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。

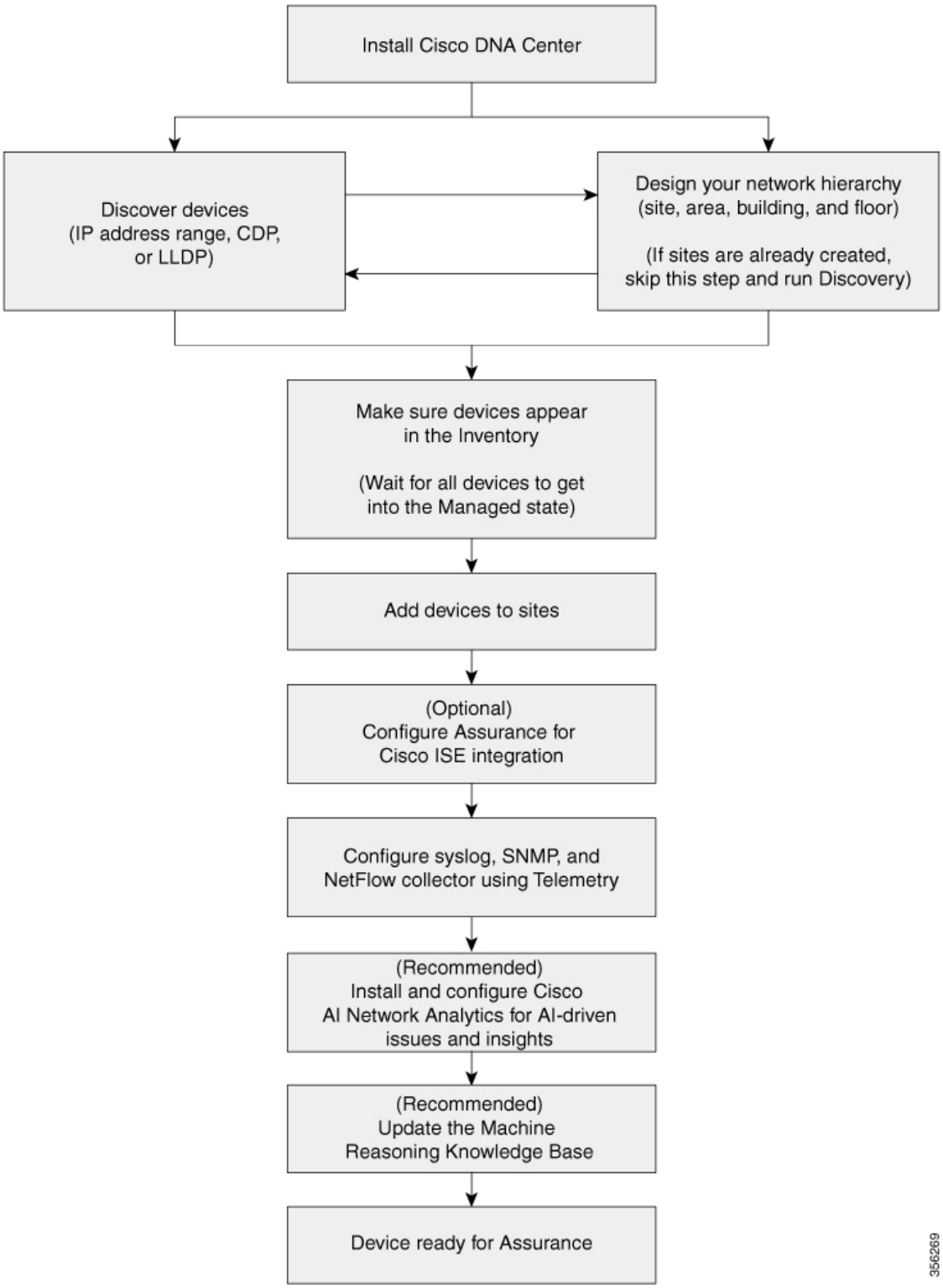
基本的な設定のワークフロー

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 （12 ページ）、およびLLDP を使用したネットワークの検出 （16 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作成 （21 ページ）または既存の Cisco ネットワーク階層の使用 （24 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 （44 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 （50 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 （52 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 （56 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 の設定 （57 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 （60 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。

ディスカバリ クレデンシャル

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

- ネットワークデバイス：CLI と SNMP のクレデンシャル。

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

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

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

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

ディスカバリクレデンシャルを定義するには、メニューアイコン（☰）をクリックして、**[Tools]** > **[Discovery]** > **[Add Discovery]**の順にクリックします。続行するには、次の手順とディスカバリクレデンシャルを使用します。

- CDP を使用したネットワークの検出 （12 ページ）
- 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）
- LLDP を使用したネットワークの検出 （16 ページ）

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。

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

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。

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。

フィールド	説明
Username	SNMPv3 設定に関連付けられている名前。
Mode	SNMP メッセージを必要とするセキュリティ レベル。次のいずれかのモードを選択します。 • [Authentication and Privacy]：認証と暗号化の両方を行います。 • [Authentication, No Privacy]：認証は行いますが、暗号化は行いません。 • [No Authentication, No Privacy]：認証も暗号化も行いません。
Auth. Type	使用する認証タイプ（[Mode] として [Authentication and Privacy] または [Authentication, No Privacy] 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 (not recommended)]：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 [Authentication and Privacy] を選択した場合に有効になります）。次のいずれかのプライバシー タイプを選択します。 • [AES128]：暗号化の 128 ビット CBC モード AES。 • **CISCOAES192**：シスコのデバイス上での暗号化の 192 ビット CBC モード AES。 • **CISCOAES256**：シスコのデバイス上での暗号化の 256 ビット CBC モード AES。 （注） • ディスカバリ機能とインベントリ機能は、CISCOAES192 プライバシータイプと CISCOAES256 プライバシータイプのみをサポートします。 • Cisco DNA アシュアランス は、これらのプライバシータイプをサポートしていません。
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。

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 (in Seconds)]	再試行の時間間隔（秒単位）。

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。
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。

表 *6 : NETCONF* 設定

フィールド	説明
Port	デバイスのポート。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

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、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）およびLLDP を使用したネットワークの検出 （16 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 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。
ウィンドウが表示されます。

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 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 5 [Credentials]エリアを展開し、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に構成します。

既存のクレデンシャルを使用する場合は、それらを選択してください。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 6 独自のクレデンシャルを構成するには、[Add Credentials] をクリックします。

CLI および SNMP v2c クレデンシャルを設定する必要があります。その他のクレデンシャルはオプションです。フィールド情報については、「ディスカバリ クレデンシャル （7 ページ）」[英語] を参照してください。

現在のジョブのクレデンシャルのみを保存するには、[Save] をクリックします。現在のジョブと将来のジョブのクレデンシャルを保存するには、[Save as global settings] チェックボックスをオンにして、[Save] をクリックします。

ステップ 7 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。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 8 [Start] をクリックします。

（注）
- 最大 5 台のデバイスを繰り返しスケジュールするように設定できます。
- 定期的な検出では、新しいデバイスのみが検出されます。デバイスが Cisco DNA Center にすでに存在する場合、そのデバイスは検出では更新されません。

[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。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 （12 ページ）およびLLDP を使用したネットワークの検出 （16 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 メニューアイコン（☰）をクリックして、**[Tools]** > **[Discovery]**。
[Discovery] ウィンドウがダッシュレットとともに表示されます。

ステップ 2 Add Discovery をクリックします。
[新規検出（New Discovery）] ウィンドウが表示されます。

ステップ 3 [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 4 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) [Discovery Type] で、[IP Address/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) （任意） 検出スキャンから除外する IP アドレス/範囲またはサブネットを [Subnet Filter] フィールドに入力します。個別の IP アドレス（*x.x.x.x*）またはクラスレスドメイン間ルーティング（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。

e) [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 5 [Credentials]エリアを展開し、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に構成します。

既存のクレデンシャルを使用する場合は、それらを選択してください。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 6 独自のクレデンシャルを構成するには、[Add Credentials] をクリックします。

CLI および SNMP v2c クレデンシャルを設定する必要があります。その他のクレデンシャルはオプションです。フィールド情報については、「ディスカバリ クレデンシャル （7 ページ）」[英語] を参照してください。

現在のジョブのクレデンシャルのみを保存するには、[Save]をクリックします。現在のジョブと将来のジョブのクレデンシャルを保存するには、[Save as global settings] チェックボックスをオンにして、[Save] をクリックします。

ステップ 7 （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。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 8 [Start] をクリックします。

（注）
- 最大 5 台のデバイスを繰り返しスケジュールするように設定できます。
- 定期的な検出では、新しいデバイスのみが検出されます。デバイスが Cisco DNA Center にすでに存在する場合、そのデバイスは検出では更新されません。

[Discoveries] ウィンドウにスキャンの結果が表示されます。

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

LLDP を使用したネットワークの検出

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

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 （12 ページ）およびIP アドレス範囲を使用したネットワークの検出 （15 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 メニューアイコン（☰）をクリックして、**[Tools]** > **[Discovery]**。
[Discovery] ウィンドウがダッシュレットとともに表示されます。

ステップ 2 Add Discovery をクリックします。
[新規検出（New Discovery）] ウィンドウが表示されます。

ステップ 3 [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 4 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 5 [Credentials]エリアを展開し、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に構成します。

既存のクレデンシャルを使用する場合は、それらを選択してください。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 6 独自のクレデンシャルを構成するには、[Add Credentials] をクリックします。

CLI および SNMP v2c クレデンシャルを設定する必要があります。その他のクレデンシャルはオプションです。フィールド情報については、「ディスカバリ クレデンシャル （7 ページ）」[英語] を参照してください。

現在のジョブのクレデンシャルのみを保存するには、[Save]をクリックします。現在のジョブと将来のジョブのクレデンシャルを保存するには、[Save as global settings] チェックボックスをオンにして、[Save] をクリックします。

ステップ 7 （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。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 8 [Start] をクリックします。

（注）
- 最大 5 台のデバイスを繰り返しスケジュールするように設定できます。
- 定期的な検出では、新しいデバイスのみが検出されます。デバイスが Cisco DNA Center にすでに存在する場合、そのデバイスは検出では更新されません。

[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、[View All Discoveries] 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、[View All Discoveries] をクリックします。

ステップ 3 左側のペインで、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、[View All Discoveries] をクリックします。

ステップ 3 左側のペインで、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。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、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作成（21 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 既存の Cisco ネットワーク階層の使用 （24 ページ） または 既存の Ekahau ネットワーク階層の使用 （28 ページ）を参照してください。

新しいネットワーク階層の作成

新しいサイト（またはエリア）、建物、およびフロアを作成して、新しいネットワーク階層を作成します。

サイトの作成、編集、削除

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 このウィンドウから、サイトを追加、編集、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
サイトを追加します。	**1.** 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。 **2.** [Area Name] フィールドに、サイト名を入力します。 **3.** [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。 **4.** [Add]をクリックします。
サイトを編集します。	**1.** 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。 **2.** [Edit Area] ダイアログボックスで、必要な編集を行います。 **3.** [更新（Update）] をクリックします。
サイトを削除する。	**1.** 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。 **2.** [OK] をクリックします。

ビルディングの追加、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 このウィンドウから、ビルディングを追加、編集、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
ビルディングを追加します。	1. [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。 2. [Add Building] ダイアログボックスでビルディングの詳細を追加します。 フィールドに住所を入力するか、マップをクリックできます。住所を追加すると、[Longitude] および [Latitude] の座標フィールドが自動的に設定されます。これらの座標は、ビルディングの北西角に対応し、Cisco DNA Center と統合されている場合は、Cisco DNA Spaces や Cisco Connected Mobile Experiences（CMX）などのロケーションサービスで使用されます。 3. [Add]をクリックします。
ビルディングを編集します。	1. 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 Building] を選択します。 2. [Edit Building] ダイアログボックスで、必要な編集を行います。 3. [更新（Update）] をクリックします。
ビルディングを削除します。	1. 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。 2. [OK] をクリックします。

フロアの追加、編集、および削除

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してフロアマップを後から追加することも、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。

フロアとフロアマップを同時に追加するには、『*Cisco DNA Center ユーザガイド*』[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、 **[Design]** > **[Network Hierarchy]**。

ステップ 2 このウィンドウから、フロアを追加、編集、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
基本フロアを追加します。	**1.** 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。 **2.** [Floor Name] フィールドにフロアの名前を入力します。 **3.** ワイレスデバイスがある場合、[Type (RF Model)] ドロップダウンリストで、フロアに適用する RF モデルを選択します。 RF モデルにより、カバレッジエリア内の RF 信号の相対強度を示す 2D および 3D ヒートマップを計算するときの RF の計算方法が決まります。 **4.** [Floor Number]、[Floor Type]、および [Floor Thickness] フィールドを設定します。 フロアのタイプと厚さは、ワイヤレスデバイスのヒートマップを計算するときに使用されます。 **5.** [Floor Image] エリアでのフロアマップイメージのアップロードをスキップします。 **6.** [Width]、[Length]、および [Height] フィールドでマップの寸法を設定します。 **7.** [Add]をクリックします。
フロアを編集します。	**1.** 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。 **2.** [Edit Floor] ダイアログボックスで、必要な変更を行います。 **3.** [更新（Update）] をクリックして変更を保存します。
フロアを削除します。	**1.** 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、[Delete Floor] を選択します。 **2.** [OK] をクリックします。

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。

Cisco Prime Infrastructure からのサイト階層のエクスポート

Cisco Prime Infrastructure からサイト階層を CSV ファイル形式でエクスポートできます。CSV ファイルには、サイト名、親階層、フロア数、場所、サイトアドレスなどの詳細が含まれています。

始める前に

サイト階層のエクスポートは Cisco Prime Infrastructure リリース 3.2 以降でサポートされます。

ステップ 1 Cisco Prime Infrastructure で、**[Inventory]** > **[Group Management]** > **[Network Device Groups]** の順に選択します。

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

ステップ 3 [Export Groups] ダイアログボックスで、[APIC-EM] オプションボタンをクリックします。

ステップ 4 CSV ファイルをダウンロードするには、[OK] をクリックします。

CSV ファイルがダウンロードされます。

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

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

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

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

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

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

ステップ 4 次のオプションの少なくとも 1 つを選択します。

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

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

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

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

次のメッセージは、操作の進行状況を示しています。

```
Exporting data is in progress
```

TAR ファイルが作成され、ローカルマシンに保存されます。

ステップ 6 [Done] をクリックします。

Cisco DNA Center へのサイト階層のインポート

Cisco Prime Infrastructure から CSV ファイルとしてエクスポートしたサイト階層をインポートできます。サイト階層のエクスポートについては、*Cisco 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 DNA Center へのマップアーカイブのインポート

マップアーカイブ TAR ファイルを Cisco DNA Center にインポートできます。たとえば、Cisco Prime Infrastructure からエクスポートした TAR ファイルをアップロードできます。

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

サイト階層のエクスポートについては、「Cisco Prime Infrastructure からのマップアーカイブのエクスポート （26 ページ）」を参照してください。

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

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

ステップ 3 [Import Maps] ダイアログボックスに、マップアーカイブファイルをドラッグアンドドロップします。

ステップ 4 [Import] をクリックします。

マップアーカイブファイルがインポートされます。

既存の Ekahau ネットワーク階層の使用

Ekahau Pro ツールを使用すると、フロアレイアウト、AP の場所、障害物など、企業の完全なネットワーク計画を作成できます。フロアレイアウトを作成したら、シミュレートしたネットワーク計画を Ekahau プロジェクトファイルとしてエクスポートできます。実際のサイト調査データを、Cisco DNA Center で使用できる形式にエクスポートすることもできます。

Cisco DNA Center からの Ekahau プロジェクトのエクスポート

Ekahau Pro からネットワーク階層をエクスポートし、さらに計画するために Cisco DNA Center にインポートできます。

始める前に

Cisco DNA Center は、Ekahau Pro ツールバージョン 10.2 をサポートします。

ステップ 1 Ekahau Pro ツールでフロアレイアウトを計画します。

- ビルディングとフロアを作成します。

  Ekahau Pro ツールでビルディングを作成することは必須ではありません。

- フロアプランをインポートします。
- 計画された AP または仮定の AP を追加します。
- ビルディングの座標を追加します。
- サイト名を定義します。

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

- 障害物を追加します。
- プロジェクトをエクスポートします。

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

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

ステップ 3 Cisco DNA Center で、シスコ ワイヤレス コントローラを構成します。

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

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

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

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

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

ステップ 2 サイト、ビルディング、フロアなどのネットワーク階層を設計します。

（注） 詳細については、サイトの作成、編集、削除 （22 ページ）、ビルディングの追加、編集、および削除 （22 ページ）、およびフロアの追加、編集、および削除 （23 ページ）を参照してください。

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

ステップ 3 左側のペインで、Ekahau プロジェクトをインポートするサイトの横にある省略記号 ••• のアイコンにカーソルを合わせて、[Import Ekahau Project] を選択します。

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

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

（注） 建物をインポートするには、Ekahau プロジェクト内に座標が含まれている必要があります。Ekahau Pro で座標を追加できます。Ekahau プロジェクトのインポートが成功すると、計画された各 AP は、AP 名を使用してインベントリ内の既存の実際の AP にマッピングされます。計画された AP は、フロアマップ上にアイコン [P] とともに表示されます。たとえば、計画済みの AP の名前が SJC01-02-AP-B-1 の場合、インポートプロセスでは同じ名前の実際の AP が検索されます。

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

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

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

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

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

[Assign Planned APs] パネルが表示されます。

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

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

ステップ 9 [Save] をクリックします。

Ekahau サイト調査の Cisco DNA Center へのインポート

Ekahau サイト調査をアップロードして、ネットワーク階層に建物とフロアを作成できます。サイト調査には、ワイヤレスデバイスが割り当てられているサイト、建物、フロア、およびフロアマップ上の位置など、ワイヤレスデバイスに関する情報が含まれます。ただし、AP アンテナ情報は含まれません。そのため、CSV ファイルを使用してこの情報を個別にアップロードする必要があります。

Cisco DNA Center には、ダウンロードして編集して必要な AP アンテナ情報を定義できる CSV テンプレートファイルが含まれています。

図 2 : *CSV* テンプレートファイルには、次のフィールドとデフォルトが含まれています。

	A	B	C	D	E	F	G	H	I	J
1	model	antennaName0	antennaAzimuth0	antennaElevation0	antennaName1	antennaAzimuth1	antennaElevation1	antennaName2	antennaAzimuth2	antennaElevation2
2	AP2700I	Internal-2700-5GHz	90d	0d	Internal-2700-2.4GHz	90d	0d			
3	AP1850I	Internal-1850-5GHz	90d	0d	Internal-1850-2.4GHz	90d	0d			
4	AP3800E	AIR-ANT2524DB-R-5GHz	179.9543762d	0d	AIR-ANT2524DB-R-2.4GHz	179.9543762d	0d			
5										

AP が Cisco DNA Center デバイスインベントリにない場合、計画された AP としてインポートされます。ただし、命名規則を使用して、APをデバイスインベントリに追加するときに、Cisco DNA Center ではそれを実際の AP に自動的に変換することができます。

命名規則は、AP の後に AP の MAC アドレスの最後の 4 桁が続きます（例：AP-c4:e0）。この情報を使用して、Cisco DNA Center は提供された数字を AP のイーサネット MAC アドレスまたは無線 MAC アドレスの最後の 4 桁と照合しようとします。この情報がない場合、または一致に失敗した場合は、Cisco DNA Center は AP 名の照合を試みます。

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

ステップ 2 [Add Site] > [Add Area] をクリックします。

または、左側のペインで [Global] または親サイトの横にある省略記号 ••• にカーソルを合わせ、[Add Area] を選択することもできます。詳細については、サイトの作成、編集、削除 （22 ページ）を参照してください。

ステップ 3 左側のペインで、作成したサイトの横にある省略記号 ••• アイコンにカーソルを合わせて、[Import Ekahau Survey] を選択します。

ステップ 4 [Import Ekahau Survey] ダイアログボックスの [Ekahau Survey] ボックス領域に、Ekahau 調査ファイルをドラッグアンドドロップするか、または [Choose a file] リンクをクリックして ESX ファイルを参照します。

ステップ 5 CSV ファイルを [AP Mapping CSV] ボックス領域にドラッグアンドドロップするか、[Choose a file] をクリックして CSV ファイルを参照します。

（注） CSV ファイルがない場合は、[Download AP Mapping Template] をクリックして、編集可能な CSV ファイルをダウンロードして、アップロードすることができます。

ステップ 6 [Import] をクリックします。

ファイルが正常にダウンロードされると、成功メッセージが表示されます。

ステップ 7 [View Hierarchy] をクリックし、フロアに移動して、デバイスがインポートされ、適切に配置されていることを確認します。

詳細を表示するには、デバイスにカーソルを合わせます。

2D フロアマップのデバイスとオーバーレイオブジェクトの構成

2D マップで、デバイスを設定し、フロアマップ上にオブジェクトをオーバーレイできます。『Cisco DNA アシュアランス User Guide』[英語] には、2D マップの操作に関する基本的なガイダンスが記載されています。2D マップに加えて、Cisco DNA Center はより多くの機能を備えた 3D マップをサポートします。2D と 3D の両方のマップ機能の詳細については、『*Cisco DNA Center ユーザガイド*』[英語] を参照してください。

デバイス

- [APs]：アクセスポイント（AP）は、無線ネットワークと有線ネットワーク間の接続ポイントとして、またはスタンドアロンの無線ネットワークのセントラルポイントとして機能します。2D マップでは、AP は実際にインストールされているデバイスを表します。Cisco DNA Center でサポートされる AP の一覧については、「*Cisco DNA Center 互換性マトリクス*」[英語] を参照してください。
- [Planned APs]：計画済み AP は、まだインストールされていない AP を表します。計画済み AP をマップ上に配置することで、実際に AP をインストールする前に、ワイヤレスネットワークの RF カバレッジを想定して変更を加えることができます。
- [Sensors]：センサーは、Cisco PnP を使用してブートストラップされる専用の Cisco Aironet 1800S アクティブセンサーです。Assurance 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、Assurance 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、「センサーの管理とセンサー主導のテスト」[英語] を参照してください。

オーバーレイオブジェクト

- [Coverage Areas]：デフォルトでは、フロアマップの一部として定義されたエリアは、無線カバレッジエリアと見なされます。ただし、長方形以外のビルディングがある場合、またはフロア内で長方形以外または多角形のエリアをマークする場合には、[Coverage Areas] 描画ツールを使用してカバレッジエリアを作成できます。
- [Openings]：吹き抜けはアトリウムとも呼ばれ、ビルディング内のオープンエアーまたは天窓で覆われたエリアです。吹き抜けは複数のフロアに伸びる可能性があり、ワイヤレス信号のカバレッジエリアに影響を与える可能性があります。
- [Location Regions]：ロケーションリージョンは、ヒートマップの計算に含まれるまたは除外されるエリアを定義します。包含エリアは計算に含まれ、除外エリアは計算に含めないエリアです。たとえば、ビルディング内の吹き抜け、アトリウム、階段の吹き抜けなどのエリアを除外して、作業エリア（小個室、研究室、製造現場など）を含めることができます。
- [Walls]：壁は、ビルディング内の外部または内部の垂直構造であり、さまざまな材料と厚さで作成できます。そのため、ヒートマップの計算方法に影響します。
- [Shelving Units]：シェルフユニットは、信号の減衰に影響を与える障害物です。シェルフユニットがある場所の例としては、天井が高い倉庫などがあります。

- [Markers]：マーカーは、マップ上の場所を示します。マーカーを作成するときは、後で識別しやすいように、マーカーに名前を付けて配置することができます。
- [GPS Markers]：Cisco DNA Center と統合すると、Cisco DNA Spaces や Cisco Connected Mobile Experiences（CMX）などのロケーションサービスは、GPS マーカーを使用してクライアントのおおよその地理的位置を計算します。
- [Align Points]：位置合わせポイントは、物理的な形状が異なる複数のフロアを配置するために使用されるマーカーです。3D マップでは、フロアはマップの左上隅（ポイント 0,0）に配置されます。フロアごとに独立して管理すればズレは問題ありません。ただし、一部の 3D マップの機能を使用するには、実際のフロアをそのまま配置する必要があります。このずれを補正するために、2 つ以上のフロアに 1 つ以上の位置合わせポイントを挿入して、フロアが 3D マップ内で適切に上下に配置されるようにすることができます。

AP の追加、配置、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 左側の階層ツリーで、フロアを選択します。

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

ステップ 4 このウィンドウから、AP を追加、配置、編集、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 を追加します。	**1.** マップの左側のペインで、[Add APs] をクリックします。 **2.** 追加する AP の横にある [Add] をクリックします。または複数の AP を追加する場合は、追加する AP の横の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.** 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。 **4.** AP を配置するマップ上の場所をクリックします。

アクション	手順
計画済みAPの追加	1. マップの左側のペインにある [AP Models] エリアで、追加する計画済み AP の AP モデルをクリックします。 AP モデルがリストにない場合は、[Add Model] をクリックして、リストに追加する AP モデルを選択します。 2. 計画済み AP を配置するマップ上の場所をクリックします。 3. [Edit Planned AP] スライドインペインで、歯車アイコンをクリックし、一意の名前パターンを追加します。 4. 必要に応じて、アンテナタイプと方位角と仰角を定義します。 5. 引き続き同じプロパティを持つ計画済みの AP を追加するには、マップ上の場所をクリックします。 6. 計画済み AP の追加を止めるには、**Esc** を押すか、フロアマップを右クリックします。
AP の編集	1. マップで AP を右クリックし、[Edit] を選択します。 2. 編集可能な AP 設定を変更します。次のフィールドに関する情報に注意してください。 • **Antenna**：外部の AP の場合は、アンテナを選択する必要があります。選択しないと、AP はマップに表示されません。 • **Azimuth**：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、右向きは 0 度または 360 度で、下向きは 90 度です。 値を手動で入力するか、フィールドの下の青色の矢印を使用して値を変更できます。 無指向性アンテナの場合、仰角が 0 の場合、方位角は関係ありません。 • **Elevation**：仰角（度）を手動で入力するか、フィールドの下の青色の矢印を使用して、値を変更できます。 天井に配置するように設計された AP およびアンテナモデルの場合、仰角が 0 の場合は下を向きます。壁に配置するように設計された AP およびアンテナモデルの場合、仰角が 0 の場合は水平方向を向き、負の値の場合は下を向きます。 3. [更新（Update）] をクリックします。

アクション	手順
AP の削除	**1.** AP をクリックするか、複数の AP を選択する場合は、最初の AP をクリックし、Shift キーを押しながら残りの AP をクリックします。 **2.** [Edit] ペインで、[Remove Selected] をクリックします。 **3.** マップツールバーの [Save] をクリックします。

センサーの追加、配置、および削除

始める前に

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。

ステップ 1 メニューアイコン（☰）をクリックして、を使用して無効にすることができます。

ステップ 2 フロアを 左側の階層ツリーから、 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 このウィンドウから、センサーを追加、配置、編集、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
センサーの追加	**1.** [Add Sensors] スライドインペインから、追加するセンサーの横にある [Add] をクリックします。または複数のセンサーを追加する場合は、追加するセンサーの横のチェックボックスをオンにして、[Add Selected] をクリックします。 新しく追加されたセンサーは、マップの左ペインの [Unpositioned] カテゴリに表示されます。 **2.** マップの左ペインの [Unpositioned] カテゴリから、センサーをクリックします。 **3.** センサーを配置するマップ上の場所をクリックします。 **4.** [Save] をクリックします。

アクション	手順
センサーの削除	1. センサーをクリックします。複数のセンサーを選択する場合は、最初のセンサーをクリックし、Shift キーを押しながら残りのセンサーをクリックします。 2. [Edit] ペインで、[Remove] をクリックします。 3. マップツールバーの [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

この手順では、フロアマップで長方形以外または多角形のエリアをカバレッジエリアとしてマークする方法を示します。

カバレッジエリアの詳細については、「2D フロアマップのデバイスとオーバーレイオブジェクトの構成 （32 ページ）」[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、**[Design]** > **[Network Hierarchy]**。

ステップ 2 フロアを 左側の階層ツリーから、 します。

ステップ 3 マップツールバーで、**[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。

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) マップツールバーで、**[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。

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) マップツールバーで、**[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、[Remove] を選択します。

ステップ 7 マップツールバーで [Save] をクリックします。

吹き抜けの追加、編集、コピー、および削除

吹き抜けの作成は、フロアでのオープンスペース（アトリウム）の作成と似ています。通常、複数フロアのビルディングでは、吹き抜けは複数のフロアを縦方向に伸びています。この手順では、フロアマップで吹き抜けを追加、編集、および削除する方法を示します。また、吹き抜けを他のフロアにコピーする方法も示します。

吹き抜けの詳細については、「2D フロアマップのデバイスとオーバーレイオブジェクトの構成 （32 ページ）」[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、**[Design]** > **[Network Hierarchy]**。

ステップ 2 フロアを 左側の階層ツリーから、 します。

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

ステップ 4 吹き抜けを追加するには、次の手順を実行します。

a) マップの左ペインで、[Opening] をクリックします。

b) 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。

c) 引き続きポイントを作成して、吹き抜けの形状を定義します。

（注） 吹き抜けの形状には、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、吹き抜けの形状を定義し直すことができます。

d) ダブルクリックして描画ツールを終了し、形状を確定します。

ステップ 5 吹き抜けを編集するには、次の手順を実行します。

a) マップツールバーで、**[Add/Edit]** > **[Openings]** をクリックします。

b) 吹き抜け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) 吹き抜けを移動するには、網掛けされたエリア内をクリックします。次に、吹き抜けを配置する場所にドラッグアンドドロップします。

ステップ 6 別のフロアに吹き抜けをコピーするには、次の手順を実行します。

a) マップツールバーで、**[Add/Edit]** > **[Openings]** をクリックします。

b) 吹き抜けを右クリックし、[Copy to other floors] を選択します。

c) ダイアログボックスで、関連フロアの横にあるチェックボックスをオンにします。

d) [**コピー（Copy）**] をクリックします。

e) [Close] をクリックします。

ステップ 7 吹き抜けを削除するには、次の手順を実行します。

a) マップツールバーで、**[Add/Edit]** > **[Openings]** をクリックします。

b) 吹き抜けを右クリックし、[Remove] を選択します。

ステップ 8 マップツールバーで [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

ロケーションリージョンは、ヒートマップの計算に含まれるまたは計算から除外されるマップ上の領域です。次のトピックで、ロケーションリージョンを追加、編集、および削除する方法を示します。

包含リージョンの追加、編集、および削除

この手順では、包含リージョンを追加、編集、および削除する方法を示します。次のガイドラインを使用して、フロアマップで包含リージョンを定義します。

- 包含リージョン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。

包含リージョンの詳細については、2D フロアマップのデバイスとオーバーレイオブジェクトの構成 （32 ページ）を参照してください。

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

ステップ 2 フロアを 左側の階層ツリーから、 します。

ステップ 3 マップツールバーで、**[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で、[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 [Remove] を選択します。

ステップ 8 マップツールバーで [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

この手順では、除外リージョンを追加、編集、および削除する方法を示します。次のガイドラインを使用して、フロアマップで除外リージョンを定義します。

- 除外リージョン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。
- 除外リージョンは包含リージョンの境界内で定義されます。

- フロアマップ上で除外リージョンを複数定義できます。

除外リージョンの詳細については、2D フロアマップのデバイスとオーバーレイオブジェクトの構成 （32 ページ）を参照してください。

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

ステップ 2 フロアを 左側の階層ツリーから、 します。

ステップ 3 マップツールバーで、**[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 [Remove] を選択します。

ステップ 8 マップツールバーで [Save] をクリックします。

壁の追加、編集、および削除

この手順では、フロアマップで壁を追加、編集、および削除する方法を示します。

壁の詳細については、「2D フロアマップのデバイスとオーバーレイオブジェクトの構成 （32 ページ）」[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、**[Design]** > **[Network Hierarchy]**。

ステップ 2 フロアを 左側の階層ツリーから、 します。

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

ステップ 4 壁を追加するには、次の手順を実行します。

a) マップの左側のペインで、[Others] または [On this floor] カテゴリの壁のタイプをクリックします。

（注） 壁タイプがリストにない場合は、[Add Wall Type] をクリックしてカスタムの壁タイプを作成します。

b) マップをクリックして、壁の開始ポイントを作成します。

c) 壁を終了する次のポイント、またはコーナーを作成する次のポイントにカーソルを移動して、もう一度クリックします。

d) 引き続きポイントを作成して、壁の形状を定義します。
e) 壁を終了するには、マップをダブルクリックします。

   または、左側のペインで壁のタイプをクリックします。

f) 描画ツールを終了するには、マップをもう一度ダブルクリックします。

ステップ 5 壁のタイプを変更し、壁のタイプに応じてそのパラメータを設定するには、次の手順を実行します。

a) 変更する壁をクリックします。

   [Wall Type] ダイアログボックスが表示されます。

b) [Wall Type] ドロップダウンリストから、壁のタイプを選択します。
c) 新しい壁タイプに適したその他のパラメータを設定します。
d) [更新（Update）] をクリックします。

ステップ 6 壁を移動するには、次の操作を行います。

a) 移動する壁にカーソルを合わせます。

   壁が黒くなります。これは選択されたことを意味します。

b) 壁をクリックし、新しい場所にドラッグアンドドロップします。

ステップ 7 壁を削除するには、壁を右クリックして [Remove] を選択します。

ステップ 8 マップツールバーで [Save] をクリックします。

シェルフユニットの追加、コピー、編集、および削除

この手順では、フロアマップでシェルフユニットを追加、コピー、編集、および削除する方法を示します。

シェルフユニットの詳細については、「2D フロアマップのデバイスとオーバーレイオブジェクトの構成 （32 ページ）」[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、**[Design]** > **[Network Hierarchy]**。

ステップ 2 フロアを 左側の階層ツリーから、 します。

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

ステップ 4 シェルフユニットを追加するには、次の手順を実行します。

a) マップの左ペインで、追加するシェルフタイプをクリックします。
b) シェルフダイアログボックスで、名前、寸法、向き、およびユニットが両面かどうかを構成するか、デフォルト値のままにします。向きとは、シェルフユニットの角度を意味します。シェルフユニットの向き 0 はシェルフユニットが垂直で y 軸に平行であることを意味します。

   シェルフタイプがリストにない場合は、[Add Shelving Type] をクリックしてシェルフタイプを作成します。

c) [Add Shellving] をクリックします。

シェルフユニットがマップ上に表示されます。

d) シェルフユニットをマップ上の場所にドラッグアンドドロップします。

ステップ 5 シェルフユニットのコピーまたはアレイを作成するには、次のいずれかを実行します。

- コピーを作成するには、シェルフユニットを右クリックして [Clone] を選択します。
- アレイを作成するには、シェルフユニットを右クリックして [Array] を選択します。次に、ユニットの数とそれらの間の距離を指定します。

ステップ 6 名前、寸法、向き、および両面かどうかを編集するには、シェルフユニットを右クリックし、[Edit] を選択します。

ステップ 7 シェルフユニットを削除するには、シェルフユニットを右クリックし、[削除] を選択します。

ステップ 8 マップツールバーで [Save] をクリックします。

マーカーの追加、編集、および削除

次の手順では、マーカーを追加、編集、および削除する方法を示します。

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

ステップ 2 フロアを 左側の階層ツリーから、 します。

ステップ 3 マップツールバーで、**[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で、[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 [Remove] を選択します。

ステップ 10 マップツールバーで [Save] をクリックします。

GPS マーカーの追加、編集、および削除

この手順では、GPS マーカーを追加、編集、および削除する方法を示します。GPS マーカーの詳細については、「2D フロアマップのデバイスとオーバーレイオブジェクトの構成（32 ページ）」[英語] を参照してください。

（注） GPS マーカーは建物の属性です。建物のすべてのフロアに適用できます。

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

ステップ 2 フロアを 左側の階層ツリーから、 します。

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

ステップ 4 GPS マーカーを追加するには、次の手順を実行します。

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

b) マップ上で、GPS マーカーを配置する場所をクリックします。

GPS マーカーは、外壁の内側、通常は建物の角に配置する必要があります。

c) [Place Markers] ダイアログボックスで、適切なフィールドに名前、緯度、経度、X 座標、および Y 座標を入力します。

フロアの北西角にある GPS マーカーの緯度と経度の座標が、建物の座標と一致する必要があります。

d) [GPS マーカーの追加（Add GPS Marker）] をクリックします。

ステップ 5 GPS マーカーを編集するには、GPS マーカーを右クリックして [Edit] を選択します。

ステップ 6 GPS マーカーを削除するには、GPS マーカーを右クリックして [Remove] を選択します。

ステップ 7 マップツールバーで [Save] をクリックします。

位置合わせポイントの追加、編集、および削除

この手順では、位置合わせポイントを追加、編集、および削除する方法を示します。位置合わせポイントの詳細については、「2D フロアマップのデバイスとオーバーレイオブジェクトの構成 （32 ページ）」[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、**[Design]** > **[Network Hierarchy]**。

ステップ 2 フロアを 左側の階層ツリーから、 します。

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

ステップ 4 位置合わせポイントを追加するには、次の手順を実行します。

a) マップの左側のペインで、[Align Points] アイコンをクリックします。

b) マップ上で、位置合わせポイントを配置する場所をクリックします。

ステップ 5 位置合わせポイントの名前を編集するには、次の手順を実行します。

a) 位置合わせポイントを右クリックし、[Edit] を選択します。

b) 名前を変更し、[Edit Marker] をクリックします。

ステップ 6 位置合わせポイントの位置を変更するには、次の手順を実行します。

a) 位置合わせポイントを右クリックし、[Edit] を選択します。

b) [Edit Marker] をクリックします。

c) 位置合わせポイントを新しい位置にドラッグアンドドロップします。

ステップ 7 位置合わせポイントを削除するには、位置合わせポイントを右クリックして [Remove] を選択します。

ステップ 8 マップツールバーで [Save] をクリックします。

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（43 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]** > **[Network Devices]** > **[Inventory]** の順に選択します。

ステップ 2 更新するデバイスを選択します。

ステップ 3 **[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

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

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

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

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

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

[Inventory] テーブルに 25 を超えるエントリがあり、[Focus] ドロップダウンリストから別のビューを選択した場合、新しい各ビューで同じ数のエントリが表示されます。

始める前に

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

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

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

表 *7*: インベントリ

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。
IP Address	デバイスの IP アドレス。

カラム	説明

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

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。

カラム	説明
[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。
MAC Address	デバイスの MAC アドレス。
Image Version	デバイスで現在実行されている Cisco IOS ソフトウェア。
Platform	シスコ製品の部品番号。
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の稼働時間。

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設計 （21 ページ）を参照してください。
Last Updated	Cisco DNA Center がデバイスをスキャンし、デバイスに関する新しい情報でデータベースを更新した最新の日付と時刻。
Device Family	ルータ、スイッチ、ハブ、またはワイヤレスコントローラなどの関連するデバイスのグループ。
Device Series	デバイスのシリーズ番号（Cisco Catalyst 4500 シリーズ スイッチなど）。
Resync Interval	デバイスのポーリング間隔。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。
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。この状態は、定期的な収集が行われたときに発生します。 • [Wrong Credentials]：デバイスをインベントリに追加した後にデバイスのクレデンシャルが変更された場合、この状態が表示されます。 • [In Progress]：インベントリ収集が実行されています。

カラム	説明
プロビジョニング ステータス	デバイスで試行された最後のプロビジョニング操作のステータスが示されます。過去のプロビジョニング操作のステータスを確認するには、[See Details] をクリックします。 • [Success]：デバイスでの最近の操作が成功しました。 • [Success] 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。
Credential Status	デバイスのクレデンシャルステータスが示されます。 • [Not Applied]：デバイスのクレデンシャルがデバイスに適用されていません。 • [Success]：デバイスのクレデンシャルがデバイスに正常に適用されました。 • [Failed]：デバイスのクレデンシャルがデバイスで失敗しました。 クレデンシャルの詳細を表示するには、[See Details] をクリックします。 [Credential Status] slide-in paneには、クレデンシャルの [Type]、[Name/Description]、[Status]、および [Details] が表示されます。 ステータスが [Failed] のデバイスの場合、[Actions] 列の省略記号アイコン（ *** ）の上にカーソルを置き、[Retry] または [Clear] を選択します。 • [Retry]：デバイスにクレデンシャルを適用します。 • [Clear]：デバイスのクレデンシャルをクリアします。
AP Ethernet Mac Address	AP イーサネット MAC アドレスに関する詳細を表示します。
AP CDP Neighbors	インベントリ リスト 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。

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、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 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、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 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、[Save] をクリックします。

ステップ 6 （任意） 複数のデバイスを選択して同じ場所に追加する場合は、最初のデバイスで [Apply to All] チェックボックスをオンにして残りのデバイスに同じ場所を割り当て、[Next] をクリックします。

ステップ 7 [Application and Endpoint Visibility is enabled on all applicable devices.Check this to skip enabling it on all devices] チェックボックスをオンにします。

（注） [Application and Endpoint Visibility] の有効化は、コントローラベースのアプリケーション認識（CBAR）の有効化または展開解除されたアプリケーション可視性サービス（AVS）がサポートされないデバイスについてはデフォルトでスキップされます。

ステップ 8 サマリ設定を確認し、[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 デバイスを今すぐ（[Now]）サイトに割り当てるか、後でスケジュールするかを選択します。

ステップ 11 [**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。

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

   後で、作成した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。

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

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

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

4. CLI 設定の詳細を表示し、[Deploy] をクリックします。

5. 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。

6. 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。

7. 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 をユーザー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 Install and Upgrade Guides 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 Release Note 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。『サイトの作成、編集、削除 （22 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 Endpoint Data Collection] エリアで、[Enable Cisco DNA Center Wired Endpoint Data Collection At This Site] 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 の設定

この手順では、Cisco AI Analytics 機能を有効にして、ネットワークデバイスからのネットワークイベントのデータとインベントリ、サイト階層、およびトポロジのデータを Cisco AI Cloud にエクスポートします。

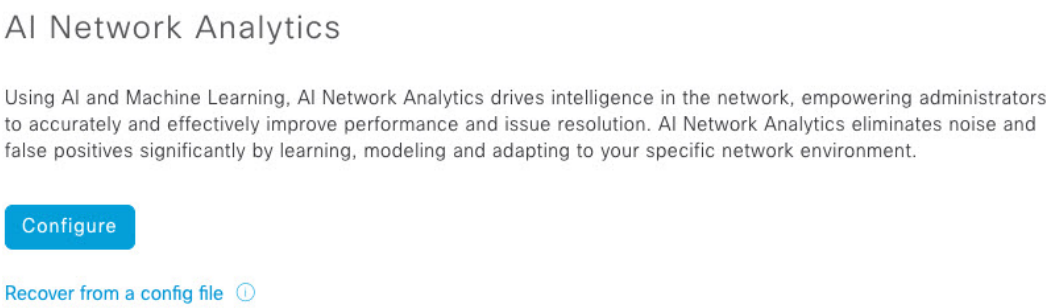
始める前に

- 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 Network Analytics アプリケーションの最新バージョンがインストールされていることを確認してください。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。

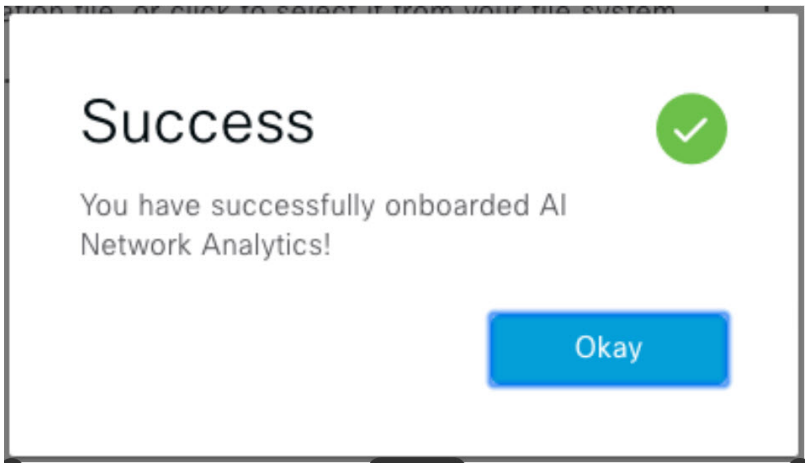


ステップ 3 次のいずれかを実行します。

- 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。



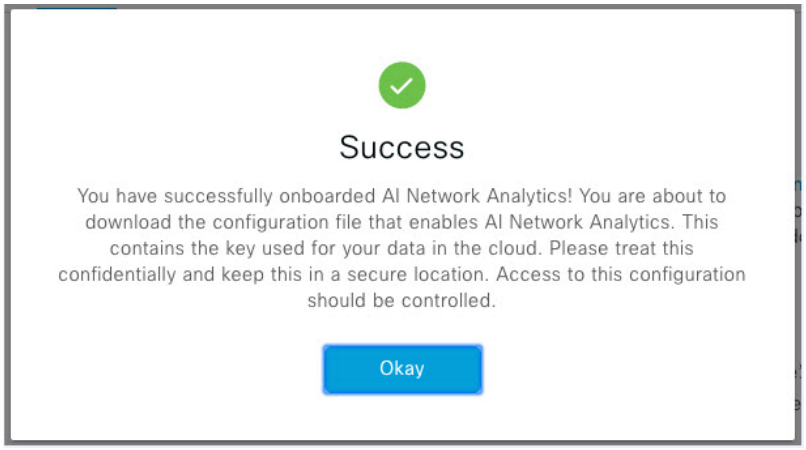
- Cisco AI Network Analytics を初めて設定する場合は、次の手順を実行します。

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。

ディセーブル Cisco AI Network Analytics

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 ウィンドウは、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. [Languages] をクリックします。
  3. [Add Languages] をクリックします。
  4. [Add languages] ダイアログボックスで、[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、[Settings] を選択します。
  2. **[Language and Appearance]** > **[Language]** エリアで、[Choose] をクリックします。
  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。

選択した言語で GUI が表示されます。

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