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 の制限事項と制約事項

アシュアランス では、ネットワークアドレス変換（NAT）を介して接続されたデバイスをサポートしません。

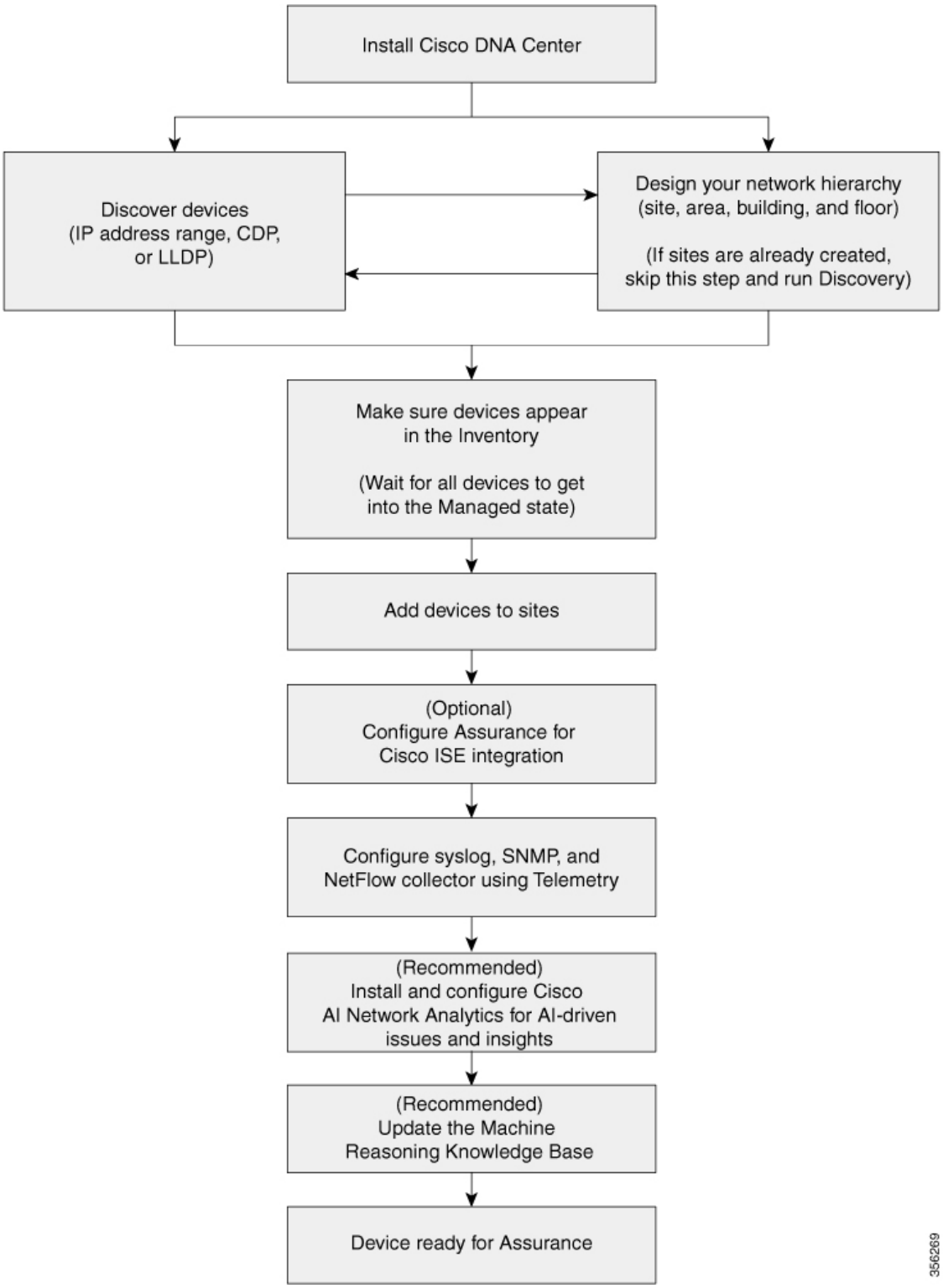
基本的な設定のワークフロー

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。

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 DNA Center ユーザガイド と併用してください。

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



始める前に

アシュアランス の制限事項と制約事項 （1 ページ）を参照してください。

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。

  IP アドレス範囲を使用したネットワークの検出 （15 ページ）、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 （23 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 のウィンドウでは、データが表示されません。

- 新しいネットワーク階層を設計するか、既存のものを使用します。

  新しいネットワーク階層の設計 （33 ページ）または既存の Cisco ネットワーク階層の使用 （33 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） デバイスをサイトに追加する前に、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 （61 ページ）を参照してください。

ステップ 5 AP がある場合は、フロアマップに追加することをお勧めします。

ステップ 6 ネットワークでのユーザー認証に Cisco Identity Services Engine（ISE）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ー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 向けの Cisco ISE の設定について （62 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 サーバーを設定します。

テレメトリを使用した Syslog、SNMP トラップ、NetFlow コレクタサーバー、および有線クライアント データ収集の設定 （66 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 （67 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 （70 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。

デバイスの検出

Cisco DNA Center ディスカバリ機能を使用してネットワーク内のデバイスをスキャンします。

検出の概要

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

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

デバイスは次の 3 つの方法で検出できます。

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

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

- [CDP Level] と [LLDP Level]：CDP または LLDP をディスカバリ方式として使用する場合は、CDP レベルまたはLLDP レベルを設定して、スキャンするシードデバイスからのホップ数を指定できます。デフォルトのレベル 16 では、大規模なネットワークの場合に時間がかかる可能性があります。そのため、検出する必要があるデバイスが少ない場合は、このレベルをより低い値に設定できます。
- [Subnet Filters]： IP アドレスの範囲を使用する場合は、特定の IP サブネット内のデバイスをディスカバリで無視するように指定できます。
- [Preferred Management IP]：CDP、LLDP、または IP アドレスの範囲のいずれを使用する場合でも、Cisco DNA Center がデバイスの任意の IP アドレスを追加するか、デバイスのループバックアドレスのみを追加するかを指定できます。

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

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

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

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、 Cisco DNA Center 互換性マトリクスを参照してください。
- Cisco DNA Center とデバイス間の望ましいネットワーク遅延は 100 ミリ秒のラウンドトリップ時間（RTT）であることに注意してください（最大遅延は 200 ミリ秒 RTT です）。
- Cisco DNA Center が使用できるように 1 つ以上の SNMP クレデンシャルがデバイス上で設定されていることを確認してください。少なくとも、これには SNMPv2C 読み取りクレデンシャルを使用できます。
- Cisco DNA Center に検出させ、管理委させるデバイスの SSH クレデンシャルを設定します。以下の基準のうち、少なくとも 1 つが満たされる場合、Cisco DNA Center はデバイスを検出し、そのインベントリに追加します。
  - デバイスへの SSH アクセスのために Cisco DNA Center が使用するアカウントが、特権 EXEC モード（レベル 15）である。
  - ディスカバリ ジョブで設定される CLI クレデンシャルの一部としてデバイスのイネーブルパスワードを設定している。詳細については、設定のガイドラインと制限事項のディスカバリ （6 ページ）を参照してください。

優先管理 IP アドレス

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

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

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

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

設定のガイドラインと制限事項のディスカバリ

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

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

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

CDP を使用したネットワークの検出

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

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

始める前に

- ネットワークデバイスで CDP を有効にします。
- ディスカバリの前提条件 （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 IP アドレスを設定します。(A host is an end-user device, such as a laptop computer or mobile device.)

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

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

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

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

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

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

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

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

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

    （注） [Use Loopback IP] の使用を選択し、デバイスにループバック インターフェイスがない場合、Cisco DNA Centerは優先管理 IP アドレス （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 5 [Credentials] エリアを展開し、使用するログイン情報を選択します。

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

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

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

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

ステップ 8 CLI クレデンシャルの場合は、次の手順を実行します。

a) 次のフィールドを設定します。

表 *1 : CLI* クレデンシャル

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

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

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

c) [Save] をクリックします。

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

a) 次のフィールドを設定します。

表 *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。

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

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

c) [Save] をクリックします。

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

a) 次のフィールドを設定します。

表 *3 : SNMPv3* のクレデンシャル

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

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

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

c) [Save] をクリックします。

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

a) 次のフィールドを設定します。

表 *4 : SNMP* のプロパティ

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

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

c) [Save] をクリックします。

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

a) 次のフィールドを設定します。

表 *5 : HTTPS* クレデンシャル

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

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

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

c) [Save] をクリックします。

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

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

- ポート 830（デフォルト）
- デバイスで使用可能なその他のポート

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

  ）。

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

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

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

c) [Save] をクリックします。

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

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

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

b) 使用する順序でプロトコルをドラッグ アンド ドロップします。

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

ステップ 15 [Discover] をクリックします。

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

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

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

1. [Later] ラジオボタンをクリックします。
2. 開始日時を定義します。
3. [Time Zone] ドロップダウンリストから、タイムゾーンを選択します。
4. [Recurrence] 領域で、[None]、[Daily]、または [Weekly] をクリックします。
   - [None]：検出は繰り返されません。
   - [Daily]：[Run at Interval（Days）] フィールドに間隔を日単位で入力します。
   - [Weekly]:[Run at Interval（Weeks）] フィールドに間隔を週単位で入力します。

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

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

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

7. [Start] をクリックします。

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

[Discoveries] ウィンドウにスキャンの結果が表示されます。

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

IP アドレス範囲を使用したネットワークの検出

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

始める前に

ディスカバリの前提条件 （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 メニューアイコン（☰）をクリックして、**[Tools]** > **[Discovery]**。

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

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

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

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

  IP アドレス範囲を追加するには、追加アイコン（[+]）をクリックします。

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

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

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

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

    （注） [Use Loopback IP] の使用を選択し、デバイスにループバック インターフェイスがない場合、Cisco DNA Centerは優先管理 IP アドレス （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 5 [Credentials] エリアを展開し、使用するログイン情報を選択します。

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

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

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

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

ステップ 8 CLI クレデンシャルの場合は、次の手順を実行します。

a) 次のフィールドを設定します。

表 6 : CLI クレデンシャル

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

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

b) これらのログイン情報を後で使用するために保存する場合は、[Save as global settings] チェックボックスをオンにします。このチェックボックスをオンにしなかった場合、ログイン情報を使用できるのは現在の検出ジョブに対してのみです。

c) [Save] をクリックします。

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

a) 次のフィールドを設定します。

表 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。

b) これらのログイン情報を後で使用するために保存する場合は、[Save as global settings] チェックボックスをオンにします。このチェックボックスをオンにしなかった場合、ログイン情報を使用できるのは現在の検出ジョブに対してのみです。

c) [Save] をクリックします。

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

a) 次のフィールドを設定します。

表 *8 : SNMPv3* のクレデンシャル

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

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

b) これらのログイン情報を後で使用するために保存する場合は、[Save as global settings] チェックボックスをオンにします。このチェックボックスをオンにしなかった場合、ログイン情報を使用できるのは現在の検出ジョブに対してのみです。

c) [Save] をクリックします。

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

a) 次のフィールドを設定します。

表 *9 : SNMP* のプロパティ

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

b) これらのログイン情報を後で使用するために保存する場合は、[Save as global settings] チェックボックスをオンにします。このチェックボックスをオンにしなかった場合、ログイン情報を使用できるのは現在の検出ジョブに対してのみです。

c) [Save] をクリックします。

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

a) 次のフィールドを設定します。

表 *10 : HTTPS* クレデンシャル

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

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

b) （任意） これらのログイン情報を後で使用するために保存する場合は、[Save as global settings] チェックボックスをオンにします。このチェックボックスをオンにしなかった場合、ログイン情報を使用できるのは現在の検出ジョブに対してのみです。

c) [Save] をクリックします。

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

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

- ポート 830（デフォルト）
- デバイスで使用可能なその他のポート
- Cisco DNA Center で構成するカスタムポート。（デバイス可制御性が有効になっている場合にのみ、カスタムポートを使用できます詳細については、*Cisco DNA Center* 管理者ガイドの「Device Controllability」の項を参照してください

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

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

b) これらのログイン情報を後で使用するために保存する場合は、[Save as global settings] チェックボックスをオンにします。このチェックボックスをオンにしなかった場合、ログイン情報を使用できるのは現在の検出ジョブに対してのみです。

c) [Save] をクリックします。

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

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

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

b) 使用する順序でプロトコルをドラッグ アンド ドロップします。

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

ステップ 15 [Discover] をクリックします。

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

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

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

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

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

7. [Start] をクリックします。

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

[Discoveries] ウィンドウにスキャンの結果が表示されます。

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

LLDP を使用したネットワークの検出

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

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

始める前に

- ネットワークデバイスで LLDP を有効にします。
- ディスカバリの前提条件 （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 メニューアイコン（☰）をクリックして、**[Tools]** > **[Discovery]**。

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

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

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

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

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

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

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

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

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

    （注） [Use Loopback IP] の使用を選択し、デバイスにループバック インターフェイスがない場合、Cisco DNA Centerは優先管理 IP アドレス （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 5 [Credentials] エリアを展開し、ディスカバリ ジョブで使用するクレデンシャルを設定します。

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

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

表 *11 : CLI* クレデンシャル

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

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

d) [SNMP v2c] をクリックして、次のフィールドを設定します。

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

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

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

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

表 *14 : SNMP* のプロパティ

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

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

表 *15 : HTTPS* クレデンシャル

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

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

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

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

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

b) 使用する順序でプロトコルをドラッグ アンド ドロップします。

ステップ 7 [Discover] をクリックします。

[Discover Devices] スライドインペインが表示されます。

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

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

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

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

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

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

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

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

7. [Start] をクリックします。

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

[Discoveries] ウィンドウにスキャンの結果が表示されます。

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

ディスカバリ ジョブの管理

ここでは、ディスカバリジョブの管理方法について説明します。

ディスカバリ ジョブの停止および開始

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

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

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

a) 左側の [Discoveries] ペインで、ディスカバリジョブをクリックします。
b) 下部ペインの右側で、[Stop] をクリックします。

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

a) 左側の [Discoveries] ペインで、ディスカバリジョブをクリックします。
b) 下部ペインの右側で、[Re-discover] をクリックします。

ディスカバリ ジョブの複製

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

始める前に

少なくとも 1 つのディスカバリ ジョブを実行する必要があります。

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

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

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

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

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

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

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

ディスカバリ ジョブの削除

アクティブまたは非アクティブに関係なく、検出ジョブを削除できます。

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

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

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

ステップ 4 下部ペインの右側で、[Delete] をクリックします。

ステップ 5 [OK] をクリックして確定します。

ディスカバリ ジョブ情報の表示

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

始める前に

少なくとも 1 つのディスカバリジョブを実行します。

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

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

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

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

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

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

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

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。

ネットワーク階層の概要

ネットワークの地理的な場所を表すネットワーク階層を作成できます。この階層構造により、デザインの設定や構成を特定の階層要素に簡単に適用できます。たとえば、デザインの設定をエリア全体に適用したり、床のみに適用したりすることができます。

デザインの設定を適用する場所を後で識別できるように、階層要素に名前を付けることができます。

作成できる階層要素には、その階層要素をどの要素に配置できるか、またどの要素をその階層要素に配置できるかを指定するルールがあります。

- [Global]：他のすべての階層要素がその中に存在するデフォルトの要素。[Global] の直下に配置することが可能な要素は、エリアおよびサイトのみです。
- [Areas] と [Sites]：エリア（Area）とサイト（Site）は、[Global] または他のエリアやサイトに存在します。エリアとサイトには物理アドレスがありません。最大の要素として、地理的地域を識別します。エリアとサイトにより、エリアおよびサイトのグループ化が可能になります。

- [Buildings]：建物（Building）は、エリアまたはサイトに存在します。建物を作成する場合、物理アドレスまたは緯度と経度の座標を指定する必要があります。建物にエリアを含めることはできません。ただし、フロアを含めることはできます。
- [Floors]：フロア（Floor）は建物に存在します。壁や窓など、建物のさまざまなコンポーネントを含むマップの有無にかかわらず、建物にフロアを追加できます。フロアマップを使用する場合は、手動で作成するか、DXF、DWG、JPG、GIF、PNG、またはPDFを含むファイルタイプのファイルからインポートできます。次に、ワイヤレスデバイスをフロアマップに配置して、ワイヤレスネットワークのカバレッジを視覚化できます。

  プロビジョニングされていないデバイスのサイト階層は、フロアマップ上の AP の場所を維持したまま変更できます。ただし、既存のフロアを別の建物に移動できないことに注意してください。

開始するには、次のいずれかの方法を使用してネットワーク階層を構築します。

- 新しいネットワーク階層を作成する。詳細については、「新しいネットワーク階層の設計（33 ページ）」を参照してください。
- Cisco Prime Infrastructure または Ekahau Pro から既存のネットワーク階層をインポートする。詳細については、Cisco DNA Center ユーザガイド の を参照してください。

新しいネットワーク階層の設計

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

これらのタスクは、[Design] 領域で実行します。

ステップ 1 ネットワーク階層を作成します。

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。

既存の Cisco ネットワーク階層の使用

Cisco Prime Infrastructure に既存のネットワーク階層がある場合は、エクスポートしてから Cisco DNA Center にインポートすることで、新しいネットワーク階層の作成に費やす時間と労力を削減できます。

次の情報を使用して、ネットワーク階層を再作成できます。

- **サイト階層**：既存のサイト階層を CSV ファイル形式でダウンロードします。CSV ファイルには、サイト名、親階層、フロア数、場所、サイトアドレスなどの詳細が含まれています。
- **マップアーカイブ**：マップ情報を TAR ファイル形式のマップアーカイブとしてダウンロードします。マップアーカイブファイルには、日時、フロアの数、AP などのデータが格納されます。ダウンロードするものに応じて、マップアーカイブには、フロアの寸法（長さ、幅、高さ）や、フロアマップに配置されている AP およびオーバーレイオブジェクトに関する詳細などのマップ情報も含めることができます。各フロアに適用されている RF 減衰モデルなどのキャリブレーション情報をダウンロードすることもできます。

  マップアーカイブの基礎をグローバル階層に置くか、次のように単一のサイト、建物、またはフロアの階層に置くかを選択できます。

  - [Site]：選択したサイトとそのすべてのサブサイト、建物、およびフロアがエクスポートされます。
  - [Building]：選択した建物とそのすべてのフロアがエクスポートされます。
  - [Floor]：選択したフロアがエクスポートされます。

（注） Cisco DNA Center は米国の連邦情報処理標準（FIPS）をサポートしています。FIPS は、Cisco DNA Center イメージのインストール時に有効にできるオプションのモードです。デフォルトでは、FIPS モードはディセーブルです。

FIPS モードは、マップアーカイブのエクスポートとインポートに次の影響を与えます。

FIPS モードが有効な場合：

- エクスポートされるマップアーカイブは暗号化されません。
- 暗号化されていないマップアーカイブのみをインポートできます。

FIPS モードが無効な場合：

- エクスポートされるマップアーカイブは暗号化されます。
- 暗号化されたマップアーカイブと暗号化されていないマップアーカイブの両方をインポートできます。

詳細については、Cisco DNA Center ユーザガイドを参照してください。

マップ内で使用するイメージファイルに関するガイドライン

マップイメージファイルを使用するには、次のガイドラインに従ってください。

- マップのイメージファイルを .jpg、.gif、.png、.pdf、.dxf、.dwg などの形式で保存できるグラフィカル アプリケーションを使用します。
- マップのイメージファイルのサイズはさまざまです。Cisco DNA Center は元のイメージをフル解像度でデータベースにインポートしますが、表示中は、ワークスペースに合わせてサイズが自動的に変更されます。
- インポートする前に、サイトの縦と横の寸法をフィートまたはメートル単位で取得してください。これにより、マップ インポート時にこれらの寸法を指定できます。
- 回転メタデータを持つフロアマップイメージは、CMX や Cisco DNA Spaces に同期したときに正しく表示されないことがあるため、使用しないようにします。フロアマップイメージは Cisco DNA Center でサポートされているフォーマットだとしても、特定のツールがメタデータを追加する方法によって、異なる方法でレンダリングされる可能性があります。たとえば、回転メタデータを含むイメージファイルを 3 つの異なるアプリケーションで開くと、2 つのアプリケーションでは水平にレンダリングされ、もう一方のアプリケーションでは垂直にレンダリングされる場合があります。

ネットワーク階層のサイトの作成

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

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

世界地図が右側のペインに表示されます。

ステップ 2 マップツールバーから、**[+ Add Site]** > **[Add Area]** をクリックします。

または、左側のペインで親サイトの横にある省略記号 ••• にカーソルを合わせ、[Add Area] を選択することもできます。

ステップ 3 [Area Name] フィールドに、サイト名を入力します。

ステップ 4 [Parent] ドロップダウンリストから、親ノードを選択します。[Global] がデフォルトの親ノードです。

ステップ 5 [Add]をクリックします。

左側ペインの親ノードにサイトが作成されます。

建物の追加

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

ステップ 2 [Network Hierarchy] ウィンドウで、**[+Add Site]** > **[Add Building]** をクリックします。

または、左側のペインで親サイトの横にある省略記号 ••• にカーソルを合わせ、[Add Building] を選択することもできます。

ステップ 3 [Add Building] ダイアログボックスで建物の詳細を追加します。

a) [Building Name] フィールドに建物の名前を入力します。
b) [Parent] ドロップダウンリストから、親ノードを選択します。[Global] がデフォルトの親ノードです。
c) [Address] フィールドにアドレスを入力します。

また、マップをクリックしてアドレスを入力することもできます。アドレスを追加すると、[Longitude] および [Latitude] の座標フィールドが自動的に設定されます。経度と緯度の座標を手動で変更して、アドレスを変更できます。

ステップ 4 [Add] をクリックします。

左側ペインの親サイトに建物が作成され、表示されます。

建物への基本フロアの追加

ビルディングを追加したら、それにフロアを追加できます。フロアマップのない基本フロアを追加することも、フロアを追加すると同時にフロアマップを含めることもできます。

建物に基本フロアを追加するには、次の手順を使用します。

CAD、非 CAD、または Ekahau ファイルのフロアマップを含むフロアを追加するには、Cisco DNA Center ユーザガイドを参照してください。:

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

ステップ 2 左側のペインで、建物の横にある省略記号 ••• の上にカーソルを置き、[Add Floor] を選択します。

ステップ 3 [Floor Name] フィールドにフロアの名前を入力します。

ステップ 4 [Type（RF Model）] ドロップダウンリストから、フロアに適用する RF モデルを選択します。

（注） RF モデルは、フロアの特性に基づいて RF を計算する方法を決定します。

ステップ 5 [Add] をクリックします。

ネットワーク階層の管理

Cisco DNA Center へのサイト階層のインポート

Cisco Prime Infrastructure から CSV ファイルとしてエクスポートしたサイト階層をインポートできます。サイト階層のエクスポートについては、Cisco DNA Center ユーザガイドを参照してください。

始める前に

- Cisco DNA Center インベントリにシスコ ワイヤレス コントローラおよび AP があることを確認します。ない場合は、[Discovery] 機能を使用して検出します。
- フロアマップ上に AP を追加して配置します。
- Cisco Prime Infrastructure にあるサイトを Cisco DNA Center で手動作成した場合は、インポートする前にそれらのサイトを Cisco DNA Center から削除する必要があります。

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

ステップ 2 マップツールバーから [Import] をクリックし、[Import Sites] を選択します。

ステップ 3 ダイアログボックスで、次のいずれかのオプションボタンをクリックします。

- [Merge with Existing Sites]：ダウンロードしたサイト情報を既存のサイト情報と結合します。
- [Overwrite Existing Sites]：Cisco DNA Center に同じサイトがすでに存在する場合、既存のサイト情報はダウンロードしたサイト情報で上書きされます。

ステップ 4 ダイアログボックスで、CSV ファイルをダウンロードエリアにドラッグアンドドロップします。または、[Choose a file] をクリックして CSV ファイルの場所に移動し、[Upload] をクリックすることもできます。

（注） CSV ファイルがない場合は、[Download Template] をクリックして、CSV ファイルをダウンロードし、編集してからアップロードできます。

Cisco Prime Infrastructure からのマップアーカイブのエクスポート

Cisco Prime Infrastructure からマップアーカイブファイルをエクスポートし、それらを Cisco DNA Center にインポートできます。マップアーカイブには、フロア寸法などのマップ情報と Cisco Prime Infrastructure の各フロアに適用されている無線周波数（RF）減衰モデルなどのキャリブレーション情報が含まれています。

ステップ 1 Cisco Prime Infrastructure GUI から、**[Maps]** > **[Wireless Maps]** > **[Site Maps (New)]** の順に選択します。

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

[Export Map Archive] ウィンドウが開き、デフォルトで [Select Sites] ウィンドウが開きます。

ステップ 3 エクスポートする特定のサイト、キャンパス、ビルディング、またはフロアのチェックボックスをオンにします。すべてのマップをエクスポートする場合は、[Select All] チェックボックスをオンにします。

ステップ 4 次のオプションの少なくとも 1 つを選択します。

- [Map Information]：[On] ボタンをクリックして、フロアの寸法（長さ、幅、高さ）と、フロアマップに配置された AP およびオーバーレイオブジェクトに関する詳細をエクスポートします。
- [Calibration Information]：[On] ボタンをクリックして、各フロアに適用されている RF 減衰モデルをエクスポートします。既存のキャリブレーションデータを Cisco Prime Infrastructure からエクスポートすることをお勧めします。それ以外の場合は、キャリブレーションの詳細を手動で再入力する必要があります。

  キャリブレーション情報を含めることを選択した場合は、次のように、選択したマップの情報を含めるか、すべての情報を含めるかを指定する必要もあります。

  - [Calibration Information for selected maps]：選択したサイトマップのキャリブレーション情報がエクスポートされます。
  - [All Calibration Information]：選択したマップに加えて、システムで使用可能なその他のキャリブレーション情報もエクスポートされます。

ステップ 5 [マップアーカイブを生成（Generate Map Archive）] をクリックします。

次のメッセージは、操作の進行状況を示しています。

```
Exporting data is in progress
```

TAR ファイルが作成され、ローカルマシンに保存されます。

ステップ 6 [Done] をクリックします。

ネットワーク階層の検索

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

ステップ 1 階層を検索するには、左側のペインの [Search Hierarchy] 検索フィールドで、検索するサイト、建物、フロア名の名称の一部または正式名称のどちらかを入力します。

階層は、検索フィールドに入力したテキストに基づきフィルタリングされます。

ステップ 2 [Site Name] と [Site Type] のフィルタ基準で階層を検索するには、[Search Hierarchy] 検索フィールドのフィルタアイコンをクリックし、次の手順を実行します。

1. [Site Name] 名前フィールドに、検索するサイトの名前を入力します。
2. 検索結果にすべての建物の住所を含めるには、[Include Address for all Building] チェックボックスをオンにします。

3. [Site Type] 領域で、フィルタ条件に含める [Area]、[Outdoor Area]、[Building]、または [Floor] の横にあるチェックボックスをオンにします。
4. [Search] をクリックします。

   フィルタ基準に基づいて、階層がフィルタリングされます。
5. 左側のペインの検索条件を除外するには、それぞれの条件の横にある X マークをクリックします。

サイトの編集

ステップ 1 メニューアイコン（☰）をクリックして、**[Design]** > **[Network Hierarchy]**。
ステップ 2 左側のペインで、サイトの横にある省略記号 ••• にカーソルを合わせて、[Edit Area] を選択します。
ステップ 3 [Edit Area] ダイアログボックスで、必要な編集を行います。
ステップ 4 [Update] をクリックして変更を保存します。

サイトの削除

ステップ 1 メニューアイコン（☰）をクリックして、**[Design]** > **[Network Hierarchy]**。
ステップ 2 左側のペインで、サイトの横にある省略記号 ••• にカーソルを合わせて、[Delete Area] を選択します。
ステップ 3 ダイアログボックスで [OK] をクリックして、削除を確定します。

ビルディングの編集

ステップ 1 メニューアイコン（☰）をクリックして、**[Design]** > **[Network Hierarchy]**。
ステップ 2 左側のペインで、ビルディングの横にある省略記号 ••• にカーソルを合わせて、[Edit Building] を選択します。
ステップ 3 [Edit Building] ダイアログボックスで、必要な編集を行います。
ステップ 4 [Update] をクリックして変更を保存します。

ビルディングの削除

ビルディングを削除すると、そのコンテナマップもすべて削除されます。削除されたマップ内の AP は、未割り当ての状態に移行します。

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

ステップ 2 左側のペインで、ビルディングの横にある省略記号 ••• にカーソルを合わせて、[Delete Building] を選択します。

ステップ 3 ダイアログボックスで [OK] をクリックして、削除を確定します。

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 [Menu] アイコン（≡）をクリックして、**[Design]** > **[Network Hierarchy]**の順に選択します。

ステップ 2 左側のペインで、そのフロアの横にある省略記号 ••• にカーソルを合わせて、[Edit Floor] を選択します。

ステップ 3 [Edit Floor] ポップアップで、必要な変更を行います。

ステップ 4 [Update] をクリックして変更を保存します。

2D でのフロアマップのモニタリング

[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 [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。

2D マップでのフロアマップ要素とオーバーレイの構成

2D マップを表示しているときに、マップツールバーの [Add/Edit] をクリックして編集モードに入ります。編集モードでは、次のことができます。

- 次のデバイスを追加、配置、および削除します。
  - アクセスポイント（AP）と計画されたアクセスポイント（PAP）
  - Sensor
- 次のオーバーレイ オブジェクトを追加、編集、および削除します。
  - カバレッジエリア
  - ロケーションリージョン
  - 壁
  - 棚ユニット
  - マーカー
  - \[GPS Markers\]
  - ポイントの位置合わせ

フロアマップでの AP の操作

Cisco DNA Center Cisco DNA Center によって、カバレッジエリアの無線周波数（RF）信号の相対強度を表示する全体マップのヒートマップが計算されます。2D ワイヤレスマップの場合、このヒートマップは、石壁や金属の物体など、ビルディングのさまざまな素材の減衰は考慮されておらず、RF信号が障害物に跳ね返る影響も表示されないため、実際のRF信号強度の近似値に過ぎません。

フロア マップに AP を配置する際は、次の注意事項を考慮してください。

- 部屋や建物の屋外の近くにデバイスが置かれるように、カバレッジ領域の境界に沿ってAPを設置します。このようなカバレッジ領域の中心に設置されたAPからは、場合によっては他の全 AP から等距離に見えてしまうデバイスに関しても有益なデータが得られます。
- AP 全体の密度を高め、AP をカバレッジ エリアの周辺部に近づけることにより、位置精度を向上させることができます。
- 細長いカバレッジ領域では、直線的に AP を配置しないようにします。各 AP でデバイスロケーションのスナップショットが他と異なるように、それらを交互にずらします。
- 設計では高帯域幅アプリケーションにも十分に対応できる AP 密度が提供されますが、位置に関しては、単一デバイスの各 AP ビューが似ているという弱点があります。そのことが位置の判別を困難にしています。AP をカバレッジ領域の周辺に移動して、それらを交互にずらします。それぞれにおいてデバイスの見え方が明確に異なる可能性が高くなり、結果としてより位置精度が高まります。

- フロアマップでのヒートマップの表示を最適化するには、AP の高さを約 10 フィート （3 m）以下に設定します。

AP の追加、配置、編集、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。2D ワイヤレスマップの場合、このヒートマップは実際の RF 信号強度の近似値にすぎません。信号に影響を与える RF 信号の反射やその他の影響が考慮されていないためです。

始める前に

インベントリにシスコの AP があることを確認してください。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。「検出の概要」を参照してください。

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

ステップ 2 左側のペインで、サイトをクリックしてからビル名をクリックし、最後に関心のあるフロアをクリックします。

ステップ 3 マップツールバーで [AP] トグルボタンが有効になっていることを確認します。

ステップ 4 マップツールバーから、[Add/Edit] をクリックします。

ステップ 5 マップから、AP を追加、編集、配置、再配置、および削除できます。詳細については、次の表を参照してください。

アクション	手順
APの追加	**1.** マップの左側のペインで、[Add APs] をクリックします。 **2.** [Add APs] スライドインペインでは、次のいずれかの操作を実行できます。 • **単一の AP を追加するには**：追加する AP の横にある [Add] をクリックします。 • **複数の AP を追加するには**：追加する AP の横にあるチェックボックスをオンにして、[Add Selected] をクリックします。 新しく追加された AP は、マップの左ペインの [Unpositioned] カテゴリに表示されます。 **3.** [Save] をクリックします。

アクション	手順
AP の配置	**1.** マップの左ペインの [Unpositioned] カテゴリから、AP をクリックします。 **2.** AP を配置するフロアマップ上の場所をクリックします。 **3.** [Save] をクリックします。
AP の位置変更	**1.** マップで、AP をクリックして選択します。 **2.** AP を新しい位置にドラッグアンドドロップします。 **3.** [Save] をクリックします。
AP の編集	**1.** マップで、AP をクリックします。 **2.** [Edit AP] スライドインペインから、必要に応じて AP 設定を構成します。 **3.** [Save] をクリックします。
複数の AP の編集 （注） 複数の AP を編集する場合、属性値は、値が同じであれば表示されます。そうでない場合は空白です。アンテナの値は、選択した AP のモデル番号と無線（無線の数と動作帯域）が同じである場合にのみ編集できます。計画された AP のモデル番号は変更できますが、追加された AP は変更できません。	**1.** 次のいずれかの方法を使用して、AP を選択します。 • 最初のデバイスをクリックし、Shift キーを押しながら残りのデバイスをクリックします。 • マップ ナビゲーション ツールバーで、[Select by rectangle] をクリックします。次に、マップの領域をクリックし、強調表示された長方形をドラッグして、連続した領域内の AP を選択します。長方形内で強調表示されているすべての AP が選択されています。 **2.** [Edit AP] スライドインペインから、必要に応じて AP 設定を構成します。 **3.** [Apply] をクリックします。 **4.** [Save] をクリックします。
AP の削除	**1.** AP または計画された AP をクリックします。 **2.** マップの左側のペインで、[Remove APs] をクリックします。 **3.** [Save] をクリックします。

AP のクイック ビュー

フロアマップ上の AP アイコン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。

- [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 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。

（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。

マップへのセンサーの追加

（注） インベントリに Cisco AP 1800S センサーがあることを確認します。Cisco Aironet 1800s アクティブセンサーをインベントリで表示するには、プラグアンドプレイを使用してプロビジョニングする必要があります。

センサーデバイスは AP 1800s センサー専用です。Cisco Aironet 1800s アクティブセンサーは、PnP を使用してブートストラップされます。アシュアランス サーバーに到達可能かどうかの詳細情報を取得してから アシュアランス サーバーと直接通信します。センサーテストに関する情報を含む詳細については、『Cisco DNA アシュアランス User Guide』を参照してください。

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

ステップ 2 フロアを 左側の階層ツリーで、次を選択します。 します。

ステップ 3 マップツールバーから、**[2D]** > **[Add/Edit]** > **[Sensors]** をクリックします。

ステップ 4 [Add Sensors] スライドインペインから、追加するセンサーのチェックボックスをオンにします。またはセンサー行の横にある [Add] をクリックします。

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

新しく追加されたセンサーは、編集モードのマップの左ペインの [Unpositioned] カテゴリに表示されます。

ステップ 5 完了したら、[Save] をクリックします。

カバレッジエリアの追加、編集、および削除

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

長方形以外の建物がある場合、またはフロア内で長方形以外の領域をマークする場合には、マップ描画ツールを使用してカバレッジエリアまたは多角形の領域を作成できます。

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

ステップ 2 フロアを 左側の階層ツリーで、次を選択します。 します。

ステップ 3 マップツールバーから、**[2D]** > **[Add/Edit]** > **[Overlays]** > **[Coverage Areas]** をクリックします。

ステップ 4 カバレッジエリアを追加するには、次の手順を実行します。

a) [Coverage Area] ダイアログボックスで、フィールドにカバレッジエリアの名前を入力します。
b) [Add Coverage] をクリックします。
c) マップをクリックしてポイントを作成し、描画ツールを開始します。
d) 引き続きポイントを作成して、カバレッジエリアの形状を定義します。

（注） カバレッジエリアの形状には、少なくとも 3 つのポイントが必要です。ポイントをクリックしてドラッグすると、カバレッジエリアの形状を定義し直すことができます。

e) ダブルクリックして描画ツールを終了し、カバレッジエリアの形状を確定します。
f) マップツールバーの [Save] をクリックします。

ステップ 5 カバレッジエリアを編集するには、次の手順を実行します。

a) マップツールバーから、**[Add/Edit]** > **[Coverage Areas]**をクリックします。
b) カバレッジエリアの形状を定義し直すには、ポイントをクリックしてドラッグします。
c) カバレッジエリアの名前を編集するには、カバレッジエリアを右クリックして [Edit] を選択します。

d) 完了したら、マップツールバーの [Save] をクリックします。

ステップ 6 カバレッジエリアを削除するには、次の手順を実行します。

a) マップツールバーから、**[Add/Edit]** > **[Coverage Areas]**をクリックします。
b) カバレッジエリアを右クリックし、[Delete] を選択します。
c) カバレッジエリアが削除されたら、マップツールバーから [Save] をクリックします。

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 メニューアイコン（☰）をクリックして、**[Design]** > **[Network Hierarchy]**。

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 [Edit] をクリックします。

ステップ 4 [Obstacles] の横にある [Overlays] パネルで、[Add] をクリックします。

ステップ 5 [Obstacle Creation] ダイアログ ボックスで、[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、[Thick Wall]、[Light Wall]、[Heavy Door]、[Light Door]、[Cubicle]、および [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 [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 エリアの輪郭を描画したら、そのエリアをダブルクリックして強調表示します。

ステップ 10 [Obstacle Creation] ウィンドウで [Done] をクリックします。

ステップ 11 [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、[Obstacles] の隣にある [Overlays] パネルで、[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、[Save] をクリックします。

ステップ 14 障害を削除するには、[Obstacles] の隣にある [Overlays] パネルで、[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 [Save] をクリックします。

ロケーションリージョンの追加、編集、および削除

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

マップ上での包含および除外領域を定義するには、次のガイドラインを使用します。

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

マップ上での包含および除外領域の定義

マップ上での包含および除外領域を定義するには、次のガイドラインを使用します。

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

包含リージョンの追加、編集、および削除

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

ステップ 2 フロアを 左側の階層ツリーで、次を選択します。 します。

ステップ 3 マップツールバーから、**[2D]** > **[Add/Edit]** > **[Overlays]** > **[Location Regions]** をクリックします。

ステップ 4 マップの左側のペインから、[Inclusion] アイコンをクリックします。

ステップ 5 包含リージョンを作成するには、描画ツールを使用します。

a) マップをクリックして、包含リージョンを開始するポイントを作成します。
b) カーソルを次のポイントに移動して、もう一度クリックします。
c) 引き続きポイントを作成して、包含リージョンの形状を定義します。
d) 形状を完成させるには、マップをダブルクリックします。

または、マップの左側のペインから、[Inclusion] アイコンをクリックします。

e) 描画ツールを終了するには、マップをもう一度ダブルクリックします。

ステップ 6 包含リージョンの場所を編集するには、その形状を新しい場所にドラッグアンドドロップします。

ステップ 7 包含リージョンを削除するには、形状を右クリックして [Delete] を選択します。

ステップ 8 マップツールバーの [Save] をクリックします。

除外リージョンの追加、編集、および削除

フロアの計算の精度を高めるため、計算から除外するリージョン（除外リージョン）を定義できます。たとえば、建物内のアトリウムや階段の吹き抜けなどのリージョンを除外できます。原則として、除外リージョンは包含リージョンの境界内に定義されます。

ステップ 1 メニューアイコン（≡）をクリックして、**[Design]** > **[Network Hierarchy]**。
ステップ 2 フロアを 左側の階層ツリーで、次を選択します。 します。
ステップ 3 マップツールバーから、**[2D]** > **[Add/Edit]** > **[Overlays]** > **[Location Regions]** をクリックします。
ステップ 4 マップの左側のペインから、[Exclusion] アイコンをクリックします。
ステップ 5 除外リージョンを作成するには、描画ツールを使用します。

a) マップをクリックして、除外リージョンを開始するポイントを作成します。
b) カーソルを次のポイントに移動して、もう一度クリックします。
c) 引き続きポイントを作成して、除外リージョンの形状を定義します。
d) 形状を完成させるには、マップをダブルクリックします。

   または、マップの左側のペインから、[Exclusion] アイコンをクリックします。

e) 描画ツールを終了するには、マップをもう一度ダブルクリックします。

ステップ 6 除外リージョンの場所を編集するには、その形状を新しい場所にドラッグアンドドロップします。
ステップ 7 除外リージョンを削除するには、形状を右クリックして [Delete] を選択します。
ステップ 8 マップツールバーの [Save] をクリックします。

ロケーション リージョンの編集

ステップ 1 **[Overlays]** パネルで、**[Location Regions]** の横にある **[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、**[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 **[Overlays]**パネルで、**[Location Regions]** の横にある **[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、**[Delete]** をクリックします。
ステップ 3 [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（ユーザー定義）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）からモニターされる距離を表します。

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

ステップ 2 左ペインで、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 [Edit] をクリックします。

ステップ 4 [Rails] の横にある [Overlays] パネルで、[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、[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 [Save] をクリックします。

ステップ 9 [Overlays] パネルで、[Rails] の横にある [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、[Save] をクリックします。

ステップ 11 [Overlays] パネルで、[Rails] の横にある [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、[Delete] をクリックします。

ステップ 13 [Save] をクリックします。

マーカーの追加、編集、および削除

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

ステップ 2 フロアを 左側の階層ツリーで、次を選択します。 します。

ステップ 3 マップツールバーから、**[2D]** > **[Add/Edit]** > **[Overlays]** > **[Markers]** をクリックします。

ステップ 4 マップの左側のペインから、[Markers] アイコンをクリックします。

ステップ 5 [Place Markers] ダイアログボックスで、マーカーの名前を入力し、[Add Marker] をクリックします。

ステップ 6 マーカーを配置するには、マーカーを配置するマップをクリックします。

ステップ 7 マーカーを移動するには、マーカーが青色に変わるまでカーソルを合わせます。次に、マーカーを新しい場所にドラッグアンドドロップします。

ステップ 8 マーカーを編集するには、マーカーを右クリックして [Edit] を選択します。

ステップ 9 マーカーを削除するには、マーカーを右クリックして [Delete] を選択します。

ステップ 10 マップツールバーの [Save] をクリックします。

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 **[View Options]** をクリックします。フロア マップと [Access Points]、[Sensor]、[Overlay Objects]、[Map Properties]、および [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、[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

アクセスポイントをマップ上に表示するには、[Access Points] の横にある [On/Off] ボタンをクリックします。[Access Points] 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、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。
  - [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。
  - [Name]：AP 名。
  - [AP MAC Address]：AP の MAC アドレス。
  - [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。
  - [Radio MAC Address]：無線 MAC アドレス。
  - **IP Address**
  - [Channel]：Cisco Radio のチャネル番号または [Unavailable]（アクセスポイントが接続されていない場合）。
  - [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。

- [TX Power]：現在の Cisco Radio の送信電力レベル（1 が高い）または [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。Cisco Aironet 1000 シリーズ Lightweight アクセスポイントは **1** ～ **5** の値を受け入れます。Cisco Aironet 1230AG シリーズ アクセスポイントは **1** ～ **7** の値を受け入れます。Cisco Aironet 1240AG シリーズ アクセスポイントおよび Cisco Aironet 1100 シリーズ アクセスポイントは **1** ～ **8** の値を受け入れます。

- [Channel and Tx Power]：チャネルと送信電力レベルまたは [Unavailable]（アクセスポイントが接続されていない場合）。

- [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。

- [Tx Utilization]：指定されたインターフェイスの送信（Tx）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。

- [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。

- [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。

- [Health Score]：AP の正常性スコア。

- **問題数**

- **カバレッジの問題**

- **APダウンの問題**

- [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。[Heatmap Type] ドロップダウンリストからヒートマップのタイプを選択してください。ヒートマップのタイプは次のとおりです。

  - [None]

  - [AP RSSI]：特定の帯域のワイヤレス信号の強度を特定するカバレッジヒートマップ。

    - [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。

    - [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。

- [Heatmap Color Scheme]：緑色はヒートマップカバレッジ状態が良好であることを示し、赤色はヒートマップカバレッジ状態が悪いことを示します。

- [Client Density]：関連付けられたクライアントの密度。
  - [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。

- [IDS]：ワイヤレスクライアントに提供されるモニターモードアクセスポイントカバレッジをフロアマップ上に示すヒートマップ。
- [Planned Heatmap]：計画ヒートマップは、フロアマップ上の計画アクセスポイントの可能なカバレッジを示す架空のヒートマップです。
- [Coverage]：モニターモードアクセス ポイントが除外されたヒートマップ（モニターモード アクセス ポイントがフロアプラン上にある場合にのみ利用可能）。

AP の詳細はすぐにマップに反映されます。マップ上の AP アイコンにカーソルを合わせると、AP の詳細、RX ネイバーの詳細、クライアントの詳細、およびスイッチの情報が表示されます。

センサーオプションの表示

[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。[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

オーバーレイオブジェクト をこれらの設定を構成するパネルに展開します。[On]/[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]
- [Location Regions]
- [Obstacles]
- [Rails]
- [Markers]

マップ プロパティの設定

[Map Properties] パネルを展開して、以下を構成します。

- [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。[Auto Refresh] ドロップダウンリストから、時間間隔（[None]、[1 min]、[2 mins]、[5 mins]、または [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

[Global Map Properties] パネルを展開し、次のように設定します。

- [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 [Feet] または [Meters] のいずれかに設定します。

ネットワーク階層マップでのデバイスデータのフィルタ処理

2D ワイヤレスマップの場合、アクセスポイントやセンサーにさまざまなフィルタを適用できます。開始するには、マップツールバーの [Data] をクリックします。フィルタ条件に基づいて、検索結果がテーブルに表示されます。

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

インベントリは、必要に応じて次のプロトコルを使用します。

- リンク層検出プロトコル（LLDP）
- IP デバイス トラッキング（IPDT）またはスイッチ統合セキュリティ機能（SISF）（IPDT または SISF をデバイス上で有効にする必要があります）。
- LLDP Media Endpoint Discovery （このプロトコルは IP フォンや一部のサーバーの検出に使用されます）。
- ネットワーク設定プロトコル（NETCONF）デバイスのリストについては、ディスカバリの前提条件 （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 24 時間ごとです。ただし、この間隔は、ネットワーク環境の

必要性に応じて変更できます。詳細については、デバイスポーリング間隔の更新（54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。

デバイスポーリング間隔の更新

[System] > **[Settings]** > **[Network Resync Interval]** の順に選択すると、グローバルレベルですべてのデバイスのポーリング間隔を更新できます。また、[Device Inventory] を選択すると、デバイスレベルで特定のデバイスのポーリング間隔を更新できます。[Network Resync Interval] を使用してポーリング間隔を設定すると、その値が [Device Inventory] ポーリング間隔値よりも優先されます。

デバイスにポーリングさせない場合は、ポーリングを無効にできます。

始める前に

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

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

ステップ 2 更新するデバイスを選択します。

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

ステップ 4 [Edit Device] slide-in pane で、[Resync Interval] をクリックします。

ステップ 5 再同期タイプを選択します。

（注）
- 再同期タイプをグローバルとして設定するには、**[System]** > **[Settings]**の順に移動します。
- デバイス固有のポーリング時間は、グローバルなポーリング時間より優先されます。デバイス固有のポーリング時間を設定した後でグローバルなポーリング時間を変更した場合、Cisco DNA Center は引き続きデバイス固有のポーリング時間を使用します。

ステップ 6 [Resync Interval (in Mins)] 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。

ステップ 7 [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

インベントリで検出されたデバイスに関する情報を表示およびフィルタリングできます。[Device] テーブルに表示される情報をカスタマイズまたは変更できます。

始める前に

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

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

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

ステップ 2 （任意）インベントリビューを変更するには、右上隅にあるトグルボタン（ ）を使用します。既定のビュー（リストレイアウト）を、トポロジやマップレイアウトなどの他のレイアウトに変更できます。

ステップ 3 （任意） [Devices] テーブルのフォーカスビューを変更するには、[Focus] ドロップダウンリストから、[Default] 、[Inventory] 、または [Software Images] などのビューを選択します。

（注）
- 表示される列は、選択したフォーカスビューに応じて変わります。
- 選択したデバイスは、それぞれの新しいフォーカスビューで保持されます。

ステップ 4 （任意） [Devices] テーブルで特定のデバイスの詳細をフィルタ処理するには、次の操作を実行できます。

- デバイスファミリをフィルタ処理するには、[Inventory] ウィンドウの上部にある 1 つまたは複数のデバイスファミリボタンを選択します。

  たとえば、[Routers] をクリックすると、テーブル内にルーターのみを表示できます。

- デバイスの作業項目をフィルタ処理するには、左側のペインで、1 つ以上の作業項目のチェック ボックスをオンにします。テーブルは、作業項目に対してすぐにフィルタ処理されます。

  たとえば、[Unreachable] チェックボックスをオンにして、到達不能なデバイスのみをテーブルに表示できます。

- 特定のデバイスの詳細をフィルタ処理するには、[Filter devices] をクリックし、フィルタオプション（[Quick Filters] 、[Advanced Filters] 、[Recent Filters] ）から選択します。次に、[Apply] をクリックします。

ステップ 5 （任意） 右上隅にある[Take a tour] をクリックすると、[Inventory] ウィンドウの詳しい説明が見られます。

ステップ 6 （任意） [Devices] テーブルのすべてのデータをエクスポートするには、右上隅の[Export] をクリックします。

ステップ 7 （任意） [Devices] テーブルをカスタマイズするには、右上隅にある設定アイコン（⚙）をクリックし、[Table Settings] slide-in paneで次のオプションから選択して、[Apply] をクリックします。

- [Table Appearance] ：デフォルトまたはコンパクトなテーブルビューと、テーブルストライピングにしたい場合に選択します。
- [Edit Table Columns] ：カスタムビューを作成したい場合と、列の表示・非表示を選択します。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。

以下の表に、テーブルの特定の列に関係する重要な情報をまとめました。

カラム	説明
Device Name	デバイスの名前。 デバイス名をクリックすると、そのデバイスの詳細情報が表示されます。 （注） 赤で表示されているデバイス名は、インベントリがデバイスをポーリングしておらず、30 分を超える期間にわたってその情報を更新していないことを意味しています。
Support Type	デバイスのサポートレベルが表示されます。 • [Supported]：Cisco DNA Center のすべてのアプリケーションに対してデバイスプロファイルがテスト済みです。これらのデバイスのいずれかの Cisco DNA Center 機能が動作しない場合は、サービスリクエストを開くことができます。 • [Limited]：レガシーデバイス用のデバイスプロファイルは、Cisco DNA Center の次の機能のみを対象にベストエフォートベースでのみテストされています。 • 検出 • トポロジ • デバイスの到達可能性 • 構成変更監査 • インベントリ • ソフトウェアイメージ管理（ソフトウェアイメージは、cisco.com に記載の EOL デバイスでは利用できない場合があります。EOL デバイスには推奨されません。） • テンプレート プロビジョニング（スイッチにのみ適用されます。） 詳細については、『Cisco DNA Center Compatibility Matrix』を参照してください。 • [Third Party]：デバイスプロファイルは、SNMP MIB-2 値を入力できるサードパーティデバイスの Cisco DNA Center でテストされています。Cisco DNA Center はベストエフォートベースで、インベントリやトポロジなどの限られた基本的な自動化機能をサポートします。 • [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シスコデバイスとサードパーティ製デバイス。これらのデバイスについて、Cisco DNA Center でさまざまな機能をベストエフォートとして試すことができます。ただし、Cisco DNA Center の機能が期待どおりに動作しない場合 、サービスリクエストやバグを申請することはできません。

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

カラム	説明
Device Role	スキャン プロセス中に、検出された各デバイスに割り当てられているロール。デバイス ロールは、ネットワーク内での役目と配置に従って、デバイスを識別およびグループ分けするために使用されます。Cisco DNA Center でデバイス ロールを特定できない場合、デバイス ロールは不明に設定されます。 （注） デバイス ロールを手動で変更すると、割り当ては静的のままになります。 Cisco DNA Center は、後続のデバイスの再同期中に変更が検知されたとしても、デバイス ロールは更新されません。 必要に応じて、このカラムのドロップダウン リストを使用して、割り当てられたデバイス ロールを変更することができます。
Site	デバイスに割り当てられているサイト。デバイスがどのサイトにも割り当てられていない場合は、[Assign] をクリックします。[Choose a site] をクリックし、階層からサイトを選択して [Save] をクリックします。詳細については、ネットワーク階層の概要 （32 ページ） を参照してください。
Last Updated	Cisco DNA Center がデバイスをスキャンし、デバイスに関する新しい情報でデータベースを更新した最新の日付と時刻。
Resync Interval	デバイスのポーリング間隔。再同期間隔は、[Inventory] ウィンドウから **[Actions]** > **[Edit Device]** > **[Resync Interval]** の順に選択して設定します。再同期タイプを [Global] として設定するには、メインメニューから **[System]** > **[Settings]** の順に選択します。詳細については、『*Cisco DNA Center Administrator Guide*』を参照してください。
プロビジョニング ステータス	デバイスで試行された最後のプロビジョニング操作のステータスが示されます。過去のプロビジョニング操作のステータスを確認するには、[See Details] をクリックします。 • [Success]：デバイスでの最近の操作が成功しました。 • [Success] と警告アイコン：デバイスでの最近の操作は成功しましたが、過去のプロビジョニング操作による障害があるため、注意が必要です。 • [Failed]：デバイスでの最近の操作が失敗しました。 • [Failed] と警告アイコン：デバイスでの最近の操作が失敗しました。過去のプロビジョニング操作による障害があるため、注意が必要です。 • [Configuring]：デバイスは現在設定中です。 • [Pending]：システムは、進行中のプロビジョニング操作によってデバイスが影響を受けるかどうかを判断しようとしています。 • [Not Provisioned]：デバイスは一度もプロビジョニングされていません。 • [Out of Sync]：デバイスのネットワーク設定またはネットワークプロファイルが、最後のプロビジョニング操作の後に変更されました。

カラム	説明
Credential Status	デバイスのクレデンシャルステータスが示されます。 • [Not Applied]：デバイスのクレデンシャルがデバイスに適用されていません。 • [Success]：デバイスのクレデンシャルがデバイスに正常に適用されました。 • [Failed]：デバイスのクレデンシャルがデバイスで失敗しました。 クレデンシャルの詳細を表示するには、[See Details] をクリックします。 [Credential Status] slide-in paneには、クレデンシャルの [Type]、[Name/Description]、[Status]、および [Details] が表示されます。 ステータスが [Failed] のデバイスの場合、[Actions] 列の省略記号アイコン（ ••• ）の上にカーソルを置き、[Retry] または [Clear] を選択します。 • [Retry]：デバイスにクレデンシャルを適用します。 • [Clear]：デバイスのクレデンシャルをクリアします。
AP CDP Neighbors	[Inventory] ウィンドウの AP に接続されているスイッチとポートに関する詳細が表示されます。 このウィンドウには、接続されたアクセススイッチが Cisco DNA Center によって管理されている場合でも、AP CDP ネイバーに関する情報が表示されます。

- [Edit Custom Views] ：最初に、[Edit Table Columns] タブでカスタム ビューを作成する必要があります。それから、カスタムビューを編集できます。
- [Reset All Settings] ：テーブル設定をデフォルト設定にリセットします。

ステップ 8 （任意） [Devices] テーブルからデバイスを管理するには、次のオプションがあります。

名前	説明
Add Device	[Add Device] をクリックして、ネットワークまたはコンピューティングデバイスを追加するか、Meraki ダッシュボードまたは Firepower Management Center (FMC) をCisco DNA Centerと統合できます。
タグ	[Tag] をクリックして、デバイスにタグを付けたり、タグを編集および削除したり、ポートグループを作成したりできます。
[Actions] ドロップダウン リスト	[Actions] ドロップダウンリストを使用して、デバイス、ソフトウェアイメージ、テレメトリなどを管理できます。 各アクションオプションの詳細を表示するには、右隣の情報アイコン（ⓘ）をクリックします。

ステップ 9 （任意） [Devices] テーブルでは、次の操作を実行できます。

- 昇順または降順で列をソートするには、列ヘッダーをクリックします。

- デバイスの詳細を表示するには、デバイス名をクリックしてから、[View Device Details] をクリックします。
- デバイスのコンプライアンスの詳細を表示するには、[Compliance] 列で [Non-Compliant] または [Compliant] をクリックします。
- サイトをデバイスに割り当てるには、[Site] 列の下の [Assign] をクリックします。
- デバイスロールを変更するには、[Device Role] 列の下にある編集アイコンをクリックし、[ACCESS] や [CORE] などのオプションから選択します。
- イメージをゴールデンとしてマークするか、必要な更新を表示するには、[Software Image] 列で [Mark Golden] または [Needs Update] をクリックします。
- エントリの数を変更するには、ウィンドウの一番下までスクロールし、[Show Records] ドロップダウン リストから、表示するエントリの数を選択します。

  テーブルに 25 を超えるエントリがあり、別のフォーカスビューを選択した場合、新しい各ビューで同じ数のエントリが表示されます。

（注） 各フォーカスビューには異なる列が表示され、テーブル ビューをカスタマイズして、[Compliance]、[Site]、[Device Role]、[Software Image] などの列を含めることができます。

ネットワーク デバイスの削除

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

インベントリからワイヤレスセンサーを削除すると、センサーは工場出荷時のデフォルト状態にリセットされるため、再接続すると現在の構成が採用されます。

始める前に

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

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

ステップ 2 削除するデバイスの横にあるチェックボックスをオンにします。

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

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

ステップ 4 [Warning] ウィンドウで、[Config Clean-Up] チェックボックスをオンにして、選択したデバイスからネットワーク設定およびテレメトリ設定を削除します。

ステップ 5 [OK] をクリックして、アクションを確認します。

デバイスをサイトに追加する

デバイスをサイトに追加すると、Syslog サーバーおよび SNMP トラップサーバーとして Cisco DNA Center が設定されます。Syslog レベル 2 が有効になり、グローバルテレメトリを設定できます。

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

ステップ 2 サイトに割り当てるデバイスのチェックボックスをオンにします。

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

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

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

ステップ 6 [Save] をクリックします。

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

ステップ 8 [Next] をクリックします。

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

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

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

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

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

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

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

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

- [Work Items] ウィンドウで、設定プレビュー要求を送信した CLI プレビュータスクをクリックします。

- CLI 設定の詳細を表示し、[Deploy] をクリックします。

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

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

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

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ー認証に 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、ユーザー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 の設定は NCP（ネットワーク制御プラットフォーム）内に一元化されているため、単一の 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. メニューアイコン（☰）をクリックして、**[System]** > **[Settings]** > **[External Services]** > **[Authentication and Policy Servers]** の順に選択して、Cisco ISE サーバーの詳細を入力します。
2. Cisco ISE サーバー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。

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 および 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 サーバーで Cisco DNA Center を登録します。これには、AAA サーバーと Cisco DNA Center の共有秘密を定義することが含まれます。
  - AAA サーバーで 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 サーバー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、以下の点を確認してください。
  - Cisco ISE をネットワークに展開していること。サポートされている Cisco ISE バージョンの詳細については、『Cisco DNA Center Compatibility Matrix』を参照してください。Cisco ISE のインストールについては、Cisco Identity Services Engine インストールおよびアップグレードガイド [英語] を参照してください。
  - スタンドアロン ISE 展開環境がある場合は、Cisco DNA Center を Cisco ISE ノードと統合し、そのノード上で pxGrid サービスと外部 RESTful サービス（ERS）を有効にする必要があります。

（注） 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 2.2.1.x 以前のリリースは 2 つを超える pxGrid ノードをサポートしていません。

  - 分散型 Cisco ISE 展開がある場合：
    - Cisco DNA Center をプライマリポリシー管理ノード（PAN）と統合し、PAN 上で ERS を有効にする必要があります。

（注） PAN 経由で ERS を使用することを推奨します。ただし、バックアップの場合は、PSN 上で ERS を有効にできます。

    - 分散型展開環境内のいずれかの Cisco ISE ノード上で pxGrid サービスを有効化する必要があります。PAN 上で pxGrid サービスを有効化することを選択できますが、必須ではありません。分散型展開環境にある任意の Cisco ISE ノード上で pxGrid を有効にできます。
    - TrustSec または SD-Access のコンテンツと PAC を処理するように Cisco ISE で設定する PSN は、**[Work Centers]** > **[Trustsec]** > **[Trustsec Servers]** > **[Trustsec AAA**

Servers] でも定義する必要があります。詳細については、『Cisco Identity Services Engine Administrator Guide』を参照してください。

- ポート 443、5222、8910、9060 で Cisco DNA Center と Cisco ISE の通信を有効にする必要があります。
- pxGrid が有効化されている Cisco ISE ホストには、Cisco ISE eth0 インターフェイスの IP アドレス上の Cisco DNA Center から到達できる必要があります。
- Cisco ISE ノードは、アプライアンス NIC 経由でファブリック アンダーレイ ネットワークに到達できます。
- Cisco ISE 管理ノード証明書のサブジェクト名またはサブジェクト代替名（SAN）のいずれかに Cisco ISE の IP アドレスまたは FQDN が含まれている必要があります。
- Cisco DNA Center システム証明書の SAN フィールドに、Cisco DNA Center アプライアンスの IP アドレスと FQDN の両方がリストされている必要があります。

（注） Cisco ISE 2.4 パッチ 13、2.6 パッチ 7、および 2.7 パッチ 3 では、pxGrid 証明書に Cisco ISE のデフォルトの自己署名証明書を使用している場合、証明書が Cisco ISE によって拒否されることがあります。これは、その証明書の古いバージョンに、SSL サーバとして指定された Netscape Cert Type 拡張があるためです。これは、クライアント証明書が必要なため失敗します。

この問題は Cisco ISE 3.0 以降では発生しません。詳細については、Cisco Cloud APIC リリースノート [英語] を参照してください。

ステップ 1 メニューアイコン（☰）をクリックして、**[System]** > **[Settings]** > **[External Services]** > **[Authentication and Policy Servers]**。

ステップ 2 [Add] ドロップダウンリストから、[AAA] または [ISE] を選択します。

ステップ 3 プライマリ AAA サーバーを設定するには、次の情報を入力します。

- [Server IP Address]：AAA サーバの IP アドレス。
- [Shared Secret]：デバイス認証のキー。共有秘密の長さは、最大 100 文字です。

ステップ 4 Cisco ISE サーバーを設定するには、次の詳細情報を入力します。

- [Server IP Address]：ISE サーバーの IP アドレス。
- [Shared Secret]：デバイス認証のキー。
- [Username]：Cisco ISE CLI にログインするために使用するユーザー名。

（注） このユーザーにはスーパーユーザーの管理権限が必要です。

- [Password]：Cisco ISE CLI ユーザー名に対応するパスワード。
- [FQDN]：Cisco ISE サーバー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 サーバーの FQDN は ise.cisco.com である可能性があります。

- [Virtual IP Address（es）]：Cisco ISE ポリシーサービスノード（PSN）が背後に配置されてい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。

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

- [Connect to pxGrid]：pxGrid 接続を有効にするには、このチェックボックスをオンにします。

  Cisco DNA Center システム証明書を pxGrid クライアント証明書として使用する場合（pxGrid クライアントとして Cisco DNA Center システムを認証するために Cisco ISE に送信）、[Use Cisco DNA Center Certificate for pxGrid] チェックボックスをオンにします。動作環境で使用されるすべての証明書を同じ CA で生成する必要がある場合は、このオプションを使用できます。このオプションを無効にすると、Cisco DNA Center は、システムが使用する pxGrid クライアント証明書を生成するための要求を Cisco ISE に送信します。

  このオプションを有効にする場合は、次のことを確認してください。

  - Cisco DNA Center 証明書が、Cisco ISE で使用中の CA と同じ認証局（CA）によって生成されていること（そうでない場合、pxGrid 認証は失敗します）。
  - [Certificate Extended Key Use（EKU）] フィールドに「クライアント認証」が含まれていること。

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

  注目 ここで Cisco ISE サーバーの TACAS を有効にしない場合は、ネットワークデバイス認証用に AAA サーバーを設定するときに、**[Design]** > **[Network Settings]** > **[Network]**で Cisco ISE サーバーを TACAS サーバーとして設定できません。

- [Authentication Port]：AAA サーバーへの認証メッセージのリレーに使用されるポート。デフォルトの UDP ポートは 1812 です。
- [Accounting Port]：AAA サーバーへの重要なイベントのリレーに使用されるポート。デフォルトの UDP ポートは 1813 です。
- [Port]：デフォルトの TACACS 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 サーバーの応答を待機するタイムアウト期間。デフォルトのタイムアウトは 4 秒です。

（注） 必要な情報を入力すると、Cisco ISE は 2 つのフェーズを経て Cisco DNA Center と統合されます。統合が完了するまでには数分かかります。フェーズごとの統合ステータスは、[Authentication and Policy Servers] ウィンドウと [System 360] ウィンドウに表示されます。

Cisco ISE サーバー登録フェーズ：

- [Authentication and Policy Servers] ウィンドウ：「進行中」
- [System 360] ウィンドウ：「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] ウィンドウ：「アクティブ」
- [System 360] ウィンドウ：「プライマリ使用可能」および「pxGrid 使用可能」

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

ステップ 6 [Add] をクリックします。

ステップ 7 セカンダリサーバーを追加するには、前述の手順を繰り返します。

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

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

始める前に

サイトを作成し、サイトにデバイスを割り当てます。『ネットワーク階層のサイトの作成（35 ページ）』を参照してください。

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

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

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

ステップ 3 [Syslogs] エリアで、次のいずれかを実行します。

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

ステップ 4 [NetFlow] エリアで、次のいずれかを実行します。

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

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

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

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

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

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

ステップ 7 [Save] をクリックします。

Cisco AI Network Analytics データ収集の設定

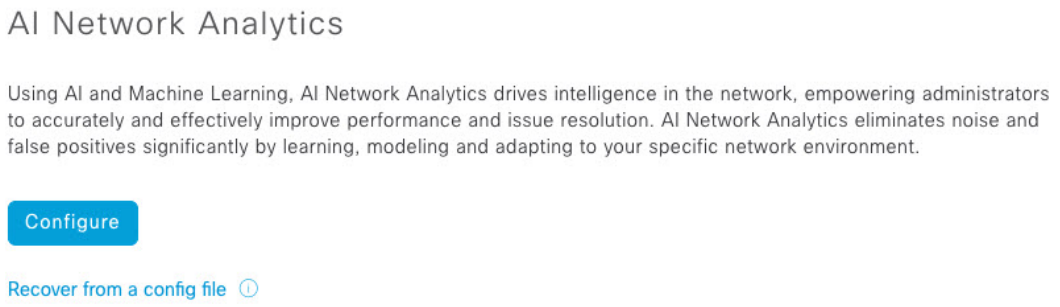
Cisco AI Network Analytics が、ネットワークデバイスおよびサイト階層から Cisco DNA Center にネットワークイベントデータをエクスポートできるようにするには、次の手順を実行します。

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）

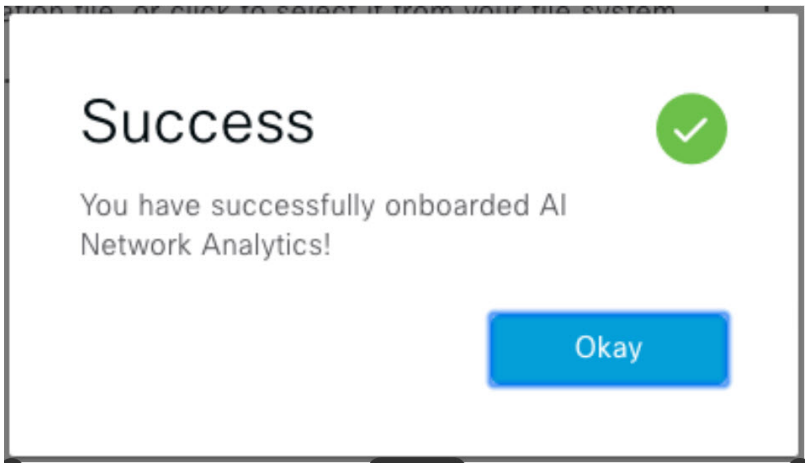
ステップ 1 メニューアイコン（☰）をクリックして、**[System]** > **[Settings]**の順に選択します。

ステップ 2 [External Services] までスクロールし、[Cisco AI Analytics] を選択します。
[**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 3 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。



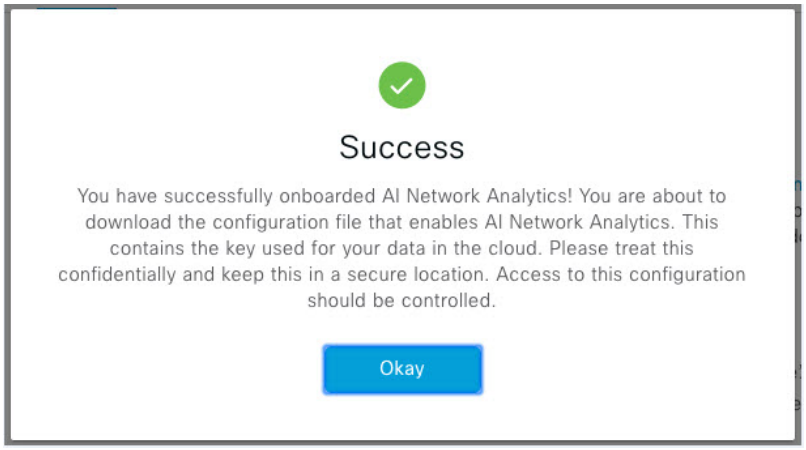
- Cisco AI Network Analytics を初めて設定する場合は、次の手順を実行します。

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. **[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。



ステップ 4 [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、[Enable AI Network Analytics] トグルボタン が表示されます。

ステップ 5 （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。

Cisco AI Network Analytics データ収集の無効化

Cisco AI Network Analytics のデータ収集を無効にするには、次のように AI Network Analytics 機能を無効にする必要があります。

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

ステップ 2 [External Services] までスクロールし、[Cisco AI Analytics] を選択します。
各機能のチェックマーク（☑）は、その機能が有効になっていることを示します。チェックボックスがオフの場合（☐）、機能は無効になっています。

ステップ 3 [AI Network Analytics] 領域で、[Enable AI Network Analytics] トグルボタンをクリックしてオフにします（☐）。

ステップ 4 [Update] をクリックします。

ステップ 5 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ます。

ステップ 6 （オプション）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 メニューアイコン（☰）をクリックして、**[System]** > **[Settings]**の順に選択します。

ステップ 2 [External Services] まで下にスクロールし、[Machine Reasoning Knowledge Base]を選択します。
[Machine Reasoning Knowledge Base] ウィンドウには、次の情報が表示されます。

- [INSTALLED]：インストールされている機械推論ナレッジベースパッケージのバージョンとインストール日が表示されます。

機械推論ナレッジベースの新しいアップデートがある場合は、[Machine Reasoning Knowledge Base] ウィンドウに [AVAILABLE UPDATE] 領域が表示され、アップデートの [Version] と [Details] が示されます。

- [AUTO UPDATE]：機械推論ナレッジベースが Cisco DNA Center で自動的に毎日更新されます。
- [CISCO CX CLOUD SERVICE FOR NETWORK BUG IDENTIFIER AND SECURITY ADVISORY]：自動構成を実行できる CX Cloud と Cisco DNA Center を統合します。この統合により、Cisco DNA Center のセキュリティ アドバイザリ ツールからデバイスの強化された脆弱性検出が直接提供されます。

ステップ 3 （推奨）[AUTO UPDATE] チェックボックスをオンにして、機械推論ナレッジベースを自動的に更新します。
[Next Attempt] 領域に、次回の更新の日付と時刻が表示されます。

自動更新は、Cisco DNA Center がクラウドの機械推論エンジンに正常に接続されている場合にのみ実行できます。

ステップ 4 機械推論ナレッジベースを Cisco DNA Center で手動で更新するには 、次のいずれかを実行します。

- [AVAILABLE UPDATES] の下にある [Update] をクリックします。[Success] ポップアップウィンドウが表示され、更新のステータスが表示されます。
- 機械推論ナレッジベースをローカルマシンに手動でダウンロードして Cisco DNA Center にインポートします。次の手順を実行します。

  1. [Download] をクリックします。

     [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. [Import] をクリックして、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 にインポートします。

ステップ 5 [CISCO CX CLOUD SERVICE FOR NETWORK BUG IDENTIFIER AND SECURITY ADVISORY] チェックボックスをオンにして、ネットワークバグ ID およびセキュリティアドバイザリとの Cisco CX Cloud の連携を有効にします。

ステップ 6 [Security Advisories Settings] エリアで、[RECURRING SCAN] トグルボタンをクリックして、毎週の定期的なスキャンを有効または無効にします。

ステップ 7 [CISCO CX CLOUD] トグルボタンをクリックして、Cisco CX Cloud を有効または無効にします。

ローカリゼーションの有効化

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

デフォルトの言語を変更するには、次のタスクを実行します。

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

- Google Chrome から、次の手順を実行します。

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

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

- Mozilla Firefox から、次の手順を実行します。

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

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

ステップ 2 Cisco DNA Center にログインします。

GUI 画面は、選択した言語で表示されます。

図 *2* : ローカライズされたログイン画面の例

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。