アシュアランス を使用するための Cisco DNA Center の設定

アシュアランス アプリケーションの使用を開始する前に、アシュアランス を設定する必要があります。ここでは、アシュアランスを設定するために実行する必要がある基本タスクについて説明します。この章は、Cisco Digital Network Architecture Center ユーザ ガイド と併用してください。

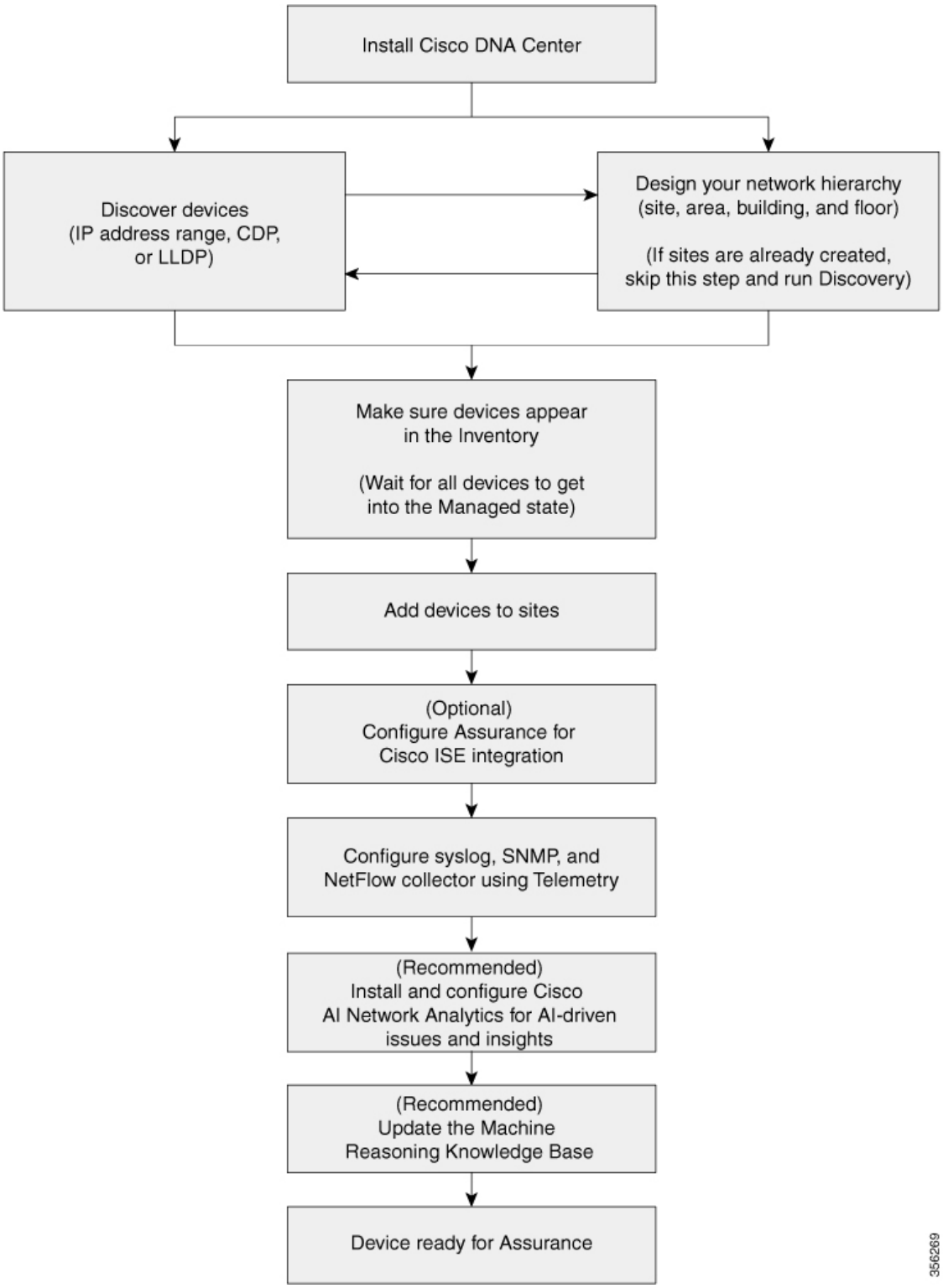
基本的な設定のワークフロー

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

（注） アシュアランス Cisco DNA Center では、管理対象デバイスへの NAT 接続はサポートされていません。

基本的なワークフローを理解するために、次の図と次の手順を参照してください。

図 *1 :* アシュアランスを使用するための *Cisco DNA Center* の設定の基本的なワークフロー



ステップ 1 Cisco DNA Center をインストールします。

Cisco DNA Center 設置ガイドを参照してください。

ステップ 2 任意の順序で次の操作を行います。

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

  Discover Your Network Using an IP Address Range （13 ページ）、CDP を使用したネットワークの検出 （7 ページ）、またはLLDP を使用したネットワークの検出 （19 ページ）を参照してください。

  （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。

- ネットワーク階層を設計します。エリア、サイト、ビルディング、フロアなど、デバイスの場所を設定します。

  ネットワーク階層のサイトの作成 （29 ページ）、ビルディングの追加 （30 ページ）、およびビルディングへのフロアの追加 （30 ページ）を参照してください。

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

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

「インベントリに関する情報の表示 （54 ページ）」を参照してください。

（注） すべてのデバイスが管理状態になるのを待つ必要があります。

ステップ 4 サイトへのデバイスの追加

「デバイスをサイトに追加する （59 ページ）」を参照してください。

ステップ 5 AP を追加する場合は、フロア マップに割り当てて配置することをお勧めします。

「AP の追加、配置、および削除 （31 ページ）」を参照してください。

ステップ 6 ネットワークでのユーザ認証に Cisco Identity Services Engine を使用している場合、アシュアランス を設定して Cisco ISE を統合できます。統合することで、アシュアランスのユーザ名やオペレーティングシステムなど、有線クライアントの詳細な情報を参照できます。

「Cisco ISE 版 Cisco DNA Center の統合の設定 （60 ページ）」を参照してください。

ステップ 7 テレメトリを使用して、Syslog、SNMP トラップ、および NetFlow コレクタ サーバを設定します。

テレメトリを使用した Syslog、SNMP トラップ、Netflow コレクタ サーバの設定 （64 ページ）を参照してください

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

「Cisco AI Network Analytics データ収集の設定 （71 ページ）」を参照してください。

ステップ 9 （推奨）最新の機械推論ワークフローにアクセスするには、機械推論ナレッジベースを更新します。

「機械推論ナレッジベースの更新 （75 ページ）」を参照してください。

ステップ 10 アシュアランス アプリケーションの使用を開始します。

Discover Devices

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

ディスカバリについて

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

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 Assurance については、デバイスのループバックアドレスを指定することをお勧めします。

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

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

ディスカバリの前提条件

ディスカバリを実行する前に、次の最小要件を満たしてください。

- Cisco DNA Center によって検出されるデバイスの情報については、「サポート対象デバイスのリスト」を参照してください。
- Cisco DNA Center とデバイス間の最大ネットワーク遅延は 100 ミリ秒であることに注意してください（最大遅延は 200 ミリ秒です）。
- Cisco DNA Center が使用できるように 1 つ以上の SNMP クレデンシャルがデバイス上で設定されていることを確認してください。少なくとも、これには SNMPv2C 読み取りクレデンシャルを使用できます。
- Cisco DNA Center に検出させ、管理委させるデバイスの SSH クレデンシャルを設定します。以下の 2 つの基準のうち、少なくとも 1 つっが満たされる場合、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 （6 ページ）を参照してください。
  -

重要 ディスカバリの実行後にデータを匿名化すると、システムに投入される新規データは匿名になりますが、既存のデータは匿名になりません。

優先管理 IP アドレス

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

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

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

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

設定のガイドラインと制限事項のディスカバリ

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

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

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

CDP を使用したネットワークの検出

Cisco Discovery Protocol（CDP）IP アドレス範囲、または LLDP を使用してデバイスを検出できます。この手順では、CDP を使用してデバイスとホストを検出する方法を示します。ディスカバリ メソッドの詳細については、Discover Your Network Using an IP Address Range （13 ページ）およびLLDP を使用したネットワークの検出 （19 ページ）を参照してください。

（注）

- ディスカバリ機能では、正しい SNMP 読み取り専用（RO）コミュニティ ストリングが必要です。SNMP RO コミュニティ ストリングが指定されていない場合、ベスト エフォートとして、ディスカバリ機能はデフォルトの SNMP RO コミュニティ ストリングを公的に使用します。
- CLI 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 （5 ページ）で説明されているように、ネットワークデバイスを設定します。
- クライアント IP アドレスとしてネットワークデバイスのホストの IP アドレスを設定します。(A host is an end-user device, such as a laptop computer or mobile device.)

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

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

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

a) [ディスカバリ タイプ（Discovery Type）] で、[CDP] をクリックします。

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

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

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

d) をクリックします。

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

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

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

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

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

（注） [ループバック IP を使用（Use Loopback IP）] の使用を選択し、デバイスにループバックインターフェイスがない場合、Cisco DNA Centerは優先管理 IP アドレス （6 ページ）で説明されているロジックを使用して、管理 IP アドレスを選択します。

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

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

すでに作成されているグローバル クレデンシャルのいずれかを選択するか、独自のディスカバリ クレデンシャルを設定します。独自のログイン情報を設定する場合は、[Save] をクリックして現在のジョブに対してのみ保存することもできれば、[Save as global settings] チェックボックスをクリックし、次に [Save] をクリックして、現在または将来のジョブに対して保存することもできます。

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

表 *1 : CLI* クレデンシャル

フィールド	説明
名前/説明	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
[パスワードを有効にする（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 *2 : 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 *3 : SNMPv3* のクレデンシャル

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

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

表 *4 : SNMP Properties*

フィールド	説明
リトライ	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。
タイムアウト	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 *5 : HTTPS* クレデンシャル

フィールド	説明
タイプ	設定している HTTPS クレデンシャルのタイプを指定します。有効なタイプは、[読み取り（Read）] または [書き込み（Write）] です。
Read	最大 5 つの HTTPS 読み取りログイン情報を設定できます。 • [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 5 つの HTTPS 書き込みログイン情報を設定できます。 • [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

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

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

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

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

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

b) 使用する順序でプロトコルをドラッグ アンド ドロップします。

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

• 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。

- 後で検出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、[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タスクを表示します。検出を開始する前に検出タスクを編集するには、[Edit] をクリックします。スケジュールされた検出ジョブを開始する前にキャンセルするには、[Cancel] をクリックします。

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

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

Discover Your Network Using an IP Address Range

IP アドレス範囲、CDP、または LLDP を使用してデバイスを検出できます。この手順では、IP アドレス範囲を使用してデバイスとホストを検出する方法を示します。ディスカバリ メソッドの詳細については、CDP を使用したネットワークの検出 （7 ページ）およびLLDP を使用したネットワークの検出 （19 ページ）を参照してください。

始める前に

ディスカバリの前提条件 （5 ページ）で説明されているように、デバイスには必須のデバイス設定が存在する必要があります。

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

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

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

a) [ディスカバリ タイプ（Discovery Type）] で、[範囲（Range）] をクリックします。

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

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

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

c) （任意） ステップ b を繰り返して、追加の IP アドレス範囲を入力します。

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

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

（注） [ループバック IP を使用（Use Loopback IP）] の使用を選択し、デバイスにループバックインターフェイスがない場合、Cisco DNA Centerは優先管理 IP アドレス （6 ページ）で説明されているロジックを使用して、管理 IP アドレスを選択します。

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

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

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

表 *6 : CLI* クレデンシャル

フィールド	説明
名前/説明	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。
[パスワードを有効にする（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 *7 : 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 *8 : SNMPv3* のクレデンシャル

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

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

表 *9 : SNMP Properties*

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

フィールド	説明
タイムアウト	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 *10* : *HTTPS* クレデンシャル

フィールド	説明
タイプ	設定している HTTPS クレデンシャルのタイプを指定します。有効なタイプは、[読み取り（Read）] または [書き込み（Write）] です。
Read	最大 5 つの HTTPS 読み取りログイン情報を設定できます。 • [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 5 つの HTTPS 書き込みログイン情報を設定できます。 • [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

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

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

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

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

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

b) 使用する順序でプロトコルをドラッグ アンド ドロップします。

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

- 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。
- 後で検出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、[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タスクを表示します。検出を開始する前に検出タスクを編集するには、[Edit] をクリックします。スケジュールされた検出ジョブを開始前にキャンセルする場合は、[Cancel] をクリックします。

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

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

LLDP を使用したネットワークの検出

Link Layer Discovery Protocol（LLDP）、CDP、または IP アドレス範囲を使用してデバイスを検出できます。この手順では、LLDP を使用してデバイスとホストを検出する方法を示します。ディスカバリ メソッドの詳細については、CDP を使用したネットワークの検出 （7 ページ）およびDiscover Your Network Using an IP Address Range （13 ページ）を参照してください。

（注）

- ディスカバリ機能では、正しい SNMP 読み取り専用（RO）コミュニティ ストリングが必要です。SNMP RO コミュニティ ストリングが指定されていない場合、ベスト エフォートとして、ディスカバリ機能はデフォルトの SNMP RO コミュニティ ストリングを公的に使用します。
- CLI 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 （5 ページ）で説明されているように、ネットワークデバイスを設定します。
- クライアント IP アドレスとしてネットワークデバイスのホストの IP アドレスを設定します。(A host is an end-user device, such as a laptop computer or mobile device.)

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

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

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

a) [ディスカバリ タイプ（Discovery Type）] で、[LLDP] をクリックします。

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

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

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

d) をクリックします。

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

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

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

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

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

（注） このオプションを選択し、デバイスにループバック インターフェイスがない場合、Cisco DNA Center は優先管理 IP アドレス （6 ページ）で説明されているロジックを使用して、管理 IP アドレスを選択します。

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

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

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

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

表 *11 : CLI* クレデンシャル

フィールド	説明
名前/説明	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。
[パスワードを有効にする（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 *12 : 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 *13 : SNMPv3* のクレデンシャル

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

フィールド	説明
モード	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（認証モードとして [AuthPriv] または [AuthNoPriv] を選択した場合に有効になります）。次のいずれかの認証タイプを選択します。 • [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。（認証モードとして [AuthPriv] を選択すると有効になります）。次のいずれかのプライバシー タイプを選択します。 • [DES]：CBC DES-56 規格に基づく認証に DES 56-bit 暗号化を追加。 • **AES128**：暗号化の CBC モード AES。 • [None]：プライバシー設定はありません。

フィールド	説明
Privacy Password	DES または AES128 暗号化をサポートしているデバイスで交換されるメッセージを暗号化するための秘密鍵を生成するために使用される SNMPv3プライバシーパスワード。パスワード（またはパスフレーズ）は、8 文字以上にする必要があります。 （注） • 一部のシスコ ワイヤレス コントローラでは、パスワード（あるいはパスフレーズ）は少なくとも12文字以上である必要があります。ワイヤレス コントローラのパスワードの最小要件を必ず確認してください。パスワードに必要な最低限の文字数が守られないと、デバイスではCisco DNA Centerによる検出、監視、管理が行われなくなります。 • パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。

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

表 *14 : SNMP Properties*

フィールド	説明
リトライ	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。
タイムアウト	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 *15 : HTTPS* クレデンシャル

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

フィールド	説明
Read	最大 5 つの HTTPS 読み取りログイン情報を設定できます。 • [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 5 つの HTTPS 書き込みログイン情報を設定できます。 • [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 5 （任意） デバイスとの接続に使用されるプロトコルを設定するには、[詳細（Advanced）] エリアを展開し、次のタスクを実行します。

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

b) 使用する順序でプロトコルをドラッグ アンド ドロップします。

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

- 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。
- 後で検出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、[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タスクを表示します。検出を開始する前に検出タスクを編集するには、[Edit] をクリックします。スケジュールされた検出ジョブを開始前にキャンセルする場合は、[Cancel] をクリックします。

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

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

[検出ジョブの管理（Manage Discovery Jobs）]

ディスカバリ ジョブの停止および開始

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

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

a) **[ディスカバリ（Discoveries）]** ペインで、関連するディスカバリ ジョブを選択します。

b) [Stop] をクリックします。

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

a) **[ディスカバリ（Discoveries）]** ペインで、関連するディスカバリ ジョブを選択します。

b) [Re-discover] をクリックして、選択した検出ジョブを再起動します。

ディスカバリ ジョブの複製

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

始める前に

少なくとも 1 つのディスカバリ ジョブを実行する必要があります。

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

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

ステップ 3 [Clone & Edit] をクリックします。

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

ステップ 4 （任意） 検出ジョブの名前を変更します。

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

ディスカバリ ジョブの削除

アクティブまたは非アクティブに関係なく、検出ジョブを削除できます。

始める前に

少なくとも 1 つのディスカバリ ジョブを実行する必要があります。

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

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

ステップ 3 [削除（Delete）] をクリックします。

ステップ 4 [OK] をクリックして確定します。

ディスカバリ ジョブ情報の表示

使用された設定やクレデンシャルなどの、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 Cisco DNA Center のホームページで、**[ディスカバリ（Discovery）]** をクリックします。

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

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

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

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

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

ネットワーク階層の設計

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

新しいネットワーク インフラストラクチャの設計

[設計（Design）]領域では、ネットワーク全体のデバイスに適用可能な物理トポロジ、ネットワーク設定、デバイスのタイプやプロファイルなど、ネットワークの構造とフレームワークを作成します。既存のインフラストラクチャがない場合は、設計ワークフローを使用します。既存のインフラストラクチャがある場合は、**ディスカバリ**機能を使用します。詳細については、「ディスカバリについて （4 ページ）」を参照してください。

これらのタスクは、[設計（Design）] 領域で実行します。

ステップ 1 ネットワーク階層を作成します。

ステップ 2 グローバル ネットワーク設定を定義します。

ステップ 3 ネットワーク プロファイルを定義します。

About Network Hierarchy

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

ネットワーク階層は、次の事前設定された階層をもちます。

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

実行できるタスクのリストを以下に示します。

- 新しいネットワーク階層を作成する。詳細については、ネットワーク階層のサイトの作成（29 ページ）を参照してください。
- Cisco Prime Infrastructure から既存のネットワーク階層をアップロードする。詳細については、既存のサイト階層をアップロード （34 ページ）を参照してください。

マップ内で使用するイメージファイルに関するガイドライン

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

ネットワーク階層のサイトの作成

Cisco DNA Center 複数の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 Cisco DNA Center のホームページから、**[Design]** > **[Network Profiles]** を選択します。

世界のマップが表示されます。

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

ステップ 3 サイトの名前を入力し、親ノードを選択します。デフォルトでは、**[グローバル（Global）]** が親ノードです。

ステップ 4 [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。

既存の階層をアップロードすることもできます。詳細については、「既存のサイト階層をアップロード（34 ページ）」を参照してください。

ビルディングの追加

ステップ 1 Cisco DNA Center のホームページから、**[設計（Design）] > [ネットワーク階層（Network Hierarchy）]** を選択します。

世界のマップが表示されます。

ステップ 2 [ネットワーク階層（Network Hierarchy）] ウィンドウで、[+サイトの追加（Add Site）] をクリックするか、または左側のツリー ペインの親サイトの隣にある歯車アイコン をクリックして、[ビルディングの追加（Add Building）] を選択します。

ステップ 3 既存の階層をアップロードすることもできます。既存のサイト階層をアップロード （34 ページ）を参照してください。

ステップ 4 ビルディングの名前を入力します。

ステップ 5 [アドレス（Address）]テキストフィールドに、アドレスを入力します。インターネットに接続している場合、アドレスを入力すると同時に、設計アプリケーションが、入力されたアドレスを既知のアドレスを絞り込みます。適切なアドレスがウィンドウに表示されたことを確認したら、それを選択します。既知の所在地を選択すると、[経度（Longitude）]および[緯度（Latitude）]の座標フィールドが自動的に設定されます。

ステップ 6 [Add] をクリックします。

左側のメニューの親サイトの下に、作成したビルディングが追加されます。

ステップ 7 別のエリアまたはビルディングを追加するには、階層フレームで、既存のエリアまたは親ノードにしたいビルディングの隣にある歯車アイコン をクリックします。

ビルディングへのフロアの追加

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

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

ステップ 2 [グローバル（Global）]サイトと以前に作成した領域を展開し、以前に作成したすべてのビルディングを確認します。

ステップ 3 フロアを追加するビルディングの横にある歯車アイコン をクリックし、次に[フロアを追加（Add Floor）] をクリックします。

ステップ 4 フロアの名前を入力します。フロア名には21文字の制限があります。フロア名は文字またはハイフン（-）で始める必要があり、最初の文字に続く文字列は、次の 1 つ以上を含めることができます。

- 大文字または小文字、またはその両方

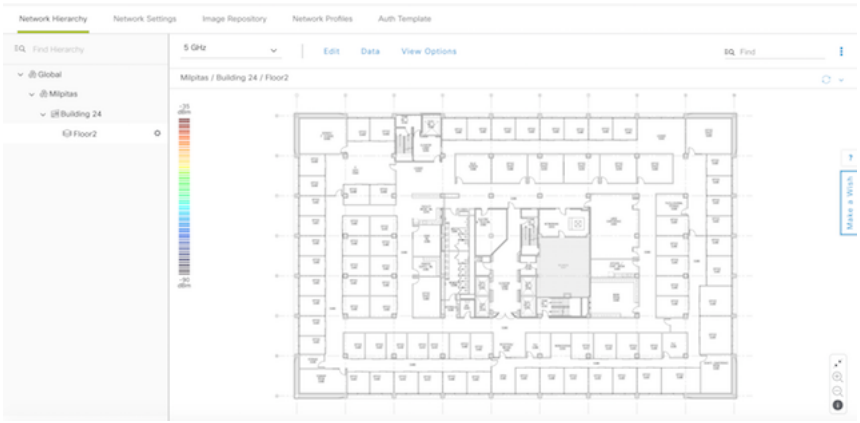
- 数字
- アンダースコア（_）
- ハイフン（-）
- ピリオド(.)
- スペース ( )

ステップ 5 [タイプ（RFモデル）（Type（RF Model））] ドロップダウン リストから無線周波数（RF）モデルを選択して、フロアのタイプを定義します（[屋内天井高（Indoor High Ceiling）]、[屋外オープンスペース（Outdoor Open Space）]、[乾式壁オフィスのみ（Drywall Office Only）]、および [キューブと壁で囲まれたオフィス（Cubes And Walled Offices）]）。これにより、フロアがオープンスペースであるか、乾式壁のオフィスであるかなどを定義します。選択した RF モデルに基づいて、ワイヤレス信号強度、ヒートマップの分布が計算されます。

ステップ 6 フロア プランをマップにドラッグしたり、ファイルをアップロードしたりできます。Cisco DNA Center は、.jpg、.gif、.png、dxf、および .dwg の各ファイル タイプをサポートしています。

マップをインポートした後は、必ず [オーバーレイの可視性（Overlay Visibility）] を [ON] にしてください（[フロア（Floor）]>[表示オプション（View Option）]>[オーバーレイ（Overlays）]）。デフォルトでは、マップをインポートした後にオーバーレイは表示されません。

図 *2:* フロア プランの例



ステップ 7 [追加（Add）] をクリックします。

AP の追加、配置、および削除

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

インベントリにシスコの AP があることを確認してください。デバイスがない場合は、ディスカバリ機能を使用して AP を検出します。「ディスカバリについて （4 ページ）」を参照してください。

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

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

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

ステップ 2 左ペインで、フロアを選択します。

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

ステップ 4 [アクセス ポイント（Access Points）] の横にある [フロア要素（Floor Elements）] パネルで、[追加（Add）] をクリックします。

フロアに割り当てられていないアクセス ポイントが一覧に表示されます。

ステップ 5 [APの追加（Add Aps）] ウィンドウで、アクセス ポイントのチェック ボックスをオンにして AP を一括で選択し、[選択項目の追加（Add Selected）] をクリックします。または、アクセス ポイントに隣接する [追加（Add）] をクリックします。

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

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

ステップ 7 新しく追加した AP はフロア マップの右上隅に表示されます。

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

- AP を配置するには、AP をクリックして、フロア マップ上の適切な場所にドラッグアンドドロップします。または、[選択したAPの詳細（Selected AP Details）] ウィンドウで x 座標と y 座標および AP の高さを更新することもできます。マップ上のアクセスポイントをドラッグすると、その水平（x）と垂直（y）の位置が、テキストフィールドに表示されます。選択すると、右ペインにアクセスポイントの詳細が表示されます。[選択したAPの詳細（Selected AP Details）] ウィンドウには、次の情報が表示されます。
  - [3点による位置決め（Position by 3 points）] : フロア マップに 3 つの点を記入し、その点を使用して AP の位置決めができます。手順は次のとおりです。
    1. [3ポイントによる位置付け（Position by 3 points）] をクリックします。

2. ポイントを定義するには、フロア マップの任意の場所をクリックして最初のポイントの描画を開始します。ポイントの描画を終了するには、再度をクリックします。最初の点までの距離を設定するためにダイアログ ボックスが表示されます。距離をメートル単位で入力し、[距離の設定（Set Distance）] をクリックします。
3. 2 番目と 3 番目の点を同様の方法で定義し、[保存（Save）] をクリックします。

- [2つの壁による位置決め（Position by 2 Walls）] : フロア マップに 2 つの壁を定義し、定義した壁の間に AP の位置決めができます。これによって、2 つの壁の間の AP の位置を把握できるようになります。これは、壁の間の AP の位置を把握するのに役立ちます。

1. [2つの壁による位置付け（Position by 2 Walls）] をクリックします。
2. 最初の壁を定義するには、フロア マップの任意の場所をクリックして線の描画を開始します。線の描画を終了するには、再度をクリックします。最初の壁までの距離を設定するためにダイアログ ボックスが表示されます。距離をメートル単位で入力し、[距離の設定（Set Distance）] をクリックします。
3. 2 番目の壁を同様の方法で定義し、[保存（Save）] をクリックします。

   AP が、壁の間の定義された距離に従って自動的に配置されます。

- [AP名（AP Name）] : AP 名を表示します。
- [APモデル（AP Model）] : 選択したアクセス ポイントの AP モデルを示します。
- [MACアドレス（MAC Address）] : MAC アドレスが表示されます。
- [X] : マップの水平の距離をフィートで入力します。
- [Y] : マップの垂直の距離をフィートで入力します。
- [AP高さ（AP Height）] : アクセス ポイントの高さを入力します。
- [プロトコル（Protocol）] : このアクセス ポイントのプロトコル : [802.11a/n/ac]、[802.11b/g/n]（ハイパー ロケーション AP の場合）、または [802.11a/b/g/n]。
- [アンテナ（Antenna）] : このアクセス ポイントのアンテナ タイプ。

  （注） 外部の AP の場合は、アンテナを選択する必要があります。選択しなければ、AP はマップに存在しません。

- [アンテナ画像（Antenna Image）] : AP イメージが表示されます。
- [アンテナの方向（Antenna Orientation）] : [方位角（Azimuth）] と [仰角（Elevation）] の方向を度数で入力します。
- [方位角（Azimuth）] : 全方向アンテナのパターンでは方位角が存在しなくなるため、このオプションは表示されません。

  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。Cisco DNA Center では、北は 0 または 360 度で、東は 90 度です。

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

ヒート マップは、AP の新しい位置に基づいて生成されます。

Cisco Connected Mobile 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」を参照してください。

ステップ 10 [アクセス ポイント（Access Points）] の横にある [フロア要素（Floor Elements）] パネルで、[削除（Delete）] をクリックします。
[APの削除（Delete APs）] ウィンドウには、割り当てられて、配置されたアクセス ポイントすべてを一覧表示します。

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

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

ネットワーク階層の管理

既存のサイト階層をアップロード

既存のネットワーク階層を含んでいる CSV ファイルまたはマップ アーカイブ ファイルをアップロードすることができます。たとえば、Cisco Prime Infrastructure からエクスポートしたロケーション情報を含む CSV ファイルをアップロードできます。詳細については、Prime Infrastructure からマップをエクスポートする方法に関する マップ アーカイブのエクスポート（35 ページ）を参照してください。

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

ステップ 1 Cisco DNA Center のホームページから、**[Design]** > **[Network Hierarchy]**を選択し、[mport] > [Import Sites] を選択します。

世界地図が右側のペインに表示されます。

ステップ 2 CSV ファイルをドラッグしてドロップするか、または、CSV ファイルがある場所に移動し、**[インポート（Import）]** をクリックして、Cisco Prime Infrastructure グループ CSV ファイルをインポートします。

既存の CSV ファイルがない場合は、**[テンプレートをダウンロード（Download Template）]** をクリックして、編集可能な CSV ファイルをダウンロードして、その後、アップロードすることができます。

ステップ 3 Cisco Prime Infrastructure マップ tar.gz アーカイブファイルをインポートするには**[Import]** > **[Map Import]**をクリックします。

ステップ 4 **[サイト階層アーカイブのインポート（Import Site Hierarchy Archive）]** ダイアログボックスのボックス エリアにマップ アーカイブ ファイルをドラッグしてドロップするか、または、**[クリックして選択（click to select）]** リンクをクリックして、アーカイブ ファイルを参照します。

ステップ 5 **[Save（保存）]** を選択してファイルをアップロードします。

[インポート プレビュー（Import Preview）]ウィンドウが表示され、インポートされたファイルが示されます。

マップ アーカイブのエクスポート

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

ステップ 1 Cisco Prime Infrastructure のユーザー インターフェイスから、**[マップ（Map）]** > **[ワイヤレス マップ（Wireless Maps）]** > **[サイト マップ（新規）（Site Maps (New)）]**を選択します。

ステップ 2 [エクスポート（Export）] ドロップダウン リストから [マップ アーカイブ（Map Archive）] を選択します。

ステップ 3 [サイトの選択（Select Sites）] ウィンドウで、次のように設定します。マップ アーカイブに含めるマップ情報またはキャリブレーション情報を選択できます。

- マップ情報（Map Information）：アーカイブにマップ情報を含めるには、**オンまたはオフ** ボタンをクリックします。
- キャリブレーション情報（Calibration Information）：キャリブレーション情報をエクスポートするには、**オンまたはオフ** ボタンをクリックします。[選択したマップのキャリブレーション情報（Calibration Information for selected maps）] オプション ボタンか、または [すべてのキャリブレーション情報（All Calibration Information）] オプション ボタンをクリックします。[選択したマップのキャリブレーション情報（Calibration Information for selected maps）] を選択すると、選択したサイト マップのキャリブレーション情報がエクスポートされます。[すべてのキャリブレーション情報（All Calibration Information）] を選択すると、選択したマップとともに、システムで使用可能なその他のキャリブレーション情報もエクスポートされます。
- 左側のペインの [サイト（Sites）] で、エクスポートするサイト、キャンパス、ビルディング フロア、または屋外領域の 1 つ以上のチェックボックスをオンにします。すべてのマップをエクスポートするには、[すべて選択（Select All）] チェックボックスをオンにします。

ステップ 4 **[** マップアーカイブを生成（Generate Map Archive） **]** をクリックします。「データをエクスポートしています（`Exporting data is in progress`）」というメッセージが表示されます。

tar ファイルが作成され、ローカル マシンに保存されます。

ステップ 5 [Done] をクリックします。

Search the Network Hierarchy

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

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

サイトの編集

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

ステップ 2 左側のツリー ペインで、編集するサイトに移動します。

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

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

サイトの削除

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

ステップ 2 左側のペインで、削除するサイトに移動します。

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

ステップ 4 削除を確認します。

ビルディングの編集

ステップ 1 **[設計（Design）]** > **[ネットワーク階層（Network Hierarchy）]** を選択します。

ステップ 2 左側のツリー ペインで、編集するビルディングに移動します。

ステップ 3 ビルディングの横にある歯車アイコン ⚙ をクリックし、[ビルディングの編集（Edit Building）] を選択します。

ステップ 4 [ビルディングの編集（Edit Building）] ウィンドウで必要な変更を加え、[更新（Update）] をクリックします。

ビルディングの削除

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

ステップ 2 左側のペインで、削除するビルディングに移動します。

ステップ 3 ビルディングの隣にある歯車アイコン をクリックし、[ビルディングの削除（Delete Building）] を選択します。

ステップ 4 削除を確認します。

（注） ビルディングを削除すると、そのコンテナマップもすべて削除されます。AP は、削除されたマップから未割り当ての状態に移動します。

フロアの編集

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

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

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

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

フロア マップのモニタリング

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

- フロア マップ ウィンドウの右上隅にある [検索（Find）] 機能を使用して、AP、センサー、クライアントなど特定のフロア要素を検索します。検索基準に一致する要素は、右側のペインでテーブルとともにフロア マップに表示されます。マウスをテーブルの上に置くと、フロア マップ上の検索要素が接続線で示されます。

- フロア マップ ウィンドウの右上隅にある アイコンをクリックして、次の作業を行います。

  - フロア プランを PDF としてエクスポートします。

- フロア マップで距離を測定します。
- スケールを設定してフロア面積を変更します。

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

フロア要素とオーバーレイの編集

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

- 次のフロア要素を追加、配置、および削除します。
  - アクセス ポイント（Access Points）
  - 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
  - 障害物
  - ロケーション リージョン
  - Rails
  - マーカー

アクセス ポイントの配置に関するガイドライン

フロア マップに AP を配置する際は、次の注意事項を考慮してください。

- 部屋や建物の屋外の近くにデバイスが置かれるように、カバレッジ領域の境界に沿ってアクセス ポイントを設置します。このようなカバレッジ領域の中心に設置されたアクセス ポイントからは、場合によっては他の全 AP から等距離に見えてしまうデバイスに関して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。

AP の追加、配置、および削除

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

インベントリにシスコの AP があることを確認してください。デバイスがない場合は、ディスカバリ機能を使用して AP を検出します。「ディスカバリについて （4 ページ）」を参照してください。

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

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

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

ステップ 2 左ペインで、フロアを選択します。

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

ステップ 4 [アクセス ポイント（Access Points）] の横にある [フロア要素（Floor Elements）] パネルで、[追加（Add）] をクリックします。

フロアに割り当てられていないアクセス ポイントが一覧に表示されます。

ステップ 5 [APの追加（Add Aps）] ウィンドウで、アクセス ポイントのチェック ボックスをオンにして AP を一括で選択し、[選択項目の追加（Add Selected）] をクリックします。または、アクセス ポイントに隣接する [追加（Add）] をクリックします。

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

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

ステップ 7 新しく追加した AP はフロア マップの右上隅に表示されます。

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

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

       AP が、壁の間の定義された距離に従って自動的に配置されます。
  - [AP名（AP Name）] : AP 名を表示します。
  - [APモデル（AP Model）] : 選択したアクセス ポイントの AP モデルを示します。
  - [MACアドレス（MAC Address）] : MAC アドレスが表示されます。
  - [X] : マップの水平の距離をフィートで入力します。
  - [Y] : マップの垂直の距離をフィートで入力します。
  - [AP高さ（AP Height）] : アクセス ポイントの高さを入力します。
  - [プロトコル（Protocol）] : このアクセス ポイントのプロトコル：[802.11a/n/ac]、[802.11b/g/n]（ハイパー ロケーション AP の場合）、または [802.11a/b/g/n]。
  - [アンテナ（Antenna）] : このアクセス ポイントのアンテナ タイプ。

（注） 外部の AP の場合は、アンテナを選択する必要があります。選択しなければ、AP はマップに存在しません。

- [アンテナ画像（Antenna Image）]：AP イメージが表示されます。
- [アンテナの方向（Antenna Orientation）]：[方位角（Azimuth）] と [仰角（Elevation）] の方向を度数で入力します。
- [方位角（Azimuth）]：全方向アンテナのパターンでは方位角が存在しなくなるため、このオプションは表示されません。

  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。Cisco DNA Center では、北は 0 または 360 度で、東は 90 度です。

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

ヒート マップは、AP の新しい位置に基づいて生成されます。

Cisco Connected Mobile 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」を参照してください。

ステップ 10 [アクセス ポイント（Access Points）] の横にある [フロア要素（Floor Elements）] パネルで、[削除（Delete）] をクリックします。
[APの削除（Delete APs）] ウィンドウには、割り当てられて、配置されたアクセス ポイントすべてを一覧表示します。

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

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

AP のクイック ビュー

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

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

- [Model]：AP モデル番号。
- [Admin/Mode]：AP モードの管理ステータス。
- [Type]：無線タイプ。
- [OP/Admin]：動作ステータスおよび AP モード。
- [Channel]：AP のチャネル番号。
- [Antenna]：アンテナ名。
- [Azimuth]：アンテナの方向。

- [Rxネイバー（Rx Neighbors）] ラジオ ボタンをオンにすると、マップ上に選択した AP に隣接する Rx ネイバーが接続回線とともに表示されます。また、フロア マップには AP が関連付けられているかどうかも AP 名とともに表示されます。
- [Device 360] をクリックすると、特定のネットワーク要素（ルータ、スイッチ、AP、またはシスコ ワイヤレス コントローラ）の 360 度ビューが表示されます。Cisco DNA Assurance ユーザガイド の「*Monitor and Troubleshoot the Health of a Device*」トピックを参照してください。

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

センサーの追加、配置、および削除

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

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

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

ステップ 2 左ペインで、フロアを選択します。

ステップ 3 フロア プランの上にある [編集（Edit）] をクリックします。

ステップ 4 [センサー（Sensors）] の横にある [フロア要素（Floor Elements）] パネルで、[追加（Add）] をクリックします。

ステップ 5 [Add Sensors] ウィンドウで、追加するセンサーのチェックボックスをオンにするか、またはセンサー行の横にある [Add] をクリックしてセンサーを追加します。

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

ステップ 6 フロア マップへセンサーを割り当てたら、[センサーの追加（Add Sensors）] ウィンドウを閉じます。新しく追加したセンサーはフロア マップの右上隅に表示されます。

ステップ 7 センサーを正しく設定するには、[センサー（Sensors）] の横にある [フロア要素（Floor Elements）] ペインで、[位置（Position）] をクリックして、マップに正しくセットします。

ステップ 8 センサーの設定と調整が完了したら、[保存（Save）] をクリックします。

ステップ 9 センサーを削除するには、[センサー（Sensors）] の横にある [フロア要素（Floor Elements）] ペインで、[削除（Delete）] をクリックします。
[Delete Sensors] ウィンドウには、割り当てられて設定されたすべてのセンサーが一覧表示されます。

ステップ 10 削除するセンサーのチェックボックスをオンにし、[Delete Selected] をクリックします。

- すべてのセンサーを削除するには、[すべて選択（Select All）]をクリックし、[選択済みの削除（Delete Selected）] をクリックします。
- フロアからセンサーを削除するには、そのセンサーの横にある [削除（Delete）]アイコンをクリックします。
- [Quick Filter] を使用して、名前、MAC アドレス、モデルのいずれかで検索します。検索では大文字と小文字は区別されません。検索結果がテーブルに表示されます。[削除（Delete）] アイコンをクリックして、フロア領域から 1 つ以上のセンサーを削除します。

カバレッジ エリアの追加

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

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

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

ステップ 2 左ペインで、フロアを選択します。

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

ステップ 4 [オーバーレイ（Overlays）] パネルで、[カバレッジエリア（Coverage Areas）] の横にある [追加（Add）] をクリックします。
[カバレッジの作成（Coverage creation）] ダイアログボックスが表示されます。

ステップ 5 カバレッジ領域を描画するには、[タイプ（Type）] ドロップダウンリストから、[カバレッジエリア（Coverage Area）] を選択します。

1. 定義するエリアの名前を入力し、[カバレッジを追加（Add Coverage）]をクリックします。カバレッジエリアは、頂点が3つ以上の多角形でなければなりません。
2. 輪郭を描く領域に描画ツールを移動します。
3. このツールをクリックして、描線を開始および停止します。
4. エリアの輪郭を描いてからダブルクリックすると、そのエリアが強調表示されます。

（注） マップ上で輪郭を描いた領域を強調表示するには、閉じたオブジェクトである必要があります。

ステップ 6 多角形領域を描画するには、[タイプ（Type）] ドロップダウンリストから、[周辺（Perimeter）] を選択します。

1. 定義する領域の名前を入力し、[Ok] をクリックします。
2. 輪郭を描く領域に描画ツールを移動します。
   - このツールをクリックして、描線を開始および停止します。
   - エリアの輪郭を描いてからダブルクリックすると、そのエリアがページ上で強調表示されます。

ステップ 7 カバレッジ領域を編集するのには、[オーバーレイ（Overlays）]パネルで、[カバレッジエリア（Coverage Areas）] の横にある [編集（Edit）]をクリックします。

使用可能なカバレッジ領域がマップ上で強調表示されます。

ステップ 8 変更を加え、変更後に [保存（Save）] をクリックします。

ステップ 9 カバレッジ領域を削除するのには、[オーバーレイ（Overlays）]パネルで、[カバレッジエリア（Coverage Areas）] の横にある [削除（Delete）] をクリックします。

使用可能なカバレッジ領域がマップ上で強調表示されます。

ステップ 10 カバレッジ エリアにマウス カーソルを合わせ、クリックして削除します。

ステップ 11 削除後に [保存（Save）] をクリックします。

障害物の作成

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

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

ステップ 2 左ペインで、フロアを選択します。

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

ステップ 4 [障害（Obstacles）] の横にある [オーバーレイ（Overlays）] パネルで、[追加（Add）] をクリックします。

ステップ 5 [障害を作成（Obstacle Creation）] ダイアログ ボックスで、[障害のタイプ（Obstacle Type）] ドロップダウン リストから障害のタイプを選択します。作成可能な障害のタイプは、[厚い壁（Thick Wall）]、[薄い壁（Light Wall）]、[重い扉（Heavy Door）]、[軽い扉（Light Door）]、[キュービクル（Cubicle）]、および [ガラス（Glass）] です。
選択した障害のタイプの予測信号損失が自動的に取り込まれます。信号損失は、これらのオブジェクトの周辺の RF 信号強度を計算するために使用されます。

ステップ 6 [障害物の追加（Add Obstacle）] をクリックします。

ステップ 7 障害物を作成する領域に描画ツールを移動します。

ステップ 8 描画ツールをクリックして、描線を開始および停止します。

ステップ 9 エリアの輪郭を描いてからダブルクリックすると、そのエリアが強調表示されます。

ステップ 10 表示される [障害の作成（Obstacle Creation）] ウィンドウで [完了（Done）] をクリックします。

ステップ 11 [保存（Save）] をクリックして、障害をフロア マップに保存します。

ステップ 12 障害を編集するには、[障害（Obstacles）] の隣にある [オーバーレイ（Overlays）] パネルで、[編集（Edit）] をクリックします。

すべての使用可能な障害物がマップ上で強調表示されます。

ステップ 13 変更が完了したら、[保存（Save）] をクリックします。

ステップ 14 障害を削除するには、[障害（Obstacles）] の隣にある [オーバーレイ（Overlays）] パネルで、[削除（Delete）] をクリックします。

すべての使用可能な障害物がマップ上で強調表示されます。

ステップ 15 障害にマウス カーソルを合わせ、クリックして削除します。

ステップ 16 **[保存 (Save)]** をクリックします。

ロケーション リージョンの作成

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

フロア マップ上に包含領域と除外領域を配置するためのガイドライン

- 包含領域と除外領域は多角形領域で表され、最低 3 点で構成される必要があります。
- フロア上の包含リージョンを 1 つだけ定義できます。デフォルトでは、各フロア領域が作成されるときに、各フロア領域に対して包含領域が定義されます。包含領域は、水色の実線で示され、通常はフロア領域全体の輪郭を描きます。
- フロア領域に複数の除外領域を定義することができます。

フロア上の包含リージョンの定義

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

ステップ 2 左ペインで、フロアを選択します。

ステップ 3 **[オーバーレイ（Overlays）]** パネルで、**[ロケーションリージョン（Location Regions）]** の横にある **[追加（Add）]** をクリックします。

ステップ 4 **[ロケーション リージョンの作成（Location Region Creation）]** ダイアログ ウィンドウで、**[包含タイプ（Inclusion Type）]** ドロップダウン リストからオプションを選択します。

ステップ 5 **[位置領域の追加（Add Location Region）]** をクリックします。

包含領域の輪郭を描画するための描画アイコンが表示されます。

ステップ 6 包含領域の定義を開始するには、描画ツールをマップ上の開始ポイントに移動して、1回クリックします。

ステップ 7 含める領域の境界に沿ってカーソルを移動させ、クリックして境界線を終了します。

再びクリックすると、次の境界線を定義できます。

ステップ 8 領域の輪郭が描画されるまでステップ 7 を繰り返したら、描画アイコンをダブルクリックします。

水色の実線によって包含領域が定義されます。

ステップ 9 **[保存 (Save)]** をクリックします。

フロア上の除外リージョンの定義

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

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

ステップ 2 左ペインで、フロアを選択します。

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

ステップ 4 **[オーバーレイ（Overlays）]** パネルで、**[ロケーションリージョン（Location Regions）]** の横にある **[追加（Add）]** をクリックします。

ステップ 5 **[ロケーション リージョンの作成（Location Region Creation）]** ウィンドウで、**[除外タイプ（Exclusion Type）]** ドロップダウン リストから値を選択します。

ステップ 6 [ロケーションリージョン（Location Region）] をクリックします。

除外領域の輪郭を描画するための描画アイコンが表示されます。

ステップ 7 除外領域の定義を開始するには、描画アイコンをマップ上の開始ポイントに移動して、1回クリックします。

ステップ 8 除外するエリアの境界に沿って描画アイコンを移動させます。

1 回クリックして境界線を開始し、再びクリックして境界線を終了します。

ステップ 9 エリアの輪郭が描画されるまで前の手順を繰り返したら、描画アイコンをダブルクリックします。定義された除外領域は、領域が完全に定義されると紫色で網掛けされます。

ステップ 10 さらに除外領域を定義するには、手順 5 から手順 9 を繰り返します。

ステップ 11 すべての除外領域が定義されている場合は、**[保存（Save）]** をクリックします。

ロケーション リージョンの編集

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

ステップ 2 必要な変更を行って、**[保存（Save）]** をクリックします。

ロケーション リージョンの削除

ステップ 1 **[オーバーレイ（Overlays）]**パネルで、**[ロケーション リージョン（Location Regions）]** の横にある **[削除（Delete）]** をクリックします。
使用可能なロケーション リージョンがマップ上で強調表示されます。

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

ステップ 3 **[保存 (Save)]** をクリックします。

レールの作成

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

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

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

ステップ 2 左ペインで、フロアを選択します。

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

ステップ 4 **[レール（Rails）]** の横にある **[オーバーレイ（Overlays）]** パネルで、**[追加（Add）]** をクリックします。

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

描画アイコンが表示されます。

ステップ 6 レール ラインの開始ポイントで描画アイコンをクリックします。ラインの描画を停止するときやラインの方向を変える際は、再びクリックします。

ステップ 7 フロア マップ上にレール ラインを描画したら、描画アイコンを 2 回クリックします。レール ラインはマップ上に表示され、片側は定義されたスナップ幅リージョンに接します。

ステップ 8 **[保存 (Save)]** をクリックします。

ステップ 9 **[オーバーレイ（Overlays）]** パネルで、**[レール（Rails）]** の横にある **[編集（Edit）]** をクリックします。

使用可能なレールがマップ上で強調表示されます。

ステップ 10 変更を加えて、[保存（Save）] をクリックします。

ステップ 11 **[オーバーレイ（Overlays）]** パネルで、**[レール（Rails）]** の横にある **[削除（Delete）]** をクリックします。

使用可能なすべてのレール ラインがマップ上で強調表示されます。

ステップ 12 削除するレール ラインの上にマウスのカーソルを合わせ、クリックして削除します。

ステップ 13 **[保存 (Save)]** をクリックします。

マーカーの配置

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

ステップ 2 左ペインで、フロアを選択します。

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

ステップ 4 **[オーバーレイ（Overlays）]** パネルで、**[マーカー（Markers）]** の横にある **[追加（Add）]** をクリックします。

描画アイコンが表示されます。

ステップ 5 マーカーの名前を入力し、[マーカーの追加（Add Marker）] をクリックします。

ステップ 6 描画アイコンをクリックし、マーカーをマップ上に配置します。

ステップ 7 **[Save（保存）]** をクリックします。

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

使用可能なマーカーがマップ上で強調表示されます。

ステップ 9 変更を加えて、[保存（Save）] をクリックします。

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

使用可能なすべてのマーカーがマップ上で強調表示されます。

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

ステップ 12 **[保存 (Save)]** をクリックします。

フロア ビュー オプション

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

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

アクセス ポイントの表示オプション

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

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

    電力レベルはアクセス ポイントのタイプによって異なります。1000 シリーズの AP では 1 ～ 5 の値、1230 アクセス ポイントでは 1 ～ 7 の値、1240 および 1100 シリーズのアクセス ポイントでは 1 ～ 8 の値をとります。

- [チャネルおよび送信電力（Channel and Tx Power）]：チャネルと送信電力レベルまたは [使用不可（Unavailable）]（アクセス ポイントが接続されていない場合）。
- [使用率（Utilization）]：関連付けられたクライアントデバイスで使用されている帯域幅のパーセンテージ（受信、送信、およびチャネル使用率を含む）。アソシエーションを解除されたアクセス ポイントでは **[Unavailable]**、monitor-only モードのアクセス ポイントでは **[MonitorOnly]** が表示されます。
- [送信使用率（Tx Utilization）]：指定されたインターフェイスの送信（Tx）使用率。
- [受信使用率（Rx Utilization）]：指定されたインターフェイスの受信（Rx）使用率。
- [チャネル使用率（Ch Utilization）]：指定されたアクセス ポイントのチャネル使用率。
- **関連付けられたClients**）]：関連付けられたクライアントの総数。
- [デュアルバンド無線（Dual-Band Radios）]：Cisco Aironet 2800 および 3800 シリーズ アクセス ポイント上の XOR デュアルバンド無線を識別してマークします。
- [ヘルス スコア（Health Score）]：AP のヘルス スコア。
- **問題数**
- **カバレッジの問題**
- **APダウンの問題**

- [ヒートマップ タイプ（Heatmap Type）]：ヒートマップは、変数から取得した値をマップに色として表した、無線周波数（RF）ワイヤレス データのグラフィック表示です。現在のヒートマップは、RSSI予測モデル、アンテナの方向、およびAP送信電力に基づいて計算されます。[ヒートマップ タイプ（Heatmap Type）] ドロップダウンリストから、ヒートマップのタイプ（[なし（None）] または [カバレッジ（Coverage）]）を選択してください。
  - **None**
  - [カバレッジ（Coverage）]：フロア プランにモニタ モード アクセス ポイントがある場合は、カバレッジ ヒートマップを選択できます。カバレッジ ヒートマップでは、モニタ モード アクセス ポイントは除外されます。
- [ヒートマップの不透明度（%）（Heatmap Opacity (%)）]：スライダを 0 ～ 100 の範囲でドラッグして、ヒートマップの不透明度を設定します。
- [RSSIカットオフ（dBm）（RSSI Cut off (dBm)）]：スライダをドラッグして RSSI カットオフ レベルを設定します。RSSI Cutoff の範囲は -60 dBm ～ -90 dBm です。
- [マップの不透明度（%）（Map Opacity (%)）]：スライダをドラッグしてマップの不透明度を設定します。

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

View Options for Sensors

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

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

オーバーレイ オブジェクトの表示オプション

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

- **Coverage Areas**
- **ロケーション リージョン**
- **障害物**
- **レール**
- **Markers**

マップ プロパティの設定

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

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

グローバル マップ プロパティの設定

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

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

データのフィルタリング

アクセスポイントデータのフィルタ処理

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

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

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

センサーデータのフィルタ処理

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

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

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

インベントリの管理

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

インベントリについて

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

また、インベントリ機能は、デバイスの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（ネットワーク設定がデバイスに存在しない場合）。

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 （5 ページ） を参照してください。

初期検出後、Cisco DNA Center は定期的にデバイスをポーリングすることでインベントリを維持します。デフォルトの間隔は 6 時間です。ただし、この間隔は、ネットワーク環境の必要性に応じて、最高 24 時間まで変更できます。詳細については、「デバイスの再同期間隔の更新（53 ページ）」を参照してください。また、デバイスの設定変更によって SNMP トラップがトリガーされ、次にデバイスの再同期がトリガーされます。ポーリングはデバイス、リンク、ホスト、およびインターフェイスごとに実行されます。アクティブ状態が 1 日未満のデバイスのみが表示されます。これによって、古いデバイス データが表示されないようにします。500 個のデバイスのポーリングに約 20 分かかります。

デバイスの再同期間隔の更新

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

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

始める前に

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

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

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

ステップ 2 更新するデバイスを選択します。

ステップ 3 **[アクション（Actions）]** ドロップダウンリストから **[インベントリ（Inventory）]** > **[デバイスの編集（Edit Device）]** の順に選択します。

[デバイスの編集（Edit Device）] ダイアログボックスが表示されます。

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

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

ステップ 6 [更新（Update）] をクリックします。

インベントリに関する情報の表示

[インベントリ（Inventory）] テーブルには、検出された各デバイスの情報が表示されます。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。

始める前に

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

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

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

表 *16 : Inventory*

カラム	説明
デバイス名（Device Name）	デバイスの名前。 名前をクリックすると、ダイアログボックスが開き、次の情報が表示されます。 • [Details]：デバイス名、デバイスタイプ、IPアドレス、シリアル番号、ソフトウェアイメージなどの詳細が表示されます。 • [Configuration]：**show running-config** コマンドの出力で表示される内容に似た詳細な設定情報が表示されます。 （注） この機能は、アクセスポイント (AP) とワイヤレス コントローラにはサポートされていません。したがって、これらのデバイス タイプの場合は設定データは返されません。 • [Interface]：デバイスのインターフェイスの [Interface Name]、[MAC Address]、および [Status] が表示されます。 • [Stack]：MAC アドレス、ロール、状態、プライオリティが表示されます。 （注） [Stack] タブは、プライマリスタックと複数の下位スタックを構成するスイッチスタックデバイスの場合のみ表示されます。 [Stack] タブには、通常のスタックの [Switch Port] > [Neighbor Port] 列が表示されます。 [Stack] タブには、SVL スタックの [SVL Local] > [SVL Remote] および [Dad Interface Name] 列が表示されます。 • [Run Commands]：デバイスで CLI コマンドを実行するためのコマンドランナーを開きます。 • [View 360]：360 ウィンドウが表示されます。360 を開くには、アシュアランス アプリケーションをインストールしている必要があります。 （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
サポートタイプ	以下に示す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。 • [Unsupported]：Cisco DNA Center でテストおよび認定されていない他のすべての Cisco デバイスとサードパーティ製デバイス。これらのデバイスについて、Cisco DNA Center でさまざまな機能をベストエフォートとして試すことができます。ただし、Cisco DNA Center の機能が期待どおりに動作しない場合 、サービスリクエストまたはバグを発生させることは求められていません。 • [Third Party]：デバイスパックは、顧客/ビジネスパートナーによって構築され、認定プロセスを通過しています。サードパーティ製デバイスは、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して修正を依頼する必要があります。
Reachability	以下は、さまざまなステータスのリストです。 • [Connecting]：Cisco DNA Center がデバイスに接続しています。 • [Reachable]：Cisco DNA Center がデバイスに接続されており、CLI を使用して Cisco コマンドを実行できます。 （注） 失敗は、Cisco DNA Center がデバイスに接続されていますが、CLI を使用して Cisco コマンドを実行できなかったことを示します。この状態は通常、デバイスがシスコデバイスではないことを示します。 • [Authentication Failed]：Cisco DNA Center がデバイスに接続されていますが、デバイスのタイプを判別できません。 • [Unreachable]：Cisco DNA Center がデバイスに接続できません。 （注） デバイスに接続できないのは、ディスカバリ ジョブにクレデンシャルが存在しないか、ディスカバリ ジョブに誤ったクレデンシャルが存在するためである場合があります。これに該当する疑いがある場合は、新しいディスカバリ ジョブを実行し、デバイスの正しいクレデンシャルを指定します。
MAC アドレス	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。

カラム	説明
Platform	シスコ製品の部品番号。
シリアル番号（Serial Number）	シスコ デバイスのシリアル番号。
Uptime	デバイスが起動してから、稼働している時間。
デバイス ロール	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。次のデバイス ロールを使用できます。 • **不明** • **アクセス** • **[Core]** • **[Distribution]** • **[Border Router]**
サイト	デバイスに割り当てられているサイト。デバイスがどのサイトにも割り当てられていない場合は、[Assign] をクリックします。[Choose a Site] をクリックし、階層からサイトを選択して [Save] をクリックします。詳細については、「About Network Hierarchy （28 ページ）」を参照してください。
最終更新日	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。
デバイス ファミリ	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（たとえば、Cisco Catalyst 4500 シリーズスイッチ）。
再同期間隔	デバイスのポーリング間隔。この間隔は、[設定（Settings）] でグローバルに設定するか、またはインベントリ内の特定のデバイスに対して設定できます。詳細については、「Cisco DNA Center 管理者ガイド」を参照してください。

カラム	説明
Last Sync Status	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]：デバイスログイン情報がデバイスをインベントリに追加した後に変更された場合、この状態が表示されます。 • [In Progress]：インベントリ収集が発生しています。

ネットワーク デバイスの削除

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

始める前に

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

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

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

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

ステップ 2 削除するデバイスの横にあるチェックボックスをオンにします。

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

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

ステップ 4 [OK] をクリックして、アクションを確認します。

デバイスをサイトに追加する

サイトにデバイスを追加すると、Cisco DNA Center は Syslog として SNMP トラップ サーバを設定し、Syslog レベル 2 が有効になります。

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

ステップ 2 サイトに割り当てるデバイスのチェックボックスをオンにします。

ステップ 3 [Actions] メニューから、**[Provision]** > **[Assign Device to Site]** を選択します。
[Assign Device to Site] スライドインペインが表示されます。

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

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

ステップ 6 **[保存 (Save)]** をクリックします。

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

ステップ 8 [**Assign**] をクリックします。

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

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

Cisco DNA Center リリース 1.3 以降 、Cisco ISE の設定は NCP（ネットワーク制御プラットフォーム）内で一元管理されます。これにより、1 箇所の GUI で Cisco ISE を設定できます。Cisco ISE の設定ワークフローは次のとおりです。

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

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

Cisco ISE 版 Cisco DNA Center の統合の設定

Cisco ISE 版 Cisco DNA Center の統合を設定するには、次の手順を実行します。

始める前に

- Cisco ISE pxGrid サービスを有効にします。
- Cisco ISE の CLI と GUI のユーザアカウントには、同じユーザ名とパスワードを使用する必要があります。
- Cisco DNA Center のバージョンが 1.3 以降であることを確認してください。

（注） Cisco DNA Center は Cisco ISE の内部認証局（CA）を アシュアランス との統合の署名済み証明書として使用します。CA 署名付き証明書を使用するには：

- Cisco DNA Center pxGrid クライアント証明書には、拡張キー使用法（EKU）の拡張子に「クライアント認証」が含まれる必要があります。
- Cisco ISE truststore.jks ファイル内の証明書の発行元である必要があります。

ステップ 1 Cisco DNA Center のホームページで、⚙ > **[System Settings]** > **[Data Platform]** > **[Collectors]** を選択します。**[コレクタ（Collectors）]** ウィンドウが表示されます。

ステップ 2 [COLLECTOR-ISE] をクリックします。

[COLLECTOR-ISE] ウィンドウが表示されます。

（注） [COLLECTOR-ISE] ウィンドウは読み取り専用モードです。

ステップ 3 [Current Configurations] で、[Click to configure] をクリックします。
[Authentication and Policy Servers] ウィンドウが表示されます。

ステップ 4 Cisco ISE サーバを設定するには、認証サーバとポリシー サーバの設定 （61 ページ）を参照してください。

注目 ISE コレクタの設定は存在するものの、[Authentication and Policy Servers] ウィンドウで Cisco ISE が適切に設定されていない場合は、バナーが表示されます。バナーには、[Authentication and Policy Servers] ウィンドウで Cisco ISE の設定を追加するよう Cisco DNA Center の管理者に指示するメッセージが表示されます。

ステップ 5 （任意）ユーザIDやデバイスホスト名などの個人識別データを匿名化（スクランブル）するには、次の手順を実行します。

a) アイコンをクリックし、**[System Settings]** > **[Settings]** を選択します。
b) [Anonymize Data] をクリックします。
[Anonymize Data] ウィンドウが表示されます。
c) [Enable Anonymization] をクリックします。

（注）
- 匿名化を有効にすると、デバイスでは MAC アドレス、IP アドレスなどの匿名以外の情報を使用した検索機能のみ実行できます。
- Cisco DNA Center リリース 1.2.10 以前で匿名化が有効になっていた場合、その設定は、Cisco DNA Center リリース 1.3 にアップグレードしても維持されます。

注意 [Discovery] を実行する前に、匿名化が有効になっていることを確認します。[Discovery] を実行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。

認証サーバとポリシー サーバの設定

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

始める前に

- Cisco ISE を使用してポリシーと AAA 機能の両方を実行する場合、Cisco DNA Center と Cisco ISE が統合されていることを確認します。
- 他の製品（Cisco ISE 以外）で AAA 機能を使用している場合、以下に注意してください。
  - AAA サーバで Cisco DNA Center を登録します。これには、AAA サーバと Cisco DNA Center の共有秘密を定義することが含まれます。
  - AAA サーバで Cisco DNA Center の属性名を定義します。
  - Cisco DNA Center マルチホストクラスタの設定の場合は、AAA サーバのマルチホストクラスタに、すべての個別のホスト IP アドレスと仮想 IP アドレスを定義します。
- Cisco ISE を設定する前に、次のことを確認します。
  1. ネットワークに Cisco ISE バージョン 2.3 以降を導入した。マルチホスト Cisco ISE を導入している場合は、Cisco ISE 管理ノードと統合している。
  2. Cisco ISEノードで SSH を有効にしている。
  3. Cisco DNA Center と統合する予定の Cisco ISE ホストで pxGrid サービスが有効になっており、ERS サービスが読み取り/書き込み操作に対して有効になっている。

（注） Cisco ISE 2.4 以降では、pxGrid 2.0 および pxGrid 1.0 がサポートされています。pxGrid 2.0 では Cisco ISE の展開で最大 4 つの pxGrid ノードを使用できますが、Cisco DNA Center は現在 2 つを超える pxGrid ノードをサポートしていません。

4. Cisco ISE GUI と Cisco ISE シェルのユーザ名とパスワードが同じである。
5. Cisco DNA Center と Cisco ISE の間にプロキシが設定されていない。プロキシサーバが Cisco ISE に設定されている場合、Cisco DNA Center の IP アドレスはそのプロキシサーバをバイパスする必要があります。
6. Cisco DNA Center と Cisco ISE の間にファイアウォールがない。ファイアウォールがある場合は、Cisco DNA Center と Cisco ISE 間の通信を開きます。
7. Cisco DNA Center と Cisco ISE の間の ping が、IP アドレスとホスト名の両方で成功する。
8. Cisco ISE 管理ノード証明書のサブジェクト名または SAN のいずれかに Cisco ISE の IP アドレスまたは FQDN が含まれている。
9. サードパーティ証明書を使用している場合は、証明書の SAN フィールドにすべての IP アドレスが含まれている。
10. Cisco ISE の pxGrid 承認が自動または手動に設定されており、Cisco DNA Center の pxGrid 接続が有効になっている。

ステップ 1 Cisco DNA Center のホームページで、⚙ > **[System Settings]** > **[Settings]** > **[Authentication and Policy Servers]** 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 次の情報を入力して、プライマリ AAA サーバを設定します。

- [Server IP Address]：AAA サーバの IP アドレス。
- [Shared Secret]：デバイス認証のキー。共有秘密情報の長さは、最大 128 文字です。

ステップ 4 AAA サーバ（Cisco ISE 以外）を設定するには [Cisco ISE Server] トグルボタンを [Off] 位置のままにして、次の手順に進みます。

Cisco ISE サーバを設定するには、[Cisco ISE Server] トグルボタンを [On] に設定し、次の各フィールドに情報を入力します

- [Cisco ISE]：サーバが Cisco ISE サーバであるかどうかを示す設定。[Cisco ISE] トグルボタンをクリックして Cisco ISE を有効にします。
- [Username]：Cisco ISE CLI にログインするために使用する名前。

  （注） このユーザにはスーパーユーザの管理権限が必要です。

- [Password]：CLI ユーザ名に対応するパスワード。
- [FQDN]：Cisco ISE サーバの完全修飾ドメイン名（FQDN）。

（注）
- Cisco ISE（**[Administration]** > **[Deployment]** > **[Deployment Nodes]** > **[List]**）で定義されている FQDN をコピーして、このフィールドに直接貼り付けることをお勧めします。
- 入力した FQDN は、Cisco ISE 証明書で定義されている FQDN、共通名（CN）または Subject Alternative Name（SAN）と一致する必要があります。

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

hostname.domainname.com

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

- [Subscriber Name]：Cisco ISE pxGrid サービス登録時の pxGrid クライアントを識別する一意のテキスト文字列（例：`acme`）。サブスクライバ名は、Cisco DNA Center から Cisco ISE への統合時に使用されます。
- [SSHキ Key]：SSH キーは Base64 エンコード形式の Diffie-Hellman 暗号キーです。このキーは、Cisco ISE 管理コンソールへの SSH 接続にセキュリティを提供します。Cisco ISE CLI コマンド **show crypto authorized_keys** および **show crypto host_keys** を使用してキーを取得できます。
- [Virtual IP Address(es)]：Cisco ISE ポリシーサービスノード（PSN）の前面にあるロードバランサの仮想 IP アドレス。異なるロードバランサの背後に複数の PSN ファームがある場合は、最大 6 つの仮想 IP アドレスを入力できます。

（注） 必要な情報を入力すると、Cisco ISE は Cisco DNA Center と 2 つのフェーズを経て統合されます。統合が完了するまでに数分かかります。フェーズごとの統合ステータスは、次のように [Authentication And Policy Servers] ページと [System 360] ページに表示されます。

Cisco ISE サーバ登録フェーズ：

- [Authentication and Policy Servers] ページ：「進行中」
- [System 360] ページ：「プライマリ使用可能」

pxGrid サブスクリプション登録フェーズ：

- [Authentication and Policy Servers] ページ：「アクティブ」
- [System 360] ページ：「プライマリ使用可能」および「PXGRID 使用可能」

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

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

- [Protocol]：[TACACS] と [RADIUS]。[RADIUS] がデフォルトです。両方のプロトコルを選択できます。

注目　Cisco ISE サーバに [TACAS] を選択しない場合、Cisco ISE ノードの設定に使用できません。

- [Authentication Port]：AAA サーバへの認証メッセージのリレーに使用されるポート。デフォルト値は UDP ポート 1812 です。
- [Accounting Port]：AAA サーバへの重要なイベントのリレーに使用されるポート。これらのイベントの情報は、セキュリティと請求の目的で使用されます。デフォルトの UDP ポートは 1813 です。
- [Port]：TACAS によって使用されるポート。デフォルト ポートは 49 です。
- [Retries]：接続の試行が中止される前に、Cisco DNA Center が AAA サーバへの接続を試みた回数。デフォルトの試行回数は 3 回です。
- [Timeout]：接続の試行が中止される前に、デバイスが AAA サーバの応答を待機する時間。デフォルトのタイムアウトは 4 秒です。

ステップ 6　[Add] をクリックします。

ステップ 7　セカンダリサーバを追加するには、ステップ 2 ～ 6 を繰り返します。

テレメトリを使用した Syslog、SNMP トラップ、Netflow コレクタ サーバの設定

ステップ 1　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 （29 ページ）」を参照してください。

ステップ 2　Syslog、SNMP、および Netflow コレクタ サーバの IP アドレスを設定します。次の手順を実行します。

a) Cisco DNA Center のホームページで、**[Design]** > **[Network Settings]** > **[Network]** の順に選択します。

b) [SYSLOG Server] フィールドに、Syslog サーバの IP アドレスを入力します。

（注）　[Cisco DNA Center as syslog server] 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。これは、アシュアランスに必要です。このオプションでは、アシュアランスを有効にして Syslog イベントを使用し、特定の問題をトリガーして [Device 360] ウィンドウに Syslog イベントを表示します。

c) [SNMP サーバ（SNMP Server）] フィールドに、SNMP サーバの IP アドレスを入力します。

（注）　[Cisco DNA Center as snmp server] 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。これは、アシュアランスに必要です。

d) [Time Zone] ドロップダウンリストで、サイトの地理的な場所に基づいて選択したサイトのタイムゾーンを選択します。

（注） デフォルトでは、サーバタイムがタイムゾーン設定で使用されます。タイムゾーンは、デバイスの更新またはプロビジョニングをスケジュールする際に使用されます。

e) [Message of the day (MOTD)] フィールドに、デバイスにログオンするときに MOTD バナーとして表示されるメッセージを入力します。

（注） MOTD のカスタムメッセージは、最大 40 行まで設定できます。各行は 80 文字以下にする必要があります。英数字、大文字と小文字、#以外の特殊文字を使用できます。デバイス上の既存の MOTD メッセージをオーバーライドしない場合は、[MOTD] フィールドの下にあるチェックボックスをオンにします。

ステップ 3 サイトにデバイスを追加します。それにより、Cisco DNA Center からデバイスに設定がプッシュされます。

「デバイスをサイトに追加する （59 ページ）」を参照してください。

ステップ 4 デバイスのテレメトリ指数（TQ）プロファイルを適切なログレベルに適用します。次の手順を実行します。

a) **[Design]** > **[Network Settings]** > **[Network]** を選択し、**[Network Telemetry]** をクリックします。
b) [サイトの表示（Site View）] タブをクリックします。
デバイスのリストが表示されます。
c) ルータ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、次のログレベルを選択します。

- [Maximal Visibility]：これにより、Syslog レベル 6（情報）が有効になります。
- [Optimal Visibility]：これにより、Syslog レベル 6 およびルータ上のネットワークが有効になります。
- **テレメトリの無効化**

ステップ 5 （任意）NetFlow コレクタサーバを追加するには、**[Design]** > **[Network Settings]** > **[Network]** を選択し、[Add Servers] をクリックします。

[サーバの追加（Add Servers）] ウィンドウが表示されます。

a) [NetFlow Collector] のチェックボックスをオンにします。NetFlow Collector サーバが [Network] ウィンドウに追加されます。
b) [NetFlow コレクタ サーバ（NetFlow Collector Server）] エリアで、NetFlow コレクタ サーバの IP アドレスとポート番号を入力します。
c) **[保存 (Save)]** をクリックします。

スイッチの Syslog、SNMP トラップ、および NetFlow コレクタとその他の設定の例

```
crypto pki trustpoint DNAC-CA
 enrollment mode ra
 enrollment terminal
 usage ssl-client
 revocation-check crl none
!
!
crypto pki certificate chain DNAC-CA
 certificate ca 009156FDDCC160F24A
```

```
  308202F7 308201DF A0030201 02020900 9156FDDC C160F24A 300D0609 2A864886
  F70D0101 0B050030 12311030 0E060355 04030C07 6B756265 2D636130 1E170D31
  38303530 33303035 3932335A 170D3231 30313237 30303539 32335A30 12311030
  0E060355 04030C07 6B756265 2D636130 82012230 0D06092A 864886F7 0D010101
  05000382 010F0030 82010A02 82010100 D04771B0 47DF3C65 26AF54CB 32D606B0
  CB9C6023 8CD6FDDD 5E26A340 715F506D AEF2BF13 37D9BA1C C79577A9 1800424F
  5FE5C49C 5694E6E2 A53EFE15 8AC8A186 161A8D88 D44F2F66 BD9D3142 743D20BA
  31DF43A5 E46E5E0B EEACE9BF 68280E1A 80622500 9D031B15 9FD45E18 121C2726
  69B7D768 8EDAC319 7CDBF68C 137A5676 8EE7D5C5 71B34592 CAD1A4B8 590DC27A
  A8172A76 104C0E50 1E0F1D0C 2E649C5B 734E5C9F 0453E248 36937F5E 486191C3
  65667BC9 9393B864 C0674594 9194EF4E C2B4845E 1ACCEB3F 82FE0C48 1548136C
  53015248 0FF8DEA5 3F4281BB 79A3183A 22E76AAF 20D91016 94CC9339 BF2F9C4A
  3D345E2F 8DDC0EA3 453D5FEB 670C9F6B 02030100 01A35030 4E301D06 03551D0E
  04160414 63528371 86225027 1A79B16E D2645368 929A96C0 301F0603 551D2304
  18301680 14635283 71862250 271A79B1 6ED26453 68929A96 C0300C06 03551D13
  04053003 0101FF30 0D06092A 864886F7 0D01010B 05000382 01010094 5751DB9B
  6C460EB0 892A32F2 450AAEFB 5C7D41AA 8E7CCD3D ECE78771 F3AD1CA2 76444620
  90CAB088 BE07A2ED A2D13325 019568BB F1FE9EAC 123A6A7F C81277D5 74556B3B
  4BBD6691 785EB7CD 581A95F0 8306101D 54AE51D0 02DB7F32 C210A14E 449A1F57
  02815C71 E8A53C33 1828B08D 4CCE3707 1FE4B867 5A88E1A2 9E8E106A 87F43E69
  37234473 F00E1773 733CAF76 E5807A00 158F6501 E1B45537 17E3F2BE BBC520D0
  C54EE06C B18A30F1 AC4D1A2E 809DFFB0 B282E318 18C95393 23A13FA8 45DBC79D
  01A90F87 C9262FDB DDF258AD 86E70B64 1426B072 3F31BAD8 14F4CAC5 FC039912
  E288A1CF 5F2EC94C ED0B820B 3AF84E3F 32C501F3 5E71A656 BEABE3
      quit
interface GigabitEthernet1/0/2
 ip device tracking maximum 10
!
interface GigabitEthernet1/0/3
 ip device tracking maximum 10

!
flow exporter 10.4.48.218
 destination 10.4.48.218
!
snmp-server community cisco RO
snmp-server community cisco123 RW
!
logging host 7.7.7.7
!
snmp-server community cisco1 RO
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps flowmon
snmp-server enable traps transceiver all
snmp-server enable traps call-home message-send-fail server-fail
snmp-server enable traps rf
snmp-server enable traps memory
snmp-server enable traps wireless bsnMobileStation bsnAccessPoint bsnRogue bsn80211Security bsnAutoRF

 bsnGeneral SI mobility mfp RRM AP rogue client
snmp-server enable traps cpu threshold
snmp-server enable traps tty
snmp-server enable traps eigrp
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-change nssa-trans-change
snmp-server enable traps ospf cisco-specific state-change shamlink interface
snmp-server enable traps ospf cisco-specific state-change shamlink neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific retransmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server enable traps auth-framework sec-violation
```

```
snmp-server enable traps flash insertion removal
snmp-server enable traps power-ethernet group 1
snmp-server enable traps power-ethernet police
snmp-server enable traps energywise
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps license
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps stackwise
snmp-server enable traps port-security
snmp-server enable traps fru-ctrl
snmp-server enable traps entity
snmp-server enable traps trustsec-sxp conn-srcaddr-err msg-parse-err conn-config-err binding-err
conn-up conn-down binding-expn-fail oper-nodeid-change binding-conflict
snmp-server enable traps trustsec-server radius-server provision-secret
snmp-server enable traps trustsec authz-file-error cache-file-error keystore-file-error
keystore-sync-fail random-number-fail src-entropy-fail
snmp-server enable traps trustsec-interface unauthorized sap-fail authc-fail supplicant-fail authz-fail
snmp-server enable traps trustsec-policy peer-policy-updated authz-sgacl-fail
snmp-server enable traps bgp cbgp2
snmp-server enable traps cef resource-failure peer-state-change peer-fib-state-change inconsistency
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps event-manager
snmp-server enable traps hsrp
snmp-server enable traps ipmulticast
snmp-server enable traps isis
snmp-server enable traps local-auth
snmp-server enable traps msdp
snmp-server enable traps ospfv3 state-change
snmp-server enable traps ospfv3 errors
snmp-server enable traps pim neighbor-change rp-mapping-change invalid-pim-message
snmp-server enable traps vstack
snmp-server enable traps bridge newroot topologychange
snmp-server enable traps stpx inconsistency root-inconsistency loop-inconsistency
snmp-server enable traps syslog
snmp-server enable traps ipsla
snmp-server enable traps ike policy add
snmp-server enable traps ike policy delete
snmp-server enable traps ike tunnel start
snmp-server enable traps ike tunnel stop
snmp-server enable traps ipsec cryptomap add
snmp-server enable traps ipsec cryptomap delete
snmp-server enable traps ipsec cryptomap attach
snmp-server enable traps ipsec cryptomap detach
snmp-server enable traps ipsec tunnel start
snmp-server enable traps ipsec tunnel stop
snmp-server enable traps ipsec too-many-sas
snmp-server enable traps errdisable
snmp-server enable traps mac-notification change move threshold
snmp-server enable traps vlan-membership
snmp-server enable traps bulkstat collection transfer
snmp-server enable traps vrfmib vrf-up vrf-down vnet-trunk-up vnet-trunk-down
snmp-server host 8.8.8.8 public
!
ip http client source-interface GigabitEthernet1/0/1
!
ip ssh source-interface GigabitEthernet1/0/1
```

ルータの Syslog、SNMP トラップ、および NetFlow コレクタとその他の設定の例

```
crypto pki trustpoint DNAC-CA
 enrollment mode ra
```

```
 enrollment terminal
 usage ssl-client
 revocation-check crl none
!
crypto pki certificate chain DNAC-CA
 certificate ca 00D97DCBDFA3EB517E
  308202F7 308201DF A0030201 02020900 D97DCBDF A3EB517E 300D0609 2A864886
  F70D0101 0B050030 12311030 0E060355 04030C07 6B756265 2D636130 1E170D31
  38303531 35303531 3131375A 170D3231 30323038 30353131 31375A30 12311030
  0E060355 04030C07 6B756265 2D636130 82012230 0D06092A 864886F7 0D010101
  05000382 010F0030 82010A02 82010100 A68A3FCD 5423262C CD10E16B A0517BCF
  17E085F5 705B26E1 7B1251F2 353CB489 A049FB68 00E65F21 C15E14B5 D5EFF90C
  8B78CBC1 9F749819 466E5924 0B1780F2 4B31CDA3 1E0EED5D FFF4D29F FE935413
  DAD2DB46 9778ACD8 44FC1AD8 9042BE47 11ED9E29 97D9B4C9 E51C3767 98AE61B0
  38254DAB F4417F8B AE80695E 5236D36C 47052F02 E2E234A6 564D71D4 44F09D98
  C1B5BF3B CDED2108 DA04C6B0 7E9A8EE5 036F4913 575C1567 97EEC40A AA53E91A
  7E4E2419 D990E031 4E40F561 F766A4E2 B76B4281 E95AB7BA 01F6A42C 1EF040BD
  97358EBC 9A9BC46F C127DE3E FA1841F9 41B45392 4E546AE3 396D1D25 4B2DD897
  6D5CD7AF 6E342548 2CF1BA48 DAA51C21 02030100 01A35030 4E301D06 03551D0E
  04160414 A811B663 0573E872 B4913BEF 698A2405 9A92D2F5 301F0603 551D2304
  18301680 14A811B6 630573E8 72B4913B EF698A24 059A92D2 F5300C06 03551D13
  04053003 0101FF30 0D06092A 864886F7 0D01010B 05000382 0101007B 67E62397
  B47E806D 57E5F75B 18F567A5 1373E05E FB381F07 0F306852 A3DF1048 AB3D0F2C
  2CE40F77 8251F171 1B82E671 0BA0DC05 4694DA48 D13BC4FC 1482B0A1 6ECD607F
  EB03C9B9 A6BB99C3 649E1957 DD48E0E5 60FDEF22 E468997B 77BB91AB 4CC4B319
  1A21C571 804AEC36 BEC14C8F 78D1C133 E65B5D18 F4E310B6 3353EF73 511189CF
  CF47C243 8D40A0B3 738BB94E E6434F74 D20D3E99 D0E96858 B25DC9C7 08CAF030
  AE7A68C6 F9BC351C 97FEDF0E 76525B07 60E13693 583BAC0B 7AFB3DA4 8EF24861
  FAC8B688 0FB24D79 3E16B380 38A39B82 AD8D566B 16883040 A5415C5D 82E6C1BF
  AEDEBE91 12F4208B 88C9FC28 3A12B3EE 7EDFBA7B 588C355C D94B29
   quit
!
flow exporter 10.4.48.218
destination 10.4.48.218
!
snmp-server community cisco RO
snmp-server community cisco123 RW
!
logging host 7.7.7.7
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps vrrp
snmp-server enable traps pfr
snmp-server enable traps flowmon
snmp-server enable traps ds1
snmp-server enable traps entity-perf throughput-notif
snmp-server enable traps ds3
snmp-server enable traps call-home message-send-fail server-fail
snmp-server enable traps tty
snmp-server enable traps eigrp
snmp-server enable traps casa
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-change nssa-trans-change
snmp-server enable traps ospf cisco-specific state-change shamlink interface
snmp-server enable traps ospf cisco-specific state-change shamlink neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific retransmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server enable traps license
snmp-server enable traps smart-license
snmp-server enable traps cef resource-failure peer-state-change peer-fib-state-change inconsistency
snmp-server enable traps memory bufferpeak
```

```
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps dsp card-status
snmp-server enable traps dsp oper-state
snmp-server enable traps dsp video-usage
snmp-server enable traps dsp video-out-of-resource
snmp-server enable traps fru-ctrl
snmp-server enable traps entity
snmp-server enable traps event-manager
snmp-server enable traps frame-relay multilink bundle-mismatch
snmp-server enable traps frame-relay
snmp-server enable traps frame-relay subif
snmp-server enable traps hsrp
snmp-server enable traps ip local pool
snmp-server enable traps pppoe
snmp-server enable traps cpu threshold
snmp-server enable traps syslog
snmp-server enable traps l2tun session
snmp-server enable traps l2tun pseudowire status
snmp-server enable traps atm subif
snmp-server enable traps pki
snmp-server enable traps ethernet evc status create delete
snmp-server enable traps ether-oam
snmp-server enable traps ethernet cfm cc mep-up mep-down cross-connect loop config
snmp-server enable traps ethernet cfm crosscheck mep-missing mep-unknown service-up
snmp-server enable traps entity-state
snmp-server enable traps entity-qfp mem-res-thresh throughput-notif
snmp-server enable traps adslline
snmp-server enable traps vdsl2line
snmp-server enable traps flash insertion removal lowspace
snmp-server enable traps srp
snmp-server enable traps entity-diag boot-up-fail hm-test-recover hm-thresh-reached scheduled-test-fail
snmp-server enable traps isdn call-information
snmp-server enable traps isdn layer2
snmp-server enable traps isdn chan-not-avail
snmp-server enable traps isdn ietf
snmp-server enable traps cnpd
snmp-server enable traps bfd
snmp-server enable traps otn
snmp-server enable traps ipsla
snmp-server enable traps sonet
snmp-server enable traps dlsw
snmp-server enable traps resource-policy
snmp-server enable traps stpx inconsistency root-inconsistency loop-inconsistency
snmp-server enable traps c3g
snmp-server enable traps LTE
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps firewall serverstatus
snmp-server enable traps trustsec-sxp conn-srcaddr-err msg-parse-err conn-config-err binding-err
conn-up conn-down binding-expn-fail oper-nodeid-change binding-conflict
snmp-server enable traps lisp
snmp-server enable traps aaa_server
snmp-server enable traps dhcp
snmp-server enable traps auth-framework sec-violation
snmp-server enable traps pw vc
snmp-server enable traps mpls rfc ldp
snmp-server enable traps mpls ldp
snmp-server enable traps mpls rfc traffic-eng
snmp-server enable traps mpls traffic-eng
snmp-server enable traps mpls fast-reroute protected
snmp-server enable traps rsvp
```

```
snmp-server enable traps ipmulticast
snmp-server enable traps msdp
snmp-server enable traps pim neighbor-change rp-mapping-change invalid-pim-message
snmp-server enable traps mvpn
snmp-server enable traps pimstdmib neighbor-loss invalid-register invalid-join-prune rp-mapping-change

 interface-election
snmp-server enable traps isis
snmp-server enable traps bgp cbgp2
snmp-server enable traps ospfv3 state-change
snmp-server enable traps ospfv3 errors
snmp-server enable traps nhrp nhs
snmp-server enable traps nhrp nhc
snmp-server enable traps nhrp nhp
snmp-server enable traps nhrp quota-exceeded
snmp-server enable traps ike policy add
snmp-server enable traps ike policy delete
snmp-server enable traps ike tunnel start
snmp-server enable traps ike tunnel stop
snmp-server enable traps ipsec cryptomap add
snmp-server enable traps ipsec cryptomap delete
snmp-server enable traps ipsec cryptomap attach
snmp-server enable traps ipsec cryptomap detach
snmp-server enable traps ipsec tunnel start
snmp-server enable traps ipsec tunnel stop
snmp-server enable traps ipsec too-many-sas
snmp-server enable traps gdoi gm-start-registration
snmp-server enable traps gdoi gm-registration-complete
snmp-server enable traps gdoi gm-re-register
snmp-server enable traps gdoi gm-rekey-rcvd
snmp-server enable traps gdoi gm-rekey-fail
snmp-server enable traps gdoi ks-rekey-pushed
snmp-server enable traps gdoi gm-incomplete-cfg
snmp-server enable traps gdoi ks-no-rsa-keys
snmp-server enable traps gdoi ks-new-registration
snmp-server enable traps gdoi ks-reg-complete
snmp-server enable traps gdoi ks-role-change
snmp-server enable traps gdoi ks-gm-deleted
snmp-server enable traps gdoi ks-peer-reachable
snmp-server enable traps gdoi ks-peer-unreachable
snmp-server enable traps bulkstat collection transfer
snmp-server enable traps alarms informational
snmp-server enable traps ethernet cfm alarm
snmp-server enable traps rf
snmp-server enable traps transceiver all
snmp-server enable traps mpls vpn
snmp-server enable traps mpls rfc vpn
snmp-server enable traps vrfmib vrf-up vrf-down vnet-trunk-up vnet-trunk-down
snmp-server host 8.8.8.8 public

ip http client source-interface GigabitEthernet0/0/1
!
ip ssh source-interface GigabitEthernet0/0/1
```

シスコ ワイヤレス コントローラの Syslog、SNMP トラップ、および NetFlow コレクタとその他の設定の例

```
config snmp community create cisco
config snmp community create cisco123
config snmp community mode enable cisco
config snmp community ipaddr 0.0.0.0 0.0.0.0 cisco
config snmp community mode enable cisco123
config snmp community accessmode rw cisco123
config snmp community ipaddr 0.0.0.0 0.0.0.0 cisco123
```

```
config network assurance server idtoken 1 6b5af7c9808a0b1b7824fc9a801b5478
de751722396b0fe0b221b3be71f3a94ef2fe0716 16 88664b59c40e1f1f2ffc14097897ed620000000
config network assurance server url https://10.4.48.132
config network assurance on-change enable

config flow create exporter 10.4.48.218 10.4.48.218 port 6007
config logging level critical
config logging syslog level 2
config logging syslog facility syslog
config logging syslog host 7.7.7.7
config snmp trapreceiver create 8.8.8.8 8.8.8.8
config snmp trapreceiver ipsec profile none 8.8.8.8
config snmp trapreceiver mode enable 8.8.8.8

config trapflags client enhanced-802.11-deauthenticate enable
config trapflags client enhanced-802.11-associate enable
config trapflags client max-warning-threshold enable
config trapflags client 802.11-authfail disable
config trapflags client 802.11-associate disable
config trapflags client 802.11-disassociate disable
config trapflags client authentication disable
config trapflags client webauthuserlogout enable
config trapflags client 802.11-deauthenticate disable
config trapflags client neighborclientsignal disable
config trapflags client webauthuserlogin enable
config trapflags client 802.11-assocfail disable
config trapflags client excluded enable
config trapflags client enhanced-802.11-stats enable
config trapflags client enhanced-authentication enable
config trapflags client nac-alert enable
config trapflags client enhanced-802.11-disassociate-stats disable
```

Cisco AI Network Analytics データ収集の設定

Cisco AI Network Analytics が、ワイヤレスコントローラおよびサイト階層から Cisco DNA Center にネットワークイベントデータをエクスポートできるようにするには、次の手順を実行します。

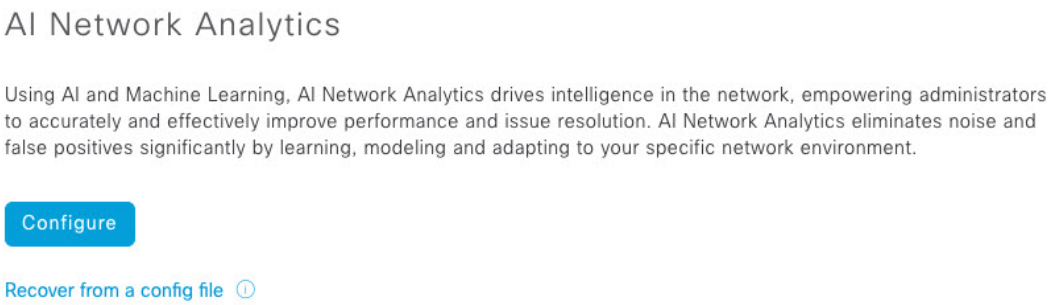
始める前に

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

• [api.euc1.prd.kairos.ciscolabs.com]（EU 中央地域）

ステップ 1 Cisco DNA Center のホームページで、⚙ > **[System Settings]** > **[Settings]** > **AI ネットワーク分析** の順に選択します。
[**AI ネットワーク分析**（SIP MWI notification mechanism）] ウィンドウが表示されます。

図 *3 : [AI Network Analytics]* ウィンドウ



ステップ 2 次のいずれかを実行します。

• アプライアンスに以前のバージョンの Cisco AI Network Analytics がインストールされている場合は、次の手順を実行します。

1. [Recover from a config file] をクリックします。

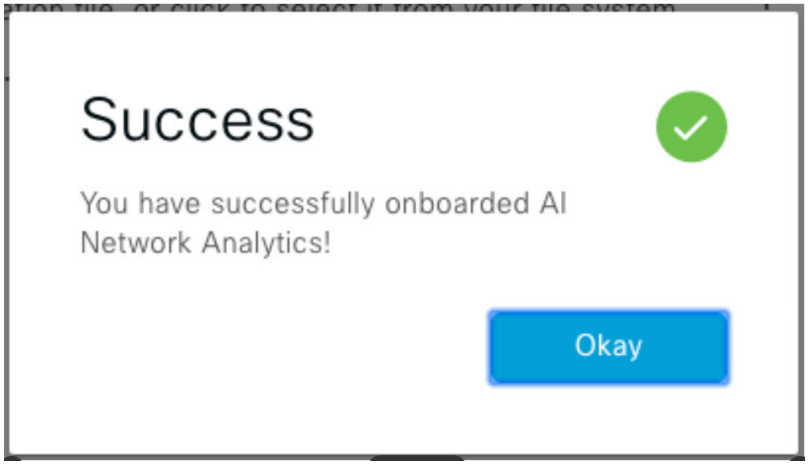
   [Restore AI ネットワーク分析] ウィンドウが表示されます。

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

3. [Restore] をクリックします。

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

図 *4 : [Success]* ダイアログボックス



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

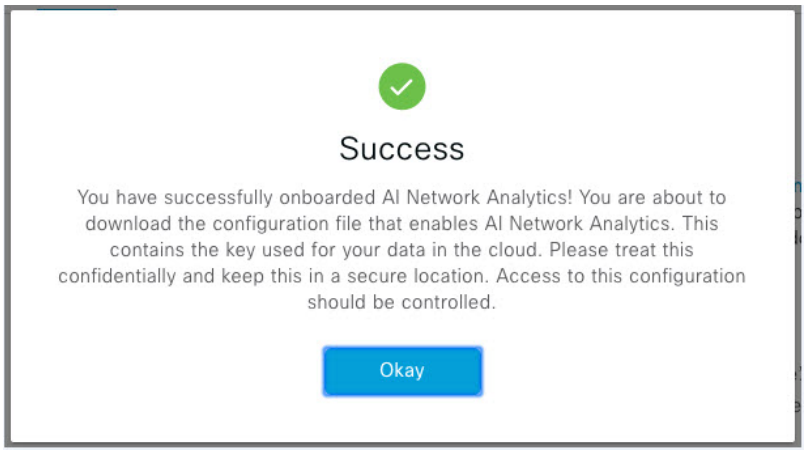
1. [Configure] をクリックします。
2. [Where should we securely store your data?] 領域で、データを保存する場所を選択します。[Europe (Germany)] または [US East (North Virginia)] を選択できます。

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

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

   Cisco AI Network Analytics が有効になるまでに数分かかる場合があり、その後、[Success] ダイアログボックスが表示されます。

図 *5 : [Success]* ダイアログボックス



ステップ 3 [Success] ダイアログボックスで [Okay] をクリックします。
AI ネットワーク分析 ウィンドウが表示され、[Cloud Connection] エリアに が表示されます。

ステップ 4 （推奨）**AI ネットワーク分析** ウィンドウで、[Download Configuration] ファイルをクリックします。

関連トピック

Cisco AI Network Analytics データ収集の無効化 （74 ページ）

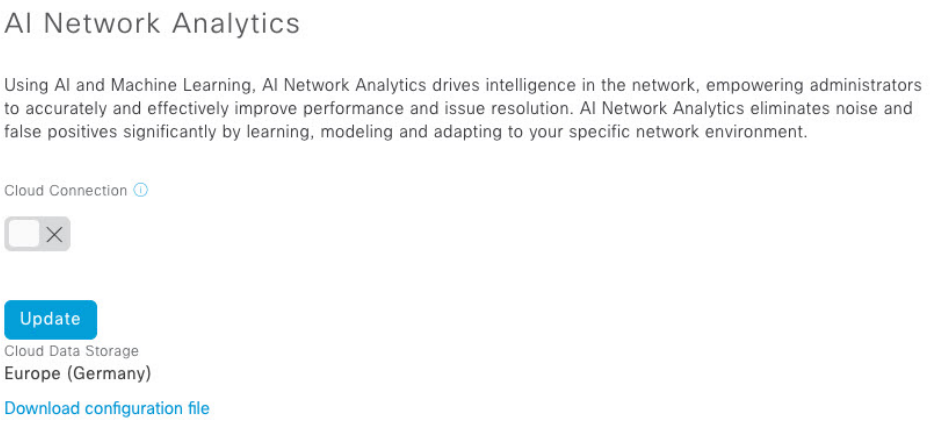
Cisco AI Network Analytics データ収集の無効化

Cisco AI Network Analytics データ収集を無効にするには、 Cisco AI Network Analytics クラウドサービスへの接続をオフ（無効）にする必要があります。これにより、AI駆動型の問題、ネットワークヒートマップ、サイトの比較、ピアの比較など、Cisco AI Network Analytics 関連のすべての機能が無効になります。

ステップ 1 Cisco DNA Center のホームページで、 > **[System Settings]** > **[Settings]** > **AI ネットワーク分析** の順に選択します。
[**AI ネットワーク分析**（SIP MWI notification mechanism）] ウィンドウが表示されます。

ステップ 2 [Cloud Connection] エリアで、 が表示されるように、ボタンをクリックしてオフにします。

図 *6* : データ収集を無効にした *[AI Network Analytics]* ウィンドウ



ステップ 3 [Update] をクリックします。

ステップ 4 Cisco AI Network Analytics クラウドからネットワークデータを削除するには、Cisco Technical Response Center（TAC）に連絡してサポートリクエストをオープンしてください。

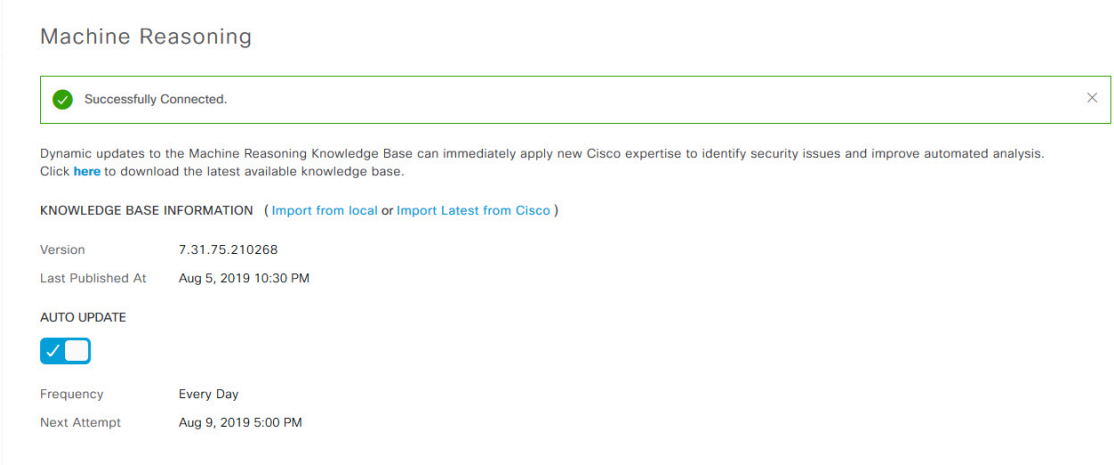
ステップ 5 （任意）以前の設定が間違って配置されている場合は、[Download configuration file] をクリックします。

機械推論ナレッジベースの更新

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

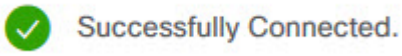
ステップ 1 Cisco DNA Center のホームページで、歯車アイコン（⚙）をクリックし、**[System Settings]** > **[Settings]** > **[Machine Reasoning]** の順に選択します。
[Machine Reasoning] ウィンドウが表示されます。

図 *7 : [Machine Reasoning]* ウィンドウ



ステップ 2 （推奨）Cisco DNA Center で機械推論ナレッジベースを自動的に更新するには、[Auto Update] をクリックして有効にし、✓マークが表示されるようにします。
次の更新の頻度、日付、および時刻は、[Frequency] および [Next Attempt] エリアに表示されます。

（注） 自動更新を実行できるのは、 Cisco DNA Center がクラウド内の機械推論エンジンに正常に接続されている場合のみです。



ステップ 3 手動更新を実行するには、次のいずれかを実行します。

- 機械推論ナレッジベースをローカルマシンにダウンロードして、Cisco DNA Center にインポートします。次の手順を実行します。

  1. ハイパーリンクされた**ここ**のテキストをクリックします。

     ```
     Dynamic updates to the Machine Reasoning knowledge base can immediately apply new Cisco
     expertise to identify security issues
     and improve automated analysis.
     Click here to download the latest available knowledge base.
     ```

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

  2. ダウンロードしたファイルを開くか、ローカルマシンの目的の場所に保存して、[OK] をクリックします。

  3. ダウンロードした機械推論ナレッジベースをローカルマシンから Cisco DNA Center にインポートするには、[Import from local] をクリックします。

- 最新の機械推論ナレッジベースをシスコから直接 Cisco DNA Center にインポートするには、[Import Latest from Cisco] をクリックします。[Success] ポップアップウィンドウが、更新のステータスとともに右下隅に表示されます。

ローカリゼーションの有効化

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

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

デフォルトの言語を変更するには、次のタスクを実行します。

ステップ 1 ブラウザでロケールを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 *8 :* ローカライズされたログイン画面の例