーション コントロール	説明
	[Third Person View]：このアイコンをクリックして、一人称ビューと三人称ビューを切り替えます。マップ上の自分を配置したい場所にアイコンをドラッグアンドドロップすることもできます。 青い球は、マップ上の自分の位置を示しています。マップ全体にわたって移動すると、視野が変化します。左下隅にあるミニマップを使用して、視野と方向を把握できます。 ビューのコントロールなどの詳細については、3D ワイヤレスマップの一人称ビューと三人称ビューの使用 （221 ページ）を参照してください。

マップ ナビゲーション コントロール	説明
	[Place a pin]：このアイコンをクリックして、フロアマップ上の特定のポイントの予測測定値（x、y、z座標）を表示します。ピンを配置すると、ピンからヤードスティックの端までの距離の測定値を表示できます。ズームインまたはズームアウトすると、測定の位置が調整され、ビューに収まります。次のように、ピンをドラッグアンドドロップして位置を変更します。 • **ピンを水平に移動するには**：水平の矢印をクリックして、ピンを左、右、前、または後ろにドラッグします。選択した矢印とヤードスティックは、アクティブなときは強調表示されます。 • **ピンを垂直に移動するには**：垂直の矢印をクリックして、ピンを上下にドラッグします。選択した矢印とヤードスティックは、アクティブなときは強調表示されます。 ビデオデモンストレーションについては、ここをクリックしてください。 **図 *15*：ピンの調整** 
	[Zoom In]：このアイコンをクリックしてビューを拡大します。マウスホイールを使用して拡大することもできます。
	[Zoom Out]：このアイコンをクリックして、画像のサイズを縮小し、視野を広げます。マウスホイールを使用して縮小することもできます。

マップ ナビゲーション コントロール	説明
	[Map Rotation and Default Map View]：方向を示す矢印をクリックしてカメラの角度を変更します。 デフォルトのビューに戻るには、[Return Home] アイコンをクリックしてマップをリセットします。

3D ワイヤレスマップの一人称ビューと三人称ビューの使用

一人称ビューと三人称ビューを使用すると、ワイヤレスネットワークの異なる視点を得ることができます。

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

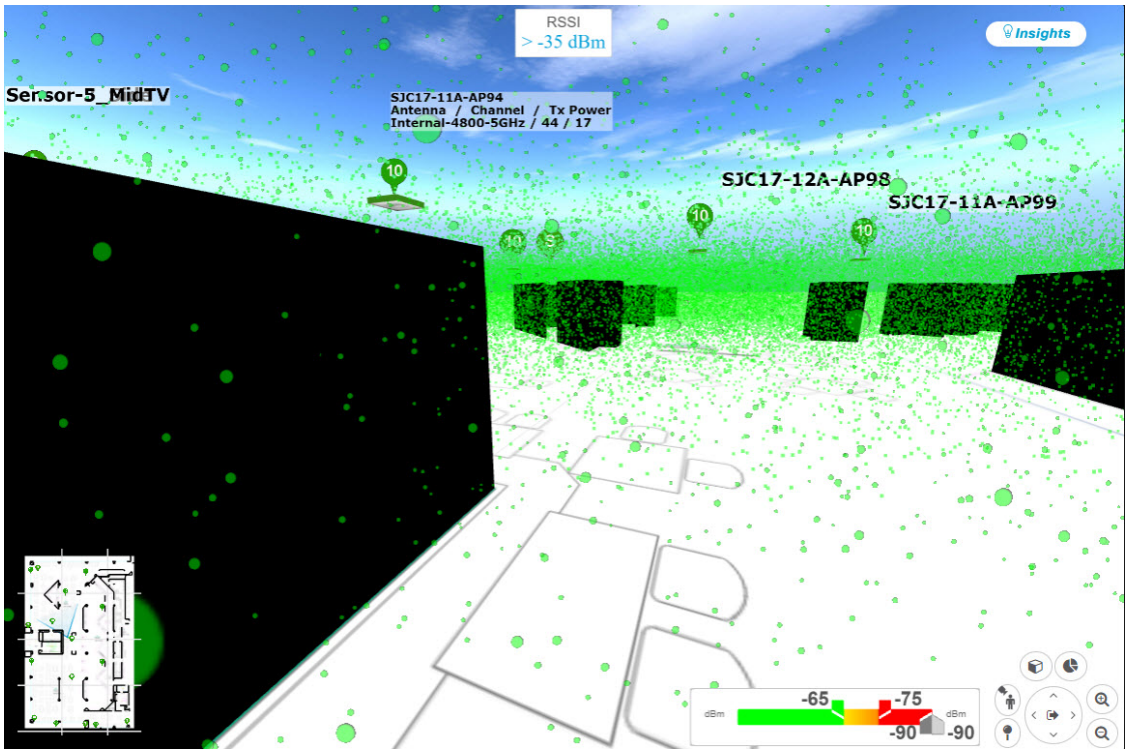
ステップ 2 フロアを 左側の階層ツリーで、次を選択します。 します。

ステップ 3 マップツールバーから、[3D] をクリックします。

ステップ 4 一人称ビューを使用するには、マップ ナビゲーション コントロールの一人称ビューのアイコン  をクリックします。必要に応じて、人のアイコン  をマップ上の特定の場所にドラッグアンドドロップできます。

マップビューが一人称ビューに変わります。

図 *16* : 一人称ビュー



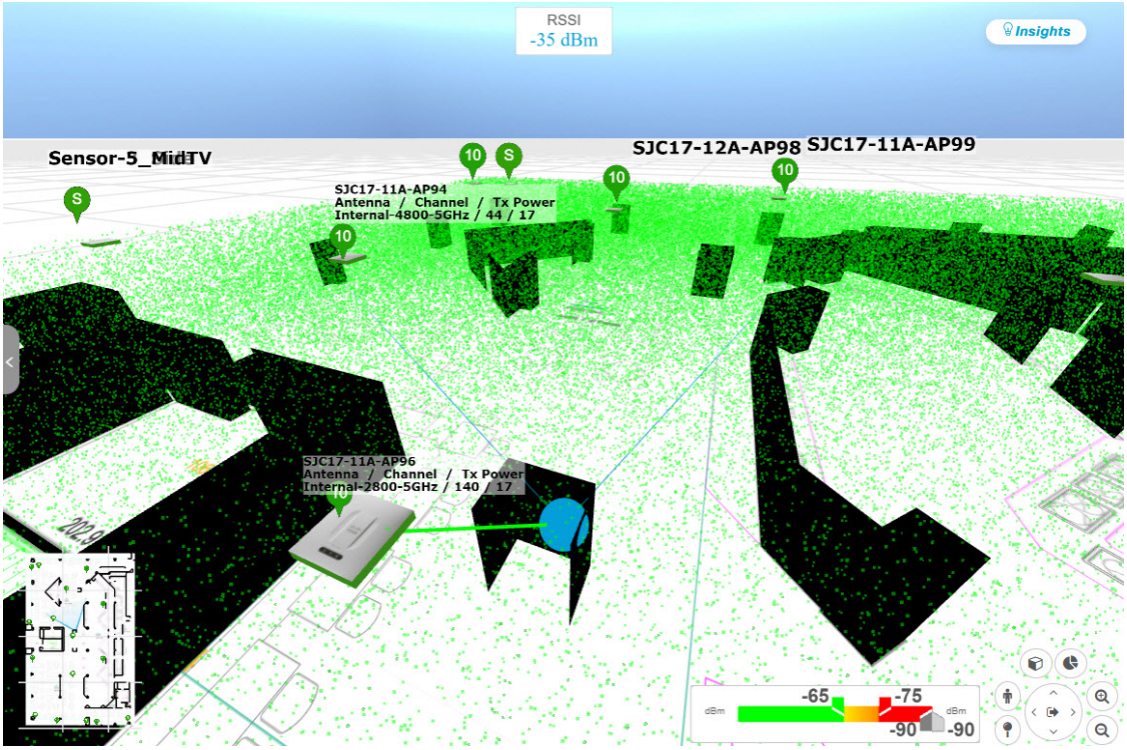
ステップ 5 次の操作により、一人称ビューを制御できます。

Action	コントロール
前後左右に移動します。	**W**、**A**、**S**、および **D** キーまたは矢印キーを使用します。
カメラアングルを変更します。	マップ上でマウスの左ボタンをクリックしたまま、マウスホイールを動かします。
カメラアングルの高度を上げます。	**スペースバー**を押しつづけます。
カメラアングルの高度を下げます。	**Shift** + **スペースバー**を押しつづけます。

ステップ 6 三人称ビューを使用するには、マップ ナビゲーション コントロールの三人称ビューのアイコン  をクリックします。

マップビューが三人称ビューに変わります。

図 *17* : 三人称ビュー



ステップ 7 次の操作により、三人称ビューを制御できます。

Action	コントロール
前後左右に移動します。	**W**、**A**、**S**、および **D** キーまたは矢印キーを使用します。
カメラアングルを変更します。	マップをクリックしてドラッグします。
カメラアングルの高度を上げます。	**スペースバー**を押しつづけます。
カメラアングルの高度を下げます。	**Shift** + **スペースバー**を押しつづけます。

ステップ 8 デフォルトのビューに戻るには、ホームに戻るアイコン をクリックします。

AP およびクライアントに関する詳細の表示

Cisco DNA Spaces または Cisco Connected Mobile Experiences（CMX） などの位置情報サービスが Cisco DNA Center にインストールされている場合は、フロア上のクライアントの位置を表示できます。クライアントは、マップ上で小さな青いボール（●）として識別されます。

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

ステップ 2 フロアを 左側の階層ツリーで、次を選択します。 します。

ステップ 3 マップツールバーから、[3D] をクリックします。

（注） 3D ヒートマップは、デフォルトで、フロア全体の幅と長さであるカバレッジエリアによって区切られます。ヒートマップ境界のポリゴンを指定するには、2D マップビューで [Coverage Area] フィールドの値を編集する必要があります。ただし、フロア全体の幅と長さが 2D マップビューで使用されるため、これらの境界は 2D マップビューには適用されません。

ステップ 4 AP に関する詳細を表示するには、その AP をクリックします。

ステップ 5 クライアントに関する情報を表示するには、カーソルをボール（クライアント）の上に置きます。

クライアントとそれに関連付けられた AP の間に線が描画されます。クライアントの IPv4 アドレス、IPv6 IP アドレス、RSSI 値などの情報を含むダイアログボックスが表示されます。[Client 360] ページを開くには、ダイアログボックスの [Client 360] リンクをクリックします。

ステップ 6 RSSI、SNR、または正常性スコアに対応する色でクライアントを表示するには、次の手順を実行します。

a) **[View Options]** > **[Devices and Client]** をクリックします。

b) [Clients] チェックボックスをオンにします。

c) [Clients] チェックボックスで、[None]（デフォルトの青色）、[RSSI]、[SNR]、または [Health Score] をクリックします。

ステップ 7 ボールのサイズを変更するには、[View Options] ペインの [Ball Size] スライダを使用します。この機能は、クライアントが多い場合や少ない場合にクライアントを表示するのに役立ちます。たとえば、クライアントが多い場合はボールを小さくし、クライアントが少ない場合はボールを大きくします。

3D ワイヤレスマップからのインサイトの取得

Cisco DNA Center は、3D ワイヤレスマップのネットワークパフォーマンスをアクティブにモニターし、サービスレベル契約（SLA）が満たされていないエリアへのインサイトを提供します。

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

ステップ 2 フロアを 左側の階層ツリーで、次を選択します。 します。

ステップ 3 マップツールバーから、[3D] をクリックします。

ステップ 4 マップの右上隅にある [Insights] をクリックします。

[Insights] エリアが表示されます。

図 *18 : [Insights]* エリア

ステップ 5 [Insights] エリアでは、次の操作を実行できます。

アクション	詳細
インサイトの詳細を確認する。	[Insights] エリアには、特定の KPI しきい値（たとえば、RSSI≥-70 dBm）を満たさないカバレッジエリアに関するエントリが表示されます。 インサイトをさらに表示するには、[Next] および [Previous] をクリックします。
インサイトの設定をカスタマイズする。	インサイトの設定をカスタマイズすることにより、インサイトの KPI しきい値を変更できます。 [View All Insights] をクリックし、カスタマイズするインサイト設定の [Edit Configuration] をクリックします。 マップツールバーの歯車のアイコン にカーソルを合わせて、[Insights Configurations] を選択してインサイトの設定をカスタマイズすることもできます。
インサイトをミュートする。	Cisco DNA Center によるインサイトのレポートを停止するには、[Mute Insight] をクリックします。 ミュートされたインサイトは、[All Insights] スライドインペインのリストの下部に表示されます。
すべてのインサイトの概要を取得する。	[View All Insights] をクリックして、すべてのインサイト（アクティブおよびミュート）を表示する [All Insights] スライドインペインを開きます。

3D ワイヤレスマップのシミュレーションの作成

3D ワイヤレスマップのシミュレーションを作成することができます。

（注） シミュレーションモードは 3D マップでのみ使用でき、2D マップでは使用できません。

シミュレーションを使用すると、実際に実装せずにデバイス構成を変更できます。複数のシミュレーションを作成し、いつでもロードすることができます。

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

ステップ 2 フロアを 左側の階層ツリーで、次を選択します。 します。

ステップ 3 マップツールバーから、[3D] をクリックします。

ステップ 4 マップツールバーから、[Simulation] トグルボタンをクリックします。

3D ワイヤレスマップがシミュレーションモードになります（下のマップツールバーが水色になります）。

ステップ 5 マップツールバーから、[Add/Edit] をクリックします。

シミュレーションモードでは、特定の属性のみが編集可能であり、ヒートマップで変更の影響をプレビューするためにのみ使用できます。

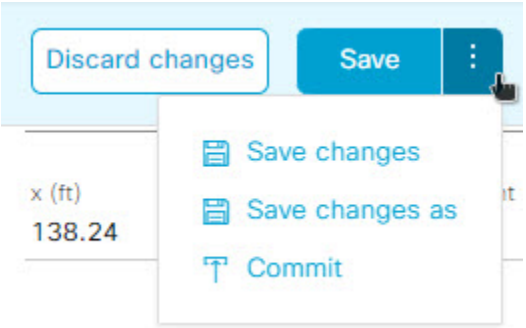
ステップ 6 必要に応じて、デバイスに変更を加えます。

- **AP**：モデル、チャネル、および送信電力を変更できます。
- **PAP**：チャネルと送信電力を変更できます。

a) [Apply] をクリックします。

ステップ 7 マップツールバーで、垂直の省略記号にカーソルを合わせて、[Save changes as] を選択します。

図 *19*：シミュレーションとして保存

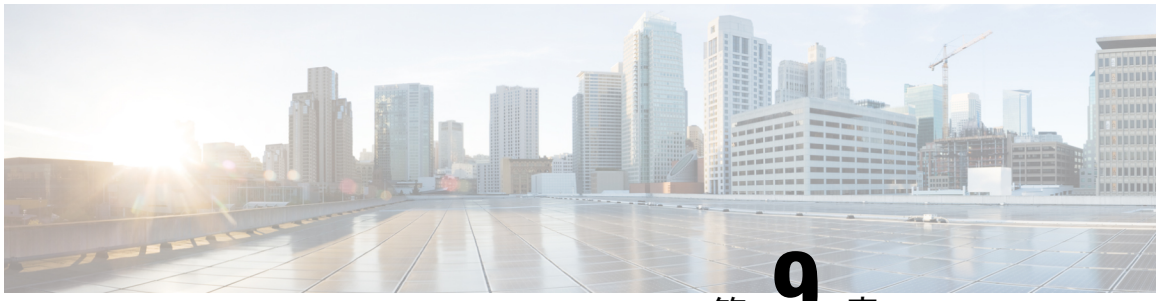


（注） [Save changes] を選択すると、変更が動作モードに保存されます。

[Commit] を選択すると、変更が実稼働デバイスに保存されます。

ステップ 8 [Save Simulation] ダイアログボックスで、シミュレーションの名前を入力し、[Save] をクリックします。

ステップ 9 シミュレーションをロードするには、[Simulation] トグルボタンをクリックし、[Select Simulation] ドロップダウンリストからシミュレーションを選択します。保存されたシミュレーションがない場合は、[None available] が表示されます。



第 9 章

ネットワークの設定

ネットワーク設定の概要

ネットワーク全体のデフォルトになるネットワーク設定を作成できます。ネットワーク内の設定を定義可能な主なエリアは次の 2 つです。

- [Global settings]：ここで定義されている設定はネットワーク全体に適用されます。DHCP、DNS、AAA、NTP などのサーバー、IP アドレスプール、デバイス クレデンシャル プロファイル、Syslog、トラップ、Netflow などのテレメトリの設定が含まれます。
- [Site settings]：ここで定義されている設定はグローバル設定をオーバーライドします。また、サーバー、IPアドレスプール、デバイスのログイン情報プロファイルの設定を含めることができます。

（注） アクティブなファブリックで使用されているネットワーク設定の変更はサポートされていません。それらのネットワーク設定には、サイト階層、IPプールの名前変更など複数の機能が含まれます。

（注） 一部のネットワーク設定は、デバイスの可制御性機能を使用してデバイスに自動的に設定できます。Cisco DNA Center によるデバイスの設定または更新時に、トランザクションが Cisco DNA Center の監査ログにキャプチャされます。監査ログを使用すると、変更を追跡し、問題をトラブルシューティングするのに役立ちます。

[Design] > **[Network Settings]** の順に選択して該当するタブをクリックし、次のグローバルネットワーク設定を定義できます。

- AAA、DHCP、DNS サーバーなどのネットワーク サーバー：詳細については、グローバル ネットワーク サーバーの設定 （230 ページ）を参照してください。
- CLI、SNMP、HTTP（S）などのデバイス クレデンシャル：詳細については、グローバル CLI クレデンシャルの設定 （230 ページ）、グローバル SNMPv2c クレデンシャルの設定 （231 ページ）、グローバル SNMPv3 クレデンシャルの設定 （233 ページ）、およびグローバル HTTPS クレデンシャルの設定 （235 ページ）を参照してください。
- IP アドレス プール：詳細については、IP アドレス プールを設定する （241 ページ）を参照してください。
- SSID、ワイヤレス インターフェイス、および無線周波数プロファイルなどのワイヤレス設定：詳細については、グローバル ワイヤレス設定の構成 （247 ページ）を参照してください。
- テレメトリを使用して、syslog、SNMP、NetFlow コレクタサーバーなどのグローバルテレメトリ設定を構成します。

Cisco ISE またはその他の AAA サーバーの追加

Cisco Identity Services Engine（ISE）サーバーまたはその他の同様の AAA サーバーを、ネットワーク、クライアント、およびエンドポイント認証のためにサイトまたはグローバル レベルで定義することができます。ネットワーク認証では、RADIUS および TACACS プロトコルがサポートされています。クライアントとエンドポイント認証では、RADIUS のみがサポートされます。Cisco DNA Center あたり、1 つの Cisco ISE のみサポートされます。

マルチ ISE 設定をサポートするために、RADIUS または TACACS サーバーグループの下に送信元インターフェイスを設定できます。各 Cisco ISE ISE クラスタには独自のサーバーグループがあります。RADIUS サーバーと TACACS サーバーに使用される送信元インターフェイスは、次のように決定されます。

- デバイスに Loopback0 インターフェイスが設定されている場合、Loopback0 は送信元インターフェイスとして設定されます。
- それ以外の場合は、Cisco DNA Center を管理 IP として使用するインターフェイスが送信元インターフェイスとして設定されます。

あるサイトに Cisco ISEサーバーを設定すると、サイトに割り当てられているデバイスは、対応する Cisco ISE サーバーで、自動的に a /32 マスクに更新されます。その後、Cisco ISE でこれらのデバイスに変更が行われると、Cisco DNA Center に自動的に送信されます。

FIPS モードの展開の場合、共有シークレットは、共有シークレット、キーラップ、およびメッセージ認証コードキーで構成されます。

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

ステップ 2 [サーバーの追加（Add Servers）] をクリックして AAA サーバーを追加します。

ステップ 3 [サーバーの追加（Add Servers）] ウィンドウで、[AAA] チェック ボックスをオンにし、[OK] をクリックします。

ステップ 4 AAA サーバーをネットワークユーザー、クライアント/エンドポイントユーザー、またはその両方に設定します。

ステップ 5 [Network] または [Client/Endpoint] チェックボックスをオンにし、AAA サーバーのサーバーとプロトコルを設定します。

ステップ 6 認証と認可のための [Servers] を選択します（[ISE] または [AAA]）。

- [ISE] を選択した場合は、次のように設定します。
  - [ネットワーク] ドロップダウンリストから、Cisco ISE サーバーの IP アドレスを選択します。[Network] ドロップダウンリストには、Cisco DNA Center のホームページの [System Settings] に登録されている 、Cisco ISE サーバーのすべての IP アドレスが含まれています。Cisco ISE の IP を選択すると、選択した Cisco ISE のポリシーサービスノード（PSN）の IP アドレスを持つプライマリおよび追加 IP アドレスのドロップダウンリストが表示されます。AAA サーバーの IP アドレスを入力することも、[IP Address (Primary)] と [IP Address (Additional)] ドロップダウンリストから PSN IP アドレスを選択することもできます。
  - [Protocol] を選択します（[RADIUS] または [TACACS]）。

    （注） 特定のワイヤレスコントローラの物理サイトと管理サイトの AAA 設定が一致する必要があります。一致しない場合、プロビジョニングは失敗します。

- [AAA] を選択した場合は、次のように設定します。
  - AAA サーバーの IP アドレスを入力することも、[IP Address（Primary] および [IP Address（Additional] ドロップダウンリストから IP アドレスを選択することもできます。これらのドロップダウンリストには、[System Settings] で登録されている Cisco ISE 以外の AAA サーバーが含まれています。

ステップ 7 [Save] をクリックします。

グローバル ネットワーク サーバーの設定

ネットワーク全体のデフォルトになるグローバル ネットワーク サーバーを定義することができます。

（注） サイト固有の設定を定義することで、サイトのグローバル ネットワーク設定を上書きできます。

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

ステップ 2 **[DHCP Server]** フィールドに、DHCP サーバーの IP アドレスを入力します。

（注） プラスアイコンをクリックすると、IPv4 アドレスと IPv6 アドレスの両方を入力できます。

IP アドレス プールを作成するには、少なくとも 1 つの DHCP サーバーを定義する必要があります。

ステップ 3 **[DNS Server]** フィールドに、DNS サーバーのドメイン名を入力します。

（注） プラスアイコンをクリックすると、IPv4 アドレスと IPv6 アドレスの両方を入力できます。

IP アドレス プールを作成するために、少なくとも 1 つの DNS サーバーを定義する必要があります。

ステップ 4 [Save] をクリックします。

グローバル デバイス クレデンシャルの概要

「グローバル デバイス クレデンシャル」とは、ネットワーク内のデバイスに関する情報を検出して収集するために Cisco DNA Center で使用される共通の CLI、SNMP、および HTTPS クレデンシャルを指します。Cisco DNA Center は、グローバル クレデンシャルを使用して設定済みデバイス クレデンシャルを共有するネットワーク内のデバイスを認証し、アクセスします。グローバル デバイス クレデンシャルの追加、編集、および削除することができます。また、グローバル サイトまたは特定のサイトにクレデンシャルを関連付けることもできます。

グローバル CLI クレデンシャルの設定

最大 10 のグローバル CLI クレデンシャルを設定して保存できます。

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

ステップ 2 グローバル サイトを選択した状態で、[CLI Credentials] エリアで [Add] をクリックします。

ステップ 3 次のフィールドに情報を入力します。

表 *37 : CLI* クレデンシャル

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

ステップ 4 [Save] をクリックします。

サイトにクレデンシャルを適用するには、左側の階層にあるサイトをクリックし、クレデンシャルの横にあるボタンを選択して、[Save] をクリックします。

ステップ 5 既存のクレデンシャルを変更する場合は、デバイスで新しいクレデンシャルを今すぐ更新するか、後で更新をスケジュールすることが求められます。

- 新しいクレデンシャルを今すぐ更新するには、[Now] ラジオボタンをクリックし、[Apply] をクリックします。
- 後で更新をスケジュールするには、[Later] ラジオボタンをクリックして更新の日時を定義し、[Apply] をクリックします。

（注） [Time Zone] チェック ボックスを使用して、サイトのタイム ゾーンに従って更新を行うか、特定のタイム ゾーンに従って更新を行うかを指示します。

グローバル SNMPv2c クレデンシャルの設定

ネットワークデバイスをモニタおよび管理するために、グローバル SNMPv2c クレデンシャルを設定できます。

（注） Cisco DNA Center は、FIPS モードが有効になっている場合、SNMPv2c デバイスクレデンシャルをサポートしません。代わりに、SNMPv3 クレデンシャルを指定する必要があります。

始める前に

ネットワークの SNMP 情報は必須です。

ステップ 1 [設計（Design）] > [ネットワーク設定（Network Settings）] > [デバイスクレデンシャル（Device Credentials）]。メニューアイコン（☰）をクリックして、> >

ステップ 2 グローバル サイトを選択した状態で、[SNMP Credentials] エリアで [Add] をクリックします。

ステップ 3 [Type] で、[SNMP v2c] をクリックし、次の情報を入力します。

表 *38 : SNMPv2c* のクレデンシャル

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

ステップ 4 [Save] をクリックします。

ステップ 5 既存のクレデンシャルを変更する場合は、デバイスで新しいクレデンシャルを今すぐ更新するか、後で更新をスケジュールすることが求められます。

- 新しいクレデンシャルを今すぐ更新するには、[Now] ラジオボタンをクリックし、[Apply] をクリックします。
- 後で更新をスケジュールするには、[Later] ラジオボタンをクリックして更新の日時を定義し、[Apply] をクリックします。

（注） [Time Zone] チェック ボックスを使用して、サイトのタイム ゾーンに従って更新を行うか、特定のタイム ゾーンに従って更新を行うかを指示します。

グローバル SNMPv3 クレデンシャルの設定

ネットワークデバイスをモニタおよび管理するために、グローバル SNMPv3 クレデンシャルを設定できます。

始める前に

ネットワークの SNMP 情報は必須です。

ステップ 1 [設計（Design）] > [ネットワーク設定（Network Settings）] > [デバイスクレデンシャル（Device Credentials）]。メニューアイコン（☰）をクリックして、> >

ステップ 2 グローバル サイトを選択した状態で、[SNMP Credentials] エリアで [Add] をクリックします。

ステップ 3 [Type] で、**[SNMP v3]** をクリックし、次の情報を入力します。

表 39 : SNMPv3 のクレデンシャル

フィールド	説明
Name/Description	追加した SNMPv3 設定の名前または説明。
Username	SNMPv3 設定に関連付けられている名前。
Mode	SNMP メッセージを必要とするセキュリティ レベル。次のいずれかのモードを選択します。 • [noAuthNoPriv]：認証または暗号化を提供しません。 • [AuthNoPriv]：認証を提供しますが、暗号化は提供しません。 • [AuthPriv]：認証と暗号化の両方を提供します。
Auth Type	使用する認証タイプ（[Mode] として [AuthPriv] または [AuthNoPriv] を選択した場合に有効になります）。次のいずれかの認証タイプを選択します。 • [SHA]：HMAC-SHA に基づく認証。 • [MD5]：HMAC-MD5 に基づく認証。

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

ステップ 4 [Save] をクリックします。

ステップ 5 既存のクレデンシャルを変更する場合は、デバイスで新しいクレデンシャルを今すぐ更新するか、後で更新をスケジュールすることが求められます。

- 新しいクレデンシャルを今すぐ更新するには、[Now] ラジオボタンをクリックし、[Apply] をクリックします。
- 後で更新をスケジュールするには、[Later] ラジオボタンをクリックして更新の日時を定義し、[Apply] をクリックします。

（注） [Time Zone] チェックボックスを使用して、サイトのタイムゾーンに従って更新を行うか、特定のタイムゾーンに従って更新を行うかを指示します。

グローバル HTTPS クレデンシャルの設定

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

ステップ 2 グローバル サイトを選択した状態で、[HTTPS Credentials] エリアで [Add] をクリックします。

ステップ 3 次の情報を入力します。

表 *40 : HTTPS* クレデンシャル

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

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

ステップ 4 [Save] をクリックします。

ステップ 5 既存のクレデンシャルを変更する場合は、デバイスで新しいクレデンシャルを今すぐ更新するか、後で更新をスケジュールすることが求められます。

- 新しいクレデンシャルを今すぐ更新するには、[Now] ラジオボタンをクリックし、[Apply] をクリックします。
- 後で更新をスケジュールするには、[Later] ラジオボタンをクリックして更新の日時を定義し、[Apply] をクリックします。

（注） [Time Zone] チェックボックスを使用して、サイトのタイムゾーンに従って更新を行うか、特定のタイムゾーンに従って更新を行うかを指示します。

グローバルデバイスのログイン情報の編集に関する注意事項

既存のグローバル デバイス クレデンシャルの編集に関する注意事項と制約事項は、次のとおりです。

- Cisco DNA Center グローバル デバイス クレデンシャルを編集、保存、および適用する際は、次のプロセスが使用されます。

  1. Cisco DNA Center からローカル認証を持つデバイスにログイン情報がプッシュされます。ローカル認証では、ログイン情報の変更が適用され、Cisco DNA Center はこれらのログイン情報を使用してデバイスを管理します。

     （AAA サーバーが継承または設定されたサイトにあるデバイスには、Cisco DNA Center から CLI ログイン情報の変更はプッシュされません。AAA 認証では、ログイン情報の変更は適用されません。Cisco DNA Center は、同じログイン情報が AAA サーバーに存在する場合にのみ、これらのログイン情報を使用してデバイスを管理します）

  2. クレデンシャルがデバイスに正常にプッシュされると、Cisco DNA Center は新しいクレデンシャルを使用してデバイスに到達できることを確認します。

（注） この手順に失敗すると、Cisco DNA Center が新しいクレデンシャルをデバイスにプッシュしていても、インベントリでは古いクレデンシャルを使用してデバイスが管理されます。この場合、既存のログイン情報を更新すると、**[Provision]** > **[Inventory]** ウィンドウでデバイスが管理対象外であると示される可能性があります。

  3. 新しいクレデンシャルを使用してデバイスに正常に到達すると、Cisco DNA Center のインベントリは、新しいクレデンシャルを使用してデバイスの管理を開始します。

- サイトには、SNMPv2c クレデンシャルと SNMPv3 クレデンシャルを使用するデバイスを含めることができます。SNMPv2c または SNMPv3 のグローバル クレデンシャルを編集し

て保存すると、Cisco DNA Center はその変更をデバイスにプッシュし、そのクレデンシャルを有効にします。たとえば、SNMPv2c を使用するデバイスがあるのに、SNMPv3 のグローバル クレデンシャルを編集して保存すると、Cisco DNA Center は関連付けられたサイトのすべてのデバイスに新しい SNMPv3 のクレデンシャルをプッシュして、そのクレデンシャルを有効にします。つまり、以前は SNMPv2c が有効になっていたデバイスを含め、すべてのデバイスが SNMPv3 を使用して管理されるようになります。

- 混乱が生じないようにするために、CLI ログイン情報を編集する際は [User Name] を変更してください。これにより、新しい CLI クレデンシャルが作成され、既存の CLI クレデンシャルは変更されません。

グローバル デバイス クレデンシャルの編集

準備が整うまで、Cisco DNA Center でクレデンシャルの変更を適用せずに、グローバル デバイス クレデンシャルを編集および保存できます。変更の適用を決定すると、Cisco DNA Center は、変更したデバイスクレデンシャルを参照するすべてのサイトを検索し、すべてのデバイスに変更をプッシュします。

新しいグローバル デバイス クレデンシャルを更新または作成できますが、Cisco DNA Center はデバイスからクレデンシャルを削除することはありません。

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

ステップ 2 グローバルサイトを選択した状態で、[Manage Credentials] をクリックし、変更するデバイスクレデンシャルのチェックボックスをオンにして、**[Actions]** > **[Actions]**を選択します。

ステップ 3 [Edit Credentials] ダイアログボックスで、変更を加えて、[Save] をクリックします。

（注） CLI パスワードログイン情報には、*ASCII* 印刷可能文字（文字コード 32 ー 127。https://en.wikipedia.org/wiki/ASCII#Printable_characters を参照）だけを使用できます。

ステップ 4 クレデンシャルタイルで、[Apply] をクリックします。

ステップ 5 [Apply Credentials] ダイアログボックスで、デバイスで新しいクレデンシャルを今すぐ更新するか、後で更新をスケジュールするかを選択します。

- 新しいクレデンシャルを今すぐ更新するには、[Now] ラジオボタンをクリックし、[Apply] をクリックします。
- 後で更新をスケジュールするには、[Later] ラジオボタンをクリックして更新の日時を定義し、[Apply] をクリックします。

（注） [Time Zone] チェック ボックスを使用して、サイトのタイム ゾーンに従って更新を行うか、特定のタイム ゾーンに従って更新を行うかを指示します。

ステータスメッセージに、デバイスログイン情報の変更が成功したか、失敗したかが示されます。

ステップ 6 クレデンシャル変更のステータスを表示するには、**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。

[クレデンシャル ステータス（Credential Status）] 列に、次のいずれかのステータスが表示されます。

- [Success]：Cisco DNA Center はログイン情報の変更を正常に適用しました。
- [Failed]：Cisco DNA Center はログイン情報の変更を適用できませんでした。失敗したログイン情報の変更とその理由に関する追加情報を表示するには、アイコンの上にカーソルを重ねます。
- [Not Applicable]：ログイン情報はデバイスタイプに適用できません。

複数のクレデンシャル（CLI、SNMP、HTTPS など）を編集して保存した場合、がいずれかのクレデンシャルを適用できなかったときには、[クレデンシャルステータス（Credential Status）] 列に [失敗（Failed）] と表示されます。Cisco DNA Center 失敗したログイン情報の変更に関する追加情報を表示するには、アイコンの上にカーソルを重ねます。

デバイス クレデンシャルのサイトへの関連付け

グローバルサイトを作成するサイトは、グローバルなデバイスのクレデンシャルを継承できます。または特定サイトの別のデバイスのクレデンシャルを作成することができます。

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

ステップ 2 左側のペインの階層からサイトを選択します。

ステップ 3 [Manage Credentials] をクリックします。

ステップ 4 選択したサイトに関連付けるクレデンシャルを選択し、次に [Assign] をクリックします。

デバイスのクレデンシャルとサイトとの関連付けが正常に成功したことを示すメッセージが、画面の下部に表示されます。

デバイス クレデンシャルの管理

ログイン情報管理ワークフローでは、ログイン情報を作成または編集したり、割り当てたり、デバイスに適用することができます。

ログイン情報は、[Global]、または選択したサイト、建物、またはフロアに割り当てられます。グローバルレベルでログイン情報を割り当てる場合、すべてのサイト、建物、およびフロアは、グローバルレベルから設定を継承します。

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

ステップ 2 必要に応じて、左側のペインで、[Global]、または特定のサイト、建物、フロアを選択します。

ステップ 3 [Manage Credentials] をクリックします。
[Manage Credentials] ウィンドウが開きます。

ステップ 4 [Add] ドロップダウンリストから、次のいずれかのログイン情報を選択します。

- **CLI**
- **HTTP（HTTPS）読み取り**
- **HTTP（HTTPS）書き込み**
- **SNMPv2c 読み取り**
- **SNMPv2c 書き込み**
- **SNMPv3**

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

1. 必要なフィールドに入力します。
2. [Assign credential to site] チェックボックスをオンにします。

   （注） ボックスがオフの場合、ログイン情報は作成されますが、どのサイトにも割り当てられません。

3. [**保存（Save）**] をクリックします。

新しく作成したログイン情報が [Manage Credentials] ウィンドウに表示されます。

ステップ 6 割り当てるログイン情報を選択し、[Assign] をクリックします。

ステップ 7 ログイン情報を適用するには、次のいずれかを実行します。

- サイト階層全体にログイン情報を適用するには、[Manage Credentials] に移動し、目的のログイン情報の [Actions] メニューにマウスカーソルを合わせて、[Apply] を選択します。
- 特定のサイトだけにログイン情報を適用するには、左側のペインで目的のサイトを選択し、そのログイン情報に対応するカードで [Assign] をクリックします。

ステップ 8 [Apply Credentials] ウィンドウで、次の手順を実行します。

- 新しいログイン情報を今すぐ適用するには、[Now] オプションボタンをクリックし、[Apply] をクリックします。
- 新しいログイン情報を後で適用するには、[Later] オプションボタンをクリックします。その後、更新の日時を定義し、[Apply] をクリックします。

ログイン情報は、該当するすべてのサイトに適用されます。

まだ開始されていないログイン情報適用タスクは、再スケジュールすることができます。

ステップ 9 タスクのステータスを表示するには、次のいずれかを実行します。

- [Device Credentials] ページで、右上隅にある更新のアイコンをクリックします。ログイン情報カードの見出しの横にあるアイコンにマウスカーソルを合わせます。
- **[Provision]** > **[Inventory]** の順に選択します。[Credential Status] 列にステータスが表示されます。

- **[Activities]** > **[Audit Logs]** の順に選択します。

ステップ 10 ログイン情報を編集するには、次の手順を実行します。

1. 対応するログイン情報の横にある編集アイコンをクリックします。

   または、[Manage Credentials] ウィンドウで、ログイン情報名の横にある省略記号のアイコンにカーソルを合わせて、[Edit] をクリックします。

2. [Edit Information] ウィンドウで、[OK] をクリックします。
3. [Edit Credentials] ウィンドウで必要な変更を加えます。
4. [**保存（Save）**] をクリックします。

ステップ 11 ログイン情報適用の開始日時を再スケジュールするには、次のいずれかの手順を実行します。

- **グローバルにスケジュールされたタスク**：[Manage Credentials] ウィンドウで、ログイン情報名の横にある水平の省略記号のアイコンにカーソルを合わせて、[Apply] を選択してから、[Apply] をクリックします。
- **サイト、建物、またはフロアのメインページからスケジュールされたタスク**：タスクが最初にスケジュールされたサイト、建物、またはフロアに戻り、対応するログイン情報カードで [Apply] をクリックします。

（注） タイムゾーンは変更できません。

IP アドレス プールを設定する

Cisco DNA Center IPv4 と IPv6 のデュアルスタック IP プールがサポートされています。

IPv4 および IPv6 アドレスプールは手動で設定できます。

Cisco DNA Center を外部 IP アドレス マネージャと通信するように設定することもできます。詳細については、Cisco DNA Center 管理者ガイドを参照してください。

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

ステップ 2 [Add] をクリックし、[Add IP Pool] ウィンドウの必須入力フィールドをすべて入力します。

Cisco DNA Center が外部の IP アドレスマネージャと通信するように設定した場合、外部 IP アドレスマネージャの既存の IP アドレスプールと重複する IP プールを作成することはできません。

ステップ 3 **[Save]** をクリックします。

新しく追加されたプールが IP アドレスプールテーブルに表示されます。IPv4 または IPv6 のアドレスプールのみを表示する場合は、[SUBNET TYPE] 領域で [IPv4] または [IPv6] オプションをクリックします。

（注） IP アドレス プールを編集して、DHCP を変更すると、その IP アドレス プールを使用してデバイスを再設定する必要はありません。

IP アドレスマネージャから IP アドレスプールをインポートする

Bluecat または Infoblox から IP アドレスプールをインポートできます。

（注） IP アドレスプールはサブプールを持つことができず、IP アドレスプールから割り当てられた IP アドレスを持つことはできません。

外部 IP アドレスマネージャ（IPAM）と通信するには Cisco DNA Center を設定する必要があります。詳細については、Cisco DNA Center 管理者ガイドを参照してください。

ステップ 1 メニューアイコン（≡）をクリックして、**[Design]** > **[Network Settings]** > **[IP Address Pools]**。

ステップ 2 [Actions] ドロップダウンリストから、[Import from IPAM Server] を選択し、必須フィールドに値を入力します。

ステップ 3 CIDR を入力し、**[Retrieve]** をクリックして、インポートできる IP プールのリストを取得します。

ステップ 4 [Select All] をクリックするか、またはインポートする IP アドレスプールを選択して [Import] をクリックします。

CSV ファイルから IP アドレスプールをインポートする

CSV ファイルから IP アドレスプールをインポートできます。

ステップ 1 メニューアイコン（≡）をクリックして、**[Design]** > **[Network Settings]** > **[IP Address Pools]**。

ステップ 2 [Actions] ドロップダウンリストから、[Import from CSV File] を選択します。

ステップ 3 [Download Template] をクリックして最新のサンプルファイルをダウンロードします。

ステップ 4 ファイルに IP アドレスプールを追加して、ファイルを保存します。

ステップ 5 次のアクションのいずれかを実行して、CSV ファイルをアップロードします。

a) ドラッグ アンド ドロップ エリアにファイルをドラッグ アンド ドロップします。

b) **[クリックして選択（click to select）]** が表示される場所をクリックしてファイルを選択します。

ステップ 6 **[インポート (Import)]** をクリックします。

IP プールの予約

始める前に

1 つまたは複数の IP アドレスプールが作成されていることを確認します。

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

ステップ 2 [hierarchy] ペインを展開し、サイトを選択します。

ステップ 3 [Reserve] をクリックして以下のフィールドに入力し、使用可能なグローバル IP アドレスプールのすべてまたは一部を特定のサイト用に予約します。

- [IP Address Pool Name]：予約した IP アドレスプールの一意の名前。
- [Type]：IP アドレスプールのタイプ。LAN 自動化の場合は、**LAN** を選択します。次のオプションがあります。
  - [LAN]：該当するアンダーレイの LAN インターフェイスに IP アドレスを割り当てます。
  - [Management]：IP アドレスを管理インターフェイスに割り当てます。
  - [Service]：IP アドレスをサービスインターフェイスに割り当てます。
  - [WAN]：IP アドレスを WAN インターフェイスに割り当てます。
  - [Generic]：他のすべてのネットワークタイプで使用されます。
- [IP Address Space]：すべてまたは一部の IP アドレスを予約する IPv4 および IPv6 アドレスプール。
- **CIDR Prefix/Number of IP Addresses**：IP subnet and mask address used to reserve all or part of the global IP address pool or the number of IP addresses you want to reserve. IPv6 IP プールの [CIDR Prefix] として \64 を選択すると、[SLAAC] オプションがオンになります。（[SLAAC] が選択されている場合、デバイスは DHCP サーバーを必要とせずに、自動的に IP アドレスを獲得します）。
- [Gateway]：ゲートウェイ IP アドレス。
- [DHCP Servers]：DHCP サーバーの IP アドレス。
- [DNS Servers]：DNS サーバーのアドレス。

ステップ 4 [予約（Reserve）] をクリックします。

IPv4 と IPv6 の両方のアドレスプールを予約している場合（ファブリックがデュアルスタック IP プールでプロビジョニングされている場合）で、IPv6 プールがすでに VN に接続されているときは、シングルスタック IP プールに戻すことはできません。

ただし、IPv6 プールが VN に接続されていない場合は、デュアルスタック IPv6 プールからシングルスタック IPv4 プールにダウングレードできます。シングルスタックにダウングレードするには、[IP Address Pools]

ウィンドウで、デュアルスタック IP プールの [Edit] をクリックします。[Edit IP Pool] ウィンドウで、[IPv6] チェックボックスをオフにして、[Save] をクリックします。

IP プールの編集

ステップ 1 メニューアイコン（≡）をクリックして、**[Design]** > **[Network Settings]** > **[IP Address Pools]**。

ステップ 2 グローバルサイトを選択するか、階層ツリーを展開して目的のサイトを選択します。

ステップ 3 すべての IP プールを一括で編集するには、次の手順を実行します。

a) [Actions] ドロップダウンリストから、[Edit All] を選択します。

b) [Warning] メッセージで [Yes] をクリックします。

c) [Edit IP Pool] ウィンドウで、必要な変更を行い、[Save] をクリックします。

ステップ 4 目的の IP プールのみを編集するには、次の手順を実行します。

a) 目的の IP プールを選択し、[Actions] ドロップダウンリストから [Edit Selected] をクリックします。

選択した IP プールに対応する [Edit] をクリックすることもできます。

b) [Edit IP Pool] ウィンドウで、必要な変更を行い、[Save] をクリックします。

IP プールの削除

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

ステップ 2 グローバルサイトを選択するか、階層ツリーを展開して目的のサイトを選択します。

ステップ 3 すべての IP プールを一括で削除するには、次の手順を実行します。

a) [Actions] ドロップダウンリストから、[Delete All] を選択します。

b) [Warning] メッセージで [Yes] をクリックします。

ステップ 4 目的の IP プールのみを削除するには、次の手順を実行します。

a) 目的の IP プールを選択し、[Actions] ドロップダウンリストから [Delete Selected] をクリックします。

選択した IP プールに対応する [Delete] をクリックすることもできます。

b) [Warning] メッセージで [Yes] をクリックします。

IP プールの複製

サイトレベルで既存の IP プールを複製できます。IP プールを複製すると、DHCP サーバーと DNS サーバーの IP アドレスが自動的に入力されます。

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

ステップ 2 階層ツリーを展開し、サイトを選択します。

ステップ 3 目的の IP プールを見つけ、[Actions] 領域で [Clone] をクリックします。

ステップ 4 [Clone IP Pool] ウィンドウで、次の手順を実行します。

a) 必要に応じて、プール名を編集します（タイプ、IP アドレス空間、またはグローバルプール値は、複製元のプールから継承されるため編集できません）。

b) 必要に応じて、CIRD プレフィックス値を編集します。

c) [Clone] をクリックします。

IP プールのリリース

サイトレベルで予約されているシングルスタックおよびデュアルスタックプールをリリースできます。

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

ステップ 2 グローバルサイトを選択するか、階層ツリーを展開して目的のサイトを選択します。

ステップ 3 すべての IP プールを一括でリリースするには、次の手順を実行します。

a) [Actions] ドロップダウンリストから、[Release All] を選択します。

b) [Warning] メッセージで [Yes] をクリックします。

c) プロンプトで [Release] をクリックします。

ステップ 4 目的の IP プールのみをリリースするには、次の手順を実行します。

a) 目的の IP プールを選択し、[Actions] ドロップダウンリストから [Release Selected] をクリックします。

b) プロンプトで [Release] をクリックします。

IP アドレスプールの表示

この手順では、テーブルビューとツリービューで 10 個以上の IP アドレスプールを表示する方法を示します。

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

ステップ 2 左側のペインの階層からサイトを選択します。

ステップ 3 トグルボタンを使用して、テーブルビューとツリービューを切り替えます。

- IP プールが 10 個以上の場合は、デフォルトではテーブルビューにプールが表示されます。
- IP プールが 10 個未満の場合は、デフォルトではツリービューにプールが表示されます。

（注） テーブルマップビューとツリーマップビューの切り替えは、UI でのユーザーの選択ではなくプール数に基づきます。

ツリービューは、グローバルプールとサイトプールに適用されます。

ステップ 4 [IP Address Pools] テーブルビューには、[Name]、[Type]、[IPv4 Subnet]、[IPv4 Used]、[IPv6 Subnet]、[IPv6 Used]、および [Actions] に基づいてIP アドレスプールのリストが表示されます。

（注）
- [IPv4 Used] および [IPv6 Used] の横にある [i] アイコンにカーソルを合わせます。[IPv4 Used]、[IPv6 Used]、[Free]、[Unassignable]、[Assigned]、および [Default Assigned] の IP アドレスプールに関する詳細情報を示すツールチップが表示されます。
- [IPv4] 列と [IPv6] 列で、特定の IP アドレスプールに対応する [IPv4] と [IPv6] の使用率の横にある [i] アイコンにカーソルを合わせます。ツールチップには、[Free]、[Unassignable]、[Assigned]、および [Default Assigned] の IP アドレスプールの割合が表示されます。

ステップ 5 テーブルビューで [IPv4] または [Dual-Stack] のアドレスプールのみを表示する場合は、[Sbunet Type] エリアで [IPv4 only] または [Dual-Stack] オプションをクリックします。

ステップ 6 ツリービューで、目的の IP アドレスプールにカーソルを合わせてクリックすると、次の情報を含むスライドインペインが表示されます。

- IP アドレスプールのサブネットタイプ。
- それぞれのプール下にある使用可能な IP アドレスと [Pool CIDR]、[Gateway]、[DHCP Server(s)]、および [DNS Server(s)] の割合。
- 各プールで使用されている IP アドレスの割合。

ステップ 7 [Used] エリアで、[Assigned] をクリックすると、[Device Name]、[IP Address]、および [Site] に基づいてフィルタ処理されたデバイスに割り当てられた IP アドレスのリストが表示されます。

ステップ 8 [Unassignable] をクリックすると、[Device Name]、[IP Address]、および [Site] に基づいてフィルタ処理されたデバイスに割り当てることができない未割り当て IP アドレスのリストが表示されます。

ステップ 9 [Edit] をクリックして、IP アドレスプールを編集します。

ステップ 10 [Release] をクリックして、IP アドレスプールを解放します。

（注）
- グローバルプールのサイドバーでは、特定のプールについて、すべての子プールにおける使用状況を確認できます。
- グローバル IP アドレスプールとサイト IP アドレスプールには、ブロックリストに登録された IP アドレスを設定できます。
- サブプールにはブロックリストに登録された IP アドレスを含めることはできません。
  - Cisco DNA Center は、ブロックリストに登録された IP アドレスが含まれている場合、CIDR アドレスプールの IP アドレスプール作成要求を拒否します。
  - 次の空き IP アドレスプール要求では、Cisco DNA Center はブロックリストに登録された IP アドレスをスキップして、次の IP アドレス空きプールを見つけます。

ステップ 11 （オプション）テーブルデータをエクスポートするには、サイドバーで [Export] をクリックします。

サービス プロバイダ プロファイルの設定

特定の WAN プロバイダのサービス クラスを定義するサービス プロバイダ（SP）プロファイルを作成することができます。サービスモデルには、4 クラス、5 クラス、6 クラス、および 8 クラスを定義できます。SP プロファイルの作成後、アプリケーションポリシーの範囲内（必要に応じてインターフェイスのサブラインレート設定を含む）のアプリケーションポリシーと WAN インターフェイスにそのプロファイルを割り当てることができます。

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

ステップ 2 **[Qos]** 領域で、**[Add]** をクリックします。

ステップ 3 **[Profile Name]**フィールドに、SP プロファイルの名前を入力します。

ステップ 4 [WAN Provider] ドロップダウンリストから、新しいサービスプロバイダを入力するか、既存のプロバイダを選択します。

ステップ 5 [Model] ドロップダウンリストから、クラスモデル（[4 class]、[5 class]、[6 class]、および [8 class]）のいずれかを選択します。

これらのクラスの詳細については、サービス プロバイダのプロファイル（648 ページ）を参照してください。

グローバル ワイヤレス設定の構成

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

（注） ワイヤレス センサー デバイス プロファイルを作成できるのは、Cisco Aironet 1800s アクティブ センサー デバイスに対してのみです。

エンタープライズ ワイヤレス ネットワーク用 SSID の作成

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

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

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

ステップ 2 [Wireless] タブをクリックします。

ステップ 3 左側のペインで、[Global] を選択します。

ステップ 4 [SSID] テーブルで、Add ドロップダウン アイコンから [Enterprise] を選択します。

ステップ 5 [Wireless SSID] ワークフローで、[Basic Settings] のセットアップを完了します。

a) [Sensor] トグル ボタンが使用可能な場合は、無効になっていることを確認します。

b) [Wireless Network Name (SSID)] フィールドに、ワイヤレス ネットワークの一意の名前を入力します。

c) [Wireless Option] の設定で、次のいずれかのオプション ボタンをクリックします。

- [Multi band operation (2.4GHz, 5GHz, 6GHz)]：WLAN は 2.4 GHz、5 GHz、および 6 GHz 用に作成され、バンドセレクトは無効になっています。
- [Multi band operation with band select] ：WLAN は 2.4 GHz、5 GHz、および 6 GHz 用に作成され、バンドセレクトは有効になっています。
- [5 GHz only]：WLAN が 5 GHz 用に作成され、バンドセレクトは無効になっています。
- [2.4 GHz only]：WLAN が 2.4 GHz 用に作成され、バンドセレクトは無効になっています。
- [6 GHz only]：WLAN は 6 GHz 用に作成され、バンドセレクトは無効になっています。

d) [Primary Traffic Type] 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。

- [VoIP (Platinum)]：ワイヤレス ネットワークの QoS は、ワイヤレス音声およびデータ トラフィック用に最適化されています。
- [Video (Gold)]：ワイヤレス ネットワークの QoS はビデオ トラフィック用に最適化されています。
- [Best Effort (Silver)]：ワイヤレス ネットワークの QoS は、ワイヤレス データ トラフィック用にのみ最適化されています。

- [Non-real Time (Bronze)]：ワイヤレスネットワークの QoS は、低帯域幅の使用に最適化されています。

e) [SSID STATE] 設定では、トグルボタンをクリックして、次の設定を有効または無効にします。

- [Admin Status]：このトグルボタンを使用して、AP の無線をオンまたはオフにします。[Admin Status] が無効になっている場合、AP は ワイヤレスコントローラ に関連付けられたままで、アクセス可能であり、AP には引き続きライセンスが必要です。
- [Broadcast SSID]：範囲内のすべてのワイヤレスクライアントに対して SSID の可視性を有効または無効にするには、このトグルボタンを使用します。

ステップ 6 [Security Settings] の設定を完了します。

a) [Level of Security] で、このネットワークの暗号化および認証タイプを選択します。サイト、ビルディング、およびフロアは、グローバル階層から設定を継承することに注意してください。サイト、ビルディング、またはフロアレベルでセキュリティレベルをオーバーライドできます。

- [Enterprise]：それぞれのチェックボックスをオンにすることで、[WPA2] と [WPA3] の両方のセキュリティ認証を設定できます。デフォルトでは、[WPA2] チェックボックスが有効になっています。

  （注） Wi-Fi Protected Access（WPA2）では、Counter Mode と暗号ブロック連鎖メッセージ認証コードプロトコルを使用した、より強力な高度暗号化規格アルゴリズム（AES-CCMP）が使用されます。

  WPA3 は、WPA の最新バージョンです。これは、Wi-Fi ネットワークの認証と暗号化を提供するプロトコルとテクノロジーのスイートです。WPA3 エンタープライズは、センシティブ データ ネットワーク用に、より高いグレードのセキュリティプロトコルを提供します。

  2.4 GHz および 5 GHz 帯域のみを使用するマルチバンド操作の場合、WPA2 を有効にする必要があります（WPA3 はオプションです）。2.4 GHz、5 GHz、および 6 GHz 帯域を使用したマルチバンド動作の場合、Cisco IOS 17.7 以降を搭載したデバイスで 6 GHz 帯域を動作するには、WPA3 を有効にし WPA2 を無効にする必要があります。

- [Personal]：[Personal] を選択した場合は、[Pass Phrase] フィールドにパスフレーズキーを入力します。このキーは、クライアントと認証サーバー間のペアワイズマスターキー（PMK）として使用されます。

（注） WPA3-Personal は、パスワードベースの堅牢な認証を提供することによって、個人ユーザーに対する保護を強化します。これにより、ブルートフォース辞書攻撃がはるかに困難になり、時間がかかるようになります。

WPA2 パーソナルの場合は、サイト、ビルディング、またはフロアレベルで、事前共有キー（PSK）をオーバーライドできます。ビルディングレベルで PSK をオーバーライドすると、後続のフロアは新しい設定を継承します。詳細については、事前共有キーのオーバーライド （253 ページ）を参照してください。

2.4 GHz および 5 GHz 帯域のみを使用するマルチバンド操作の場合、WPA2 を有効にする必要があります（WPA3 はオプションです）。2.4 GHz、5 GHz、および 6 GHz 帯域を使用したマルチバンド動作の場合、Cisco IOS 17.7 以降を搭載したデバイスで 6 GHz 帯域を動作するには、WPA3 を有効にし WPA2 を無効にする必要があります。

- [Open Secured]：[Assign Open SSID] ドロップダウンリストから、クライアントをオープンでセキュアな SSID にリダイレクトするためのオープン SSID を選択します。オープンでセキュアなポリシーは、最小限のセキュリティを提供します。

  （注） Fast Transition は、オープンでセキュアな SSID には適用できません。

  オープンでセキュアな SSID はオープン SSID に依存しているため、オープンでセキュアな SSID でアンカーを有効にする前に、オープン SSID でアンカーを有効にしておく必要があります。

- [Open]：オープンなポリシーはセキュリティを備えていません。すべてのデバイスが認証なしでワイヤレスネットワークに接続できます。

b) [Authentication, Authorization, and Accounting Configuration] で、[Configure AAA] をクリックして、エンタープライズ ワイヤレス ネットワーク SSID 用の AAA サーバーを追加および設定します。

詳細については、「エンタープライズ ワイヤレス ネットワーク用の AAA サーバーの設定」を参照してください。

c) 次のチェックボックスの 1 つ以上をオンにします。

- [Fast Lane]：このネットワークで fastlane 機能を有効にするには、このチェックボックスをオンにします。

  （注） fastlane を有効にすると、最適化されたレベルのワイヤレス接続と 拡張 QoS を受信するように Cisco IOS デバイスを設定できます。

- [Identity PSK]（個人レイヤ 2 セキュリティ用）：SSID 内の個人またはユーザーグループのために作成できる一意の事前共有キーを有効にするには、このチェックボックスをオンにします。

- [MAC Filtering]：ワイヤレスネットワークでの MAC ベースのアクセス制御またはセキュリティを有効にするには、このチェックボックスをオンにします。

  （注） MAC フィルタリングを有効にすると、ワイヤレス LAN に追加した MAC アドレスにのみ WLAN への接続が許可されます。

- [Deny RCM Clients]：ランダム化された MAC アドレスを持つクライアントを拒否するには、このチェックボックスをオンにします。
- [Enable Posture]：ポスチャ評価を有効にするには、このチェックボックスをオンにします。ポスチャを有効にすると、[Pre-Auth ACL List Name] ドロップダウンリストが表示されます。ポスチャは、Cisco Identity Services Engine（ISE）のサービスです。ポスチャを使用すると、ネットワークに接続されているすべてのエンドポイントの企業セキュリティ ポリシーとのコンプライアンスに関するステート（ポスチャとも呼ばれる）をチェックできます。これにより、ネットワークの防護領域にアクセスするクライアントを制御できます。
- [Pre-Auth ACL List Name]：ドロップダウンリストから、SSID にマッピングするために作成した ACL リスト名を選択します。

（注） ポスチャには AAA 設定が必須です。[Configure AAA] をクリックして、エンタープライズ ワイヤレス ネットワーク SSID 用の AAA サーバーを追加します。

d) [Next] をクリックします。

ステップ 7 [Advance Settings] の設定を完了します。

a) [Fast Transition (802.11r)] で、次の手順を実行します。

- [Adaptive]、[Enable]、または [Disable] モードを選択します。

（注） 802.11r を使用すると、ワイヤレスクライアントは、ある AP から別の AP にすばやくローミングできます。Fast Transition によって、ワイヤレスクライアントが AP から別の AP にローミングするときの接続の中断が軽減されます。

- 分散システム経由の高速移行を有効にするには、[Over the DS] チェックボックスをオンにします。

b) [MFP Client Protection] で、[Optional]、[Required]、または [Disabled] 設定を選択します。

（注） 管理フレーム保護（MFP）により、管理フレームのセキュリティが強化されます。これによって、AP とクライアントとの間で送受信される、保護および暗号化されていない 802.11 管理メッセージのセキュリティが確保されます。MFP は、インフラストラクチャとクライアントサポートの両方を実現します。

デフォルトでは、[Optional] が選択されています。[Required] を選択すると、MFP がネゴシエートされている場合（つまり、WPA2 が ワイヤレスコントローラ 上で設定されており、クライアントも WPA2 用に設定されていて、CCXv5 MFP をサポートしている場合）にのみ、クライアントはアソシエーションを許可されます。

c) [11K] で、次の設定を指定します。

- [Neighbor List]：このチェックボックスをオンにして、すべての 11k 対応クライアントが、ローミングの候補となる既知のネイバーAP に関するネイバーレポートを要求できるように設定します。

（注） ローミングを容易に行うため、AP にアソシエートした 11k 対応クライアントは、ネイバーAPのリストに対する要求を送信します。この要求は、アクションフレームと呼ばれる 802.11 管理フレームの形式で送信されます。AP は、同じ WLAN 上にあるネイバー AP の Wi-Fi チャネル番号が付いたリストを使用して応答します。この応答もアクション フレームです。クライアントは応答フレームに基づき、次のローミング先の AP 候補を識別します。

- [Session Timeout]：クライアントセッションがアクティブである最大時間を設定するには、このチェックボックスをオンにします。この時間が経過すると再認証を受ける必要があります。

  （注） デフォルトでは、[Session Timeout] が 1800 秒のタイムアウト付きで有効になります。

- [Client Exclusion]：クライアント除外タイマーを設定するには、このチェックボックスをオンにします。

  （注） ユーザーが認証に失敗すると、ワイヤレスコントローラ はクライアントを接続から除外します。除外タイマーが期限切れになるまで、クライアントはネットワークへの接続を許可されません。デフォルトでは、[Client Exclusion] が 180 秒のタイムアウト付きで有効になります。

d) [11v BSS Transition Support] で、次の設定を指定します。

- [BSS Max Idle Service]：アイドル期間タイマー値を設定するには、このチェックボックスをオンにします。アイドル期間タイマー値は、AP からクライアントへのアソシエーションおよび再アソシエーション応答フレームを使用して送信されます。

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

- [Client User Idle Timeout]：WLAN のユーザー アイドル タイムアウトを設定するには、このチェックボックスをオンにします。

  （注） クライアントが送信するデータがユーザー アイドル タイムアウトとして指定されたしきい値のクォータを超える場合、クライアントはアクティブであると見なされ、ワイヤレスコントローラ は別のタイムアウト期間を開始します。

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

- [Directed Multicast Service]：Directed Multicast Service 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。

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

e) [Radius Client Profiling] で、このトグルボタンを使用して WLAN での RADIUS プロファイリングを有効または無効にします。

（注） この機能を有効にするには、1 つ以上の AAA または PSN サーバーが必要です。

f) （オプション）[NAS-ID] で、次の設定を指定します。

- [NAS-ID Opt] ドロップダウンリストから、必要なタイプのネットワーク アクセス サーバー識別子（NAS ID）を選択します。
- （オプション）NAS ID のカスタムスクリプトを指定するには、[NAS-ID Opt] ドロップダウンリストから [Custom Option] を選択し、対応する [Custom Script for Opt] フィールドにカスタムスクリプトを入力します。カスタムスクリプトには、最大 31 文字の英数字、特殊文字、およびスペースを入力できます。Cisco DNA Center はカスタムスクリプトでの特殊文字？" < および末尾のスペースをサポートしていません。

  （注） Cisco DNA Center は、Cisco IOS XE リリース 17.7 以降を実行する Cisco Catalyst 9800 シリーズ ワイヤレスコントローラに対してのみ、カスタムスクリプトで NAS ID をサポートします。

- （オプション）[+] をクリックして、別のネットワーク アクセス サーバー識別子を追加します。最大 3 つの NAS ID を追加できます。

  （注） Cisco DNA Center では Cisco AireOS コントローラに 1 つの NAS ID のみを適用します。**[Design]** > **[Network Settings]** > **[Wireless]** ウィンドウからサイトレベルで NAS ID を上書きできます。

g) [Next] をクリックします。

ステップ 8 [Associate SSID to Profile] の手順を完了します。

a) 左側のペインからプロファイルを選択し、[Associate Profile] をクリックします。

プロファイルがない場合は、[Add Profile] をクリックして、プロファイル設定を指定します。詳細については、ワイヤレス用のネットワークプロファイルの作成 （304 ページ）を参照してください。

b) [Next] をクリックします。

ステップ 9 [Summary] 設定を確認します。変更が必要な場合は、[Edit] をクリックします。

ステップ 10 **[保存 (Save)]** をクリックします。

SSID が作成されます。

事前共有キーのオーバーライド

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

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

ステップ 2 左側のペインで、PSK を編集するサイト、ビルディング、またはフロアを選択します。

ステップ 3 [Enterprise Wireless] の下の [Passphrase] フィールドをクリックし、PSK SSID の新しいパスフレーズを入力します。

ステップ 4 **[保存（Save）]** をクリックします。

「`Passphrase for the SSID(s) updated successfully`」という成功メッセージが表示されます。

SSID の横にある検証アイコン にカーソルを合わせると、この設定の継承元が表示されます。

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

認証前アクセスコントロールリストの作成

認証前 ACL 機能を使用すると、Web 認証用の認証前 ACL を作成して、認証が完了する前に特定のタイプのトラフィックを許可できます。この ACL は、Cisco Identity Services Engine（ISE）の access-accept で参照され、ACL によって許可されるトラフィックと拒否されるトラフィックを定義します。シスコ ワイヤレス コントローラで設定した ACL は、管理インターフェイス、AP マネージャインターフェイス、任意の動的インターフェイス、または WLAN に適用されてワイヤレスクライアントとの間の双方向のデータトラフィックを制御します。または、コントローラの中央処理装置（CPU）に適用してCPU宛のすべてのトラフィックを制御します。IPv4 と IPv6 の両方の ACL を設定できます。

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

ステップ 2 [Wireless] タブをクリックします。

ステップ 3 左側のペインで、[Global] を選択します。

ステップ 4 [Pre-Auth Access Control Lists] エリアで、[Add] をクリックして新しい認証前 ACL を作成します。

ステップ 5 [New Pre-Auth ACL] スライドインペインで、次のように設定します。

- [Pre-Auth ACL List Name] フィールドに、ACL リストの名前を入力します。
- [Pre-Auth ACL Name] フィールドに、認証前 ACL の名前を入力します。
- [IP Addresses] タブをクリックし、作成する ACL タイプ（[IPV4] または [IPV6]）を選択します。

ステップ 6 [IP Addresses] タブをクリックし、作成する ACL タイプ（[IPV4] または [IPV6]）を選択します。

- [Protocol] ドロップダウン リストから、この ACL に使用する IP パケットのプロトコル ID を選択します。プロトコルオプションは、[Any]、[TCP]、または [UDP] です。

- [Source Port] フィールドに、送信元ポート番号を入力します。指定できる範囲は 0 ～ 65535 です。ポートオプションは、ネットワーキング スタックとのデータ送受信をするアプリケーションによって使用されます。一部のポートは、Telnet、SSH、HTTP など特定のアプリケーション用に指定されています。
- [Source IP Address] フィールドに、送信元の IP アドレスとネットマスクを入力します。IPv6 ACL を設定している場合は、[Source IP Address] フィールドに送信元の IPv6 アドレスとプレフィックスの長さを入力します。
- [Source Subnet] ドロップダウンリストから、送信元サブネットの値を選択します。
- [Destination Port] に宛先ポート番号を入力します。
- [Destination IP Address] に、宛先の IP アドレスおよびネットマスクを入力します。IPv6 ACL を設定している場合は、宛先の IPv6 アドレスとプレフィックス長を入力します。
- [Destination Subnet] ドロップダウンリストから、宛先サブネットの値を選択します。
- アイコンをクリックすると、複数のルールを追加できます。最大 256 個のルールを追加できます。

ステップ 7 [Walled Garden URLs] タブをクリックして、キャプティブポータルとウォールドガーデンの Web 認証の許可リストに特定の URL を追加します。URL の許可リストにアクセスする際に認証は必要ありません。許可リストに含まれていないサイトにアクセスしようとすると、ログインページにリダイレクトされます。

- [URL] フィールドに URL を入力し、をクリックして Web 認証の許可リストに URL を追加します。最大 32 個の URL エントリを追加できます。

ステップ 8 **[Save]** をクリックします。

ステップ 9 エンタープライズワイヤレスネットワークの SSID を作成するときに、ACL を SSID にマッピングします。

エンタープライズ ワイヤレス ネットワーク用の AAA サーバーの設定

始める前に

- **[System Settings]** > **[External Services]** > **[Authentication and Policy Servers]** ページで、AAA サーバーが定義されていることを確認してください。
- この手順を実行するには、管理者（ROLE_ADMIN）またはポリシー管理者（ROLE_POLICY_ADMIN）権限、および適切な RBAC スコープが必要です。

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

ステップ 2 [Wireless] タブをクリックします。

ステップ 3 左側のペインで [Global] が選択されていることを確認します。

ステップ 4 [SSID] テーブルの [Action] 列で、AAA サーバーを設定する SSID に対して [Configure AAA] をクリックします。

[Configure AAA Server] スライドインペインが表示されます。

ステップ 5 [Server] ドロップダウンリストから、[Search] フィールドに名前を入力してサーバーの IP アドレスを検索するか、AAA IP アドレスを選択します。

（注） [Configure AAA] 機能は、Mobility Express デバイスではサポートされていません。

ステップ 6 [+] をクリックして、**追加のサーバー**を追加します。

（注） Catalyst 9000 スイッチ用 Cisco Catalyst 9800 組み込みワイヤレスコントローラのエンタープライズ ワイヤレス ネットワークの SSID には、最大 6 つの AAA サーバーを設定できます。

ステップ 7 [Additional Server] ドロップダウンリストから、サーバーの IP アドレスを選択します。

ステップ 8 （任意） サーバーまたは追加のサーバーを削除するには、各サーバーの横にある削除アイコンをクリックします。

ステップ 9 [構成] をクリックします。

（注） Cisco DNA Center では、サイトレベルで SSID の一連の AAA サーバー設定をオーバーライドできます。SSID ごとにオーバーライドされた一連の AAA 設定ごとに、対応する AAA サーバーがマッピングされた新しい WLAN プロファイルが Cisco DNA Center によって作成されます。異なるフロアの SSID がオーバーライドされ、AAA サーバーで変更を行うと、フロア数に等しい数の新しい WLAN プロファイルが Cisco DNA Center によって作成されます。

サイトレベルで AAA サーバーをオーバーライドするためには、デバイスを再プロビジョニングする必要があります。「ワイヤレス デバイス プロビジョニングの概要」を参照してください。

ゲスト ワイヤレス ネットワークの SSID の作成

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

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

ステップ 2 [Wireless] タブをクリックします。

ステップ 3 左側のペインで、[Global] が選択されていることを確認します。

ステップ 4 [SSID] テーブルで、Add ドロップダウンアイコンから [Guest] を選択します。

ステップ 5 [Wireless SSID] ワークフローで、[Basic Settings] のセットアップを完了します。

a) [Wireless Network Name (SSID)] フィールドに、ワイヤレスネットワークの一意の名前を入力します。

b) [Wireless Option] の設定で、次のいずれかのオプションボタンをクリックします。

- [Multi band operation (2.4GHz, 5GHz, 6GHz)]：WLAN は 2.4 GHz、5 GHz、および 6 GHz 用に作成され、バンドセレクトは無効になっています。

- [Multi band operation with band select] ：WLAN は 2.4 GHz、5 GHz、および 6 GHz 用に作成され、バンドセレクトは有効になっています。
- [5 GHz only]：WLAN が 5 GHz 用に作成され、バンドセレクトは無効になっています。
- [2.4 GHz only]：WLAN が 2.4 GHz 用に作成され、バンドセレクトは無効になっています。
- [6 GHz only]：WLAN は 6 GHz 用に作成され、バンドセレクトは無効になっています。

c) [Primary Traffic Type] 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。

- [VoIP (Platinum)]：ワイヤレスネットワークの QoS は、ワイヤレス音声およびデータトラフィック用に最適化されています。
- [Video (Gold)]：ワイヤレスネットワークの QoS はビデオトラフィック用に最適化されています。
- [Best Effort (Silver)]：ワイヤレスネットワークの QoS は、ワイヤレス データ トラフィック用にのみ最適化されています。
- [Non-real Time (Bronze)]：ワイヤレスネットワークの QoS は、低帯域幅の使用に最適化されています。

d) [SSID STATE] 設定では、トグルボタンをクリックして、次の設定を有効または無効にします。

- [Admin Status]：このトグルボタンを使用して、AP の無線をオンまたはオフにします。[Admin Status] が無効になっている場合、AP は ワイヤレスコントローラ に関連付けられたままで、アクセス可能であり、AP には引き続きライセンスが必要です。
- [Broadcast SSID]：範囲内のすべてのワイヤレスクライアントに対して SSID の可視性を有効または無効にするには、このトグルボタンを使用します。

ステップ 6 [Security Settings] の設定を完了します。

a) [L2 Security] 設定で、L2 暗号化および認証タイプを選択します。

- [Enterprise]：[WPA2] または [WPA3] のいずれかのセキュリティ認証タイプを設定するには、それぞれのチェックボックスをオンにします。デフォルトでは、[WPA2] チェックボックスが有効になっています。

（注） Wi-Fi Protected Access（WPA2）では、Counter Mode と暗号ブロック連鎖メッセージ認証コードプロトコルを使用した、より強力な高度暗号化規格アルゴリズム（AES-CCMP）が使用されます。Fast transition は、エンタープライズ WPA2 SSID に適用できます。

WPA3 セキュリティ認証は、WPA の最新バージョンです。これは、Wi-Fi ネットワークの認証と暗号化を提供するプロトコルとテクノロジーのスイートです。WPA3 エンタープライズは、センシティブ データ ネットワーク用に、より高いグレードのセキュリティプロトコルを提供します。

2.4 GHz および 5 GHz 帯域のみを使用するマルチバンド操作の場合、WPA2 を有効にする必要があります（WPA3 はオプションです）。2.4 GHz、5 GHz、および 6 GHz 帯域を使用したマルチバンド動作の場合、Cisco IOS 17.7 以降を搭載したデバイスで 6 GHz 帯域を動作するには、WPA3 を有効にし WPA2 を無効にする必要があります。

- [Personal]：**WPA2** と **WPA3** の両方を設定したり、**WPA2** と **WPA3** を個別に設定したりするには、それぞれのチェックボックスをオンにします。

（注） WPA3 パーソナルセキュリティ認証は、パスワードベースの堅牢な認証を提供することによって個人ユーザーに対する保護を強化します。これにより、ブルートフォース辞書攻撃がはるかに困難になり、時間がかかるようになります。

[Pass Phrase] フィールドにパスフレーズキーを入力します。このキーは、クライアントと認証サーバーの間で Pairwise Master Key（PMK; ペアワイズ マスター キー）として使用されます。

2.4 GHz および 5 GHz 帯域のみを使用するマルチバンド操作の場合、WPA2 を有効にする必要があります（WPA3 はオプションです）。2.4 GHz、5 GHz、および 6 GHz 帯域を使用したマルチバンド動作の場合、Cisco IOS 17.7 以降を搭載したデバイスで 6 GHz 帯域を動作するには、WPA3 を有効にし WPA2 を無効にする必要があります。

- [Open Secured]：[Assign Open SSID] ドロップダウンリストから、オープン SSID に関連付けるためのオープン SSID を選択します。関連付けにより、オープン SSID が保護されます。オープンでセキュアな SSID に関連付ける前に、オープン SSID が作成されている必要があります。

（注） Fast Transition は、オープンでセキュアな SSID には適用できません。

オープンでセキュアな SSID はオープン SSID に依存しているため、オープンでセキュアな SSID でアンカーを有効にする前に、オープン SSID でアンカーを有効にしておく必要があります。

- [Open]：オープンなポリシーはセキュリティを備えていません。すべてのデバイスが認証なしでワイヤレスネットワークに接続できます。

b) [L3 Security] 設定で、L3 暗号化および認証タイプを選択します。

- [Web Policy]：L3 セキュリティを強化します。

[Authentication Server] で、これらの認証サーバー設定を指定します。

認証サーバ タイプ	説明
Central Web Authentication（中央 Web 認証）	中央 Web 認証（CWA）に AAA サーバーを使用します。 （オプション）CWA に Cisco ISE を選択した場合は、[What kind of portal are you creating today?] ドロップダウンリストで、作成するポータルのタイプを選択します。 • [Self Registered]：ゲストは自己登録ゲストポータルにリダイレクトされ、情報を提供して登録して、自動的にアカウントを作成します。 • [HotSpot]：ゲストはログイン情報なしでネットワークにアクセスできます。 （オプション）CWA に Cisco ISE を選択した場合は、[Where will your guests redirect after successful authentication?] ドロップダウンリストで、認証が成功した後にゲストをリダイレクトする場所を選択します。 • [Success page]：ゲストは [Authentication Success] ウィンドウにリダイレクトされます。 • [Original URL]：ゲストは最初にリクエストした URL にリダイレクトされます。 • [Custom URL]：ゲストはここで特定されたカスタム URL にリダイレクトされます。[Redirect URL] フィールドにリダイレクト URL を入力します。
• **Web 認証（内部）** • **Web 認証（外部）**	レイヤ 3 セキュリティ方式である Web 認証（Web Auth）を使用すると、クライアントは、何らかの認証方式に合格するまでの間、Dynamic Host Configuration Protocol（DHCP）およびドメインネームシステム（DNS）のトラフィックを通過させることができます。 Web 認証（内部）の場合、クライアントは シスコ ワイヤレス コントローラによって作成されたページにリダイレクトされます。 Web 認証（外部）の場合は、クライアントが、指定された URL にリダイレクトされます。[Web Auth Url] フィールドにリダイレクト URL を入力します。
• **Web パススルー（内部）** • **Web パススルー（外部）**	Web パススルーは、ゲストアクセスに使用されるソリューションであり、認証ログイン情報は必要ありません。Web パススルー認証では、ワイヤレスユーザーがインターネットを初めて使用するとき、使用ポリシーページにリダイレクトされます。ポリシーを承認すると、ユーザーはインターネットを使用できます。

- [Open]：レイヤ 3 レベルのセキュリティがなく、どのデバイスも SSID に接続できます。

c) [Web Authentication Internal]、[Web Authentication External]、[Web Passthrough Internal]、または [Web Passthrough External] を選択した場合、[Timeout Settings for sleeping clients] の設定で、スリープしているクライアントの認証を選択します。

- [Always authenticate]：スリープ状態のクライアントの認証が有効になります。
- [Authenticate after]：再認証が必要になるまでスリープ状態にあるクライアントが記憶される期間を入力します。有効な範囲は 10 ～ 43200 分、デフォルト期間は 720 分です。

（注） ゲストアクセスで Web 認証済みクライアントは、ログインページから別の認証プロセスを実行せずにスリープおよび復帰することを許可されています。再認証が必要になるまでスリープ状態にあるクライアントが記録される期間を設定できます。有効な範囲は 10 ～ 43200 分、デフォルトは 720 分です。WLAN にマッピングされるユーザ グループ ポリシーと WLAN に、期間を設定できます。スリープ タイマーは、アイドル タイムアウト後に有効になります。クライアントタイムアウトが WLAN のスリープタイマーに設定された時間より短い場合は、クライアントのライフタイムがスリープ時間として使用されます。

d) [Authentication, Authorization, and Accounting Configuration] の設定で、[Configure AAA] をクリックして、ゲスト ワイヤレス ネットワーク SSID 用の AAA サーバーを追加および設定します。

詳細については、「ゲスト ワイヤレス ネットワーク用の AAA サーバーの設定」を参照してください。

e) 次のチェックボックスをオンにします（複数可）。

- [Fast Lane]：このネットワークで fastlane 機能を有効にするには、このチェックボックスをオンにします。

（注） fastlane を有効にすると、最適化されたレベルのワイヤレス接続と拡張 QoS を受信するように Cisco IOS デバイスを設定できます。

- [Identity PSK]（個人 L2 セキュリティ用）：SSID 内の個人またはユーザーグループのために作成できる一意の事前共有キーを有効にするには、このチェックボックスをオンにします。
- [MAC Filtering]：ワイヤレスネットワークでの MAC ベースのアクセス制御またはセキュリティを有効にするには、このチェックボックスをオンにします。

（注） MAC フィルタリングを有効にすると、ワイヤレス LAN に追加した MAC アドレスにのみ WLAN への接続が許可されます。

- [Deny RCM Clients]：ランダム化された MAC アドレスを持つクライアントを拒否するには、このチェックボックスをオンにします。

f) [Next] をクリックします。

ステップ 7 [Advance Settings] の手順を完了します。

a) [Fast Transition (802.11r)] で、次のように設定します。

- [Adaptive]、[Enable]、または [Disable] モードを選択します。

（注） 802.11r を使用すると、ワイヤレスクライアントは、ある AP から別の AP にすばやくローミングできます。Fast Transition によって、ワイヤレスクライアントが AP から別の AP にローミングするときの接続の中断が軽減されます。

- 分散システム経由の高速移行を有効にするには、[Over the DS] チェックボックスをオンにします。

b) [MFP Client Protection] 設定で、[Optional]、[Required]、または [Disabled] を選択します。

（注） 管理フレーム保護（MFP）により、管理フレームのセキュリティが強化されます。これによって、AP とクライアントとの間で送受信される、保護および暗号化されていない 802.11 管理メッセージのセキュリティが確保されます。MFP は、インフラストラクチャとクライアントサポートの両方を実現します。

デフォルトでは、[Optional] が選択されています。[Required] を選択すると、MFP がネゴシエートされている場合（つまり、WPA2 が ワイヤレスコントローラ 上で設定されており、クライアントも WPA2 用に設定されていて、CCXv5 MFP をサポートしている場合）にのみ、クライアントはアソシエーションを許可されます。

c) [11K] で、次のように設定します。

- [Neighbor List]：このチェックボックスをオンにすると、すべての 11k 対応クライアントが、ローミングの候補となる既知のネイバー AP に関するネイバーレポートを要求できるようになります。

（注） ローミングを容易に行うため、AP にアソシエートした 11k 対応クライアントは、ネイバーAP のリストに対する要求を送信します。この要求は、アクションフレームと呼ばれる 802.11 管理フレームの形式で送信されます。AP は、同じ WLAN 上にあるネイバー AP の Wi-Fi チャネル番号が付いたリストを使用して応答します。この応答もアクション フレームです。クライアントは応答フレームに基づき、次のローミング先の AP 候補を識別します。

- [Session Timeout]：クライアントセッションがアクティブである最大時間を設定するには、このチェックボックスをオンにします。この時間が経過すると再認証を受ける必要があります。

（注） デフォルトでは、[Session Timeout] が 1800 秒のタイムアウト付きで有効になります。

- [Client Exclusion]：クライアント除外タイマーを設定するには、このチェックボックスをオンにします。

（注） ユーザーが認証に失敗すると、ワイヤレスコントローラ はクライアントを接続から除外します。除外タイマーが期限切れになるまで、クライアントはネットワークへの接続を許可されません。デフォルトでは、[Client Exclusion] が 180 秒のタイムアウト付きで有効になります。

d) [11v BSS Transition Support] で、次のように設定します。

- [BSS Max Idle Service]：アイドル期間タイマー値を設定するには、このチェックボックスをオンにします。アイドル期間タイマー値は、APからクライアントへのアソシエーションおよび再アソシエーション応答フレームを使用して送信されます。

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

- [Client User Idle Timeout]：WLAN のユーザー アイドル タイムアウト期間を設定するには、このチェックボックスをオンにします。

  （注） クライアントが送信するデータがユーザー アイドル タイムアウト期間として指定されたしきい値のクォータを超える場合、クライアントはアクティブであると見なされ、ワイヤレスコントローラは別のタイムアウト期間を開始します。

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

- [Directed Multicast Service]：Directed Multicast Service 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。

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

e) （オプション）[NAS-ID] で、次の設定を指定します。

- [NAS-ID Opt] ドロップダウンリストから、必要なタイプのネットワーク アクセス サーバー識別子（NAS ID）を選択します。
- （オプション）NAS ID のカスタムスクリプトを指定するには、[NAS-ID Opt] ドロップダウンリストから [Custom Option] を選択し、対応する [Custom Script for Opt] フィールドにカスタムスクリプトを入力します。カスタムスクリプトには、最大 31 文字の英数字、特殊文字、およびスペースを入力できます。Cisco DNA Center はカスタムスクリプトでの特殊文字？" < および末尾のスペースをサポートしていません。

  （注） Cisco DNA Center は、Cisco IOS XE リリース 17.7 以降を実行する Cisco Catalyst 9800 シリーズ ワイヤレスコントローラに対してのみ、カスタムスクリプトで NAS ID をサポートします。

- （オプション）[+] をクリックして、別のネットワーク アクセス サーバー識別子を追加します。最大 3 つの NAS ID を追加できます。

  （注） Cisco DNA Center では Cisco AireOS コントローラに 1 つの NAS ID のみを適用します。**[Design]** > **[Network Settings]** > **[Wireless]** ウィンドウからサイトレベルで NAS ID を上書きできます。

f) [Next] をクリックします。

ステップ 8 [Associate SSID to Profile] の手順を完了します。

a) 左側のペインで、プロファイルをクリックします。

b) プロファイルがない場合は、[Add Profile] をクリックして、プロファイル設定を指定します。

- [Profile Name]：ワイヤレスプロファイルの名前を入力します。
- [Fabric]：SSID がファブリックか非ファブリックかを指定します。

（注） ファブリック SSID は、ソフトウェア定義型アクセス（SD-Access）の一部であるワイヤレスネットワークです。SD アクセスは、有線およびワイヤレスネットワークの設定、ポリシー、およびトラブルシューティングを自動化し、簡素化するソリューションです。ファブリック SSID を使用する場合は、SD アクセスが必須です。非ファブリックは、SD アクセスを必要としない従来のワイヤレスネットワークです。

非ファブリック SSID の場合は、次の設定を選択します。

- [Interface]：[Interface Management] ドロップダウンリストからインターフェイスを選択するか、プラスアイコン をクリックして新しいワイヤレスインターフェイスを追加します。

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

- [VLAN Group]：[VLAN Group Name] ドロップダウンリストから VLAN グループを選択するか、プラスアイコン をクリックして VLAN グループを追加します。

- [Do you need Anchor for this SSID?]：SSID をアンカーにするかどうかを選択します。
- [Flex Connect Local Switching]：WLAN のローカルスイッチングを有効にするには、チェックボックスをオンにします。ローカルスイッチングを有効化すると、この WLAN をアドバタイズするすべての FlexConnect AP がデータパケットをローカルにスイッチできます。

（注） SSID に関して [Flex Connect Local Switching] を有効にしている場合、ネットワークプロファイルがマッピングされている特定のフロア上のすべての AP が FlexConnect モードに切り替わります。

c) [Associate Profile] をクリックして、プロファイルを選択します。

d) [Next] をクリックします。

ステップ 9 [Summary] の手順を確認します。変更が必要な場合は、[Edit] をクリックします。

ステップ 10 SSID の設定を保存するには、[Save] をクリックします。

SSID が作成されます。

ゲスト ワイヤレス ネットワーク用の AAA サーバーの設定

始める前に

- **[System Settings]** > **[External Services]** > **[Authentication and Policy Servers]** ウィンドウで、AAA サーバーが定義されていることを確認してください。
- この手順を実行するには、管理者（ROLE_ADMIN）またはポリシー管理者（ROLE_POLICY_ADMIN）権限、および適切な RBAC スコープが必要です。

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

ステップ 2 [Wireless] タブをクリックします。

ステップ 3 左側のペインで [Global] が選択されていることを確認します。

ステップ 4 [SSID] テーブルの [Action] 列で、AAA サーバーを設定する SSID の [Configure AAA] をクリックします。

ステップ 5 [Configure AAA Server] スライドインペインの [Server] ドロップダウンリストから、[Search] フィールドに名前を入力して AAA IP アドレスを検索するか、AAA IP アドレスを選択します。

（注）
- ゲスト ワイヤレス ネットワークの中央 Web 認証（CWA）SSID 用に少なくとも 1 つの AAA またはポリシーサービスノード（PSN）サーバーを設定する必要があります。
- Cisco DNA Center では、アイデンティティ サービス エンジンの PSN とサードパーティ AAA IP の任意の組み合わせで AAA サーバーをマッピングできます。
- [Server] ドロップダウンリストで、**AAA** IP アドレスと PSN IP アドレスが対応するセクションにおいてグループ化されています。
- [Configure AAA] 機能は、Mobility Express（ME）デバイスではサポートされていません。

ステップ 6 [+] をクリックして、**追加のサーバー**を追加します。

（注） Catalyst 9000 スイッチ用 Cisco Catalyst 9800 組み込みワイヤレスコントローラのゲスト ワイヤレス ネットワークの SSID には、最大 6 つの AAA サーバーを設定できます。

ステップ 7 [Additional Server] ドロップダウンリストから、サーバーの IP アドレスを選択します。

ステップ 8 （任意）サーバーまたは追加のサーバーを削除するには、各サーバーの横にある削除アイコンをクリックします。

ステップ 9 [構成] をクリックします。

（注） Cisco DNA Center では、サイトレベルで SSID の一連の AAA サーバー設定をオーバーライドできます。SSID ごとにオーバーライドされた一連の AAA 設定ごとに、対応する AAA サーバーがマッピングされた新しい WLAN プロファイルが Cisco DNA Center によって作成されます。異なるフロアの SSID がオーバーライドされ、AAA サーバーで変更を行うと、フロア数に等しい数の新しい WLAN プロファイルが Cisco DNA Center によって作成されます。

サイトレベルで AAA サーバーをオーバーライドするためには、デバイスを再プロビジョニングする必要があります。「ワイヤレス デバイス プロビジョニングの概要」を参照してください。

AP の 802.1x 認証の設定

PnP を使用して、AP を安全にオンボードするように認証設定を構成できます。Cisco DNA Center のグローバルレベルまたはサイトレベルの階層で設定された認証設定に基づいて、AP を要求する際に PnP から 802.1x（Dot1x）サプリカントと証明書がプッシュされます。AP は 802.1x サプリカントを使用して Cisco ISE で認証されます。

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

ステップ 2 [Wireless] タブをクリックします。

ステップ 3 左側のペインで、[Global] が選択されていることを確認します。

（注） グローバルレベルで作成された 802.1x 認証は、サイトレベルで上書きできます。

ステップ 4 [Access Points Authentication for Plug n Play (PnP)] エリアで、次の手順を実行します。

a) 認証方法を選択します。

- [NO-AUTH]：デフォルトでは、この認証方法が選択されています。
- [EAP-TLS]：Extensible Authentication Protocol-Transport Level Security（EAP-TLS）は、EAP のいくつかの弱点を軽減するために設計された認証方式です。EAP-TLS には PEAP が提供する多くの利点がありますが、従来の認証方式をサポートしていない点が異なります。

  [EAP-TLS] を選択する場合、[Username] フィールドにユーザー名を入力します。証明書が生成され、PnP 要求プロセスで適用されます。
- [EAP-PEAP]：EAP-Protected Extensible Authentication Protocol（EAP-PEAP）では、相互認証が提供され、脆弱なユーザーログイン情報の機密性と整合性が保証されます。またこのプロトコルでは、自身をパッシブ（盗聴）およびアクティブ（中間者）攻撃から保護し、セキュアに暗号キー関連情報を生成します。PEAP は、IEEE 802.1X 標準および RADIUS プロトコルと互換性があります。

  [EAP-PEAP] を選択する場合、ユーザ名とパスワードを入力します。証明書が生成され、PnP 要求プロセスで適用されます。
- [EAP-FAST]：EAP-Flexible Authentication via Secure Tunneling（EAP-FAST）は、相互認証を提供する認証プロトコルであり、共有秘密を使用してトンネルを確立します。このトンネルは、パスワー

ドに基づく弱い認証方式を保護するために使用されます。Protected Access Credentials（PAC）キーと呼ばれる共有秘密は、トンネルのセキュリティを確保するときにクライアントとサーバを相互認証するために使用されます。

[EAP-FAST] を選択する場合、ユーザー名とパスワードを入力します。証明書が生成され、PnP 要求プロセスで適用されます。

b) [Username] と [Password] を入力します。
c) [Save] をクリックします。

ワイヤレスインターフェイスの作成

非ファブリック展開でのみワイヤレスインターフェイスを作成できます。

ステップ 1 メニューアイコン（☰）をクリックして、**[Design]** > **[Network settings]**。
ステップ 2 [Wireless] タブをクリックします。
ステップ 3 左側のペインで [Global] が選択されていることを確認します。
ステップ 4 [Wireless Interfaces] テーブルで、[+Add] をクリックします。
ステップ 5 [Create a Wireless Interface] スライドペインでワイヤレスインターフェイスの設定を指定します。
a) [Interface Name] フィールドに、動的なインターフェイスの名前を入力します。
b) [VLAN ID] フィールドに、このインターフェイスの VLAN ID を入力します。
ステップ 6 [保存（**Save**）] をクリックします。

ワイヤレスインターフェイスが作成され、[Wireless Interfaces] テーブルに表示されます。

非ファブリック展開用のインターフェイスまたは VLAN グループの設計とプロビジョニング

Cisco DNA Center では、異なる VLAN を介して複数のブロードキャストドメインを持つネットワークを設定できます。同じ AP のセットが同じ WLAN をブロードキャストする場合、ブロードキャストドメインは、インターフェイスグループを介して同じ WLAN 上の複数の VLAN によって制御されます。

Cisco DNA Center インターフェイスグループは、ユーザー設定を容易にするインターフェイスの論理グループであり、同じインターフェイスグループを複数の WLAN で設定できます。その一方で、AP グループごとに WLAN インターフェイスをオーバーライドできます。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。WLAN は、インターフェイスまたはインターフェイス グループに関連付けることができます。

（注） インターフェイス グループの名前とインターフェイスの名前を同じにすることはできません。

Cisco DNA Center VLAN グループ機能は、VLAN グループを使用して WLAN を 1 つまたは複数の VLAN にマッピングします。VLAN グループは、ポリシープロファイルに関連付けることができます。

次の手順では、非ファブリック展開のインターフェイスまたは VLAN グループを設計およびプロビジョニングする方法について説明します。

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

ステップ 2 [Wireless] タブをクリックします。

ステップ 3 [VLAN Group] テーブルで、[Add] をクリックします。

[Add VLAN Group] スライドインペインが表示されます。

ステップ 4 有効な [VLAN Group Name] を入力し、リストから単一または複数のインターフェイスを選択して、[Save] をクリックします。

（注） 15 を超えるインターフェイスを選択すると、選択したインターフェイスが画面に正しく表示されない場合があります。

ステップ 5 [Edit Network Profile] ページで、VLAN グループが SSID に関連付けられます。

SSID の作成方法については、「エンタープライズ ワイヤレス ネットワーク用 SSID の作成」を参照してください。

ステップ 6 VLAN グループにさらに SSID を追加するには、[Add SSID] をクリックします。

ステップ 7 [Interface] または [VLAN] グループを選択します。

ステップ 8 [Add] アイコンをクリックして、新しいインターフェイスまたは VLAN グループを作成します。

（注） インターフェイスまたは VLAN グループは FlexConnect ローカルスイッチングには適用されません。

ステップ 9 [**保存（Save）**] をクリックします。

ステップ 10 [Configure Interface and VLAN] では、インターフェイス名、インターフェイスグループ名、およびインターフェイスと VLAN の設定に必要なその他のパラメータのリストを確認できます。

（注） インターフェイスグループには、64 を超えるインターフェイスを含めることはできません。

ステップ 11 メニューアイコン（☰）をクリックして、**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。

ステップ 12 デバイスを選択します。

ステップ 13 [Actions] ドロップダウンメニューから、**[Provision]** > **[Provision Device]** の順に選択します。

ステップ 14 [Assign Site]、[Configuration]、[Model Configuration]、[Advanced Configuration]、および [Summary] 画面で詳細を確認します。各画面で、[Next] をクリックして次の画面に進みます。

ステップ 15 [展開（Deploy）] をクリックします。

[Provision Device] ダイアログボックスが表示されます。

ステップ 16 [Now] を選択し、[Apply] をクリックします。

「Task Scheduled view status in Tasks」というメッセージが表示されます。

ワイヤレス無線周波数プロファイルの作成

デフォルトの無線周波数プロファイル（低、標準、高）を使用することも、カスタムの無線周波数プロファイルを作成することもできます。

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

ステップ 2 [Wireless] タブをクリックします。

ステップ 3 [Wireless Radio Frequency Profile] のテーブルで [Add] をクリックします。

[Wireless Radio Frequency Profile] ウィンドウが表示されます。

ステップ 4 [Profile Name] フィールドに RF プロファイルの名前を入力します。

ステップ 5 [2.4 GHz] 無線タイプでは、次を設定します。

1. [2.4 GHz] トグルボタンが有効になっていることを確認します。

   （注）
   - Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の場合、[2.4 GHz] トグルボタンを無効にすると、Cisco DNA Center は、[2.4 GHz] RF プロファイルの管理ステータスを無効にします。
   - Cisco AireOS ワイヤレスコントローラ の場合、[2.4 GHz] トグルボタンを無効にすると、 Cisco DNA Center は、この RF プロファイルを使用するすべての AP で、該当する無線の管理ステータスを無効にします。

2. [Parent Profile] で、[High]、[Medium（Typica）]、[Low]、[Custom] のいずれかを選択します。（[データレート（Data Rate）] および [Tx設定（Tx Configuration）] フィールドは、選択された親プロファイルによって変更されます。たとえば、[High] を選択した場合、2.4 GHz のデバイスで使用可能なプロファイル設定が追加されます。[Data Rate] および [Tx Configuration] の入力済みの設定を変更すると、[Parent Profile] が自動的に [Custom] に変更されます。選択したカスタム プロファイルに対してのみ、新しい RF プロファイルが作成されることに注意してください。

   （注） [Low]、[Medium（Typical）]、および [High] は、デフォルトの RF プロファイルです。デフォルトの RF プロファイルを選択するとデバイスのそれぞれの RF プロファイルが使用され、ワイヤレスコントローラ では新しい RF プロファイルは作成されません。

3. [DCA] は、RF グループへのチャネルの割り当てを動的に管理し、AP 無線ごとに割り当てを評価します。

- **[すべて選択（Select All）]** チェックボックスをオンにして、DCA チャネル **[1]**、**[6]**、および **[11]** を選択します。または、チャネル番号の横にある個々のチェックボックスをオンにします。
- **[詳細オプション（Advanced Options）]** の下で **[詳細設定を表示（Show Advanced）]** をクリックし、チャネル番号を選択します。[Select All] チェックボックスをオンにして、[Advanced Options] の下にある DCA チャネルを選択するか、個々のチャネル番号の横にあるチェックボックスをオンにします。B プロファイルで使用可能なチャネル番号は、[2]、[3]、[4]、[5]、[7]、[8]、[9]、[10]、[12]、[13]、[14] です。

（注） Cisco AireOS ワイヤレスコントローラ の場合、Cisco DNA Center はグローバル RRM DCA チャネルリストで選択した DCA チャネルを自動的に設定します。

デバイスの国コードに基づいて DCA チャネルを選択します。プロビジョニングでは、ワイヤレスコントローラ で設定した国に対して使用が許可されているチャネルのみが考慮され、サポートされていないチャネルは無視されます。コントローラに設定されている国コードでは、選択したすべてのチャネルがサポート対象外になる場合、プロビジョニングに失敗する可能性があります。

4. アクセスポイントとクライアント間でデータを転送できるレートを設定するには、[サポートされているデータレート（Supported Data Rate）] スライダを使用します。使用可能なデータ レートは、[1]、[2]、[5.5]、[6]、[9]、[11]、[12]、[18]、[24]、[36]、[48]、[54] です。
5. [Tx Power Configuration] で、AP の電力レベルと電力しきい値を設定できます。
   - **電力レベル**：AP の電力を削減する必要があるかどうかを決定します。AP の電力を削減すると、同一チャネルまたは近接するチャネル上の別の AP との同一チャネル干渉を軽減するのに役立ちます。[電力レベル（Power Level）] スライダを使用して、電力レベルの最小または最大値を設定します。指定できる範囲は -10 ～ 30 dBm で、デフォルトは -10 dBM です。
   - **電力しきい値**：無線リソース管理（RRM）を使用したカットオフ信号レベルで、AP の電力を削減するかどうかを判断します。[Power Threshold] スライダを使用して電力値を増減させ、AP をより高い、またはより低い送信電力レートで動作させるようにします。指定できる範囲は -50 ～ 80 dBM で、デフォルトのしきい値は -70 dBM です。
   - **RX SOP**：レシーバのパケット検出開始しきい値（RX SOP）は、AP の無線がパケットの変調および復調を行う Wi-Fi 信号レベル（dBm 単位）を決定します。[RX SOP] ドロップダウン リストから、各 802.11 バンドのしきい値を、[高（High）]、[中（Medium）]、[低（Low）]、および [自動（Auto）] から選択します。

ステップ 6 [5 GHz] 無線タイプでは、次を設定します。

1. [5 GHz] トグルボタンが有効になっていることを確認します。

（注）
- Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の場合、[5 GHz] トグルボタンを無効にすると、Cisco DNA Center は、[5 GHz] RF プロファイルの管理ステータスを無効にします。
- Cisco AireOS ワイヤレスコントローラ の場合、[5 GHz] トグルボタンを無効にすると、 Cisco DNA Center は、この RF プロファイルを使用するすべての AP で、該当する無線の管理ステータスを無効にします。

2. **[親プロファイル（Parent Profile）]** ドロップダウンリストから、**[高（High）]**、**[中（標準）（Medium (Typical)）]**、**[低（Low）]**、または **[カスタム（Custom）]** を選択します。（[データレート（Data Rate）] および [Tx設定（Tx Configuration）] フィールドは、選択された親プロファイルによって変更されます。たとえば、[高（High）] を選択した場合、2.4 GHz のデバイスで使用可能な設定が追加されます。[Data Rate] フィールドおよび [Tx Configuration] フィールドの入力済みの設定を変更すると、[Parent Profile] が自動的に [Custom] に変更されます。選択したカスタムプロファイルに対してのみ、新しい RF プロファイルが作成されます。

   （注） [Low]、[Medium (Typical)]、および [High] は、デフォルトの RF プロファイルです。デフォルトの RF プロファイルを選択するとデバイスに既に存在するそれぞれの RF プロファイルが使用され、ワイヤレスコントローラ では新しい RF プロファイルは作成されません。

3. [Channel Width] ドロップダウンリストから、チャネル帯域幅オプションとして [Best]、[20 MHz]、[40 MHz]、[80 MHz]、または [160 MHz] のいずれかを選択します。

4. [DCA Channel] を設定して、チャネルの割り当てを管理します。

   （注） Cisco AireOS ワイヤレスコントローラ の場合、Cisco DNA Center はグローバル RRM DCA チャネルリストで選択した DCA チャネルを自動的に設定します。

   デバイスの国コードに基づいて DCA チャネルを選択します。プロビジョニングでは、ワイヤレスコントローラ で設定した国に対して使用が許可されているチャネルのみが考慮され、サポートされていないチャネルは無視されます。コントローラに設定されている国コードでは、選択したすべてのチャネルがサポート対象外になる場合、プロビジョニングに失敗する可能性があります。

   - [UNNI-1 36-48]：UNII-1 バンドで使用可能なチャネルは、[36]、[40]、[44]、[48] です。[UNII-1 36-48] チェックボックスをオンにしてすべてのチャネルを含めるか、チャネルのチェックボックスをオンにして、個別に選択します。
   - [UNII-2 52-144]：UNII-2 バンドで使用可能なチャネルは、[52]、[56]、[60]、[64]、[100]、[104]、[108]、[112]、[116]、[120]、[124]、[128]、[132]、[136]、[140]、[144] です。[UNII-2 52-144] チェックボックスをオンにしてすべてのチャネルを含めるか、チャネルのチェックボックスをオンにして、個別に選択します。
   - [UNII-3 149-165]：UNII-3 バンドで使用可能なチャネルは、[149]、[153]、[157]、[161]、[165] です。[UNII-3 149-165] チェックボックスをオンにしてすべてのチャネルを含めるか、チャネルのチェックボックスをオンにして、個別に選択します。

5. アクセス ポイントとクライアント間でデータを送信できるレートを設定するには、[データレート（Data Rate）] スライダを使用します。使用可能なデータ レートは、[6]、[9]、[12]、[18]、[24]、[36]、[48]、[54] です。
6. [Tx Power Configuration] で、AP の電力レベルと電力しきい値を設定できます。
   - [Power Level]：AP の電力を削減する必要があるかどうかを判断します。AP の電力を削減すると、同一チャネルまたは近接するチャネル上の別の AP との同一チャネル干渉を軽減するのに役立ちます。[電力レベル（Power Level）] スライダを使用して、電力レベルの最小または最大値を設定します。指定できる範囲は -10 ～ 30 dBm で、デフォルトは -10 dBM です。
   - **電力しきい値**：無線リソース管理（RRM）を使用したカットオフ信号レベルで、AP の電力を削減するかどうかを判断します。[Power Threshold] スライダを使用して電力値を増減させ、AP をより高い、またはより低い送信電力レートで動作させるようにします。指定できる範囲は -50 ～ 80 dBM で、デフォルトのしきい値は -70 dBM です。
   - [RX SOP]：レシーバのパケット検出開始しきい値（RX SOP）は、AP の無線がパケットを復調してデコードする dBm 単位の Wi-Fi 信号レベルを決定します。[RX SOP] ドロップダウン リストから、各 802.11 バンドのしきい値を、[高（High）]、[中（Medium）]、[低（Low）]、および [自動（Auto）] から選択します。

ステップ 7 [6 GHz] 無線タイプでは、次を設定します。

1. [6 GHz] トグルボタンが有効になっていることを確認します。

   （注） Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の場合、[6 GHz] トグルボタンを無効にすると、Cisco DNA Center は、[6 GHz] RF プロファイルの管理ステータスを無効にします。

2. [DCA Channel] を設定して、チャネルの割り当てを管理します。
   - [Select All] チェックボックスをオンにしてすべての DCA チャネルを含めるか、個々のチェックボックスをオンにして個々の DCA チャネルを選択します。
   - [Show Advanced] をクリックして、残りの DCA チャネル番号を選択します。
     - **UNII-5 1-93**
     - **UNII-6 97-113**
     - **UNII-7 117-185**
     - **UNII-8 189-233**

   （注） デバイスの国コードに基づいて DCA チャネルを選択します。プロビジョニングでは、ワイヤレスコントローラ で設定した国に対して使用が許可されているチャネルのみが考慮され、サポートされていないチャネルは無視されます。コントローラに設定されている国コードでは、選択したすべてのチャネルがサポート対象外になる場合、プロビジョニングに失敗する可能性があります。

3. アクセスポイントとクライアント間でデータを転送できるレートを設定するには、[サポートされているデータレート（Supported Data Rate）] スライダを使用します。使用可能なデータ レートは、[6]、[9]、[12]、[18]、[24]、[36]、[48]、[54] です。
4. [Mandatory Data Rates] エリアで、個々のデータレートの横にあるチェックボックスをオンにします。最大 2 つのデータレートを選択できます。使用可能なデータ レートは、[6]、[9]、[12]、[18]、[24]、[36]、[48]、[54] です。
5. [Tx Power Configuration] で、AP の電力レベルと電力しきい値を設定できます。
   - [Power Level]：AP の電力を削減する必要があるかどうかを判断します。AP の電力を削減すると、同一チャネルまたは近接するチャネル上の別の AP との同一チャネル干渉を軽減するのに役立ちます。[電力レベル（Power Level）] スライダを使用して、電力レベルの最小または最大値を設定します。指定できる範囲は -10 ～ 30 dBm で、デフォルトは -10 dBM です。
   - **電力しきい値**：無線リソース管理（RRM）を使用したカットオフ信号レベルで、AP の電力を削減するかどうかを判断します。[Power Threshold] スライダを使用して電力値を増減させ、AP をより高い、またはより低い送信電力レートで動作させるようにします。指定できる範囲は -50 ～ 80 dBM で、デフォルトのしきい値は -70 dBM です。
   - [RX SOP]：レシーバのパケット検出開始しきい値（RX SOP）は、AP の無線がパケットを復調してデコードする dBm 単位の Wi-Fi 信号レベルを決定します。[RX SOP] ドロップダウン リストから、各 802.11 バンドのしきい値を、[高（High）]、[中（Medium）]、[低（Low）]、および [自動（Auto）] から選択します。

ステップ 8 **[Save]** をクリックします。

ステップ 9 プロファイルをデフォルトの RF プロファイルとしてマークするには、[Profile Name] チェックボックスをオンにし、[Mark Default] をクリックします。

ステップ 10 **[警告（Warning）]** ウィンドウで **[OK]** をクリックします。

次のタスク

デバイスに RF プロファイルを適用するには、AP をプロビジョニングする必要があります。詳細については、シスコ製 AP のプロビジョニング：Day 1 AP プロビジョニング （430 ページ）を参照してください。

基本無線周波数プロファイルの編集または削除

次の手順では、基本 RF プロファイルを編集または削除する方法について説明します。

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

ステップ 2 [Wireless] タブをクリックします。

ステップ 3 左側のペインで、[Global] サイトをクリックします。

ステップ 4 [Wireless Radio Frequency Profile] 領域で、[Basic RF Profile] タブをクリックします。

（注） [Basic RF Profile] テーブルには、[Profile Name]、[Type]、[2.4 GHz Data Rates]、[5 GHz Data Rates]、[6 GHz Data Rates]、[Channel Width]、および [Profile Type] に基づいて作成された基本 RF プロファイルの数がリストされます。

ステップ 5 編集する基本プロファイル名の横にあるチェックボックスをオンにします。

ステップ 6 [Actions] ドロップダウンリストから、[Edit/View] を選択します。

（注） 一度に 1 つの基本 RF プロファイルを編集できます。

ステップ 7 [Edit Wireless Radio Frequency Profile] ウィンドウで、基本 RF プロファイル設定を構成します。詳細については、ワイヤレス無線周波数プロファイルの作成 （268 ページ）を参照してください。

ステップ 8 [保存（**Save**）] をクリックします。

ステップ 9 基本 RF プロファイルを削除するには、基本 RF プロファイル名の横にあるチェックボックスをオンにします。

ステップ 10 [Actions] ドロップダウンリストから、[Delete] を選択してから [Yes] をクリックします。

ステップ 11 基本 RF プロファイルをデフォルトとしてマークするには、基本 RF プロファイル名の横にあるチェックボックスをオンにします。

ステップ 12 [Action] ドロップダウンリストから、[Mark Default] を選択してから [Yes] をクリックします。

次のタスク

ワイヤレスコントローラ や AP ですでにプロビジョニング済みの RF プロファイルを更新する場合は、ワイヤレスコントローラ を再プロビジョニングする必要があります。AP を再プロビジョニングする必要はありません。ワイヤレスコントローラ のプロビジョニングの詳細については、Cisco AireOS コントローラのプロビジョニング （422 ページ）およびCisco Catalyst 9800 シリーズ ワイヤレスコントローラのプロビジョニング （462 ページ）を参照してください。

AI 無線周波数プロファイルの作成

次の手順では、建物の人工知能無線周波数プロファイルを作成する方法について説明します。

始める前に

- システム設定で Cisco AI Network Analytics を有効にする必要があります。詳細については、Cisco DNA Center 管理者ガイドの「Cisco AI Network Analytics データ収集の設定」を参照してください。
- システム設定の [Cisco AI Analytics] で [AI Enhanced RRM] を有効にする必要があります。メニューアイコン（☰）をクリックして、**[System]** > **[Settings]** > **[External Services]** の順に選択します。

  [Cisco AI Analytics] ウィンドウの [AI ENHANCED RRM] エリアで、トグルボタンをクリックして AI 拡張 RRM を有効にします。

- Cisco AI RF プロファイルは、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ および Cisco IOS-XE 17.7.1 以降でのみサポートされています。
- 次のタスクを実行するには、**スーパー管理者**または**ネットワーク管理者**である必要があります。

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

ステップ 2 [Wireless] タブをクリックします。

ステップ 3 左側のペインで、[Global] サイトをクリックします。

ステップ 4 [Wireless Radio Frequency Profile] エリアで、[Add] ドロップダウンリストから [AI RF Profile] を選択します。

[Create AI Radio Frequency Profile] ウィンドウが表示されます。

ステップ 5 [Profile Name] フィールドに RF プロファイルの名前を入力します。

ステップ 6 [Basic Settings] を展開します。

ステップ 7 [Radio Frequency Settings] エリアで、[2.4 GHz] または [5 GHz] チェックボックスをオンにします。

無線周波数はデフォルトでオンになっています。無線周波数をオフにすると、Cisco DNA Center では対応する RF プロファイルの管理ステータスが無効になります。

ステップ 8 [Busy Hours] エリアで、サイトのタイムゾーンの開始時刻と終了時刻を定義します。

（注） ビジー時間は、建物のタイムゾーンによって異なります。それぞれの建物のネットワーク設定でタイムゾーンを構成する必要があります。

ステップ 9 [Busy Hour Sensitivity] エリアで、[Low]、[Medium]、または [High] オプションボタンをクリックして、ビジー時間間隔の無線リソース管理（RRM）感度のしきい値を定義します。

ステップ 10 [Enable RF Settings] エリアで、[2.4 GHz] または [5 GHz] 列の下にあるトグルボタンをクリックして、それぞれの RF 設定の無線帯域を有効または無効にします。

サポートされている RF 設定は次のとおりです。

- [Flexible Radio Assignment (FRA)]：FRA は帯域ごとの無線カバレッジを最適化し、冗長無線の最適なロール割り当てを決定します。
- [Dynamic Channel Assignment (DCA)]：DCA は、RF グループへのチャネルの割り当てを動的に管理し、AP 無線ごとに割り当てを評価します。
- [Transmit Power Control (TPC)]：TPC は AP の電力を管理および送信します。また、干渉の低減中に SNR を最大化します。
- [Dynamic Bandwidth Selection (DBS)]：DBS は、チャネル幅を監視および調整して、パフォーマンスと干渉のバランスをとります。

（注）
- FRA の 2.4 GHz 無線帯域を無効にすると、FRA の 5 GHz 無線帯域が自動的に無効になります。逆の場合も同様です。
- DCA の 5 GHz 無線帯域を無効にすると、FRA の 2.4 GHz 無線帯域と FRA と DBS の 5 GHz 無線帯域が無効になります。
- DCA および TPC の 2.4 GHz 無線帯域と、DCA、TPC、および DBS の 5 GHz 無線帯域を個別に有効にすることができます。

ステップ 11 [Advanced] を展開し、[2.4 GHz] トグルボタンをクリックします。

1. [DCA Channel] エリアで、[Select All] チェックボックスをオンにして、DCA チャネル [1]、[6]、および [11] を選択します。または、チャネル番号の横にある個々のチェックボックスをオンにします。
2. [Advanced Options] エリアで、[Select All] チェックボックスをオンにして、すべての DCA チャネルを選択します。
3. [Show Advanced] をクリックして、残りのチャネル番号を選択します。
4. 個々のチャネル番号の横にあるチェックボックスをオンにします。プロファイルで使用可能なチャネル番号は、[2]、[3]、[4]、[5]、[7]、[8]、[9]、[10]、[12]、[13]、[14] です。

   （注） デバイスの国コードに基づいて DCA チャネルを選択します。プロビジョニングでは、ワイヤレスコントローラ で設定した国に対して使用が許可されているチャネルのみが考慮され、サポートされていないチャネルは無視されます。コントローラに設定されている国コードでは、選択したすべてのチャネルがサポート対象外になる場合、プロビジョニングに失敗する可能性があります。

5. AP とクライアント間でデータを転送できるレートを設定するには、[Supported Data Rate] スライダを使用します。使用可能なデータ レートは、[1]、[2]、[5.5]、[6]、[9]、[11]、[12]、[18]、[24]、[36]、[48]、[54] です。
6. [Mandatory Data Rates] エリアで、個々のデータレートの横にあるチェックボックスをオンにします。最大 2 つのデータレートを選択できます。使用可能なデータ レートは、[1]、[2]、[5.5]、[6]、[9]、[11]、[12]、[18]、[24]、[36]、[48]、[54] です。
7. [Enable 802.11b data rates] チェックボックスをオンにして、802.11b データレートを有効にします。このアクションにより、[Mandatory Data Rates] エリアの [802.11b supported data rate] チェックボックスも有効になります。
8. [Tx Power Configuration] エリアで、次を設定します。
   - [Power Level]：AP の電力を削減する必要があるかどうかを判断します。AP の電力を削減すると、同一チャネル干渉を軽減できます。
   - [Power Threshold]：RRM を使用したカットオフ信号レベルです。AP の電力を削減するかどうかを判断します。
   - **RX SOP**：レシーバのパケット検出開始しきい値（RX SOP）は、AP の無線がパケットの変調および復調を行う Wi-Fi 信号レベル（ dBm 単位）を決定します。

9. [電力レベル（Power Level）] スライダを使用して、電力レベルの最小または最大値を設定します。指定できる範囲は -10 ～ 30 dBm で、デフォルトは -10 dBM です。
10. [Power Threshold] スライダを使用して電力値を増減させ、AP をより高い、またはより低い送信電力レートで動作させるようにします。指定できる範囲は -50 ～ 80 dBM で、デフォルトのしきい値は -70 dBM です。
11. [RX SOP] ドロップダウンリストから、各 802.11 バンドのしきい値を、[High]、[Medium]、[Low]、および [Auto] から選択します。

ステップ 12 [Advanced] エリアで、[5 GHz] トグルボタンをクリックします。

1. [DBS Max Width] スライダを使用して、AI RF プロファイルのチャネル幅を設定します。

   使用可能なチャネル幅オプションは、[20 MHz]、[40 MHz]、[80 MHz]、または [160 MHz] です。

   [Auto Channels Logic] エリアには、チャネル幅の色分けされたチャネルロジックが表示されます。

   DBS が有効な場合にのみ、[DBS Max Width] を選択できます。

   DBS を無効にすると、Cisco DNA Center ではチャネル幅を選択できます。
2. [DCA Channels] を設定して、次のチャネルの割り当てを管理します。
   - [UNII-1 36-48]：UNII-1 バンドで使用可能なチャネルは、[36]、[40]、[44]、[48] です。
   - [UNII-2 52-144]：UNII-2 バンドで使用可能なチャネルは、[52]、[56]、[60]、[64]、[100]、[104]、[108]、[112]、[116]、[120]、[124]、[128]、[132]、[136]、[140]、[144] です。
   - [UNII-3 149-165]：UNII-3 バンドで使用可能なチャネルは、[149]、[153]、[157]、[161]、[165] です。
3. [Select All] チェックボックスをオンにしてすべての DCA チャネルを含めるか、個々のチェックボックスをオンにして個々の DCA チャネルを選択します。
4. [Show Advanced] をクリックして、残りの DCA チャネル番号を選択します。
5. [UNII-1 36-48] チェックボックスをオンにしてすべてのチャネルを含めるか、チャネルのチェックボックスをオンにして、個別に選択します。
6. [UNII-1 36-48] チェックボックスをオンにしてすべてのチャネルを含めるか、チャネルのチェックボックスをオンにして、個別に選択します。
7. [UNII-3 149-165] チェックボックスをオンにしてすべてのチャネルを含めるか、チャネルのチェックボックスをオンにして、個別に選択します。

   （注） デバイスの国コードに基づいて DCA チャネルを選択します。プロビジョニングでは、ワイヤレスコントローラ で設定した国に対して使用が許可されているチャネルのみが考慮され、サポートされていないチャネルは無視されます。コントローラに設定されている国コードでは、選択したすべてのチャネルがサポート対象外になる場合、プロビジョニングに失敗する可能性があります。

8. AP とクライアント間でデータを転送できるレートを設定するには、[Supported Data Rate] スライダを使用します。使用可能なデータ レートは、[1]、[2]、[5.5]、[6]、[9]、[11]、[12]、[18]、[24]、[36]、[48]、[54] です。
9. [Tx Power Configuration] エリアで、[Power Level]、[Power Threshold]、および [RX SOP] を設定します。
10. [電力レベル（Power Level）] スライダを使用して、電力レベルの最小または最大値を設定します。指定できる範囲は -10 ～ 30 dBm で、デフォルトは -10 dBM です。
11. [Power Threshold] スライダを使用して電力値を増減させ、AP をより高い、またはより低い送信電力レートで動作させるようにします。指定できる範囲は -50 ～ 80 dBm で、デフォルトのしきい値は -70 dBm です。
12. [RX SOP] ドロップダウンリストで、しきい値を、[High]、[Medium]、[Low]、および [Auto] から選択します。

ステップ 13 **[Save]** をクリックします。

次のタスク

デバイスに RF プロファイル設定を適用するには、AP をプロビジョニングする必要があります。詳細については、シスコ製 AP のプロビジョニング：Day 1 AP プロビジョニング（430 ページ）を参照してください。

AI 無線周波数プロファイルの編集および削除

次の手順では、AI RF プロファイルを編集または削除する方法について説明します。

始める前に

- Cisco AI RF プロファイルは、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ および Cisco IOS-XE 17.7.1 以降でのみサポートされています。
- 次のタスクを実行するには、**スーパー管理者**または**ネットワーク管理者**である必要があります。

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

ステップ 2 [Wireless] タブをクリックします。

ステップ 3 左側のペインで、[Global] サイトをクリックします。

ステップ 4 [Wireless Radio Frequency Profile] エリアで、[AI RF Profile] タブをクリックします。

[AI RF Profile] テーブルには、[Profile Name]、[Busy Hours]、[Busy Hour Sensitivity]、[FRA]、[DCA]、[DBS]、[TPC]、および [Mapped Buildings] に基づいて作成された AI RF プロファイルの数がリストされます。

ステップ 5 編集する AI RF プロファイル名の横にあるチェックボックスをオンにします。

一度に 1 つの AI RF プロファイルを編集できます。

ステップ 6 [Edit/View] をクリックします。

ステップ 7 [Edit AI RF Profile] ウィンドウで、AI RF プロファイル設定を構成します。詳細については、AI 無線周波数プロファイルの作成 （273 ページ）を参照してください。

ステップ 8 [保存（**Save**）] をクリックします。

ステップ 9 AI RF プロファイルを削除するには、削除する AI RF プロファイルの横にあるチェックボックスをオンにします。

ステップ 10 [Delete] をクリックし、[Yes] をクリックします。

（注） Cisco DNA Center では、建物にすでに割り当てられている AI RF プロファイルを削除することはできません。

次のタスク

ワイヤレスコントローラ や AP ですでにプロビジョニング済みの RF プロファイルを更新する場合は、ワイヤレスコントローラ を再プロビジョニングする必要があります。AP を再プロビジョニングする必要はありません。ワイヤレスコントローラ のプロビジョニングの詳細については、Cisco Catalyst 9800 シリーズ ワイヤレスコントローラのプロビジョニング （462 ページ）およびを参照してください。

AI 無線周波数プロファイルの構成

次の手順では、AI RF プロファイルを建物に割り当てる方法について説明します。

始める前に

- Cisco AI RF プロファイルは、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ および Cisco IOS-XE 17.7.1 以降でのみサポートされています。
- 次のタスクを実行するには、**スーパー管理者**または**ネットワーク管理者**である必要があります。

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

ステップ 2 [Assign AI RF Profiles] ウィンドウで、[Let's Do it] をクリックしてワークフローに直接移動します。

ステップ 3 [Configure AI RF Profile] ウィンドウが表示されます。

[Task Name] フィールドにタスク名を入力します。

ステップ 4 [Select Locations to Assign AI RF Profiles] ウィンドウで、AI 対応 RF プロファイルを割り当てる場所を選択します。[Find Hierarchy] フィールドに名前を入力してサイトを検索するか、[Global] を展開してサイトを選択します。

[Site selection summary] テーブルには、サイト階層内のサイト選択に基づいてサイトがリストされ、選択されたサイトの [Selected Location] と [Impacted Location] が表示されます。

- [Selected Locations]：AI RF プロファイルが有効になっている場所。
- [Impacted Locations]：選択した場所と同じワイヤレスコントローラによって部分的に管理されている場所。

（注） コントローラが複数の建物を管理していて、1 つの建物でのみ AI RF プロファイルを有効にすると、Cisco DNA Center は自動的に他の建物で同じ AI RF プロファイルを有効にします。

たとえば、2 つのコントローラが 3 つの建物を管理していて、1 つの建物で AI RF プロファイルを有効にすると、Cisco DNA Center は自動的に他の 2 つの建物で同じ AI RF プロファイルを有効にします。

ステップ 5 [Select AI RF Profiles to assign] ウィンドウの [Building] テーブルには、[Location]、[Floors]、[Current RF Profiles]、および [Replace with AI RF Profiles] に基づいた AI RF プロファイルが一覧表示されます。

a) [Building] テーブルで、場所の横にあるチェックボックスをオンにして、AI RF プロファイルを選択します。

b) 場所に基づいて、[Replace with AI RF Profiles] の下のドロップダウンリストから AI 対応 RF プロファイルを選択して、現在の AI RF プロファイルに置き換えます。

（注） AI RF プロファイルが作成されていない場合は、[Action] 列の下にある 3 つのドットをクリックして新しい RF プロファイルを作成するか、現在の RF プロファイルと AI 設定をコピーします。

[Select AI RF Profiles to assign] ウィンドウの [Create a new AI RF Profile to apply] リンクから AI RF プロファイルを作成することもできます。詳細については、AI 無線周波数プロファイルの作成 （273 ページ）を参照してください。

ステップ 6 [Details of selected AI RF Profile] ウィンドウで、AI 対応 RF プロファイルの [AI Settings]、[Common Settings]、および [Assignment] の詳細を確認します。

（注） AI 拡張 RRM の計算は 30 分ごとに発生します。RRM の決定は、計算後に更新され、デバイスにプッシュされます。

ステップ 7 [Summary] ウィンドウで、[Task Details]、[Select Locations to Assign AI RF Profiles]、[Select AI RF Profiles to assign] を確認します。

ステップ 8 [Deploy the AI RF Profiles] ウィンドウで、[Now] をクリックして、AI RF プロファイルをすぐに展開します。[Later] をクリックして、後で展開をスケジュールします。

ステップ 9 [Continue] をクリックします。
タスク完了Done! AI RF Profiles Assigned] ウィンドウが表示されます。

ステップ 10 メニューアイコン（≡）をクリックして、**[Activities]** > **[Tasks]**の順に選択します。

ステップ 11 [Tasks] ウィンドウで、タスクのリンクをクリックします。

スライドインペインに、[Assigned Building(s)]、[Selected AI RF Profile]、および [Selected AI RF Profile] が表示されます。

既存の AI RF プロファイルへの場所の割り当て

次の手順では、既存の AI RF プロファイルに場所を割り当てる方法について説明します。

始める前に

- Cisco AI RF プロファイルは、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ および Cisco IOS-XE 17.7.1 以降でのみサポートされています。
- 次のタスクを実行するには、**スーパー管理者**または**ネットワーク管理者**である必要があります。

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

ステップ 2 [Wireless] タブをクリックします。

ステップ 3 左側のペインで、[Global] サイトをクリックします。

ステップ 4 [Wireless Radio Frequency Profile] エリアで、[AI RF Profile] タブをクリックします。
[AI RF Profile] テーブルに、作成された AI RF プロファイルの数が一覧表示されます。

ステップ 5 AI RF プロファイルの [Action] 列の下にある 3 つのドットをクリックします。

ステップ 6 ドロップダウンリストから [Assign Location] を選択します。

[Manage Location Assignment] ウィンドウが表示されます。

ステップ 7 [Search] フィールドに名前を入力してサイトを検索するか、[All Sites] を展開してサイトを選択します。

（注）
- サイト階層は、AI 対応の場所を示しています。
- AI プロファイルの対象とならないサイトまたは建物は無効になっています。
- 建物の下のフロアは選択できません。AI 対応 RF プロファイルに建物を選択すると、その下のフロアが自動的に割り当てられます。

同じワイヤレスコントローラが他の建物を管理している場合は、[Confirm Impacted Sites] ウィンドウが表示されます。

ステップ 8 確認し、[Confirm] をクリックして、選択したサイトを AI 対応 RF プロファイルに割り当てます。

ステップ 9 [**Assign**] をクリックします。

[Download a Backup of Current RF Settings] ウィンドウが表示され、選択した建物全体の RF 設定のバックアップをダウンロードできます。

ステップ 10 （オプション）バックアップリンクをクリックして、.csv ファイルをローカルマシンにダウンロードします。

ステップ 11 [Confirm] をクリックします。

ステップ 12 表示される確認ウィンドウで、[Confirm] をクリックします。

[AI RF Profile] テーブルでは、AI RF プロファイルに割り当てられた場所が [Mapped Buildings] 列の下に表示されます。

次のタスク

AI RF プロファイル対応建物のデバイスのプロビジョニング

次の手順では、AI RF プロファイルを展開するためにロケーション全体のデバイスをプロビジョニングする方法について説明します。

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

   [Inventory] ウィンドウの [Device] テーブルには、検出された AI RF プロファイルに関連付けられたデバイスが一覧表示されます。

2. プロビジョニングする AI RF プロファイルに関連付けられたデバイス名の横にあるチェックボックスをオンにします。

3. [Actions] ドロップダウンリストから、**[Provision]** > **[Provision Device]** を選択します。

4. すべての手順を実行し、[Summary] ステップで [Deploy] をクリックします。

5. [Summary] ウィンドウで、デバイスにプッシュされる残りのネットワーク設定を確認します。詳細については、ワイヤレスデバイスプロビジョニングの概要（421 ページ）を参照してください。

既存の AI RF プロファイルへの場所の割り当ての解除

次の手順では、既存の AI RF プロファイルから場所の割り当てを解除する方法について説明します。

始める前に

- Cisco AI RF プロファイルは、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ および Cisco IOS-XE 17.7.1 以降でのみサポートされています。
- 次のタスクを実行するには、**スーパー管理者**または**ネットワーク管理者**である必要があります。

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

ステップ 2 [Wireless] タブをクリックします。

ステップ 3 左側のペインで、[Global] サイトをクリックします。

ステップ 4 [Wireless Radio Frequency Profile] エリアで、[AI RF Profile] タブをクリックします。
[AI RF Profile] テーブルに、作成された AI RF プロファイルの数が一覧表示されます。

ステップ 5 AI RF プロファイルの [Action] 列の下にある 3 つのドットをクリックします。

ステップ 6 ドロップダウンリストから [Unassign Location] を選択します。

[Unassign AI RF Profile] ウィンドウが表示されます。

ステップ 7 サイトの横にあるチェックボックスをオンにして、AI RF プロファイルの割り当てを解除します。

ステップ 8 [Select from available RF Profiles] オプションボタンをクリックして、選択した場所に割り当てる使用可能な RF プロファイルを選択します。

ステップ 9 [Select RF Profile to Replace] ドロップダウンリストから、RF プロファイルを選択します。

[Select RF Profile to Replace] ドロップダウンリストには、AI RF プロファイルと基本 RF プロファイルが表示されます。

ドロップダウンリストから基本的な RF プロファイルを選択すると、[Confirm Impacted Sites] ウィンドウで、同じワイヤレスコントローラが他のサイトを管理しているかどうかが検証されます。

[Confirm Impacted Sites] ウィンドウを確認し、[Confirm] をクリックして、選択したサイトを選択した RF プロファイルに割り当てます。

ステップ 10 [Upload a CSV with RF settings back] をクリックして、ローカルマシンから RF 設定のバックアップをアップロードします。

ステップ 11 [Choose a file] をクリックして CSV ファイルをインポートするか、CSV ファイルをドラッグ アンド ドロップ エリアにドラッグアンドドロップします。

（注） CSV ファイルの最大サイズは 10 MB です。

アップロードされた CSV ファイルから、選択したロケーション名に基づく RF 設定が見つかった場合、[Confirm RF Settings for Selected Locations] ウィンドウに [Location] と [Matched RF Profiles] が表示されます。

ステップ 12 [Confirm RF Settings for Selected Locations] ウィンドウを確認し、[Confirm] をクリックします。

ステップ 13 [Unassign] をクリックします。

ステップ 14 確認ウィンドウで、[Continue] をクリックします。

ステップ 15 メニューアイコン（☰）をクリックして、**[Activities]** > **[Tasks]**を選択して、AI RF プロファイルタスクへの次回、進行中、完了、および失敗したロケーションの割り当て解除を表示します。

次のタスク

AI RF プロファイル対応建物のデバイスのプロビジョニング

次の手順では、AI RF プロファイルが割り当てられたロケーション全体にデバイスをプロビジョニングして、AI RF プロファイルを展開する方法について説明します。

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

[Inventory] ウィンドウの [Device] テーブルには、検出された AI RF プロファイルに関連付けられたデバイスが一覧表示されます。

2. プロビジョニングする AI RF プロファイルに関連付けられたデバイス名の横にあるチェックボックスをオンにします。
3. [Actions] ドロップダウンリストから、**[Provision]** > **[Provision Device]** を選択します。
4. すべての手順を実行し、[Summary] ステップで [Deploy] をクリックします。
5. [概要] ウィンドウで、デバイスにプッシュされる残りのネットワーク設定を確認します。詳細については、ワイヤレスデバイスプロビジョニングの概要（421 ページ）を参照してください。

基本無線周波数プロファイルをAI無線周波数プロファイルにアップグレードする

始める前に

AI 拡張 RRM サービスにサイトをオンボードするには、次のサービスの少なくとも 1 つを有効にする必要があります。

- フレキシブル ラジオ アサインメント（FRA）
- 動的チャネル割り当て（DCA）
- 伝送パワー コントロール（TPC）[でんそうぱわーこんとろーるTPC]
- 動的帯域幅選択（DBS）

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

ステップ 2 [Wireless] タブをクリックします。

ステップ 3 左側のペインで、[Global] サイトをクリックします。

ステップ 4 AI RF プロファイルにアップグレードする基本 RF プロファイル名の横にあるチェックボックスをオンにします。

ステップ 5 [Action] ドロップダウンリストから、[Upgrade to AI] を選択します。

ステップ 6 確認ウィンドウで [Yes] をクリックします。

ステップ 7 [Edit AI RF Profile] ウィンドウで、AI RF プロファイル設定を構成します。詳細については、AI 無線周波数プロファイルの作成 （273 ページ）を参照してください。

非ファブリック展開用の Cisco センサー SSID のプロビジョニング

- Cisco DNA Center センサーは、Cisco センサー プロビジョニング サービス セット識別子（SSID）を使用して、プラグアンドプレイ（PnP）サーバーと通信し、テストを実行するための Day-0 設定を取得します。

（注） Cisco センサープロビジョニング SSID は、センサーとして動作する AP には適用されません。

- ファブリック展開の場合、Cisco センサープロビジョニング SSID は、Cisco DNA Center と通信するためにインフラストラクチャ仮想ネットワーク アクセスポイント（INFRA VN-AP）プールにマッピングされます。
- 次のプラットフォームは Cisco センサープロビジョニング SSID をサポートしています。
  - Cisco AireOS コントローラ
  - Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ（ファブリック展開と非ファブリック展開の両方）
- Cisco センサープロビジョニング SSID は次のネットワークコントローラをサポートしています。
  - クラウド向け Cisco Catalyst 9800 ワイヤレスコントローラ
  - Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ
  - Cisco AireOS コントローラ

次の手順で、非ファブリック展開の Cisco センサープロビジョニング SSID を設定できます。

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

ステップ 2 [Wireless] タブをクリックします。

ステップ 3 [SSID] テーブルから、Add にカーソルを合わせて、[Enterprise] を選択します。

ワイヤレス SSID ワークフローが表示されます。

ステップ 4 [Sensor] フィールドを切り替えて、[Next] をクリックします。

（注） SSID のパラメータは自動的に入力され、編集できません。

ステップ 5 [Next] をクリックします。

ステップ 6 [Wireless Profiles] 画面で、[Profiles] のプロファイルを確認します。

[Edit Wireless Profile] ダイアログボックスが表示されます。

ステップ 7 [Fabric] で [Yes] を選択し、[Save] をクリックします。

「Success Profile sensorProfile selected」というメッセージが表示されます。

ステップ 8 [Finish] をクリックします。

ステップ 9 メニューアイコン（☰）をクリックして、**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。

ステップ 10 デバイスを確認し、[Actions] ドロップダウンメニューから **[Provision]** > **[Provision Device]** の順に選択します。

ステップ 11 [Assign Site]、[Configuration]、[Model Configuration]、[Advanced Configuration]、および [Summary] で詳細を確認します。各画面で [Next] をクリックしてください。

ステップ 12 [Deploy] をクリックします。

[Provision Device] ダイアログボックスが表示されます。

ステップ 13 [Now] を選択し、[Apply] をクリックします。

結果：「Task Scheduled view status in Tasks」というメッセージが右下隅に表示されます。

バックホールの設定の管理

ワイヤレスセンサのバックホール設定を表示、作成、管理するには、次の手順を実行します。ワイヤレスセンサーには、Cisco DNA Center と通信するためのバックホール SSID が必要です。

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

[Sensor List] ウィンドウが表示されます。

ステップ 2 [Settings] タブにカーソルを合わせ、[Backhaul Settings] を選択します。

ステップ 3 バックホール SSID を追加および管理するには、次の手順を実行します。

a) [Add Backhaul] をクリックします。

[Create Sensor Backhaul SSID Assignment] ウィンドウが表示され、[Wired Backhaul] と [Wireless Backhaul] の 2 つの領域が表示されます。

b) [Settings name] フィールドでバックホール SSID の名前を入力します。

c) [Wired Backhaul] 領域で、次を設定します。

- [Level of Security]：選択した SSID で使用されている暗号化と認証タイプが表示されます。使用可能なセキュリティのオプションは次のとおりです。
  - [802.1x EAP]：Extensible Authentication Protocol（EAP）を有線 LAN で渡すために使用される規格。
  - [Open]：セキュリティまたは認証は使用されません。
- [EAP Method]：[802.1x EAP] を選択した場合は、ドロップダウンリストからユーザ認証に次のいずれかの EAP 方式を選択する必要があります。

- [EAP-FAST]：指定されたフィールドにユーザ名とパスワードを入力します。
- [PEAP-MSCHAPv2]：指定されたフィールドにユーザ名とパスワードを入力します。
- [EAP-TLS]：[Enroll Using Certificate Bundle] または [Enroll Using SCEP] を選択します。

  [Enroll Using Certificate Bundle] を選択した場合は、[Certificate Bundle] の下にあるドロップダウン矢印をクリックし、[+ Add New Certificate Bundle] をクリックして、ユーザ名と証明書バンドルパスワードを入力します。
- [PEAP-TLS]：[Enroll Using Certificate Bundle] または [Enroll using SCEP] を選択します。

  [Enroll Using Certificate Bundle] を選択した場合は、[Certificate Bundle] の下にあるドロップダウン矢印をクリックし、[+ Add New Certificate Bundle] をクリックして、ユーザ名と証明書バンドルパスワードを入力します。

d) [Wireless Network Name（SSID）] 領域で、ワイヤレスネットワーク（SSID）を選択し、次を設定します。

- [Level of Security]：選択した SSID で使用されている暗号化と認証タイプが表示されます。使用可能なセキュリティのオプションは次のとおりです。
  - [WPA2 Enterprise]：拡張可能認証プロトコル（EAP）（802.1x）を使用してより高レベルのセキュリティを実現し、リモート RADIUS サーバでネットワークユーザを認証および承認します。
  - [WPA2-Personal]：パスフレーズまたは事前共有キー（PSK）を使用して、良好なセキュリティを実現します。ワイヤレスネットワークにアクセスするパスキーがあれば誰でも使用できます。

    [WPA2 Personal] を選択した場合は、[Passphrase] テキストボックスにパスフレーズを入力します。
  - [PSK Format]：使用可能な事前共有キーの形式は次のとおりです。
    - [ASCII]：ASCII PSK パスフレーズをサポートします。
    - [HEX]：64 文字の HEX キー PSK パスワードをサポートします。
  - [Open]：セキュリティまたは認証は使用されません。

e) [Save] をクリックします。

ステップ 4 既存のバックホール設定を編集するには、次の手順を実行します。

a) バックホール設定のチェックボックスをオンにします。
b) [Actions] ドロップダウンリストにカーソルを合わせて、[Edit] を選択します。

ステップ 5 バックホール設定を削除するには、次の手順を実行します。

a) バックホール設定のチェックボックスをオンにします。

b) [Actions] ドロップダウンリストにカーソルを合わせて、[Delete] を選択します。

Cisco Connected Mobile Experiences の統合について

Cisco DNA Center ワイヤレスマップのためのコネクテッドモバイルエクスペリエンス（CMX）の統合をサポートしています。CMX を統合すると、Cisco DNA Center ユーザーインターフェイス内で、フロアマップ上でのワイヤレスクライアント、不正アクセスポイントおよび干渉源の正確な場所を把握できます。

CMX の設定は、ユーザーの要件に応じて、グローバルレベルで、あるいはサイト、ビルディング、またはフロアレベルで作成できます。小企業の場合はグローバルレベル（親ノード）で CMX を割り当てることができます。すべての子ノードが親ノードから設定を継承します。中企業の場合はビルディング レベルで CMX を割り当てることができ、小企業の場合はフロアレベルで CMX を割り当てることができます。

（注） セキュリティ上の理由から、CMX は匿名にする必要があります。

Cisco CMX 設定の作成

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

ステップ 2 [External Services] セクションで、[DNA Spaces/CMX Servers] をクリックします。

[DNA Spaces/CMX Servers] ウィンドウが表示されます。

ステップ 3 [CMX Servers] テーブルから、[Add] をクリックします。

ステップ 4 [Add CMX Server] スライドインペインで、次のフィールドに入力します。

- [IP Address]：CMX Web GUI の有効な IP アドレスを入力します。
- [User Name]：CMX Web GUI のユーザー名を入力します。
- [Password]：パスワードログイン情報を入力します。
- [SSH User Name]：CMX 管理者のユーザー名を入力します。
- [SSH Password]：CMX 管理者のパスワードログイン情報を入力します。

（注） CMX が到達可能であることを確認してください。

ステップ 5 [Add]をクリックします。

CMX サーバーが正常に追加されました。

ステップ 6 CMX サーバーをサイト、建物、またはフロアに割り当てるには、メニューアイコンをクリックし、**[Design]** > **[Network Settings]**の順に選択します。

ステップ 7 [Wireless] タブをクリックします。

ステップ 8 左側の [Tree View] メニューで、[Global] か、興味のあるエリア、ビルディング、フロアを選択します。

ステップ 9 [DNA Spaces/CMX Servers] セクションで、ドロップダウンリストを使用して、CMX サーバーを選択します。

ステップ 10 [Save] をクリックします。

[Create CMX Settings] ページが表示されます。

CMX の追加後に [Network Hierarchy] ページのフロアに変更を加えた場合、その変更は自動的に CMX と同期されます。

CMX が同期されると、Cisco DNA Center はクライアントロケーションを CMX に照会し、その場所がフロアマップに表示されます。

ステップ 11 フロアマップでは、次のことを実行できます。

- クライアントの場所を表示します。これは青色のドットとして表示されます。
- AP 上にカーソルを移動します。ダイアログボックスは、[Info]、[Rx Neighbor]、[Clients] タブで表示されます。詳細については、各タブをクリックしてください。[Device 360] をクリックして、デバイス 360 ウィンドウを開き、問題を表示します。問題をクリックして、問題の場所とクライアント デバイスの場所を表示します。
- AP をクリックして、AP に関する詳細を含むサイド バーを開きます。
- Intelligent Capture と CMX を統合するときにリアルタイムでクライアント トラッキングを実行します。

ステップ 12 変更を加えたときにCMXがダウンした場合は、手動で同期する必要があります。同期するには、[Network Hierarchy] ページで、左側のツリーペインで変更を加えた建物やフロアの隣にある省略記号 ••• の上にカーソルを置き、[Sync: DNA Spaces/CMX] を選択して、変更を手動でプッシュします。

ステップ 13 CMX サーバーの詳細を編集する場合や CMX サーバーを削除する場合は、次の手順を実行します。

a) メニューアイコン（≡）をクリックして、**[System]** > **[Settings]**の順に選択します。
b) [External Services] セクションで、[DNA Spaces/CMX Servers] をクリックします。
c) 編集する CMX サーバーを選択して変更を加え、[Update] をクリックします。
d) 削除する CMX サーバーを選択し、[Delete] をクリックします。
e) [OK] をクリックして削除を実行します。

CMX 認証に失敗した場合

- Cisco DNA Center で CMX 設定の作成時に指定したログイン情報で、CMX Web GUI にログインできるか確認します。
- SSH を使用して CMX コンソールにログインできるかどうかを確認します。
- CMX GUI の API ドキュメンテーションリンクを使用して CMX REST API を使用できるかどうかを確認します。

クライアントが Cisco DNA Center フロアマップに表示されない場合

- 特定のフロアのシスコ ワイヤレス コントローラが CMX で設定されており、アクティブになっているか確認します。
- CMX GUI でフロアマップにクライアントが表示されるか確認します。
- Cisco DNA Center マップ API を使用して、フロアにクライアントをリスト表示します。

```
curl -k -u <user>:<password> -X GET
/api/v1/dna-maps-service/domains/<floor group
id>/clients?associated=true
```

Cisco DNA Spaces の統合について

現実の世界で事業を行っている企業は、これまで、建物内の人々や接続されたアセットの動きを可視化できませんでした。Cisco DNA Spaces は、基盤となるすべてのシスコ ワイヤレス ネットワークによって提供されるロケーション感知インテリジェンスを使用し、データをビジネス対応の洞察に変換することで、この物理的な死角の問題を解決します。

Cisco DNA Center は、Cisco DNA Spaces の統合をサポートします。Cisco DNA Spaces を統合すると、Cisco DNA Center の GUI 内で、フロアマップ上でのワイヤレスクライアント、不正 AP、および干渉源の正確な場所を把握できます。Cisco DNA Spaces の設定は、ユーザーの要件に応じて、グローバルレベルで、あるいはサイト、ビルディング、またはフロアレベルで作成できます。

（注） 現在、Cisco DNA Center と Cisco DNA Spaces の統合は、自動マップエクスポートとロケーション階層の同期のみに制限されています。この統合では、キャプティブポータルベースの認証機能はサポートされません。

Cisco DNA Spaces と Cisco DNA Center の統合

Cisco DNA Spaces と Cisco DNA Center を統合するには、次の手順を使用します。

ステップ 1 Cisco DNA Spaces クライアントをオンボードします。

a) 電子メール ID を使用して Cisco DNA Spaces にログインし、[Continue] をクリックします。
b) [Select Customer] ドロップダウンリストから、Cisco DNA Center インスタンスの Spaces テナント（たとえば、dna-center-dev-US）を選択し、[Proceed] をクリックします。
c) Cisco DNA Spaces GUI でメニューアイコンをクリックして、**[Setup]** > **[Wireless Networks]**の順に選択します。
d) [Connect your wireless network] ウィンドウで、『*Cisco DNA Spaces Configuration Guide*』に記載されている手順 1 ー 3 を実行して、Cisco DNA Spaces クライアントをオンボードします。

『*Cisco DNA Spaces Configuration Guide*』には、**[Need Help?]** > **[View Configuration Steps]**の下にある右側のペインからアクセスできます。

ステップ 2 Cisco DNA Center を Cisco DNA Spaces に登録します。

a) 電子メール ID を使用して Cisco DNA Spaces にログインし、[Continue] をクリックします。

b) [Select Customer] ドロップダウンリストから、Cisco DNA Center インスタンスの Spaces テナント（たとえば、dna-center-dev-US）を選択し、[Proceed] をクリックします。

c) Cisco DNA Spaces GUI でメニューアイコンをクリックし、**[Integrations]** > **[Cisco DNA Center]**の順に選択します。

d) [DNAC Integration] ウィンドウで、[Create Token] をクリックします。

[Create new token] ダイアログボックスが表示されます。

e) [Instance Name] フィールドに、インスタンスの一意の名前を入力し、[Create Token] をクリックします。

インスタンスの新しいトークンが開きます。

f) トークンの右側までスクロールし、[Copy Token] を選択します。

g) トークンを Cisco DNA Center GUI に貼り付けるには、Cisco DNA Center にログインします。

h) Cisco DNA Center GUI でメニューアイコン（☰）をクリックして、**[System]** > **[Settings]**の順に選択します。

i) 左側のナビゲーションウィンドウで、下にスクロールして [DNA Spaces/CMX Servers] を選択します。

[DNA Spaces/CMX Servers] ウィンドウが表示されます。

j) [Cisco DNA Spaces] エリアで、[Activate] を選択します。

[Integrate DNA Spaces] ダイアログボックスが表示されます。

k) [Tenant Token] テキストボックスで、Ctrl+V キーを押して Cisco DNA Spaces からコピーしたトークンを貼り付け、[Connect] をクリックします。

[Success] ダイアログボックスに次の情報が表示されます。

```
This cluster is integrated with Cisco DNA Spaces successfully.
```

[DNA Spaces/CMX Servers] ウィンドウに緑色の✓[Activated] ステータスが表示され、Cisco DNA Spaces で選択したテナント（たとえば、dna-center-dev-US）が [Tenant] フィールドに表示されます。

ステップ 3 Cisco DNA Spaces を Cisco DNA Center のサイトに割り当てます。

a) Cisco DNA Center GUI でメニューアイコン（☰）をクリックして、**[Design]** > **[Network settings]**。

b) [Wireless] タブをクリックします。

c) 左側のツリービューメニューで、[Global] か、Cisco DNA Spaces に割り当てるエリア、ビルディング、またはフロアを選択します。

d) [DNA Spaces/CMX Servers] セクションのドロップダウンリストを使用してサイトを選択します（たとえば、DNA Spaces - dna-center-dev-US）。

e) [**保存**（**Save**）] をクリックします。

ステップ 4 Cisco DNA Spaces を使用して Cisco DNA Center のサイトをモニターします。

a) Cisco DNA Center GUI でメニューアイコン（☰）をクリックして、**[Design]** > **[Network Hierarchy]**。

b) 左側のツリービューメニューで、[Global] か、Cisco DNA Spaces にモニターさせるエリア、ビルディング、またはフロアを選択します。

Cisco DNA Center により、サイト情報が Cisco DNA Spaces に自動的に展開されます。

c) Cisco DNA Spaces が動作していることを確認するには、次の図に示すように、Cisco DNA Spaces/CMX ステータスアイコンがモニターするフロアに表示されていることを確認します。

図 *20 : Cisco DNA Spaces* ステータスアイコン

FlexConnect VLAN の設定

次の FlexConnect VLAN 設定を指定することができます。

- [Native VLAN]：FlexConnect グループが AP と シスコ ワイヤレス コントローラ の間で管理トラフィックを伝送できるようにします。
- [AAA Override VLAN]：ローカルでスイッチングされるクライアントの動的 VLAN 割り当てを提供します。

これらの設定をグローバルレベルで適用して、サイト、ビルディング、またはフロアレベルの設定をオーバーライドすることができます。

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

ステップ 2 [Wireless] タブをクリックします。

ステップ 3 左側のペインで、適切な範囲を選択します。

- [Global]：すべてのサイトに対してグローバルレベルで VLAN を設定します。
- [Site]、[Building]、または [Floor]：選択したレベルでのみ VLAN を設定します。

ステップ 4 [Native VLAN ID] フィールドに、VLAN ID の値を入力します。有効な範囲は 1 ～ 4094 です。

ステップ 5 [AAA Override VLAN] 設定の場合は、VLAN ID と VLAN 名のマッピングを、対応する [VLAN ID] フィールドと [VLAN Name] フィールドに入力します。さらにマッピングを追加するには、[Add] アイコンをクリックします。

（注） FlexConnect 展開に対して定義できる VLAN マッピングの最大数は 16 です。ただし、Cisco Catalyst 9800 ワイヤレスコントローラの場合、この数には、デフォルトの WLAN VLAN と、AAA によってプッシュされた VLAN が含まれます。

ステップ 6 [保存（**Save**）] をクリックします。

次のタスク

ワイヤレス ネットワーク プロファイルを作成するか、SSID を設定します。

- **ワイヤレス ネットワーク プロファイル**：ワイヤレス ネットワーク プロファイルを作成する場合は、[FlexConnect Local Switching] チェックボックスがオンになっていることを確認します。詳細については、ワイヤレス用のネットワークプロファイルの作成（304ページ）を参照してください。
- [SSID]：SSID を設定する場合は、エンタープライズ ワイヤレス ネットワーク用 SSID の作成（248 ページ）およびゲスト ワイヤレス ネットワークの SSID の作成（256 ページ）を参照してください。

保存済みの FlexConnect VLAN 設定をワイヤレスコントローラで設定するには、ワイヤレスコントローラをプロビジョニングする必要があります。詳細については、Cisco AireOS コントローラのプロビジョニング（422 ページ）またはCisco Catalyst 9800 シリーズ ワイヤレス コントローラの設定とプロビジョニング（437 ページ）を参照してください。

ワイヤレスコントローラ のプロビジョニング後に、コントローラに関連付けられている AP をプロビジョニングする必要があります。

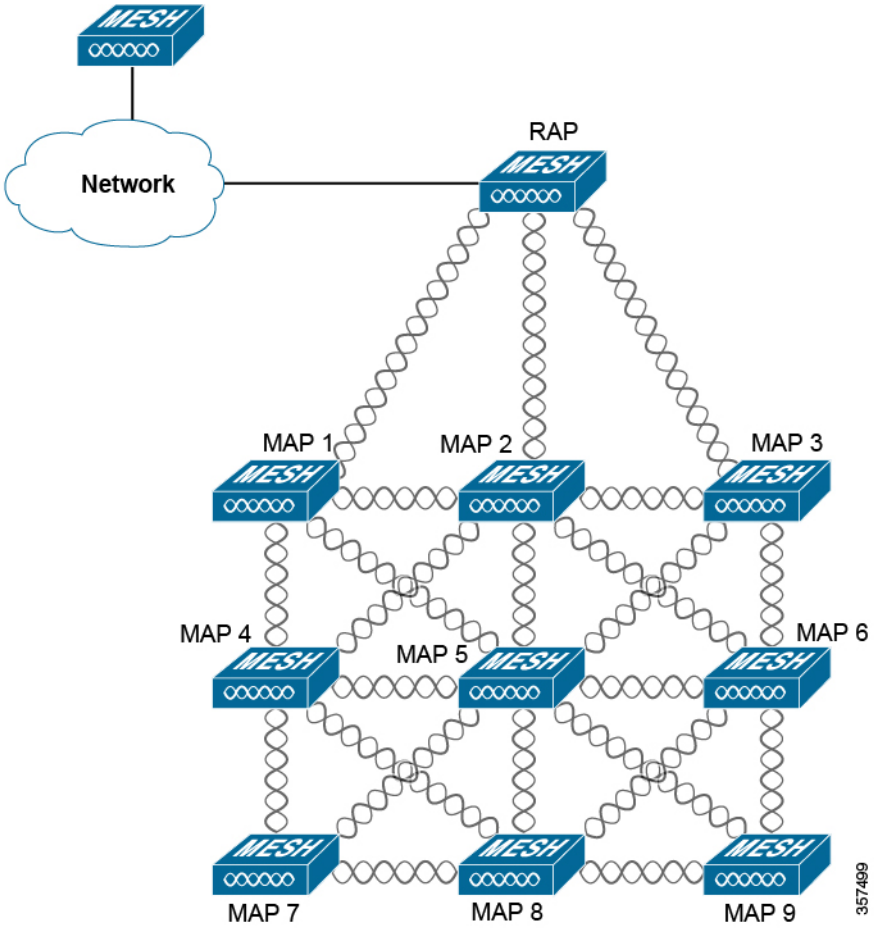
ワイヤレス メッシュ ネットワークについて

シスコ ワイヤレス メッシュ ネットワーク内のアクセスポイント（AP）は、次の 2 つの方法のいずれかで動作します。

- ルートアクセスポイント（RAP）：それぞれの場所で有線ネットワークに接続します。
- メッシュアクセスポイント（MAP）：ワイヤレスで通信し、安全でスケーラブルなワイヤレス LAN を提供します。

（注） すべての AP は MAP として設定され、出荷されています。AP を RAP として使用するには、AP を RAP として再設定する必要があります。すべてのメッシュネットワークで、少なくとも 1 つの RAP があることを確認します。

RAP は、それぞれの場所で有線ネットワークに接続します。すべてのダウンストリーム AP は、MAP として動作し、ワイヤレスリンクを使用して通信します。



MAP と RAP はいずれも WLAN クライアントアクセスを提供します。ただし、一般に、RAP の場所は高い確率でクライアントアクセスの提供に向いていません。

MAP から CAPWAP セッションを終端させるオンサイトコントローラがある建物もありますが、CAPWAP セッションはワイドエリアネットワーク（WAN）を介してコントローラにバックホールできるため、それは必須要件ではありません。

Cisco ワイヤレス バックホール ネットワークでは、トラフィックを MAP と RAP の間でブリッジできます。このトラフィックは、ワイヤレスメッシュによってブリッジされている有線デバイスからのトラフィックか、MAP からの CAPWAP トラフィックになります。このトラフィックは、ワイヤレス バックホールなどのワイヤレス メッシュ リンクを通過する際に必ず AES 暗号化されます。

メッシュネットワークの詳細については、最新の『Cisco Wireless Mesh Access Points, Design and Deployment Guide』を参照してください。

AP Configuration

メッシュネットワークモードで使用する既存の AP がある場合は、最初に [Configure Access Point] ワークフローを使用して AP モードを [Bridge] または [Flex+Bridge] に変更する必要があります。詳細については、AP ワークフローの設定 （791 ページ）を参照してください。

AP を [Bridge] モードまたは [Flex+Bridge] モードに設定すると、[AP 360] ウィンドウにメッシュ設定が表示されます。この時点で、AP を新しい設定でプロビジョニングする必要があります。シスコ製 AP のプロビジョニング：Day 1 AP プロビジョニング （430 ページ）。

シスコ ワイヤレス コントローラ の設定

メッシュネットワークの場合は、コントローラで許可 AP のリストを設定する必要があります。コントローラは、許可リストに含まれている MAP からの要求にのみ応答します。

（注） Cisco DNA Center は、Cisco IOS リリース 17.5 以降を実行している Cisco Catalyst 9800 ワイヤレスコントローラでの許可リストの設定をサポートしています。

AireOS ワイヤレスコントローラと Catalyst 9800 ワイヤレスコントローラの両方で、Cisco DNA Center を使用してブリッジグループ名（BGN）と RAP ダウンリンク バックホール メッシュの設定を指定することができます。Catalyst 9800 ワイヤレスコントローラでは、MAP の最大範囲、バックホール クライアント アクセス、およびバックホールデータレートを設定することもできます。

これらの設定は、[Wireless Network Settings] ウィンドウで、フロアレベルで指定されます。詳細については、シスコ ワイヤレス コントローラ でのメッシュ設定の指定 （294 ページ）を参照してください。

シスコ ワイヤレス コントローラ でのメッシュ設定の指定

AireOS および Catalyst 9800 ワイヤレスコントローラでメッシュ設定を指定することができます。

（注） 範囲、バックホールクライアントアクセス、およびバックホールデータレートは、Cisco DNA Center を介して AireOS コントローラに適用できません。

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

ステップ 2 [Wireless] タブをクリックします。

ステップ 3 左側のペインで、フロアを選択します。

（注） メッシュ設定は、フロアごとにのみ指定されます。

ステップ 4 [Authorized Access Points] で、[Manage Authorized Access Points] をクリックします。

ステップ 5 [Manage Authorized Access Points] ペインで、コントローラへの参加を許可する MAP の MAC アドレスを入力します。コントローラは、認証リストに含まれている MAP からの CAPWAP 要求にのみ応答します。

次のいずれかの方法で MAC アドレスを入力してください。

- **CSV ファイルのアップロード**：CSV テンプレートファイルをダウンロードし、そのファイルに MAC アドレスを追加します。次に、CSV ファイルをドラッグしてドロップエリアにドロップすることにより、または [Choose a file] をクリックし、CSV ファイルを参照して選択することにより、ファイルをアップロードします。
- **MAC アドレスの手動追加**：設定する MAC アドレスが少数の場合は、[Add] をクリックし、[MAC Address] の下に表示されるフィールドに MAC アドレスを入力します。さらに MAC アドレスを追加するには、[Add] をクリックします。

ステップ 6 [保存（**Save**）] をクリックします。

ステップ 7 [Mesh Settings] で、次のパラメータを設定します。

- [Bridge Group Name]：ブリッジグループ名（最大 10 文字）を入力します。ブリッジグループ名（BGN）によって、MAP の関連付けが制御されます。無線をグループ化することにより、同じチャネル上にあるが BGN が異なる 2 つのネットワークが互いに通信することはできません。この設定はまた、ネットワーク内の同一セクター（エリア）に複数のルートアクセスポイント（RAP）がある場合にも便利です。

  NULL VALUE という BGN がデフォルトで設定されています。この BGN は表示されませんが、これにより、ネットワーク固有の BGN を割り当てる前に MAP をネットワークに参加させることができます。

- [Range (in Ft)]：ネットワーク内のすべての MAP の最大範囲（フィート単位）。

- [Backhaul Client Access]：無線バックホールを介したワイヤレス クライアント アソシエーションを許可します。無線バックホールには、大部分の MAP で 5 GHz 帯が使用されます。つまり、バックホール無線は、バックホール トラフィックとクライアント トラフィックの両方を伝送できます。

  [Backhaul Client Access] が無効な場合は、バックホールトラフィックのみがバックホール無線を介して送信され、クライアント アソシエーションは 2 次的な無線のみを介して送信されます。

- [RAP Downlink Backhaul]：[5 GHz] または [2.4 GHz] オプションボタンをクリックします。お住まいの国で 5 GHz の使用が禁止されている場合は 2.4 GHz を選択します。5 GHz が許可されている国でも、メッシュまたはブリッジの距離がはるかに長くなる 2.4 GHz の無線周波数の使用が適している場合もあります。

  （注） RAP 設定が 5 GHz から 2.4 GHz に変更されると、更新は RAP からすべての MAP に伝播されます。この時点で、MAP は 5 GHz ネットワークから切断され、2.4 GHz ネットワークに接続します。

- [Backhaul Data Rates]：[5GHz Band Radio Type] および [2.4GHz Band Radio Type] のドロップダウンリストから、インターフェイスレートを選択します。有効なバックホールインターフェイス レートは、アクセスポイントに応じて、[802.11abg]、[802.11n]、[802.11ac]（5GHz 帯域無線のみ）、[802.11ax]、および [Auto] です。バックホールは、アクセスポイント間でワイヤレス接続を作成するために使用されます。利用可能な RF スペクトラムを効果的に使用するにはレート選択が重要です。このレートは、クライアント デバイスのスループットにも影響を与える可能性があります

[Auto] データレートを使用すると、各リンクは、そのリンク品質に対して可能な限り最高のレートで到達できます。

メッシュバックホールのデータレートは [Auto] に設定することをお勧めします。

ステップ 8 [Save] をクリックします。

第 10 章

ネットワークプロファイルの設定

ネットワークプロファイルの概要

ネットワークプロファイルを使用すると、設定を構成し、特定のサイトまたはサイトの特定のグループに適用できます。Cisco DNA Center のさまざまな要素のネットワークプロファイルを作成できます。

アシュアランス用のネットワークプロファイルの作成

アシュアランスのネットワークプロファイルを作成すると、問題を設定して、グローバルな問題の設定とは別にサイトまたはサイトのグループに適用できます。問題を有効または無効にしたり、優先順位を変更したりできます。

注：

- アシュアランスでは、ネットワークデバイスの正常性スコアへの同期は、グローバルな問題設定に対してのみ使用できます。カスタムの問題設定では使用できません。詳細については、Cisco DNA Assurance ユーザガイドを参照してください。
- 一部のグローバルな問題はカスタマイズできません。これらの問題は、変更するカスタム問題のリストには表示されません。
- 変更された問題をリストの一番上に表示するには、[Last Modified] でソートします。
- カスタム設定を削除するには、最初にすべてのサイトの割り当てを解除する必要があります。

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

ステップ 2 [+Add Profile] をクリックし、[Assurance] を選択します。

ステップ 3 [Profile Name] フィールドに有効なプロファイルの名前を入力し、[Next] をクリックします。

Cisco DNA Center によってプロファイルが追加され、[Edit Profile] ウィンドウが表示されます。

ステップ 4 設定する問題のタイプを表示するには、[DEVICE TYPE] と [CATEGORY] フィルタを設定します。

ステップ 5 [Issue Name] 列の問題をクリックすると、設定を含むスライドインペインが開きます。

（注） いくつかの問題については、設定に加えられた変更は複数のデバイスタイプで共有されます。スライドインペインに、影響を受けるデバイスタイプを示す注意が Cisco DNA Center によって表示されます。

ステップ 6 この問題の Cisco DNA Center によるモニターリングを有効または無効にするには、[Enabled] トグルボタンをクリックします。

ステップ 7 問題の優先順位を設定するには、[Priority] ドロップダウンリストをクリックし、優先順位を選択します。次のオプションがあります。

- [P1]：ネットワーク運用に幅広い影響を与える可能性があり、早急な対応を必要とする重大な問題。
- [P2]：複数のデバイスまたはクライアントに影響を与える可能性がある重大な問題。
- [P3]：局所的または最小限の影響を与える軽微な問題。
- [P4]：ただちに問題になるものではないが、対処するとネットワークのパフォーマンスを最適化できる警告レベルの問題。

ステップ 8 （一部の問題のみ）[Trigger Condition] エリアで、問題が報告される条件のしきい値を変更できます。

トリガー条件の例：

```
No Activity on Radio(2.4 GHz) >= 60 minutes.

Memory Utilization of Access Points greater than 90%.
```

ステップ 9 （任意） 設定に変更がある場合は、[View Default Settings] の上にカーソルを置くと、デフォルトの設定が表示されます。問題の設定をすべてデフォルト値に復元するには、[Use Default] をクリックします。

ステップ 10 [Apply] をクリックします。

ステップ 11 （特定の問題について）[Manage Subscriptions] をクリックすると、サポートされている問題がトリガーされたときの外部通知に登録できます。

ステップ 12 このプロファイルをサイトに割り当てるには、[Assign Sites] をクリックします。このプロファイルを関連付けるサイトの横にあるチェックボックスをオンにし、[Save] をクリックします。

[Edit Profile] ウィンドウが表示されます。

（注） 親ノードまたは個々のサイトを選択できます。親ノードを選択すると、その親ノードに属する子もすべて選択されます。チェックボックスをオフにして、サイトの選択を解除できます。

ステップ 13 [Done] をクリックします。

新しく追加されたプロファイルが、[Network Profiles] ウィンドウに表示されます。

ファイアウォール用のネットワークプロファイルの作成

このワークフローでは、次を実行する方法を示します。

1. カスタム構成を作成します。
2. Firepower Threat Defense（FTD）構成を作成します。
3. プロファイルの概要を表示します。

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

ステップ 2 [+Add Profile] をクリックし、[Firewall] を選択します。

[Firewall Type] ページが表示されます。

ステップ 3 適応型セキュリティアプライアンス（ASA）ファイアウォールなどの通常のファイアウォール用のカスタム構成を作成するには、次の手順を実行します。

a) [Name] フィールドに、プロファイルの名前を入力します。

b) [Devices] ドロップダウンリストからデバイスの番号を選択します。

（注） プロファイルごとに最大 10 のデバイスを選択できます。

c) [Device Type] ドロップダウンリストからデバイスのタイプを選択します。
d) （任意） [Device Tag] ドロップダウンリストからデバイスタグを選択します。
e) [Next] をクリックします。

[Custom Configuration] ページが表示されます。

f) [Template] ドロップダウンリストからテンプレートを選択します。

（注） テンプレートがない場合は、**[Tools]** > **[Template Editor]** で少なくとも 1 つのテンプレートを作成する必要があります。詳細については、テンプレートの作成 （316ページ）を参照してください。

g) [Next] をクリックします。

[Summary] ページが表示されます。このページには、カスタム構成の概要が表示されます。選択されたデバイスタイプに基づいて、ハードウェアの推奨事項が提示されます。

h) [Save] をクリックします。

[Network Profiles] ページが表示されます。

i) ネットワークプロファイルにサイトを割り当てるには、[Assign Sites] をクリックします。詳細については、ネットワーク階層のサイトの作成 （166 ページ）を参照してください。

ステップ 4 FTD デバイスを設定するための FTD 構成を作成するには、次の手順を実行します。

a) [Name] フィールドに、プロファイルの名前を入力します。
b) [Devices] ドロップダウンリストからデバイスの番号を選択します。

（注） プロファイルごとに最大 10 のデバイスを選択できます。

c) FTD ファイアウォールをプロビジョニングするには、[FTD] チェックボックスをオンにします。
d) [Device Type] ドロップダウンリストからデバイスのタイプを選択します。
e) （任意） [Device Tag] ドロップダウンリストからデバイスタグを選択します。
f) [Next] をクリックします。

[FTD Configuration] ページが表示されます。

g) [Routed Mode] または [Transparent Mode] オプションボタンをクリックします。
h) [Next] をクリックします。

[Summary] ページが表示されます。このページには、FTD 構成の概要が表示されます。選択されたデバイスタイプに基づいて、このページにハードウェアの推奨事項が示されます。

i) [Save] をクリックします。

[Network Profiles] ページが表示されます。

j) ネットワークプロファイルにサイトを割り当てるには、[Assign Sites] をクリックします。詳細については、ネットワーク階層のサイトの作成 （166 ページ）を参照してください。

ルーティング用のネットワークプロファイルの作成

このワークフローでは、次を実行する方法を示します。

1. ルータ WAN を設定します。
2. ルータ LAN を設定します。
3. 統合スイッチ構成を設定します。
4. カスタム構成を作成します。
5. プロファイルの概要を表示します。

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

ステップ 2 [+Add Profile] をクリックし、[Routing] を選択します。

ステップ 3 [Router WAN Configuration] ウィンドウが表示されます。

- [Name] テキスト ボックスにプロファイル名を入力します。
- ドロップダウンリストから、[Service Providers] および [Devices] の数を選択します。プロファイルあたり最大 3 つのサービスプロバイダと 10 つのデバイスがサポートされています。
- ドロップダウンリストから [Service Provider Profile] を選択します。詳細については、サービス プロバイダ プロファイルの設定 （247 ページ）を参照してください。
- ドロップダウンリストから [Device Type]デバイスタイプを選択します。
- [Device Tag] に一意の文字列を入力して異なるデバイスを識別するか、ドロップダウンリストから既存のタグを選択します。2 つ以上のデバイスが同じタイプの場合は、デバイスタグを使用します。すべてのデバイスが異なるタイプの場合、デバイスタグはオプションです。選択内容は、ネットワークプロファイルに適用される Day-0 および Day-N テンプレートの一致基準の一部として使用されるため、適切なタグを選択してください。
- デバイスごとに 1 つ以上の回線リンクを有効にするには、[O] をクリックし、[Connect] の横のチェックボックスをオンにします。ドロップダウンリストから、[Line Type] を選択します。[OK] をクリックします。

  複数のサービスプロバイダを選択した場合は、プライマリインターフェイスをギガビットイーサネットとして、セカンダリをセルラーとして、または両方のインターフェイスをギガビットイーサネットとして選択できます。また、プライマリインターフェイスをセルラーとして、セカンダリインターフェイスをギガビットイーサネットとして選択することもできます。

  （注） Cisco 1100 シリーズ サービス統合型ルータ、Cisco 4200 シリーズ サービス統合型ルータ、Cisco 4300 シリーズ サービス統合型ルータ、および Cisco 4400 シリーズ サービス統合型ルータのみが、セルラーインターフェイスをサポートしています。

- **[Next]** をクリックします。

ステップ 4 [Router WAN Configuration] ページが表示されます。

- [Configure Connection] オプションボタンをクリックし、[L2] または [L3]、あるいはその両方を選択します。
- [L2] を選択した場合は、ドロップダウンリストから [Type] を選択し、[VLAN ID/Allowed VLAN] および [Description] を入力します。
- [L3] を選択した場合は、ドロップダウンリストから [Protocol Routing] を選択し、[Protocol Qualifier] を入力します。

[Skip] をクリックして、設定をスキップできます。

- **[Next]** をクリックします。

ステップ 5 [Integrated Switch Configuration] ページが表示されます。

統合スイッチの設定では、新しい VLAN を追加したり、ルータの LAN 設定で選択した以前の設定を保持したりすることができます。

- 1 つ以上の新しい VLAN を追加するには、[+] をクリックします。
- VLAN を削除するには、[x] をクリックします。
- [Next] をクリックします。

（注） Switchport インターフェイスのサポートは、Cisco 1100 シリーズおよび Cisco 4000 シリーズ サービス統合型ルータでのみ使用できます。

ステップ 6 [Custom Configuration] ページが表示されます。

カスタム構成はオプションです。この手順をスキップしても、[Network Profiles] ページでいつでも構成を適用できます。

カスタム構成の追加を選択した場合：

- 必要に応じて、[Onboarding Template（s）] または [Day-N Templates] タブをクリックします。
- ドロップダウンリストからテンプレートを選択します。テンプレートは、[Device Type] と [Tag Name] でフィルタ処理されます。
- [Next] をクリックします。

ステップ 7 [Summary] ページで、[Save] をクリックします。

このページには、ルータ設定の概要が表示されます。選択されたデバイスとサービスに基づいて、ハードウェアの推奨事項が提供されます。

ステップ 8 [Network Profiles] ページが表示されます。

[Assign Sites] をクリックして、ネットワークプロファイルにサイトを割り当てます。詳細については、ネットワーク階層のサイトの作成 （166 ページ）を参照してください。

スイッチ用のネットワークプロファイルの作成

スイッチングプロファイルには、次の 2 つのタイプの設定テンプレートを適用できます。

- オンボーディングテンプレート
- Day N テンプレート

始める前に

デバイスに適用する [Onboarding Configuration] テンプレートを定義します。このようなテンプレートには、ネットワーク上で管理できるようにデバイスをオンボードするための基本的なネットワーク設定コマンドが含まれています。デバイス設定の変更を自動化するテンプレートの作成 （315 ページ）を参照してください。

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

ステップ 2 [+Add Profile] をクリックし、[Switching] を選択します。

ステップ 3 [Switching profile] ウィンドウで、[Profile Name] テキストボックスにプロファイル名を入力します。

作成するテンプレートのタイプに応じて、[OnBoarding Template（s）] または [Day-N Template（s）] を選クリックします。

- [Add] をクリックします。
- [Device Type] ドロップダウンリストから、[Switches and Hubs] を選択します。
- ドロップダウンリストから [Tag Name] を選択します。この手順は任意です。選択したタグがすでにテンプレートに関連付けられている場合は、そのテンプレートのみが [Template] ドロップダウンリストで使用できます。
- ドロップダウンリストから [Device Type] を選択します。
- ドロップダウンリストから [Template] を選択します。すでに作成済みの [Onboarding Configuration] テンプレートを選択できます。

ステップ 4 [Save] をクリックします。

スイッチに設定されているプロファイルは、スイッチのプロビジョニング時に適用されます。サイトを有効にするには、サイトにネットワークプロファイルを追加する必要があります。

Cisco DNA トラフィック テレメトリ アプライアンス のネットワークプロファイルの作成

始める前に

テレメトリアプライアンスに適用するテンプレートを定義します。『デバイス設定の変更を自動化するテンプレートの作成 （315 ページ）』を参照してください。

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

ステップ 2 [+Add Profile] をクリックし、[Telemetry Appliance] を選択します。

ステップ 3 [Telemetry Appliance Type] ウィンドウで、次の情報を入力します。

a) [名前（Name）] テキスト ボックスにプロファイル名を入力します。

b) [Devices] ドロップダウンリストから、デバイスの数を選択します。

c) [Device Tag] ドロップダウンリストから、Cisco DNA Center で定義されている既存のデバイスタグを選択するか、新しいタグを入力します。この手順は任意です。選択したタグがすでにテンプレートに関連付けられている場合は、そのテンプレートのみが [Template] ドロップダウンリストで使用できます。

d) [Next] をクリックします。

ステップ 4 [Custom Configuration] ウィンドウで、テンプレートを選択します。選択したテンプレートは、デバイスが Cisco DNA Center のインベントリで管理されるようになると、そのデバイスに適用されます。

ステップ 5 [Next] をクリックします。

ステップ 6 [Summary] ウィンドウで、[Save] をクリックします。

ワイヤレス用のネットワークプロファイルの作成

始める前に

[Design] > **[Network Settings]** > **[Wireless]** タブでワイヤレス SSID を作成していることを確認します。

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

ステップ 2 [+Add Profile] をクリックし、[Wireless] を選択します。

ステップ 3 [Profile Name] フィールドに有効なプロファイル名を入力します。

ステップ 4 サイトをプロファイルに追加するには、[Assign] をクリックして、次の手順を実行します。

a) [Add Sites To Profile] スライドインペインで、このプロファイルを関連付けるサイトの横にあるチェックボックスをオンにします。

親ノードまたは個々のサイトを選択できます。親サイトを選択すると、その親ノードの下にある子もすべて選択されます。サイトの選択を解除するには、チェックボックスをオフにします。

b) [**保存（Save**）] をクリックします。

ステップ 5 次のタブで必要な設定を構成します。

- [SSIDs]：詳細については、ネットワークプロファイルへの SSID の追加（305 ページ）を参照してください。
- （オプション）[AP Zones]：詳細については、ネットワークプロファイルへの AP ゾーンの追加（306 ページ）を参照してください。
- [Model Configs]：詳細については、ネットワークプロファイルへのモデル設定の追加（307 ページ）を参照してください。
- [Templates]：詳細については、ネットワークプロファイルへのテンプレートの追加（308 ページ）を参照してください。
- （オプション）[Advanced Settings]：詳細については、ネットワークプロファイルの AP グループ、Flex グループ、サイトタグ、およびポリシータグの事前プロビジョニング（308 ページ）を参照してください。

ステップ 6 [Save] をクリックして、ネットワークプロファイルを追加します。

Cisco DNA Center は、**[Design]** > **[Network Profiles]** ウィンドウに新しいネットワーク プロファイルを表示します。

ネットワークプロファイルへの SSID の追加

始める前に

[Design] > **[Network Settings]** > **[Wireless]** タブでワイヤレス SSID を作成していることを確認します。

ステップ 1 [Add a Network Profile] ウィンドウで、[SSID] タブをクリックします。

ステップ 2 [Add SSID] をクリックします。

ステップ 3 [SSID] ドロップダウンリストで、作成済みの SSID を選択します。

ステップ 4 [Yes] または [No] オプションボタンを使用して、SSID がファブリックであるか、非ファブリックであるかを指定します。

非ファブリック SSID を作成する場合は、[No] をクリックして、次のパラメータを設定します。

- トラフィックスイッチングにインターフェイスを使用するには、[Interface] オプションボタンをクリックします。[Interface Name] ドロップダウンリストから、SSID のインターフェイス名を選択するか、[+] をクリックしてワイヤレスインターフェイスを作成します。

- トラフィックスイッチングに VLAN グループを使用するには、[VLAN Group] オプションボタンをクリックします。[VLAN Group Name] ドロップダウンリストから、SSID の VLAN グループ名を選択するか、[+] をクリックして VLAN グループを作成します。
- SSID にアンカーを追加するには、[Do you need Anchor for this SSID?] エリアで、[Yes] をクリックします。デフォルトでは、[No] が選択されています。
- [No] をクリックした場合、[Flex Connect Local Switching] チェックボックスをオンにして、WLAN のローカルスイッチングを有効にします。

  SSID にアンカーを追加することを選択した場合、[Flex Connect Local Switching] を有効にすることはできません。

  SSID に関して [Flex Connect Local Switching] を有効にしている場合、ネットワークプロファイルがマッピングされているフロア上のすべての AP が FlexConnect モードに切り替わります。

  [Flex Group] オプションは、[Advanced Settings] タブで有効になります。詳細については、ネットワークプロファイルの AP グループ、Flex グループ、サイトタグ、およびポリシータグの事前プロビジョニング （308 ページ）を参照してください。

  ローカルスイッチングを有効化すると、この WLAN をアドバタイズするすべての FlexConnect AP がデータパケットをローカルにスイッチングできるようになります。
- [Flex Connect Local Switching] チェックボックスをオンにしている場合は、[Local to VLAN] フィールドに VLAN ID の値を入力します。

ステップ 5 （任意） 別の SSID を追加するには、[+] をクリックしてそのパラメータを設定します。

ネットワークプロファイルへの AP ゾーンの追加

AP ゾーンを使用すると、同じサイト上の一連の AP に異なる SSID と RF プロファイルを関連付けることができます。デバイスタグを使用して、AP ゾーンを適用する AP を識別できます。[AP Zones] タブから、デバイスタグのネットワークプロファイルで設定された SSID のサブセットを使用して個別の AP ゾーンを作成できます。

Cisco DNA Center は、AP プロビジョニング中に AP ゾーン設定を AP に適用します。

（注）
- Cisco DNA Center は、プラグアンドプレイ（PnP）プロセスから要求された AP に AP ゾーン設定を適用しません。
- AP ですでにプロビジョニング済みの AP ゾーンの設定を更新する場合は、ワイヤレスコントローラ を再プロビジョニングする必要があります。AP を再プロビジョニングする必要はありません。

AP プロビジョニング時：

- AP のデバイスタグとサイトに基づいて、Cisco DNA Center は対応する AP ゾーンを選択し、RF プロファイルを自動的に割り当てます。
- AP に 2 つの AP ゾーンが設定されている場合、必要な AP ゾーンを選択できます。
- AP の AP ゾーンがない場合は、必要な RF プロファイルを選択できます。

始める前に

[Design] > **[Network Settings]** > **[Wireless]** タブでワイヤレス SSID を作成していることを確認します。

ステップ 1 [Add a Network Profile] ウィンドウで、[AP Zones] タブをクリックします。

ステップ 2 [Add AP Zone] をクリックします。

ステップ 3 AP ゾーンの名前を入力します。

ステップ 4 [Device Tags] ドロップダウンリストから、選択するデバイスタグの横にあるチェックボックスをオンにします。

ステップ 5 [RF Profile] ドロップダウンリストから、RF プロファイルを選択します。

ステップ 6 [SSID] ドロップダウンリストから、SSID を選択します。

ステップ 7 （任意） 別の AP ゾーンを追加するには、[+] をクリックしてそのパラメータを設定します。

次のタスク

AP ゾーン設定を AP に適用するには、次の手順を実行します。

1. ワイヤレスコントローラ を再プロビジョニングします。詳細については、Cisco AireOS コントローラのプロビジョニング （422 ページ）およびCisco Catalyst 9800 シリーズ ワイヤレスコントローラのプロビジョニング （462 ページ）を参照してください。
2. AP をプロビジョニングします。詳細については、シスコ製 AP のプロビジョニング：Day 1 AP プロビジョニング （430 ページ）を参照してください。

ネットワークプロファイルへのモデル設定の追加

モデル構成設計をネットワーク プロファイルに添付できます。

ステップ 1 [Add a Network Profile] ウィンドウで、[Model Configs] タブをクリックします。

ステップ 2 [Add Model Config] をクリックします。

ステップ 3 [Add Model Config] スライドインペインで、次の操作を実行します。

1. [Device Type(s)] ドロップダウンリストから、デバイスタイプを選択します。

[Search] フィールドに名前を入力してデバイス名を検索するか、[Switches and Hubs] または [Wireless Controller] を展開してデバイスタイプを選択できます。

2. [Wireless] を展開し、このワイヤレスプロファイルに関連付けるモデル設定の設計を選択します。
3. [APPLICABILITY] の [Tags] ドロップダウンリストから、該当するタグを選択します。
4. [Add] をクリックします。

ネットワークプロファイルへのテンプレートの追加

テンプレートをネットワークプロファイルに関連付けることができます。

ステップ 1 [Add a Network Profile] ウィンドウで、[Templates] タブをクリックします。

ステップ 2 [+ Add template] をクリックします。

ステップ 3 [Add Template] スライドインペインで、次の操作を実行します。

1. [Device Type（s）] ドロップダウンリストから、デバイスタイプを選択します。

   [Search] フィールドに名前を入力してデバイス名を検索するか、または [Wireless Controller] を展開してデバイスタイプを選択できます。

2. [Template] エリアで、テンプレートを選択します。
3. [Tags] ドロップダウンリストから、選択するデバイスタグのチェックボックスをオンにします。

   テンプレートではタグを使用できます。これを使用するのは、デバイスタグに基づいて同じデバイスタイプに対して異なるテンプレートをプッシュする必要がある場合だけです。

4. [Add] をクリックします。

ネットワークプロファイルの AP グループ、Flex グループ、サイトタグ、およびポリシータグの事前プロビジョニング

Cisco DNA Center では、ネットワークプロファイルの AP グループ、Flex グループ、サイトタグ、およびポリシータグを事前プロビジョニングできます。事前プロビジョニングすると、反復的な構成変更の必要がなくなることで AP プロビジョニング時の時間を節約でき、デバイス間の一貫性を確保できます。[Advanced Settings] タブから、AP グループ、サイトタグ、およびポリシータグのカスタム名を定義できます。

（注） Flex グループ設定は、ネットワークプロファイルに少なくとも 1 つのフレックスベースの SSID が関連付けられている場合にのみ使用できます。

Cisco DNA Center は シスコ ワイヤレス コントローラ のプロビジョニング時に、このタブで指定されたカスタム名を設定し AP に適用します。カスタム名を設定しない場合、Cisco DNA Center は自動生成された AP グループ名と AP のタグを使用します。

（注）

- AP グループと Flex グループの設定を Cisco AireOS ワイヤレスコントローラ に適用できます。
- サイトタグとポリシータグの設定を Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ に適用できます。

  サイトとポリシータグの設定は、AP のプロビジョニングにのみ適用されます。ワイヤレスコントローラ だけをプロビジョニングしても、AP のタグは設定されません。プロビジョニング後にタグを変更する場合は、ワイヤレスコントローラ または AP を再プロビジョニングする必要があります。

  ワイヤレスコントローラおよび AP をプロビジョニングまたは再プロビジョニングするときは、次のシナリオに注意してください。

  - ネットワークプロファイルにカスタムサイトやポリシータグが設定されていない場合、Cisco DNA Center では自動生成されたタグが ワイヤレスコントローラ に設定され、AP プロビジョニング時にのみ AP に適用されます。
  - ネットワークプロファイルにカスタムサイトやポリシータグが設定されている場合、Cisco DNA Center ではカスタムタグが ワイヤレスコントローラ に設定され、AP プロビジョニング時にのみ AP に適用されます。
  - ワイヤレスコントローラ および AP が自動生成タグを使用してすでにプロビジョニングされていて、ネットワークプロファイルで新しいカスタムタグを作成する場合は、ワイヤレスコントローラ または AP を再プロビジョニングして変更を適用する必要があります。
  - ワイヤレスコントローラ および AP がすでにカスタムタグを使用してプロビジョニングされていて、ネットワークプロファイルからカスタムタグを削除する場合は、ワイヤレスコントローラ または AP を再プロビジョニングする必要があります。

    ワイヤレスコントローラ を再プロビジョニングすると、カスタムタグ設定が削除され、ワイヤレスコントローラ および関連する AP に自動生成されたタグが設定されます。

    ワイヤレスコントローラ を再プロビジョニングせずに、AP を直接再プロビジョニングすると、自動生成されたタグが AP に設定されますが、カスタムタグ設定は ワイヤレスコントローラ から削除されません。タグは、次回の ワイヤレスコントローラ の再プロビジョニング時に削除されます。
  - FlexConnect ネイティブ VLAN のオーバーライドが設定されていて、サイトタグがサイト内のすべてのフロアに対して同じカスタム Flex プロファイルにマッピングされている状態で Cisco DNA Center にアップグレードした場合は、フロアごとに異なるサイトタグを使用してネットワークプロファイルを再設定する必要があります。再設定しないと、プロビジョニングが失敗する可能性があります。

始める前に

- ネットワークプロファイルにサイト（フロア）が割り当てられていることを確認します。
- Flex グループ名を作成するには、[SSIDs] タブで、[Flex Connect Local Switching] チェックボックスをオンにし、[Local to VLAN] テキストボックスで VLAN ID を定義して、非ファブリック SSID を Flex ベースの SSID としてマークしていることを確認します。詳細については、ネットワークプロファイルへの SSID の追加 （305 ページ）を参照してください。

  SSID に関して [Flex Connect Local Switching] を有効にしている場合、ネットワークプロファイルがマッピングされているフロア上のすべての AP が FlexConnect モードに切り替わります。

ステップ 1 [Add a Network Profile] ウィンドウで、[Advanced Settings] タブをクリックします。

ステップ 2 ネットワークプロファイルで AP グループを作成するには、[AP Group] を展開し、[Create AP Group] をクリックします。

[Create an AP Group] ウィンドウで、次の手順を実行します。

a) [AP Group Name] フィールドに、AP グループ名を入力します。

b) [AP Zone] ドロップダウンリストから、AP ゾーンを選択します。

ネットワークプロファイルに関連付けられたすべての SSID をブロードキャストするには、[Not Applicable] を選択します。

（注） このドロップダウンリストは、[AP Zones] タブでネットワークプロファイルに AP ゾーンを追加した場合に有効になります。詳細については、ネットワークプロファイルへの AP ゾーンの追加 （306 ページ）を参照してください。

AP ゾーンを選択した場合、RF プロファイルが AP ゾーン設定から継承されます。

c) [RF Profile] ドロップダウンリストから、RF プロファイルを選択します。

（注） [AP Zone] ドロップダウンリストから AP ゾーンを選択した場合、このドロップダウンリストは無効になります。

d) [Select Sites] エリアで、名前を入力してサイトを検索するか、[Global] を展開してサイトを選択します。

e) [Save] をクリックします。

ステップ 3 ネットワークプロファイルで Flex グループを作成するには、[Flex Group] を展開し、[Create Flex Group] をクリックします。

[Create Flex Group] ウィンドウで、次の手順を実行します。

a) [Flex Group Name] フィールドに、Flex グループ名を入力します。

b) [Select Sites] エリアで、名前を入力してサイトを検索するか、[Global] を展開してサイトを選択します。

c) [Save] をクリックします。

ステップ 4 ネットワークプロファイルでサイトタグを作成するには、[Site Tag] を展開し、[Create Site Tag] をクリックします。

[Create a Site Tag] ウィンドウで、次の手順を実行します。

a) [Site Tag Name] フィールドに、サイトタグ名を入力します。
b) [Flex Profile Name] 名前フィールドに、Flex プロファイル名を入力します。

（注） [Flex Profile Name] 名前フィールドを有効にするには、[Edit Network Profile] ウィンドウの [Flex Connect Local Switching] チェックボックスをオンにします。

c) [Select Sites] エリアで、名前を入力してサイトを検索するか、[Global] を展開してサイトを選択します。
d) [Save] をクリックします。

ステップ 5 ネットワークプロファイルでポリシータグを作成するには、[Policy Tag] を展開し、[Create Policy Tag] をクリックします。

[Create Policy Tag] ウィンドウで、次の手順を実行します。

a) [Policy Tag Name] フィールドに、ポリシータグ名を入力します。
b) [AP Zone] ドロップダウンリストから、AP ゾーンを選択します。
c) [Select Sites] エリアで、名前を入力してサイトを検索するか、[Global] を展開してサイトを選択します。
d) [Save] をクリックします。

第 IV 部

ネットワークデバイスの設定と保守

第 11 章

デバイス設定の変更を自動化するテンプレートの作成

テンプレート エディタについて

Cisco DNA Center Cisco DNA Center には、CLI テンプレートを作成するためのテンプレートエディタと呼ばれるインタラクティブなエディタがあります。パラメータ化された要素または変数を使用して、事前に定義された設定で簡単にテンプレートを設計できます。テンプレートを作成したら、そのテンプレートを再度使用して、ネットワーク内の任意の場所に設定されている 1 つ以上のサイトにデバイスを展開できます。

テンプレートエディタを使用すると、次のことができます。

- テンプレートの作成、編集、および削除
- インタラクティブ コマンドの追加
- テンプレート内のエラーの検証
- 追跡のためのテンプレートのバージョン管理
- テンプレートのシミュレーション

（注） Cisco DNA Center によってプッシュされるネットワークインテント設定がテンプレートによって上書きされないように注意してください。

プロジェクトの作成

ステップ 1 [Tools] > [Template Editor]メニューアイコン（≡）をクリックして、> を選択します。

ステップ 2 左側のペインで、⊕ > **[プロジェクトの作成（Create Project)）]** の順にクリックします。

[Add New Project] スライドインペインが表示されます。

ステップ 3 [Name] フィールドに、プロジェクトの名前を入力します。

ステップ 4 （任意） [Description] フィールドに、プロジェクトの説明を入力します。

ステップ 5 [Add] をクリックします。

プロジェクトが作成され、左側のペインに表示されます。

テンプレートの作成

テンプレートは、パラメータ要素と変数を使用して設定を簡単に事前定義する方法を提供します。テンプレートにより、管理者は複数のネットワークデバイスを一貫して設定するのに使用する CLI コマンドの設定を定義できるようになり、展開時間を短縮できます。テンプレートの変数を使用すると、デバイスごとに特定の設定をカスタマイズできます。

標準テンプレートの作成

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

（注） デフォルトでは、[Onboarding Configuration] プロジェクトは、day-0 テンプレートの作成に使用できます。独自のカスタムプロジェクトを作成できます。カスタムプロジェクトで作成されたテンプレートは、day-N テンプレートとして分類されます。

ステップ 2 左側のペインで、テンプレートを作成するプロジェクトを選択します。

ステップ 3 左側のペインで、歯車アイコン ⚙ をクリックし、[Add Template] を選択します。

（注） day-0 用に作成したテンプレートは、day-N にも適用できます。

ステップ 4 標準テンプレートの設定を指定します。

a) [Template Type] については、オプションが [Regular Template] に設定されたままにします。

b) [Template Language] については、テンプレートのコンテンツに使用する言語（[Velocity] または [Jinja]）を選択します。

c) [Name] フィールドにテンプレートの一意の名前を入力します。

d) （任意） [Description] フィールドにテンプレートの説明を入力します。

e) [Tags] フィールドで、ドロップダウンリストをクリックし、テンプレートのタグを選択します。

（注） タグはキーワードのようなもので、テンプレートを見つけるのに役立ちます。

タグを使用してテンプレートをフィルタ処理する場合は、テンプレートを適用するデバイスに同じタグを適用する必要があります。適用しないと、プロビジョニング中に「Cannot select the device. Not compatible with template.」というエラーメッセージが表示されます。

f) [Device Type (s)] については、[Edit] をクリックし、このテンプレートを適用するデバイスタイプを選択します。

[Select Device Type(s)] スライドインペインが表示されます。デフォルトでは、すべてのデバイスタイプが表示されます。

（注）
- [Select Device Type(s)] スライドペインでは、[Full Device List] ビューと [Favorite Devices] ビューを切り替えることができます。
- [Full Device List] ビューでは、デバイスタイプ階層の各デバイスモデルがアルファベット順に並べ替えられます。

- [Find] 機能でデバイス名を入力してデバイスをすばやく検索するか、またはデバイスタイプを展開してからテンプレートに適用するデバイスタイプの横にあるチェックボックスをオンにします。

  選択済みのデバイスを表示するには、[Show] ドロップダウンリストから [Selected] を選択します。

階層構造から選択するデバイスタイプには、さまざまな細かいレベルがあります。プロビジョニング時にデバイスタイプを使用して、指定したデバイスタイプの条件に一致するデバイスにテンプレートが確実に展開されるようにします。これにより、特定のデバイスモデルに対して専用のテンプレートを作成できます。

テンプレートエディタには、デバイスの製品ID（PID）は表示されません。代わりに、デバイスのシリーズとモデルの説明が表示されます。Cisco.com を使用すると、PIDに基づいたデバイスデータシートの検索、デバイスシリーズとモデルの説明の検索、適切なデバイスタイプの選択を実行できます。

g) 階層で、デバイスタイプを展開し、お気に入りとしてマークするデバイスモデルの横に表示される星のマークをクリックします。

（注） [Favorite Devices] ビューに切り替えて、お気に入りのマークが付いたデバイスモデルのリストを表示することができます。

h) デバイスタイプを選択したら、[Back to Add New Template] をクリックします。

i) [Software Type] については、ドロップダウンリストをクリックし、ソフトウェアのタイプを選択します。

（注） シスコ ワイヤレス コントローラのサポート対象ソフトウェアバージョンおよびサポートされている最小バージョンの詳細については、『Cisco DNA Center Compatibility Matrix』を参照してください。

たとえば、ソフトウェアタイプに IOS を選択すると、IOS XE や IOS XR など、すべてのソフトウェアタイプにコマンドを適用できます。この値は、プロビジョニング時に、選択したデバイスがテンプレートの選択に準拠しているかどうかを確認するために使用されます。

j) [Software Version] フィールドにソフトウェアのバージョンを入力します。

（注） プロビジョニングの間、Cisco DNA Center は、選択したデバイスにテンプレートに記載されているのと同じソフトウェアバージョンがあるか確認します。不一致がある場合、テンプレートはプロビジョニングされません。

ステップ 5 [Add]をクリックします。

テンプレートが作成され、左側のペインの選択したプロジェクトの下に表示されます。

ステップ 6 左側のペインで作成したテンプレートを選択して、テンプレートの内容を編集することができます。テンプレートの内容の編集の詳細については、テンプレートの編集 （321 ページ）を参照してください。

ブロックリストコマンド

ブロックリストコマンドは、テンプレートに追加できないコマンド、またはテンプレートを介してプロビジョニングできないコマンドです。テンプレートでブラックリストコマンドを使用すると、テンプレートに警告が表示されます。この場合、一部の Cisco DNA Center プロビジョニング アプリケーションと競合している可能性があります。

このリリースでは、次のコマンドがブロックされています。

- **router lisp**
- **hostname**

サンプル テンプレート

テンプレートの変数を作成する際は、次のサンプルテンプレートを参照してください。

ホスト名を設定します

```
hostname$name
```

インターフェイスの設定

```
interface $interfaceName
description $description
```

シスコ ワイヤレス コントローラでの NTP の設定

```
config time ntp interval $interval
```

複合テンプレートの作成

2つ以上の標準テンプレートは、連続した複合テンプレートにまとめられます。一連のテンプレートに対し、デバイスに集合的に適用される連続的な複合テンプレートを作成できます。たとえば、ブランチを展開するときに、ブランチルータの最小設定を指定する必要があります。作成したすべてのテンプレートは、単一の複合テンプレートに追加できます。これは、ブランチルータに必要なすべての個々のテンプレートを集約したものです。複合テンプレートに含まれるテンプレートが、デバイスに展開される順序を指定してください。

（注） 複合テンプレートには、コミットされたテンプレートのみを追加できます。

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

ステップ 2 左側のペインで、テンプレートを作成するプロジェクトを選択します。

ステップ 3 左側のペインで、歯車アイコン ⚙ > **[Add Template]** の順にクリックします。

[Add New Template] スライドインペインが表示されます。

ステップ 4 複合テンプレートの設定を指定します。

a) [Template Type] で、複合テンプレートの [Composite Sequence] を選択します。

b) [Template Language] については、テンプレートのコンテンツに使用する言語（[Velocity] または [Jinja]）を選択します。

c) [Name] フィールドにテンプレートの一意の名前を入力します。

d) （任意） [Description] フィールドにテンプレートの説明を入力します。

e) [Tags] フィールドで、ドロップダウンリストをクリックし、テンプレートのタグを選択します。

（注） タグはキーワードのようなもので、テンプレートを見つけるのに役立ちます。

タグを使用してテンプレートをフィルタ処理する場合は、テンプレートを適用するデバイスに同じタグを適用する必要があります。適用しないと、プロビジョニング中に「Cannot select the device. Not compatible with template.」というエラーメッセージが表示されます。

f) [Device Type(s)] については、[Edit] をクリックし、このテンプレートを適用するデバイスタイプを選択します。

[Select Device Type(s)] スライドインペインが表示されます。デフォルトでは、すべてのデバイスタイプが表示されます。

（注）
- [Select Device Type(s)] スライドペインでは、[Full Device List] ビューと [Favorite Devices] ビューを切り替えることができます。
- [Full Device List] ビューでは、デバイスタイプ階層の各デバイスモデルがアルファベット順に並べ替えられます。

- [Find] 機能でデバイス名を入力してデバイスをすばやく検索するか、またはデバイスタイプを展開してからテンプレートに適用するデバイスタイプの横にあるチェックボックスをオンにします。

  選択済みのデバイスを表示するには、[Show] ドロップダウンリストから [Selected] を選択します。

g) 階層で、デバイスタイプを展開し、お気に入りとしてマークするデバイスモデルの横に表示される星のマークをクリックします。

（注） [Favorite Devices] ビューに切り替えて、お気に入りのマークが付いたデバイスモデルのリストを表示することができます。

h) デバイスタイプを選択したら、[Back to Add New Template] をクリックします。

i) [Software Type] については、ドロップダウンリストをクリックし、ソフトウェアのタイプを選択します。

（注） ソフトウェアタイプに固有のコマンドがある場合は、特定のソフトウェアタイプ（IOS XE や IOS XR など）を選択できます。ソフトウェアタイプに IOS を選択すると、IOS XE や IOS XR など、すべてのソフトウェアタイプにコマンドを適用できます。この値は、プロビジョニング時に、選択したデバイスがテンプレートの選択に準拠しているかどうかを確認するために使用されます。

j) [Software Version] フィールドにソフトウェアのバージョンを入力します。

（注） プロビジョニングの間、Cisco DNA Center は、選択したデバイスにテンプレートに記載されているのと同様のソフトウェアバージョンがあるか確認します。不一致がある場合、プロビジョニングはテンプレートをスキップします。

ステップ 5 [Add]をクリックします。

複合テンプレートが作成され、左側のペインの選択したプロジェクトの下に表示されます。

ステップ 6 左側のビューペインで作成した複合テンプレートをクリックします。

ステップ 7 [Template Editor] ウィンドウで、左側のペインからテンプレートを順番にドラッグアンドドロップします。

テンプレートは順序付けされた順序に基づいて導入されます。[テンプレートエディタ（Template Editor）] ウィンドウでテンプレートの順序を変更できます。

（注） デフォルトでは、[View] フィルタで [Applicable] オプションが選択されています。複合テンプレートに追加できる適用可能なテンプレートのみが [Template Editor] ウィンドウに表示されます。[View] フィルタで [All] オプションを選択すると、[Template Editor] ウィンドウにすべてのテンプレートを表示できます。[All] オプションビューでは、選択したデバイスタイプとソフトウェアバージョンに一致するテンプレートがプラスアイコンでマークされます。

複合テンプレートと同じデバイスタイプ、ソフトウェアタイプ、およびソフトウェアバージョンを持つテンプレートをドラッグアンドドロップできます。

ステップ 8 最初のテンプレートで障害が発生した場合に展開プロセスをキャンセルするには、[Template Editor] ウィンドウで最初のテンプレートを選択し、[Abort sequence on targets if deployment fails] チェックボックスをオンにします。

ステップ 9 **[Actions]** ドロップダウンリストで、**[Commit]** を選択してテンプレートのコンテンツをコミットします。

テンプレートの編集

テンプレートを作成したら、テンプレートを編集して内容を記述できます。

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

ステップ 2 左側のペインで、編集するテンプレートを選択します。

[Template Editor] ウィンドウが表示されます。

ステップ 3 [テンプレート エディタ（Template Editor）] ウィンドウで、テンプレートのコンテンツを入力します。単一行設定または複数選択設定を含むテンプレートを使用できます。

ステップ 4 [Template Language] から、内容の記述に使用する言語を選択します。

- [Velocity]：Velocity Template Language（VTL）を使用します。詳細については、http://velocity.apache.org/engine/devel/vtl-reference.htmlを参照してください。

  Velocity テンプレートフレームワークでは、数字で始まる変数の使用が制限されます。変数名の先頭は数字ではなく文字にしてください。

  （注） Velocityテンプレートの使用中は、ドル記号（$）を使用しないでください。ドル記号（$）を使用すると、その後ろの値は変数として扱われます。たとえば、パスワードを「$a123$q1ups1$va112」として設定すると、テンプレートエディタはこれを変数「a123」、「q1ups」、および「va112」として扱います。この問題を回避するために、Velocityテンプレートによるテキスト処理に合わせて Linux シェルスタイルを使用してください。

  （注） Velocity テンプレートでは、変数を宣言する場合にのみドル（$）記号を使用してください。

- [Jinja]：Jinja 言語を使用します。詳細については、https://www.palletsprojects.com/p/jinja/を参照してください。

ステップ 5 [Actions] ドロップダウンリストから [Check for errors] を選択してテンプレートを検証します。

Cisco DNA Center 次のエラーをチェックし、報告します。

- 言語構文エラー。
- ブラックリストコマンドとの競合。詳細については、ブロックリストコマンド （318 ページ）を参照してください。

ステップ 6 [Actions] ドロップダウンリストから、[Save] を選択します。

テンプレートを保存後、Cisco DNA Center がテンプレート内のすべてのエラーをチェックします。構文エラーがある場合、テンプレートの内容は保存されず、テンプレートで定義されているすべての入力変数が保存プロセス中に自動的に識別されます。ローカルの値（ループ用に使用され、セットを通じて割り当てられる変数など）は無視されます。

ステップ 7 [Actions] ドロップダウンリストから、[Commit] を選択します。

（注） ネットワーク プロファイルにコミットされたテンプレートのみを関連付けることができます。

テンプレートのシミュレーション

インタラクティブ テンプレート シミュレーションを使用すると、変数にテストデータを指定することで、変数をデバイスに送信する前に、テンプレートのCLI生成をシミュレーションすることができます。テストシミュレーションの結果を保存し、必要に応じてそれらを後で使用することができます。

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

ステップ 2 左側のペインで、プロジェクトを展開し、シミュレーションを実行するテンプレートをクリックします。

テンプレートが表示されます。

ステップ 3 右上隅にある [Simulator Editor] トグル  をクリックします。

ステップ 4 [Actions] ドロップダウンリストをクリックし、[Create Simulation] を選択します。

[Simulation Input] フォームが表示されます。

ステップ 5 [Simulation Name] フィールドにシミュレーションの名前を入力します。

（注） テンプレートに暗黙的な変数がある場合、[edit] リンクをクリックし、[Simulation Input] フォームでデバイスまたはサイトを選択して、バインディングに基づいて実際のデバイスに対してシミュレーションを実行できます。

ステップ 6 [シミュレーション入力（Simulation Input）] フォームの必須フィールドを入力し、[実行（Run）] をクリックします。

結果は、 [テンプレート プレビュー（Template Preview）] ウィンドウに表示されます。

テンプレートのエクスポート

テンプレートまたは複数のテンプレートを JSON フォーマットで 1 つのファイルにエクスポートできます。

ステップ 1 [Tools] > [Template Editor]メニューアイコン（☰）をクリックして、 > を選択します。

ステップ 2 左側のペインで、エクスポートするテンプレートを選択します。[Export] を選択します。⚙ >

- 1 つのプロジェクトの下に複数のテンプレートをエクスポートするには、左側のペインでプロジェクトを選択し、⚙ > **の [Export Template (s)] を選択します。**

  [Export Template(s)] ウィンドウからテンプレートを選択し、[Export] をクリックします。

- 異なるプロジェクトの下に複数のテンプレートをエクスポートするには、左側のペインで⊕の [Export Project(s)] をクリックします。

  [Export Project(s)] ウィンドウからエクスポートするテンプレートを選択し、[Export] をクリックします。

ステップ 3 プロンプトが表示されたら、[Save] をクリックします。

テンプレートの最新バージョンがエクスポートされます。

テンプレートの以前のバージョンをエクスポートするには、[Actions] > [Show History] > [View] からテンプレートを開きます。

[Actions] > [Export] の順にクリックします。

テンプレートのインポート

プロジェクトの下に 1 つまたは複数のテンプレートをインポートできます。

ステップ 1 [Tools] > [Template Editor]メニューアイコン（☰）をクリックして、 > を選択します。

ステップ 2 左側のペインで、テンプレートをインポートするプロジェクトを選択します。⚙ の [Import Template(s)] を選択します。 >

ステップ 3 [Import Template(s)] ウィンドウで [Select a File from your computer] をクリックし、JSON テンプレートファイルの場所を参照します。

ステップ 4 JSON ファイルを選択し、[Open] をクリックします。

テンプレートは、選択したプロジェクトの下にインポートされます。同じ名前のテンプレートが存在する場合、Cisco DNA Center はエラーメッセージを表示し、テンプレートをインポートしません。

（注） 既存のものと同じ名前のテンプレートをインポートするには、[Import Template(s)] ウィンドウの [Create new version of imported template/project when template/project with the same name already exists in the hierarchy] チェックボックスをオンにします。

このオプションを選択すると、既存のテンプレートの新しいバージョンが作成されます。

テンプレートの複製

テンプレートのコピーを作成して、その一部を再利用することができます。

ステップ 1 [Tools] > [Template Editor]メニューアイコン（≡）をクリックして、> を選択します。

ステップ 2 左側のペインで、エクスポートするテンプレートを選択します。[複製（Clone）]⚙ > を選択します。

ステップ 3 [Clone template] ウィンドウの [Name] フィールドに、複製されたテンプレートの名前を入力します。

ステップ 4 [Project Name] ドロップダウンリストからプロジェクトを選択します。

ステップ 5 [Clone] をクリックします。

ステップ 6 複製されたテンプレートを確定するには、ウィンドウの左ペインからテンプレートを選択し、[Actions] > [Commit] をクリックします。

テンプレートの最新バージョンが複製されます。

テンプレートの以前のバージョンを複製するには、[Actions] > [Show History] > [View] からテンプレートを開きます。

[Actions] > [Clone] をクリックします。

プロジェクトのエクスポート

プロジェクトまたは複数のプロジェクト (テンプレートを含む) を JSON フォーマットの 1 つのファイルにエクスポートできます。

ステップ 1 [Tools] > [Template Editor]メニューアイコン（≡）をクリックして、> を選択します。

ステップ 2 左側のペインで、エクスポートするプロジェクトを選択します。の [Export Project] を選択します。⚙ >

プロジェクトを一括してエクスポートするには、左側のペインで⊕ > **の [Export Project (s)] をクリックします。**

エクスポートするプロジェクトを選択し、[Export] をクリックします。

ステップ 3 プロンプトが表示されたら、[Save] をクリックします。

プロジェクトのインポート

テンプレートを使用して、1 つまたは複数のプロジェクトを Cisco DNA Center テンプレートエディタにインポートできます。

ステップ 1 [Tools] > [Template Editor]メニューアイコン（≡）をクリックして、 > を選択します。

ステップ 2 左側のペインで、[Import Project(s)] > をクリックします。

ステップ 3 [Import Project(s)] ウィンドウで [Select a File from your computer] をクリックし、JSON プロジェクトファイルの場所を参照します。

ステップ 4 JSON ファイルを選択し、[Open] をクリックします。

プロジェクトとそのテンプレートがインポートされます。同じ名前のプロジェクトが存在する場合、Cisco DNA Center はエラーメッセージを表示し、プロジェクトをインポートしません。

（注） 既存のものと同じ名前のプロジェクトをインポートするには、[Import project(s)] ウィンドウの [Create new version of imported template/project when template/project with the same name already exists in the hierarchy] チェックボックスをオンにします。

このオプションを選択すると、既存のプロジェクトの新しいバージョンが作成されます。

テンプレート フォーム エディタ

テンプレート フォーム エディタは、追加のメタデータ情報をテンプレート内のテンプレート変数に追加するために使用します。またフォームエディタを使用して、最大長や範囲などの変数の検証を提供することもできます。

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

ステップ 2 左側のペインで、プロジェクトを展開し、テンプレートをクリックします。

テンプレートが表示されます。

ステップ 3 [Form Editor] トグル  をクリックします。

フォームエディタでは、テンプレート変数にメタデータを追加できます。テンプレートで識別されたすべての変数が表示されます。以下のメタデータを設定できます。

- 文字列を変数として考慮しない場合は、変数を選択し、[Not a Variable] チェックボックスをオンにします。

- [Field Name]テキストボックスに、フィールド名を入力します。これは、プロビジョニング中に各変数の UI ウィジェットに使用されるラベルです。
- [ツールチップ（Tooltip）] テキスト ボックスに、各変数に表示されるツールチップのテキストを入力します。
- [デフォルト値（Default Value）] テキスト ボックスに、デフォルト値を入力します。この値は、プロビジョニング中にデフォルト値として表示されます。
- [説明文（Instructional Text）] テキスト ボックスに、任意の説明文を入力します。説明文は UI ウィジェット内に表示されます（たとえば、**「ここにホスト名を入力してください」**など）。ユーザーがテキストを入力するためにウィジェットをクリックすると、ウィジェット内のテキストは消去されます。
- [データタイプ（Data Type）] ドロップダウンリストから、データタイプ：[文字列（String）] 、[整数（Integer）] 、[IP アドレス（IP Address）] 、または [MAC アドレス（Mac Address）] を選択します。
- これがプロビジョニング中に必要な変数の場合、[必須（Required）] チェック ボックスにチェックを付けます。デフォルトでは、すべての変数に [必須（Required）] マークが付いています。これはつまり、プロビジョニング時にこの変数の値を入力する必要があることを意味します。パラメータに [Required] マークがなく、このパラメータに何も値を渡さない場合は、実行時に空の文字列に置換されます。変数の不足は、コマンドの失敗につながります。また、構文上正しくない可能性があります。[Required] マークが付いていない変数に基づいてコマンド全体をオプションにしたい場合は、テンプレートで **if-else** ブロックを使用します。
- [表示タイプ（Display Type）] ドロップダウンリストから、プロビジョニング時に作成する UI ウィジェットのタイプ：[テキスト フィールド（Text Field）] 、[単一選択（Single Select）] 、または [複数選択 （Multi Select）] を選択します。
- [最大文字数 （Maximum Characters）] テキスト ボックスに、入力できる最大文字数を入力します。これは文字列データタイプの場合にのみ適用可能です。

ステップ 4 メタデータ情報を設定したら、[Actions] ドロップダウンリストから [Save] を選択します。

ステップ 5 テンプレートを保存したら、バージョンを付ける必要があります。テンプレートは、変更を加えるたびにバージョンを付ける必要があります。[Actions] ドロップダウンリストから、[Commit] を選択します。[コミット（Commit）] ウィンドウが表示されます。[コミット メモ（Commit Note）] テキスト ボックスに、コミットのメモを入力することができます。バージョン番号はシステムによって自動的に生成されます。

ステップ 6 履歴を表示するには、[アクション（Actions）] ドロップダウンリストから、[履歴の表示（Show History）] を選択します。以前作成してバージョンを付けたテンプレートが表示されます。

ポップアップウィンドウが表示されます。

- 古いバージョンのコンテンツを表示するには、ポップアップ ウィンドウの [表示（View）] をクリックします。
- テンプレートを編集するには、ポップアップ ウィンドウの [編集（Edit）] をクリックします。

変数バインド

テンプレートを作成する場合、コンテキストに合わせて置き換わる変数を指定できます。これらの変数の多くは、[Template Editor] ドロップダウンリストで使用できます。

テンプレートエディタには、編集中または入力フォーム機能拡張（DHCP サーバー、DNS サーバー、syslog サーバーなど）から、ソースオブジェクト値を使用してテンプレートで変数をバインドまたは使用するオプションがあります。

一部の変数については、対応するソースに常にバインドされ、動作を変更することはできません。暗黙の変数のリストを表示するには、[Code Editor] ウィンドウまたは [Form Editor] ウィンドウで [Template System Variables] リンクをクリックします。

事前定義済みのオブジェクト値は、次のいずれかにすることができます。

- ネットワークプロファイル
  - SSID
  - ポリシープロファイル
  - AP グループ
  - Flex グループ
  - Flex プロファイル
  - サイト タグ
  - ポリシー タグ
- 共通設定
  - DHCP サーバ
  - Syslog サーバー
  - SNMP トラップ レシーバ
  - NTP サーバ
  - タイムゾーンサイト
  - デバイスバナー
  - DNS サーバ
  - NetFlow コレクタ
  - AAA ネットワークサーバー
  - AAA エンドポイントサーバー
  - AAA サーバー PAN ネットワーク
  - AAA サーバー PAN エンドポイント

- WLAN 情報
- RF プロファイル情報

- クラウド接続
  - クラウド router-1 トンネル IP
  - クラウド router-2 トンネル IP
  - クラウド router-1 ループバック IP
  - クラウド router-2 ループバック IP
  - ブランチ router-1 トンネル IP
  - ブランチ router-2 トンネル IP
  - クラウド router-1 パブリック IP
  - クラウド router-2 パブリック IP
  - ブランチ router-1 IP
  - ブランチ router-2 IP
  - プライベート subnet-1 IP
  - プライベート subnet-2 IP
  - プライベート subnet-1 IP マスク
  - プライベート subnet-2 IP マスク

- インベントリ
  - デバイス
  - Interface
  - AP グループ
  - Flex グループ
  - WLAN
  - ポリシープロファイル
  - Flex プロファイル
  - Web 認証パラメータマップ
  - サイト タグ
  - ポリシー タグ
  - RF プロファイル

- [Common Settings]：**[Design]** > **[Network Settings]** > **[Network]** で利用可能な設定。共通設定の変数バインドによって、デバイスが属するサイトに基づいた値が解決されます。

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

ステップ 2 テンプレートを選択し、[Input Form] アイコンをクリックして、テンプレート内の変数をネットワーク設定にバインドします。

ステップ 3 変数をネットワーク設定にバインドするには、[Input Form] ペインで変数を選択し、[Required] チェックボックスをオンにします。

ステップ 4 [Display] ドロップダウンリストから、プロビジョニング時に作成する UI ウィジェットのタイプを選択します。[Text Field]、[Single Select]、または [Multi Select]。

ステップ 5 変数をネットワーク設定にバインドするには、[Input Form] で各変数を選択し、[Content] の下の [Bind to Source] チェックボックスをオンにします。

- それぞれのドロップダウンリストで、[Source]、[Entity]、および [Attributes] を選択します。
- ソースタイプが [CommonSettings] の場合は、次のエンティティのいずれかを選択します。[dhcp.server]、[syslog.server]、[snmp.trap.receiver]、[ntp.server]、[timezone.site]、[device.banner]、[dns.server]、[netflow.collector]。

  [dns.server] または [netflow.collector] 属性にフィルタ処理を適用して、デバイスのプロビジョニング時に、[bind] 変数の関連リストのみを表示することができます。属性にフィルタ処理を適用するには、[Filter by] ドロップダウンリストから属性を選択します。[Condition] ドロップダウンリストから、[Value] と一致させるための条件を選択します。
- ソースタイプが [NetworkProfile] の場合、エンティティタイプとして [SSID] を選択します。入力される SSID エンティティは、**[Design]** > **[Network Profile]** で定義されます。バインドにより、SSID 名、サイト、および SSID カテゴリの組み合わせであるわかりやすい SSID 名が生成されます。[Attributes] ドロップダウンリストから、[wlanid] を選択します。この属性は、テンプレートのプロビジョニング時の高度な CLI 設定中に使用されます。
- ソースタイプが [Inventory] の場合、次のいずれかのエンティティを選択します。[Device]、[Interface]、[AP Group]、[Flex Group]、[Wlan]、[Policy Profile]、[Flex Profile]。エンティティタイプ [Device] および [Interface] の場合、[Attribute] ドロップダウンリストにデバイスまたはインターフェイスの属性が表示されます。変数は、テンプレートを適用するデバイスで設定されている AP グループと Flex グループの名前を解決します。

  [Device]、[Interface]、または [Wlan] 属性にフィルタ処理を適用して、デバイスのプロビジョニング時に、[bind] 変数の関連リストのみを表示することができます。属性にフィルタ処理を適用するには、[Filter by] ドロップダウンリストから属性を選択します。[Condition] ドロップダウンリストから、[Value] と一致させるための条件を選択します。

変数を共通設定にバインドしたら、テンプレートをワイヤレスプロファイルに割り当て、テンプレートをプロビジョニングするときに、**[Network Settings]** > **[Network]** の下で定義したすべてのネットワーク設定がドロップダウンリストに表示されます。これらの属性は、ネットワークの設計時に **[Network Settings]** > **[Network]** の下で定義する必要があります。

ステップ 6 テンプレートに特定の属性にバインドする変数バインディングが含まれていて、テンプレートコードがそれらの属性に直接アクセスする場合は、次のいずれかを実行する必要があります。

- 属性へのバインディングではなくオブジェクトへのバインディングを変更します。
- テンプレートコードを更新して、属性に直接アクセスしないようにします。

たとえば、テンプレートコードが次のようになっていて、**$interfaces** が特定の属性にバインドされている場合、次の例に示すようにコードを更新するか、属性へのバインディングではなくオブジェクトへのバインディングを変更する必要があります。

古いコードの例：

```
#foreach ( $interface in $interfaces )
 $interface.portName
      description "something"
#end
```

新しいコードの例：

```
#foreach ( $interface in $interfaces )
 interface $interface
           description "something"
#end
```

特別なキーワード

テンプレートを通じて実行されるすべてのコマンドは、常に **config t** モードになります。そのため、テンプレートで明示的に **enable or config t** コマンドを指定する必要はありません。

Day-0 テンプレートは特別なキーワードをサポートしていません。

イネーブル モード コマンド

config t コマンドの他に任意のコマンドを実行する場合は、**#MODE_ENABLE** コマンドを指定します。

次の構文を使用して、CLI テンプレートに **enable mode** コマンドを追加します。

```
#MODE_ENABLE
<<commands>>
#MODE_END_ENABLE
```

インタラクティブコマンド

ユーザー入力が必要なコマンドを実行する場合は、**#INTERACTIVE** を指定します。

インタラクティブコマンドには、コマンドの実行後に入力する必要がある入力が含まれています。[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
```

ここで、**<IQ>** および **<R>** タグは、デバイスに表示される内容に対して提供されるテキストを評価します。

インタラクティブな質問では、正規表現を使用して、デバイスから受け取ったテキストが入力されたテキストと類似しているかどうかを検証します。**<IQ><R>** タグに入力された正規表現が見つかった場合は、インタラクティブな質問が検証を通過し、出力テキストの一部が表示されます。つまり、質問の一部を入力する必要がありますが、質問全体を入力する必要はありません。**<IQ>**と **<R>** タグの間に「Yes」または「No」を入力するだけで十分ですが、デバイスからの質問の出力に「Yes」または「No」のテキストが表示されていることを確認する必要があります。これを行う最善の方法は、デバイスでコマンドを実行し、出力を確認することです。さらに、入力された正規表現のメタ文字または改行が適切に使用されるか、完全に回避されることを確認する必要があります。一般的な正規表現のメタ文字は **です。( ) [ ] { } |* + ? \ $ ^: &**。

たとえば、次のコマンドには、メタ文字と改行を含む出力があります。

```
Switch(config)# no crypto pki trustpoint DNAC-CA
% Removing an enrolled trustpoint will destroy all certificates received from the related
 Certificate Authority
Are you sure you want to do this? [yes/no]:
```

テンプレートにこれを入力するには、メタ文字または改行がない部分を選択する必要があります。ここでは、使用可能なものの例をいくつか紹介します。

```
#INTERACTIVE
no crypto pki trustpoint DNAC-CA<IQ>yes/no<R>yes
#ENDS_INTERACTIVE


#INTERACTIVE
no crypto pki trustpoint DNAC-CA<IQ>Removing an enrolled<R>yes
#ENDS_INTERACTIVE


#INTERACTIVE
no crypto pki trustpoint DNAC-CA<IQ>Are you sure you want to do this<R>yes
#ENDS_INTERACTIVE


#INTERACTIVE
crypto key generate rsa general-keys <IQ>yes/no<R> no
#ENDS_INTERACTIVE
```

ここで、**<IQ>** タグおよび **<R>** タグは大文字と小文字を区別し、大文字で入力する必要があります。

（注） 応答後にインタラクティブな質問に対応するとき、改行文字が必要ない場合は **<SF>** タグを入力する必要があります。**<SF>** タグの前にスペースを 1 つ含めます。**<SF>** タグを入力すると、**</SF>** タグが自動的にポップアップ表示されます。**</SF >** タグは不要なため削除できます。

次に例を示します。

```
#INTERACTIVE
config advanced timers ap-fast-heartbeat local enable 20 <SF><IQ>Apply(y/n)?<R>y
#ENDS_INTERACTIVE
```

インタラクティブ イネーブル モード コマンドの組み合わせ

次の構文を使用して、インタラクティブな **Enable Mode** コマンドを結合します。

```
#MODE_ENABLE
#INTERACTIVE
commands<IQ>interactive question<R> response
#ENDS_INTERACTIVE
#ENDS_END_ENABLE

#MODE_ENABLE
#INTERACTIVE
mkdir <IQ>Create directory<R>xyz
#ENDS_INTERACTIVE
#MODE_END_ENABLE
```

複数行コマンド

CLI テンプレートで複数行をラップする場合は、**MLTCMD** タグを使用します。そうしなければ、コマンドは 1 行ずつデバイスに送信されます。[CLI Content] 領域にマルチライン コマンドを入力するには、次の構文を使用します。

```
<MLTCMD>first line of multiline command
second line of multiline command
...
...
last line of multiline command</MLTCMD>
```

- ここで、**<MLTCMD>** および **</MLTCMD>** は大文字と小文字を区別し、大文字で入力する必要があります。
- 複数行のコマンドは、**<MLTCMD>** タグと **</MLTCMD>** タグの間に挿入する必要があります。
- タグをスペースで開始することはできません。
- 1 行に **<MLTCMD>** タグと **</MLTCMD>** タグを使用することはできません。

テンプレートのネットワークプロファイルへの関連付け

始める前に

テンプレートをプロビジョニングする前に、テンプレートがネットワークプロファイルに関連付けられており、そのプロファイルがサイトに割り当てられていることを確認してください。

プロビジョニング中にデバイスが特定のサイトに割り当てられると、ネットワークプロファイルを介してサイトに関連付けられたテンプレートが詳細設定に表示されます。

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

次のタイプのプロファイルを使用できます。

- [Firewall]：ファイアウォール プロファイルの作成時にこれをクリックします。
- [Routing]：ルーティングプロファイルの作成時にこれをクリックします。
- [Switching]：スイッチングプロファイルの作成時にこれをクリックします。
  - 必要に応じて、[Onboarding Templates] または [Day-N Templates] をクリックします。
  - [Profile Name] フィールドに、プロファイルの名前を入力します。
  - [+Add Template] をクリックして、[Device Type]、[Tag Name]、および [Template] ドロップダウンリストから、デバイスのタイプ、タグ、およびテンプレートを選択します。

    必要なテンプレートが見つからない場合は、テンプレートエディタで新しいテンプレートを作成できます。標準テンプレートの作成 （316 ページ）を参照してください。
  - [**保存（Save）**] をクリックします。
- [Telemetry Appliance]：Cisco DNA トラフィック テレメトリ アプライアンス プロファイルの作成時にこれをクリックします。
- [Wireless]：ワイヤレスプロファイルの作成時にこれをクリックします。ワイヤレス ネットワーク プロファイルを割り当てる前に、ワイヤレス SSID が作成されていることを確認してください。
  - [Profile Name] フィールドに、プロファイルの名前を入力します。
  - [+ SSIDの追加（+ Add SSID）] をクリックします。**[Network Settings]** > **[Wireless]** で作成された SSID が表示されます。
  - [Attach Template(s)] で、[Template] ドロップダウンリストからプロビジョニングするテンプレートを選択します。
  - **[Save]** をクリックします。

（注） スイッチングプロファイルとワイヤレスプロファイルは、[Cards] ビューおよび [Table] ビューで表示できます。

ステップ 2 [Network Profiles] ウィンドウには、次のリストが表示されます。

- **Profile Name**
- **Type**
- **Version**
- **Created By**
- [Sites]：[Assign Site] をクリックして、選択したプロファイルにサイトを追加します。

ステップ 3 Day-N プロビジョニングの場合は、**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。

a) プロビジョニングするデバイス名の横にあるチェックボックスをオンにします。
b) [Actions] ドロップダウンリストから、[Provision] を選択します。
c) [サイトの割り当て（Assign Site）] ウィンドウで、プロファイルが添付されたサイトを割り当てます。
d) [Choose a Site] フィールドで、コントローラと関連付けるサイトの名前を入力するか、[Choose a Site] ドロップダウンリストから選択します。

e) **[次へ (Next)]** をクリックします。

f) [設定（Configuration）] ウィンドウが表示されます。[管理対象 AP ロケーション（Managed AP Locations）] フィールドで、このコントローラによって管理される AP の場所を入力します。サイトの変更、削除、または再割り当てができます。これはワイヤレスプロファイルにのみ適用可能です。

g) [Next] をクリックします。

h) **[Advanced Configuration（詳細設定）]** ウィンドウが表示されます。ネットワークプロファイルを介してサイトに関連付けられたテンプレートが詳細設定に表示されます。

- テンプレート内のインテントからの構成を上書きして、変更を上書きする場合は、[Provision these templates even if they have been deployed before] チェックボックスをオンにします（このオプションは、デフォルトで無効です）。
- [Copy running config to startup config] オプションはデフォルトで有効になっています。つまり、テンプレート構成を展開した後、write mem が適用されます。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適用しない場合は、このチェック ボックスをオフにする必要があります。
- [Find] 機能を使用し、デバイス名を入力してすばやくデバイスを検索するか、左側のペインでテンプレートフォルダを展開してテンプレートを選択します。右側のペインで、送信元にバインドされている属性の値を選択します。
- テンプレートを導入する間にテンプレートの変数を CSV ファイルにエクスポートするには、右側のペインで [エクスポート（Export）] をクリックします。CSV ファイルを使用して変数設定に必要な変更を加え、右側のペインで [Import] をクリックすると、後でそれを Cisco DNA Center にインポートできます。

i) [次へ（Next）] をクリックしてテンプレートを導入します。

j) テンプレートを今すぐ展開する場合は [Now] を選択します。または、後で展開するようにスケジュールすることを選択します。
展開が正常に完了すると、[Device Inventory] ウィンドウの [Status] 列に「SUCCESS」と表示されます。

ステップ 4 [Export Deployment CSV] をクリックして、1 つのファイルに含まれるすべてのテンプレートからテンプレート変数をエクスポートします。

ステップ 5 [Import Deployment CSV] をクリックして、1 つのファイルに含まれるすべてのテンプレートからテンプレート変数をインポートします。

ステップ 6 Day-0 プロビジョニングの場合は、**[Provision]** > **[Network Devices]** > **[Plug and Play]** の順に選択します。

a) デバイスを選択し、[Actions] ドロップダウンリストから [Claim] をクリックします。

b) [Next] をクリックし、[Site Assignment] ウィンドウで、[Site] ドロップダウンリストからサイトを選択します。

c) [Next] をクリックし、[Configuration] ウィンドウで、イメージと Day-0 テンプレートを選択します。

d) [Next] をクリックし、[Advanced Configuration] ウィンドウで場所を入力します。

e) [Next] をクリックして、[Device Details]、[Image Details]、[Day-0 Configuration Preview]、および [Template CLI Preview] を表示します。

第 12 章

設計モデルの設定

モデル設定エディタの概要

モデル設定では、プロビジョニング アプリケーション内にカプセル化される Cisco Validated Design（CVD）の高度なカスタマイズを定義できます。モデル設定は、高レベルのサービスインテントとデバイス固有の CLI テンプレートとともにネットワークデバイスに展開できる、モデルベースの検出可能かつカスタマイズ可能な構成機能のセットです。

モデル設定機能は、複雑なデバイス構成を抽象化し、デバイス固有の CLI の代わりに直感的な GUI を使用してカスタマイズ可能なネットワーク構成を容易にすることにより、ネットワークのプロビジョニングを簡素化します。共通の設計は、統一された方法で、さまざまなデバイス ハードウェア プラットフォームとソフトウェアタイプに展開されます。展開時に、Cisco DNA Center インフラストラクチャは、抽出された設計を自動的に検証してデバイス固有の CLI コマンドに変換します。

モデル設定設計をプロビジョニングするには、次の手順を実行します。

1. [Model Config Editor] ウィンドウ（メニューアイコンから **[Tools]** > **[Model Config Editor]** の順に選択）を使用して、新しいモデル設定の設計を作成します。
2. モデル設定設計をさまざまなネットワークプロファイルに適用します。

3. プロビジョニング ワークフローを使用して、ネットワークプロファイルで指定されたモデル設定設計をネットワークデバイスに適用します。

サポートされているモデル設定設計タイプ

Cisco DNA Center では、次のタイプのワイヤレスモデル設定設計がサポートされています。

- AAA RADIUS 属性
- 高度な SSID 構成
- CleanAir 構成
- Dot11ax 構成
- グローバル IPv6 構成
- マルチキャストの設定

レガシーデバイスからの設計の検出と作成

モデル設定エディタを使用して手動で設計を作成する代わりに、[Discover Model Configs] 機能を使用して使用可能な既存のモデル設定の設計をレガシーデバイスから検出し、それらをテンプレートとして使用して新しい設計を作成することができます。

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

ステップ 2 [Discovery] タブをクリックします。

[Inventory] ウィンドウにある使用可能な検出済みデバイスのリストが表示されます。

ステップ 3 デバイス名の横にあるオプションボタンをクリックし、[Discover Model Configs] をクリックします。

ステップ 4 右側のペインで、[Wireless] を展開し、モデル設定の設計タイプを選択します。

選択したモデル設定のタイプで使用可能な設定が表示されます。たとえば、[Wireless] の [CleanAir Configuration] を選択した場合、CleanAir についての使用可能な設定が表示されます。

ステップ 5 新しい設計を作成するためのテンプレートとして使用する設定の横にあるオプションボタンをクリックし、[Create Design] をクリックします。

ステップ 6 表示されるウィンドウで、必要な変更を行ってから [Save] をクリックします。

AAA RADIUS 属性のモデル設定設計の作成

Cisco AireOS コントローラおよび Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの Called-station-id パラメータ値を定義するには、「**AAA RADIUS 属性設定**」モデル設定を使用します。

「**Default AAA_Radius_Attributes_Configuration**」により、called-station ID が **ap-macaddress-ssid** として定義されます。このデフォルトのモデル設定は編集または削除できません。ただし、特定のネットワーク設計用にカスタムモデル設定を作成することができます。

この手順では、新しい AAA RADIUS 属性設定のモデル設定を作成する方法について説明します。

始める前に

検出されたデバイスが [Inventory] ウィンドウに一覧表示されるように、[Discovery] 機能を使用してネットワーク内のデバイスを検出しておきます。

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

ステップ 2 左側のペインで、[Search] フィールドにモデル設定の名前を入力して検索するか、[Wireless] を展開して [AAA Radius Attributes Configuration] を選択します。

ステップ 3 [Design Instances] ウィンドウで、[Add] をクリックします。

[Add Called-station-id] スライドインペインが表示されます。

ステップ 4 [Design Name] フィールドにモデル設定設計の名前を入力します。

ステップ 5 [Called-station-id] ドロップダウンリストから、次の属性値のいずれかを選択します。

- **ap-ethmac-only**
- **ap-ethmac-ssid**
- **ap-group-name**
- **ap-label-address**
- **ap-label-address-ssid**
- **ap-location**
- **ap-macaddress**
- **ap-macaddress-ssid**
- **ap-name**
- **ap-name-ssid**
- **ipaddress**
- **macaddress**

- **vlan-id**

ステップ 6 [保存（Save）] をクリックします。

[Design Instances] ウィンドウに新しい設計インスタンスが表示されます。

ステップ 7 （オプション）設計を編集するには、編集する設計の名前の横にあるチェックボックスをオンにして [Edit] をクリックします。変更を加えたら、[Save] をクリックします。

ステップ 8 ワイヤレスコントローラに展開できるようにするために、作成した設定の設計をネットワークプロファイルに関連付けます。メニューアイコン（☰）をクリックして、**[Design]** > **[Network Profiles]** の順に選択します。

詳細については、ワイヤレス用のネットワークプロファイルの作成 （304 ページ）を参照してください。

ステップ 9 ネットワークプロファイルで指定されたモデル設定設計をネットワークデバイスにプロビジョニングします。メニューアイコン（☰）をクリックして、**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。

詳細については、Cisco AireOS コントローラのプロビジョニング （422 ページ）またはCisco Catalyst 9800 シリーズ ワイヤレスコントローラのプロビジョニング （462 ページ）を参照してください。

高度な SSID のモデル設定設計の作成

SSID は、WLAN に基づいてインターフェイスまたはインターフェイスグループに関連付けられます。WLAN で、セキュリティ、Quality of Service（QoS）、無線ポリシーなど、ワイヤレスネットワークのパラメータが設定されます。ワイヤレスコントローラごとに最大 512 個の WLAN を設定できます。

デバイスの高度なサービスセット識別子（SSID）パラメータの設定には、高度な SSID モデル設定を使用します。

始める前に

検出されたデバイスが [Inventory] ウィンドウに一覧表示されるように、[Discovery] 機能を使用してネットワーク内のデバイスを検出しておきます。

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

ステップ 2 左側のペインで、[Search] フィールドにモデル設定の名前を入力して検索するか、[Wireless] を展開して [Advanced SSID Configuration] を選択します。

ステップ 3 [Design Instances] ペインで、[Default Advanced SSID Design] チェックボックスをオンにして、デフォルトの拡張 SSID 設計を使用します。

（注） デフォルトの高度な SSID 設計を編集または削除することはできません。

ステップ 4 [Design Instances] ペインで [Add Design] をクリックします。

[Add Advanced SSID Configuration] ウィンドウが表示されます。

ステップ 5 [Design Name] フィールドにモデル設定の名前を入力します。

ステップ 6 [General] タブで、[Peer-to-Peer Blocking] ドロップダウンリストをクリックして、ピアツーピアブロッキングのオプションを選択します。

ピアツーピアブロッキングは、個々の WLAN に適用されます。クライアントは、それぞれが関連付けられている WLAN からピアツーピアブロッキング設定を継承します。ピアツーピアブロッキングを使用すると、トラフィックの転送方法を細かく制御できます。

- [DISABLE]：ピアツーピアブロッキングを無効にし、可能な場合はワイヤレスコントローラ内においてローカルでトラフィックを転送し ます。
- [DROP]：ワイヤレスコントローラでクライアントパケットを破棄します。
- [FORWARD UP]：クライアントパケットをアップストリームの VLAN に転送します。これらのパケットに対して行われる動作は、ワイヤレスコントローラよりも上流にあるデバイスにより決定されます。このデバイスは、ルータまたはレイヤ 3 スイッチのいずれかになります。
- [ALLOW PVT GROUP]：事前共有キー（PSK）クライアントにのみ適用されます。送信元と宛先のクライアントデバイスに関連付けられている Identity PSK（IPSK）タグに基づいてトラフィックが転送されます。

ステップ 7 パッシブクライアント機能を有効にするには、[Passive Client Enable] トグルボタンをクリックします。

パッシブクライアントとは、固定 IP アドレスが設定されている、スケールやプリンタなどのワイヤレスデバイスです。これらのクライアントは、アクセスポイントとの関連付けの際に IP 情報（IP アドレス、サブネットマスク、ゲートウェイ情報など）を送信しません。その結果、パッシブクライアントが使用された場合、それらのクライアントが DHCP を使用しない限り、ワイヤレスコントローラではその IP アドレスは認識されません。

ステップ 8 WLAN の経由ローミング予測リストを設定するには、[Assisted Roaming Prediction Optimization] トグルボタンをクリックします。

ステップ 9 デュアル無線バンドのネイバーリストを設定するには、[Neighbor List Dual Band] トグルボタンをクリックします。

ステップ 10 WLAN で SNMP NAC サポートを有効にするには、[Network Admission Control (NAC-SNMP)] トグルボタンをクリックします。

ステップ 11 WLAN で RADIUS NAC サポートを有効にするには、[Network Admission Control (NAC-Radius)] トグルボタンをクリックします。

ステップ 12 [DHCP Required] ドロップダウンリストで、RUN 状態（クライアントからのトラフィックがワイヤレスコントローラを通過できる状態）になるために DHCP 要求が必要かどうかに応じて、[Yes] または [No] のいずれかを選択します。

ステップ 13 [DHCP Server] を展開し、[IP Address] フィールドに DHCP サーバーの IP アドレスを入力します。

ステップ 14 FlexConnect ローカル認証を有効にするには、[FlexConnect Local Authentication] トグルボタンをクリックします。

ステップ 15 [802.11ax Status] トグルボタンをクリックして、802.11ax 構成パラメータを有効にします。

ステップ 16 [Aironet IE] トグルボタンをクリックして、この SSID で Aironet IE のサポートを有効にします。

ステップ 17 [Load Balance Enable] トグルボタンをクリックして、負荷分散機能を有効にします。

ステップ 18 [DTIM Period 5GHz Band (In Beacon Intervals) [1-255]] フィールドに、5GHz 無線の値を入力します。

有効な範囲は 1 ～ 255 です。デフォルト値は 1（ブロードキャストフレームおよびマルチキャストフレームはビーコンのたびに送信）です。

802.11 ネットワークのビーコン間隔が 100 ミリ秒で DTIM 値が 1 に設定されている場合、アクセスポイントは、バッファされたブロードキャストフレームおよびマルチキャストフレームを毎秒 10 回送信します。ビーコン期間が 100 ミリ秒で DTIM 値が 2 に設定されている場合、アクセスポイントは、バッファされたブロードキャストフレームおよびマルチキャストフレームを毎秒 5 回送信します。これらの設定はいずれも、ブロードキャスト フレームおよびマルチキャスト フレームの頻度を想定する、Voice over IP（VoIP）を含むアプリケーションに適しています。

ただし、DTIM 値は 255 まで設定できます（255 回のビーコンごとにブロードキャストフレームおよびマルチキャストフレームを送信します）。

ステップ 19 [DTIM Period 2.4GHz Band (In Beacon Intervals) [1-255]] フィールドに、2.4GHz 無線の値を入力します。有効な範囲は 1 ～ 255 です。デフォルト値は 1（ブロードキャスト フレームおよびマルチキャスト フレームはビーコンのたびに送信）です。

ステップ 20 [Scan Defer Time [0-60000msecs]] フィールドにミリ秒単位で時間を設定します。

有効な値は 0 ～ 60000 ミリ秒、デフォルト値は 100 ミリ秒です。時間を 0 に設定すると、スキャンの保留は実行されません。スキャンの保留時間は同じ WLAN のすべてのプライオリティに共通です。また、スキャンは保留プライオリティのいずれかでパケットが送信または受信される場合に保留されます。

ステップ 21 [Max Clients Per WLAN] フィールドに、WLAN への参加を許可されるクライアントの最大数を入力します。

有効な範囲は 1 ～ 10000 です。

ステップ 22 [Max Clients Per AP Radio Per WLAN [0-200]] フィールドに、WLAN への参加を許可される AP ごとのクライアントの最大数を入力します。

有効な範囲は、0 ～ 200 です。

ステップ 23 [Max Clients Per AP Radio Per WLAN [0-400]] フィールドに、AP ごとに許可されるクライアント接続の最大数を入力します。

有効な範囲は、0 ～ 400 です。

ステップ 24 [WMM Policy] ドロップダウンリストから、WMM ポリシーとして [Allowed]、[Disabled]、または [Required] を選択します。

デフォルトでは、WMM ポリシーが許可されています。

ステップ 25 [NAS ID] フィールドにネットワークアクセスサーバー識別子を入力します。

ステップ 26 [Client Data Rates] をクリックし、次の各フィールドに値を入力して、クライアントごとにクライアントデータレート制限を設定します。

- Average Downstream Data Rate Per Client (kbps)
- Burst Downstream Data Rate Per Client (kbps)
- Average Downstream Real-Time Rate Per Client (kbps)
- Burst Downstream Real-Time Rate Per Client (kbps)
- Average Upstream Data Rate Per Client (kbps)
- Burst Upstream Data Rate Per Client (kbps)
- Average Upstream Real-Time Rate Per Client (kbps)
- Burst Upstream Real-Time Rate Per Client (kbps)

ステップ 27 [SSID Data Rate] をクリックし、次の各フィールドに値を入力して、SSID ごとに SSID データレート制限を設定します。

- Average Upstream Data Rate Per SSID (kbps)
- Burst Upstream Data Rate Per SSID (kbps)
- Average Upstream Real-Time Rate Per SSID (kbps)
- Burst Upstream Real-Time Rate Per SSID (kbps)
- Average Downstream Data Rate Per SSID (kbps)
- Burst Downstream Data Rate Per SSID (kbps)
- Average Downstream Real-Time Rate Per SSID (kbps)
- Burst Downstream Real-Time Rate Per SSID (kbps)

（注） 設計のすべてのプロパティをロックするには、[Lock all] をクリックします。特定のプロパティをロックするには、そのプロパティの横にあるロック記号をクリックします。

ステップ 28 [802.11ax Configuration] をクリックし、802.11ax BSS 設定のパラメータを設定します。トグルボタンを使用して次の設定パラメータを有効または無効にすることができます。

- BSS ターゲット起動時間
- ダウンリンク OFDMA
- アップリンク OFDMA
- ダウンリンク MU-MIMO
- アップリンク MU-MIMO

（注） 設計のすべてのプロパティをロックするには、[Lock all] をクリックします。特定のプロパティをロックするには、そのプロパティの横にあるロック記号をクリックします。

ステップ 29 **[保存（Save）]** をクリックします。

作成した設計インスタンスが [Design Instances] ウィンドウの [Advanced SSID Configuration - Model Configs] 領域に表示されます。

ステップ 30 設計を編集するには、編集する設計の名前の横にあるチェックボックスをオンにして [Edit] をクリックします。変更を加えたら、[Save] をクリックします。

ステップ 31 ワイヤレスコントローラに展開できるようにするために、作成した設定の設計をネットワークプロファイルに関連付けます。メニューアイコン（☰）をクリックして、**[Design]** > **[Network Profiles]** の順に選択します。

詳細については、ワイヤレス用のネットワークプロファイルの作成（304 ページ）を参照してください。

ステップ 32 ネットワークプロファイルで指定されたモデル設定設計をネットワークデバイスにプロビジョニングします。メニューアイコン（☰）をクリックして、**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。

詳細については、Cisco AireOS コントローラのプロビジョニング （422 ページ）を参照してください。

Cisco CleanAir の設計の作成

CleanAir は、共有ワイヤレススペクトラムに関する問題に予防的に対応するスペクトルインテリジェンス ソリューションです。この機能を使用すると、共有スペクトラムの全ユーザーを確認できます（ネイティブデバイスと外部干渉源の両方）。また、ネットワークにおいて、これらの情報に基づいて対処できるようになります。たとえば、干渉デバイスを手動で排除することや、システムによって自動的にチャネルをステアリングして干渉を受けないようにすることができます。CleanAir は、スペクトラム管理と無線周波数（RF）の可視性を提供します。

始める前に

検出されたデバイスが [Inventory] ウィンドウに一覧表示されるように、[Discovery] 機能を使用してネットワーク内のデバイスを検出しておきます。

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

ステップ 2 左側のペインで、[Search Capability] フィールドにモデル設定機能の名前を入力して検索するか、[Wireless] モデル設定を展開して [CleanAir Configuration] を選択します。

ステップ 3 [Design Instances] ペインで、[Default CleanAir 802.11a Design] または [Default CleanAir 802.11b Design] チェックボックスをオンにして、デフォルトの CleanAir 設計を使用します。

（注） [Default CleanAir 802.11a Design] または [Default CleanAir 802.11b Design] は編集および削除できません。

ステップ 4 [Design Instances] ウィンドウで、[Add] をクリックします。

[Add CleanAir Configuration] ウィンドウが表示されます。

ステップ 5 [Design Name] フィールドに設計の名前を入力します。

ステップ 6 [Radio Band] ドロップダウンリストから [2.4 GHz] または [5 GHz] を選択します。

ステップ 7 [CleanAir Enable] トグルボタンをクリックして、2.4 GHz または 5 GHz の無線帯域で CleanAir 機能を有効にします。

[CleanAir Enable] トグルボタンが有効になっている場合は、そのトグルボタンをクリックしてスペクトル干渉を シスコ ワイヤレス コントローラ で検出しないようにします。

ステップ 8 [CleanAir Device Reporting Enable] トグルボタンをクリックして、干渉源が検出された場合に CleanAir システムから報告されるようにします。

[CleanAir Device Reporting Enable] トグルボタンが有効になっている場合は、トグルボタンをクリックして干渉源が シスコ ワイヤレス コントローラ から報告されないようにします。

ステップ 9 CleanAir で検出できる永続型デバイスに関する情報を伝達できるように、[Persistent Device Propagation] トグルボックスをオンにします。

永続型デバイスの伝達を有効にすると、同じシスコ ワイヤレス コントローラに接続されているネイバー AP に永続型デバイスの情報を伝達できます。永続型の干渉源は、検出されない場合でも、常に存在し、WLAN の動作に干渉します。

ステップ 10 [Enable Interferers Features] を展開し、CleanAir システムで検出および報告する必要がある干渉源の横にあるチェックボックスをオンにします。

- Ble Beacon
- Bluetooth Paging Inquiry
- Bluetooth SCO ACL
- Generic Dect
- Generic TDD
- Generic Waveform
- Jammer
- 電子レンジ
- Motorola Canopy
- SI FHSs
- Spectrum 802.11 FH
- Spectrum 802.11 Non STD Channel
- Spectrum 802.11 Spec Inverted
- Spectrum 802.11 Super AG SuperAG
- Spectrum 802.15.4
- ビデオ
- Wimax Fixed

- Wimax Mobile
- XBox

ステップ 11 [CleanAir Description] フィールドに説明を入力します。

ステップ 12 [Apply] をクリックします。
作成した設計インスタンスが [Design Instances] ウィンドウの [CleanAir Configuration - Model Configs] 領域に表示されます。

ステップ 13 設計を編集するには、編集する設計の名前の横にあるチェックボックスをオンにして [Edit] をクリックします。変更を加えたら、[Save] をクリックします。

ステップ 14 ワイヤレスコントローラに展開できるようにするために、作成した設定の設計をネットワークプロファイルに関連付けます。メニューアイコン（☰）をクリックして、**[Design]** > **[Network Profiles]** の順に選択します。

詳細については、ワイヤレス用のネットワークプロファイルの作成（304ページ）を参照してください。

ステップ 15 ネットワークプロファイルで指定されたモデル設定設計をネットワークデバイスにプロビジョニングします。メニューアイコン（☰）をクリックして、**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。

詳細については、Cisco AireOS コントローラのプロビジョニング （422 ページ）を参照してください。

Dot11ax 設定のモデル設定設計の作成

Cisco DNA Center の Dot11ax モデル設定機能により、デバイスの Dot11ax パラメータが設定されます。

Dot11ax 設定には、高効率（HE）ワイヤレスとも呼ばれる 802.11ax ワイヤレス仕様標準が含まれます。Dot11ax は 2.4 GHz と 5 GHz のデュアルバンドテクノロジーです。Dot11ax 設定パラメータは、Wi-Fi 6 をサポートしている Cisco Catalyst 9100 シリーズアクセスポイントでのみ設定できます。

（注） BSS カラーは、重複する基本サービスセット（OBSS）を識別するために使用されます。BSS 設定は、Wi-Fi 6 対応アクセスポイントでのみプッシュされます。Cisco Catalyst 9100 シリーズアクセスポイントは、高密度の高解像度アプリケーションに最適な次世代の Wi-Fi 802.11ax アクセスポイントです。

始める前に

検出されたデバイスが [Inventory] ウィンドウに一覧表示されるように、[Discovery] 機能を使用してネットワーク内のデバイスを検出する必要があります。

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

ステップ 2 左側のペインで、[Search Capability] フィールドにモデル設定の名前を入力するか、[Wireless] を展開して [Dot11ax Configuration] を選択することで、モデル設定を検索できます。

ステップ 3 [Design Instances] ペインで [Default Dot11ax Design] チェックボックスをオンにしてデフォルトの Dot11ax 設計を使用します。

（注） [Default dot11ax Design] の値は編集および削除できません。

ステップ 4 [Design Instances] ウィンドウで、[Add Design] をクリックします。

[Add Dot11ax Configuration] ウィンドウが表示されます。

ステップ 5 [Design Name] フィールドにモデル設定設計の名前を入力します。

ステップ 6 [BSS Color] トグルボタンをクリックして、2.4 GHz または 5 GHz の無線帯域で BSS カラー機能を有効にします。デフォルト値は [disabled] です。

ステップ 7 [Target Wakeup Time] トグルボタンをクリックしてターゲットのウェイクアップ時間を有効にします。デフォルト値は [disabled] です。

ステップ 8 [Radio Band] ドロップダウンリストから 2.4 GHz または 5 GHz の無線帯域を選択します。

（注） 設計のすべてのプロパティをロックするには、[Lock all] をクリックします。特定のプロパティをロックするには、各プロパティの横にあるロック記号をクリックします。

ステップ 9 [**保存（Save）**] をクリックします。

作成した設計インスタンスが [Design Instances] ウィンドウの [Dot11ax Configuration - Model Configs] エリアに表示されます。

ステップ 10 設計を編集するには、編集する設計の名前の横にあるチェックボックスをオンにして [Edit] をクリックします。変更を加えたら、[Save] をクリックします。

ステップ 11 アクセスポイントに展開できるようにするために、作成した設定の設計をネットワークプロファイルに関連付けます。メニューアイコン（☰）をクリックして、**[Design]** > **[Network Profiles]** の順に選択します。詳細については、「ワイヤレス用のネットワークプロファイルの作成」を参照してください。

ステップ 12 ネットワークプロファイルで指定されたモデル設定設計をネットワークデバイスにプロビジョニングします。メニューアイコン（☰）をクリックして、**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。詳細については、Cisco AireOS コントローラのプロビジョニング （422 ページ）を参照してください。

イベント駆動型 RRM のモデル設定設計の作成

イベント駆動型 RRM モデル設定機能は、2.4 GHz、5 GHz、および 6 GHz 無線のイベント駆動型 RRM パラメータを設定します。

始める前に

検出されたデバイスが [Inventory] ウィンドウに一覧表示されるように、[Discovery] 機能を使用してネットワーク内のデバイスを検出しておきます。

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

ステップ 2 左側のペインで、[Search] フィールドにモデル設定の名前を入力して検索するか、[Wireless] を展開して [Event Driven RRM Configuration] を選択します。

ステップ 3 [Design Instances] ペインで、[Default Event Driven 2.4GHz Design] または [Default Event Driven 5 GHz Design] チェックボックスをオンにして、デフォルトの高度な SSID 設計を使用します。

（注） デフォルトのイベント駆動型 RRM 設計を編集または削除することはできません。

ステップ 4 [Design Instances] ペインで [Add Design] をクリックします。

[Add Event Driven RRM Configuration] スライドインウィンドウが表示されます。

ステップ 5 [Design Name] フィールドにモデル設定の名前を入力します。

ステップ 6 [Radio Band] ドロップダウンリストから、無線帯域（[2.4GHz]、[5GHz]、または [6GHz]）を選択します。

（注） 6 GHz 無線帯域は、Cisco AireOS ワイヤレスコントローラではサポートされていません。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ バージョン 17.6 以降は、6 GHz 無線帯域をサポートします。

ステップ 7 [Event Driven RRM] トグルボタンをクリックして、CleanAir 対応 AP が重大なレベルの干渉を検出したときに RRM を実行します。

ステップ 8 [Sensitivity Threshold] ドロップダウンリストで、次のオプションから RRM をトリガーする感度しきい値レベルを選択します。

AP の干渉がしきい値レベルを上回ると、RRM はローカルの動的チャネル割り当て（DCA）の実行を開始し、ネットワーク パフォーマンスを改善できる場合は影響を受ける AP 無線のチャネルを変更します。

- [Low]：電波品質（AQ）値が示す非 Wi-Fi 干渉への感度を最低に指定します。
- [Medium]：電波品質（AQ）値が示す非 Wi-Fi 干渉への感度を中間に指定します。
- [High]：AQ 値によって示される非 Wi-Fi 干渉に対する最も高い感度を指定します。
- [Custom]：AQ 値によって示される非 Wi-Fi 干渉に対するカスタム感度を指定します。このオプションを選択した場合は、[Custom Threshold [1-99]] フィールドでカスタム値を指定する必要があります。

ステップ 9 **[Save]** をクリックします。

作成した設計インスタンスが [Design Instances] ウィンドウの [Event Driven RRM Configuration - Model Configs] 領域に表示されます。

ステップ 10 設計を編集するには、編集する設計の名前の横にあるチェックボックスをオンにして [Edit] をクリックします。変更を加えたら、[Save] をクリックします。

ステップ 11 ワイヤレスコントローラに展開できるようにするために、作成した設定の設計をネットワークプロファイルに関連付けます。メニューアイコン（☰）をクリックして、**[Design]** > **[Network Profiles]** の順に選択します。

詳細については、ワイヤレス用のネットワークプロファイルの作成（304ページ）を参照してください。

ステップ 12 ネットワークプロファイルで指定されたモデル設定設計をネットワークデバイスにプロビジョニングします。メニューアイコン（☰）をクリックして、**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。

詳細については、Cisco AireOS コントローラのプロビジョニング （422 ページ）を参照してください。

Flex 構成の設計の作成

flex モデル設定機能を使用して、デバイスで FlexConnect 設定を構成します。

始める前に

[Discovery] 機能を使用して、検出されたデバイスが [Inventory] ウィンドウに一覧表示されるように、ネットワーク内のデバイスを検出します。

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

ステップ 2 左側のペインで、[Search Capability] フィールドにモデル設定機能の名前を入力して検索するか、[Wireless] モデル設定を展開して [Flex Configuration] を選択します。

ステップ 3 [Design Instances] ペインで [Default Flex Configuration] チェックボックスをオンにしてデフォルトの FlexConnect 設計を使用します。

（注） [Default Flex Configuration] 設計は編集および削除できません。

ステップ 4 [Design Instances] ウィンドウで、[Add] をクリックします。

[Add CleanAir Configuration] ウィンドウが表示されます。

ステップ 5 [Design Name] フィールドに設計の名前を入力します。

ステップ 6 [Radio Band] ドロップダウンリストから [2.4 GHz] または [5 GHz] を選択します。

ステップ 7 [CleanAir Enable] トグルボタンをクリックして、2.4 GHz または 5 GHz の無線帯域で CleanAir 機能を有効にします。

[CleanAir Enable] トグルボタンが有効になっている場合は、そのトグルボタンをクリックしてスペクトル干渉を シスコ ワイヤレス コントローラ で検出しないようにします。

ステップ 8 [CleanAir Device Reporting Enable] トグルボタンをクリックして、干渉源が検出された場合に CleanAir システムから報告されるようにします。

[CleanAir Device Reporting Enable] トグルボタンが有効になっている場合は、トグルボタンをクリックして干渉源が シスコ ワイヤレス コントローラ から報告されないようにします。

ステップ 9 CleanAir で検出できる永続型デバイスに関する情報を伝達できるように、[Persistent Device Propagation] トグルボックスをオンにします。

永続型デバイスの伝達を有効にすると、同じシスコ ワイヤレス コントローラに接続されているネイバーAPに永続型デバイスの情報を伝達できます。永続型の干渉源は、検出されない場合でも、常に存在し、WLAN の動作に干渉します。

ステップ 10 [Enable Interferers Features] を展開し、CleanAir システムで検出および報告する必要がある干渉源の横にあるチェックボックスをオンにします。

- Ble Beacon
- Bluetooth Paging Inquiry
- Bluetooth SCO ACL
- Generic Dect
- Generic TDD
- Generic Waveform
- Jammer
- 電子レンジ
- Motorola Canopy
- SI FHSs
- Spectrum 802.11 FH
- Spectrum 802.11 Non STD Channel
- Spectrum 802.11 Spec Inverted
- Spectrum 802.11 Super AG SuperAG
- Spectrum 802.15.4
- ビデオ
- Wimax Fixed
- Wimax Mobile
- XBox

ステップ 11 [CleanAir Description] フィールドに説明を入力します。

ステップ 12 [Apply] をクリックします。
作成した設計インスタンスが [Design Instances] ウィンドウの [CleanAir Configuration - Model Configs] 領域に表示されます。

ステップ 13 設計を編集するには、編集する設計の名前の横にあるチェックボックスをオンにして [Edit] をクリックします。変更を加えたら、[Save] をクリックします。

ステップ 14 ワイヤレスコントローラに展開できるようにするために、作成した設定の設計をネットワークプロファイルに関連付けます。メニューアイコン（☰）をクリックして、**[Design]** > **[Network Profiles]** の順に選択します。

詳細については、ワイヤレス用のネットワークプロファイルの作成（304ページ）を参照してください。

ステップ 15 ネットワークプロファイルで指定されたモデル設定設計をネットワークデバイスにプロビジョニングします。メニューアイコン（☰）をクリックして、**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。

詳細については、Cisco AireOS コントローラのプロビジョニング （422 ページ）を参照してください。

グローバル IPv6 の設計の作成

始める前に

検出されたデバイスが [Inventory] ウィンドウに一覧表示されるように、[Discovery] 機能を使用してネットワーク内のデバイスを検出しておきます。

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

ステップ 2 左側のペインで、[Search Capability] フィールドにモデル設定の名前を入力して検索するか、[Wireless] を展開して [Global IPV6 Configuration] を選択します。

ステップ 3 [Design Instances] ペインで、[Default Global IPv6 Design] チェックボックスをオンにして、デフォルトのグローバル IPV6 設計を使用します。

（注） [Default Global IPv6 Design] は編集も削除もできません。

ステップ 4 [Design Instances] ウィンドウで、[Add Design] をクリックします。

[Add Global IPV6 Configuration] ウィンドウが表示されます。

ステップ 5 [Design Name] フィールドにモデル設定の名前を入力します。

ステップ 6 [Global IPV6 Config] トグルボタンをクリックして、IPv6 をデバイスでグローバルに有効にします。

ステップ 7 [Apply] をクリックします。

作成した設計インスタンスが [Design Instances] ウィンドウの [Global IPV6 Configuration - Model Config] 領域に表示されます。

ステップ 8 設計を編集するには、編集する設計の名前の横にあるチェックボックスをオンにして [Edit] をクリックします。変更を加えたら、[Save] をクリックします。

ステップ 9 ワイヤレスコントローラに展開できるようにするために、作成した設定の設計をネットワークプロファイルに関連付けます。メニューアイコン（☰）をクリックして、**[Design]** > **[Network Profiles]** の順に選択します。

詳細については、ワイヤレス用のネットワークプロファイルの作成（304ページ）を参照してください。

ステップ 10 ネットワークプロファイルで指定されたモデル設定設計をネットワークデバイスにプロビジョニングします。メニューアイコン（☰）をクリックして、**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。

詳細については、Cisco AireOS コントローラのプロビジョニング （422 ページ）を参照してください。

マルチキャストのモデル設定設計の作成

デバイスでマルチキャストパラメータを設定するには、マルチキャストモデル設定機能を使用します。

ネットワークがパケットのマルチキャストをサポートしている場合は、シスコ ワイヤレス コントローラが使用するマルチキャストの方法を設定できます。ワイヤレスコントローラは次のいずれかのモードでマルチキャストを実行します。

- ユニキャストモード：このモードでは、ワイヤレスコントローラは、ワイヤレスコントローラに関連付けられているすべてのアクセスポイントにすべてのマルチキャストパケットをユニキャストします。このモードはそれほど効率的ではありませんが、マルチキャストをサポートしていないネットワークでは必要です。
- マルチキャストモード：このモードでは、ワイヤレスコントローラはマルチキャストパケットを CAPWAP マルチキャストグループに送信します。この方法では、ワイヤレスコントローラプロセッサのオーバーヘッドが軽減され、パケットレプリケーションの処理がネットワークに移されます。この方式は、ユニキャスト方式より効率的です。

始める前に

検出されたデバイスが [Inventory] ウィンドウに一覧表示されるように、[Discovery] 機能を使用してネットワーク内のデバイスを検出しておきます。

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

ステップ 2 左側のペインで、[Search Capability] フィールドにモデル設定の名前を入力するか、[Wireless] を展開して [Multicast Configuration] を選択することで、モデル設定を検索できます。

ステップ 3 [Design Instances] ペインで、[Default Multicast Design] チェックボックスをオンにして、デフォルトのマルチキャスト設計を使用します。

（注） [Default Multicast Design] は編集も削除もできません。

ステップ 4 [Design Instances] ウィンドウで、[Add Design] をクリックします。

[Add Multicast Configuration] ウィンドウが表示されます。

ステップ 5 [Design Name] フィールドにモデル設定設計の名前を入力します。

ステップ 6 [Enable Global Multicast Mode] トグルボタンをクリックして、マルチキャストパケットの送信を設定します。デフォルト値は [disabled] です。

ステップ 7 [AP Multicast Mode] ドロップダウンリストから、[UNICAST] または [MULTICAST] を選択します。

- ワイヤレスコントローラからユニキャスト方式でパケットをブロードキャストするように設定するには、[UNICAST] を選択します。
- ワイヤレスコントローラからマルチキャスト方式でCAPWAPマルチキャストグループにパケットをブロードキャストするように設定するには、[MULTICAST] を選択します。

ステップ 8 [IPV4 Multicast Group Address] を展開し、[IP Address] フィールドに IPv4 マルチキャストアドレスを入力します。

ステップ 9 [IPV6 Multicast Group Address] を展開し、[IP Address] フィールドに IPv6 マルチキャストアドレスを入力します。

ステップ 10 [Apply] をクリックします。

作成した設計インスタンスが [Design Instances] ウィンドウの [Multicast - Model Config] 領域に表示されます。

ステップ 11 設計を編集するには、編集する設計の名前の横にあるチェックボックスをオンにして [Edit] をクリックします。変更を加えたら、[Save] をクリックします。

ステップ 12 ワイヤレスコントローラに展開できるようにするために、作成した設定の設計をネットワークプロファイルに関連付けます。メニューアイコン（☰）をクリックして、**[Design]** > **[Network Profiles]** の順に選択します。

詳細については、ワイヤレス用のネットワークプロファイルの作成（304ページ）を参照してください。

ステップ 13 ネットワークプロファイルで指定されたモデル設定設計をネットワークデバイスにプロビジョニングします。メニューアイコン（☰）をクリックして、**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。

詳細については、Cisco AireOS コントローラのプロビジョニング （422 ページ）を参照してください。

RRM 一般パラメータのモデル設定設計の作成

無線リソース管理（RRM）の一般設定のモデル設定機能は、2.4 GHz、5 GHz、および 6 GHz 無線の RRM 一般パラメータを設定します。

始める前に

検出されたデバイスが [Inventory] ウィンドウに一覧表示されるように、[Discovery] 機能を使用してネットワーク内のデバイスを検出しておきます。

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

ステップ 2 左側のペインで、[Search] フィールドにモデル設定の名前を入力して検索するか、[Wireless] を展開して [RRM General Configuration] を選択します。

ステップ 3 [Design Instances] ペインには、次のデフォルトの RRM の一般設定設計が表示されます。デフォルトの設計を使用するには、それぞれのデフォルトの [RRM General Design] チェックボックスをオンにします。

デフォルトの RRM 一般設計は編集も削除もできません。

- デフォルトの RRM 一般 2.4 GHz 設計
- デフォルトの RRM 一般 5 GHz 設計
- デフォルトの RRM 一般 6 GHz 設計

（注） 6 GHz 無線帯域は、Cisco AireOS ワイヤレスコントローラではサポートされていません。

（注） Cisco Catalyst 9800 シリーズ ワイヤレスコントローラ 17.6 以降のリリースは、6 GHz 無線帯域をサポートします。

ステップ 4 [Design Instances] ペインで [Add Design] をクリックします。

[Add RRM General Configuration] スライドインウィンドウが表示されます。

ステップ 5 設計のすべてのプロパティをロックするには、[Lock all] をクリックします。特定のプロパティをロックするには、そのプロパティの横にあるロック記号をクリックします。

ステップ 6 [Design Name] フィールドにモデル設定の名前を入力します。

ステップ 7 [Radio Band] タブで、[Radio Band] ドロップダウンリストから無線帯域を 2.4 GHz、5 GHz、または 6 GHz から選択します。

ステップ 8 [Threshold] タブで、[Throughput Threshold (1000-10000000 Bps)] フィールドで選択した無線帯域のスループットしきい値を設定します。

ステップ 9 [Monitoring] タブで、モニタリングチャネルとネイバー探索タイプを設定します。

- [Monitoring Channels] ドロップダウンリストから次のオプションのいずれかを選択して、AP で RRM によるスキャンに使用されるチャネルのセットを指定します。デフォルトでは、モニタリングチャネルは [Country] に設定されています。
  - [All]：選択した無線でサポートされているすべてのチャネルで、RRM によるチャネルスキャンが実行されます。使用国で有効でないチャネルも対象となります。
  - [Country]：使用国内のデータチャネルのみで、RRM によるチャネルスキャンが実行されます。これはデフォルト値です。
  - [DCA]：RRM チャネルスキャンは、DCA アルゴリズムによって使用されるチャネルセットでのみ発生します。

- [Neighbor Discover Type] ドロップダウンリストから、ネイバー探索タイプを選択します。デフォルトでは、モードは [transparent] に設定されます。
  - [transparent]：ネイバー探索タイプを「transparent」に設定します。パケットはそのまま送信されます。
  - [protected]：ネイバー探索タイプを「protected」に設定します。パケットが暗号化されます。

ステップ 10 [Coverage] タブで、[Global Coverage Hole Detection Enabled] トグルボタンをクリックして、カバレッジホールの検出を有効にします。デフォルトで、この値が選択されています。

カバレッジホールの検出を有効にすると、カバレッジが不完全な領域に位置する可能性のあるクライアントを持つ AP があるかどうかを、AP から受信したデータに基づいて Cisco ワイヤレスコントローラが自動的に判断します。

ステップ 11 **[Save]** をクリックします。

作成した設計インスタンスが [Design Instances] ウィンドウの [RRM General Configuration - Model Configs] 領域に表示されます。

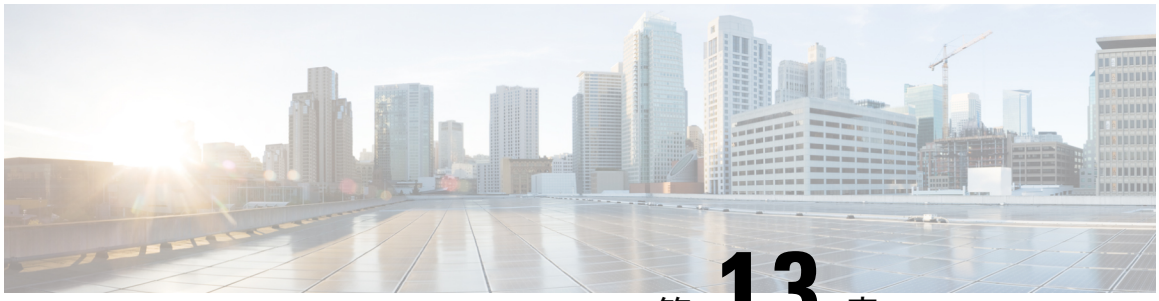
ステップ 12 設計を編集するには、編集する設計の名前の横にあるチェックボックスをオンにして [Edit] をクリックします。変更を加えたら、[Save] をクリックします。

ステップ 13 ワイヤレスコントローラに展開できるようにするために、作成した設定の設計をネットワークプロファイルに関連付けます。メニューアイコン（☰）をクリックして、**[Design]** > **[Network Profiles]** の順に選択します。

詳細については、ワイヤレス用のネットワークプロファイルの作成（304ページ）を参照してください。

ステップ 14 ネットワークプロファイルで指定されたモデル設定設計をネットワークデバイスにプロビジョニングします。メニューアイコン（☰）をクリックして、**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。

詳細については、Cisco AireOS コントローラのプロビジョニング （422 ページ）を参照してください。



第 13 章

ソフトウェア イメージの管理

イメージ リポジトリについて

Cisco DNA Center は、ネットワークにあるデバイスのすべてのソフトウェアイメージとソフトウェア メンテナンス アップデート（SMU）、サブパッケージ、ROMMON イメージなどを保存します。イメージ リポジトリには次の機能があります。

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

イメージリポジトリ機能を使用する前に、Cisco Catalyst 3000、4000、および 6000 などの古いデバイスで Transport Layer Security（TLS）プロトコルを有効にする必要があります。システムアップグレード後は、TLS を再度有効にする必要があります。詳細については、『Cisco DNA Center 管理者ガイド』[英語] の「Cisco DNA Center のセキュリティの構成」を参照してください。

（注） リリース 2.3.3 以降、Cisco DNA Center では、IE3x00 シリーズおよび IE9x00 シリーズ スイッチのソフトウェアイメージ管理（SWIM）およびソフトウェア メンテナンスアップデート（SMU）のプライマリブートオプションとして内部ブートフラッシュのみをサポートします。

Cisco DNA Center の以前のリリース（リリース 2.3.3 より前）があり、ネットワーク内の IE3x00 または IE9x00 デバイスがセキュアデジタル（SD）フラッシュメモリモジュールですでに起動されている場合は、**boot flash-primary** コマンドを使用して、内部ブートフラッシュをデバイスのプライマリブートオプションとして設定してください。

実行コンフィギュレーションを SD フラッシュからブートフラッシュに保存して同期するには、**sync** コマンドを使用します。

ソフトウェア イメージの整合性検証

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

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

ソフトウェアイメージの表示

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

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

[Image Repository] ウィンドウには、デバイスファミリ、ソフトウェアイメージ、およびアドバイザリに関する詳細が要約されています。

- [SUMMARY]：デバイスファミリ、デバイス、およびイメージリポジトリにゴールデンイメージがないデバイスファミリの数を表示します。
- [TOTAL IMAGES]：イメージリポジトリ内の実行中のイメージ、インポートされたイメージ、およびゴールデンイメージの数を表示します。
- [ADVISORIES]：クリティカルおよび高のアドバイザリの数を表示します。

[Image Families] テーブルには、デバイスファミリごとに [Family Name]、[Devices]、[Images]、[Advisories]、および [Images Marked Golden] の詳細が表示されます。

（注） cisco.com のログイン情報が設定されていない場合、警告アラートが表示されます。

ステップ 2 ウィンドウの上部にある [Routers]、[Switches]、[Wireless Controllers]、[Security and VPN]、[Sensors]、または [Virtual Devices] をクリックするか、[Image Families] テーブルの検索またはフィルタアイコンをクリックして、デバイスファミリをフィルタリングします。

デフォルトでは、[Image Repository] ウィンドウにすべてのデバイスファミリが表示されます。

ステップ 3 [Sync Updates] をクリックし、後続の警告メッセージで [OK] をクリックして、Cisco DNA Center のすべての管理対象デバイスの cisco.com からのイメージ情報を同期します。

Cisco.com のログイン情報が設定されていない場合は、ログイン情報を指定するよう求められます。

[Show Tasks] でタスクの進捗状況を確認することができます。タスクが成功すると、すべてのデバイスファミリのイメージ情報が更新されます。

（注） イメージ情報を取得できるのは 1 時間に 1 回のみです。

ステップ 4 [Show Tasks] をクリックして、ソフトウェアイメージに関連するすべてのタスクのステータスを表示します。

[Recent Tasks] スライドインペインには、最近の 50 件のタスクのステータスが表示されます。[Task Status] ドロップダウンリストから、[All]、[Failed]、[In-Progress]、または [Successful] を選択して、ステータスに基づいてタスクをフィルタリングします。

ステップ 5 [Import Image] をクリックして、ソフトウェアイメージまたはソフトウェア イメージ アップデートをインポートします。詳細については、ソフトウェアイメージのインポート（360ページ）を参照してください。

ステップ 6 [Update Devices] をクリックして、インベントリ内のデバイスを更新します。

[Inventory] ウィンドウでデバイスを選択し、**[Actions]** > **[Inventory]**に移動して、インベントリ内のデバイスを編集、再同期、再起動、または削除します。

ステップ 7 [Image Families] テーブルで、[Imported Images] をクリックして、インポートされたソフトウェアイメージの詳細を表示します。[Imported Images] 行は、常にテーブルの最初の行として表示されます。

[Imported Image Family] ウィンドウの [Images] テーブルには、インポートされたすべてのソフトウェアイメージの [Image Name]、[Version]、[Device Series Assigned]、および [Action] が表示されます。

[Action] 列で [Assign] をクリックして、ソフトウェアイメージをデバイスファミリに割り当てます。詳細については、デバイスファミリへのソフトウェアイメージの割り当て（361 ページ）を参照してください。

ステップ 8 [Image Families] テーブルで、デバイスファミリの名前をクリックして、特定のデバイスファミリに関連付けられているすべてのソフトウェアイメージを表示します。

[Image Family] ウィンドウの [Images] テーブルには、すべてのソフトウェアイメージの [Image Name]、[Version]、[Devices]、[Advisories]、[Golden Image] および [Device Roles & Tags] が表示されます。

[Image Family] ウィンドウで、次の手順を実行します。

a) 左側のペインで、[Roles & Tags]、[Major Versions]、または [Golden Images] をクリックするか、[Images] テーブルの検索またはフィルタアイコンをクリックして、ソフトウェアイメージをフィルタリングします。

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

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

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

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

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

サブパッケージはゴールデンとしてタグ付けすることはできません。

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

c) [Device(s)] 列でデバイスの数をクリックすると、そのイメージを使用しているデバイスが表示されます。

d) [Advisory] 列で、[Critical] または [High] のアドバイザリの数をクリックして、特定のソフトウェアイメージのアドバイザリを表示します。

[Image Advisory] スライドインペインには、ソフトウェアイメージの**ファミリ名**、**バージョン**、および**アドバイザリ**が表示されます。アドバイザリは、[Critical]、[High]、[Medium]、[Low]、および [Informational] に分類されます。

[CRITICAL]、[HIGH]、または [MEDIUM] をクリックして、各カテゴリに固有のアドバイザリを表示します。

アドバイザリを修正するには、次の手順を実行します。

1. [Fix Advisories] をクリックします。

   [Image Update] ウィンドウが表示されます。

2. デバイスを更新する推奨ソフトウェアイメージを選択します。

   推奨されるソフトウェアイメージがイメージリポジトリにない場合は、cisco.com からダウンロードできます。

3. [Download and Mark Golden] をクリックします。

   [Download Image] ダイアログボックスで、次のいずれかを実行します。

- [Mark the image as gold after download] チェックボックスをオン（デフォルト）のままにします。その後、[Download] をクリックします。ソフトウェアイメージがダウンロードされ、ゴールデンとしてマークされます。
- [Mark the image as golden after download] チェックボックスをオフにし、[Download] をクリックします。ソフトウェアイメージがリポジトリにダウンロードされますが、ゴールデンとはマークされません。

4. [OK] をクリックします。

   ソフトウェアイメージがダウンロードされます。[Show Tasks] で進捗状況を確認することができます。

e) [Golden Image] 列で、星のアイコンをクリックして、ソフトウェアイメージをゴールデンとして指定します。

ゴールデンとして指定したソフトウェアイメージが Cisco DNA Center リポジトリにまだアップロードされていない場合は、ダウンロードアイコンをクリックして、ソフトウェアイメージをインポートします。

ゴールデンイメージの詳細については、ゴールデン ソフトウェアのイメージについて （363 ページ）およびゴールデン ソフトウェア イメージの指定 （363 ページ）を参照してください。

f) [Device Roles & Tags] 列で、次の手順を実行します。

1. 編集アイコンをクリックして、デバイスロールやタグを割り当てます。

   注：デバイスロールやタグを割り当てるには、対応するソフトウェアイメージがインポートされている必要があります。

2. [Assign Device Roles & Tags] スライドインペインで、これがゴールデン ソフトウェア イメージであることを示すデバイスロールとタグを選択します。

   （注）
   - ソフトウェアイメージに両方が選択されている場合、「デバイスタグ」は「デバイスロール」よりも優先されます。
   - **[Provision]** > **[Network Devices]** > **[Inventory]** で新しいデバイスタグを作成して割り当てることができます。

3. [Save] をクリックします。

推奨されるソフトウェア イメージの使用

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

（注） シスコが推奨する最新のソフトウェアイメージのみをダウンロードできます。

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

ステップ 2 cisco.com に接続するための正しいログイン情報が入力されていることを確認します。

ステップ 3 メニューアイコン（☰）をクリックして、**[Design]** > **[Image Repository]**。

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

ステップ 4 推奨のイメージをゴールデンとして指定します。詳細については、「ゴールデン ソフトウェア イメージの指定 （363 ページ）」を参照してください。

ステップ 5 推奨のソフトウェア イメージをネットワーク内のデバイスにプッシュします。詳細については、「ソフトウェア イメージのプロビジョニング （366 ページ）」を参照してください。

ソフトウェア イメージのインポート

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

インポートされたイメージは、特定のデバイスファミリに存在するさまざまなスーパーバイザに基づいて分類されます。異なるスーパーバイザによる分類では、Cisco Catalyst 9400 シリーズ ファミリのみがサポートされます。

FTP を使用して FTP サーバからイメージをインポートする場合は、FTP 標準を使用します。

```
ftp://username:password@ip_or_hostname/path
```

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

ステップ 2 [Import Images] をクリックします。

ステップ 3 [Import Image/Add-on] スライドインペインで、[Select from computer] オプションボタンをクリックし、[Choose a file] をクリックして、ローカルに保存されているソフトウェアイメージまたはソフトウェアイメージ更新に移動します。

または、[Enter URL] オプションボタンをクリックして、[Enter Image URL] フィールドに、ソフトウェアイメージのインポート元またはソフトウェアイメージの更新元となる HTTP または FTP を指定するイメージ URL を入力します。

（注） ソフトウェアイメージは、連邦情報処理標準（FIPS）に準拠しています。Cisco DNA Center で FIPS モードが有効になっている場合、URL からイメージをインポートすることはできません。コンピュータまたは cisco.com からイメージをインポートします。

ステップ 4 インポートするイメージがサードパーティ（シスコ以外）ベンダー向けの場合、[Source] で [Third Party]を選択します。[Application Type] を選択して、デバイスの [Family] を示し、[Vendor] を特定します。

ステップ 5 [Import] をクリックします。

ウィンドウにインポートの進行が表示されます。

ステップ 6 **[タスクの表示（Show Tasks）]** をクリックして、イメージが正常にインポートされたことを確認します。

SMU をインポートした場合、Cisco DNA Center は自動的に SMU を適切なソフトウェア イメージに適用し、対応するソフトウェア イメージの下に **[Add-On]** リンクが表示されます。

ステップ 7 **[Add-On]** リンクをクリックすると、SMU が表示されます。

ステップ 8 [Device Role] フィールドで、この SMU をゴールデンとしてマークするロールを選択します。ゴールデン ソフトウェア イメージの指定 （363 ページ）を参照してください。

SMU をゴールデンとしてマークするには、事前に対応するソフトウェアイメージをゴールデンとしてマークしている必要があります。

（注） Cisco DNA Center では、FMC によって管理される FTD デバイスのソフトウェアイメージをインポートすることはできません。インベントリに追加した FMC が「Managed」状態になると、FMC に存在するソフトウェアイメージがイメージリポジトリに表示され、デバイスファミリに基づいて分類されます。

デバイスファミリへのソフトウェアイメージの割り当て

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

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

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

ステップ 2 [Imported Images] をクリックします。

ステップ 3 対応するイメージ名の行の [Assign] をクリックします。

ステップ 4 [Assign Device Family] ウィンドウで、[Device Series from Cisco.com] または [All Device Series] を選択し、イメージのマッピング先の [Assign] リンクをクリックします。

注：Cisco.com ログイン情報が設定されていない場合は、**[System]** > **[Settings]** > **[Cisco.com Credentials]** の順に選択して、ログイン情報を指定します。

ステップ 5 グローバル階層から適切なサイトを選択して [Assign] をクリックし、[Save] をクリックします。

ステップ 6 イメージの割り当てを解除するには、グローバル階層からサイトを選択し、[Action]列の [Unassign] リンクをクリックします。

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

デバイスファミリがゴールデンイメージとしてマークされている場合、そのイメージをデバイスファミリから削除することはできません。

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

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

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

デバイスのソフトウェアイメージをインストールモードでアップロード

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

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

ステップ 2 [Image Name] カラムで、[Install Mode] で実行中のデバイスのソフトウェアイメージを検索します。

ステップ 3 [インポート（Import）] をクリックして、インストール モードであるイメージのバイナリ ソフトウェア イメージ ファイルをアップロードします。

ステップ 4 [ファイルの選択（Choose File）] をクリックしてローカルに保存されているソフトウェア イメージへ移動するか、または [イメージのURLを入力（Enter image URL）] でソフトウェア イメージのインポート元となる HTTP または FTP を指定します。

ステップ 5 [Import] をクリックします。

ウィンドウにインポートの進行が表示されます。

ステップ 6 [タスクの表示（Show Tasks）]をクリックして、インポートしたソフトウェアイメージが、正常にインポートされ、Cisco DNA Center リポジトリに追加されたことを示す緑色であることを確認します。

ステップ 7 [Refresh] をクリックします。

[Image Repository] ウィンドウを更新します。Cisco DNA Centerにソフトウェアイメージが表示され、[Golden Image] および [Device Role] 列がグレー表示ではなくなります。

ゴールデン ソフトウェアのイメージについて

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

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

ゴールデン ソフトウェア イメージの指定

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

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

デバイス タイプに従ってソフトウェア イメージが表示されます。

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

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

ステップ 4 ゴールデンとして指定したソフトウェアイメージが Cisco DNA Center リポジトリにすでにアップロードされている場合は、[Golden Image] 列のスターアイコンをクリックします。

ソフトウェアイメージがゴールデンとしてマークされます。

ステップ 5 ゴールデンとして指定したソフトウェアイメージが Cisco DNA Center リポジトリにまだアップロードされていない場合は、[Golden Image] 列のダウンロードアイコンをクリックします。

この処理には、しばらく時間がかかる場合があります。

（注）　デバイスからソフトウェアイメージをインポートすることはできません。

ステップ 6 [Download Image] ダイアログボックスで、次のいずれかを実行します。

- [Mark the image as golden after download] チェックボックスはデフォルトのオンのままにし、[Download] をクリックします。ソフトウェアイメージがダウンロードされ、ゴールデンとしてマークされます。

  （注）　Cisco.com のログイン情報が設定されていない場合は、ログイン情報を指定するよう求められます。

  進行中のソフトウェアイメージのダウンロードが [Device Role] 列に表示されます。

  ソフトウェアイメージがダウンロードされ、ゴールデンとして正常にマークされると、スターアイコンが金色に変わります。ソフトウェアイメージのダウンロードが失敗すると、スターアイコンが赤色に変わり、[Please Retry] ステータスが表示されます。

- [Mark the image as golden after download] チェックボックスをオフにし、[Download] をクリックします。ソフトウェアイメージがリポジトリにダウンロードされますが、ゴールデンとはマークされません。

ステップ 7 **[Device Role]** 列で、ゴールデン イメージを指定するデバイス ロールを選択します。同じデバイス ファミリのデバイスを所有していたとしても、各デバイス ロールに異なるゴールデン イメージを指定することができます。物理イメージのデバイス ロールのみ選択できます。仮想イメージは選択できないことに注意してください。

イメージ配信サーバの設定

イメージ配信サーバーは、ソフトウェアイメージの保管と配信に役立ちます。ソフトウェアイメージを配信するように外部イメージ配信サーバを設定できます。また、新しく追加されたイメージ配信サーバーに 1 つ以上のプロトコルを設定できます。

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

ステップ 2 [Device Settings] ドロップダウンリストから、[Image Distribution Servers] を選択します。

ステップ 3 [Image Distribution Servers] ウィンドウで、[Servers] をクリックします。

[Image Distribution Servers] テーブルには、イメージ配信サーバーのホスト、ユーザー名、SFTP、SCP、および接続の詳細が表示されます。

ステップ 4 [Add] をクリックして新しいイメージ配信サーバを追加します。

[Add a New Image Distribution Server] スライドインペインが表示されます。

ステップ 5 イメージ配信サーバについて、次の項目を設定します。

- [Host]：イメージ配信サーバーのホスト名または IP アドレスを入力します。

- [Root Location]：ファイル転送にルートディレクトリを使用する場合は、[Use root directory for file transfers] チェックボックスをオンにします。それ以外の場合は、[Use root directory for file transfers] チェックボックスをオフにしてルートの場所を入力します。

  （注） Cisco AireOS コントローラの場合、設定されたパスが 16 文字を超えると、イメージの配信は失敗します。

- [SFTP and SCP] 領域を展開します。
- [Username]：イメージ配信サーバーへのログインに使用されるユーザー名を入力します。ユーザー名は、サーバーの作業ルートディレクトリに対する読み取り/書き込み権限を持ちます。
- [パスワード]：イメージ配信サーバへのログインに使用されるパスワード。
- [ポート番号]：イメージ配信サーバーが実行されているポート番号を入力します。

ステップ 6 [**Save**] をクリックします。

ステップ 7 （オプション）設定を編集するには、[Action] 列で対応するイメージ配信サーバーの [Edit] アイコンをクリックし、[Edit] ウィンドウで必要な変更を行って [Save] をクリックします。

ステップ 8 （オプション）イメージ配信サーバーを削除するには、[Action] 列で対応するイメージ配信サーバーの [Delete] アイコンをクリックし、[Delete] をクリックします。

イメージ配信サーバーのプロトコル順序の変更

イメージ配信サーバーのプロトコル順序を変更できます。プロトコルの順序は、イメージ配信サーバーで検証チェックを実行するのに役立ちます。デフォルトでは、ソフトウェアイメージはプロトコル順序の最初のプロトコルを使用して配信されます。

ステップ 1 メニューアイコン（☰）をクリックして、**[System]** > **[Settings]** > **[Device Settings]** > **[Image Distribution Servers]**。

ステップ 2 [Image Distribution Servers] ウィンドウで、[Preferences] をクリックします。

デフォルトのプロトコル順序が表示されます。

ステップ 3 [On/Off] トグルボタンをクリックしてプロトコルを有効または無効にします。

（注） イメージを配信するには HTTPS または SCP プロトコルを有効にする必要があります。すべてのプロトコル順序で SFTP プロトコルを有効にする必要があります。

HTTPS プロトコルが無効になっているか、HTTPS プロトコル使用時にイメージ配信に失敗した場合、ソフトウェアイメージは SCP プロトコルを使用して配信されます。

ステップ 4 プロトコルをドラッグアンドドロップしてプロトコルの順序を変更します。

ステップ 5 [Save] をクリックします。

サイトへのイメージ配信サーバの追加

地理的に異なる地域にある SFTP サーバを、サイト、ビルディング、およびフロアに関連付けることができます。ネットワーク階層内のすべてのデバイスは、ネットワークのアップグレードの際、関連付けられたイメージ配信サーバを使用します。

始める前に

イメージ配信サーバを設定する必要があります。『イメージ配信サーバの設定（364ページ）』を参照してください。

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

ステップ 2 左ペインで、イメージ配信サーバを関連付けるサイトを選択します。

ステップ 3 [サーバの追加（Add Servers）] をクリックします。

ステップ 4 [Add Servers] ウィンドウで、[Image Distribution] チェックボックスをオンにします。

ステップ 5 [OK] をクリックします。

ステップ 6 [Primary] ドロップダウンリストをクリックし、プライマリとして設定するイメージ配信サーバを選択します。

ステップ 7 [Secondary] ドロップダウンリストをクリックし、セカンダリとして設定するイメージ配信サーバを選択します。

ステップ 8 [Save] をクリックします。

ソフトウェア イメージのプロビジョニング

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

（注） 複数のデバイスに対して事前チェックを実行できます。

Cisco DNA Center は、各デバイスのソフトウェアイメージを、その固有のデバイスタイプに対してゴールデンと指定したイメージと比較します。デバイスのソフトウェアイメージとゴールデンイメージに違いがある場合、Cisco DNA Center はデバイスのソフトウェアイメージを無効とします。これらのデバイスに対するアップグレード準備の事前チェックがトリガーされま

す。すべての事前チェックをクリアしたら、新しいイメージをデバイスに配信（コピー）し、有効化（新しいイメージを実行中のイメージにすることが）できます。新しいイメージの有効化には、デバイスの再起動が必要です。再起動によって現在のネットワークアクティビティが中断される可能性があるため、後でプロセスをスケジュールすることができます。

そのデバイスタイプにゴールデンイメージを指定していない場合、そのデバイスのイメージは更新できません。『ゴールデン ソフトウェア イメージの指定（363 ページ）』を参照してください。

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

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

（注） デバイスの事前チェックが成功すると、[Software Image] 列の [Outdated] リンクに緑色のチェックマークが付きます。デバイスのアップグレードを準備するための事前チェックでいずれかに失敗した場合、[Outdated] リンクのマークが赤色に変わり、そのデバイスのソフトウェアイメージを更新できなくなります。先に進む前に [Outdated] リンクをクリックし、エラーを修正します。「デバイスのアップグレードの準備の事前チェックリスト」を参照してください。

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

[Image Upgrade] ウィンドウが表示されます。

ステップ 4 [Analyze Selection]：アップグレードするデバイスを選択し、[Next] をクリックします。

ステップ 5 [Distribute]：[Now] をクリックしてすぐに配信を開始するか、[Later] をクリックして特定の時間に配信のスケジュールを設定します。

現在のワークフローで実行する検証ツールを選択し、新しいカスタムチェックを追加するには、次の手順を実行します。

a) 情報アイコンにマウスポインタを合わせると、検証に使用される検証基準と CLI コマンドが表示されます。

b) オンとオフを切り替えるトグルボタンをクリックして、現在のワークフローで実行しない検証ツールをオフにします。

c) （任意）新しいカスタム事前チェックおよび事後チェックを追加するには、次の手順を実行します。

- [Add a New Check] リンクをクリックして、[Add a New Custom Check] ウィンドウを開きます。
- カスタムチェックの名前を [Name] に入力します。
- [When] ドロップダウン矢印をクリックし、事前か事後またはその両方を選択します。
- [Select a Test Device] ドロップダウン矢印をクリックし、カスタムチェックを実行するデバイスを選択します。
- [Open Command Runner] をクリックし、CLI コマンドを入力します。
- [Additional Criteria] 領域を展開します。

- [Operation] ドロップダウン矢印をクリックし、[Distribution] を選択します。
- [Device Series] ドロップダウン矢印をクリックし、カスタムチェックを実行するデバイスシリーズを選択します。
- **[Save]** をクリックします。
- カスタムチェックを編集する場合は、対応する [More] アイコンをクリックし、[Edit] を選択して、必要な変更を行い、[Save] をクリックします。
- カスタムチェックを削除する場合は、対応する [More] アイコンをクリックし、[Delete] を選択して、[Confirm Delete] メッセージで [Delete] をクリックします。

（注）
- 外部イメージ配信サーバをネットワーク階層に関連付けた場合、ネットワーク階層下のすべてのデバイスにイメージ配信サーバからイメージが配信されます。サイトへのイメージ配信サーバの追加 （366 ページ）を参照してください。
- 選択したデバイスにイメージが配信されている場合は、[Next] をクリックします。
- [SWIM Events for ITSM (ServiceNow)] バンドルが有効になっている場合は、後でイメージを更新（配布およびアクティブ化）する必要があります。イメージを更新するために [Now] をクリックしないでください。ここでイメージを更新する必要がある場合は、まずバンドルとその統合ワークフロー（ServiceNowでのイメージ更新スケジュールの承認）を無効にする必要があります。バンドルにアクセスするには、[Platform] > [Manage] > [Bundles] > [SWIM Events for ITSM（ServiceNow）] の順に選択します。[SWIM Events for ITSM（ServiceNow）] ウィンドウの [Disable] ボタンをクリックします。バンドルとワークフローを無効にするプロセスには数秒かかるため、イメージの更新に進む前に数秒待ちます。

ステップ 6 **[Next]** をクリックします。

ステップ 7 [Activate]：[Now] をクリックして直ちに有効化を開始するか、[Later] をクリックして特定の時間に有効化をスケジュールします。

[FLASH CLEANUP]：実行中のソフトウェアイメージのみを保存し、デバイスに保存されている以前のソフトウェアイメージをすべて削除します。

[Initiate Flash Cleanup after Activation] チェックボックスをオンにして、デバイスに保存されている以前のソフトウェアイメージをすべて削除します。

現在のワークフローで実行する検証ツールを選択し、新しいカスタムチェックを追加するには、次の手順を実行します。

a) 情報アイコンにマウスポインタを合わせると、検証に使用される検証基準と CLI コマンドが表示されます。
b) オンとオフを切り替えるトグルボタンをクリックして、現在のワークフローで実行しない検証ツールをオフにします。
c) （任意）新しいカスタム事前チェックおよび事後チェックを追加するには、次の手順を実行します。
   - [Add a New Check] リンクをクリックして、[Add a New Custom Check] ウィンドウを開きます。

- カスタムチェックの名前を [Name] に入力します。
- [When] ドロップダウン矢印をクリックし、事前か事後またはその両方を選択します。
- [Select a Test Device] ドロップダウン矢印をクリックし、カスタムチェックを実行するデバイスを選択します。
- [Open Command Runner] をクリックし、CLI コマンドを入力します。
- [Additional Criteria] 領域を展開します。
- [Operation] ドロップダウン矢印をクリックし、[Activation] を選択します。
- [Device Series] ドロップダウン矢印をクリックし、カスタムチェックを実行するデバイスシリーズを選択します。
- **[Save]** をクリックします。
- カスタムチェックを編集する場合は、対応する [More] アイコンをクリックし、[Edit] を選択して、必要な変更を行い、[Save] をクリックします。
- カスタムチェックを削除する場合は、対応する [More] アイコンをクリックし、[Delete] を選択して、[Confirm Delete] メッセージで [Delete] をクリックします。

ステップ 8 [Next] をクリックします。

ステップ 9 [Summary] ウィンドウで、イメージのアップグレード設定を確認します。変更を加える場合は [Back] をクリックし、それ以外の場合は [Submit] をクリックします。

ステップ 10 [Actions] ドロップダウンリストから、**[Software Images]** > **[Image Update Status]** の順に選択し、更新ステータスを確認します。

ISSU 互換性マトリクスのインポート

In-Service Software Upgrade（ISSU）は、再起動なしで、またはサービスの中断を最小限に抑えて、デバイス上のイメージをアップグレードするプロセスです。Catalyst スイッチの Cisco IOS XE ISSU 互換性マトリックスの例については、https://software.cisco.com/download/home/286316172/type/286326638/release/17.7.1 を参照してください。ISSU を使用してデバイスをアップグレードする際は、ISSU 互換性マトリックスを Cisco DNA Center にダウンロードしてインポートすることができます。

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

ステップ 2 [Import Images] をクリックします。

ステップ 3 [Import Image/Add-on] スライドインペインで、[Select ISSU compatibility matrix] オプションボタンをクリックし、[Choose a file] をクリックして、ローカルに保存されている ISSU 互換性マトリックスファイルに移動します。

ステップ 4 [Import] をクリックします。

ステップ 5 [Show Tasks] をクリックして ISSU 互換性マトリクスファイルのインポートステータスを表示します。

ISSU を使用したソフトウェアイメージのアップグレード

In-Service Software Upgrade（ISSU）を使用してデバイスをアップグレードすると、再起動する必要がなくなり、サービスの中断が減少します。

始める前に

ISSU を使用してデバイスをアップグレードする前に、ISSU 互換性マトリクスファイルをインポートする必要があります。ISSU 互換性マトリクスのインポート （369 ページ）を参照してください。

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

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

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

[Image Upgrade] ウィンドウが表示されます。

ステップ 4 [Analyze Selection] ウィンドウで、ISSU アップグレードを有効にします。

a) ISSU でアップグレードするデバイスを選択します。

（注） [To Image] 列には ISSU 検証ステータスが表示されます。

- **オレンジ色で表示される ISSU**：選択したイメージに ISSU との互換性がないため、ISSU の検証に失敗しました。
- **灰色で表示される ISSU**：ISSU の検証が成功し、デバイスは ISSU をサポートしています。

b) [ISSU] ドロップダウンリストから [Enable ISSU Upgrade] を選択します。

c) [Next] をクリックします。

ステップ 5 [Distribute] ウィンドウから [Now] をクリックして即座にイメージ配信を開始するか、[Later] をクリックして特定の時間に配信をスケジュールします。

現在のワークフローで実行する検証ツールを選択し、新しいカスタムチェックを追加するには、次の手順を実行します。

a) 情報アイコンにカーソルを合わせると、検証に使用される検証基準と CLI コマンドが表示されます。

b) トグルボタンをクリックして、現在のワークフローで実行しない検証ツールをオフにします。

c) （任意）新しいカスタム事前チェックおよび事後チェックを追加するには、次の手順を実行します。

- [Add a New Check] をクリックして、[Add a New Custom Check] ウィンドウを開きます。

- カスタムチェックの名前を [Name] に入力します。
- [When] ドロップダウンリストをクリックし、事前か事後またはその両方を選択します。
- [Select a Test Device] ドロップダウンリストから、カスタムチェックを実行するデバイスを選択します。
- [Open Command Runner] をクリックし、CLI コマンドを入力します。
- [Additional Criteria] 領域を展開します。
- [Operation] ドロップダウン矢印をクリックし、[Distribution] を選択します。
- [Device Series] ドロップダウン矢印をクリックし、カスタムチェックを実行するデバイスシリーズを選択します。
- **[Save]** をクリックします。
- カスタムチェックを編集する場合は、対応する [More] アイコンをクリックし、[Edit] を選択して、必要な変更を行い、[Save] をクリックします。
- カスタムチェックを削除する場合は、対応する [More] アイコンをクリックし、[Delete] を選択して、[Confirm Delete] メッセージで [Delete] をクリックします。

（注）
- ネットワーク階層に関連付けられている外部イメージ配信サーバーは、ネットワーク階層内のすべてのデバイスにイメージを配信します。サイトへのイメージ配信サーバの追加 （366 ページ）を参照してください。
- 選択したデバイスにイメージが配信されている場合は、[Next] をクリックします。
- [SWIM Events for ITSM (ServiceNow)] バンドルが有効になっている場合は、後でイメージを更新（配布およびアクティブ化）する必要があります。イメージを更新するために [Now] をクリックしないでください。

  ここでイメージを更新する必要がある場合は、まずバンドルとその統合ワークフロー（ServiceNow でのイメージ更新スケジュールの承認）を無効にする必要があります。バンドルにアクセスするには、[Platform] > [Manage] > [Bundles] > [SWIM Events for ITSM（ServiceNow）] の順に選択します。[SWIM Events for ITSM（ServiceNow）] ウィンドウの [Disable] ボタンをクリックします。バンドルとワークフローを無効にするプロセスには数秒かかるため、イメージを更新する前に数秒待ちます。

ステップ 6 [Next] をクリックします。

ステップ 7 [Activate] ウィンドウから、[Now] をクリックして直ちに有効化を開始するか、[Later] をクリックして特定の時間に有効化をスケジュールします。

[FLASH CLEANUP]：実行中のソフトウェアイメージのみを保存し、デバイスに保存されている以前のソフトウェアイメージをすべて削除します。

[Initiate Flash Cleanup after Activation] チェックボックスをオンにして、デバイスに保存されている以前のソフトウェアイメージをすべて削除します。

現在のワークフローで実行する検証ツールを選択し、新しいカスタムチェックを追加するには、次の手順を実行します。

a) 情報アイコンにカーソルを合わせると、検証に使用される検証基準とCLIコマンドが表示されます。
b) トグルボタンをクリックして、現在のワークフローで実行しない検証ツールをオフにします。
c) （任意）新しいカスタム事前チェックおよび事後チェックを追加するには、次の手順を実行します。
   - [Add a New Check] リンクをクリックして、[Add a New Custom Check] ウィンドウを開きます。
   - カスタムチェックの名前を [Name] に入力します。
   - [When] ドロップダウンリストをクリックし、必要に応じて事前か事後またはその両方を選択します。
   - [Select a Test Device] ドロップダウンリストをクリックし、カスタムチェックを実行するデバイスを選択します。
   - [Open Command Runner] をクリックし、CLI コマンドを入力します。
   - [Additional Criteria] 領域を展開します。
   - [Operation] ドロップダウンリストをクリックし、[Activation] を選択します。
   - [Device Series] ドロップダウンリストをクリックし、カスタムチェックを実行するデバイスシリーズを選択します。
   - **[Save]** をクリックします。
   - カスタムチェックを編集する場合は、対応する [More] アイコンをクリックし、[Edit] を選択して、必要な変更を行い、[Save] をクリックします。
   - カスタムチェックを削除する場合は、対応する [More] アイコンをクリックし、[Delete] を選択して、[Confirm Delete] メッセージで [Delete] をクリックします。

ステップ 8 [Next] をクリックします。

ステップ 9 [Summary] ページから、イメージのアップグレード設定を確認します。変更を加える場合は [Back] をクリックし、それ以外の場合は [Submit] をクリックします。

ステップ 10 [Actions] ドロップダウンリストから、**[Software Images]** > **[Image Update Status]** の順に選択し、更新ステータスを確認します。

デバイスのアップグレードの準備の事前チェック リスト

事前チェック	説明
ファイル転送のチェック	HTTPS と SCP を通じてデバイスに到達できるかどうかをチェックします。 プロトコルのデフォルトの順序は、HTTPSが先で、SCP はその後です。

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

イメージ更新ステータスの表示

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

ステップ 2 [Focus] ドロップダウンリストから [Software Images] を選択します。

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

デフォルトでは、[Image Update Status] ウィンドウにすべてのイメージ更新タスクが表示されます。

ステップ 4 更新ステータスに基づいてタスクをフィルタ処理するには、[In Progress]、[Success]、または [Failure] をクリックします。

ステップ 5 左側のペインで、[Task Names] または [Image Versions] をクリックして、操作またはイメージバージョンに基づいてタスクをフィルタ処理します。

[Status] 列には、タスクの現在のステータスが表示されます。進行中のタスクの場合、進捗状況バーにイメージ更新の進捗状況が示されます。

ステップ 6 デバイス名をクリックすると、タスクの詳細情報が表示されます。詳細については、イメージ更新ワークフローの表示 （374 ページ）を参照してください。

ステップ 7 [Upcoming Tasks] をクリックして、後で実行するようにスケジュールされているタスクを確認します。

[Upcoming Tasks] スライドインペインが表示されます。

ステップ 8 [Devices Scheduled] 列のデバイスの数をクリックして、イメージ更新タスクがスケジュールされているデバイスを確認します。

ステップ 9 チェックボックスをオンにしてタスクが失敗したデバイスを選択し、[Retry] をクリックしてイメージの更新を再試行します。

[Image Upgrade] ウィンドウが表示されます。このウィンドウから、イメージ更新タスクを今すぐ実行するように、または後で実行するようにスケジュールできます。詳細については、ソフトウェアイメージのプロビジョニング （366 ページ）を参照してください。

イメージ更新ワークフローの表示

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

ステップ 2 [Focus] ドロップダウンリストから [Software Images] を選択します。

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

ステップ 4 [Image Update Status] ウィンドウで、デバイスの名前をクリックして、イメージのアップグレードに関する詳細情報を表示します。

ステップ 5 [Operations] タブをクリックします。

スライドインペインには、[Distribution] および [Activation] 操作に関連付けられている各タスクのステータスと、各操作の完了にかかった時間が表示されます。

ステップ 6 [Distribution] を展開して、[Distribution] 操作に関連付けられている次のタスクのステータスと、各タスクの完了にかかった時間を表示します。

- [Verify Image Availability]（レガシーデバイスのみ）：イメージリポジトリ内のソフトウェアイメージを確認します。
- [Image Integrity Verification(KGV)]：ソフトウェアイメージのソフトウェアおよびハードウェア プラットフォームチェックサム値を、既知の正常値（KGV）でプラットフォームに対して識別されたチェックサム値と比較します。
- [Pre Distribution Operation]：ソフトウェアイメージ配布用に選択されたすべての事前チェックを実行します。
- [Distribution]：プライマリ外部イメージ配布サーバーを介してソフトウェアイメージを配布します。

  ソフトウェアイメージの配布がプライマリ外部イメージ配布サーバーを介して失敗した場合、ソフトウェアイメージはセカンダリイメージ配布サーバーを介して配布されます。配布が両方の外部サーバーを介して失敗した場合、ソフトウェアイメージは内部 Cisco DNA Center サーバーを介して配布されます。
- [Post Distribution Operation]：ソフトウェアイメージ配布用に選択されたすべての事後チェックを実行します。

- [Image Checksum Verification On Device]：デバイス上のソフトウェアイメージのチェックサム値を検証します。
- [Unpack Image]（Polaris のみ）：CLI で「install-add」コマンドを実行します。イメージの解凍は、イメージがインストールモードの場合にのみ実行されます。
- [AP Pre-Image Download]（アクセスポイントのみ）：デバイスに関連付けられたすべてのアクセスポイントの配布プロセスに関する詳細を表示します。

ステップ 7 [Activation] を展開して、[Activation] 操作に関連付けられている次のタスクのステータスと、各タスクの完了にかかった時間を表示します。

- [Pre Activation Operation]：ソフトウェア イメージ アクティベーション用に選択されたすべての事前チェックを実行します。
- [Image Activation]：CLI で「install-activate」コマンドを実行します。このステップでは、イメージのアクティベーションプロセスに関する詳細情報が表示されます。

  （注） Cisco Catalyst 9000 シリーズ スタック スイッチの場合、「スタックの検証」事前チェックにより、スイッチ内のすべてのスタックメンバーの状態が検証されます。スタックメンバーがゴールデンイメージを実行していない場合、「auto-upgrade」コマンドが実行されます。

- [Staggered AP Upgrade]（アクセスポイントのみ）：デバイスに関連付けられたすべてのアクセスポイントのアクティベーションプロセスに関する詳細を表示します。
- [Install Commit]（Polaris のみ）：CLI で「install-commit」コマンドを実行します。
- [Remove Inactive Images]：デバイスに保存されている以前のソフトウェアイメージをすべて削除し、実行中のイメージのみを保存します。
- [Collect Running Image Details]：実行中のイメージの詳細を収集します。
- [Verify Image Activation]：ソフトウェアイメージが適切にアップグレードされているかどうかを確認します。
- [Post Activation Operation]：ソフトウェア イメージ アクティベーション用に選択されたすべての事後チェックを実行します。

（注）
- IOS-XE ソフトウェアで実行されている Cisco Catalyst 9800 組み込みワイヤレス コントローラ デバイスおよび Cisco Catalyst 9000 シリーズ スイッチの場合、ソフトウェアイメージは（次の 3 つのコマンドを実行することにより）、**install-add**（配布でのイメージの解凍ステップ）、**install-activate**（アクティベーションでのイメージのアクティベーションステップ）、および **install-commit**（アクティベーションでのインストール コミット ステップ）の 3 つのステップでアップグレードされます。
- デバイスが非アクティブ状態の場合、CLI で最初に「install-add」コマンドが実行されます。続いて、「install-activate」および「install-commit」コマンドが実行されます。デバイスが未コミット状態の場合、「install-commit」コマンドが直接実行されます。
- 「install-activate」および「install-commit」コマンドは、アクティベーション中に別々のマイルストーンで順番に実行されるため、ユーザーは更新を中止、ロールバック、またはコミットできます。

ステップ 8 [タスク（Tasks）] タブをクリックします。

ステップ 9 [Tasks] タブには、タスクに関連付けられている事前チェックおよび事後チェックのステータスと詳細情報が表示されます。各スクリプトに対応する [Differences] 列の相違の数をクリックして、事前チェックと事後チェックの相違を確認します。

自動フラッシュクリーンアップ

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

- **自動フラッシュクリーンアップをサポートしているデバイスの場合**：フラッシュのチェックが失敗し、警告メッセージが表示されます。このようなデバイスの場合、十分な容量を確保するために、イメージの配信プロセス中に自動クリーンアッププロセスが試行されます。自動フラッシュクリーンアップの一環として、Cisco DNA Center は未使用の .bin、.pkg、および .conf ファイルを特定し、デバイスに十分な空き容量ができるまでそれらのファイルの削除を繰り返します。イメージの配信はフラッシュ クリーンアップ後に試行されます。削除されたファイルは **[System]** > **[Audit Logs]** で確認できます。

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

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

第 14 章

ネットワークデバイスのコンプライアンス監査

コンプライアンスの概要

コンプライアンスは、元のコンテンツに影響を与えることなく注入または再設定される可能性があるネットワークのインテント逸脱やアウトオブバンドの変更を特定するのに役立ちます。

ネットワーク管理者は、Cisco DNA Center でソフトウェアイメージ、PSIRT、ネットワークプロファイルなどコンプライアンスのさまざまな側面のコンプライアンス要件を満たさないデバイスを簡単に特定できます。

コンプライアンスチェックは、自動化することも、オンデマンドで実行することもできます。

- 自動コンプライアンスチェック：Cisco DNA Center でデバイスから収集された最新のデータを使用します。このコンプライアンスチェックは、インベントリやSWIMなどさまざまなサービスからのトラップと通知をリッスンして、データを評価します。
- 手動コンプライアンスチェック：Cisco DNA Center でユーザーが手動でコンプライアンスをトリガーできます。
- スケジュールされたコンプライアンスチェック：スケジュールされたコンプライアンスジョブは、毎週実行されるコンプライアンスチェック（毎週土曜日の午後 11 時に実行）です。

手動コンプライアンスの実行

Cisco DNA Center では、コンプライアンスチェックを手動でトリガーできます。

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

ステップ 2 一括してコンプライアンスチェックを行う場合は、次の手順を実行します。

a) 該当するすべてのデバイスを選択します。

b) [Actions] ドロップダウンリストから、**[Compliance]** > **[Run Compliance]** の順に選択します。

ステップ 3 デバイスごとにコンプライアンスチェックを行う場合は、次の手順を実行します。

a) コンプライアンスチェックを実行するデバイスを選択します。

b) [Actions] ドロップダウンリストから、**[Compliance]** > **[Run Compliance]** の順に選択します。

c) あるいは、[Compliance] 列（使用可能な場合）をクリックし、[Run Compliance] をクリックします。

ステップ 4 デバイスの最新のコンプライアンスステータスを表示するには、次の手順を実行します。

a) デバイスとインベントリを選択します。デバイス情報の再同期 （129 ページ）を参照してください。

b) [Actions] ドロップダウンリストから、**[Compliance]** > **[Run Compliance]** の順に選択します。

（注）
- 到達不能のデバイスやサポートされていないデバイスに対してコンプライアンスの実行をトリガーすることはできません。
- デバイスに対してコンプライアンスを手動で実行しない場合、コンプライアンスチェックはコンプライアンスのタイプに応じて一定期間後に実行されるように自動的にスケジュールされます。
- CLIテンプレートコンプライアンスは、実現されたテンプレートをデバイスの実行コンフィギュレーションと比較します。実行コンフィギュレーションは、デバイスで使用可能な最新のアーカイブから取得されます。

  イベントベースのアーカイブは、トラップを受信してから更新されるまでに少なくとも 5 分かかります。したがって、正確な結果を得るには、構成の変更後にコンプライアンスを手動で実行する前に、少なくとも 5 分間待つことをお勧めします。

コンプライアンスサマリーの表示

インベントリページには、デバイスごとにコンプライアンスの集約ステータスが表示されます。

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

コンプライアンス列には、デバイスごとに集約コンプライアンスステータスが表示されます。

ステップ 2 コンプライアンスステータスをクリックすると、コンプライアンス サマリー ウィンドウが開きます。このウィンドウには、選択したデバイスに適用可能な次のコンプライアンスチェックが表示されます。

- スタートアップ設定と実行中の設定
- ソフトウェア イメージ
- 重大なセキュリティの脆弱性
- ネットワークプロファイル
- ファブリック
- アプリケーションの可視性

（注） [Network Profile]、[Fabric]、および [Application Visibility] はオプションであり、デバイスが必要なデータでプロビジョニングされている場合にのみ表示されます。

デバイスのスタートアップ設定と実行中の設定の同期

デバイスのスタートアップ コンフィギュレーションと実行コンフィギュレーションに不一致がある場合、修復同期を実行して設定を一致させることができます。

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

ステップ 2 一括修復の場合は、次の手順を実行します。

a) 該当するすべてのデバイスを選択します。

b) [Actions] ドロップダウンリストから、**[Compliance]** > **[Sync Start vs Run Configuration]** の順に選択します。

デバイスごとの修復の場合は、次の手順を実行します。

a) 修復同期を実行するデバイスを選択します。

b) [Actions] ドロップダウンリストから、**[Compliance]** > **[Sync Start vs Run Configuration]** の順に選択します。または、コンプライアンスの列をクリックし、**[Compliance Summary]** > **[Startup vs Running Configuration]** > **[Sync Device Config]** の順に選択します。

ステップ 3 デバイスの修復ステータスを表示するには、次の手順を実行します。

a) メニューアイコン（☰）をクリックして、**[Provision]** > **[Inventory]** の順に選択します。

b) [Actions] ドロップダウンリストから、**[Compliance]** > **[Compliance Remedial Status]** の順に選択します。

コンプライアンスのタイプ

コンプライアンスタイプ	コンプライアンスチェック	コンプライアンスステータス
スタートアップ設定と実行中の設定	このコンプライアンスチェックは、デバイスのスタートアップ設定と実行中の設定が同期しているかどうかを識別するために役立ちます。デバイスのスタートアップ設定と実行中の設定が同期していない場合は、コンプライアンスがトリガーされ、アウトオブバンド変更の詳細レポートが表示されます。スタートアップ設定と実行中の設定の比較に関するコンプライアンスは、アウトオブバンド変更の 5 分以内にトリガーされます。	• [Noncompliant]：スタートアップ設定と実行中の設定は同じではありません。詳細ビューには、スタートアップと実行中との違いか、または実行中と以前の実行中との違いが表示されます。 • [Compliant]：スタートアップ設定と実行中の設定は同じです。 • [NA (Not Applicable)]：このコンプライアンスタイプのデバイス（AireOS など）はサポートされていません。
ソフトウェアイメージ	このコンプライアンスチェックは、Cisco DNA Center のタグ付きのゴールデンイメージがデバイスで実行されているかどうかをネットワーク管理者が確認するために役立ちます。これにより、デバイスのゴールデンイメージと実行中のイメージとの違いがわかります。ソフトウェアイメージに変更があると、遅延なくすぐにコンプライアンスチェックがトリガーされます。	• [Noncompliant]：デバイスは、デバイスファミリのタグ付きのゴールデンイメージを実行していません。 • [Compliant]：デバイスは、デバイスファミリのタグ付きのゴールデンイメージを実行しています。 • [NA (Not Applicable)]：選択したデバイスファミリではゴールデンイメージを使用できません。
重大なセキュリティ（PSIRT）	このコンプライアンスチェックでは、ネットワークデバイスが重大なセキュリティの脆弱性なしで実行されているかどうかを確認できます。	• [Noncompliant]：デバイスに重要なアドバイザリがあります。詳細レポートには、その他のさまざまな情報が表示されます。 • [Compliant]：デバイスに重大な脆弱性はありません。 • [NA (Not Applicable)]：Cisco DNA Center でネットワーク管理者がセキュリティ アドバイザリ スキャンを実行していないか、デバイスがサポートされていません。

コンプライアンスタイプ	コンプライアンスチェック	コンプライアンスステータス
ネットワークプロファイル	Cisco DNA Centerでは、ネットワークプロファイルでインテント設定を定義して、そのインテントをデバイスにプッシュできます。アウトオブバンド変更またはその他の変更のために任意の時点で違反が検出された場合、このチェックにより、それが識別されて、評価され、フラグが立てられます。違反は、コンプライアンス サマリー ウィンドウの [Network Profiles] でユーザーに対して表示されます。 （注） ネットワークプロファイルコンプライアンスは、ルータおよびワイヤレスコントローラに適用されます。	• [Noncompliant]：デバイスでプロファイルのインテント設定が実行されていません。 • [Compliant]：ネットワークプロファイルがデバイスに適用されており、同時に、Cisco DNA Center からプッシュされたデバイス設定がデバイスでアクティブに実行されています。 • [Error]：根本的なエラーのため、コンプライアンスがステータスを計算できませんでした。詳細については、エラーログを参照してください。
ファブリック（SDA） この機能はベータ版です。	ファブリックコンプライアンスは、ファブリックインテント違反（ファブリック関連の設定のアウトオブバンド変更など）の識別に役立ちます。	• [Noncompliant]：デバイスでインテント設定が実行されていません。 • [Compliant]：デバイスでインテント設定が実行されています。
アプリケーションの可視性	Cisco DNA Centerでは、アプリケーション可視性インテントを作成して、CBARおよびNBARを介してデバイスにプロビジョニングできます。デバイスにインテント違反がある場合、このチェックにより、違反が識別されて、評価され、[Application Visibility] ウィンドウに準拠または非準拠として表示されます。 自動コンプライアンスチェックは、トラップの受信の 5 時間後に実行されるようにスケジュールされます。	• [Noncompliant]：デバイスで CBAR/NBAR 設定が実行されていません。 • [Compliant]：デバイスで CBAR/NBAR のインテント設定が実行されています。
モデル設定	このコンプライアンスチェックにより、ネットワーク管理者は、モデル設定の設計意図との不一致をチェックできます。違反は、[Compliance Summary] ウィンドウの [Network Profiles] に表示されます。	• [Noncompliant]：モデル設定の属性の実際の値と意図された値が一致しません。 • [Compliant]：モデル設計の属性が意図した値に一致します。

コンプライアンスタイプ	コンプライアンスチェック	コンプライアンスステータス
CLIテンプレート	Cisco DNA Center ではネットワーク管理者は、CLI テンプレートをデバイスの実行コンフィギュレーションと比較できます。コンフィギュレーションの不一致にはフラグが立てられます。違反は、[Compliance Summary] ウィンドウの [Network Profiles] に表示されます。 CLI テンプレート コンプライアンス用の実行コンフィギュレーションは、デバイスで使用可能な最新のアーカイブから取得されます。イベントベースのアーカイブは、トラップを受信してから更新されるまでに少なくとも 5 分かかります。したがって、正確な結果を得るには、構成の変更後にコンプライアンスを手動で実行する前に、少なくとも 5 分間待つことをお勧めします。 （注） CLI テンプレート コンプライアンスにはいくつかの制限があります。「CLI テンプレート コンプライアンスの制限事項 （383 ページ）」を参照してください。	• [Noncompliant]：CLI テンプレートとデバイスの実行コンフィギュレーションが一致しません。 • [Compliant]：CLI テンプレートとデバイスの実行コンフィギュレーションの間に不一致はありません。

ネットワークデバイスのコンプライアンス監査レポートの生成

Cisco DNA Center では、個々のネットワークデバイスのコンプライアンスステータスを示す統合されたコンプライアンス監査レポートを取得できます。このレポートを使用すると、ネットワークを完全に可視化できます。

詳細については、『Cisco DNA Center Platform User Guide』の「Run a Compliance Report」を参照してください。

デバイスのアップグレード後のコンプライアンス動作

- デバイスのアップグレードが正常に完了すると、該当するすべてのデバイス（システムでコンプライアンスが実行されたことがないデバイス）のコンプライアンスチェックがトリガーされます。

- コンプライアンスは、[Startup vs Running] タイプを除き、インベントリに含まれるデバイスのステータスを計算して表示します。
- アップグレード後、[Startup vs Running] タイルに [NA] が「Configuration data is not available」というテキストとともに表示されます。
- アップグレードが正常に完了してから 1 日後に、1 回限りのスケジューラが実行され、デバイスで構成データを使用できるようになります。[Startup vs Running] タイルに、正しいステータス（[Compliant]/[Non-Compliant]）と詳細データが表示され始めます。
- トラップを受信すると、設定アーカイブサービスが構成データを収集し、コンプライアンスチェックが再度実行されます。

（注） アップグレードセットアップでは、[Flex Profile] インターフェイスのコンプライアンスの不一致は無視してください。インターフェイス名の場合、[1] が [management] にマッピングされます。

CLI テンプレート コンプライアンスの制限事項

Cisco DNA Center では、CLI テンプレートをデバイスの実行コンフィギュレーションと比較して、意図との不一致を識別することができます。次のコンパレータエンジンの制限事項に注意してください。

- CLI テンプレートコンパレータは、変数と値の大文字の使用をサポートしています。
- コマンドキーワードに大文字を使用しないでください。
- CLI テンプレートコンパレータは、エイリアスの使用をサポートしています。
- 非準拠としてフラグが設定されている省略または短縮コマンドの使用は避けてください。
- コマンドが欠落していて、それがセクションレベルにある場合、欠落しているコマンドに続くセクションレベルのコマンドにもフラグが付けられます。インデントを付けることで、この問題を回避できます。

  次に例を示します。

  インデントのないコマンドの CLI テンプレートコンパレータ出力：

実現されたテンプレート	実行コンフィギュレーション	出力
#interface Vlan111 #description SVI interface kan-111 #ip address 111.2.3.4 255.255.255.0 #ip helper-address 7.7.7.8 #no mop enabled #no mop sysid #!	#interface Vlan111 # description SVI interface kan-111 # ip address 111.2.3.4 255.255.255.0 # ip helper-address 7.7.7.7 # ip helper-address 7.7.7.8 # no mop enabled # no mop sysid #!	以下のコマンドが欠落としてマークされています。 # ip helper-address 7.7.7.7 # ip helper-address 7.7.7.8 # no mop enabled # no mop sysid

インデントを含むコマンドの CLI テンプレートコンパレータ出力：

実現されたテンプレート	実行コンフィギュレーション	出力
#interface Vlan111 # description SVI interface kan-111 # ip address 111.2.3.4 255.255.255.0 # ip helper-address 7.7.7.8 # no mop enabled # no mop sysid #!	#interface Vlan111 # description SVI interface kan-111 # ip address 111.2.3.4 255.255.255.0 # ip helper-address 7.7.7.7 # ip helper-address 7.7.7.8 # no mop enabled # no mop sysid #!	欠落しているコマンドのみに、コンパレータによってフラグが付けられます。 #ip helper-address 7.7.7.7

- 対話型およびイネーブルモードのコマンドは、コンプライアンスのために比較されません。コマンドですべてのオプションと値を指定することにより、対話型コマンドの代替形式を使用できます。

  たとえば、テンプレートコードが以下のように **#ENABLE** と **#INTERACTIVE** モードのコマンドを一緒に指定した場合、コマンドの比較は行われません。

```
#MODE_ENABLE
 #INTERACTIVE
    mkdir <IQ>Create directory<R>xyz
 #ENDS_INTERACTIVE
 #MODE_END_ENABLE
#end
```

- コンパレータによってフラグが設定されているコマンドでは範囲を使用しないでください。範囲は拡張形式で使用する必要があります。
- 同じテンプレート内のオーバーライドしているコマンドにフラグが付けられます。以下に示すように、コマンドを ignore - Compliance 構文で囲むことで、不一致を回避できます。

  次に例を示します。

実現されたテンプレート	実行コンフィギュレーション	出力

`#no banner motd #Welcome to Cisco .:|:.#`
`#banner motd #Welcome to Cisco .:|:.#`
	`#banner motd ^CWelcome to Cisco .:|:.^C`	• 以下のコマンドは、欠落としてフラグが付けられています。
		`no banner motd #Welcome to Cisco .:|:.#`
		• 実行中のコマンドはすでに上記のコマンドと比較されているため、以下のコマンドも欠落としてマークされています。
		`banner motd #Welcome to Cisco .:|:.#`

不一致を回避するには、次の操作を行います。

実現されたテンプレート	実行コンフィギュレーション	出力

`#! @start-ignore-compliance`
`#no banner motd #Welcome to Cisco .:|:#`
`#! @end-ignore-compliance`
`#banner motd #Welcome to Cisco .:|:.#`
	`#banner motd ^CWelcome to Cisco .:|:.^C`	構文で囲まれたコマンドは比較されないため、不一致はありません。

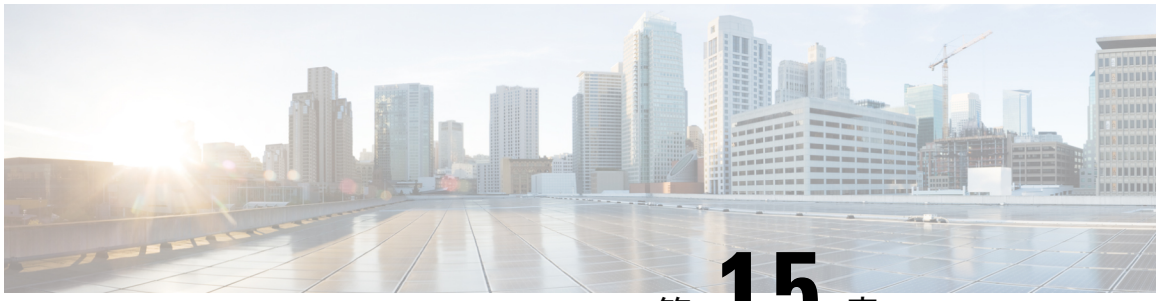
- Cisco IOS XE の以降のリリースでは、一部のデフォルトコマンドは、**show run** コマンドではなく、**show run all** コマンドが発行された場合にのみ表示されます。したがって、これらのコマンドは実行コンフィギュレーションに表示されず、非準拠としてフラグが設定されます。
- パスワードを含むコマンドは、デバイスに暗号化された形式で保存されるため、コンパレータによってフラグが設定されます。

（注） 次の構文でコマンドを囲むことで、パスワードを含むコマンドと一部のデフォルトコマンドの不一致を回避できます。

```
! @start-ignore-compliance
! @end-ignore-compliance
```

次に、変更が表示されるようにテンプレートを再プロビジョニングします。

CLIテンプレートとデバイスの実行コンフィギュレーションとの不一致を避けるために、実行コンフィギュレーションと同様のコマンドを使用することをお勧めします。



第 15 章

デバイスの診断コマンドを実行

コマンドランナーの概要

コマンドランナー ツールでは、選択したデバイスに診断CLIコマンドを送信できます。現在、**show** とその他の読み取り専用コマンドが許可されています。

デバイスの診断コマンドを実行

コマンド ランナーを使用すると、選択したデバイスで診断 CLI コマンドを実行し、結果のコマンド出力を表示できます。コマンドランナーは、スタンドアロン端末の一部として使用可能なショートカットのサブセットのみをサポートします。

始める前に

コマンドランナーの使用を開始するには、次の手順を実行します。

1. メニューアイコン（☰）をクリックして、**[System]** > **[Software Updates]** > **[Installed Apps]** の順に選択します。
2. [Command Runner] アプリケーションを検索し、[Install] をクリックします。
3. インストール後、ディスカバリ ジョブを実行し、デバイスに Cisco DNA Center を入力します。これらデバイスの一覧が表示され、ここから診断 CLI コマンドを実行します。

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

ステップ 2 [Command Runner] ウィンドウの [Search] フィールドで、ドロップダウン矢印をクリックして、[Device IP] または [Device Name] で検索します。

ステップ 3 診断 CLI コマンドを実行するデバイス（複数可）を選択します。

[Device List] に選択内容が表示されます。

ステップ 4 （任意） リストに追加する別のデバイスを選択します。到達可能なデバイスを 20 台まで選択できます。

（注） デバイス一覧にはインベントリで利用可能なデバイスがすべて表示されますが、コマンドランナーはワイヤレス アクセス ポイント デバイスおよび Cisco Meraki デバイスではサポートされていません。アクセス ポイント デバイスまたは Cisco Meraki デバイスを選択すると、コマンドが実行されないという警告メッセージが表示されます。

ステップ 5 [Select/Enter commands] フィールドに CLI コマンドを入力し、[Add] をクリックします。

コマンドランナーでは、先行入力がサポートされています。入力を開始すると、選択可能なコマンドがコマンドランナーによって表示されます。新しい有効なコマンドを入力することもできます。

ステップ 6 [コマンドの実行（Run Command(s)）] をクリックします。

成功すると、「コマンドは正常に実行されました」 というメッセージが表示されます。

ステップ 7 コマンド出力を表示するには、デバイスの下に表示されているコマンドをクリックします。

（注） [Command Runner] ウィンドウにすべてのコマンド出力が表示されます。パスワードなどの機密情報は、コマンド出力でマスクされます。

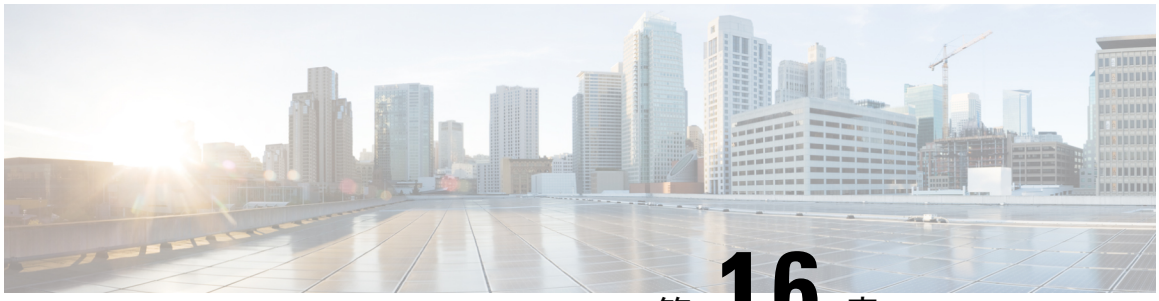
ステップ 8 （任意） [Export all CLI Output] をクリックすると、コマンド出力をテキストファイルにエクスポートしてローカルに保存できます。

ステップ 9 [Go Back] をクリックすると前のウィンドウに戻ります。

（注） 必要に応じて、デバイス名の横にある [x] をクリックすると、デバイス一覧からデバイスが削除されます。同様に、コマンドの横にある [x] をクリックすると、コマンド一覧からコマンドが削除されます。

第 V 部

ネットワークのプロビジョニング



第 16 章

プラグアンドプレイを使用したデバイスのオンボーディングとプロビジョニング

プラグ アンド プレイ プロビジョニングの概要

プラグ アンド プレイ プロビジョニングは、最小限のネットワーク管理者およびフィールド担当者の関与で、新しいネットワーク デバイスを自動的かつリモートにプロビジョニングおよびオンボードする方法を提供します。

プラグ アンド プレイ プロビジョニングを使用すると、次の操作を実行できます。

- サイトの割り当て、サイト設定の展開、デバイス ソフトウェア イメージのインストール、およびカスタム オンボード設定の適用によって、デバイスをプロビジョニングする。
- インストールの前に、デバイス情報を入力し、プロビジョニング操作を選択してデバイスを計画します。デバイスはオンラインになると Cisco DNA Center に接続します。次に、デバイスのプロビジョニングとオンボーディングが自動で実行されます。
- 事前の計画なしにネットワーク上に表示される新しいデバイスである、要求されていないネットワーク デバイスをプロビジョニングします。

- Cisco スマート アカウントの Cisco Plug and Play Connect クラウド ポータルから、デバイス インベントリをプラグ アンド プレイに同期して、すべてのデバイスが Cisco DNA Center に表示されるようにします。
- ネットワーク デバイスの詳細なオンボーディング ステータスを表示します。

ここでは、プラグアンドプレイプロビジョニングの一般的な使用例とワークフローについて説明します。

計画されたプロビジョニング

管理者は、次のように新しいサイトまたはその他のネットワーク デバイス グループのプロビジョニングを計画できます。

1. ネットワーク階層内のサイトを定義することをお勧めします。ネットワーク階層の概要（155 ページ）を参照してください。
2. デバイスに適用する [Onboarding Configuration] テンプレートを定義します。このようなテンプレートには、ネットワーク上で管理できるようにデバイスをオンボードするための基本的なネットワーク設定コマンドが含まれています。多くの場合、Day 0 設定をカスタマイズする必要がない限り、このようなテンプレートは必要ありません。デバイス設定の変更を自動化するテンプレートの作成 （315 ページ）を参照してください。

（注） Day 0 テンプレートは、対話型コマンドをサポートしていません。

3. 展開するデバイスのタイプについて、ネットワーク プロファイルを定義します。「ネットワークプロファイルの概要 （297 ページ）」を参照してください。
4. 展開するデバイスのデバイスログイン情報（CLI および SNMPv2c/SNMPv3）を定義することをお勧めします。SNMPv2c を使用している場合は、読み取りと書き込みの両方のログイン情報を指定する必要があります。

（注） ログイン情報が不足していると、プロビジョニング後にデバイスをインベントリに追加できなくなります。

5. プロビジョニングするデバイスのソフトウェアイメージがアップロードされ、イメージリポジトリ内でゴールデンとしてマークされていることを確認します。ソフトウェアイメージのインポート （360 ページ）を参照してください。
6. CSV ファイルを使用して一度にまたは一括で、計画したデバイスに関する詳細を追加します。デバイスの追加または編集 （402 ページ）またはデバイスの一括追加 （404 ページ）を参照してください。
7. デバイスが起動し、自動的にプロビジョニングされます。

要求されていないプロビジョニング。

計画前に新しいネットワーク デバイスをネットワークに追加すると、このネットワーク デバイスは要求のないデバイスとしてラベル付けされます。要求のないデバイスは、管理者が手動で追加することも、プラグ アンド プレイ プロビジョニングの前提条件 （394 ページ）で説明されているいずれかの検出方法を使用して自動的に追加することもできます。管理者は、次の方法でデバイスをプロビジョニングできます。

1. 要求のないデバイスでフィルタリングするか、名前で検索して、デバイス リストのデバイスを検索します。「デバイスの表示 （400 ページ）」を参照してください。
2. サイト、イメージ、設定テンプレート、またはプロファイルを割り当てて、デバイスを要求します。「プラグアンドプレイ対応デバイスのプロビジョニング （407 ページ）」を参照してください。サイトを割り当てずにデバイスを要求することもできます。

（注） サイトが割り当てられていないデバイスの場合、グローバルデバイスログイン情報が必要です。サイトが割り当てられているデバイスの場合、サイトレベルのグローバルデバイスログイン情報が必要です。

Cisco スマート アカウントの同期およびプロビジョニング

ネットワーク デバイスは、シスコのプラグ アンド プレイ接続クラウド サービスによって Cisco スマート アカウントを通じて自動的に登録されます。管理者は Cisco Plug and Play Connect から Cisco DNA Center プラグ アンド プレイにデバイス インベントリを同期することができます。これにより、すべてのデバイスが Cisco DNA Center に表示されます。次に、これらのデバイスを要求してプロビジョニングすることができます。

1. スマートアカウントと同期するバーチャルアカウントを登録して同期します。「バーチャル アカウント プロファイルの登録または編集 （404 ページ）」を参照してください。
2. スマート アカウントからデバイス インベントリを同期します。スマート アカウントからのデバイスの追加 （406 ページ）を参照してください。
3. 要求のないデバイスでフィルタリングするか、名前で検索して、デバイス リストのデバイスを検索します。「デバイスの表示 （400 ページ）」を参照してください。
4. サイト、イメージ、設定テンプレート、またはプロファイルを割り当てて、デバイスを要求します。「プラグアンドプレイ対応デバイスのプロビジョニング （407 ページ）」を参照してください。
5. デバイスが起動し、自動的にプロビジョニングされます。

プラグ アンド プレイ プロビジョニングの前提条件

プラグ アンド プレイ プロビジョニングを使用する前に、すべてのデバイスタイプで必要な前提条件が満たされていることを確認してください。さらに、ワイヤレスデバイスまたはセンサーデバイスを展開している場合は、それらの前提条件が満たされていることを確認してください。その他の前提条件はオプションですが、それらを実行することにした場合は、プラグアンドプレイを使用してデバイスをプロビジョニングする前に実行する必要があります。

すべてのデバイスの前提条件

すべてのデバイスタイプが次の前提条件を満たしていることを確認します。

- デバイスが、次のいずれかの方法で Cisco DNA Center コントローラを自動的に検出できることを確認します。
  - DHCP：DHCP コントローラ ディスカバリ （396 ページ）を参照してください。
  - DNS：DNS コントローラ ディスカバリ （397 ページ）を参照してください。
  - Cisco Plug and Play Connect クラウドサービス：Plug and Play Connect コントローラ ディスカバリ （398 ページ）を参照してください。
- メインの Cisco DNA Center の設定で、**[System]** > **[Settings]** > **[Smart Account]** を使って、Cisco スマートアカウントのクレデンシャルを設定します。
- **[System]** > **[Settings]** > **[Device EULA Acceptance]**を使用して、メインの Cisco DNA Center の設定でシスコ エンド ユーザー ライセンス契約（EULA）に同意します。
- プロビジョニングするシスコネットワークデバイスについて、サポートされているソフトウェアリリースがあり、工場出荷時のデフォルト状態になっていることを確認します。以前に設定されたネットワークデバイス、または不明な状態になっているネットワークデバイスを使用している場合は、『Network Plug and Play Troubleshooting Guide for Cisco DNA Center』で、デバイスのクリーンアップとリセットの詳細を参照してください。

ワイヤレスデバイスまたはセンサーデバイスの前提条件

前述の前提条件に加えて、ワイヤレスデバイスまたはセンサーデバイスが次の要件を満たしていることを確認してください。

- ワイヤレス AP デバイスの場合は、ワイヤレス AP を管理している シスコ ワイヤレス コントローラ がインベントリに追加され、ワイヤレス AP が割り当てられるサイトに割り当てられていることを確認します。この要件は、Mobility Express AP では必要ありません。
- ワイヤレス AP デバイスの場合は、ワイヤレス無線周波数プロファイルを定義します。ワイヤレス無線周波数プロファイルの作成（268ページ）を参照してください。この要件は、Mobility Express AP では必要ありません。
- Mobility Express AP の場合は、IP アドレスプールと管理インターフェイスを定義します。IP アドレス プールを設定する （241 ページ）を参照してください。

- センサーの場合は、センサーが Cisco DNA Center エンタープライズ IP アドレス（private/enp9s0）を介して到達可能であることを確認します。DHCP オプション 43 の文字列を使用すると、デバイスが Cisco DNA Center の未要求モードで到達可能になります。ただし、デバイスを要求するには、インターフェイス enp9s0 IP アドレスから到達可能である必要があります。DHCP サーバで ASCII 値「5A1D;B2;K4;I172.16.x.x;J80」を使用して、NTP サーバ（DHCP オプション 42）とベンダー固有の DHCP オプション 43 を設定します。ここで、172.16.x.x は enp9s0 インターフェイスに関連付けられた Cisco DNA Center の仮想 IP アドレスです。

オプションの前提条件

次の前提条件はオプションですが、プラグ アンド プレイ プロビジョニング プロセスを自動化するのに役立ちます。

- ネットワーク階層内のサイトを定義します。ネットワーク階層の概要 （155 ページ）を参照してください。
- デバイスの CLI および SNMP ログイン情報を定義します。グローバル デバイス クレデンシャルの概要 （230 ページ）を参照してください。

（注） CLI、SNMPv2c、または SNMPv3 ログイン情報を使用してワイヤレスデバイスを要求できます。SNMPv2c を使用している場合は、読み取りと書き込みの両方のログイン情報を指定します。

- イメージを展開する場合は、プロビジョニングされるデバイスのソフトウェアイメージをアップロードし、イメージリポジトリ内でゴールデンとしてマークされるようにします。ソフトウェア イメージのインポート （360 ページ）を参照してください。

（注） Day-0 プロビジョニング中にプラグアンドプレイで使用されるイメージ導入プロセスは、後でデバイスイメージの更新時に使用されるプロセスと同じではありません。これはソフトウェアイメージのプロビジョニング （366 ページ）で説明されています。プラグアンドプレイプロビジョニングでは、デバイスが工場出荷時のデフォルト状態にあると想定されているため、デバイスの事前チェック、自動フラッシュクリーンアップ、事後チェックは行われません。

- デバイスに適用する [Onboarding Configuration] テンプレートを定義します。このようなテンプレートには、ネットワーク上で管理できるようにデバイスをオンボードするための基本的なネットワーク設定コマンドが含まれています。デバイス設定の変更を自動化するテンプレートの作成 （315 ページ）を参照してください。

（注） [Onboarding Configuration] テンプレートで `ip http client source-interface` CLI コマンドを使用できます。これにより、Cisco DNA Center は、特に複数の IP または VRF のシナリオにおいて、その IP アドレスをデバイスの管理 IP アドレスとして使用できます。

- デバイスのネットワークプロファイルを定義します。ネットワークプロファイルの概要（297 ページ）を参照してください。

DHCP コントローラ ディスカバリ

シスコのネットワークデバイスは初回起動時にスタートアップ設定を使用しない場合、DHCP オプション 43 を使用して Cisco DNA Center コントローラの検出を試行します。

DHCP による検出方法の前提条件は次のとおりです。

- 新しいデバイスが DHCP サーバにアクセスできる。
- DHCP サーバが Cisco Plug and Play のオプション 43 を使用して設定されている。このオプションにより、Cisco DNA Center コントローラの IP アドレスを持つネットワークデバイスが通知されます。

  DHCP サーバが文字列「ciscopnp」を含むオプション 60 を使用してデバイスから DHCP の検出メッセージを受信すると、オプション 43 の情報を含む応答をデバイスに返します。デバイスの Cisco Plug and Play IOS エージェントは、応答から Cisco DNA Center コントローラの IP アドレスを抽出し、このアドレスを使用してコントローラと通信します。

DHCP オプション 43 は、DHCP サーバとして機能する Cisco ルータ CLI で、次のように設定された文字列の値で構成されます。

```
ip dhcp pool pnp_device_pool          <-- Name of DHCP pool
network 192.168.1.0 255.255.255.0     <-- Range of IP addresses assigned to clients
default-router 192.168.1.1            <-- Gateway address
option 43 ascii "5A1N;B2;K4;I172.19.45.222;J80;"    <-- Option 43 string
```

このオプション 43 の文字列には、セミコロンで区切られた次のコンポーネントが含まれています。

- 5A1N;（プラグ アンド プレイ用の DHCP サブオプション、アクティブ動作、バージョン 1、デバッグ情報なし）。文字列のこの部分は変更する必要がありません。
- B2;（IP アドレスのタイプ）：
  - B1 = ホスト名
  - B2 = IPv4（デフォルト）

- I*xxx.xxx.xxx.xxx*;：Cisco DNA Center コントローラの IP アドレスまたはホスト名（大文字の i の後）。この例では、IP アドレスは 172.19.45.222 です。
- J*xxxx*：Cisco DNA Center コントローラへの接続に使用するポート番号。この例では、ポート番号は 80 です。HTTP のデフォルトはポート 80、HTTPS のデフォルトはポート 443 です。
- K4;：デバイスとコントローラの間で使用されるトランスポート プロトコル。
  - K4 = HTTP（デフォルト）
  - K5 = HTTPS
- T*trustpoolBundleURL*：デフォルト（Cisco DNA Centerコントローラ）以外の別の場所から trustpool バンドルを取得する場合は、このオプション パラメータを使用して trustpool バンドルの外部 URL を指定します。APIC-EM コントローラは、Cisco InfoSec Cloud（http://www.cisco.com/security/pki/）からバンドルを取得します。たとえば、10.30.30.10 の TFTP サーバからバンドルをダウンロードするには、パラメータを「Tftp://10.30.30.10/ios.p7b」と指定します。

  trustpool セキュリティを使用していて、T パラメータを指定しない場合、デバイスは Cisco DNA Center コントローラから trustpool バンドルを取得します。
- Z*xxx.xxx.xxx.xxx*;（NTP サーバの IP アドレス）。trustpool セキュリティを使用してすべてのデバイスを同期させる場合、このパラメータは必須です。

DHCP の設定の詳細については、『*Cisco IOS Command Reference*』を参照してください。

DHCP オプション 43 が設定されていない場合、デバイスが DHCP サーバに接続できない場合、またはこの方法が別の理由で失敗する場合は、ネットワークデバイスは DNS を使用して検出を試行します。詳細については、DNS コントローラ ディスカバリ （397 ページ）を参照してください。

Cisco DNA Center システム証明書に FQDN のみの SAN フィールドがある場合、PnP を開始する前に、シードデバイスの DHCP プールを編集して、FQDN、B2 ー B1、dns-server、および domain-name を含むオプション 43 文字列を含める必要があります。

DHCP プールが Cisco スイッチまたはルータに依存している場合の設定例は次のとおりです。

```
ip dhcp pool PnP_Pool
network 214.2.64.0255.255.255.0
default-router 214.2.64.1
option 43 ascii "5A1D;B1;K4;I<FQDN>;J80;"
domain-name sitdns.com
dns-server 17.1.104.100
```

DNS コントローラ ディスカバリ

DHCP ディスカバリが Cisco DNA Center コントローラの IP アドレスを取得できない場合、ネットワークデバイスは DNS ルックアップ方式にフォールバックします。DHCP サーバから返されたネットワークドメイン名に基づき、事前設定されたホスト名「pnpserver」を使用して、コ

ントローラの完全修飾ドメイン名（FQDN）を作成します。NTP のサーバ名は、事前設定されたホスト名 pnpserver に基づいています。

たとえば、DHCP サーバからドメイン名「customer.com」が返された場合、ネットワークデバイスは「pnpserver.customer.com」というコントローラの FQDN を作成します。次に、この FQDN の IP アドレスを解決するために、ローカル ネーム サーバを使用します。NTP サーバ名の FQDN は pnpntpserver.customer.com です。

DNS による検出方法の前提条件は次のとおりです。

- 新しいデバイスが DHCP サーバにアクセスできる。
- Cisco DNA Center コントローラがホスト名「pnpserver」を使用して展開されている。
- NTP のサーバ名はホスト名「pnpserver」で展開される。

Plug and Play Connect コントローラ ディスカバリ

DHCP または DNS による検出方法の使用がオプションでない場合は、Cisco Plug and Play Connect クラウド サービスによって、デバイスが Cisco DNA Center コントローラの IP アドレスを検出できます。ネットワークデバイスが起動すると、DHCP または DNS を介してコントローラを特定できない場合に、devicehelper.cisco.com に接続して Plug and Play Connect を試行し、組織に定義されている適切なコントローラの IP アドレスを取得します。通信を保護するために、デバイスは Plug and Play Connec に接続するときに、最初に Cisco trustpool バンドルをダウンロードしてインストールします。

次の手順では、検出に Plug and Play Connect を使用して、Cisco Plug and Play でシスコのネットワークデバイスを展開する方法についての概要を説明します。

始める前に

シスコの各種ネットワークデバイスは、Cisco Plug and Play をサポートし、Cisco Plug and Play Connect クラウドサービスに接続している Cisco IOS イメージを実行しています。

ステップ 1 ネットワーク管理者は、Cisco スマートアカウントの Web ポータルにある Plug and Play Connect を使用して、組織に適した Cisco DNA Center コントローラのコントローラ プロファイルを設定します。詳細については、web ポータルのスマートアカウントのマニュアルを参照してください。

ステップ 2 Cisco Commerce Workspace（CCW）を介してプラグ アンド プレイ ネットワークデバイスを注文した場合、Cisco スマートアカウントが注文に割り当てられていれば、Plug and Play Connect を使用してネットワークデバイスが自動的に登録されます。Cisco Plug and Play で使用する各デバイスに、NETWORK-PNP-LIC オプションを追加します。

このオプションにより、デバイスのシリアル番号と PID がプラグアンドプレイ用にスマート アカウントで自動登録されます。デフォルト コントローラを指定済みの場合、注文の処理時にデバイスがそのコントローラに自動的に割り当てられます。

ステップ 3 または、Plug and Play Connect の Web ポータルからデバイスを手動で追加することもできます。

ステップ 4 Cisco DNA Center を、Cisco Plug and Play Connect のコントローラとして、リダイレクト サービス用に Cisco スマート アカウントに登録します。バーチャル アカウント プロファイルの登録または編集（404 ページ）を参照してください。

CCW を通してプラグアンドプレイ ネットワーク デバイスを注文し、これらのネットワークデバイスがスマートアカウント経由で Plug and Play Connect に自動登録される場合には、この手順が必須です。

ステップ 5 Cisco Plug and Play Connect クラウド ポータルのスマート アカウントから、デバイス インベントリを Cisco DNA Center プラグ アンド プレイに同期します。

Plug and Play Connect の Web ポータルに登録されたデバイスがコントローラに同期され、SmartAccount のソースとともにプラグ アンド プレイのデバイス リストに表示されます。

ステップ 6 新しく同期されたデバイスを要求します。プラグアンドプレイ対応デバイスのプロビジョニング（407 ページ）を参照してください。

ステップ 7 デバイス インストーラによって、シスコ ネットワークデバイスがインストールされ、電源が投入されます。

ステップ 8 デバイスは、Plug and Play Connect サービスをクエリして Cisco DNA Center コントローラを検出し、Cisco DNA Center でプラグ アンド プレイのシリアル番号によってコントローラを識別します。次に、要求プロセス中に計画された内容に従ってプロビジョニングされます。

（注） デバイスが定義済みの NTP サーバ **time-pnp.cisco.com** または **pool.ntp.org** と同期できない場合、デバイスは Plug and Play Connect のコンタクトに失敗します。この問題を解決するには、これらの 2 つのホスト名への NTP トラフィックをブロック解除するか、これら 2 つの NTP ホスト名を DNS サーバのローカル NTP サーバ アドレスにマップします。

プラグアンドプレイ導入ガイド

プラグアンドプレイを使用する場合は、次の推奨事項に従ってください。

- デバイスの起動順序：一般に、ルーティングとアップストリームデバイスは最初に展開する必要があります。ルータおよびすべてのアップストリームデバイスがアップされてプロビジョニングされると、スイッチとダウンストリームデバイスを展開できます。デバイスのプラグ アンド プレイ エージェントは最初のデバイスの起動時のみ、Cisco DNA Center コントローラの自動検出を試みます。現時点で、デバイスがコントローラに接続できない場合、デバイス プロビジョニングは失敗するため、アップストリーム デバイスは最初にプロビジョニングする必要があります。
- シスコのルータトランク/アクセスポートの構成：一般的なブランチネットワークには、ルータとスイッチが含まれます。1 つ以上のスイッチは WAN ルータに接続され、IP フォンやアクセス ポイントなどの他のエンドポイントはスイッチに接続します。スイッチがアップストリームルータに接続されると、次の導入モデルはプラグアンドプレイでサポートされます。

- ダウンストリーム スイッチはルータのスイッチ ポートを使用してルータに接続されます。このタイプの接続では、ルータのスイッチ ポートをトランクまたはアクセス ポートとして設定できます。
- ルータのルーテッド ポートを使用してダウンストリーム スイッチをルータに接続する。この場合、ルーテッド ポートはサブインターフェイスを使用して複数の VLAN をサポートできます。プラグアンドプレイのプロセス中、スイッチはそのポートを自動的にトランクポートとして設定します。大規模ブランチの場合は、ルータとダウンストリーム スイッチ間に複数の VLAN を設置する必要があります。このような使用例をサポートするには、スイッチをルーテッド ポートに接続する必要があります。

- 非 VLAN 1 構成：プラグアンドプレイは、VLAN 1 を使用して、デフォルトでデバイスをサポートします。1 以外の VLAN を使用するには、隣接するアップストリームデバイスでサポート対象のリリースが実行されていなければなりません。また、そのアップストリームデバイスに「**pnp startup-vlan** *x*」グローバル CLI コマンドを設定して、以降のプラグアンドプレイデバイスにこの CLI をプッシュする必要があります。隣接するアップストリーム デバイスでこのコマンドを実行した場合、そのアップストリーム デバイスでは VLAN メンバーシップの変更は行われません。ただし、アップストリームに接続された、以降のプラグアンドプレイデバイス上のアクティブインターフェイスは、指定された VLAN に変更されます。このガイドラインは、ルータとスイッチの両方に適用され、アクセスモードではなくトランクモードのシナリオでのみ使用する必要があります。

デバイスの表示

[Plug and Play] ウィンドウでデバイスに関する情報を表示できます。

さらに、このウィンドウからいくつかのタスクを実行できます。詳細については、次のトピックを参照してください。

- デバイスの追加または編集 （402 ページ）
- デバイスの一括追加 （404 ページ）
- スマート アカウントからのデバイスの追加 （406 ページ）
- プラグアンドプレイ対応デバイスのプロビジョニング （407 ページ）
- デバイスのリセット （418 ページ）
- デバイスの削除 （418 ページ）

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

[Plug and Play] ウィンドウには、次のデバイス情報を含むテーブルが表示されます。

表 *41* : デバイス情報

カラム	説明
#	行番号。
Device Name	デバイスのホスト名。このリンクをクリックすると、デバイスの詳細ウィンドウが開きます。スタック アイコンはスイッチ スタックを示します。
Serial Number	デバイスのシリアル番号。
Product ID	デバイスの製品 ID。
IP Address	デバイスの IP アドレス。
Source	デバイスエントリの送信元： • [User]：ユーザーが GUI または API を介してデバイスを追加しました。 • [Network]：コントローラに接続されたデバイスが要求解除されました。 • [SmartAccount]：デバイスはスマートアカウントから同期されました。
状態	• [Unclaimed]：デバイスはプロビジョニングされていません。 • [Planned]：デバイスはすでに要求されていますが、まだサーバーと接続していません。 • [Onboarding]：デバイスオンボーディングが進行中です。 • [Provisioned]：デバイスは正常にオンボーディングされ、インベントリに追加されています。 • [Error]：デバイスにエラーがあり、プロビジョニングできませんでした。
Onboarding State	デバイスのオンボーディング状態。デバイスの履歴に移動するには、経過表示バーをクリックします。
Site	デバイスが関連付けられているサイト。
Last Contact	デバイスが最後にプラグ アンド プレイに接続した日時。
Smart Account	デバイスが関連付けられている Cisco スマート アカウント。
Virtual Account	デバイスが関連付けられている（Cisco スマート アカウント内の）バーチャル アカウント。
Created	デバイスがプラグ アンド プレイに追加された日時。

デバイステーブルには、各デバイスについて、以下の表に示した情報が表示されます。一部の列はソートに対応しています。

（注） デフォルトの列表示設定では一部の列が非表示になっています。これは、列の見出しの右端にある 3 つの点（ ⋮ ）をクリックするとカスタマイズできます。

ステップ 2 [Plug and Play] ウィンドウから、次の方法でデバイス情報の表示を制御できます。

- 行を昇順または降順に並べ替えるには、キャロット矢印アイコン ▲ が付いている列ヘッダーをクリックします。
- 特定の状態のデバイスを表示するには、[Device Status] フィルタから、[Unclaimed]、[Error]、[Provisioned] または [All] を選択します。
- ビューをフォーカスするには、[Focus] ドロップダウンリストから [Default] または [All] を選択します。
- テーブル情報の更新のタイミングを変更するには、[Auto-Refresh] ドロップダウンリストをクリックして、望ましい更新間隔を選択します。デフォルトでは、デバイステーブルは 30 秒ごとに更新されます。
- 特定のデバイスを見つけるには、[Filter] または [Find] オプションを使用します。
- デバイスの詳細を表示するには、デバイス名をクリックします。

  その他の詳細を表示するには、開いたウィンドウで、[Details]、[History]、または [Configuration] タブをクリックします。スイッチスタックの場合は、[Stack] タブをクリックすることもできます。一部のタブには、クリックしてさらに詳細を表示できる追加のリンクがあります。

デバイスの追加または編集

この手順では、[Plug and Play Devices] リストからデバイスを追加または編集する方法について説明します。代わりに、[編集（Edit）] をクリックしてデバイスの詳細ウィンドウからデバイスを編集することもできます。

表 *42 : [デバイス（Device）] フィールド*

フィールド	説明
[Serial Number]	デバイス シリアル番号（デバイスを編集している場合は読み取り専用）。
Product ID	デバイス製品 ID（デバイスを編集している場合は読み取り専用）。
[Device Name]	デバイス名

フィールド	説明
Enable SUDI Authorization	セキュアな固有デバイス識別子（SUDI）認証をサポートするデバイスで有効にします。
SUDI Serial Numbers	SUDI をサポートするデバイスには、シャーシのシリアル番号と SUDI シリアル番号（デバイス ラベルのライセンス SN と呼ばれる）の 2 つのシリアル番号があります。SUDI 認証を使用するデバイスを追加するときは、このフィールドに 1 つまたは複数の SUDI シリアル番号をカンマで区切って入力します。このフィールドは、[SUDI 認証の有効化（Enable SUDI Authorization）] がチェックされている場合にのみ表示されます。
This Device Represents a Stack	デバイスがスタックを表します（デバイスを編集している場合、この項目は読み取り専用です）。サポート対象のスタッカブル スイッチにのみ適用されます。

始める前に

デバイスにログイン情報が必要な場合は、グローバルデバイスログイン情報が **[Design]** > **[Network Settings]** > **[Device Credentials]** ページで設定されていることを確認します。詳細については、グローバル CLI クレデンシャルの設定 （230 ページ）を参照してください。

ステップ 1 メニューアイコン（☰）をクリックして、**[Provision]** > **[Plug and Play]**。

ステップ 2 テーブル内のデバイスを表示します。

[Device State] のいずれかのボタンを使用してデバイスの状態でフィルタ処理したり、[Filter] オプションを使用して特定のデバイスを検索したりできます。[Refresh] をクリックしてデバイスリストを更新します。

ステップ 3 次のようにデバイスを追加または編集します。

- デバイスを追加するには、[Add Devices] をクリックし、[Single Device] をクリックします。
- デバイスを編集するには、編集するデバイス名の横にあるチェック ボックスをオンにして、デバイス テーブルの上部にあるメニューバーから [アクション（Actions）]>[編集（Edit）] をクリックします。**[デバイスの編集（Edit Device）]** ダイアログが表示されます。

ステップ 4 必要に応じてフィールドを設定します。詳細については上記の表を参照してください。

ステップ 5 次のいずれかの操作を実行して、設定を保存します。

- デバイスを追加し、後で要求するには、[デバイスの追加（Add Device）] をクリックします。
- デバイスを追加し、すぐに要求するには、[追加 + 要求（Add + Claim）] をクリックします。デバイスの要求の詳細についてはプラグアンドプレイ対応デバイスのプロビジョニング （407 ページ）、を参照してください。
- デバイスを編集する場合は、[デバイスの編集（Edit Device）] をクリックします。

デバイスの一括追加

この手順では、CSV ファイルからデバイスを一括で追加する方法を示します。

ステップ 1 メニューアイコン（☰）をクリックして、**[Provision]** > **[Plug and Play]**。

ステップ 2 [Add Devices] をクリックします。

[デバイスの追加（Add Device）] ダイアログが表示されます。

ステップ 3 [Bulk Devices] をクリックします。

ステップ 4 [Download File Template] をクリックしてファイルテンプレートをダウンロードします。

さまざまなデバイスの必須のフィールドとオプションのフィールドについては、ファイルテンプレートを参照してください。

ステップ 5 各デバイスの情報をファイルに追加し、ファイルを保存します。デバイスタイプによっては、特定のフィールドが必須になることに注意してください。

ステップ 6 次のアクションのいずれかを実行して、CSV ファイルをアップロードします。

- ドラッグ アンド ドロップ エリアにファイルをドラッグ アンド ドロップします。
- **[クリックして選択（click to select）]** が表示される場所をクリックしてファイルを選択します。

ステップ 7 **[デバイスのインポート（Import Devices）]** をクリックします。

CSV ファイル内のデバイスがテーブルにリストされます。

ステップ 8 インポートする各デバイスの横にあるチェックボックスをオンにするか、上部にあるチェックボックスをオンにしてすべてのデバイスを選択します。

ステップ 9 次のいずれかの操作を実行して、デバイスを追加します。

- デバイスを追加し、それらを後で要求するには、**[デバイスの追加（Add Devices）]** をクリックします。
- デバイスを追加し、それらをすぐに要求するには、[追加 + 要求（Add + Claim）] をクリックします。デバイスの要求の詳細についてはプラグアンドプレイ対応デバイスのプロビジョニング （407 ページ）、を参照してください。

バーチャル アカウント プロファイルの登録または編集

この手順により、Cisco DNA Center コントローラを、リダイレクション サービス向けの Cisco スマート アカウントに、Cisco Plug and Play Connect のデフォルトのコントローラとして登録できます。また、これによって Cisco Plug and Play Connect クラウド ポータルから Cisco DNA Center プラグ アンド プレイにデバイス インベントリを同期することができます。

表 *43* : バーチャルアカウント フィールド

フィールド	説明
スマートアカウントの選択	Cisco スマート アカウント名
バーチャル アカウントの選択	バーチャルアカウント名バーチャルアカウントは、Cisco スマートアカウント内のサブアカウントです。
IP または **FQDN**	この Cisco DNA Center コントローラの IP アドレスまたは完全修飾ドメイン名。
プロファイル名	コントローラのプロファイル名
デフォルト コントローラ プロファイルとして使用	Cisco DNA Center コントローラを Cisco プラグアンドプレイ接続のクラウド ポータルにデフォルト コントローラとして登録するには、このボックスにチェックを付けます。

始める前に

メインの Cisco DNA Center の設定で、**[System]** > **[Settings]** > **[Smart Account]** を使って、Cisco スマートアカウントのクレデンシャルを設定します。

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

ステップ 2 テーブル内のバーチャルアカウントを表示します。

このテーブルには、登録されている Plug and Play Connect のバーチャル アカウント プロファイルがすべて一覧表示されます。

ステップ 3 次のように、バーチャル アカウント プロファイルを追加または編集します。

- バーチャルアカウントを登録するには、[Register] をクリックします。[Register Virtual Account] ダイアログが表示されます。
- 登録済みのバーチャルアカウントプロファイルを編集するには、編集したいプロファイル名の横にあるラジオボタンをクリックし、テーブルの上にあるメニュー バーの [Edit Profile] をクリックします。[edit virtual account] ダイアログが表示されます。

ステップ 4 上述の [Virtual Account Fields] テーブルを参照して、必要に応じてフィールドを設定します。

ステップ 5 次のいずれかの操作を実行して、設定を保存します。

- 新しいバーチャルアカウント プロファイルを登録する場合は、[Register] をクリックします。
- バーチャル アカウント プロファイルを編集する場合は、[Change] をクリックします。

次のタスク

Cisco Plug and Play Connect クラウド ポータルから、デバイス インベントリを Cisco DNA Center プラグ アンド プレイに同期します。詳細については、スマート アカウントからのデバイスの追加 （406 ページ）を参照してください。

スマート アカウントからのデバイスの追加

このタスクにより、Cisco Plug and Play Connect クラウド ポータルのスマート アカウントから Cisco DNA Center プラグ アンド プレイにデバイス インベントリを同期することができます。

バーチャル アカウント テーブルには、プロファイルごとに情報が表示されます。

表 *44* : バーチャル アカウント情報

カラム	説明
バーチャル アカウント	バーチャルアカウント名
スマート アカウント	バーチャルアカウントが関連付けられているスマートアカウント
同期ステータス	直近の同期プロセスのステータス
同期の結果	最後の同期プロセスの結果

始める前に

Cisco プラグアンドプレイ接続クラウド ポータルからデバイスインベントリを同期する前に、バーチャルアカウントを登録する必要があります。バーチャル アカウント プロファイルの登録または編集 （404 ページ）を参照してください。**[Add Devices]** > **[Smart Account Devices]** ダイアログの **[PnP Connect]** リンクをクリックすると、[PnP Connect] 設定ページに直接移動できます。

ステップ 1 メニューアイコン（☰）をクリックして、**[Provision]** > **[Plug and Play]** を選択します。

ステップ 2 [Add Device] をクリックします。

[デバイスの追加（Add Device）] ダイアログが表示されます。

ステップ 3 [Smart Account Devices] をクリックします。

ステップ 4 Cisco.com ID を入力する必要がある場合（Cisco.com ID は「Not Associated（関連付けなし）」として表示されます）、次の手順を実行します。

a) [Add] リンクをクリックします。
b) Cisco.com ユーザ名とパスワードを入力します。
c) ログイン情報を Cisco DNA Center で永続的に保存する場合は [Save For Later] をクリックします。ログイン情報を 1 回のみ使用する場合は、このチェックボックスをオフのままにします。
d) [Submit] をクリックします。`

ステップ 5 デバイスを追加する Plug and Play Connect バーチャル アカウント プロファイルの名前の横にあるラジオ ボタンをクリックします。

PnP Connect バーチャル アカウント プロファイルを登録する必要がある場合は、[PnP Connect] リンクをクリックします。Cisco.com のログイン情報を追加する必要がある場合は、[Cisco.com ID] の横にある [Add] リンクをクリックします。Cisco ID を変更する場合は、[Not me?] リンクをクリックします。

ステップ 6 [Sync] をクリックして、このバーチャル アカウントの Cisco Plug and Play Connect から Cisco DNA Center プラグ アンド プレイに、デバイス インベントリを同期させます。

追加されたデバイスは、SmartAccount に設定されたソースとともに [Plug and Play Devices] テーブルに表示されます。

次のタスク

新しく同期されたデバイスを要求します。デバイスの要求の詳細についてはプラグアンドプレイ対応デバイスのプロビジョニング （407 ページ）、を参照してください。

プラグアンドプレイ対応デバイスのプロビジョニング

デバイスを要求すると、プロビジョニングのプロセスが開始されます。デバイスがプロビジョニングされると、Cisco DNA Center は次のアクションを実行します。

1. イメージをデバイスに展開します。
2. 次の設定を構成するシステム構成 CLI コマンドを展開します。
   - デバイスのログイン情報（CLI および SNMP）
   - SSH v2 および SCP サーバの有効化
   - HTTP および HTTPS サーバの無効化
   - スイッチでは、vtp モードの透過が有効になっています
3. デバイスのタイプに対応するデバイスオンボーディング構成テンプレートを展開します。
   - 有線デバイスの場合、Cisco DNA Center は定義したオンボーディング構成（Day-0）テンプレートを展開します。
   - ワイヤレスデバイスの場合、Cisco DNA Center はサイトに割り当てられたネットワークプロファイルに基づいて構成を展開します。

   オンボーディング構成テンプレートに同じシステム構成 CLI コマンドのいずれかが含まれている場合、オンボーディング構成テンプレートはシステム構成 CLI コマンドの後にデバイスに適用されるため、システム構成 CLI コマンドはオーバーライドされます。
4. デバイスをインベントリに追加します。

（注） あるデバイスについてデバイスの可制御性が有効になっている場合（デフォルトで有効）、デバイスがインベントリに追加された、またはサイトに割り当てられたときに、追加の設定がデバイスにプッシュされます。詳細については、*Cisco DNA Center* 管理者ガイドの「Device Controllability」の項を参照してください。

まだ起動していないデバイスを初めて要求する場合、デバイスは起動時に自動的にプロビジョニングされます。このプロセスは、デバイスのプランニングと呼ばれます。

デバイスをプロビジョニングするための手順は、デバイスのタイプによって次のように異なります。

- スイッチとルータの参照資料：スイッチまたはルータ デバイスのプロビジョニング （408 ページ）
- シスコ ワイヤレス コントローラ、アクセスポイントおよびセンサー：ワイヤレスまたはセンサー デバイスのプロビジョニング （412 ページ）

スイッチまたはルータ デバイスのプロビジョニング

この手順では、[Plug and Play Devices] リストからデバイスを要求する方法について説明します。代わりに、[Claim] をクリックしてデバイスの詳細ウィンドウからデバイスを要求することもできます。

始める前に

プラグ アンド プレイ プロビジョニングの前提条件が満たされていることを確認します。詳細については、プラグ アンド プレイ プロビジョニングの前提条件 （394 ページ）を参照してください。

ステップ 1 メニューアイコン（☰）をクリックして、**[Provision]** > **[Plug and Play]**。

ステップ 2 テーブル内のデバイスを表示します。

デバイスを表示するには、[Focus] ドロップダウンリストから [Default] または [All] を選択します。

デフォルトでは、デバイステーブルは 30 秒ごとに更新されます。[Auto-Refresh] ドロップダウンリストをクリックして、望ましい更新間隔を選択します。

[Filter] または **[Find]** オプションを使用して、特定のデバイスを見つけることができます。

ステップ 3 要求する 1 つ以上のデバイスの横にあるチェックボックスをオンにします。

ステップ 4 デバイス テーブルの上にあるメニュー バーで、[Actions] > [Claim] をクリックします。

ステップ 5 （任意） [Assign Site] ウィンドウで、次の手順を実行します。

a) 必要に応じてデバイスのホスト名を変更します。

b) 次のいずれかを実行して、サイトを割り当てます。

- 各デバイスに異なるサイトを割り当てるには、[Assign] をクリックし、[Select a Site] ドロップダウンリストから、サイトを選択します。
- 最初のデバイスと同じサイトを他のすべてのデバイスに割り当てるには、[Actions] 列で、省略記号アイコン ••• の上にカーソルを置き、[Apply Site to All] を選択します。
- あるデバイスのサイトを別のデバイスに割り当てるには、[Actions] 列で、省略記号アイコン ••• の上にカーソルを置き、[Assign this Site to Other Devices] をクリックし、デバイスを選択して [Assign] をクリックします。
- デバイスに割り当てられたサイトをクリアするには、[Clear Site] をクリックします。

c) [Next] をクリックします。

ステップ 6 [Assign Configuration] ウィンドウで、次の手順を実行します。

a) [Configuration] 列で、設定するデバイスの [Assign] をクリックします。

b) デバイス構成を変更する必要がない場合は、[Cancel] をクリックして、ステップ 7 に進みます。それ以外の場合は、次の設定のいずれかを変更または構成します。

- [Device Name]：必要に応じてデバイスのホスト名を変更します。
- [Image]：このドロップダウンリストで、デバイスに適用するゴールデン ソフトウェア イメージを選択します。イメージリポジトリにこのデバイスタイプのゴールデンイメージが 1 つしかない場合は、そのイメージがデフォルトで選択されます。
- [Template]：このドロップダウンリストで、デバイスに適用するオンボーディング設定テンプレートを選択します。このデバイスタイプに対して定義されているオンボーディング設定テンプレートが 1 つしかない場合は、そのテンプレートがデフォルトで選択されます。

  （注） デバイスをサイトに割り当てていない場合は、デバイスのテンプレートを選択してから先に進む必要があります。

- [Apply the PKCS12 device certificate on the device]：PKCS12 証明書をデバイスに展開するには、このチェックボックスをオンにします。このオプションは、ルータの場合にのみ使用可能です。
- [RTU License Level]：このドロップダウンリストから、[Lanbase] または [IP Services] を選択します。このオプションは、Cisco Industrial Ethernet（IE）4000 および 5000 シリーズ スイッチでのみ使用できます。

  （注） [IP Services] を選択するには、**[System]** > **[Settings]** > **[Device EULA Acceptance]** で、エンドユーザーライセンス契約（EULA）に同意します。

- [Select a Cabling Scheme]：スタックの番号を付け直す場合は、このドロップダウンリストで、スタックのケーブル配線スキームを選択します。

  この項目は、スタック構成をサポートしているスイッチが次のいずれかのケーブル配線スキームに従って接続されている場合にのみ表示されます。

図 *21 :* ケーブル配線スキーム

- [Select a Top of Stack serial Number]：スタックの番号を付け直す場合は、このドロップダウンリストで、スタック最上位スイッチのシリアル番号を選択します。

  この項目は、スタック構成をサポートしているスイッチが図のように接続されている場合にのみ表示されます。

- [Select a License Level]：このドロップダウンリストで、スタックのライセンスレベルを選択します。

  この項目は、スタック構成をサポートしているスイッチにのみ表示されます。

c) **[Save]** をクリックします。

d) [Clear Configuration] ドロップダウンリストから、次のオプションのいずれかを選択します。

- [Clear Device Certificates]：このオプションを選択し、証明書をクリアする各デバイスのチェックボックスをオンにして、[Clear] をクリックします。
- [Clear Image]：このオプションを選択し、イメージをクリアする各デバイスのチェックボックスをオンにして、[Clear] をクリックします。
- [Clear Templates]：このオプションを選択し、テンプレートをクリアする各デバイスのチェックボックスをオンにして、[Clear] をクリックします。
- [Clear License Levels]：このオプションを選択し、ライセンスレベルをクリアする各デバイスのチェックボックスをオンにして、[Clear] をクリックします。

e) あるデバイスのイメージまたはテンプレートを他のデバイスに適用するには、[Actions] 列で、省略記号アイコン ••• の上にカーソルを置き、[Apply Image to Other Devices] または [Apply Template to Other Devices] を選択します。

スタック構成のデバイスの場合は、[Apply License Level to Other Devices] をクリックして、デバイスのライセンスレベルを他のデバイスに適用できます。

f) プロビジョニングするデバイスを複数選択した場合は、リストにある次のデバイスの [Assign] クリックし、この設定手順を繰り返します。これを、すべてのデバイスに対して実行します。

g) すべてのデバイスの構成が完了したら、[Next] をクリックします。

ステップ 7 すべてのデバイスのテンプレートパラメータ値をまとめて設定するには、ステップ 8 に進みます。デバイスのテンプレートパラメータ値を 1 つずつ設定するには、[Provision Templates] ウィンドウから、次の手順を実行します。

a) 設定するデバイスの名前をクリックします。
b) デバイスに設定テンプレートが割り当てられている場合は、テンプレートで定義されたパラメータの値を指定します。

各デバイスのフィールドに各パラメータの値を入力します。レッド アスタリスクは必須フィールドを表します。

c) 選択したデバイスの起動構成に実行中の構成をコピーする場合、[Copy running config to startup config] チェックボックスをオンにします。
d) 複数のデバイスを選択してプロビジョニングした場合は、ウィンドウの左側にあるリストで次のデバイスをクリックし、パラメータ値を入力します。これを、すべてのデバイスに対して実行します。
e) [Next] をクリックします。

ステップ 8 すべてのデバイスのパラメータ値を一括で指定するには、[Provision Templates] ウィンドウから次の手順を実行します。

a) [Export] をクリックして、CSV テンプレートファイルを保存します。
b) 各パラメータの値をファイルに追加して、ファイルを保存します。
c) [Import] をクリックします。
d) ドラッグ アンド ドロップ エリアにファイルをドラッグ アンド ドロップするか、**[click to select]** と表示されている場所をクリックしてファイルを選択します。
e) [Import] をクリックします。
f) [Next] をクリックします。

ステップ 9 [Summary] ウィンドウで、デバイスに関する詳細や設定プレビューステータスを確認できます。

ステップ 10 設定プレビューが成功したかどうかを確認するには、各デバイスの [Day-0 Config] 列を確認します。

プレビューにエラーが表示された場合は、表の上にあるエラーメッセージの [Actions] リンクをクリックして、実行する必要があるアクションを確認します。アクションをクリックすると、変更が必要なウィンドウで新しいタブを開くことができます。

プロビジョニングエラーを回避するには、デバイスを要求する前に問題を解決します。「テンプレートのプロビジョニング」手順に戻ってパラメータ値やテンプレートを変更したり、[Design]エリアに再度アクセスしてネットワーク設計の設定を更新したり、ネットワーク接続の問題を解決したりすることが必要になる場合があります。

問題を解決したら、このタブに戻り、[Retrying get Day-0 configuration Preview for failed device（s）] をクリックし、[OK] をクリックします。

ステップ 11 [Day-0 Config] 列のリンクをクリックして、デバイス、その構成、構成プレビューエラーの詳細を確認します。

ステップ 12 [Claim] をクリックします。

ステップ 13 確認のダイアログボックスで [Yes] をクリックしてデバイスを要求します。

次のタスク

ネットワーク設定を構成している場合は、デバイスでこれらの設定をプロビジョニングします。詳細については、プロビジョニングプロセスの完了（417ページ）を参照してください。

ワイヤレスまたはセンサー デバイスのプロビジョニング

この手順では、[プラグアンドプレイデバイス（Plug And Play Devices）] リストからデバイスを要求する方法について説明します。代わりに、[Claim] をクリックしてデバイスの詳細ウィンドウからデバイスを要求することもできます。

始める前に

プラグ アンド プレイ プロビジョニングの前提条件が満たされていることを確認します。詳細については、プラグ アンド プレイ プロビジョニングの前提条件 （394 ページ）を参照してください。

ステップ 1 メニューアイコン（☰）をクリックして、**[Provision]** > **[Plug and Play]**。

ステップ 2 テーブル内のデバイスを表示します。

[フィルタ（Filter）] または **[検索（Find）]** オプションを使用して、特定のデバイスを見つけることができます。

ステップ 3 要求する 1 つ以上のワイヤレスデバイスの横にあるチェックボックスをオンにします。

ステップ 4 デバイステーブルの上にあるメニューバーで、**[Actions]** > **[Claim]**の順に選択します。

[Claim Devices] ウィンドウが開き、最初の手順「サイトの割り当て」が表示されます。代わりに、サイトの定義やデバイスログイン情報の定義などの必須タスクを示すウィンドウが表示された場合は、[Add Site] をクリックしてサイトを定義し、[Add device credentials] をクリックしてデバイスログイン情報を定義する必要があります。これらは要求プロセスの前提条件であり、これらのタスクが完了したら、このウィンドウで [Refresh] をクリックしてデバイスの要求に戻ることができます。

ステップ 5 （オプション）必要に応じて、最初の列のデバイス名を変更します。

ステップ 6 （オプション）必要に応じて、2番目の列のデバイスタイプを変更します。デバイスが使用しているモードに応じて、AP または ME（Mobility Express）を選択できます。

誤ったモードを選択すると、デバイスのプロビジョニングエラーにつながります。この項目は、シスコ ワイヤレス コントローラ やセンサーデバイスには表示されません。

ステップ 7 [Select a Site] ドロップダウンリストから、各デバイスに割り当てるサイトとフロアを選択します。AP デバイスは、ワイヤレスコントローラを備えたフロアに割り当てる必要があります。

同じサイトを最初のデバイスとしてすべての他のデバイスに適用するには、[Apply Site to All] チェックボックスをオンにします。あるデバイスのサイトを他のいくつかデバイスに割り当てるには、[Assign this

Site to Other Devices] をクリックし、デバイスを選択して [Assign] をクリックします。ワイヤレスデバイスは、ビルディング自体ではなくビルディング内のフロアにのみ割り当てることができます。

ステップ 8 **[Next]** をクリックします。
[Assign Configuration] ウィンドウが表示されます。

ステップ 9 （任意）テーブルに表示される列を変更するには、テーブル見出しの右端にある3つの点をクリックし、目的の列を選択します。[Apply] をクリックして、変更内容を保存します。

ステップ 10 [Configuration] 列で、設定するデバイスの [Assign] をクリックし、次の手順を実行します。

a) デバイス設定の概要を表示し、変更が不要な場合は [Cancel] をクリックします。
b) （任意）[デバイス名（Device Name）] フィールドで、必要に応じてデバイス名を変更します。
c) AP デバイスの場合、[Radio Frequency Profile] ドロップダウンリストで、デバイスに適用する無線周波数プロファイルを選択します。これは、1つのプロファイルをデフォルトとして指定した場合に設定できます。
d) ワイヤレスコントローラ の場合、[Wireless Management IP]、[Subnet mask]、[Gateway]、[IP interface name]、また任意で [VLAN ID] の各フィールドに値を入力します。
e) Mobility Express デバイスの場合は、[Wireless management IP]、[Subnet Mask]、および [Gateway] の各フィールドに値を入力します。
f) ワイヤレスセンサーデバイスの場合、[Sensor Settings] ドロップダウンリストで、デバイスに適用するセンサーデバイスプロファイル（バックホール）を選択します。

（注） リリース 1.3.1.2 よりも前の Cisco Aironet 1800s アクティブセンサーの場合は、センサーデバイス プロファイル **`CiscoProvisioningSSID`** を選択しないようにしてください。代わりに、バックホール用に独自の SSID を選択します。

g) 変更した場合は、[Save] をクリックします。それ以外の場合は、[Cancel] をクリックしてリストに戻り、他のデバイスを設定します。
h) **[Actions]** 列の **[他のデバイスに...を適用（Apply … to Other Devices）]** をクリックして、あるデバイスに割り当てた設定を同じタイプの他のデバイスに適用できます。

ステップ 11 （オプション）ワイヤレスセンサーデバイスの場合、ソフトウェアイメージを割り当てるには、次の手順を実行します。

1. [Image] 列で、[Assign] をクリックします。
2. [Image] ドロップダウンリストから、ゴールデン ソフトウェア イメージを選択します。
3. [**保存（Save）**] をクリックします。

ステップ 12 デバイスが Cisco Catalyst 9800-CL ワイヤレスコントローラの場合は、[Configuration] 列の [Image] の横にある [Assign] をクリックし、次の手順を実行します。

a) （オプション）[イメージ（Image）] ドロップダウンリストで、デバイスに適用するゴールデン ソフトウェア イメージを選択します。イメージリポジトリにこのデバイスタイプのゴールデンイメージが 1 つしかない場合は、そのイメージがデフォルトで選択されます。
b) [**保存（Save）**] をクリックします。

ステップ 13 複数のデバイスを選択してプロビジョニングした場合は、リストで次のデバイスに**[割り当て（Assign）]** をクリックし、この設定手順を繰り返します。これを、すべてのデバイスに対して実行します。

ステップ 14 **[Next]** をクリックします。
[概要（Summary）] ウィンドウが表示されます。ここで、デバイスや設定に関する詳細を確認できます。

ステップ 15 設定プレビューが成功したかどうかを確認するには、各デバイスの [Day-0 Config] 列をチェックします。

プレビューにエラーが表示された場合は、表の上にあるエラーメッセージの [Actions] リンクをクリックして、実行する必要のあるアクションを確認します。アクションをクリックすると、変更が必要なウィンドウで新しいタブを開くことができます。デバイスを要求する前に問題を解決してプロビジョニングエラーを回避する必要があります。[割り当ての設定（Assign Configuration）] 手順に戻って設定を変更したり、[設計（Design）] エリアに再度アクセスしてネットワーク設計の設定を更新したり、ネットワーク接続の問題を解決したりすることが必要になる場合があります。問題を解決したら、このタブに戻り、[Retrying get Day-0 configuration Preview for failed device(s)] をクリックし、[OK] をクリックします。デバイスを管理しているワイヤレスコントローラがインベントリに追加され、ワイヤレスデバイスが割り当てられているサイトに割り当てられていることを確認します。

ステップ 16 [要求（Claim）] をクリックします。

ステップ 17 確認ダイアログボックスで [Yes] をクリックしてデバイスを要求し、プロビジョニングプロセスを開始します。

次のタスク

ネットワーク設定を構成している場合は、デバイスでこれらの設定をプロビジョニングします。詳細については、プロビジョニングプロセスの完了 （417 ページ）Cisco DNA Center ユーザガイドを参照してください。

Cisco DNA トラフィック テレメトリ アプライアンス のプロビジョニング

この手順では、[Plug And Play Devices] リストからCisco DNA トラフィック テレメトリ アプライアンスを要求する方法について説明します。

始める前に

- プロビジョニングするシスコネットワークデバイスについて、ソフトウェアリリースがサポート対象であり、工場出荷時のデフォルト状態になっていることを確認します。以前に設定されたネットワークデバイス、または不明な状態になっているネットワークデバイスを使用している場合は、『Network Plug and Play Troubleshooting Guide for Cisco DNA Center』で、デバイスのクリーンアップとリセットの詳細を参照してください。
- プロビジョニングされているデバイスで Cisco DNA Center を検出して接続できることを確認します。
- ネットワーク階層内のサイトを定義します。ネットワーク階層の概要 （155 ページ）を参照してください。

- デバイスの CLI および SNMP ログイン情報を定義します。SNMPv2c を使用している場合は、読み取りと書き込みの両方のログイン情報を指定する必要があります。

（注） SNMPv3 の制限事項：

- 認証用の SHA とプライバシー用の AES128 がサポートされています。
- MD5 はサポートされていません。

- イメージを展開する場合は、プロビジョニングされるデバイスのソフトウェアイメージがアップロードされていて、イメージリポジトリ内でゴールデンとしてマークされていることを確認します。ソフトウェア イメージのインポート （360 ページ）を参照してください。

（注） Day-0 プロビジョニング中にプラグアンドプレイで使用されるイメージ展開プロセスは、後でデバイスイメージの更新時に使用される展開プロセスとは異なります。詳細については、ソフトウェア イメージのプロビジョニング （366 ページ）を参照してください。プロビジョニング中、プラグアンドプレイではデバイスの事前チェック、自動フラッシュクリーンアップ、または事後チェックは実行されません。デバイスは工場出荷時のデフォルト状態である必要があります。

- デバイスのネットワークプロファイルを定義します。Cisco DNA トラフィック テレメトリ アプライアンス のネットワークプロファイルの作成 （304 ページ）を参照してください。

ステップ 1 メニューアイコン（☰）をクリックして、**[Provision]** > **[Plug and Play]**。

ステップ 2 テーブル内のデバイスを表示します。

[Filter] または [Find] オプションを使用して、Cisco DNA トラフィック テレメトリ アプライアンス を見つけることができます。

ステップ 3 要求する 1 つ以上のデバイスの横にあるチェックボックスをオンにします。

ステップ 4 デバイステーブルの上にあるメニューバーで、**[Actions]** > **[Claim]**の順に選択します。

[Claim Devices] ウィンドウが開き、最初の手順「サイトの割り当て」が表示されます。代わりに、サイトの定義やデバイスログイン情報の定義などの必須タスクを示すウィンドウが表示された場合は、[Add Site] をクリックしてサイトを定義し、[Add device credentials] をクリックしてデバイスログイン情報を定義する必要があります。これらの必須タスクは、要求プロセスの前提条件です。これらのタスクが完了したら、このウィンドウで [Refresh] をクリックしてデバイスの要求に戻ることができます。

ステップ 5 （任意） 必要に応じて、最初の列のデバイスのホスト名を変更します。

ステップ 6 [Select a Site] ドロップダウンリストから、各デバイスに割り当てるサイトを選択します。

同じサイトを最初のデバイスとしてすべての他のデバイスに適用するには、[Apply Site to All] チェックボックスをオンにします。あるデバイスのサイトを他のいくつかデバイスに割り当てるには、[Assign this Site to Other Devices] をクリックし、デバイスを選択して [Assign] をクリックします。

ステップ 7 **[Next]** をクリックします。
[Assign Configuration] ウィンドウが表示されます。

ステップ 8 [Configuration] 列で、設定するデバイスの [Assign] をクリックし、次の手順を実行します。

a) デバイス設定の概要を表示し、変更が不要な場合は [Cancel] をクリックします。
b) （任意） [Device Name] フィールドで、必要に応じてデバイスのホスト名を変更します。
c) （任意） [Image] ドロップダウンリストで、デバイスに適用するゴールデン ソフトウェア イメージを選択します。イメージリポジトリにこのデバイスタイプのゴールデンイメージが 1 つしかない場合は、そのイメージがデフォルトで選択されます。
d) 何らかの変更を行った場合は、[Save] をクリックします。変更していない場合は、[Cancel] をクリックしてリストに戻り、他のデバイスを設定します。

ステップ 9 プロビジョニングするデバイスを複数選択した場合は、リストにある次のデバイスの [Assign] をクリックします。すべてのデバイスを設定するまで、設定手順を繰り返します。

ステップ 10 [Next] をクリックします。

[Summary] ウィンドウが表示されます。ここで、デバイスに関する詳細や設定プレビューステータスを確認できます。

ステップ 11 設定プレビューが成功したかどうかを確認するには、各デバイスの [Day-0 Config] 列をチェックします。

プレビューにエラーが表示された場合は、表の上にあるエラーメッセージの [Actions] リンクをクリックして、実行する必要があるアクションを確認します。アクションをクリックすると、ウィンドウで変更が必要な新しいタブが開きます。プロビジョニングエラーを回避するには、デバイスを要求する前に問題を解決する必要があります。場合によっては、[Design] 領域に再度アクセスしてネットワーク設計の設定を更新したり、ネットワーク接続の問題を解決したりする必要があります。問題を解決したら、このタブに戻り、[Retrying get Day-0 configuration Preview for failed device(s)] をクリックし、[OK] をクリックします。

ステップ 12 [Day-0 Config] 列のリンクをクリックして、デバイス、その構成、構成プレビューエラーの詳細を確認します。

ステップ 13 [Claim] をクリックします。

ステップ 14 確認のダイアログボックスで [Yes] をクリックしてデバイスを要求します。

次のタスク

プロビジョニングプロセスを完了するには、デバイスがインベントリに追加された後、[Inventory] タブに移動し、デバイスを選択し、**[Actions]** > **[Provision]** > **[Provision Device]**を選択します。すべての手順を実行し、[Summary]ステップで [Deploy] をクリックします。[Summary] ウィンドウで、デバイスにプッシュされる残りのネットワーク設定を確認できます。詳細については、ワイヤレスデバイスプロビジョニングの概要（421 ページ）を参照してください。このプ

ロセスは、[Design] エリアで設定した可能性のあるネットワーク設定をプッシュする場合に必要です。プラグアンドプレイ プロビジョニング中は、デバイスのログイン情報とオンボーディング設定のみがデバイスにプッシュされます。[Inventory] からプロビジョニングが完了するまで、他のネットワーク設定はプッシュされません。

プロビジョニングプロセスの完了

プラグアンドプレイのプロビジョニング中に、デバイスのログイン情報とオンボーディング設定のみがデバイスにプッシュされます。他のネットワーク設定はプッシュされません。プラグアンドプレイのプロビジョニングが完了したら、[Design] 領域で構成されているネットワーク設定をプッシュすることで、プロビジョニングプロセスを完了できます。

ネットワーク設定には AAA サーバー設定が含まれます（設定されている場合）。Cisco ISE の場合、Cisco DNA Center は Cisco ISE のデバイスを RADIUS または TACACS の AAA クライアントとして設定します。

ワイヤレスおよびセンサーデバイスの場合、ネットワーク設定には、RF プロファイルやアンテナ無線プロファイルなどのワイヤレス設定が含まれます（設定されている場合）。詳細については、「ワイヤレス デバイス プロビジョニングの概要 （421 ページ）」を参照してください。

始める前に

- 次のいずれかの手順を使用して、デバイスがプロビジョニング（オンボード）されていることを確認します。
  - スイッチまたはルータ デバイスのプロビジョニング （408 ページ）
  - ワイヤレスまたはセンサー デバイスのプロビジョニング （412 ページ）
- ネットワークの設定値を設定します。詳細については、ネットワークの設定 （227ページ）を参照してください。

ステップ 1 Cisco DNA Center GUI でメニューアイコン（☰）をクリックして、**[Provision]** > **[Inventory]** の順に選択します。

ステップ 2 デバイスを選択し、**[Actions]** > **[Provision]** > **[Provision Device]** を選択します。

ステップ 3 ワークフローの手順を進めます。

ステップ 4 [Summary] ウィンドウで、残りのネットワーク設定を確認します。変更を加えるには、関連するカテゴリの横にある [Edit] をクリックします。それ以外の場合は、[Deploy] をクリックします。

デバイスの削除

デバイスを削除すると、デバイスはプラグアンドプレイのデータベースから削除されますが、リセットはされません。エラー状態のデバイスをリセットする場合は、[Reset] を使用します。

この手順では、[Plug and Play Devices] リストからデバイスを削除する方法について説明します。代わりに、[削除（Delete）] をクリックしてデバイスの詳細ウィンドウからデバイスを削除することもできます。

（注） デバイスがプロビジョニングの状態の場合は、[Inventory] タブからのみ削除できます。

ステップ 1 メニューアイコン（☰）をクリックして、**[Provision]** > **[Plug and Play]**。

ステップ 2 テーブル内のデバイスを表示します。

[Device State] のいずれかのボタンを使用してデバイスの状態でフィルタ処理したり、[Filter] オプションを使用して特定のデバイスを検索したりできます。[Refresh] をクリックしてデバイスリストを更新します。

ステップ 3 削除する 1 つ以上のデバイスの横にあるチェックボックスをオンにします。

ステップ 4 デバイステーブルの上にあるメニューバーで、**[Actions]** > **[Delete]**の順に選択します。

ステップ 5 [Yes] クリックして、このデバイスを削除することを確認します。

デバイスのリセット

デバイスのリセットはエラー状態のデバイスにのみ適用され、状態が [Unclaimed] にリセットされデバイスがリロードされますが、プラグアンドプレイ データベースからは削除されません。デバイスを削除する場合は、**[Ddelete]** を使用します。

（注） デバイスで保存された設定が工場出荷時のデフォルトまたは同様の最小限の設定である場合、このオプションを選択すると、デバイスはプロビジョニングプロセスを再起動します。ただし、デバイスに以前に保存されたスタートアップ コンフィギュレーションがある場合は、これによってデバイスのプロビジョニングプロセスの再起動を回避できますが、工場出荷時のデフォルトにリセットする必要があります。ワイヤレスデバイスおよびセンサーデバイスでは、デバイスの状態だけがリセットされ、デバイスはリロードされません。

この手順では、[Plug and Play Devices] リストからデバイスをリセットする方法を示します。代わりに、[Reset] をクリックしてデバイスの詳細ウィンドウからリセットすることもできます。

ステップ 1 メニューアイコン（☰）をクリックして、**[Provision]** > **[Plug and Play]**。

ステップ 2 テーブル内のデバイスを表示します。

[Device State] のいずれかのボタンを使用してデバイスの状態でフィルタ処理したり、[Filter] オプションを使用して特定のデバイスを検索したりできます。[Refresh] をクリックしてデバイスリストを更新します。

ステップ 3 リセットする 1 個以上のデバイスの横にあるチェック ボックスをオンにします。

ステップ 4 デバイス テーブルの上にあるメニュー バーで、**[Actions（アクション）] > [Reset（リセット）]** をクリックします。

確認のダイアログボックスが表示されます。

ステップ 5 次のいずれかのオプションを選択します。

- [Reset and keep current claim parameters]：現在の請求パラメータが維持され、デバイスは [Planned] 状態になります。
- [Reset and remove all claim parameters]：現在の請求パラメータを削除し、デバイスが [Unclaimed] 状態になります。

ステップ 6 [Reset] をクリックします。

第 17 章

ワイヤレスデバイスのプロビジョニング

ワイヤレス デバイス プロビジョニングの概要

次のセクションでは、さまざまなシスコワイヤレスデバイスをプロビジョニングする方法について説明します。

ワイヤレスデバイスと国コードについて

コントローラおよびアクセスポイントは、法的な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。アクセスポイント内の無線は、製造時に特定の規制ドメインに割り当てられています（ヨーロッパの場合はEなど）が、国コードを使用すると、規制ドメイン内で稼働する特定の国を指定できます（フランスの場合はFR、スペインの場合はESなど）。国

番号を設定すると、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。

Cisco DNA Center は、割り当てられたサイトに応じて、国コードを使用してコントローラをプロビジョニングします。コントローラの場合は、複数のサイトに割り当てることができます。そのため、複数の国コードを割り当てることができます。Cisco DNA Center は、プロビジョニング中に、サイトをサイトの国コードとともにコントローラに割り当てます。たとえば、インドと米国の両方のサイトを管理するコントローラには、IN と US の国コードが割り当てられます。

アクセスポイントは、プロビジョニングされると、フロアに割り当てられます。アクセスポイントが ROW AP の場合、Cisco DNA Center は、サイトの国コードを取得して AP に割り当てます。同じフロア上の追加の AP には、同じ国コードが割り当てられます。

RF プロファイルを選択して AP をプロビジョニングする際、RF プロファイルで設定されたすべての動的チャネル割り当て（DCA）チャネルのうち、国コードに従ってサポートされているチャネルのみが考慮されます。サポートされていない DCA チャネルのリストは、Cisco DNA Center の AP 事前プロビジョニング ワークフローの AP 事前プロビジョニング手順の概要で確認できます。

国コード情報は、コントローラとアクセスポイントのデバイス 360 ページに表示されます。

サポートされている国コードの製品ごとの完全なリストについては、https://www.cisco.com/c/dam/assets/prod/wireless/wireless-compliance-tool/index.html を参照してください。

Cisco AireOS コントローラのプロビジョニング

始める前に

- シスコ ワイヤレス コントローラ をプロビジョニングする前に、次のグローバル ネットワーク設定を定義したことを確認します。
  - AAA、DHCP、および DNS などのネットワーク サーバー。

    詳細については、グローバル ネットワーク サーバーの設定（230 ページ）を参照してください。
  - CLI、SNMP、HTTP、HTTPS などのデバイス クレデンシャル。

    詳細については、グローバル CLI クレデンシャルの設定（230 ページ）、グローバル SNMPv2c クレデンシャルの設定（231 ページ）、グローバル SNMPv3 クレデンシャルの設定（233 ページ）、およびグローバル HTTPS クレデンシャルの設定（235 ページ）を参照してください。
  - IP アドレス プール

    詳細については、「IP アドレス プールを設定する（241 ページ）」を参照してください。

- SSID、ワイヤレス インターフェイス、およびワイヤレス無線周波数プロファイルなどのワイヤレス設定です。

  詳細については、「グローバル ワイヤレス設定の構成（247 ページ）」を参照してください。

- インベントリに シスコ ワイヤレス コントローラがあることを確認します。ない場合は、[Discovery] 機能を使用してコントローラを検出します。
- サイトに シスコ ワイヤレス コントローラ が追加されたことを確認してください。詳細については、デバイスをサイトに追加する （118 ページ）を参照してください。
- デバイスで既存の VLAN を再利用することはできません。デバイスにすでに存在する同じ VLAN を Cisco DNA Center がプッシュすると、プロビジョニングは失敗します。
- Cisco DNA Center によって管理されている ワイヤレスコントローラ の設定に手動で変更を加えることはできません。Cisco DNA Center GUI からすべての設定を実行する必要があります。

ステップ 1 メニューアイコン（☰）をクリックして、**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。

[Inventory] ウィンドウが表示され、検出されたデバイスが一覧表示されます。

ステップ 2 左側のペインで [Global] サイトを展開し、関心のあるサイト、ビルディング、またはフロアを選択します。

選択したサイトで使用可能なデバイスが [Inventory] ウィンドウに表示されます。

ステップ 3 [DEVICE TYPE] リストから [WLCs] タブをクリックし、[Reachability] リストから [Reachable] タブをクリックして、検出され到達可能な ワイヤレスコントローラ のリストを取得します。

ステップ 4 プロビジョニングするデバイス名の横にあるチェックボックスをオンにします。

ステップ 5 [Actions] ドロップダウンリストから、**[Provision]** > **[Provision Device]** を選択します。

[サイトの割り当て（Assign Site）] ウィンドウが表示されます。

ステップ 6 [Choose a site] をクリックして ワイヤレスコントローラ にサイトを割り当てます。

ステップ 7 [Add Sites] ウィンドウで、ワイヤレスコントローラを関連付けるサイト名の横にあるチェックボックスをオンにして、[Save] をクリックします。

ステップ 8 [Apply] をクリックします。

ステップ 9 **[次へ (Next)]** をクリックします。

[設定（Configuration）] ウィンドウが表示されます。

ステップ 10 ワイヤレスコントローラのロールを選択します（[Active Main WLC] または [Guest Anchor WLC]）。

ステップ 11 [Select Primary Managed AP Locations] をクリックして、ワイヤレスコントローラ の管理 AP の場所を選択します。

ステップ 12 [Managed AP Location] ウィンドウで、サイト名の横にあるチェックボックスをオンにします。親サイトまたは個々のサイトのいずれかを選択できます。親サイトを選択すると、親サイトの下にある子は自動的に選択されます。

（注） 管理 AP の場所を継承することで、サイトをその下のビルディングやフロアとともに自動で選択できます。1 つの ワイヤレスコントローラ で管理できるのは 1 つのサイトのみです。

ステップ 13 **[Save]** をクリックします。

ステップ 14 [Interface and VLAN Configuration] で [+ Add] をクリックして、アクティブメイン ワイヤレスコントローラ のインターフェイスと VLAN の詳細を設定します。

インターフェイスおよび VLAN の設定は、非ファブリックの ワイヤレスコントローラ プロビジョニングにのみ適用できます。

[インターフェイスと VLAN の設定（Configure Interface and VLAN）] ウィンドウが表示されます。

ステップ 15 [インターフェイス名（Interface Name）] ドロップダウン リストからインターフェイス名を選択します。

ステップ 16 [VLAN ID] フィールドに、VLAN の値を入力します。

ステップ 17 [Interface IP Address] フィールドに、インターフェイス IP アドレスの値を入力します。

ステップ 18 [Interface Net Mask (in bits)] フィールドに、インターフェイスのサブネットマスクを入力します。

ステップ 19 [Gateway IP Address] フィールドにゲートウェイ IP アドレスを入力します。

ステップ 20 [LAG/Port Number] ドロップダウンリストから、リンク集約またはポート番号を選択します。

ステップ 21 [OK] をクリックします。

ステップ 22 （オプション）ゲスト アンカー ワイヤレスコントローラ の場合、[Assign Guest SSIDs to DMZ site] で [VLAN ID] を変更して、VLAN ID 設定を変更します。

ステップ 23 [Mobility Group] で [Configure] をクリックして、ワイヤレスコントローラをモビリティピアとして設定します。

[Configure Mobility Group] サイドパネルが表示されます。

ステップ 24 [Mobility Group Name] ドロップダウンリストで、[+] をクリックして新しいモビリティグループを追加するか、既存のモビリティグループの中から選択します。

既存のモビリティピア情報は、 Cisco DNA Center で使用可能なインテントからロードされます。

ステップ 25 [RF Group Name] テキストボックスに RF グループの名前を入力します。

ステップ 26 [Mobility Peers] で [Add] をクリックして、ワイヤレスコントローラをモビリティピアとして設定します。

ステップ 27 [Device Name] ドロップダウンリストからコントローラを選択します。

デバイスがプロビジョニングされると、Cisco DNA Center はデバイスにモビリティグループを作成し、RF グループを割り当て、ピアのすべての終端を設定します。モビリティグループの設定は、選択したすべてのピアデバイスに自動的に展開されます。

ステップ 28 **[Save]** をクリックします。

ステップ 29 モビリティグループ名と RF グループ名をリセットするには、次のいずれかを実行します。

- [Configure Mobility Group] サイドパネルで、[Mobility Group Name] ドロップダウンリストから [default] を選択します。
- **[Provision]** > **[Configuration]** ページの [Mobility Group] で、[Reset] をクリックします。

これにより、[RF Group Name] が自動的に [default] に設定され、すべてのピアが削除されます。プロビジョニングが完了すると、デバイスのモビリティが設定され、そのデバイスは他のすべてのピアから削除されます。

ステップ 30 [Next] をクリックします。

[Model Configuration] ウィンドウが表示されます。

ステップ 31 [Devices] ペインで、[Find] フィールドにモデル設定設計の名前を入力して検索するか、デバイスを展開してモデル設定設計を選択します。

選択したモデル設定設計が右側のペインに表示されます。

ステップ 32 プロビジョニングするモデル設定設計の [Design Name] の横にあるチェックボックスをオンにし、[Configure] をクリックして編集します。

この手順では、すべての設定を編集することはできません。

ステップ 33 必要な変更を加えて、[Apply] をクリックします。

ステップ 34 [Next] をクリックします。

[Advanced Configuration] ウィンドウが表示されます。ここでは、事前定義されたテンプレート変数の値を入力できます。

ステップ 35 [Devices] パネルでデバイスまたはテンプレートを検索します。

ステップ 36 [wlanid] フィールドに、事前定義されたテンプレート変数の値を入力します。

ステップ 37 [Next] をクリックします。
[Summary（サマリ）] ウィンドウには、次の情報が表示されます。

- **Device Details**
- **ネットワーク設定**
- **SSID**
- **Managed Sites**
- **Interfaces**
- **Advanced Configuration**
- **モビリティ グループの設定**
- **モデル設定**

ステップ 38 [Deploy] をクリックして、コントローラをプロビジョニングします。

ステップ 39 [Provision Devices] ウィンドウで、次の手順を実行して CLI 設定をプレビューします。

- [Generate Configuration Preview] オプションボタンをクリックします。

- [Task Name] フィールドに、CLI プレビュータスクの名前を入力し、[Apply] をクリックします。
- [Task Submitted] メッセージで、[Work Items] リンクをクリックします。

（注） [Task Submitted] メッセージが表示されなかった場合は、メニューアイコン（☰）をクリックし、**[Activities]** > **[Work Items]**の順に選択します。

- [Work Items] ウィンドウで、設定プレビュー要求を送信した CLI プレビュータスクをクリックします。
- CLI 設定の詳細を表示し、[Deploy] をクリックします。
- 即座にデバイスを展開するには、[Now] オプションボタンをクリックし、[Apply] をクリックします。
- 将来の日付と時刻でデバイスの展開をスケジュールするには、[Later] オプションボタンをクリックし、展開する日時を定義します。
- [Information] ポップアップで、次の手順を実行します。
  - [Work Items] ウィンドウから CLI プレビュータスクを削除する場合は、[Yes] をクリックします。
  - [Work Items] ウィンドウでタスクを保持する場合は、[No] をクリックします。

（注） CLI タスクは、[Work Items] ウィンドウで完了済みとしてマークされます。このタスクの CLI 設定は表示することはできますが、再度展開することはできません。

ステップ 40 セカンダリコントローラをプロビジョニングします。

ステップ 41 展開が正常に完了すると、[Device Inventory] ウィンドウの [Status] 列に「SUCCESS」と表示されます。

プロビジョニング後に何らかの変更を行う場合は、[Design] をクリックしてサイトのプロファイルを変更し、もう一度 ワイヤレスコントローラ をプロビジョニングします。

ステップ 42 デバイスが正常に展開されると、[Provision Status] が [Configuring] から [Success] に変わります。

ステップ 43 [Device Inventory] ウィンドウで、[Provision Status] 列の [See Details] をクリックし、ネットワークインテントの詳細情報を取得するか、実行する必要があるアクションのリストを表示します。

ステップ 44 [Device Provisioning] の下の [See Details] をクリックします。

ステップ 45 [Deployment of network intent] の下の [View Details] をクリックし、デバイス名をクリックします。

ステップ 46 [Configuration Summary] エリアを展開して、操作の詳細、機能名、および管理機能を表示します。

[Configuration Summary] には、デバイスのプロビジョニング中に発生したエラーも表示されます。

ステップ 47 デバイスに送信される正確な設定の詳細を表示するには、[Provision Summary] エリアを展開します。

シスコ ワイヤレス コントローラの高可用性の設定

シスコ ワイヤレス コントローラ高可用性（HA）を Cisco DNA Center から設定できます。現在、ワイヤレスコントローラ HA の形成および中断の両方がサポートされています。スイッチオーバーオプションはサポートされていません。

ハイ アベイラビリティ用 Cisco ワイヤレス コントローラ設定の前提条件

- ワイヤレスコントローラ 1 とワイヤレスコントローラ 2 の検出機能とインベントリ機能が正常である必要があります。デバイスが [Managed] 状態になっている必要があります。
- ワイヤレスコントローラ 1 とワイヤレスコントローラ 2 のサービスポートと管理ポートが設定されている必要があります。
- ワイヤレスコントローラ 1 とワイヤレスコントローラ 2 の冗長ポートが物理的に接続されている必要があります。
- ワイヤレスコントローラ 1 とワイヤレスコントローラ 2 の管理アドレスが同じサブネット内にある必要があります。ワイヤレスコントローラ 1 とワイヤレスコントローラ 2 の冗長管理アドレスも同じサブネット内にある必要があります。
- ワイヤレスコントローラで次のブート変数を手動で設定します。

```
config t
boot system bootflash::<device_iosxe_image_filename>
config-register 0x2102

show boot.  (IOSXE cli)

BOOT variable = bootflash:<device_iosxe_image_filename>,12;
Configuration register is 0x2102
```

シスコ ワイヤレス コントローラ HA の設定

ステップ 1 メニューアイコン（☰）をクリックして、**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。

[Inventory] ウィンドウが表示され、検出されたデバイスが一覧表示されます。

ステップ 2 プライマリコントローラとして設定するコントローラ名の横にあるチェックボックスをオンにします。

ステップ 3 [Actions] ドロップダウンリストから、**[Provision]** > **[Configure WLC HA]** を選択します。

[High Availability] ページが表示されます。

ステップ 4 [Redundancy Management IP] と [Peer Redundancy Management IP] のアドレスをそれぞれテキストボックスに入力します。

冗長性管理 IP およびピア冗長性管理 IP に使用される IP アドレスは、シスコ ワイヤレス コントローラ の管理インターフェイスと同じサブネットに設定する必要があります。これらの IP アドレスがこのサブネット範囲内で未使用の IP アドレスであることを確認します。

ステップ 5 [Select Secondary WLC] ドロップダウンリストから、セカンダリコントローラを選択します。

（注） プライマリコントローラのワイヤレス管理インターフェイス IP サブネットに基づいてセカンダリコントローラを選択すると、冗長性管理 IP が自動入力され、**[High Availability]** ウィンドウの上部に **[i]** アイコンが表示され、次のメッセージが表示されます。「冗長性管理 IP とピア冗長性管理 IP が他のネットワークエンティティに割り当てられていないことを確認してください。**使用する場合は、IP を適宜変更して設定します」**。

ステップ 6 [Configure HA] をクリックします。
HA 設定は、CLI コマンドを使用してバックグラウンドで開始されます。最初に、プライマリ ワイヤレス コントローラが設定されます。成功したら、セカンダリ ワイヤレス コントローラが設定されます。設定が完了したら、両方のワイヤレスコントローラが再起動します。このプロセスは、完了するまで最大 2.5 分かかります。

ステップ 7 HA 設定を確認するには、**[Devices]** > **[Inventory]** ページで、HA デバイスとして設定したデバイスをクリックします。

ステップ 8 [Wireless Info] タブをクリックします。

[Redundancy Summary] には、[Sync Status] が [In Progress] として表示されます。Cisco DNA Center で HA のペアリングが成功したことが検出されると、[Sync Status] が [Complete] に変わります。

これは、インベントリポーラーまたは手動による再同期によってトリガーされます。これで、セカンダリ ワイヤレス コントローラ（ワイヤレスコントローラ 2）は、Cisco DNA Center から削除されます。このフローは、ワイヤレスコントローラでの正常な HA 設定を示しています。

高可用性プロセス中および完了後に起こること

1. Cisco WLC-1 および WLC-2 は、冗長管理、冗長ユニット、および SSO とともに設定されます。ワイヤレス コントローラはロールをアクティブまたはスタンバイとしてネゴシエートするために再起動します。設定は、アクティブからスタンバイに同期されます。
2. [冗長性の概要の表示（Show Redundancy Summary）] ウィンドウで、次の設定を確認できます。
   - SSO が有効になっています
   - ワイヤレス コントローラがアクティブ状態になっています
   - ワイヤレス コントローラがホット スタンバイ状態になっています
3. アクティブ ワイヤレス コントローラの管理ポートは、両方のコントローラによって共有され、アクティブ コントローラを指します。スタンバイ ワイヤレス コントローラのユーザー インターフェイス、Telnet、および SSH は機能しません。コンソールとサービス ポート インターフェイスを使用して、スタンバイ ワイヤレス コントローラを制御できます。

高可用性を設定および確認するためのコマンド

シスコ ワイヤレス コントローラ HA を設定するには、Cisco DNA Center で次のコマンドを送信します。

Cisco DNA Center で次のコマンドを ワイヤレスコントローラ 1 に送信します。

- **config interface address redundancy-management 198.51.100.xx peer-redundancy-management 198.51.100.yy**
- **config redundancy unit primary**
- **config redundancy mode sso**

Cisco DNA Center で次のコマンドを ワイヤレスコントローラ 2 に送信します。

- **config interface address redundancy-management 198.51.100.yy peer-redundancy-management 198.51.100.xx**
- **config redundancy unit secondary**
- **config port adminmode all enable**
- **config redundancy mode sso**

ワイヤレスコントローラ から HA 設定を検証するには、次のコマンドを入力します。

- HA 関連の詳細情報を確認する場合：**config redundancy mode sso**
- 設定済みのインターフェイスを確認する場合：**show redundancy summary**

既存の展開での高可用性が設定されたデバイスの無効化

Cisco DNA Center の高可用性無効化機能は、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ と Cisco AireOS コントローラでサポートされています。

始める前に

既存の展開の高可用性デバイスが Cisco DNA Center の外部で設定されていることを確認します。

ステップ 1 メニューアイコン（☰）をクリックして、**[Provision]** > **[Device]** > **[Inventory]** の順に選択します。

[Inventory] ウィンドウが表示され、検出されたデバイスが一覧表示されます。

ステップ 2 無効にする高可用性機能を持つワイヤレスコントローラの名前の横にあるチェックボックスをオンにします。

ステップ 3 [Actions] ドロップダウンリストから、**[Provision]** > **[Configure WLC HA]** を選択します。

[High Availability] ページが表示されます。

[High Availability] ページには、Cisco DNA Center の外部から設定された、選択されたワイヤレスコントローラの**冗長性の概要**が表示されます。

ステップ 4 **[警告（Warning）]** ウィンドウで **[OK]** をクリックします。

選択されたワイヤレスコントローラの高可用性が正常に無効になったことを示す成功メッセージが画面の下部に表示されます。

シスコ製 AP のプロビジョニング：Day 1 AP プロビジョニング

始める前に

- インベントリにシスコの AP があることを確認してください。ない場合は、ディスカバリ機能を使用して AP を検出します。詳細については、ネットワークの検出 （45 ページ）を参照してください。
- 新しい AP ゾーンや SSID を追加する場合は、ワイヤレスコントローラ を再プロビジョニングする必要があります。詳細については、Cisco AireOS コントローラのプロビジョニング （422 ページ）およびCisco Catalyst 9800 シリーズ ワイヤレスコントローラのプロビジョニング （462 ページ）を参照してください。
- AP ゾーンの設定を更新する場合は、ワイヤレスコントローラ を再プロビジョニングする必要があります。詳細については、Cisco AireOS コントローラのプロビジョニング （422 ページ）およびCisco Catalyst 9800 シリーズ ワイヤレスコントローラのプロビジョニング （462 ページ）を参照してください。

ステップ 1 メニューアイコン（≡）をクリックして、**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。

[Inventory] ウィンドウには、検出プロセス中に収集されたデバイス情報が表示されます。

（注） 名前を入力してサイトを検索するか、[Global] を展開してサイトを選択することがします。選択したサイトで使用可能なデバイスが [Inventory] ウィンドウに表示されます。

デバイスファミリや到達可能性ステータスなどのさまざまな基準に基づいてデバイスをフィルタ処理するには、[Filter] をクリックして、必要な選択を行い、[Apply] をクリックします。

ステップ 2 プロビジョニングする AP の横にあるチェックボックスをオンにします。

ステップ 3 [Actions] ドロップダウンリストから、**[Provision]** > **[Provision Device]** の順に選択します。

ステップ 4 [Assign Site] ステップで、次のパラメータを設定します。

a) [Choose a floor] をクリックし、サイトに AP を割り当てます。

b) [Choose a Floor] スライドインペインで、AP が存在するフロアを選択し、[Save] をクリックします。

c) **[Next]** をクリックします。

（注） Cisco DNA Center では、このサイトは AP の場所として設定されません。[Configure Access Points] ワークフローを使用して AP の場所を設定できます。詳細については、AP ワークフローの設定 （791 ページ）を参照してください。

ステップ 5 [Configuration] ステップで、次のパラメータを設定します。

a) [Advanced Configuration] をクリックして、アンテナスロットの無線アンテナプロファイルを設定します。

（注） 高度な設定は、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ ソフトウェア リリース 17.6 以降を搭載した Cisco Catalyst 9130AXE ユニファイド アクセス ポイントでサポートされています。

b) [Slot 1] および [Slot 2] ドロップダウンリストから、AP 無線スロット 1 およびスロット 2 のビーム選択値を設定します。
c) [**保存（Save**）] をクリックします。
d) [AP Zone Name] ドロップダウンリストから、AP ゾーンを選択します。

（注） このドロップダウンリストは、サイトのネットワークプロファイルに AP ゾーンが追加されている場合にのみ有効になります。

AP ゾーンを選択した場合、RF プロファイルが AP ゾーン設定から継承されます。

e) [RF Profile] ドロップダウンリストから、デフォルト設定を使用するか、リストから別の値を選択します。

デフォルトの RF プロファイルは、**[Design] > [Network Settings] > [Wireless] > [Wireless Radio Frequency Profile]** でデフォルトとマークしたカスタムプロファイルです。

（注） [AP Zone] ドロップダウンリストから AP ゾーンを選択した場合、このドロップダウンリストは無効になります。

f) [Mesh Role] ドロップダウンリストで、[Root] または [Mesh] を選択します。
g) [Next] をクリックします。

ステップ 6 [Summary] ステップでデバイスの詳細を確認し、[Deploy] をクリックして AP をプロビジョニングします。

[Provision Device] スライドインペインが表示されます。

ステップ 7 [Provision Device] スライドインペインで、次の手順を実行します。

- 即座にデバイスを展開するには、[Now] オプションボタンをクリックし、[Apply] をクリックします。
- 将来の日付と時刻でデバイスの展開をスケジュールするには、[Later] オプションボタンをクリックし、展開する日時を定義します。
- CLI 設定をプレビューするには、[Generate Configuration Preview] オプションボタンをクリックします。

ステップ 8 AP グループの作成または変更が進行中であることを示すメッセージに続き、プロビジョニング後に AP がリブートすることを示すメッセージが表示されます。[OK] をクリックします。

展開が正常に完了した場合、[Inventory] ウィンドウの [Last Sync Status] 列に「SUCCESS」と表示されます。

FlexConnect モードの AP への ICMP ping の有効化

到達不能状態にある FlexConnect モードの AP への Internet Control Message Protocol（ICMP）ping を有効にすることができます。Cisco DNA Center は、ICMP を使用して、到達不能状態にある FlexConnect AP への ping を 5 分ごとに実行することで到達可能性を強化してから、[Inventory] ウィンドウの到達可能性ステータスを更新します。

ステップ 1 メニューアイコン（☰）をクリックして、**[System]** > **[Settings]** > **[Device Settings]** > **[ICMP Ping]** の順に選択します。

ステップ 2 [Enable ICMP ping for unreachable access Points in FlexConnect mode] チェックボックスをオンにして ICMP ping を有効にします。

ステップ 3 [**保存（Save）**] をクリックします。

「ICMP Ping status updated successfully」という成功メッセージが表示されます。

Cisco DNA Center は、シスコ ワイヤレス コントローラとの関連付けは解除されているが到達可能な FlexConnect AP への ping を開始します。到達可能性ステータスは [Inventory] ウィンドウで確認できます。

ステップ 4 到達可能性ステータスを確認するには、**[Provision]** > **[Inventory]** を選択します。

ステップ 5 デバイスが ICMP ping によって到達可能である場合、[Reachability] 列に [Ping Reachable] と表示されます。

Cisco AireOS Mobility Express AP の Day 0 ワークフロー

始める前に

Cisco Mobility Express ワイヤレス ネットワーク ソリューションは、1 つ以上の 802.11ac Wave 2 Cisco Aironet シリーズのアクセスポイント（AP）と、ネットワーク内のその他の AP を管理する内蔵ソフトウェアベースのワイヤレスコントローラで構成されます。ワイヤレスコントローラとして機能している AP は、「プライマリ *AP*」と呼ばれます。このプライマリ AP によって管理される Cisco Mobility Express ネットワーク内のその他の AP は「従属 *AP*」と呼ばれます。

- サイト、ビルディング、フロアなどのネットワーク階層を設計します。詳細については、ネットワーク階層のサイトの作成（166 ページ）、建物の追加（167 ページ）、および建物への基本フロアの追加（169 ページ）を参照してください。
- CLI、SNMP、HTTP、HTTPS などのデバイスログイン情報をグローバルレベルで定義します。グローバルレベルで定義されたログイン情報は、サイトによって継承されます。詳細については、グローバル CLI クレデンシャルの設定（230 ページ）、グローバル SNMPv2c クレデンシャルの設定（231 ページ）、およびグローバル SNMPv3 クレデンシャルの設定（233 ページ）を参照してください。
- WLAN、インターフェイス、RF プロファイルを作成します。

- DHCP サーバーにオプション #43 とオプション #60 を設定します。これは Cisco DNA Center プラグアンドプレイサーバーの IP アドレスです。この IP アドレスを使用して、AP は PnP サーバーに接続し、設定をダウンロードします。
- インベントリに Mobility Express AP があることを確認してください。ない場合は、[Discovery] 機能を使用して検出します。詳細については、CDP を使用したネットワークの検出 （51 ページ）、IP アドレス範囲を使用したネットワークの検出 （59 ページ）、およびインベントリについて （84 ページ）を参照してください。
- AP は、シスコ ワイヤレス コントローラ 設定なしで初期設定へリセットされた状態である必要があります。

ステップ 1 Cisco Mobility Express は DHCP サーバーに接続し、Cisco DNA Center プラグアンドプレイサーバーに接続します。

ステップ 2 DHCP サーバーは、Cisco DNA Center プラグアンドプレイサーバーの IP アドレスであるオプション #43 で IP アドレスを割り当てます。

ステップ 3 Mobility Express AP は PnP エージェントを開始し、PnP サーバーに接続します。

（注） ネットワーク内に一連の Mobility Express AP がある場合、内部プロトコルを通過します。プロトコルは 1 つの Mobility Express AP を選択します。これは、シスコ ワイヤレス コントローラ で、PnP サーバーに到達するためのプライマリ AP として設定されます。

ステップ 4 **[Provision]** > **[Network Devices]** > **[Plug and Play]** タブで未要求 AP を検索します。

テーブルには、すべての未要求デバイスが一覧表示されます。[State] 列が [Unclaimed] として表示されます。[Filter] または [Find option] を使用して、特定のデバイスを検索することができます。

[Onbording Status] が [Initialized] になるまで待機する必要があります。

ステップ 5 この AP を要求するには、AP デバイス名の横にあるチェックボックスをオンにします。

ステップ 6 デバイステーブルの上にあるメニューバーで、[Actions] > [Claim] の順に選択します。 >

[Claim Devices] ウィンドウが表示されます。

ステップ 7 [Site Assignement] ウィンドウで、[Site] ドロップダウンリストからサイトを選択します。

選択された AP のこの特定のサイトに対する要求は、関連付けられている構成にも適用されます。

ステップ 8 **[次へ (Next)]** をクリックします。

ステップ 9 デバイスを設定するには、[Configuratio] ウィンドウのデバイス名をクリックします。

ステップ 10 [Configuration for device name] ウィンドウで、デバイスの静的 IP の詳細を割り当てます。

- **[Management IP]**
- **[Subnet Mask]**
- **[Gateway]**

ステップ 11 [Save] をクリックします。

ステップ 12 [Next] をクリックします。

[Summary] ウィンドウが表示されます。

ステップ 13 [Summary] ウィンドウで [Claim] をクリックします。

Mobility Express AP が要求されると、設定された IP アドレスが Mobility Express AP に割り当てられます。

要求したデバイス（AP）とワイヤレスコントローラが **[Provision]** > **[Device Inventory]** > **[Inventory]** に表示されることを確認します。

ステップ 14 （オプション）CSV ファイルからデバイスを一括して追加します。

詳細については、デバイスの一括追加 （404 ページ）を参照してください。

CSV を使用して Mobility Express AP を一括インポートすると、すべての Mobility Express AP が **[Device]** > **[Plug and Play]** ウィンドウに表示されます。VRRP プロトコルに基づいて、インポートされた Mobility Express AP のうち 1 台だけがプライマリ AP になります。残りの AP は従属 AP になります。プライマリ AP を要求した後、下位 AP を要求する必要はありません。Cisco DNA Center は、[Plug and Play] ウィンドウから下位 AP をクリアしません。これらの下位 AP は、**[Devices]** > **[Plug and Play]** ウィンドウから手動で削除する必要があります。

ステップ 15 シスコ ワイヤレス コントローラ をプロビジョニングするには、Cisco AireOS コントローラのプロビジョニング （422 ページ） を参照してください。

既存の展開での Cisco AireOS コントローラのプロビジョニング

始める前に

Cisco DNA Center を使用すると、既存サイトの以前から存在しているインフラストラクチャに属している シスコ ワイヤレス コントローラ を追加してプロビジョニングできます。

- 初めに、デバイスについてディスカバリを実行します。すべてのデバイスが [インベントリ（Inventory）] ウィンドウに表示されます。詳細については、ネットワークの検出 （45 ページ）およびインベントリについて （84 ページ）を参照してください。
- ワイヤレスコントローラ は到達可能で、 [インベントリ（Inventory）] ウィンドウで管理状態でなければなりません。詳細については、インベントリについて （84 ページ）を参照してください。

ステップ 1 メニューアイコン（≡）をクリックして、**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。

[Inventory] ウィンドウが表示され、検出されたデバイスが一覧表示されます。

ステップ 2 [フィルタ（Filter）] をクリックして、選択したフィルタ フィールドに適切な値を入力します。たとえば、[デバイス名（Device Name）] フィルタの場合、デバイスの名前を入力します。

[デバイス（Devices）]テーブルに表示されるデータは、選択したフィルタに従って自動で更新されます。

ステップ 3 プロビジョニングする ワイヤレスコントローラ デバイス名の横にあるチェックボックスをオンにします。

ステップ 4 [Actions] ドロップダウンリストから、**[Provision]** > **[Learn Device Config]** の順に選択します。

ステップ 5 [Assign Site] ステップで、サイトをコントローラに関連付けます。

a) [Choose a site] をクリックして、コントローラにサイトを割り当てます。

b) [Choose a site] スライドインペインで、ワイヤレスコントローラ を関連付けるサイトを選択し、[Save] をクリックします。

c) [Next] をクリックします。

ステップ 6 [Resolve Conflict] ステップに、解決する必要がある Cisco DNA Center の競合する設定が表示されます。

ステップ 7 [Next]をクリックします。

ステップ 8 [Design Object] ウィンドウに、学習したすべての設定が一覧表示されます。

a) 左ペインで [Network] をクリックします。

右側のペインに、デバイス設定学習の一部として学習されたネットワーク設定と、次の情報が表示されます。

- **[** AAA サーバー（AAA Server） **]** の詳細。
- システム設定。AAA サーバーの IP アドレスとプロトコルについての詳細情報を含みます。
- [DHCP Server] の詳細。
- AAA サーバーの共有秘密を入力します。

b) 左ペインで [ワイヤレス（Wireless）] をクリックします。

右側のペインには、企業 SSID、ゲスト SSID、アンテナ無線プロファイル、およびワイヤレスインターフェイスの詳細が一覧表示されます。

事前共有キー（PSK）を使用する SSID の場合、事前共有キーを入力します。

c) 左ペインで [破棄された設定（Discarded Config）] をクリックします。

右ペインに、Cisco DNA Center 上で競合する設定、または既に存在する設定が一覧表示されます。破棄された設定エントリは、次のように分類されます。

- 設計エンティティの重複
- 無線ポリシーの不明なデバイス設定

d) [Next]をクリックします。

[ネットワーク プロファイル（Network Profile）] ウィンドウに、AP と WLAN の組み合わせに基づいて作成されたネットワーク プロファイルまたはサイト プロファイルが一覧表示されます。

e) **[Save]** をクリックします。

ステップ 9 **[Design]** > **[Network Profile]** を選択して、サイトをネットワークプロファイルに割り当てます。

ステップ 10 [Network Profiles] ウィンドウで、次の項目を設定します。

a) [Assign Site] をクリックして、選択したプロファイルにサイトを追加します。

b) [サイトをプロファイルに追加（Add Sites to Profile）] ウィンドウでドロップダウンリストからサイトを選択して、[保存（Save）] をクリックします。

ステップ 11 メニューアイコン（☰）をクリックして、**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。

a) [Filter] をクリックして、プロビジョニングするデバイスを見つけます。

[デバイス（Devices）] テーブルに表示されるデータは、選択したフィルタに従って自動で更新されます。

b) プロビジョニングするコントローラ デバイス名の隣にあるチェック ボックスをオンにします。

c) [アクション（Actions）] ドロップダウン リストから、[プロビジョニング（Provision）]を選択します。

d) [サイトの割り当て（Assign Site）] ウィンドウで詳細を確認して、[次へ（Next）] をクリックします。

[Configurations] ステップが表示されます。

e) [インターフェイスと VLAN の設定（Interface and VLAN Configuration）] で、[+ 追加（+ Add）] をクリックしてインターフェイスと VLAN の詳細を設定します。

f) [インターフェイスと VLAN の設定（Configure Interface and VLAN）] ウィンドウで必要なフィールドを設定して、[OK] をクリックします。

g) [Next] をクリックします。

ステップ 12 次の情報が表示される [Summary] ステップを確認します。

- **Device Details**
- **ネットワークの設定**
- **SSID**
- **Managed Sites**
- **Interfaces**

ステップ 13 [展開（Deploy）] をクリックします。

ステップ 14 [Provision Devices] スライドインペインで、次の手順を実行して CLI 設定をプレビューします。

- [Generate Configuration Preview] オプションボタンをクリックします。
- [Task Name] フィールドに、CLI プレビュータスクの名前を入力し、[Apply] をクリックします。
- [Task Submitted] ポップアップで、[Work Items] リンクをクリックします。

（注） [Task Submitted] ポップアップが表示されなかった場合は、メニューアイコン（☰）をクリックし、**[Activities]** > **[Work Items]** の順に選択します。

- [Work Items] ウィンドウで、設定プレビュー要求を送信した CLI プレビュータスクをクリックします。

- CLI 設定の詳細を表示し、[Deploy] をクリックします。
- 即座にデバイスを展開するには、[Now] オプションボタンをクリックし、[Apply] をクリックします。
- 将来の日付と時刻でデバイスの展開をスケジュールするには、[Later] オプションボタンをクリックし、展開する日時を定義します。
- [Information] ポップアップで、次の手順を実行します。
  - [Work Items] ウィンドウから CLI プレビュータスクを削除する場合は、[Yes] をクリックします。
  - [Work Items] ウィンドウでタスクを保持する場合は、[No] をクリックします。

（注） CLI タスクは、[Work Items] ウィンドウで完了済みとしてマークされます。このタスクの CLI 設定は表示することはできますが、再度展開することはできません。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの設定とプロビジョニング

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの概要

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラは、インテントベース ネットワーク用に構築された次世代のワイヤレスコントローラです。Cisco Catalyst 9800 シリーズ ワイヤレス コントローラは Cisco IOS XE ベースであり、Aironet の優れた RF 性能と Cisco IOS XE のインテントベースのネットワーキング機能を統合して、組織にクラス最高水準のワイヤレスエクスペリエンスを生み出します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラはモジュール型オペレーティングシステムに基づいて構築され、オープンでプログラマブルな API 機能が搭載されていて、0 日目から N 日目のネットワーク運用を自動化できます。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラは、次のような複数のフォームファクタで使用できます。

- Catalyst 9800-40 ワイヤレスコントローラ。
- Catalyst 9800-80 ワイヤレスコントローラ。
- Catalyst 9800-CL Cloud ワイヤレスコントローラ：プライベートクラウド（ESXi、KVM、Cisco ENCS、および Hyper-V）に展開可能、Cisco DNA Center で管理可能。
- Catalyst 9300 シリーズ スイッチ、Catalyst 9400 シリーズ スイッチ、および Catalyst 9500H シリーズ スイッチ用 Catalyst 9800 組み込みワイヤレスコントローラ。
- Cisco Catalyst 9800-L ワイヤレスコントローラ：中小企業向けにシームレスなソフトウェアアップデートを提供します。Cisco Catalyst 9800-L ワイヤレスコントローラは 2 つのバリ

エーションで使用できます。銅線と光ファイバアップリンクのいずれかを選択でき、ネットワークの柔軟性が向上します。

次の表に、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラでサポートされている仮想プラットフォームおよびハードウェア プラットフォームを一覧表示します。

プラットフォーム	説明
Cisco Catalyst 9800-80 ワイヤレスコントローラ	最大 6000 アクセスポイントと 64,000 クライアントをサポートします。 最大 80 Gbps のスループットをサポートし、2 ラックユニットスペースを使用します。 最大 100-GE のアップリンクおよびシームレスなソフトウェアアップデートを搭載したモジュール型ワイヤレスコントローラ。
Cisco Catalyst 9800-40 ワイヤレスコントローラ	シームレスなソフトウェアアップデートを備えた、中小企業やキャンパスでの導入向けの固定ワイヤレスコントローラ。 最大 2000 アクセスポイントと 32,000 クライアントをサポートします。 最大 40 Gbps のスループットをサポートし、1 ラックユニットスペースを使用します。 4 つの 1-GE または 10-GE アップリンクポートを提供します。
Cisco Catalyst 9800-CL Cloud ワイヤレス コントローラ	Cisco Catalyst 9800-CL クラウド ワイヤレス コントローラは、プライベートクラウドまたはパブリッククラウドに Infrastructure as a Service（IaaS）として導入できます。 Cisco Catalyst 9800-CL クラウド ワイヤレス コントローラは、ハイアベイラビリティとセキュリティを実現するために構築された次世代のエンタープライズクラスの仮想ワイヤレスコントローラです。 Cisco Catalyst 9800-CL クラウド ワイヤレスコントローラの仮想フォームファクタは、ESXi、KVM、Cisco ENCS、および Hyper-V ハイパーバイザをサポートするプライベートクラウド向けです。
Catalyst 9000 シリーズスイッチ用 Cisco Catalyst 9800 組み込みワイヤレスコントローラ	Catalyst 9000 シリーズスイッチ用 Cisco Catalyst 9800 組み込みワイヤレスコントローラは、有線およびワイヤレス インフラストラクチャを一貫したポリシーと管理とともに提供します。 この導入モデルは、小規模キャンパスや分散型ブランチ向けの安全性に優れたソリューションである Cisco SD-Access でのみサポートされます。組み込みコントローラは、ファブリックモードでのみアクセスポイント（AP）をサポートします。

プラットフォーム	説明
Cisco Catalyst 9800-L ワイヤレス コントローラ	Cisco Catalyst 9800-L ワイヤレスコントローラは、中小企業向けにシームレスなソフトウェアアップデートを提供します。Cisco Catalyst 9800-L ワイヤレスコントローラは 2 つのバリエーションで使用できます。銅線と光ファイバアップリンクのいずれかを選択でき、ネットワークの柔軟性が向上します。 • Cisco Catalyst 9800-L Copper シリーズ ワイヤレス コントローラ（9800-L-C RJ45） • Cisco Catalyst 9800-L ファイバ シリーズ ワイヤレス コントローラ（9800-L-F SFP）

次の表に、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラでサポートされているホスト環境を一覧表示します。

ホスト環境	ソフトウェア バージョン
VMware ESXi	• VMware ESXi vSphere 6.0 • VMware ESXi vSphere 6.5[3] • VMware ESXi vCenter 6.0 • VMware ESXi VCenter 6.5
KVM	• Red Hat Enterprise Linux 7.1 および 7.2 をベースとした Linux KVM • Ubuntu 14.04.5 LTS、Ubuntu 16.04.5 LTS
NFVIS	Cisco ENCS 3.8.1 および 3.9.1

[3] ESXi vSphere を使用した C9800-CL の .ova ファイルのインストールは機能しません。これは C9800 ova に限定されませんが、他の製品に影響します。シスコと VMware は、問題解決に向けて積極的に取り組んでいます。問題が修正されたかどうかを確認するには、シスコのアカウント担当者にお問い合わせください。VMware 6.5 および C9800-CL OVA ファイルの展開に固有の問題があります。「必要なディスクイメージがありません。（A required disk image was missing）」という警告が表示され、「VM の展開に失敗しました：postNFCData に失敗しました：ディスク以外のファイルに POST できません。（Failed to deploy VM: postNFCData failed: Cannot POST to non-disk files.）」というエラーで展開が失敗します。VMware ESXi 6.5 に C9800-CL をインストールするには、次のいずれかを実行します。1）ESXi 組み込み GUI を使用して C9800-CL の .iso ファイルをインストールする（ESXI 6.5 クライアントバージョン 1.29.0 はテスト済みで必須）。2）OVF ツールを使用して C9800-CL の .ova ファイルをインストールする。

次の表に、Cisco DNA Center でサポートされている Cisco Enterprise Network Function Virtualization Infrastructure Software（NFVIS）のバージョンを示します。

（注） Cisco Enterprise NFVIS デバイスは、N-1 から N へのアップグレードパスのみをサポートします。たとえば、Cisco Enterprise NFVIS 3.11.x からは Cisco Enterprise NFVIS 3.12.x へのアップグレードのみがサポートされています。Cisco Enterprise NFVIS 3.11.x から Cisco Enterprise NFVIS 4.1.x へのアップグレードはサポートされていません。

Cisco Enterprise NFVIS バージョン	エンタープライズ ネットワーク コンピューティング システム デバイス プラットフォーム	注記
4.1.2 4.1.1 3.12.3 3.11.3 3.11.2 3.11.1	ENCS 5400 UCS-E UCS-C	Cisco DNA Center は、次の NFVIS アップグレードパスをサポートします。NFVIS v3.11.1 > 3.11.2 > 3.11.3 > 3.12.3 > 4.1.1 > 4.1.2。 Cisco Enterprise NFVIS 3.12.1 は、Cisco DNA Center のいずれのバージョンでもサポートされていません。 Cisco DNA Center を使用した、Cisco Enterprise NFVIS 3.11.x から Cisco Enterprise NFVIS 3.12.1 へのアップグレードはサポートされていません。 Cisco DNA Center を使用した、Cisco Enterprise NFVIS 3.12.1 から Cisco Enterprise NFVIS 3.12.2 へのアップグレードはサポートされていません。 Cisco DNA Center を使用した、Cisco Enterprise NFVIS 3.11.2 から 3.12.2 へのアップグレードはサポートされていません。 Cisco Enterprise NFVIS 3.12.2 は、Cisco DNA Center でサポートされています。
3.12.2 3.11.3 3.11.2 3.11.1	ENCS 5100	Cisco 5100 ENCS は、Cisco Enterprise NFVIS 3.10.x をサポートしていません。

Cisco DNA Center で Cisco Catalyst 9800 ワイヤレスコントローラを設定するためのワークフロー

1. Cisco DNA Center をインストールします。

   詳細については、『CISCO DNA Center インストール ガイド』を参照してください。

2. ソフトウェアイメージのアップグレードに関する詳細については、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラでのソフトウェアイメージのアップグレードのサポート（444 ページ） を参照してください。

3. Cisco DNA Center GUI にログインし、必要なアプリケーションが [Running] 状態であることを確認します。

   メニューアイコン（☰）をクリックして、**[System Settings]** > **[Software Updates]** > **[Installed Apps]** の順に選択します。

4. Cisco Identity Services Engine と Cisco DNA Center を連動させます。統合後、関連する設定やデータとともに Cisco DNA Center が検出されたデバイスは、Cisco ISEにプッシュされます。

5. Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ を検出します。

   Cisco Catalyst 9800 シリーズ ワイヤレス コントローラを検出するには、NETCONF を有効にしてポートを 830 に設定する必要があります。NETCONF は、ネットワークデバイスの設定をインストール、操作、削除するためのメカニズムです。

   詳細については、CDP を使用したネットワークの検出 （51 ページ）またはIP アドレス範囲を使用したネットワークの検出 （59 ページ）を参照してください。

   ワイヤレス管理 IP アドレスを手動で追加する必要があります。

   [Discovery] ウィンドウで Cisco Discovery Protocol（CDP）または IP アドレス範囲を使用して検出を実行する場合は、[Preferred Management IP] ドロップダウンリストから [Use Loopback] を選択して、デバイスのループバック インターフェイスの IP アドレスを指定します。

6. 検出されたデバイスが [Device Inventory] ページに [Managed] 状態で表示されていることを確認します。

   詳細については、インベントリについて （84 ページ）およびインベントリに関する情報の表示 （85 ページ）を参照してください。

   デバイスが [Managed] 状態になるまで待機する必要があります。

7. Cisco Catalyst 9800 シリーズ ワイヤレス コントローラとのアシュアランス接続を確認するには、次のコマンドを使用します。

   - **#show crypto pki trustpoints | sec DNAC-CA**

   ```
   Trustpoint DNAC-CA
       Subject Name:
       cn=kube-ca
             Serial Number (hex): 00E***************
       Certificate configured.
   ```

   - **#show crypto pki trustpoints | sec sdn-network**

   ```
   Trustpoint sdn-network-infra-iwan:
       Subject Name:
       cn=sdn-network-infra-ca
   ```

```
        Serial Number (hex): 378***************
    Certificate configured.
```

- **#show telemetry ietf subscription all**

```
Telemetry subscription brief

  ID               Type        State       Filter type
  ------------------------------------------------------
  1011             Configured  Valid       tdl-uri
  1012             Configured  Valid       tdl-uri
  1013             Configured  Valid       tdl-uri
```

- **#show telemetry internal connection**

```
Telemetry connection

Address Port Transport State Profile
------------------------------------------------------
IP address 25103 tls-native Active sdn-network-infra-iwan
```

- **#show network-assurance summary**

```
Network-Assurance                       : True
Server Url                              : https://10.***.***.***
ICap Server Port Number                 : 3***
Sensor Backhaul SSID                    :
Authentication                          : Unknown
```

8. 認証サーバーとポリシーサーバーの設定時に TACACS サーバーを設定します。

   Cisco Catalyst 9800 シリーズ ワイヤレス コントローラでユーザー名をローカルに設定している場合、TACACS の設定は必須ではありません。

9. サイト、ビルディング、フロアを追加してネットワーク階層を設計すると、後で設計の設定や構成を適用する場所を簡単に特定できるようになります。

   新しいネットワーク階層を作成します。または Cisco Prime Infrastructure に既存のネットワーク階層がある場合は、それを Cisco DNA Center にインポートできます。

   既存のネットワーク階層をインポートしてアップロードするには、Cisco DNA Center へのサイト階層のインポート （159 ページ）を参照してください。

   新しいネットワーク階層を作成するには、ネットワーク階層のサイトの作成 （166 ページ）および建物の追加 （167 ページ）を参照してください。

10. AP の位置情報を追加し、フロアマップに配置して、ヒートマップカバレッジを可視化します。

    詳細については、「フロアマップでの AP の操作 （178 ページ）」を参照してください。

11. AAA（Cisco ISE がネットワークとクライアントエンドポイント向けに設定されている）、NetFlow コレクタ、NTP、DHCP、DNS、syslog、SNMP トラップなどのネットワーク設定を定義します。これらのネットワークサーバーが、ネットワーク全体のデフォルトになります。AAA サーバーを追加するときに、TACACS サーバーを追加できます。

    詳細については、ネットワーク設定の概要 （227 ページ）、グローバル ネットワーク サーバーの設定 （230 ページ）、および「Cisco ISE またはその他の AAA サーバーの追加」を参照してください。

12. カスタムとして、親プロファイルでワイヤレス無線周波数プロファイルを作成します。

    詳細については、「ワイヤレス無線周波数プロファイルの作成 （268 ページ）」を参照してください。

13. IP アドレスプールをグローバルレベルで作成します。

    Cisco DNA Center Cisco DNA Center は、IP アドレスプールを使用して、SD-Access ネットワークの設定と展開を自動化します。

    IP アドレスプールを作成するには、IP アドレス プールを設定する （241 ページ）を参照してください。

    プロビジョニングするビルディング用に IP アドレスプールを予約する必要があります。詳細については、「LAN 自動化によるネットワークのプロビジョニング」を参照してください。

14. エンタープライズおよびゲスト ワイヤレス ネットワークを作成します。グローバルワイヤレス設定を 1 回定義します。次に、Cisco DNA Centerは地理的な場所全体でさまざまなデバイスに設定をプッシュします。

    ワイヤレスネットワークの設計は、2 段階のプロセスです。まず SSID を作成し、次に作成した SSID をワイヤレス ネットワーク プロファイルに関連付ける必要があります。このプロファイルは、サイトにデバイスを展開するために使用されるトポロジを構築するのに役に立ちます。

    詳細については、エンタープライズ ワイヤレス ネットワーク用 SSID の作成 （248 ページ）およびゲスト ワイヤレス ネットワークの SSID の作成 （256 ページ）を参照してください。その他のワイヤレス設定については、グローバル ワイヤレス設定の構成 （247 ページ）を参照してください。

15. バックホールの設定を行います。詳細については、「バックホールの設定の管理 （285 ページ）」を参照してください。

16. Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの [Policy] ウィンドウで、次のように設定します。

    - 仮想ネットワークを作成します。仮想ネットワークを使用して、物理ネットワークを複数の論理ネットワークにセグメント化できます。
    - グループベースのアクセス コントロール ポリシーを作成し、契約を追加する。詳細については、「グループベースのアクセス コントロール ポリシーの作成 （614 ページ）」を参照してください。

17. 高可用性を設定します。

    詳細については、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラで高可用性を設定する （445 ページ）」を参照してください。

18. 設計フェーズ中に追加された設定を使用して、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ をプロビジョニングします。

詳細については、「Cisco Catalyst 9800 シリーズ ワイヤレスコントローラのプロビジョニング （462 ページ）」を参照してください。

19. Cisco Catalyst 9800 シリーズ ワイヤレス コントローラでアプリケーションポリシーを設定および展開します。

詳細については、アプリケーション ポリシーの作成 （660 ページ）、アプリケーション ポリシーの展開 （666 ページ）、およびアプリケーション ポリシーの編集 （664 ページ）を参照してください。

（注） アプリケーションポリシーを展開する前に、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラデバイスをプロビジョニングする必要があります。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ デバイスの場合、2 つの異なる SSID で異なるビジネスとの関連性を持つ2つの異なるポリシーは機能しません。関連性を設定するときは、最後に展開したポリシーが常に優先されます。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ デバイスの場合、アプリケーションのデフォルトのビジネスとの関連性を変更しても、FlexConnect モードでは機能しません。

非ファブリック SSID にのみアプリケーションポリシーを適用できます。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラでのソフトウェアイメージのアップグレードのサポート

始める前に

- Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ を検出します。

  Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ を検出するには、NETCONF を有効にしてポートを 830 に設定します。NETCONF は、ネットワークデバイスの設定をインストール、操作、削除するためのメカニズムです。これにより、コントローラでワイヤレスサービスが有効になります。

  詳細については、CDP を使用したネットワークの検出 （51 ページ）またはIP アドレス範囲を使用したネットワークの検出 （59 ページ）を参照してください。

- デバイスが [Device Inventory] に [Managed] 状態で表示されていることを確認します。

  詳細については、インベントリについて （84 ページ）およびインベントリに関する情報の表示 （85 ページ）を参照してください。

ステップ 1 メニューアイコン（☰）をクリックして、**[Design]** > **[Image Repository]**。

[Inventory] ウィンドウが表示され、検出されたデバイスが一覧表示されます。

ステップ 2 ローカルコンピュータまたは URL から、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ ソフトウェアイメージをインポートします。

詳細については、「ソフトウェア イメージのインポート （360 ページ）」を参照してください。

ステップ 3 ソフトウェアイメージをデバイスファミリに割り当てます。

詳細については、「デバイスファミリへのソフトウェアイメージの割り当て （361 ページ）」を参照してください。

ステップ 4 デバイスファミリまたは特定のデバイスロールの星印をクリックして、ソフトウェアイメージをゴールデンとしてマークできます。

詳細については、「ゴールデン ソフトウェア イメージの指定 （363 ページ）」を参照してください。

ステップ 5 ソフトウェアイメージのプロビジョニング

メニューアイコン（☰）をクリックして、**[Provision]** > **[Device]** > **[Inventory]** の順に選択します。

ステップ 6 [Inventory] ウィンドウで、イメージをアップグレードする Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の横にあるチェックボックスをオンにします。

ステップ 7 [Actions] ドロップダウンリストから、**[Software Image]** > **[Update Image]** の順に選択します。

詳細については、ソフトウェア イメージのプロビジョニング （366 ページ）を参照してください。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラで高可用性を設定する

始める前に

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラで高可用性（HA）を設定するには、次の前提条件を満たす必要があります。

- 両方の Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ デバイスが同じソフトウェアバージョンを実行していて、プライマリ Catalyst 9800 シリーズ ワイヤレス コントローラ上にアクティブなソフトウェアイメージがあります。
- Catalyst 9800 シリーズ ワイヤレス コントローラ 1 と Catalyst 9800 シリーズ ワイヤレス コントローラ 2 のサービスポートおよび管理ポートが設定されています。
- Catalyst 9800 シリーズ ワイヤレス コントローラ 1 および Catalyst 9800 シリーズ ワイヤレス コントローラ 2 の冗長ポートが物理的に接続されています。
- インターフェイス設定、ルート追加、SSH回線設定、NETCONF-YANG設定などの事前設定は、Catalyst 9800 シリーズ ワイヤレス コントローラアプライアンスで完了します。
- Catalyst 9800 シリーズ ワイヤレス コントローラ 1 と Catalyst 9800 シリーズ ワイヤレス コントローラ 2 の管理インターフェイスは同じサブネット内にあります。

- Catalyst 9800 シリーズ ワイヤレス コントローラ 1 デバイスおよび Catalyst 9800 シリーズ ワイヤレス コントローラ 2 デバイスのディスカバリとインベントリは、Cisco DNA Center から正常に実行されます。
- デバイスは到達可能で、[Managed] 状態になっています。

ステップ 1 メニューアイコン（☰）をクリックして、**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。

[Inventory] ウィンドウが表示され、検出されたデバイスが一覧表示されます。

ステップ 2 特定のサイトで使用可能なデバイスを表示するには、左側のペインで [Global] サイトを展開し、関心のあるサイト、ビルディング、またはフロアを選択します。

選択したサイトで使用可能なすべてのデバイスが [Inventory] ウィンドウに表示されます。

ステップ 3 [Device Type] リストから [WLCs] タブをクリックし、[Reachability] リストから [Reachable] タブをクリックして、検出済みで到達可能なワイヤレスコントローラのリストを取得します。

ステップ 4 [Inventory] ウィンドウで目的の Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ 名をクリックし、プライマリコントローラとして設定します。

ステップ 5 [High Availability] タブをクリックします

デフォルトで選択された Catalyst 9800 シリーズ ワイヤレス コントローラがプライマリコントローラになり、[Primary C9800] フィールドはグレー表示されます。

ステップ 6 [Select Primary Interface] および [Secondary Interface] ドロップダウンリストから、HA 接続に使用するインターフェイスを選択します。

HA インターフェイスは次の目的で使用されます。

- IOSd が起動する前に、コントローラペア間の通信を有効にする。
- すべてのコントローラペアに IPC のトランスポートを提供する。
- コントローラペア間で交換される制御メッセージ全体の冗長性を有効にする。制御メッセージには、HA ロールの解決、キープアライブ、通知、HA 統計情報などがあります。

ステップ 7 [Select Secondary C9800] ドロップダウン リストから、HA ペアを作成するセカンダリコントローラを選択します。

（注） プライマリコントローラのワイヤレス管理インターフェイス IP サブネットに基づいてセカンダリコントローラを選択すると、冗長性管理 IP が自動入力され、**[High Availability]** ウィンドウの上部に **[i]** アイコンが表示され、次のメッセージが表示されます。「冗長性管理 IP とピア冗長性管理 IP が他のネットワークエンティティに割り当てられていないことを確認してください。**使用する場合は、IP を適宜変更して設定します**」。

ステップ 8 各フィールドに [Redundancy Management IP] と [Peer Redundancy Management IP] のアドレスを入力します。

（注） 冗長性管理 IP およびピア冗長性管理 IP に使用される IP アドレスは、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの管理インターフェイスと同じサブネットに設定する必要があります。これらの IP アドレスがそのサブネット範囲内で未使用の IP アドレスであることを確認します。

ステップ 9 [Netmask] フィールドに、ネットマスクアドレスを入力します。

ステップ 10 [Configure HA] をクリックします。

HA設定は、CLIコマンドを使用してバックグラウンドで開始されます。最初に、プライマリコントローラが設定されます。成功すると、セカンダリコントローラが設定されます。HAが有効になると、両方のデバイスが再起動します。このプロセスは、完了するまで最大 2.5 分かかります。

ステップ 11 HA が開始されたら、[High Availability] タブの [Redundancy Summary] に、[Sync Status] が [HA Pairing is in Progress]として表示されます。HA ペアリングが成功したことを Cisco DNA Center が検出すると、[Sync Status] が [Complete] になります。

これは、インベントリポーラーまたは手動による再同期によってトリガーされます。これで、セカンダリコントローラ（Catalyst 9800 シリーズ ワイヤレス コントローラ 2）が Cisco DNA Center から削除されます。このフローは、Catalyst 9800 シリーズ ワイヤレス コントローラ での正常な HA 設定を示しています。

ステップ 12 手動でコントローラを再同期するには、**[Provision]** > **[Inventory]** ウィンドウで、手動で同期するコントローラを選択します。

ステップ 13 [Actions] ドロップダウンリストから、[Resync] を選択します。

ステップ 14 プロセスが完了した後に発生するアクションのリストを次に示します。

- Catalyst 9800 シリーズ ワイヤレス コントローラ 1 および Catalyst 9800 シリーズ ワイヤレス コントローラ 2 は、冗長性管理、冗長性単位、およびシングルサインオン（SSO）を使用して設定されます。デバイスは、ロールをアクティブコントローラまたはスタンバイコントローラとしてネゴシエートするために再起動します。設定はアクティブからスタンバイへと同期されます。
- [冗長性の概要の表示（Show Redundancy Summary）] ウィンドウで、次の設定を確認できます。
  - SSO は有効
  - Catalyst 9800 シリーズ ワイヤレス コントローラ 1 がアクティブ状態である
  - Catalyst 9800 シリーズ ワイヤレス コントローラ 2 がスタンバイ状態である

ハイ アベイラビリティについて

高可用性（HA）によって、コントローラのフェールオーバーが原因で生じるワイヤレスネットワークのダウンタイムを短縮できます。Cisco DNA Center を介して Cisco Catalyst 9800 シリーズ ワイヤレス コントローラで高可用性を設定できます。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラで高可用性を設定するためのコマンド

ステップ 1 次のコマンドを使用して、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのプライマリで HA を設定します。

- **chassis ha-interface GigabitEthernet <redundancy interface num> local-ip <redundancy ip> <netmask> remote-ip <peer redundancy ip>** コマンドを実行して、HA シャーシインターフェイスを設定します。

  次に、HA シャーシインターフェイスの設定例を示します。

  ```
  chassis ha-interface GigabitEthernet 3 local-ip 192.0.2.2 255.255.255.0
  remote-ip 192.0.2.3
  ```

- **reload** コマンドを実行して、変更が有効になるようにデバイスをリロードします。

ステップ 2 次のコマンドを使用して、Catalyst 9800 シリーズ ワイヤレス コントローラのセカンダリで HA を設定します。

- **chassis ha-interface GigabitEthernet <redundancy interface num> local-ip <redundancy ip> <netmask> remote-ip <peer redundancy ip>** コマンドを実行して、HA シャーシインターフェイスを設定します。

  次に、HA シャーシインターフェイスの設定例を示します。

  ```
  chassis ha-interface GigabitEthernet 2 local-ip 192.0.2.3 255.255.255.0
  remote-ip 192.0.2.2
  ```

ステップ 3 **chassis clear** コマンドを実行して、すべての HA 関連のパラメータ（ローカル IP、リモート IP、HA インターフェイス、マスク、タイムアウト、プライオリティなど）をクリアまたは削除します。

（注） **reload** コマンドを実行して、変更を反映するためにデバイスをリロードします。

ステップ 4 Cisco Catalyst 9800-40 ワイヤレスコントローラおよび Cisco Catalyst 9800-80 ワイヤレス コントローラ デバイスのプライマリに HA を設定するには、次のコマンドを使用します。

- HA シャーシインターフェイスを設定するには、**chassis ha-interface local-ip <redundancy ip> <netmask> remote-ip <peer redundancy ip>** コマンドを実行します。

  次に、HA シャーシインターフェイスの設定例を示します。

  ```
  chassis ha-interface local-ip 192.0.2.2 255.255.255.0 remote-ip 192.0.2.3
  ```

- **reload** コマンドを実行して、変更が有効になるようにデバイスをリロードします。

ステップ 5 次のコマンドを使用して、Cisco Catalyst 9800-40 ワイヤレス コントローラおよび Cisco Catalyst 9800-80 ワイヤレス コントローラ デバイスのセカンダリに HA を設定します。

- HA シャーシインターフェイスを設定するには、**chassis ha-interface local-ip <redundancy ip> <netmask> remote-ip <peer redundancy ip>** コマンドを実行します。

  次に、HA シャーシインターフェイスの設定例を示します。

```
chassis ha-interface local-ip 192.0.2.3 255.255.255.0 remote-ip 192.0.2.2
```

ステップ 6 **chassis clear** コマンドを実行して、すべての HA 関連のパラメータ（ローカル IP、リモート IP、HA インターフェイス、マスク、タイムアウト、プライオリティなど）をクリアまたは削除します。

（注） **reload** コマンドを実行して、変更を反映するためにデバイスをリロードします。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの高可用性を確認するためのコマンド

次のコマンドを使用して、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラから高可用性設定を検証します。

- **config redundancy mode sso** コマンドを実行して、HA 関連の詳細情報を確認します。
- **show chassis** コマンドを実行して HA ペアのシャーシ設定を表示します。これには、MAC アドレス、ロール、スイッチプライオリティ、および冗長 HA ペア内の各コントローラデバイスの現在の状態が含まれています。
- **show ip interface brief** コマンドを実行して、プラットフォームで設定されている設定モードではなく、デバイスで実行されている実際に稼働中の冗長モードを表示します。
- **show redundancy states** コマンドを実行して、アクティブコントローラとスタンバイコントローラの冗長性状態を表示します。
- **show redundancy summary** コマンドを実行して、設定されているインターフェイスを確認します。
- ハイアベイラビリティ設定の詳細を確認するには、**show romvar** コマンドを実行します。

N+1 高可用性

N+1 高可用性の概要

Cisco DNA Center では、Cisco AireOS ワイヤレスコントローラおよび Cisco Catalyst 9800 シリーズ ワイヤレス コントローラでの N+1 高可用性（HA）がサポートされています。

Cisco AireOS ワイヤレスコントローラには、N+1 コントローラ向けの専用の型番（SKU）があります。Cisco Catalyst 9800 シリーズ ワイヤレス コントローラには専用の SKU がありません。HA には同じモデルを使用する必要があります。

N+1 HA アーキテクチャは、低い導入コストで、地理的に離れたデータセンター間のコントローラに冗長性をもたらします。

N+1 HA では、シスコ ワイヤレス コントローラを複数のプライマリコントローラのバックアップコントローラとして使用できます。これらのワイヤレスコントローラは互いに独立していて、インターフェイスの設定や IP アドレスを共有しません。AP フォールバックオプションが

有効の場合、プライマリ ワイヤレスコントローラが動作を再開すると、APはバックアップ ワイヤレスコントローラからプライマリ ワイヤレスコントローラに自動的にフォールバックします。

Cisco DNA Center Cisco DNA Center は、N+1 HA のプライマリおよびセカンダリコントローラの設定をサポートします。

N+1 HA は、グローバルレベルではなく AP レベルで設定されます。設定はAPに直接プッシュされます。

（注） プライマリコントローラとセカンダリコントローラは、同じデバイスタイプである必要があります。たとえば、プライマリデバイスが Catalyst 9800 シリーズ ワイヤレス コントローラの場合は、セカンダリデバイスも Catalyst 9800 シリーズ ワイヤレス コントローラにする必要があります。

プライマリコントローラで高い優先順位が設定されている AP は、優先順位の低い AP が排除されることになっても、常に最初にバックアップコントローラに接続されます。

N+1 HA 設定には次の制限があります。

- VLAN ID の設定が原因で、セカンダリコントローラの自動プロビジョニングはサポートされていません。
- プライマリコントローラに変更を加えた場合、最新の設計の設定を使用してセカンダリコントローラを手動で再プロビジョニングする必要があります。
- Cisco DNA Center Cisco DNA Center では耐障害性はサポートされていません。
- アクセスポイントのステートフル スイッチ オーバー（AP SSO）機能は、N+1 HA ではサポートされていません。AP Control and Provisioning of Wireless Access Points（CAPWAP）ステートマシンは、プライマリコントローラに障害が発生したときに再起動されます。

Cisco DNA Center から N+1 高可用性を設定するための前提条件

- [Discovery] 機能を実行して、プライマリコントローラとセカンダリコントローラを検出します。

  詳細については、CDP を使用したネットワークの検出 （51 ページ）またはIP アドレス範囲を使用したネットワークの検出 （59 ページ）を参照してください。

- ワイヤレスコントローラが到達可能で、[Managed] 状態である必要があります。

  詳細については、インベントリについて （84 ページ）およびインベントリに関する情報の表示 （85 ページ）を参照してください。

- デバイス間のネットワーク接続を確認します。プライマリコントローラがダウンしたときに、AP が N+1 の設定に従ってセカンダリコントローラに参加できるようにする必要があります。

- 2 つのビルディングを作成して、両方のデバイスのプライマリおよびセカンダリの場所を管理します。たとえば、ビルディング *A* とビルディング *B* という 2 つのビルディングを作成し、ビルディング A をコントローラ 1 のプライマリ管理場所かつコントローラ 2 のセカンダリ管理場所に設定し、ビルディング B をコントローラ 2 のプライマリ管理場所としてのみ設定できます。

  詳細については、ネットワーク階層のサイトの作成（166 ページ）および建物の追加（167 ページ）を参照してください。

- 設計フェーズ中にカバレッジヒートマップが可視化されるようにするには、フロアマップに AP を追加して配置します。

  詳細については、「フロアマップでの AP の操作 （178 ページ）」を参照してください。

- 2つの SSID を作成し、バックホール SSID として関連付けます。

  詳細については、エンタープライズ ワイヤレス ネットワーク用 SSID の作成 （248 ページ）およびゲスト ワイヤレス ネットワークの SSID の作成 （256 ページ）を参照してください。

Cisco DNA Center からの N+1 高可用性の設定

この手順では、シスコ ワイヤレス コントローラおよび Cisco Catalyst 9800 シリーズ ワイヤレス コントローラで N+1 高可用性（HA）を設定する方法を示します。

ステップ 1 メニューアイコン（☰）をクリックして、**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。

[Inventory] ウィンドウが表示され、検出されたデバイスが一覧表示されます。

ステップ 2 プライマリコントローラとしてプロビジョニングするには、目的のコントローラの隣にあるチェックボックスをオンにします。

ステップ 3 [Actions] ドロップダウンリストから、**[Provision]** > **[Provision]** の順に選択します。

[Assign Site] ウィンドウが表示されます。

ステップ 4 プライマリコントローラのプライマリ管理 AP 場所を割り当てるには、[Choose a site] をクリックします。

ステップ 5 [Choose a site] ウィンドウで、サイトを選択して [Save] をクリックします。

ステップ 6 [Next] をクリックします。

[Configuration] ウィンドウが表示され、プライマリデバイスのプライマリ管理対象 AP の場所が表示されます。

ステップ 7 [Select Primary Managed AP Locations] をクリックして、プライマリコントローラの管理対象 AP のロケーションを追加または更新できます。

ステップ 8 [Managed AP Location] ウィンドウで、サイト名の隣にあるチェックボックスをオンにして、[Save] をクリックします。

親サイトまたは個々のサイトのいずれかを選択できます。

ステップ 9 インターフェイスと VLAN の詳細を設定します。

ステップ 10 [Configure Interface and VLAN] 領域で、IP アドレスとサブネットマスクの詳細を設定し、[Next] をクリックします。

ステップ 11 [Advanced Configuration] ウィンドウで、事前定義されたテンプレート変数の値を設定し、[Next] をクリックします。

ステップ 12 [Summary] ウィンドウでプライマリコントローラの管理対象 AP の場所およびその他の設定の詳細を確認し、[Deploy] をクリックします。

- デバイスをすぐに展開するには、[Now] オプションボタンをクリックし、[Apply] をクリックします。
- 将来の日付と時刻でデバイスの展開をスケジュールするには、[Later] オプションボタンをクリックし、展開する日時を定義します。

ステップ 13 次に、セカンダリコントローラをプロビジョニングします。

ステップ 14 [Inventory] ウィンドウで目的のコントローラの隣にあるチェックボックスをオンにし、セカンダリコントローラとしてプロビジョニングします。

ステップ 15 [Actions] ドロップダウンリストから、**[Provision]** > **[Provision]** の順に選択します。

[Assign Site] ウィンドウが表示されます。

ステップ 16 セカンダリコントローラの管理対象 AP の場所を割り当てるには、[Choose a site] をクリックします。

セカンダリコントローラの管理対象 AP の場所は、プライマリコントローラの管理対象 AP の場所と同じにする必要があります。

ステップ 17 [Choose a site] ウィンドウで、セカンダリコントローラを関連付けるサイト名の隣にあるチェックボックスをオンにして、[Save] をクリックします。

ステップ 18 **[Next]** をクリックします。

[Configuration] ウィンドウが表示され、セカンダリデバイスのプライマリ管理対象 AP の場所とセカンダリ管理対象 AP の場所が表示されます。

ステップ 19 [Select Secondary Managed AP Locations] をクリックして、セカンダリコントローラの管理対象 AP の場所を追加または更新できます。

ステップ 20 [Managed AP Location] ウィンドウで、サイト名の隣にあるチェックボックスをオンにして、[Save] をクリックします。

親サイトまたは個々のサイトのいずれかを選択できます。

ステップ 21 セカンダリコントローラのインターフェイスと VLAN の詳細を設定します。

ステップ 22 [Configure Interface and VLAN] 領域で、セカンダリコントローラの IP アドレスとサブネットマスクの詳細を設定し、[Next] をクリックします。

ステップ 23 [Advanced Configuration] ウィンドウで、事前定義されたテンプレート変数の値を設定し、[Next] をクリックします。

ステップ 24 [Summary] ウィンドウで、セカンダリコントローラの管理対象 AP の場所やその他の設定の詳細を確認し、[Deploy] をクリックします。

- デバイスをすぐに展開するには、[Now] オプションボタンをクリックし、[Apply] をクリックします。

- 将来の日付と時刻でデバイスの展開をスケジュールするには、[Later] オプションボタンをクリックし、展開する日時を定義します。

ステップ 25 プライマリコントローラおよびセカンダリコントローラの管理対象場所を確認するには、**[Provision]** > **[Network Devices]** > **[Inventory]** ウィンドウでプロビジョニングしたコントローラのデバイス名をクリックします。

ステップ 26 [Device details] ウィンドウで、[Managed ap locations] タブをクリックして、プライマリおよびセカンダリの管理対象場所の詳細を表示します。

ステップ 27 プライマリコントローラの AP をプロビジョニングします。

ステップ 28 **[Network Devices]** > **[Inventory]** ウィンドウで、プロビジョニングする AP の横にあるチェックボックスをオンにします。

ステップ 29 [Action] ドロップダウンリストから、**[Provision]** > **[Provision]** の順に選択します。

ステップ 30 [Assign Site] ウィンドウで、[Choose a Floor] をクリックして、プライマリの管理対象場所からフロアを選択します。

ステップ 31 **[次へ (Next)]** をクリックします。

[設定（Configuration） **]** ウィンドウが表示されます。

ステップ 32 デフォルトでは、**[Design]** > **[Network Settings]** > **[Wireless]** > **[Wireless Radio Frequency Profile]** でデフォルトとマークしたカスタム RF プロファイルが、[RF Profile] ドロップダウンリストで選択されています。

[RF Profile] ドロップダウンリストから値を選択して、AP のデフォルト RF プロファイル値を変更できます。

ステップ 33 **[Next]** をクリックします。

ステップ 34 [Summary] ウィンドウで、詳細を確認します。

ステップ 35 [Deploy] をクリックして、プライマリ AP をプロビジョニングします。

ステップ 36 AP グループの作成または変更が進行中であることを示すメッセージが表示されます。

「プロビジョニング後にAPがリブートします。続行しますか?（After provisioning AP(s) will reboot. Do you want to continue?）」というメッセージが表示されます。

ステップ 37 [OK] をクリックします。

展開が成功すると、[Device Inventory] ウィンドウの [Last Sync Status] 列に、[SUCCESS] と表示されます。

モビリティ設定の概要

Cisco DNA Center のモビリティ設定では、一連の シスコ ワイヤレス コントローラ をモビリティグループにグループ化して、ワイヤレスクライアントのシームレスなローミング体験を実現できます。

モビリティグループを作成すると、ネットワーク内で複数のワイヤレスコントローラを有効にして、コントローラ間またはサブネット間のローミングが発生した際に、動的に情報を共有し

てデータトラフィックを転送できます。異なるモビリティグループ名を同じ無線ネットワーク内の異なるワイヤレスコントローラに割り当てると、モビリティグループによって、1つの企業内の異なるフロア、ビルディング、キャンパス間でのローミングを制限できます。

Cisco DNA Center では、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ および Cisco AireOS コントローラなどのさまざまなプラットフォーム間でモビリティグループを作成できます。

モビリティ設定には、次の注意事項および制限事項があります。

- [Provision] ページでは、モビリティを設定するために複数のコントローラを選択することはできません。
- グループ名をデフォルトにしてモビリティグループを作成することはできません。これにより、モビリティおよび RF グループ名がデフォルトとしてリセットされ、すべてのピアが削除されます。
- アンカーコントローラでモビリティグループ名を設定することはできません。
- Cisco AireOS コントローラでモビリティグループを設定しているときに仮想 IP アドレスが変更された場合は、ワイヤレスコントローラ を手動で再起動する必要があります。
- 同じモビリティグループ名を持つワイヤレスコントローラは、自動的に1つのモビリティグループにグループ化され、互いにピアとして追加されます。
- Cisco AireOS コントローラでモビリティグループを設定するときに、ワイヤレスコントローラ に IP アドレス 192.0.2.1 がない場合、Cisco DNA Center は仮想 IP アドレス 192.0.2.1 をすべての ワイヤレスコントローラ にプッシュします。
- ゲストアンカーコントローラをモビリティグループに明示的に追加しないでください。プロビジョニングされたゲストアンカーコントローラは、[Mobility Configuration] ページでピアを追加している間、ドロップダウンリストに表示されません。
- ワイヤレスコントローラをゲストアンカーとしてプロビジョニングする場合は、それがモビリティグループに追加されていないことを確認します。

モビリティ設定ワークフロー

次に、シスコ ワイヤレス コントローラ でモビリティを設定するために使用できるワークフローを示します。

- モビリティを設定するには、モビリティグループ名、RF グループ名、およびモビリティピアを使用して ワイヤレスコントローラ をプロビジョニングする必要があります。
- ワイヤレスコントローラのプロビジョニング中に適用される設定は、そのグループに設定されているすべてのモビリティピアに自動的に複製されます。
- ワイヤレスコントローラ を再同期して、最新のトンネルステータスを取得します。

モビリティ設定の使用例

次の使用例では、コントローラ間のモビリティの設定手順について説明します。

使用例 1

シスコ ワイヤレス コントローラ 1、ワイヤレスコントローラ 2、およびワイヤレスコントローラ 3 は、モビリティグループ名（デフォルト）を使用して Cisco DNA Center に新たに追加されていて、まだプロビジョニングされていません。

1. モビリティグループ名、RF グループ名を設定し、ワイヤレスコントローラ 2 および ワイヤレスコントローラ 3 をピアとして追加することによって、ワイヤレスコントローラ 1 をプロビジョニングします。
2. ワイヤレスコントローラ 2 をプロビジョニングします。

   [Provision] ウィンドウでは、ワイヤレスコントローラ 2 のモビリティ設定がグループ名とピアとともに自動的に入力されます。
3. ワイヤレスコントローラ 3 をプロビジョニングします。
4. すべての ワイヤレスコントローラ をプロビジョニング後、ワイヤレスコントローラ を再同期して、最新のトンネルステータスを受信します。

使用例 2

異なるモビリティグループ名を持つシスコ ワイヤレス コントローラ 1、ワイヤレスコントローラ 2、および ワイヤレスコントローラ 3はすでに Cisco DNA Center に追加され、プロビジョニングされています。

1. モビリティグループ名、RF グループ名を設定してワイヤレスコントローラ 1 をプロビジョニングし、ピアとしてワイヤレスコントローラ 2 およびワイヤレスコントローラ 3 を追加します。
2. モビリティ設定は、 ワイヤレスコントローラ 2、 ワイヤレスコントローラ 3 などの他のピア間で自動的に複製されます。
   - ワイヤレスコントローラ 1 のプロビジョニングが成功すると、 ワイヤレスコントローラ 2 と ワイヤレスコントローラ 3 がピアとして ワイヤレスコントローラ 1 に追加されます。
   - ワイヤレスコントローラ 1 と ワイヤレスコントローラ 3 は、ワイヤレスコントローラ 2 のピアとして追加されます。
   - ワイヤレスコントローラ 1 と ワイヤレスコントローラ 2 は、ワイヤレスコントローラ 3 のピアとして追加されます。

モビリティグループの設定

ステップ 1 メニューアイコン（☰）をクリックして、**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。

[Inventory] ウィンドウが表示され、検出されたすべてのデバイスが一覧表示されます。

ステップ 2 **[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。

ステップ 3 モビリティを設定する Catalyst 9800 シリーズ ワイヤレス コントローラ の名前の横にあるチェックボックスをオンにします。

ステップ 4 [Actions] ドロップダウンリストから、**[Provision]** > **[Provision WLC Mobility]** の順に選択します。

[Configure Mobility Group] サイドパネルが表示されます。

詳細については、「モビリティ設定の概要 （453 ページ）」を参照してください。

ステップ 5 [Mobility Group Name] ドロップダウンリストで、[+] をクリックして新しいモビリティグループを追加するか、既存のモビリティグループの中から選択できます。

既存のモビリティピア情報は、 Cisco DNA Center で使用可能なインテントからロードされます。

ステップ 6 [RF Group Name] テキストボックスに RF グループの名前を入力します。

ステップ 7 モビリティの暗号化設定を有効または無効にするには、[DTLS High Cipher Only] ボタンをクリックします。

暗号方式の設定は、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ リリース 17.5 以降に適用されます。変更を有効にするには、デバイスを手動で再起動する必要があります。

ステップ 8 DTLS（Data Datagram Transport Layer Security）暗号方式の設定を変更した後にデバイスを手動で再起動して、プロビジョニング後に変更を有効にするには、[Restart for DTLS Ciphers to take effect] ボタンをクリックします。

ステップ 9 DTLS データ暗号化を有効にするには、[Data Link Encryption] ボタンをクリックします。

ステップ 10 [Mobility Peers] で [Add] をクリックして、モビリティピアを設定します。

ステップ 11 [Device Name] ドロップダウンリストからコントローラを選択します。

デバイスがプロビジョニングされると、 Cisco DNA Center はデバイスにモビリティグループを作成し、RF グループを割り当て、ピアのすべての終端を設定します。モビリティグループの設定は、選択したすべてのピアデバイスに自動的に展開されます。

ステップ 12 **[Save]** をクリックします。

ステップ 13 モビリティグループ名と RF グループ名をリセットするには、次のいずれかの方法を実行します。

- [Configure Mobility Group] サイドパネルで、[Mobility Group Name] ドロップダウンリストから [default] を選択します。
- **[Provision]** > **[Configuration]** ページの [Mobility Group] で、[Reset] をクリックします。

これにより、[RF Group Name] が自動的に [default] に設定され、すべてのピアが削除されます。プロビジョニングが完了すると、デバイスのモビリティが設定され、そのデバイスは他のすべてのピアから削除されます。

DTLS 暗号スイートについて

暗号スイートは、無線 LAN 上の無線通信を保護するように設計された暗号と完全性アルゴリズムのセットです。

リリース 17.5 以降を実行している Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ、Catalyst 9000 シリーズスイッチ用 Cisco Catalyst 9800 組み込みワイヤレスコントローラ、およびCatalyst アクセスポイント上のシスコ組み込みワイヤレスコントローラ プラットフォームでは複数の DTLS（Data Datagram Transport Layer Security）暗号スイートを設定できます。

複数の DTLS 暗号スイートの設定

DTLS 暗号スイートは、グローバルレベルまたはサイトレベルで設定できます。

始める前に

- **[System]** > **[Settings]** > **[Device Settings]** > **[Device Controllability]** ページでデバイス可制御性機能が有効になっていることを確認します。
- 検出されたデバイスが [Inventory] ウィンドウに一覧表示されるように、[Discovery] 機能を使用してネットワーク内の Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ を検出します。

ステップ 1 メニューアイコン（☰）をクリックして、**[Design]** > **[Network Settings]** > **[Wireless]** の順に選択します。

ステップ 2 同じ DTLS 暗号スイート設定ですべてのサイトを設定するには、左側のツリーメニューで [Global] を選択します。

DTLS暗号スイートをサイトレベルで設定するには、左側のツリーメニューでサイトを選択します。DTLS暗号スイートの設定は、その特定のサイトで使用可能なコントローラにプッシュされます。

ステップ 3 暗号スイートをデバイスの可制御性の一部として設定するには、[Skip DTLS Ciphersuite Config] チェックボックスをオフにします。

ステップ 4 デフォルト暗号スイートまたはカスタム暗号スイートを設定します。

デフォルトでは、**デフォルト**暗号スイートが選択されています。

[Default Ciphersuite] ボックスにはデフォルト暗号スイートのリストが示され、これらの暗号スイートが、デバイスでデフォルトとして設定されています。これらのデフォルト暗号スイートの優先順位は変更できません。

ステップ 5 カスタム暗号スイートを設定するには、[Custom] ボタンをクリックします。

カスタム暗号スイートは、優先順位に従ってデフォルト暗号スイートを上書きします。

ステップ 6 [Version] ドロップダウンリストから、DTLS のバージョンを選択します。

Cisco DNA Center は、DTLS のバージョンに基づいて、使用可能な暗号スイートを表示します。

ステップ 7 暗号スイートを適用しない場合は、その暗号スイートの横にある青色のボタンをクリックします。

ステップ 8 暗号スイートの優先順位を変更するには、各暗号スイートをクリックしたままドラッグします。

ステップ 9 [**保存（Save）**] をクリックします。

「DTLS Ciphersuite Config Saved successfully」というメッセージが表示されます。

ステップ 10 暗号スイートの設定を適用するには、デバイスをプロビジョニングする必要があります。

詳細については、Cisco Catalyst 9800 シリーズ ワイヤレスコントローラのプロビジョニング （462 ページ）を参照してください。

N+1 ローリング AP アップグレードについて

ローリング AP アップグレード機能は、N+1 ハイアベイラビリティ設定の Cisco Catalyst 9800 シリーズ ワイヤレス コントローラでのみサポートされます。この機能は、ワイヤレス LAN ネットワーク内の Cisco Catalyst 9800 シリーズ ワイヤレス コントローラに関連付けられている AP のソフトウェアイメージをアップグレードするのに便利です。ゼロダウンタイムを実現するために、N+1 ローリング AP アップグレード機能を使用して、段階的に AP をアップグレードすることができます。

プライマリコントローラは、無線リソース管理ネイバー AP マップを使用して、候補の AP を識別します。アップグレードプロセスは、イメージが候補の AP に事前ダウンロードされている間に、ソフトウェアイメージをプライマリコントローラにダウンロードすることから始まります。候補の AP がアップグレードされて再起動されると、これらの AP は、セカンダリコントローラに段階的に参加します。すべての AP がセカンダリコントローラに参加した後、プライマリコントローラは再起動します。これらの AP は、再起動された後、段階的にプライマリコントローラに再度参加します。

次に、ローリング AP アップグレードを設定するための前提条件を示します。

- 2 つの ワイヤレスコントローラ（1 つはプライマリコントローラ、もう 1 つはセカンダリとして）の N+1 ハイアベイラビリティ設定。
- プライマリコントローラと N+1 コントローラの設定は同じで、ネットワーク内の同じ場所を管理します。
- N+1 コントローラではすでにゴールデンイメージが実行されているため、ローリング AP アップグレードはダウンタイムなしで動作します。

  ゴールデンイメージは、ネットワークデバイスの標準化されたイメージであり、Cisco DNA Center は Cisco.com からイメージを自動的にダウンロードします。イメージの標準化は、デバイスのセキュリティと、デバイスのパフォーマンスの最適化に役立ちます。

- N+1 コントローラはに到達可能であり、Cisco DNA Center で [Managed] 状態になっています。
- 両方のコントローラが同じモビリティグループの一部であり、プライマリコントローラと N+1 コントローラの間にモビリティトンネルが確立されます。プライマリコントローラと N+1 コントローラ間のアップグレード情報は、モビリティトンネルを介して交換されます。

（注） ワイヤレスコントローラ 1 が ワイヤレスコントローラ 2 に対して N+1、ワイヤレスコントローラ 2 がワイヤレスコントローラ 1 に対して N+1 となっている循環型 N+1 展開がある場合、両方のデバイスでローリング AP アップグレードを実行することはできません。その代わりに、1 つのコントローラで通常のアップグレードを行う必要があります。最初のコントローラがローリング AP アップグレードなしでアップグレードされると、もう一方のコントローラでローリング AP アップグレードを実行できます。

ローリング AP アップグレードを設定するワークフロー

この手順では、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラでローリング AP アップグレードを設定する方法を示します。

（注） N+1 ローリング AP アップグレードは、ファブリックおよび非ファブリックの展開でサポートされています。

ステップ 1 Cisco DNA Center をインストールします。

詳細については、Cisco Digital Network Architecture Center 設置ガイド [英語] を参照してください。

ステップ 2 Cisco DNA Center GUI にログインし、必要なアプリケーションが**実行**状態であることを確認します。

メニューアイコン（☰）をクリックして、**[System]** > **[Software Updates]** > **[Installed Apps]** の順に選択します。

ステップ 3 ディスカバリ機能を使用して ワイヤレスコントローラを検出します。

Catalyst 9800 シリーズ ワイヤレス コントローラを検出するには、NETCONF を有効にしてポートを 830 に設定する必要があります。NETCONF は、ネットワークデバイスの設定をインストール、操作、削除するためのメカニズムです。

詳細については、CDP を使用したネットワークの検出 （51 ページ）またはIP アドレス範囲を使用したネットワークの検出 （59 ページ）を参照してください。

ステップ 4 検出されたデバイスが [Device Inventory] ウィンドウに [Managed] 状態で表示されていることを確認します。

詳細については、インベントリについて （84 ページ）およびインベントリに関する情報の表示 （85 ページ）を参照してください。

デバイスが [Managed] になるまで待機する必要があります。

ステップ 5 サイト、ビルディング、フロアを追加してネットワーク階層を設計すると、後で設計の設定や構成を適用する場所を簡単に特定できるようになります。

新しいネットワーク階層を作成します。または Cisco Prime Infrastructure に既存のネットワーク階層がある場合は、それを Cisco DNA Center にインポートできます。

既存のネットワーク階層をインポートしてアップロードするには、Cisco DNA Center へのサイト階層のインポート （159 ページ）を参照してください。

新しいネットワーク階層を作成するには、ネットワーク階層のサイトの作成 （166 ページ）および建物の追加 （167 ページ）を参照してください。

ステップ 6 AP の位置情報を追加し、フロアマップに配置して、ヒートマップカバレッジを可視化します。

詳細については、「フロアマップでの AP の操作 （178 ページ）」を参照してください。

ステップ 7 プライマリ管理対象 AP の場所、およびローリング AP アップグレード有効、ピアとしてのセカンダリコントローラとのモビリティグループを設定の状態で、プライマリコントローラをプロビジョニングします。

これを行うには、**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択し、プライマリコントローラ名の横にあるチェックボックスをオンにします。

ステップ 8 モビリティグループ設定で、モビリティピアとして N+1 コントローラを設定します。

詳細については、「モビリティ設定の概要 （453 ページ）」を参照してください。

ステップ 9 プライマリコントローラのプライマリ管理対象 AP の場所を N+1 コントローラのセカンダリ管理対象 AP の場所として設定することによって、N+1 HA コントローラをプロビジョニングします。これにより、セカンダリコントローラが N+1 コントローラとして設定されます。

詳細については、「Cisco Catalyst 9800 シリーズ ワイヤレスコントローラのプロビジョニング （462 ページ）」を参照してください。

ステップ 10 プライマリコントローラに関連付けられている AP をプロビジョニングします。

ステップ 11 ソフトウェアイメージをリポジトリにインポートします。

詳細については、「ソフトウェア イメージのインポート （360 ページ）」を参照してください。

ステップ 12 ソフトウェアイメージをデバイスファミリに割り当てます。

詳細については、「デバイスファミリへのソフトウェアイメージの割り当て （361 ページ）」を参照してください。

ステップ 13 デバイスファミリまたはデバイスロールの星印をクリックして、ソフトウェアイメージをゴールデンとしてマークします。

詳細については、ゴールデン ソフトウェア イメージの指定 （363 ページ）を参照してください。

ステップ 14 イメージをアップグレードする前に、両方のデバイスでイメージの準備状況チェックが成功していることを確認してください。

また、[N+1 Device Check] と [Mobility Tunnel Check] のステータスに緑色のチェックマークが付いていることも確認してください。

- イメージ更新の準備状況チェックを実行するには、**[Provision]** > **[Network Devices]** > **[Software Images]** の順に選択します。
- [Focus] ドロップダウンリストから [Software Images] を選択します。イメージをアップグレードするデバイスを選択します。
- デバイスの事前チェックが成功すると、[Image Precheck Status] 列の [Status] リンクに緑色のチェックマークが付きます。デバイスのアップグレード準備状況の事前チェックのいずれかが失敗した場合、[Image Precheck Status] リンクのマークが赤色に変わり、そのデバイスの OS イメージは更新できません。先に進む前に [Status] リンクをクリックし、エラーを修正します。

ステップ 15 プライマリコントローラでアップグレードを開始します。

ステップ 16 [Software Images] ウィンドウで、プライマリコントローラの横にあるチェックボックスをオンにします。

ステップ 17 [Actions] ドロップダウンリストから、**[Software Image]** > **[Update Image]** の順に選択します。

詳細については、ソフトウェア イメージのプロビジョニング （366 ページ）を参照してください。

ステップ 18 イメージのアップグレードの進行状況をモニターするには、[Software Image] 列で [In Progress] をクリックします。

[Device Status] ウィンドウに、次の情報が表示されます。

- [Distribution Operation]：イメージ配信プロセスに関する情報が表示されます。イメージは Cisco DNA Center からプライマリデバイスにコピーされます。配信プロセスが完了すると、アクティブ化操作が開始されます。
- [Activate Operation]：アクティブ化操作の詳細が表示されます。このプロセス中に、ローリング AP アップグレードが開始されます。
- [Rolling AP Upgrade Operation]：ローリング AP アップグレードタスクが完了したかどうか、保留中の AP の数、再起動中の AP の数、N+1 コントローラに参加している AP の数など、ローリング AP アップグレードの概要が表示されます。

  [View AP Status] をクリックすると、プライマリコントローラ、N+1 コントローラ、デバイス名、現在のステータス、および反復に関する詳細が表示されます。

Cisco Catalyst 9800 シリーズ ワイヤレスコントローラのプロビジョニング

始める前に

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のプロビジョニングを行う前に、Cisco DNA Center で Cisco Catalyst 9800 ワイヤレスコントローラを設定するためのワークフロー（440 ページ） の手順を完了したことを確認します。

ステップ 1 メニューアイコン（☰）をクリックして、**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。

[Inventory] ウィンドウが表示され、検出されたすべてのデバイスが一覧表示されます。

ステップ 2 プロビジョニングする Catalyst 9800 シリーズ ワイヤレス コントローラ 名の横にあるチェックボックスをオンにします。

ステップ 3 [Actions] ドロップダウンリストから、**[Provision]** > **[Provision Device]** を選択します。

ステップ 4 [Assign Site] ウィンドウで、[Choose a Site] をクリックしてサイトと関連付けます。

ステップ 5 [Choose a Sites] スライドインウィンドウで、Catalyst 9800 シリーズ ワイヤレス コントローラを関連付けるサイト名の横にあるチェックボックスをオンにして、[Save] をクリックします。

親サイトまたは個々のサイトのいずれかを選択できます。親サイトを選択すると、その下にあるすべての子も選択されます。このチェックボックスをオフにすると、個々のサイトの選択を解除できます。

ステップ 6 **[次へ (Next)]** をクリックします。

[設定（Configuration）] ウィンドウが表示されます。

ステップ 7 Cisco Catalyst 9800 シリーズ ワイヤレスコントローラのロールとして [Active Main WLC] または [Anchor] を選択します。

ステップ 8 プライマリコントローラの管理対象 AP の場所を選択するには、[Select Primary Managed AP Locations] をクリックします。

ステップ 9 セカンダリコントローラの管理対象 AP の場所を選択するには、[Select Secondary Managed AP Locations] をクリックします。

ステップ 10 親サイトまたは個々のサイトのいずれかを選択できます。[Save] をクリックします。

親サイトを選択すると、その下にあるすべての子も選択されます。チェックボックスをオフにして、特定のサイトの選択を解除することができます。

（注） 管理対象 AP の場所を継承することで、サイトおよび特定のサイトのビルディングとフロアを自動的に選択できます。1 つのサイトは、1 つのワイヤレスコントローラのみによって管理されます。

ステップ 11 アクティブなメインのワイヤレスコントローラでは、インターフェイスと VLAN の詳細を設定する必要があります。

ステップ 12 [Assign Interface] エリアで、次の操作を実行します。

- [VLAN ID]：VLAN ID の値を入力します。
- [Interface IP Address]：インターフェイスの IP アドレスの値を入力します。
- [Gateway IP Address]：ゲートウェイ IP アドレスを入力します。
- [Subnet Mask (in bits)]：インターフェイスのサブネットマスクの詳細を入力します。

（注） Cisco Catalyst 9800 シリーズ ワイヤレスコントローラでは、IP アドレス、ゲートウェイ IP アドレス、およびサブネットマスクを割り当てる必要はありません。

ステップ 13 [Skip AP Provision] チェックボックスをオンにして、Cisco Catalyst 9800 シリーズ ワイヤレスコントローラのプロビジョニング中に AP 関連のコマンドの設定をスキップします。

ステップ 14 [Next] をクリックします。

[Model Configuration] ウィンドウが表示されます。

ステップ 15 [Devices] ペインで、[Find] フィールドにモデル設定設計の名前を入力して検索するか、デバイスを展開してモデル設定設計を選択します。

選択したモデル設定設計が右側のペインに表示されます。

ステップ 16 プロビジョニングするモデル設定設計の [Design Name] の横にあるチェックボックスをオンにし、[Configure] をクリックして編集します。この手順では、すべての設定を編集することはできません。

ステップ 17 必要な変更を加えて、[Apply] をクリックします。

ステップ 18 [Next] をクリックします。

[Advanced Configuration] ウィンドウが表示されます。ここでは、事前定義されたテンプレート変数の値を入力できます。

ステップ 19 [Devices] パネルでデバイスまたはテンプレートを検索します。

ステップ 20 [wlanid] フィールドに、事前定義されたテンプレート変数の値を入力し、[Next] をクリックします。

ステップ 21 [Summary] ウィンドウで、次の設定を確認します。

- デバイスの詳細
- ネットワークの設定
- SSID
- 管理サイト
- ローリング AP アップグレード
- モデル設定
- インターフェイス
- 詳細設定

ステップ 22 [Deploy] をクリックして、Cisco Catalyst 9800 シリーズ ワイヤレスコントローラをプロビジョニングします。

- デバイスをすぐに展開するには、[Now] オプションボタンをクリックし、[Apply] をクリックします。
- 将来の日付と時刻でデバイスの展開をスケジュールするには、[Later] オプションボタンをクリックし、展開する日時を定義します。

ステップ 23 Cisco DNA Center からデバイスにプッシュされた設定を確認するには、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ デバイスで次のコマンドを使用します。

- #show wlan summary
- #show run | sec line
- #show running-configuration

ステップ 24 デバイスが正常に展開されると、[Provision Status] が [Configuring] から [Success] に変わります。

ステップ 25 [Inventory] ウィンドウで、デバイスの [Provision Status] カラムの [See Details] をクリックし、ネットワークインテントの詳細情報を取得するか、アクションのリストを表示します。

ステップ 26 [Device Provisioning] の下の [See Details] をクリックします。

ステップ 27 [Deployment of network intent] の下の [View Details] をクリックし、デバイス名をクリックします。

ステップ 28 デバイス名をクリックして展開します。

ステップ 29 [Configuration Summary] エリアを展開して、操作の詳細、機能名、および管理機能を表示します。また、[Configuration Summary] には、デバイスのプロビジョニング中に発生したエラーも理由とともに表示されます。

ステップ 30 デバイスに送信される正確な設定の詳細を表示するには、[Provision Summary] エリアを展開します。

ステップ 31 AP をプロビジョニングします。

既存のインフラストラクチャでのシスコ ワイヤレス コントローラの設定

Cisco DNA Center を使用すると、既存の展開にシスコ ワイヤレス コントローラや Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ などのデバイスを追加してプロビジョニングできます。

始める前に

- 初めに、デバイスについてディスカバリを実行します。すべてのデバイスが [インベントリ（Inventory）] ウィンドウに表示されます。詳細については、ネットワークの検出 （45 ページ）およびインベントリについて （84 ページ）を参照してください。
- ワイヤレスコントローラ は到達可能で、 [インベントリ（Inventory）] ウィンドウで管理状態でなければなりません。詳細については、インベントリについて （84 ページ）を参照してください。

- Cisco Catalyst 9800 シリーズ ワイヤレス コントローラを検出するには、NETCONF を有効にしてポートを 830 に設定する必要があります。詳細については、検出の概要 （45 ページ）を参照してください。
- サイト、ビルディング、フロアを追加してネットワーク階層を設計すると、後で設計の設定や構成を適用する場所を簡単に特定できるようになります。新しいネットワーク階層を作成できるほか、Cisco Prime Infrastructure に既存のネットワーク階層がある場合はその階層を Cisco DNA Center にインポートすることもできます。

  既存のネットワーク階層のインポートとアップロードの詳細については、Cisco DNA Center へのサイト階層のインポート （159 ページ）を参照してください。

  新しいネットワーク階層の作成については、ネットワーク階層のサイトの作成 （166 ページ）および建物の追加 （167 ページ）を参照してください。

ステップ 1 メニューアイコン（☰）をクリックして、**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。

[Inventory] ウィンドウが表示され、検出されたデバイスが一覧表示されます。

ステップ 2 [フィルタ（Filter）] をクリックして、選択したフィルタ フィールドに適切な値を入力します。たとえば、[デバイス名（Device Name）] フィルタの場合、デバイスの名前を入力します。

[デバイス（Devices）]テーブルに表示されるデータは、選択したフィルタに従って自動で更新されます。

ステップ 3 プロビジョニングする ワイヤレスコントローラ デバイス名の横にあるチェックボックスをオンにします。

ステップ 4 [Actions] ドロップダウンリストから、**[Provision]** > **[Learn Device Config]** の順に選択します。

ステップ 5 [Learn Device Configuration] ワークフローの [Site Assignment] ウィンドウが開きます。

デバイスと既存のインフラストラクチャからデバイス構成を学習する （800 ページ）の手順 3 から手順 13 に従います。

ステップ 6 メニューアイコン（☰）をクリックして、**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。

ステップ 7 [Filter] をクリックして、プロビジョニングするデバイスを見つけます。

[デバイス（Devices）]テーブルに表示されるデータは、選択したフィルタに従って自動で更新されます。

ステップ 8 プロビジョニングするワイヤレスコントローラの横にあるチェックボックスをオンにします。

ステップ 9 [Actions] ドロップダウンリストから、**[Provision]** > **[Provision Device]** の順に選択します。

ステップ 10 [Assign Site] ステップで詳細を確認して、[Next] をクリックします。

ステップ 11 [Configuration] ステップで、次の項目を設定します。

a) [インターフェイスと VLAN の設定（Interface and VLAN Configuration）] で、[+ 追加（+ Add）] をクリックしてインターフェイスと VLAN の詳細を設定します。

b) [インターフェイスと VLAN の設定（Configure Interface and VLAN）] ウィンドウで必要なフィールドを設定して、[OK] をクリックします。

c) [Next] をクリックします。

ステップ 12 [Model Configuration] の手順で、以下を構成します。

- [Devices] ペインで、[Find] フィールドにモデル設定設計の名前を入力して検索するか、デバイスを展開してモデル設定設計を選択します。選択したモデル設定設計が右側のペインに表示されます。
- プロビジョニングするモデル設定設計の [Design Name] の横にあるチェックボックスをオンにし、[Configure] をクリックして編集します。この手順では、すべての設定を編集することはできません。
- 必要な変更を加えて、[Apply] をクリックします。
- [Next] をクリックします。

ステップ 13 [Advanced Configuration] ウィンドウで、事前定義されたテンプレート変数の値を入力できます。

- [Devices] パネルでデバイスまたはテンプレートを検索します。
- [wlanid] フィールドに、事前定義されたテンプレート変数の値を入力し、[Next] をクリックします。

ステップ 14 [Summary] ウィンドウで、次の設定を確認します。

- **Device Details**
- **ネットワークの設定**
- **SSID**
- **Managed Sites**
- **ローリング AP アップグレード**
- **Interfaces**
- **Advanced Configuration**

ステップ 15 [展開（Deploy）] をクリックして、デバイスをプロビジョニングします。

a) デバイスを今すぐ展開するか、または展開を後の時間でスケジュールするかどうかを求められます。

デバイスを今すぐ展開するには、[Now] オプションボタンをクリックし、[Apply] をクリックします。

将来の日付と時刻でデバイスの展開をスケジュールするには、[Later] オプションボタンをクリックし、展開する日時を定義します。

ステップ 16 AP をプロビジョニングします。

詳細については、シスコ製 AP のプロビジョニング：Day 1 AP プロビジョニング（430 ページ）を参照してください。

Cisco Embedded Wireless Controller on Catalyst Access Points 対応 Day 0 ワークフロー

Catalyst アクセスポイント上のシスコ組み込みワイヤレスコントローラ（EWC-AP）は、次世代の Wi-Fi ソリューションであり、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ に Cisco Catalyst 9100 シリーズ アクセスポイントを統合し、進化および成長し続ける組織にそのクラスで最高のワイヤレスエクスペリエンスをもたらします。

始める前に

- サイト、ビルディング、フロアなどのネットワーク階層を設計します。

  詳細については、ネットワーク階層のサイトの作成（166ページ）および建物の追加（167ページ）を参照してください。

- CLI、SNMP、HTTP、HTTPS などのデバイスログイン情報をグローバルレベルで定義します。グローバルレベルで定義されたログイン情報は、サイトによって継承されます。

  詳細については、グローバル CLI クレデンシャルの設定 （230 ページ）、グローバル SNMPv2c クレデンシャルの設定 （231 ページ）、およびグローバル SNMPv3 クレデンシャルの設定 （233 ページ）を参照してください。

- SSID、ワイヤレスインターフェイス、および無線周波数プロファイルを作成します。

  詳細については、エンタープライズ ワイヤレス ネットワーク用 SSID の作成 （248 ページ）、ゲスト ワイヤレス ネットワークの SSID の作成 （256 ページ）、ワイヤレスインターフェイスの作成 （266 ページ）、およびワイヤレス無線周波数プロファイルの作成（268 ページ）を参照してください。

（注） Catalyst アクセスポイント上のシスコ組み込みワイヤレスコントローラ では、Flex ベースの SSID の作成のみがサポートされています。

- Catalyst アクセスポイント上のシスコ組み込みワイヤレスコントローラ が接続されているスイッチでオプション #43 を使用して DHCP サーバーを設定します。これは Cisco DNA Center プラグアンドプレイサーバーの IP アドレスです。この IP アドレスを使用して、AP は PnP サーバーに接続し、設定をダウンロードします。

- インベントリに Catalyst アクセスポイント上のシスコ組み込みワイヤレスコントローラ があることを確認します。ない場合は、[Discovery] 機能を使用して検出します。詳細については、CDP を使用したネットワークの検出 （51 ページ）、IP アドレス範囲を使用したネットワークの検出 （59 ページ）、およびインベントリについて （84 ページ）を参照してください。

- AP は、シスコ ワイヤレス コントローラ 設定なしで初期設定へリセットされた状態である必要があります。

Catalyst アクセスポイント上のシスコ組み込みワイヤレスコントローラ は、次のような複数のフォームファクタで使用できます。

- Catalyst 9115AX アクセスポイント上の Cisco 組み込みワイヤレスコントローラ
- Catalyst 9117AX アクセスポイントの Cisco 組み込みワイヤレスコントローラ
- Catalyst 9120AX アクセスポイントの Cisco 組み込みワイヤレスコントローラ
- Catalyst 9130AX アクセスポイントの Cisco 組み込みワイヤレスコントローラ

ステップ 1 Catalyst アクセスポイント上のシスコ組み込みワイヤレスコントローラ が DHCP サーバーと通信します。

DHCP サーバーからの応答で、IP アドレスとともに、Cisco プラグアンドプレイサーバーの IP アドレスを含むオプション #43 が返されます。

ステップ 2 オプション #43 に基づいて、 Catalyst アクセスポイント上のシスコ組み込みワイヤレスコントローラ はプラグアンドプレイ エージェントをオンにし、Cisco DNA Center プラグアンドプレイサーバーに接続します。

（注） ネットワーク内に Catalyst アクセスポイント上のシスコ組み込みワイヤレスコントローラ のセットがある場合、それらは内部プロトコルを通過します。プロトコルは、PnP サーバーに到達するために シスコ ワイヤレス コントローラ 上でプライマリ AP として設定されている 1 つの Catalyst アクセスポイント上のシスコ組み込みワイヤレスコントローラ を選択します。

ステップ 3 **[Provision]** > **[Network Devices]** > **[Plug and Play]** タブで未要求 Catalyst アクセスポイント上のシスコ組み込みワイヤレスコントローラ を検索します。

テーブルには、すべての未要求デバイスが一覧表示されます。[State] 列が [Unclaimed] として表示されます。[Filter] または [Find option] を使用して、特定のデバイスを検索することができます。

[Onboarding State] 列の下でオンボーディングステータスが [Initialized] になるまで待つ必要があります。

ステップ 4 Catalyst アクセスポイント上のシスコ組み込みワイヤレスコントローラ を要求するには、AP デバイス名の横にあるチェックボックスをオンにします。

ステップ 5 デバイステーブルの上にあるメニューバーで、[Actions] > [Claim] の順に選択します。 >

[Claim Devices] ウィンドウが表示されます。

ステップ 6 [Site Assignement] ウィンドウで、[Site] ドロップダウンリストからサイトを選択します。

選択された AP のこの特定のサイトに対する要求は、関連付けられている構成にも適用されます。

ステップ 7 **[次へ (Next)]** をクリックします。

ステップ 8 デバイスを設定するには、[Configuratio] ウィンドウのデバイス名をクリックします。

ステップ 9 [Configuration for device name] ウィンドウで、デバイスの静的 IP の詳細を割り当てます。

- **[Management IP]**
- **[Subnet Mask]**
- **[Gateway]**

ステップ 10 [Save] をクリックします。

ステップ 11 [Next] をクリックします。

[Summary] ウィンドウが表示されます。

ステップ 12 [Summary] ウィンドウで [Claim] をクリックします。

Catalyst アクセスポイント上のシスコ組み込みワイヤレスコントローラ が要求されると、設定された IP アドレスが Cisco Embedded Wireless Controller に割り当てられます。

要求したデバイス（内部 AP を備えた Cisco 組み込みワイヤレスコントローラ）が **[Provision]** > **[Network Devices]** > **[Inventory]** に表示されることを確認します。

ステップ 13 追加のコントローラをプロビジョニングするには、Cisco AireOS コントローラのプロビジョニング （422 ページ）を参照してください。

ステップ 14 CSV ファイルからデバイスを一括インポートするには、デバイスの一括追加 （404 ページ） を参照してください。

ステップ 15 デバイスを手動で追加するには、「デバイスの追加または編集」を参照してください。

Cisco DNA Center を使用した Cisco Catalyst 9800 シリーズ ワイヤレス コントローラへの Cisco AireOS コントローラの移行

始める前に

- サイト、ビルディング、フロアなどのネットワーク階層を設計します。
- ディスカバリ機能を実行して Cisco Catalyst 9800 シリーズ ワイヤレス コントローラを検出し、インベントリに追加します。デバイスステータスが到達可能で、管理対象状態になっていることを確認します。

  Catalyst 9800 シリーズ ワイヤレス コントローラを検出するには、NETCONF を有効にし、ポートを 830 に設定する必要があります。NETCONF は、ネットワークの設定をインストール、操作、削除するためのメカニズムです。
- Cisco AireOS コントローラを検出して、インベントリに追加します。デバイスステータスが到達可能で、管理対象状態になっていることを確認します。

ステップ 1 メニューアイコン（≡）をクリックして、**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。

[Inventory] ウィンドウが表示され、検出されたデバイスが一覧表示されます。

ステップ 2 Cisco AireOS コントローラの横にあるチェックボックスをオンにします。

ステップ 3 [Actions] ドロップダウンリストから、**[Provision]** > **[Assign Device to Site]** の順に選択します。

ステップ 4 [Assign Device to Site] ウィンドウで、[Choose a Site] をクリックします。

ステップ 5 [Add Sites] ウィンドウで、Cisco AireOS コントローラと関連付けるサイト名の横にあるチェックボックスをオンにします。

ステップ 6 [**保存（Save**）] をクリックします。

ステップ 7 [Action] ドロップダウンリストから、**[Provision]** > **[Learn Device Config]** の順に選択して、Cisco AireOS コントローラデバイスから構成を学習します。

ステップ 8 [Assign Site] ウィンドウで、[Next] をクリックします。

ステップ 9 [Resolve Conflict] ウィンドウに、解決する必要がある Cisco DNA Center の競合する設定が表示されます。[Next]をクリックします。

ステップ 10 [Design Object] ウィンドウで、[Next] をクリックします。

ステップ 11 左側のペインで [Network] をクリックします。

右側のペインに、デバイス構成学習プロセスの一部として学習されたネットワーク構成と、次の情報が表示されます。

- AAA サーバーの詳細。
- システム設定。AAA サーバーの IP アドレスとプロトコルについての詳細情報を含みます。パスワードは暗号化されており、Cisco DNA Center はパスワードを学習できないため、AAA サーバーの共有秘密を入力します。
- HCP サーバー。デバイスで使用可能なすべての DHCP サーバーに関する詳細が表示されます。
- NTP サーバー。デバイスで使用可能なすべての NTP サーバーに関する詳細が表示されます。

ステップ 12 [Next] をクリックします。

ステップ 13 左ペインで [Wireless] をクリックします。

[Wireless] ウィンドウに、デバイスに存在するエンタープライズ SSID、ゲスト SSID、ワイヤレスインターフェイス、および RF プロファイルが一覧表示されます。

ステップ 14 事前共有キー（PSK）を使用する SSID の場合、事前共有キーを入力します。

ステップ 15 左ペインで、[Discarded Config] をクリックします。

Cisco DNA Center の競合する設定と既存の設定が表示されます。破棄される構成エントリは次のカテゴリに分類されます。

- 設計エンティティの重複
- 無線ポリシーの不明なデバイスの設定

ステップ 16 [Next]をクリックします。

ステップ 17 [ネットワーク プロファイル（Network Profile）] ウィンドウに、AP と WLAN の組み合わせに基づいて作成されたネットワーク プロファイルまたはサイト プロファイルが一覧表示されます。

ステップ 18 **[Save]** をクリックします。

成功メッセージが表示されます。

ステップ 19 **[Design]** > **[Network Settings]** > **[Wireless]** の順に選択して、Cisco DNA Center が Cisco AireOS コントローラから学習した SSID とインターフェイス設定を表示します。

ステップ 20 **[Design]** > **[Network Profile]** を選択して、サイトをネットワークプロファイルに割り当てます。

ステップ 21 [ネットワーク プロファイル（Network Profile）] ページで [サイトの割り当て（Assign Site）] をクリックして、選択したプロファイルにサイトを追加します。

ステップ 22 [Add Sites to Profile] ウィンドウでドロップダウンリストからサイトを選択して、[Save] をクリックします。

ステップ 23 [プロビジョニング（Provision）] タブをクリックします。

ステップ 24 プロビジョニングする Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの横にあるチェックボックスをオンにします。

ステップ 25 [アクション（Actions）] ドロップダウン リストから、[プロビジョニング（Provision）]を選択します。

ステップ 26 [Choose a site] をクリックして Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ にサイトを割り当てます。

ステップ 27 [Choose a site] ウィンドウで、サイト名の横にあるチェックボックスをオンにして Catalyst 9800 シリーズ ワイヤレス コントローラを関連付けます。

ステップ 28 **[次へ (Next)]** をクリックします。

[設定（Configuration） **]** ウィンドウが表示されます。

ステップ 29 Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のロールを [Active Main WLC] として選択します。

ステップ 30 プライマリ コントローラの管理 AP の場所を設定するには、[Select Primary Managed AP Locations] をクリックします。

ステップ 31 [Managed AP Location] ウィンドウで、サイト名の横にあるチェックボックスをオンにします。親サイトまたは個々のサイトのいずれかを選択できます。親サイトを選択すると、その親サイトの下にある子は自動的に選択されます。

ステップ 32 [Save] をクリックします。

ステップ 33 [Next] をクリックします。

ステップ 34 [Summary] ウィンドウには、Cisco AireOS コントローラから Cisco Catalyst 9800 シリーズ ワイヤレス コントローラにプッシュされる設定が表示されます。

次の詳細情報を確認します。

- デバイスの詳細
- ネットワークの設定
- SSID
- 管理サイト
- インターフェイス
- 詳細設定

ステップ 35 [Deploy] をクリックして、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラをプロビジョニングします。

- デバイスをすぐに展開するには、[Now] オプションボタンをクリックし、[Apply] をクリックします。
- 将来の日付と時刻でデバイスの展開をスケジュールするには、[Later] オプションボタンをクリックし、展開する日時を定義します。

ステップ 36 デバイスが正常に展開されると、[Provision Status] が [Configuring] から [Success] に変わります。

ステップ 37 [Device Inventory] ウィンドウで、[Provision Status] 列の [See Details] をクリックし、ネットワークインテントの詳細情報を取得するか、実行する必要があるアクションのリストを表示します。

ステップ 38 手動で Cisco Catalyst 9800 シリーズ ワイヤレス コントローラを再同期するには、**[Provision]** > **[Inventory]** ウィンドウで、手動で同期するコントローラを選択します。

ステップ 39 [Actions] ドロップダウンリストから、[Resync] を選択します。

ステップ 40 AP をプロビジョニングします。

Catalyst 9000 シリーズ スイッチ用 Cisco Catalyst 9800 組み込みワイヤレスコントローラの設定とプロビジョニング

サポートされているハードウェア プラットフォーム

デバイスロール	プラットフォーム
組み込みワイヤレスコントローラ	Cisco Catalyst 9300 シリーズ スイッチ Cisco Catalyst 9400 シリーズ スイッチ Cisco Catalyst 9500-H シリーズ スイッチ
ファブリックエッジ	Cisco Catalyst 9300 シリーズ スイッチ Cisco Catalyst 9400 シリーズ スイッチ Cisco Catalyst 9500-H シリーズ スイッチ Cisco Catalyst 3600 シリーズ スイッチ Cisco Catalyst 3850 シリーズ スイッチ
AP	Cisco 802.11ac Wave 2 AP： • Cisco Aironet 1810 シリーズ OfficeExtend アクセス ポイント • Cisco Aironet 1810W シリーズ アクセス ポイント • Cisco Aironet 1815i アクセスポイント • Cisco Aironet 1815w アクセスポイント

デバイスロール	プラットフォーム
	• Cisco Aironet 1815m アクセスポイント • Cisco 1830 Aironet シリーズ アクセスポイント • Cisco Aironet 1850 シリーズ アクセス ポイント • Cisco Aironet 2800 シリーズ アクセス ポイント • Cisco Aironet 3800 シリーズ アクセス ポイント • Cisco Aironet 4800 シリーズ アクセス ポイント Cisco 802.11ac Wave 1 AP • Cisco Aironet 1700 シリーズ アクセス ポイント • Cisco Aironet 2700 シリーズ アクセス ポイント • Cisco Aironet 3700 シリーズ アクセス ポイント Cisco Catalyst 9105 シリーズ Wi-Fi 6 アクセスポイント Cisco Catalyst 9115 シリーズ Wi-Fi 6 アクセスポイント Cisco Catalyst 9117 シリーズ Wi-Fi 6 アクセスポイント Cisco Catalyst 9120 シリーズ Wi-Fi 6 アクセスポイント Cisco Catalyst 9124 シリーズ Wi-Fi 6 アクセスポイント Cisco Catalyst 9130 シリーズ Wi-Fi 6 アクセスポイント Cisco Catalyst 9136 シリーズ Wi-Fi 6 アクセスポイント

事前設定

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラで、スイッチが **aaa new-model** ですでに設定されている場合は、次のコマンドが存在することを確認してください。

```
aaa new-model
aaa authentication login default local
aaa authorization exec default local
aaa session-id common
```

これは、NETCONF の設定では必須です。プロビジョニングに自動アンダーレイを使用している場合、これらの設定は必要ありません。

Catalyst 9000 スイッチ用 Cisco Catalyst 9800 組み込みワイヤレスコントローラを設定するためのワークフロー

1. Cisco DNA Center をインストールします。

   詳細については、『CISCO DNA Center インストール ガイド』を参照してください。

2. Cisco DNA Center GUI にログインし、必要なアプリケーションが**実行**状態であることを確認します。

   メニューアイコン（☰）をクリックして、**[System]** > **[Software Updates]** > **[Installed Apps]** の順に選択します。

3. Cisco Identity Services Engine と Cisco DNA Center を連動させます。Cisco ISE が Cisco DNA Center に登録されると、Cisco DNA Center が検出するすべてのデバイスが、関連する設定データやその他のデータとともに Cisco ISE にプッシュされます。

4. Cisco Catalyst 9000 シリーズスイッチおよびエッジスイッチを検出します。

   Catalyst 9000 シリーズ スイッチの Cisco Catalyst 9800 組み込みワイヤレスコントローラを検出するには、NETCONF を有効にし、ポートを 830 に設定する必要があります。

   エッジスイッチを検出するために NETCONF を有効にする必要はありません。

   詳細については、CDP を使用したネットワークの検出 （51 ページ）およびIP アドレス範囲を使用したネットワークの検出 （59 ページ）を参照してください。

   [Preferred Management IP] を [Use Loopback] に変更します。

5. デバイスが [Device Inventory] に [Managed] 状態で表示されていることを確認します。

   詳細については、インベントリについて （84 ページ）およびインベントリに関する情報の表示 （85 ページ）を参照してください。

   デバイスが**管理対象**状態になっていることを確認します。

6. ネットワークの地理的な場所を表すネットワーク階層を設計します。サイト、ビルディング、フロアを作成すると、後で設計の設定や構成を適用する場所を簡単に特定できるようになります。

   新しいネットワーク階層を作成します。または Cisco Prime Infrastructure に既存のネットワーク階層がある場合は、それを Cisco DNA Center にインポートできます。

   既存のネットワーク階層をインポートしてアップロードするには、Cisco DNA Center へのサイト階層のインポート （159 ページ）を参照してください。

   新しいネットワーク階層を作成するには、ネットワーク階層のサイトの作成 （166 ページ）および建物の追加 （167 ページ）を参照してください。

7. 非ファブリックネットワークで設計フェーズ中にヒートマップの可視化を取得するには、フロアマップに AP を追加して配置します。

ファブリックネットワークの場合、設計時にフロアマップに AP を配置することはできません。APは、ファブリックネットワークにデバイスを追加した後にオンボードされます。

詳細については、「フロアマップでの AP の操作 （178 ページ）」を参照してください。

8. AAA（Cisco ISE がネットワークおよびクライアントエンドポイント用に設定されている）、NetFlow コレクタ、NTP、DHCP、DNS、syslog、および SNMP トラップなどのネットワーク設定を定義します。これらのネットワークサーバーが、ネットワーク全体のデフォルトになります。

   SSID の作成時に、[Wireless] ウィンドウで最大 6 つの AAA サーバーを設定できます。

   詳細については、ネットワーク設定の概要 （227 ページ）、グローバル ネットワーク サーバーの設定 （230 ページ）、および「Cisco ISE またはその他の AAA サーバーの追加」を参照してください。

9. CLI、SNMP、HTTP などのデバイスのログイン情報を設定します。

   詳細については、グローバル デバイス クレデンシャルの概要 （230 ページ）、グローバル CLI クレデンシャルの設定 （230 ページ）、グローバル SNMPv2c クレデンシャルの設定 （231 ページ）、グローバル SNMPv3 クレデンシャルの設定 （233 ページ）、グローバル HTTPS クレデンシャルの設定 （235 ページ）を参照してください。

10. IP アドレスプールをグローバルレベルで設定します。

    IP アドレスプールを設定するには、IP アドレス プールを設定する （241 ページ）を参照してください。

    プロビジョニングするビルディングの IP アドレスプールを予約するには、「LAN 自動化によるネットワークのプロビジョニング」を参照してください。

11. エンタープライズおよびゲストワイヤレスネットワークを作成します。グローバルワイヤレス設定を 1 回定義すると、Cisco DNA Center はあらゆる場所にあるさまざまなデバイスに設定をプッシュします。

    ワイヤレスネットワークの設計は、2 段階のプロセスです。初めに、[Wireless] ウィンドウで SSID を作成する必要があります。次に、作成した SSID をワイヤレス ネットワーク プロファイルに関連付けます。このプロファイルは、サイトにデバイスを展開するために使用されるトポロジを構築するのに役に立ちます。

    詳細については、エンタープライズ ワイヤレス ネットワーク用 SSID の作成 （248 ページ）およびゲスト ワイヤレス ネットワークの SSID の作成 （256 ページ）を参照してください。

12. バックホールの設定を行います。

13. [Policy] ウィンドウで、次のように設定します。

    - 仮想ネットワークを作成します。仮想ネットワークを使用して、物理ネットワークを複数の論理ネットワークにセグメント化できます。

- グループベースのアクセス コントロール ポリシーを作成し、契約を追加します。詳細については、「グループベースのアクセス コントロール ポリシーの作成 （614 ページ）」を参照してください。

14. 設計フェーズ中に追加された設定を使用して、Cisco Catalyst 9000 シリーズスイッチとエッジノードスイッチをプロビジョニングします。
    - ファブリックサイトを作成します。
    - CP+ボーダー+エッジまたはCP+ボーダーを作成して、デバイスをファブリックネットワークに追加します。
    - Catalyst 9000 シリーズ スイッチの Cisco Catalyst 9800 組み込みワイヤレスコントローラで、組み込みワイヤレス機能を有効にします。
    - ファブリックドメインで AP をオンボードします。

    デバイスが正常に展開されると、展開ステータスが [Configuring] から [Success] に変わります。

Cisco Catalyst 9000 シリーズ スイッチでの組み込みワイヤレスのプロビジョニング

始める前に

Catalyst 9000 シリーズ スイッチの Cisco Catalyst 9800 組み込みワイヤレスコントローラをプロビジョニングする前に、Catalyst 9000 スイッチ用 Cisco Catalyst 9800 組み込みワイヤレスコントローラを設定するためのワークフロー（474 ページ）の手順を完了していることを確認します。

この手順では、Cisco Catalyst 9300 シリーズ スイッチ、Cisco Catalyst 9400 シリーズ スイッチ、および Cisco Catalyst 9500H シリーズ スイッチに組み込みワイヤレスをプロビジョニングする方法について説明します。

ステップ 1 メニューアイコン（☰）をクリックして、**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。

[Inventory] ウィンドウが表示され、検出されたデバイスが一覧表示されます。

ステップ 2 Catalyst 9000 シリーズ スイッチデバイスと、サイトに関連付けるエッジスイッチの横にあるチェックボックスをオンにします。

ステップ 3 [Actions] ドロップダウンリストから、**[Provision]** > **[Assign Device to Site]** の順に選択します。

ステップ 4 [Assign Device to Site] ステップで、次を実行します。

a) [Choose a site] をクリックします。

b) [Choose a site] スライドインペインで、サイトの横にあるチェックボックスをオンにして、デバイスを関連付けます。
c) **[Save]** をクリックします。
d) [Apply] をクリックします。
次の手順では、設計フェーズ中に追加された設定を使用して、Catalyst 9000 シリーズ スイッチとエッジノードをプロビジョニングします。

ステップ 5 **[Devices]** > **[Inventory]** ウィンドウで、プロビジョニングするデバイス名の横にあるチェックボックスをオンにします。

a) [Actions] ドロップダウンリストから、**[Provision]** > **[Provision Device]** を選択します。
b) **[Next]** をクリックします。
c) [Summary] ステップで設定を確認し、[Deploy] をクリックします。
d) [Provision Devices] ウィンドウで、次の手順を実行して CLI 設定をプレビューします。

- [Generate Configuration Preview] オプションボタンをクリックします。
- [Task Name] フィールドに、CLI プレビュータスクの名前を入力し、[Apply] をクリックします。
- [Task Submitted] ポップアップで、[Work Items] リンクをクリックします。

（注） [Task Submitted] ポップアップが表示されなかった場合は、メニューアイコン（☰）をクリックし、**[Activities]** > **[Work Items]** の順に選択します。

- [Work Items] ウィンドウで、設定プレビュー要求を送信した CLI プレビュータスクをクリックします。
- CLI 設定の詳細を表示し、[Deploy] をクリックします。
- 即座にデバイスを展開するには、[Now] オプションボタンをクリックし、[Apply] をクリックします。
- 将来の日付と時刻でデバイスの展開をスケジュールするには、[Later] オプションボタンをクリックし、展開する日時を定義します。
- [Information] ポップアップで、次の手順を実行します。
  - [Work Items] ウィンドウから CLI プレビュータスクを削除する場合は、[Yes] をクリックします。
  - [Work Items] ウィンドウでタスクを保持する場合は、[No] をクリックします。

（注） CLI タスクは、[Work Items] ウィンドウで完了済みとしてマークされます。このタスクの CLI 設定は表示することはできますが、再度展開することはできません。

ステップ 6 エッジスイッチをプロビジョニングするには、プロビジョニングするエッジスイッチの横にあるチェックボックスをオンにします。

a) [Actions] ドロップダウンリストから、[Provision] を選択します。
b) **[Next]** をクリックします。

c) [Summary] ウィンドウで設定を確認し、[Deploy] をクリックします。

デバイスが正常に展開されると、[Provision Status] が [Configuring] から [Success] に変わります。

ステップ 7 ファブリックサイトにデバイスを追加するには、メニューアイコン（☰）をクリックし、**[Provision]** > **[Fabric Sites]** の順に選択します。

ステップ 8 ファブリックサイトを作成します。詳細については、「ファブリックサイトの追加（511 ページ）」を参照してください。

ステップ 9 IP トランジットネットワークを追加します。

ステップ 10 デバイスを追加して、ファブリックサイトに仮想ネットワークを関連付けます。

ステップ 11 Cisco Catalyst 9000 シリーズ スイッチをコントロールプレーン、ボーダーノード、およびエッジノードか、またはコントロールプレーンとボーダーノードとして追加します。

a) デバイスをクリックし、[Add as CP+Border+Edge] または [Add as CP+Border] を選択します。

b) エッジノードをクリックして、[Add to Fabric] を選択します。

c) **[Save]** をクリックします。

ステップ 12 デバイス上で組み込みのワイヤレスを有効にするには、[Edge]、[CP+Border+Edge] または [CP+Border] として追加されたデバイスをクリックし、[Embedded Wireless] をクリックします。

a) ワイヤレス機能を有効にする前に Cisco Catalyst 9000 シリーズ スイッチにワイヤレスパッケージをインストールしなかった場合は、Cisco DNA Center に「機能を有効にするには、`9800-SW` イメージが必要です`[OK]` をクリックして、`9800-SW` イメージを手動でインポートしてください。（`9800-SW image is necessary for turning on the capability. Click "OK" to import the 9800-SW image manually`）」という警告メッセージが表示されます。

b) [OK] をクリックして、イメージを手動でインストールします。

c) [Download Image] ウィンドウで、[Choose File] をクリックしてローカルに保存されているソフトウェアイメージに移動するか、または [Enter image URL] でソフトウェアイメージのインポート元となる HTTP または FTP を指定します。

d) [Import] をクリックします。

インポートの進捗状況が表示されます。

e) [Activate image on device] をクリックします。

「デバイスでイメージが有効化されると、デバイスがリブートします。デバイスをリブートしてもよろしいですか。（`Activate image on device will reboot the device. Are you sure you want to reboot the device?`）」という警告メッセージが表示されます。

f) [Yes] をクリックします。

デバイスパッケージのアップグレードが完了すると、デバイスがリブートし、オンラインになります。

g) 表示されるダイアログボックスに、コントローラで管理されている AP の場所が表示されます。ここからサイトの変更、削除、または再割り当てができます。

h) **[Next]** をクリックします。

ステップ 13 [Summary] ステップで詳細を確認し、[Save] をクリックします。

ステップ 14 [Modify Fabric] ステップで、[Now] をクリックして変更を確定し、[Apply] をクリックして設定を適用します。
次の手順では、ファブリックサイトで AP をオンボードします。

ステップ 15 Cisco DNA Center GUI で、[Provision] タブをクリックします。

ステップ 16 **[Fabric]** タブをクリックします。

ファブリックサイトのリストが表示されます。

ステップ 17 作成したファブリックサイトを選択し、[Host Onboarding] タブをクリックして、AP の IP プールを有効にします。

ステップ 18 ファブリックサイト内のデバイスに適用される認証テンプレートを選択します。これらのテンプレートは、Cisco ISE から取得される事前定義済みの設定です。認証テンプレートを選択したら、[Save] をクリックします。

ステップ 19 [Virtual Networks] の下で、[INFRA_VN] をクリックして、選択した仮想ネットワークに 1 つ以上の IP プールを関連付けます。

ステップ 20 [Virtual Network] の下で、ゲスト仮想ネットワークをクリックして、選択したゲスト仮想ネットワークの IP プールを関連付けます。

ステップ 21 設計フェーズ中に AP 用に作成された [IP Pool Name] チェックボックスをオンにします。

ステップ 22 [Update] をクリックして設定を保存します。

AP は、指定したプールから IP アドレスを取得します。このプールは、AP VLAN に関連付けられていて、いずれかの検出方法を通じてシスコ ワイヤレス コントローラに登録されます。

ステップ 23 ホストがアクセスできるネットワーク内のワイヤレス SSID を指定します。[Wireless SSID] セクションで、ゲスト SSID または企業 SSID を選択してアドレスプールを割り当ててから、[Save] をクリックします。

ステップ 24 [Inventory] > [Resync] を実行して手動で再同期をトリガーし、組み込みのワイヤレス用の Cisco DNA Center で AP を確認します。
検出された AP が [Provision] ページの [Inventory] に表示され、[Status] は [Not Provisioned] として表示されます。

ステップ 25 AP をプロビジョニングします。

詳細については、シスコ製 AP のプロビジョニング：Day 1 AP プロビジョニング （430 ページ）を参照してください。

ステップ 26 アプリケーションポリシーを設定および展開します。詳細については、アプリケーション ポリシーの作成（660 ページ）、アプリケーション ポリシーの展開 （666 ページ）、およびアプリケーション ポリシーの編集 （664 ページ）を参照してください。

アプリケーションポリシーを展開する前に、Catalyst 9300 シリーズ スイッチおよび Cisco Catalyst 9500H シリーズ スイッチをプロビジョニングします。

2 つの異なる SSID で異なるビジネスとの関連性を持つ 2 つの異なるポリシーは機能しません。関連性を設定するときは、最後に展開したポリシーが常に優先されます。

アプリケーションのデフォルトのビジネスとの関連性を変更しても、FlexConnect モードでは動作しません。

非ファブリック SSID にのみアプリケーションポリシーを適用できます。

Cisco Catalyst 9000 シリーズスイッチに Catalyst 9800 組み込みワイヤレスを搭載したファブリックインアボックス

ファブリックインアボックスに関する情報

Cisco Catalyst 9000 シリーズ スイッチには、Cisco DNA Center を使用して設定できる、単一のスイッチでファブリックエッジ、コントロールプレーン、ボーダー、および組み込みのワイヤレス機能をホストする機能があります。

この機能を使用すると、小規模サイトの場所での設定が簡素化され、Cisco SD-Access の導入コストが削減されます。

Cisco Catalyst 9000 シリーズスイッチに CP+ ボーダー + エッジノードを追加する方法については、Cisco Catalyst 9800 シリーズ ワイヤレスコントローラのプロビジョニング （462 ページ）を参照してください。

拡張性に関する情報

次の表に、デバイスの拡張性に関する情報を示します。

ファブリックの構造	Cisco Catalyst 9300 シリーズ スイッチ	Cisco Catalyst 9400 シリーズ スイッチ	Cisco Catalyst 9500 シリーズ スイッチ	Cisco Catalyst 9500-H シリーズ スイッチ
仮想ネットワーク	256	256	256	256
ローカルエンドポイント/ホスト	4 K	4 K	4 K	4 K
SGT/DGT テーブル	8K	8K	8K	8K
SGACL（セキュリティ ACE）	5K	18K	18K	18K

リリース間コントローラモビリティの概要

リリース間コントローラモビリティ（IRCM）は、異なるソフトウェアバージョンのさまざまなシスコ ワイヤレス コントローラ で実行されるシームレスなモビリティとワイヤレスサービスをサポートします。

Cisco DNA Center は、次のデバイスの組み合わせでゲストアンカー機能をサポートしています。

- アンカーコントローラとしての Cisco AireOS コントローラとフォーリンコントローラとしての Cisco AireOS コントローラの設定。
- フォーリンコントローラとしての Cisco Catalyst 9800 シリーズ ワイヤレス コントローラとゲストアンカーコントローラとしての Cisco AireOS コントローラの設定。
- アンカーコントローラとしての Cisco Catalyst 9800 シリーズ ワイヤレス コントローラとフォーリンコントローラとしての Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの設定。

コントローラデバイスでの IRCM の設定には、次の制約事項があります。

- フォーリンコントローラとしての Cisco AireOS コントローラの設定、およびアンカーコントローラとしての Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの設定はサポートされていません。
- ファブリックゲストアンカーの設定はサポートされていません。
- 複数のアンカーコントローラの設定、および 1 つのフォーリンコントローラの設定はサポートされていません。
- ゲスト SSID のみがサポートされています。
- ゲストアンカーモードでの非ゲストアンカー SSID のブロードキャストはサポートされていません。
- モビリティトンネルは暗号化されません。

ゲスト アンカーの設定とプロビジョニング

ゲスト アンカー シスコ ワイヤレス コントローラ を設定するには、次の手順に従います。

ステップ 1 サイト、ビルディング、フロアなどのネットワーク階層を設計します。詳細については、ネットワーク階層のサイトの作成 （166 ページ）を参照してください。

ステップ 2 AAA、DHCP、DNS サーバーなどのネットワーク サーバーを設定します。詳細については、グローバル ネットワーク サーバーの設定 （230 ページ）およびCisco ISE またはその他の AAA サーバーの追加 （228 ページ）を参照してください。

ステップ 3 Cisco Identity Services Engine を設定し、外部 Web 認証と中央 Web 認証を使用してゲスト ワイヤレス ネットワークの SSID を作成します。

ステップ 4 Cisco Discovery Protocol（CDP）または IP アドレス範囲を使用して ワイヤレスコントローラ を検出し、そのデバイスが **[Devices]** > **[Inventory]** ウィンドウに [Managed] 状態で表示されていることを確認します。詳細については、「検出の概要 （45 ページ）」を参照してください。

ステップ 5 アクティブなメイン ワイヤレスコントローラ として外部 ワイヤレスコントローラ をプロビジョニングします。「Cisco AireOS コントローラのプロビジョニング （422 ページ）」を参照してください。

ステップ 6 ゲスト アンカーとして ワイヤレスコントローラ のロールを選択し、ゲスト アンカー コントローラをプロビジョニングします。詳細については、「Cisco AireOS コントローラのプロビジョニング （422 ページ）」を参照してください。

ステップ 7 CLI、SNMP、HTTP、HTTPS などのデバイス クレデンシャルを設定します。詳細については、グローバル CLI クレデンシャルの設定 （230 ページ）、グローバル SNMPv2c クレデンシャルの設定 （231 ページ）、グローバル SNMPv3 クレデンシャルの設定 （233 ページ）、およびグローバル HTTPS クレデンシャルの設定 （235 ページ）を参照してください。

IRCM：Cisco AireOS コントローラと Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ

始める前に

- Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ および Cisco AireOS コントローラを検出します。

  Catalyst 9800 シリーズ ワイヤレス コントローラを検出するには、NETCONF を有効にしてポートを 830 に設定する必要があります。NETCONF は、ネットワークデバイスの設定をインストール、操作、削除するためのメカニズムです。

  詳細については、CDP を使用したネットワークの検出 （51 ページ）またはIP アドレス範囲を使用したネットワークの検出 （59 ページ）を参照してください。

- サイト、ビルディング、フロアを追加してネットワーク階層を設計すると、後で設計の設定や構成を適用する場所を簡単に特定できるようになります。

  新しいネットワーク階層を作成するには、ネットワーク階層のサイトの作成（166ページ）および建物の追加 （167 ページ）を参照してください。

- AP の位置情報を追加し、フロアマップに配置して、ヒートマップカバレッジを可視化します。

  詳細については、「フロアマップでの AP の操作 （178 ページ）」を参照してください。

- AAA（Cisco ISE がネットワークとクライアントエンドポイント向けに設定されている）、NetFlow コレクタ、NTP、DHCP、DNS、syslog、SNMP トラップなどのネットワーク設定を定義します。これらのネットワークサーバーが、ネットワーク全体のデフォルトになります。AAA サーバーを追加するときに、TACACS サーバーを追加できます。

詳細については、ネットワーク設定の概要（227ページ）、グローバル ネットワーク サーバーの設定（230 ページ）、および「Cisco ISE またはその他の AAA サーバーの追加」を参照してください。

- ゲスト ワイヤレス ネットワークの SSID を作成します。

  詳細については、「ゲスト ワイヤレス ネットワークの SSID の作成（256 ページ）」を参照してください。

- フォーリンコントローラとアンカーコントローラの WLAN プロファイル名は、モビリティに対して同じにする必要があります。

ステップ 1 メニューアイコン（☰）をクリックして、**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。

[Inventory] ウィンドウが表示され、検出されたデバイスが一覧表示されます。

ステップ 2 フォーリンコントローラとしてプロビジョニングする Catalyst 9800 シリーズ ワイヤレス コントローラの横にあるチェックボックスをオンにします。

ステップ 3 [Actions] ドロップダウンリストから、**[Provision]** > **[Provision]** を選択します。

ステップ 4 [Assign Site] ウィンドウで、[Choose a Site] をクリックして Catalyst 9800 シリーズ ワイヤレス コントローラ デバイスにサイトを割り当てます。

ステップ 5 [Add Sites] ウィンドウで、サイト名の横にあるチェックボックスをオンにして Catalyst 9800 シリーズ ワイヤレス コントローラ を関連付けます。

ステップ 6 **[Save]** をクリックします。

ステップ 7 [Apply] をクリックします。

ステップ 8 **[次へ (Next)]** をクリックします。

ステップ 9 Catalyst 9800 シリーズ ワイヤレス コントローラ のロールを [Active Main WLC] として選択します。

ステップ 10 アクティブなメイン ワイヤレスコントローラ では、インターフェイスと VLAN の詳細を設定する必要があります。

ステップ 11 [Assign Interface] エリアで、次の操作を実行します。

- [VLAN ID]：VLAN ID の値を入力します。
- [IP Address]：インターフェイス IP アドレスを入力します。
- [Gateway IP Address]：ゲートウェイ IP アドレスを入力します。
- [Subnet Mask (in bits)]：インターフェイスのネットマスクの詳細を入力します。

（注） Catalyst 9800 シリーズ ワイヤレス コントローラ では、IP アドレス、ゲートウェイ IP アドレス、およびサブネットマスクを割り当てる必要はありません。

ステップ 12 **[Next]** をクリックします。

ステップ 13 [Summary] ウィンドウで、設定の詳細を確認します。

ステップ 14 [Deploy] をクリックし、Catalyst 9800 シリーズ ワイヤレス コントローラ をフォーリンコントローラとしてプロビジョニングします。

ステップ 15 **[Devices]** > **[Inventory]** ウィンドウで、ゲストアンカーコントローラとしてプロビジョニングする Cisco AireOS コントローラの横にあるチェックボックスをオンにします。

ステップ 16 手順 3 ～ 8 を繰り返します。

ステップ 17 Cisco AireOS コントローラのロールを [Guest Anchor] として選択します。

ステップ 18 ゲストアンカー ワイヤレスコントローラ の場合は、インターフェイスと VLAN の詳細を設定する必要があります。

ステップ 19 手順 11 ～ 14 を繰り返します。

Meraki デバイスのプロビジョニング

この手順では、Meraki ダッシュボードによって管理されている Cisco Meraki デバイスに SSID をプロビジョニングする方法について説明します。

始める前に

- Meraki ダッシュボードを Cisco DNA Center と統合します。Meraki ダッシュボードの統合（113 ページ）を参照してください。
- SSID を作成します。エンタープライズ ワイヤレス ネットワーク用 SSID の作成（248 ページ）を参照してください。

（注） Meraki ダッシュボードは、次の種類の SSID をサポートしています。

- [Open]：この SSID は、Meraki ダッシュボードの [Open] に対応しています。
- [WPA2 Personal]：この SSID は、Meraki ダッシュボードの [preshared key with WAP2] に対応しています。
- [WPA2 Enterprise]：この SSID は、Cisco Meraki ダッシュボードの Meraki 認証またはマイ Radius サーバーを使用した WAP-2 暗号化に対応しています。Cisco DNA Center における建物レベルのクライアントおよびエンドポイントの認証用に AAA サーバーまたは Cisco ISE サーバーを定義している場合は、その設定が Meraki ダッシュボードの [my Radius server] にプロビジョニングされます。それ以外の場合は、Merakiデバイスによる認証に [Meraki Radius] が使用されます。

すべての SSID に対して、インターフェイス名を選択できます。Cisco DNA Center で [Management] インターフェイスを選択した場合、VLAN ID は 0 です。つまり、Cisco Meraki ダッシュボードではサポートされないため、Cisco Meraki ダッシュボードでは VLAN タギングは無効になります。Cisco DNA Center で SSID のカスタムインターフェイスを作成すると、Cisco Meraki ダッシュボードで、カスタムインターフェイス名と VLAN ID を使用して AP タグが作成されます。

- ネットワークプロファイルを作成し、SSID がプロビジョニングされるサイトに割り当てます。

（注） Cisco DNA Center のネットワーク階層 **[Sites]** > **[Buildings]** は、Meraki ダッシュボードの **[Organization]** > **[Network]** に対応しています。ワークフローの [Add Sites to Profile] ウィンドウで、[Buildings] を選択することをお勧めします。

（注） Cisco DNA Center Meraki ネットワークを作成して、SSID をネットワークにプロビジョニングします。Meraki ダッシュボードは、Meraki ネットワーク構成を Meraki デバイスにプロビジョニングします。

ステップ 1 メニューアイコン（☰）をクリックして、**[Provision]**。

[Network Devices] > **[Inventory]** ウィンドウが表示され、検出されたすべてのデバイスが示されます。

ステップ 2 Meraki ダッシュボードを表示するには、左側のペインで [Global] サイトを展開し、ビルディングを選択します。

選択したビルディングで使用可能なすべての Meraki ダッシュボードが表示されます。

ステップ 3 プロビジョニングする Meraki ダッシュボードの横にあるチェックボックスをオンにします。

ステップ 4 [Actions] ドロップダウンリストから、**[Provision]** > **[Provision Device]** を選択します。

[Assign Site] ウィンドウが表示され、Meraki ダッシュボードと関連付けられたビルディングを確認できます。

ステップ 5 関連付けられたビルディングを変更するには、[Choose a site] をクリックします。

ステップ 6 [Choose a site] ウィンドウで、ビルディングを選択して [Save] をクリックします。

ステップ 7 **[次へ (Next)]** をクリックします。

[設定（Configuration）] ウィンドウが表示されます。管理ビルディングは、プライマリロケーションで表示できます。

ステップ 8 Meraki ダッシュボードのセカンダリ管理ロケーションを選択するには、[Select Secondary Managed AP Locations] をクリックします。

ステップ 9 [Managed AP Location] ウィンドウで、ビルディング名の横にあるチェックボックスをオンにします。

ステップ 10 [Save] をクリックします。

ステップ 11 [Next] をクリックします。
[Summary（サマリ）] ウィンドウには、次の情報が表示されます。

- **Device Details**
- **ネットワーク設定**
- **SSID**

  （注） Meraki 展開では、各ネットワークで最大 15 の SSID がサポートされています。

- **管理サイト**

ステップ 12 [展開（Deploy）] をクリックします。

ステップ 13 [Provision Devices] ウィンドウで、次の手順を実行して CLI 設定をプレビューします。

- [Generate Configuration Preview] オプションボタンをクリックします。
- [Task Name] フィールドに、CLI プレビュータスクの名前を入力し、[Apply] をクリックします。
- [Task Submitted] ポップアップで、[Work Items] リンクをクリックします。

  （注） [Task Submitted] ポップアップが表示されなかった場合は、メニューアイコン（☰）をクリックし、**[Activities]** > **[Work Items]** の順に選択します。

- [Work Items] ウィンドウで、設定プレビュー要求を送信した CLI プレビュータスクをクリックします。
- CLI 設定の詳細を表示し、[Deploy] をクリックします。
- 即座にデバイスを展開するには、[Now] オプションボタンをクリックし、[Apply] をクリックします。
- 将来の日付と時刻でデバイスの展開をスケジュールするには、[Later] オプションボタンをクリックし、展開する日時を定義します。
- [Information] ポップアップで、次の手順を実行します。
  - [Work Items] ウィンドウから CLI プレビュータスクを削除する場合は、[Yes] をクリックします。
  - [Work Items] ウィンドウでタスクを保持する場合は、[No] をクリックします。

（注） CLI タスクは、[Work Items] ウィンドウで完了済みとしてマークされます。このタスクの CLI 設定は表示することはできますが、再度展開することはできません。

展開が正常に完了すると、[デバイス インベントリ（Device Inventory）] ウィンドウの [プロビジョニング ステータス （Provision Status）] 列に「成功（SUCCESS）」と表示されます。

リモート テレワーカー デバイスのプロビジョニング

次のトピックでは、リモートテレワーカーサイトのコンポーネントと、リモートテレワーカーデバイスをプロビジョニングする手順について説明します。

リモートテレワーカーの導入の概要

導入コンポーネント

Cisco リモートテレワーカーの導入は、シスコ ワイヤレスコントローラ、Cisco OfficeExtend アクセスポイント（AP）、および企業ファイアウォールの 3 つの主要コンポーネントを中心に構築されています。次のモデルがこの導入でサポートされています。

- **ワイヤレスコントローラ**：Cisco AireOS 5520、8540、3504 コントローラ[4]、Cisco Catalyst 9800-40、9800-80 および 9800-L ワイヤレスコントローラ
- **アクセスポイント**：Cisco Aironet 1815T（テレワーカー）アクセスポイント、Cisco Catalyst 9800 シリーズ アクセスポイント

シスコ ワイヤレス コントローラについて

Cisco のコントローラは、システム全体のワイヤレス WLAN 機能（セキュリティポリシー、侵入防御、RF 管理、Quality of Service（QoS）、モビリティなど）を担っています。シスコの AP

[4] Cisco Aironet 1815 テレワーカー アクセス ポイントのみでサポートされます。

と連携して動作し、テレワーカーのビジネスクリティカルなワイヤレスアプリケーションをサポートします。コントローラは、ネットワーク管理者が安全かつスケーラブルなテレワーカー環境を構築するために必要な制御、スケーラビリティ、セキュリティ、および信頼性を提供します。

ユーザーが会社のデバイスを組織のオンサイト ワイヤレス ネットワークに接続できるようにするために、リモート テレワーク ソリューションは、組織内でデータと音声をサポートするものと同じワイヤレス Secure Set Identifier（SSID）をテレワーカーの自宅で提供します。

Cisco OfficeExtend アクセス ポイント

APをコントローラから独立して動作させることはできません。APは、コントローラリソースと通信するときに、必要に応じてその設定をダウンロードし、ソフトウェアまたはファームウェアイメージを同期します。AP は、コントローラへのセキュアな Datagram Transport Layer Security（DTLS）接続を構築し、企業のオフィスと同じプロファイルを使用してリモートWLAN接続を確立します。セキュアなトンネリングにより、すべてのトラフィックを一元化されたセキュリティ ポリシーに対して検証でき、家庭用のファイアウォールに関連する管理オーバーヘッドを最小限に抑えられます。

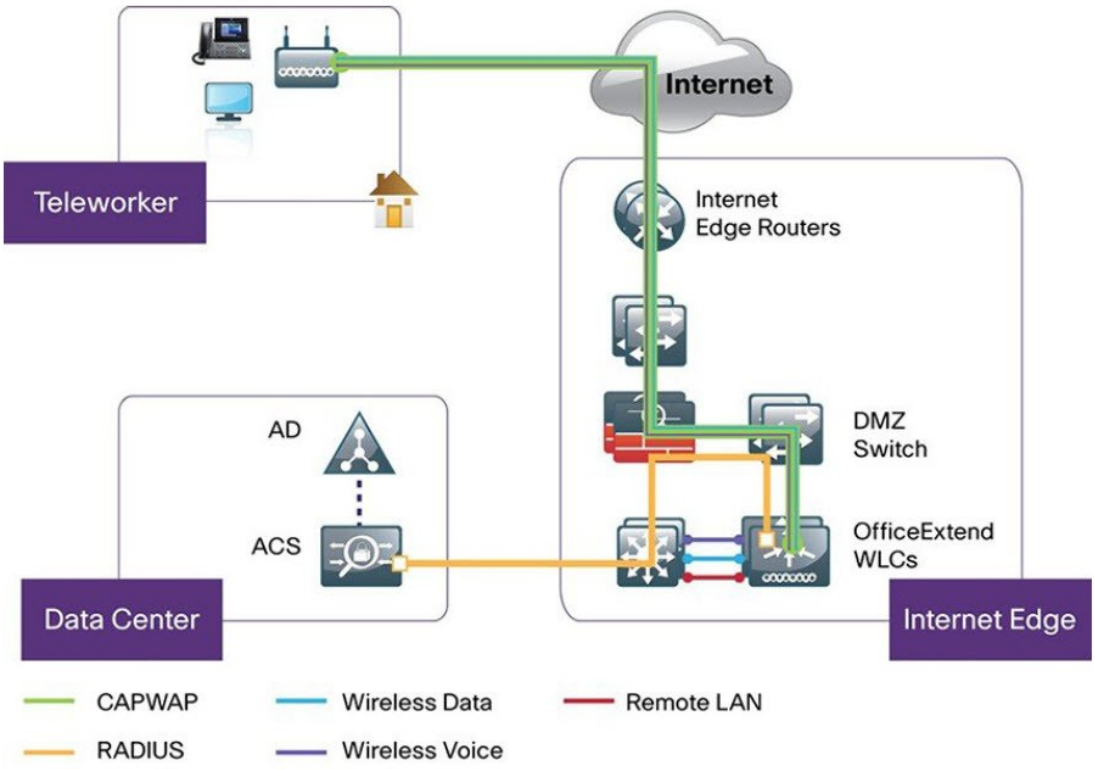
企業のファイアウォール

コントローラは緩衝地帯（DMZ）に配置する必要があり、企業ファイアウォールは、ファイアウォール経由でのコントローラへの CAPWAP 制御とデータトラフィックを許可する必要があります。ファイアウォールの一般設定では、ファイアウォール経由での CAPWAP 制御およびCAPWAP管理ポート番号が許可されます。コントローラとAPの間の通信用に、ファイアウォールで UDP 5246 および 5247 ポートを開く必要があります。

展開設定（Deployment Configuration）

最も柔軟で安全なリモートテレワーカー構成を実現するには、専用のコントローラペアをインターネットエッジ DMZ 専用に展開します。インターネットからのトラフィックは、内部ネットワークではなく DMZ で終端しますが、リモート AP は引き続き内部ネットワークに直接接続されています。

図 *22* : サンプルのリモートテレワーカー導入シナリオ



リモートテレワーカーサイトの作成

リモートテレワーカーサイトは、ワイヤレスコントローラとリモート テレワーカー アクセス ポイント（AP）を管理するためだけに使用される専用サイトです。リモートテレワーカーサイトを作成するには、サイトでリモートテレワーカー機能を有効にする必要があります。一度有効にすると、リモートテレワーカー機能は、サイトの階層内のサイト、建物、またはフロアに対して個別に無効にすることはできません。サイトでは、リモートテレワーカー機能のみを管理できます。

テレワーカーサイトでは、切り替えはコントローラから集中的に実行されます。ローカルスイッチングで Flex Connect のネットワークプロファイルを設定することはできません。

始める前に

- テレワーカーの展開で使用されるサポート対象デバイスを理解します。
- インベントリにシスコ ワイヤレスコントローラおよびシスコの AP があることを確認してください。ない場合は、デバイスを検出するか、手動で追加します。詳細については、ネットワークの検出 （45 ページ）またはネットワーク デバイスを追加 （98 ページ）を参照してください。

- ネットワークに適したグローバル ワイヤレス ネットワーク設定を構成します。詳細については、グローバル ワイヤレス設定の構成 （247 ページ）を参照してください。

ステップ 1 リモートテレワーカーAPを管理するためのサイトを作成します。「ネットワーク階層のサイトの作成 （166 ページ）」を参照してください。

ステップ 2 建物とフロアを追加します。「建物の追加 （167 ページ）」を参照してください。

ステップ 3 リモートテレワーカーサイトのワイヤレスネットワーク設定を構成します。

a) メニューアイコン（☰）をクリックして、**[Design]** > **[Network Settings]** > **[Wireless]** の順に選択します。
b) ナビゲーションツリーから、リモートテレワーカーサイトを選択します。
c) 下にスクロールして、[Enable Remote Teleworker] チェックボックスをオンにします。
d) **[Save]** をクリックします。

ステップ 4 コントローラをサイトに割り当てます。「デバイスをサイトに追加する （118 ページ）」を参照してください。

ステップ 5 AP をサイトに割り当てます。「デバイスをサイトに追加する （118 ページ）」を参照してください。

シリアル番号またはMACアドレスを使用できますが、両方を混在させることはできません。または、CSV ファイルをアップロードすることがきます。

ステップ 6 ワイヤレスネットワーク設定で、AP を承認済み AP リストに追加します。

a) 左側の階層ツリーで、次を選択します。 [Global] を選択します。
b) メニューアイコン（☰）をクリックして、**[Design]** > **[Network Settings]** > **[Wireless]** の順に選択します。
c) [Authorized Access Points] で、[Manage Authorized Access Points] をクリックします。
d) [Manage Authorized Access Points] ペインで、AP の MAC アドレス、シリアル番号、またはその両方を入力して、コントローラへの参加が許可される AP を識別します。

コントローラは、認証リストに含まれている AP からの CAPWAP 要求にのみ応答します。

ステップ 7 コントローラをプロビジョニングします。

a) メニューアイコン（☰）をクリックして、**[Provision]** > **[Inventory]** の順に選択します。

[Inventory] ウィンドウが表示され、検出されたデバイスが一覧表示されます。

b) プロビジョニングするコントローラを見つけます。
c) デバイス名の横にあるチェックボックスをオンにします。
d) [Actions] ドロップダウンリストから、**[Provision]** > **[Provision Device]** を選択します。
e) [Assign Site] ウィンドウで、割り当てられたサイトを選択して [Save] をクリックします。
f) [Next] をクリックします。
g) （任意） [Configuration] ウィンドウの [NAT Address for Remote Teleworker] で、[Enable NAT Address] チェックボックスをオンにして、NAT IP アドレスを入力します。
h) [Next] をクリックします。
i) [Model Configuration] ウィンドウで [Next] をクリックします。

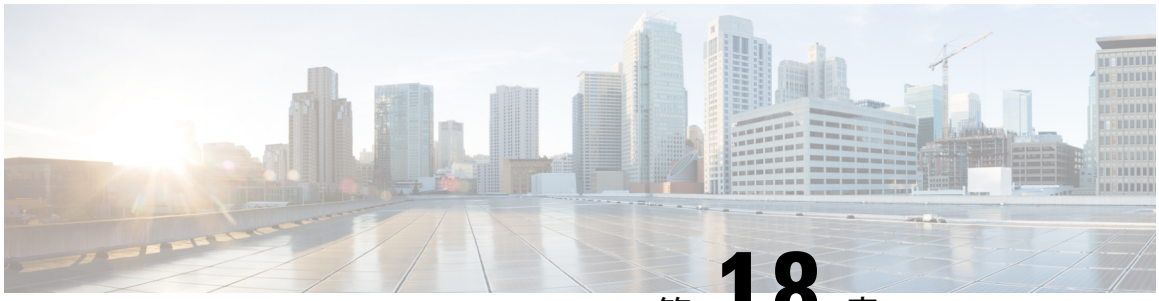
j) [Advanced Configuration] ウィンドウで [Next] をクリックします。
k) [Summary] ウィンドウで設定を確認し、[Deploy] をクリックします。
l) [Provision Device] スライドインペインで、[Now] を選択し、[Apply] をクリックします。

ステップ 8 シスコ ワイヤレス コントローラがプロビジョニングされたら、AP をプロビジョニングできます。

a) メニューアイコン（☰）をクリックして、**[Provision]** > **[Inventory]** の順に選択します。

[Inventory] ウィンドウが表示され、検出されたデバイスが一覧表示されます。

b) プロビジョニングする AP を見つけます。
c) デバイス名の横にあるチェックボックスをオンにします。
d) [Actions] ドロップダウンリストから、**[Provision]** > **[Provision Device]** を選択します。
e) [Assign Site] ウィンドウで、[Choose a floor] をクリックし、AP をフロアに割り当てます。
f) [Save] をクリックします。
g) [Next] をクリックします。
h) [Configuration] ウィンドウで [Next] をクリックします。
i) [Summary] ウィンドウで設定を確認し、[Deploy] をクリックします。
j) [Provision Device] スライドインペインで、[Now] を選択し、[Apply] をクリックします。



第 18 章

ルーティングプロファイルのプロビジョニング

ルーティングプロファイルのプロビジョニング

始める前に

ルーティングプロファイルをプロビジョニングする前に、次のグローバルネットワーク設定を定義したことを確認します。

- AAA、DHCP、および DNS などのネットワーク サーバー。詳細については、グローバル ネットワーク サーバーの設定 （230 ページ）を参照してください。
- CLI、SNMP、HTTP、HTTPS などのデバイス クレデンシャル。詳細については、グローバル CLI クレデンシャルの設定 （230 ページ）、グローバル SNMPv2c クレデンシャルの設定 （231 ページ）、グローバル SNMPv3 クレデンシャルの設定 （233 ページ）、およびグローバル HTTPS クレデンシャルの設定 （235 ページ）を参照してください。
- IP アドレス プール詳細については、「IP アドレス プールを設定する （241 ページ）」を参照してください。
- SP プロファイル。詳細については、「サービス プロバイダ プロファイルの設定 （247 ページ）」を参照してください。

ステップ 1 メニューアイコン（☰）をクリックして、**[Provision]** の順に選択します。

[Network Devices] > [Inventory] ウィンドウが表示されます。このウィンドウには、すべての検出済みデバイスが一覧表示されます。

ステップ 2 特定のサイトで使用可能なデバイスを表示するには、左側のペインで [Global] サイトを展開し、関心のあるサイト、ビルディング、またはフロアを選択します。

選択したサイトで使用可能なすべてのデバイスが [Inventory] ウィンドウに表示されます。

ステップ 3 [Device Type] リストから [Routers] タブをクリックし、[Reachability] リストから [Reachable] タブをクリックして、検出され到達可能なデバイスのリストを取得します。

ステップ 4 プロビジョニングするデバイス名の横にあるチェックボックスをオンにします。

ステップ 5 サイトで [Assign] をクリックすると、[Assign Device to Site] ウィンドウが表示されます。[Choose a Site] をクリックします。

ステップ 6 [Actions] ドロップダウンリストから、**[Provision]** > **[Provision Device]** を選択します。

ルータをプロビジョニングするには、次の手順を実行します。

- [Confirm Profile] ウィンドウで詳細を確認し、[Next] をクリックします。
- [Router WAN Configuration] ウィンドウで詳細を確認します。
  - 回線インターフェイスとしてギガビットイーサネットを選択した場合は [O] をクリックし、静的 IP アドレスを選択した場合は WAN IP アドレスを入力します。[DHCP] を選択した場合は、DHCP サーバーの IP アドレスを入力します。プライマリ WAN がすでに PnP を使用して設定されている場合は、[Do Not Change] を選択して、ドロップダウンリストからプライマリ WAN として設定されているインターフェイスを選択します。
  - 回線インターフェイスとしてセルラーを選択した場合は、[O] をクリックして、[IP Negotiated] を選択し、ドロップダウンリストから [Interface Name] を選択して [Access Point Name (APN)] を入力します。サービスプロバイダに応じて、[PAP] チェックボックスまたは [CHAP] チェックボックスをオンにします。
  - 複数のサービスプロバイダを利用している場合は、バックアップ WAN インターフェイスの [IP SLA Address] を入力します。

  仮想ルータをプロビジョニングしている場合、このウィンドウは表示されません。
- [Router LAN Configuration] ウィンドウで詳細を確認し、[Next] をクリックします。

  [Interface(s)] ドロップダウンリストから 1 つの L3 インターフェイスまたは 1 つまたは複数の L2 インターフェイスを選択できるようになりました。
- [Integrated Switch Configuration] ウィンドウで詳細を確認し、[Next] をクリックします。
- [Summary] ページで詳細を確認します。

ステップ 7 [展開（Deploy）] をクリックします。

ステップ 8 [Provision Devices] ウィンドウで、次の手順を実行して CLI 設定をプレビューします。

- [Generate Configuration Preview] オプションボタンをクリックします。
- [Task Name] フィールドに、CLI プレビュータスクの名前を入力し、[Apply] をクリックします。
- [Task Submitted] ポップアップで、[Work Items] リンクをクリックします。

  （注） [Task Submitted] ポップアップが表示されなかった場合は、メニューアイコン（☰）をクリックし、**[Activities]** > **[Work Items]** の順に選択します。

- [Work Items] ウィンドウで、設定プレビュー要求を送信した CLI プレビュータスクをクリックします。
- CLI 設定の詳細を表示し、[Deploy] をクリックします。
- 即座にデバイスを展開するには、[Now] オプションボタンをクリックし、[Apply] をクリックします。
- 将来の日付と時刻でデバイスの展開をスケジュールするには、[Later] オプションボタンをクリックし、展開する日時を定義します。
- [Information] ポップアップで、次の手順を実行します。
  - [Work Items] ウィンドウから CLI プレビュータスクを削除する場合は、[Yes] をクリックします。
  - [Work Items] ウィンドウでタスクを保持する場合は、[No] をクリックします。

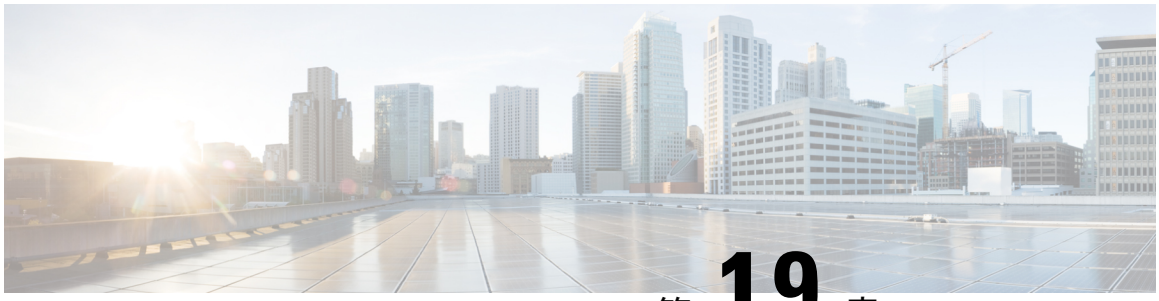
  （注） CLI タスクは、[Work Items] ウィンドウで完了済みとしてマークされます。このタスクの CLI 設定は表示することはできますが、再度展開することはできません。

展開が正常に完了すると、[デバイス インベントリ（Device Inventory）] ウィンドウの [プロビジョニング ステータス （Provision Status）] 列に「成功（SUCCESS）」と表示されます。[SUCCESS] をクリックして詳細なプロビジョニング ログ ステータスを確認します。

VPC インベントリ収集

クラウドインベントリ収集が正常に完了すると、[Provision] セクションの [Cloud] タブに、収集した AWS VPC インベントリのビューが表示されます。左側のナビゲーションを展開して、クラウドプロファイルまたはアクセスキーのクラウド領域を表示できます。左側のナビゲーション項目をキーワードでフィルタ処理してクリックすると、選択した領域またはアクセスキーに対してのみ VPC が表示されます。

[VPC Inventory] ビューでは、VPC をクリックして、その VPC のサブネットや仮想インスタンスなどの詳細を確認することもできます。AWS VPC インベントリ収集は、すべてのインベントリ収集のデフォルト間隔で行われるようにスケジュールされており、クラウドアクセスキーの歯車メニューの [Sync] アクションを使用して、オンデマンドでトリガーすることもできます。インベントリ収集のステータスを表示するには、[VPC Inventory] ビューで [Show Sync Status] をクリックします。



第 19 章

ファイアウォール プロファイルのプロビジョニング

ファイアウォール プロファイルのプロビジョニング

この手順では、Firepower Management Center（FMC）によって管理される Firepower Threat Defense（FTD）デバイスをプロビジョニングする方法について説明します。

始める前に

- FMC と Cisco DNA Center を統合します。Firepower Management Center の統合 （114 ページ）を参照してください。
- ネットワーク階層内でサイトを作成します。ネットワーク階層のサイトの作成（166 ページ）を参照してください。
- ファイアウォールのネットワークプロファイルを作成し、FTDデバイスがプロビジョニングされるサイトに割り当てます。ファイアウォール用のネットワークプロファイルの作成（299 ページ）を参照してください。

ステップ 1 メニューアイコン（☰）をクリックして、**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。

[Inventory] ページには、ディスカバリプロセス中に収集されたデバイス情報が表示されます。

ステップ 2 プロビジョニングする FTD デバイスの横にあるチェックボックスをオンにして、[Site] 列の下にある [Assign] をクリックします。

ステップ 3 [Assign Device to Site] ウィンドウで、[Choose a Site] をクリックします。

ステップ 4 [Choose a Site] ウィンドウで、階層からサイトを選択して [Save] をクリックします。

ステップ 5 [Next] をクリックします。

ステップ 6 [Now] をクリックしてデバイスをサイトにすぐに割り当てるか、[Later] をクリックして特定の時間にスケジュールします。

ステップ 7 [**Assign**] をクリックします。

（注） **[Activities]** > **[Tasks]** で、サイトへのデバイスの割り当てのステータスを確認できます。

ステップ 8 [Actions] ドロップダウンリストから、**[Provision]** > **[Provision Device]** を選択します。

[Provision Firewall Profile] ウィンドウが表示されます。

ステップ 9 [Confirm Profile] ページで詳細を確認し、[Next] をクリックします。

ステップ 10 [Firewall Type] ページで詳細を確認し、[Next] をクリックします。

[FTD Configuration] ページが表示されます。

ステップ 11 ルーテッドモードのファイアウォールをサイトに関連付けている場合は、次の手順を実行します。

a) [Outside Interface] エリアを展開し、[Select Physical Interface] ドロップダウンリストから外部インターフェイスを選択して、[Static IP] または [DHCP] オプションボタンを選択します。

- [Static IP]：IP アドレスおよびサブネットマスクを入力します。
- [DHCP]：IP アドレスは DHCP から取得されます。

b) [Inside Interface] エリアを展開し、[Select Physical Interface] ドロップダウンリストから内部インターフェイスを選択して、[Static IP] または [DHCP] オプションボタンを選択します。

- [Static IP]：IP アドレスおよびサブネットマスクを入力します。
- [DHCP]：IP アドレスは DHCP から取得されます。

ステップ 12 トランスペアレントモードのファイアウォールをサイトに関連付けている場合は、次の手順を実行します。

a) [Outside Interface] エリアを展開し、[Select Physical Interface] ドロップダウンリストから外部インターフェイスを選択します。

b) [Inside Interface] エリアを展開し、[Select Physical Interface] ドロップダウンリストから内部インターフェイスを選択します。

c) [Bridge Virtual Interface] エリアを展開し、次の手順を実行します。

- [Bridge Group Number]：ブリッジグループ番号を入力します。有効な値は 1 ー 250 です。
- [IP]：FTD デバイスの IP アドレスを入力します。
- [Subnet Mask]：サブネットマスクを入力します。

ステップ 13 [Next] をクリックします。

[Summary] ページが表示されます。このページには、デバイスの仕様の概要が表示されます。

ステップ 14 [Summary] ページで詳細を確認し、[Deploy] をクリックします。

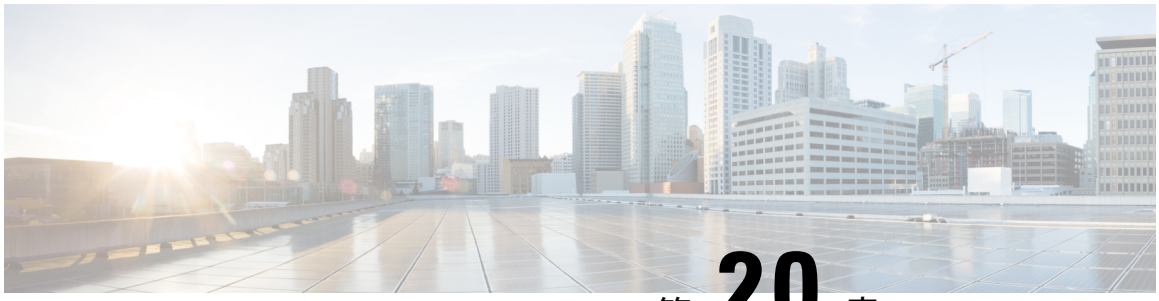
[Provision Firewall device(s)] ダイアログボックスが表示されます。

ステップ 15 [Now]、[Later]、または [Generate configuration preview] オプションボタンをクリックします。

- [Now]：プロビジョニングがすぐに開始されます。
- [Later]：特定の時間にプロビジョニングがスケジュールされます。
- [Generate configuration preview]：選択したデバイスに展開するために後で使用できるプレビューを作成します。

ステップ 16 [Apply] をクリックします。

（注） **[Activities]** > **[Tasks]** で、ファイアウォールデバイスのステータスを確認できます。[Provision Firewall device(s)] ダイアログボックスで [Generate configuration preview] を選択した場合は、**[Activities]** > **[Work Items]** でステータスを表示できます



第 20 章

LAN アンダーレイのプロビジョニング

LAN 自動化によるネットワークのプロビジョニング

始める前に

- ネットワーク階層を設定します。（デバイスをサイトに追加する （118ページ） を参照）。
- 以下のグローバルネットワーク設定が定義済みであることを確認します。
  - AAA、DHCP、DNS サーバーなどのネットワークサーバー（グローバル ネットワーク サーバーの設定 （230 ページ） を参照）。
  - CLI、SNMP、HTTP、HTTPS などのデバイスのクレデンシャル(グローバル CLI クレデンシャルの設定 （230ページ）、グローバル SNMPv2c クレデンシャルの設定 （231 ページ）、グローバル SNMPv3 クレデンシャルの設定 （233 ページ）、グローバル HTTPS クレデンシャルの設定 （235 ページ）を参照)。
  - IP アドレスプール（IP アドレス プールを設定する （241 ページ） を参照）。
- インベントリに少なくとも 1 つのデバイスがあることを確認してください。デバイスがない場合は、ディスカバリ機能を使用して検出します。

（注） 検出されたサイトがユーザー名「cisco」の CLI ログイン情報を使用して設定されている場合、LAN 自動化はブロックされます。

- ネットワークに Cisco Catalyst 9400 スイッチが設定されている場合は、LAN 自動化で 40G ポートが自動的に有効になるように設定されたスイッチで次の操作が実行されていることを確認します。

- Day-0 設定はスイッチで実行されます。
- 40G Quad Small Form-Factor Pluggable（QSFP）トランシーバはスーパバイザのポート 9 またはポート 10 のいずれかに挿入されます。スーパバイザ上の 1 ～ 8 のポートには、10G または 1G Small Form-Factor Pluggable（SFP）トランシーバは挿入されません。デュアル スーパーバイザ エンジンがある場合は、40G QSFP がポート 9 に挿入されていることを確認します。

  Catalyst 9400 シリーズ スーパーバイザの詳細については、『Cisco Catalyst 9400 Series Supervisor Installation Note』を参照してください。

ステップ 1 プロビジョニングするサイト用に IP アドレスプールを予約します。

（注） LAN 自動化 IP アドレスプールのサイズは、25 ビットのネットマスク以上である必要があります。

a) メニューアイコン（☰）をクリックして、**[Design]** > **[Network Settings]** > **[IP Address Pools]** の順に選択します。
b) [Network Hierarchy] ペインで、サイトを選択します。
c) [Reserve] をクリックし、[Reserve IP Pool] ウィンドウで次のフィールドに値を入力して、使用可能なグローバル IP アドレスプールのすべてまたは一部を特定のサイト用に予約します。
   - [IP Address Pool Name]：予約した IP アドレスプールの一意の名前。
   - [Type]：IP アドレスプールのタイプ。LAN 自動化の場合は、**LAN** を選択します。
   - [IP Address Space]：[IPv4] または [IPv6] をオンにしてアドレスプールを作成します。デュアルスタックプールを作成するには、[IPv4] と [IPv6] の両方のチェックボックスをオンにします。
   - [Global IP Pool]：IP アドレスのすべてまたは一部を予約する IPv4 アドレスプール。

     （注） LAN 自動化では、IPv4 サブネットのみが使用されます。

   - [Prefix length / Number of IP Addresses]：グローバル IP アドレスプールのすべてまたは一部を予約するために使用する IP サブネットとマスクアドレス、または予約する IP アドレスの数。
   - [Gateway]：ゲートウェイ IP アドレス。
   - [DHCP Server(s)]：DHCP サーバーの IP アドレス。
   - [DNS Server(s)]：DNS サーバーの IP アドレス。
d) [Reserve] をクリックします。

ステップ 2 デバイスを検出してプロビジョニングします。

a) メニューアイコン（☰）をクリックして、**[Provision]** > **[Inventory]** の順に選択します。

   すべての検出されたデバイスが表示されます。
b) [Actions] > [Provision] > [LAN Automation] の順にクリックします。

c) [LAN Automation] ウィンドウで、次のフィールドに値を入力します。

- [Primary Site]：このサイトからプライマリデバイスを選択します。
- Primary Device：Cisco DNA Center が新しいデバイスを検出しプロビジョニングする起点として使用するプライマリデバイスを選択します。
- [Peer Site]：このサイトは、ピアデバイスの選択に使用されます。このサイトは、プライマリサイトとは異なる場合がありますので注意してください。
- Peer Device：ピアデバイスを選択します。
- SELECTED PORTS OF PRIMARY DEVICE：新規デバイスの検出とプロビジョニングに使用するポート。[Modify Selections] をクリックしてポート番号を入力します。
- Discovered Device Site：新たに検出されたすべてのデバイスがこのサイトに割り当てられます。このサイトは、プライマリサイトおよびピアサイトとは異なる場合があります。
- Main IP Pool：LAN 自動化用に予約された IP アドレスプール（ステップ 1 を参照）。
- [Overlapping IP Pool]：他のサイトと共有される IP アドレスプール。アンダーレイでポイントツーポイントリンクに対する /31 IP アドレスを設定するために使用されます。

  リンク重複 IP プールには、親サイトから継承されるサブプールか他のサイトで定義されているサブプールを指定できます。

  リンク重複 IP プールを使用すると、マルチサイト展開で /31 IP アドレスの重複が可能になります。異なるサイトのホストにおいて、/31 リンクで IP アドレスを再利用できます。

  リンク重複 IP プールを定義した場合、[Main IP Pool] フィールドで定義されたアドレスが管理 IP（ループバックアドレスや VLAN アドレスなど）に使用されます。
- [IS-IS Domain Password]：LAN 自動化が開始するときにユーザーが指定する IS-IS パスワード。パスワードがすでにシード デバイスに存在する場合は、再使用され、上書きされることはありません。ユーザーが指定するパスワードが入力され、既存の IS-IS パスワードがデバイスにない場合、ドメインパスワードが使用されます。プライマリとセカンダリシードの両方がドメインパスワードをもつ場合、それらが一致することを確認してください。
- [Advertise LAN Automation summary route into BGP]：LAN 自動化が [Main IP pool] をプライマリおよびピアシードデバイスの BGP にアドバタイズする場合は、このチェックボックスをオンにします。LAN 自動化は、シードデバイスで BGP が構成されている場合にのみ、シードデバイスにサマリールートをアドバタイズします。

  デフォルトでは、このチェックボックスは無効になっていることに注意してください。プライマリまたはピアシードデバイスに自律システム（AS）番号が設定されている場合にのみ有効になります。
- Enable Multicast：このチェックボックスをオンにすると、アンダーレイ ネイティブ マルチキャストが有効になります。LAN 自動化によって、シードデバイスを RP とし、検出されたデバイスをサブスクライバとするマルチキャストツリーが作成されます。
- Device Name Prefix：プロビジョニングしているデバイスの名前プレフィックス。Cisco DNA Center で各デバイスをプロビジョニングするときに、ここで指定されたテキストでデバイスにプレフィッ

クスを付与し、末尾に一意の番号を追加します。たとえば、名前プレフィックスとして **Access** を入力した場合、各デバイスがプロビジョニングされると、Access-1、Access-2、Access-3 のように名前が付けられます。

- [Choose a File]：[Browse] をクリックして、ホスト名マップファイルを選択します。選択した CSV ファイルに記述されているシリアル番号とホスト名のマッピングを使用して、検出されたデバイスに対してユーザーが指定した名前が設定されます。検出されたデバイスがスタックの場合、スタックのすべてのシリアル番号が CSV ファイルで指定されます。

  サンプルの CSV ファイルは次のとおりです。

```
standalone-switch,FCW2212L0NF
stack-switch,"FCW2212E00Y,FCW2212L0GV"
```

d) [Start] をクリックします。

Cisco DNA Center は、新規デバイスの検出とプロビジョニングを開始します。

LAN 自動化では、VLAN 1 のシードデバイスで IP アドレスを設定します。シードデバイスのこの VLAN 1 IP アドレスが Cisco DNA Center から到達できない場合は、[LAN Automation Status] ウィンドウにエラーメッセージが表示されます。エラーの詳細および可能な修復アクションを表示するには、このウィンドウの [See Details] リンクにマウスカーソルを合わせます。

ステップ 3 プロビジョニングしているデバイスの進行状況をモニターして確認します。

a) **[Actions]** > **[Provision]** > **[LAN Automation Status]** の順に選択します。

[LAN Automation Status] ウィンドウに、デバイスのプロビジョニングの進捗状況が表示されます。

（注） 新しいデバイスのプロビジョニングには数分かかる場合があります。

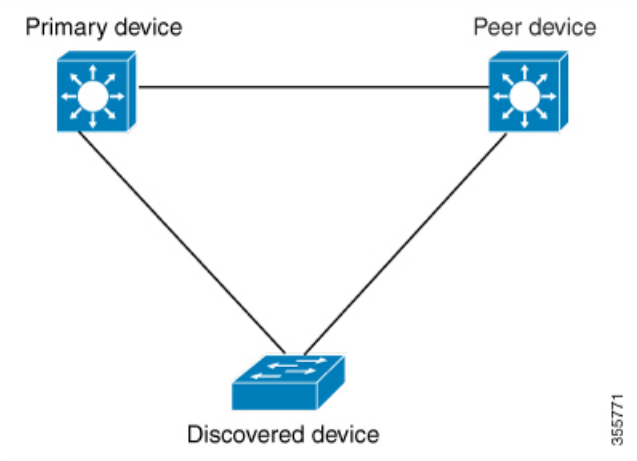
b) すべてのデバイスが検出されてインベントリに追加され、管理状態になったら、[LAN Automation Status] ウィンドウで [Stop] をクリックします。

LAN 自動化プロセスが完了し、新規デバイスがインベントリに追加されます。

LAN 自動化のピアデバイスの使用事例

デュアル ホームのスイッチのプロビジョニング

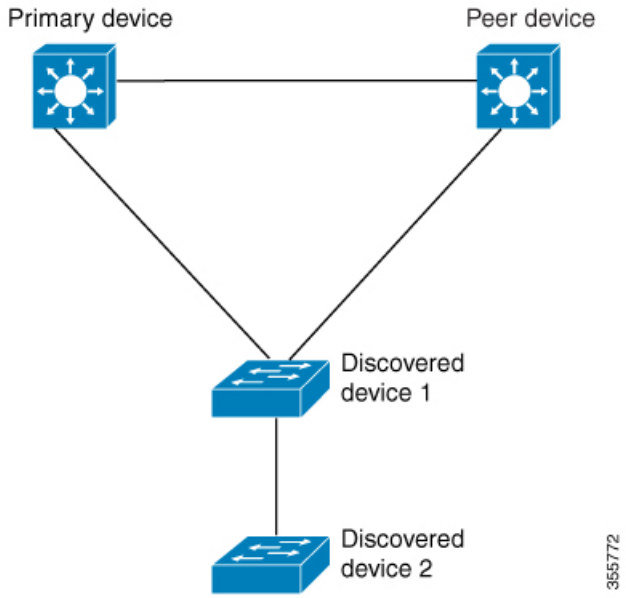
デュアル ホームのスイッチのプロビジョニングのために、常にピア デバイスを選択する必要があります。



Cisco DNA Center プライマリ デバイスで DHCP サーバーを設定します。Cisco DNA Center が検出されたデバイスがプライマリ デバイスとピア デバイスの両方に接続されていることを理解しているため、LAN 自動化タスクが停止されると、2 つのレイヤー 3 ポイントツーポイント接続を設定します。1 つの接続は、検出されたデバイスとプライマリ デバイスの間で確立されます。もう 1 つの接続は検出されたデバイスとピア デバイスの間で確立されます。

（注） LAN 自動化ジョブが実行される前に、プライマリ デバイスとピア デバイスの間のリンクが設定される場合、ピア デバイスを Cisco DNA Center のLAN 自動化設定の一部としてピア デバイスに接続するプライマリ デバイスのインターフェイスを選択する必要があります。

LAN 自動化の 2 段階制限



前述のトポロジの場合、Cisco DNA Center は次のリンクを設定します。

- ポイントツーポイントのレイヤ 3 は 検出されたデバイス *1* から プライマリ デバイス に接続するためにルートする
- ポイントツーポイントのレイヤ 3 は 検出されたデバイス *1* から ピア デバイス に接続するためにルートする
- ポイントツーポイントのレイヤ 3 は 検出されたデバイス *1* から 検出されたデバイス *2* に接続するためにルートする

検出されたデバイス *3*という名前のデバイスが以下の検出されたデバイス *2*に直接接続されるシナリオを考えてください。検出されたデバイス *2* と 検出されたデバイス *3*の間の接続は、LAN 自動化ジョブの一部として設定されません。プライマリ デバイスから 2 段階以上離れているためです。

LAN 自動化の状態を確認

実行中の LAN 自動化ジョブのステータスを確認できます。

始める前に

LAN 自動化ジョブを作成し、開始する必要があります。

ステップ 1 メニューアイコン（☰）をクリックして、**[Provision]** > **[Inventory]** の順に選択します。

すべての検出されたデバイスが表示されます。

ステップ 2 **[Actions]** > **[Provision]** > **[LAN Automation Status]** の順に選択します。

[LAN Automation Status] ウィンドウに、実行中と完了のすべての LAN 自動化ジョブのステータスが表示されます。

第 21 章

ファブリックネットワークのプロビジョニング

ファブリックネットワークについて

ファブリックネットワークは、1 つまたは複数の場所で単一のエンティティとして管理されるデバイスの論理グループです。ファブリックネットワークを使用すると、仮想ネットワークやユーザーおよびデバイスグループの作成、高度なレポート作成などが可能になります。その他の機能には、アプリケーション認識、トラフィック分析、トラフィックの優先順位付け、最適なパフォーマンスと運用効率のためのステアリングのインテリジェントサービスがあります。

Cisco DNA Center では、デバイスをファブリックネットワークに追加できます。これらのデバイスは、ファブリックネットワーク内のコントロールプレーン、ボーダーデバイスまたはエッジデバイスとして機能するように設定できます。

ファブリックサイト

ファブリックサイトは、コントロールプレーン、ボーダー、エッジ、ワイヤレスコントローラ、ISE PSN のネットワークデバイスの固有のセットを持つ独立したファブリック領域です。異なるレベルの冗長性とスケールは、DHCP、AAA、DNS、インターネットなどのローカルリソースを含むことにより、サイトごとに設計することができます。

ファブリックサイトは、単一の物理的ロケーション、複数のロケーション、またはロケーションのサブセットのみをカバーすることができます。

- 単一の場所: ブランチ、キャンパスまたはメトロ キャンパス
- 複数の場所: メトロ キャンパス + 複数ブランチ
- ロケーションのサブセット: キャンパス内での構築または領域

Software-Defined Access ファブリックネットワークは、複数のサイトで構成されることがあります。各サイトは、優れた拡張性、復元力、生存性、およびモビリティを備えます。ファブリックサイトの全体的な集約は、多数のエンドポイントに対応し、モジュール方式で（または水平方向に）拡張します。複数のファブリックサイトは、トランジットサイトを使用して相互接続されます。

トランジットサイト

トランジットサイトとは、2 つ以上のファブリックサイトを相互接続したり、ファブリックサイトと外部ネットワーク（インターネット、データセンターなど）を接続するサイトです。トランジットネットワークには 2 つのタイプがあります。

- IP トランジット：通常の IP ネットワークを使用して、外部ネットワークに接続するか 2 つ以上のファブリックサイトを接続します。IP トランジットは、従来型の IP ベース（VRF-LITE、MPLS）ネットワークを利用します。これには、サイト間での VRF と SGT の再マッピングが必要です。
- SD-Access トランジット：LISP/VxLAN のカプセル化を使用して 2 つのファブリックサイトを接続します。SD-Access トランジットエリアは、独自のコントロールプレーンノードを持つがエッジノードやボーダーノードはないファブリックの一部として定義できます。ただし、外部ボーダーを持つファブリックを使用することもできます。SD-Access トランジットを使用すると、エンドツーエンドポリシープレーンは SGT グループタグを使用して維持されます。

ファブリックの準備状況とコンプライアンスのチェック

ファブリックの準備状況チェック

ファブリックの準備状況チェックは、デバイスがファブリックに追加される準備が整っていることを確認するために、デバイス上で実行される事前プロビジョニングチェックのセットです。ファブリックの準備状況チェックは、デバイスのプロビジョニング時に自動的に実行されるようになりました。インターフェイス VLAN とマルチ VRF の設定チェックは、ファブリックの準備状況チェックの一環としては行われません。

ファブリックの準備状況チェックには、次の項目が含まれます。

- 接続チェック：エッジノードからマップサーバーへの接続、エッジノードからボーダーへの接続など、デバイス間で必要な接続を確認します。
- 既存の設定チェック：SD-Access を介してプッシュされる設定と競合する設定がデバイスにあり、それが後でエラーになる可能性がないかを確認します。
- ハードウェアバージョン：デバイスのハードウェアバージョンがサポートされているかどうかを確認します。
- イメージタイプ：サポートされているイメージタイプ（IOS XE、IOS、NXOS、Cisco Controller）を使用してデバイスが実行されているかどうかを確認します。
- ループバック インターフェイス：デバイス上のループバック インターフェイスの設定を確認します。SDA アプリケーションを使用するには、デバイスにループバック インターフェイスが設定されている必要があります。
- ソフトウェアライセンス：デバイスが適切なソフトウェアライセンスを使用して実行されているかどうかを確認します。
- ソフトウェアバージョン：デバイスが適切なソフトウェアイメージを使用して実行されているかどうかを確認します。

サポートされているソフトウェアバージョンの詳細については、「Cisco SD-Access Hardware and Software Compatibility Matrix」を参照してください。

ファブリックの準備状況チェックの実行中にエラーが検出された場合、エラー通知が [topology] エリアに表示されます。問題を修正し、デバイスのプロビジョニング ワークフローを続行できます。

ファブリック コンプライアンス チェック

ファブリック コンプライアンスとは、ファブリック プロビジョニング中に設定されたユーザー インテントに従って動作するデバイスの状態です。ファブリック コンプライアンス チェックは、次の条件に基づいてトリガーされます。

- 有線デバイスの場合は 24 時間ごと、ワイヤレスデバイスの場合は 6 時間ごと。
- 有線デバイスで設定が変更された場合。

  有線デバイスの設定変更によって SNMP トラップがトリガーされ、それによってコンプライアンスチェックがトリガーされます。Cisco DNA Center サーバーが SNMP サーバーとして設定されていることを確認します。

次のコンプライアンスチェックを実行し、デバイスがファブリックに準拠していることを確認します。

- 仮想ネットワーク：Cisco DNA Center 上の仮想ネットワークのユーザーインテントの現在の状態に準拠するように、必要な VRF がデバイスに設定されているかどうかを確認します。
- ファブリックロール：デバイスの設定が Cisco DNA Center のファブリックロールのユーザーインテントに準拠しているかどうかを確認します。
- セグメント：セグメントの VLAN 設定と SVI 設定を確認します。
- ポートの割り当て：VLAN および認証プロファイルのインターフェイス設定を確認します。

SD-Access の新しい自動化

強化された Cisco SD-Access ユーザーインターフェイス（UX）では、シンプルさ、柔軟性、豊富で直感的なコンテキストが統合されています。Cisco SD-Access UX のベータ版は、ユーザーエクスペリエンスを強化し、次の機能を提供します。

- 仮想ネットワークやファブリックサイトなどのファブリック要素間の関連付けの明確化
- 強化されたワークフロー
- ファブリック要素とその属性の簡潔なビュー

拡張 Cisco SD-Access UX は、次のもので構成されています。

- 仮想ネットワーク、ファブリックサイト、およびトランジットネットワークごとの概要ページ
- [Virtual Networks] の概要ビューには、次の 4 つのセクションがあります。
  - 最初のセクションには、さまざまな段階のタスクの数、レイヤ 3 仮想ネットワークとエニーキャストゲートウェイの数、エニーキャストゲートウェイ、レイヤ 2 仮想ネットワークとそれらの VLAN の数が表示されます。
  - 2 番目のセクションには、仮想ネットワークタスクがグラフィカルに表示されます。
  - 3 番目のセクションには、保存されたヒントのリストが表示されます。
  - 最後のセクションには、提供されるさまざまなワークフローのカードベースのビューが表示されます。
- [Fabric Sites] ページには、[Summary] ビュー、[Map] ビュー、および [Table] ビューの 3 つのビューがあります。

[Summary] ビューには、ヒントとインサイト、および進行中のワークフローが表示されます。また、ファブリックサイト、ファブリックゾーン、ファブリックデバイス、コントロールプレーン、およびボーダーノードの数の概要も提供します。

- [Transits] ページには、SD-Access トランジット、SDWAN トランジット、および IP ベースのトランジットの数の概要が表示されます。このページには、トランジットネットワークを作成するオプションもあります。

Cisco DNA Center メニューバーの [Preview New SD-Access] トグルボタンを使用して、古い Cisco SD-Access UX と拡張 Cisco SD-Access UX を切り替えます。

（注） この章で説明するすべてのタスクは、拡張 Cisco SD-Access UX に関連しています。

ファブリックサイトの追加

始める前に

IP デバイストラッキング（IPDT）がすでにサイトに設定されている場合にのみ、ファブリックサイトを作成できます。

ステップ 1 メニューアイコン（≡）をクリックして、 **[Provision]** > **[Fabric Sites]**.

ステップ 2 [SUMMARY] で、ファブリックサイトの数を示す数字をクリックします。

ステップ 3 [Create Fabric Sites and Fabric Zones] をクリックします。

または、最初の 3 つの手順の代わりに、メニューアイコン（≡）をクリックして、 **[Workflow]** > **[Create Fabric Sites]**の順に選択します。

ステップ 4 [Create Fabric Sites and Fabric Zones] ウィンドウで、[Let's Do it] をクリックして、ワークフローに直接移動します。

ステップ 5 [Fabric Site Location] ウィンドウで、ファブリックゾーンとして追加するエリア、建物、またはフロアを選択します。

ステップ 6 [Wired Endpoint Data Collection] ウィンドウで、[Monitor wired clients] チェックボックスがオンになっていることを確認します。

ステップ 7 [Authentication Template] ウィンドウで、次の手順を実行します。

a) ファブリックサイトの認証テンプレートを選択します。

- [Closed Authentication]：認証前のすべてのトラフィック（DHCP、DNS、ARP など）が廃棄されます。
- **オープン認証（Open Authentication）**：ホストには、802.1X 認証を受ける必要なくネットワーク アクセスが許可されます。

- [Low Impact]：スイッチポートに ACL を適用することでセキュリティを追加して、認証前に非常に制限されたネットワークアクセスを許可します。ホストが正常に認証されると、追加のネットワーク アクセスが許可されます。
- **None**

b) （オプション）[Closed Authentication]、[Open Authentication]、または [Low Impact] を選択した場合は、[Edit] をクリックして認証設定を編集します。

- [First Authentication Method]：[802.1x] または [MAC Authentication Bypass (MAB)] を選択します
- [802.1x Timeout (in seconds)]：スライダを使用して、802.1x タイムアウトを秒単位で指定します。
- [Wake on LAN]：[Yes] または [No] を選択します。
- [Number of Hosts]：[Unlimited] または [Single] を選択します。
- [BPDU Guard]：このチェックボックスを使用して、すべての [Closed Authentication] ポートでブリッジ プロトコル データ ユニット（BPDU）ガードを有効または無効にします。
- [Pre-Authentication Access Control List]：トグルボタンを有効にして、[Low Impact] 認証の事前認証制御を構成します。[Implicit Action] ドロップダウンリストから、暗黙的なアクションを選択します。ルールの説明を入力します。アクセスコントラクトを追加するには、[Add Contract Action] をクリックし、ルールを選択して、[Apply Table] をクリックします。

ステップ 8 [Fabric Zones] ウィンドウで、次のいずれかのオプションを選択します。

- ファブリックゾーンを指定し、範囲指定されたサブネットを作成するには、[Setup Fabric Zones Now] をクリックし、表示されたネットワーク階層からファブリックサイトを選択します。
- 後でファブリックゾーンを指定するには、[Setup Fabric Zones Later] をクリックします。

ステップ 9 [Summary] ウィンドウで、ファブリックサイトの設定を確認します。

ここでファブリックサイトまたはゾーン設定を編集できます。

ステップ 10 [Deploy] をクリックします。

サイトとゾーンがプロビジョニングされるまでに数秒かかります。サイトの作成が成功すると、「Success!Your fabric site is created」というメッセージが表示されます。

ファブリックサイトのデバイスの構成

次のタブを使用して、ファブリックサイトのデバイスを構成できます。

- [Fabric Infrastructure] タブ：デバイスをファブリックロールに割り当てます。
- [Authentication Template] タブ：ファブリック用の認証テンプレートを選択します。認証テンプレートは、Cisco ISE から取得される一連の定義済みの設定です。

- [Wireless SSIDs] タブ：ホストがアクセスできるネットワーク内のワイヤレス SSID を指定します。ゲスト SSID またはエンタープライズ SSID を選択してアドレス プールを割り当て、[保存（Save）] をクリックできます。
- [Port Assignment] タブ：ファブリックサイトに接続するデバイスのタイプに応じて、各ポートに固有の設定を適用します。これを行うには、固有の割り当てが必要なポートを選択し、[Assign] をクリックして、ドロップダウンリストからポートタイプを選択します。

  次の制約事項に注意してください。

  - Cisco SD-Access 展開環境では、AP、拡張ノード、およびユーザーデバイス（単一のコンピュータまたは単一のコンピュータと電話機など）と、トランクポートを必要とするデバイス（単一サーバーなど）のみがサポートされます。
  - 内部スイッチまたは仮想スイッチを備えたサーバーはサポートされていません。
  - その他のネットワーキング機器（ハブ、ルータ、スイッチなど）はサポートされていません。

ファブリックへのデバイスの追加

ファブリックサイトを作成すると、そのファブリックサイトにデバイスを追加できます。デバイスがコントロールプレーンノード、エッジノード、またはボーダーノードとして機能する必要があるかどうかも指定できます。

IP デバイストラッキング（IPDT）がファブリックサイトに設定されている場合にのみ、新しいデバイスをファブリックサイトに追加できます。

アクセスロールが割り当てられ、サイトで IPDT を有効にする前にプロビジョニングされたデバイスは、ファブリックに追加できません。このようなデバイスは、ファブリックサイトに追加する前に再プロビジョニングしてください。プロビジョニング ワークフローを調べて、デバイスでの [Deployment of IPDT] のステータスを確認します。

（注）

- ファブリックサイト内のデバイスをコントロールプレーンノードまたはボーダーノードとして指定する手順はオプションです。それらのロールがないデバイスもあります。ただし、各ファブリックサイトには、少なくとも 1 つのコントロール プレーン ノード デバイスと 1 つのボーダーノードデバイスが存在する必要があります。有線ファブリックの現在のリリースでは、冗長性を確保するために最大 6 つのコントロール プレーン ノードを追加できます。
- 現在、シスコ ワイヤレス コントローラは 2 つのコントロールプレーンノードとのみ通信します。

始める前に

デバイスをプロビジョニングします（まだプロビジョニングしていない場合）。

- **[Provision]** > **[Network Devices]** > **[Inventory]** ウィンドウに、検出されたデバイスが表示されます。
- ファブリックの準備状況チェックに合格し、プロビジョニングする準備が整ったら、トポロジビューにデバイスがグレー色で表示されます。
- ファブリックの準備状況チェックの実行中にエラーが検出された場合、エラー通知が [topology] エリアに表示されます。[See more details] をクリックして、結果のウィンドウに一覧表示された問題のあるエリアを確認します。問題を修正し、[Re-check] をクリックして問題が解決されていることを確認します。
- 問題解決の一環としてデバイスの設定を更新する場合は、デバイスで**[Inventory]** > **[Resync]** を実行して、デバイス情報を再同期してください。

（注） ファブリックの準備状況チェックに失敗しても、デバイスのプロビジョニングを続行できます。

ステップ 1 メニューアイコン（☰）をクリックして、 **[Provision]** > **[Fabric Sites]**.

ステップ 2 [SUMMARY] で、ファブリックサイトの数を示す数字をクリックします。

ステップ 3 デバイスを追加するファブリックサイトを選択します。

インベントリされたネットワーク内のすべてのデバイスが結果のトポロジビューに表示されます。トポロジ表示では、ファブリックに追加されるすべてのデバイスは青です。

ステップ 4 [Fabric Infrastructure] タブの [List] ビューで、デバイスをクリックします。スライドインペインには、次の [Fabric] オプションが表示されます。

オプション	説明
エッジノード	選択したデバイスをエッジノードとして有効にするには、このオプションの横にあるボタンをトグルします。
ボーダー ノード	選択したデバイスをボーダーノードとして有効にするには、このオプションの横にあるボタンをトグルします。
コントロール プレーン ノード	選択したデバイスをコントロールプレーンノードとして有効にするには、このオプションの横にあるボタンをトグルします。

デバイスをファブリックインアボックスとして設定するには、[Control Plane Node]、[Border Node]、および [Edge Node] オプションを選択します。

デバイスをコントロールプレーンおよびボーダーノードとして設定するには、[Control Plane Node] と [Border Node] の両方を選択します。

ステップ 5 [Add] をクリックします。

次のタスク

デバイスがファブリックに追加されると、ファブリック コンプライアンス チェックが自動的に実行され、デバイスがファブリックに準拠していることが確認されます。トポロジには、ファブリック コンプライアンス チェックに失敗したデバイスが青色で、横に十字マークが付いた状態で表示されます。エラー通知の [詳細の表示（See more details）] をクリックして問題領域を特定し、修正します。

ボーダーノードとしてのデバイスの追加

ファブリックにデバイスを追加する場合、ファブリックへのデバイスの追加（513 ページ）で説明したように、コントロールプレーン、ボーダーノード、またはエッジノードとして動作するようにさまざまな組み合わせで追加できます。

ボーダーノードとしてデバイスを追加するには、次の手順を実行します。

ステップ 1 メニューアイコン（☰）をクリックして、**[Provision]** > **[Fabric Sites]**。

ステップ 2 [Fabric Sites] タブ の [SUMMARY] で、ファブリックサイトの数を示す数字をクリックします。

ステップ 3 ボーダーノードを設定するファブリックサイトを選択します。
インベントリされたネットワーク内のすべてのデバイスが結果のトポロジビューに表示されます。トポロジ表示では、ファブリックに追加されるすべてのデバイスは青です。

ステップ 4 [Fabric Infrastructure] タブの [List] ビューで、デバイスをクリックします。

ステップ 5 スライドインペインで、[Border Node] トグルボタンを有効にします。

ステップ 6 表示されたスライドインペインで、[Layer 3 Handoff] タブをクリックします。

ステップ 7 [Enable Layer-3 Handoff] チェックボックスを選択します。

ステップ 8 デバイスの [ローカル自律番号（Local Autonomous Number）] を入力します。

ローカル自律番号がデバイスですでに設定されている場合は、その番号が表示され、このフィールドは無効になります。デバイスですでに設定されているローカル自律番号を変更することはできません。

ステップ 9 ボーダーノードの優先度を設定するには、[Modify Border Priority] チェックボックスをオンにして、優先度の値を入力します。

優先度の範囲は、1 ～ 10 です。値が小さいほど、ボーダーの優先度が高くなります。（1 は最高の優先度を示します。10 は最も低い優先度を示します）デフォルトでは、ボーダーの優先度の値は 10 に設定されています。

ネットワークに 2 つ以上のボーダーが設定されている場合、トラフィックは優先度の高いボーダーを介してルーティングされます。優先順位が設定されていない場合、トラフィックはボーダーノード間で負荷分散されます。

ステップ 10 デフォルトでは、ボーダーは外部ボーダーとして指定され、外部ルートをインポートせずに、すべての不明なトラフィックへのゲートウェイとして機能します。ボーダーを内部ボーダーとして設定すると、既知のトラフィックへのゲートウェイとして、特定の外部ルートをインポートするように設定できます。ボーダーには、内部ボーダーおよび外部ボーダーを組み合わせたロールを設定することもできます。

- ボーダーを外部ボーダーとして指定し、不明なネットワークへの接続を提供するには、[Default to all Virtual Networks] および [Do not Import External Routes] の両方のチェックボックスをオンにします。
- ボーダーを内部ボーダーとして指定し、特定のネットワークアドレスのゲートウェイとして動作させるには、[Default to all virtual networks] および [Do not import external routes] の両方のチェックボックスをオフにします。
- このボーダーノードを内部および外部ボーダーとして指定するには、[Default to all virtual networks] チェックボックスをオンにします。これは、エッジノードから送信されたすべての既知のトラフィックおよび不明なトラフィックへのゲートウェイとして機能します（[Do not import external routes] チェックボックスはオンにしないでください）。

ステップ 11 [Add Transit Site] にカーソルを合わせ、ボーダーデバイスで有効にするトランジットネットワークを選択します。

a) [IP:BGP IP TRANSIT] の場合、IP インターフェイスを構成します。

- [Add External Interface] をクリックします。
- 表示されるウィンドウで、次の手順を実行します。

1. [External Interface] を選択します。
2. [Remote AS Number] は、選択したトランジットまたはピアネットワークから自動的に導出されます。
3. [Interface Description] に説明を入力します。
4. （オプション）[Actions] ドロップダウンリストにカーソルを合わせて、[Enable All] または [Disable All] を選択します。
5. 目的の仮想ネットワークの [Enable Layer-3 Handoff] ボタンを切り替えます。この仮想ネットワークは、ボーダーによってリモートピアにアドバタイズされます。1 つ、複数、またはすべての仮想ネットワークを選択できます。
6. 選択した仮想ネットワークの VLAN ID を入力します。
7. **[Save]** をクリックします。

- [Select IP Pool] ドロップダウンリストから、IP プールを選択します。選択したプールは、ボーダーノードと IP ピア間で IP ルーティングを自動化するために使用されます。

ステップ 12 （オプション）ファブリックネットワークに非ファブリックネットワークを接続している場合、または従来のネットワークから SDA ネットワークに移行する場合にのみ、この手順を実行します。[Layer 2 Handoff] タブをクリックします。

仮想ネットワークのリストと、各仮想ネットワークの IP プールの数が表示されます。

a) ハンドオフする仮想ネットワークをクリックします。

仮想ネットワークに存在する IP アドレスプールのリストと、ファブリック以外のデバイスを接続できるインターフェイスのリストが表示されます。

b) [External Interface] を選択してください。
c) [Interface Description] に説明を入力します。
d) ファブリックを拡張する必要がある [External VLAN] 番号を入力します。

Cisco DNA Center 2.1.2.6 より前のリリースでは、仮想ネットワークは 1 つのインターフェイスでのみハンドオフできます。複数のインターフェイス経由で同じ仮想ネットワークを処理することはできません。

Cisco DNA Center リリース 2.1.2.6 以降のリリースでは、仮想ネットワークは単一のインターフェイスまたは複数のインターフェイスでハンドオフできます。セグメントのレイヤ 2 ハンドオフを 2 つの異なるデバイスで実行することもできます。いずれの場合も、ネットワークにループが形成されていないことを確認します。

e) **[Save]** をクリックします。

ステップ 13 [Add] をクリックします。

LISP Pub/Sub の設定

最初のコントロールプレーンをファブリックに追加する場合にのみ、ファブリックサイトで LISP Pub/Sub を設定できます。

始める前に

ファブリックデバイスが Cisco IOS XE リリース 17.6.1 以降で動作することを確認します。

ステップ 1 メニューアイコン（☰）をクリックして、 **[Provision]** > **[Fabric Sites]**.

ステップ 2 [SUMMARY] で、ファブリックサイトの数を示す数字をクリックします。

ステップ 3 デバイスを追加するファブリックサイトを選択します。

インベントリされたネットワーク内のすべてのデバイスが結果のトポロジビューに表示されます。トポロジ表示では、ファブリックに追加されるすべてのデバイスは青です。

ステップ 4 [Fabric Infrastructure] タブの [List] ビューで、コントロールプレーンとして設定するデバイスをクリックします。

ステップ 5 スライドインペインで、[Control Plane Node] トグルボタンを有効にして、このプレーンを設定します。

ステップ 6 [Configure Control Plane] スライドインペインで、[LISP PubSub] ルート配布プロトコルを選択し、[Add] をクリックします。

ステップ 7 [Add]をクリックします。

ステップ 8 [展開（Deploy）] をクリックします。

ステップ 9 [Modify Fabric] ウィンドウで、操作をスケジュールし、[Apply] をクリックします。

ファブリックサイトの LISP Pub/Sub の設定を確認するには、[SITE SUMMARY] ウィンドウで LISP Pub/Sub のステータスを確認します。

IP のトランジット ネットワークの作成

ステップ 1 メニューアイコン（☰）をクリックして、 **[Provision]** > **[Transits]**.

ステップ 2 [Create Transit] をクリックします。

ステップ 3 [Transit] スライドインペインで、トランジットネットワークの名前を入力します。

ステップ 4 [IP-Based] を選択します。
ルーティング プロトコルが BGP にデフォルトとして設定されます。

ステップ 5 トランジットネットワークの自律システム番号（ASN）を入力します。

ステップ 6 [Save] をクリックします。

SD-Access トランジットネットワークの作成

SD-Access トランジットネットワークを追加するには、次の手順に従います。

ステップ 1 メニューアイコン（☰）をクリックして、 **[Provision]** > **[Transits]**.

ステップ 2 [Create Transit] をクリックします。

ステップ 3 [Transit] スライドインペインで、トランジットネットワークの名前を入力します。

ステップ 4 SD-Access の [Transit Type] を選択します。

LISP Pub/Sub コントロールプレーンのないファブリックサイトのトランジットを設定する場合は、[SD-Access (LISP/BGP)] を選択してください。

LISP Pub/Sub コントロールプレーンのあるファブリックサイトのトランジットを設定する場合は、[SD-Access (LISP PubSub)] を選択してください。

[SD-Access (LISP PubSub)] トランジットを他の Cisco DNA Center クラスタと共有する場合は、[Yes, Share] を選択してください。共有しない場合は、[No, keep it local] を選択してください。

（注） [Yes, Share] オプションは、**複数の Cisco DNA Center** パッケージがすべての Cisco DNA Center クラスタにインストールされている場合にのみ表示されます。

ステップ 5 ドロップダウンリストから [Transit Control Plane Node Site] を選択します。少なくとも 1 つのトランジット マップ サーバーを選択します。

ステップ 6 ドロップダウンリストからトランジットネットワークの [Transit Control Plane Node] を選択します。

ステップ 7 （オプション）追加のマップサーバーを構成するには、プラスアイコン（⊕）をクリックし、ステップ 5（518 ページ）とステップ 6（519 ページ）を繰り返します。

ステップ 8 [Save] をクリックします。

トランジットネットワークを作成すると、[Transits] ウィンドウに、新しく作成されたトランジットとその属性が表示されます。

（注） LISP/BGP コントロールプレーンを使用するファブリックサイトに [SD-Access (LISP PubSub)] トランジットを追加することはできません。LISP Pub/Sub コントロールプレーンを使用するファブリックサイトに [SD-Access (LISP/BGP)] トランジットを追加することはできません。

次のタスク

ファブリックサイトを SD-Access トランジットと相互接続するには、トランジットをボーダーノードに追加します。

認証テンプレートの選択

ファブリックサイト内のすべてのデバイスに適用される認証テンプレートを設定できます。

ステップ 1 メニューアイコン（≡）をクリックして、 **[Provision]** > **[Fabric Sites]**.

ステップ 2 [SUMMARY] で、ファブリックサイトの数を示す数字をクリックします。

ステップ 3 ファブリックサイトを選択します。

ステップ 4 [Authentication Template] タブをクリックします。

ステップ 5 [Select Authentication Template] で、サイトの認証テンプレートを選択します。

- **オープン認証（Open Authentication）**：ホストには、802.1X 認証を受ける必要なくネットワーク アクセスが許可されます。
- **クローズ認証（Closed Authentication）**：認証前のすべてのトラフィック（DHCP、DNS、ARP を含む）は廃棄されます。
- [Low Impact]：スイッチポートに ACL を適用することでセキュリティを追加して、認証前に制限されたネットワークアクセスを許可します。ホストが正常に認証されると、追加のネットワーク アクセスが許可されます。
- **None**

選択した認証テンプレートの設定を編集して、サイト固有の認証要件に対応することができます。

サイトレベルの認証を変更する前に、マクロまたは Autoconf を使用してアクセスポイントがオンボーディングされ、かつまだ定期的な再同期が行われていないファブリックデバイスがあれば再同期する必要があります。

ステップ 6 （オプション）選択した認証方式の設定を編集するには、[Edit] をクリックします。

a) スライドインペインで、次の手順を実行します。

- [First Authentication Method]：[802.1x] または [MAC Authentication Bypass (MAB)] を選択します
- [802.1x Timeout (in seconds)]：スライダを使用して、802.1x タイムアウトを秒単位で指定します。
- [Wake on LAN]：[Yes] または [No] を選択します。
- [Number of Hosts]：[Unlimited] または [Single] を選択します。

（注） [Number of Hosts] は、1 つのポートに接続できるデータホストの数を指定します。[Single] の場合、ポートでは 1 つのデータクライアントのみを保持できます。[Unlimited] の場合、ポートで複数のデータクライアントと 1 つの音声クライアントを保持できます。

- [Pre-Authentication Access Control List]：トグルボタンを有効にして、[Low Impact] 認証の事前認証制御を構成します。[Implicit Action] ドロップダウンリストから、暗黙的なアクションを選択します。ルールの説明を入力します。アクセスコントラクトを追加するには、[Add Contract Action] をクリックし、ルールを選択して、[Apply Table] をクリックします。

b) **[Save]** をクリックします。

保存された変更は、認証テンプレートが編集されているサイトにのみ適用されます。

ステップ 7 [展開（Deploy）] をクリックします。
ヒットレス認証変更機能を使用すると、ファブリックからデバイスを削除することなく、1 つの認証方式から別の認証方式に切り替えることができます。

ファブリックサイト内のポートの設定

[Port Assignment] タブで、ファブリックサイトの各アクセスデバイスを設定できます。デバイスの各ポートのネットワーク動作設定を指定できます。

ステップ 1 メニューアイコン（≡）をクリックして、 **[Provision]** > **[Fabric Sites]**.
ステップ 2 [SUMMARY] で、ファブリックサイトの数を示す数字をクリックします。
ステップ 3 ファブリックサイトを選択します。
ステップ 4 [Port Assignment] タブをクリックします。
ステップ 5 ファブリックデバイスのリストから、構成するデバイスのドロップダウンを展開します。
デバイスで利用可能なポートが表示されます。
ステップ 6 デバイスのポートのチェックボックスをオンにします。
ステップ 7 [Configure] にカーソルを合わせ、[Assign Ports] を選択します。
ステップ 8 slide-in pane で、ドロップダウンリストの次のオプションから [Connected Device Type] を選択します。

オプション	説明
[User Devices (ip-phone, computer, laptop)]	ホストデバイスに接続するポートを設定します。

オプション	説明
アクセス ポイント（AP）	アクセスポイントに接続するポートを設定します。
トランク	ポートをトランク ポートとして設定します。
サプリカントベースの拡張ノード	サプリカントベースの拡張ノードを受信するようにポートを設定します。

- ホストデバイスを接続するには、[User Devices (ip-phone, computer, laptop)] を選択し、次の手順を実行します。
  1. [VLAN Name (Data)] ドロップダウンリストからデータの VLAN 名を選択します。
  2. [Security Group] ドロップダウンリストからセキュリティグループを選択します。

     セキュリティグループは、[None] 認証テンプレートでのみサポートされます。
  3. [VLAN Name (Voice)] ドロップダウンリストから音声の VLAN 名を選択します。
  4. [Authentication Template] ドロップダウンリストから認証タイプを選択します。
  5. コネクテッドデバイスに関する [Description] を入力します。
- アクセスポイントを接続するには、[Access Point (AP)] を選択し、次の手順を実行します。
  1. [VLAN Name (Data)] ドロップダウンリストから VLAN 名を選択します。
  2. [Authentication Template] ドロップダウンリストから認証タイプを選択します。
  3. コネクテッドデバイスに関する [Description] を入力します。
- サプリカントベースの拡張ノードデバイスを接続するには、[Supplicant-Based Extended Node] を選択します。
- トランクポートを接続するには、[Trunk] を選択し、ポートの説明を [Description] に入力します。

ステップ 9 [更新（Update）] をクリックします。

ファブリックネットワークのワイヤレス SSID の設定

始める前に

ワイヤレスデバイスをファブリックサイトに追加してください。

ステップ 1 メニューアイコン（☰）をクリックして、 **[Provision]** > **[Fabric Sites]**.

ステップ 2 [SUMMARY] で、ファブリックサイトの数を示す数字をクリックします。

ステップ 3 ファブリックサイトを選択します。

ステップ 4 [Wireless SSID] タブをクリックし、ホストがアクセス可能なネットワーク内のワイヤレス SSID を指定します。

ステップ 5 [Choose Pool] をクリックし、SSID の IP プール予約を選択します。

ステップ 6 [Assign SGT] ドロップダウンリストから、SSID のセキュリティグループを選択します。

ステップ 7 SSID でワイヤレスマルチキャストを有効にするには、[Enable Wireless Multicast] チェックボックスをオンにします。

仮想ネットワーク

仮想ネットワークは、共通物理ネットワークインフラストラクチャ内でトラフィックをセグメント化するために使用されるオーバーレイです。これは「マクロセグメンテーション」とも呼ばれます。レイヤ 2 仮想ネットワークはスイッチドトラフィックをセグメント化し、レイヤ 3 仮想ネットワークはルーテッドトラフィックをセグメント化します。Cisco SD-Access ファブリックに接続されている各エンドポイントは、静的エッジポート設定または Identity Service Engine からの動的ポリシーに基づいて、特定の仮想ネットワークに割り当てられます。仮想ネットワークのエンドポイントは、マイクロセグメンテーションポリシーによって明示的にブロックされていないかぎり、相互に通信できます。異なる仮想ネットワークにまたがるエンドポイントは、デフォルトでは、相互に通信できません。仮想ネットワーク間トラフィックの場合は、接続ポリシーを Cisco SD-Access ファブリックの外部（フュージョンデバイス上など）で実装する必要があります。

仮想ネットワークの一般的な使用例は、社内エンドポイントとビルディング管理システムの両方を含むオフィスビルです。社内エンドポイントは、照明、暖房、換気、空調などのビルディングシステムとは別にセグメント化する必要があります。この場合、ネットワーク管理者は、2 つ以上の仮想ネットワークを使用して社内エンドポイントとビルディングシステムをマクロセグメント化することにより、ビルディングシステムと社内エンドポイントの間の不正アクセスをブロックすることができます。

レイヤ 3 仮想ネットワークは、複数のファブリックサイトやネットワークドメイン（ワイヤレス LAN、キャンパス LAN、および WAN）にまたがる場合があります。レイヤ 2 仮想ネットワークは、単一のファブリックサイト内に存在します。

レイヤ 3 仮想ネットワークの作成

ステップ 1 メニューアイコン（☰）をクリックして、**[Workflows]** > **[Create Layer 3 Virtual Networks]** の順に選択します。

または、**[Provision]** > **[Virtual Networks]** で [Layer 3] タブに移動し、[Create Layer 3 Virtual Networks] をクリックすることもできます。

ステップ 2 タスクの概要ウィンドウが開いたら、[Let's Do it] をクリックして、ワークフローに直接移動します。

ステップ 3 [Choose your creation process] ウィンドウで、作成するレイヤ 3 仮想ネットワークの数を入力します。

ステップ 4 [Create your Layer 3 virtual networks] ウィンドウで、レイヤ 3 仮想ネットワークの名前を入力します。

ステップ 5 [Select your Fabric Sites] ウィンドウで、次のいずれかをクリックします。

- [By Layer 3 Virtual Network] タブ：レイヤ 3 仮想ネットワークを複数のファブリックサイトに関連付けるには、対応するドロップダウンリストからレイヤ 3 仮想ネットワークとファブリックサイトを選択します。仮想ネットワークは複数のファブリックサイトに割り当てることができます。作成したすべてのレイヤ 3 仮想ネットワークについて、この関連付けを繰り返します。
- [By Fabric Site] タブ：複数のレイヤ 3 仮想ネットワークをファブリックサイトに割り当てるには、対応するドロップダウンリストからファブリックサイトとレイヤ 3 仮想ネットワークを選択します。複数のレイヤ 3 仮想ネットワークを 1 つのファブリックサイトに割り当てることができます。必要なすべてのファブリックサイトについて、この関連付けを繰り返します。

ステップ 6 [Configuring traffic exit behavior] ウィンドウで、この仮想ネットワークが複数のファブリックサイトに関連付けられている場合のトラフィックの出口動作を設定します。

- デフォルトでは、[Local Exit] が選択されています。このオプションにより、関連付けられている各ファブリックサイトのローカルボーダーを通過してトラフィックが出るようになります。
- 仮想ネットワークを位置指定し、指定された境界でトラフィックが出られるようにするには、[Anchor (Multisite Remote Border)] を選択します。

  関連付けられているファブリックサイトのリストから、この仮想ネットワークにおけるすべてのトラフィックに関して出口として機能するボーダーを持つサイトを選択します。関連付けられている他のファブリックサイトは、この仮想ネットワークを継承します。

ステップ 7 [Summary] ウィンドウで、レイヤ 3 仮想ネットワークの設定を確認します。

ステップ 8 [Let's begin deploying your Layer 3 virtual network] ウィンドウで、[Create] をクリックして仮想ネットワークのコンテキストを作成します。

ステップ 9 選択したサイトに仮想ネットワークを割り当てるには、[Deploy] をクリックします。

ステップ 10 仮想ネットワークの作成を確認するには、[View All Virtual Networks] をクリックします。

[Virtual Networks] ウィンドウに、ファブリックに含まれるすべてのレイヤ 3 仮想ネットワークの詳細情報が表示されます。

レイヤ 2 仮想ネットワークの作成

ステップ 1 メニューアイコン（☰）をクリックして、**[Workflows]** > **[Create Layer 2 Virtual Networks]** の順に選択します。

または、**[Provision]** > **[Virtual Networks]** で [Layer 2] タブに移動し、[Create Layer 2 Virtual Networks] をクリックすることもできます。

ステップ 2 タスクの概要ウィンドウが開いたら、[Let's Do it] をクリックして、ワークフローに直接移動します。

ステップ 3 [Configure VLANs] ウィンドウで、ファブリックに接続する VLAN の数を入力するには、次の手順を実行します。

a) 各 VLAN の **VLAN 名**とオプションの **VLAN ID** を入力します。

b) [Traffic Type] ドロップダウンリストで、[Data] または [Voice] を選択します。
レイヤ 2 仮想ネットワークではフラッディングがデフォルトで有効になっています。

c) （オプション）[Wireless] ボタンを切り替えてワイヤレスを有効にします。

ステップ 4 [Select a fabric site for each Layer 2 virtual network] ウィンドウで、レイヤ 2 仮想ネットワークのファブリックサイトを選択します。

必要に応じて、このレイヤ 2 仮想ネットワークに関連付けるレイヤ 3 仮想ネットワークを選択できます。

（注） [L3VN Name] ドロップダウンでレイヤ 3 仮想ネットワークを選択しないことで、純粋なレイヤ 2 仮想ネットワークを作成できます。

ステップ 5 [Summary] ウィンドウで、レイヤ 2 仮想ネットワークの設定を確認して、[Create] をクリックします。

ステップ 6 レイヤ 2 仮想ネットワークのプロビジョニングを確認するために、[Submit] をクリックします。

レイヤ 2 仮想ネットワークがプロビジョニングされると、成功メッセージが表示されます。

ステップ 7 レイヤ 2 仮想ネットワークの作成を確認するには、[Virtual Network Overview] をクリックします。[Virtual Networks] ウィンドウの [Layer 2] タブには、ファブリックに含まれるすべてのレイヤ 2 仮想ネットワークの詳細情報が表示されます。

ファブリックサイトへのレイヤ 3 仮想ネットワークの追加

ステップ 1 メニューアイコン（☰）をクリックして、**[Provision]** > **[Virtual Networks]**。

ステップ 2 [NETWORK OBJECTS] で、[Layer 3 Virtual Networks] の数を示す数字をクリックします。

表示されるウィンドウに、グローバルレベルで作成されたすべてのレイヤ 3 仮想ネットワークが示されます。

ステップ 3 [Layer 3] タブの、目的のレイヤ 3 仮想ネットワークの [Actions] 列で、カーソルを省略記号アイコン（ ••• ）の上に置き、[Add to Fabric Site] を選択します。

ステップ 4 [Select Fabric Site] スライドインペインで、サイトを選択し、[Select] をクリックします。

エニーキャストゲートウェイの作成

始める前に

レイヤ 3 仮想ネットワークが作成されていることを確認します。

ステップ 1 メニューアイコン（☰）をクリックして、**[Provision]** > **[Virtual Networks]**。

ステップ 2 [LAYER 2] で、[Anycast Gateways] の数を示す数字をクリックします。

ステップ 3 [Anycast Gateway] タブで、[Create Anycast Gateway] をクリックします。

または、[Layer 3] タブで、レイヤ 3 仮想ネットワークの [Actions] 列の下にある省略記号アイコン（ ••• ）の上にカーソルを置き、[Create Anycast Gateways] を選択してステップ 6（525 ページ）へスキップします。

ステップ 4 [Let's Do it] をクリックします。

ステップ 5 [Select Layer 3 Virtual Networks to configure] ウィンドウで、ゲートウェイを追加する 1 つ以上の仮想ネットワークを選択します。

ステップ 6 [Add IP Pools and VLANs] ウィンドウの左側のペインで、ゲートウェイを作成するレイヤ 3 仮想ネットワークを選択し、次の手順を実行します。

a) ドロップダウンリストから [IP Pool] を選択します。

b) INFRA_VN に対して、次の手順を実行します。

- [Pool Type] ドロップダウンリストから [AP] または [Extended Node] を選択します。
- [VLAN Name] に有効な VLAN 名を入力するか、[Auto generate VLAN name] チェックボックスをオンにします。
- [VLAN ID] に仮想ネットワークのカスタム VLAN ID を入力します。
- サプリカントベースの拡張ノードをオンボードするには、[Supplicant-Based Extended Node Onboarding] チェックボックスをオンにします。

（注） このチェックボックスは、[Extended Node] プールタイプを選択した場合にのみ表示されます。

c) IP ダイレクトブロードキャスト機能を有効にするには、[Directed Broadcast] トグルボタンをクリックします。

（注）
- ダイレクトブロードキャストを有効にする前に、レイヤ 2 フラッディングを有効にします。
- ルータおよび Nexus 7000 シリーズ スイッチは、ダイレクトブロードキャストをサポートしていません。
- ダイレクトブロードキャストを有効にする前に、アンダーレイマルチキャストが有効になっていることを確認してください。

d) [VLAN Name] に有効な VLAN 名を入力するか、[Auto generate VLAN name] チェックボックスをオンにします。

e) [VLAN ID] に仮想ネットワークのカスタム VLAN ID を入力します。

（注）
- VLAN ID 1、1002 ー 1005、2046、および 4095 は予約済みで、使用できません。
- カスタム VLAN ID を指定しない場合は、Cisco DNA Center が 1021 ー 2020 の範囲の VLAN ID を生成します。

f) [Traffic Type] ドロップダウンリストから、[Data] または [Voice] を選択します。

g) ドロップダウンリストから [Security Group] を選択します。

h) この IP プールをクリティカル IP アドレスプールに含めるには、[Critical VLAN] トグルボタンをクリックします。

認証サーバーを使用できない場合、クリティカルプールがクローズド認証プロファイルに使用されます。認証サーバーがない場合、クリティカルプールにクリティカル VLAN が割り当てられ、未認証のすべてのホストがそのクリティカル VLAN に配置されます。

i) レイヤ 2 仮想ネットワークを有効にするには、[Enable] トグルボタンをクリックします。

j) レイヤ 2 フラッディングを有効にするには、[Flooding] トグルボタンをクリックします。

（注） レイヤ 2 フラッディングにはアンダーレイマルチキャストが必要であり、これは LAN 自動化中に設定されます。LAN 自動化でアンダーレイをプロビジョニングしない場合は、アンダーレイマルチキャストを手動で設定します。

k) この IP プールをワイヤレス IP アドレスプールとして有効にするには、[Wireless] トグルボタンをクリックします。

l) ファブリック対応のワイヤレスネットワークに接続されているブリッジモードの仮想マシンのオンボーディングを有効にするには、[Bridge Mode VM] トグルボタンをクリックします。

（注） [Bridge-Network Virtual Machine] トグルボタンは、ワイヤレストグルボタンを有効にした場合にのみ表示されます。

m) IP プールをさらに関連付けるには、アイコンをクリックして上記の手順を繰り返します。

ステップ 7 [Summary] ウィンドウで、エンドポイントの接続設定を確認します。

ステップ 8 [Let's begin creating your Gateway] ウィンドウで、[Create] をクリックします。

ステップ 9 成功メッセージが表示された後にゲートウェイの作成を確認するには、[View All Virtual Networks] をクリックします。

ファブリックゾーンの設定

ファブリックサイト（親サイト）は、ネットワークを簡単に管理できるように、より小さなサブネットによるファブリックゾーンに分割できます。ファブリックゾーンは、独自のエッジノードと拡張ノードを持つことができますが、コントロールプレーンとボーダーのために親サイトに接続します。以前の Cisco DNA Center のリリースから現在のリリースに移行した場合は、既存のファブリックサイトにファブリックゾーンを作成することができます。このファブリックゾーンは、親サイトのすべてのプロパティを継承します。

はじめる前に

- ネットワーク階層がグローバルサイトの下に作成されていることを確認します。
- 階層の最下位に位置していない親サイトを選択します。

次に、ファブリックゾーンを設定するためのワークフローの概要を示します。

1. 次のいずれかの方法でファブリックゾーンを作成します。
   - [Create a Fabric Site] ワークフローを使用して、ファブリックサイトとそのゾーンを作成します。詳細については、ファブリックサイトおよびそのファブリックゾーンの作成 （527 ページ）を参照してください。
   - 既存のファブリックサイトを編集して、ファブリックゾーンを追加します。詳細については、ファブリックサイト内のファブリックゾーンの作成 （529 ページ）を参照してください。
2. ファブリックゾーンにエッジノードと拡張ノードを追加します。詳細については、ファブリックへのデバイスの追加 （513 ページ）を参照してください。
3. ファブリックゾーンにレイヤ 3 仮想ネットワークとセグメントを割り当てます。詳細については、ファブリックゾーンへのレイヤ 3 仮想ネットワークの追加 （529 ページ）を参照してください。

（注） ファブリックゾーンで使用できるのは親サイトの仮想ネットワークとセグメントのみです。

（注） ファブリックゾーンに追加されたセグメントは、親サイトでは更新できません。

親サイトのファブリックゾーンのエッジノードおよび拡張ノードは編集できません。

ファブリックゾーンのエッジノードは、親サイトのコントロールプレーンまたはボーダーとして設定できます。

ファブリックサイトおよびそのファブリックゾーンの作成

ステップ 1 メニューアイコン（☰）をクリックして、**[Provision]** > **[Fabric Sites]**。

ステップ 2 [Create Fabric Site] をクリックします。

または、メニューアイコンをクリックして**[Workflows]** > **[Create Fabric Site]**の順に選択します。

ステップ 3 タスクの概要ウィンドウが表示されたら、[Let's Do It] をクリックして、ワークフローに直接移動します。

ステップ 4 [Fabric Site Location] ウィンドウで、ファブリックゾーンとして追加するエリア、建物、またはフロアを選択します。

ステップ 5 [Wired Endpoint Data Collection] ウィンドウで、[Monitor wired clients] チェックボックスがオンになっていることを確認します。

ステップ 6 [Authentication Template] ウィンドウで、次の手順を実行します。

a) ファブリックサイトの認証テンプレートを選択します。

- [Closed Authentication]：認証前のすべてのトラフィック（DHCP、DNS、ARP など）が廃棄されます。
- **オープン認証（Open Authentication）**：ホストには、802.1X 認証を受ける必要なくネットワークアクセスが許可されます。
- [Low Impact]：スイッチポートに ACL を適用することでセキュリティを追加して、認証前に制限されたネットワークアクセスを許可します。ホストが正常に認証されると、追加のネットワークアクセスが許可されます。
- **None**

b) （オプション）[Closed Authentication]、[Open Authentication]、または [Low Impact] を選択した場合は、[Edit] をクリックして認証設定を編集します。

- [First Authentication Method]：[802.1x] または [MAC Authentication Bypass (MAB)] を選択します
- [802.1x Timeout (in seconds)]：スライダを使用して、802.1x タイムアウトを秒単位で指定します。
- [Wake on LAN]：[Yes] または [No] を選択します。
- [Number of Hosts]：[Unlimited] または [Single] を選択します。
- [BPDU Guard]：このチェックボックスを使用して、すべての [Closed Authentication] ポートでブリッジ プロトコル データ ユニット（BPDU）ガードを有効または無効にします。
- [Pre-Authentication Access Control List]：トグルボタンを有効にして、[Low Impact] 認証の事前認証制御を構成します。[Implicit Action] ドロップダウンリストから、暗黙的なアクションを選択します。ルールの説明を入力します。アクセスコントラクトを追加するには、[Add Contract Action] をクリックし、ルールを選択して、[Apply Table] をクリックします。

ステップ 7 [Fabric Zones] ウィンドウで、ファブリックゾーンを指定し、範囲指定されたサブネットを作成するには、[Setup Fabric Zones Now] をクリックします。

ファブリックゾーンを有効にするには、ネットワーク階層でファブリックサイトを選択します。

ステップ 8 [Summary] ウィンドウで、ファブリックサイトの設定を確認します。

ここでファブリックサイトまたはゾーン設定を編集できます。

ステップ 9 [Deploy] をクリックします。

サイトとゾーンがプロビジョニングされるまでに数秒かかります。サイトの作成が成功すると、「Success!Your fabric site is created」というメッセージが表示されます。

サイト階層ペインでは、新しく作成されたファブリックゾーンに「FZ」というタグが付けられます。

ファブリックサイト内のファブリックゾーンの作成

ステップ 1 メニューアイコン（☰）をクリックして、**[Provision]** > **[Fabric Sites]**。

ステップ 2 [SUMMARY] で、ファブリックサイトの数を示す数字をクリックします。

ステップ 3 ファブリックゾーンを指定するファブリックサイトの [Actions] 列で、省略記号アイコン（ ••• ）の上にカーソルを置き、[Edit Fabric Zone] を選択します。

ステップ 4 [Fabric Zones] ウィンドウで、エリア、建物、またはフロアを選択します。

ステップ 5 [Next] をクリックします。

ステップ 6 [Summary] ウィンドウに表示されるファブリックサイトの設定を確認します。

ここでファブリックサイトまたはゾーン設定を編集できます。

ステップ 7 [Deploy] をクリックします。

サイトとゾーンがプロビジョニングされるまでに数秒かかります。「**Success!**Your fabric site is created」というメッセージが表示されます。

サイト階層ペインでは、新しく作成されたファブリックゾーンに「FZ」というタグが付けられます。

次のタスク

- 新しく作成したファブリックゾーンにエッジノードデバイスと拡張ノードデバイスのみを追加します。

  ファブリックゾーンに割り当てられたデバイスを親サイトに割り当てることはできません。ただし、ファブリックゾーンに割り当てられたエッジノードデバイスを親サイトのコントロールプレーンまたはボーダーノードとして設定することは引き続き可能です。

- ファブリックゾーンに IP プールと仮想ネットワークを割り当てます。

ファブリックゾーンへのレイヤ 3 仮想ネットワークの追加

始める前に

ファブリックゾーンが作成されていることを確認します。

（注） ファブリックゾーンに追加できるのは親サイトのレイヤ 3 仮想ネットワークのみです。

ステップ 1 メニューアイコン（☰）をクリックして、**[Provision]** > **[Virtual Networks]**。

ステップ 2 [NETWORK OBJECTS] で、[Layer 3 Virtual Networks] の数を示す数字をクリックします。

表示されるウィンドウに、グローバルレベルのすべてのレイヤ 3 仮想ネットワークが示されます。

ステップ 3 [Global] ファブリックサイトをクリックします。

ステップ 4 [Select Fabric Site] スライドインペインで、ファブリックゾーンを選択し、[Select] をクリックします。

ステップ 5 [Layer 3] タブで、[Add Layer 3 VN] をクリックします。

ステップ 6 [Add Virtual Network] スライドインペインで、ファブリックゾーンに追加する仮想ネットワークを選択します。[更新（Update）] をクリックします。

ファブリックゾーンへのレイヤ 2 仮想ネットワークの追加

始める前に

（注） ファブリックゾーンに追加されたゲートウェイは、親サイトでは更新できません。

ステップ 1 メニューアイコン（☰）をクリックして、**[Provision]** > **[Virtual Networks]**。

ステップ 2 [LAYER 2] で、[Layer 2 Virtual Networks] の数を示す数字をクリックします。

表示されるウィンドウに、グローバルレベルのすべてのレイヤ 2 仮想ネットワークが示されます。

ステップ 3 [Global] ファブリックサイトをクリックします。

ステップ 4 [Select Fabric Site] スライドインペインで、ファブリックゾーンを選択し、[Select] をクリックします。

ステップ 5 [Layer 2] タブで、[Add Layer 2 Virtual Network] をクリックします。

ステップ 6 [Select L2VNs] スライドインペインで、レイヤ 2 仮想ネットワークを選択します。

ステップ 7 [Add] をクリックします。

ファブリックゾーンへのエニーキャストゲートウェイの追加

始める前に

ファブリックゾーンが作成されていることを確認します。

（注） 親サイトのエニーキャストゲートウェイのみをファブリックゾーンに追加できます。

ファブリックゾーンに追加されたエニーキャストゲートウェイは、親サイトでは更新できません。

ステップ 1 メニューアイコン（☰）をクリックして、**[Provision]** > **[Virtual Networks]**。

ステップ 2 [LAYER 2] で、[Anycast Gateways] の数を示す数字をクリックします。

表示されるウィンドウに、グローバルレベルのすべてのエニーキャストゲートウェイが示されます。

ステップ 3 [Global] ファブリックサイトをクリックします。

ステップ 4 [Select Fabric Site] スライドインペインで、ファブリックゾーンを選択し、[Select] をクリックします。

ステップ 5 [Anycast Gateway] タブで、[Add Anycast Gateway] をクリックします。

ステップ 6 [Select Anycast Gateway(s)] スライドインペインで、レイヤ 3 仮想ネットワークを選択し、[Next] をクリックします。

ステップ 7 追加するエニーキャストゲートウェイを選択します。

ステップ 8 [Add] をクリックします。

拡張ノードデバイスの設定

拡張ノードは、自動化されたワークフローによって設定されます。設定後、拡張ノードデバイスがファブリックトポロジビューに表示されます。[Port Assignment] タブを使用して、拡張ノードにポートを割り当てることができます。

（注） 拡張ノードは、GUI ベースのプロビジョニング ワークフローではオンボードできません。拡張ノードをオンボードするには、デバイス設定を工場出荷時の初期状態にリセットし、デバイスの電源をオンにした後に、SD-Access 自動化ワークフローを使用する必要があります。

デバイスは、拡張ノードネイバーの Cisco DNA ライセンスおよびデバイスの Cisco DNA ライセンスに応じてオンボードされます。

- ネイバーが Cisco DNA Essentials ライセンスで動作している場合、デバイスは、その Cisco DNA ライセンスに関係なく、標準の拡張ノードとしてオンボードされます。
- ネイバーが Cisco DNA Advantage ライセンスで動作している場合、デバイスは、Cisco DNA Essentials ライセンスがあれば、標準の拡張ノードとしてオンボードされます。
- ネイバーが Cisco DNA Advantage ライセンスで動作している場合、デバイスは、Cisco DNA Advantage ライセンスがあれば、ポリシー拡張ノードとしてオンボードされます。
- デバイスに複数のネイバーがあり、それらのネイバーに異なる Cisco DNA ライセンスレベルがある場合、デバイスは Cisco DNA ライセンスに関係なく、標準の拡張ノードとしてオンボードされます。

拡張ノードデバイスは、マルチキャストトラフィックをサポートします。

ポリシー拡張ノードは、仮想ネットワーク内のセキュリティポリシーをサポートする拡張ノードです。ポリシー拡張ノードのポート割り当て時に、[Group] を選択できます。

ポリシー拡張ノードデバイスには、Cisco IOS XE リリース 17.1.1s 以降を実行している Cisco Catalyst Industrial Ethernet（IE）3400、IE 3400 Heavy Duty シリーズ スイッチ、および Cisco Catalyst 9000 シリーズ スイッチがあります。

シスコ デジタルビルディング シリーズ スイッチ、Cisco Catalyst 3560-CX スイッチ、および Cisco Industrial Ethernet 4000、4010、5000 シリーズ スイッチは、ポリシー拡張ノードとして構成することはできません。

拡張ノードの設定手順

Cisco Catalyst 9300、Cisco Catalyst 9400、および Cisco Catalyst 9500 シリーズスイッチは、ファブリックエッジとして設定されたときに拡張ノードをサポートします。

（注） ファブリックエッジノードとして設定されている Cisco Catalyst 9200 シリーズ スイッチは、拡張ノードデバイスをサポートしていません。

以下に、拡張ノードでサポートされている最小ソフトウェアバージョンを示します。

- Cisco Industrial Ethernet 4000、4010、5000 シリーズ スイッチ：15.2(7)E0s（LAN ベースライセンスが有効になっている）

  IP サービスライセンスがある場合は、Switch Database Management（SDM）テンプレートを `dual-ipv4-and-ipv6 default` に手動で変更する必要があります。

- Cisco Catalyst IE 3400、3400 Heavy Duty（X-coded および D-coded）シリーズ スイッチ：Cisco IOS XE リリース 17.1.1s。
- Cisco Catalyst IE 3300 シリーズ スイッチ：Cisco IOS XE リリース 16.12.1s。
- Cisco Digital Building シリーズ スイッチ、Cisco Catalyst 3560-CX スイッチ：リリース 15.2(7)E0s。

ポリシー拡張ノードデバイス、およびポリシー拡張ノードをサポートするエッジノードデバイスで必要な最小ソフトウェアバージョンは Cisco IOS XE リリース 17.1.1 s です。

次の設定手順は、標準の拡張ノードとポリシー拡張ノードの両方に適用されます。

始める前に

ポリシー拡張ノードとしてデバイスを設定するには、デバイスとそれをサポートするエッジノードの両方で、Network Advantage と Cisco DNA Advantage のライセンスレベルが有効になっている必要があります。

ステップ 1 拡張ノードのネットワーク範囲を設定します。IP アドレス プールを設定する （241 ページ） を参照してください。この手順では、IP アドレスプールを追加し、サイトレベルで IP プールを予約します。CLI および SNMP クレデンシャルが設定されていることを確認します。

ステップ 2 拡張 IP アドレスプールを INFRA_VN に割り当てます。エニーキャストゲートウェイの作成 （524 ページ） を参照してください。[Pool Type] として [Extended Node] を選択します。

Cisco DNA Center Cisco DNA Center は、サポートされているファブリックエッジデバイスで拡張 IP アドレスプールと VLAN を設定します。これにより、拡張ノードのオンボーディングが有効になります。

ステップ 3 拡張 IP アドレスプールとオプション 43 を使用して DHCP サーバーを設定します。拡張 IP アドレスプールが Cisco DNA Center から到達可能であることを確認します。

（注） オプション 43 の詳細については、DHCP コントローラ ディスカバリ （396 ページ） を参照してください。

ステップ 4 ファブリックエッジデバイスに拡張ノードデバイスを接続します。拡張ノードデバイスからファブリックエッジへ複数のリンクを設定できます。

ステップ 5 拡張ノードに接続されているファブリックエッジノードでポートチャネルを作成します。リングまたはデイジーチェーン内の後続の拡張ノードに関して、それが接続している、前の拡張ノードでポートチャネルを作成します。

（注） この手順は、ファブリックのグローバル認証モードが [Open Authentication]、[Low Impact]、または [Closed Authentication] の場合にのみ完了してください。ファブリックサイトが [None] 認証モードに設定されている場合、ポートチャネルは、プラグ アンド プレイ プロビジョニングを使用した拡張ノードのオンボーディング中に自動的に作成されます。

ポートチャネルを作成するには、次の手順を実行します。

a) メニューアイコン（☰）をクリックして、**[Provision]** > **[Fabric Sites]**。
b) [Fabric Sites] タブで、ファブリックサイトの数を示す数字をクリックします。
c) ファブリックサイトを選択します。
d) [Fabric Infrastructure] タブで、ファブリックエッジノード（または接続に応じて拡張ノード）を選択します。
e) スライドインペインの [Port Channel] タブで、[Create Port Channel] をクリックします。
f) 次の手順を実行します。

- [Connected Device Type] ドロップダウンリストから [Extended Node] を選択します。
- 説明を入力します。
- [Port Aggregation Protocol (PAgP Desirable)] を選択します。

  Cisco IOS XE リリース 17.1.1s 以降、IE 3300 および IE 3400 デバイスは PAgP をサポートしています。
- Cisco IOS XE リリース 17.1.1s よりも前のバージョンを実行している場合は、IE 3300 および IE 3400 デバイスの [On] を選択します。

（注） 拡張ノードのオンボーディングではLink Aggregation Control Protocol（LACP）は機能しません。

- ポートチャネルとしてバンドルするポートを選択します。

g) [Done] をクリックします。

これで、ファブリックエッジノード（または拡張ノード）にポートチャネルが作成され、拡張デバイスがオンボードされます。

ステップ 6 以前の設定がない場合は、拡張ノードデバイスの電源をオンにします。拡張ノードデバイスに設定がある場合は、以前の設定の書き込み消去を実行して、拡張ノードデバイスをリロードします。

Cisco DNA Center Cisco DNA Center では、拡張ノードデバイスをインベントリに追加し、同じサイトをファブリックエッジとして割り当てます。次に、拡張ノードデバイスがファブリックに追加されます。これで、拡張ノードデバイスがオンボードされ、管理できるようになりました。

設定が完了すると、拡張ノードがファブリックトポロジに、拡張ノードであることを示すタグ（X）とともに表示されます。

拡張ノードのポリシー拡張ノードへのアップグレード

Cisco SD-Access の自動化は、Cisco DNA Essentials ライセンスを持つポリシー拡張ノード対応デバイスを拡張ノードとしてオンボーディングします。ライセンスを Cisco DNA Advantage にアップグレードすることにより、この拡張ノードデバイスをポリシー拡張ノードに変換できます。

デイジーチェーンでは、アップストリームデバイスが拡張ノードである場合、拡張ノードをポリシー拡張ノードにアップグレードすることはできません。

リングでは、隣接するノードが両方とも拡張ノードである場合、拡張ノードをポリシー拡張ノードにアップグレードすることはできません。

ポリシー拡張ノードにアップグレードされたノードを、拡張ノードとして再構成することはできません。

拡張ノードをポリシー拡張ノードに変換するには、次の手順を実行します。

始める前に

- 拡張ノードがすでにオンボーディングされていることを確認してください。
- Cisco DNA Center でスマートライセンス認証情報を更新します。

ステップ 1 Cisco DNA Center ライセンスマネージャを使用して、デバイスでのライセンスレベルを Cisco DNA Essentials から Cisco DNA Advantage に変更します。

a) メニューアイコン（☰）をクリックして、**[Tools]** > **[License Manager]** の順に選択します。

b) [Devices] タブで、デバイスを選択します。
c) **[Actions]** > **[Change License]** > **[Change DNA License]** を選択します。
d) [Change DNA License Level] ウィンドウで、[Advantage] をクリックします。
e) [Confirm] をクリックします。
f) [Success] メッセージウィンドウで、[OK] をクリックします。

デバイスがリロードします。

ステップ 2 ノードが [Reachable] になり、[Managed] 状態になるのを待ちます。

[Provision] > **[Network Devices]** > **[Inventory]** ウィンドウに、すべてのデバイスの到達可能性ステータスが表示されます。

ステップ 3 「Netconf Connection Refused」エラーが表示された場合は、デバイスを再同期します。エラーがなくなるまで、再同期プロセスを繰り返します。

a) **[Provision]** > **[Network Devices]** > **[Inventory]** ウィンドウで、デバイスを選択します。
b) **[Actions]** > **[Inventory]** > **[Resync Device]** の順に選択します。

ステップ 4 ポリシー拡張ノードへアップグレードします。

a) **[Provision]** > **[Fabric Sites]** ウィンドウで、デバイスがオンボーディングされているサイトを選択します。
b) [Fabric Infrastructure] タブで、デバイスをクリックしてその属性を編集します。
c) [Fabric] タブで、[Extended Node Attributes] の下の [Policy] ボタンを切り替えます。
d) 表示される [Policy Extended Node Upgrade] ウィンドウで、[Upgrade] をクリックします。

拡張ノードの削除

このタスクでは、拡張ノード、ポリシー拡張ノード、および認証済み拡張ノードを削除する手順について説明します。

ステップ 1 ファブリックから拡張ノードデバイスを削除します。

a) メニューアイコン（≡）をクリックして、**[Provision]** > **[Fabric Sites]**。
b) [Fabric Sites] タブで、ファブリックサイトの数を示す数字をクリックします。
c) 拡張ノードデバイスを含むファブリックサイトを選択します。
d) [Fabric Infrastructure] タブで、拡張ノードデバイスをクリックします。
e) スライドインペインで、[Remove From Fabric] をクリックします。
f) [Add] をクリックします。

ステップ 2 デバイスを [Inventory] から削除します。

インベントリからデバイスを削除する手順については、ネットワーク デバイスの削除 （129 ページ）を参照してください。

ステップ 3 サプリカントベースの拡張ノードデバイスの場合、ファブリックエッジノードまたは FIAB でポート割り当て設定を削除します。

拡張ノードおよびポリシー拡張ノードの REP リングトポロジの設定

拡張ノードによってネットワーク障害の回復時間が 50 ms 未満となる冗長性を実現するには、ファブリックサイトの Resilient Ethernet Protocol（REP）リングを設定します。

特に明記されていないかぎり、「拡張ノード」という用語はポリシー拡張ノードも表します。

REP リングでは、次のデバイスを設定できます。

- 拡張ノード：

  Cisco IOS 15.2(7)E3 以降のリリースが動作する Cisco Industrial Ethernet (IE) 4000、4010、5000 シリーズ スイッチ。

  Cisco IOS XE 17.3.3 以降のリリースが動作する Cisco Catalyst IE3300 シリーズ スイッチ。

- ポリシー拡張ノード：

  Cisco IOS XE 17.3.3 以降のリリースが動作する Cisco Catalyst IE3400、IE3400H シリーズ スイッチ。

REP リングの制約事項

- 拡張ノードを既存の REP リングに追加するには、最初に REP リングを削除します。REP リングを削除すると、Per VLAN Spanning Tree Protocol（PVSTP）が有効になり、レイヤ 2 ループが回避されます。次に、新しい拡張ノードをファブリックに追加し、REP リングを再度作成して、新しい拡張ノードを含めます。
- 特定の REP リング内の複数のリングおよびリングのリングはサポートされていません。
- REP リング内のノードには、デイジーチェーン方式で他のノードを接続できます。ただし、デイジーチェーンのノードには、ノードのリングを接続することはできません。
- REP リングまたはデイジーチェーンでは、拡張ノードとポリシー拡張ノードを混在させることはできません。REP リングまたはデイジーチェーンは、拡張ノードのみで、またはポリシー拡張ノードのみで構成されている必要があります。
- デフォルトでは、1 つの REP リングに最大 18 台のデバイスをオンボードできます。19 台以上のデバイスをオンボードするには、**spanning-tree vlan** *infra VN VLAN* **max-age 40** コマンドを使用して BPDU タイマーを増やします。このコマンドを設定するには、Cisco DNA Center のテンプレートを使用します。

リングの最後の 2 つのノードが同時にオンボードを試みると、まれに、これらのノード間にポートチャネルが作成されない場合があることに注意してください。REP リングが作成されると、リングの最後の 2 つのノード間にポートチャネルが確立されます。

特に明記されていないかぎり、次の手順は拡張ノードとポリシー拡張ノードの両方に適用されます。

始める前に

ファブリックエッジノードと拡張ノードがオンボードされていることを確認します。

REP リングの終端となっているファブリックエッジノードとそのインターフェイスを特定します。

（注） REP リング設定手順により、ネットワークトラフィックが短時間中断される可能性があります。

ステップ 1 メニューアイコン（☰）をクリックして、**[Workflows]** > **[Configure REP Ring]** の順に選択します。

または、ファブリックサイトトポロジビューに移動して、REP リングを作成するファブリックエッジノードまたは FIAB ノードを選択し、[REP Rings] タブで [Create REP Ring] をクリックすることもできます。

ステップ 2 タスクの概要ウィンドウが表示されたら、[Let's Do It] をクリックして、ワークフローに直接移動します。

ステップ 3 [Select a fabric site] ウィンドウで、エッジノードと拡張ノードの両方があるサイトを選択します。

ステップ 4 [Select a fabric edge node] ウィンドウで、ファブリックエッジノードを選択します。

ステップ 5 [Select Extended Nodes connected to Fabric Edge] ウィンドウで、ファブリックエッジノードに接続する拡張ノードを選択します。

ファブリックエッジノードに接続する 2 つの拡張ノードを選択できます。

ステップ 6 ファブリックサイト、エッジノード、および拡張ノードの選択を確認し、必要に応じて編集します。

ステップ 7 REP リングの設定を開始するには、[Provision] をクリックします。

[REP Ring Configuration Status] ウィンドウで、設定の進捗状況の詳細なステータスを確認できます。

ステップ 8 [REP Ring Summary] ウィンドウに、作成された REP リングの詳細情報が、検出されたデバイスとともに表示されます。

ステップ 9 REP リングの作成後、成功メッセージが表示されます。

REP リングの作成を確認するには、ファブリックサイトウィンドウに移動し、ファブリックエッジノードをクリックします。

スライドインウィンドウの [REP Ring] タブで、そのエッジノードに存在するすべての REP リングのリストを確認できます。

リスト内の REP リング名をクリックすると、リングに存在するデバイス、リングに接続する各デバイスのポートなどの詳細情報が表示されます。

REP リングステータスの表示

REP リング内のデバイスのステータスを表示するには、次の手順を実行します。

ステップ 1 Cisco DNA Center GUI でメニューアイコン（☰）をクリックして、**[Provision]** > **[Fabric Sites]**。

ステップ 2 [Fabric Sites] タブで、ファブリックサイトの数を示す数字をクリックします。

ステップ 3 すべてのファブリックサイトを表示するリストからファブリックサイトを選択します。

ステップ 4 [Fabric Infrastructure] タブで、ファブリックエッジノードまたは FIAB をクリックします。

スライドインウィンドウに、選択したファブリックエッジノードまたは FIAB の詳細が表示されます。

ステップ 5 [REP Rings] タブで、[View] をクリックして [REP Ring Topology Status] を表示します。

[REP Topology Status] セクションには、REP リング内のすべてのデバイスの現在の状態が表示されます。[Role] 列に表示される状態は、[Open]、[Fail]、または [Alt] です。

[Open] は、デバイスリンクが稼働していて、トラフィックを転送していることを示します。

[Fail] は、デバイスリンクがダウンしていることを示します。

[Alt] は、デバイスリンクがアップしているが、ポートがトラフィックを転送できないことを示します。

REP リングの削除

ステップ 1 メニューアイコン（☰）をクリックして、**[Provision]** > **[Fabric Sites]**。

ステップ 2 [Fabric Infrastructure] タブで、REP リングを終了するファブリックエッジノードをクリックします。

スライドインウィンドウに、選択したファブリックエッジノードの詳細が表示されます。

ステップ 3 [REP Rings] タブで、目的の REP リングの **[Actions (…)]** > **[Delete]**をクリックします。

これにより、REP リングが削除されます。

REP リングからのノードの削除

このタスクでは、REP リングから 1 つまたは複数の拡張ノードを削除する手順について説明します。

（注） 拡張ノードが削除された後、ダウンサイジングされた REP リングは既存のインターフェイスを使用して隣接デバイスへのリンクを作成する必要があります。

始める前に

ノードが属する REP リングが不完全でないことを確認してください。

ステップ 1 拡張ノードデバイスをネットワークから手動で削除します。

または、REP リング内のデバイスがダウンすると、[Fabric Infrastructure] ウィンドウに通知が表示されます。

ステップ 2 メニューアイコン（☰）をクリックして、**[Provision]** > **[Fabric Sites]**。

ステップ 3 [Fabric Infrastructure] タブで、REP リングを終了するファブリックエッジノードをクリックします。

slide-in paneに、選択したファブリックエッジノードの詳細が表示されます。

ステップ 4 [REP Rings] タブで、目的の REP リングについて、**[Actions (…)]** > **[Rediscover]**を選択します。

REP リングから拡張ノードデバイスが削除され、REP リングの表示が更新されます。

サプリカントベースの拡張ノードの設定

Authenticated Extended Node（AEN）とも呼ばれるサプリカントベースの拡張ノードは、IEEE 802.1x（Dot1x）サプリカント設定を受け取り、完全な認証と承認の後にのみ SD-Access ネットワークにオンボードされる拡張ノードデバイスです。サプリカントベースの拡張ノードデバイスをオンボードするには、ファブリックエッジのオーセンティケータポートをクローズド認証テンプレートで設定する必要があります。

次のプラットフォームは、サプリカントベースの拡張ノードオンボーディングをサポートしています。

ファブリックエッジまたは FIAB：

Cisco Catalyst 9000 シリーズ：Cisco IOS XE 17.7.1 以降で動作する C9300、C9400、C9500、および C9500H スイッチ。

サプリカントベースの拡張ノード：

Cisco Catalyst 9000 シリーズ：Cisco IOS XE 17.7.1 以降で動作する C9200、C9300、C9400、C9500、および C9500H スイッチ。

サプリカントベースの拡張ノードの設定手順

始める前に

- Cisco ISE を構成して、リリース 3.1 以降で動作することを確認します。「サプリカントベースの拡張ノードをオンボードするための Cisco Identity Services Engine の設定（542 ページ）」を参照してください。

- ファブリックエッジノードまたは FIAB デバイスをファブリックに追加し、それが Cisco IOS XE 17.7.1 以降で動作することを確認します。
- ファブリックエッジノードと Cisco ISE の間のパスに適切なパス MTU を設定します。値は 9100 をお勧めします。パス MTU は、LAN 自動化中、またはアンダーレイの構成時に、ファブリック内のすべてのデバイスに設定されることに注意してください。

ステップ 1 Cisco DNA Center で AAA サーバー設定を構成します。

a) **[System]** > **[Settings]** > **[External Services]** > **[Authentication and Policy Servers]** ウィンドウで、デバイス認証用の AAA サーバーとして Cisco ISE を定義します。

詳細な手順については、『Cisco DNA Center Administrator Guide』の「Configure Authentication and Policy Servers」を参照してください。

b) Cisco ISE サーバーをグローバルサイトに追加します。詳細については、Cisco ISE またはその他の AAA サーバーの追加 （228 ページ）を参照してください。

ステップ 2 （オプション）オンボーディング前にデバイスを認証するように Cisco DNA Center を構成します。

a) メニューアイコン（☰）をクリックして、 **[System]** > **[Settings]** > **[Device Settings]** > **[PnP Device Authorization]** の順に選択します。
b) [Device Authorization] チェックボックスをオンにしてデバイスで許可を有効にします。
c) [Save] をクリックします。

ステップ 3 PKI 証明書を管理するように Cisco DNA Center アプライアンスを構成します。

a) メニューアイコン（☰）をクリックして、**[System]** > **[Settings]** > **[Trust & Privacy]** > **[PKI Certificates]** の順に選択します。
b) [PKI Certificates] ウィンドウで、[Use Cisco DNA Center] をクリックします。
c) [CA Management] タブで、[Download CA Certificate] をクリックします。
d) Cisco ISE の信頼できる証明書ストアに証明書を追加します。詳細については、『Cisco Identity Services Engine Administrator Guide』を参照してください。https://www.cisco.com/c/en/us/support/security/identity-services-engine/products-installation-and-configuration-guides-list.html

外部証明書を使用する場合は、その証明書を Cisco ISE の信頼できる証明書ストアに追加します。

ステップ 4 拡張 IP アドレスプールとオプション 43 を使用して DHCP サーバーを設定します。拡張 IP アドレスプールが Cisco DNA Center から到達可能であることを確認します。

オプション 43 の詳細については、DHCP コントローラ ディスカバリ （396 ページ）を参照してください。

ステップ 5 ファブリックサイトで [Closed Authentication] を有効にし、ブリッジ プロトコル データ ユニット（BPDU）ガードを無効にします。

デフォルトでは、[Closed Authentication] を選択すると、すべてのダウンリンクアクセスポートに BPDU ガード設定がプッシュされます。拡張ノードのようなリモートスイッチが接続されている場合、BPDU ガードはポートをエラーディセーブルモードにプッシュします。BPDU ガードを無効にするには、クローズド認証の設定時に、[Enable BPDU Guard] チェックボックスをオフにします。

詳細については、「認証テンプレートの選択」 を参照してください。

ステップ 6 エニーキャストゲートウェイの作成 （524 ページ）に記載されているように、拡張 IP アドレスプールを INFRA_VN に割り当てます。

[Create Anycast Gateways] ワークフローで、[Pool Type] として [Extended Node] を選択し、[Supplicant-Based Extended Node Onboarding] チェックボックスをオンにします。

Cisco DNA Center Cisco DNA Center は、サポートされているファブリックエッジデバイスで拡張 IP アドレスプールと VLAN を設定します。これにより、拡張ノードのオンボーディングが有効になります。

（注） 拡張 IP アドレスプールは、ファブリックエッジデバイスが Cisco IOS XE 17.7.1 以降で動作している場合にのみ正常に割り当てられます。Cisco DNA Center の以前のリリースからアップグレードした場合は、拡張 IP アドレスプールを構成する前に、サプリカントベースの拡張ノードの移行を完了する必要があります。

ステップ 7 ファブリックエッジデバイスまたは FIAB に拡張ノードデバイスを接続します。

オンボーディングの前にデバイスを認証することを選択した場合（ステップ 2）、電源をオンにした後、拡張ノードデバイスは [Pending Authorization] 状態になります。**[Provision]** > **[Plug and Play]** ウィンドウでデバイスのステータスを確認できます。

ステップ 8 （オプション）デバイスを認証します。

この手順は、デバイスが [Pending Authorization] 状態の場合にのみ実行してください。

a) メニューアイコン（☰）をクリックして、**[Provision]** > **[Plug and Play]**。
b) [Plug and Play] ウィンドウで、サプリカントベースの拡張ノードデバイスを選択し、**[Actions]** > **[Authorize]** の順に選択します。

認証プロセスは、Cisco ISE で証明書ベースの EAP-TLS 認証を完了するために、サプリカントベースの拡張ノードデバイスをプロビジョニングします。認証後、Cisco ISE はサプリカントベースの拡張ノードデバイスに完全なアクセスを許可します。サプリカントベースの拡張ノードデバイスは、SD-Access ファブリックに完全にオンボードされます。

サプリカントベースの拡張ノードデバイスがファブリックにオンボードされた後は、ファブリック エッジサプリカント ポートへのアクセスは認証ステータスのみに基づきます。デバイスまたはポートがダウンすると、認証セッションがクリアされ、ポートでトラフィックが許可されなくなります。ポートが再び起動すると、IEEE 802.1x（Dot1x）認証プロセスを経て、SD-Access ネットワークへのアクセスが回復します。

障害のあるポートの交換

オーセンティケータ（ファブリックエッジまたは FIAB）ポートとサプリカントポート間のリンクがダウンした場合、障害のあるポートを交換し、[Port Assignment] メニューから新しいポートを設定できます。

ステップ 1 サプリカントポートを交換するには、次の手順に従います。

a) 新しいサプリカントポートの設定をクリアします。
b) 既存の設定を現在のサプリカントポートから新しいサプリカントポートにコピーして、802.1X 認証を可能にします。

ステップ 2 オーセンティケータポートを交換するには、次の手順に従います。

a) サプリカントポートをオーセンティケータの新しいインターフェイスに割り当てます。ポートの割り当てについては、「ファブリックサイト内のポートの設定」を参照してください。[Connected Device Type] として [Supplicant-Based Extended Node] を選択します。
b) オーセンティケータの古いインターフェイスの既存のポート割り当てをクリアします。

ステップ 3 オーセンティケータとサプリカントの古いポート間の物理接続を切断します。オーセンティケータとサプリカントの新しいポート間をケーブルで接続します。このリンクを確立します。

ステップ 4 オーセンティケータとサプリカントの新しいポート間のリンクが確立したら、次の手順を実行します。

a) オーセンティケータとサプリカントの両方に対して **[Inventory]** > **[Resync Device]** を実行して、Cisco DNA Center のデバイス情報を再同期します。「デバイス情報の再同期」を参照してください。
b) 新しいサプリカントポートをオーセンティケータに割り当てます。ポートの割り当てについては、「ファブリックサイト内のポートの設定」を参照してください。[Connected Device Type] として [Authenticator Switch] を選択します。
c) 古いサプリカントポートのポート割り当てをクリアします。

サプリカントベースの拡張ノードをオンボードするためのCiscddentity Services Engine の設定

このタスクでは、Cisco Identity Services Engine（ISE）でサプリカントベースの拡張ノード（SBEN）デバイスをプロファイリングする方法について説明します。以下にリストされている手順は、Cisco ISE 設定手順の一部です。詳細については、『Cisco Identity Services Engine Administrator Guide』を参照してください。

始める前に

Cisco DNA Center から CA 証明書をダウンロードします。

ステップ 1 CA 証明書を Cisco ISE にインポートします。

Cisco ISE ホームページから、**[Administration]** > **[System]** > **[Certificates]** > **[System Certificate]** > **[Import]** を選択します。[Import] ウィンドウで、[Trust for client authentication and Syslog] チェックボックスがオンになっていることを確認します。詳細については、『Cisco Identity Services Engine Administrator Guide』の「Import the Root Certificates to the Trusted Certificate Store」セクションを参照してください。

ステップ 2 RADIUS 属性を使用して、次の認証プロファイルを設定します。

Cisco ISE メインメニューから、**[Policy]** > **[Policy Elements]** > **[Results]** > **[Authorization]** > **[Authorization Profiles]** を選択します。

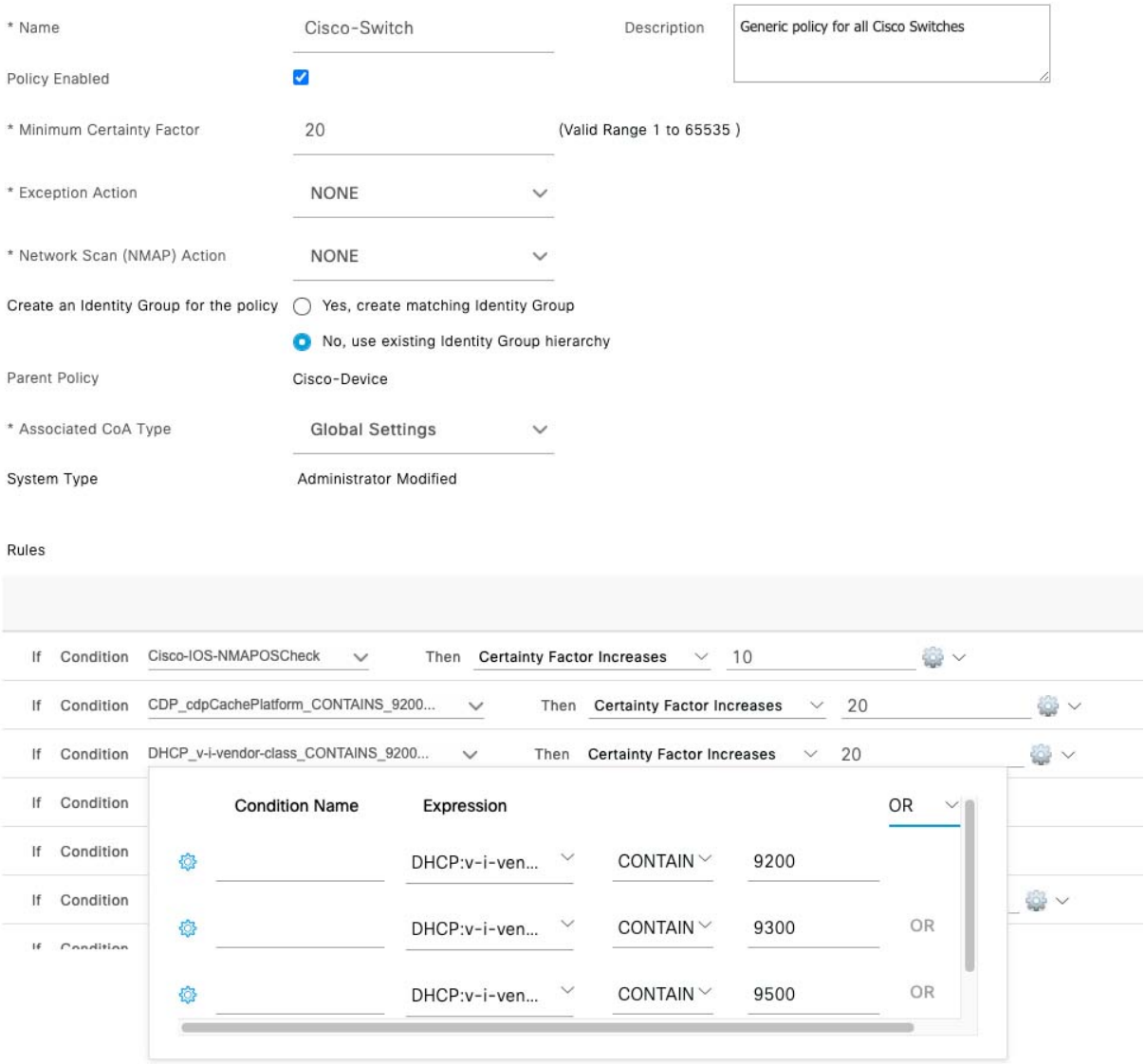
次のプロファイルを構成します。

```
SBEN-DHCP:
Access Type = ACCESS_ACCEPT
Filter-ID = SBEN_DHCP_ACL.in

SBEN_LIMITED_ACCESS_AUTHZ:
Access Type = ACCESS_ACCEPT
Filter-ID = SBEN_MAB_ACL.in
cisco-av-pair = interface-template-name=SWITCH_SBEN_MAB_TEMPLATE

SBEN_FULL_ACCESS_AUTHZ :
Access Type = ACCESS_ACCEPT
cisco-av-pair = interface-template-name=SWITCH_SBEN_FULL_ACCESS_TEMPLATE
```

ステップ 3 [Profiling Policies] ウィンドウでデバイス プロファイリング ポリシーを定義します。

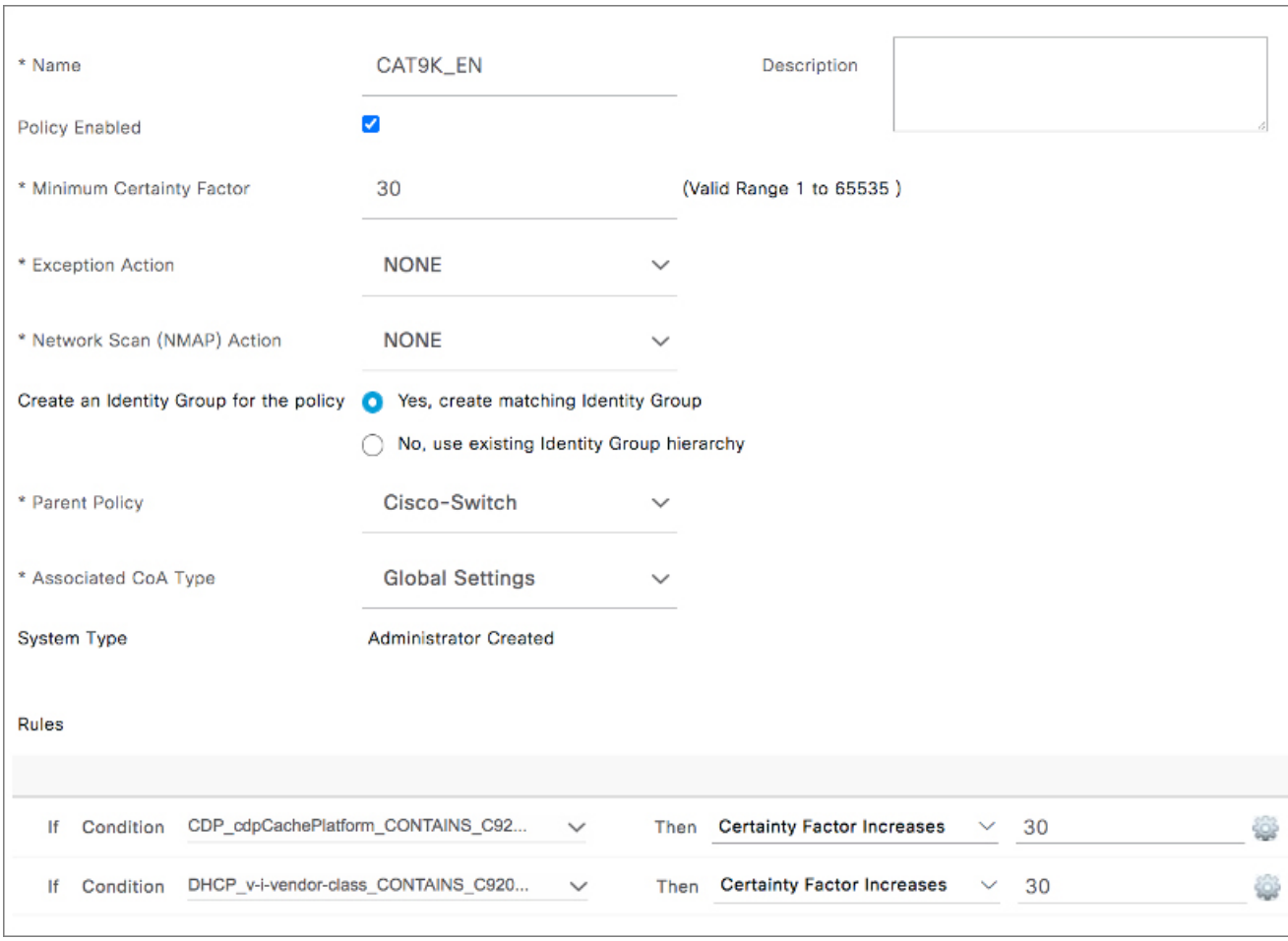
a) Cisco ISE のメインメニューから、**[Policy]** > **[Profiling]** > **[Profiling Policies]**を選択します。

b) [Profiling Policies] ウィンドウで、[Cisco-Device]：[Cisco-Switch] ポリシーの新しい [DHCP-v-i-vendor-class] 条件を追加します。



c) サプリカントデバイスの新しい子ポリシーを [Cisco-Switch] の下に作成し、[CdpCachePlatform] および [V-I-Vendor-Class] 条件を適用します。

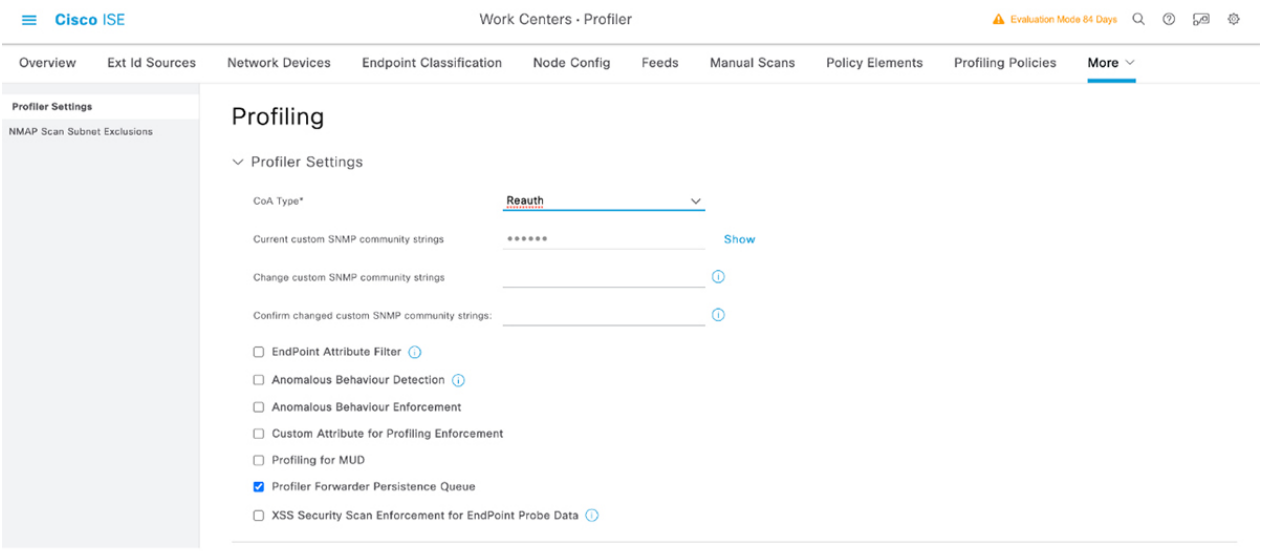
子ポリシーの [Minimum Certainty Factor] の値が親ポリシーの値よりも高いことを確認してください。



ステップ 4 グローバル認可変更（CoA）タイプを [Reauth] に設定します。

[CoA Type] を設定するには、Cisco ISE ホームページから、**[Work Centers]** > **[Profiler]** > **[Settings]**の順に移動します。

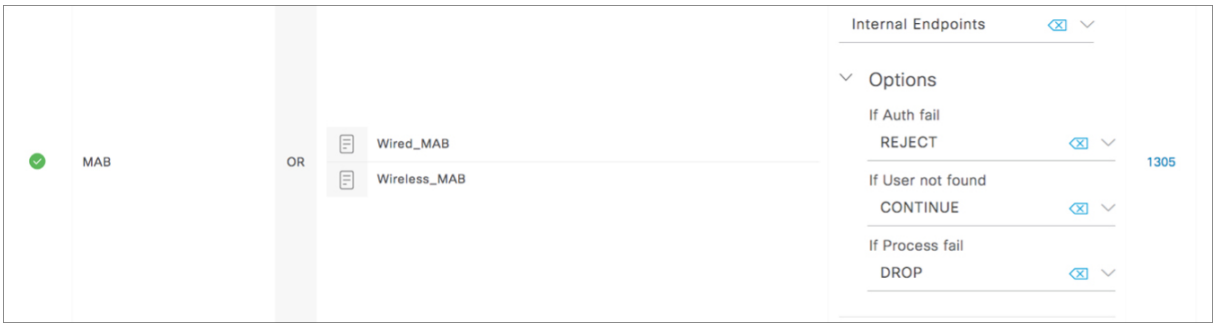
[CoA Type] ドロップダウンリストから [Reauth] を選択します。



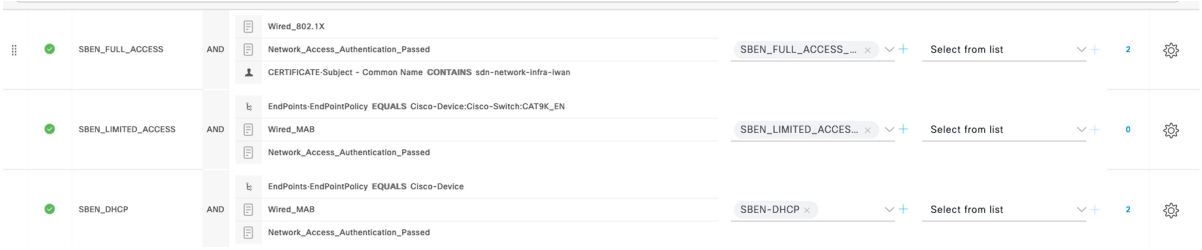
ステップ 5 [Authorization Policy] ウィンドウで認証ポリシーを定義します。

a) Cisco ISE ホームページから、**[Policy]** > **[Policy Sets]** > **[Default]** > **[Authorization Policy]**を選択します。

b) デフォルト MAB ポリシーの [If User not found] フィールドが [CONTINUE] オプションに設定されていることを確認します。



c) [Authorization Policy] ウィンドウで、サプリカントデバイスの認証ポリシーを構成し、ポリシーを以前に作成した認証プロファイル（SBEN-DHCP、SBEN_LIMITED_ACCESS_AUTHZ、SBEN_FULL_ACCESS_AUTHZ）に関連付けます。



ポートチャネルの設定

単一のエンティティとして機能するようにバンドルされたポートのグループは、ポートチャネルと呼ばれます。ファブリックエッジと、拡張ノードやサーバーなどリモート接続されたデバイスとの間のポートチャネルでは、接続の復元力と帯域幅が増加します。

ポート チャネルの作成

認証が [Closed Authentication] の場合にのみ、次の手順を実行します。

（注） 他の認証モードでは、次の手順は自動化されています。

ステップ 1 メニューアイコン（☰）をクリックして、**[Provision]** > **[Fabric Sites]**。

ステップ 2 [SUMMARY] で、ファブリックサイトの数を示す数字をクリックします。

ステップ 3 ファブリックサイトを選択します。

ステップ 4 [Fabric Infrastructure] タブで、ファブリックエッジノードをクリックします。

ステップ 5 スライドインペインの [Port Channel] タブで、[Create Port Channel] をクリックします。

ステップ 6 [Connected Device Type] ドロップダウンから、接続済みのデバイスのタイプを選択します。

- ファブリックエッジノードと拡張ノードの間または 2 つの拡張ノードの間にポートチャネルを作成する場合は、[Extended Node] を選択します。
- 片側にファブリックエッジノードまたは拡張ノードがあり、反対側にサードパーティデバイスまたはサーバーポートがあるポートチャネルを作成するには、[Trunk] を選択します。

ステップ 7 新しいポートチャネルの説明を [Description] に入力します。

ステップ 8 プロトコルを選択します。

- Cisco IOS XE リリース 16.12.1s および以前のリリースを実行する拡張ノードの場合は、プロトコルとして [On] を選択します。
- Cisco IOS XE リリース 17.1.1s および以降のリリースを実行する拡張ノードの場合は、プロトコルとして [Port Aggregation Protocol (PAgP)] を選択します。
- [Link Aggregation Control Protocol (LACP)] を拡張ノードのプロトコルとして選択しないでください。LACP モードでは、トランクポートまたはサーバーポートのみを接続できます。

ステップ 9 表示されたポートの一覧から、バンドルするポートを選択します。

（注） LACP モードで接続されたポートチャネルには、16 を超えるメンバーを含めることはできません。

PAgP モードで接続されたポートチャネルには 8 つを超えるメンバーを含めることはできません。

ステップ 10 [Done] をクリックします。

ポートチャネルの更新

始める前に

ポートチャネルを更新する前に、少なくとも 1 つのメンバーインターフェイスが存在することを確認します。

ステップ 1 メニューアイコン（☰）をクリックして、**[Provision]** > **[Fabric Sites]**。

ステップ 2 [SUMMARY] で、ファブリックサイトの数を示す数字をクリックします。

ステップ 3 ファブリックサイトを選択します。

ステップ 4 [Fabric Infrastructure] タブで、ファブリックエッジノードをクリックします。

ステップ 5 スライドインペインで、[Port Channel] タブをクリックします。

ステップ 6 表示されるポートチャネルのリストから、更新するポートチャネルをクリックします。

結果のウィンドウに、選択したポートチャネルのすべてのインターフェイスとステータスが表示されます。

ステップ 7 ポートチャネルを更新します。

ポートチャネルにインターフェイスを追加したり、ポートチャネルの既存のインターフェイスを削除したりできます。

ステップ 8 [Done] をクリックします。

ポートチャネルの削除

ステップ 1 メニューアイコン（☰）をクリックして、**[Provision]** > **[Fabric Sites]**。

ステップ 2 [SUMMARY] で、ファブリックサイトの数を示す数字をクリックします。

ステップ 3 ファブリックサイトを選択します。

ステップ 4 [Fabric Infrastructure] タブで、ファブリックエッジノードをクリックします。

ステップ 5 スライドインペインで、[Port Channel] タブをクリックします。

[Port Channel] ビューには、既存のポートチャネルがすべて一覧表示されます。

ステップ 6 ポートチャネルの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 7 プロンプトで [Yes] をクリックします。

マルチキャスト

マルチキャスト トラフィックは、次のような異なる方法で転送されます。

- ランデブー ポイントを使用した共有ツリー経由。この場合、PIM SM が使用されます。
- 最短パス ツリー（SPT）経由。PIM Source Specific Multicast（SSM）では SPT だけが使用されます。PIM SM は、受信側が接続しているエッジ ルータで送信元が認識されると SPT に切り替わります。

『IP マルチキャスト ルーティング テクノロジーの概要（IP Multicast Technology Overview）』を参照してください。

マルチキャストの設定

Cisco DNA Center には、仮想ネットワークでグループ通信またはマルチキャストトラフィックを有効にするためのワークフローが用意されています。このワークフローでは、ネットワークでのマルチキャスト実装（ネイティブマルチキャストまたはヘッドエンドレプリケーション）を選択することもできます。

（注） ボーダーがマルチサイト リモート ボーダーとして機能する仮想ネットワークでマルチキャストを有効にすることができます。このような仮想ネットワークでマルチキャストを設定すると、継承された仮想ネットワークにすでにセグメントが含まれている場合は、継承された仮想ネットワークのデバイスにもマルチキャストが設定されます。継承された仮想ネットワークにセグメントがない場合、マルチキャストは、最初のセグメントが作成された後にのみ展開されます。仮想ネットワークとその継承ネットワークが同じタイプのマルチキャスト実装を展開していることを確認してください。継承された仮想ネットワークのエッジノードデバイスをランデブーポイント（RP）として設定することはできません。

ステップ 1 メニューアイコン（☰）をクリックして、[Workflows] > [Configure Multicast] の順に選択します。
ステップ 2 タスクの概要ウィンドウが表示されたら、[Let's Do It] をクリックして、ワークフローに直接移動します。
ステップ 3 [Select a site to enable multicast] ウィンドウで、ドロップダウンリストから [Site] を選択します。
ステップ 4 [Enabling Multicast] ウィンドウで、ネットワークのマルチキャスト実装方式を次の中から選択します。

- **Native Multicast**
- **Head-end replication**

ステップ 5 [Virtual Networks] ウィンドウで、マルチキャストを設定する仮想ネットワークを選択します。

（注） 継承された仮想ネットワークを選択してマルチキャストを設定することはできません。

ステップ 6 [Multicast pool mapping] ウィンドウで、[IP Pools] ドロップダウンリストから IP アドレスプールを選択します。選択した IP アドレスプールは、選択した仮想ネットワークに関連付けられます。

ステップ 7 [Select multicast type] ウィンドウで、実装するマルチキャストのタイプを選択します。

- **SSM**（送信元特定マルチキャスト）
- **ASM**（任意の固有のマルチキャスト）

ステップ 8 次の手順を実行します。

a) [SSM] を選択した場合は、仮想ネットワークごとに IP グループの範囲を追加して、SSM リストを設定します。仮想ネットワークに複数の IP グループ範囲を追加できます。

1. 225.0.0.0 ～ 239.255.255.255 の IP グループ範囲を選択します。
2. IP グループの [Wildcard Mask] を入力します。

b) [ASM] の選択時に、RP のタイプ（内部または外部）を選択します。

ステップ 9 ランデブーポイントを設定するには、次の手順を実行します。

内部ランデブーポイントを設定する場合は、次のようにします。

a) 内部ランデブーポイントとして設定する必要があるデバイスを選択します。選択した 2 番目のランデブーポイントは、冗長ランデブーポイントになります。**[次へ (Next)]** をクリックします。
b) 一覧表示されている各仮想ネットワークに内部ランデブーポイントを割り当てます。

外部ランデブーポイントを設定する場合は、次のようにします。

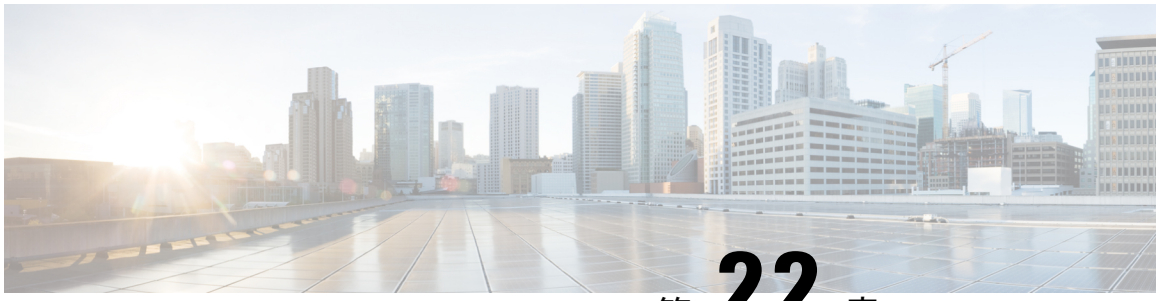
a) [Setup your External RP] ウィンドウで、外部ランデブーポイントの IPv4 または IPv6 アドレスを入力します。

（オプション）2 番目の IPv4 または IPv6 アドレスのセットを入力します。

b) [Select which RP IP Address(es) to utilize] ウィンドウで、各仮想ネットワークの IP アドレスを選択します。

ステップ 10 設定を送信する前に、[Summary] ウィンドウに表示されているマルチキャスト設定を確認し、必要に応じて変更します。

[Finish] をクリックして、マルチキャストの設定を完了します。



第 22 章

サービスのプロビジョニング

アプリケーション

ここでは、アプリケーションについて説明します。

アプリケーションの可視性について

アプリケーション可視性サービスを使用すると、組み込みアプリケーション、カスタムアプリケーション、およびアプリケーションセットを管理できます。

アプリケーション可視性サービスは、Cisco DNA Center 内でアプリケーションスタックとしてホストされているため、特定のデバイスでコントローラベースのアプリケーション認識（CBAR）機能を有効にして、数千のネットワークと自社製のアプリケーションおよびネットワークトラフィックを分類することができます。

次のパッケージをインストールします。

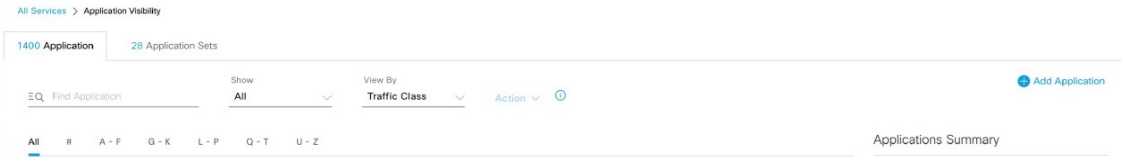
- [Application Policy]：キャンパスやブランチ内の LAN、WAN、およびワイヤレスで QoS ポリシーを自動化できます。
- [Application Registry]：アプリケーションとアプリケーションセットを表示、管理、および作成できます。
- [Application Visibility Service]：Network-Based Application Recognition（NBAR）および CBAR の技術を使用してアプリケーションを分類できます。

NBAR は、Cisco Catalyst 9000 デバイスでの最大 450 のインターフェイスのプロビジョニングをサポートしています。Cisco DNA Center のアプリケーション可視性は、この 450 インターフェイスの制限を超えません。

パッケージは必要に応じて任意にインストールできます。

（注） 互換性を確保するには、上記のパッケージのパッケージバージョンが同じである必要があります。

アプリケーションレジストリ、またはアプリケーションレジストリとアプリケーションポリシーの両方をインストールした場合、メニューアイコン（☰）をクリックして **[Provision]** > **[Services]** > **[Application Visibility]** を選択したときに、[Application] と [Application Sets] のタブが表示されます。



アプリケーションレジストリとアプリケーション可視性サービス、またはアプリケーションレジストリ、アプリケーションポリシー、およびアプリケーション可視性サービスをインストールした場合は、メニューアイコン（☰）をクリックして **[Provision]** > **[Services]** > **[Application Visibility]** を選択したときに、[Applications]、[Application Sets]、および [Discovered Applications] のタブが表示されます。

アプリケーション可視性サービスには、次のフェーズがあります。

- Day 0：初回サービスの有効化。
- Day N：継続的なモニターリングと設定の変更。

アプリケーションの可視性サービスを有効にする Day 0 セットアップウィザード

Day 0 セットアップウィザードに従って、Cisco DNA Center でアプリケーションの可視性サービスを有効にします。

ステップ 1 メニューアイコン（☰）をクリックして、**[Provision]** > **[Services]** > **[Application Visibility]** の順に選択します。

アプリケーションの可視性サービスの簡潔な概要を表示できます。

ステップ 2 [Application Visibility] ページで [Next] をクリックします。

アプリケーションの可視性サービスを有効にするためのポップアップウィンドウが表示されます。ポップアップウィンドウで [Yes] をクリックして、Cisco DNA Center で CBAR を有効にします。

ステップ 3 （オプション）[Enable CBAR on all Ready Devices] チェックボックスをオンにするか、[CBAR Readiness Status] が [Ready] 状態のデバイスを選択します。

CBAR を有効にする準備ができていないデバイスを選択する場合は、情報メッセージに従って [Ready] 状態に移行してからセットアップウィザードに進みます。

ステップ 4 [Next] をクリックして、デバイスで CBAR を有効にします。

ステップ 5 （オプション）Microsoft Office 365 クラウドコネクタなどの外部の信頼できるソースを選択すると、未分類のトラフィックの分類や、改善された署名の作成に役立ちます。

ステップ 6 [完了（Finish）] をクリックします。

[Overview] ページには、アプリケーションレジストリ、デバイス認識方式、デバイスの CBAR の準備状況、過去 2、24、または 48 時間にネットワークで観察されたアプリケーション（CBAR が少なくとも 1 つのデバイスで有効になっている場合にのみ有効）、サービス正常性、および CBAR 正常性スコアのクイックビューが表示されます。

Day-N アプリケーションの可視性ビュー

[Day-N Application Visibility] ページには、アプリケーションレジストリ、デバイス認識方式、デバイスの CBAR の準備状況、過去 2、24、または 48 時間にネットワークで観察されたアプリケーション（CBAR が少なくとも 1 つのデバイスで有効になっている場合にのみ有効）、および CBAR 正常性のクイックビューが表示されます。

次の表に、[プロビジョニング（Provision）] > [サービス（Services）] > [アプリケーションの可視性（Application Visibility）] の [概要（Overview）] タブに表示される情報を示します。

表 *45 : [Day-N Application Visibility]* ビュー：チャート

グラフ	説明
レジストリ内のアプリケーション	このチャートには、Cisco DNA Center アプリケーションレジストリ内のアプリケーションのうち、アプリケーションポリシーで使用できるアプリケーションの数が表示されます。アプリケーションは次のように分類されます。 • [Custom]：ユーザーによって追加されたアプリケーション • [Built-in]: インストールされているアプリケーション Cisco DNA Center • [Discovered]：さまざまな認識方法で検出され、アプリケーションレジストリにインポートされたアプリケーション
ネットワークで確認されたアプリケーション	このチャートには、過去 2 時間、24 時間、または 48 時間に観察されたアプリケーションが表示され、ネットワークトラフィック率が最も高いアプリケーションが一覧表示されます。 （注） このチャートには、CBAR が有効なデバイスでのみ観察されたアプリケーションが表示されます。
アクティブな認識方法によるデバイス	このチャートには、各アプリケーション認識方式によって分類されたデバイスの数が表示されます。 • CBAR 対応デバイス：ルータとスイッチ • NBAR ベースのデバイス：ルータ、スイッチ、シスコ ワイヤレス コントローラ、および Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ • IP/ポートベースのデバイス：スイッチ • サポートされていないデバイス：上記のいずれの方式でもサポートされていないデバイス

グラフ	説明
CBAR 準備状況ステータス	このチャートには、各 CBAR の準備状況ステータスのデバイス数が表示されます。 • [Enabled]：CBAR が有効になっているデバイス • [Ready]：CBAR を有効にする準備が整っているデバイス （注） [Ready] ステータスの横にある情報アイコンは、それぞれのデバイスがワイヤレス対応であることを示しています。 • [Not Ready]：CBAR をサポートしているが、いくつかの問題により CBAR を有効にする準備ができていないデバイス • [Not Supported]：CBAR をサポートしていないデバイス
Service Health and CBAR Health	このウィジェットには、すべての CBAR 対応デバイスのサービス正常性と平均正常性スコアが表示されます。デバイスに未処理のエラーまたは警告がない場合、そのデバイスは正常です。 CBAR 正常性スコアは、すべての CBAR 対応デバイスで計算されます。 各 CBAR 対応デバイスの CBAR 正常性を確認できます。0% の CBAR 正常性スコアは、デバイスに少なくとも 1 つのエラー（P1）があることを示します。50% の CBAR 正常性スコアは、デバイスにエラーはないが、少なくとも 1 つの警告（P2）があることを示します。100% の CBAR 正常性スコアは、正常なデバイスを示します。 このウィジェットには、サービスの問題と修復（P1、P2、および P3）も表示されます。緑色のチェックマークは、正常なサービスを示します。赤色の X マークは、少なくとも 1 つの P1 の問題を示します。警告アイコンは、少なくとも 1 つの P2 の問題を示します。P1、P2、および P3 をクリックすると、サービスの問題と修復についての詳細が表示されます。
CBAR 正常性の問題と修復	すべての問題は、次のように優先順位によって分類されます。 • エラー（P1） • 警告（P2） • その他 （P3） [P1]、[P2]、および [P3] タブをクリックすると、デバイスの問題と修復の詳細が表示されます。

[Site Devices Table]：このテーブルには、デバイスの情報とステータスが表示されます。[Quick Filter] および [Device Table Filter] を使用して、デバイスをフィルタ処理できます。

表 *46 : [Day-N Application Visibility]* ビュー：*[Site Devices Table]*

カラム	説明
[Device Name]	デバイスの名前。デバイス名をクリックして、CBAR サービスのステータスを表示します。
[Management IP]	デバイスの IP アドレス。
デバイス タイプ	ルータ、スイッチとハブ、ワイヤレス コントローラなど、関連するデバイスのグループ。
Site	デバイスに割り当てられているサイト。
ファブリック	デバイスが割り当てられているファブリック ドメイン。
ロール（Role）	スキャン プロセス中に、検出された各デバイスに割り当てられているロール。デバイス ロールは、ネットワーク内での役目と配置に従って、デバイスを識別およびグループ分けするために使用されます。Cisco DNA Center でデバイス ロールを特定できない場合、デバイス ロールは不明に設定されます。
アクティブな認識方法	デバイス認識方式（CBAR、NBAR、IP/Port、または Not supported）が表示されます。
[OS Version]	デバイスで現在実行されている Cisco IOS ソフトウェア。
CBAR 準備状況ステータス	[CBAR Readiness Status] 列に表示されているステータスにカーソルを合わせると、対応策メッセージが表示されます。
プロトコルパックバージョン	デバイスにインストールされているプロトコルパックの現在のバージョンと、プロトコルパックの更新ステータスが表示されます。
デバイス レジストリ ステータス	デバイスとアプリケーション レジストリとの同期ステータスが表示されます。情報アイコンまたはエラーアイコンにカーソルを合わせると、同期ステータスに関する詳細が表示されます。
展開ステータス	CBAR の展開ステータスが表示されます。
サービス正常性ステータス	[Service Health Status] 列の [Issues] をクリックすると、[CBAR Service Status] ページが開きます。このページには、問題の完全なリストとデバイスのサービス ステータス情報が表示されます。Cisco Catalyst 9K デバイスの名前をクリックすると、CBAR サービスのフットプリント（サービス負荷、CPU、フロー）を確認できます。

カラム	説明
Application QoS Policy	デバイスに適用されているアプリケーションポリシー。シスコ ワイヤレス コントローラに複数のアプリケーションポリシーがある場合は、適用されているアプリケーションポリシーの数と適用されているすべてのアプリケーションポリシーの名前が表示されます。
WAN インターフェイス	WAN インターフェイスの数が表示されます。[WAN interface details] をクリックすると、デバイスの WAN 接続設定が表示されます。

アプリケーションおよびアプリケーション セット

アプリケーションは、ネットワーク内で使用されているソフトウェアプログラムまたはネットワーク シグナリング プロトコルです。Cisco DNA Center は、約 1400 の異なるアプリケーションから成る Cisco Next Generation Network-Based Application Recognition（NBAR2）ライブラリの全アプリケーションをサポートしています。

アプリケーションは、アプリケーションセットと呼ばれる論理グループに分類されています。アプリケーションセットには、ポリシー内でのビジネスとの関連性を割り当てることができます。

アプリケーションは、同様のトラフィック処理要件が規定されている RFC 4594 の定義に従い、業界標準ベースのトラフィッククラスにマッピングされています。トラフィッククラスでは、割り当てられているビジネスとの関連性グループに基づいて、アプリケーショントラフィックに適用される処理（Differentiated Services Code Point（DSCP）マーキング、キューイング、破棄など）を定義します。

Cisco DNA Center に含まれていない追加のアプリケーションがある場合は、カスタム アプリケーションとして追加して、アプリケーション セットに割り当てることができます。

単方向と双方向のアプリケーション トラフィック

一部のアプリケーションは、完全な左右対称であり、接続の両端に同一の帯域幅プロビジョニングを必要とします。このようなアプリケーションのトラフィックを、双方向のトラフィックと呼びます。たとえば、100 kbps の低遅延キューイング（LLQ）が一方向の音声トラフィックに割り当てられている場合、逆方向の音声トラフィックにも 100 kbps の LLQ をプロビジョニングする必要があります。このシナリオは、同じ Voice over IP（VoIP）コーダ/デコーダ（コーデック）が両方の方向で使用されており、マルチキャスト保留音（MOH）のプロビジョニングが考慮されていないことが前提となっています。ただし、ストリーミングビデオやマルチキャスト MoH などの特定のアプリケーションは、ほとんどの場合、単方向です。したがって、ブランチからキャンパスに向かう方向のトラフィックフローでは、ブランチルータでこのようなトラフィック向けの帯域幅保証をプロビジョニングするのは、不要であるばかりか非効率的となる可能性があります。

Cisco DNA Center では、アプリケーションが特定のポリシーに関して単方向か双方向かを指定できます。

スイッチおよびワイヤレスコントローラでは、NBAR2 やカスタムアプリケーションがデフォルトで単方向となっています。ただし、ルータでは、NBAR2 アプリケーションはデフォルトで双方向です。

カスタム アプリケーション

カスタムアプリケーションは、Cisco DNA Center に追加するアプリケーションです。カスタムアプリケーションの横にはオレンジ色のバーが表示され、標準 NBAR2 アプリケーションおよびアプリケーション セットと区別されます。有線デバイスについては、サーバー名、IP アドレスとポート、または URL に基づいてアプリケーションを定義できます。Cisco AireOS コントローラではなく、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラに対してカスタムアプリケーションを定義できます。

IP アドレスとポートに従ってアプリケーションを定義する場合は、DSCP 値とポート分類を定義することもできます。

設定プロセスを簡素化するために、類似のトラフィックおよびサービスレベル要件を持つ別のアプリケーションに基づいてアプリケーションを定義できます。Cisco DNA Center は、他のアプリケーションのトラフィック クラス設定を、定義しているアプリケーションにコピーします。

Cisco DNA Center は、カスタムアプリケーションの一部として定義される場合でも、ポート番号 80、443、53、5353、および 8080 の ACL を設定しません。カスタム アプリケーションでトランスポート IP が定義されている場合、Cisco DNA Center はデバイス上のアプリケーションを設定します。

（注） ポリシーが展開されているときにデバイス上のカスタムアプリケーションをプログラムする場合は、そのカスタム アプリケーションを、ポリシーで定義されているいずれかのアプリケーション セットに割り当てる必要があります。

検出されたアプリケーション

検出されるアプリケーションには、Infoblox DNS サーバーなどの推奨されるカスタマイズからインポートされたアプリケーションと、推奨される未分類のアプリケーションフローからインポートされたアプリケーションがあります。

未分類のトラフィックには、CBAR 対応デバイスで識別されるフローからのトラフィックのうち、NBAR エンジンでは認識されないフローからのトラフィックが含まれます。このような場合、意味のあるビットレートを持つアプリケーションが未分類として報告され、Cisco DNA Center でインポートしてアプリケーションとして使用することができます。

アプリケーション可視性サービスでは、Cisco DNA Center を Microsoft Office 365 クラウドコネクタなどの外部の信頼できるソースに接続して、未分類のトラフィックを分類したり、改善されたシグニチャを生成したりできます。

（注） Microsoft Office 365 クラウドコネクタを設定する前に、NBAR クラウドコネクタを設定する必要があります。

検出されたアプリケーションはアプリケーションレジストリにインポートされます。

お気に入りのアプリケーション

Cisco DNA Center では、他のすべてのアプリケーションよりも先に設定するアプリケーションにフラグを付けることができます。お気に入りとしてアプリケーションにフラグを付けることで、デバイス上のお気に入りのアプリケーションに対して QoS ポリシーが設定されていることを確認できるようにします。詳細については、リソースが制限されているデバイスの処理順（652 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と、お気に入りのアプリケーションとしてマークされます。

お気に入りとしてマークできるアプリケーションの数に制限はありませんが、お気に入りのアプリケーションをごく少数にとどめると（たとえば、25 未満）、ネットワークデバイスの TCAM（Ternary Content Addressable Memory）が限られている展開で、お気に入りのアプリケーションがビジネス関連の観点から正しく処理されるようになります。

お気に入りのアプリケーションは、ビジネス関連のグループまたはトラフィック クラスに属させることが可能で、ポリシー単位ではなくシステム全体で設定されます。たとえば、お気に入りとして cisco-jabber-video アプリケーションにフラグを付けた場合、そのアプリケーションはすべてのポリシーでお気に入りのフラグが付きます。

ビジネス関連のアプリケーションだけでなく、ビジネスに関係のないアプリケーションにもお気に入りのフラグを付けられることに注意してください。たとえば、ネットワーク上に大量の望ましくない Netflix トラフィックがある場合、Netflix にお気に入りのアプリケーションとしてフラグを付けることができます（Netflix がビジネスに関係のないアプリケーションとして割り当てられている場合でも可能）。この場合、Netflix は、その他のビジネスに関係のないアプリケーションより先にデバイスポリシーに組み込まれるようになり、このアプリケーションを制御するビジネス上の目的が確実に実現されます。

アプリケーションおよびアプリケーション セットの設定

次のサブセクションでは、アプリケーションとアプリケーションセットのコンテキストで実行できるさまざまなタスクについて説明します。

（注） 編集または削除できるのは、カスタムアプリケーションと検出されたアプリケーションだけです。また、一度に編集または削除できる数は、カスタムアプリケーションと検出されたアプリケーションの合計で最大 100 個までです。編集または削除する対象として NBAR アプリケーションを選択した場合、選択した NBAR アプリケーションの数を除く、編集または削除が可能なアプリケーションの数を示す通知メッセージが表示されます。

アプリケーション設定の変更

既存の NBAR アプリケーション、カスタムアプリケーション、検出されたアプリケーションのアプリケーションセットやトラフィッククラスを変更できます。

ステップ 1 メニューアイコン（☰）をクリックして、**[Provision]** > **[Services]** > **[Application Visibility]** > **[Application]** の順に選択します。

ステップ 2 [Search]、[Show]、または [View By] フィールドを使用して、変更するアプリケーションを見つけます。

名前、ポート番号、およびトラフィッククラスに基づいてアプリケーションを検索できます。

ステップ 3 [アプリケーション名（Application Name）] をクリックします。

ステップ 4 ダイアログボックスで、1 つまたは両方の設定を変更します。

- [Traffic Class]：ドロップダウンリストからトラフィッククラスを選択します。有効なトラフィック クラスは、BROADCAST_VIDEO、BULK_DATA、MULTIMEDIA_CONFERENCING、MULTIMEDIA_STREAMING、NETWORK_CONTROL、OPS_ADMIN_MGMT、REAL_TIME_INTERACTIVE、SIGNALING、TRANSACTIONAL_DATA、VOIP_TELEPHONY です。
- [Application Set]：ドロップダウンリストからアプリケーションの設定を選択します。有効なアプリケーションセットは、認証サービス、バックアップおよびストレージ、コラボレーションアプリケーション、コンシューマ ブラウジング、コンシューマ ファイル シェアリング、コンシューマゲーミング、コンシューマメディア、コンシューマ misc、コンシューマ ソーシャル ネットワーキング、データベースアプリケーション、デスクトップ仮想化、電子メール、企業 ipc、ファイル共有、一般的なブラウジング、一般的なメディア、一般的な misc、トンネリング、ローカルサービス、ネーミングサービス、ネットワーク制御、ネットワーク管理、リモートアクセス、saas アプリケーション、シグナリング、ソフトウェア開発ツール、ソフトウェアアップデート、ストリーミングメディアです。

ステップ 5 [Save] をクリックします。

サーバー名に基づくカスタム アプリケーションの作成

Cisco DNA Centerに存在しないアプリケーションがある場合、カスタム アプリケーションとして追加することができます。

ステップ 1 メニューアイコン（☰）をクリックして、**[Provision]** > **[Services]** > **[Application Visibility]** の順に選択します。

ステップ 2 [Application] タブをクリックします。

ステップ 3 [アプリケーションの追加（Add Application）] をクリックします。

ステップ 4 ダイアログボックスで、次のフィールドに必要な情報を入力します。

フィールド	説明
Application name	カスタム アプリケーションの名前。名前には、下線とハイフンも含めて最大 24 文字の英数字を指定できます。アプリケーション名で使用できる特殊文字は、下線とハイフンのみです。
Type	ユーザーがアプリケーションにアクセスする方法。サーバー経由でアクセス可能なアプリケーションの [サーバー名（Server Name）] を選択します。
サーバー名	アプリケーションをホストするサーバーの名前。
Similar to	類似するトラフィック処理要件を持つアプリケーション。オプションボタンをクリックしてこのオプションを選択し、ドロップダウンリストからアプリケーションを選択します。Cisco DNA Centerは、他のアプリケーションのトラフィッククラスを、定義しているアプリケーションにコピーします。
トラフィッククラス	アプリケーションが属するトラフィック クラス。有効な値は BULK_DATA、TRANSACTIONAL_DATA、OPS_ADMIN_MGMT、NETWORK_CONTROL、VOIP_TELEPHONY、MULTIMEDIA_CONFERENCING、MULTIMEDIA_STREAMING、BROADCAST_VIDEO、REAL_TIME_INTERACTIVE、および SIGNALING です。
アプリケーションセット	アプリケーションを配置するアプリケーションセット。有効なアプリケーションセットは、認証サービス、バックアップおよびストレージ、コラボレーションアプリケーション、コンシューマブラウジング、コンシューマ ファイル シェアリング、コンシューマゲーミング、コンシューマメディア、コンシューマ misc、コンシューマ ソーシャル ネットワーキング、カスタムアプリケーション、データベースアプリケーション、デスクトップ仮想化、電子メール、企業 ipc、ファイル共有、一般的なブラウジング、一般的なメディア、一般的な misc、トンネリング、ローカルサービス、ネーミングサービス、ネットワーク制御、ネットワーク管理、リモートアクセス、saasアプリケーション、シグナリング、ソフトウェア開発ツール、ソフトウェアアップデート、ストリーミングメディアです。

ステップ 5 [OK] をクリックします。

IP アドレスおよびポート ベースのカスタム アプリケーションの作成

Cisco DNA Centerに存在しないアプリケーションがある場合、カスタム アプリケーションとして追加することができます。

ステップ 1 メニューアイコン（☰）をクリックして、**[Provision]** > **[Services]** > **[Application Visibility]** の順に選択します。

ステップ 2 [Application] タブをクリックします。

ステップ 3 [アプリケーションの追加（Add Application）] をクリックします。

ステップ 4 [Application Name] フィールドに、アプリケーションの名前を入力します。名前には、下線とハイフンも含めて最大 24 文字の英数字を指定できます。アプリケーション名で使用できる特殊文字は、下線とハイフンのみです。

ステップ 5 [種類（Type）] エリアで、[サーバー IP/ポート（Server IP/Port）] ラジオボタンをクリックして、アプリケーションが IP アドレスとポートを通じてアクセスできます。

ステップ 6 [DSCP] チェックボックスをオンにして、DSCP 値を定義します。値を定義しない場合のデフォルト値は [Best Effort] です。ベストエフォートサービスとは原則的に、いずれの QoS も適用されないネットワークデバイスのデフォルト動作です。

ステップ 7 [IP/Port Classifiers] チェックボックスをオンにして、アプリケーションの IP アドレスおよびサブネット、プロトコル、ポートまたはポート範囲を選択します。有効なプロトコルは、[IP]、[TCP]、[UDP]、[TCP/UDP] です。[IP] プロトコルを選択した場合は、ポート番号または範囲は定義しません。＋をクリックして、さらに分類子を追加します。

ステップ 8 次のいずれかの方法を使用して、アプリケーショントラフィック処理要件を定義します。

- [Similar To]：お使いのアプリケーションに既存のアプリケーションと同様のトラフィック処理要件がある場合は、[Similar To] オプションボタンをクリックし、ドロップダウンリストからアプリケーションを選択します。Cisco DNA Center は、他のアプリケーションのトラフィッククラスを、定義しているアプリケーションにコピーします。
- [Traffic Class]：アプリケーションに定義するトラフィッククラスがわかっている場合は、[Traffic Class] オプションボタンをクリックし、ドロップダウンリストからトラフィッククラスを選択します。有効な値は BULK_DATA、TRANSACTIONAL_DATA、OPS_ADMIN_MGMT、NETWORK_CONTROL、VOIP_TELEPHONY、MULTIMEDIA_CONFERENCING、MULTIMEDIA_STREAMING、BROADCAST_VIDEO、REAL_TIME_INTERACTIVE、および SIGNALING です。

ステップ 9 [Application Set] ドロップダウンリストから、アプリケーションが属するアプリケーションセットを選択します。有効なアプリケーションセットは、認証サービス、バックアップおよびストレージ、コラボレーションアプリケーション、コンシューマブラウジング、コンシューマファイルシェアリング、コンシューマゲーミング、コンシューマメディア、コンシューマ misc、コンシューマ ソーシャル ネットワーキング、カスタムアプリケーション、データベース アプリケーション、デスクトップ仮想化、電子メール、企業 ipc、ファイル共有、一般的なブラウジング、一般的なメディア、一般的な misc、トンネリング、ローカルサービス、ネーミングサービス、ネットワーク制御、ネットワーク管理、リモートアクセス、saas アプリケーション、シグナリング、ソフトウェア開発ツール、ソフトウェアアップデート、ストリーミングメディアです。

ステップ 10 [OK] をクリックします。

URL に基づくカスタム アプリケーションの作成

Cisco DNA Centerに存在しないアプリケーションがある場合、カスタム アプリケーションとして追加することができます。

ステップ 1 メニューアイコン（☰）をクリックして、**[Provision]** > **[Services]** > **[Application Visibility]** の順に選択します。

ステップ 2 [Application] タブをクリックします。

ステップ 3 [アプリケーションの追加（Add Application）] をクリックします。

[アプリケーションの追加（Add Application）] ダイアログボックスが表示されます。

ステップ 4 [アプリケーション名（Application Name）] フィールドに、アプリケーションの名前を入力します。名前には、下線とハイフンも含めて最大 24 文字の英数字を指定できます。（アプリケーション名で使用できる特殊文字は、下線とハイフンのみです。）

ステップ 5 **タイプ**については、[**URL**] オプションボタンをクリックします。

ステップ 6 [**Url**] フィールドに、アプリケーションに到達するために使用する url を入力します。

ステップ 7 トラフィック クラスの設定:

- 同様のトラフィック処理要件を持つ別のアプリケーションと同じトラフィッククラスを使用するには、オプションボタンをクリックして、ドロップダウンリストからアプリケーションを選択します。
- トラフィッククラスを指定するには、[**トラフィッククラス (Traffic class)**] オプションボタンをクリックし、ドロップダウンリストからトラフィッククラスを選択します。有効な値は BULK_DATA、TRANSACTIONAL_DATA、OPS_ADMIN_MGMT、NETWORK_CONTROL、VOIP_TELEPHONY、MULTIMEDIA_CONFERENCING、MULTIMEDIA_STREAMING、BROADCAST_VIDEO、REAL_TIME_INTERACTIVE、および SIGNALING です。

ステップ 8 [**アプリケーションセット (Application set)**] ドロップダウンリストから、アプリケーションを配置するアプリケーションセットを選択します。

ステップ 9 [OK] をクリックします。

カスタム アプリケーションの編集または削除

必要な場合は、カスタム アプリケーションを変更または削除できます。

（注） アプリケーション ポリシーによって直接参照されているカスタム アプリケーションを削除することはできません。通常、アプリケーションポリシーはアプリケーションセットを参照し、個々のアプリケーションを参照しません。ただし、ポリシーにアプリケーションの特別な定義（コンシューマまたはプロデューサの割り当てや双方向の帯域幅プロビジョニングなど）が設定されている場合、ポリシーはそのアプリケーションを直接参照します。そのため、アプリケーションを削除する前に、特別な定義を削除するか、またはアプリケーションへの参照を削除する必要があります。

ステップ 1 メニューアイコン（☰）をクリックして、**[Provision]** > **[Services]** > **[Application Visibility]** の順に選択します。

ステップ 2 [Application] タブをクリックします。

ステップ 3 [Search]、[Show]、または [View By] フィールドを使用して、変更するアプリケーションを見つけます。

名前、ポート番号、およびトラフィッククラスに基づいてアプリケーションを検索できます。

ステップ 4 アプリケーションを編集するには、次の手順を実行します。

a) アプリケーション名をクリックして、必要な変更を行います。フィールドの詳細については、サーバー名に基づくカスタム アプリケーションの作成（560 ページ）、IP アドレスおよびポート ベースのカスタム アプリケーションの作成（562 ページ）、またはURL に基づくカスタム アプリケーションの作成（563 ページ）を参照してください。

b) [OK] をクリックします。

（注） ポリシーを再展開しても、編集したカスタムアプリケーションは再設定されません。Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ

ステップ 5 アプリケーションを削除するには、アプリケーションボックスにある 🗑 をクリックし、次に [OK] をクリックして確定します。

アプリケーションをお気に入りにする

アプリケーションをお気に入りとしてマークして、アプリケーションの QoS 設定を、他のアプリケーションの QoS 設定の前にデバイスに展開する必要あることを指定できます。お気に入りとしてマークされたアプリケーションには、その横に黄色の星が付いています。

ポリシーを追加または編集すると、お気に入りとしてマークされたアプリケーションがアプリケーションセットの上部に表示されます。

アプリケーションは、個々のポリシーベースではなくシステム全体で設定されます。詳細については、「お気に入りのアプリケーション （559 ページ）」を参照してください。

ステップ 1 メニューアイコン（☰）をクリックして、**[Provision]** > **[Services]** > **[Application Visibility]** の順に選択します。

ステップ 2 [Application] タブをクリックします。
ステップ 3 お気に入りとしてマークするアプリケーションを特定します。
ステップ 4 スターアイコンをクリックします。

カスタム アプリケーション設定の作成

使用したいアプリケーションセットがない場合、カスタム アプリケーション セットを作成できます。

ステップ 1 メニューアイコン（☰）をクリックして、**[Provision]** > **[Services]** > **[Application Visibility]** の順に選択します。
ステップ 2 [Application Sets] タブをクリックします。
ステップ 3 [Add Application Set] をクリックします。
ステップ 4 ダイアログ ボックスに、新しいアプリケーション設定の名前を入力します。

Cisco DNA Center で新しいアプリケーションセットが作成されますが、アプリケーションは含まれません。

ステップ 5 [OK] をクリックします。
ステップ 6 [Search] を使用して [Show] または [View By] フィールドを使用して、アプリケーション設定を見つけます。

名前、ポート番号、およびトラフィッククラスに基づいてアプリケーションを検索できます。

ステップ 7 新しいアプリケーション設定に移動させるアプリケーションを見つけます。
ステップ 8 移動させるアプリケーションの横にあるチェック ボックスをオンにします。
ステップ 9 新しいアプリケーション設定にアプリケーションをドラッグ アンド ドロップします。

カスタム アプリケーション セットの編集または削除

必要な場合は、カスタム アプリケーションを変更または削除できます。

（注） アプリケーション ポリシーによって参照されているカスタム アプリケーション セットを削除することはできません。アプリケーション セットを削除する前に、ポリシーからアプリケーション セットを削除する必要があります。

ステップ 1 メニューアイコン（☰）をクリックして、**[Provision]** > **[Services]** > **[Application Visibility]** の順に選択します。
ステップ 2 Click the **APplication Sets** tab.
ステップ 3 [検索（Search）]、[表示（Show）]、または [表示方法（View By）] フィールドを使用して、変更するアプリケーション セットを見つけます。

名前、ポート番号、およびトラフィッククラスに基づいてアプリケーションを検索できます。

ステップ 4 次のいずれかを実行します。

- アプリケーション設定するには、アプリケーション設定に、またはアプリケーション設定からアプリケーションをドラッグアンドドロップします。[OK]をクリックして、それぞれの変更を確定します。
- アプリケーション設定を削除するには、アプリケーション設定ボックスにある をクリックし、次に [OK] をクリックして確定します。

CBAR 対応デバイスでのプロトコルパックの更新

CBAR をサポートする任意のデバイスのプロトコルパックを最新または特定のプロトコルパックにアップグレードできます。

始める前に

- [System Settings] で Cisco ログイン情報を設定します。シスコのログイン情報の設定に関する詳細については、『Cisco DNA Center Administrator Guide』を参照してください。
- デバイスは CBAR をサポートしている必要があります。
- デバイスで CBAR が有効になっている必要があります。
- デバイスのプロトコルパックは cisco.com で使用可能である必要があります。

ステップ 1 メニューアイコン（≡）をクリックして、**[Provision]** > **[Services]** > **[Application Visibility]** の順に選択します。

ステップ 2 Day-N の [Overview] ページで、下にスクロールして、[Site Devices] テーブルを表示します。

ステップ 3 [Site Devices] テーブルの [Protocol Pack Version] カラムに表示されているステータスを確認します。

[Outdated] ステータスをクリックすると、[Update Protocol Pack] ウィンドウに該当するプロトコルパックのリストが表示されます。

ステップ 4 [Update Protocol Pack] ウィンドウで、必要なプロトコルパックのバージョンに対応する [Update] をクリックします。

[Protocol Pack Version] カラムに [In progress] ステータスが表示されます。現在更新中のバージョンを表示するには、情報アイコンをクリックします。[Protocol Pack Version] カラムに [Update failed] ステータスが表示されたら、エラーアイコンをクリックして失敗の原因を確認します。

ステップ 5 すべてのデバイスまたは選択したデバイスを最新のプロトコルパックに更新する場合は、次の手順を実行します。

該当するすべての CBAR 対応デバイスでプロトコルパックを更新するには、次のようにします。

- [Update Protocol Pack] ドロップダウンリストから、[All Devices] を選択し、後続の警告ポップアップウィンドウで [Yes] をクリックします。

選択したデバイスでプロトコルパックを更新するには、次のようにします。

- [Site Devices] テーブルでデバイスを選択します。
- [Update Protocol Pack] ドロップダウンリストから、[Selected Devices] を選択し、後続の警告ポップアップウィンドウで [Yes] をクリックします。

未分類アプリケーションの検出

Cisco DNA Center のアプリケーション可視性サービスは、分類済みと未分類のドメインおよびソケットに関する情報をデバイスから取得し、その情報を [Observed Traffic] チャートに表示します。アプリケーション可視性サービスによって検出された未分類のサーバー名と IP/ポートの数は、[Recommendations] の下に表示されます。

未分類のサーバー名と IP/ポートはアプリケーションレジストリに追加できます。

（注） 最大 1100 の検出されたアプリケーションをアプリケーションレジストリに追加できます。

ステップ 1 メニューアイコン（☰）をクリックして、**[Provision]** > **[Services]** > **[Application Visibility]** の順に選択します。

ステップ 2 [Discovered Applications] タブをクリックします。

ステップ 3 [Recommendations] の下の [discovered server names] リンクまたは [discovered IP/Ports] リンクをクリックします。

表に、未分類の検出されたサーバーまたはIP/ポートのリストが表示されます。表内で選択したサーバーまたは IP/ポートを非表示にする場合は、サーバーを選択して [Hide Ignored Applications] チェックボックスをオンにします。

ステップ 4 アプリケーションレジストリでアプリケーションとしてインポートするサーバーまたはIP/ポートを選択します。

ステップ 5 ドロップダウンリストから、必要な [Application]、[Application Set]、および [Traffic Class] を選択します。

ステップ 6 [Import] をクリックします。

ステップ 7 [Applications] タブをクリックし、**[Show]** > **[Discovered]** を選択して、インポートされたアプリケーションを確認します。

NBAR クラウドコネクタの設定

アプリケーション可視性サービスでは、NBAR クラウドコネクタを使用してプロトコルパックを拡充し、クラウドからデータを送受信することによって不明なアプリケーションの可視性を強化します。

ステップ 1 メニューアイコン（☰）をクリックして、**[Provision]** > **[Services]** > **[Application Visibility]** の順に選択します。

ステップ 2 [Discovered Applications] タブをクリックします。

ステップ 3 [NBAR Cloud] ウィンドウで、[Configure] をクリックします。

ステップ 4 [Configure NBAR Cloud] ウィンドウで、トグルボタンをクリックして状態を [Enable] にします。

ステップ 5 [Cisco API Console] リンクをクリックして、キーとクライアントシークレットを取得します。

ステップ 6 Cisco ログイン情報を入力して新しいブラウザタブで [Cisco API Console] を開き、次の手順を実行します。

a) [My Apps & Keys] タブで、[Register a New App] をクリックします。

b) [Register an Application] 画面の次のフィールドに入力します。

- [Name of Your Application]：アプリケーション名を入力します。
- [OAuth2.0 Credentials]：[Client Credentials] チェックボックスをクリックします。
- [Select APIs]：[Hello API] チェックボックスをクリックします。

c) [Register] をクリックします。

登録したアプリケーションの詳細が [My Apps & Keys] タブに表示されます。

d) 登録したアプリケーションのキーとクライアントシークレットを [Cisco API Console] からコピーします。

ステップ 7 [Configure NBAR Cloud] で、次のようにフィールドを設定します。

a) [Client ID] フィールドに、前の手順で [My Apps & Keys] タブからコピーしたキーを入力します。

b) [Client Secret] フィールドに、前の手順で [My Apps & Keys] タブからコピーしたクライアントシークレットを入力します。

c) [Organization Name] フィールドに、組織名を入力します。

d) [Improve my network using NBAR Cloud telemetry] 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（デフォルトではオンになっています）。

e) [NBAR classification telemetry data is being sent to region] で、目的のロケーションを選択します。

ステップ 8 [Save] をクリックします。

アプリケーション可視性サービスのサポート： Cisco DNA トラフィック テレメトリ アプライアンス

Cisco DNA トラフィック テレメトリ アプライアンスは、ミラーリングされた IP ネットワーク トラフィックからエンドポイントテレメトリを生成し、エンドポイントの可視性とセグメンテーションのために Cisco DNA Center とテレメトリデータを共有します。

Cisco DNA トラフィック テレメトリ アプライアンスで CBAR を有効にするための前提条件には、次のものが含まれます。

- デバイスをサイトに割り当てる必要があります。
- デバイスロールを [Distribution] モードに設定する必要があります。

QoS ポリシーを設定せずに、Cisco DNA トラフィック テレメトリ アプライアンス で属性セットとマップを使用してカスタムアプリケーションを設定することができます。詳細については、アプリケーション ポリシーの作成（660 ページ）およびアプリケーション ポリシーの展開（666 ページ）を参照してください。

Infoblox アプリケーションの検出

Cisco DNA Center を組織の Infoblox DNS サーバーと統合して、未分類のトラフィックをサーバー名に基づいて解決することができます。

始める前に

- バージョン 1.5 以降の Infoblox WAPI が必要です。Infoblox WAPI のバージョンを確認するには、Infoblox サーバーにログインし、**[Help]** > **[Documentation]** > **[WAPI Documentation]** の順に選択します。
- 少なくとも読み取り専用権限を持つロールを作成し、そのロールを Infoblox ユーザーに割り当てます。詳細については、『Cisco DNA Center Administrator Guide』の「Manage Users」を参照してください。

ステップ 1 メニューアイコン（☰）をクリックして、**[Provision]** > **[Services]** > **[Application Visibility]** の順に選択します。

ステップ 2 [Discovered Applications] タブをクリックします。

ステップ 3 [Infoblox DNS Server] の [Configure] をクリックします。

ステップ 4 [Infoblox Connector Settings] ウィンドウで [Here] リンクをクリックして、Cisco DNA Center で IPAM/DNS サーバーのログイン情報を設定します。

ステップ 5 IPAM の設定を行います。詳細については、『Cisco DNA Center Administrator Guide』の「Configure an IP Address Manager」を参照してください。

ステップ 6 [Infoblox Connector Settings] に戻り、次の設定を行います。

- [All DNS Zones] チェックボックスをオンにするか、[DNS Zones to Inspect] ドロップダウンリストから必要な DNS ゾーンを選択します。ドロップダウンリストには、Infoblox サーバーで定義されている DNS ゾーンが表示されます。
- [Inspect] ドロップダウンリストから必要な検査レコードを選択します。
- [Read Application name from] チェックボックスをオンにし、[Extensible Attribute] または [AVC RRTYPE format] のいずれかのオプションボタンをクリックします。[Extensible Attribute] オプションボタンをクリックした場合は、わかりやすいアプリケーション名を含む拡張機能属性名を入力します。
- [Default Traffic Class] から、Infoblox アプリケーションを分類するためのデフォルトのトラフィッククラスを選択します。
- [Default Application Set] から、Infoblox アプリケーションを分類するためのデフォルトのアプリケーションセットを選択します。

ステップ 7 **[保存（Save）]** をクリックします。

[Poll Infoblox to Import Applications] リンクが [Recommendations] の下に表示されます。

ステップ 8 [Poll Infoblox to Import Applications] リンクをクリックして、[Infoblox Connector Settings] で設定した DNS ゾーンからアプリケーションのリストを取得します。

ステップ 9 インポートするアプリケーションを選択し、次の手順を実行します。

- アプリケーションの名前が Infoblox サーバーで定義された名前と異なる場合は、アプリケーション名を編集します。
- [Infoblox Connector Settings] に定義されているデフォルトのアプリケーションセットとトラフィッククラスを変更する場合は、ドロップダウンリストから必要なアプリケーションセットとトラフィッククラスを選択します。

ステップ 10 [Import] をクリックします。

ステップ 11 [Applications] タブをクリックして [Show] ドロップダウンリストから [Discovered] を選択し、インポートされた Infoblox アプリケーションを確認して必要に応じて編集します。

アプリケーションのインポート後にアプリケーションのサーバー名を変更すると、[Infoblox Discovered Applications] ウィンドウの [Application Status] 列に、アプリケーションのステータスが [Updated] と表示されます。[Application Status] 列に表示されるアプリケーション名は、アプリケーションの新しいサーバー名です。アプリケーションの古いサーバー名を表示するには、情報アイコンをクリックします。

Microsoft Office 365 クラウドコネクタを使用した未分類トラフィックの解決

Cisco DNA Center は、Microsoft Office 365 クラウドコネクタなどの外部の信頼できるソースに接続して、未分類のトラフィックを分類するか、または改善された署名を生成できるようにします。

始める前に

- Cisco DNA Center がインターネットに接続していることを確認します。
- NBAR クラウドが有効になっていることを確認します。

ステップ 1 メニューアイコン（☰）をクリックして、**[Provision]** > **[Services]** > **[Application Visibility]** の順に選択します。

ステップ 2 [Discovered Applications] タブをクリックします。

ステップ 3 [MS Office 365 Cloud] トグルボタンをクリックして、MSFT シグニチャのポーリングを有効にします。

- Microsoft Office 365 コネクタを有効にすると、コントローラは Microsoft Office 365 から新しいドメインの情報のインポートを開始し、新しいドメインに適したアプリケーションを検出します。
- 新しいセカンダリパックは、Cisco DNA Centerベースのプロトコルパックとともにインストールされ、新しいドメインが自動的にサポートされます。

検出されたアプリケーションの編集と削除

必要に応じて、検出されたアプリケーションを編集または削除できます。

ステップ 1 メニューアイコン（☰）をクリックして、**[Provision]** > **[Services]** > **[Application Visibility]** の順に選択します。

ステップ 2 [Application] タブをクリックします。

ステップ 3 [Search]、[Show]、[View By] のいずれかのフィールドを使用して、変更する検出済みのアプリケーションを見つけます。

名前、ポート番号、およびトラフィッククラスに基づいてアプリケーションを検索できます。

ステップ 4 アプリケーションを編集するには、次の手順を実行します。

a) アプリケーション名をクリックして、必要な変更を行います。

検出済みのアプリケーションの場合、[Attribute Set] と [Traffic Class] のみを編集できます。

b) [OK] をクリックします。

ステップ 5 アプリケーションを削除するには、アプリケーションのボックスで 🗑 をクリックし、[OK] をクリックします。

アプリケーション ホスティング

ここでは、アプリケーション ホスティングについて説明します。

アプリケーション ホスティングについて

アプリケーション ホスティングを使用すると、Cisco DNA Centerによって管理されているデバイス上のサードパーティ製アプリケーションのライフサイクルを管理できます。Cisco IOS-XE ソフトウェアバージョン 16.12.1s 以降を実行している Cisco Catalyst 9300 シリーズ スイッチ、Cisco IOS-XE ソフトウェアバージョン 17.3.1 以降を実行している Cisco Catalyst 9100 シリーズ アクセスポイント、および Cisco IOS-XE ソフトウェアバージョン 17.1 以降を実行している Cisco Catalyst 9400 シリーズ スイッチでサードパーティ製 Docker アプリケーションをホストできます。

（注） Cisco DNA Centerでは、ホストされるアプリケーションに割り当てられるディスク容量は5 GBに制限されています。

アプリケーション ホスティング サービス パッケージのインストールと更新

始める前に

SUPER-ADMIN-ROLE 権限を持つユーザのみがこの手順を実行することができます。

ステップ 1 メニューアイコン（☰）をクリックして、**[System]** > **[Software Updates]**。または、クラウドアイコンをクリックし、[Go to Software Updates] リンクをクリックします。

ステップ 2 [Software Updates] ウィンドウで、次のタブを確認します。

- [Updates]：システムとアプリケーションの更新が表示されます。[System Update] では、インストールされているシステムのバージョンと、Cisco Cloud からダウンロードされ、利用可能なシステムの更新が表示されます。[Application Updates] は、Cisco Cloud からダウンロードしてインストールできる使用可能なアプリケーション、アプリケーションのサイズ、適切なアクション（**ダウンロード**、**インストール**、または**更新**）を示します。パッケージにカーソルを合わせると、使用可能なバージョンと基本的な説明が表示されます。
- [Installed Apps]：現在インストールされているアプリケーションパッケージが示されます。

ステップ 3 アプリケーション ホスティング パッケージをダウンロードするには、**[Updates]** > **[Application Updates]** でアプリケーション ホスティングの名前の横にある [Install] をクリックします。

ステップ 4 アプリケーション ホスティング パッケージを更新するには、**[Updates]** > **[Application Updates]** でアプリケーション ホスティングの名前の横にある [Update] をクリックします。

ステップ 5 [Installed Apps] タブでバージョンを調べて、アプリケーションが更新されていることを確認します。

（注） アプリケーション ホスティング サービス パッケージをインストールしたら、いったん Cisco DNA Center からログアウトしてブラウザのキャッシュをクリアし、再度 Cisco DNA Center にログインする必要があります。

アプリケーション ホスティングの前提条件

Cisco Catalyst 9000 デバイスでアプリケーション ホスティングを有効にするには、次の前提条件を満たしている必要があります。

- ディスカバリの前に、デバイスの NETCONF ポートを設定します。
- アプリケーションをホストするスイッチでセキュア HTTP サーバーを設定します。
- スイッチ上の HTTPS ユーザー認証用にローカル認証サーバーまたは AAA 認証サーバーを設定します。ユーザー名およびパスワードは特権レベル 15 で設定する必要があります。
- Cisco Catalyst 9300 シリーズ スイッチが Cisco IOS XE 16.12.x 以降のバージョンを実行し、Cisco Catalyst 9400 シリーズ スイッチが Cisco IOS XE 17.1.x 以降のバージョンを実行していることを確認します。
- デバイスに着脱可能な USB SSD 外部ストレージがあることを確認します（9300 ファミリのスイッチの場合のみ）。
- スイッチ上の設定が正しいことを確認します。スイッチで WebUI を開き、HTTPS ユーザーとしてログインします。

  次の例は、スイッチの動作設定を示しています。

```
prompt# sh run | sec http
ip http server
ip http authentication local
ip http secure-server
ip http max-connections 16
ip http client source-interface Loopback0
```

  17.3.3 より前のリリースの Cisco IOS XE を搭載するスイッチの追加設定：

```
ip http secure-active-session-modules dnac
ip http session-module-list dnac NG_WEBUI
ip http active-session-modules none
```

  Cisco IOS XE 17.3.3 以降のスイッチの追加設定：

```
ip http secure-active-session-modules webui
ip http session-module-list webui NG_WEBUI
ip http session-module-list pki OPENRESTY_PKI
ip http active-session-modules pki
```

- Cisco DNA Center で、デバイスを手動で追加するときに HTTPS ログイン情報を設定します。アプリケーション ホスティングには、HTTPS ユーザー名、パスワード、およびポート番号が必須です。デフォルトのポート番号は443です。デバイスログイン情報を編集することもできます。ネットワーク デバイス クレデンシャルの更新（103 ページ）を参照してください。すでに管理されているデバイスを編集する場合は、インベントリでそのデバイスを再同期してから、アプリケーション ホスティング関連のアクションに使用します。

（注） アプリケーション ホスティングの HA は、3 ノードの Cisco DNA Center クラスタではサポートされていません。

アプリケーションをホストするデバイスの準備状況の表示

スイッチにアプリケーションをインストールする前に、Cisco Catalyst 9300 シリーズ スイッチのアプリケーションをホスティングするための準備状況を確認する必要があります。

ステップ 1 メニューアイコン（≡）をクリックして、**[Provision]** > **[Services App]** > **[Hosting for Switches]** の順に選択します。

ステップ 2 [All Devices] をクリックします。

ステップ 3 アプリケーションをホストできるデバイスのリストが表示されます。[App Hosting Status] は、デバイスがアプリケーションをホストするための準備状況を示します。[See Details] をクリックして、デバイスで実行された準備状況チェックのリストを表示します。

アプリケーションの追加

シスコパッケージまたは Docker アプリケーションを追加できます。

始める前に

- [Cisco Package]：IOS SDK ツールを使用してアプリケーションをパッケージ化し、アプリケーションが IOS XE オペレーティングシステムと互換性を持つようにする必要があります。
- [Docker]：Docker イメージを tar ファイルとして保存する必要があります。Docker イメージを tar ファイルとして保存するには、次のコマンドを入力します。

```
docker save -o <path for generated tar file> <image name:tag>
Example: docker save -o alpine-tcpdump.tar itsthenetwork/alpine-tcpdump:latest
```

ステップ 1 メニューアイコン（≡）をクリックして、**[Provision]** > **[Services App]** > **[Hosting for Switches]** の順に選択します。

ステップ 2 [New Application] をクリックします。

ステップ 3 ドロップダウンリストからアプリケーションとカテゴリを選択します。

ステップ 4 [Select] をクリックして、アップロードするアプリケーションを選択します。

ステップ 5 [Upload] をクリックします。

新しく追加されたアプリケーションは、[App Hosting] ページで確認できます。

ThousandEyes Enterprise Agent アプリケーションの自動ダウンロード

ThousandEyes Enterprise Agent アプリケーションを使用すると、ネットワークをモニターし、内部、外部、キャリア、およびインターネットネットワーク全体のネットワーク トラフィック パスをリアルタイムで監視できます。ThousandEyes Enterprise Agent アプリケーションの利点は、Cisco DNA Center アプリケーション ホスティング サービスにこのアプリケーションを手動でインポートする必要がないことです。ネットワークでスイッチおよびハブが有効になっている場合、アプリケーション ホスティング サービスの開始から 10 分以内に、ThousandEyes Enterprise Agent アプリケーションが自動的にダウンロードされます。アプリケーションを手動でダウンロードするには、ThousandEyes Enterprise Agent .tar ファイルへの次のリンクをクリックします。

thousandeyes-enterprise-agent.cat9k.tar

インターネット接続がない場合は、次のコマンドを使用してコンソールからプロキシ接続を設定できます。

```
magctl service setenv app-hosting http_proxy <proxy-value>
```

ThousandEyes Enterprise Agent アプリケーションに接続するプロキシ値を設定します。

アプリケーションの更新

Cisco DNA Center で追加されたアプリケーションを更新できます。

ステップ 1 メニューアイコン（☰）をクリックして、**[Provision]** > **[Services App]** > **[Hosting for Switches]** の順に選択します。

使用可能なアプリケーションは、[App Hosting] ウィンドウで確認できます。

ステップ 2 更新するアプリケーションを選択します。

ステップ 3 [Update App] をクリックします。

ステップ 4 アップロードする新しいバージョンのアプリケーションを選択します。

ステップ 5 [Upload] をクリックします。

アプリケーションの起動

Cisco DNA Center でアプリケーションを起動できます。

ステップ 1 メニューアイコン（≡）をクリックして、**[Provision]** > **[Services App]** > **[Hosting for Switches]** の順に選択します。

ステップ 2 アプリケーションを選択し、[Manage] をクリックして、アプリケーションを使用するデバイスを表示します。

ステップ 3 起動するアプリケーションがあるデバイスを選択します。

ステップ 4 [Actions] ドロップダウンリストから [Start App] を選択します。

アプリケーションの停止

Cisco DNA Center でアプリケーションを停止できます。

ステップ 1 メニューアイコン（≡）をクリックして、**[Provision]** > **[Services App]** > **[Hosting for Switches]** の順に選択します。

ステップ 2 アプリケーションを選択し、[Manage] をクリックして、アプリケーションを使用するデバイスを表示します。

ステップ 3 停止するアプリケーションがあるデバイスを選択します。

ステップ 4 [Actions] ドロップダウンリストから [Stop App] を選択します。

デバイスでホストされているアプリケーションの表示

始める前に

前提条件を満たします。詳細については、「アプリケーションホスティングの前提条件」を参照してください。

ステップ 1 メニューアイコン（≡）をクリックして、**[Provision]** > **[Services App]** > **[Hosting for Switches]** の順に選択します。

ステップ 2 すべてのデバイスを表示するには、右上隅の [All Devices] をクリックします。特定のアプリケーションを使用するデバイスのみを表示するには、アプリケーションを選択して [Manage] をクリックします。

（注）
- すべてのデバイスを表示することを選択した場合、[All Devices] ページには、アプリケーションをホストできるデバイスに関する情報（[Hostname]、[IP Address]、[Image Version]、[App Hosting Status]、[Last Updated]）が表示されます。
- 特定のアプリケーションのデバイスのリストを表示することを選択した場合、[Devices]ページには、アプリケーションをホストできるデバイスに関する次の情報（**ホスト名**、**デバイス IP**、**アプリケーションバージョン**、**アプリケーションステータス**、**最終検知プラットフォームバージョン**、および**アクションステータス**）が表示されます。

ステップ 3 [Devices] ページで [Summary] をクリックすると、デバイス上で失敗または停止したアプリケーション、および実行中のアプリケーションの概要が表示されます。

ステップ 4 アプリケーションでアクションを実行するには、[Action] ドロップダウンリストをクリックし、[Start]、[Stop]、[Edit]、[Upgrade]、または [Uninstall] を選択します。

ステップ 5 インストールされているホスティング アプリケーションを表示するデバイスリンクをクリックします。

[Applications]ページには、インストールされているアプリケーションの**名前**、**バージョン**、**アプリケーションステータス**、**モニタリング アプリケーション**、**正常性**、および**詳細情報**が表示されます。

（注） **モニタリングアプリケーション**には、アプリケーションモニタリングダッシュボードへのリンクが含まれています。このリンクは、the, Cisco DNA Center application package controller, .yaml ファイルで提供されます。このファイルにアプリケーション ダッシュボード URL が含まれていない場合、この**モニタリングアプリケーション**の列（[Monitor App]）は適用されません。

ステップ 6 [Details] 列で [View] をクリックすると、デバイスのアプリケーションステータスに関する詳細情報が表示されます。

[App Details] ウィンドウには、アプリケーションの**リソース**、**ネットワーク**、および **Docker ランタイムオプション**情報が表示されます。

ステップ 7 特定のアプリケーションのログをダウンロードするには、アプリケーションを選択して [Application Logs] をクリックします。

ステップ 8 デバイスからテクニカルサポートをダウンロードするには、[Tech Support logs] をクリックします。

Cisco Catalyst 9300 デバイスへのアプリケーションのインストール

Cisco DNA Center Cisco Catalyst 9300 シリーズ スイッチにアプリケーションをインストールできます。

始める前に

- 前提条件を満たします。詳細については、「アプリケーション ホスティングの前提条件（573 ページ）」を参照してください。
- アプリケーションを Cisco DNA Center に追加します。詳細については、「アプリケーションの追加 （574 ページ）」を参照してください。

- アプリケーションをホストするためのスイッチの準備状況を確認します。詳細については、「アプリケーションをホストするデバイスの準備状況の表示（574 ページ）」を参照してください。

ステップ 1 メニューアイコン（☰）をクリックして、**[Provision]** > **[Services App]** > **[Hosting for Switches]** の順に選択します。

ステップ 2 アプリケーションを選択し、[Install] をクリックします。

ステップ 3 [Get Started] ウィンドウで、[Task Name] フィールドにワークフローの一意の名前を入力し、[Next] をクリックします。

ステップ 4 [Select Site] ウィンドウで、アプリケーションを有効にするサイトを選択し、[Next] をクリックします。

ステップ 5 [Select Switches] ウィンドウで、アプリケーションのインストール先デバイスを選択し、[Next] をクリックします。

ステータスが [Ready] および [Partially Ready] のデバイスを選択できます。[See Details] をクリックして、デバイスで実行された準備状況チェックのリストを表示します。

[Partially Ready] ステータスのデバイスの場合は、[Readiness Check] ページの [Check Now] リンクをクリックして、HTTPS ログイン情報を検証します。

[Devices] テーブルに目的のデバイスがない場合は、[Import] をクリックして CSV ファイルからデバイスを追加します。

ステップ 6 [Configuration App] ウィンドウで、以降の設定を実行します。

- **[Network Settings]**：
  - [Select Network] ドロップダウンリストをクリックし、アプリケーションを設定する VLAN を選択します。
  - [Address Type] ドロップダウンリストをクリックし、[Static] または [Dynamic] を選択します。[Static] を選択した場合は、サムネイルアイコンをクリックして、アプリケーションの [IP Address]、[Gateway]、[Prefix/Mask]、および [DNS] を入力します。
- [App Resources]：[Allocate all resources available on a device] または [Customize resource allocation] チェックボックスをオンにします。[Customize resource allocation] チェックボックスをオンにすると、[CPU]、[Memory]、および [Persistent Storage] の最大値を低い値に変更できます。
- [Custom Settings]：シスコ パッケージ アプリケーションにのみ適用されます。アプリケーションによって指定された属性の設定の詳細を入力します。
- [App Data]：アプリケーション固有のファイルを参照してアップロードします。必要なアプリケーション固有のファイルを特定するには、関連するアプリケーションのドキュメントを参照してください。
- [Docker Runtime Options]：アプリケーションに必要な Docker ランタイムオプションを入力します。

ステップ 7 [Next] をクリックし、[Summary] ウィンドウでアプリケーション設定を確認します。

ステップ 8 （任意） [Configuration Preview] をクリックし、選択したデバイスに設定をプッシュするために使用される設定テンプレートを確認します。

ステップ 9 [Provision] をクリックします。

ステップ 10 確認ウィンドウで [Yes] をクリックして、選択したデバイスでのアプリケーションのインストールを完了します。

次のタスク

アプリケーションをインストールすると、デバイスの Cisco IOS-XE 設定も変更されます。実行中の設定に対するこの変更は、ルータのリロード後にアプリケーションが期待どおりに機能するように、スタートアップ設定にコピーする必要があります。アプリケーションのインストールが完了したら、[Template Editor] を使用して実行中の設定をスタートアップ設定にコピーします。

Cisco Catalyst 9300 デバイスからのアプリケーションのアンインストール

Cisco Catalyst 9300 シリーズ スイッチからアプリケーションをアンインストールできます。

ステップ 1 メニューアイコン（☰）をクリックして、**[Provision]** > **[Services App]** > **[Hosting for Switches]** の順に選択します。

ステップ 2 アプリケーションを選択し、[Manage] をクリックして、アプリケーションを使用するデバイスを表示します。

ステップ 3 アンインストールするアプリケーションがあるデバイスを選択します。

ステップ 4 [Actions] ドロップダウンリストから [Uninstall App] を選択します。

Cisco Catalyst 9300 デバイスでのアプリケーション構成の編集

Cisco Catalyst 9300 シリーズ スイッチでアプリケーションを稼働させるための設定が必要な場合は、アプリケーション設定を編集できます。

ステップ 1 メニューアイコン（☰）をクリックして、**[Provision]** > **[Services App]** > **[Hosting for Switches]** の順に選択します。

ステップ 2 アプリケーションを選択し、[Manage] をクリックして、アプリケーションを使用するデバイスを表示します。

ステップ 3 編集するアプリケーションがあるデバイスを選択します。

ステップ 4 [Actions] ドロップダウンリストから、[Edit App Config] を選択します。

アプリケーションの削除

Cisco DNA Center からアプリケーションを削除できます。

始める前に

アプリケーションを使用しているすべてのデバイスからアプリケーションをアンインストールする必要があります。詳細については、Cisco Catalyst 9300 デバイスからのアプリケーションのアンインストール （579 ページ）を参照してください。

ステップ 1 メニューアイコン（☰）をクリックして、**[Provision]** > **[Services App]** > **[Hosting for Switches]** の順に選択します。

ホストされている削除可能なアプリケーションは、[App Hosting] ウィンドウで確認できます。

ステップ 2 削除するアプリケーションを選択します。

ステップ 3 [Delete Application] をクリックします。

ステップ 4 確認ダイアログボックスで、[OK] をクリックします。

アプリケーションが削除されるのは、Cisco DNA Center によって管理されているいずれのデバイスでも使用されていない場合のみです。

それ以外の場合、エラーメッセージに、アプリケーションを使用しているデバイスの数が表示されます。確認ダイアログボックスで [Cancel] をクリックし、アプリケーションをアンインストールします。詳細については、Cisco Catalyst 9300 デバイスからのアプリケーションのアンインストール （579 ページ）を参照してください。

アプリケーションログのダウンロード

アプリケーションログは Cisco DNA Center からダウンロードできます。

ステップ 1 メニューアイコン（☰）をクリックして、**[Provision]** > **[Services]** > **[IoT Services]** の順に選択します。

ステップ 2 [All Devices] をクリックします。

アプリケーションをホストできるデバイスのリストが表示されます。

ステップ 3 [APp logs] をクリックして、Cisco DNA Center からアプリケーションログをダウンロードします。

ステップ 4 [App Logs] ポップアップウィンドウで、ダウンロードするアプリケーション ログ ファイルを選択し、[Download] をクリックします。

デバイス テクニカル サポート ログのダウンロード

トラブルシューティングを行うために、Cisco DNA Center からデバイスのテクニカルサポートのログをダウンロードできます。

ステップ 1 メニューアイコン（☰）をクリックして、**[Provision]** > **[Services]** > **[IoT Services]** の順に選択します。

ステップ 2 [All Devices] をクリックします。

アプリケーションをホストできるデバイスのリストが表示されます。

ステップ 3 [Tech Support logs] をクリックして、デバイスのテクニカルサポートログをダウンロードします。

Cisco Catalyst 9100 シリーズ アクセス ポイントでのアプリケーション ホスティング

ここでは、Cisco Catalyst 9100 シリーズ アクセス ポイントでのアプリケーション ホスティングについて説明します。

Cisco Catalyst アクセスポイントでのアプリケーションホスティングについて

仮想環境への移行により、再利用可能なポータブルかつスケーラブルなアプリケーションを構築する必要性が高まりました。アプリケーションのホスティングによって、管理者には独自のツールやユーティリティを利用するためのプラットフォームが与えられます。ネットワークデバイスでホスティングされているアプリケーションは、さまざまな用途に利用できます。これは、既存のツールのチェーンによる自動化から、設定管理のモニタリング、統合に及びます。

アプリケーション ホスティングを使用すると、Cisco DNA Center によって管理されているデバイス上のサードパーティ製アプリケーションのライフサイクルを管理できます。このリリースでは、Cisco IOS-XE ソフトウェアバージョン 17.3 以降を搭載した Cisco Catalyst 9100 シリーズ アクセスポイントでサードパーティ製 SES-imagotag IoT Connector アプリケーションを利用できます。

Cisco Catalyst 9100 シリーズ アクセスポイントの SES-imagotag IoT Connector は、あらゆる Electronic Shelf Label（ESL）通信に対応しています。

Cisco Catalyst 9100 シリーズ アクセス ポイントでの USB のインストールと管理のアプリケーション ホスティング ワークフロー

始める前に

デバイスでアプリケーションホスティングを有効にするには、次の前提条件を満たしている必要があります。

- Cisco Catalyst 9100 シリーズ アクセス ポイントを検出するには、NETCONF を有効にし、ポートを 830 に設定する必要があります。
- Cisco Catalyst 9100 シリーズ アクセス ポイントでは、IP が Cisco DNA Center に直接到達できることが必要です。
- Cisco Catalyst 9800 シリーズ ワイヤレス コントローラで Cisco IOS XE 17.3.x 以降のソフトウェアが実行されていることを確認します。
- Cisco DNA Center アプライアンスが最新の Cisco DNA Center ISO を実行していることを確認します。
- USB ドングルが AP に挿入されていることを確認します。これは、SES-imagotag Connector アプリケーションを実行するために必要です。

ステップ 1 Cisco Catalyst 9800 シリーズ ワイヤレス コントローラと Cisco Catalyst 9100 シリーズ アクセス ポイントのアプリケーションをホスティングするための準備状況を確認してから、アプリケーションをインストールください。

詳細については、アプリケーションをホストするデバイスの準備状況の表示 （574 ページ）を参照してください。

ステップ 2 Cisco DNA Center にアプリケーション ホスティング サービスをインストールします。

詳細については、アプリケーション ホスティング サービス パッケージのインストールと更新 （572 ページ）を参照してください。

ステップ 3 Cisco Catalyst 9800 シリーズ ワイヤレス コントローラを Cisco DNA Center に追加します。

詳細については、ネットワーク デバイスを追加 （98 ページ）を参照してください。

（注） NETCONF が有効になっていることを確認し、ポートを 830 に設定します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラが [Managed] 状態になるまで待機する必要があります。

ステップ 4 [Network Hierarchy] ウィンドウで AP をフロアに割り当てます。

詳細については、フロアマップでの AP の操作 （178 ページ）を参照してください。

ステップ 5 USB アプリケーション（SES-imagotag コネクタ）を Cisco DNA Center にアップロードします。

詳細については、アプリケーションの追加 （574 ページ）を参照してください。

ステップ 6 IoT サービスを有効にします。

詳細については、Cisco Catalyst 9100 シリーズ アクセス ポイントでの IoT サービスの有効化 （789 ページ）を参照してください。

ステップ 7 『Application Hosting on Catalyst APs Deployment Guide』の説明に従って、コンテナを設定します。
https://www.cisco.com/c/en/us/products/collateral/wireless/access-points/guide-c07-744305.html

Cisco Catalyst 9100 シリーズ アクセスポイントにインストールされているホスティング アプリケーションの表示

始める前に

前提条件を満たします。詳細については、「アプリケーション ホスティングの前提条件」を参照してください。

ステップ 1 メニューアイコン（☰）をクリックして、**[Provision]** > **[Services]** > **[IoT Services]** の順に選択します。

ステップ 2 すべてのデバイスを表示するには、右上隅の [All Devices] をクリックします。特定のアプリケーションを使用するデバイスのみを表示するには、アプリケーションを選択して [Manage] をクリックします。

（注）
- すべてのデバイスを表示することを選択した場合、[All Devices] ページには、アプリケーションをホストできるデバイスに関する情報（[Hostname]、[IP Address]、[Image Version]、[App Hosting Status]、[Last Updated]）が表示されます。
- 特定のアプリケーションのデバイスのリストを表示することを選択した場合、[Devices]ページには、アプリケーションをホストできるデバイスに関する次の情報（**ホスト名**、**デバイス IP**、**アプリケーションバージョン**、**アプリケーションステータス**、**最終検知プラットフォームバージョン**、**およびアクションステータス**）が表示されます。

ステップ 3 [Devices] ページで [Summary] をクリックすると、デバイス上で失敗または停止したアプリケーション、および実行中のアプリケーションの概要が表示されます。

ステップ 4 [Action] ドロップダウンリストをクリックして、アプリケーションを開始、停止、編集、アップグレード、およびアンインストールします。

ステップ 5 インストールされているホスティング アプリケーションを表示するデバイスリンクをクリックします。

[Applications]ページには、インストールされているアプリケーションの**名前**、**バージョン**、**アプリケーションステータス**、**IP アドレス**、**正常性**、および**詳細情報**が表示されます。

ステップ 6 [Details] 列で [View] をクリックすると、デバイスのアプリケーションステータスに関する詳細情報が表示されます。

[App Details] ウィンドウには、アプリケーションの**リソース**および**ネットワーク**情報が表示されます。

ステップ 7 アプリケーションログをダウンロードするには、アプリケーションログをダウンロードするアプリケーションを選択し、[Application Logs] をクリックします。

ステップ 8 テクニカルサポートログをダウンロードするには、テクニカルサポートログをダウンロードするアプリケーションを選択し、[Tech Support Logs] をクリックします。

Cisco Catalyst 9100 デバイスからのアプリケーションのアンインストール

Cisco Catalyst 9100 シリーズ AP からアプリケーションをアンインストールできます。

ステップ 1 メニューアイコン（☰）をクリックして、**[Provision]** > **[Services]** > **[IoT Services]** の順に選択します。

ステップ 2 アプリケーションを選択し、[Manage] をクリックして、そのアプリケーションを使用するデバイスを表示します。

ステップ 3 アンインストールするアプリケーションがあるデバイスを選択します。

ステップ 4 [Actions] ドロップダウンリストから [Uninstall App] を選択します。

Cisco Catalyst 9100 デバイスからのアプリケーションの削除

Cisco Catalyst 9100 シリーズ AP からアプリケーションを削除できます。

始める前に

アプリケーションを使用しているすべてのデバイスからアプリケーションをアンインストールする必要があります。詳細については、「Cisco Catalyst 9100 デバイスからのアプリケーションのアンインストール」を参照してください。

ステップ 1 メニューアイコン（☰）をクリックして、**[Provision]** > **[Services]** > **[IoT Services]** の順に選択します。

[IoT Services] ページで使用可能なホストされたアプリケーションを表示できます。

ステップ 2 削除するアプリケーションを選択します。

ステップ 3 [Delete Application] をクリックします。

ステップ 4 確認ダイアログボックスで、[OK] をクリックします。

アプリケーションが削除されるのは、Cisco DNA Center によって管理されているいずれのデバイスでも使用されていない場合のみです。

それ以外の場合、エラーメッセージに、アプリケーションを使用しているデバイスの数が表示されます。[Cancel] をクリックし、アプリケーションをアンインストールします。詳細については、「Cisco Catalyst 9100 デバイスからのアプリケーションのアンインストール」を参照してください。

サイト間 VPN の設定

サイト間 VPN を作成し、既存のサイト間 VPN を編集または削除できます。

サイト間 VPN の作成

この手順では、サイト間 VPN を作成する方法を示します。

始める前に

- ネットワーク階層内のサイトを定義します。ネットワーク階層の概要（155 ページ）を参照してください。
- VPN トンネルに使用する IP アドレスプールを設定します。IP アドレスプールには、少なくとも 6 つの空き IP アドレスが必要です。IP アドレス プールを設定する（241 ページ）を参照してください。

ステップ 1 メニューアイコン（☰）をクリックして、**[Provision]** > **[Site to Site VPN]**。

サイト間 VPN は、このほかに **[Workflows]** > **[Site to Site VPN]** ウィンドウからも作成できます。

ステップ 2 VPN を作成するには、[Add] をクリックします。
[Choose Your Sites] ワークフローが表示されます。

ステップ 3 [Choose Your Sites] ワークフローで、次の手順を実行します。

a) 最初のフィールドに VPN 名を入力します。

b) [Site 1] ドロップダウンリストから、最初のサイト、そのサイトのデバイス、およびそのデバイスの WAN インターフェイスを選択します。WAN インターフェイスは、デバイスがプロビジョニングされている場合はデフォルトで設定されます。

c) [Site 2] ドロップダウンリストから、2 番目のサイト、そのサイトのデバイス、およびそのデバイスの WAN インターフェイスを選択します。WAN インターフェイスは、デバイスがプロビジョニングされている場合はデフォルトで設定されます。

ステップ 4 [Select Networks] ウィンドウで、次を実行します。

a) [Tunnel IP Pool] ドロップダウンリストから、IP アドレスプールを選択します。

b) それぞれのサイトについて、使用するサブネットの横にあるチェックボックスをオンにします。

c) （オプション）サイトのカスタムネットワークを追加する場合は、下部にある [Add Custom Networks] リンクをクリックし、必要なフィールドに入力します。

ステップ 5 [Configure VPN] ウィンドウで、次の手順を実行します。

a) 暗号化の事前共有キーを入力します。

b) 必要に応じて、暗号化アルゴリズムと整合性アルゴリズムを設定します。デフォルトの設定を使用することを推奨します。設定を変更した場合にデフォルトの選択に戻すには、[Use Cisco recommended IKEV2 & Transform Set Values] チェックボックスをオンにします。

ステップ 6 [Summary] ウィンドウで、VPN 設定を確認し、変更が必要な場合は該当するセクションで [Edit] をクリックして、[Create VPN] をクリックします。

次のステータス画面では、完了した順に各ステップの横にチェックマークが表示されます。[Services] をクリックして [Site to Site VPN] ウィンドウに戻ると、新しく作成した VPN が表示されます。

サイト間 VPN の編集

ステップ 1 メニューアイコン（☰）をクリックして、**[Provision]** > **[Site to Site VPN]**。

ステップ 2 編集する VPN の横にあるチェックボックスをオンにします。

ステップ 3 リストの上方にあるメニューバーで [Edit] をクリックします。

[Summary] 画面が表示されます。

ステップ 4 VPN 設定を確認し、変更が必要な場合は該当するセクションで [Edit] をクリックします。

ステップ 5 [Edit VPN] をクリックして変更を送信します。

次のステータス画面では、完了した順に各ステップの横にチェックマークが表示されます。[Services] をクリックして [Site to Site VPN] 画面に戻ります。

サイト間 VPN の削除

ステップ 1 メニューアイコン（☰）をクリックして、**[Provision]** > **[Site to Site VPN]**。

ステップ 2 削除する VPN の横にあるチェックボックスをオンにします。

ステップ 3 リストの上方にあるメニューバーで [Delete] をクリックします。

確認のダイアログボックスが表示されます。

ステップ 4 [Yes] をクリックして、VPN を削除することを確認します。

ユーザー定義のネットワークサービスの作成

Cisco DNA Center では、[Cisco User Defined Network] サービスを、**[Provision]** > **[Service Catalog]** > **[Cisco User Defined Network]**ページから設定できます。[Configure Cisco User Defined Network] サービスは、このほかに**[Workflows]** > **[Configure Cisco UDN]**ページからも作成できます。詳細については、「Cisco ユーザー定義のネットワークの設定」の章を参照してください。

ユーザー定義のネットワークサービスのプロビジョニングステータスの確認

この手順では、Cisco ユーザー定義のネットワークサービスのプロビジョニングステータスを **[Provision]** > **[All Services]** ウィンドウから確認する方法を示します。Cisco ユーザー定義のネットワークサービスの設定が正常に完了した後に、[Configure Cisco User Defined Network] 画面で [View Provisioning Status] ボタンをクリックする方法もあります。

始める前に

Cisco ユーザー定義のネットワークサービスを **[Workflows]** > **[Configure Cisco User Defined Network]** ウィンドウから設定してプロビジョニングします。

ステップ 1 メニューアイコン（☰）をクリックして、 **[Provision]** > **[All Services]** > **[Cisco User Defined Network]** の順に選択します。

[Site Provisioning Status] ウィンドウに、サイト名、デバイス名、使用されている SSID の数、およびサイトのプロビジョニングのステータスが表示されます。

ステップ 2 [Refresh] をクリックすると、最新のプロビジョニングステータスが表示されます。

ステップ 3 サイト名をクリックすると、プロビジョニングされたデバイスについて、SSIDの名前、ユーザー定義ネットワーク（UDN）のステータス、ユニキャストトラフィックの封じ込めなどの追加の詳細が表示されます。

ステップ 4 [Activities] をクリックすると、[Scheduled Tasks] ウィンドウでスケジュールされたタスクのステータスを追跡できます。

スイッチでのテレメトリの有効化

スイッチでスイッチポートアナライザ（SPAN）およびカプセル化リモート スイッチ ポート アナライザ（ERSPAN）セッションを設定して、アプリケーション アシュアランスとエンドポイント分析のために IP トラフィックを共有することができます。

始める前に

スイッチとトラフィック テレメトリ アプライアンス（TTA）が到達可能であり、Cisco DNA Center を介して管理されていることを確認します。スイッチは、サイトに割り当てられており、デバイスロールが [Distribution] である必要があります。

ステップ 1 メニューアイコン（☰）をクリックして、**[Provision]** > **[Service Catalog]** > **[Telemetry Appliance Setup]**の順に選択します。

ステップ 2 [+ Setup] をクリックして新しいワークフローを作成します。

ステップ 3 [Get Started] ウィンドウで、ワークフロー名と説明を入力します。

ステップ 4 [Choose Source Endpoint] ウィンドウで、テレメトリアプライアンスにトラフィックを送信するデバイスを選択します。

（注） スイッチとハブは、[Distribution] ロールによって管理されるワークフローでサポートされる送信元デバイスです。

ステップ 5 [Choose Destination Endpoint] ウィンドウで、宛先エンドポイントとして TTA デバイスを選択します。

（注） リストから選択できる TTA デバイスは 1 つだけです。

ステップ 6 [Choose Type for Configuration] ウィンドウで、[SPAN] または [ERSPAN] を選択します。

ステップ 7 [Choose Mapping Between Source and Destination] ウィンドウで、次の手順を実行します。

SPAN の場合：

1. 着信トラフィックをモニタする送信元インターフェイスを選択します。
2. トラフィック テレメトリ アプライアンスが接続された、トラフィックを転送できるスイッチの宛先インターフェイスを選択します。
3. 着信トラフィックを処理するレシーバインターフェイスを選択し、分析を行います

ERSPAN の場合：

1. 着信トラフィックをモニタする送信元インターフェイスを選択します。
2. 着信トラフィックをフィルタ処理する VLAN を入力します。
3. 着信トラフィックを処理するレシーバインターフェイスを選択し、分析を行います
4. レシーバインターフェイスの宛先 IP アドレスを入力します。
5. レシーバインターフェイスの宛先ネットマスクを入力します。

ステップ 8 [Scheduler] ウィンドウで、[Now] または [Later] をクリックして、いつ構成を開始するかを指定します。

ステップ 9 [Summary] ウィンドウで設定を確認し、[Deploy] をクリックします。

ステップ 10 [View Status] をクリックして、個々のデバイスのプロビジョニングステータスを確認します。

Cisco Umbrella の設定

ここでは、Cisco Umbrella と Cisco DNA Center との統合について説明します。

Cisco Umbrella について

Cisco Umbrella の DNS レイヤセキュリティにより、最も迅速かつ簡単にネットワークのセキュリティを強化できます。セキュリティの可視性を向上させ、侵害されたシステムを検出します。脅威がネットワークやエンドポイントに到達する前に阻止することにより、あらゆるポートやプロトコルでネットワーク内外を問わずユーザーを保護します。

Cisco DNA Center は、次のデバイス上の Cisco Umbrella 設定をサポートします。

- Cisco IOS-XE ソフトウェアバージョン 16.12 以降を搭載した Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ
- Cisco Catalyst 9100 シリーズ AP
- Cisco IOS-XE ソフトウェアバージョン 17.3.1 以降を搭載した Cisco Catalyst 9200 アクセス スイッチ
- Cisco IOS-XE ソフトウェアバージョン 17.3.1 以降を搭載した Cisco Catalyst 9300 アクセス スイッチ

Cisco Umbrella のロールベース アクセス コントロールの設定

Cisco DNA Center で Cisco Umbrella を設定したり、ネットワークデバイスで Cisco Umbrella をプロビジョニングしたりするには、必要な RBAC 権限を持つ Cisco Umbrella のユーザーロールを作成する必要があります。詳細については、『Cisco DNA Center Administrator Guide』の「Manage Users」を参照してください。

表 *47 : Cisco Umbrella* の *RBAC* 権限マトリックス

機能	アクセス	権限
Cisco Umbrella の設定 Cisco DNA Center	[Network Design] > [Advanced Network Settings]	書き込み
システム 360 での Cisco Umbrella ダッシュレットの追加	[Network Design] > [Advanced Network Settings]	書き込み

機能	アクセス	権限
ネットワークデバイスでの Cisco Umbrella のプロビジョニング	[Network Provision] > [Provision]	書き込み
	[Network Design] > [Network Hierarchy]	読み取り
	[Network Provision] > [Inventory Management]	読み取り
	システム	読み取り
	[Network Provision] > [Scheduler]	書き込み
	[Network Services] > [Umbrella]	書き込み

Cisco Umbrella の設定 Cisco DNA Center

始める前に

- Cisco Umbrella アカウントを作成します。
- *login.umbrella.com* にログインし、API キー、レガシートークン、管理キー、シークレットなどの必要なキーを作成します。
- Cisco Umbrella ログイン URL の組織 ID をメモします。
- Cisco Umbrella でローカルバイパスドメインを作成します。
- Cisco DNA Center と管理しているネットワークデバイスやソフトウェアアップデートをダウンロードする Cisco cloud との間にプロキシサーバーがある場合は、プロキシサーバーへのアクセスを設定する必要があります。詳細については、『Cisco DNA Center Administrator Guide』の「Configure the Proxy」セクションを参照してください。
- Cisco DNA Center で Cisco Umbrella パッケージをインストールします。『Cisco DNA Center Administrator Guide』の「Download and Install Packages and Updates」セクションを参照してください。
- 必要な RBAC 権限を持つ Cisco Umbrella のユーザーロールを作成します。Cisco Umbrella のロールベース アクセス コントロールの設定 （589 ページ）を参照してください。

（注） IPv6 で設定された Cisco DNA Center クラスタに Cisco Umbrella パッケージをインストールすることはできません。

ステップ 1 メニューアイコン（☰）をクリックして、**[System]** > **[Settings]** > **[External Services]** > **[Umbrella]** の順に選択します。

ステップ 2 Cisco Umbrella から手動で取得した次の詳細を入力します。

- **Organization ID**
- **Network Device Registration API Key**
- **Network Device Registration Secret**
- **Management API Key**
- **Management Secret**
- **Legacy Device Registration Token**

ステップ 3 [Save] をクリックします。

Umbrella ダッシュレットの追加

[System 360] ページに [Umbrella] ダッシュレットを追加できます。[Umbrella] ダッシュレットには、Cisco DNA Center での Cisco Umbrella の構成ステータスが表示されます。

始める前に

Cisco Umbrella パッケージをインストールする必要があります。

ステップ 1 メニューアイコン（≡）をクリックして、**[System]** > **[System 360]** の順に選択します。

ステップ 2 [Actions] メニューから、[Edit Dashboard] を選択し、[Add Dashlet] をクリックします。

ステップ 3 [Umbrella Dashlet] を選択し、[Add] をクリックします。

[Umbrella] ダッシュレットが [System 360] ページの [Externally Connected Systems] に表示されます。Cisco Umbrella が Cisco DNA Center で設定されていれば、[Umbrella] ダッシュレットにステータスが [Available] と表示され、組織 ID が表示されます。

Cisco Umbrella が Cisco DNA Center で設定されていない場合は、[Configure] リンクをクリックし、**[System]** > **[Settings]** > **[External Services]** > **[Umbrella]** のフィールドに値を入力できます。Cisco Umbrella の設定 Cisco DNA Center （590 ページ）を参照してください。

Cisco Umbrella でキーが変更された場合は、[Update] リンクをクリックし、**[System]** > **[Settings]** > **[External Services]** > **[Umbrella]** のキーを更新できます。Cisco Umbrella の設定 Cisco DNA Center （590 ページ）を参照してください。

Umbrella サービス統計ダッシュボードの表示

[Umbrella Service Stats] ダッシュボードを表示するには、メニューアイコン（≡）をクリックして、**[Provision]** > **[Services]** > **[Umbrella]** の順に選択します。

ダッシュボードには、次のダッシュレットが表示されます。

- [Total Umbrella DNS Queries]：選択したサイトでブロックされた DNS クエリと許可された DNS クエリの数を示します。
- [Blocked Umbrella DNS Queries]：選択したサイトでセキュリティポリシーおよびコンテンツポリシーによってブロックされた DNS クエリの数を示します。

デフォルトでは、このダッシュレットには過去 3 時間の統計情報が表示されます。過去 24 時間または 7 日間の統計情報を表示するには、[Umbrella Service Stats] ページの左上隅にあるドロップダウンリストからその目的の時間を選択します。

ネットワークデバイスでの Cisco Umbrella のプロビジョニングの前提条件

ネットワークデバイスで Cisco Umbrella をプロビジョニングする前に、次の点を確認します。

- Cisco Umbrella が Cisco DNA Center で設定されている。
- Cisco Umbrella をプロビジョニングするデバイスについて、ワイヤレスプロビジョニングが完了している。
- SSID 設定が非ファブリックである。
- デバイスが FlexConnect モードの非ファブリック SSID として設定されている場合、AP がプロビジョニングされている。
- デバイスからダイレクト インターネット アクセスで Cisco Umbrella への接続が確立されている。
- Cisco Umbrella ルート証明書が Cisco DNA Center トラストプールで使用可能である。『Cisco DNA Center Administrator Guide』の「Configure Trustpool」を参照してください。
- デバイスの Cisco Umbrella 設定が Cisco DNA Center から設定されていない場合は、デバイスから Cisco Umbrella 設定を削除し、デバイスを Cisco DNA Center と再同期する。

ネットワークデバイスでの Cisco Umbrella のプロビジョニング

ステップ 1 メニューアイコン（☰）をクリックして、**[Workflows]** > **[Umbrella Deployment]** の順に選択します。
または、次の手順を実行します。

- メニューアイコン（☰）をクリックして、**[Provision]** > **[Umbrella]** の順に選択します。
- Cisco Umbrella を展開するサイトをネットワーク階層から選択します。
- [Select Devices] ウィンドウが表示されます。手順 4 に進んで展開ワークフローを続けます。

ステップ 2 タスクの概要ウィンドウが表示されたら、[Let's Start] をクリックして、ワークフローに直接移動します。

ステップ 3 [Choose Site] ウィンドウが表示されます。

a) 各サイトのデバイスの準備状況が次のステータスで示されます。

- [Eligible Devices]：Cisco Umbrella の構成に適格なデバイス。ネットワークデバイスでの Cisco Umbrella のプロビジョニングの前提条件 （592 ページ）を参照してください。
- [Enabled Devices]：Cisco DNA Center からすでに設定されているデバイス。

b) 展開するサイトを選択し、[Next] をクリックします。

（注） 一度に選択できるサイトは 1 つだけです。親サイトを選択すると、すべての子サイトに同時に Cisco Umbrella を展開できます。

ステップ 4 [Select Device Type] ウィンドウで、[Switches] または [Wireless Controllers] を選択します。

ステップ 5 [Select Device Type] ウィンドウで [Switches] を選択した場合は、次の手順を実行します。

a) [Select Devices] ウィンドウで、有線デバイスを選択します。

b) [Configure Interface] ウィンドウで、次の手順を実行します。

1. 設定するポートを選択し、[Define Umbrella Interfaces] をクリックします。
2. [Select Configuration] ダイアログボックスで、[Define Umbrella Interfaces] ドロップダウンリストをクリックし、[IN(LAN)]、[OUT(WAN)]、または [Disable Umbrella] を選択し、[Save] をクリックします。

（注） 次の手順に進むには、少なくとも 1 つの [IN] インターフェイスと 1 つの [OUT] インターフェイスを選択する必要があります。

c) [Define Umbrella Policy Mapping (Wired)] ウィンドウで、グローバルレベルまたはインターフェイスレベルの Umbrella ポリシーを選択します。

d) [Configure Policies for Your Devices] ウィンドウで、[IN(LAN)] インターフェイスを選択し、[Define Umbrella Policies] をクリックします。

e) [Select Policy] ダイアログボックスで、選択したインターフェイスのポリシーを選択し、[Save] をクリックします。

ステップ 6 [Select Device Type] ウィンドウで [Wireless Controllers] を選択した場合は、次の手順を実行します。

a) [Select Devices] ウィンドウで、ワイヤレスデバイスを選択します。

b) SSID を選択し、各 SSID に必要な Cisco Umbrella ポリシーを選択します。

（注）
- このページには、非ファブリック SSID のみが表示されます。
- SSID は選択し、Cisco Umbrella ポリシーは選択しない場合には、デフォルトポリシーが SSID にマッピングされます。
- 複数のポリシーを選択した場合に、ポリシーが適用される順序は、Cisco Umbrella クラウドポータルに定義されています。

c) [Umbrella Policy Association (Wireless)] ウィンドウで、SSID に適用されるデフォルトのポリシーを確認します。

SSID に関連付けられているポリシーを変更する場合は、[Cisco Umbrella] リンクをクリックします。Cisco DNA Center からの Cisco Umbrella の展開が完了すると、Cisco Umbrella コンソールにネットワーク アイデンティティが表示されます。Cisco IOS-XE ソフトウェアバージョン 16.xx を搭載したデバイスの場合、ネットワーク アイデンティティはグローバルと表示されます。Cisco IOS-XE ソフトウェアバージョンが 16.xx 以降のデバイスの場合、ネットワーク アイデンティティは、サイトと SSID 名に基づいて作成されたカスタム名として表示されます。

ステップ 7 [Review Internal Domains] ウィンドウで、内部ドメインのリストを追加または削除します。[Internal Domain] リストのドメインに一致する DNS クエリは、Cisco Umbrella ではなくローカル DNS サーバーに転送されます。

ステップ 8 [DNS Crypt] ウィンドウが表示されます。[Enable DNS Packet Encryption] オプションがデフォルトで選択されています。

a) [DNS Crypt] ウィンドウで、[Next] をクリックします。

b) DNS パケット暗号化を使用しない場合は、[Enable DNS Packet Encryption] チェックボックスをオフにします。

ステップ 9 [Summary] ウィンドウで詳細を確認し、変更が必要な場合は [Edit] をクリックし、[Deploy] をクリックします。

ステップ 10 [Schedule] ウィンドウが表示されたら、[Now] または [Later] をクリックして構成を展開する時期を指定し、[Apply] をクリックします。

ステップ 11 [Deployment] ウィンドウで、[View Status] をクリックし、[Scheduled Tasks] ウィンドウで展開ステータスを確認します。

デバイスの Cisco Umbrella 展開ステータスと Cisco Umbrella でのデバイス構成ステータスを確認できます。Cisco Umbrella の展開ログは [Audit Logs] ウィンドウでも確認できます。

（注） 組織のネットワークでの Cisco Umbrella の展開は、*login.umbrella.com* からのみモニタできます。

ネットワークデバイスでの Cisco Umbrella の無効化

ステップ 1 メニューアイコン（☰）をクリックして、**[Workflows]** > **[Umbrella Deployment]** の順に選択します。
または、次の手順を実行します。

- メニューアイコン（☰）をクリックして、**[Provision]** > **[Services]** > **[Umbrella]** の順に選択します。
- Cisco Umbrella を無効にするサイトをネットワーク階層から選択します。
- [Select Devices] ウィンドウが表示されます。手順 4 に進んで無効化ワークフローを続けます。

ステップ 2 タスクの概要ウィンドウが表示されたら、[Let's Start] をクリックして、ワークフローに直接移動します。

ステップ 3 [Choose Site] ウィンドウが表示されます。

a) 各サイトのデバイスの準備状況が次のステータスで示されます。

- [Ready Devices]：Cisco Umbrella 構成の前提条件を満たしているデバイス。ネットワークデバイスでの Cisco Umbrella のプロビジョニングの前提条件 （592 ページ）を参照してください。
- [Not Ready Devices]：前提条件を満たしていないデバイス。
- [Enabled Devices]：Cisco DNA Center からすでに設定されているデバイス。

b) 無効にするサイトを選択し、[Next] をクリックします。

（注） 一度に選択できるサイトは 1 つだけです。親サイトを選択すると、すべての子サイトで同時に Cisco Umbrella が無効になります。

ステップ 4 [Select Device Type] ウィンドウで、[Switches] または [Wireless Controllers] を選択します。

ステップ 5 [Select Devices] ウィンドウで、[Enabled] タブをクリックし、デバイスを選択します。

ステップ 6 [Disable] オプションボタンをクリックし、デバイスを選択します。

ステップ 7 [Summary] ウィンドウで、[Deploy] をクリックします。

ステップ 8 [Schedule] ウィンドウが表示されたら、[Now] または [Later] をクリックして構成を無効にする時期を指定し、[Apply] をクリックします。

ステップ 9 [Deployment] ウィンドウで、[View Status] をクリックし、[Scheduled Tasks] ウィンドウで展開ステータスを確認します。

Cisco Umbrella の展開ログは [Audit Logs] ウィンドウで確認できます。

ネットワークデバイスでの Cisco Umbrella 設定の更新

ステップ 1 メニューアイコン（☰）をクリックして、**[Workflows]** > **[Umbrella Deployment]** の順に選択します。

または、次の手順を実行します。

- メニューアイコン（☰）をクリックして、**[Provision]** > **[Services]** > **[Umbrella]** の順に選択します。
- Cisco Umbrella 構成を更新するサイトをネットワーク階層から選択します。
- [Select Devices] ウィンドウが表示されます。手順 4 に進んで更新ワークフローを続けます。

ステップ 2 タスクの概要ウィンドウが表示されたら、[Let's Start] をクリックして、ワークフローに直接移動します。

ステップ 3 [Choose Site] ウィンドウが表示されます。

a) 各サイトのデバイスの準備状況が次のステータスで示されます。

- [Ready Devices]：Cisco Umbrella 構成の前提条件を満たしているデバイス。ネットワークデバイスでの Cisco Umbrella のプロビジョニングの前提条件 （592 ページ）を参照してください。

- [Not Ready Devices]：前提条件を満たしていないデバイス。
- [Enabled Devices]：Cisco DNA Center からすでに設定されているデバイス。

b) 更新するサイトを選択し、[Next] をクリックします。

（注） 一度に選択できるサイトは 1 つだけです。親サイトを選択すると、すべての子サイトで同時に Cisco Umbrella が更新されます。

ステップ 4 [Select Device Type] ウィンドウで、[Switches] または [Wireless Controllers] を選択します。

ステップ 5 [Select Device Type] ウィンドウで [Switches] を選択した場合は、次の手順を実行します。

a) [Select Devices] ウィンドウで、有線デバイスを選択し、[Update] オプションボタンをクリックします。

b) [Configure Interface] ウィンドウで、次の手順を実行します。

1. ポートを選択し、[Define Umbrella Interfaces] をクリックします。
2. [Select Configuration] ダイアログボックスで、[Define Umbrella Interfaces] ドロップダウンリストをクリックし、[IN(LAN)]、[OUT(WAN)]、または [Disable Umbrella] を選択し、[Save] をクリックします。

（注） 次の手順に進むには、少なくとも 1 つの [IN] インターフェイスと 1 つの [OUT] インターフェイスを選択する必要があります。

c) [Define Umbrella Policy Mapping (Wired)] ウィンドウで、グローバルレベルまたはインターフェイスレベルの Umbrella ポリシーを選択し、[Next] をクリックします。

d) [Configure Policies for Your Devices] ウィンドウで、[IN(LAN)] インターフェイスを選択し、[Define Umbrella Policies] をクリックします。

e) [Select Policy] ダイアログボックスで、選択したインターフェイスのポリシーを選択し、[Save] をクリックします。

ステップ 6 [Select Device Type] ウィンドウで [Wireless Controllers] を選択した場合は、次の手順を実行します。

a) [Select Devices] ウィンドウで、ワイヤレスデバイスを選択し、[Update] オプションボタンをクリックします。

b) [Define Umbrella Policy Map (Wireless)] ウィンドウで SSID を選択し、マッピングする Cisco Umbrella ポリシーを選択するか、SSID の選択を解除して Cisco Umbrella を無効にします。

ステップ 7 [Review Internal Domains] ウィンドウで、内部ドメインのリストを追加または削除します。[Internal Domain] リストのドメインに一致する DNS クエリは、Cisco Umbrella ではなくローカル DNS サーバーに転送されます。

ステップ 8 [DNS Crypt] ウィンドウが表示されます。[Enable DNS Packet Encryption] オプションがデフォルトで選択されています。

DNS パケット暗号化を使用しない場合は、[Enable DNS Packet Encryption] チェックボックスをオフにします。

ステップ 9 [Summary] ウィンドウで、[Deploy] をクリックします。

ステップ 10 [Schedule] ウィンドウが表示されたら、[Now] または [Later] をクリックして構成を更新する時期を指定し、[Apply] をクリックします。

ステップ 11 [Deployment] ウィンドウで、[View Status] をクリックし、[Scheduled Tasks] ウィンドウで展開ステータスを確認します。

Cisco Umbrella の展開ログは [Audit Logs] ウィンドウで確認できます。

第 VI 部

ポリシーの設定

第 23 章

グループベースのアクセス コントロール ポリシーおよび分析の設定

グループベースのアクセスコントロール

Cisco DNA Center は、次の 2 つの方法で Software-Defined Access を実装します。

- 仮想ネットワーク（VN）は、たとえば、企業のネットワークから IoT デバイスを分離するといった、マクロレベルのセグメンテーションを提供します。
- グループベースのポリシーは、たとえば、エンジニアリンググループと HR グループの間で許可または拒否するネットワークトラフィックのタイプを制御するといった、マイクロレベルのセグメンテーションを提供します。

グループベースのアクセス コントロール ポリシーには、次の利点があります。

- ネットワークの自動化とアシュアランスの利点を備えた、豊富なアイデンティティベースのアクセス制御機能。
- きめ細かいアクセス制御。
- セキュリティグループは、すべての仮想ネットワークに適用されるため、ポリシー管理が簡素化されます。
- ポリシービューは、全体的なポリシー構造を理解し、必要なアクセス コントロール ポリシーを作成または更新するのに役立ちます。
- さまざまなアプリケーションを切り替えてセキュリティグループを管理し、保護される資産を定義する必要がなくなります。
- エンタープライズ全体のアクセス コントロール ポリシーを展開するための拡張機能を提供します。

- アイデンティティまたはネットワーク アドミッション コントロール（NAC）アプリケーションが配置される前に、ランサムウェアなどの脅威のラテラルムーブメントを制限します。
- サードパーティのアイデンティティ アプリケーションを使用しているが、Cisco ISE に移行したいユーザーに対して、Cisco Identity Services Engine（Cisco ISE）への簡単な移行パスを提供します。

Cisco DNA Center での IP プール、サイト、および仮想ネットワークの作成方法については、Cisco DNA Center のユーザーガイドを参照してください。

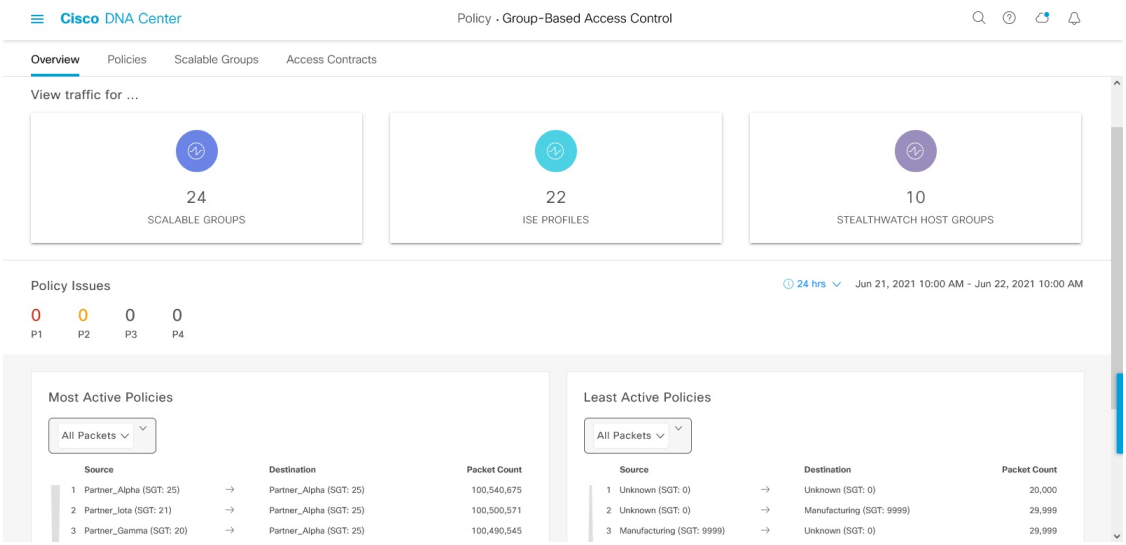
Cisco DNA Center for Cisco ISE の設定の詳細については、Cisco DNA Center のインストールガイドを参照してください。

Cisco ISE for Cisco DNA Center の設定の詳細については、Cisco Identity Services Engine 管理者ガイド [英語] を参照してください。

グループベースのアクセス コントロール ポリシー ダッシュボード

グループベースのアクセスコントロールポリシーダッシュボードでは、ネットワークアクティビティ、ポリシー関連の問題、およびトラフィックトレンドの概要が提供されます。このダッシュボードを表示するには、メニューアイコン（☰）をクリックして、**[Policy]**>**[Group-Based Access Control]** > **[Overview]** の順に選択します。

図 *23* : グループベースのアクセス コントロール ポリシー ダッシュボード



このダッシュボードでは、次の詳細方法を表示できます。

- [View Traffic]：セキュリティグループ、Cisco ISE プロファイル、および Stealthwatch ホストグループのトラフィックを表示できます。このデータを表示するには、グループベースポリシー分析パッケージをインストールする必要があります。グループベースポリシー分析で提供される分析情報により、新しいアクセスコントロールの導入による影響を評価す

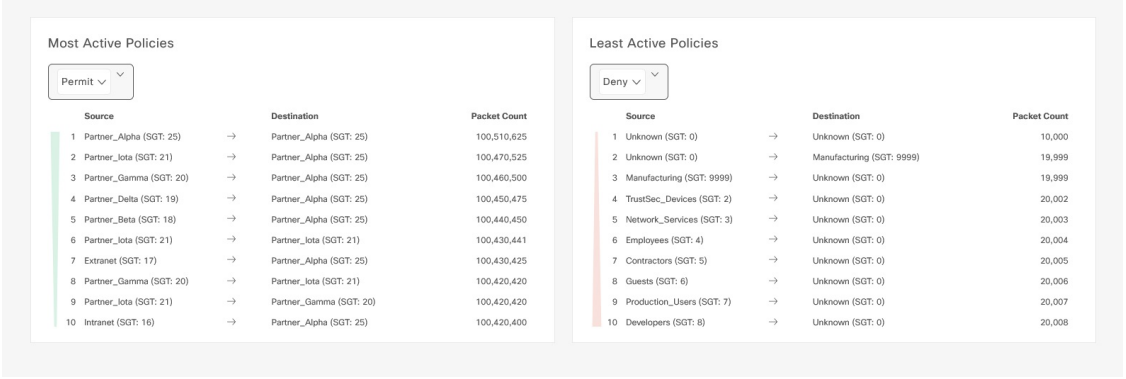
るために、資産間の通信を可視化してグループベースポリシーを作成したり、そのポリシーで許可する必要があるプロトコルを正確に特定することができます。シスコのグループベースポリシー分析では、ネットワーク上のアセットのグループとそれらの通信に関する情報が集約されます。詳細については、シスコのグループベースポリシー分析（617ページ）を参照してください。

- [View Policy-Related Issues]：ポリシー関連の問題の数が表示されます。数をクリックすると詳細情報が表示されます。新しいブラウザタブで [Assurance Issues] ダッシュボードが開きます。ここで、詳細情報を確認できます。

  このポリシー関連の問題のビューは、現在選択されている期間に関するものであることに注意してください。必要に応じて、時間セレクタを使用して時間枠を調整します。

- [View Most Active and Least Active Policies]：最もアクティブなポリシーと最もアクティブでないポリシーの詳細情報が提供されます。デフォルトでは、このビューは、各ポリシー（各送信元/宛先グループペア）に関してネットワークで確認されたパケットの総数に基づいています。ドロップダウンリストを使用して、許可されたパケットまたはドロップされたパケットのみを選択することができます。ドロップされたパケットのオプションを使用すると、ポリシーベースのドロップが最もアクティブに実行されているポリシーを確認することができます。

図 *24*：最もアクティブなポリシーのダッシュレットと最もアクティブでないポリシーのダッシュレット



このポリシーアクティビティのビューは、現在選択されている期間に関するものであることに注意してください。必要に応じて、時間セレクタを使用して時間枠を調整します。

グループベースのアクセス コントロール ポリシー

アクセス コントロール ポリシーでは、送信元セキュリティグループから宛先セキュリティグループに渡すことができるネットワークトラフィックを定義します。

- [Security Group]：ユーザー、ネットワークデバイス、またはリソースを割り当てることができる分類カテゴリ。セキュリティグループは、アクセス コントロール ポリシーで使用されます。組織のネットワーク設定、アクセス要件、および制限に基づいて、セキュリティグループを仮想ネットワークに関連付けることができます。

- [Contract]：アクセス契約は、送信元と宛先のセキュリティグループ間の通過を許可されるネットワークトラフィックのタイプを制御する一連のルールです。つまり、契約はトラフィックフィルタの定義です。アクセス契約は、トラフィックがネットワーク アプリケーション、プロトコル、およびポートに一致したときに実行されるアクション（許可または拒否）を定義します。他のルールが一致しない場合、デフォルトアクションではCatch Allルールが使用されます。
- **グループベースのアクセス コントロール ポリシー**：グループベースのアクセス コントロール ポリシーは、特定の送信元と宛先グループのペアを識別し、アクセス契約を関連付けます。アクセス契約は、送信元グループと宛先グループの間で許可または拒否されるトラフィックのタイプを指定します。これらのポリシーは単方向です。

  セキュリティグループおよびアクセス契約は、アクセス コントロール ポリシーの基本的な構成要素です。アクセスコントロールポリシーを作成する際には、前に作成したセキュリティグループと契約を使用したり、ポリシーの作成時に新しいセキュリティグループと契約を作成したりできます。特定の送信元グループからアクセスできるネットワークリソースを指定する場合は、1つの送信元グループと複数の宛先グループを含むアクセス コントロールポリシーを作成できます。一方、特定のネットワークリソースへのアクセスが許可されている送信元グループを指定する場合は、1 つの宛先グループと複数の送信元グループを含むアクセス コントロール ポリシーを作成できます。たとえば、「請負業者」送信元セキュリティグループに関連付けられたユーザーがアクセスできるネットワークリソースを指定する場合は、1つの送信元グループと複数の宛先グループを含むアクセス コントロールポリシーを作成できます。「財務サーバー」宛先セキュリティグループへのアクセスが許可されている送信元グループを指定する場合は、1 つの宛先グループと複数の送信元グループを含むアクセス コントロール ポリシーを作成できます。

  送信元と宛先のセキュリティグループの組み合わせに契約が指定されていない場合に使用するデフォルトポリシーを指定できます。デフォルトポリシーは [Permit] です。必要に応じて、このポリシーを [Deny]、[Permit_IP_Log]、または [Deny_IP_Log] に変更できます。ネットワークタイプ、オープンネットワーク、またはクローズドネットワークに基づいて、デフォルトポリシーを設定できます。

（注） すべてのネットワーク インフラストラクチャ デバイスに必要なネットワークトラフィックを許可する明示的なポリシーを作成した場合のみ、デフォルトポリシーを [Permit] から [Deny] に変更することをお勧めします。そのようにしない場合、すべてのネットワーク接続が失われる可能性があります。

リスト ビュー

[Group-Based Access Control] ウィンドウの右上にある [List] アイコンをクリックして、[List] ビューを起動します。

- [Source View]：送信元グループに基づいて編成された既存のポリシーのリストが表示されます。各行を展開して、特定の送信元と宛先のポリシーの詳細を表示できます。

- [Destination View]：宛先グループに基づいて編成された既存のポリシーのリストが表示されます。各行を展開して、特定の送信元と宛先のポリシーの詳細を表示できます。

特定の送信元グループから使用可能な宛先グループを確認するには、[Source] ビューを使用します。特定の宛先グループへのアクセスが許可されている送信元グループを確認するには、[Destination] ビューを使用します。たとえば、「請負業者」送信元セキュリティグループの一部であるユーザーが使用できる宛先グループを確認するには、[Source] ビューを使用します。「財務サーバー」宛先セキュリティグループにアクセスできる送信元グループを確認するには、[Destination] ビューを使用します。

ポリシー適用統計データをポリシーリストテーブルで表示することもできます。選択した期間内のポリシーの許可と拒否の総数が表示されます。

ポリシー適用統計は、グループベースのポリシーおよびテレメトリデータ言語（TDL）サブスクリプション用にプロビジョニングされたネットワークデバイスから収集されます。これらの設定は、通常、ファブリックの一部であるネットワークデバイスに関して自動的にプロビジョニングされます。非ファブリック ネットワークデバイスに関しては手動設定を実行できます。

ポリシー適用統計データを使用する場合は、次の点に注意してください。

- ポリシー適用統計データは、グループベースポリシー分析パッケージが展開されている場合にのみ使用できます。
- テレメトリ サブスクリプションは、ファブリック ネットワーク デバイスと非ファブリック ネットワーク デバイスの両方に関する基本プロビジョニングの一部として追加されます。新しいネットワークデバイスが Cisco DNA Center に追加され、サイトに割り当てられると、TrustSec 適用コマンドがプッシュされます。
- Software-Defined Access（SD-Access）は、ファブリックに追加されたネットワークデバイスに TrustSec 適用を追加します。TrustSec テレメトリデータは、ネットワークデバイスでこの適用が有効になっている場合にのみ収集されます。有効になっていない場合は、ポリシーモニターリングに使用されるテレメトリ サブスクリプションが TrustSec の TDL データの収集に使用されます。
- Cisco IOS XE 16.12 以降では、TDL ストリーミングデータがサポートされています。
- ネットワークデバイスで NETCONF を有効にする必要があります。
- 非ファブリック ネットワーク デバイスについては、次の設定を手動で追加する必要があります。

  ```
  cts role-based enforcement vlan-list <VLAN of the endpoints>
  ```

- アップグレード後、[Provision] > [Network Devices] > [Inventory] ウィンドウに次のメッセージが表示される場合があります。

  IOS-XE デバイスがネットワークで検出されました。これには、保証データの新しいテレメトリ サブスクリプションを有効にし、既存のサブスクリプションの一部をパフォーマンスのために最適化する必要があります。netconf を有効にし、これらのデバイスのインベントリクレデンシャルで netconf ポートを設定する必要があることに注意してください。また、これらのデバイスは、グループベースのポリシー モニターリング テレメトリの新しいサブスクリプションを受信することに注意してください。これらのサブスクリプションをプロビジョニングするためのアクションを実行しますか?

[Apply Fix] をクリックして、サイトが割り当てられているすべてのネットワークデバイスに設定をプッシュします。

マトリクス ビュー

[Group-Based Access Control] ウィンドウの右上にある [Grid] アイコンをクリックして、[Matrix] ビューを起動します。[Matrix] ビューは中核となるポリシービューであり、すべてのセキュリティグループのすべてのポリシー（明示的とデフォルトの両方）の概要を提供します。[Matrix] ビューを使用して、すべての送信元と宛先のポリシーを表示し、全体的なポリシー構造を理解できます。[Matrix] ビューからアクセスコントロールポリシーを表示、作成、および更新できます。

[Matrix] ビューには、次の 2 つの軸があります。

- 送信元軸：垂直軸にはすべての送信元セキュリティグループがリストされます。
- 宛先軸：水平軸にはすべての宛先セキュリティグループがリストされます。

特定の送信元セキュリティグループと宛先セキュリティグループのポリシーを表示するには、セルにカーソルを置きます。セルの色は、そのセルに適用されるポリシーに基づいています。次の色は、各セルに適用されるポリシーを示しています。

- [Permit]：緑色
- [Deny]：赤色
- [Custom]：金色
- [Default]：灰色

マトリックスの上部に表示される [Permit]、[Deny]、[Custom]、または [Default] アイコンにカーソルを置くと、そのポリシーが適用されているセルが表示されます。

セルをクリックすると、[Create Policy] または [Edit Policy] slide-in pane が開き、選択したセルのポリシーを作成または編集できます。[Create Policy] slide-in pane には、送信元と宛先のセキュリティグループが読み取り専用フィールドとして表示されます。ポリシーのステータスとアクセス契約を更新できます。

ポリシーマトリックスのカスタムビューを作成して、関心のあるポリシーだけに絞り込むことができます。これを実行するには、[View] ドロップダウンリストをクリックし、[Create View] を選択します。カスタムビューを作成するときに、カスタムビューに含めるセキュリティグループのサブセットを指定できます。必要に応じて、カスタムビューを保存し、後で編集することができます。[View] ドロップダウンリストをクリックし、[Manage Views] を選択して、カスタムビューを作成、編集、複製、または削除します。[Default View] には、すべての送信元および宛先セキュリティグループが表示されます。

カーソルでマトリックスコンテンツ領域をドラッグするか、または水平および垂直スクロールバーを使用して、マトリックス内を移動できます。ミニマップを使用して、マトリックス内を移動することもできます。ミニマップを使用すると、マトリックスのサイズが大きく、画面サイズを超えている場合に、マトリックス内を簡単に移動できます。ミニマップは、画面上の任

意の場所に移動して配置できます。ミニマップにはマトリックスビュー全体が表示されます。ミニマップの薄い灰色の部分は、画面に現在表示されているマトリックスの部分を表します。この領域をドラッグして、マトリックスをスクロールできます。

（注） ミニマップはデフォルトで閉じられています。[Expand]アイコンをクリックして、ミニマップを展開して表示します。

[Matrix] ビューでは、セルを選択すると、そのセルと対応する行（送信元セキュリティグループ）と列（宛先セキュリティグループ）が強調表示されます。選択したセルの座標（送信元および宛先セキュリティグループ）がマトリックスコンテンツ領域の近くに表示されます。

[Filter] オプションを使用して、選択した一連の送信元および宛先グループのポリシーマトリックスのサブセットを表示できます。フィルタを作成して、関心のあるポリシーだけに絞り込むことができます。フィルタを作成するには、含める送信元および宛先グループを選択します。

Cisco DNA Center と Cisco ISE を統合します。Cisco ISE は、Cisco DNA Center の代わりにネットワークデバイスにポリシーをダウンロードするためのランタイム ポリシー プラットフォームを提供します。ポリシーの同期の問題を防ぐために、セキュリティグループ、セキュリティグループ アクセス コントロール リスト（SGACL）、およびイーグレスポリシーの [TrustSec Workcenter] ユーザーインターフェイス画面が Cisco ISE に読み取り専用モードで表示されます。

ポリシー作成の概要

1. 組織の分類を定義するか、または最初に使用する組織の一部を定義します。
2. 特定した分類のセキュリティグループを作成します。
3. 制御するネットワークトラフィックのタイプのアクセス契約を作成します。すべてのトラフィックを許可または拒否するためのサンプルアクセス契約が事前に定義されています。また、一部の契約例では、より具体的なトラフィックフィルタリングが示されています。特定のアプリケーション定義に基づいて、さらにきめ細かいアクセス契約を作成できます。
4. アプリケーションサーバーや他のネットワークへの接続など、特定のネットワークリソースへのアクセスを必要とするネットワークユーザーのカテゴリを決定します。
5. アクセスポリシーを作成し、送信元グループ、宛先グループ、およびアクセス契約を関連付け、送信元から宛先へのトラフィックのフローを許可する方法を定義します。

セキュリティグループの作成

始める前に

次のタスクを実行するには、スーパー管理者またはネットワーク管理者である必要があります。

ステップ 1 メニューアイコン（☰）をクリックして、**[Policy]** > **[Group-Based Access Control]** > **[Security Groups]** の順に選択します。

ステップ 2 [セキュリティグループの作成（Create Security Group）] をクリックします。

ステップ 3 [Create Security Group] スライドインペインで、セキュリティグループの名前と説明（任意）を入力します。

（注） [Name] フィールドでサポートされる文字は次のとおりです：

- 英数字
- アンダースコア (_)

セキュリティグループ名は英字で開始する必要があります。

Cisco DNA Center タグ値を生成します。必要に応じて、この値を更新できます。指定した値が既存のセキュリティグループによってすでに使用されている場合は、エラーメッセージが表示されます。有効な範囲は 2 ～ 65519 です。

ステップ 4 [Virtual Networks] ドロップダウンリストから、このセキュリティグループに関連付ける仮想ネットワークを選択します。デフォルトでは、デフォルトの仮想ネットワークが選択されています。

（注） Cisco DNA Center 2.3.3 以降が Cisco ISE 3.2 以降と統合されている場合、セキュリティグループは仮想ネットワークに関連付けられません。したがって、これらのリリースでは[Virtual Networks] フィールドは表示されません。ただし、Cisco ISE 3.1 以前のリリースを使用している場合は、セキュリティグループと仮想ネットワークの関連付けの詳細が表示されます。

ステップ 5 セキュリティグループを Cisco Application-Centric Infrastructure（ACI）に伝播する場合は、[Propagate to ACI] チェックボックスをオンにします。

ステップ 6 次のいずれかのオプションを選択します。

- セキュリティグループを今すぐ作成するには、[Save Now] をクリックします。
- このタスクを特定の時刻にスケジュールするには、[Schedule Later] をクリックして、次の操作を行います。
  1. [Scheduler] スライドインペインで、スケジュールされたタスクの名前を入力します。
  2. このタスクの開始日時を指定します。
  3. [Time Zone] ドロップダウンリストから、必要なタイムゾーンを選択します。
  4. [Apply] をクリックします。

[Cisco DNA Center Automation Events for ITSM (ServiceNow)] バンドルが有効になっている場合、[Save Now] オプションは無効になり、グループベースのポリシー変更に対する [Schedule Later] オプションのみが有効になります。スケジュールされたタスクは、スケジュールされた時刻の前に IT サービス管理（ITSM）で承認される必要があります。スケジュールされた時刻までにタスクが承認されない場合、タスクは失敗します。ITSM と Cisco DNA Center の統合方法の詳細については、『Cisco DNA Center ITSM Integration Guide』を参照してください。

[Security Groups] ウィンドウの右上隅で、今後のタスク、進行中のタスク、および失敗したタスクの合計数を確認できます。[Activities] > [Tasks] でタスクのステータスリンクをクリックすると、タスクの詳細が表示されます。タスクは、実行前に編集またはキャンセルできます。

[Security Groups] ウィンドウには、セキュリティグループ名、タグ値、および関連するポリシーが表示されます。このウィンドウでは、セキュリティグループのサンプルを表示することもできます。これらのセキュリティグループを使用または削除できます。

セキュリティグループは、[Security Groups] ウィンドウから編集または削除できます。[Security Group Name] 列のリンクをクリックして、セキュリティグループの詳細を表示します。

セキュリティグループを編集するには、対応するセキュリティグループの横にあるチェックボックスをオンにして、[Edit] をクリックします。[Edit Security Group] スライドインペインで、必要な変更を加えた後、次の操作を実行します。

- 変更をすぐに保存するには、[Save Now] をクリックします。
- 特定の時間に更新をスケジュールするには、[Schedule Later] をクリックします。[Scheduler] スライドインペインで、開始時刻、日付、およびタイムゾーンを指定し、[Apply] をクリックします。

セキュリティグループを削除するには、対応するセキュリティグループの横にあるチェックボックスをオンにして、次のいずれかのオプションを選択します。

- セキュリティグループをすぐに削除するには、[Delete Now] をクリックします。
- 後でセキュリティグループを削除するには、[Delete Later] をクリックします。[Schedule Delete] スライドインペインで、開始時刻、日付、およびタイムゾーンを指定し、[Apply] をクリックします。

セキュリティグループを更新する場合は、ネットワークデバイスに変更を展開する必要があります。[Deploy Now] をクリックして変更をすぐに展開するか、[Deploy Later] をクリックして変更を後で展開します。

セキュリティグループの [Policies] 列のリンクをクリックすると、そのセキュリティグループとそのグループが属するポリシーを使用するアクセスコントロールルールが表示されます。セキュリティグループがいずれかのアクセスポリシーで使用されている場合、そのセキュリティグループは削除できません。

Cisco ISE との同期が完了していない場合は、セキュリティグループの横にオレンジ色の三角形のアイコンが表示されます。

Cisco ISE は、内部エンドポイントグループ（IEPG）を同期し、Cisco ISE に関連付けられている読み取り専用セキュリティグループを作成することで、ACI から TrustSec ドメインへのパケットをサポートします。これらのセキュリティグループは、[Created In] 列の値が **ACI** となって [Security Groups] ウィンドウに表示されます。ACI から学習したセキュリティグループは編集も削除もできませんが、ポリシーで使用することはできます。

[Associated Contracts] 列には、ACI から学習したセキュリティグループに関連付けられている契約が表示されます。[Associated Contracts] 列に表示されるリンクをクリックすると、関連付けられた契約に関する詳細が表示されます。

IEPG が ACI で更新されると、対応するセキュリティグループ設定が Cisco ISE で更新されます。Cisco ISE でセキュリティグループが作成されると、新しい EEPG が ACI に作成されます。

（注） 名前が「ANY」またはタグ値が 0xFFFF/65535 のセキュリティグループは作成できません。セキュリティグループ ANY/65535 は、Cisco DNA Center デフォルトポリシーに使用される予約済みの内部セキュリティグループです。

Cisco DNA Center 内のセキュリティグループを Cisco ISE と同期しているときは、次のように動作します。

- セキュリティグループが Cisco DNA Center に存在し、Cisco ISE に存在しない場合は、Cisco ISE に作成されます。
- セキュリティグループが Cisco ISE に存在し、Cisco DNA Center に存在しない場合は、Cisco DNA Center に作成されます。
- セキュリティグループ名が Cisco DNA Center と Cisco ISE の両方で同じで、説明と ACI データが異なっている場合、Cisco DNA Center は Cisco ISE で指定されたデータを使用して更新されます。
- Cisco DNA Center と Cisco ISE でセキュリティグループ名が同じで、タグ値が異なっている場合、Cisco ISE で指定されたタグ値を持つ新しいセキュリティグループが Cisco DNA Center に作成されます。Cisco DNA Center にすでにあるセキュリティグループの名前は、サフィックス **_DNAC** で更新されます。
- タグの値が同じでセキュリティグループ名が異なる場合、Cisco DNA Center のセキュリティグループ名が Cisco ISE で指定された名前で更新されます。

アクセス契約の作成

アクセス契約は、送信元と宛先のセキュリティグループ間の通過を許可されるネットワークトラフィックのタイプを制御する一連のルールです。アクセス契約は、トラフィックがネットワークアプリケーション、プロトコル、およびポートに一致したときに実行されるアクション（許可または拒否）を定義します。

（注） Cisco ISE のセキュリティ グループ アクセス コントロール リスト（SGACL）は、Cisco DNA Center の**アクセス契約**と呼ばれます。

始める前に

次のタスクを実行するには、スーパー管理者またはネットワーク管理者である必要があります。

ステップ 1 メニューアイコン（☰）をクリックして、**[Policy]** > **[Group-Based Access Control]** > **[Access Contracts]** の順に選択します。

ステップ 2 [Create Access Contract] をクリックします。

ステップ 3 [Create Access Contract] スライドインペインで、契約の名前と説明を入力します。

ステップ 4 トラフィックフィルタルールを作成します。

- [Action] ドロップダウンリストで、[Deny] または [Permit] を選択します。
- From the **APplication** drop-down list, choose the application for which you want to apply that action. ポートとプロトコルは、選択したアプリケーションに基づいて自動的に選択されます。

  トランスポートプロトコル、送信元ポート、および宛先ポートを指定する場合は、[Application] ドロップダウンリストから [Advanced] オプションを選択します。

複数のルールを作成できます。1 つの契約に複数のルールを作成するには、[+] 記号をクリックし、[Action] 列と [Application] 列の設定を選択します。ルールは、契約に記載されている順序でチェックされます。ルールの左端にあるハンドルアイコンを使用してドラッグして、ルールの順序を変更します。

[Logging] トグルを使用して、任意のトラフィックフィルタルール（デフォルトアクションを含む）のロギングを有効化または無効化できます。ロギングはデフォルトではディセーブルになっています。ロギングが有効になっている場合、トラフィックフィルタルールにヒットすると、ネットワークデバイスは syslog メッセージを送信します。これは、ポリシーのトラブルシューティングと初期化テストに役立つ場合があります。ただし、ネットワークデバイスのリソースとパフォーマンスに影響を与える可能性があるため、このオプションは慎重に使用することを推奨します。

ステップ 5 [Default Action] ドロップダウンリストで、[Deny] または [Permit] を選択します。

必要に応じて、デフォルトアクションのロギングを有効にできます。

ステップ 6 次のいずれかのオプションを選択します。

- アクセス契約をすぐに作成するには、[Save Now] をクリックします。
- このタスクを特定の時刻にスケジュールするには、[Schedule Later] をクリックして、次の操作を行います。

  1. [Scheduler] スライドインペインで、スケジュールされたタスクの名前を入力します。
  2. このタスクの開始日時を指定します。

3. [Time Zone] ドロップダウンリストから、必要なタイムゾーンを選択します。
4. [Apply] をクリックします。

[Cisco DNA Center Automation Events for ITSM (ServiceNow)] バンドルが有効になっている場合、[Save Now] オプションは無効になり、グループベースのポリシー変更に対する [Schedule Later] オプションのみが有効になります。スケジュールされたタスクは、スケジュールされた時刻の前に IT サービス管理（ITSM）で承認される必要があります。スケジュールされた時刻までにタスクが承認されない場合、タスクは失敗します。ITSM と Cisco DNA Center の統合方法の詳細については、『Cisco DNA Center ITSM Integration Guide』を参照してください。

[Access Contract] ウィンドウの右上隅で、今後のタスク、進行中のタスク、および失敗したタスクの合計数を表示できます。[Activities] > [Tasks] でタスクのステータスリンクをクリックすると、タスクの詳細が表示されます。タスクは、実行前に編集またはキャンセルできます。

[Access Contracts] ウィンドウで、契約の表示、作成、複製、更新、および削除ができます。

また、[Access Contracts] ウィンドウでサンプル契約を表示することもできます。それらのサンプル契約は使用または削除できます。ただし、デフォルトの契約（Permit IP、Deny IP、Permit_IP_Log、Deny_IP_Log）は削除できません。

[Contract Name] 列のリンクをクリックして、契約の詳細を表示します。

アクセス契約を編集するには、対応するアクセス契約の横にあるチェックボックスをオンにして、[Actions] > [Edit] を選択します。[Edit Access Contract] ウィンドウで、必要な変更を加えた後に次の操作を実行します。

- 変更をすぐに保存するには、[Save Now] をクリックします。
- 特定の時間に更新をスケジュールするには、[Schedule Later] をクリックします。[Scheduler] スライドインペインで、開始時刻、日付、およびタイムゾーンを指定し、[Apply] をクリックします。

Cisco ISE との同期が完了していない場合、アクセス契約の横にオレンジ色の三角形のアイコンが表示されます。

ACI から学習した契約は [Access Contracts] ウィンドウに表示され、[Created In] 列の値が [ACI] になります。ACI から学習したアクセス契約を編集したり削除したりすることはできませんが、ACI から学習したセキュリティグループの使用中にポリシーで使用することはできます。マトリックスビューからポリシーを作成または更新する場合に、ACI から学習したセキュリティグループを接続先グループとして選択すると、関連するアクセス契約が [Preferred Contracts] タブに表示されます。[All Contracts] タブですべてのアクセス契約を確認できます。

[Rules Count] 列で、各アクセス契約で使用されているルールの数を確認できます。

アクセス契約を使用するポリシーを表示するには、そのアクセス契約の [Policies] 列のリンクをクリックします。

ポリシーで使用されている場合、契約を削除することはできません。契約を削除する前に、そのポリシーから契約を削除する必要があります。

アクセス契約を編集するには、対応するアクセス契約の横にあるチェックボックスをオンにして、次のいずれかのオプションを選択します。

- アクセス契約をすぐに削除するには、[Delete Now] をクリックします。
- 後でアクセス契約を削除するには、[Delete Later] をクリックします。[Schedule Delete] スライドインペインで、開始時刻、日付、およびタイムゾーンを指定し、[Apply] をクリックします。

セキュリティグループ、契約、またはポリシーを更新する場合は、ネットワークデバイスに変更を展開する必要があります。ポリシーを更新し、更新したポリシーを展開しない場合、ポリシーの変更に関する通知はネットワークデバイスに送信されず、ネットワークで現在アクティブになっているポリシーは、Cisco DNA Center に表示されるポリシー情報と一致しない可能性があります。この状況を解決するには、ネットワークデバイスに、更新したポリシーを展開する必要があります。[Deploy Now] をクリックして変更をすぐに展開するか、[Deploy Later] をクリックして変更を後で展開します。

既存のアクセス契約を複製し、必要な詳細情報を編集して新しいアクセス契約を作成できます。アクセス契約を複製すると、既存のアクセス契約に含まれるすべての情報がコピーされ、コピーされた契約は、既存の契約名の末尾に文字列**Copy**が付加された名前になります。[Save Now] をクリックして複製契約をすぐに作成するか、[Schedule Later] をクリックして複製契約を後で作成します。

[Filter] オプションを使用して、探している契約を検索できます。

Cisco DNA Center のアクセス契約を Cisco ISE と同期している間：

- 契約が Cisco DNA Center に存在し、Cisco ISE に存在しない場合は、Cisco ISE に作成されます。
- コントラクトがに存在Cisco ISEし、にCisco DNA Center存在しない場合は、にCisco DNA Center作成されます。
- 契約名が Cisco DNA Center と Cisco ISE で同じであるが、説明とトラフィックルールの内容が異なっている場合、Cisco DNA Center は Cisco ISE で指定されたデータを使用して更新されます。
- 契約名とルールが同じで、説明が異なっている場合、Cisco DNA Center は Cisco ISE で指定された説明を使用して更新されます。
- Cisco ISE の Text SGACL コマンドラインは、解析できないコンテンツとして移行されます。これらの契約は編集できますが、Cisco DNA Center では構文解析や構文チェックは行われません。Cisco DNA Center で加えた変更は、Cisco ISE に反映されます。
- Cisco ISE でポリシーに複数の SGACL がある場合、それらの契約は Cisco DNA Center のデフォルトポリシーとして移行されます。

グループベースのアクセス コントロール ポリシーの作成

セキュリティグループおよびアクセス契約は、アクセス コントロール ポリシーの基本的な構成要素です。アクセス コントロール ポリシーを作成する際には、前に作成したセキュリティグループと契約を使用したり、ポリシーの作成時に新しいセキュリティグループと契約を作成したりできます。

特定の送信元グループからアクセスできるネットワークリソースを指定する場合は、1 つの送信元グループと複数の宛先グループを含むアクセス コントロール ポリシーを作成できます。一方、特定のネットワークリソースへのアクセスが許可されている送信元グループを指定する場合は、1つの宛先グループと複数の送信元グループを含むアクセスコントロールポリシーを作成できます。

たとえば、「請負業者」送信元セキュリティグループに関連付けられたユーザーがアクセスできるネットワークリソースを指定する場合は、1 つの送信元グループと複数の宛先グループを含むアクセス コントロール ポリシーを作成できます。「財務サーバー」宛先セキュリティグループへのアクセスが許可されている送信元グループを指定する場合は、1 つの宛先グループと複数の送信元グループを含むアクセス コントロール ポリシーを作成できます。

グループベースのアクセス コントロール ポリシーは、送信元グループと宛先グループの特定ペアのトラフィックフローに基づいて作成または更新することもできます。

グループベースのアクセス コントロール ポリシーを作成するには、次の手順を使用します。

ステップ 1 [Policy List] または [Matrix] ビューで、[Create Policies] をクリックします。

ステップ 2 1つの送信元グループと複数の宛先グループを含むアクセスコントロールポリシーを作成するには、[Source To Destination(s)] をクリックし、次の手順を実行します。

a) 選択する送信元セキュリティグループの横にあるオプションボタンをクリックします。

必要なセキュリティグループが存在しない場合は、[Create Security Group] をクリックして新しいセキュリティグループを作成します。このオプションは、[Cisco DNA Center Automation Events for ITSM (ServiceNow)] バンドルが有効になっている場合は使用できません。

b) [Next] をクリックします。

c) 選択した送信元セキュリティグループにマッピングする宛先セキュリティグループを選択します。

必要に応じて、セキュリティグループの詳細を表示したり、セキュリティグループを編集したりできます。

（注） 送信元と宛先の間にポリシーがすでに存在する場合、セキュリティグループの近くにはオレンジ色の三角形のアイコンが表示されます。

d) **[次へ (Next)]** をクリックします。

e) 選択する契約の横にあるオプションボタンをクリックします。必要に応じて、契約の詳細を表示および編集できます。

必要な契約が存在しない場合は、[Create Contract] をクリックして新しい契約を作成します。このオプションは、[Cisco DNA Center Automation Events for ITSM (ServiceNow)] バンドルが有効になっている場合は使用できません。

（注） 1 つのポリシーに対して 1 つの契約のみを選択できます。

f) **[次へ (Next)]** をクリックします。

[Summary] ウィンドウには、選択したセキュリティグループと契約に基づいて作成されたポリシーが一覧表示されます。

g) 次のいずれかのオプションを選択します。

- ポリシーを今すぐ保存するには、[Save Now] をクリックします。
- このタスクを特定の時刻にスケジュールするには、[Schedule Later] をクリックして、次の操作を行います。
  1. [Schedule Create Policy] スライドインペインで、スケジュールされたタスクの名前を入力します。
  2. このタスクの開始日時を指定します。
  3. [Time Zone] ドロップダウンリストから、必要なタイムゾーンを選択します。
  4. [Apply] をクリックします。

ステップ 3 1 つの宛先グループと複数の送信元グループを含むアクセス コントロール ポリシーを作成するには、[Destination to Source(s)] をクリックし、次の手順を実行します。

a) 選択する宛先セキュリティグループの横にあるオプションボタンをクリックします。

必要なセキュリティグループが存在しない場合は、[Create Security Group] をクリックして新しいセキュリティグループを作成します。このオプションは、[Cisco DNA Center Automation Events for ITSM (ServiceNow)] バンドルが有効になっている場合は使用できません。

b) [Next] をクリックします。

c) 選択した宛先セキュリティグループにマッピングする送信元セキュリティグループを選択します。

必要に応じて、セキュリティグループの詳細を表示したり、セキュリティグループを編集したりできます。

（注） 送信元と宛先の間にポリシーがすでに存在する場合、セキュリティグループの近くにはオレンジ色の三角形のアイコンが表示されます。

d) **[次へ (Next)]** をクリックします。

e) 選択する契約の横にあるオプションボタンをクリックします。

必要な契約が存在しない場合は、[Create Contract] をクリックして新しい契約を作成します。このオプションは、[Cisco DNA Center Automation Events for ITSM (ServiceNow)] バンドルが有効になっている場合は使用できません。

（注） 1 つのポリシーに対して 1 つの契約のみを選択できます。

f) **[次へ (Next)]** をクリックします。

[Summary] ウィンドウには、選択したセキュリティグループと契約に基づいて作成されたポリシーが一覧表示されます。

g) 次のいずれかのオプションを選択します。

- ポリシーを今すぐ保存するには、[Save Now] をクリックします。
- このタスクを特定の時刻にスケジュールするには、[Schedule Later] をクリックして、次の操作を行います。

  1. [Schedule Create Policy] スライドインペインで、スケジュールされたタスクの名前を入力します。
  2. このタスクの開始日時を指定します。
  3. [Time Zone] ドロップダウンリストから、必要なタイムゾーンを選択します。
  4. [Apply] をクリックします。

[Cisco DNA Center Automation Events for ITSM (ServiceNow)] バンドルが有効になっている場合、[Save Now] オプションは無効になり、グループベースのポリシー変更に対する [Schedule Later] オプションのみが有効になります。スケジュールされたタスクは、スケジュールされた時刻の前に IT サービス管理（ITSM）で承認される必要があります。スケジュールされた時刻までにタスクが承認されない場合、タスクは失敗します。ITSM と Cisco DNA Center の統合方法の詳細については、『Cisco DNA Center ITSM Integration Guide』を参照してください。

[Policies] ウィンドウの右上隅で、今後のタスク、進行中のタスク、および失敗したタスクの合計数を表示できます。[Activities] > [Tasks] でタスクのステータスリンクをクリックすると、タスクの詳細が表示されます。タスクは、実行前に編集またはキャンセルできます。

トラフィックフローに基づいてグループベースのアクセス コントロール ポリシーを作成または変更するには、次の手順を実行します。

1. ポリシーマトリックスビューで、グループベースのアクセス コントロール ポリシーを作成または変更するセルをクリックします。
2. [Policy Details] スライドインペインで、[View Traffic Flows] をクリックします。

   [View Traffic Flows] スライドインペインの左側のペインでは、選択した契約のルールまたはデフォルトのポリシーを確認できます。右側のペインでは、選択したルールに一致するトラフィックフローを確認できます。
3. [Default Action] ルールの [View Traffic] をクリックして、そのルールに一致するフローのリストを表示します。追加のルールを持つアクセス契約を使用して既存のポリシーを変更する際、任意のルールの [View Traffic] オプションを使用して、そのルールに一致するフローのリストを表示します。

[Default Action] ルール（明示的に選択されたアクセス契約がない）を使用しているポリシーの場合、アクセス契約を選択するか、そのポリシーで使用される新しいアクセス契約を作成することができます。

アクセス契約の PERMIT または DENY を使用したポリシーの場合、アクセス契約を選択するか、そのポリシーで使用される新しいアクセス契約を作成することができます。

カスタムアクセス契約を使用したポリシーの場合、選択したアクセス契約を編集できます。

新しく作成または編集した契約を保存する際は、次のオプションがあります。

- 変更を既存の契約に保存します。変更は、その契約を参照するすべてのポリシーに影響します。
- 変更を新しい契約として保存します。変更は現在のポリシーにのみ適用されます。
- 変更を新しい契約として保存します。変更はどのポリシーにも適用されません。

Cisco DNA Center でポリシーを Cisco ISE と同期する場合、次のようになります。

- ポリシーが Cisco DNA Center に存在し、Cisco ISE に存在しない場合は、Cisco ISE に作成されます。
- 契約が Cisco ISE に存在し、Cisco DNA Center に存在しない場合は、Cisco DNA Center に作成されます。
- Cisco ISE でポリシー契約が異なる場合、 Cisco DNA Center は Cisco ISE で指定された契約で更新されます。
- ポリシーモード情報（有効、無効、またはモニター）も Cisco ISE からインポートされます。

Cisco ISE には、単一のポリシーに対して複数の SGACL を許可するオプションがあります（このオプションは Cisco ISE ではデフォルトで有効になっていません）。Cisco DNA Center では、単一のポリシーに対して複数のアクセス契約を使用することはサポートされていません。ポリシーの同期中に、Cisco ISE のポリシーに複数の SGACL がある場合、Cisco DNA Center 管理者には、そのポリシーを変更して契約を選択しないようにするオプションがあります（デフォルトポリシーを使用する場合）。管理者は、ポリシーの同期が完了した後に、そのポリシーに対して新規または既存のアクセス契約を選択できます。

シスコのグループベースポリシー分析

シスコのグループベースポリシー分析について

グループベースポリシー分析で提供される情報を使用することで、資産間の通信を可視化してグループベースポリシーを作成したり、新しいアクセスコントロールの導入による影響を評価したり、ポリシーで許可する必要があるプロトコルを正確に特定したりできます。

シスコのグループベースポリシー分析では、ネットワーク上の資産のグループとそれらの通信に関する次のような情報が集約されます。

- 相互に通信しているグループ
- 通信の種類
- 特定の資産が属するグループ

インストール

Cisco DNA Center のライセンスの種類は次のとおりです。

- Cisco DNA Essentials
- Cisco DNA Advantage
- Cisco DNA Premier

Cisco DNA Advantage と Cisco DNA Premier には、グループベースポリシー分析パッケージが含まれています。このパッケージは、次のアーカイブ（.tar.gz ファイル）で構成されています。

- バックエンド
- ユーザー インターフェイス
- サマライザパイプライン
- 集約の定義

シスコのグループベースポリシー分析は Cisco DNA Center の一部ですが、デフォルトではインストールされません。メニューアイコン（☰）をクリックして、**[System]** > **[Software Updates]** > **[Installed Apps]** の順に選択します。[Policy Applications] で [Group-Based Policy Analytics] まで下にスクロールします。[Install] をクリックしてアプリケーションをインストールします。

ハードウェアとソフトウェアの互換性

プラットフォーム サポート

シスコのグループベースポリシー分析は、次のハードウェアプラットフォームでサポートされています。

- 44 コアのシングルノードクラスタと 3 ノードクラスタ
- 56 コアのシングルノードクラスタと 3 ノードクラスタ
- 112 コアのシングルノードクラスタと 3 ノードクラスタ

これらのプラットフォームは、ここで説明するパフォーマンスと拡張性の要件を満たしている必要があります。

サポートされているハードウェアの詳細については、「Cisco UCS M4 appliances」または「Cisco UCS M5 appliances」を参照してください。

次の表に、Cisco DNA Center およびシスコのグループベースポリシー分析でサポートされるパフォーマンスメトリックをコアプラットフォームごとに示します。NetFlow メトリックは、シスコのグループベースポリシー分析で導入されています。

（注） 次の表に、スタンドアロン展開のパフォーマンスメトリックを示します。これらの値は、クラスタ内のノードの数とインストールされているパッケージの数によって異なる場合があります。

表 *48 :* パフォーマンスメトリック

メトリック	44 コア、3 ノード	56 コア	112 コア
デバイス （NAD）	5000 スイッチが 1000、ルータが 1000、またはその両方の組み合わせ、AP が 4000	8000 スイッチが 2000、ルータが 2000、またはその両方の組み合わせ、AP が 6000	18,000 スイッチが 5000、ルータが 5000、またはその両方の組み合わせ、AP が 13,000
Clients （エンドポイント）	25,000 ワイヤレスが 20,000、有線が 5,000	40,000 ワイヤレスが 30,000、有線が 10,000	100,000 ワイヤレスが 60,000、有線が 40,000
NetFlow/秒	30,000	48,000	120,000

デバイス サポート

シスコのグループベースポリシー分析を使用するには、NetFlow を有効にする必要があります。次の表に、さまざまなネットワークデバイスで NetFlow を有効にする方法を示します。

表 *49* : デバイス サポート

ネットワーク デバイス（**Network Devices**）	シリーズ	**Cisco DNA Center UI** の **[Network Settings]** の **[Telemetry]** セクションでの **NetFlow** の設定（**Flexible NetFlow** または **Application Visibility and Control** ベースの **NetFlow**）	**Cisco DNA Center UI** のテンプレート エディタ ツールを使用した **NetFlow** の設定（**Flexible NetFlow** または **Application Visibility and Control** ベースの **NetFlow**）	ファブリック展開での **NetFlow** の収集	非ファブリック展開での **NetFlow** の収集
ルータ	Cisco 1000 シリーズ サービス統合型ルータ（ISR1K）	対応	対応	対応	対応
	Cisco 4000 シリーズ サービス統合型ルータ（ISR4K）	対応	対応	対応	対応
	Cisco 1000v シリーズ クラウド サービス ルータ（CSR 1000v）	対応	対応	対応	対応
	Cisco 1000 シリーズ アグリゲーション サービス ルータ（ASR1K）	対応	対応	対応	対応
スイッチ	Cisco Catalyst 9200 シリーズ	対応	対応	対応	対応
	Cisco Catalyst 9300 シリーズ	対応	対応	対応	対応
	Cisco Catalyst 9400 シリーズ	対応	対応	対応	対応
	Cisco Catalyst 9500 シリーズ	非対応	対応	対応	対応
	Cisco Catalyst 9600 シリーズ	非対応	対応	対応	対応
	Cisco Catalyst 2k シリーズ	非対応	対応	該当なし	対応
	Cisco Catalyst 3560 シリーズ	非対応	対応	該当なし	対応
	Cisco Catalyst 3650 シリーズ	非対応	対応	対応	対応
	Cisco Catalyst 3850 シリーズ	非対応	対応	対応	対応
	Cisco Catalyst 4k シリーズ	非対応	対応	対応	対応
	Cisco Catalyst 6500 シリーズ スイッチ	非対応	対応	対応	対応
	Cisco Catalyst 6800 シリーズ スイッチ	非対応	対応	対応	対応

ネットワークデバイス（Network Devices）	シリーズ	Cisco DNA Center UI の [Network Settings] の [Telemetry] セクションでの NetFlow の設定（Flexible NetFlow または Application Visibility and Control ベースの NetFlow）	Cisco DNA Center UI のテンプレートエディタツールを使用した NetFlow の設定（Flexible NetFlow または Application Visibility and Control ベースの NetFlow）	ファブリック展開での NetFlow の収集	非ファブリック展開での NetFlow の収集
ワイヤレス コントローラ	Cisco 3504 ワイヤレスコントローラ（AireOS ベース）	対応	対応	非対応	対応、中央スイッチング SSID のみ
	Cisco 5520 ワイヤレスコントローラ（AireOS ベース）	対応	対応	非対応	対応、中央スイッチング SSID のみ
	Cisco 8540 ワイヤレスコントローラ（AireOS ベース）	対応	対応	非対応	対応、中央スイッチング SSID のみ
	Cisco Catalyst 9800 ベースのコントローラ	対応	対応	対応	対応

Cisco ISE

Cisco ISE 2.4 パッチ 7 以降、Cisco ISE 2.6 パッチ 1 以降、および Cisco ISE 2.7 以降がサポートされています。

Cisco StealthWatch

Cisco Stealthwatch 7.x 以降がサポートされています。

コネクタについて

シスコのグループベースポリシー分析は、次のソース（コネクタとも呼ばれます）からテレメトリを収集します。コネクタを設定するには、シスコのグループベースのポリシー分析の初期設定 （622 ページ） ワークフローに従うか、**[Policy]** > **[Group-Based Access Control]** > **[Analytics]** > **[Configurations]** > **[Analytics Settings]** の順に選択します。

グループデータコネクタ

グループデータコネクタは、資産が分類されるグループに関する情報を収集します。グループデータコネクタには Cisco ISE と Cisco Stealthwatch があります。

- **Cisco ISE**

  Cisco ISE は、アイデンティティおよびアクセス コントロール ポリシーを管理する次世代のプラットフォームとして、企業のコンプライアンス遵守、インフラストラクチャ セキュリティの強化、サービスオペレーションの効率化を実現します。Cisco ISE は、仮想マシンまたは物理マシン、あるいはその両方の組み合わせにインストールされます。Cisco ISE

は、Cisco Platform Exchange Grid（pxGrid）サービスを、SessionDirectory、セキュリティグループ、およびその他の情報を共有するためのパブリッシャ/サブスクライバモジュールとして使用します。PxGridは、クエリインターフェイスを使用し、一括ダウンロードをサポートしています。ネットワークのユーザーの認証、許可、アカウンティングが行われ、セッションディレクトリが維持されます。ユーザーイベントは、SessionDirectoryサービスに登録されているコネクタにパブリッシュされます。セキュリティグループ通知などの他のサービスにも登録できます。

ネットワークに入ってきたパケットは、認証で取得したユーザーアイデンティティとデバイスの情報を使用して分類されます。このパケット分類は、パケットがネットワークに入ってきたときに、そのパケットにタグ付けすることによって維持されます。これにより、パケットはデータパス全体で正しく識別され、セキュリティおよびその他のポリシー基準が適用されるようになります。このタグは、セキュリティ グループ タグ（SGT）と呼ばれることもあります。ネットワークデバイスでSGTに応じてトラフィックをフィルタリングできるようにすることにより、Cisco ISEでアクセス コントロール ポリシーを適用できるようになります。

さらに、Cisco ISEは、ネットワークに接続されているエンドポイントの情報も収集します。これには、デバイスのタイプ、OS、OSのバージョン、IPアドレスなどの属性が含まれます。これらはISEプロファイルと呼ばれます。

Cisco ISEコネクタは、シスコのグループベースポリシー分析に使用するSGTの定義とプロファイルをCisco ISEから提供します。

- **Cisco StealthWatch**

  Cisco Stealthwatchは、高度な脅威検出、脅威への迅速な対応、およびネットワークトラフィックのセキュリティ分析を可能にするネットワークベースの異常検出システムです。Cisco Stealthwatchコネクタは、Cisco Stealthwatchで設定されているホストグループを取得します。ホストグループは基本的に、場所、機能、トポロジなどの類似の属性を持つ複数のホストIPアドレスまたはIPアドレス範囲の仮想コンテナです。

通信コネクタ

通信コネクタは、グループベースのポリシーの決定に役立つグループ間のトラフィックに関する情報を収集します。これは、Cisco DNA Centerで管理しているネットワークデバイスからのNetFlowを使用して実行されます。Cisco DNA Centerでは、NetFlowがネイティブで収集および集約されます。

シスコのグループベースのポリシー分析の初期設定

このワークフローでは、Cisco ISE、Cisco Stealthwatch、NetFlowなどの特定のソースからネットワークアクティビティやエンドポイントに関連するテレメトリデータを収集するために必要なデータコネクタを設定できます。このタスクは、初めてデータコネクタを設定するときに便利です。

始める前に

Cisco DNA Center にシスコのグループベースポリシー分析がインストールされている必要があります。

ステップ 1 メニューアイコン（☰）をクリックして、**[Policy]** > **[Group-Based Access Control]** > **[Overview]** の順に選択します。[Create policies with more confidence] ウィンドウが表示されます。

ステップ 2 [Get Started] をクリックします。
[Configure your data connectors] ウィンドウが表示されます。

ステップ 3 [Let's Do it] をクリックします。

[Configure Group Data Connectors] ウィンドウが表示されます。

（注） Cisco ISE のバージョンがシスコのグループベースポリシー分析を実行するために必要なバージョンよりも前のバージョンの場合は、次のエラーメッセージが表示されます。

ステップ 4 設定するコネクタの下部にある [Configure] をクリックします。
新しいウィンドウが開き、Cisco DNA Center の [Settings] ウィンドウにリダイレクトされます。ここで必要なコネクタを設定できます。Cisco ISE コネクタを設定する必要があります。Cisco Stealthwatch コネクタの設定は任意です

ステップ 5 [Settings] ウィンドウを閉じます。[Configure Group Data connectors] ウィンドウで、正常に設定されたコネクタの [Configure] オプションの横に緑色のドットが表示されます。

ステップ 6 [Next] をクリックします。

[Configure Communication Connectors] ウィンドウが表示されます。

ステップ 7 次のいずれかのオプションを使用して、通信コネクタ（NetFlow）を設定します。

- Cisco DNA Center のデバイスインターフェイスで NetFlow を手動でプロビジョニングします。
- [Template Editor] をクリックし、Cisco DNA Center の**テンプレートエディタツール**を使用して NetFlow を設定します。
- [Telemetry in Network Settings] をクリックし、ネットワーク設定のテレメトリのセクションで NetFlow を設定します。

ステップ 8 [Next] をクリックします。
[Summary] ウィンドウにコネクタの設定の詳細情報が表示されます。

ステップ 9 グループとエンドポイントの検出を開始するには、[Done] をクリックします。

グループとエンドポイントの確認

ここでは、各種グループ間のトラフィックを可視化するさまざまな方法について説明します。

複数のグループから複数のグループ

[Overview] ウィンドウの [Security Groups] ボックスに表示されている数をクリックすると、[Explore Security Groups] ウィンドウが表示されます。このウィンドウでは、セキュリティグループのすべてのグループ間通信の概要を確認できます。デフォルトでは、過去 24 時間の時間範囲のデータが表示されます。これは、過去 14 日間に設定された [Overview] ウィンドウの時間範囲とは異なることに注意してください。チャートには、特定の期間に一意のフロー数が多い送信元セキュリティグループなど、上位 25 の送信元セキュリティグループとその対応するやり取りが表示されます。

 アイコンをクリックするとチャートビューが表示され、  をクリックするとテーブルビューが表示されます。

テーブルビューで、特定の行の [See destinations] リンクをクリックすると、選択した送信元セキュリティグループに対応するすべての宛先セキュリティグループが表示されたウィンドウが開き、各宛先セキュリティグループの一意のフロー数が表示されます。

送信元グループをクリックすると、**単一のグループから複数のグループ**のウィンドウが表示されます。

リンクにカーソルを合わせると強調表示され、ツールチップに一意のトラフィックフローの数が表示されます。リンクをクリックすると、**単一のグループから単一のグループ**のウィンドウに切り替わります。

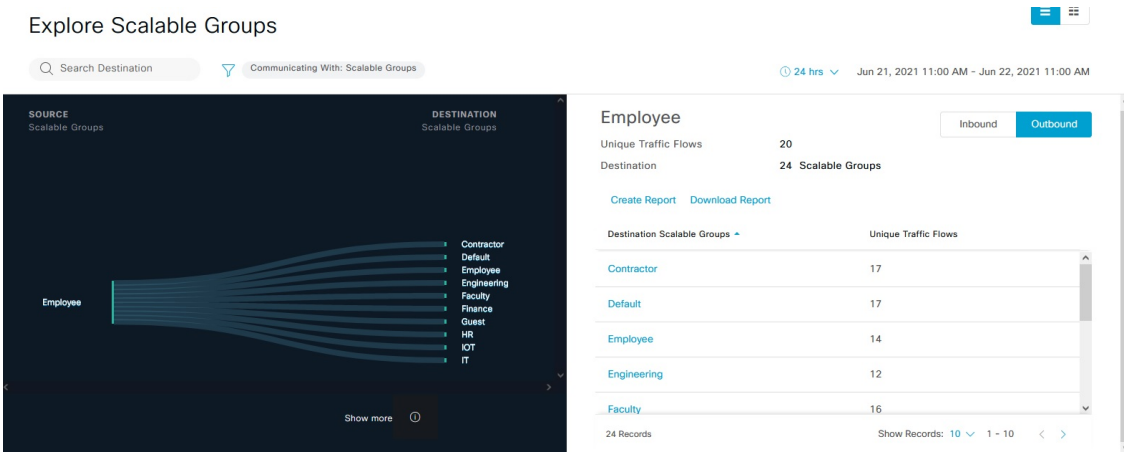
[Overview] ウィンドウの [ISE Profiles] ボックスに表示されている数をクリックすると、[Explore ISE Profiles] ウィンドウが表示されます。このウィンドウでは、送信元が ISE プロファイルで宛先がセキュリティグループであるすべての通信の概要を確認できます。グループベースポリシーを決定することが目的の場合は、このビューで送信元または宛先のいずれかのカテゴリをセキュリティグループにする必要があります。

[Overview] ウィンドウの [Stealthwatch Host Groups] ボックスに表示されている数をクリックすると、[Explore Stealthwatch Host Groups] ウィンドウが表示されます。このウィンドウでは、送信元が Stealthwatch ホストグループで宛先がセキュリティグループであるすべての通信の概要を確認できます。グループベースポリシーを決定することが目的の場合は、このビューで送信元または宛先のいずれかのカテゴリをセキュリティグループにする必要があります。

単一のグループから複数のグループ

単一のグループから複数のグループ：アウトバウンド

このウィンドウには、単一の送信元グループと複数の宛先グループの間のアクティビティが表示されます。送信元と宛先の少なくとも一方がセキュリティグループである必要があります。デフォルトでは過去 24 時間の時間範囲のデータが表示され、表示されるリンクまたはレコードのデフォルト数は 10 です。



アイコンをクリックするとチャートビューが表示され、 をクリックするとテーブルビューが表示されます。

[Outbound] をクリックすると、選択したセキュリティグループから開始された接続が表示されます。[Inbound] をクリックすると、このセキュリティグループに対して別のグループから開始された接続が表示されます。

任意の列をクリックして、昇順または降順で並べ替えることができます。

グループをクリックすると、選択したグループを宛先とする**単一のグループから単一のグループ**のウィンドウが表示されます。送信元グループは変わりません。

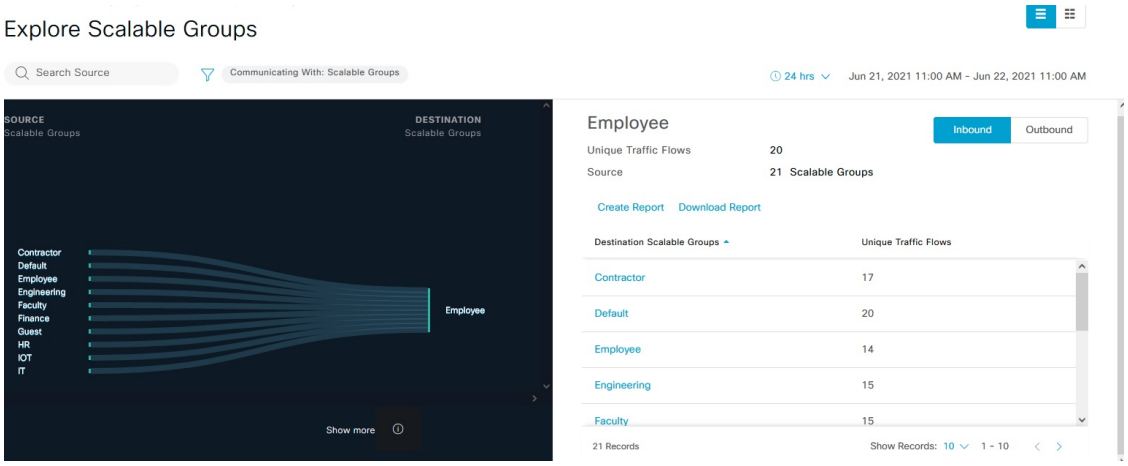
リンクにカーソルを合わせると強調表示され、ツールチップに一意のトラフィックフローの数が表示されます。リンクをクリックすると、**単一のグループから単一のグループ**のウィンドウに切り替わります。

[Create Report] をクリックすると、このビューの情報から CSV 形式の新しいレポートが生成されます。表示される [Reports] ウィンドウで、生成されたレポートを確認できます。このウィンドウから、以前生成されたレポートにアクセスし、レポートをダウンロードすることもできます。

[Download Report] をクリックして、生成されたレポートを表示します。表示される [Reports] ウィンドウで、[Last Run] 列のダウンロードアイコンをクリックするとレポートをダウンロードできます。

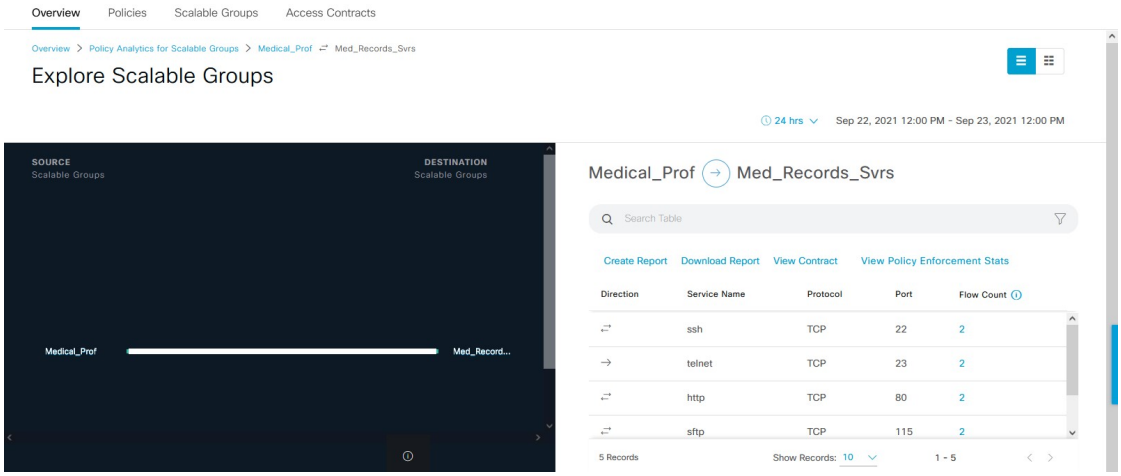
単一のグループから複数のグループ：インバウンド

[Inbound] をクリックすると、選択したセキュリティグループを宛先としていずれかのグループから開始されたすべての接続が表示されます。



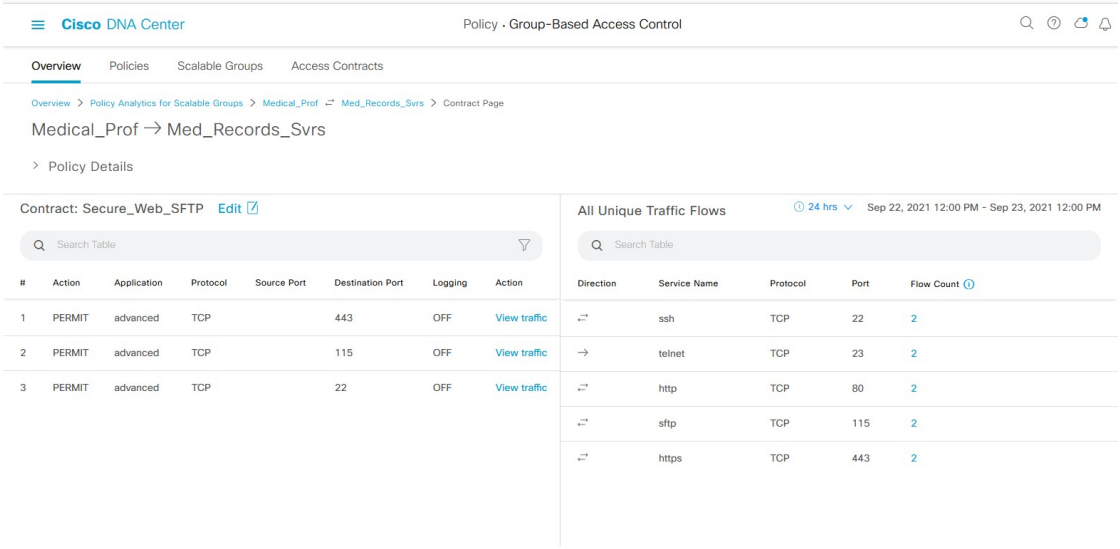
単一のグループから単一のグループ

このウィンドウには、1 つの送信元グループと 1 つの宛先グループの間のアクティビティが表示されます。送信元グループと宛先グループの少なくとも一方がセキュリティグループである必要があります。デフォルトでは過去 24 時間の時間範囲のデータが表示され、表示されるリンクまたはレコードのデフォルト数は 10 です。

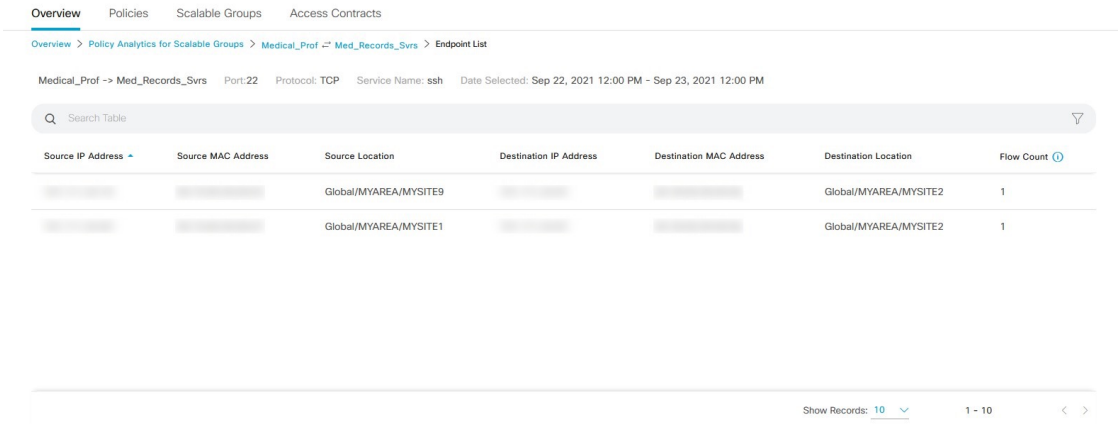


送信元グループと宛先グループの間に表示されている方向矢印をクリックすると、このビューの送信元グループと宛先グループが入れ替わります。

[View Contract] をクリックして、トラフィックフローと、この送信元と宛先グループのペアに有効なアクセス契約のルールを 1 対 1 で比較します。



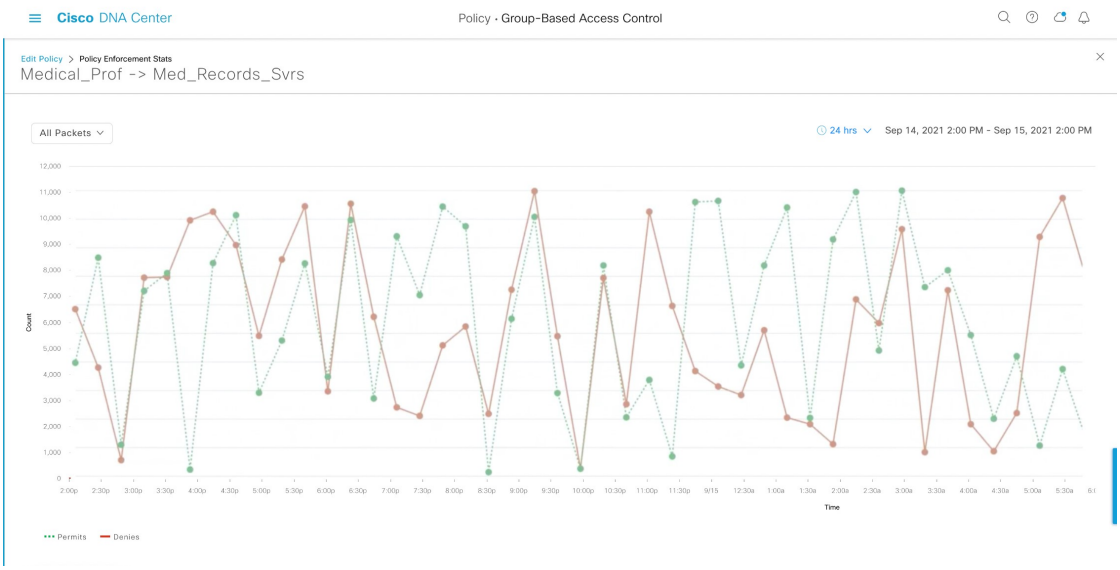
[View Contract] ウィンドウの左側のペインに、送信元グループと宛先グループ間で許可および拒否されるトラフィックのルールが表示されます。右側のペインでは、選択したルールに一致するトラフィックフローを確認できます。右側のペインで、フローの方向、サービス名、フロー数、ポート、およびプロトコルの詳細を表示できます。[Flow Count] 列には、選択した期間に特定のサービス、ポート、およびプロトコルの組み合わせで検出されたフローの数が表示されます。フロー数のリンクをクリックして、各エンドポイントのフローの詳細を表示できます。



（注） フロー数に基づいて [Traffic Flows] テーブルを並べ替えると、1000 レコードのみが表示されます。

[View Policy Enforcement Stats] をクリックして、任意の送信元および宛先グループペアの許可カウントと拒否カウントの時系列グラフを表示します。これにより、ポリシーごとの適用統計情報が可視化されます。[All Packets] ドロップダウンリストを使用して、許可されたパケットまたはドロップされたパケットのみを選択することができます。グラフデータポイントは、15

分のデータ収集期間ごとに表示されます。データポイントにカーソルを合わせると、許可と拒否の数が表示されます。データポイントまたは期間をクリックして、選択した期間の契約とトラフィックフローの詳細を表示できます。



（注） フローデータの集計は 60 分ごとに実行されるため、選択した期間は、選択したデータポイントに対応する 15 分間隔を含む時間になることに注意してください。

ポリシーの作成または編集中に、[Policy Details] スライドインペインから [Traffic Flows] テーブルにアクセスすることもできます。

アイコンをクリックするとチャートビューが表示され、 をクリックするとテーブルビューが表示されます。

日時セレクタを使用して日付と時刻を設定できます。

[Create Report] をクリックすると、このビューの情報から CSV 形式の新しいレポートが生成されます。表示される [Reports] ウィンドウで、生成されたレポートを確認できます。このウィンドウから、以前生成されたレポートにアクセスし、レポートをダウンロードすることもできます。

[Download Report] をクリックして、生成されたレポートを表示します。表示される [Reports] ウィンドウで、[Last Run] 列のダウンロードアイコンをクリックするとレポートをダウンロードできます。

アクセス契約

アクセス契約は [Analytics] ワークフローで直接作成および変更できるようになりました。

View Contract

[View Contract] ウィンドウを起動するには、[Explore Security Groups] ウィンドウで [View Contract] をクリックします。[View Contract] ウィンドウの左側のペインに、送信元グループと宛先グループ間で許可および拒否されるトラフィックのルールが表示されます。右側のペインでは、選択したルールに一致するトラフィックフローを確認できます。

この表には [Policies] ウィンドウからもアクセスできます。メニューアイコン（☰）をクリックして、**[Policy]** > **[Group-Based Access Control]** > **[Policies]** の順に選択します。

ポリシーマトリックスビューで、契約を作成または変更するセルをクリックします。[Policy Details] スライドインペインで、[View Traffic Flows] をクリックします。

現在、送信元グループと宛先グループの間に契約が割り当てられていない場合、データは表示されません。[Change Contract] または [Create Access Contract] オプションを使用して、契約を作成または変更することができます。

[Action] 列の [View traffic] をクリックして、そのルールに一致するフローのリストを表示します。

アクセス契約の作成

[Contract Content] ウィンドウを起動するには、[Policy Details] ペインで [Create Access Contract] をクリックします。トラフィックフィルタルールを作成するには、次の手順を実行します。

1. [Action] ドロップダウンリストで、[Deny] または [Permit] を選択します。
2. From the **APplication** drop-down list, choose the application for which you want to apply that action. ポートとプロトコルは、選択したアプリケーションに基づいて自動的に選択されます。

   トランスポートプロトコル、送信元ポート、および宛先ポートを指定する場合は、[Application] ドロップダウンリストから [Advanced] オプションを選択します。

複数のルールを作成できます。1 つの契約に複数のルールを作成するには、プラスのアイコンをクリックし、[Action] 列と [Application] 列の設定を選択します。ルールは、契約に記載されている順序でチェックされます。ルールの左端にあるハンドルのアイコンを使用して、ルールをドラッグして順序を変更します。

[All Unique Traffic Flows] ペインの [Add to Contract] オプションを使用して契約にエントリを追加することができます。

新しく作成または編集した契約を保存する際は、次のオプションがあります。

- [Update current policy only]：契約の複製が作成され、現在のポリシーに適用されます。この契約を参照する他のポリシーは影響を受けません。
- [Update contract for all referenced policies]：契約が更新され、現在のポリシーとこの契約を参照する他のポリシーに適用されます。
- [Create a new contract with no policies affected]：契約の複製が作成されますが、どのポリシーにも適用されません。

契約の変更

[Change Contract] ウィンドウを起動するには、[Policy Details] ペインで [Change Contract] をクリックします。使用可能なすべての契約が表示されます。必要な契約を選択し、[Change] をクリックすると、その契約をポリシーに追加できます。

契約の編集

[Edit] オプションは、契約がすでにポリシーに追加されている場合にのみ表示されます。契約の詳細を編集するには、契約の名前の後に表示される [Edit] をクリックします。

契約を更新したら、[Save] をクリックします。次のオプションを使用できます。

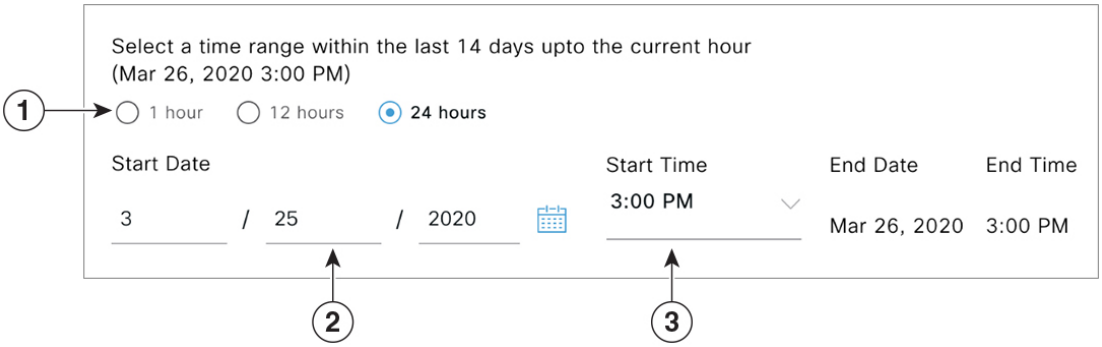
- [Update current policy only]：契約の複製が作成され、現在のポリシーに適用されます。この契約を参照する他のポリシーは影響を受けません。
- [Update contract for all referenced policies]：契約が更新され、現在のポリシーとこの契約を参照する他のポリシーに適用されます。
- [Create a new contract with no policies affected]：契約の複製が作成されますが、どのポリシーにも適用されません。

適切なオプションを選択した後に、名前と説明を入力し（1 つ目または 3 つ目のオプションを選択した場合）、[Confirm] をクリックします。

日時セレクタ

接続の概要を表示する期間を選択できます。過去 14 日から現在の 1 時間までの時間範囲を選択できます。

図 *25 :* 日時セレクタ



1. 次のいずれかのオプションを選択します。[End Time] は自動的に調整されます。
2. 月、日、年を手動で入力するかカレンダーアイコンを使用して [Start Date] を指定します。
3. [Start Time] をドロップダウンメニューから選択します。

検索の使用

[Overview] ウィンドウには、セキュリティグループ、ISE プロファイル、Stealthwatch ホストグループ、IP アドレス、または MAC アドレスのデータ全体を検索するための [Search] フィールドが用意されています。

検索フィールドへの文字入力を開始すると、セキュリティグループ、ISE プロファイル、および Stealthwatch ホストグループの自動検索が実行され、グループタイプごとに最大 3 件の結果が表示されます。MAC アドレスの場合、関連文字は 16 進数とコロンです。

Cisco グループベースポリシー分析は、エンドポイントに対し IPv4 アドレスと IPv6 アドレスの両方をサポートしています。IPv4 または IPv6 アドレスを使用してエンドポイントを検索およびフィルタリングできます。

- 次の文字を使用して、IPv4 アドレスを検索およびフィルタリングできます。
  - 数字（0 ～ 9）
  - ドット（.）

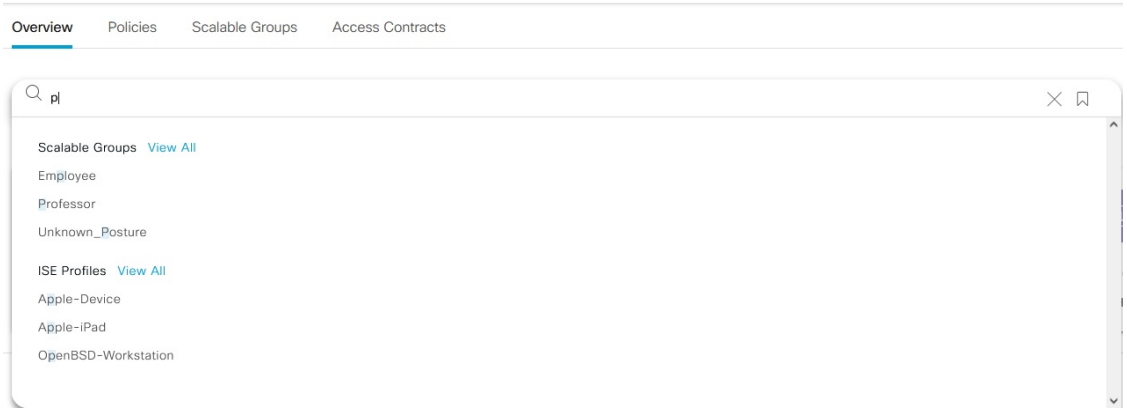
  フィルタフィールドには、最大 15 文字入力できます。
- 次の文字を使用して、IPv6 アドレスを検索およびフィルタリングできます。
  - 数字（0 ～ 9）
  - 小文字と大文字の英字（a～f、A～F）
  - コロン（:）

  フィルタフィールドには、最大 39 文字入力できます。

（注）

- [Search Results] ウィンドウは、[View All] リンクをクリックするまで開きません。
- 読み取り専用ユーザーは、IP アドレスや MAC アドレスは検索できません。詳細については、「ロールベース アクセス コントロール」を参照してください。

図 *26 : [Search]* ウィンドウ



[Focus] ドロップダウンリストから、検索条件を変更するために必要なオプションを選択します。

フィルタのアイコン（ ）は高度なフィルタ処理に使用され、MAC アドレスまたは IP アドレスを検索する場合にのみ使用できます。 アイコンをクリックすると、各列の列名の上に検索フィールドが表示されます。

列ごとの検索条件は、最大 3 つまで入力できます。列ごとの条件を複数入力する場合は、OR 演算または AND 演算を指定できます。このように作成したクエリでは、複数の列を対象に AND 演算が実行されます。

アイコンをクリックして [Save Current Search] オプションを使用すると、現在表示されている検索を保存できます。

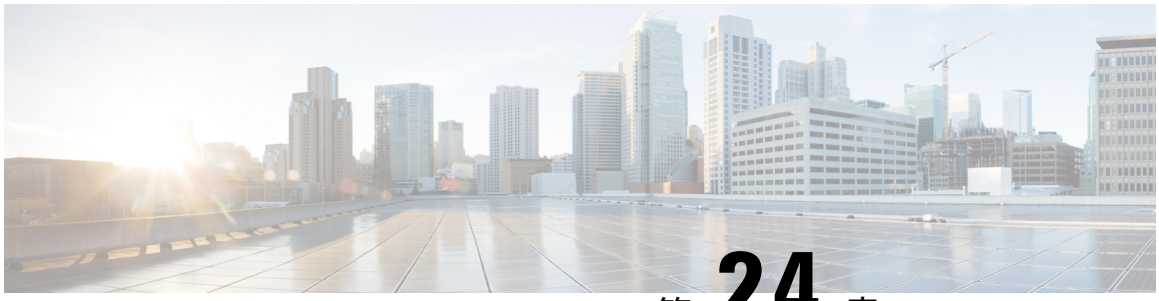
保存した検索を削除するには、 アイコンをクリックします。保存した検索の名前にカーソルを合わせ、 アイコンをクリックします。[Delete Saved Filter] ダイアログボックスで [Yes] をクリックすると、フィルタが完全に削除されます。

ロールベース アクセス コントロール

シスコのグループベースポリシー分析は、ロールベース アクセス コントロールをサポートしています。読み取り/書き込みユーザーと読み取り専用ユーザーが区別されます。ただし、シスコのグループベースポリシー分析は可視化を主としたもので、システムに変更は加えられないため、読み取り専用ユーザーに対する制限は限られたものになります。

- 読み取り専用ユーザーは検索クエリを保存できません。

- 読み取り専用ユーザーは シスコのグループベースのポリシー分析の初期設定 （622 ページ） ウィンドウで変更を行うことはできません。
- データのエクスポートはHTTPS POST操作であるため、読み取り専用ユーザーはデータをエクスポートできません。
- 読み取り専用ユーザーはグループによる検索のみを実行でき、HTTPS POST操作を伴う他の検索機能は実行できません。



第 24 章

IP ベースのアクセス コントロール ポリシーの設定

IP ベースのアクセス コントロール ポリシー

IP ベースのアクセス コントロール ポリシーは、アクセス コントロール リスト（ACL）と同じ方法でシスコ デバイスに出入りするトラフィックを制御します。ACL と同様に、IP ベースのアクセス コントロール ポリシーにはプロトコル タイプ、送信元 IP アドレス、宛先 IP アドレス、宛先ポート番号などのさまざまな条件に基づいてトラフィック フローに適用される許可条件および拒否条件のリストが含まれています。

IP ベースのアクセス コントロール ポリシーを使用して、セキュリティ、モニターリング、ルート選択、ネットワーク アドレス変換などのさまざまな目的のためにトラフィックをフィルタ処理できます。

IP ベースのアクセス コントロール ポリシーには、次の 2 つの主要コンポーネントがあります。

- [IP Network Groups]：IP ネットワーク グループは、同じアクセス制御要件を共有する IP サブネットで構成されています。これらのグループは Cisco DNA Center でのみ定義できます。IP ネットワーク グループに含めることができる IP サブネットは 1 つだけです。
- [Access Contract]：アクセス コントラクトは、IP ベースのアクセス コントロール ポリシーとグループベースのアクセス コントロール ポリシーの両方で使用される共通の構成要素

です。これはアクセス制御ポリシーを構成するルールを定義します。これらのルールでは、トラフィックが特定のポートまたはプロトコルに一致したときに実行されるアクション（許可または拒否）や他のルールが一致しないときに実行される暗黙のアクション（許可または拒否）を指定します。

IP ベースのアクセス コントロール ポリシー設定のワークフロー

始める前に

- 新しい IP ベースのアクセス コントロール ポリシーを作成中に、**[Policy]** > **[IP & URL Based Access Control]** > **[IP Network Groups]** ウィンドウでグループを追加する場合は、Cisco ISE は必須ではありません。
- 次のグローバルネットワーク設定が定義されていることを確認し、デバイスをプロビジョニングします。
  - ネットワークサーバー（AAA、DHCP、DNS サーバーなど）：グローバル ネットワーク サーバーの設定 （230 ページ） を参照してください。
  - CLI、SNMP、HTTP、HTTPS などのデバイスのログイン情報：グローバル デバイス クレデンシャルの概要 （230 ページ）を参照。
  - IP アドレスプール：IP アドレス プールを設定する （241 ページ）を参照。
  - SSID、ワイヤレスインターフェイス、ワイヤレス無線周波数プロファイルなどのワイヤレス設定：グローバル ワイヤレス設定の構成 （247 ページ）を参照。
  - デバイスのプロビジョニング。

ステップ 1 IP ネットワーク グループを作成します。

詳細については、「IP ネットワーク グループの作成 （637 ページ）」を参照してください。

ステップ 2 IP ベースのアクセス制御契約を作成します。

IP ベースのアクセス制御契約は、送信元と宛先の間の一連のルールを定義します。これらのルールは、ネットワーク デバイスが、指定されたプロトコルまたはポートに一致するトラフィックに基づいて実行するアクション（許可または拒否）を指定します。詳細については、「IP ベースのアクセス コントロール契約の作成 （638 ページ）」を参照してください。

ステップ 3 IP ベースのアクセス コントロール ポリシーの作成アクセス コントロール ポリシーは、送信元と宛先の IP ネットワーク グループ間のトラフィックを制御するアクセス制御契約を定義します。

詳細については、IP ベースのアクセス コントロール ポリシーの作成（639 ページ）を参照してください。

グローバル ネットワーク サーバーの設定

ネットワーク全体のデフォルトになるグローバル ネットワーク サーバーを定義することができます。

（注） サイト固有の設定を定義することで、サイトのグローバル ネットワーク設定を上書きできます。

ステップ 1 メニューアイコン（☰）をクリックして、**[Design]** > **[Network Settings]** > **[Network]** の順に選択します。

ステップ 2 **[DHCP Server]** フィールドに、DHCP サーバーの IP アドレスを入力します。

（注） プラスアイコンをクリックすると、IPv4 アドレスと IPv6 アドレスの両方を入力できます。

IP アドレス プールを作成するには、少なくとも 1 つの DHCP サーバーを定義する必要があります。

ステップ 3 **[DNS Server]** フィールドに、DNS サーバーのドメイン名を入力します。

（注） プラスアイコンをクリックすると、IPv4 アドレスと IPv6 アドレスの両方を入力できます。

IP アドレス プールを作成するために、少なくとも 1 つの DNS サーバーを定義する必要があります。

ステップ 4 [Save] をクリックします。

IP ネットワーク グループの作成

ステップ 1 メニューアイコン（☰）をクリックして、**[Policy]** > **[IP & URL Based Access Control]** > **[IP Network Groups]** の順に選択します。

ステップ 2 **[グループの追加（Add Group）]** をクリックします。

ステップ 3 **[名前（Name）]** フィールドに、IP ネットワーク グループの名前を入力します。

ステップ 4 **[説明（Description）]** フィールドに、IP ネットワーク グループを説明する単語またはフレーズを入力します。

ステップ 5 **[IP アドレスまたは IP/CIDR（IP Address or IP/CIDR）]** フィールドに、IP ネットワーク グループを構成する IP アドレスを入力します。

ステップ 6 [Save] をクリックします。

IP ネットワーク グループの編集または削除

ステップ 1 メニューアイコン（☰）をクリックして、**[Policy]** > **[IP & URL Based Access Control]** > **[IP Network Groups]** の順に選択します。

ステップ 2 **[IP ネットワーク グループ（IP Network Groups）]** テーブルで、編集または削除するグループの横にあるチェックボックスをオンにします。

ステップ 3 次のいずれか 1 つのタスクを実行します。

- グループを変更するには、**[編集（Edit）]**をクリックします。フィールドの定義については、IP ネットワーク グループの作成 （637 ページ） を参照してください。必要な変更を行って、[Save] をクリックします。
- グループを削除するには、**[削除（Delete）]** をクリックし、次に **[はい（Yes）]** をクリックして確定します。

IP ベースのアクセス コントロール契約の作成

ステップ 1 メニューアイコン（☰）をクリックして、**[Policy]** > **[IP & URL Based Access Control]** > **[Access Contract]** の順に選択します。

ステップ 2 [コントラクトの追加（Add Contract）] をクリックします。

ステップ 3 契約の名前と説明を入力します。

ステップ 4 **[暗黙的アクション（Implicit Action）]** ドロップダウン リストから、**[拒否（Deny）]** または **[許可（Permit）]** を選択します。

ステップ 5 テーブルの **[アクション（Action）]** ドロップダウン リストから、**[拒否（Deny）]** または **[許可（Permit）]** を選択します。

ステップ 6 **[ポート/プロトコル（Port/Protocol）]** ドロップダウン リストから、ポートまたはプロトコルを選択します。

a) Cisco DNA Centerに必要なポートまたはプロトコルがない場合は、**[ポート/プロトコルの追加（Add Port/Protocol）]** をクリックして、自分で作成します。
b) **[名前（Name）]** フィールドで、ポートまたはプロトコルの名前を入力します。
c) [Protocol] ドロップダウンリストから、[UDP]、[TDP]、または [TCP/UDP] を選択します。
d) **[ポート範囲（Port Range）]** フィールドにポート範囲を入力します。
e) Cisco DNA Centerで定義したとおりにポートまたはプロトコルを設定し、競合をレポートしないようにするには、**[競合を無視する（Ignore Conflict）]** チェックボックスをオンにします。

f) **[保存（Save）]** をクリックします。

ステップ 7 （任意） 契約にさらにルールを含めるには、**[追加（Add）]** をクリックして、手順 5 および 6 を繰り返します。

ステップ 8 [Save] をクリックします。

IP ベースのアクセス コントロール ポリシー契約の編集または削除

ポリシーで使用されている契約を編集すると、**[IP ベースのアクセス コントロール ポリシー（IP Based Access Control Policies）]** ウィンドウのポリシーの状態が **[変更（MODIFIED）]** に変わります。変更されたポリシーは、ネットワークに導入されたポリシーと一致しないため、古いと見なされます。この問題を解決するには、ネットワークにポリシーを再展開する必要があります。

ステップ 1 メニューアイコン（☰）をクリックして、**[Policy]** > **[IP & URL Based Access Control]** > **[Access Contract]** の順に選択します。

ステップ 2 編集または削除する契約の横にあるチェックボックスをオンにして、次のいずれかのタスクを実行します。

- 契約を変更するには、[編集（Edit）]をクリックして変更を行い、[保存（Save）] をクリックします。フィールドの定義については、IP ベースのアクセス コントロール契約の作成 （638 ページ）を参照してください。

  （注） ポリシーで使用されている契約を変更した場合は、**[Policy]** > **[IP & URL Based Access Control]** > **[IP & URL Access Control Policies]**の順に選択し、ポリシー名の横にあるチェックボックスをオンにして、[Deploy] をクリックすることによって、変更したポリシーを展開する必要があります。

- 契約を削除するには、[削除（Delete）] をクリックします。

IP ベースのアクセス コントロール ポリシーの作成

IP ネットワーク グループ間のトラフィックを制限する、IP ベースのアクセス コントロール ポリシーを作成します。

- 1 つのポリシーに異なる設定で複数のルールを追加することができます。
- IP グループと契約の分類子の特定の組み合わせでルールが作成され、デバイスにプッシュされます。この数は、シスコ ワイヤレス コントローラ が ACL でのルールを最大 64 に制限しているため、64 個のルールを超えることはできません。

- **展開された** ポリシー内で使用されるカスタム契約または IP グループが変更された場合、そのポリシーは古いものであり、デバイスにプッシュする新しい設定のために再展開される必要があることを示す [変更済み（Modified）] というステータスでフラグが付けられます。

ステップ 1 メニューアイコン（☰）をクリックして、**[Policy]** > **[IP & URL Based Access Control]** > **[IP & URL Access Control Policies]** の順に選択します。

ステップ 2 [ポリシーの追加（Add Policy）] をクリックします。

ステップ 3 次のフィールドに入力します。

フィールド	説明
Policy Name	ポリシーの名前。
Description	ポリシーを表す単語またはフレーズ。
SSID	SSID の設計中に作成された FlexConnect SSID および 非 FlexConnect SSID をリストします。選択した SSID が FlexConnect モードで設定されている場合、アクセス ポリシーも FlexConnect モードで設定されます。そうでない場合は、通常の方法で設定されます。 （注） SSID が 1 つのポリシーの一部である場合は、その SSID は別のポリシーで使用できません。 ポリシーの展開には有効なサイト SSID の組み合わせが必要です。選択した SSID がデバイスの下でプロビジョニングされていない場合、ポリシーを展開することはできません。
Site Scope	サイトのポリシーが適用される範囲。有線ポリシーを設定すると、ポリシーは、サイト範囲内のすべての有線デバイスに適用されます。同様に、選択したサービス セット識別子（SSID）のワイヤレス ポリシーを設定すると、範囲内で SSID が定義されているすべてのワイヤレス デバイスにポリシーが適用されます。詳細については、サイトの範囲 （644 ページ）を参照してください。
Source	契約の影響を受けるトラフィックの送信元。[Source] ドロップダウンリストから、IP ネットワークグループを選択します。使用したい IP ネットワークがない場合は、[+ グループの追加（+Group）] をクリックして作成します。
Contract	ACL 内で送信元と宛先間のネットワーク連携を管理するルール。[契約の追加（Add Contract）] をクリックして、ポリシーの契約を定義します。ダイアログボックスで、使用する契約の横にあるラジオ ボタンをクリックします。または、契約の [許可（permit）]（すべてのトラフィックを許可）または [拒否（deny）]（すべてのトラフィックを拒否）を選択することもできます。

フィールド	説明
Destination	契約の影響を受けるトラフィックの宛先。[宛先（Destination）] ドロップダウン リストをクリックして、IP ネットワーク グループを選択します。使用したい IP ネットワークがない場合は、[+ IP ネットワーク グループの作成（+Create IP Network Group）] をクリックして作成します。
Direction	送信元と宛先間のトラフィック フローの関係を設定します。送信元から宛先へのトラフィック フローの契約を有効にするには、[一方向（One-Way）] を選択します。両方向（送信元から宛先へ、および宛先から送信元へ）でのトラフィック フローの契約を有効にするには、[双方向（Bi-directional）] を選択します。

ステップ 4 （任意） IP ネットワーク グループを作成するには、[IP ネットワーク グループの作成（Create IP Network Group）] をクリックします。

ステップ 5 （任意） 別のルールを追加するには、プラス記号をクリックします。

（注） ルールを削除するには、[x] をクリックします。

ステップ 6 （任意） ルールの順序を変更するには、変更したい順序でルールをドラッグ アンド ドロップします。

ステップ 7 [Deploy] をクリックします。

「IP ベースのアクセス コントロール ポリシーが作成され、正常に展開されました」という成功メッセージが表示されます。選択した SSID によっては、FlexConnect ポリシーまたは標準ポリシーが異なるマッピング情報レベルで作成され、展開されます。ポリシーの [ステータス（Status）] は、[展開済み（DEPLOYED）] として表示されます。[ポリシー名（Policy Name）] の横にあるワイヤレス アイコンは、展開されたアクセス ポリシーがワイヤレス ポリシーであることを示しています。

IP ベースのアクセス コントロール ポリシーの編集または削除

必要な場合は、IP ベースのアクセス コントロール ポリシーを変更または削除できます。

（注） ポリシーを編集すると、[IPベースのアクセスコントロールポリシー（IP-Based Access Control Policies）] ウィンドウのポリシーの状態が [変更（MODIFIED）] に変わります。変更されたポリシーは、ネットワークに導入されたポリシーと一致しないため、古いと見なされます。この問題を解決するには、ネットワークにポリシーを再展開する必要があります。

ステップ 1 メニューアイコン（☰）をクリックして、**[Policy]** > **[IP & URL Based Access Control]** > **[IP & URL Access Control Policies]** の順に選択します。

ステップ 2 編集または削除するポリシーの横にあるチェック ボックスをオンにして、次のいずれかのタスクを実行します。

- 変更するには、[編集（Edit）] をクリックします。完了したら、[Save] をクリックします。フィールドの定義については、IP ベースのアクセス コントロール ポリシーの作成（639 ページ）を参照してください。
- ポリシーを削除するには、**[削除（Delete）]** をクリックします。

ステップ 3 ポリシーを変更した場合は、ポリシー名の横にあるチェック ボックスをオンにして [展開（Deploy）] をクリックすることによって、変更したポリシーを展開します。

IP ベースのアクセス コントロール ポリシーの展開

ポリシーの設定に影響する変更を加えた場合は、これらの変更を実装するポリシーを再度展開する必要があります。

ステップ 1 メニューアイコン（☰）をクリックして、**[Policy]** > **[IP & URL Based Access Control]** > **[IP & URL Access Control Policies]** の順に選択します。

ステップ 2 展開するポリシーを探します。

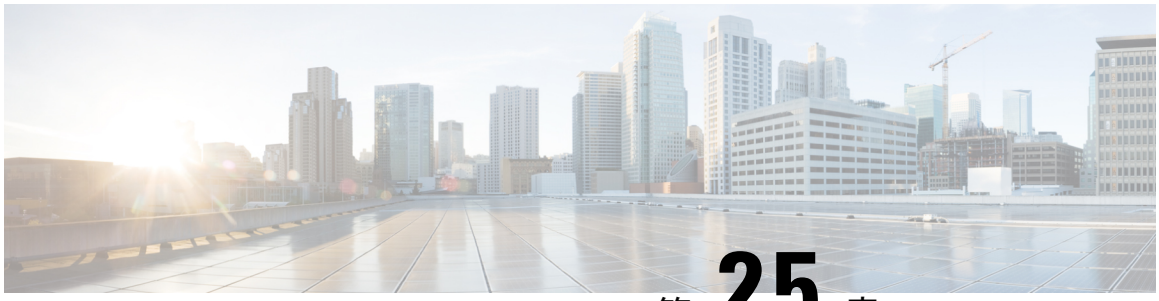
ステップ 3 ポリシーの横にあるチェック ボックスをオンにします。

ステップ 4 [Deploy] をクリックします。
ポリシーを今すぐ展開するか、または後でスケジュールするかどうかを求められます。

ステップ 5 次のいずれかを実行します。

- ポリシーをすぐに展開するには、**[今すぐ実行（Run Now）]** ラジオ ボタンをクリックし、**[適用（Apply）]** をクリックします。
- 将来の日付と時刻でポリシー展開をスケジュールするには、**[後でスケジュール（Schedule Later）]** ラジオ ボタンをクリックし、展開する日時を定義します。

（注） アプリケーション ポリシーの展開のスケジュール設定では、サイトのタイム ゾーンの設定はサポートされていません。



第 25 章

アプリケーションポリシーの設定

アプリケーションポリシーの概要

Quality of Service（QoS）とは、選択したネットワーク トラフィックに、優先的なサービスやニーズに合ったサービスを提供するネットワーク機能を意味します。QoS を設定することで、ビジネスの目標（音声品質が会社の標準規格を満たしていることの保証、ビデオの高い Quality of Experience（QoE）の確保など）を引き続き順守しながら、ネットワーク リソースを最も効率的に使用する方法でネットワーク トラフィックを処理することができます。

QoS は、Cisco DNA Center のアプリケーション ポリシーを使用してネットワークに設定できます。アプリケーション ポリシーは、次の基本的なパラメータで構成されています。

- [Application Sets]：同様のネットワークトラフィックを必要とする一連のアプリケーション。各アプリケーションセットには、トラフィックの優先順位を定義するビジネスとの関連性グループ（ビジネス関連、デフォルト、またはビジネスと無関係）が割り当てられます。QoS パラメータは、Cisco Validated Design（CVD）に基づいて 3 つのグループごとに定義されます。一部のパラメータは、それぞれの目的に合わせてより詳細に調整できます。

- [Site Scope]：アプリケーションポリシーが適用されているサイト。有線ポリシーを設定すると、ポリシーは、サイト範囲内のすべての有線デバイスに適用されます。同様に、選択したサービス セット識別子（SSID）のワイヤレス ポリシーを設定すると、範囲内で SSID が定義されているすべてのワイヤレス デバイスにポリシーが適用されます。

Cisco DNA Center はこれらのパラメータをすべて受け取り、適切なデバイスの CLI コマンドに変換します。Cisco DNA Center はポリシーの展開時に、サイトの範囲で定義されているデバイスに各コマンドを設定します。

（注） Cisco DNA Center はデバイスで使用可能な QoS 機能セットに基づいて、各デバイスに QoS ポリシーを設定します。デバイスの QoS 実装の詳細については、対応するデバイスの製品マニュアルを参照してください。

アプリケーション ポリシーでの CVD ベースの設定

アプリケーション ポリシーのデフォルトの QoS 信頼およびキューイング設定は、Enterprise Medianet の QoS デザイン向けの Cisco Validated Design（CVD）に基づいています。CVD は、一般的な使用例や現行のシステム設計上の優先事項に基づき、システム設計の基盤を提示しています。CVD には、お客様のニーズに応じるための幅広いテクノロジー、機能、アプリケーションが組み込まれています。それぞれのソリューションには、エンジニアによる包括的なテストと文書化が実施されており、迅速で、信頼性が高く、予測可能な導入が確保されています。

QoS に関連する最新の検証済み設計は、Cisco Press の書籍『*End-to-End QoS Network Design: Quality of Service for Rich-Media & Cloud Networks*, 2nd Edition』（http://www.ciscopress.com/store/end-to-end-qos-network-design-quality-of-service-for-9781587143694）で公開されています。追加情報については、次のシスコのドキュメントを参照してください。

- シスコ検証済みデザイン（CVD）
- Enterprise Medianet Quality of Service Design 4.0
- Medianet Campus QoS Design 4.0
- Medianet WAN Aggregation QoS Design 4.0

サイトの範囲

サイト範囲は、アプリケーション ポリシーが適用されるサイトを定義します。ポリシーを定義するときに、ポリシーが有線デバイス用かワイヤレス デバイス用かを設定します。また、サイト範囲も設定します。有線ポリシーを設定すると、ポリシーは、サイト範囲内のすべての有線デバイスに適用されます。同様に、選択したサービス セット識別子（SSID）のワイヤレス ポリシーを設定すると、サイト範囲内で SSID が定義されている、サイト範囲内のすべてのワイヤレス デバイスにポリシーが適用されます。

これにより、有線ネットワーク セグメントとワイヤレス ネットワークセグメントの動作の相違を補うために、必要に応じてトレードオフを実施できます。たとえば、ワイヤレス ネットワークでは通常、有線ネットワークと比較した場合に低帯域幅、低速、パケット損失増加の特徴があります。個々のワイヤレスセグメントは、ローカルの RF 干渉、輻輳、ネットワーク デバイスの機能の違いなどの要因によってさらに変動が見られます。個々のワイヤレスセグメントにセグメントごとのポリシーを適用できるすることで、優先順位の高いトラフィックが受ける、ワイヤレス ネットワークの劣化による影響が小さくなるように、トラフィック処理ルールを調整できます。

ビジネス関連のグループ

ビジネス関連グループは、ビジネスや事業への関連性に応じて、指定されたアプリケーションセットを分類します。

ビジネス関連グループ（ビジネス関連、デフォルト、ビジネスと無関係）は、基本的に3種類のトラフィック（高優先順位、ニュートラル、低優先順位）にマッピングされます。

- **ビジネス関連（Business Relevant）**：（高優先トラフィック）このグループのアプリケーションは組織の目的に直接関与し、音声、ビデオ、ストリーミング、コラボレーション型マルチメディア アプリケーション、データベース アプリケーション、エンタープライズ リソース アプリケーション、電子メール、ファイル転送、コンテンツ配布など、さまざまな種類があります。ビジネス関連として指定されているアプリケーションは、Internet Engineering Task Force（IETF）RFC 4594 の規定に従い、業界推奨のベスト プラクティスに従って処理されます。
- **デフォルト（Default）**：（平均的優先度のトラフィック）このグループは、ビジネスに関連している場合もあればしていない場合もあるアプリケーションを対象としています。たとえば一般的な HTTP または HTTPS トラフィックは、組織の目的に寄与する場合もしない場合もあります。たとえば、レガシーアプリケーションや新しく導入されたアプリケーションなどでも、一部のアプリケーションの目的については分析していない場合があります。したがって、これらのアプリケーションのトラフィック フローは、IETF RFC 2747 および 4594 で説明されているように、デフォルトの転送サービスで処理する必要があります。
- **ビジネスと無関係（Business Irrelevant）**：（低優先トラフィック）このグループは、組織の目的達成に寄与しないと識別されたアプリケーションを対象としています。主にコンシューマ向けかエンターテイメント向け、あるいは本質的にその両方に該当するアプリケーションです。この種類のトラフィックは、IETF RFC 3662 および 4594 で説明されている「スカベンジャ」サービスとして処理することをお勧めします。

アプリケーションはアプリケーションセットに分類されて、ビジネス関連グループにソートされます。アプリケーションセットはポリシーに現状のまま含めることができます。または、ビジネス目標やネットワーク構成のニーズを満たすように変更することができます。

たとえば、YouTube はコンシューマ メディア アプリケーション セットのメンバーです。一般的に、ほとんどのお客様がこのアプリケーションをこのように分類しているため、（デフォルトでは）YouTube はビジネスと無関係です。ただし、この分類がすべての企業に当てはまるわけではありません。たとえば、いくつかのビジネスでは YouTube をトレーニング目的で使用することがあります。このような場合、管理者は、デフォルトでビジネス関連であるストリーミング ビデオ アプリケーション セットに YouTube アプリケーションを移動できます。

コンシューマとプロデューサ

あるアプリケーションから別のアプリケーションにトラフィックが送られた（特定の a から b へのトラフィック フローが作成された）ときにトラフィックが特定の方法で処理されるよう

に、アプリケーション間の関係を設定することができます。このような関係のアプリケーションをプロデューサとコンシューマと呼び、次のように定義しています。

- **プロデューサ**：アプリケーション トラフィックの送信元。たとえば、クライアント/サーバー アーキテクチャでは、トラフィック フローは主にサーバーからクライアントの方向であるため、アプリケーション サーバーがプロデューサと見なされます。ピアツーピア アプリケーションの場合は、リモート ピアがプロデューサと見なされます。
- **コンシューマ**：アプリケーション トラフィックの受信者。コンシューマに該当するのは、クライアント/サーバ アーキテクチャの場合はクライアント エンドポイント、ピアツーピア アプリケーションの場合はローカル デバイスなどです。コンシューマはエンドポイントデバイスの場合がありますが、そのようなデバイスの特定のユーザーの場合もあります（通常、IP アドレスまたは特定のサブネットによって識別される）。また、あるアプリケーションが別のアプリケーション トラフィック フローのコンシューマになる場合もあります。

この関係を設定することにより、このシナリオに一致するトラフィックに関して特定のサービスレベルを設定できます。

マーキング、キューイング、ドロッピングの処理

Cisco DNA Center は、IETF RFC 4594 およびアプリケーションに割り当てられたビジネス関連のカテゴリでの処理のマーキング、キューイング、およびドロッピングをベースとしています。Cisco DNA Center は、デフォルト カテゴリのすべてのアプリケーションをデフォルトの転送アプリケーション クラスに割り当て、無関係なビジネス カテゴリのすべてのアプリケーションをスカベンジャ アプリケーション クラスに割り当てます。関連するビジネス カテゴリのアプリケーションについては、Cisco DNA Center はアプリケーションのタイプに基づいてトラフィック クラスをアプリケーションに割り当てます。次の表に、アプリケーションクラスとそれぞれの処理を示します。

表 *50*：マーキング、キューイング、ドロッピングの処理

ビジネス関連性	アプリケーションクラス	ホップ毎の挙動	キューイングとドロッピング	アプリケーションの説明
該当する	VoIP[5]	Expedited Forwarding（EF）	プライオリティキューイング（PQ）	VoIP テレフォニー（ベアラのみ）トラフィック。たとえば、Cisco IP 電話。
	ブロードキャストビデオ	クラス セレクタ（CS）5	PQ	ブロードキャスト TV、ライブイベント、ビデオ監視フロー、同様の非弾性ストリーミング メディア フロー（Cisco IP Video Surveillance や Cisco Enterprise TV など）。（非弾性フローとは、非常にドロップされやすく、再送信またはフロー制御機能のいずれか、または両方がないフローを意味します。）
	リアルタイムインタラクティブ	CS4	PQ	非弾性の高解像度インタラクティブ ビデオ アプリケーションおよびそれらのアプリケーションのオーディオおよびビデオコンポーネント（Cisco TelePresence など）。
	マルチメディア会議	相対的優先転送（AF）41	帯域幅（BW）キューと Differentiated Services Code Point（DSCP）Weighted Random Early Detect（WRED）	デスクトップソフトウェアのマルチメディア コラボレーション アプリケーションおよびそれらのアプリケーションのオーディオおよびビデオコンポーネント（Cisco Jabber や Cisco Webex など）。
	マルチメディアストリーミング	AF31	BW キューと DSCP WRED	ビデオオンデマンド（VoD）ストリーミング ビデオフローおよび仮想デスクトップアプリケーション。たとえば、Cisco Digital Media System。
	ネットワーク制御	CS6	BW キューのみ[6]	EIGRP、OSPF、BGP、HSRP、IKE などのエンタープライズ ネットワークの信頼性の高い運用のために必要とされるネットワーク コントロール プレーン トラフィック。
	シグナリング	CS3	BW キューと DSCP	IP 音声およびビデオ テレフォニー インフラストラクチャのコントロールプレーン トラフィック。
	Operations, Administration, and Management（OAM）	CS2	BW キューと DSCP[7]	SSH、SNMP、syslog などのネットワーク運用、管理、管理トラフィック
		AF21		

ビジネス関連性	アプリケーションクラス	ホップ毎の挙動	キューイングとドロッピング	アプリケーションの説明
	トランザクションデータ（低遅延データ）		BW キューと DSCP WRED	エンタープライズ リソース プランニング（ERP）、顧客関係管理（CRM）、およびその他のデータベース アプリケーションなどのインタラクティブ（フォアグラウンド）データ アプリケーション。
	バルクデータ（高スループットデータ）	AF11	BW キューと DSCP WRED	電子メール、File Transfer Protocol（FTP）、バックアップ アプリケーションなどの非インタラクティブ（バックグラウンド）データ アプリケーション。
デフォルト	デフォルトの転送（ベストエフォート）	DF	デフォルト キューと RED	デフォルトのアプリケーション、およびデフォルトのビジネス関連グループに割り当てられるアプリケーション。プライオリティ、保証された帯域幅、または差分サービス クラスに割り当てられるのはごく少数のアプリケーションであるため、大部分のアプリケーションは引き続きデフォルトでベストエフォート型サービスになります。
非関連	スカベンジャー	CS1	最小 BW キュー（ディファレンシャル）と DSCP	非ビジネス関連のトラフィック フロー、およびビジネス関連でないグループに割り当てられているアプリケーション（エンターテイメント向けのデータやメディア アプリケーションなど）。たとえば、YouTube、Netflix、iTunes、Xbox Live。

[5] VoIP シグナリング トラフィックは、コール シグナリング クラスに割り当てられます。
[6] ネットワーク制御トラフィックはドロップされるべきではないため、このクラスでは WRED が有効になりません。
[7] OAM トラフィックはドロップされるべきではないため、このクラスでは WRED が有効になりません。

サービス プロバイダのプロファイル

サービス プロバイダ（SP）プロファイルは、特定の WAN プロバイダのサービス クラスを定義します。4 クラス、5 クラス、6 クラス、8 クラスのモデルを定義できます。

アプリケーション ポリシーがデバイスに展開されると、各 SP プロファイルには、各 SP クラスを DSCP 値と帯域幅割り当てのパーセンテージにマップする特定のサービス レベル契約（SLA）が割り当てられます。

アプリケーション ポリシーを設定するときに SP プロファイルの DSCP 値と 帯域幅割り当てのパーセンテージをカスタマイズできます。

SPプロファイルを作成したら、そのプロファイルをWANインターフェイスで設定する必要があります。

表 *51 : 4* クラスでの *SP* プロファイルのデフォルト *SLA* 属性

クラス名	DSCP	プライオリティクラス	SLA	
			帯域幅（%）	Remaining Bandwidth (%)
音声	EF	はい	10	—
クラス 1 データ	AF31	—	—	44
クラス 2 データ	AF21	—	—	25
デフォルト	0	—	—	31

表 *52 : 5* クラスでの *SP* プロファイルのデフォルト *SLA* 属性

クラス名	DSCP	プライオリティクラス	SLA	
			帯域幅（%）	Remaining Bandwidth (%)
音声	EF	はい	10	—
クラス 1 データ	AF31	—	—	44
クラス 2 データ	AF21	—	—	25
クラス 3 データ	AF11	—	—	1
デフォルト	ベストエフォート	—	—	30

表 *53 : 6* クラスでの *SP* プロファイルのデフォルト *SLA* 属性

クラス名	DSCP	プライオリティクラス	SLA	
			帯域幅（%）	Remaining Bandwidth (%)
クラス 1 データ	AF31	—	—	10
クラス 3 データ	AF11	—	—	1
ビデオ	AF41	—	—	34
音声	EF	はい	10	—
デフォルト	0	—	—	30

クラス名	DSCP	プライオリティ クラス	SLA	
			帯域幅（%）	Remaining Bandwidth (%)
クラス 2 データ	AF21	—	—	25

表 *54 : 8* クラスでの *SP* プロファイルのデフォルト *SLA* 属性

クラス名	DSCP	プライオリティ クラス	SLA	
			帯域幅（%）	Remaining Bandwidth (%)
ネットワーク-コントロール管理	CS6	—	—	5
ストリーミング ビデオ	AF31	—	—	10
コール シグナリング	CS3	—	—	4
スカベンジャー	CS1	—	—	1
インタラクティブ ビデオ	AF41	—	—	30
音声	EF	はい	10	—
デフォルト	0	—	—	25
重要なデータ	AF21	—	—	25

キューイング プロファイル

キューイング プロファイルでは、インターフェイス速度とトラフィック クラスに基づいたインターフェイスの帯域幅割り当てを定義することができます。

（注） キューイングプロファイルは、サービス プロバイダ プロファイルに接続されている WAN 側インターフェイスには適用されません。

次のインターフェイス速度がサポートされます。

- 100 Gbps
- 10/40 Gbps
- 1 Gbps

- 100 Mbps
- 10 Mbps
- 1 Mbps

インターフェイスの速度が 2 つのインターフェイス速度の間である場合、Cisco DNA Center は、より低いインターフェイス速度でインターフェイスを取り扱います。

（注） Cisco DNA Center は、正しいポリシーを適用するためにインターフェイスの動作速度の検出を試みます。ただし、スイッチ ポートが管理上ダウンしている場合、Cisco DNA Center は速度を検出できません。この場合、Cisco DNA Center は、インターフェイスのサポートされた速度を使用します。

キューイング ポリシーは、アプリケーション ポリシーの一部として定義します。アプリケーション ポリシーを展開すると、サイト範囲内の選択されたサイトのデバイスが、割り当てられた LAN キューイング ポリシーで設定されます。LAN キューイング ポリシーが割り当てられていない場合、アプリケーション ポリシーはデフォルトの CVD キューイング ポリシーを使用します。

すでに展開されているアプリケーション ポリシーのキューイング ポリシーを変更すると、ポリシーは失効し、変更をデバイスに適用するにはポリシーを展開しなおす必要があります。

キューイング ポリシーに関する次の追加の注意事項および制約事項に注意してください。

- LAN キューイング プロファイルは、ポリシーで使用されている場合には削除できません。
- ポリシーに関連付けられているキューイング プロファイルを更新すると、ポリシーは期限切れとしてマーキングされます。最新の変更をプロビジョニングするには、ポリシーを展開しなおす必要があります。
- トラフィック クラス キューイングをカスタマイズしても、シスコのサービス プロバイダ スイッチおよびルータのインターフェイスは影響を受けません。これらのインターフェイスの設定は、引き続き Cisco DNA Center を使用することなく実施します。

表 *55* : デフォルト *CVD LAN* キューイング ポリシー

トラフィック クラス	デフォルトの帯域幅（合計= 100%）[8]
ビジネス関連の音声	10%
ビジネス関連のブロードキャストビデオ	10%
ビジネス関連のリアルタイム インタラクティブ	13%
ビジネス関連のマルチメディア会議	10%

トラフィック クラス	デフォルトの帯域幅（合計= 100%）[8]
ビジネス関連のマルチメディア ストリーミング	10%
ビジネス関連のネットワーク制御	3%
ビジネス関連のシグナリング	2%
ビジネス関連の OAM	2%
ビジネス関連のトランザクションデータ	10%
ビジネス関連のバルクデータ	4%
ビジネス関連のスカベンジャ	1%
ビジネス関連のベストエフォート	25%

[8] 音声、ブロードキャストビデオ、およびリアルタイムインタラクティブ トラフィック クラスの合計帯域幅を 33% 以下にすることを推奨します。

リソースが制限されているデバイスの処理順

ネットワーク デバイスの中には、ネットワーク アクセス コントロール リスト（ACL）および ACE を格納するためのメモリ（TCAM と呼ばれる）が制限されているものがあります。このため、アプリケーション用の ACL と ACE がこれらのデバイス上に設定されている場合は、利用可能な TCAM 領域が使用されます。When the TCAM space is depleted, QoS settings for additional applications cannot be configured on that device.

そのようなデバイスで最も重要なアプリケーションの QoS ポリシーが確実に設定されるように、Cisco DNA Center は次の順序で TCAM スペースを割り当てます。

1. [Rank]：カスタムアプリケーションおよびお気に入りのアプリケーションに割り当てられた番号（ただし既存のデフォルト NBAR アプリケーションは除く）。ランクの番号が小さくなるほど、優先順位が高くなります。たとえば、ランク 1 のアプリケーションはランク 2 のアプリケーションよりも優先順位が高くなります。ランクがない場合は、優先順位が最も低くなります。

（注）
- カスタム アプリケーションには、デフォルトでランク 1 が割り当てられています。
- NBAR アプリケーションをお気に入りとしてマークすると、ランクは 1000 に設定されます。

2. [Traffic Class]：優先順位は次の順序に基づいています。シグナリング、バルクデータ、ネットワーク制御、Operations Administration Management（Ops Admin Mgmt）、トランザクショ

ンデータ、スカベンジャ、マルチメディアストリーミング、マルチメディア会議、リアルタイム インタラクティブ、ブロードキャストビデオ、VoIP テレフォニー。

3. [Popularity]：CVD の基準に基づいて割り当てられた番号（1 ～ 10）。ポピュラリティの番号は変更できません。ポピュラリティが 10 のアプリケーションは、ポピュラリティが 9 のアプリケーションよりも優先順位が高くなります。

（注）
- カスタムアプリケーションには、ポピュラリティ 0 が割り当てられます。
- デフォルト NBAR アプリケーションには、CVD の基準に基づいてポピュラリティ番号（1 ～ 10）が割り当てられます。アプリケーションをお気に入りとしてマークしても、ポピュラリティ番号は変わりません（ランクのみ変更されます）。

4. [Alphabetization]：2 つ以上のアプリケーションのランクとポピュラリティ番号が同一の場合、それらのアプリケーションはアプリケーション名のアルファベット順にソートされ、ソート順に従い優先順位が割り当てられます。

たとえば、次のアプリケーションを指定したポリシーを定義する場合を想定しましょう。

- カスタム アプリケーション custom_realtime。デフォルトでランク 1 とポピュラリティ 10 が割り当てられています。
- カスタム アプリケーション custom_salesforce。デフォルトでランク 1 とポピュラリティ 10 が割り当てられています。
- corba-iiop という名前のトランザクション データ トラフィック クラスのアプリケーション。お気に入りとして指定されており、ランク 10,000、および（CVD に基づいて）ポピュラリティ 9 が付与されています。
- gss-http という名前の Ops Admin Mgmt トラフィック クラスのアプリケーション。お気に入りとして指定されており、ランク 10,000、および（CVD に基づいて）ポピュラリティ 10 が付与されています。
- 他のすべてのデフォルト NBAR アプリケーションにはランクはありませんが、トラフィック クラスと（CVD に基づいて）デフォルト ポピュラリティに従って処理されます。

優先順位付けのルールに従って、アプリケーションはデバイスにおいて次の順序で設定されます。

アプリケーションの設定順	理由
1. カスタム アプリケーション custom_realtime	カスタム アプリケーションには最も高い優先順位が付与されます。custom_salesforce アプリケーションと custom_realtime アプリケーションのランクおよびポピュラリティが同じであるとすると、これらのアプリケーションはアルファベット順にソートされ、custom_realtime が custom_salesforce より前になります。
2. カスタム アプリケーション custom_salesforce	

アプリケーションの設定順	理由
3. お気に入りのアプリケーション gss-http	これら両方のアプリケーションはお気に入りとして指定されているため、同じアプリケーション ランクになります。そのため、Cisco DNA Center は各アプリケーションをトラフィック クラスに基づいて評価します。gss-http は Ops Admin Mgmt トラフィッククラスに属しているため最初に処理され、その後、トランザクション データ トラフィック クラスに属している corba-iiop アプリケーションが処理されます。トラフィック クラスによって処理順が決まっているため、ポピュラリティは考慮されません。
4. お気に入りのアプリケーション corba-iiop	
5. 他のすべてのデフォルト NBAR アプリケーション	他のすべてのアプリケーションは、トラフィック クラスとポピュラリティに従って次に優先され、ポピュラリティが同じアプリケーションは、アプリケーション名のアルファベット順にソートされます。

ポリシーのドラフト

ポリシーを作成するときに、ポリシーを展開せずにドラフトとして保存できます。ドラフトとして保存すると、後でポリシーを開いて変更できます。また、展開したポリシーを変更して、ドラフトとして保存することもできます。

（注） ポリシーを保存または展開した後に、名前を変更することはできません。

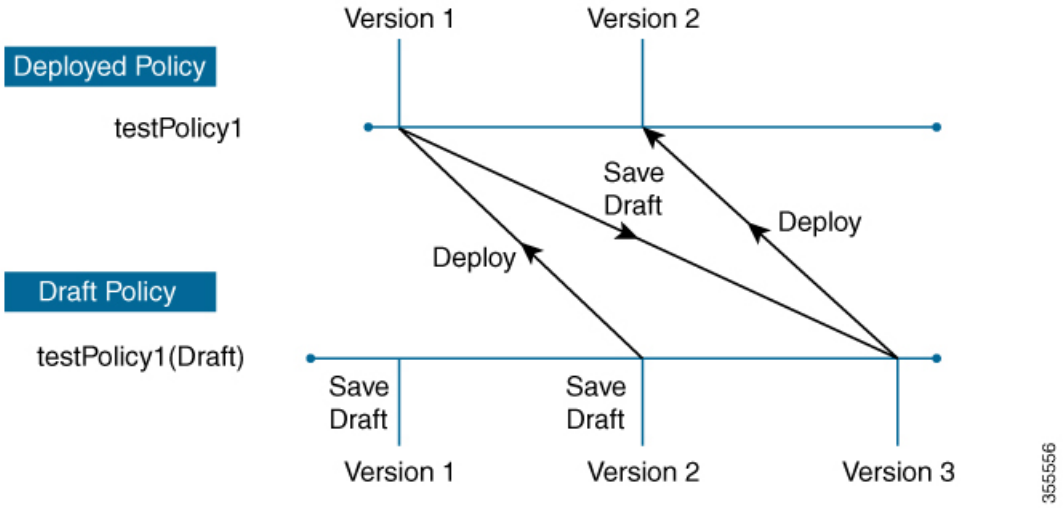
ドラフトポリシーと展開したポリシーは相互に関連付けられますが、それぞれ独自にバージョン管理されます。

ポリシーをドラフトとして保存すると、Cisco DNA Center はポリシー名に (Draft) を追加してバージョン番号を 1 つ上げます。ポリシーを展開すると、Cisco DNA Center が展開したポリシーのバージョン番号を 1 つ上げます。

たとえば、次の図に示すように、testPolicy1 という名前のポリシーを作成してドラフトとして保存します。ポリシーは testPolicy1 (Draft)、バージョン番号 1 として保存されます。ドラフトを変更して、再度保存します。ポリシーの名前は同じ testPolicy1 (Draft) のままですが、バージョン番号は 2 に上がります。

ポリシーが気に入ったのでネットワークに展開します。ポリシーは testPolicy1 という名前で展開され、バージョン番号は 1 です。展開したポリシーを変更して、ドラフトとして保存します。ドラフトポリシー testPolicy1 (Draft) は、バージョン番号 3 に上がります。最終的にそのバージョンを展開するとき、testPolicy1 はバージョン 2 になります。

図 *27* : 展開したポリシーとドラフト ポリシーのバージョン管理



ドラフトポリシーまたは展開したポリシーのいずれかを変更および保存するときは、ドラフトポリシーのバージョン番号が上がります。同様に、ドラフトポリシーまたは変更した展開済みポリシーのいずれかを展開するときは、展開したポリシーのバージョンが上がります。

展開したポリシーと同様に、ドラフト ポリシーの履歴を表示し、以前のバージョンにロールバックすることができます。

ポリシー バージョンの履歴表示と以前のバージョンへのロール バックについては、ポリシーのバージョン管理 （656 ページ）を参照してください。

ポリシーのプレビュー

ポリシーを展開する前に、デバイスに適用される CLI を生成できます。

プレビュー操作では、ポリシーのCLIコマンドが生成され、デバイスの実行コンフィギュレーションのCLIコマンドと比較され、デバイスでポリシーを設定するのに必要な残りのCLIだけが返されます。

プレビュー出力の確認後、範囲内の全デバイスにポリシーを展開するか、ポリシーの変更を続行することができます。

ポリシーの事前チェック

アプリケーションポリシーを作成するとき、ポリシーを展開する前に、サイト範囲のデバイスでサポートされるかどうかを確認できます。事前チェック機能では、デバイス タイプ、モデル、ライン カード、およびソフトウェア イメージが作成したアプリケーション ポリシーをサポートするかどうかチェックします。これらのコンポーネントのいずれかがサポートさCisco DNA Centerれていない場合、はデバイスの障害を報告します。Cisco DNA Centerまた、障害を修正する方法についても説明します。これらの対応で障害が修正されない場合、サイト範囲からデバイスを削除できます。

アプリケーション ポリシーをそのまま展開すると、事前チェック プロセス中に障害が報告されたデバイスでポリシー展開が失敗します。失敗を回避するには、サイト範囲からデバイスを削除するか、デバイス コンポーネントをアプリケーション ポリシーがサポートするレベルに更新します。サポートされるデバイスのリストについては、『Cisco DNA Center Compatibility Matrix』を参照してください。

ポリシーのスケジューリング

ポリシーを作成または変更した後に、そのポリシーを、ポリシーに関連付けられたデバイスに展開または再展開できます。このポリシーの展開/再展開は、すぐに行うことも、特定の日時（たとえば、週末のオフピーク時）に行うこともできます。ポリシー導入のスケジューリングは有線またはワイヤレスのデバイスに対して実施できます。

展開するポリシーのスケジュールを設定すると、そのポリシーとサイト範囲がロックされます。ポリシーの表示は可能ですが、編集することはできません。ポリシーを展開する予定が変更された場合は、その展開をキャンセルできます。

（注） スケジュール イベントが発生すると、ポリシーは、さまざまなポリシー コンポーネント（アプリケーション、アプリケーションセット、およびキューイング プロファイルなど）に対して検証されます。この検証に失敗すると、ポリシーの変更は行われません。

ポリシーのバージョン管理

このポリシーのバージョン管理により、次のタスクが可能になります。

- 以前のバージョンと現在（最新）のバージョンを比較して相違点を確認する。
- ポリシーの以前のバージョンを表示し、サイト範囲内のデバイスに再適用するバージョンを選択する。

あるバージョンのポリシーを編集しても、そのポリシーの別のバージョンやポリシーのコンポーネント（そのポリシーによって管理されるアプリケーションセットなど）は影響を受けません。たとえば、ポリシーからアプリケーションセットを削除しても、そのアプリケーションセットは Cisco DNA Center、そのポリシーの別のバージョン、または他のポリシーからは削除されません。ポリシーとアプリケーションセットは互いに独立して存在するため、存在しなくなったアプリケーションセットを含むバージョンのポリシーを保持できます。存在しなくなったアプリケーションセットを参照するポリシーを展開しようとしたり、それらのポリシーを古いバージョンにロールバックしようとしたりすると、エラーが発生します。

（注） ポリシーのバージョン管理では、アプリケーション（ランク、ポート、プロトコルなど）、アプリケーション セット メンバー、LAN キューイング プロファイル、およびサイトの変更は取得されません。

オリジナルポリシーの復元

初めてデバイスにポリシーを展開する際、Cisco DNA Centerは、デバイスの元のCisco Modular QoS CLIポリシー設定をデタッチしますが、それらはデバイス上に残ります。Cisco DNA Centerは、デバイスの元のNBAR設定をCisco DNA Centerに保存します。このアクションにより、必要に応じてオリジナルのモジュラー式QoS CLIポリシーとNBAR設定を後でデバイスに復元することが可能になります。

（注） このようにモジュラー式QoS CLIポリシーはデバイスから削除されませんが、ユーザーがこれらのポリシーを削除すると、元のポリシー復元するCisco DNA Centerの機能を使用してそれらを復元することができなくなります。

元のポリシー設定をデバイスに復元する際、Cisco DNA Centerは、展開されている既存のポリシー設定を削除し、デバイス上にあった元の設定に戻します。

アプリケーション ポリシーを展開する前に存在していたモジュラー式QoS CLIポリシー設定はすべて、インターフェイスに再アタッチされます。ただし、マルチレイヤ スイッチング（MLS）設定などのキューイング ポリシーは復元されません。代わりに、デバイスは、Cisco DNA Centerによって最後に適用されたMLS設定を維持します。

元のポリシー設定をデバイスに復元すると、Cisco DNA Centerに保存されているポリシーが削除されます。

この機能には、次のような追加のガイドラインと制限事項があるので、注意してください。

- 初めてポリシーをデバイスに展開する試みが失敗すると、Cisco DNA Centerは、元のポリシー設定をデバイスに復元することを自動的に試みます。
- そのポリシーがデバイスに適用された後にデバイスがアプリケーションポリシーから削除された場合、そのポリシーはデバイス上に残ります。Cisco DNA Centerは、ポリシーを自動的に削除したり、デバイスのQoS設定を元の(事前Cisco DNA Center)設定に復元したりしません。

陳腐化したアプリケーション ポリシー

ポリシーで参照されているものの設定を変更すると、アプリケーションポリシーが陳腐化する可能性があります。アプリケーションポリシーが陳腐化した場合、変更を有効化するためにアプリケーション ポリシーを再展開する必要があります。

アプリケーション ポリシーは、次の理由で陳腐化する可能性があります。

- アプリケーション設定で参照されているアプリケーションの変更。
- SPプロファイルの割り当て、WANサブ回線のレート、WANまたはLANマーキングなどのインターフェイスの変更。
- キューイング プロファイルの変更。

- ポリシーの親サイト下への新規サイトの追加。
- ポリシーによって参照されるサイトへのデバイスの追加。
- ポリシーが同じサイト間でのデバイスの移動。
- インターフェイス除外/包含の変更。
- デバイスコントローラベースのアプリケーション認識（CBAR）ステータスの変更。

アプリケーション ポリシーのガイドラインと制限事項

- Cisco DNA Center は、ワイヤレスコントローラ上で同じ SSID 名を使用して複数の WLAN を学習できません。シスコ ワイヤレス コントローラ には、名前は同じで WLAN プロファイル名が異なる複数のエントリを含めることもできますが、Cisco DNA Center はどの時点においても、一意の名前を持つ WLAN に対するエントリを 1 つだけ持ちます。

  ワイヤレスコントローラ ごとに重複する SSID 名を意図的に持つことも、Cisco DNA Center を使用して重複する SSID 名を持つ ワイヤレスコントローラ を誤って追加してしまうこともあります。いずれの場合も、ワイヤレスコントローラ ごとに重複する SSID 名を持つことは一部の機能にとって問題になります。

  - **設定の学習**：Cisco DNA Center は ワイヤレスコントローラ ごとにランダムに選択された 1 つの SSID 名のみ学習し、残りの重複する SSID 名はすべて破棄します。（**設定の学習**は、通常は既存の展開シナリオで使用されます。）
  - [Application Policy]：Cisco DNA Center は、アプリケーションポリシーの展開時に、重複するいずれかの SSID 名にのみポリシーをランダムに適用して、他には適用しません。さらに、ポリシーの復元、CLI プレビュー、EasyQoS ファーストレーン、および PSK オーバーライド機能が失敗するか、予期しない結果が生じることになります。
  - [Multiscale Network]：MULTISCALE ネットワークでは、複数のデバイスの複数の重複する SSID 名が原因で問題が発生することがあります。たとえば、1 台のデバイスには非ファブリック SSID として WLAN が設定されていて、2 台目のデバイスには同じ WLAN がファブリック SSID として設定されている場合、[設定の学習（Learn Config）] を実行すると、1 つの SSID 名のみ学習されます。その他のデバイスの他の SSID 名は破棄されます。この動作により、特に、2 台目のデバイスがファブリック SSID 名のみサポートしていて、Cisco DNA Center が非ファブリック SSID 名を持つデバイスに対して操作を実行しようとする場合に競合が生じることがあります。
  - [IPACL Policy]：Cisco DNA Center は、IPACL ポリシーの展開時に、重複する SSID のいずれか 1 つにのみランダムにポリシーを適用します。また、Flex Connect が関係するシナリオも影響を受けます。

- Cisco DNA Center では、デバイス設定に対するアウト オブ バンド（OOB）の変更は推奨されません。OOB に変更を加えると、Cisco DNA Center のポリシーとデバイスに設定されているポリシーは一貫性のない状態になります。2 つのポリシーは、Cisco DNA Center のポリシーをデバイスに再度展開するまで一貫性のない状態のままになります。

- QoS trust 機能は変更できません。
- ワイヤレスコントローラではカスタムアプリケーションはサポートされていません。したがって、ワイヤレス アプリケーション ポリシーの作成時にはカスタムアプリケーションは選択されません。
- 設計から SSID を削除してワイヤレスコントローラを再プロビジョニングする前に、対応するワイヤレス アプリケーション ポリシーを必ず削除してください。
- Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のワイヤレスアプリケーションは、学習された設定からプロビジョニングされた SSID ではサポートされません。
- Cisco DNA Center は、Cisco Catalyst IE 3300 高耐久性シリーズ スイッチおよび Cisco Catalyst IE 3400 Heavy Duty シリーズ スイッチに対する ACL ベースのアプリケーションポリシーのサポートを提供します。最大 8 つのポートベースのカスタムアプリケーションを展開できます。ただし、DSCP ベースのアプリケーションには制限はありません。

（注） Cisco DNA Center では、AireOS および Catalyst 9800 シリーズ ワイヤレス コントローラ プラットフォームの FlexConnect ローカルスイッチングモードはサポートされていません。

アプリケーション ポリシーの管理

ここでは、アプリケーション ポリシーの管理の方法に関する情報について説明します。

前提条件

アプリケーションポリシーを設定する場合は、次の要件に対応する必要があります。

- Cisco DNA Center は、ほとんどの Cisco LAN、WAN、WLAN デバイスをサポートしています。ネットワーク内のデバイスとソフトウェアのバージョンがサポートされているかどうかを確認するには、『Cisco DNA Center Compatibility Matrix』を参照してください。
- ISR-G2、ASR 1000、ワイヤレスコントローラなど、シスコのネットワーク デバイスに Application Visibility and Control（AVC）機能ライセンスがインストールされていることを確認します。詳細については、「*NBAR2 (Next Generation NBAR) Protocol Pack FAQ*」を参照してください。
- AVC サポートは、スイッチで自動 QoS が設定されていない場合にのみ、Cisco IOS-XE 16.9 を実行しているスイッチで使用できます。AVC サポートを利用するには、自動 QoS のスイッチを Cisco IOS-XE 16.11 以降にアップグレードする必要があります。
- ポリシーが必要な WAN インターフェイスを Cisco DNA Center で特定するには、インターフェイス タイプ（WAN）および（必要に応じて）副回線レートとサービス プロバイダのサービス クラス モデルを指定する必要があります。詳細については、サービス プロバイ

ダ プロファイルの WAN インターフェイスへの割り当て （674 ページ）を参照してください。

- ディスカバリプロセス中にデバイスに割り当てられたデバイスロールが、ネットワークに適切であることを確認します。必要に応じて、不適切なデバイスロールを変更します。詳細については、デバイスのロールの変更（インベントリ） （126 ページ）を参照してください。

アプリケーション ポリシーの作成

ここでは、アプリケーションポリシーの作成方法について説明します。

始める前に

- ビジネス目標を定義します。例えば、ネットワーク応答時間を最短化させたり、非ビジネスアプリケーションを特定して優先度を下げたりすることで、ユーザの生産性を向上させるようなものです。これらの目標に基づいて、どのビジネスとの関連性カテゴリがアプリケーションに分類されるかを決定します。
- インベントリにデバイスがあることを確認します。デバイスがない場合は、ディスカバリ機能を使用して検出します。
- ディスカバリプロセス中にデバイスに割り当てられたデバイスロールが、ネットワークに適切であることを確認します。必要に応じて、不適切なデバイスロールを変更します。詳細については、デバイスのロールの変更（インベントリ） （126 ページ）を参照してください。
- サイトへのデバイスの追加詳細については、「デバイスをサイトに追加する （118 ページ）」を参照してください。
- SP 向けのトラフィック用に対してこのポリシーを SP プロファイルで設定する場合は、SP プロファイルが設定されていることを確認してください。アプリケーションポリシーの作成後に SP プロファイルに戻り、SLA 属性をカスタマイズして SP プロファイルを WAN インターフェイスに割り当てます。詳細については、サービス プロバイダ プロファイルの設定 （247 ページ）を参照してください。

ステップ 1 メニューアイコン（☰）をクリックして、**[Policy]** > **[Application QoS]** > **[Application Policies]** の順に選択します。

ステップ 2 [Add Policy] をクリックします。

ステップ 3 [Application QoS Policy Name] フィールドに、ポリシーの名前を入力します。

ステップ 4 [有線（Wired）] または [ワイヤレス（Wireless）] ラジオ ボタンのいずれかを選択します。

ステップ 5 ワイヤレスネットワークの場合は、[SSID] ドロップダウンリストからプロビジョニングされた SSID を選択します。

ステップ 6 [サイトの範囲（Site Scope）] をクリックし、展開するポリシーの横にあるチェック ボックスをオンにします。

（注） 有線デバイスのポリシーでは、別のポリシーに割り当て済みのサイトは選択することができません。ワイヤレス デバイスのポリシーでは、同じ SSID で別のポリシーに割り当て済みのサイトを選択することができません。

ステップ 7 有線デバイスのポリシーでは、デバイスまたは特定のインターフェイスがポリシーで設定されないようにすることができます。

a) [サイトの範囲（Site Scope）] ペインで、興味のあるサイトの横にある ⚙ をクリックします。

選択した範囲内のデバイスのリストが表示されます。

b) 除外するデバイスを見つけ、関連する [ポリシーの除外（Policy Exclusions）] 列にあるトグル ボタンをクリックします。

c) 特定のインターフェイスを除外するには、[Exclude Interfaces] をクリックします。

d) [Applicable Interfaces] のリストから、除外するインターフェイスの横にあるトグルボタンをクリックします。

デフォルトでは、[Applicable Interfaces] のみが表示されます。すべてのインターフェイスを表示するには、[Show] ドロップダウンリストから [All] を選択します。

e) [< Back to Devices in *Site-Name*] をクリックします。

f) [< サイト範囲へ戻る（< Back to Site Scope）] をクリックします。

ステップ 8 WAN デバイスでは、特定のインターフェイスを設定できます。

a) [Site Scope] ペインで、目的のサイトの横にある ⚙ をクリックします。

b) サイトのデバイスのリストで、目的のデバイスの横にある [SP Profile Settings] 列の [Configure] をクリックします。

（注） このオプションは、ルータの場合にのみ使用可能です。

c) [WAN インターフェイス（WAN Interface）] 列で、[インターフェイスの選択（Select Interface）] ドロップダウン リストからインターフェイスを選択します。

d) [ロール（Role）] 列で[ロールの選択（Select Role）] ドロップダウン リストから設定するインターフェイスのタイプに従ってロールを選択します。

- 物理インターフェイス：[WAN] を選択します。このロールは、物理インターフェイスに対してのみ有効なロールです。
- トンネルインターフェイス：[DMVPN Branch] または [DMVPN Hub] のいずれかを選択します。[DMVPN ハブ（DMVPN Hub）] を選択した場合、関連するブランチに帯域幅を定義することもできます。

（注） これらのポリシー設定を展開する前に、デバイスにトンネル インターフェイスが作成されていることを確認します。

e) [サービス プロバイダ プロファイル（Service Provider Profile）] 列で、[プロファイルの選択（Select Profile）] ドロップダウン リストから SP プロファイルを選択します。

f) （任意） 必要に応じて、[サブ回線のレート（Mbps）（Sub-Line Rate（Mbps））] 列で、インターフェイスに必要なアップストリーム帯域幅を入力します。

g) （任意） 追加の WAN インターフェイスを設定するには、[+] をクリックし、手順 c ～ f を繰り返します。
h) **[Save]** をクリックします。
i) [< サイト範囲へ戻る（< Back to Site Scope）] をクリックします。

ステップ 9 [サイトの範囲（Site Scope）] ペインで、[OK] をクリックします。

ステップ 10 （任意） Cisco Validated Design（CVD）キューイング プロファイルがニーズを満たしていない場合は、カスタム キューイング プロファイルを作成することができます。

a) [キューイング プロファイル（Queuing Profiles）] をクリックします。
b) 左ペインのリストから、キューイング プロファイルを選択します。
c) [Select] をクリックします。

ステップ 11 （任意） このポリシーが SP 向けトラフィックである場合は、SP プロファイルの SLA 属性をカスタマイズします。

a) [SP プロファイル（SP Profile）] をクリックします。
b) SP プロファイルを選択します。
c) SLA 属性をカスタマイズします（[DSCP]、[SP 帯域幅（%）（SP Bandwidth %）]、および [キューイング帯域幅（%）（Queuing Bandwidth %）]）。

ステップ 12 （任意） ネットワークで使用されるアプリケーション セットのビジネスとの関連性を設定します。

Cisco DNA Center には、ビジネス関連性グループに事前設定されたアプリケーション セットが付属しています。あるビジネス関連性グループから別のグループにアプリケーションセットをドラッグアンドドロップして、この設定を維持したり、変更したりすることができます。

お気に入りとしてマークされたアプリケーションは、アプリケーションセットの上部に表示されます。お気に入りを変更するには、[Applications registry] に移動します。

ステップ 13 （任意） コンシューマを作成してアプリケーションに割り当てるか、アプリケーションを双方向としてマークすることにより、アプリケーションをカスタマイズします。

a) アプリケーション グループを展開します。
b) 目的のアプリケーションの横にある歯車アイコン をクリックします。
c) [トラフィックの方向（Traffic Direction）] エリアで、[単方向（Unidirectional）] または [双方向（Bi-directional）] ラジオ ボタンを選択します。
d) 既存のコンシューマを選択するには、[コンシューマ（Consumer）] ドロップダウン リストから設定するコンシューマを選択します。新しいコンシューマを作成するには、[+ コンシューマの追加（+ Add Consumer）] をクリックして、[コンシューマ名（Consumer Name）]、[IP/サブネット（IP/Subnet）]、[プロトコル（Protocol）]、および [ポート/範囲（Port/Range）] を定義します。
e) [OK] をクリックします。

ステップ 14 ホスト トラッキングを設定します。[ホスト トラッキング（Host Tracking）] トグル ボタンをクリックして、ホスト トラッキングのオンとオフを切り替えます。

アプリケーションポリシーを展開する際に、Cisco DNA Center では、コラボレーション エンドポイント（テレプレゼンスユニットやシスコ電話など）が接続されているスイッチに、ACL のエントリを自動的に適用します。

ACE は、コラボレーション エンドポイントによって生成された音声およびビデオトラフィックを照合し、音声およびビデオトラフィックが正しくマークされるようにします。

ホストトラッキングがオンの場合、Cisco DNA Center はサイトの範囲内でコラボレーション エンドポイントの接続をトラッキングし、コラボレーション エンドポイントがネットワークに接続されるか、1 つのインターフェイスから別のインターフェイスに移動したときに、ACL エントリを自動的に再設定します。

ホストトラッキングが終了すると、Cisco DNA Center は、コラボレーション エンドポイントが新しいインターフェイスに移動または接続したときに、デバイスにポリシーを自動的に展開しません。代わりに、コラボレーションエンドポイントで正しく設定されるように、ACL のポリシーを再展開する必要があります。

ステップ 15 （任意） デバイスに送信される CLI コマンドをプレビューします。詳細については、「アプリケーション ポリシーのプレビュー （670 ページ）」を参照してください。

ステップ 16 （任意） ポリシーを展開するデバイスを事前にチェックします。詳細については、「アプリケーション ポリシーの事前チェック （670 ページ）」を参照してください。

ステップ 17 次のいずれか 1 つのタスクを実行します。

- [ドラフトの保存（Save Draft）] をクリックして、ポリシーをドラフトとして保存します。詳細については、「ポリシーのドラフト （654 ページ）」を参照してください。
- [展開（Deploy）] をクリックしてポリシーを展開します。ポリシーを今すぐ展開するか、または後でスケジュールできます。

  ポリシーをすぐに展開するには、[今すぐ実行（Now）] ラジオボタンをクリックし、[適用（Apply）] をクリックします。

  将来の日付と時刻でポリシー展開をスケジュールするには、[後で実行（Later）] ラジオ ボタンをクリックし、展開する日時を定義します。詳細については、ポリシーのスケジューリング （656 ページ）を参照してください。

  （注） アプリケーション ポリシーの展開のスケジュール設定では、サイトのタイム ゾーンの設定はサポートされていません。

アプリケーションポリシー情報の表示

作成および展開したアプリケーション ポリシーに関するさまざまな情報を表示できます。

始める前に

少なくとも 1 つの展開されたアプリケーション ポリシーがなければなりません。

ステップ 1 メニューアイコン（☰）をクリックして、**[Policy]** > **[Application QoS]** > **[Application Policies]** の順に選択します。

ステップ 2 ポリシーを名前で並べ替えたり、名前、ステータス、キューイングプロファイルによってフィルタ処理したりします。

ステップ 3 ポリシーのリストと、それぞれに関する次の情報が表示されます。

- [Policy Name]：ポリシーの名前。
- [Version]：ポリシーの反復。ポリシーが展開されるか、または、ドラフトとして保存されるたびに、バージョンが 1 ずつ増分されます。たとえば、ポリシーを作成して展開すると、ポリシーはバージョン 1 になります。ポリシーを変更して、再度展開すると、ポリシーのバージョンはバージョン 2 に増分されます。詳細については、ポリシーのドラフト（654 ページ）およびポリシーのバージョン管理（656 ページ）を参照してください。
- [Policy Status]：ポリシーの状態。Cisco Catalyst 3850、Catalyst 4500、および Catalyst 9000 デバイスに適用されたポリシーがポートチャネルの更新（作成/変更/削除）によって影響を受ける場合は、アラートがポリシーステータスに表示されます。
- [Deployment Status]：最新の展開の状態（デバイスごと）。次の概要を示します。
  - 正常にプロビジョニングされたデバイス
  - プロビジョニングに失敗したデバイス
  - 展開が終了したためにプロビジョニングされなかったデバイス。

  最新の導入の状態をクリックすると、[ポリシーの展開（Policy Deployment）] ウィンドウが表示され、ポリシーが展開されたデバイスのフィルタ処理可能なリストが示されます。デバイスごとに、次の情報が表示されます。
  - デバイスの詳細（名前、サイト、タイプ、ロール、および IP アドレス）
  - 成功した導入のステータス。ステータスの横にある歯車のアイコンをクリックすると、[Effective Marking Policy] ウィンドウが開き、[Business Relevant] および [Business Irrelevant] アプリケーションと、それらが最終的に渡されるトラフィッククラスキューが表示されます。TCAM リソースまたは古い NBAR プロトコルパックに限定されているデバイスの場合は、ポリシーに含まれるアプリケーションのサブセットのみをプロビジョニングでき、それらがビューで表示されます。
  - 障害ステータスには、障害の理由が示されます。
- [Scope]：ポリシーに割り当てられているサイト（デバイスではなく）の数。ワイヤレスデバイスのポリシーの場合は、ポリシーの適用先の SSID の名前が含まれます。
- [LAN Queuing Profile]：ポリシーに割り当てられている LAN キューイングプロファイルの名前。

アプリケーション ポリシーの編集

アプリケーション ポリシーを編集できます。

始める前に

少なくとも 1 つのポリシーを作成しておく必要があります。

ステップ 1 メニューアイコン（☰）をクリックして、**[Policy]** > **[Application QoS]** > **[Application Policies]** の順に選択します。

ステップ 2 編集するポリシーを見つけるには、[フィルタ（Filter）] フィールドを使用します。

ステップ 3 対応するポリシーの横にあるラジオ ボタンをクリックします。

ステップ 4 [Actions] ドロップダウン リストから、[Edit] を選択します。

ステップ 5 必要に応じて、アプリケーション ポリシーを変更します。

ステップ 6 アプリケーションのビジネスとの関連性を変更するには、ビジネス関連、ビジネスと無関係、およびデフォルトグループの間でアプリケーションセットを移動します。

アプリケーションポリシーの設定については、アプリケーション ポリシーの作成 （660 ページ）を参照してください。

ステップ 7 キューイングプロファイルを更新するには、[Queuing Profiles] をクリックし、左ペインのリストからキューイングプロファイルを選択します。

ステップ 8 [Select] をクリックします。

ステップ 9 次のいずれか 1 つのタスクを実行します。

- [ドラフトの保存（Save Draft）] をクリックして、ポリシーをドラフトとして保存します。詳細については、「ポリシーのドラフト （654 ページ）」を参照してください。
- [展開（Deploy）] をクリックしてポリシーを展開します。ポリシーを今すぐ展開するか、または後でスケジュールできます。

  ポリシーをすぐに導入するには、[今すぐ実行（Run Now）] ラジオボタンをクリックし、[適用（Apply）] をクリックします。

  将来の日付と時刻でポリシー導入をスケジュールするには、[後でスケジュール（Schedule Later）] ラジオ ボタンをクリックし、導入する日時を定義します。詳細については、ポリシーのスケジューリング （656 ページ）を参照してください。

  （注） アプリケーションポリシーの展開のスケジュール設定では、サイトのタイム ゾーンの設定はサポートされていません。

アプリケーション ポリシーのドラフトの保存

ポリシーを作成、編集、または複製する際、ドラフトとして保存し、後で変更を続けることができます。また、展開したポリシーを変更して、ドラフトとして保存することもできます。

ステップ 1 メニューアイコン（☰）をクリックして、**[Policy]** > **[Application QoS]** > **[Application Policies]** の順に選択します。

ステップ 2 ポリシーを作成、編集、または複製します。

ステップ 3 [ドラフトの保存（Save Draft）] をクリックします。

詳細については、ポリシーのドラフト （654 ページ）を参照してください。

アプリケーション ポリシーの展開

新しいアプリケーションの追加や、アプリケーションをお気に入りとしてマークするなど、ポリシーの設定に影響する変更を加えた場合は、ポリシーを再展開してこれらの変更を実装する必要があります。

（注） Cisco IOS 16.x 以降を搭載した Cisco Catalyst 3650、Catalyst 3850、および Catalyst 9000 デバイスでは、ポリシーを展開する前に、自動 QoS 設定が自動的に削除されます。

カスタムアプリケーションの作成後、デバイスに関して CBAR が有効になっている場合、そのデバイスでカスタムアプリケーションが自動的に設定されます。デバイスにアプリケーションポリシーを展開する前に、最新のアプリケーションレジストリへの同期の完了を待つ必要があります。**Provision** > **Services** > **Service Catalog** > **Application Visibility** で同期ステータスを確認することができます。

デバイスに関して CBAR が有効になっている場合、カスタムアプリケーションは CBAR を介して設定されるため、アプリケーションポリシーの展開時には属性セットおよびマップだけがデバイスで設定されます。

ステップ 1 メニューアイコン（☰）をクリックして、**[Policy]** > **[Application QoS]** > **[Application Policies]** の順に選択します。

ステップ 2 導入するポリシーを見つけるには、[フィルタ（Filter）] フィールドを使用します。

ステップ 3 導入するポリシーの横のラジオ ボタンをクリックします。

ステップ 4 [アクション（Actions）] ドロップダウンリストから、[導入（Deploy）] を選択します。

a) ポリシーを再展開すると、ポリシーの範囲から削除されたデバイスに対して適切なアクションを実行するように求められます。次のいずれかのアクションを選択します。

- デバイスからポリシーを削除する（推奨）
- ポリシーの範囲からデバイスを削除する
- ポリシーの範囲からデバイスを削除し、デバイスを既存の設定に復元する

b) [Apply] をクリックします。

ステップ 5 ポリシーを今すぐ展開するか、後で展開するようにスケジュールするかを求められます。次のいずれかを実行します。

- ポリシーをすぐに導入するには、[今すぐ実行（RunNow）]ラジオボタンをクリックし、[適用（Apply）]をクリックします。
- 将来の日付と時刻でポリシー導入をスケジュールするには、[後でスケジュール（Schedule Later）]ラジオ ボタンをクリックし、導入する日時を定義します。

（注） アプリケーションポリシーの展開のスケジュール設定では、サイトのタイムゾーンの設定はサポートされていません。

ポリシー導入のキャンセル

[導入（Deploy）]をクリックすると、Cisco DNA Center は、サイト範囲内のデバイスに関するポリシーの設定を開始します。間違いが見つかった場合は、ポリシーの展開をキャンセルできます。

ポリシー設定プロセスはバッチ処理として実行され、一度に40台のデバイスが設定されます。デバイスが 40 台以下の場合にポリシーの展開をキャンセルしても、デバイスの最初のバッチへの展開がすでに行われているため、デバイスが設定されている可能性があります。ただし、何百台ものデバイスがある場合は、必要に応じてポリシーの展開をキャンセルできます。

[中止（Abort）]をクリックすると、Cisco DNA Centerによって設定がまだ開始されていないデバイスの設定プロセスがキャンセルされ、デバイスのステータスが [ポリシーの中止（Policy Aborted）] に変更されます。Cisco DNA Center では、完了している、または完了する予定の処理での導入はキャンセルされません。これらのデバイスでは、更新されたポリシー設定が維持され、ポリシー設定の状態（設定中、成功、または失敗）が反映されます。

ポリシー導入中に[中止（Abort）]をクリックしてポリシー設定プロセスをキャンセルします。

アプリケーション ポリシーの削除

不要になったアプリケーション ポリシーを削除できます。

ポリシーを削除すると、クラスマップ、ポリシーマップ、およびポリシーマップとワイヤレス ポリシー プロファイルの関連付けが削除されます。

ステップ 1 メニューアイコン（≡）をクリックして、**[Policy]** > **[Application QoS]** > **[Application Policies]** の順に選択します。

ステップ 2 削除するポリシーを見つけるには、[フィルタ（Filter）] フィールドを使用します。

ステップ 3 削除するポリシーの横にあるラジオ ボタンを選択します。

ステップ 4 [Actions] ドロップダウンリストから、[Undeploy Policy] を選択します。

ステップ 5 [Undeploy Policy] ウィンドウで、[Delete policy from devices] オプションボタンをクリックし、[Apply] をクリックします。

ステップ 6 削除を確定する場合は、[OK] をクリックします。それ以外の場合は、[Cancel] をクリックします。

ステップ 7 削除を確認するメッセージが表示されたら、[OK] を再度クリックします。

[Application QoS Policies] ページで、ポリシーの削除ステータスを確認できます。ステータスに [deletion failed] と表示された場合は、次の手順を実行します。

a) [Application QoS Policies] ページの [Deployment Status] の下にある失敗状態リンクをクリックします。
b) [Undeployment Status] ウィンドウで、[Retry] をクリックしてポリシーを削除します。

アプリケーション ポリシーの複製

既存のアプリケーションポリシーに、新しいポリシーで必要な設定のほとんどが含まれている場合は、既存のポリシーの複製し、変更してから異なる範囲に展開することで時間を節約できます。

始める前に

少なくとも 1 つのポリシーを作成しておく必要があります。

ステップ 1 メニューアイコン（≡）をクリックして、**[Policy]** > **[Application QoS]** > **[Application Policies]** の順に選択します。

ステップ 2 複製するポリシーを見つけるには、[フィルタ（Filter）] フィールドを使用します。

ステップ 3 複製するポリシーの横にあるラジオ ボタンを選択します。

ステップ 4 [アクション（Actions）] ドロップダウンリストから、[複製（Clone）] を選択します。

ステップ 5 必要に応じてアプリケーションポリシーを設定します。アプリケーションポリシーの設定については、アプリケーション ポリシーの作成 （660 ページ）を参照してください。

ステップ 6 次のいずれか 1 つのタスクを実行します。

- [ドラフトの保存（Save Draft）] をクリックして、ポリシーをドラフトとして保存します。詳細については、「ポリシーのドラフト （654 ページ）」を参照してください。
- [展開（Deploy）] をクリックしてポリシーを展開します。ポリシーを今すぐ展開するか、または後でスケジュールできます。

  ポリシーをすぐに導入するには、[今すぐ実行（Run Now）] ラジオボタンをクリックし、[適用（Apply）] をクリックします。

  将来の日付と時刻でポリシー展開をスケジュールするには、**[後でスケジュール（Schedule Later）]** ラジオ ボタンをクリックし、展開する日時を定義します。詳細については、ポリシーのスケジューリング （656 ページ）を参照してください。

  （注） アプリケーションポリシーの展開のスケジュール設定では、サイトのタイムゾーンの設定はサポートされていません。

アプリケーション ポリシーの復元

ポリシーを作成または変更してから、最初からやり直すことを決定した場合、Cisco DNA Center を使ってこれを設定する前に、デバイスにあった元の QoS 設定を復元することができます。

ステップ 1 メニューアイコン（☰）をクリックして、**[Policy]** > **[Application QoS]** > **[Application Policies]** の順に選択します。

ステップ 2 リセットするポリシーを見つけるには、[フィルタ（Filter）] フィールドを使用します。

ステップ 3 ポリシーの横にあるラジオ ボタンをクリックします。

ステップ 4 [Actions] ドロップダウンリストから、[Undeploy Policy] を選択します。

ステップ 5 [Undeploy Policy] ウィンドウで、[Restore devices to original configurations] オプションボタンをクリックし、[Apply] をクリックします。

ステップ 6 [OK] をクリックして変更を確定するか、[Cancel] をクリックして変更をキャンセルします。

[Application QoS Policies] ページで、ポリシーの復元ステータスを確認できます。ステータスに [restoration failed] と表示された場合は、次の手順を実行します。

a) [Application QoS Policies] ページの [Deployment Status] の下にある失敗状態リンクをクリックします。
b) [Undeployment Status] ウィンドウで、[Retry] をクリックしてポリシーを復元します。

デフォルトの CVD アプリケーション ポリシーをリセット

CVD 設定は、アプリケーションのデフォルト設定です。ポリシーの作成または変更を行った後で最初からやり直す必要が生じた場合は、アプリケーションを CVD 設定にリセットすることができます。CVD設定の詳細については、アプリケーションポリシーの概要（643 ページ）を参照してください。

ステップ 1 メニューアイコン（☰）をクリックして、**[Policy]** > **[Application QoS]** > **[Application Policies]** の順に選択します。

ステップ 2 リセットするポリシーを見つけるには、[フィルタ（Filter）] フィールドを使用します。

ステップ 3 ポリシーの横にあるラジオ ボタンをクリックします。

ステップ 4 [Actions] ドロップダウン リストから、[Edit] を選択します。

ステップ 5 [シスコ検証済みデザインのリセット（Reset to Cisco Validated Design）] をクリックします。

ステップ 6 [OK] をクリックして変更を確定するか、[Cancel] をクリックして変更をキャンセルします。

ステップ 7 次のいずれか 1 つのタスクを実行します。

- ポリシーのドラフトを保存するには、[ドラフトの保存（Save Draft）] をクリックします。
- ポリシーを展開するには、[展開（Deploy）] をクリックします。

アプリケーション ポリシーのプレビュー

ポリシーを展開する前に、デバイスに適用する CLI を生成して設定をプレビューできます。

ステップ 1 メニューアイコン（☰）をクリックして、**[Policy]** > **[Application QoS]** > **[Application Policies]** の順に選択します。

ステップ 2 アプリケーション ポリシーの作成 （660 ページ）またはアプリケーション ポリシーの編集 （664 ページ）の説明に従って、ポリシーを作成または編集します。

ステップ 3 ポリシーを展開する前に、[プレビュー（Preview）] をクリックします。

範囲内のデバイスのリストが表示されます。

ステップ 4 対象のデバイスの横にある [生成（Generate）] をクリックします。

Cisco DNA Center により、ポリシーの CLI が生成されます。

ステップ 5 [表示（View）] をクリックして CLI を表示するか、CLI をクリップボードにコピーします。

アプリケーション ポリシーの事前チェック

アプリケーションポリシーを展開する前に、サイト範囲内のデバイスがサポート対象であるかどうかをチェックできます。事前チェック プロセスには、デバイスのモデル、ライン カード、およびソフトウェア イメージの検証が含まれます。

ステップ 1 メニューアイコン（☰）をクリックして、**[Policy]** > **[Application QoS]** > **[Application Policies]** の順に選択します。

ステップ 2 アプリケーション ポリシーの作成 （660 ページ）またはアプリケーション ポリシーの編集 （664 ページ）の説明に従って、ポリシーを作成または編集します。

ステップ 3 [事前チェック（Pre-check）] をクリックします。

Cisco DNA Center は、デバイスをチェックして、問題があれば [事前チェック結果（Pre-Check Result）] 列に内容を報告します。[Errors] タブには、このポリシーをサポートしていないデバイスが表示されます。[Warnings] タブには、デバイスにこのポリシーを展開することを選択した場合に、サポートされていない制限や機能が表示されます。[Warnings] タブに一覧表示されているデバイスのポリシーを展開することもできます。問題を解決するには、『Cisco DNA Center Compatibility Matrix』に記載されている仕様にデバイスを準拠させます。

アプリケーション ポリシー履歴の表示

アプリケーションポリシーのバージョン履歴を表示できます。バージョン履歴には、ポリシーのシリーズ番号（反復）と、バージョンが保存された日付と時刻が含まれています。

ステップ 1 メニューアイコン（☰）をクリックして、**[Policy]** > **[Application QoS]** > **[Application Policies]** の順に選択します。

ステップ 2 表示したいポリシーの横にあるラジオ ボタンをクリックします。

ステップ 3 [アクション（Actions）] ドロップダウン リストから、[履歴（History）] を選択します。

ステップ 4 [ポリシー履歴（Policy History）] ダイアログボックスでは、次のことを実行できます。

- 現在のバージョンとバージョンを比較するには、関心のあるバージョンの横にある [差異（Difference）] をクリックします。
- ポリシーの前のバージョンにロールバックするには、ロールバック先となるバージョンの横にある [ロールバック（Rollback）] をクリックします。

ポリシーの以前のバージョンにロール バック

ポリシー設定を変更し、その後その設定が不適切だと判明した場合、またはネットワークで目的の効果が得られなかった場合、最大で 5 バージョン前のポリシーに戻すことができます。

始める前に

以前のポリシーバージョンにロールバックするには、少なくとも 2 つのポリシーバージョンを作成しておく必要があります。

ステップ 1 メニューアイコン（☰）をクリックして、**[Policy]** > **[Application QoS]** > **[Application Policies]** の順に選択します。

ステップ 2 表示したいポリシーの横にあるラジオ ボタンをクリックします。

ステップ 3 [アクション（Actions）] ドロップダウンリストから、[履歴の表示（Show History）] を選択します。

選択したポリシーの以前のバージョンは降順に表示され、最も新しいバージョン（最も大きい番号）が一覧の最上部に表示され、最も古いバージョン（最も小さい番号）が最下部に表示されます。

ステップ 4 （任意） 選択したバージョンと最新バージョンの間の差異を表示するには、[View] 列で [Difference] をクリックします。

ステップ 5 ロールバックする先のポリシー バージョンを決定した場合、そのポリシー バージョンに対して [Rollback] をクリックします。

（注） 選択したサイトの範囲がポリシー バージョン間で変更された場合、ロールバックは選択されている現在（最新）のサイトでは行われません。ポリシーのコンテンツのみがロールバックされます。

ステップ 6 [OK] をクリックして、ロールバック手順を確定します。

ロールバック先のバージョンが最新バージョンになります。

キューイング プロファイルの管理

次のセクションでは、キューイングプロファイルを管理するために実行できるさまざまなタスクについて詳しく説明します。

キューイング プロファイルの作成

Cisco DNA Center では、デフォルトの CVD キューイング プロファイル（CVD_QUEUING_PROFILE）を提供します。このキューイングプロファイルがニーズを満たしていない場合は、カスタム キューイング プロファイルを作成することができます。

ステップ 1 メニューアイコン（☰）をクリックして、**[Policy]** > **[Application QoS]** > **[Queuing Profiles]** の順に選択します。

ステップ 2 [Add Profile] をクリックします。

ステップ 3 [Profile Name] フィールドに、プロファイルの名前を入力します。

ステップ 4 スライダを使用して各トラフィック クラスに帯域幅を設定します。プラス記号（+）またはマイナス（-）記号をクリックするか、フィールドに特定の数値を入力します。

数値は、選択したアプリケーション クラスに確保されるインターフェイス帯域幅の合計に対しての割合を示します。帯域幅の合計は 100 なので、1 つのアプリケーション クラスに帯域幅を追加すると、別のアプリケーション クラスから帯域幅が差し引かれます。

開いた錠のアイコンは、そのアプリケーション クラスの帯域幅を編集できることを示します。閉じた錠のアイコンは、編集できないことを示します。

間違えた場合は、[シスコ検証済みデザインのリセット（Reset to Cisco Validated Design）] をクリックして CVD 設定に戻ることができます。

中央のグラフは、各アプリケーション クラスを設定している帯域幅の量の視覚化に役立ちます。

ステップ 5 （高度なユーザー向け）Cisco DNA Center が各トラフィック クラスで使用する DSCP コード ポイントをカスタマイズするには、[表示（Show）] ドロップダウン リストで、[DSCP値（DSCP Values）] を選択し、フィールドに特定の数値を入力して、各アプリケーション クラスの値を設定します。

SP のクラウド内で必要な DSCP コード ポイントをカスタマイズするには、SP のプロファイルを設定します。

ステップ 6 [Save] をクリックします。

キューイング プロファイルの編集または削除

ステップ 1 メニューアイコン（☰）をクリックして、**[Policy]** > **[Application QoS]** > **[Queuing Profiles]** の順に選択します。

ステップ 2 [キューイング プロファイル（Queuing Profile）] ペインで、編集または削除するキューイング プロファイルの横にあるラジオ ボタンをクリックします。

ステップ 3 次のいずれか 1 つのタスクを実行します。

- プロファイルを編集するには、プロファイル名を除くフィールドの値を変更し、[保存（Save）] をクリックします。フィールドの詳細については、キューイング プロファイルの作成 （672 ページ）を参照してください。
- プロファイルを削除するには、[削除（Delete）] をクリックします。

  アプリケーション ポリシーによって参照されている場合は、キューイング プロファイルを削除できません。

WAN インターフェイスのアプリケーション ポリシーの管理

次のセクションでは、WAN インターフェイスのアプリケーション プロファイルを管理するために実行できるさまざまなタスクについて詳しく説明します。

サービス プロバイダ プロファイルの SLA 属性をカスタマイズ

自身のクラス モデルによって SP プロファイルに割り当てられたデフォルトの SLA 属性を使用しない場合は、要件に合わせて SP プロファイルの SLA 属性をカスタマイズすることができます。SP プロファイルのデフォルトの SLA 属性の詳細については、サービス プロバイダのプロファイル （648 ページ）を参照してください。

始める前に

インベントリにデバイスがあることを確認します。デバイスがない場合は、ディスカバリ機能を使用して検出します。

ステップ 1 メニューアイコン（☰）をクリックして、**[Policy]** > **[Application QoS]** > **[Application Policies]** の順に選択します。

ステップ 2 変更するポリシーを見つけるには、[フィルタ（Filter）] フィールドを使用します。

ステップ 3 ポリシーの横にあるラジオ ボタンを選択します。

ステップ 4 [Actions] ドロップダウン リストから、[Edit] を選択します。

ステップ 5 [SPプロファイル（SP Profiles）] をクリックし、SP プロファイルを選択します。

ステップ 6 次のフィールドの情報を変更できます。

- [DSCP]：Differentiated Services Code Point（DSCP）値。有効値は 0 ～ 63 です。
  - Expedited Forwarding（EF）

- クラスセレクタ（CS）：CS1、CS2、CS3、CS4、CS5、CS6
- 相対的優先転送：AF11、AF21、AF41
- [Default Forwarding (DF)]

これらの DSCP 値の詳細については、マーキング、キューイング、ドロッピングの処理（646 ページ）を参照してください。

- [SP Bandwidth %]：特定のサービスクラスに割り当てられた帯域幅の割合。
- [Queuing Bandwidth %]：各トラフィッククラスに割り当てられた帯域幅の割合。次のうちいずれかの変更を行うことができます。
  - キューイング帯域幅をカスタマイズするには、鍵アイコンをクリックして、帯域幅の設定をアンロックし、帯域幅の割合を調整します。
  - SP 帯域幅から自動的にキューイング帯域幅を計算するには、鍵アイコンをクリックしてキューイング帯域幅の設定をロックし、次に [OK] をクリックして確認します。デフォルトでは、Cisco DNA Center は、SP クラスのすべてのトラフィック クラスのキューイング帯域幅の合計がそのクラスの SP 帯域幅の割合と一致するように、キューイング帯域幅の割合を自動的に配信します。

ステップ 7 [OK] をクリックします。

サービス プロバイダ プロファイルの WAN インターフェイスへの割り当て

アプリケーション ポリシーがすでに作成済みで、SP プロファイルを WAN インターフェイスに割り当てる場合は、ポリシーを編集してこの設定を実行し、必要に応じてインターフェイスに Subline Rate の設定を含めます。

始める前に

ポリシーを作成していない場合は、ポリシーを作成し、同時に SP プロファイルを WAN インターフェイスに割り当てることができます。詳細については、「アプリケーション ポリシーの作成（660 ページ）」を参照してください。

ステップ 1 メニューアイコン（☰）をクリックして、**[Policy]** > **[Application QoS]** > **[Application Policies]** の順に選択します。

ステップ 2 編集するポリシーを見つけるには、[フィルタ（Filter）] フィールドを使用します。

ステップ 3 ポリシーの横にあるラジオ ボタンをクリックします。

ステップ 4 [Actions] ドロップダウン リストから、[Edit] を選択します。

ステップ 5 [Site Scope] ペインで、対象のサイトの横にある歯車アイコンをクリックします。

ステップ 6 対象のデバイスの [SPプロファイル設定（SP Profile Settings）] 列にある [設定（Configure）] をクリックします。

ステップ 7 [WAN インターフェイス（WAN Interface）] 列で、[インターフェイスの選択（Select Interface）] ドロップダウン リストからインターフェイスを選択します。

ステップ 8 [ロール（Role）] 列で[ロールの選択（Select Role）] ドロップダウン リストから設定するインターフェイスのタイプに従ってロールを選択します。

- **物理インターフェイス**：[WAN] を選択します。このロールは、物理インターフェイスに対してのみ有効なロールです。
- **トンネルインターフェイス**：[DMVPN Branch] または [DMVPN Hub] のいずれかを選択します。[DMVPN ハブ（DMVPN Hub）] を選択した場合、関連するブランチに帯域幅を定義することもできます。

（注） これらのポリシー設定を展開する前に、デバイスにトンネル インターフェイスが作成されていることを確認します。

ステップ 9 [サービス プロバイダー プロファイル（Service Provider Profile）] 列で、[プロファイルの選択（Select Profile）] ドロップダウン フィールドをクリックし、SP プロファイルを選択します。

ステップ 10 必要に応じて、[サブ回線のレート（Mbps）（Sub-Line Rate（Mbps））] 列で、インターフェイスに必要なアップストリーム帯域幅を入力します。

ステップ 11 追加の WAN インターフェイスを設定するには [+] をクリックし、ステップ 7 ～ 10 を繰り返します。

ステップ 12 **[Save]** をクリックします。

ステップ 13 [< サイト範囲へ戻る（< Back to Site Scope）] をクリックします。

ステップ 14 [OK] をクリックします。

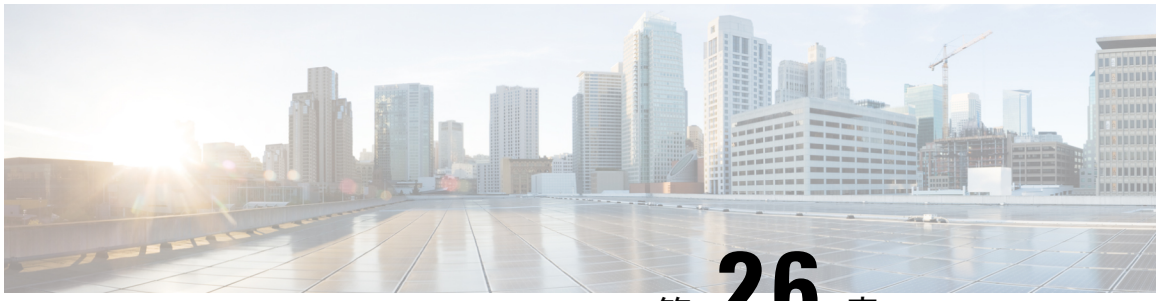
ステップ 15 [Deploy] をクリックします。

ポリシーを今すぐ導入するか、または後でスケジュールするかどうかを求められます。

ステップ 16 次のいずれかを実行します。

- ポリシーをすぐに導入するには、[今すぐ実行（Run Now）] ラジオ ボタンをクリックし、[適用（Apply）] をクリックします。
- 将来の日付と時刻でポリシー導入をスケジュールするには、[後でスケジュール（Schedule Later）] ラジオ ボタンをクリックし、導入する日時を定義します。

（注） アプリケーション ポリシーの展開のスケジュール設定では、サイトのタイム ゾーンの設定はサポートされていません。



第 26 章

トラフィックコピーポリシーの設定

トラフィック コピー ポリシー

Cisco DNA Center を使用して、2 つのエンティティ間の IP トラフィック フローがモニターリングまたはトラブルシューティングのために指定された宛先にコピーされるように Encapsulated Remote Switched Port Analyzer（ERSPAN）を設定できます。

Cisco DNA Center を使用して ERSPAN を設定するには、コピーするトラフィック フローの送信元と宛先を定義するトラフィック コピー ポリシーを作成します。トラフィックのコピーを送信するデバイスおよびインターフェイスを指定するトラフィック コピー契約も定義できます。

（注） トラフィックコピーポリシーにはセキュリティグループまたは IP ネットワークグループのいずれかを含めることができるため、このガイド全体を通して、「グループ」という用語を使用する場合は他に指定がなければセキュリティグループおよび IP ネットワークグループの両方を指します。

送信元、宛先、およびトラフィックのコピー先

Cisco DNA Center トラフィックのモニターリングプロセスを簡素化します。物理ネットワークトポロジを知っている必要はありません。必要なのは、トラフィック フローの送信元および宛先とコピーされたトラフィックの宛先となるトラフィック コピーの宛先を定義することだけです。

- [送信元（Source）]：モニターするトラフィックが通過する 1 つまたは複数のネットワーク デバイス インターフェイス。このインターフェイスは、エンドポイント デバイス、これらのデバイスの特定ユーザー、またはアプリケーションに接続することがあります。送信元グループを構成できるのは、イーサネット、ファストイーサネット、ギガビットイーサネット、10 ギガビット イーサネット、またはポート チャネル インターフェイスのみです。
- [宛先（Destination）]：モニターするトラフィックが流れる IP サブネットです。IP サブネットはサーバー、リモート ピア、またはアプリケーションに接続することがあります。
- [トラフィックコピーの宛先（Traffic Copy Destination）]：ERSPAN データを受信、処理、および分析するデバイス上にあるレイヤ 2 またはレイヤ 3 の LAN インターフェイス。このデバイスは、通常、分析用にトラフィックのコピーを受信するパケットキャプチャ ツールまたはネットワーク分析ツールになります。

（注） 宛先では、スイッチ プローブ デバイスなどのネットワーク アナライザやその他のリモート モニターリング（RMON）プローブを使用してトラフィック分析を実行することを推奨します。

使用可能なインターフェイス タイプは、イーサネット、ファストイーサネット、ギガビット イーサネット、または 10 ギガビット イーサネットのみです。宛先として設定されると、そのインターフェイスはコピーされたトラフィックのみを受信するために使用されます。このインターフェイスは今後その他のタイプのトラフィックを受信できなくなり、トラフィック コピー機能が必要とする以外のトラフィックを転送できません。トランク インターフェイスを宛先として設定できます。この設定により、インターフェイスはカプセル化されたトラフィックを送信できるようになります。

（注） 1 つのトラフィック コピー契約で使用できるトラフィック コピーの宛先は 1 つのみです。

トラフィック コピー ポリシーの注意事項と制限事項

トラフィック コピー ポリシー機能には次の制約事項があります。

- 最大 8 つのトラフィック コピー ポリシー、16 のコピー契約、および 16 のコピーの宛先を作成できます。
- 同じインターフェイスを複数のトラフィック コピーの宛先に使用することはできません。
- Cisco DNA Center は、トラフィック コピー ポリシーが変更され、ネットワークに展開されているポリシーとの整合性が失われていることを示すステータス メッセージを表示しません。ただし、トラフィック コピー ポリシーが展開された後に変更されたことが分かった場合は、そのポリシーを展開しなおすことができます。
- 管理インターフェイスを送信元グループまたはトラフィック コピーの宛先として設定することはできません。

トラフィック コピー ポリシー設定のワークフロー

始める前に

- モニター対象にするには、トラフィックコピーポリシーで使用されている送信元セキュリティグループが、スイッチとそれらのインターフェイスに静的にマッピングされている必要があります。
- トラフィック コピー ポリシー宛先グループは、IP ネットワーク グループとして設定されている必要があります。詳細については、「IP ネットワーク グループの作成 （637 ページ）」を参照してください。

ステップ 1 トラフィック コピーの宛先を作成します。

これは、さらに分析するためにトラフィック フローがコピーされる、デバイス上のインターフェイスです。詳細については、トラフィック コピーの宛先の作成 （680 ページ）を参照してください。

ステップ 2 トラフィック コピーの契約を作成します。

契約はコピーの宛先を定義します。詳細については、トラフィック コピー契約の作成 （680 ページ）を参照してください。

ステップ 3 トラフィック コピー ポリシーを作成します。

ポリシーは、トラフィック フローの送信元と宛先、およびコピーされたトラフィックが送信される宛先を指定するトラフィック コピーの契約を定義します。詳細については、トラフィック コピー ポリシーの作成 （681 ページ）を参照してください。

トラフィック コピーの宛先の作成

ステップ 1 メニューアイコン（≡）をクリックして、[Policy] > [Traffic Copy] > [Traffic Copy Destination] の順に選択します。

ステップ 2 トラフィック コピーの宛先の名前と説明を入力します。

ステップ 3 デバイスと 1 つまたは複数のポートを選択します。

ステップ 4 [Save] をクリックします。

トラフィック コピーの宛先の編集または削除

ステップ 1 メニューアイコン（≡）をクリックして、[Policy] > [Traffic Copy] > [Traffic Copy Destination] の順に選択します。

ステップ 2 編集または削除する宛先の横にあるチェックボックスをオンにします。

ステップ 3 次のいずれかを実行します。

- 変更を行うには、**[編集（Edit）]** をクリックして必要な変更を行い、**[保存（Save）]** をクリックします。
- 宛先を削除するには、**[削除（Delete）]** をクリックします。

トラフィック コピー契約の作成

ステップ 1 メニューアイコン（≡）をクリックして、[Policy] > [Traffic Copy] > [Traffic Copy Contract] の順に選択します。

ステップ 2 [Add]をクリックします。

ステップ 3 ダイアログボックスに、契約の名前と説明を入力します。

ステップ 4 **[コピー先（Copy Destination）]** ドロップダウン リストから、コピー先を選択します。

（注） コピー先は、1 つのトラフィック コピー契約に対し 1 つだけ指定できます。

選択可能なコピー先がない場合は、1 つ作成できます。詳細については、トラフィック コピーの宛先の作成 （680 ページ）を参照してください。

ステップ 5 [Save] をクリックします。

トラフィック コピー契約の編集または削除

ステップ 1 メニューアイコン（☰）をクリックして、[Policy] > [Traffic Copy] > [Traffic Copy Contract] の順に選択します。

ステップ 2 編集または削除する契約の横にあるチェックボックスをオンにします。

ステップ 3 次のいずれかを実行します。

- 変更を行うには、**[編集（Edit）]** をクリックして必要な変更を行い、**[保存（Save）]** をクリックします。
- 契約を削除するには、[削除（Delete）] をクリックします。

トラフィック コピー ポリシーの作成

ステップ 1 [Policy] > [Traffic Copy] > [Traffic Copy Policies] の順に選択します。メニューアイコン（☰）をクリックして、

ステップ 2 [Add Policy] をクリックします。

ステップ 3 [ポリシー名（Policy Name）] フィールドに名前を入力します。

ステップ 4 [説明（Description）] フィールドにポリシーを表す単語またはフレーズを入力します。

ステップ 5 [契約（Contract）] フィールドで、[契約の追加（Add Contract）] をクリックします。

ステップ 6 使用する契約の隣にあるラジオ ボタンをクリックし、次に [保存（Save）] をクリックします。

ステップ 7 [使用可能なグループ（Available Groups）] エリアから、[送信元（Source）]エリアにグループをドラッグアンド ドロップします。

ステップ 8 [使用可能なグループ（Available Groups）]エリアから、[宛先（Destination）]エリアにグループをドラッグアンド ドロップします。

ステップ 9 [Save] をクリックします。

トラフィックコピーポリシーの編集または削除

ステップ 1 [Policy] > [Traffic Copy] > [Traffic Copy Policies] の順に選択します。メニューアイコン（☰）をクリックして、

ステップ 2 編集または削除したいポリシーの横のチェック ボックスをオンにします。

ステップ 3 次のいずれかを実行します。

- 変更を行うには、**[編集（Edit）]** をクリックして必要な変更を行い、**[保存（Save）]** をクリックします。
- ポリシーを削除するには、**[削除（Delete）]** をクリックします。

第 VII 部

ネットワークのモニタリングとトラブルシューティング

第 27 章

Cisco AI エンドポイント分析

Cisco AI エンドポイント分析の概要

可視性は、エンドポイントを保護するための最初のステップです。Cisco AI エンドポイント分析は、エンドポイントと Internet of Things（IoT）デバイスの識別とプロファイリングに役立つエンドポイント可視性ソリューションです。Cisco AI エンドポイント分析エンジンを使用すると、さまざまなソースからネットワーク経由で受信したテレメトリ情報を使用して、エンドポイントにラベルを割り当てることができます。

Cisco AI エンドポイント分析で使用できるプロファイリングラベルは、エンドポイントタイプ、ハードウェアモデル、製造元、およびオペレーティング システム タイプです。これは多要素分類と呼ばれます。

Cisco AI エンドポイント分析は、潜在的に危険なエンドポイントやデバイスを特定して対処することを可能にする信頼スコアなどの機能により、ネットワークにおける繊細な可視化と処置を実現します。Cisco AI エンドポイント分析の GUI から Cisco ISE を介して ANC ポリシーを適用することにより、潜在的なリスクを管理することもできます。Cisco AI エンドポイント分析でエンドポイントのランダムおよび変更 MAC アドレスの問題をモニターして回避し、MAC アドレスの代わりに「DUID」と呼ばれる一意の属性を使用してエンドポイントを正確に識別することができます。

Cisco AI エンドポイント分析は、さまざまなソースからエンドポイントテレメトリを収集するのに役立ちます。主要なソースは、Network-Based Application Recognition（NBAR）メカニズムです。NBAR メカニズムは、Cisco Catalyst 9000 シリーズ スイッチ（アクセスデバイス）に組み込まれていて、ディープ パケット インスペクション（DPI）を実行します。Cisco AI エンドポイント分析は、Cisco DNA トラフィック テレメトリ アプライアンスからテレメトリを受信することもできます。

Cisco ISE、自己登録型ポータル、ServiceNow のような構成管理データベース（CMDB）ソフトウェアなど、さまざまなソースからエンドポイントコンテキスト情報を収集できます。

Cisco AI エンドポイント分析を使用すると、さまざまなネットワークデバイスからのデータインフローが可能になり、エンドポイントをより高い精度で容易に識別してプロファイリングし、異常に対処する機能が拡張されます。Cisco AI エンドポイント分析では、さまざまなエンドポイント情報を集約し、そのデータを使用してエンドポイントをプロファイリングできます。エンドポイントのプロファイリング後、AI と機械学習アルゴリズムを使用して、さまざまな方法を直感的に活用することで不明なエンドポイントの数を減らすこともできます。

Cisco AI エンドポイント分析の主な機能

- **Cisco AI エンドポイント分析ダッシュボード**

  Cisco AI エンドポイント分析ダッシュボードでは、ネットワークに接続されているエンドポイントの全体像を確認できます。既知のエンドポイント、不明なエンドポイント、プロファイリングされたエンドポイント、プロファイリングされていないエンドポイント、信頼スコアが低いエンドポイント、およびランダム MAC アドレスを使用するエンドポイントの数を表示できます。[AI Proposals] ダッシュレットには、エンドポイントのプロファイリングと管理を強化するためのインテリジェントなプロファイリングの提案が表示されます。

- **潜在的に危険なエンドポイントにフラグを付ける信頼スコア**

  Cisco AI エンドポイント分析は、エンドポイントに信頼スコアを割り当てます。これにより、ネットワーク内の潜在的に危険なエンドポイントを簡単にモニタして対処することができます。異常な動作がモニタおよび追跡され、追跡された異常の数と頻度に基づいて信頼スコアが割り当てられます。エンドポイントの信頼スコア （707 ページ）を参照してください。

- **ランダム MAC アドレスを使用するエンドポイントの検出**

  Cisco AI エンドポイント分析を使用すると、Cisco ISE から「DUID」と呼ばれる（Cisco ISE では「GUID」とも呼ばれます）一意のエンドポイント識別子を受信することにより、ランダムおよび変更 MAC アドレスの問題を処理できます。Cisco AI エンドポイント分析は、MAC アドレスの代わりに、エンドポイントの識別子として DUID を使用します。

- **機械学習機能を使用したネット内の不明なエンドポイントの削減**

  Cisco AI エンドポイント分析では、エンドポイントのグループ化で学習した情報に基づいてプロファイリング提案が提供されます。このような提案を使用して、ネットワーク内の

不明なエンドポイントやプロファイリングされていないエンドポイントの数を減らすことができます。

- **システムルールおよびカスタム プロファイリング ルールによるエンドポイントの管理**

  ネットワークに接続されたエンドポイントを確実にプロファイリングおよび管理するには、シスコが提供するシステムルールと自分で設計したカスタムルールを使用します。

- **Cisco AI エンドポイント分析によるエンドポイントの登録**

  Cisco AI エンドポイント分析を使用して、エンドポイントをオンボードおよびプロファイリングできます。この登録プロセスでエンドポイント属性データが収集されて、エンドポイントのプロファイリングに使用されます。

- **外部ソースを使用したエンドポイントの登録**

  構成管理データベース（CMDB）などエンドポイントデータの外部ソースの中には、Cisco AI エンドポイント分析に接続できるものがあります。これにより、ネットワーク内のエンドポイントを簡単に登録、管理、およびプロファイリングできます。

- **定義された非アクティブ期間後のエンドポイントのパージ**

  定義された時間にわたって非アクティブだったエンドポイントをネットワークから削除するには、エンドポイント パージ ポリシーを定義します。エンドポイントを削除する必要があるまでの非アクティブ期間を定義できます。また、プロファイリング属性に基づいて特定のエンドポイントのセットに作用するようにパージポリシーをカスタマイズすることもできます。

FIPS Compliance

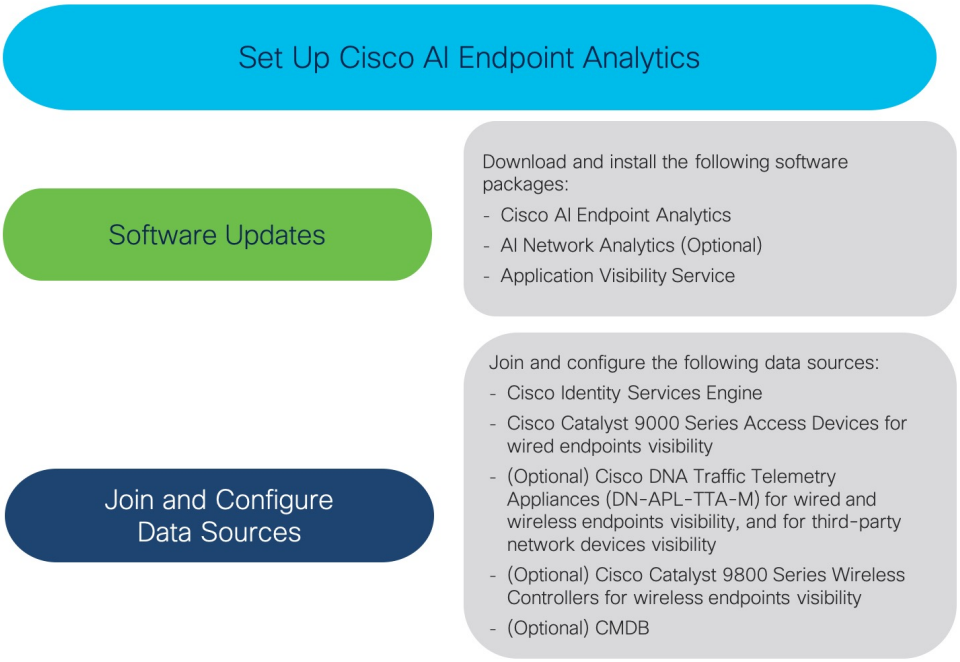
（注） Cisco DNA Center は米国の連邦情報処理標準（FIPS）をサポートしています。FIPS は、Cisco DNA Center イメージのインストール時に有効にできるオプションのモードです。デフォルトでは、FIPS モードはディセーブルです。

Cisco DNA Center で FIPS モードが有効になっている場合、Cisco DNA Center GUI の次の機能は使用できません。

- [AI Endpoint Analytics Setup] ウィンドウの [Optional Configurations] セクションにある [Enable AI Network Analytics] ダッシュレット。
- **[Policy]** > **[AI Endpoint Analytics]** > **[Overview]**の [AI Proposals] ダッシュレット。
- **[Policy]** > **[AI Endpoint Analytics]** > **[Overview]** > **[Configuration]** の [Profile Rule Settings] タブ。
- **[Policy]** > **[AI Endpoint Analytics]** > **[Overview]** > **[Configuration]** > **[Trust Score Sources]** の [AI Spoofing Detection] セクション。

- [Policy] > [AI Endpoint Analytics] > [Endpoint Inventory] の特定のエンドポイントの [Trust Score] の詳細の下にある [Endpoint Anomaly Detection] の [AI Spoofing Detection] セクション。
- **[Policy]** > **[AI Endpoint Analytics]** > **[Endpoint Inventory]** > **[Focus as Trust Score]** の [AI Spoofing Detection] 列。

Cisco DNA Center での Cisco AI エンドポイント分析のセットアップ



ソフトウェア アップデートのインストール

次の手順で説明するように、Cisco AI エンドポイント分析を使用するためのソフトウェアアップデートを Cisco DNA Center にインストールします。

ステップ 1 Cisco DNA Center にログインします。

ステップ 2 メニューアイコン（☰）をクリックして、**[System]** > **[Software Updates]** の順に選択します。

ステップ 3 [Updates] タブで、[Cisco AI Endpoint Analytics]、[AI Network Analytics]、および [Application Visibility Service] が [Application Updates] セクションにリストされているかどうかを確認してください。これらのアプリケーション更新が表示されている場合は、[Install All] ボタンをクリックします。

- Cisco DNA Center でエンドポイント プロファイリング ソリューションにアクセスするには、[Cisco AI Endpoint Analytics] 更新をインストールします。
- 機械学習と AI の機能を使用してインテリジェントなプロファイリング提案を受け取るには、[AI Network Analytics] 更新をインストールします。
- NBAR およびコントローラベースのアプリケーション認識（CBAR）の技術を使用してエンドポイント プロファイリングを通知するには、[Application Visibility Service] 更新をインストールします。

ステップ 4 これらの更新のいずれも [Updates] タブにリストされていない場合は、[Installed Apps] タブをクリックして、更新がすでにインストールされ、使用可能であるかどうかを確認してください。[Installed Apps] タブでは、ソフトウェアインストールが正常に完了しているかどうかも確認できます。

データソースの接続と有効化

Cisco AI エンドポイント分析が使用するデータソースは、すでに Cisco DNA Center に接続されている可能性があります。データソースが接続されている場合は、次の手順を参照して、Cisco AI エンドポイント分析でデータソースを使用できることを確認します。

Cisco AI エンドポイント分析が結果を提供できるようにするには、Cisco ISE または Catalyst 9000 シリーズ アクセスデバイスを Cisco DNA Center に追加する必要があります。

ステップ 1 Cisco ISE を Cisco DNA Center に接続します。

『Cisco DNA Center Appliance Installation Guide』の「Complete First-Time Setup」にある「Integrate Cisco ISE with Cisco DNA Center」セクションを参照してください。

次の Cisco ISE リリースが Cisco AI エンドポイント分析をサポートします。

- 2.4 パッチ 11 以降
- 2.6 パッチ 5 以降
- 2.7 パッチ 1 以降
- 3.0 以降

Cisco ISE 管理ポータルで次を実行します。

a) **[Work Centers]** > **[Profiler]** > **[Settings]** の順に選択します。
b) [Endpoint Analytics Settings] エリアで、次のチェックボックスをオンにします。
   - [Publish Endpoint Attributes to AI Endpoint Analytics]
   - [Consume Endpoint Profiles from AI Endpoint Analytics]

   Cisco ISE が 802.1X または MAB 認証方式でエンドポイントを認証すると、収集されたエンドポイント属性が Cisco AI エンドポイント分析で使用可能になります。Cisco ISE はまた Cisco AI エンドポイント分析とテレメトリデータを共有します。

ステップ 2 有線エンドポイントが表示されるように、Cisco 9000 シリーズ アクセスデバイスを Cisco DNA Center に接続します。

『*Cisco DNA Center User Guide*』の「Discover Your Network」を参照してください。

Cisco AI エンドポイント分析機能を有効にするには、Cisco 9000 シリーズアクセスデバイスを Cisco IOS-XE リリース 17.6 以降にアップグレードします。

必要なアクセスデバイスの CBAR を有効にするには、

a) Cisco DNA Center GUI でメニューアイコン（☰）をクリックして、**[Provision]** > **[Services]** > **[Application Visibility]** の順に選択します。
b) データが必要な Cisco Catalyst 9000 アクセスデバイスを選択します。[Site Devices] セクションのデバイス名の横にあるチェックボックスをオンにします。
c) [Enable CBAR] をクリックします。
d) 表示される確認ウィンドウで、[Yes] をクリックします。
e) [Enable CBAR] slide-in paneで、サポートされている SSID タイプの横にあるチェックボックスをオンにします。
f) [Enable] をクリックします。

ステップ 3 （任意）ワイヤレスエンドポイントを可視化するには、Cisco Catalyst 9800 シリーズ ワイヤレスコントローラを Cisco DNA Center に接続します。

次の Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ モデルは Cisco AI エンドポイント分析によりサポートされます。

- 9800-CL
- 9800-40
- 9800-80
- 9800-L

Cisco DNA Center リリース 2.3.2 以降は、Cisco IOS XE リリース 17.7.1 以降を搭載した Cisco Catalyst 9800 シリーズ ワイヤレスコントローラで FlexConnect をサポートします。SD-AVC バージョン 6 はサポートされていません。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの概要 （437 ページ） で Cisco Catalyst 9800 シリーズ ワイヤレス コントローラを設定およびプロビジョニングするには、Cisco DNA Centerを参照してください。

ステップ 4 （オプション）Cisco Catalyst IE9300 高耐久性シリーズ スイッチを Cisco DNA Center に接続します。

Cisco Catalyst IE9300 高耐久性シリーズ スイッチは Cisco AI エンドポイント分析でサポートされます。

『Cisco DNA Center User Guide』の「Discover Your Network」を参照してください。

ステップ 5 （任意）有線およびワイヤレスエンドポイントを可視化し、サードパーティのネットワークデバイスを可視化するには、Cisco DNA トラフィック テレメトリ アプライアンスを Cisco DNA Center に接続します。

Cisco DNA トラフィック テレメトリ アプライアンス（DN-APL-TTA-M）は、ミラーリングされたネットワークトラフィックからテレメトリを生成してエンドポイントを分析できるようにします。このアプライ

アンスでは、Network-Based Application Recognition ベース（NBAR ベース）のプロトコル検査、およびエンドポイント属性の抽出が可能です。

テレメトリアプライアンスで収集されたエンドポイント属性を Cisco AI エンドポイント分析で受信するには、Cisco ISE と Cisco DNA Center を統合する必要があります。

Cisco DNA Center でのアプライアンスのインストール、接続の構成、およびアプライアンスの管理については、『Cisco DNA Traffic Telemetry Appliances』を参照してください。

Cisco DNA トラフィック テレメトリ アプライアンスに接続されたアクセススイッチのスイッチドポートアナライザ（SPAN）受信ポートで CBAR を有効にするには、次のコマンドを使用します。

```
ip nbar protocol-discovery
```

テレメトリアプライアンスに接続されているすべてのエンドポイントが Cisco AI エンドポイント分析に表示されるわけではありません。Cisco DNA アシュアランス で管理されるネットワーク アクセス デバイス（NAD）にも接続されているエンドポイントのみが、Cisco AI エンドポイント分析 に表示されます。

ステップ 6 （任意）Cisco DNA Center で ServiceNow を有効にします。

a) ServiceNow を Cisco DNA Center に接続した後に、メニューアイコン（☰）をクリックして、**[Platform]** > **[Manage]** > **[Bundles]** の順に選択します。

b) バンドル [Endpoint Attribute Retrieval with ITSM (ServiceNow)] の [Status] が [New] の場合は、バンドルの [Enable] をクリックします。

ステップ 7 （任意）Cisco DNA Center で Cisco AI 分析を有効にします。

AI ベースのエンドポイントグループ化、カスタム プロファイリング ルール自動化、およびエンドポイントラベルに関する提案を受け取るには、また、ネットワーク内のスプーフィングされている可能性のあるデバイスを検出するには、[Cisco AI Analytics] ウィンドウで、必要な設定を有効にする必要があります。

これらの AI ベースの提案を受け取るには、AI ネットワーク分析ソフトウェアをインストールする必要があります。

a) メニューアイコン（☰）をクリックして、**[System]** > **[Settings]** > **[External Services]** > **[Cisco AI Analytics]** の順に選択します。

b) 有効にする次の各サービスのトグルボタンをクリックします。

- **AI エンドポイント分析**：AI ネットワーク分析は、機械学習を利用してネットワークのインテリジェンスを推進し、ネットワークパフォーマンスを効果的に改善して問題解決を加速できるようにします。AI ネットワーク分析は、ネットワークの動作を分析し、ネットワーク環境に適応することで、ノイズや誤検出を大幅に削減します。

- **エンドポイントスマートグループ化**：エンドポイントスマートグループ化は、AI と機械学習を使用して、AI ベースのエンドポイントグループ化、自動化されたカスタム プロファイリング ルール、クラウドソーシングされたエンドポイントラベルを提供することにより、ネットワーク内の不明なエンドポイントの数を減らします。

- **AI スプーフィング検出**：AI スプーフィング検出は、事前トレーニング動作モデルに基づいてスプーフィングされているエンドポイントを識別します。 [Enable AI Spoofing Detection] トグルボタンを有効にすると、Cisco DNA Center はこれらの動作モデルとネットワークデバイスによって提供されるフロー情報を使用して、スプーフィングされたエンドポイントを検出できます。参加して

いる顧客から収集されたフロー情報を使用して、いくつかの行動モデルが集中的にトレーニングされます。[Send data to help Cisco improve the model] トグルボタンを有効にすることにより、匿名での打ち切りデータの収集を可能にすることもできます。これにより、シスコによって動作モデルがさらに強化されます。

エンドポイント テレメトリ ソース

Cisco AI エンドポイント分析は、次の方法でテレメトリデータを受信します。

- **ディープ パケット インスペクション**

  ディープ パケット インスペクションは、Cisco Catalyst 9000 シリーズ アクセス デバイスによって実行される高度なパケット分析方法です。これらのアクセスデバイスは、NBAR を実行します。NBAR は、アプリケーション トラフィックを検査し、プロトコル分析を実行して、精度の高いエンドポイントを検出および識別し、プロファイリングします。

  ディープ パケット インスペクションのプロファイリングは、ネットワークへのエンドポイントトラフィックから収集されたさまざまな属性に基づいています。これらの属性は、パケットヘッダーレイヤ 4 ～ 7 から複数のプロトコルにわたって収集されます。

- **構成管理データベース接続**

  Cisco AI エンドポイント分析は、エンドポイント プロファイリングの精度を高めるために、構成管理データベース（CMDB）接続からエンドポイントデータを受信します。ServiceNow との接続により、CMDB から Cisco AI エンドポイント分析への情報を受信できます。

- **機械学習機能**

  プロファイリング用に収集されたデータは、匿名化されて、Cisco Cloud でデバイスデータレイクとして機能する場所に送信されます。ここでは、機械学習アルゴリズムで使用可能なデータを分析し、必要に応じて評価して適用できるプロファイリングルールを作成します。エンドポイント プロファイリングと管理を簡素化かつ効率化できるように、Cisco AI エンドポイント分析によってスマート プロファイリング ルールが提案されます。既存のルールも評価され、この継続学習に基づいて改善提案が提供されます。

[Cisco AI Endpoint Analytics Overview] ウィンドウ

メニューアイコン（☰）をクリックして、**[Policy]** > **[AI Endpoint Analytics]**の順に選択します。

[Overview] ウィンドウに次のダッシュレットが表示されます。

- **合計エンドポイント数**

  このダッシュレットでは、ネットワーク内のエンドポイントの合計数が [Fully Profiled] と [Missing Profiles] の 2 つのグループに分かれて表示されます。Cisco AI エンドポイント分

析は、エンドポイントタイプ、OS タイプ、ハードウェアモデル、およびハードウェア製造元の 4 つの要因に基づいてエンドポイントをプロファイリングします。エンドポイントにこれらの要因の 1 つ以上が欠落している場合は、[Missing Profiles] グループにプロファイリングされます。

[Missing Profiles Labels] をクリックすると、ネットワーク内のプロファイルが欠落しているエンドポイントの数が、プロファイルラベルタイプで分類されて表示されます。特定のプロファイルラベルが欠落しているエンドポイントを確認するには、プロファイルラベルの横にある数字をクリックします。[Endpoint Inventory] タブが、対応するエンドポイントのリストとともに表示されます。

- **AI 提案**

  Cisco AI エンドポイント分析は、スマートグループ化アルゴリズムを使用して、ネットワーク内で類似するプロファイリングデータを持つ不明なエンドポイントをグループ化します。AI エンドポイント分析を有効にした場合、次のタイプのルール提案が表示されます。これらのルール提案は、次のようにエンドポイントクラスタから学習した内容に基づいています。

  - 類似している可能性があるエンドポイントをプロファイリングするための新しいルール。
  - 以前に受け入れられていたルールの変更提案。
  - 不要になったプロファイリングルールの確認。

  詳細については、スマートグループ化のための Cisco AI ルール （733 ページ）を参照してください。

- **信頼スコア**

  [Trust Scores] ダッシュレットには、ネットワーク内のエンドポイントに割り当てられている信頼スコアの全体像が示されます。エンドポイントの信頼スコア （707 ページ）を参照してください。

- **設定**

  [Overview] エリアの右上隅にある [Configuration] リンクをクリックすると、次の設定にアクセスできます。

  - [Profile Rule Settings]：システムプロファイルルールの自動更新をスケジュールします。エンドポイントプロファイリング用の自動システムルール更新 （729 ページ）を参照してください。
  - [ISE Integration]：Cisco ISE への許可属性の公開 （699 ページ）を参照してください。
  - [Trust Score Sources]：信頼スコアのソースを有効または無効にするには、このトグルボタンをクリックします。[Authentication Method] ソースを無効にすることはできません。アクティブな Cisco ISE 統合が設定されている場合、エンドポイントが使用する認証方式およびそのポスチャステータスによって、エンドポイントの信頼スコアが通知されます。[AI Spoofing Detection]、[Changed Profile Labels]、[NAT Mode Detection]、

[Concurrent MAC Addresses]、[Security Sensor] などの信頼スコアデータのその他のソースは、有効または無効にすることができます。

「エンドポイントの信頼スコア （707 ページ）」を参照してください。

- [Endpoint Purge Policy]：エンドポイント パージ ポリシー （700 ページ）を参照してください。
- [Endpoint Subnet Inspection]：エンドポイントサブネット検査の設定 （701 ページ）を参照してください。

- **エンドポイント MAC ランダム化**

[Endpoint MAC Randomization] には、ネットワーク内の静的MACアドレスとランダムおよび変更 MAC アドレスの数が表示されます。ランダムおよび変更 MAC アドレスを持つエンドポイントの信頼スコア （715 ページ）を参照してください。

Cisco AI エンドポイント分析とTalos インテリジェンスの統合

Talos インテリジェンス は、包括的な脅威検出ネットワークです。Talos インテリジェンスは、脅威検出アナリストと、Web リクエスト、電子メール、マルウェアサンプル、オープンソースデータセット、エンドポイントインテリジェンス、ネットワーク侵入に及ぶリアルタイムの自動検出システムで構成されています。Cisco AI エンドポイント分析 を Talos と統合して、信頼できない IP アドレスに到達するネットワーク接続にフラグを立て、それらを隔離し、最も一般的なサイバー脅威からネットワークを保護します。

Cisco DNA Cloud は Talos インテリジェンス クラウド サービスと通信して、更新された IP のレピュテーションデータを 30 分ごとに取得します。IP のレピュテーションデータのこの更新は、すべての登録済みの Cisco DNA Center デバイスにプッシュされます。

Cisco DNA Center デバイスで Talos Intelligence をセットアップするには、次の手順を実行します。

始める前に

Cisco AI エンドポイント分析 を Talos インテリジェンスと統合するための前提条件は次のとおりです。

- Cisco DNA Center は Cisco DNA Cloud に登録する必要があります。

（注） ユーザーが Cisco DNA Cloud に登録されていない場合、Cisco DNA Center GUI の [Talos IP Reputation] 設定の下にあるトグルボタンの横に警告が表示されます。

- アカウントは、Cisco DNA Cloud の Talos オファーに登録されている必要があります。

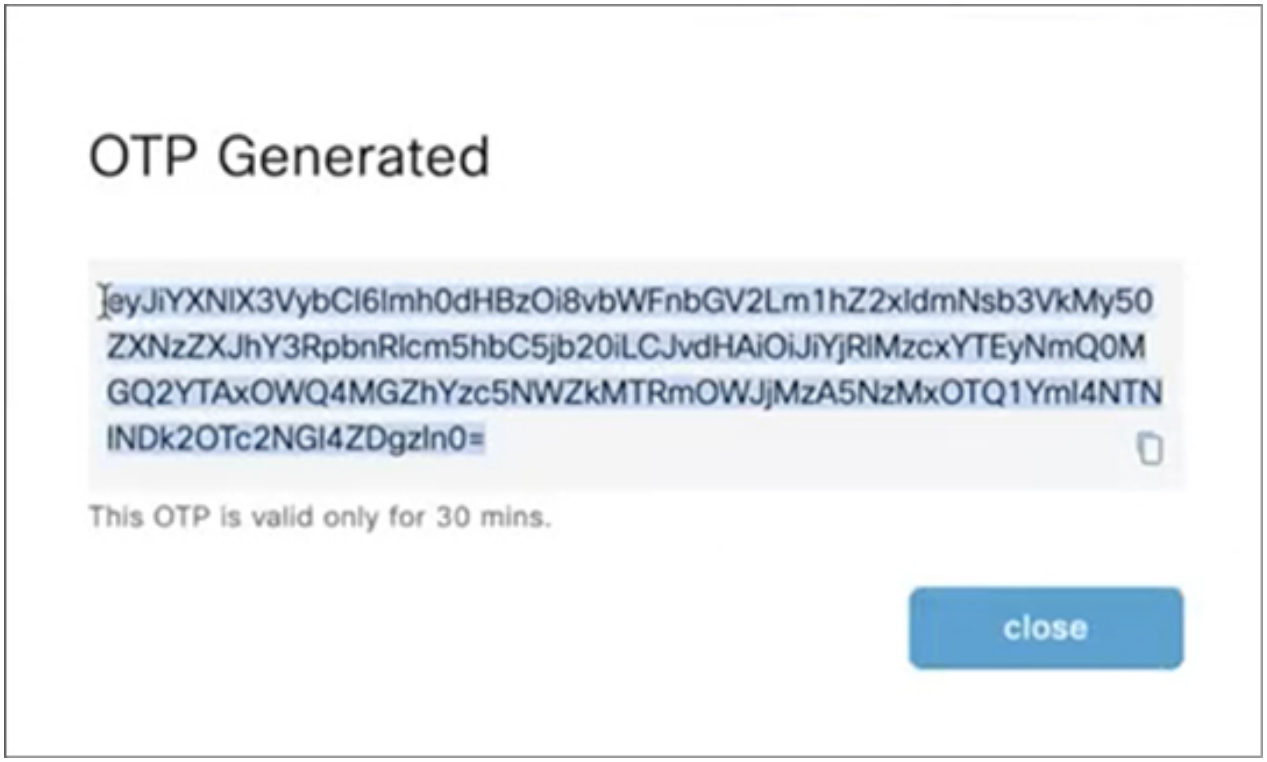
- Talos IP レピュテーション機能がスムーズに動作するには、アプリケーションテレメトリを有効にして、NetFlow コレクタとして Cisco DNA Center を選択します。

ステップ 1 Cisco DNA Cloud アカウントを作成します。Cisco DNA Cloud で、Talos オファー登録し、適切な Cisco DNA Center リージョンを選択します。

図 *28 : Talos* オファーへの登録

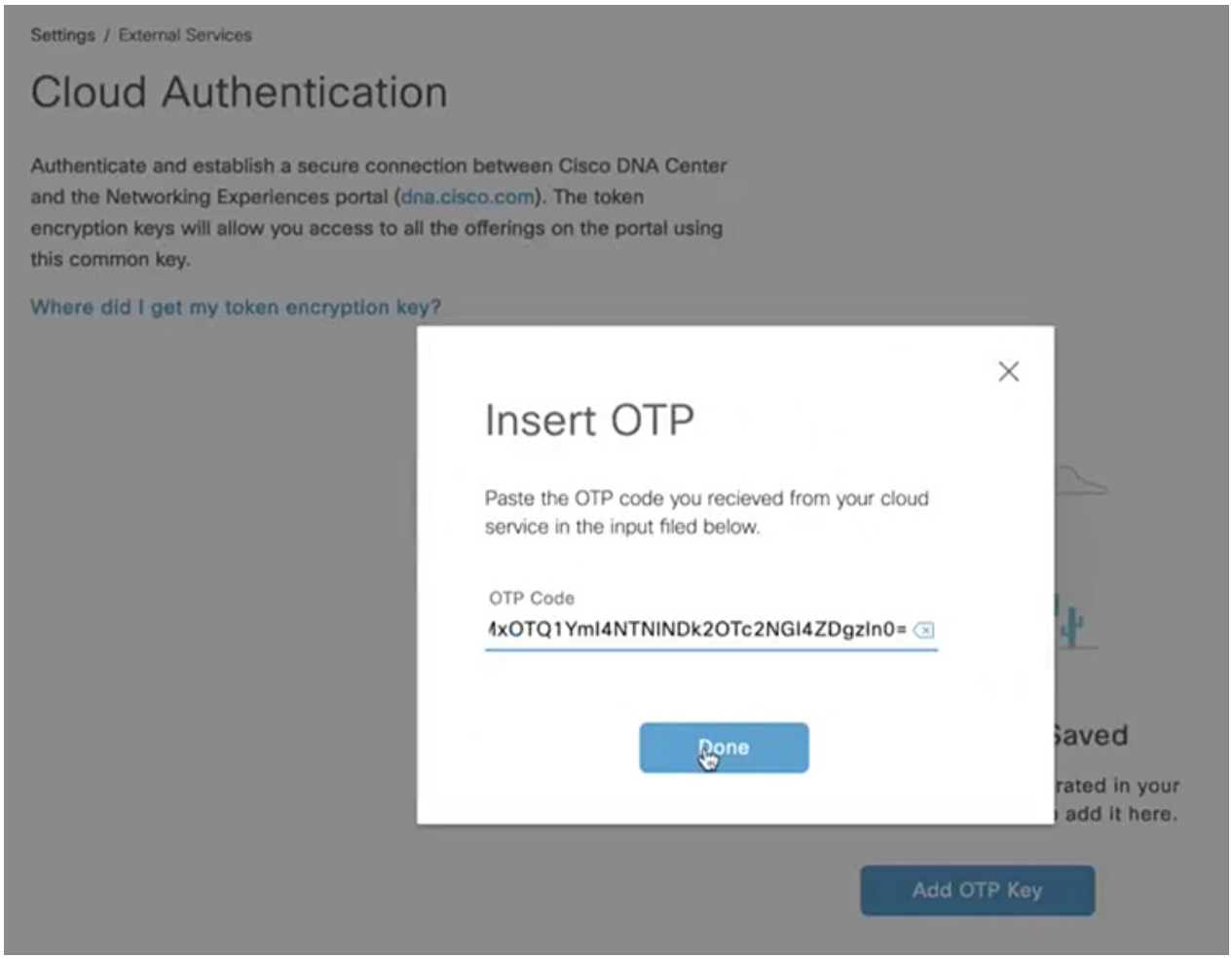
ステップ 2 [On-prem Connections] で Cisco DNA Center デバイスを登録します。ワンタイムパスワード（OTP）がデバイスに送信されます。この OTP は 30 分間有効です。

図 *29* : デバイスに送信される *OTP*



ステップ 3 Cisco DNA Center ホームページで、クラウド認証の OTP を使用して Cisco DNA Center デバイスを Cisco DNA Cloud に登録します（**[System-Settings]** > **[Cloud Authentication]**）。

図 *30 : OTP* を使用した *Cisco DNA Center* の *Cisco DNA Cloud* への登録



（注） Cisco DNA Center デバイスを Cisco DNA Cloud に登録したら、3 分待ってから次のステップに進みます。

ステップ 4 [Cisco DNA Center AI Endpoint Analytics] ウィンドウ（**[AI Endpoint Analytics]** > **[Configurations]** > **[Trust Score Sources]**）で、[Talos IP Reputation] トグルボタンをクリックして有効にします。[Trust Score] ウィンドウまたは [Cisco DNA Center System Settings] ウィンドウから [Talos IP Reputation] を有効にできます。[Talos IP Reputation] を有効にすると、Cisco DNA Center は更新された IP のレピュテーションデータが利用可能になるたびにそのデータを受信します。ネットワーク内のエンドポイントがブロックされた IP アドレスにアクセスしようとすると、フラグが設定され、エンドポイントの [Trust Score] ビューの Talos IP レピュテーションに対して、「Detected」という警告メッセージが表示されます。この警告により、エンドポイントの全体的な信頼スコアが低下します。Talos IP レピュテーション機能には、アクセスされた信用されていない IP アドレスと、エンドポイントによるアクセス試行回数に関する情報が含まれています。この情報は、ネットワークのセキュリティを強化することを決定するときに役立ちます。

[Talos Reputation] ウィンドウ（**[Cisco DNA Center System Settings]** > **[Talos IP Reputation]**）には、Talos から受信したさまざまなファイルの最新バージョンが表示されます。これらのファイルを受信した時刻も表

示されます。IPv4 および IPv6 ファイルは Talos IP レピュテーション データ ファイルであり、通常 1 日に 1 回更新されます。ただし、Threat Level ファイルはメタデータであり、このファイルが変更されることはほとんどありません。

Cisco ISE への許可属性の公開

ネットワークへのエンドポイントアクセスを承認し、エンドポイントを制御するために、Cisco ISE へ AI エンドポイント分析プロファイルデータを公開します。Cisco AI エンドポイント分析によって共有される属性情報には、AI エンドポイント分析ディクショナリを介して Cisco ISE 管理者が簡単にアクセスできるようになります。Cisco ISE 管理者は、Cisco ISE で許可ポリシーを簡単に作成できます。次の属性が Cisco ISE と共有されます。

1. 全体的な信頼スコアと、記録された各異常スコア。
2. CMDB 属性。
3. 多要素プロファイリング属性：ハードウェア製造元、ハードウェアモデル、オペレーティングシステム、およびエンドポイントタイプ。

Cisco DNA Center が Cisco ISE リリース 3.1 以降とアクティブに統合されており、認証属性を Cisco ISE に公開する必要がある場合は、次のタスクを実行します。

ステップ 1 Cisco DNA Center で属性共有を有効にするには、次の手順を実行します。

a) Cisco AI エンドポイント分析の [Overview] ウィンドウで、[Configurations] をクリックします。
b) 左側のパネルから [ISE Integration] をクリックします。
c) [Enable Profile Publishing to ISE] トグルボタンをクリックしてこの機能を有効にします。
d) 属性情報を Cisco ISE に公開するために使用するトピックのタイプに応じて、[Asset Topic Based Integration] チェックボックスと [Enhanced Authorization Integration] チェックボックスのいずれかまたは両方をオンにします。
e) **[Save]** をクリックします。

ステップ 2 Cisco ISE で pxGrid サブスクリプションを有効にするには、次の手順を実行します。

a) Cisco ISE GUI でメニューアイコンをクリックし、**[Work Center]** > **[Profiler]** > **[Settings]** の順に選択します。
b) Cisco ISE Release 3.1 に接続している場合、[Endpoint Analytics Settings] 領域で、次のチェックボックスをオンにします。
   - [Publish Endpoint Attributes to AI Endpoint Analytics]
   - [Consume Endpoint Profiles from AI Endpoint Analytics]

次のタスク

サブスクリプションを検証するには、Cisco ISE メインメニューから、**[Administration]** > **[pxGrid Services]** > **[Diagnostics]** > **[WebSocket]** > **[Clients]** の順に選択します。新しく作成された「com.cisco.ea.data.ise-<Cisco ISE node>」を含むサブスクリプションが、PSN ノードの [Subscription] 列に表示されます。

Cisco ISE の **[Policy]** > **[Policy Sets]** ウィンドウで、[Conditions Studio] に「**Endpoint-Analytics**」という名前の新しいディクショナリが表示されます。

Cisco ISE の **[Context Visibility]** > **[Endpoints]** ウィンドウで、エンドポイントの詳細情報の [MAC Address] をクリックします。その詳細情報の属性エリアに、Cisco AI エンドポイント分析から受信された属性の「EA-」というプレフィックスを含む属性が表示されます。

エンドポイント パージ ポリシー

定義された時間にわたって非アクティブだったエンドポイントをネットワークから削除するには、エンドポイント パージ ポリシーを定義します。エンドポイントを削除する必要があるまでの非アクティブ期間を定義できます。また、プロファイリング属性に基づいて特定のエンドポイントのセットに作用するようにパージポリシーをカスタマイズすることもできます。パージポリシーは毎日午前2時（サーバー時間）に実行され、定義されたパージ要件を満たすエンドポイントがネットワークから削除されます。

Cisco AI エンドポイント分析にインポートされた登録済みエンドポイントおよび静的エンドポイントは、エンドポイント パージ ポリシーの影響を受けません。

Cisco DNA Center のバックアップ/復元操作、およびエンドポイント パージ アクティビティを同時に実行することはできません。バックアップ/復元操作が午前 2 時に進行中の場合、パージアクティビティは開始されません。エンドポイント アクティビティの進行中にバックアップ/復元操作が開始されると、エンドポイントパージの実行は停止され、パージアクティビティは未完了のままになります。残りのエンドポイントは、次のパージが翌日の午前 2 時（サーバー時間）に実行されるまで処理されません。

エンドポイントパージポリシーを表示、編集、または追加するには、メニューアイコン（☰）をクリックし、**[Policy]** > **[AI Endpoint Analytics]** > **[Configurations]** > **[Endpoint Purge Policy]** を選択します。デフォルトでは、次のポリシーを使用できます。

- **Default**
- **Random MAC Default**

これらのデフォルトポリシーは編集できません。有効または無効にすることだけが可能です。

パージポリシーの作成

ステップ 1 メニューアイコン（☰）をクリックして、**[Policy]** > **[AI Endpoint Analytics]** > **[Configurations]** > **[Endpoint Purge Policy]**の順に選択します。

ステップ 2 [Add Endpoint Purge Policy] をクリックします。

ステップ 3 [Add Endpoint Purge Policy] ダイアログボックスで、[Let's Do It] をクリックしてワークフローに直接移動します。

ステップ 4 [Define Policy Details] ウィンドウで、次の手順を実行します。

1. ポリシーの名前を [Rule Name] フィールドに入力します。
2. [Select Status] ドロップダウンリストで [Enabled] または [Disabled] を選択します。
3. エンドポイントがパージされるまでの非アクティブ時間を定義します。[Elapsed Greater than or Equal to] フィールドに値（日単位）を入力してください。有効な値の範囲は 5 ー 180 日です。

ステップ 5 （オプション）[Define Additional Policy Conditions] ウィンドウで、このパージポリシーの影響を受けるエンドポイントをフィルタ処理するためのプロファイリング属性を選択します。選択する属性の横にあるチェックボックスをオンにして、その属性に関して表示されるドロップダウンリストで必要な値を選択してください。

ステップ 6 [Summary] ウィンドウに、パージポリシーの設定が表示されます。表示される詳細情報を確認し、[Done] をクリックしてポリシーを作成します。

次のタスク

エンドポイント パージ アクティビティの監査ログ

エンドポイント パージ ポリシーを有効にして、パージアクティビティが実行された後に、エンドポイント パージ アクティビティの監査ログを確認することができます。

1. メニューアイコン（☰）をクリックして、**[Activities]** > **[Audit Logs]** の順に選択します。
2. 監査ログの説明フィールドを調べて、監査ポリシーの実行に関連するログを見つけます。
3. 適切な監査ログをクリックして、実行されたパージポリシーの詳細情報を確認します。

エンドポイントサブネット検査の設定

展開内では、アクセスレイヤにあるデバイスとアクセスレイヤよりも上にあるデバイスの IP サブネットが異なります。シスコの TTA デバイスの場合、エンドポイント プロファイリングの精度は、Cisco AI エンドポイント分析によってサウスバウンドトラフィックのみが分析される場合に最大になります。エンドポイントプロファイリングを向上させるには、Cisco AI エンドポイント分析 で分析する必要がある特定の IP サブネットまたはサブネット範囲を設定します。

その後、このフィルタ処理されたサブネットに関する設定は、Cisco SD-AVC サーバーと共有されます。この設定は、Cisco SD-AVC サーバーを介して Cisco TTA デバイスに適用されます。

ステップ 1 メニューアイコン（☰）をクリックして、**[Policy]** > **[AI Endpoint Analytics]** > **[Configurations]** > **[Endpoint Subnet Inspection]**の順に選択します。

ステップ 2 [IP Subnet] フィールドに必要な値を入力します。

ステップ 3 [+] をクリックして IP サブネットを追加します。このウィンドウでは、複数のサブネットまたはサブネット範囲を追加できます。

Endpoint Inventory

[Endpoint Inventory] タブには、設定されたデータソースを介して Cisco AI エンドポイント分析に接続されているエンドポイントの詳細が表示されます。このタブには、[Focus] ドロップダウンリストを使用して選択できる 2 つのビューがあります。

- [All Endpoints]：これは [Endpoint Inventory] タブのデフォルトビューです。このビューには、接続されているすべてのエンドポイントのプロファイリング情報が表示されます。

  表示されるエンドポイント インベントリ テーブルを編集またはカスタマイズするには、テーブルの上部の右隅にある歯車アイコンをクリックします。表示されるペインには、[Table Appearance]、[Edit Table Columns]、および [Edit Custom Views] メニューが含まれており、テーブルビューやテーブルに表示する情報を選択したり、カスタムビューを作成したりできます。

  [Apply] をクリックして変更を保存するか、[Reset All Settings] をクリックしてエンドポイント インベントリ テーブルのデフォルト設定を適用します。

- [Trust Score]：このビューには、エンドポイントの全体的な信頼スコアを示すさまざまな要因の列が表示されます。信頼スコアは、動作異常が検出されたエンドポイントを特定するために役立ちます。これにより、エンドポイントの詳細情報を調べて、必要な修復アクションを実行することができます。低い信頼スコアを管理するためにエンドポイントに ANC ポリシーを適用する場合、[Trust Score] ビューには、適用された ANC ポリシーの名前とポリシーが適用された日時も表示されます。エンドポイントの信頼スコア （707 ページ）を参照してください。

要件に基づいて一連のエンドポイントを簡単にフィルタ処理できます。テーブルの上部にある検索バーを使用すると、フィルタパラメータを簡単に見つけることができます。入力して検索支援機能を使用するか、表示されるドロップダウンをスクロールして必要なパラメータを見つけて選択することができます。

[All Endpoints] テーブルと [Trust Score] テーブルのほとんどの列には、クイックフィルタが含まれています。一部のフィルタでは値を選択できるドロップダウンメニューが表示され、一部のフィルタは入力可能なテキストフィールドです。

エンドポイントを登録したり、登録済みのエンドポイントを編集、削除、およびプロファイリングしたりできます。単一または複数のエンドポイントを選択するには、MAC アドレスの横にあるチェックボックスをオンにします。これにより、選択したエンドポイントに対して、[Actions] ドロップダウンリストから特定のアクションをフィルタリングして実行することができます。

エンドポイントのプロファイリングの完全な詳細を表示するには、エンドポイントの [MAC Address] をクリックします。表示されるスライドインダイアログボックスには、ユーザーの詳細、エンドポイントの詳細、およびエンドポイントの属性の詳細が含まれます。

Cisco DNA Center リリース 2.2.2 以降では、[Details] タブに次の新しいフィールドが表示され、Cisco ISE から受信した詳細が示されます。

- [Authentication Status]：このフィールドには、エンドポイントが Cisco ISE で認証された場合は [Started]、そうでない場合は [Disconnected] と表示されます。
- [Authorization Profile]：Cisco ISE のエンドポイントに設定されている認証ポリシーがここに表示されます。
- [Security Group Tag]：Cisco ISE でエンドポイントに設定されたセキュリティグループタグがここに表示されます。

これらの属性の詳細については、使用する Cisco ISE リリースの Cisco ISE 管理者ガイド [英語] を参照してください。

Cisco DNA Center 2.2.2 以降では、エンドポイントの詳細を示すスライドイン ダイアログボックスに [Trust Score] タブがあります。このタブには、エンドポイントの信頼スコアを示すさまざまな要因の詳細が表示されます。エンドポイントの信頼スコア （707 ページ）を参照してください。

Cisco DNA Center 2.2.3 以降では、[Details] タブに [Previous MAC Addresses] エリアがあり、MAC ランダム化機能が有効になっているエンドポイントで使用された MAC アドレスが表示されます。ランダムおよび変更 MAC アドレスを持つエンドポイントの信頼スコア （715 ページ）を参照してください。

Cisco AI エンドポイント分析データのエクスポート

このウィンドウからエンドポイントとエンドポイントの詳細のリストをエクスポートするには、[Export] をクリックします。[Endpoint Inventory] ウィンドウでフィルタを適用すると、フィルタ処理されたエンドポイントのみがエクスポート用に処理されます。すべてのエンドポイントの詳細をエクスポートするには、フィルタが適用されていないことを確認して、[Export] をクリックします。

[Export] をクリックすると、[Reports] ウィンドウで新しいタブが開きます。[Generated Reports] ウィンドウには、開始されたエクスポートのリストが表示され、リストの一番上に最新のエクスポート要求が表示されます。[Endpoint Inventory] ウィンドウから生成されたレポートの [Template Category] 列に [AI Endpoint Analytics] が含まれています。レポートの生成には数分かかります。レポートのダウンロード準備ができると、[Last Run] 列の値が [Not Initiated] から、その横にダウンロードアイコンがあるタイムスタンプに変わります。タイムスタンプは、エクスポートリストが生成された時刻を示します。ダウンロードアイコンをクリックして、エンドポイントのリストの CSV ファイルをシステムにダウンロードします。

次の手順で、[Reports] ウィンドウから Cisco AI エンドポイント分析データをエクスポートすることもできます。

（注） エンドポイントの AI エンドポイント分析データの最初のエクスポートは [Endpoint Inventory] ウィンドウから実行する必要があります。その後、[Reports] ウィンドウから直接 AI エンドポイント分析レポートを生成できます。

ステップ 1 メニューアイコン（≡）をクリックして、 **[Reports]** > **[Report Templates]** > **[AI Endpoint Analytics]**の順に選択します。

ステップ 2 タスクの概要ウィンドウが表示されたら、[Let's Do It] をクリックして、ワークフローに直接移動します。

（注） 今後この画面をスキップするには、[Don't show this to me again] チェックボックスをオンにします。

ステップ 3 [Select Report Template] ウィンドウでは、[Endpoint Profiling] テンプレートがデフォルトで適用されています。

ステップ 4 [Setup Report Scope] ウィンドウで、次の手順を実行します。

a) [Report Name] フィールドに名前を入力します。

b) [Endpoint Inventory] ウィンドウからエクスポートするエンドポイントのリストに適用するフィルタを定義します。

c) すべてのエンドポイントの詳細をエクスポートするには、[Scope]エリアで値を選択しないでください。

ステップ 5 [Select File Type] ウィンドウの [Client Details] エリアで、選択したパラメータを確認できます。関連するフィールドの横にあるチェックボックスをオンまたはオフにして、エクスポートする情報を編集します。

ステップ 6 [Schedule Report] ウィンドウで、[Run Now]、[Run Later]（[One-Time] または [Run Recurring]）オプションボタンをクリックします。

（注） [Run Later] の [One-Time] および [Run Recurring] オプションには、エクスポートの時間を定義するスケジューリングフィールドが表示されます。

ステップ 7 [Delivery and Notification] ウィンドウでは、[Email Report] チェックボックスをオンにしないでください。

ステップ 8 [Summary] ウィンドウで、すべての設定を確認します。変更するには、[Edit] をクリックします。

ステップ 9 生成されたレポートのリストを表示するには、このウィンドウの [View Reports] リンクをクリックします。レポートが生成され、このウィンドウに表示されるまでに数分かかります。

エンドポイントのフィルタ処理

この手順を使用して、プロファイリングデータ、プライマリ プロファイリング ラベル、既知のプロファイル、および正常性ステータスに基づいてエンドポイントをフィルタ処理します。

ステップ 1 [Endpoint Inventory] ウィンドウで、[Filter] をクリックします。

ステップ 2 必要に応じて、対応するドロップダウンリストから値を選択するか、必要な値のオプションボタンをクリックして、次のフィルタを定義します。

- **Mac Address**
- **信頼得点**
- **エンドポイント タイプ**
- **ハードウェア モデル**
- **ハードウェア製造元**
- **OS Type**
- **Registered**
- **Is Random Mac**

ステップ 3 [Apply] をクリックします。

また、4 つのプライマリ プロファイリング ラベルで表示されるプロファイリング済みのエンドポイントをフィルタ処理することもできます。[View Known Profiles] セクションで 1 つ以上のラベルをクリックします。

エンドポイントの正常性ステータスは 5 分ごとに更新されます。

属性用語集

属性用語集は、Cisco ISE プローブデータから使用可能なすべてのプロファイリング属性のリストです。

すべてのプロファイリング属性を表示するには、次の手順を実行します。

ステップ 1 [Endpoint Inventory] ウィンドウで、エンドポイントの MAC アドレスをクリックします。

ステップ 2 右側に表示される新しい領域で、[View Attribute Glossary] をクリックします。

[Attribute Glossary] ウィンドウに、属性ごとに次の情報が表示されます。

- **キープロファイリング属性**
- **説明**
- **関連付けられたプロファイルラベル**
- **[Source]**
- **Dictionary**
- **ディスカバリの方法**

用語集では、すべてのプロファイリング属性の詳細ビューが表示されます。プロファイリング属性がプロファイルラベルの作成に頻繁に使用される場合は、そのラベルが [Associated Profile Labels] 列に一覧表示されます。

また、ルールの論理条件の作成中に、[Choose Attribute Condition] ウィンドウに属性用語集を表示することもできます。詳細については、「カスタムルールの作成」を参照してください。

エンドポイントの登録

新しいエンドポイントをオンボードおよびプロファイリングするには、そのエンドポイントを Cisco AI エンドポイント分析に登録します。エンドポイントのプロファイリング情報は、分類のための信頼できる情報源です。また、[Register Endpoint] オプションを使用して、登録済みのエンドポイントの新しいプロファイル情報を更新することもできます。

ステップ 1 **[Actions]** > **[Register Endpoints]** の順に選択します。

ステップ 2 [Single] または [Bulk] のいずれかのオプションボタンをクリックして、単一のエンドポイントまたは複数のエンドポイントを登録するかどうかを選択します。

オプション	手順
シングル	[MAC Address]、[Endpoint Type]、[Hardware Model]、および [Hardware Manufacturer] にエンドポイントの値を入力します。
バルク（Bulk）	1. [Download .csv Template] オプションをクリックして、.csv テンプレートをダウンロードします。 2. ダウンロードした .csv ファイルに、登録する必要がある各エンドポイントの詳細を入力します。具体的には、MAC アドレス、エンドポイントタイプ、ハードウェアモデル、およびハードウェア製造元です。このファイルを保存します。 3. [Choose a File] オプションを使用して .csv ファイルをアップロードします。 [Bulk] オプションを使用すると、一度に最大 500 個のエンドポイントを登録できます。

ステップ 3 [Next] をクリックします。

ステップ 4 [Review Endpoint] ウィンドウでエンドポイントの詳細を確認します。変更が必要な場合は、エンドポイントの詳細を編集することもできます。

（注） 既存のエンドポイントの登録中は、エンドポイントのプロファイルラベルの変更が紫色で反映され、編集できます。

ステップ 5 [Next] をクリックして、登録プロセスを続行します。

ステップ 6 [登録（Register）] をクリックします。

登録済みのエンドポイントの編集

登録済みのエンドポイントのプロファイリング情報は、[Endpoint Inventory] ウィンドウから更新できます。

ステップ 1 編集するエンドポイントの MAC アドレスの横にあるチェックボックスをオンにします。

ステップ 2 [Actions] をクリックします。

ステップ 3 [Edit Endpoint] をクリックします。

ステップ 4 [Endpoint Type]、[Hardware Model]、[Hardware Manufacturer] に詳細を入力します。

ステップ 5 [Save] をクリックします。

登録済みのエンドポイントの削除

登録済みのエンドポイントがネットワークの一部ではなくなった場合は、Cisco AI エンドポイント分析から削除できます。

ステップ 1 削除するエンドポイントの MAC アドレスの横にあるチェックボックスをオンにします。

ステップ 2 [Actions] をクリックします。

ステップ 3 [Delete Endpoint] をクリックします。

次のメッセージが表示されます。

「Do you really want to delete the selected endpoint(s)?」

ステップ 4 [Yes] をクリックして、Cisco AI エンドポイント分析からエンドポイントを完全に削除します。

エンドポイントの信頼スコア

Cisco AIエンドポイント分析 は、エンドポイントに信頼スコアを割り当てます。これにより、ネットワーク内の潜在的に危険なエンドポイントを簡単にモニターして対処することができます。異常な動作がモニタおよび追跡され、追跡された異常の数と頻度に基づいて信頼スコアが割り当てられます。

信頼スコアの計算に含める必要があるソースを選択するには、Cisco AIエンドポイント分析 の [Overview] ウィンドウで、**[Configuration]** > **[Enable Trust Sources]** を選択します。有効にする各ソースのトグルボタンをクリックします。

Cisco AI エンドポイント分析 は、次の要因に基づいて履歴信頼スコアを生成します。

- エンドポイントに関連付けられた異常の履歴（このエンドポイントに関して検出された異常の数）。
- エンドポイントで検出された各異常の重大度。

Cisco DNA Center リリース 2.2.3 以降では、エンドポイントの全体的な信頼スコア計算に次の異常が考慮され、検出された異常ごとにスコアが表示されます（対応するソースが有効になっている場合）。

- **AI スプーフィング検出**

  Cisco AI エンドポイント分析 は、NetFlow テレメトリデータ、および Cisco ISE デバイスと SD-AVC デバイスからのネットワークプローブデータを分析して、スプーフィングされたエンドポイントを検出します。NetFlow コレクタサーバーの構成方法の詳細については、テレメトリを使用した Syslog、SNMP トラップ、NetFlow コレクタサーバー、および有線クライアントデータ収集の設定 （33 ページ）を参照してください。Cisco DNA Center 2.3.2 以降では、Cisco DNA トラフィック テレメトリ アプライアンスからのプローブおよび NetFlow データ（DN-APL-TTA-M）も分析されます。Cisco DNA トラフィック テレメトリ アプライアンスへのトラフィックの受信スパンを構成して、Cisco AI エンドポイント分析でエンドポイントトラフィックデータをスプーフィング検出に使用できるようにします。

  各エンドポイントタイプには、機械学習アルゴリズムを使用して開発された動作モデルがあります。エンドポイントに対して受信されたデータに基づき、エンドポイントの動作がエンドポイント タイプ プロファイルで予期されていない動作の場合、エンドポイントには [AI Spoofing Detection] 領域で低い信頼スコアが割り当てられます。エンドポイントで使用されるアプリケーションおよびサーバーポートは、このスプーフィング検出プロセスで分析されます。たとえば、プリンタとしてプロファイリングされたエンドポイントがビデオ通話アプリケーションを使用する場合、スプーフィングされたエンドポイントとして識別され、信頼スコアが割り当てられます。

  エンドポイントは、Cisco DNA Center の管理対象スイッチの MAC アドレスによって識別されます。NAT の使用、仮想マシンまたはコンテナの実行など、単一の MAC アドレスを使用する複数のエンドポイントは、Cisco AI エンドポイント分析でサポートされている構成ではありません。

  AI スプーフィング検出は現在、次のデバイスタイプをカバーしています。

  - IP 電話
  - プリンタ
  - カメラ
  - 次のハードウェアモデル属性を持つビルディングオートメーションデバイス：
    - Automated-Logic-Device
    - Honeywell-Device
    - Johnson-Controls-Device

- Rockwell-Automation-Device
- Schneider-Electric-Device
- Siemens-Automation-Device
- Siemens-Building-Device
- Trane-Device

- TelePresence：
  - 次のいずれかのハードウェアモデルを持つエンドポイント：
    - Cisco-Tandberg-Device
    - Cisco-TelePresence
    - Cisco TelePresence SX80
    - Cisco Telepresence SX20
    - Cisco-Collaboration-Room-Endpoint
    - Poly-Device
  - デバイスタイプがビデオ会議のエンドポイント

- **変化したプロファイルラベル**

  デバイスがネットワークに参加し、デバイスがアクティブであるときに定期的にプローブを実行すると、エンドポイントのプロファイリングデータが継続的にモニタされ、更新されます。エンドポイントから受信したプロファイリングデータにおける特定の変化は、Cisco AI エンドポイント分析 で異常としてフラグが付けられます。たとえば、エンドポイントが最初に Linux デバイスとしてプロファイルされ、その後で macOS デバイスとしてプロファイルされた場合、これは重大度の高い異常としてフラグが付けられます。エンドポイントの [Changed Profile Label] 列にスコアが割り当てられ、エンドポイントの全体的な信頼スコアもこの変化を反映して更新されます。

  ただし、macOS のバージョンに変化があり、エンドポイントが新しいリリースから古いリリースにダウングレードされたように見える場合、そのような変化は優先順位の低い異常としてフラグが付けられ、対応するスコアがそれに応じて更新されます。

- **NAT モード検出**

  ネットワーク内に NAT 対応ルータがある場合、NAT ルータに接続されたエンドポイントは、特定のエンドポイントの IP アドレスまたは MAC アドレスではなくルータの IP アドレスまたは MAC アドレスによって認識されます。NAT 対応ルータに関する情報は、接続先の Cisco Catalyst 9000 シリーズ デバイスから収集されます。

- **同時 MAC アドレス**

  同じ MAC アドレスを共有し、Cisco Catalyst 9000シリーズ デバイスに接続されているエンドポイントを特定してください。共有 MAC アドレスを持つエンドポイントには、同時

MAC アドレススコアが割り当てられます。これにより、容易に、それらのエンドポイントを識別して詳細情報を調べることができます。

- **セキュリティセンサー**

  セキュリティ センサー スキャン機能を使用すると、特定の Cisco Catalyst 9000 シリーズスイッチにアクティブプローブをインストールし、開いていると想定されていないのに開いているポート、クレデンシャルの脆弱性、またはその両方についてエンドポイントをスキャンするように Cisco AI エンドポイント分析 を設定できます。

エンドポイントの信頼スコアは、Cisco ISE から収集される次のイベントによっても通知されます。Cisco ISE を介して認証するすべてのエンドポイントは、次のイベントに基づいて初期信頼スコアを受け取ります。

- **認証方式**
- **ポスチャ**

（注） Cisco Catalyst 9000 シリーズ デバイスからデータを受信する信頼スコアソースの場合、デバイスで CBAR を有効にし、デバイスを Cisco IOS-XE リリース 17.6 以降にアップグレードする必要があります。

[Endpoint Inventory] ウィンドウに表示される信頼スコアは、エンドポイントの異常の履歴と重大度を考慮した全体的な信頼スコアです。[MAC Address] をクリックすると、エンドポイントに割り当てられた信頼スコアの原因の詳細情報が表示されます。たとえば、エンドポイントに関して低レベルの異常が検出され、これが異常の唯一のインスタンスである場合、異常イベントの実際の信頼スコアが 7 であっても、エンドポイントの全体的な信頼スコアは 9 になります。

複数の低レベルの異常が検出された場合は、異常の数を考慮して全体的な信頼スコアがさらに低下します。

割り当てられる信頼スコアの範囲は 1 ー 10 で、次のように分類されます。

信頼スコアカテゴリ	範囲	エンドポイントの脅威レベル
低	1 ～ 3	高
中規模	4 ～ 6	中程度
高	7 ～ 10	低

その後、Cisco ISE から適応型ネットワーク制御（ANC）ポリシーを適用して、エンドポイントで適切な修復アクションを実施することができます。*Cisco ISE の管理者ガイド*で「Maintain and Monitor」の章にある「Adaptive Network Control」を参照してください。

ANC ポリシーは、Cisco ISE で定義され、選択したエンドポイントに修復アクションを適用することを可能にします。ANC ポリシーを適用して、エンドポイントを隔離またはシャットダウンしたり、エンドポイントのポートをバウンスしたり、エンドポイントの再認証を強制的に

実行することができます。Cisco AI エンドポイント分析で望ましくない信頼スコアを持つエンドポイントに ANC ポリシーを適用すると、認可変更（CoA）が Cisco ISE からそのエンドポイントに送信されます。

エンドポイントは、MAC アドレスによって識別されます。Cisco ISE は、ANC 適用時点で識別された MAC アドレスに関してアクティブセッションを保持しているエンドポイントに CoA を送信します。その時点で Cisco ISE においてアクティブセッションを持たない、同じ MAC アドレスのエンドポイントは、新しいセッションが開始されたときに、または設定された再認証タイマーの終了時に再認証する必要がある場合に、ANC ポリシーと照合されます。

ANC ポリシーが適用されているエンドポイントを確認するには、Cisco ISE 管理ポータルにログインします。メインメニューから、**[Operations]** > **[RADIUS]** > **[Live Sessions]** の順に選択します。[Endpoint ID] 列に、スプーフィングされたエンドポイントの MAC アドレスを入力します。これにより、同じ MAC アドレスを共有し、現在 Cisco ISE でライブセッションを持つエンドポイントがフィルタ処理されます。これらが、ANC ポリシーの影響を受けるエンドポイントです。

Cisco ISE で RADIUS セッションの履歴ログを表示するには、メインメニューから、**[Operations]** > **[Reports]** > **[Reports]** > **[Endpoints and Users]** > **[RADIUS Authentications]** の順に選択します。

Cisco ISE でエンドポイントへの ANC ポリシーの適用を表示または変更するには、メインメニューから、**[Context Visibility]** > **[Endpoints]** の順に選択します。必要に応じて、エンドポイントの MAC アドレスの横にあるチェックボックスをオンにして、リストの上部に表示されるオプションをクリックしてください。

前提条件

エンドポイントの信頼スコアを受信するための前提条件：

- Cisco DNA Center がリリース 2.2.2 以降にアップグレードされている。
- Cisco ISE がオンプレミス Cisco DNA Center に接続されている。
- ネットワーク アクセス デバイスが、Cisco DNA アシュアランス と Cisco ISE の両方によって管理されている。

（注） Cisco DNA アシュアランス では 500 台の NetFlow エクスポータのみサポートされるため、エンドポイント スプーフィング検出機能は、NetFlow エクスポートフローで最大 500 台のネットワーク アクセス デバイスをサポートします。

- ネットワーク アクセス デバイスに接続されているエンドポイントが、Cisco ISE を介して認証されている。
- [Trust Score Sources] ウィンドウ（**[Policy]** > **[AI Endpoint Analytics]** > **[Configurations]** > **[Trust Score Sources]**）で、信頼スコアの計算に必要なソースが有効になっている。

変化したプロファイルラベル

Cisco AI エンドポイント分析では、エンドポイントの正確なプロファイルラベルを取得するために、さまざまなソースから複数のプローブのデータが継続的に収集されます。Cisco AI エンドポイント分析では、次のソースから、次のデータが収集されます。

Cisco ISE から：

- RADIUS プローブ
- ディレクトリからのユーザーの詳細情報
- VPN の詳細情報（AnyConnect の可用性などの）
- オプションで、ポートフォワーディングが設定されている場合のその他のデータ（DHCP の詳細情報など）

スイッチから：

- デバイス接続メッセージ（DHCP メッセージや NetBIOS メッセージなど）
- ディープ パッケージ インスペクション
- スイッチテレメトリ

Cisco AI エンドポイント分析では、これらのソースから受信した情報に基づいてシステムルールが作成されます。デバイスがネットワークに参加し、デバイスがアクティブであるときに定期的にプローブを実行すると、エンドポイントのプロファイリングデータが継続的にモニタされ、更新されます。

エンドポイントから受信したプロファイリングデータにおける特定の変化は、Cisco AI エンドポイント分析で異常としてフラグが付けられます。たとえば、エンドポイントが最初に Linux デバイスとしてプロファイルされ、その後で macOS デバイスとしてプロファイルされた場合、これは重大度の高い異常としてフラグが付けられます。エンドポイントの [Changed Profile Label] 列にスコアが割り当てられ、エンドポイントの全体的な信頼スコアもこの変化を反映して更新されます。

ただし、macOS のサブバージョンに変化があり、エンドポイントが新しいリリースから古いリリースにダウングレードされたように見える場合、そのような変化は優先順位の低い異常としてフラグが付けられ、対応するスコアがそれに応じて更新されます。

[Endpoint Inventory] ウィンドウで、[Changed Profile Label] スコアを持つエンドポイントの MAC アドレスをクリックすると、記録されたプロファイリングデータの変化を確認できます。ここにはエンドポイントの新旧のプロファイルが表示されます。プロファイリングの変化が何らかの理由で問題ないと判断できる場合、または検出されたプロファイリングの変化に誤りがあると思われる場合は、エンドポイントの詳細情報の [Changed Profile Label] エリアで対応するボタンをクリックして、スコアをリセットします。

エンドポイントの詳細情報の [Changed Profile Label] エリアにあるトグルボタンをクリックすることにより、特定のエンドポイントに関して「変化したプロファイルラベル」の検出を無効にすることもできます。

影響を受けるエンドポイントが Cisco ISE に接続されている場合は、この異常に関するデータが Cisco ISE に送信されます。このデータは、Cisco ISE 管理者がポリシーを定義するために簡単に使用できるエンドポイント分析ディクショナリ属性として使用できます。

変化したプロファイルラベルの検出は、カスタムルールが適用されているエンドポイントには使用できません。

NAT モード検出

ネットワークアドレス変換（NAT）は、登録されていないIPアドレスを使用してインターネットへ接続するプライベート IP インターネットワークを可能にします。NAT は、ネットワーク全体で1つだけのアドレスを外部にアドバタイズするように設定できます。ネットワーク内に NAT 対応ルータがある場合、NAT ルータに接続されたエンドポイントは、特定のエンドポイントの IP アドレスまたは MAC アドレスではなくルータの IP アドレスまたは MAC アドレスによって認識されます。NAT 対応ルータに関する情報は、接続先の Cisco Catalyst 9000 シリーズ デバイスから収集されます。

NAC 対応ルータとして機能するデバイスは、不正なエンドポイントをネットワークに接続させる可能性があるため、NAT 検出が信頼スコアの計算に含まれます。NAT モード検出スコアが割り当てられているエンドポイントの場合は、[Endpoint Inventory] タブで MAC アドレスをクリックすると、スライドインウィンドウにエンドポイントの詳細情報が表示されます。エンドポイントのアイデンティティがネットワーク内の NAT 対応ルータに対応していることが確実な場合は、次の手順を実行します。

1. 詳細情報のスライドインウィンドウの [Trust Score] タブで、[NAT Mode Detection] をクリックします。
2. トグルボタンをクリックして、この特定エンドポイントの NAT 検出を無効にします。

Cisco Catalyst 9000 シリーズ デバイスに接続された同時 MAC アドレスを持つエンドポイント

同じ MAC アドレスを共有し、Cisco Catalyst 9000 シリーズ デバイスに接続されているエンドポイントを特定してください。同時 MAC アドレスを持つエンドポイントの問題は、有線環境と、有線展開およびワイヤレス展開を含むハイブリッド環境で発生します。ワイヤレス環境では、常時、特定の MAC アドレスを持つエンドポイントは 1 つしかネットワークにアクセスできないため、同時 MAC アドレスは発生しません。

Cisco AI エンドポイント分析では、同時 MAC アドレススコアをエンドポイントに割り当てることにより、同時 MAC アドレスを持つエンドポイントを特定することができます。ネットワーク内で共有 MAC アドレスを持つエンドポイントを検出するには、接続されている Cisco Catalyst 9000 シリーズ デバイスで CBAR を有効にする必要があります。

同じ MAC アドレスを持つデバイスが Cisco Catalyst 9000 シリーズ デバイスに接続すると、それらのエンドポイントは同時エンドポイントとして認識され、その MAC アドレスに低いスコ

アが割り当てられます。同時 MAC アドレスを持つエンドポイントは、次のデバイスに接続できます。

- 異なる VLAN から同じ Cisco Catalyst 9000 シリーズ デバイス
- 異なる Cisco Catalyst 9000 シリーズ デバイス

表 *56 :* 同時 *MAC* アドレスの問題が発生する環境

展開 1	展開 2	ネットワークで同時 MAC アドレスが発生するか	この環境での同時 MAC アドレス検出のサポート
有線	有線	対応	対応
有線	ワイヤレス	対応	対応
ワイヤレス	有線	対応	対応
ワイヤレス	ワイヤレス	非対応	非対応

Cisco DNA Center リリース 2.2.3 以降では、[Endpoint Inventory] タブの [Trust Scores] ビューに [Concurrent MAC Address] 列があります。共有 MAC アドレスは異常として検出され、[Concurrent MAC Address] 列に低いスコアが割り当てられます。[MAC Address] をクリックすると、スライドインウィンドウが表示され、その MAC アドレスの詳細情報が示されます。[Concurrent MAC Address] をクリックすると、フィールドが展開され、MAC アドレスのさまざまな送信元に関する情報が表示されます。

[Concurrent MAC Address] エリアの [Network Device Name] 列には、エンドポイントが接続されている Cisco Catalyst 9000 シリーズ デバイスの名前が表示されます。[Interface] 列と [VLAN] 列には対応する値が表示され、エンドポイントがネットワークにどのように接続されているのかを特定するために役立ちます。

Cisco ISE からのポスチャおよび認証値を使用した初期信頼スコアアセスメント

エンドポイントが Cisco ISE を介して認証されると、認証およびポスチャの詳細情報に基づいて、エンドポイントに信頼スコアがただちに割り当てられます。認証方式スコアはデフォルトで割り当てられ、このスコアを無効にすることも、このスコアに対処することもできません。[Configurations] ウィンドウからグローバルレベルで、または [Endpoint Inventory] タブで特定のエンドポイントについて、ポスチャベースのスコアを有効または無効にすることができます。認証方式およびポスチャ値に基づいて割り当てられた信頼スコアが、エンドポイントの初期信頼スコアになります。

その後、このエンドポイントで検出されたその他の異常な動作は、この初期信頼スコアに影響を与え、異常の重大度と数に基づいて信頼スコアを低下させます。

[Endpoint Inventory] タブのエンドポイントの詳細情報に表示される**認証方式**スコアは、使用される認証方式の認識されたセキュリティレベルに基づいています。たとえば、「HTTPS を介した Web 認証」、「証明書ベースの認証」、「セキュアトンネルを使用した認証」などは、高い信頼スコアを得ます。

ポスチャスコアは、接続エンドポイントがポスチャに準拠しているかどうかに基づきます。

エンドポイントの信頼スコアが認証方式スコアのみで構成されている場合、[Reset Trust Score] ボタンは非アクティブになります。認証方式以外の信頼スコアソースにスコアが表示されている場合は、リセットオプションを使用できます。

ランダムおよび変更 MAC アドレスを持つエンドポイントの信頼スコア

プライバシー対策として、モバイルデバイスでは接続先の SSID ごとにランダムおよび変更 MAC アドレスを使用することが増えています。一部のデスクトップ オペレーティング システムは、ユーザーが定期的に MAC アドレスをランダム化する機能も提供しています。つまり、エンドポイントは、異なる SSID に接続するたびに異なる MAC アドレスを提示します。

Cisco AI エンドポイント分析を使用すると、Cisco ISE から「DUID」と呼ばれる（Cisco ISE では「GUID」とも呼ばれます）一意のエンドポイント識別子を受信することにより、ランダムおよび変更 MAC アドレスの問題を処理できます。Cisco AI エンドポイント分析は、MAC アドレスの代わりに、エンドポイントの識別子として DUID を使用します。Cisco ISE での GUID の割り当て方法の詳細については、Cisco ISE の管理者ガイド（リリース 3.1）を参照してください。

Cisco AI エンドポイント分析の [Overview] ウィンドウの [Endpoint MAC Randomization] ダッシュレットには、ネットワーク内のランダムおよび変更 MAC アドレスを使用しているエンドポイントの数がグラフィカルに表示されます。

Cisco ISE に接続され、DUID 情報を使用可能なエンドポイントの場合、この情報は Cisco AI エンドポイント分析にも表示されます。次の列には、Cisco AI エンドポイント分析の [Endpoint Inventory] ウィンドウで必要になる情報が表示されます。

- [DUID]：エンドポイントの DUID 値。
- [Previous MAC Addresses]：エンドポイントが以前にネットワークへの接続に使用していたランダムおよび変更 MAC アドレス。

DUID 値を使用することで、Cisco AI エンドポイント分析では、エンドポイントを確実に識別し、エンドポイントが以前に使用していたさまざまな MAC アドレスを追跡することが可能になっています。これは、ランダムおよび変更 MAC アドレスを持つエンドポイントの信頼スコアも高精度であることを意味します。以前の MAC アドレスでのエンドポイントの信頼スコアは、エンドポイントが提示している現在の MAC アドレスに引き継がれ、同じエンドポイントに関して受信されたプローブデータの影響を受け続けます。

デバイスで [Private Address] 設定が有効になっている場合、このデバイスの [Is MAC Random] 列に [Yes] という値が表示されます。つまり、このデバイスは、ランダムおよび変更 MAC アドレスとして認識されます。ただし、このデバイスに関して DUID 値を使用できるかどうか

は、エンドポイントが Cisco ISE を介して認証されているかどうかと、Cisco ISE でこのエンドポイントの GUID が生成されているかどうかに依存します。

オープンポートと資格情報の脆弱性を確認するためのセンサースキャン

アクティブなプローブコンテナをインストールして、ネットワーク内のエンドポイントに関する詳細情報を取得します。セキュリティ センサー スキャンを有効にすると、エンドポイントに割り当てられるトラストスコアは、開いているポートとエンドポイントのログイン情報の異常を考慮します。

センサースキャン機能は、次のスイッチでサポートされています。

- Cisco Catalyst 9300 シリーズ スイッチ
- Cisco Catalyst 9400 シリーズ スイッチ

（注） Cisco Catalyst 9800 シリーズ ワイヤレスコントローラは、センサースキャン機能をサポートしていません。

Cisco AI エンドポイント分析は、スイッチで利用可能なアプリケーション ホスティング機能を使用して、開いているポートと弱いログイン情報のスキャンを有効にします。

センサースキャンの有効化と監視

始める前に

- スキャン結果に基づいてエンドポイントポリシーを適用する場合は、Cisco ISE リリース 3.1 以降のリリースに接続します。
- Cisco Catalyst 9200、9300、または 9400 シリーズ デバイスに接続します。
- スイッチが Cisco IOS XE リリース 17.7.1 以降のリリースにアップグレードされていることを確認します。

ステップ 1 Cisco DNA Center にログインします。

ステップ 2 メインメニューから **[ポリシー（Policy）]** > **[AI エンドポイント分析（AI Endpoint Analytics）]** を選択します。

ステップ 3 表示される [Overview] ウィンドウで、[Configurations] をクリックします。

ステップ 4 左ペインから、[Trust Score Sources] を選択します。

ステップ 5 [Security Sensor] 領域には、センサース キャン機能を使用して、開いているポートと脆弱なエンドポイントのクレデンシャルを識別するための前提条件が表示されます。この領域で対応するリンクをクリックして、次のタスクを実行します。

1. Cisco Catalyst 9000 シリーズ デバイスのリリースノートで、サポートされている Cisco DNA Center および Cisco IOS-XE リリースを確認します。関連する Cisco Catalyst 9000 シリーズ デバイスのセキュリティ センサー コンテナを software.cisco.com からダウンロードします。.tar ファイルがシステムにダウンロードされます。
2. Cisco DNA Center にアプリケーション ホスティングをインストールします。手順については、アプリケーション ホスティング （572 ページ）を参照してください。
3. Cisco DNA Center アプリケーション ホスティング ウィンドウに .tar ファイルをアップロードします。[Security Sensor] 領域にアプリケーション ホスティング ウィンドウへのリンクが表示されます。
4. センサースキャンを有効にする Cisco Catalyst 9000 シリーズ デバイスごとに、.tar ファイルをインストールして有効にします。

   Cisco DNA Center アプリケーションのホスティング ウィンドウで、.tar ファイルを有効にした少なくとも 1 つの Cisco Catalyst 9000 シリーズ デバイスの [App Hosting Status] がアクティブであることを確認します。

ステップ 6 前の手順で説明したようにアクティブプローブコンテナをインストールして有効にした後、[Security Sensor] 領域で、Cisco AI エンドポイント分析の信頼スコア設定を構成して、Cisco ISE に接続されているエンドポイントと、アクティブなプローブアプリケーションが有効になっている Cisco Catalyst デバイスで、開いているポートと、脆弱なクレデンシャルをスキャンできます。

- [Open Port Scan] トグルボタンをクリックして、Cisco AI エンドポイント分析がポートスキャンをプロアクティブに実行して、ネットワーク上の定義済みエンドポイントで考えられる脆弱性を検出して解決できるようにします。
- [Credential Vulnerability Scan] トグルボタンをクリックして、ネットワーク上のエンドポイントが脆弱なクレデンシャルを使用している場合に、Cisco AI エンドポイント分析がプロアクティブに検出できるようにして、悪意のあるアクティビティを防止します。

ステップ 7 （任意） 開いているポートのスキャンを有効にすることを選択した場合は、[Open Port Scan] 領域の [Scan Configuration] をクリックしてスキャンを定義できます。

a) [Scan Configuration] ウィンドウの [Defined Scans] タブで、[Define Scan] ボタンをクリックします。
b) ポートのスキャンの範囲を定義できるダイアログボックスが表示されます。

   - エンドポイントの登録時に各エンドポイントをスキャンするには、[On enrollment, scan all endpoints] オプションボタンを選択します。
   - サブネット、プロファイル属性などにより、開いているポートのスキャンの範囲を定義するには、[Create a Custom Scan] オプションボタンを選択します。

   どちらのタイプのポートのスキャンでも、許可されていないポートのリストを定義して、常に閉じておく必要があるポートを指定します。このリストにより、Cisco AI エンドポイント分析はエンドポイントの異常なポートアクティビティを認識し、低い信頼スコアを割り当てることができます。どちらのタイプのポートのスキャンでも、設定できるスキャンの最小頻度は 12 時間です。

c) [Scan Configuration] ウィンドウの [Open Ports List] タブで、スキャンする必要があるポートのタイプと範囲、または個々のポートを指定します。

d) [Scan Configuration] ウィンドウの [Unauthorized Ports] タブで、ネットワーク内の許可されていないポートをポート番号とポートタイプで定義します。Cisco AI エンドポイント分析がこれらのポートをアクティブとして検出した場合、エンドポイントには、許可されていないポートがアクティブである異常に対して低い信頼スコアが与えられます。

ステップ 8 （任意） 脆弱なクレデンシャルの検出を有効にすることを選択した場合は、[Credential Vulnerability Scan] 領域の [Scan Configuration] をクリックしてスキャンを定義できます。この機能では、SSH および TELNET プロトコルがサポートされています。

a) [Credential Vulnerability Scan] ウィンドウの [Scan] タブで、脆弱なクレデンシャルとして識別するクレデンシャルのリストを定義します。企業の要件に従って、脆弱であると見なされるユーザー名とパスワードのリストを定義します。

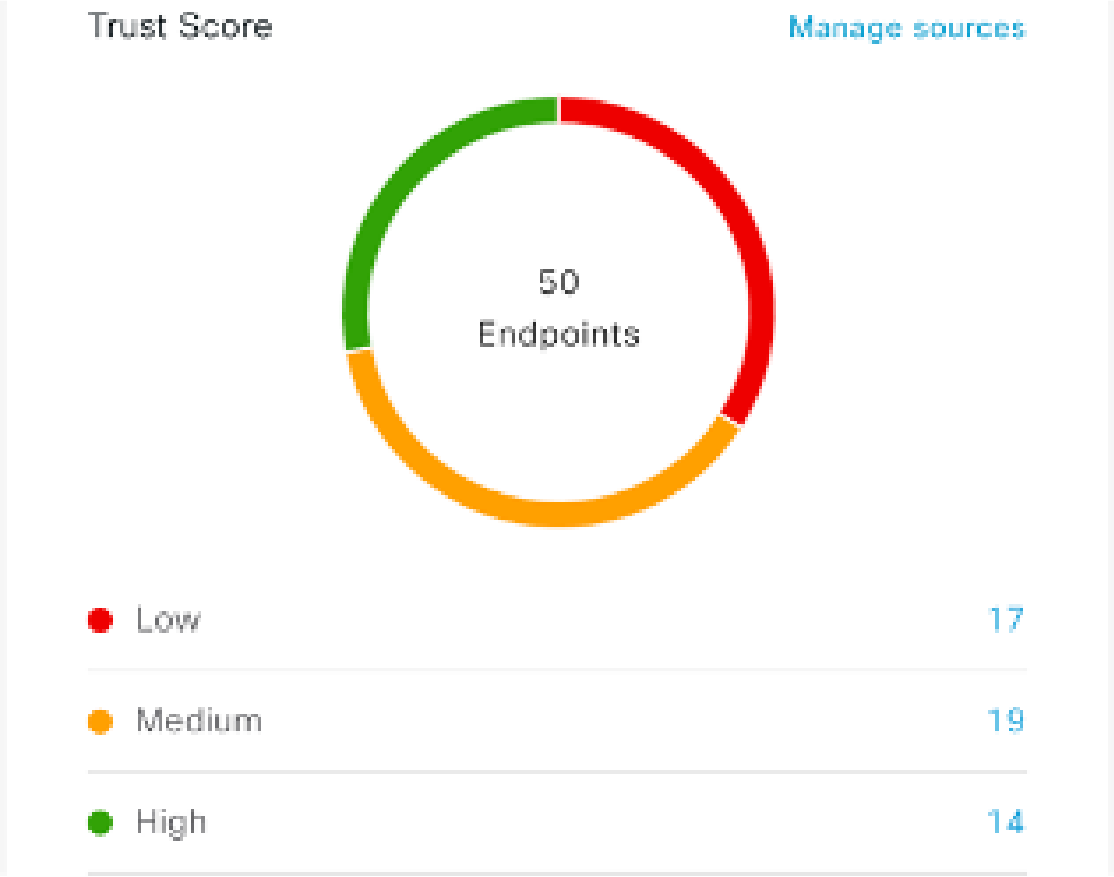
b) [Credentials] タブでは、デフォルトで、3500 を超える脆弱なクレデンシャルのデフォルトリストが利用可能です。このデフォルトリストを使用して、クレデンシャルの脆弱性スキャンを作成できます。脆弱なクレデンシャルの新しいリストを追加するには、[Create New List] をクリックします。

クレデンシャル脆弱性スキャンの設定可能な最小頻度は 12 時間です。

ステップ 9 [Security Sensor] で有効にしたスキャンでは、関連するエンドポイントがスキャンされ、開いているポートまたはクレデンシャルの確認で異常が検出された場合、これらのエンドポイントの信頼スコアがそれに応じて調整されます。[Endpoint Inventory] タブ（該当する場合）では、エンドポイントの [Trust Score] タブに、エンドポイントで開いている許可されていないポート、脆弱なユーザー名、またはその両方のリストが表示されます。

エンドポイントの信頼スコアの表示と管理

図 *31 : [Cisco AI Endpoint Analytics Overview]* タブの *[Trust Score]* ダッシュレット



Cisco DNA Center をアップグレードし、必要な信頼スコアのソースを有効にすると、Cisco AI エンドポイント分析の [Overview] タブ（メインメニュー > **[Policy]** > **[AI Endpoint Analytics]**）に [Trust Scores] ダッシュレットが表示されます。このダッシュレットには、次の情報が含まれます。

- 信頼スコアが割り当てられているエンドポイントの総数。
- 信頼スコアが低、中、および高のエンドポイントの数に関するドーナツグラフおよびリスト。

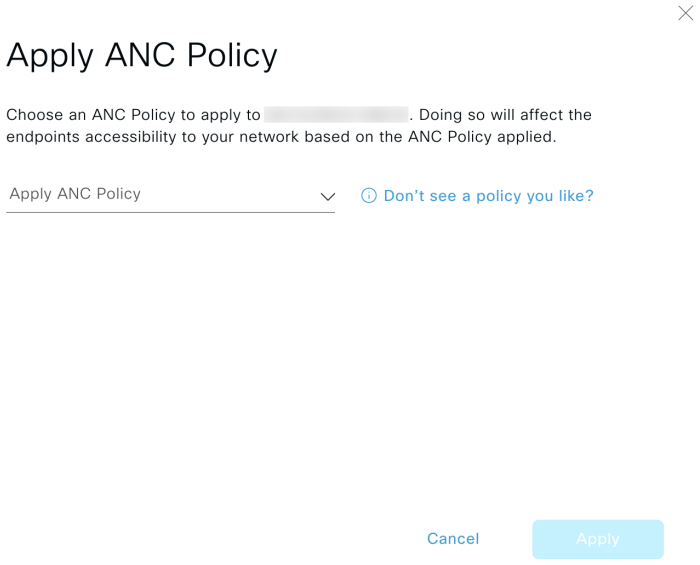
信頼スコアカテゴリのエンドポイントの詳細を表示するには、[Trust Scores] ダッシュレットでエンドポイント数をクリックします。[Endpoint Inventory] タブの [Trust Score] ビューが、適切なフィルタが適用されて表示されます。

[Endpoint Inventory] タブでは、次の 2 つの方法で信頼スコアを持つエンドポイントを表示できます。

- [Focus:] ドロップダウンリストをクリックし、[Trust Score] を選択すると、信頼スコアが割り当てられているすべてのエンドポイントが表示されます。
- 表示される警告メッセージの [View endpoints in Trust Score View] をクリックすると、低スコアと中スコアのエンドポイントが表示されます。

信頼スコアのあるエンドポイントでは、次のアクションを実行できます。

- **ANC ポリシーの適用**

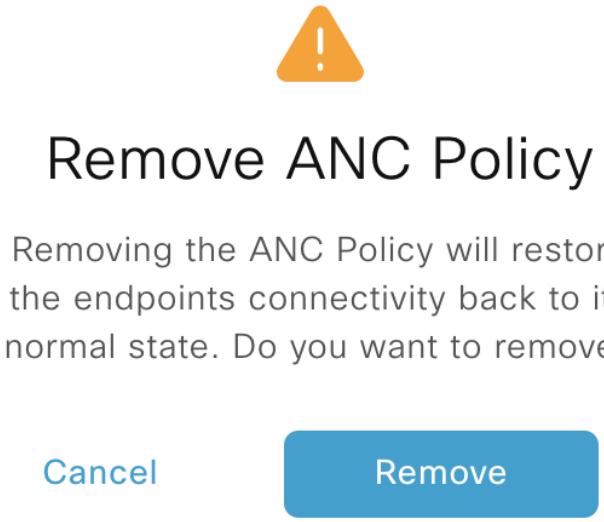


[Apply ANC Policy] ボタンをクリックして、エンドポイントに適用する ANC ポリシーを選択します。ネットワークへのエンドポイントのアクセスは、ポリシーに応じて変更されます。ANC ポリシーは Cisco ISE からインポートされ、表示されるポップアップウィンドウのドロップダウンリストに表示されます。

- **ANC ポリシーの置換**

[Change ANC Policy] ボタンをクリックして、エンドポイントの既存の ANC ポリシーを別の ANC ポリシーに置き換えます。表示されるポップアップウィンドウで、[Change ANC Policy] ドロップダウンリストから適用する新しいポリシーを選択します。

- **ANC ポリシーの削除**



適用された ANC ポリシーをエンドポイントから削除するには、[Remove ANC Policy] ボタンをクリックします。表示されるポップアップウィンドウで、[Remove] をクリックします。これにより、エンドポイントに適用された修復ポリシーが削除され、エンドポイントがネットワークに正常に接続できるようになります。

- **信頼スコアのリセット**

図 *32 : ANC* ポリシーを使用しないエンドポイントの信頼スコアのリセット

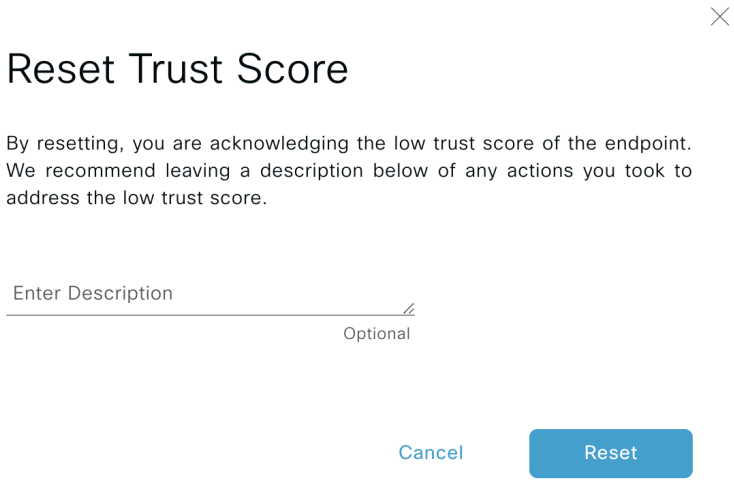
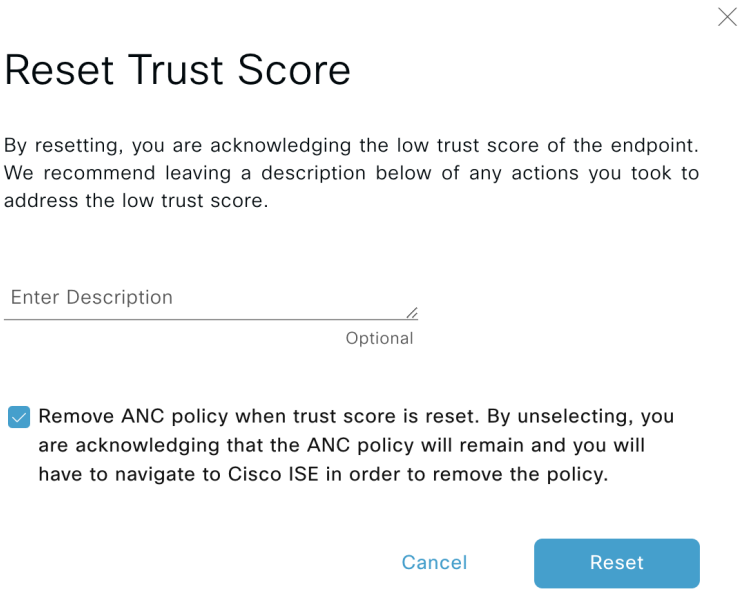


図 *33* : *ANC* ポリシーを使用したエンドポイントの信頼スコアのリセット



信頼スコアインベントリからエンドポイントを削除するには、[Reset Trust Score] ボタンをクリックします。表示されるポップアップウィンドウで、[Reset] をクリックします。

ANC ポリシーの適用後にエンドポイントに対してこのオプションを選択した場合、このエンドポイントは信頼スコアインベントリに再度表示されません。この場合、このようなエンドポイントの ANC ポリシーを変更するには、Cisco ISE からポリシーを削除する必要があります。

ANC ポリシーを適用せずにエンドポイントのスコアをリセットした場合、信頼スコアデータの次回の自動更新時に、エンドポイントが信頼スコアインベントリに再度表示されることがあります。

各アクションのボタンは、[Endpoint Inventory] タブの 2 つの場所に表示されます。アクションは、単一のエンドポイントまたは複数のエンドポイントで実行できます。

- **単一エンドポイントの信頼スコアの管理**

図 *34* : *ANC* ポリシーを使用しないエンドポイントの信頼スコアオプション

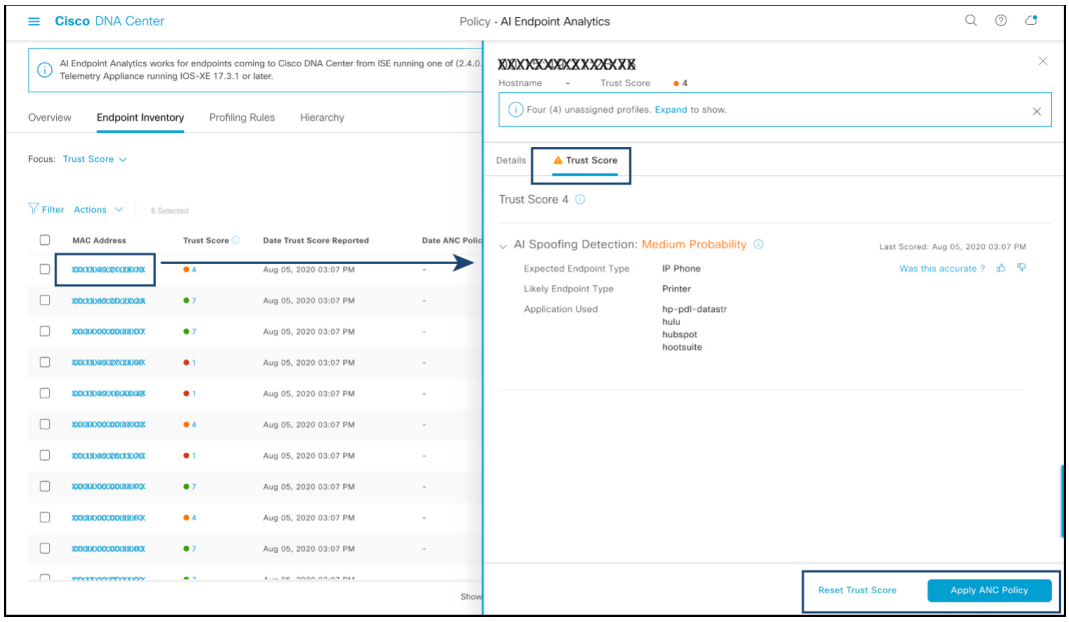
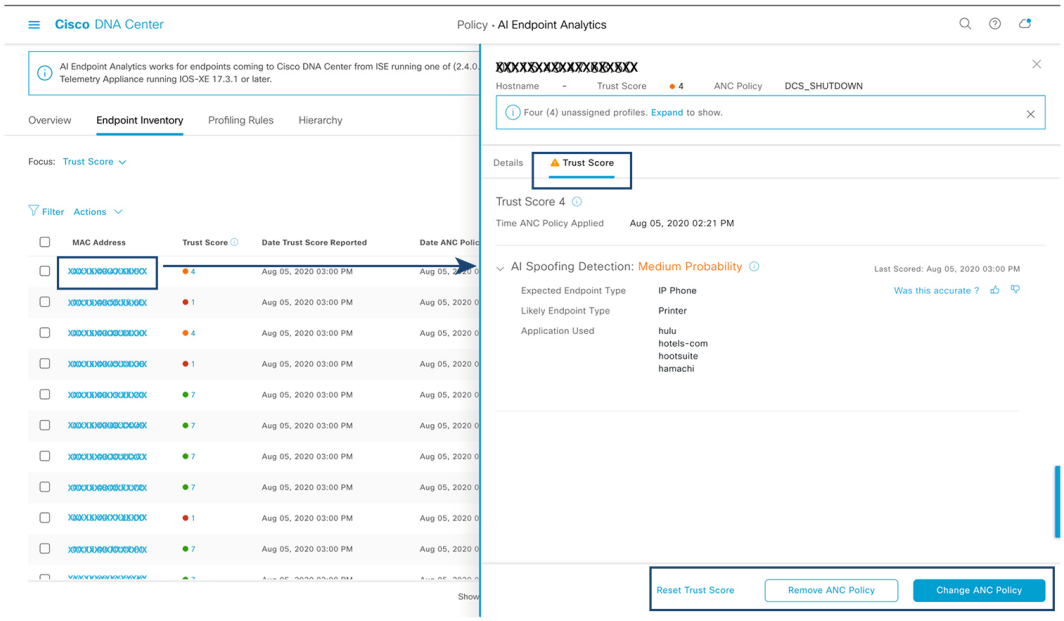


図 *35* : *ANC* ポリシーを使用したエンドポイントの信頼スコアオプション



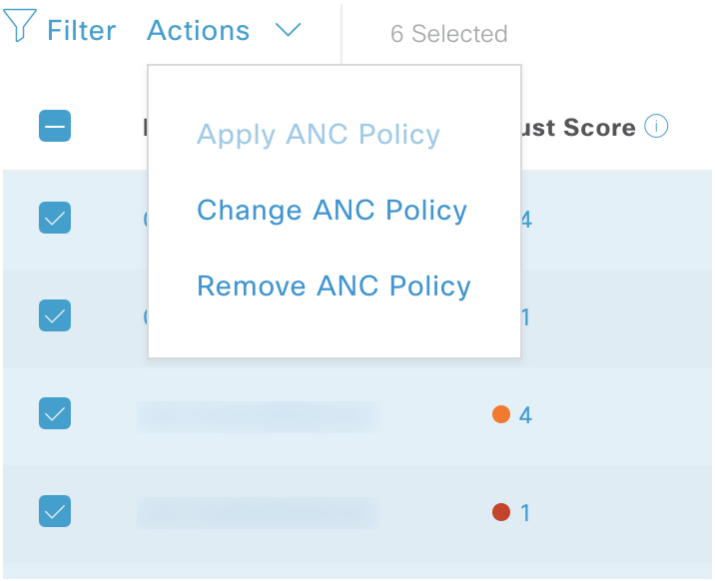
信頼スコアのあるエンドポイントのリストから、管理するエンドポイントの MAC アドレスをクリックします。表示されるエンドポイントの詳細ペインで、[Trust Score] タブをクリックします。

ここには、[Expected Endpoint Type] と [Likely Endpoint Type] の値が表示されます。[Applications Used] フィールドには、エンドポイントで使用されているアプリケーションのうち、予想されるエンドポイントタイプではないアプリケーションがリストされます。

このペインには、ANC ポリシーの受け入れと削除のワークフローを開始し、信頼スコアをリセットするためのボタンがあります。目的のタスクのボタンをクリックします。

または、[Endpoint Inventory] ウィンドウで個々のエンドポイントのチェックボックスをオンにし、[Actions] をクリックして、ドロップダウンリストから必要なオプションを選択します。

- **複数のエンドポイントの信頼スコアの管理**



[Endpoint Inventory] タブで、特定のアクションを実行する必要があるすべてのエンドポイントのチェックボックスをオンにします。[Actions] をクリックし、ドロップダウンリストから必要なアクションを選択します。

エンドポイント スプーフィングの制御

同時 MAC アドレス検出とは、同じ MAC アドレスを持つ 2 つのエンドポイントがネットワークにアクセスしてトラフィックを生成していることが検出されることを意味します。次に、実際のエンドポイントとスプーフィングされたエンドポイントを区別し、スプーフィングされたエンドポイントに対して必要な修復アクションを実行することが不可欠になります。

コントロール エンドポイント スプーフィング機能は、エンドポイントの MAC アドレス以外のネットワーク情報を提供することにより、詳細なポリシーコントロールを提供します。ネットワーク情報には、サイト情報、ネットワークデバイスの IP アドレス、ネットワークデバイスポート、最初に承認されたタイムスタンプ、最後に承認されたタイムスタンプ、およびエンドポイントがネットワークで使用可能であった期間が含まれます。従来のように MAC アドレスでエントリを区別するか、MAC アドレスと提供されたネットワーク情報の両方を使用してエントリを区別するかを選択できます。MAC アドレスと接続（ネットワーク情報）で区別することを選択した場合、スプーフィングされたエンドポイントを検出するための選択が自動的

に行われます。自動選択を使用するか、スプーフィングされたエンドポイントであると思われるものを選択して、そのエンドポイントに適切な修復アクションを適用することができます。使用可能な修復アクションは、Cisco ISE で設定された ANC（適応型ネットワーク制御）ポリシーです。

これはポリシーを適用する詳細な方法であるため、**[Operations]** > **[Adaptive Network Control]** > **[Endpoint Assignment]**にこのポリシーのリストは表示されません。

同時MACアドレス検出がなく、NATモード検出のみのエンドポイントの場合、ANCポリシーはエンドポイントの信頼スコアの表示と管理で適用されます。このようなシナリオでは、エンドポイントは Cisco ISE の [Endpoint Assignment] の下にリストされます。

同時MACアドレスとNATモードの両方の検出があるエンドポイントの場合、詳細なポリシー制御が優先されます。したがって、[Apply ANC Policy] をクリックすると、エントリを区別する 2 つのオプションがある新しい [Apply ANC Policy] ウィンドウが表示されます。

また、いつでもエンドポイントの ANC ポリシーを変更することを選択できます。ANC ポリシーの変更中に、ANC ポリシーを適用できる複数のエントリを選択するオプションがあります。

（注） 修復アクションとして [Shutdown] を選択し、アクションを変更する場合、エンドポイントはアクションの変更後に自動的に再起動されません。エンドポイントが接続されているスイッチのインターフェイスを手動でオンにする必要があります。

ANC ポリシーはいつでも削除できます。

始める前に

ダイナミック認証を、ネットワークデバイスで設定する必要があります。Cisco DNA Center から AAA 設定を使用してネットワークデバイスをプロビジョニングすることをお勧めします。

ステップ 1 Cisco DNA Center GUI から、**[Policy]** > **[AI Endpoint Analytics]** > **[Endpoint Inventory]** > **[View endpoints in trust score view]**を選択します。

ステップ 2 確認するエンドポイントをクリックして、ANC ポリシーを適用します。

ステップ 3 [Trust Score] > [Concurrent MAC Address] を選択します。

ステップ 4 [Apply ANC Policy] をクリックします。

ステップ 5 [Apply ANC Policy] ウィンドウで、[Based on MAC address] または [Based on MAC address and connectivity] を選択します。

ステップ 6 [Apply ANC Policy] ドロップダウンリストから適切な修復アクションを選択します。

ステップ 7 [Apply ANC Policy] をクリックします。

このタスクを完了した後、そのエンドポイントの [Trust Score] ビューに戻ると、ANC ポリシー名と、ポリシーが適用されたネットワークデバイスの IP アドレスと、ANC ポリシーが適用された時刻を確認できます。

設定を確認するには、Cisco ISE GUI で、[Operation] > [RADIUS] > [Live logs] を選択します。[Identity] 列をエンドポイントの MAC アドレスでフィルタリングできます。

このエンドポイントの、Cisco ISE から開始された CoA アクションのエントリが一覧表示されます。詳細を確認すると、エンドポイントに適用した ANC ポリシーが [CoA Reason] に表示されます。

プロファイリングルール

Cisco AI エンドポイント分析のプロファイリングルールを使用すると、共通の属性を組み合わせてエンドポイントをグループ化できます。これらの属性により、エンドポイントタイプ、OS タイプ、ハードウェアモデル、およびハードウェア製造元でエンドポイントを識別できます。プロファイリングルールを使用すると、多くのエンドポイントを簡単に管理できます。

Cisco AI エンドポイント分析は、DPI、メディアプロトコル、医療業界のプロトコルなどを介してネットワークデバイスからプロファイリングデータを受信します。Cisco ISE からのプロファイリングデータは、pxGrid を介して通信されます。これらのプロファイリング属性をデバイスディクショナリで使用してプロファイルルールを作成できます。

プロファイリングルールは、Cisco AI エンドポイント分析の [Profiling Rules] タブで確認できます。このタブの下に表示されるテーブルで、[Rule Name] エントリをクリックすると、割り当てられたプロファイルと使用される属性が表示されます。

Cisco AI エンドポイント分析でエンドポイントをプロファイリングするために使用されるプロファイリングルールは次のとおりです。

- システムルール
- シスコの規則
- Cisco AI ルール

ルールの優先順位付け

Cisco AI エンドポイント分析のプロファイリングルールには優先順位があります。プロファイリングルールの実行は、このルールの優先順位に従って、精度の高いエンドポイントをプロファイリングします。

Cisco AI エンドポイント分析ではユーザー入力がプライマリであるため、プロファイリングルールの優先順位は次のようになります。

- 管理者が作成した静的プロファイル（たとえば、[Register Endpoints] オプションを使用して追加したプロファイル）。
- 管理者が作成したカスタムルール。
- デフォルトで使用可能なシスコ提供のシステムルール。
- 機械学習対応のスマートグループ化ワークフローによって自動生成されたルール。

ルールに設定された優先順位を表示するには、[Profiling Rules] ウィンドウで [Rule priorityitization] をクリックします。

登録済みのエンドポイントは、さまざまなプロファイリングラベルの複数の Cisco AI エンドポイント分析ルールによってプロファイリングできます。次の表に、2 つのエンドポイントに対するプロファイリングルールの設計を示します。

エンドポイント 1	エンドポイント 2
システムルールによってプロファイリングされたハードウェアモデル Cisco AI ルールによってプロファイリングされた OS タイプ カスタムルールによってプロファイリングされたハードウェア製造元	システムルールによってプロファイリングされたハードウェアモデル カスタムルールによってプロファイリングされたハードウェアモデル Cisco AI ルールによってプロファイリングされたハードウェアモデル

エンドポイント 2 のルール優先順位では、カスタムルールが他のルールよりも優先されます。エンドポイント 2 のハードウェアモデルラベルは、カスタムルールによってプロファイリングされます。

エンドポイント 1 の場合、ルールごとに異なるプロファイルラベルが定義され、それに応じて各ラベルがプロファイリングされます。

プロファイリングルールのフィルタ処理

ステップ 1 [Profiling Rules] ウィンドウで、[Filter] をクリックします。

ステップ 2 [Rule Name] フィールドに、名前を入力します。

ステップ 3 対応するドロップダウンリストからエンドポイント属性の値を選択して、一連のエンドポイントをフィルタ処理します。

ステップ 4 [Apply] をクリックします。

更新されたプロファイリングルールの表示

ステップ 1 [Endpoint Inventory] ウィンドウに移動します。

ステップ 2 エンドポイントの MAC アドレスの横にあるチェックボックスをクリックして、エンドポイントのプロファイリングの詳細を表示します。

ステップ 3 プロファイルラベルの横にある情報アイコンをクリックし、ルール名をクリックして、割り当てられたプロファイルと属性の詳細を表示します。

システムルール

Cisco AI エンドポイント分析には、エンドポイントをプロファイリングするためのシステムルールと呼ばれる事前定義済みのルールが用意されています。Cisco AI エンドポイント分析を導入すると、特定のルールを設定することなく、エンドポイントのゼロデイ可視性を実現できます。

新しくオンボーディングされたエンドポイントは、デフォルトでシステムルールを使用してプロファイリングされます。

ネットワークデバイスは、Cisco DNA Center の **[Provision]** > **[Network Devices]** > **[Inventory]** ウィンドウで管理されます。

これらのネットワークデバイスは、システムルールによってプロファイリングされ、Cisco AI エンドポイント分析の [Endpoint Inventory] ウィンドウには表示されません。ただし、カスタムルールでプロファイリングされたエンドポイントは、カスタムルールがネットワークデバイスを [Device Type] として作成されるため表示できます。

エンドポイント プロファイリング用の自動システムルール更新

Cisco AI エンドポイント分析でエンドポイントプロファイリングに使用されるシステムルールは、プロファイリングの精度を高めるために定期的に更新されます。シスコからのエンドポイント プロファイリング システム ルールの更新を受信するように自動更新をスケジュールします。Cisco DNA Center が設定された時間に更新を受信し、変更内容が Cisco AI エンドポイント分析に適用されます。[Profiling Rules] ウィンドウ（**[Policy]** > **[AI Endpoint Analytics]** > **[Profiling Rules]**）で、エンドポイントプロファイルの変更の詳細を確認し、システムルールの更新を承認または拒否します。

承認されたシステムルールの更新によってエンドポイントのハードウェアモデルの値が変更された場合、[Endpoint Inventory] タブでエンドポイントの詳細を表示すると、[Hardware Model] フィールドにシステムルールの更新の名前があります。

始める前に

NBAR クラウドを設定し、有効にします。「NBAR クラウドコネクタの設定 （568 ページ）」を参照してください。

NBAR クラウドのステータスを確認するには、**[Policy]** > **[AI Endpoint Analytics]** > **[Overview]** の順に選択し、[Configuration] をクリックします。

ステップ 1 メインメニューから、**[System]** > **[Settings]** > **[Cisco Accounts]** > **[Profile Rule Settings]** の順に選択します。

[Schedule Automatic Updates] エリアの [Enabled] トグルボタンは、デフォルトでアクティブに設定されています。

ステップ 2 更新をスケジュールする曜日のボタンをクリックします。複数の日を選択できます。次に、[Time Slot] テキストフィールドを使用して、更新の時間を選択します。Cisco DNA Center によって更新が受信されるまでに 30 分かかります。2 番目のタイムスロット領域は編集できず、スケジュールされた更新が完了すると予想される時間が表示されます。

ステップ 3 Cisco DNA Center がシステムルールの更新を受信すると、[Profiling Rules] ウィンドウ（**[Policy]** > **[AI Endpoint Analytics]** > **[Profiling Rules]**）に通知が表示されます。ダイアログボックスで [Expand] をクリックすると、次の通知が表示されます。

最新バージョン（最新バージョンの名前）に更新され、最近のシスコプロファイリングルールによって一部のエンドポイントのプロファイルが変更されています。更新を確認します。

[Review Update] をクリックします。

ステップ 4 [Endpoint Profile Update Review] ダイアログボックスが表示されます。このダイアログボックスには、現在適用されている安定版の更新、受信した最新の更新などの情報が表示されます。また、クリックして、関連するエンドポイントプロファイルの更新を表示できる次のセクションも含まれています。

1. [Major Updates]：Linux エンドポイントとして現在記録されている Windows エンドポイントなど、プロファイルに大きな変更があったエンドポイントが一覧表示されます。
2. [Minor Updates]：Windows OS の更新バージョンなど、プロファイルにマイナーな変更があったエンドポイントが一覧表示されます。
3. [Newly Profiled]：以前にプロファイル解除され、現在プロファイル情報が割り当てられているエンドポイントが一覧表示されます。

ステップ 5 エンドポイントプロファイルの変更を確認した後、プロファイルの更新を受け入れるには、[Endpoint Profile Update Review] ダイアログボックスで [Mark As Approved Version] をクリックします。エンドポイントプロファイルの変更に同意しない場合は、[Rollback] をクリックします。

ロールバックを選択する場合、対応するオプションをクリックして、最後の実行バージョンにロールバックするか、最後に承認されたバージョンにロールバックするかを選択する必要があります。

また、[AI Endpoint Analytics] > [Overview] > [Configuration] ウィンドウから、承認およびロールバックアクションを実行することもできます。

ステップ 6 [x] をクリックして、ダイアログボックスを閉じます。

シスコの規則

システムルールのほかに、エンドポイント属性を組み合わせて、エンドポイントをプロファイリングするためのカスタムルールを作成することもできます。カスタムルールは、Cisco AI エンドポイント分析の他のエンドポイント プロファイリング ルールよりも優先されます。

プロファイリングルールの論理と条件

[Endpoint Inventory] ウィンドウでカスタムプロファイリングルールを作成できます。カスタムプロファイリングルールを作成するには、エンドポイントの属性と値に基づいて論理条件を作成する必要があります。これらの属性は、ネットワークプローブデータから収集され、[Attribute Glossary] ウィンドウで使用できる分類属性とは異なります。

値は、エンドポイントグループを一意に識別するユーザー入力です。次の演算子を使用して、属性と値から正規表現が作成されます。

演算子	説明
次の文字列を含む	属性は、選択した値を持ちます。
イコール	属性は、選択した値に厳密にマッピングされます。
一致する	属性は、選択した値の正規表現パターンと一致する必要があります。
Starts With	属性は、選択した値で始まる必要があります。

（注） Contains、Equals、および Starts With は、大文字と小文字を区別する演算子です。大文字と小文字を区別しない値の場合は、Matches 演算子を使用します。

論理（[AND] および [OR]）によってこれらの条件をさらに組み合わせて、ネストされたルールを作成できます。

論理条件の作成と編集

論理条件を作成するには、次の手順に従います。

ステップ 1 [Choose Attribute Conditions] ウィンドウで、更新する [Attribute] の横にあるチェックボックスをオンにします。

ステップ 2 [Operator] ドロップダウンリストからオプションを選択します。

ステップ 3 [Value] フィールドに値を入力します。

ステップ 4 [Next] をクリックします。

ステップ 5 表示される [Add Logic to Conditions] ウィンドウで、条件間の [AND] ロジックまたは [OR] ロジックをドラッグアンドドロップして、カスタムルールの条件の論理シーケンスを作成します。

（注） 条件の横にある垂直省略記号を使用して、[Add Logical Conditions] ウィンドウで属性条件を追加または編集することもできます。

ステップ 6 [Next] をクリックします。

カスタムルールの作成

ステップ 1 [Endpoint Inventory] ウィンドウで、プロファイリングするエンドポイントの MAC アドレスの横にあるチェックボックスをオンにします。

ステップ 2 [Actions] をクリックし、[Profile with Custom Rules] を選択します。

ステップ 3 表示される [Name Rule and Type] ウィンドウの [Rule Name] フィールドにルールの名前を入力し、[Profile Label] ドロップダウンリストからラベルを選択します。

[Profile Label] ドロップダウンリストから選択した内容に応じて、対応するフィールドが表示され、その名前は動的に更新されます。たとえば、[Endpoint Type] を選択すると、[Endpoint Type] フィールドが表示されます。

ステップ 4 表示される新しいフィールドに値を入力します。情報の入力を開始すると、一致するオプションが表示されます。要件に一致するオプションがあれば、そのオプションを選択します。なければ、タイプ名全体を入力します。

ステップ 5 [Next] をクリックします。

ステップ 6 表示される [Choose Attribute Conditions] ウィンドウで、論理条件を作成します。

詳細については、「プロファイリングルールの論理と条件」を参照してください。

ステップ 7 [Review Rule] ウィンドウで、このカスタムルールでプロファイリングされるエンドポイントのリストを確認します。

ステップ 8 [Next] をクリックします。

ステップ 9 [Profiles] をクリックします。

カスタムルールの編集

ステップ 1 [Profiling Rules] ウィンドウで、編集する管理ルールの横にあるチェックボックスをオンにします。

ステップ 2 [Actions] をクリックし、[Edit] を選択します。

ステップ 3 表示される [Edit] ウィンドウの [Rule Name] フィールドにルールの名前を入力し、ルールの作成時に選択した [Profile Label] に基づいてプロファイルの詳細を選択または入力します。

ステップ 4 [Logic and Conditions] セクションで、垂直省略記号をクリックし、[Edit] を選択して、プロファイリングルールの論理と条件を更新します。詳細については、「プロファイリングルールの論理と条件」を参照してください。

ステップ 5 **[次へ (Next)]** をクリックします。

ステップ 6 **[適用 (Apply)]** をクリックします。
既存のルールが新しいプロファイリングの詳細で更新されると、そのルールでプロファイリングされたエンドポイントが新しいプロファイリングの詳細で更新されます。

カスタムルールの削除

ステップ 1 [Profiling Rules] ウィンドウで、削除するルールの横にあるチェックボックスをオンにします。

ステップ 2 [Actions] をクリックし、[Delete] を選択します。

次のメッセージが表示されます。

「Do you really want to delete the selected Rule(s)?」

ステップ 3 [Yes] をクリックして、Cisco AI エンドポイント分析からルールを完全に削除します。

カスタムルールが削除されると、このルールでプロファイリングされたエンドポイントがシステムルールで更新されます。

展開間でのAPIを使用したカスタム プロファイリング ルールのエクスポートとインポート

Cisco DNA Center には、カスタム プロファイリング ルールのインポート、エクスポート、編集、および削除に使用できる Cisco AI エンドポイント分析 API が含まれています。

Cisco AI エンドポイント分析 API バンドルを有効にするには、次の手順を実行します。

1. メニューアイコン（☰）をクリックして、**[Platform]** > **[Manage]** > **[Bundles]** の順に選択します。
2. [AI Endpoint Analytics] という名前のバンドルを見つけ、[Enable] をクリックします。
3. [Status] 列の値が [Disabled] から [Active] に更新され、API のリストが表示されます。各 API の予期される要求および応答ペイロードを確認することもできます。
4. API バンドルを有効にすると、Cisco AI エンドポイント分析 API が Cisco DNA Center 開発者用ツールキットに追加されます。その後、[Developer Toolkit] ウィンドウ（**[Platform]** > **[Developer Toolkit]**）から API にアクセスできます。

[Bundles] ウィンドウと [Developer Toolkit] ウィンドウの両方から、次の操作を実行できます。

- コードプレビューを生成して、API を実行する別のツールで使用できる API コードを表示します。
- [Try It] をクリックして、Cisco DNA Center GUI から API を実行します。JSON 応答を受信し、それを任意のテキストエディタにコピーアンドペーストして作業を続行できます。

スマートグループ化のための Cisco AI ルール

Cisco AI エンドポイント分析の AI アルゴリズムは、展開全体のエンドポイント プロファイリング ラベルとグループに関するデータを分析し、スマートなプロファイリングルールの提案を提供します。

Cisco AI エンドポイント分析の [Overview] タブの [AI Proposal] ダッシュレットには、エンドポイントクラスタからの学習に基づいた次のルールの提案が表示されます。

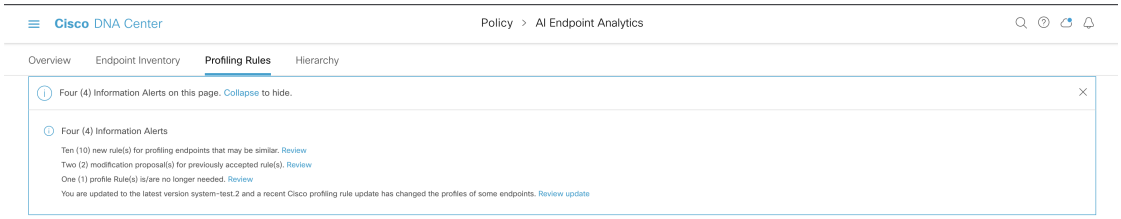
- ネットワーク内のプロファイルされていない、またはラベル付けされていないエンドポイントの新しいプロファイリングルール。詳細については、ネットワーク内の類似のエンドポイントに対する新しいプロファイリングの提案 （734 ページ）を参照してください。
- AI アルゴリズムが展開全体で学習したエンドポイント プロファイリング データの変更に基づいた、ネットワーク内の既存のプロファイリングルールの変更提案。詳細について

は、エンドポイントプロファイリングルールに対するスマート変更の提案（737ページ）を参照してください。

- AIアルゴリズムが展開全体で学習したエンドポイントプロファイリングデータの変更に基づいた、不適切なラベルを含むプロファイリングルールの削除提案。ルールの削除を受け入れると、影響を受けるエンドポイントから不適切なプロファイリングラベルが削除されます。エンドポイントのプロファイリングタイプの値は空になるか、以前に割り当てられたラベルに戻ります。詳細については、プロファイリングルールを削除するためのスマート提案（739ページ）を参照してください。

また、ワークフローを開始して、Cisco AIエンドポイント分析の[Profiling Rules]タブから、エンドポイントプロファイリングルールへの変更の提案を確認および適用することもできます。[Profiling Rules]は、情報アラートを含むダイアログボックスを表示します。情報アラートのダイアログボックスで、[Expand]をクリックして、エンドポイントプロファイリングルールの変更に関する利用可能な提案を表示します。調査する情報アラートの横にある[Review]をクリックして、対応するワークフローを開始します。

図 *36 : [Profiling Rules]* タブの情報アラート

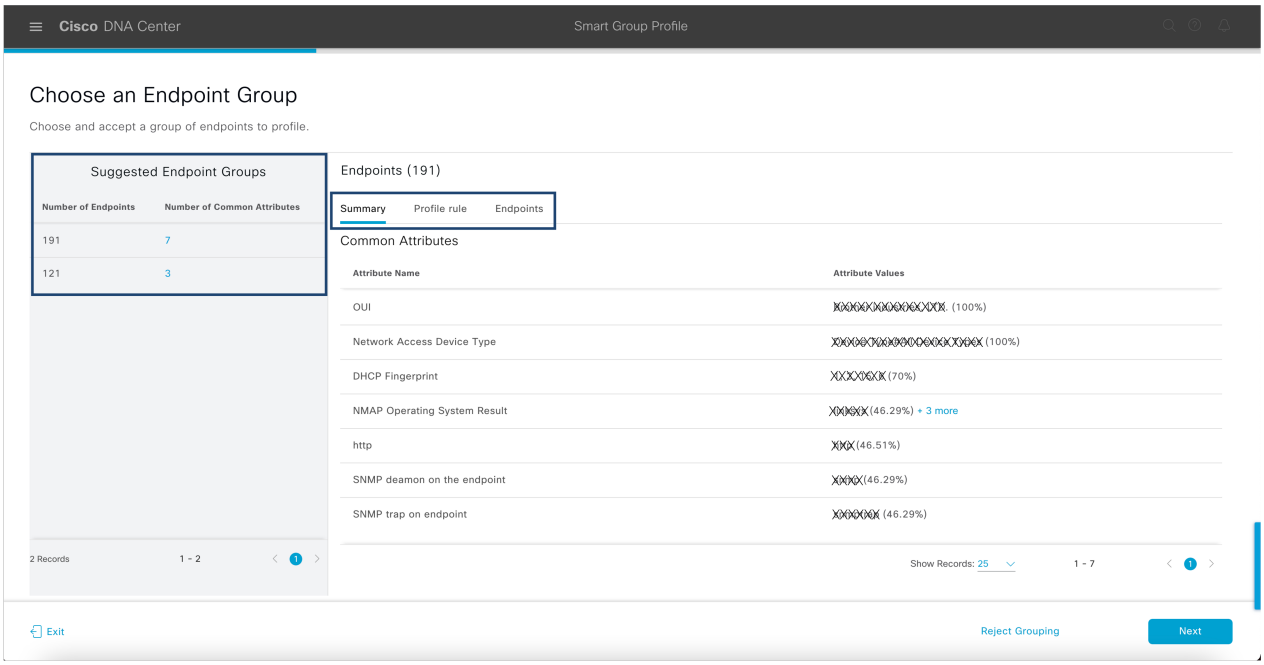


ネットワーク内の類似のエンドポイントに対する新しいプロファイリングの提案

ステップ 1 [AI Proposals]ダッシュレットで、[New rule(s) for profiling endpoints that may be similar]の横にある[Review]ボタンをクリックします。
[Smart Group Profile]ワークフローが起動されます。

ステップ 2 表示される[Choose an Endpoint Group]ウィンドウには、左側のペインに新しいプロファイリングルールの提案のリストが含まれています。リスト内のエントリをクリックして、右側のペインにプロファイリングルールの詳細を表示します。

図 *37 : [Smart Group Profile]* ワークフローの *[Choose an Endpoint Group]* ウィンドウ

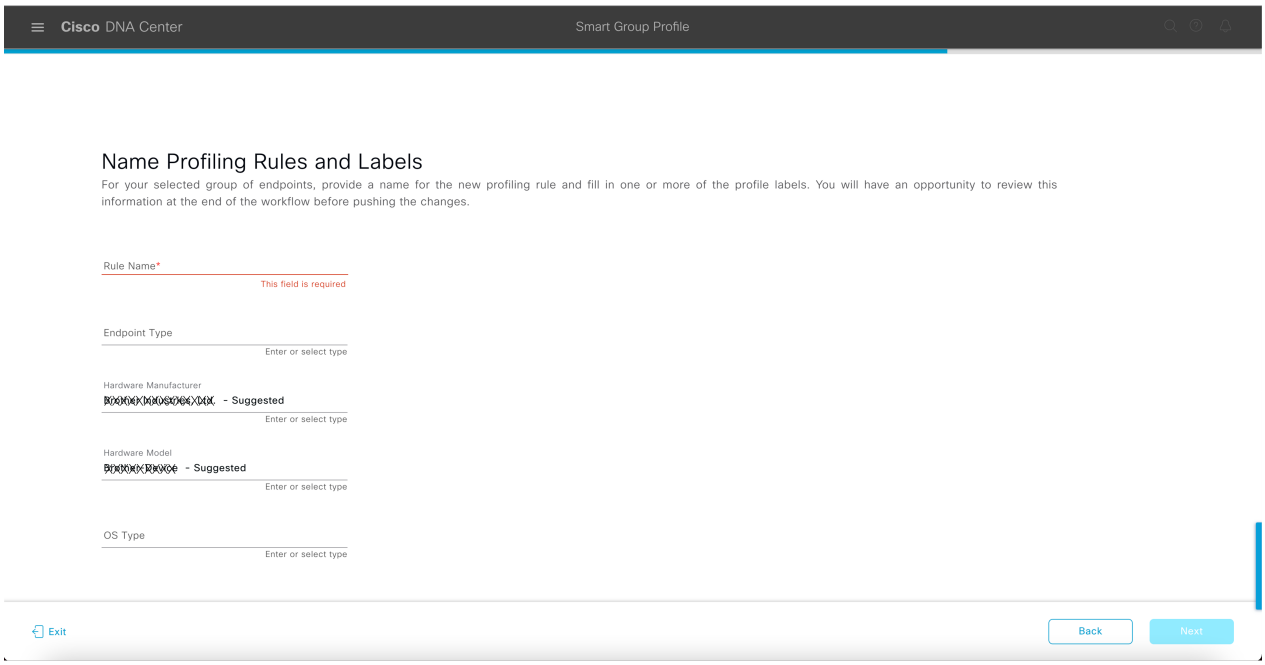


右側のペインには、[Summary]、[Profile Rule]、および [Endpoints] タブが含まれており、提案されたプロファイリングルールの詳細を簡単に表示できます。

ステップ 3 [Next] をクリックして、推奨されるプロファイリングルールを作成します。

ステップ 4 表示される [Name Profiling Rules and Labels] ウィンドウの [Rule Name] フィールドにルールの名前を入力します。

図 *38 : [Smart Group Profile]* ワークフローの *[Name Profiling Rules and Labels]* ウィンドウ



ステップ 5 次の 1 つ以上のフィールドに、必要な値を入力します。次の手順に進むには、少なくとも 1 つのフィールドに値を入力する必要があります。

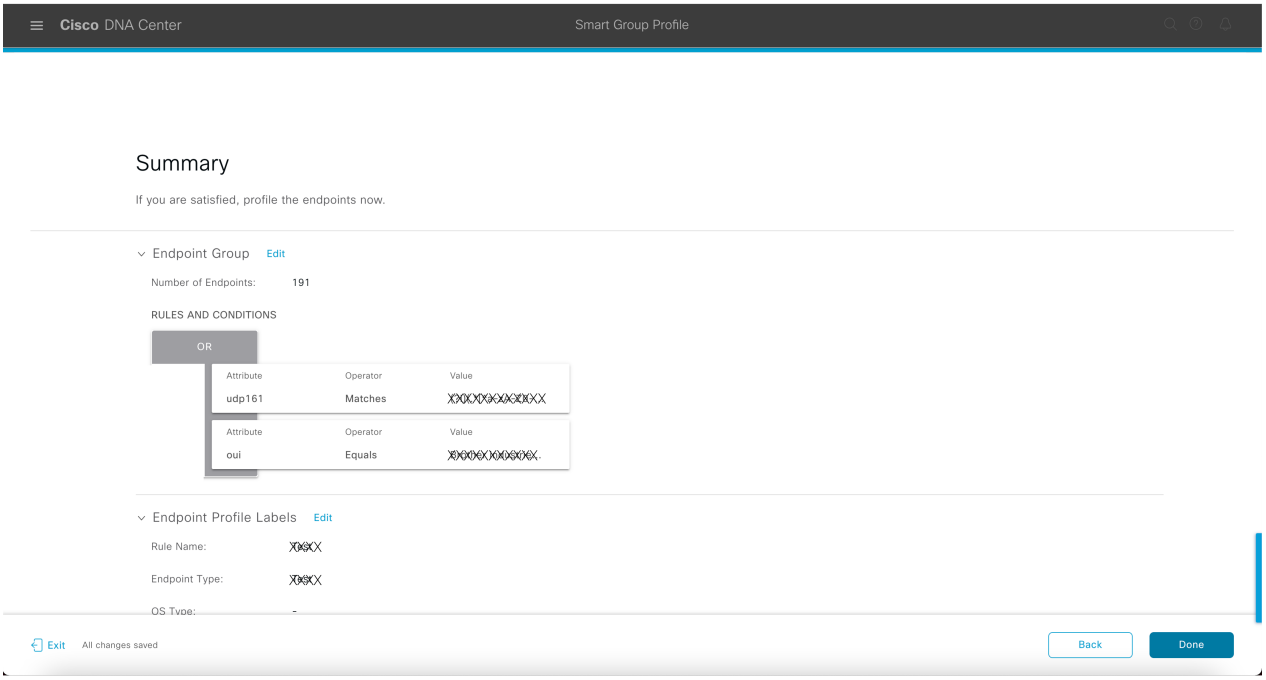
- **エンドポイント タイプ**
- **Hardware Manufacturer**
- **ハードウェア モデル**
- **OS Type**

AIアルゴリズムがエンドポイントのプロファイリングラベルを識別した場合、そのラベルは対応するフィールドに提案として表示されます。提案されたラベルで続行するか、別のラベルを選択するかを選択できます。

ステップ 6 [次へ（**Next**）] をクリックして続行します。

ステップ 7 表示される [Summary] ウィンドウで、プロファイリングルールの詳細を確認します。詳細を編集するには、ウィンドウの対応する領域に表示される [Edit] オプションをクリックします。

図 *39 : [Smart Group Profile]* ワークフローの *[Summary]* ウィンドウ



ステップ 8 プロファイリングルールを作成するには、[Done] をクリックします。

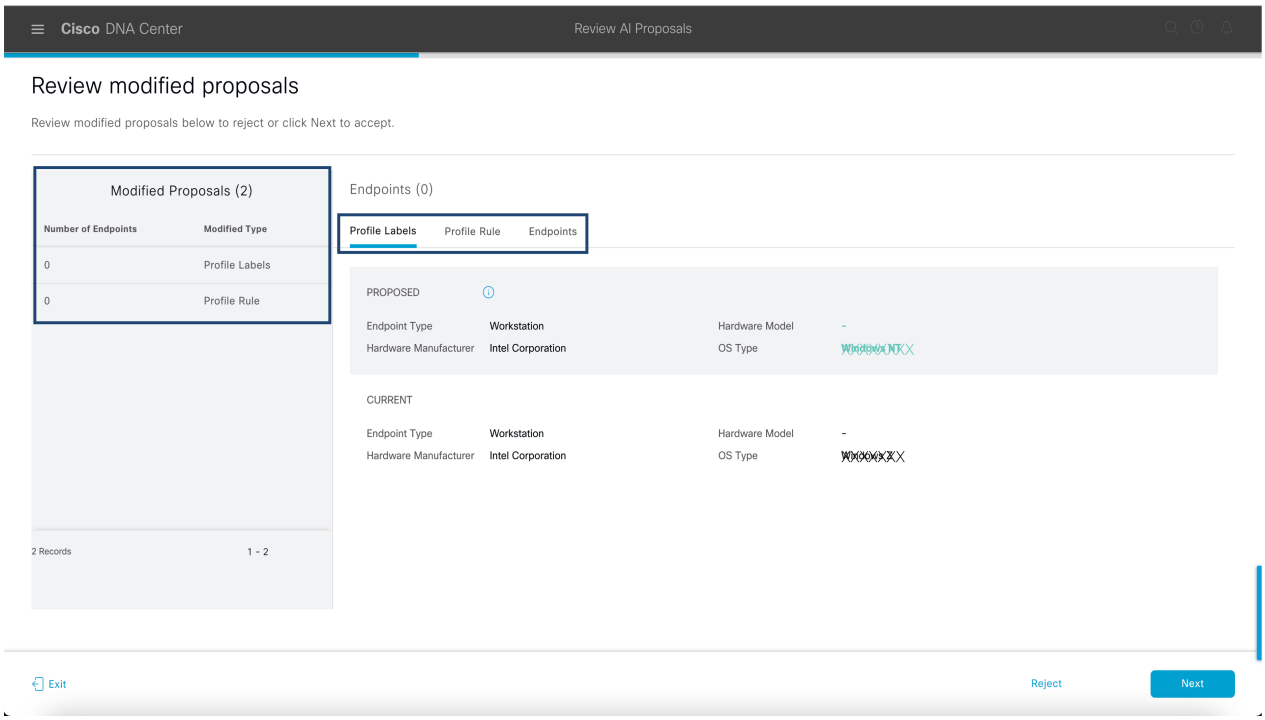
エンドポイント プロファイリング ルールに対するスマート変更の提案

ステップ 1 [AI Proposals] ダッシュレットで、[Modification proposal(s) for previously accepted rule(s)] の横にある [Review] ボタンをクリックします。

[Smart Group Profile] ワークフローが起動されます。

ステップ 2 表示される [Review modified proposals] ウィンドウには、既存のプロファイリングルールの変更提案のリストが含まれています。リスト内のエントリをクリックして、右側のペインに変更提案の詳細を表示します。

図 *40 : Review AI Proposals]* ワークフローの *[Review Modified Proposals]* ウィンドウ

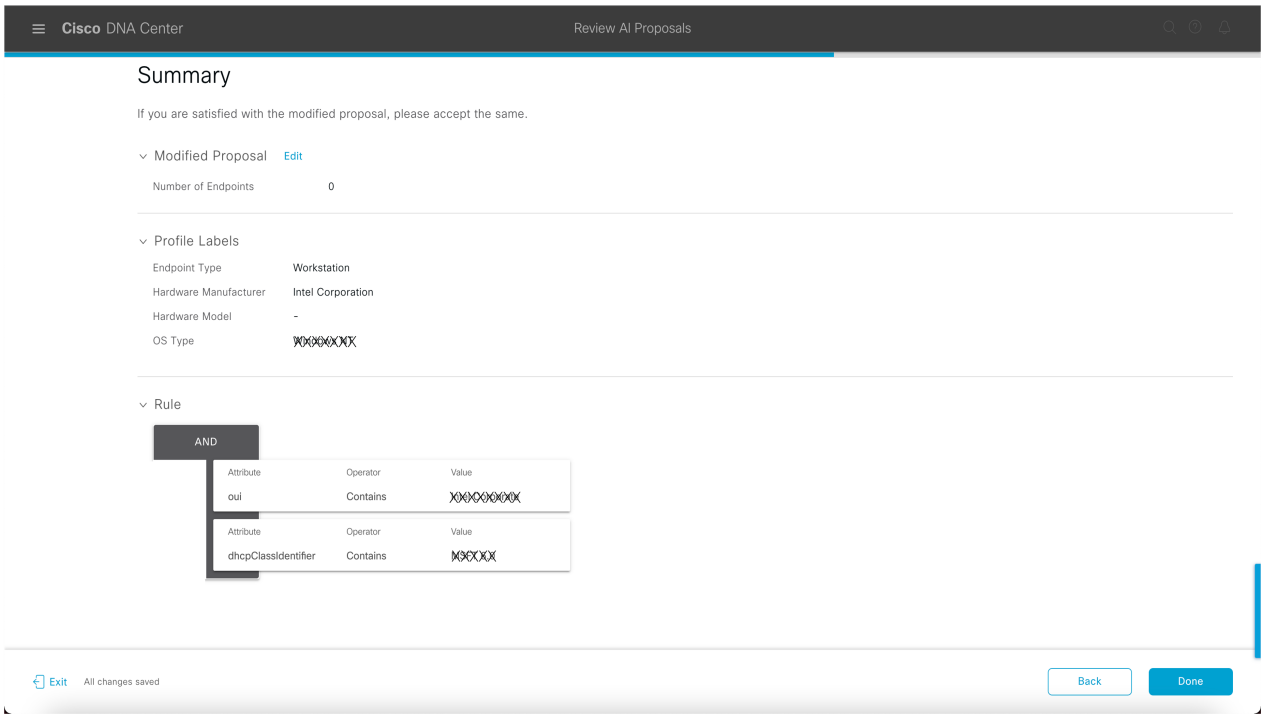


右側のペインには、[Profile Labels]、[Profile Rule]、および [Endpoints] タブが含まれており、提案された変更済みプロファイリングルールの詳細を簡単に表示できます。

ステップ 3 [Next] をクリックして、プロファイリングルールを提案どおりに更新します。

ステップ 4 表示される [Summary] ウィンドウで、プロファイリングルールの詳細を確認します。

図 *41 : [Review AI Proposals]* ワークフローの *[Summary]* ウィンドウ



ステップ 5 プロファイリングルールを更新するには、[Done] をクリックします。

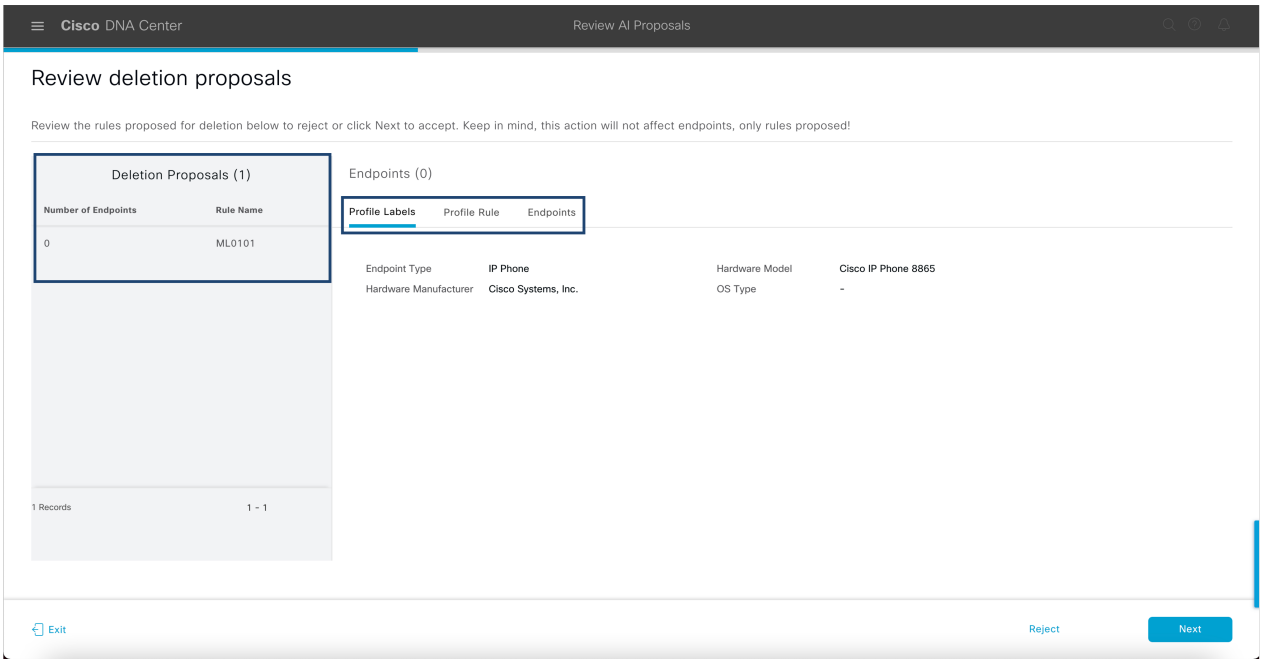
プロファイリングルールを削除するためのスマート提案

ステップ 1 [AI Proposals] ダッシュレットで、[Profiling Rules(s) is/are no longer needed] の横にある [Review] ボタンをクリックします。

[Review AI Proposals]ワークフローが開始されます。

ステップ 2 表示される [Review deletion proposals] ウィンドウには、既存のプロファイリングルールの削除提案のリストが含まれています。リスト内のエントリをクリックして、右側のペインに削除提案の詳細を表示します。

図 42 : *[Review AI Proposals]* ワークフローの *[Review Deletion Proposals]* ウィンドウ

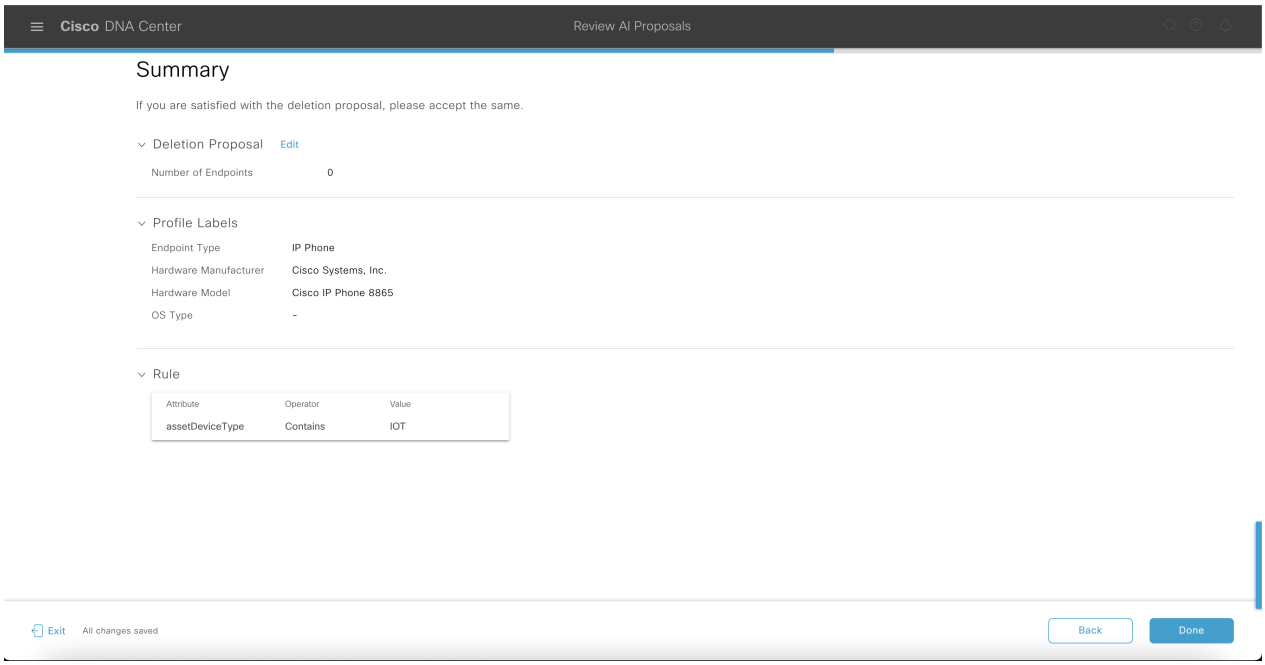


右側のペインには、[Profile Labels]、[Profile Rule]、および [Endpoints] タブが含まれており、提案された変更済みプロファイリングルールの詳細を簡単に表示できます。

ステップ 3 [Next] をクリックして、プロファイリングルールを提案どおりに更新します。

ステップ 4 表示される [Summary] ウィンドウで、プロファイリングルールの詳細を確認します。

図 43 : *[Review AI Proposals]* ワークフローの *[Summary]* ウィンドウ



ステップ 5 [Done] をクリックして、削除提案を受け入れます。

プロファイリングルールのインポート

カスタムプロファイリングルールとCisco AIルールを移行するには、.jsonファイルをインポートします。

ステップ 1 [Profiling Rule] ウィンドウで、[Actions] をクリックします。

ステップ 2 [Import Profiling Rules] を選択します。

ステップ 3 [Choose a file] をクリックし、システムの .json ファイルを参照します。

ステップ 4 [OK] をクリックします。

プロファイリングルールのエクスポート

Cisco AI エンドポイント分析からカスタムルールおよびCisco AI プロファイリングルールをエクスポートしてバックアップできます。[Export Profiling Rules] オプションは、使用可能なすべてのカスタムルールとCisco AIプロファイリングルールをエクスポートします。ルールを選択してエクスポートすることはできません。

ステップ 1 [Profiling Rules] ウィンドウで、[Actions] をクリックします。

ステップ 2 [Export Profiling Rules] を選択します。

ステップ 3 [Yes] をクリックして、すべてのカスタムルールとML プロファイリングルールをエクスポートします。終了するには、[No] をクリックします。

（注） 同じファイルを Cisco AI エンドポイント分析に再度インポートできます。

階層

Cisco AIエンドポイント分析階層は、エンドポイントタイプに基づいてエンドポイントの論理グループを作成するのに役立ちます。エンドポイントのカテゴリとサブカテゴリを作成すると、エンドポイントの可視性に焦点が当てられ、許可プロセスが簡素化されます。

デフォルトの[All Endpoints]親カテゴリからカテゴリを作成できます。エンドポイントの総数、エンドポイントタイプ、サブカテゴリなどのカテゴリの詳細が [Hierarchy] ウィンドウの個々のボックス内に表示されます。

カテゴリを作成、編集、および削除して、階層を並べ替えることができます。

カテゴリとサブカテゴリの作成

ステップ 1 [Hierarchy] ウィンドウで、親カテゴリの水平省略記号をクリックします。
ステップ 2 [Create Category] をクリックします。
ステップ 3 カテゴリ名を入力します。
ステップ 4 Enter キーを押します。

次のタスク

カテゴリを作成したら、[Endpoint Type] ウィンドウからエンドポイントタイプをドラッグアンドドロップするか、カテゴリを編集してエンドポイントを追加できます。

カテゴリまたはサブカテゴリの編集

ステップ 1 [Hierarchy] ウィンドウで、カテゴリの水平省略記号をクリックします。
ステップ 2 [Edit] をクリックします。
ステップ 3 表示される [Edit] ウィンドウで、[Category Name] に値を入力します。
ステップ 4 カテゴリを再割り当てする場合は、ドロップダウンメニューから [Parent Category] を入力します。
ステップ 5 [Endpoint Type] タブをクリックします。
ステップ 6 [Actions] をクリックし、[Add Endpoint Type] を選択します。
ステップ 7 [Search Dropdown] リストからエンドポイントタイプを選択します。
ステップ 8 **[保存（Save）]** をクリックします。

次のタスク

[Endpoint Type] ウィンドウで、[All]、[Available]、および [Assigned] でエンドポイントタイプをフィルタ処理できます。

カテゴリからのエンドポイントタイプの削除

ステップ 1 [Hierarchy] ウィンドウで、削除するカテゴリの水平省略記号をクリックします。
ステップ 2 [Edit] をクリックします。
ステップ 3 [Edit] ウィンドウで、[Endpoint Type] タブをクリックします。
ステップ 4 削除するエンドポイントタイプの横にあるチェックボックスをオンにします。
ステップ 5 [Actions] をクリックし、[Remove From Category] を選択します。

次のメッセージが表示されます。

「Are you sure you want to delete this category?」

ステップ 6 カテゴリからエンドポイントを削除するには、[Yes] をクリックします。終了するには、[No] をクリックします。

カテゴリからのエンドポイントタイプの再割り当て

ステップ 1 [Hierarchy] ウィンドウで、カテゴリの水平省略記号をクリックします。

ステップ 2 [Edit] をクリックします。

ステップ 3 [Edit] ウィンドウで、[Endpoint Type] タブをクリックします。

ステップ 4 再割り当てするエンドポイントタイプの横にあるチェックボックスをオンにします。

ステップ 5 [Actions] をクリックし、[Re-assign to existing category] または [Re-assign to a new category] を選択します。

オプション	手順
既存のカテゴリへの再割り当て	1. [Reassign] ウィンドウで、[Category] ドロップダウンリストから既存のカテゴリを選択します。 2. **[保存（Save）]** をクリックします。
新しいカテゴリへの再割り当て	1. [Reassign] ウィンドウで、[Category] ドロップダウンリストから [New Category] を選択します。 2. [Parent Category] ドロップダウンリストから親カテゴリを選択します。 3. [New Category] フィールドにカテゴリ名を入力します。 4. [Save] をクリックします。

カテゴリの削除

始める前に

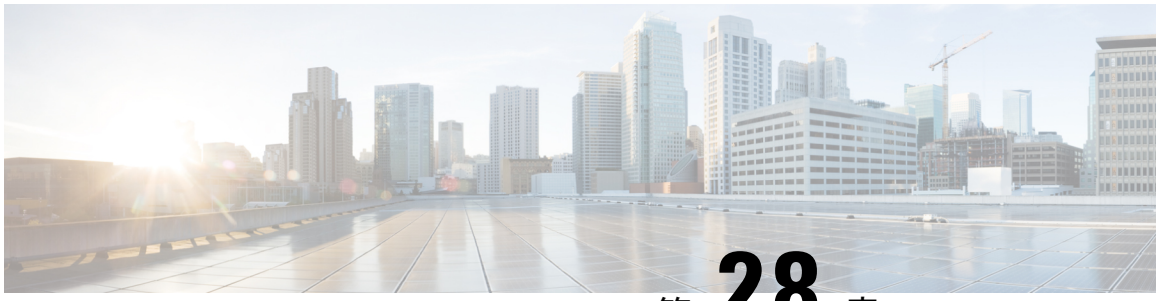
親カテゴリを削除する前に、そのサブカテゴリを確認します。サブカテゴリを別の既存のカテゴリまたは新しいカテゴリに再割り当てできます。そうしないと、すべてのサブカテゴリが親カテゴリとともに削除されます。カテゴリの削除中にサブカテゴリを再割り当てすることもできます。

ステップ 1 [Hierarchy] ウィンドウで、カテゴリの水平省略記号をクリックします。

ステップ 2 [削除（Delete）] をクリックします。

サブカテゴリが割り当てられているカテゴリを削除する場合には、[Reassign Relationships] ダイアログボックスが表示されます。次のいずれかのオプションを選択します。

オプション	条件	手順
既存のカテゴリへの再割り当て	既存のカテゴリにサブカテゴリを再割り当てします。	**1.** [Category] ドロップダウンリストからカテゴリを選択します。 **2.** [Reassign] をクリックします。 親カテゴリが削除され、選択したカテゴリにサブカテゴリが再割り当てされます。
新しいカテゴリへの再割り当て	既存のカテゴリにサブカテゴリを再割り当てします。	**1.** [Parent Category] ドロップダウンリストからカテゴリを選択します。 **2.** [New Category] フィールドにカテゴリ名を入力します。 **3.** [Reassign] をクリックします。 親カテゴリが削除され、新しいカテゴリにサブカテゴリが再割り当てされます。
カテゴリからの削除	親カテゴリとともにサブカテゴリを削除します。	[Reassign] をクリックします。 親カテゴリとそのサブカテゴリが削除されます。



第 28 章

ネットワーク推論機能を使用したネットワークデバイスのトラブルシューティング

ネットワーク推論機能の概要

ネットワーク推論機能ツールを使用すると、ネットワークのさまざまな問題を迅速にトラブルシューティングできます。メニューアイコン（≡）をクリックして、**[Tools]** > **[Network Reasoner]** の順に選択すると、ネットワーク推論機能ダッシュボードが起動します。ネットワーク推論機能ダッシュボードには、ネットワークの問題を事前にトラブルシューティングできる個別のワークフローが用意されています。ダッシュボードには、ワークフローに関する簡単な説明、過去 24 時間に影響を受けたデバイスの数、およびワークフローをネットワークで実行した場合の影響が表示されます。

（注） ネットワーク推論機能を使用するには機械推論パッケージをインストールする必要があり、インストールされていないと [Tools] メニューに表示されません。詳細については、Cisco DNA Center 管理者ガイドを参照してください。

MRE ワークフローを使用した Cisco SD-Access 移行の検証

次の MRE ワークフローは、Cisco SD-Access への移行を計画する際に役立ちます。

- SDA ハードウェアの準備状況チェック
- SDA ソフトウェアの準備状況チェック
- 冗長リンクチェック
- L3 アクセスチェック
- MTU リンクチェック
- SDA 正常性チェック
- SDA スケール制限チェック

ステップ 1 メニューアイコン（☰）をクリックして、**[Tools]** > **[Network Reasoner]** の順に選択します。

ステップ 2 [Network Reasoner] ダッシュボードで、必要に応じて次のワークフローをクリックします。

ワークフロー	説明	アクション
SDA ハードウェアの準備状況チェック	ハードウェアが Cisco SD-Access の移行準備ができているかどうかを確認します。	1. [SDA Hardware Readiness Check] をクリックします。 2. [Run Machine Reasoning] をクリックします。
SDA ソフトウェアの準備状況チェック	ソフトウェアが Cisco SD-Access の移行準備ができているかどうかを確認します。	1. [SDA Software Readiness Check] をクリックします。 2. [Run Machine Reasoning] をクリックします。
冗長リンクチェック	デバイスに冗長アップリンクが存在するかどうか、およびアクセススイッチで冗長アップリンクを設定して可用性を向上させる方法があるかどうかを確認します。	1. [Redundant Link Check] をクリックします。 2. 適切なデバイスを選択します。 3. [Troubleshoot] をクリックします。

ワークフロー	説明	アクション
L3 アクセスチェック	最小限の設計変更で Cisco SD-Access に移行するレイヤ 3 ルーティングプロトコルを実行しているアクセススイッチがネットワークにあるかどうかを確認します。	**1.** [L3 Access Check] をクリックします。 **2.** 適切なデバイスを選択します。 **3.** [Troubleshoot] をクリックします。
MTU リンクチェック	メインのネットワークデバイスとアクセス、コア、およびその他のスイッチ間のリンクが正しいMTUで設定されているかどうかを確認します。	**1.** [MTU Link Check] をクリックします。 **2.** 適切なデバイスを選択します。 **3.** [Troubleshoot] をクリックします。
SDA 正常性チェック：ファブリック数	Cisco DNA Center クラスタの正常性をチェックし、ファブリックの管理が原因でスケール制限のいずれかのしきい値に達しているかどうかを確認します。	**1.** [Fabric Count] をクリックします。 **2.** [Run Machine Reasoning] をクリックします。
SDA 正常性チェック：SDA スケール制限チェック	Cisco DNA Center に設定されているクライアントエンドポイント、ネットワークデバイス、およびファブリックの数が、公開されている SDA の制限内であるかどうかを確認します。	**1.** [SDA Scale Limits Check] をクリックします。 **2.** [Run Machine Reasoning] をクリックします。
SDA 正常性チェック：クライアント数	Cisco DNA Center クラスタの正常性をチェックし、クライアントの管理が原因でスケール制限のいずれかのしきい値に達しているかどうかを確認します。	**1.** [Client Count] をクリックします。 **2.** [Run Machine Reasoning] をクリックします。
SDA 正常性チェック：デバイス数	Cisco DNA Center クラスタの正常性をチェックし、ネットワークデバイスの管理が原因でスケール制限のいずれかのしきい値に達しているかどうかを確認します。	**1.** [Device Count] をクリックします。 **2.** [Run Machine Reasoning] をクリックします。

CPU 使用率が高い場合のトラブルシューティング

CPU 使用率のトラブルシューティングは、ソフトウェアバージョン 16.9.3 以降の次のネットワークデバイスでのみサポートされます。

- Cisco Catalyst 9400 シリーズ スイッチ
- Cisco Catalyst 9300 シリーズ スイッチ
- Cisco Catalyst 3850 シリーズ スイッチ
- Cisco Catalyst 3650 シリーズ スイッチ

始める前に

- 機械推論パッケージをインストールします。詳細については、『Cisco DNA Center Administrator Guide』の「Download and Install Packages and Updates」を参照してください。
- [System] 機能で機械推論に対する書き込み権限を持つユーザーロールを作成します。詳細については、『Cisco DNA Center Administrator Guide』の「Configure Role-Based Access Control」を参照してください。

ステップ 1 メニューアイコン（☰）をクリックして、**[Tools]** > **[Network Reasoner]** の順に選択します。

ステップ 2 [CPU Utilization] タブをクリックします。

[CPU Utilization] ウィンドウには、過去 24 時間の CPU 使用率が高いデバイスのフィルタ処理されたリストが表示されます。

[All] をクリックするとインベントリの全デバイスのリストが表示され、ワークフローを実行するデバイスを選択できます。

ステップ 3 トラブルシューティングするデバイスを選択します。

[Filter] をクリックし、[Tag]、[Device Name]、[IP Address]、[Device Type]、[Site]、または [Reachability] にデバイスの情報を入力します。

ステップ 4 [Troubleshoot] をクリックします。

ステップ 5 [Reasoner Input] ウィンドウで、[CPU Utilization Threshold] にチェックする使用率を入力します。

ステップ 6 [Run Machine Reasoning] をクリックします。

（注） 次のプロセスが確認されると、詳細な分析の対象となります。

- [MATM Process Group]：MATM RP Shim、NGWC Learning、VMATM Callback
- [IOSXE Process Group]：IP Input、ARP Input、IOSXE-RP Punt Se、SISF Main Thread、DAI Packet、ARP Snoop

[CPU Utilization] ウィンドウでは、選択したデバイスの CPU 使用率が高い原因に関する情報が [Root Cause Analysis] に表示されます。

[Reasoning Activity] タブには、トラブルシューティング プロセスで確認されるさまざまなパラメータが表示されます。

ステップ 7 （オプション）進行中の推論アクティビティを停止するには、[Stop] をクリックします。

ステップ 8 [Conclusion] タブをクリックして、CPU の消費が多いプロセスとその使用率を確認します。

ステップ 9 それぞれのプロセスについて、[View Relevant Activities] をクリックし、右側のペインで [Activity Details] を確認します。

ステップ 10 （オプション）同じデバイスについてトラブルシューティングプロセスをもう一度実行する場合は、[Run Again] をクリックします。

（注） 機械推論エンジン（MRE）では、しきい値が指定のレベルを超えた場合や非アクティブのタイムアウト要求からイベントを受信しなかった場合にネットワーク推論機能ワークフローを検出して終了するシステム終了アルゴリズムを実装しています。

電源障害のトラブルシューティング

電源トラブルシューティング ワークフローは、ソフトウェアバージョン 16.6.1 以降の次のネットワークデバイスでのみサポートされます。

- Cisco Catalyst 3650 シリーズ スイッチ
- Cisco Catalyst 3850 シリーズ スイッチ
- Cisco Catalyst 9300 シリーズ スイッチ
- Cisco Catalyst 9400 シリーズ スイッチ
- Cisco Catalyst 9500 シリーズ スイッチ

始める前に

- 機械推論パッケージをインストールします。詳細については、『Cisco DNA Center Administrator Guide』の「Download and Install Packages and Updates」を参照してください。
- [System] 機能で機械推論に対する書き込み権限を持つユーザーロールを作成します。詳細については、『Cisco DNA Center Administrator Guide』の「Configure Role-Based Access Control」を参照してください。

ステップ 1 メニューアイコン（☰）をクリックして、**[Tools]** > **[Network Reasoner]** の順に選択します。

ステップ 2 [Power Supply] タブをクリックします。

[Power Supply] ウィンドウに、過去 24 時間に電源障害が発生したデバイスのフィルタ処理されたリストが表示されます。

インベントリ内のすべてのデバイスのリストを表示するには、[All] をクリックします。ワークフローを実行する任意のデバイスを選択できます。

ステップ 3 トラブルシューティングするデバイスを選択します。

[Filter] をクリックし、[Tag]、[Device Name]、[IP Address]、[Device Type]、[Site]、または [Reachability] にデバイスの情報を入力してデバイスをフィルタ処理します。

ステップ 4 [Troubleshoot] をクリックします。

[Power Supply] ウィンドウで、選択したデバイスの電源障害の原因に関する情報が [Root Cause Analysis] に表示されます。

[Reasoning Activity] タブには、トラブルシューティング プロセスで確認されるさまざまなパラメータが表示されます。

ステップ 5 （オプション）進行中の推論アクティビティを停止するには、[Stop] をクリックします。

ステップ 6 [Conclusion] タブをクリックして、選択したデバイスの電源の [Stack Identifier]、[Product ID]、[Serial Number]、および [Status] の情報と推奨されるアクションを確認します。

ステップ 7 それぞれのスタック識別子について、[View Relevant Activities] をクリックし、右側のペインで [Activity Details] を確認します。

ステップ 8 （オプション）同じデバイスについてトラブルシューティング プロセスをもう一度実行する場合は、[Run Again] をクリックします。

（注） MRE では、しきい値が指定のレベルを超えた場合や非アクティブのタイムアウト要求からイベントを受信しなかった場合にネットワーク推論機能ワークフローを検出して終了するシステム終了アルゴリズムを実装しています。

インターフェイスが停止した場合のトラブルシューティング

インターフェイス ダウン トラブルシューティング ワークフローは、ソフトウェアバージョン 16.9.3 以降の次のネットワークデバイスでのみサポートされます。

- Cisco Catalyst 3650 シリーズ スイッチ
- Cisco Catalyst 3850 シリーズ スイッチ
- Cisco Catalyst 9300 シリーズ スイッチ
- Cisco Catalyst 9400 シリーズ スイッチ
- Cisco Catalyst 9500 シリーズ スイッチ

始める前に

- 機械推論パッケージをインストールします。詳細については、『Cisco DNA Center Administrator Guide』の「Download and Install Packages and Updates」を参照してください。

- [System] 機能で機械推論に対する書き込み権限を持つユーザーロールを作成します。詳細については、『Cisco DNA Center Administrator Guide』の「Configure Role-Based Access Control」を参照してください。

ステップ 1 メニューアイコン（☰）をクリックして、**[Tools]** > **[Network Reasoner]** の順に選択します。

ステップ 2 [Interface Down] タブをクリックします。

[Interface Down] ウィンドウには、過去 24 時間にインターフェイスが停止したデバイスのフィルタ処理されたリストが表示されます。

[All] をクリックするとインベントリの全デバイスのリストが表示され、ワークフローを実行するデバイスを選択できます。

ステップ 3 トラブルシューティングするデバイスを選択します。

[Filter] をクリックし、[Tag]、[Device Name]、[IP Address]、[Device Type]、[Site]、または [Reachability] にデバイスの情報を入力します。

ステップ 4 [Troubleshoot] をクリックします。

ステップ 5 [Reasoner Input] ウィンドウで、問題が疑われるインターフェイスの名前を入力します。

ステップ 6 [Run Machine Reasoning] をクリックします。

[Interface Down] ウィンドウには、選択したデバイスのインターフェイスが停止する原因に関する情報が [Root Cause Analysis] に表示されます。

[Reasoning Activity] タブには、トラブルシューティング プロセスで確認されるさまざまなパラメータが表示されます。

ステップ 7 （オプション）進行中の推論アクティビティを停止するには、[Stop] をクリックします。

ステップ 8 [Conclusion] タブをクリックして、インターフェイスが停止する問題についての考えられる根本原因と推奨されるアクションを確認します。

ステップ 9 それぞれの根本原因分析について、[View Relevant Activities] をクリックし、右側のペインで [Activity Details] を確認します。

ステップ 10 （オプション）同じデバイスについてトラブルシューティング プロセスをもう一度実行する場合は、[Run Again] をクリックします。

（注） MRE では、しきい値が指定のレベルを超えた場合や非アクティブのタイムアウト要求からイベントを受信しなかった場合にネットワーク推論機能ワークフローを検出して終了するシステム終了アルゴリズムを実装しています。

ネットワーク接続のトラブルシューティング

Cisco IOS-XE ソフトウェアバージョン 16.9.3 以降を実行している次のネットワークデバイスでのみ、ネットワーク接続のトラブルシューティングがサポートされています。

- Cisco Catalyst 9200 シリーズ スイッチ
- Cisco Catalyst 9300 シリーズ スイッチ
- Cisco Catalyst 9400 シリーズ スイッチ
- Cisco Catalyst 9500 シリーズ スイッチ
- Cisco Catalyst 9600 シリーズ スイッチ

次の手順を使用して、IPアドレスを使用してデバイスからエンドポイントの到達可能性を確認します。

始める前に

- 機械推論パッケージをインストールします。詳細については、『Cisco DNA Center Administrator Guide』の「Download and Install Packages and Updates」を参照してください。
- [System] 機能で機械推論に対する書き込み権限を持つユーザーロールを作成します。詳細については、『Cisco DNA Center Administrator Guide』の「Configure Role-Based Access Control」を参照してください。

ステップ 1 メニューアイコン（☰）をクリックして、**[Tools]** > **[Network Reasoner]** の順に選択します。

ステップ 2 [Network Connectivity] タブをクリックします。

ステップ 3 **デバイス名**、**IP アドレス**、**デバイスタイプ**、**サイト**、**到達可能性**、**ロール**、**プラットフォーム**などの詳細情報を含むデバイステーブルを表示できます。

ステップ 4 デバイスを選択して、[Troubleshoot] を選択します。

ステップ 5 [Reasoner Inputs] ウィンドウの [Destination IP address] フィールドに有効な IP アドレスを入力し、[Run Machine Reasoning] をクリックします。

（注） Virtual Routing and Forwarding（VRF）の名前を入力します（該当する場合）。

ステップ 6 [Root Cause Analysis] ウィンドウの [Reasoning Activity] で、トラブルシューティング プロセスの一環として検証されるさまざまなワークフローを確認できます。

ステップ 7 [Conclusions] タブで、検証チェックのステータスと推奨アクションを確認できます。

デバイスの IP 接続のトラブルシューティング

ping はシンプルなコマンドであるため、すべてのネットワークデバイスで IP 接続のトラブルシューティングをサポートできます。

始める前に

- 機械推論パッケージをインストールします。詳細については、『Cisco DNA Center Administrator Guide』の「Download and Install Packages and Updates」を参照してください。
- [System] 機能で機械推論に対する書き込み権限を持つユーザーロールを作成します。詳細については、『Cisco DNA Center Administrator Guide』の「Configure Role-Based Access Control」を参照してください。

ステップ 1 メニューアイコン（☰）をクリックして、**[Tools]** > **[Network Reasoner]** の順に選択します。

ステップ 2 [Network Reasoner] ダッシュボードで、[Ping Device] をクリックします。

ステップ 3 [Devices] ウィンドウで、デバイスを選択し、[Troubleshoot] をクリックします。

ステップ 4 [Reasoner Inputs] ウィンドウで、[Target IP Address] に値を入力し、[Run Machine Reasoning] をクリックします。

ステップ 5 [View Details] をクリックして、ping ステータスを確認します。

MRE ワークフローを使用した無線クライアントの問題のトラブルシュート

この手順を使用して、MRE ワークフローを使用してワイヤレスクライアントの問題をトラブルシューティングします。ワイヤレスクライアントのトラブルシューティング ワークフローのサポートは、Cisco IOS-XE ソフトウェアバージョン 17.3.4 以降のネットワークデバイスでのみ使用できます。

始める前に

MRE ナレッジベースが最新のナレッジパックで更新されていることを確認します。詳細については、『Cisco DNA Center Administrator Guide』の「Update the Machine Reasoning Knowledge Base」を参照してください。

ステップ 1 メニューアイコン（☰）をクリックして、[Tools] > [Network Reasoner] の順に選択します。

ステップ 2 [Wireless Client Data Collection] タイルをクリックします。
[Devices] ウィンドウに、フィルタリングされたワイヤレス コントローラ デバイスが表示されます。

ステップ 3 トラブルシューティングするワイヤレスコントローラを選択し、[Troubleshoot] をクリックします。

ステップ 4 **[Reasoner Inputs]** ウィンドウで、次のフィールドに値を入力します。

- [Troubleshoot Duration]
- [Client MAC Address]

- [PCAP Interface]：ドロップダウン矢印をクリックし、リストからインターフェイスを選択します。パケットキャプチャが必要な場合は、このオプションを使用します。

ステップ 5 [Run Machine Reasoning] をクリックします。
[Wireless Client Data Collection] スライドインペインが表示されます。

ステップ 6 [Root Cause Analysis] エリアの [Reasoning Activity] タブには、トラブルシューティング プロセスで確認されるさまざまなパラメータが表示されます。必要に応じて、[Stop] をクリックして進行中の推論アクティビティを停止します。

ステップ 7 トラブルシューティング処理が完了するまで待ちます。完了したら、[Conclusions] タブでトラブルシューティング ファイルを表示できます。

ステップ 8 （任意）同じデバイスについてトラブルシューティング プロセスをもう一度実行する場合は、[Run Again] をクリックします。

ステップ 9 （任意） ワイヤレスクライアントのトラブルシューティング ワークフローを開始すると、[Wireless Client Data Collection] スライドインペインで最新のトラブルシューティング ファイルを表示できます。

MRE ワークフローを使用したモニター対象外のデバイスのトラブルシューティング

この手順を使用して、監視されていないデバイスまたは アシュアランス データが表示されないデバイスのトラブルシューティングを行います。監視されていないデバイスのトラブルシューティング ワークフローは、スイッチ、Cisco AireOS ワイヤレスコントローラ、および Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のみをサポートします。

始める前に

MRE ナレッジベースが最新のナレッジパックで更新されていることを確認します。詳細については、『*Cisco DNA Center Administrator Guide*』の「Update the Machine Reasoning Knowledge Base」を参照してください。

ステップ 1 メニューアイコン（☰）をクリックして、**[Tools]** > **[Network Reasoner]** の順に選択します。

ステップ 2 [Assurance Telemetry Analysis] タイルをクリックします。

ステップ 3 [Devices] ウィンドウには、監視されていないデバイスがフィルタリングされて表示されます。トラブルシューティングするデバイスを選択し、[Troubleshoot] をクリックします。

[Assurance Telemetry Analysis] slide-in paneが 表示されます。

ステップ 4 [Root Cause Analysis] エリアの [Reasoning Activity] タブには、トラブルシューティング プロセスで確認されるさまざまなパラメータが表示されます。進行中の推論アクティビティを停止するには、[Stop] をクリックします。

ステップ 5 トラブルシューティング処理が完了するまで待ちます。トラブルシューティングが完了すると、[Machine Reasoning Completed] ダイアログボックスが表示されます。**[Show Details]** をクリックします。

ステップ 6 [Conclusions] タブでトラブルシューティング ファイルを表示できます。問題にはアイコン（  ）が表示され、問題の下に [Suggested Action] が表示されます。

提示された推奨案を使用して、監視されていないデバイスのトラブルシューティングを行うことができます。

ステップ 7 同じデバイスについてトラブルシューティング プロセスをもう一度実行する場合は、[Run Again] をクリックします。

ステップ 8 [Inventory] タブからデバイスのトラブルシューティングを行うことができます。スクロールバーをドラッグして、[Health Score] 列を表示します。[Health Score] 列の下の [No Health] をクリックし、[View Assurance Telemetry Analysis] をクリックして、トラブルシューティング プロセスを実行します。

ネットワークのバグのスキャン

Cisco DNA Center のネットワークバグ ID ツールを使用すると、ネットワークをスキャンして、以前に識別され、シスコが認識している、選択された一連の障害またはバグを検出することができます。

Cisco DNA Center のネットワークバグ ID は、デバイス設定またはデバイスの動作データ内の特定パターンを識別するために役立ちます。それらのパターンに基づいて、既知の障害と照合することができます。このツールは、バグに焦点を合わせたビューとデバイスに焦点を合わせたビューの両方を提供します。

Cisco DNA Center は、ネットワークデバイスで CLI コマンドを実行してネットワークデバイスの構成と運用データを収集し、その情報を CX Cloud に送信して処理することで、潜在的なセキュリティアドバイザリやバグの公開に使用されます。Cisco DNA Center はネットワークバグ識別ツールの次の CLI コマンドを呼び出します。

- **show buffers summary**
- **show cef interfaces**
- **show clock**
- **show crypto eli all**
- **show crypto isakmp sa detail**
- **show eigrp service-family ipv4 neighbors**
- **show environment all**
- **show interfaces counters error**
- **show interfaces summary**
- **show inventory**

- **show ip interface brief**
- **show ip nat translations verbose**
- **show ip nbar protocol-discovery**
- **show ip nbar resources flow**
- **show ip nhrp**
- **show ip nhrp summary**
- **show ip route**
- **show ip ssh**
- **show ip vrf**
- **show logging**
- **show performance monitor cache detail**
- **show platform software route-map fp active map**
- **show pnp profile**
- **show redundancy**
- **show redundancy application group**
- **show running-config all**
- **show scp status**
- **show stackwise-virtual**
- **show startup-config**
- **show terminal**
- **show version**

次の手順では、ネットワークバグ識別ツールを使用してバグを識別する方法について説明します。

始める前に

- Cisco DNA Center のコアパッケージをインストールします。詳細については、*Cisco DNA Center* 管理者ガイドの「Download and Install Packages and Updates」を参照してください。
- 機械推論パッケージをインストールします。詳細については、*Cisco DNA Center* 管理者ガイドの「Download and Install Packages and Updates」を参照してください。

ステップ 1 メニューアイコン（☰）をクリックして、**[Tools]** > **[Network Reasoner]** の順に選択します。

ステップ 2 [Network Bug Identifier] を選択します。

ステップ 3 [Scan Network] をクリックします。

ステップ 4 [Scan Network] ウィンドウで、次のいずれかを実行します。

- システムのバグをすぐにスキャンするには、[Now] オプションボタンをクリックして [Submit] をクリックします。
- スキャンを後で実行するようにスケジュールするには、[Later] オプションボタンをクリックし、日付と時刻を指定します。

ダッシュボードの進捗状況インジケータには、スキャンされたデバイスのリスト（10 台ずつ）が表示されます。スキャンが完了すると、[Network Bug Identifier] ウィンドウが表示されます。

ステップ 5 上部のペインを使用して、次のようにスキャンの結果に関する情報の表示、ネットワークの再スキャン、スキャン設定の変更を行います。

項目	説明
Bug Summary	ネットワーク内の [Catastrophic]、[Severe]、および [Moderate] のバグの数。
該当デバイス	スキャンされた次のデバイスタイプの数： • **Routers** • **スイッチとハブ**
Scan Mode	スキャンの実行に使用された方法： • **Essential**：Cisco Network Reasoner Engine（NRE）を使用して実行されるスキャン。 • **CX Cloud**：CX Cloud を使用して実行されるスキャン。
Re-scan Network	このボタンをクリックして、ネットワークを再度スキャンします。
Settings	[Settings] アイコンをクリックして、次の操作を行います。 • 毎週のスキャンを有効または無効にします。 • CX Cloud によるネットワークのスキャンを有効または無効にします。

ステップ 6 [Bugs on Devices] タブをクリックして次の詳細を表示します。

- **不具合 ID**
- **Name**
- **該当デバイス**
- **重大度**
- **影響を受けるバージョン**
- **回避策**

ハイパーリンクされた値をクリックすると、その値に関する詳細が表示されます。

ステップ 7 [Devices] タブをクリックして次の詳細を表示します。

- **[Device Name]**
- **Image Version**
- **IP Address**
- **Device Type**
- **バグ**
- **Scan Status**
- **Scan Mode**
- **サイト**
- **Reachability**

ハイパーリンクされた値をクリックすると、その値に関する詳細が表示されます。

ステップ 8 [Devices] タブで、[Tag Device] をクリックして、デバイスのタグを作成、編集、または削除します。

Cisco DNA Center のバグのスキャン

システムバグ ID ツールには、Cisco DNA Center のバグを識別するためのオプションがあります。次の手順では、**システムバグ ID** ツールを有効にする方法について説明します。

始める前に

- Cisco DNA Center のコアパッケージをインストールします。詳細については、*Cisco DNA Center* 管理者ガイドの「Download and Install Packages and Updates」を参照してください。
- 機械推論パッケージをインストールします。詳細については、*Cisco DNA Center* 管理者ガイドの「Download and Install Packages and Updates」を参照してください。

ステップ 1 メニューアイコン（≡）をクリックして、**[Tools]** > **[Network Reasoner]** の順に選択します。

ステップ 2 [System Bug Identifier] を選択します。

ステップ 3 [Scan System] をクリックします。

ステップ 4 [Scan System] ウィンドウで、次のいずれかを実行します。

1. システムのバグをすぐにスキャンするには、[Now] オプションボタンをクリックして [Submit] をクリックします。
2. スキャンを後で実行するようにスケジュールするには、[Later] オプションボタンをクリックし、日付と時刻を指定します。

ステップ 5 [System Bug Identifier] ウィンドウには、[BUG SUMMARY] と [Bugs Identified on Your System] テーブルが表示されます。

[Bugs Identified on Your System] テーブルでは、次の詳細を確認できます。

- 不具合 **ID**
- **Name**
- 重大度
- 最初に識別されたもの
- 最後に識別されたもの
- 識別された頻度
- 回避策
- 影響を受けるバージョン

ステップ 6 [Bug ID] をクリックします。
[Bug Details] ダイアログボックスに、バグの詳細情報が表示されます。

ステップ 7 [Bug ID] の横にある矢印をクリックし、[Bug Search Tools] ウィンドウに移動して、バグの詳細情報を確認します。

第 29 章

ネットワーク セキュリティ アドバイザリの識別

セキュリティアドバイザリの概要

Cisco Product Security Incident Response Team（PSIRTT; プロダクト セキュリティ インシデント レスポンス チーム）は、シスコ製品セキュリティインシデントに対応し、セキュリティ脆弱性ポリシーを規制し、シスコのセキュリティアドバイザリとアラートを推奨します。

セキュリティ アドバイザリ ツールは、これらの推奨されるアドバイザリを使用して、Cisco DNA Center 内のインベントリをスキャンし、既知の脆弱性を持つデバイスを検出します。

前提条件

セキュリティ アドバイザリ ツールを使用するには、機械推論パッケージをインストールする必要があります。『Cisco DNA Center Administrator Guide』の「*Download and Install Packages and Updates*」を参照してください。

オブザーバとして Cisco DNA Center にログインすると、ホームページで [Security Advisories] ツールを表示できません。

セキュリティアドバイザリの表示

ステップ 1 メニューアイコン（☰）をクリックして、**[Tools]** > **[Security Advisories]** の順に選択します。

ステップ 2 [Security Advisories] ウィンドウを初めて起動する場合は、[Scan Network] をクリックします。

Cisco DNA Center では、セキュリティの問題を特定して自動分析を改善するためにナレッジベースを使用します。最新のセキュリティアドバイザリを表示するには、定期的にナレッジベースを更新することをお勧めします。

a) メニューアイコン（☰）をクリックして、**System** > **Settings** > **Machine Reasoning Engine** の順に選択します。

b) [Import] をクリックするか、[Download Latest] をクリックして最新の使用可能なナレッジベースをダウンロードします。ダウンロードが完了したら、[Import] をクリックしてください。

c) 自動更新に登録するには、[AUTO UPDATE] トグルボタンをクリックします。

ステップ 3 [ADVISORIES] 領域には、[Critical]、[High]、[Medium]、[Low]、[Informational]、[Unknown] など、ネットワークに対するそれぞれの影響の割合が表示されます。

ステップ 4 スキャンは、各デバイスに関連付けられたライセンスに基づいてデバイスで実行されます。[SCAN CRITERIA] 領域では、次の順序に従って、アドバイザリをデバイスと一致させる必要があります。

- [Software Version]：スキャンは、**Cisco DNA Essentials** ライセンスを持つデバイスでソフトウェアバージョンに基づいて実行されます。
- [Custom]：スキャンは、**Cisco DNA Advantage** ライセンスを持つデバイスで、ソフトウェアバージョンと、デバイスの実行コンフィギュレーションに対するアドバイザリ（ある場合）に関して入力されたカスタム設定に基づいて実行されます。
- [Advanced]：スキャンは、**Cisco CX Cloud Success Track** の利用資格を持つデバイスで、ソフトウェアバージョン、設定、および運用データに基づいて実行されます。

  試用期間中はライセンス資格が適用されず、すべてのデバイスが [Advanced] レベルでスキャンされます。

（注）
- セキュリティアドバイザリダッシュボードにはシスコが公開しているセキュリティアドバイザリが表示されます。アドバイザリは現行のソフトウェアイメージに基づいており、ネットワーク上のデバイスに影響する場合があります。脆弱性が実際に存在するかどうかを判断するには、設定、プラットフォームの詳細、またはその他の基準をさらに詳しく分析する必要があります。
- セキュリティアドバイザリスキャンは、サポートされている最小ソフトウェアバージョン以上を実行しているルータおよびスイッチでのみ使用できます。詳細については、『Cisco DNA Center Compatibility Matrix』を参照してください。
- 表示されるセキュリティアドバイザリは、「シスコのセキュリティ脆弱性ポリシー」に基づいています。

次の表に、使用できる情報を記載します。

カラム	説明
アドバイザリ ID	ネットワークで検出されたセキュリティアドバイザリの ID。ID をクリックして、それぞれのアドバイザリ Web ページに移動します。
アドバイザリタイトル	ネットワークデバイスに適用可能なセキュリティ脆弱性アドバイザリの名前。
CVSS スコア	共通脆弱性評価システム（CVSS）モデルに基づいて評価されたスコア。
Impact	脆弱性がネットワークに及ぼす影響。
CVE	脆弱性の Common Vulnerabilities and Exposures（CVE）識別子。
デバイス	脆弱性の影響を受けるデバイスの数。この特定のアドバイザリに基づいて脆弱性が存在する可能性のあるデバイスを表示するには、番号をクリックし、必要に応じてデバイスをアップグレードします。
Match Type	検出された脆弱性が [Image Version] の一致と [Configuration] の一致のどちらに基づくかを示します。
検出以降の期間（日数)	脆弱性が検出されてからの経過日数。
Last updated	アドバイザリが最後に更新された日付。

ステップ 5 [Advisories] テーブルで、[All] タブをクリックして、すべてのアドバイザリをリストします。

ステップ 6 [Advisories] テーブルで、[Affecting Devices] タブをクリックして、影響するデバイスに基づいたアドバイザリを表示します。

[Devices] テーブルには、[Device Name]、[Device Family]、[Device Series]、[IP Address]、[Advisories]、[Advisories (Suppressed)]、[Platform]、[Image Version]、[Scan Status]、[Scan Criteria]、[Site]、および [Reachability] に基づいてデバイスが一覧表示されます。

ステップ 7 各デバイスに適用可能なアドバイザリの数を表示するには、[Devices] タブをクリックします。

a) デバイスに一致するものをすべて表示するには、アドバイザリの数をクリックします。
b) デバイストポロジを表示するには、右上隅にあるトポロジアイコンをクリックします。トポロジ内のデバイスをクリックすると、デバイスに一致するすべてのアドバイザリが表示されます。

デバイスの横にあるロックアイコンは、デバイスに適用可能な 1 つ以上のアドバイザリがあることを示します。

[Fixed Version] 列には、アドバイザリが適用されたバージョンが表示されます。この列に示されているバージョンにアップグレードすることで、デバイス上のアドバイザリを削除できます。

ステップ 8 [Re-scan Network] をクリックして、ネットワークのスキャンを再度実行します。

ネットワークを再スキャンして、自動構成スキャンに基づいてセキュリティアドバイザリを特定するには、ネットワークを再スキャンしてセキュリティアドバイザリを特定する（766ページ）を参照してください。

セキュリティアドバイザリスキャンのスケジュール設定

ステップ 1 メニューアイコン（☰）をクリックして、**[Tools]** > **[Security Advisories]** の順に選択します。

ステップ 2 [Scan Network] をクリックします。

[Scan Network] ウィンドウが表示されます。

ステップ 3 セキュリティアドバイザリをすぐにスキャンするには、[Now] オプションボタンをクリックし、[Start] をクリックします。

ステップ 4 スキャンを後で実行するようにスケジュールするには、[Later] オプションボタンをクリックし、日付と時刻を指定します。

ステップ 5 [Time Zone] ドロップダウンリストを使用して、スキャンのスケジュール設定に使用するタイムゾーンを選択します。

ステップ 6 繰り返しオプションとして [None]（デフォルト）、[Daily]、[Weekly] のいずれかを選択します。

ステップ 7 [Run at Interval] フィールドに、スキャンの繰り返しの間隔（日または週の数）を入力します。

ステップ 8 （オプション）スケジュールの終了日や終了までの回数を指定する場合は、[Set Schedule End] チェックボックスをオンにします。

a) スキャン終了日をスケジュールするには、[End Date] オプションボタンをクリックし、日付と時刻を定義します。
b) スキャンの繰り返し回数を定義するには、[End After] オプションボタンをクリックします。

ステップ 9 [Schedule] をクリックします。

ステップ 10 メニューアイコン（☰）をクリックして、**[Activities]** > **[Tasks]** の順に選択して、スキャンのスケジュールと繰り返しを確認します。

（注） Cisco DNA Center リリース 2.1.1.x 以降では、シスコによるテレメトリの収集を許可するかどうかを選択できます。収集を許可すると、cisco.com ID、システムテレメトリ、機能使用状況テレメトリ、ネットワーク デバイス インベントリ、およびソフトウェア利用資格の情報が収集されます。テレメトリは、アプリケーションごとや機能ごとではなく、Cisco DNA Center 全体について開示されます。Cisco DNA Center 2.1.1.x 以降では、テレメトリの収集は必須です。収集されたテレメトリは、ユーザーが使用している機能の開発に役立てられます。収集されるデータの詳しいリストについては、「*Cisco DNA Center* のデータシート」を参照してください。

セキュリティ アドバイザリ スキャンの実行時に収集されるテレメトリデータは次のとおりです。

- ナレッジパッケージの自動更新が設定されているかどうか。
- 繰り返しのスキャンおよび繰り返しのレポートが設定されているかどうか。
- 実行されたレポートの数。
- ソフトウェアのバージョンと設定に基づいて一致するセキュリティアドバイザリがあるデバイスの数。
- 各スキャンの受理と拒否の数。
- 検索で入力された手動設定とそれに関連するアドバイザリ。
- ソフトウェアのバージョンと設定（製品ファミリを含む）が一致するアドバイザリの数。
- 他のカテゴリ（アドバイザリなし、不明、サポート対象外）に基づくデバイスの数。
- スキャンの成功、失敗、終了の数。
- 平均スキャン時間。

[Try Cisco CX Cloud Success Track] を有効にして、セキュリティアドバイザリを特定する

始める前に

- CX Cloud に到達するには、Cisco DNA Center のファイアウォールに正しい URL とポートを入力する必要があります。
- Cisco CX Cloud サービスを有効にする必要があります。詳細については、Cisco DNA Center 管理者ガイドの「**Update the Machine Reasoning Knowledge Base**」を参照してください。

ステップ 1 メニューアイコン（☰）をクリックして、**[Tools]** > **[Security Advisories]** > **[Advisories]** の順に選択します。

ステップ 2 [Security Advisories] ウィンドウを初めて起動するときは、[Scan Network] をクリックして、インベントリ内のサポートされているすべてのデバイスのソフトウェアバージョンに基づいた自動スキャンをトリガーします。

ステップ 3 [Security Advisories] ウィンドウの上部にあるバナーで、[Try Cisco CX Cloud Success Track] リンクをクリックして、CX ライセンスの 60 日間の試用を有効にします。

（注） セキュリティアドバイザリの場合、CX ライセンスレベルは Success Track 1 です。

ステップ 4 [Success Tracks] の確認ウィンドウで、[OK] をクリックしてエンドユーザーライセンス契約に同意します。

[Security Advisories] ウィンドウの上部に、CX ライセンスの試用期間の有効性を示すバナーが表示されます。

セキュリティアドバイザリのために呼び出される CLI コマンド

Cisco DNA Center は、ネットワークデバイスで CLI コマンドを実行してネットワークデバイスの構成と運用データを収集し、その情報を CX Cloud に送信して処理され、可能性があるセキュリティアドバイザリやバグのリスクを可視化します。Cisco DNA Center はセキュリティアドバイザリのための次の CLI コマンドを呼び出します。

- **show inventory**
- **show running-config**
- **show version**

ネットワークを再スキャンしてセキュリティアドバイザリを特定する

次の手順では、ネットワークを再スキャンして、自動構成スキャンに基づいてセキュリティアドバイザリを特定する方法について説明します。

始める前に

Cisco CX Cloud サービスを有効にする必要があります。詳細については、Cisco DNA Center 管理者ガイドの「**Update the Machine Reasoning Knowledge Base**」を参照してください。

ステップ 1 メニューアイコン（☰）をクリックして、**[Tools]** > **[Security Advisories]** > **[Advisories]** の順に選択します。

ステップ 2 [Re-Scan Network] をクリックして、ネットワークスキャンを再度開始します。

ステップ 3 セキュリティアドバイザリをすぐに再スキャンするには、[Now] オプションボタンをクリックし、[Start] をクリックします。

ステップ 4 再スキャンを後で実行するようにスケジュールするには、[Later] オプションボタンをクリックし、詳細を指定します。詳細については、セキュリティ アドバイザリ スキャンのスケジュール設定（764 ページ）を参照してください。

[Device] テーブルで、[Advisories] 列がアドバイザリの数で更新されます。

- Cisco DNA Center ネットワークの再スキャンは、プラットフォームの詳細や CX Cloud ソフトウェアのバージョンなどの他の詳細とともに、デバイスの実行コンフィギュレーションを送信します。情報は処理され、Cisco DNA Center に返送されます。Cisco DNA Center 上で実行されている Machine Reasoning Engine（MRE）は、Cisco CX Cloud によって提供されるデバイスに対してアドバイザリをマッピングします。
- Cisco DNA Center で特定のデバイスの正しいライセンスレベルを判断できない場合、セキュリティ アドバイザリ スキャンはソフトウェアバージョンごとのスキャンにフォールバックします。

アドバイザリに対するデバイスの表示/非表示

ステップ 1 メニューアイコン（☰）をクリックして、**[Tools]** > **[Security Advisories]** の順に選択します。

ステップ 2 [Security Advisories] ページを初めて起動する場合は、[Scan Network] をクリックします。

ステップ 3 [Scan Network] ウィンドウで、[Now] を選択し、[Start] をクリックします。

ステップ 4 デバイスのアドバイザリを非表示にするには、次の手順を実行します。

a) [Focus] ドロップダウンリストから、[Advisories] を選択します。

b) [Devices] 列で、デバイスを非表示にするアドバイザリに対応するデバイス数をクリックします。

[Active] タブには、これらのアドバイザリが発行されたデバイスの数が表示されます。

c) 非表示にするデバイスを選択し、[Suppress Device] をクリックします。

非表示にしたデバイスは、[Suppressed] タブで確認できます。

d) アドバイザリウィンドウを閉じ、このアドバイザリのデバイス数の変化を確認します。

ステップ 5 デバイスをアドバイザリに復元するには、次の手順を実行します。

a) [Focus] ドロップダウンリストから、[Advisories] を選択します。

b) [Devices] 列で、デバイスを再表示するアドバイザリに対応するデバイス数をクリックします。

c) [Suppressed] タブをクリックして、非表示のデバイスを表示します。

d) 再表示するデバイスを選択し、[Mark as Active] をクリックします。

復元されたデバイスは、[Active] タブで確認できます。

e) アドバイザリウィンドウを閉じ、このアドバイザリのデバイス数の変化を確認します。

デバイスに対するアドバイザリの表示/非表示

ステップ 1 メニューアイコン（☰）をクリックして、**[Tools]** > **[Security Advisories]** の順に選択します。

ステップ 2 [Security Advisories] ページを初めて起動する場合は、[Scan Network] をクリックします。

ステップ 3 [Scan Network] ウィンドウで、[Now] を選択し、[Start] をクリックします。

ステップ 4 デバイスのアドバイザリを非表示にするには、次の手順を実行します。

a) [Focus] ドロップダウンリストから、[Devices] を選択します。

b) [Advisories] 列で、アドバイザリを非表示にするデバイスに対応するアドバイザリカウントをクリックします。

[Active] タブには、このデバイスに対して発行されたアドバイザリの数が表示されます。

c) 非表示にするアドバイザリを選択し、[Suppress Advisory] をクリックします。

非表示のアドバイザリは、[Suppressed] タブで確認できます。

d) デバイスウィンドウを閉じ、このデバイスのアドバイザリカウントの変化を確認します。

ステップ 5 デバイスのアドバイザリを復元するには、次の手順を実行します。

a) [Focus] ドロップダウンリストから、[Devices] を選択します。

b) [Advisories] 列で、アドバイザリを再表示するデバイスに対応するアドバイザリカウントをクリックします。

c) [Suppressed] タブをクリックして、非表示のアドバイザリを表示します。

d) 再表示するアドバイザリを選択し、[Mark as Active] をクリックします。

復元されたアドバイザリは、[Active] タブで確認できます。

e) デバイスウィンドウを閉じ、このデバイスのアドバイザリカウントの変化を確認します。

新しいセキュリティアドバイザリ KB の通知の追加

セキュリティアドバイザリのナレッジバンドル（KB）は、機械推論エンジン（MRE）を使用してネットワークをスキャンします。新しいセキュリティアドバイザリの KB が利用可能になったときに通知するように Cisco DNA Center を設定できます。通知を有効にすると、新しいセキュリティアドバイザリの KB が利用可能になるたびに、Cisco DNA Center から視覚的な通知と実用的なアラートが表示されます。

次の手順では、新しいセキュリティアドバイザリの KB の通知を追加する方法について説明します。

始める前に

- Cisco DNA Center のコアパッケージをインストールする必要があります。*Cisco DNA Center* 管理者ガイド の「パッケージと更新のダウンロードとインストール」を参照してください。
- 機械推論（MRE）パッケージをインストールする必要があります。*Cisco DNA Center* 管理者ガイド の「パッケージと更新のダウンロードとインストール」を参照してください。
- 次のコンテナがシステムに存在している必要があります。
  - cnsr-reasoner
  - cloud connectivity/download

ステップ 1 Cisco DNA Center GUI の右上隅にある通知アイコンをクリックします。ドロップダウンメニューから、歯車のアイコンを選択して通知設定を表示します。

ステップ 2 [My Profile and Settings] ウィンドウで、[Security Advisories] オプションを選択してセキュリティアドバイザリ通知を有効にします。

ステップ 3 [保存（**Save**）] をクリックします。

ステップ 4 [Machine Reasoning Engine] ウィンドウで、[Download Latest] リンクをクリックして最新のナレッジバンドルをダウンロードします。

ステップ 5 ナレッジベースの設定を確認して更新します。

ステップ 6 [Security Advisory Settings] セクションで、繰り返しオプションとして [None]（デフォルト）、[Daily]、または [Weekly] を選択します。

ステップ 7 **[Notification Center]** > **[Go to Security Advisories]** の順に選択して、[Security Advisories] ツールウィンドウを直接表示します。

ステップ 8 新しくダウンロードしたセキュリティアドバイザリでネットワークを再スキャンします。詳細については、セキュリティ アドバイザリ スキャンのスケジュール設定 （764 ページ）を参照してください。

[Inventory] でのセキュリティアドバイザリの表示

Cisco DNA Center のセキュリティ フォーカス ビューでは、前回のセキュリティスキャンで取得したデータに基づいて、デバイスのセキュリティアドバイザリのリストを表示します。[Security Advisories] ツールから取得したデバイスデータは [Inventory] ウィンドウに表示されます。

次の手順を使用して、セキュリティアドバイザリを表示します。

始める前に

- Cisco DNA Center のコアパッケージをインストールする必要があります。*Cisco DNA Center* 管理者ガイド の「パッケージと更新のダウンロードとインストール」を参照してください。
- 機械推論パッケージをインストールする必要があります。*Cisco DNA Center* 管理者ガイド の「パッケージと更新のダウンロードとインストール」を参照してください。

ステップ 1 メニューアイコン（≡）をクリックして、**[Tools]** > **[Security Advisories]** の順に選択します。

ステップ 2 [Scan Network] をクリックします。

ステップ 3 セキュリティアドバイザリをすぐにスキャンするには、[Now] オプションボタンをクリックし、[Start] をクリックします。

ステップ 4 メニューアイコン（≡）をクリックして、**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。

ステップ 5 [FOCUS: Inventory] ドロップダウンメニューから [Security] を選択します。
[Inventory] テーブルに [Advisories] 列が表示されます。

ステップ 6 [Device Details] ウィンドウで、デバイスを選択し、アドバイザリデータを確認します。

ステップ 7 [Manage All] をクリックして**セキュリティアドバイザリ** ツールに移動します。

一致パターンの追加

ステップ 1 メニューアイコン（≡）をクリックして、**[Tools]** > **[Security Advisories]** の順に選択します。

ステップ 2 [Security Advisories] ページを初めて起動する場合は、[Scan Network] をクリックします。

ステップ 3 [Scan Network] ウィンドウで、[Now] を選択し、[Start] をクリックします。

ステップ 4 アドバイザリを選択し、[Match Type] 列で [Add match pattern] をクリックします。

ステップ 5 [Add Configuration Match Pattern] ウィンドウで、[CONDITIONS] テキストボックスにデバイスと一致する条件を入力します。

ステップ 6 **[保存（Save）]** をクリックします。

一致パターンがアドバイザリに追加されます。

ステップ 7 [Scan Network] をクリックして、一致パターンに一致するデバイスの数を確認します。

一致パターンの AND/OR の定義

ステップ 1 メニューアイコン（≡）をクリックして、**[Tools]** > **[Security Advisories]** の順に選択します。

ステップ 2 [Security Advisories] ページを初めて起動する場合は、[Scan Network] をクリックします。

ステップ 3 [Scan Network] ウィンドウで、[Now] を選択し、[Start] をクリックします。

ステップ 4 アドバイザリを選択し、[Match Type] 列で [Add match pattern] をクリックします。

ステップ 5 [Add Configuration Match Pattern] ウィンドウで、次の手順を実行します。

a) [CONDITIONS] テキストボックスに条件を入力し、[Add] アイコンをクリックします。

b) ドロップダウンリストから、[AND] または [OR] を選択し、次の条件を入力します。

c) 条件を削除する場合は、[Remove] アイコンをクリックします。

d) **[保存（Save）]** をクリックします。
一致パターンがアドバイザリに追加されます。

ステップ 6 [Scan Network] をクリックして、一致パターンに一致するデバイスの数を確認します。

一致パターンの編集

ステップ 1 メニューアイコン（☰）をクリックして、**[Tools]** > **[Security Advisories]** の順に選択します。

ステップ 2 [Security Advisories] ページを初めて起動する場合は、[Scan Network] をクリックします。

ステップ 3 [Scan Network] ウィンドウで、[Now] を選択し、[Start] をクリックします。

ステップ 4 すでに一致パターンがあるアドバイザリを選択し、[Match Type] 列で [Edit match pattern] をクリックします。

ステップ 5 [Edit Configuration Match Pattern] ウィンドウで、[CONDITIONS] テキストボックスにデバイスと一致する条件を入力します。

ステップ 6 **[保存（Save）]** をクリックします。

一致パターンが変更されます。

ステップ 7 [Scan Network] をクリックして、一致パターンに一致するデバイスの数を確認します。

一致パターンの削除

ステップ 1 メニューアイコン（☰）をクリックして、**[Tools]** > **[Security Advisories]** の順に選択します。

ステップ 2 [Security Advisories] ページを初めて起動する場合は、[Scan Network] をクリックします。

ステップ 3 [Scan Network] ウィンドウで、[Now] を選択し、[Start] をクリックします。

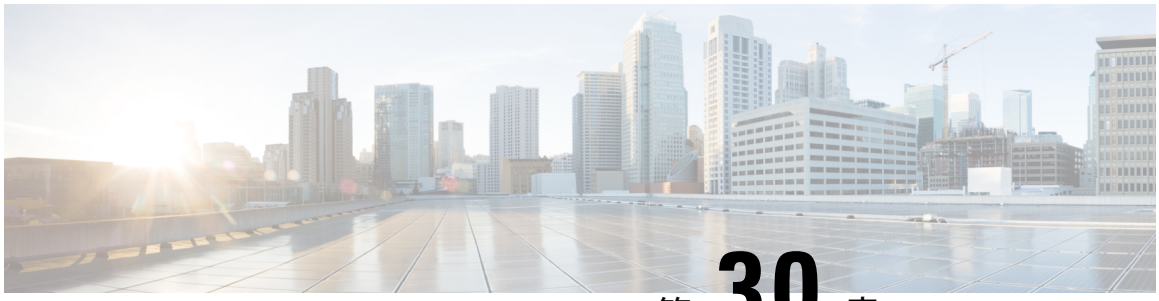
ステップ 4 すでに一致パターンがあるアドバイザリを選択し、[Match Type] 列で [Edit match pattern] をクリックします。

ステップ 5 [Edit Configuration Match Pattern] ウィンドウで、[Delete] をクリックします。

一致パターンが削除されます。

第 VIII 部

ネットワークの保証



第 30 章

Cisco DNA アシュアランス

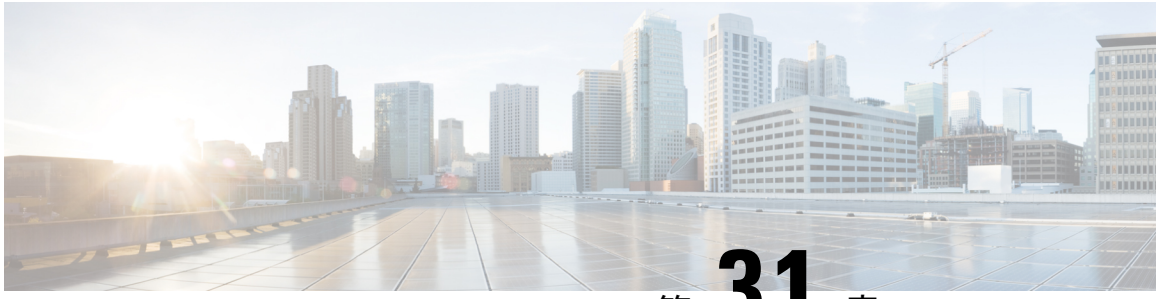
Cisco DNA アシュアランス の概要

Cisco DNA アシュアランス は、Cisco DNA Center から入手可能なアプリケーションです。

ネットワークの正常性、クライアントの正常性、およびアプリケーションの正常性をモニターおよびトラブルシューティングする方法、および NetFlow の収集を有効にする方法など、アシュアランス アプリケーションの詳細については、Cisco DNA Assurance のユーザーガイドを参照してください。

第 IX 部

Cisco DNA Center の管理



第 31 章

構築と展開のワークフロー

Cisco DNA Center ワークフローナビゲーション

Cisco DNA Center ワークフローはウィザードに似ています。ワークフローは GUI に組み込まれており、複雑すぎたり完了するには高度すぎるような多段階のタスクをガイドします。それらの多くには、さまざまなメニューオプションから、または [Workflows] メニューオプションから直接アクセスできます。

次のガイドラインを使用すると、ワークフローのナビゲートに役立ちます。

- ワークフローの手順に従い、[Next] をクリックして次のページに進みます。
- ワークフローの各ページの上部近くにカーソルを合わせると、進行状況バーが表示され、プロセスを完了するためのステップと現在実行中のステップが示されます。
- 一部のワークフローではダイアログボックスが開き、クリックすることでタスクの概要を視覚的に表示できます。タスクの概要の任意の時点で、[Let's Do it] をクリックして、ワークフローの最初に直接ジャンプできます。

  今後タスクの概要をスキップするには、[Don't show this to me again] チェックボックスをオンにします。

AP 更新ワークフロー

ここでは、Cisco DNA Center のワークフローを使用して古いアクセスポイントを新しいアクセスポイントに置き換える方法を説明します。

AP 更新ワークフローの概要

AP 更新機能では、Cisco DNA Center のワークフローを使用して古い AP モデルを新しい AP モデルに置き換えることができます。

AP 更新ワークフローでは、Cisco AireOS ワイヤレスコントローラおよび Cisco Catalyst 9800 シリーズ ワイヤレス コントローラに関連付けられている AP をサポートしています。

- Cisco Aironet 1810 シリーズ OfficeExtend アクセス ポイント
- Cisco Aironet 1810W シリーズ アクセス ポイント
- Cisco Aironet 1815i アクセスポイント
- Cisco Aironet 1815w アクセス ポイント
- Cisco Aironet 1815m アクセスポイント
- Cisco Aironet 1830 シリーズ アクセス ポイント
- Cisco Aironet 1850 シリーズ アクセス ポイント
- Cisco Aironet 1800 シリーズ アクセス ポイント
- Cisco Aironet 2800 シリーズ アクセス ポイント
- Cisco Aironet 3800 シリーズ アクセス ポイント
- Cisco Aironet 4800 シリーズ アクセス ポイント
- Cisco Aironet 1700 シリーズ アクセス ポイント
- Cisco Aironet 2700 シリーズ アクセス ポイント
- Cisco Aironet 3700 シリーズ アクセス ポイント
- Cisco Catalyst 9105 シリーズ Wi-Fi 6 アクセスポイント
- Cisco Catalyst 9115 シリーズ Wi-Fi 6 アクセスポイント
- Cisco Catalyst 9117 シリーズ Wi-Fi 6 アクセスポイント
- Cisco Catalyst 9120 シリーズ Wi-Fi 6 アクセスポイント
- Cisco Catalyst 9124 シリーズ Wi-Fi 6 アクセスポイント
- Cisco Catalyst 9130 シリーズ Wi-Fi 6 アクセスポイント

- Cisco Catalyst 9136 シリーズ Wi-Fi 6 アクセスポイント
- Cisco Catalyst IW6300 シリーズ アクセスポイント

AP 更新ワークフロー

Cisco DNA Center でプロビジョニングされた AP とプロビジョニングされていない AP の両方を新しい AP に置き換えることができます。次の手順では、古い AP を新しい AP に置き換える方法を示します。

始める前に

- 古い AP が到達不能状態であり、サイトに割り当てられていることを確認します。
- 古い AP サイトは、新しい AP が関連付けられるワイヤレスコントローラの管理対象 AP の場所としてプロビジョニングする必要があります。
- 新しい AP は、どのサイトにも割り当てることはできません。
- 新しい AP をシスコ ワイヤレス コントローラに接続する必要があります。新しい AP は、Cisco DNA Center インベントリに登録されているか、プラグアンドプレイ（PnP）を介して Cisco DNA Center に接続する必要があります。到達可能状態である必要があります。

ステップ 1 メニューアイコン（☰）をクリックして、**[Workflows]** > **[Access Point Refresh]** の順に選択します。

ステップ 2 タスクの概要ウィンドウが表示されたら、[Let's Do It] をクリックして、ワークフローに直接移動します。

ステップ 3 [Get Started] ウィンドウで、タスクの一意の名前を入力し、[Next] をクリックします。

ステップ 4 [Select Access Points] ウィンドウで、次の手順を実行します。

1. 左側のペインで、AP を更新するフロアの横にあるチェックボックスをオンにします。
2. 右側のペインで、置き換えるデバイス名の隣にあるチェックボックスをオンにします。

ステップ 5 [Assign New APs to Old APs] ウィンドウで、新しい AP の詳細を提供する方法を選択します。

- GUI を使用して新しい AP の詳細を追加するには、AP の編集アイコン（ ）をクリックします。[Edit details] ウィンドウで、次の操作を行います。

  1. （オプション）新しい AP 名を更新します。
  2. （オプション）[Choose Platform ID] ドロップダウンリストから、新しい AP のプラットフォームを選択します。
  3. [Choose Serial Number] ドロップダウンリストから、新しい AP のシリアル番号を選択します。

     新しい AP がすでにワイヤレスコントローラに関連付けられ、インベントリに登録されている場合、Cisco DNA Center ではその AP のシリアル番号は [Choose Serial Number] ドロップダウンリストに [Managed] として表示されます。

新しい AP が PnP で Cisco DNA Center に接続されている場合、Cisco DNA Center ではその AP のシリアル番号は [Choose Serial Number] ドロップダウンリストに [Unclaimed] として表示されます。

新しい AP のシリアル番号がインベントリに登録されていない場合、そのシリアル番号は [Serial Number] ドロップダウンリストに表示されません。インベントリに登録されていない新しいシリアル番号を追加するには、[Choose Serial Number] ドロップダウンリストでシリアル番号を入力して [+] をクリックします。

4. [Save] をクリックします。

- コンマ区切り値（CSV）ファイルを使用して新しい AP の詳細を追加するには、次の手順を実行します。

1. [Download CSV] をクリックします。ダウンロードした CSV テンプレートファイルには、古い AP の詳細が含まれています。デバイス名を更新し、新しい AP のシリアル番号を追加します。
2. CSV ファイルをインポートするには、[Upload CSV] をクリックします。[Upload CSV] ウィンドウで、CSV ファイルをドラッグアンドドロップ領域にドラッグアンドドロップするか、[Choose a file] をクリックして CSV ファイルの場所を参照し、[Open] をクリックします。

   Cisco DNA Center で検証チェックが実行されます。アップロードした CSV ファイルが要件を満たしていない場合は、エラーメッセージが表示されます。[View Details] をクリックすると、エラーメッセージの詳細が表示されます。
3. [Upload] をクリックします。

ステップ 6 [Configuration Copied from Old Access Point to New] ウィンドウで、古い AP から新しい AP にコピーされる設定を表示します。

ステップ 7 [Resolve Dependencies] ウィンドウに依存関係が表示される場合は、依存関係を解決してから新しい AP のプロビジョニングを行います。

（注） Cisco DNA Center で検証チェックが実行され、エラーがある場合は表示されます。続行する前に、これらのエラーを修正します。

新しい AP をプロビジョニングする前に、次の依存関係を解決します。

- cisco.com のログイン情報を入力してデバイスの EULA に同意します。
- シスコ ワイヤレス コントローラ ソフトウェア イメージ バージョンを更新します。この検証によって AP の更新が中止されることはありません。
- [AP Connected SwitchPort]：この検証メッセージによって AP の更新が中止されることはありません。

ステップ 8 [Schedule Access Point Refresh Task] ウィンドウで、[Now] をクリックします。または [Run Later] をクリックして AP 更新タスクを後の日時にスケジュールします。

ステップ 9 [Summary] ウィンドウで概要を確認し、[Provision] をクリックします。

ステップ 10 [Track Replacement Status] 画面で AP 交換ステータスをモニターします。

AP 交換ステータスの詳細を確認するには、[View Details] をクリックします。

- AP の交換に成功した場合、[Replacement Status] ウィンドウの [Replacement Status] に [REPLACED] と表示されます。
- AP の交換に失敗した場合、[Replacement Status] に [Error] と表示されます。
- 交換エントリを削除するには、[Actions] 列で青色の 3 つのドットをクリックし、[Delete] をクリックします。[Warning] ダイアログボックスで、[Yes] をクリックします。
- プロビジョニングの概要を CSV ファイルにダウンロードしてローカルに保存するには、[Export] をクリックします。
- プロビジョニング ステータス レポートをダウンロードするには、[Download Report] をクリックします。

（注） 新しい AP がインベントリでまだ検出されておらず、対応する AP 更新エントリが新しいデバイスの接続を待機している場合、または PnP 要求プロセスが進行中の場合は、シスコ ワイヤレス コントローラを再同期します。

ステップ 11 [Next] をクリックして、更新の概要を表示します。

ステップ 12 交換が正常に完了すると、Cisco DNA アシュアランス で古い AP と新しい AP についての AP 更新イベントが生成されます。

AP 更新イベントは、[AP View 360] ウィンドウの [Event Viewer] で確認できます。

Cisco DNA Center では、[Network Hierarchy] ウィンドウの対応するフロアマップで、新しい AP が自動的に更新されます。

ユーザー定義ネットワークの設定ワークフロー

ここでは、Cisco DNA Center でワークフローを使用して Cisco ユーザー定義のネットワークサービスを設定する方法を示します。

ユーザー定義のネットワークサービスの概要

プリンタ、スピーカー、Apple TV、Google Chromecast、リングドアベル、スマート電球など、ネットワーク上のホームデバイス、コンシューマデバイス、IoT デバイスは、デバイスの検出と使用が簡単になるように、Apple Bonjour などの Simple Service Discovery Protocol（SSDP）、マルチキャスト DNS（mDNS）、ユニバーサル プラグ アンド プレイ（UPnP）に依存しています。

シスコのユーザー定義ネットワークサービスは、寮の部屋、学生寮、教室、講堂などの共有環境において、クライアントデバイスのセキュアでリモートのオンボーディングを提供します。ユーザー定義のネットワークサービスを使用すると、SSDP（Apple Bonjour など）、mDNS プロトコル（AirPlay、AirPrint、画面ミラーリング、印刷など）、UPnP プロトコルのセキュアな

使用が可能になり、共有環境におけるやり取りや共有を登録されたデバイスのみで行えるようになります。

ユーザー定義のネットワークサービスは、次のソリューションを提供します。

- クライアントデバイスの簡単でセキュアなオンボーディング。
- 特定のユーザーに属するクライアントデバイスの自動セグメンテーション。
- 他のユーザーを招待してデバイスを共有する機能。

サポートされる Cisco DNA Center、Cisco Identity Services Engine、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のソフトウェアバージョンとアクセスポイントは次のとおりです。

- Cisco DNA Center リリース 1.3.1.2 以降
- Cisco Identity Services Engine リリース 2.7 以降
- Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ リリース 17.1.x
- Cisco 802.11ac Wave 2 AP：
    - Cisco Aironet 1810 シリーズ OfficeExtend アクセス ポイント
    - Cisco Aironet 1810W シリーズ アクセス ポイント
    - Cisco Aironet 1815i アクセスポイント
    - Cisco Aironet 1815w アクセスポイント
    - Cisco Aironet 1815m アクセスポイント
    - Cisco 1830 Aironet シリーズ アクセスポイント
    - Cisco Aironet 1850 シリーズ アクセス ポイント
    - Cisco Aironet 2800 シリーズ アクセス ポイント
    - Cisco Aironet 3800 シリーズ アクセス ポイント
    - Cisco Aironet 4800 シリーズ アクセス ポイント
- Cisco 802.11ac Wave 1 AP：
    - Cisco Aironet 1700 シリーズ アクセス ポイント
    - Cisco Aironet 2700 シリーズ アクセス ポイント
    - Cisco Aironet 3700 シリーズ アクセス ポイント

ユーザー定義のネットワークサービスを設定するための前提条件

Cisco ユーザー定義のネットワークサービスを設定する前に、次の前提条件を満たしている必要があります。

- AP が シスコ ワイヤレス コントローラ に参加していることを確認します。
- 検出されたデバイスが [Inventory] ウィンドウに一覧表示されるように、[Discovery] 機能を使用してネットワーク内の シスコ ワイヤレス コントローラと AP を検出します。
- AAA サーバー クライアント エンドポイントを Cisco Identity Services Engine にマッピングします。
- 認証トークンを Cisco DNA Center に追加します。
- 非ファブリック エンタープライズ SSID またはゲストワイヤレス SSID を任意のセキュリティで作成し、ネットワークプロファイルにマッピングします。
- SSID をプロビジョニングします。

Cisco ユーザー定義のネットワークの設定

この手順は、ワークフローを使用して Cisco User Defined Network（UDN）を構成する方法を示しています。

ステップ 1 メニューアイコン（☰）をクリックして、 **[Workflows]** > **[Configure Cisco UDN]** の順に選択します。

Cisco UDN は、**[Provision]** > **[Services]** > **[Cisco User Defined Network]** からも設定できます。

ステップ 2 タスクの概要ウィンドウが開いたら、[Let's Do It] をクリックして、ワークフローに直接移動します。

a) [Click here] をクリックします。

[Cloud Authentication] ウィンドウが開きます。

b) [Where did I get my token encryption key?] をクリックし、ダイアログボックスで [Go to the Portal] をクリックします。

[Cisco DNA - Cloud] アプリケーションが新しいタブで開きます。

c) Cisco.com アカウントの ID とパスワードを使用して [Cisco DNA - Cloud] にログインします。

[Cisco DNA - Cloud] ホームウィンドウが表示され、自身のリージョンのサブスクライブしているオファーがカードとして示されます。

ステップ 3 Cisco DNA Center が Cisco DNA Cloud に接続できるようにするには、Cisco DNA Cloud ポータルを使用して認証トークンを生成します。

a) [Cisco DNA - Cloud] GUI で [On-Prem Connections] を選択して、メニューアイコン（☰）をクリックして、 クラウドサブスクリプションに Cisco DNA Center を登録します。

デフォルトでは、[ALL] タブが開き、青いチェックマークで強調表示されます。[ALL] タブまたは [Cisco DNA Center] タブから登録できます。

（注） Cisco DNA - Cloud ポータルで Cisco DNA Center の登録が断続的に失敗する。これは、すべてのリージョンで Cisco DNA - Cloud から Cisco DNA Center への通信障害が原因で、1 回おきの登録解除で発生する断続的な問題です。

b) [ALL] タブから登録するには、次の手順を実行します。

- [Register Product] をクリックします。

  [Register Product] スライドインペインが表示されます。

- [Product Name] フィールドに、名前を入力します。
- [Product Type] ドロップダウン リストから、[Cisco DNA Center] を選択します。
- [Region] ドロップダウンリストから、オンプレミスの Cisco DNA Center の場所を選択します。
- [Register] をクリックします。
- Cisco DNA Center が正常に登録されると、[OTP Generated] ダイアログボックスが表示されます。OTP をコピーするには、[Copy] をクリックし、[close] をクリックします。

c) または、次の手順に従って [Cisco DNA Center] タブから登録することもできます。

- [Register Cisco DNA Center] をクリックして、シスコとそのパートナーが提供する関連クラウドアプリケーションとサービスに製品を安全に接続します。

  [Register Cisco DNA Center] スライドインペインが表示されます。

- [Cisco DNA Center Name] フィールドに、オンプレミスの Cisco DNA Center の名前を入力します。
- [Region] ドロップダウンリストから、Cisco DNA Center の場所を選択します。
- [OTP Generated] ダイアログボックスで、[Copy] をクリックして OTP をコピーし、[close] をクリックします。

ステップ 4 [Cloud Authentication] ウィンドウに戻り、接続を確立します。

a) Cisco DNA Center GUI でメニューアイコン（☰）をクリックして、[System] > [Settings] > [External Services] > [Cloud Authentication] の順に選択します。
b) [Cloud Authentication] で、[Add OTP Key] をクリックします。
c) [OTP Code] フィールドに、 Cisco DNA - Cloud アプリケーションで生成してコピーした OTP を貼り付け、[Done] をクリックします。
d) [Success] ダイアログボックスが表示されます。[OK] をクリックします。

ステップ 5 **Cisco DNA Center** と **Cisco DNA - Cloud** 間の接続が確立されたかどうかを、**[Cisco DNA - Cloud]** > **[On-Prem Connections]**ウィンドウで確認します。

登録が成功すると、[Registration Status] 列にステータスが [Registered] と表示されます。

ステップ 6 サイトを有効にし、ネットワーク上で Cisco UDN サービスをプロビジョニングします。

a) Cisco DNA Center の [Welcome to Cisco User Defined Network] ウィンドウに戻ります。
b) [Next] をクリックします。
c) [Select Sites] ウィンドウで、次を実行します。

- [Select Sites] ドロップダウンリストから、Cisco UDN サービスを有効にするサイトを選択します。

d) [SSID] ウィンドウで、次の手順を実行します。

- [SSID] ドロップダウンリストから、Cisco UDN サービスを有効にする SSID を選択します。
- 選択した SSID のユニキャストトラフィックを制限するには、[Unicast Traffic Containment] をオンにします。
- ユニキャストトラフィックの封じ込めを特定のサイトに適用するには、[Apply Individually] をクリックします。
- ユニキャストトラフィックの封じ込めをすべてのサイトに適用するには、[Apply to all] をクリックします。
- [次へ（Next）] をクリックします。

ステップ 7 [Scheduling] ウィンドウで、[Now] または [Later] をクリックして、Cisco UDN サービスをいつプロビジョニングするかを指定します。

[Next] をクリックします。

ステップ 8 [Summary] ウィンドウで、設定の詳細を確認します。

a) 設定を編集するには、対応する [Edit] ボタンをクリックします。

b) [Connection Status] エリアを展開して、Cisco DNA Center と Cisco UDN Cloud 間の接続ステータスを表示します。

Cisco DNA Center と Cisco UDN Cloud 間の接続が確立されると、「Paired with Cisco DNA - Cloud」という成功メッセージが表示されます。

c) [Configure] をクリックします。

次のウィンドウでは、完了した順に各ステップの横にチェックマークが表示されます。

スイッチでのアプリケーション ホスティングの有効化

次の手順は、ThousandEyes Enterprise Agent、iPerf などの Docker アプリケーションを特定のサイトの選択したスイッチで有効にする方法を示します。

始める前に

- 前提条件を満たします。詳細については、「アプリケーション ホスティングの前提条件（573 ページ）」を参照してください。
- アプリケーションを Cisco DNA Center に追加します。詳細については、「アプリケーションの追加 （574 ページ）」を参照してください。
- アプリケーションをホストするためのスイッチの準備状況を確認します。詳細については、「アプリケーションをホストするデバイスの準備状況の表示 （574 ページ）」を参照してください。

ステップ 1 メニューアイコン（☰）をクリックして、**[Provision]** > **[App Hosting for Switches]** の順に選択します。

ステップ 2 アプリケーションを選択し、ウィンドウの下部にある [Install] をクリックします。

または、**[Workflows]** > **[Enable Apps on Switches]** > **[Let's Do it]** を選択してワークフローを起動することもできます。

（注） ウィンドウの上部にある青色の進捗状況バーにカーソルを合わせると、一覧表示される前の手順に戻ることができます。

ステップ 3 [Select Site] ウィンドウで、アプリケーションを有効にするビルディングに移動します。

ステップ 4 [Select App] ウィンドウで、選択するアプリケーションをクリックします。

（注） [+ New App] リンクにアクセスして、Cisco DNA Center に存在しないアプリケーションを追加できます。

ステップ 5 [Select Switches] ウィンドウで、アプリケーションを有効にするデバイス名の横にあるチェックボックスをオンにします。

（注） [Select Switches] ダイアログボックスで指定したテンプレートに詳細を入力することにより、デバイスを一括でインポートまたはエクスポートできます。

ステップ 6 [Configuration App] ウィンドウで、以降の設定を実行します。

- **App Networking**
  - [Device Network]：[Select Network] ドロップダウンリストから、アプリケーションを設定する VLAN を選択します。
  - [App IP address]：[Address Type] ドロップダウンリストから [Static] または [Dynamic] を選択します。[Static] を選択した場合は、サムネイルアイコンをクリックして、アプリケーションの [IP Address]、[Gateway]、[Prefix/Mask]、および [DNS] を入力します。
- [Resource Allocation]：[Allocate resources as asked by the app] または [Allocate all resources available on a device] チェックボックスをオンにします。
- [Custom Settings]：（Cisco パッケージアプリケーションにのみ適用）アプリケーションによって指定された属性の設定の詳細を入力します。
- [App Data]：アプリケーション固有のファイルを参照してアップロードします。必要なアプリケーション固有のファイルを特定するには、関連するアプリケーションのドキュメントを参照してください。
- [Docker Runtime Options]：アプリケーションに必要な Docker ランタイムオプションを入力します。

ステップ 7 [Summary] ウィンドウで、選択したスイッチにアプリケーションをインストールする前に詳細を確認し、[Next] をクリックします。

[Provisioning Task] ウィンドウに、スイッチでのアプリケーションの展開を追跡するタスク名が表示されます。

ステップ 8 自動生成されたタスク名を確認し、[Provision] をクリックします。

ステップ 9 [Track Provisioning Status] ウィンドウで展開の進捗状況を追跡できます。

ステップ 10 [View Details] をクリックして、個々のデバイスのプロビジョニングステータスと障害を確認し（ある場合）、[Next] をクリックします。

アプリケーションが正常に有効化されました。

タスクの結果の概要と成功/失敗の回数が表示されます。

ステップ 11 [Manage App] をクリックします。ここで、アプリケーションのライフサイクル動作を管理して、N 日目のタスクを実行することができます。

IoT サービスの有効化ワークフロー

ここでは、Cisco DNA Center の [Workflows] を使用して、Cisco Catalyst 9100 シリーズ アクセス ポイントで Bluetooth、Zigbee、ESL などの IoT テクノロジーを有効にする方法について説明します。

Cisco Catalyst 9100 シリーズ アクセス ポイントでの IoT サービスの有効化

この手順では、選択した Catalyst 9100 シリーズ アクセスポイントで、Bluetooth、Zigbee、ESL などの IoT テクノロジーを有効にする方法を説明します。

ステップ 1 メニューアイコン（☰）をクリックして、[Workflows] > [Enable IOT Services] の順に選択します。

ステップ 2 タスクの概要ウィンドウが開いたら、[Let's Do It] をクリックして、ワークフローに直接移動します。

ステップ 3 [Select Site] ウィンドウで、IoT サービスを有効にするフロアまで移動し、[Next] をクリックします。

ステップ 4 [Select the Application] ウィンドウで、ネットワークで IoT を有効にするための SES-imagotag ESL Connector アプリケーションを選択し、[Next] をクリックします。

（注） Cisco DNA Center に存在しないアプリケーションを追加するには、「アプリケーションの追加」を参照してください。

[Select Access Points] ウィンドウには、特定のフロアで使用可能なすべての AP が表示されます。

ステップ 5 [Select Access Points] ウィンドウで、IoT コネクタアプリケーションをインストールするデバイスの [Device Name] の横にあるチェックボックスをオンにして、[Next] をクリックします。

ステップ 6 [Summary] ウィンドウで、選択した AP にアプリケーションをインストールする前に詳細を確認し、[Next] をクリックします。

ステップ 7 [Provisioning Task] ウィンドウが表示され、AP への任意のアプリケーションの展開を追跡するために作成されたタスク名が表示されます。自動生成されたタスク名を確認し、[Provision] をクリックします。

ステップ 8 [Track Provisioning Status] ウィンドウで展開の進捗状況を追跡できます。[View Details] をクリックして、プロビジョニングステータスを確認し、[Next] をクリックします。

ステップ 9 タスク完了[Done! Task Completed] ウィンドウが表示されます。[Manage IoT Application] をクリックして、Day N タスクを実行します。

IoT アプリケーションの管理

この手順では、IoT アプリケーションを管理する方法を示します。

始める前に

Cisco Catalyst 9000 シリーズ アクセス ポイントで IoT サービスを有効にしておく必要があります。

ステップ 1 IoT サービスを有効にした後、[Done! Task Completed] ウィンドウで [Manage IoT Application] をクリックします。

ステップ 2 [Hostname] の横にあるチェックボックスをオンにして、次のタスクを実行します。

- アプリケーションを起動するには、[Actions] ドロップダウンリストから [Start App] を選択します。
- アプリケーションを停止するには、[Actions] ドロップダウンリストから [Stop App] を選択します。
- アプリケーション設定を編集するには、[Actions] ドロップダウンリストから [Edit App Config] を選択します。
- アプリケーションをアップグレードするには、[Actions] ドロップダウンリストから [Upgrade App] を選択します。
- 選択した AP からアプリケーションをアンインストールするには、[Actions] ドロップダウンリストから [Uninstall App] を選択します。

ステップ 3 AP 名をクリックすると、次の詳細が表示されます。

- **AP 名**
- **AP ステータス**
- **IP Address**
- **ヘルス（Health）**

ステップ 4 [Tech Support logs] をクリックして、アプリケーション ホスティング ログを収集します。

Cisco DNA Center での AP 設定

[Configure Access Points] ワークフローでは、次のことができます。

- Cisco DNA Center での AP レベルおよび無線レベルのパラメータの設定および展開
- AP の定期的なイベントのスケジュール

次の AP レベルのパラメータを設定できます。

- AP の位置
- AP 管理ステータス
- AP モード
- AP LED ステータス
- LED の明るさレベル
- AP の高さ
- AP フェールオーバー優先度
- ハイ アベイラビリティ

次の無線レベルのパラメータを設定できます。

- 無線管理ステータス
- 無線出力の設定
- 無線チャンネルの設定
- CleanAir またはスペクトルインテリジェンスの設定
- アンテナの設定
- 水平
- Elevation

AP ワークフローの設定

この手順では、Cisco DNA Center で AP および無線パラメータを設定する方法を示します。

ステップ 1 メニューアイコン（☰）をクリックして、**[Workflows]** > **[Configure Access Points]** の順に選択します。

ステップ 2 タスクの概要ウィンドウが開いたら、[Let's Do It] をクリックして、ワークフローに直接移動します。

ステップ 3 [Get Started] ウィンドウで、[Task Name] フィールドにワークフローの一意の名前を入力し、[Next] をクリックします。

ステップ 4 [How do you want to configure APs?] ウィンドウで、次の操作を行います。

a) [Configure AP And Radio Parameters] オプションボタンをクリックします。

b) 設定するステップの横にあるチェックボックスをオンにします。

- **[Modify AP Name]**
- [Configure AP Parameters]
- [Configure 5 GHz Radio Parameters]
- [Configure 2.4 GHz Radio Parameters]
- [Configure 6 GHz Radio Parameters]
- [Configure Dual-Band (XOR) Radio Parameters]

（注） このウィンドウでオンにしたチェックボックスに基づいて、Cisco DNA Center では対応する後続の構成手順が表示されます。

c) [Next] をクリックします。

ステップ 5 [Select Access Points] ウィンドウで、次の手順を実行します。

a) AP 関連の設定を適用するサイトに移動します。

右側のペインに、選択したサイトで使用可能なすべての AP が一覧表示されます。

b) 設定する AP 名の横にあるチェックボックスをオンにします。

c) [Next] をクリックします。

ステップ 6 （オプション）[Modify AP Name] ウィンドウで、AP 名を変更します。

次のいずれかの方法を使用して AP の新しい名前を入力します。

a) [Create a New Naming Convention]：このオプションボタンをクリックして、命名規則に基づいて名前を入力し、[Apply Pattern] をクリックします。[Access Points] テーブルには、入力した命名パターンに基づいて新しい AP 名が表示されます。

b) [Upload a CSV file]：このオプションボタンをクリックして、サンプル CSV テンプレートファイルをダウンロードし、そのファイルに AP 名を追加します。次に、CSV ファイルをドラッグしてドロップエリアにドロップすることにより、または [Choose a file] をクリックし、CSV ファイルを参照して選択することにより、ファイルをアップロードします。

ステップ 7 （オプション）[Configure AP Parameters] ウィンドウで、AP パラメータを設定します。

次の AP パラメータを設定します。

- [Admin Status]：管理ステータスを無効にするには、このチェックボックスをオンにして、[Disable] をクリックします。
- [AP Mode]：このチェックボックスをオンにして、[Select AP Mode] ドロップダウンリストから AP モードを選択します。有効なモードは、[Local/Flexconnect]、[Monitor]、[Sniffer]、および [Bridge/Flex+Bridge] です。

（注） AP モードを [Monitor] または [Sniffer] から [Local/Flexconnect] に変更すると、Cisco DNA Center では次の設定が使用されます。

関連付けられた SSID で [FlexConnect Local Switching] が有効になっている場合は、Cisco DNA Center では AP に [FlexConnect] モードが設定されます。それ以外の場合は、AP に [Local] モードが設定されます。

割り当てられていない AP または割り当てられているがプロビジョニングされていない AP の場合、Cisco DNA Center では AP に [FlexConnect] モードが設定されます。

- Cisco AireOS ワイヤレスコントローラ：AP が存在する AP グループ内の関連付けられた SSID で FlexConnect ローカルスイッチングが有効になっている場合
- Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ：AP の現在関連付けられているサイトタグで Local サイトが無効になっている場合

- [AP Location]：このチェックボックスをオンにすると、[Enter Location] フィールドに AP の場所の詳細を入力できます。

  現在割り当てられているサイトを AP の場所として使用するには、[Use currently assigned site location] チェックボックスをオンにします。このチェックボックスをオンにすると、[Enter Location] フィールドが無効になります。

  （注） どのサイトにも割り当てられていない AP の場合、[Use currently assigned site location] チェックボックスをオンにしても、Cisco DNA Center に AP ロケーションは設定されません。

- [AP LED Status]：AP LED ステータスを無効にするには、このチェックボックスをオンにして、[Disable] をクリックします。
- [LED Brightness Level]：このチェックボックスをオンにして、[LED Brightness Level] から明るさのレベルを選択します。
- [AP Height]：このチェックボックスをオンにして、AP の高さをフィートで入力します。Cisco DNA Center での最小の高さは 3 フィートです。

  （注） Cisco DNA Center で AP がフロアに割り当てられたときに、AP の高さが AP に適用されます。AP の高さがフロアの高さを超えないようにしてください。

- [AP Failover Priority]：このチェックボックスをオンにして、[AP Failover Priority] ドロップダウンリストから AP のフェールオーバー優先順位を選択します。有効なオプションは次のとおりです。
  - [Low]：AP にプライオリティレベル 1 を割り当てます。これは最も低いプライオリティレベルです。これはデフォルト値です。
  - [Medium]：AP にプライオリティレベル 2 を割り当てます。
  - [High]：AP にプライオリティレベル 3 を割り当てます。
  - [Critical]：AP にプライオリティレベル 4 を割り当てます。これは最も高いプライオリティレベルです。

- [High Availability]：このチェックボックスをオンにして、APのプライマリ、セカンダリ、およびターシャリコントローラの名前と IP アドレスを設定します。

  プライマリコントローラとセカンダリコントローラに対して [Inherit from site / Clear] を選択した場合：

  - プロビジョニングされた状態の AP の場合、AP が割り当てられているフロアのプライマリおよびセカンダリとして設定されたコントローラが、APのプライマリおよびセカンダリコントローラとして設定されます。
  - プロビジョニングされた状態にないAPの場合、現在のプライマリ、セカンダリコントローラの情報が AP から消去されます。

  ターシャリコントローラの場合、[Clear] オプションのみが使用可能です。

  （注） コントローラで AP フォールバックが無効になっている場合、AP は新しく設定されたプライマリ、セカンダリ、およびターシャリコントローラに参加しません。

  （注） AP が ROW AP の場合は、コントローラの国のリストに、運用国のサポートが追加されていることを確認してください。コントローラの管理対象 AP ロケーションとして、運用国の少なくとも 1 つのサイトを設定する必要があります。

ステップ 8 （オプション）[Configure 5 GHz Radio Parameters] ウィンドウで、5 GHz 無線パラメータを設定します。

次の 802.11 a/n/ac/ax パラメータを設定します。

- [Admin Status]：管理ステータスを無効にするには、このチェックボックスをオンにして、[Disable] をクリックします。
- [Power Assignment]：カスタム電力値を選択するには、このチェックボックスをオンにして [Custom] をクリックします。[Select Custom Power] ドロップダウンリストから電力レベルを選択します。
- [Channel Assignment]：カスタムチャネル番号を選択するには、このチェックボックスをオンにして [Custom] ボタンをクリックします。[Select Custom Channel] ドロップダウンリストからカスタムチャネル番号を選択します。
- [Channel Width]：チャネル幅を選択するには、このチェックボックスをオンにし、[Select Channel Width] ドロップダウンリストからいずれかのチャネル帯域幅オプションを選択します。
  - **20 MHz**
  - **40 MHz**
  - **80 MHz**
  - **160 MHz**
- [CleanAir / Spectrum Intelligence]：CleanAir スペクトルインテリジェンスを無効にするには、このチェックボックスをオンにして [Disable] をクリックします。
- [Antenna Name]：アンテナ名を選択するには、このチェックボックスをオンにして、[Select Antenna Name] ドロップダウンリストからアンテナ名を選択します。アンテナ名として [Other] を選択した場

合は、[Antenna Gain(in dBi) (for Antenna-Other)] フィールドにアンテナゲイン値を入力します。外部アンテナの性能を指定する数値を入力し、領域に無線エネルギーを向けたり、収束させたりします。高ゲイン アンテナの放射パターンは、特定の方向により収束したものになります。アンテナゲイン値は 0 ー 40 です。

- [Antenna Cable]：アンテナケーブルを選択するには、このチェックボックスをオンにして、[Select Antenna Cable] ドロップダウンリストからアンテナケーブルを選択します。アンテナケーブルとして [Other] を選択した場合は、[Cable Loss (in dBi) (for Cable-Other)] フィールドにケーブル損失値を入力します。ケーブル損失値は 0 ～ 40 です。
- [Azimuth]：方位角を指定するには、このチェックボックスをオンにして、方位角方向の値を度数で入力します。方位角は、x 軸に対して測定されたアンテナの角度です。方位角の範囲は 0 ー 360 です。
- [Elevation]：仰角を指定するには、このチェックボックスをオンにし、仰角方向の値を度数で入力します。仰角方向の範囲は 0 ー 90 です。[Up] および [Down] トグルボタンを使用して、方向を指定します。

ステップ 9 （オプション）[Configure 2.4 GHz Radio Parameters] ウィンドウで、2.4 GHz 無線パラメータを設定します。

次の 802.11 b/g/n パラメータを設定します。

- [Admin Status]：管理ステータスを無効にするには、このチェックボックスをオンにして、[Disable] をクリックします。
- [Power Assignment]：カスタム電力値を選択するには、このチェックボックスをオンにして [Custom] をクリックします。[Select Custom Power] ドロップダウンリストから電力レベルを選択します。
- [Channel Assignment]：カスタムチャネル番号を選択するには、このチェックボックスをオンにして [Custom] ボタンをクリックします。[Select Custom Channel] ドロップダウンリストからカスタムチャネル番号を選択します。
- [CleanAir / Spectrum Intelligence]：CleanAir スペクトルインテリジェンスを無効にするには、このチェックボックスをオンにして [Disable] をクリックします。
- [Antenna Name]：アンテナ名を選択するには、このチェックボックスをオンにして、[Select Antenna Name] ドロップダウンリストからアンテナ名を選択します。アンテナ名として [Other] を選択した場合は、[Antenna Gain(in dBi) (for Antenna-Other)] フィールドにアンテナゲイン値を入力します。外部アンテナの性能を指定する数値を入力し、領域に無線エネルギーを向けたり、収束させたりします。高ゲイン アンテナの放射パターンは、特定の方向により収束したものになります。アンテナゲイン値は 0 ー 40 です。
- [Antenna Cable]：アンテナケーブルを選択するには、このチェックボックスをオンにして、[Select Antenna Cable] ドロップダウンリストからアンテナケーブルを選択します。アンテナケーブルとして [Other] を選択した場合は、[Cable Loss (in dBi) (for Cable-Other)] フィールドにケーブル損失値を入力します。ケーブル損失値は 0 ～ 40 です。

- [Azimuth]：方位角を指定するには、このチェックボックスをオンにして、方位角方向の値を度数で入力します。方位角は、x 軸に対して測定されたアンテナの角度です。方位角の範囲は 0 ー 360 です。
- [Elevation]：仰角を指定するには、このチェックボックスをオンにし、仰角方向の値を度数で入力します。仰角方向の範囲は 0 ー 90 です。[Up] および [Down] トグルボタンを使用して、方向を指定します。

ステップ 10 （オプション）[Configure 6 GHz Radio Parameters] ウィンドウで、6 GHz 無線パラメータを設定します。

次のパラメータを設定します。

- [Admin Status]：管理ステータスを無効にするには、このチェックボックスをオンにして、[Disable] をクリックします。
- [Radio Role Assignment]：無線の役割を選択するには、このチェックボックスをオンにして、[Auto]、[Client-Serving]、または [Monitor] ボタンをクリックします。
- [Power Assignment]：カスタム電力値を選択するには、このチェックボックスをオンにして [Custom] をクリックします。[Select Custom Power] ドロップダウンリストから電力レベルを選択します。
- [Channel Assignment]：カスタムチャネル番号を選択するには、このチェックボックスをオンにして [Custom] ボタンをクリックします。[Select Custom Channel] ドロップダウンリストからカスタムチャネル番号を選択します。
- [Channel Width]：チャネル幅を選択するには、このチェックボックスをオンにし、[Select Channel Width] ドロップダウンリストからいずれかのチャネル帯域幅オプションを選択します。
  - **20 MHz**
  - **40 MHz**
  - **80 MHz**
  - **160 MHz**
- [Azimuth]：方位角を指定するには、このチェックボックスをオンにして、方位角方向の値を度数で入力します。方位角は、x 軸に対して測定されたアンテナの角度です。方位角の範囲は 0 ー 360 です。
- [Elevation]：仰角を指定するには、このチェックボックスをオンにし、仰角方向の値を度数で入力します。仰角方向の範囲は 0 ー 90 です。[Up] および [Down] トグルボタンを使用して、方向を指定します。

ステップ 11 （オプション）[Configure Dual-Band (XOR) Radio Parameters] ウィンドウで、デュアルバンド（XOR）無線パラメータを設定します。

a) 次の AP でデュアルバンド（XOR）無線パラメータを設定できます。

- Cisco Aironet 2800 シリーズ アクセス ポイント
- Cisco Aironet 3800 シリーズ アクセス ポイント

- Cisco Aironet 4800 シリーズ アクセス ポイント
- Cisco Catalyst 9100 アクセスポイント

b) 次のパラメータを設定します。

- [Admin Status]：管理ステータスを無効にするには、このチェックボックスをオンにして、[Disable] をクリックします。
- [Radio Role Assignment]：無線の役割を選択するには、このチェックボックスをオンにして、[Auto]、[Client-Serving]、または [Monitor] ボタンをクリックします。無線帯域の必要なオプションをクリックします。
- [Power Assignment]：カスタム電力値を選択するには、このチェックボックスをオンにして [Custom] をクリックします。[Select Custom Power] ドロップダウンリストから電力レベルを選択します。
- [Channel Assignment]：カスタムチャネル番号を選択するには、このチェックボックスをオンにして [Custom] ボタンをクリックします。[Select Custom Channel] ドロップダウンリストからカスタムチャネル番号を選択します。
- [Channel Width]：チャネル幅を選択するには、このチェックボックスをオンにし、[Select Channel Width] ドロップダウンリストからいずれかのチャネル帯域幅オプションを選択します。
  - **20 MHz**
  - **40 MHz**
  - **80 MHz**
  - **160 MHz**
- [CleanAir]：CleanAir スペクトルインテリジェンスを無効にするには、このチェックボックスをオンにして [Disable] をクリックします。
- [Antenna Name]：アンテナ名を選択するには、このチェックボックスをオンにして、[Select Antenna Name] ドロップダウンリストからアンテナ名を選択します。アンテナ名として [Other] を選択した場合は、[Antenna Gain(in dBi) (for Antenna-Other)] フィールドにアンテナゲイン値を入力します。外部アンテナの性能を指定する数値を入力し、領域に無線エネルギーを向けたり、収束させたりします。高ゲイン アンテナの放射パターンは、特定の方向により収束したものになります。アンテナゲイン値は 0 ー 40 です。
- [Antenna Cable]：アンテナケーブルを選択するには、このチェックボックスをオンにして、[Select Antenna Cable] ドロップダウンリストからアンテナケーブルを選択します。アンテナケーブルとして [Other] を選択した場合は、[Cable Loss (in dBi) (for Cable-Other)] フィールドにケーブル損失値を入力します。ケーブル損失値は 0 ～ 40 です。
- [Azimuth]：方位角を指定するには、このチェックボックスをオンにして、方位角方向の値を度数で入力します。方位角は、x 軸に対して測定されたアンテナの角度です。方位角の範囲は 0 ー 360 です。

- [Elevation]：仰角を指定するには、このチェックボックスをオンにし、仰角方向の値を度数で入力します。仰角方向の範囲は 0 ー 90 です。[Up] および [Down] トグルボタンを使用して、方向を指定します。

ステップ 12 [Schedule Task] ウィンドウで、[Now] または [Later] をクリックして、AP をいつプロビジョニングするかを指定します。

ステップ 13 [Next] をクリックして、概要画面で詳細を確認します。[Summary] ウィンドウで、AP 設定の詳細を確認し、該当するセクションで [Edit] をクリックして、変更を加えます。

ステップ 14 [構成] をクリックします。

ステップ 15 [Track Provision Status] ウィンドウで、[AP Configuration Provision] ステータスを確認できます。

AP ワークフローの定期的なイベントのスケジュール

この手順は、Cisco DNA Center で AP および無線パラメータの定期的なイベントをスケジュールする方法を示しています。

ステップ 1 メニューアイコン（☰）をクリックして、**[Workflows]** > **[Configure Access Points]**の順に選択します。

ステップ 2 タスクの概要ウィンドウが表示されたら、[Let's Do It] をクリックして、ワークフローに直接移動します。

ステップ 3 [Get Started] ウィンドウで、[Task Name] フィールドにタスクの一意の名前を入力します。

ステップ 4 [How do you want to configure APs?] ウィンドウで、[Schedule Recurring Events For AP And Radio Parameters] オプションボタンをクリックします。

ステップ 5 [Select Access Points] ウィンドウで、次の手順を実行します。

a) AP 関連の設定を適用するサイトに移動します。

右側のペインに、選択したサイトで使用可能なすべての AP が一覧表示されます。

b) 選択する AP 名の横にあるチェックボックスをオンにします。

ステップ 6 [Select AP and Radio Parameters] ウィンドウで、選択した AP の定期的なイベントに設定する AP および無線パラメータを選択します。

- [Admin Status]：管理ステータスを無効にするには、このチェックボックスをオンにして、[Disable] をクリックします。
- [AP LED Status]：AP LED ステータスを無効にするには、このチェックボックスをオンにして、[Disable] をクリックします。
- [5 GHz Admin Status]：5 GHz 管理ステータスを無効にするには、このチェックボックスをオンにして、[Disable] をクリックします。

  Cisco DNA Center は、この設定を AP のスロット 1 に適用します。
- [2.4 GHz Admin Status]：2.4 GHz 管理ステータスを無効にするには、このチェックボックスをオンにして、[Disable] をクリックします。

Cisco DNA Center は、この設定を AP のスロット 0 に適用します。

- [6 GHz Admin Status]：6 GHz 管理ステータスを無効にするには、このチェックボックスをオンにして、[Disable] をクリックします。

  Cisco DNA Center は、この設定を 6 GHz 対応 AP のスロット 3 に適用します。

- [Dual-Band (XOR) Admin Status]：デュアルバンド（XOR）管理ステータスを無効にするには、このチェックボックスをオンにして、[Disable] をクリックします。

  Cisco DNA Center は、この設定をデュアルバンド（XOR）対応 AP のスロット 0 に適用します。

ステップ 7 [Schedule Provision] ウィンドウで、次のように構成します。

1. 開始日時を指定します。
2. タイム ゾーンを選択します。
3. [Recurrence] で、次のいずれかのトグルボタンをクリックします。
   - [None]：Cisco DNA Center は AP 設定タスクを 1 回だけ実行し、繰り返しません。
   - [Hourly]：Cisco DNA Center は指定した時間間隔ごとに AP 設定タスクを実行します。[Run at Interval (Hours)] フィールドで、タスクを繰り返す間隔を時間数で指定します。有効な範囲は 1 ～ 48 です。
   - [Daily]：Cisco DNA Center は指定した日間隔ごとに AP 設定タスクを実行します。[Run at Interval (Days)] フィールドで、タスクを繰り返す間隔を日数で指定します。有効な範囲は 1 ～ 14 です。
   - [Weekly]：Cisco DNA Center は指定した週間隔ごとに AP 設定タスクを実行します。[Run at Interval (Weeks)] フィールドで、タスクを繰り返す間隔を週単位で指定します。有効な範囲は 1 ～ 52 です。
4. （オプション）[Hourly]、[Daily]、または [Weekly] の繰り返し間隔を選択する場合は、[Set Schedule End] チェックボックスをオンにして、繰り返しの終了設定を完了します。
   - 終了日を指定するには、[End Date] オプションボタンをクリックして終了日を指定します。

     （注） Cisco DNA Center では、開始日から最長 3 年の終了日を設定できます。

   - 指定した回数の後に定期的なイベントを終了するには、[End After] オプションボタンをクリックして、回数を指定します。

     （注） Cisco DNA Center では、最小値 2、および開始日から最長 3 年の終了日を設定できます。

ステップ 8 [Summary] ウィンドウで概要を確認し、[Configure] をクリックします。

デバイスと既存のインフラストラクチャからデバイス構成を学習する

次の手順は、Cisco DNA Center を使用してデバイスと既存のインフラストラクチャから構成を学習する方法を示しています。

ステップ 1 メニューアイコン（☰）をクリックして、 **[Workflows]** > **[Learn Device Configuration]** > **[Let's Do it]** の順に選択してワークフローを起動します。

（注） [workflow] ウィンドウの上部で、青い進行状況バーにカーソルを合わせると、現在の手順を確認したり、前の手順のいずれかに戻ることができます。

ステップ 2 [Select a WLC to Learn Configuration] ウィンドウで、Cisco DNA Center により構成が学習されていないワイヤレスコントローラをクリックし、[Next] をクリックします。

ステップ 3 [Site Assignment] ウィンドウで、ワイヤレスコントローラと AP の既存のワイヤレス ネットワーク プロファイルに関連付けられていないサイトを選択します。

（注） サイトを割り当てなくてもデバイス構成を学習できますが、Cisco DNA Center から同じワイヤレスコントローラを管理するために必要なサイトを割り当てることをお勧めします。

a) ワイヤレスコントローラにサイトを割り当てるには、[Device Name] の横にある [Assign Site] をクリックします。

- [Assign Site] ウィンドウで、関連付ける建物に移動して [Save] をクリックします。

b) AP にサイトを割り当てるには、[Unified AP] テーブルの AP 名の隣にあるチェックボックスをオンにして、[Assign Site] をクリックします。

- [Assign Site] ウィンドウで、フロアに移動して [Save] をクリックします。

c) [Next] をクリックします。

ステップ 4 [Learned Network Settings] ウィンドウで、次の学習済みネットワーク設定を確認します。

これらの設定はそのデバイスが物理的に存在する場所に保存されます。このウィンドウに表示されるネットワークサーバーは、サイトレベルで保存されます。

- AAA サーバーの [Shared Secret] を入力します。
- **システム設定**
  - AAA サーバーを Cisco ISE サーバーとして保存するには、[Cisco ISE Server] トグルボタンをクリックし、[Username]、[Password]、および [FQDN] に詳細情報を入力します。

（注） Cisco DNA Center に Cisco ISE サーバーがすでに存在する場合は、AAA サーバーを Cisco ISE サーバーとして保存できません。

AAA サーバーを Cisco ISE サーバーとして設定すると、Cisco ISE サーバーからの証明書が自動的に受け入れられ、信頼が確立されます。

- [Virtual IP Address(es)] トグルボタンをクリックして、ロードバランサの IP アドレスを入力します。

- [AAA Server]：Cisco DNA Center で設定されたネットワークサーバーが表示されます。これらのネットワークサーバーは事前入力されます。
  - AAA サーバーの [Network] または [Client/Endpoint] をカスタマイズできます。サーバーとプロトコルはデフォルトで選択されます。
  - ドロップダウンリストから [IP Address (Primary)] と [IP Address (Secondary)] を選択します。これらのサーバーはグローバルレベルで保存されます。
    - [DHCP Server]：デバイスで使用可能なすべての DHCP サーバーが表示されます。
    - [NTP Server]：デバイスで使用可能なすべての NTP サーバーが表示されます。

- [Next] をクリックします。

ステップ 5 [Assign Sites to Configurations Learned] ウィンドウでは、構成がデバイス上で使用可能な場合、学習した次の設定を表示できます。サイトに割り当てられていない構成は無視されます。

- Flex オーバーライド
- AAA Server
- VLAN エントリ
- メッシュ設定
- リモートテレワーカーの有効化

ステップ 6 [Learned Wireless Configuration] ウィンドウでワイヤレスコントローラから学習された設定を確認します。このウィンドウに表示されるワイヤレス設定は、グローバルレベルで保存されます。

- [Supported] タブには、[SSID]、[RF Profiles]、[Interfaces]、[Interface Groups]、[aWIPS and Forensic Capture Enablement]、[Pre Auth ACLs]、[Native VLAN] などの学習された設定のリストが表示されます。
  - デフォルトでは、NAC 設定が有効になっている SSID はゲスト SSID として学習されます。[SSID] テーブルの [SSID Type] の横にある [Edit] アイコンをクリックして、[SSID Type] を [Guest] から [Enterprise] に変更します。
  - 設定を無視するには、学習した設定の横にあるチェックボックスをオンにして、対応するテーブルで [Ignore Config] をクリックします。

- 無視された SSID、RF プロファイル、インターフェイス、またはインターフェイスグループを再学習するには、再学習する対象を選択し、対応するテーブルで [Relearn Config] をクリックします。

- [Unsupported] タブには、[SSID]、[RF profile]、[interface]、[Pre Auth ACLs]、[Interface Groups] など、学習されていない設定が表示されます。これらのサポートされていない設定または不明な設定に対処し、CLI テンプレートを使用できます。

ステップ 7 [Assign Sites to Learned SSIDs] ウィンドウで、複数の WLAN プロファイルの競合を確認して解決します。

- グローバルレベルで保存され、複数の WLAN プロファイルで学習されている SSID がリストされます。競合を解決するには、WLAN プロファイルを SSID からグローバルに割り当て、別のプロファイルを特定のサイトに割り当てます。
- （オプション）WLAN プロファイルをサイトに割り当てるには、対応する SSID 行の [Assign Site] をクリックします。
  - [Assign Site] ウィンドウで、サイトを選択して [Save] をクリックします。

    （注） 上書きできるのは、ワイヤレス設定またはプロファイルが関連付けられていないサイトだけです。関連付けられていないサイトがない場合は、現在のワークフローを終了し、新しいサイトを作成してからワークフローを再開してください。

ステップ 8 [Resolve Configuration Conflicts] ウィンドウで、表示される競合を確認して解決します。

デバイスから学習された設定と、グローバルレベルで保存されている設定が表示されます。

競合を解決する設定セットを選択します。

- [Use DNAC Configuration]：グローバルレベルで設定を保存する場合。
- [Use Device Configuration]：デバイスから設定を学習する場合。

  デバイス設定を選択すると、グローバルレベルで保存されている設定が上書きされます。
- [Use Custom Configuration]：必要な [Wireless Interface] を選択することによって設定をカスタマイズする場合。

ステップ 9 [Model Configs Learned] ウィンドウで、モデル設定を確認します。

モデル設定とは、ネットワークデバイスに展開できる、モデルベースの、検出可能でカスタマイズ可能な一連の設定機能です。モデル設定は、さまざまなハードウェア プラットフォームおよびソフトウェア タイプに展開できます。Cisco DNA Center は、CLI などのデバイス固有の設定からモデル設定を検出して学習します。学習されたモデル設定は、ネットワークプロファイルに関連付けることができる設計に保存されます。

次のワイヤレスモデル設定設計タイプを展開して確認します。

- AAA Radius 属性の設定
- 高度な SSID 設定

- CleanAir の設定
- Dot11ax 設定
- イベント駆動型 RRM の設定
- グローバル IPv6 設定
- マルチキャストの設定
- RRM の一般設定

各モデル設定設計タイプからの設定を対象外にする場合は、対応するテーブルで設定を選択し、[Ignore Config] をクリックします。対象外の設定を再学習するには、対象外の設定を選択し、[Relearn Config] をクリックします。

ステップ 10 [CLI Templates Learned] ウィンドウで、CLI テンプレートを確認し、これらのテンプレートを使用して、不明の設定またはサポートされていない設定に対処します。

- 対象外になっているすべての WLAN 設定がデフォルトで選択されています。[Ignore Template] をクリックして、テンプレートによる設定への対処を制限します。[Relearn Template] をクリックして設定に対処します。
- すべての不明な設定またはサポートされていない設定がデフォルトで選択されています。[Ignore Template] をクリックして、テンプレートによる設定への対処を制限します。[Relearn Template] をクリックして設定に対処します。

ステップ 11 [Network Profiles] ウィンドウで、学習したネットワークプロファイル設定を確認します。学習した設定に基づいて、Cisco DNA Center によってネットワークプロファイルが作成されます。学習したネットワークプロファイルを使用することも、新しいネットワークプロファイルを作成することもできます。SSID は、ネットワークプロファイルの作成中に学習され、グループ化されます。

Cisco AireOS ワイヤレスコントローラでは、Flex グループと AP グループはネットワークプロファイルにマッピングされます。AP サイトの割り当てに応じて、ネットワークプロファイルは適切なサイトに割り当てられます。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラでは、サイトタグ、ポリシータグ、ネットワークプロファイルにマッピングされているサイト階層が表示されます。

- AP サイトの割り当て設定に基づいて、ネットワークプロファイルが適切なサイトに割り当てられます。[Sites Assigned] をクリックして、ネットワークプロファイルに割り当てられたサイトの詳細を表示します。
- 新しいネットワークプロファイルを作成するには、[Create New Profile] をクリックします。

  [New Profile] ウィンドウが表示されます。

  - [Network Profile Name] フィールドに、ネットワークプロファイルの名前を入力します。
  - [SSID] テーブルで、[Network Name] の横にあるチェックボックスをオンにして SSID を選択します。
  - **[Save]** をクリックします。

- （オプション）テンプレートの詳細を確認し、変更が必要な場合は編集します。
  - ネットワークプロファイルにサイトを割り当てるには、[Assign Site] をクリックします。[Assign Site] ウィンドウで、サイトを選択して [Save] をクリックします。

    [Sites Assigned] をクリックして、このプロファイルに割り当てられたサイトを確認します。
  - ネットワークプロファイルにテンプレートを関連付けるには、[Assign Template] をクリックします。[Assign Template] ウィンドウで、既存の展開の各デバイスに対して [Select Templates] ドロップダウンリストからテンプレートを選択し、[Save] をクリックします。

    [View Templates] をクリックして、プロファイルに割り当てられているテンプレートを確認します。
  - ネットワークプロファイルを対象外にするには、[Ignore Profile] をクリックし、[Continue] をクリックします。

    プロファイルが対象外としてマークされている場合、そのプロファイルのすべてのプロファイル属性が削除されます。これは、プロファイルを再学習することによって元に戻すことはできません。対象外のプロファイルを再学習するには、[Relearn Profile] をクリックします。
  - ネットワークプロファイルにサイトタグを追加するには、[Site Tag] テーブルで [Add] をクリックします。[Add Site Tag] ウィンドウで、[Select Site Tag] ドロップダウンリストからサイトタグを選択し、階層からサイトを選択して、[Save] をクリックします。

ステップ 12 （オプション）[Network Profile - Model Configurations] ウィンドウで、Cisco DNA Center によって学習されたモデル設定をネットワークプロファイルに関連付けます。

- [追加（Add）] をクリックします。
- [Add Model Configs to Network Profile] ウィンドウで、次の手順を実行します。
  - 追加するモデル設定設計を展開します。
  - 設計を選択します。[Advanced SSID Configuration] の場合は、設計ごとに [Applicable SSID] 列のドロップダウンリストから SSID を選択します。
  - [Apply] をクリックします。
- ネットワークプロファイルに追加されたモデル設定を削除するには、モデル設定を選択して、[Delete] をクリックします。
- [Next] をクリックします。

ステップ 13 [Summary] ウィンドウで、設定を確認します。変更するには、[Edit] をクリックします。

ステップ 14 **[Save]** をクリックします。

ネットワーク設定は、グローバルレベルおよびサイトレベルで適切に作成されます。

ステップ 15 メニューアイコン（☰）をクリックして、**[Design]** > **[Network settings]**。

- [Network] タブでは、デバイスから学習されたすべてのネットワーク設定を確認できます。

- [Wireless] タブでは、デバイスから学習されたすべてのワイヤレス設定を確認できます。

学習された設定は、デバイスのプロビジョニング時にデバイスにプッシュされます。

デバイスの交換ワークフロー

このワークフローでは、故障したデバイスを交換するための詳細な手順が示されます。

（注） [Inventory] ウィンドウから故障したデバイスを交換することもできます。詳細については、故障したデバイスの交換 （136 ページ）を参照してください。

始める前に

- 故障したデバイスのソフトウェア イメージ バージョンをイメージリポジトリにインポートしてから、交換するデバイスにマークを付ける必要があります。
- 故障したデバイスは到達不能な状態になっている必要があります。
- 交換用デバイスがプラグアンドプレイ（PnP）で Cisco DNA Center をオンボードしている場合は、故障したデバイスをユーザー定義のサイトに割り当てる必要があります。
- RMA ワークフローのトリガー中は、交換用デバイスがプロビジョニング状態であってはなりません。

ステップ 1 メニューアイコン（☰）をクリックして、**[Workflows]** > **[Replace Device]** の順に選択します。

ステップ 2 タスクの概要ウィンドウが開いたら、[Let's Do It] をクリックして、ワークフローに直接移動します。

ステップ 3 [Get Started] ウィンドウで、ワークフローの一意の [Task Name] を入力します。

ステップ 4 [Choose Device Type] 画面で、交換する故障したデバイスのタイプを選択します。

ステップ 5 [Choose Site] 画面で、故障したデバイスがあるサイトを選択します。

ステップ 6 [Choose Faulty Device] ウィンドウで、交換する故障したデバイスを選択します。

ステップ 7 [Choose Faulty Device] ウィンドウで故障したデバイスが見つからない場合は、次の手順を実行します。

a) [Add Faulty Device] をクリックします。
b) 故障したデバイスを選択し、[Next] をクリックします。
c) [Mark For Replacement] ウィンドウで、[Mark] をクリックします。

ステップ 8 [Choose Replace Device] ウィンドウで、[Unclaimed] タブまたは [Managed] タブから交換用デバイスを選択します。

[Unclaimed] タブには、PnP によってオンボードされたデバイスが表示されます。[Managed] タブには、インベントリまたは検出プロセスのいずれかによってオンボードされたデバイスが表示されます。

ステップ 9 （任意） 交換用デバイスがまだオンボードされていない場合は、次の手順を実行します。

a) [Choose Replace Device] ウィンドウで、[Add Device] をクリックします。
b) [Add New Device] ウィンドウで、デバイスの**シリアル番号**を入力し、[Add New Device] をクリックします。

または

a) [Choose Replace Device] ウィンドウで、[Sync with Smart Account] をクリックします。
b) [Sync with Smart Account] ウィンドウで、[Sync] をクリックします。

ステップ 10 [Schedule Replacement] ウィンドウで、[Now] をクリックしてデバイスの交換をただちに開始するか、[Later] をクリックして特定時刻でのデバイスの交換をスケジュールします。

交換用デバイスがまだオンボードされていない場合、[Now] オプションは無効になります。[Later] をクリックして特定時刻でのデバイスの交換をスケジュールすることは可能です。

ステップ 11 [Review] をクリックして、選択したデバイスタイプ、故障したデバイスの詳細情報、および交換用デバイスの詳細情報を確認します。

ステップ 12 [Summary] ウィンドウで、設定を確認します。変更するには、[Edit] をクリックします。

a) （任意） [Replacement Device] で、[View] をクリックして、交換用デバイスの設定を確認します。
b) [置換（Replace）] をクリックします。

ステップ 13 [Click Monitor Replacement Status] をクリックして [Provision] ウィンドウの [Mark for Replacement] ビューに移動します。

ステップ 14 交換用デバイスの [Replace Status] をクリックすると、RMA ワークフローのステータスが表示されます。ワークフローが完了すると、[Replace Status] が [Replaced] に更新されます。

ステップ 15 エラーメッセージが表示された場合は、エラーリンクをクリックします。[Retry] をクリックして、故障したデバイスと交換用デバイスの同じ組み合わせを使用してワークフローを再トリガーします。

（注） [Main Inventory] ウィンドウには、故障したデバイスと交換した新しいデバイスの詳細情報が表示されます。

ステップ 16 （任意） どの段階でもワークフローを終了し、後で再開することができます。[Exit] オプションは、すべてのウィンドウの左下隅に表示されます。ワークフローを終了して後で再開するには、次の手順を実行します。

a) [終了（Exit）] をクリックします。

[Exiting Workflow] 確認ウィンドウが表示されます。

b) 確認ウィンドウで、[Exit] をクリックします。

タスク名の付いたワークフローの [In Progress] カードが作成されます。

c) 終了した位置からワークフローを再開するには、[In Progress] カードをクリックします。

- デバイスに [In progress] カードがあり、**[Inventory]** > **[Marked for Replacement]** ウィンドウから同じデバイスを交換しようとすると、シリアル番号と [In progress] カードのタスク名を含む確認メッセージが表示されます。[Yes] をクリックしてワークフローを再開するか、[Cancel] をクリックして新しいワークフローを開始します。

- 交換対象としてマークされていないデバイスの [In progress] カードをクリックすると、**警告メッセージ**が表示されます。[Yes] をクリックし、障害のある別のデバイスを選択して、新しいワークフローを開始します。[Cancel] をクリックすると、ワークフローがキャンセルされます。

リモートサポート許可の作成

次の手順では、リモートサポートの許可を作成する方法について説明します。

（注） Cisco DNA Center リモートサポートの許可は、LM コンソールバージョン 0.40.5 でのみサポートされます。

ステップ 1 メニューアイコン（☰）をクリックして、**[ワWorkflows]** > **[Create a Remote Support Authorization]**の順に選択します。

ステップ 2 タスクの概要ウィンドウが表示されたら、[Let's Do It] をクリックして、ワークフローに直接移動します。

ステップ 3 [Set up the Authorization] ウィンドウで、次を入力します。

a) **シスコスペシャリストの電子メールアドレス**
b) **既存のサービスリクエスト番号**
c) **アクセスを許可する理由**

ステップ 4 [Schedule the Access] ウィンドウで、[Now] または [Later] をクリックして、シスコのスペシャリストによる Cisco DNA センターへのアクセスをいつ許可するかを指定します。

ステップ 5 [Access Permission Agreement] ウィンドウで、[I agree] にチェックを入れ、[Next] をクリックします。

（注） この許可は、アクセス前であればいつでも取り消すことができます。

ステップ 6 [Summary] ウィンドウで、詳細を確認します。[Edit] をクリックして、[Set Up the Authorization] と [Schedule the Access] ウィンドウで変更を行います。

ステップ 7 [作成（Create）] をクリックします。

タスク完了Done! Authorization is created] ウィンドウが表示されます。

ステップ 8 [View All Authorization] をクリックして、[Remote Support Authorization] ウィンドウに移動します。詳細については、リモートサポート許可ダッシュボードの表示を参照してください。

イベント通知の作成

Cisco DNA Center イベント通知を使用すると、複数のポイントで発生する選択したイベントの詳細を配信する 1 つの通知内に複数のチャネルを関連付けることができます。

ステップ 1 メニューアイコン（☰）をクリックして、**[Workflows]** > **[Create a New Notification]**の順に選択します。

ステップ 2 タスクの概要ウィンドウが開いたら、[Let's Do It] をクリックして、ワークフローに直接移動します。

ステップ 3 [Select Channels] ウィンドウで、通知チャネルを選択します。

サポートされているチャネルは、[REST]、[PAGERDUTY]、[SNMP]、[SYSLOG]、[WEBEX]、[EMAIL]、およびカスタムチャネルです。

ステップ 4 [Select Site and Events] ウィンドウで、[Select a site] ドロップダウンリストから、選択したイベントの通知を受け取る特定のサイトを選択します。

（注） 複数のサイトを同時に選択できます。

ステップ 5 イベントの横にあるプラスアイコンをクリックするか、[Add All] をクリックしてすべてのイベントをそれぞれの通知に追加します。

ステップ 6 通知からイベントを削除するには、削除するイベントの横にある X アイコンをクリックするか、[Remove All] をクリックしてイベントリストからすべてのイベントを削除します。

（注）
- 通知チャネルを選択すると、[Select Site and Events] ウィンドウのテーブルに、選択した通知チャネルでサポートされるイベントの数が一覧表示されます。
- 複数の通知チャネルを選択すると、[Select Site and Events] ウィンドウのテーブルに、選択した通知チャネルに共通のサポートされているイベントの数が一覧表示されます。

ステップ 7 [Configure Notification] ウィンドウで、次の値を設定します。

1. [EMAIL] 通知チャネルを選択した場合は、[Email Settings] ウィンドウで次のように設定します。
    1. リンクをクリックして [Email] GUI ウィンドウにアクセスし、新しいメールサーバーを設定します。

（注）
- 通知タイプは、[REST] API エンドポイント（ウェブフック）、[PAGERDUTY]、[SNMP]、[SYSLOG]、[WEBEX]、または [EMAIL] のいずれかに設定できます。[EMAIL] を選択した場合に電子メール設定が完了していないと、該当する GUI ウィンドウにアクセスして設定作業を行うよう求められます。電子メール設定は、[Email] タブで設定します。

  （オプション）[Email] タブにアクセスするには、メニューアイコン（☰）をクリックし、**[System]** > **[Settings]** > **[External Services]**を選択します。

  [External Services] を展開し、**[Destinations]**を選択して、[Email] タブをクリックします。

- 電子メール通知を受信する電子メールアドレスは、エンドポイントごとに最大 20 個まで設定できます。複数の電子メールアドレスを追加するには、各電子メールアドレスを個別に追加し、追加するたびに（キーボードの）Enter を押す必要があります。Cisco DNA Center により電子メールアドレスが検証され、構文が正しくない場合は通知されます。

- エンドポイントごとに 20 を超える電子メールアドレスを設定する必要がある場合は、グループ電子メールエイリアスを使用できます。

- イベント サブスクリプションに電子メールの宛先を使用している場合、送信される電子メールには UTC タイムスタンプ付きのイベントが表示されます。

2. [Select Existing Instance] をクリックして既存の電子メールインスタンスを使用するか、[Create New Instance] をクリックして新しい電子メールインスタンスを作成します。
3. [Select Existing Instance] をクリックした場合は、[Select Instance] ドロップダウンリストから電子メールインスタンスを選択します。
4. [From] および [To] フィールドに電子メールアドレスを入力し、電子メールの [Subject] ヘッダーに件名を入力します。

2. [SYSLOG] 通知を選択した場合は、[Syslog Settings] ウィンドウで次の値を設定します。
   1. リンクをクリックして [Syslog] GUI ウィンドウにアクセスし、新しい syslog エンドポイント（Syslog サーバーのホスト名とポート番号）を設定します。

      （注） 通知タイプは、[REST] API エンドポイント（ウェブフック）、[PAGERDUTY]、[SNMP]、[SYSLOG]、[WEBEX]、または [EMAIL] のいずれかに設定できます。[SYSLOG] を選択したが、Syslog サーバーの設定を行っていない場合、GUI ウィンドウにアクセスして設定作業を行うよう求められます。Syslog サーバーの設定は、[Syslog] タブで行います。

      （オプション）[Syslog] タブにアクセスするには、メニューアイコン（☰）をクリックし、**[System]** > **[Settings]** > **[External Services]**を選択します。

      [External Services] を展開し、**[Destinations]**を選択して、[Syslog] タブをクリックします。

   2. [Protocol] フィールドに、TCP または UDP のいずれかを入力します。
   3. [Port] フィールドに、syslog サーバーのポート番号を入力します。

4. [Hostname/IP] フィールドで、syslog サーバーのホスト名または IP アドレスを入力します。
5. [Select Instance] ドロップダウンリストで syslog インスタンスを選択します。

3. [REST] 通知を選択した場合は、[REST Settings] ウィンドウで次の値を設定します。
   - リンクをクリックして [REST Webhook] GUI ウィンドウにアクセスし、新しいウェブフックエンドポイントを設定します。

     （注） 通知タイプは、[REST] API エンドポイント（ウェブフック）、[PAGERDUTY]、[SNMP]、[SYSLOG]、[WEBEX]、または [EMAIL] のいずれかに設定できます。[REST] を選択したが、ウェブフックの設定を行っていない場合、 GUI ウィンドウにアクセスして設定作業を行うよう求められます。ウェブフックの設定は [Webhook] タブで行います。

     （オプション）[Webhook] タブにアクセスするには、**[System]** > **[Settings]** > **[External Services]**を選択します。

     [External Services] を展開し、**[Destinations]**を選択して、[Webhook] タブをクリックします。

   - [Webhook Instance] ドロップダウンリストから、通知エンドポイントと URL を選択します。
   - [URL] フィールドにイベント送信先の REST API エンドポイントの URL アドレスを入力します。

     [Trust certificate]：REST API エンドポイント通知に信頼できる証明書が必要かどうか。

     [Method]：PUT メソッドまたは POST メソッド。

   - [Basic]：クライアントが HTTP 要求を送信することで認証を行います。認証ヘッダーには「Basic」という単語が含まれ、後にスペース、「username:password」の形式の base64 でエンコードされた文字列が続きます。GUI で [Basic] を選択すると、[Headers] フィールドに「Authorization」という値が自動的に入力されます。
   - [Token]：サーバーから提供されたセキュリティトークンを使用してユーザーが認証されます。[Token] を選択すると、[Headers] フィールドに「X-Auth-Token」という値が自動的に入力されます。
   - [No Authentication]：認証が不要になります。
   - [Headers]：[Header Name] と [Header Value]。

     （注） [Headers] フィールドは、認証の選択内容に応じて自動的に値が入力される場合があります。

4. [SNMP] 通知チャネルを選択した場合は、[SNMP Settings] ウィンドウで次のように値を設定します。
   1. リンクをクリックして [SNMP] GUI ウィンドウにアクセスし、新しい SNMP エンドポイントを設定します。

（注） 通知タイプは、[REST] API エンドポイント（ウェブフック）、[PAGERDUTY]、[SNMP]、[SYSLOG]、[WEBEX]、または [EMAIL] のいずれかに設定できます。[SNMP] を選択した場合に SNMP 設定が完了していないと、該当する GUI ウィンドウにアクセスして設定作業を行うよう求められます。SNMP の設定は [SNMP] タブで行います。

（オプション）[SNMP] タブにアクセスするには、メニューアイコン（☰）をクリックし、**[System]** > **[Settings]** > **[External Services]**を選択します。

[External Services] を展開し、**[Destinations]**を選択して、[SNMP] タブをクリックします。

SNMP トラップ通知は、システム ハードウェア イベントに対してのみ使用できます。ハードウェアコンポーネントの正常性状態が変化した場合、システム ハードウェア イベントによってサブスクライバへの通知がトリガーされます。変更がモニターされるハードウェアコンポーネントには、CPU、メモリ、ディスク、NIC、ファン、電源、RAID コントローラなどがあります。

2. [SNMP Instance] ドロップダウンリストから、通知エンドポイントを選択します。
3. [Create a new endpoint]：新しいエンドポイント名と説明を入力します。
4. [Hostname/IP Address] フィールドに SNMP トラップレシーバ（サーバー）のホスト名または IP アドレスを入力します。
5. [Port] フィールドに SNMP トラップレシーバ（サーバー）のポート番号を入力します。

5. [PAGERDUTY] 通知チャネルを選択した場合は、[PAGERDUTY Settings] ウィンドウで次のように設定します。
   1. [SERVICE CONFIGURATION] エリアで、[Select Existing Instance] をクリックして既存の PagerDuty インスタンスを使用するか、[Create New Instance] をクリックして新しい PagerDuty インスタンスを作成します。
   2. [Select Instance] ドロップダウンリストで PagerDuty インスタンスを選択します。
   3. [PagerDuty Events API URL] フィールドに、PagerDuty イベント API URL を入力します。
   4. [PagerDuty Integration Key] フィールドに、PagerDuty 統合キーを入力します。
6. [WEBEX] 通知チャネルを選択した場合は、[WEBEX Settings] ウィンドウで次のように値を設定します。
   1. [Select Instance] ドロップダウンリストで Webex インスタンスを選択します。
   2. [Webex URL] フィールドに、Webex URL を入力します。
   3. [Webex Room ID] フィールドに、Webex ルーム ID を入力します。
   4. [Webex Bot Access Token] フィールドに、Webex ボットアクセストークンを入力します。

ステップ 8 **[Save]** をクリックします。

[Name and Description] ウィンドウで、次の手順を実行します。

a) [Name] フィールドに、通知の一意の名前を入力します。
b) [Description] ボックスに、通知の説明を入力します。

ステップ 9 [Summary] ウィンドウで、設定の詳細を確認し、[Finish] をクリックします。

タスク完了Done! Your new notification is complete] ウィンドウが表示されます。

IP ベースおよび URL ベースのアクセス コントロール ポリシー作成のワークフロー

ネットワークの IP ベースおよび URL ベースの認証後アクセスコントロールリスト（ACL）を作成できます。

始める前に

IP ベースのアクセス コントロール契約の作成 （638 ページ）

ステップ 1 Cisco DNA Center GUI でメニューアイコン（☰）をクリックして、**[Workflows]** > **[Create IP & URL-Based Access Control Policy]**の順に選択します。

ステップ 2 タスクの概要ウィンドウが開いたら、[Let's Do It] をクリックして、ワークフローに直接移動します。

ステップ 3 [ポリシー名と詳細] ウィンドウで、次のフィールドに入力します。

- **Policy Name**
- **説明**
- [Select ACL Type]：必要に応じて、[IP]、[URL]、またはその両方を選択します。

ステップ 4 [Select Site and SSID] ウィンドウで、次を実行します。

- ポリシーを適用するサイトを選択します
- デバイスにすでにプロビジョニングされている非ファブリック SSID を選択します。

ステップ 5 [IP Access Control List] ウィンドウで、[Add New Row] をクリックし、次を選択します。

- **送信元**
- **接続先**
- **契約**
- **Direction**

（注） このウィンドウは、[Policy Name and Details] ウィンドウで ACL タイプとして [IP] を選択した場合にのみ表示されます。

ステップ 6 [Add] をクリックします。

ステップ 7 [URL Access Control List] ウィンドウで、次の手順を実行します。

- URL を入力します。
- [Action] ドロップダウンリストをクリックして [Permit] または [Deny] を選択します。

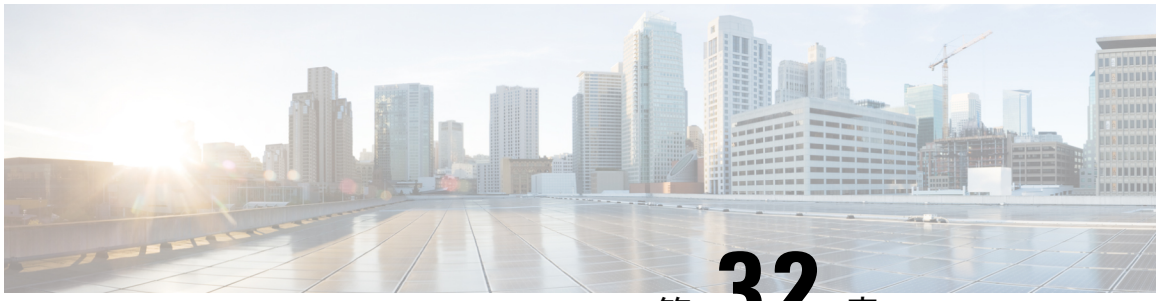
（注） このウィンドウは、[Policy Name and Details] ウィンドウで ACL タイプとして [URL] を選択した場合にのみ表示されます。

ステップ 8 [Schedule Task] ウィンドウで、次のいずれかを実行します。

- ポリシーをすぐに展開するには、[Now] オプションボタンをクリックし、[View Summary] をクリックします。
- ポリシーを後で展開するには、[Later] オプションボタンをクリックし、[Task Name] と [Start Date and Time] を指定して [View Summary] をクリックします。
- 選択したデバイスに展開するために後で使用できるプレビューを作成する場合は、[Generate Preview] をクリックします。

ステップ 9 [Summary] ウィンドウで、サイトの設定を確認します。

- 変更を加えるには [Edit] をクリックします。
- 問題がなければ、[Deploy] をクリックします。



第 32 章

データプラットフォームを使用した Cisco DNA Center のトラブルシューティング

データ プラットフォームについて

データ プラットフォームには、Cisco DNA Center アプリケーションのモニターとトラブルシューティングに役立つツールがあります。[Data Platform] には、ネットワークのパターン、トレンド、問題領域を特定するのに役立つ、さまざまな入力から合成されたデータが表示されます。たとえば、ネットワークに問題が発生した場合、パイプラインがエラー状態になっているかどうか、特定のエリアにおけるリアルタイム トラフィック フローが何かなど、問題に対する回答を迅速に得ることができます。データ プラットフォームの主なエリアは次のとおりです。

- [Analytics Ops Center]：データがコレクタとパイプラインを経由してどのように流れているかをグラフィカルに表示します。また、ネットワーク内のパターン、傾向、次のような問題領域を特定できる Grafana ダッシュ ボードも用意されています。分析 Ops センターを使用したトラブルシューティング （816 ページ）を参照してください。
- [Collectors]：さまざまなネットワークテレメトリとコンテキストデータをリアルタイムで収集します。データが取り込まれると、Cisco DNA Center はデータを関連付けて分析します。コレクタのステータスを表示し、問題領域をすばやく見分けることができます。コレクタの設定情報の表示または更新 （818 ページ）を参照してください。
- [Store Settings]：アプリケーションのデータの保存期間を表示できます。データ保持設定の表示 （819 ページ）を参照してください。
- [Pipelines]：Cisco DNA Center アプリケーションが、ストリーミングデータを処理できるようにします。データ パイプラインでは、外部ソースからの入力データを受け入れ、有用な情報を提供するためにそのデータを変換し、出力データを生成する一連の計算をカプセル

化します。パイプラインのステータスを表示し、問題領域をすばやく見分けることができます。パイプライン ステータスの表示 （819 ページ）を参照してください。

分析 Ops センターを使用したトラブルシューティング

分析 Ops センターは、データがコレクタとパイプラインを経由してどのように流れているかに関するグラフィカル表示を提供します。また、ネットワーク内のパターン、傾向、次のような問題領域を特定するために役立つ Grafana ダッシュ ボードを提供します。

- アシュアランス の見つからないデータ。
- 不正確な正常性スコア。
- デバイスがインベントリではモニター対象として表示され、アシュアランスではモニター対象外として表示される。

ステップ 1 メニューアイコン（☰）をクリックして、**[System]** > **[Data Platform]**。

ステップ 2 [Analytics Ops Center] をクリックします。
アプリケーションのリストが表示されます。

ステップ 3 メトリックを表示するアプリケーション名、たとえば、[Assurance] をクリックします。

アプリケーション内のすべての既存のコレクタとパイプラインのグラフィカル表示が現れます。また、各パイプラインに対応する CPU またはスループット値も提供されます。

各コンポーネントの現在のヘルス ステータスは、色によって示されます。

- 赤色：エラー
- 黄色：警告
- 灰色：通常動作

ステップ 4 パイプラインの履歴データを表示するには、[Timeline & Events] をクリックします。

時間間隔のデータを提供するタイムライン バーが表示されます。次のことも実行できます。

- スライダを移動して、特定の時間のデータを表示する
- Hover your cursor over an event in the timeline bar to display additional details or a group of events that occurred at the same time.
- イベントをクリックして、その特定の時点での分析 Ops センターの可視化を表示する

ステップ 5 問題のトラブルシューティングに役立つ追加の詳細を表示し、エラーまたは警告の原因を特定するには、コレクタ名をクリックします。

スライドインペインに次のタブが表示されます。

- [Metrics]：直近 30 分間に収集された使用可能なメトリックの選択肢が提示されます。コンポーネントのステータス、開始時間と停止時間、およびエラーの例外を示す概要情報が表示されます。別の時間間隔を選択することもできます。
- [Grafana]：より詳細にデバッグするために各コンポーネントに関連付けられているダッシュボードが表示されます。

ステップ 6 データが特定のパイプラインを経由して流れているかどうかを表示するには、パイプラインストリームをクリックします。

スライドインペインが表示され、内部にグラフが表示されます。グラフは、アプリケーションが基盤となるパイプラインからデータを受信しているかどうかを表示します。グラフの情報は、スライドインペインでドロップダウンリストから選択する時間間隔に基づきます。オプションは、[Last 30 Min]、[Last Hour]、[Last 2 Hours]、および [Last 6 Hours] です。デフォルトは、[Last 30 Min] です。

ステップ 7 パイプラインが通常レベルで流れていない場合は、カーソルをストリームに合わせると、遅延メトリックが表示されます。

ステップ 8 特定のパイプラインの詳細情報を表示するには、パイプライン名をクリックします。

適切な [Pipeline] ページが、次のタブとともに表示されます。

（注） [Exceptions] タブをクリックして、パイプラインで例外が発生していないかどうかを確認してください。通常の動作状況では、このタブは **null** を表示します。

- **メトリック**：グラフ中で 30 分ごとに更新されるメトリックを表示します。
- **サマリ**：統計、ランタイム、マニフェストなどのサマリ情報を表示します。
- **例外**：パイプラインで発生した例外を表示します。
- **ステージ**：パイプラインのステージを表示します。

ステップ 9 [Analytics Ops Center] ページに表示されるメトリックを変更するには、[Key Metrics] をクリックして、最大 2 つのメトリックを選択し、[Apply] をクリックします。

デフォルトでは、Cisco DNA Center は CPU とスループットのメトリックを表示します。

ステップ 10 特定のフローのメトリックを表示するには、次を実行します。

a) [View Flow Details] をクリックします。
b) コンポーネントの左上隅にあるチルダ（～）をクリックして、3つの接続されたコンポーネント（コレクタ、パイプライン、ストア）を選択します。
c) [View Flow] をクリックします。
Cisco DNA Center は、その特定のフローに関連付けられたメトリックを表示します。

コレクタの設定情報の表示または更新

コレクタは、さまざまなネットワークテレメトリおよびコンテクスチュアルデータをリアルタイムで収集します。データが取り込まれると、Cisco DNA Center はデータを関連付けて分析します。コレクタのステータスを表示し、問題領域をすばやく見分けることができます。

ステップ 1 メニューアイコン（☰）をクリックして、**[System]** > **[Data Platform]**。

ステップ 2 [Collectors] をクリックします。各コレクタの横にある色付きの点は、全体的なステータスを示しています。

ステップ 3 追加の詳細を表示するには、コレクタ名をクリックします。

適切な *[Collector]* ページが表示されます。デフォルトでは、Cisco DNA Center に **[Configuration]** タブが表示され、現在の設定リストを確認できます。

ステップ 4 構成を表示、更新、または削除するには、特定の構成名をクリックします。

ステップ 5 新規の設定を追加するには、**[Configuration]** タブで **[+ Add]** をクリックします。

スライドインペインが表示されます。

ステップ 6 設定に必要な情報をスライドインペインに入力します。

ステップ 7 （任意） **[Anonymize]** チェックボックスをオンにすると、**[WIRELESSCOLLECTOR]** などの一部コレクタのデータを匿名化できます。

（注） [Anonymize] チェックボックスをオンにすると、**[Client Health]** ウィンドウに表示されるホスト名とユーザ ID は、復号化できない一方向ハッシュを用いてスクランブル処理されます。

重要 データを匿名化する場合は、**[Discovery]** ツールを使用してデバイスを検出する前に、**[Anonymize]** チェックボックスをオンにしてください。デバイスを検出した後にデータを匿名化した場合、システムに入ってくる新しいデータは匿名化されますが、既存のデータは匿名化されません。

ステップ 8 [Save Configuration] をクリックします。

ステップ 9 設定されているインスタンスを表示するには、[Instances] タブをクリックします。

ステップ 10 概要情報とメトリックを表示するには、リストからインスタンスを選択します。

ステップ 11 （任意） Cisco DNA Center を Cisco Connected Mobile Experience（CMX）と統合する場合は、CMX 側でデータの匿名化を選択できます。次の手順を実行します。

a) SSH クライアントを使用して、cmxadmin CLI ユーザとして Cisco CMX にログインします。

b) ルートユーザに変更します。

c) `/opt/cmx/etc/node.conf` に移動し、`[location]` の下に **`user_options`** を追加します。次に例を示します。

```
[location]
…
user_options=-Dhideusername=true
```

d) Cisco CMX CLI で、次のコマンドを入力します。

```
cmxctl agent restart
cmxctl location restart
```

データ保持設定の表示

アプリケーションのデータの保存期間を表示できます。

ステップ 1 メニューアイコン（☰）をクリックして、**[System]** > **[Data Platform]**。

ステップ 2 [Store Settings] をクリックします。

ステップ 3 完了した履歴消去ジョブのリストを表示するには、[Data Purge Schedule] をクリックします。

[HISTORY] テーブルには、消去ジョブの名前、結果、時刻、その他のデータが表示されます。テーブル内のデータをソート、フィルタリング、エクスポートすることができます。

ステップ 4 現在のデータの保持または消去の設定を表示するには、[Data Retention & Purge Configuration] をクリックします。次の出力が表示されます。

- [Document Store]：最大サイズ、ウォーターマークの下限および上限しきい値など、すべての時間ベースのデータの設定。
- [Metric Graph Store]：最大サイズ、ウォーターマークの下限および上限しきい値など、すべての時間ベースのグラフィカルデータの設定。

パイプライン ステータスの表示

データ パイプラインによって、Cisco DNA Center アプリケーションは、ストリーミング データを処理できます。データ パイプラインでは、外部ソースからの入力データを受け入れ、有用な情報を提供するためにそのデータを変換し、出力データを生成する一連の計算をカプセル化します。パイプラインのステータスを表示し、問題領域をすばやく見分けることができます。

ステップ 1 メニューアイコン（☰）をクリックして、**[System]** > **[Data Platform]**。

ステップ 2 [Pipelines] をクリックします。

ステップ 3 アプリケーションが基盤となるパイプラインからデータを受信しているかどうかを表示するには、パイプライン名をクリックします。

適切な [Pipeline] ページが、次のタブとともに表示されます。

（注） [Exceptions] タブをクリックして、パイプラインで例外が発生していないかどうかを確認してください。通常の動作状況では、このタブは **null** を表示します。

- **メトリック**：グラフ中で 30 分ごとに更新されるメトリックを表示します。
- **サマリ**：統計、ランタイム、マニフェストなどのサマリ情報を表示します。
- **例外**：パイプラインで発生した例外を表示します。
- **ステージ**：パイプラインのステージを表示します。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。