



アシュアランスを使用するための Cisco DNA Center の設定

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

- [制限事項と制約事項 \(1 ページ\)](#)
- [基本的な設定のワークフロー \(1 ページ\)](#)
- [デバイスの検出 \(4 ページ\)](#)
- [ネットワーク階層の設計 \(29 ページ\)](#)
- [インベントリの管理 \(51 ページ\)](#)
- [デバイスをサイトに追加する \(62 ページ\)](#)
- [Cisco DNA Center 向けの Cisco ISE の設定について \(62 ページ\)](#)
- [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 \(67 ページ\)](#)
- [Cisco AI Network Analytics データ収集の設定 \(68 ページ\)](#)
- [機械推論ナレッジベースの更新 \(71 ページ\)](#)
- [ローカリゼーションの有効化 \(72 ページ\)](#)
- [ロールベース アクセス コントロールのサポート アシュアランス \(73 ページ\)](#)

制限事項と制約事項

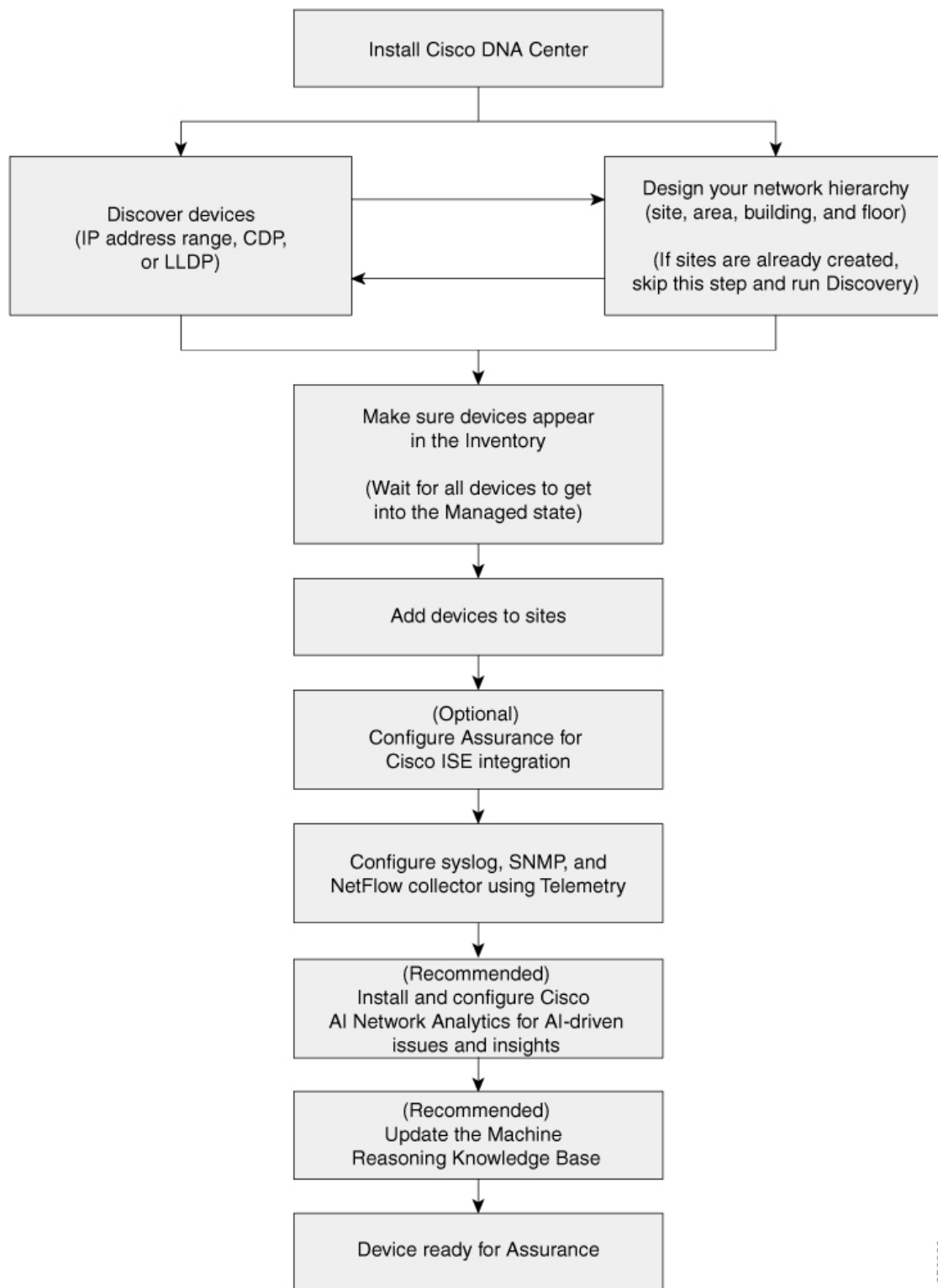
アシュアランスでは、管理対象デバイスへの NAT 接続はサポートされていません。

基本的な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。

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



356269

始める前に

[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 \(14 ページ\)](#)、[CDP を使用したネットワークの検出 \(7 ページ\)](#)、または[LLDP を使用したネットワークの検出 \(20 ページ\)](#) を参照してください。

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

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

[ネットワーク階層のサイトの作成 \(30 ページ\)](#)、[建物の追加 \(31 ページ\)](#)、および[ビルディングへのフロアの追加 \(31 ページ\)](#) 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 \(53 ページ\)](#) を参照してください。

(注) すべてのデバイスが管理状態になるのを待つ必要があります。

ステップ 4 サイトへのデバイスの追加

[デバイスをサイトに追加する \(62 ページ\)](#) を参照してください。

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

[「AP の追加、配置、および削除 \(38 ページ\)」](#) を参照してください。

ステップ 6 ネットワークでのユーザー認証に Cisco Identity Services Engine を使用している場合、アシュアランスを設定して Cisco ISE を統合できます。統合することで、アシュアランスのユーザ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 \(67 ページ\)](#) 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 \(68 ページ\)](#) 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 \(71 ページ\)](#) 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

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

ディスカバリについて

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

また、ディスカバリ機能は、デバイスの可制御性功能と連携して、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、「[サポート対象デバイスのリスト](#)」を参照してください。
- Cisco DNA Center とデバイス間の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、[インベントリ (Inventory)] ウィンドウから管理 IP アドレスを更新できます。

設定のガイドラインと制限事項のディスカバリ

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

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

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

CDP を使用したネットワークの検出

Cisco Discovery Protocol (CDP) IP アドレス範囲、または LLDP を使用してデバイスを検出できます。この手順では、CDP を使用してデバイスとホストを検出する方法を示します。ディスカバリ メソッドの詳細については、[IP アドレス範囲を使用したネットワークの検出 \(14 ページ\)](#) および [LLDP を使用したネットワークの検出 \(20 ページ\)](#) 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]**。
[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。
- [ディスカバリ タイプ (Discovery Type)] で、[CDP] をクリックします。
 - [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。
 - (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** [クレデンシヤル (Credentials)] エリアを展開し、ディスカバリ ジョブで使用するクレデンシヤルを設定します。

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

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

表 1: CLI クレデンシヤル

フィールド	説明
Name/Description	CLI クレデンシヤ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。

d) [SNMP v2c] をクリックして、次のフィールドを設定します。

表 2: *SNMPv2c* のクレデンシャル

フィールド	説明
Read	<ul style="list-style-type: none"> • [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	<ul style="list-style-type: none"> • [Name/Description] : 追加している SNMPv2c 設定の名前または説明。 • [Write Community] : デバイス上の SNMP 情報を変更するために使用される書き込みコミュニティ文字列。 (注) パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。

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

表 3: *SNMPv3* のクレデンシャル

フィールド	説明
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。

フィールド	説明
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。 <ul style="list-style-type: none"> • [noAuthNoPriv] : 認証または暗号化を提供しません。 • [AuthNoPriv] : 認証を提供しますが、暗号化は提供しません。 • [AuthPriv] : 認証と暗号化の両方を提供します。
Auth Type	使用する認証タイプ（認証モードとして [AuthPriv] または [AuthNoPriv] を選択した場合に有効になります）。次のいずれかの認証タイプを選択します。 <ul style="list-style-type: none"> • [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。 <p>(注)</p> <ul style="list-style-type: none"> • 一部のシスコ ワイヤレス コントローラでは、パスワード（あるいはパスフレーズ）は少なくとも 12 文字以上である必要があります。ワイヤレス コントローラのパスワードの最小要件を必ず確認してください。パスワードに必要な最低限の文字数が守られないと、デバイスでは Cisco DNA Center による検出、監視、管理が行われなくなります。 • パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。
Privacy Type	プライバシータイプ。（認証モードとして [AuthPriv] を選択すると有効になります）。次のいずれかのプライバシータイプを選択します。 <ul style="list-style-type: none"> • [AES128] : 暗号化の CBC モード AES。 • [None] : プライバシー設定はありません。

フィールド	説明
Privacy Password	<p>AES128 暗号化をサポートしているデバイスで交換されるメッセージを暗号化するための秘密鍵を生成するために使用される SNMPv3 プライバシーパスワード。パスワード（またはパスフレーズ）は、8 文字以上にする必要があります。</p> <p>(注)</p> <ul style="list-style-type: none"> 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 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	再試行間隔を表す秒数。

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

表 5: HTTPS クレデンシャル

フィールド	説明
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、[読み取り (Read)] または [書き込み (Write)] です。

フィールド	説明
Read	<p>最大 10 つの HTTPS 読み取りクレデンシャルを設定できます。</p> <ul style="list-style-type: none"> • [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。 <p>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。</p> <ul style="list-style-type: none"> • 小文字の英字 (a ~ z) • 大文字の英字 (A ~ Z) • 数字 (0 ~ 9) • 特殊文字 (: # _ * ?) - <p>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。</p>

フィールド	説明
Write	<p>最大 10 つの HTTPS 書き込みクレデンシャルを設定できます。</p> <ul style="list-style-type: none"> • [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。 <p>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。</p> <ul style="list-style-type: none"> • 小文字の英字 (a ~ z) • 大文字の英字 (A ~ Z) • 数字 (0 ~ 9) • 特殊文字 (: # _ * ?) - <p>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。</p>

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

(注) Cisco Catalyst 9800 シリーズワイヤレス コントローラ デバイスを検出するには、NETCONF を有効にし、ポートを次のいずれかに設定する必要があります。

- 830 (デフォルトのポート番号)
- 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)

NETCONF は、ネットワークデバイスの設定をインストール、操作、削除するメカニズムです。[Advanced] エリアで [Telnet] を選択すると、NETCONF は無効になります。

ステップ 6 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。

IP アドレス範囲を使用したネットワークの検出

ステップ 7 [Discover] をクリックして、すぐに検出を実行するか、または後で実行するために検出をスケジュールするかを選択します。

- 今すぐ検出を実行するには、[Now] ラジオボタンをクリックし、[Start] をクリックします。
- 後で検出をスケジュールするには、[Later] ラジオボタンをクリックして更新の日時を定義し、[Start] をクリックします。

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

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

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

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 \(7 ページ\)](#) および [LLDP を使用したネットワークの検出 \(20 ページ\)](#) 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。

- [Discovery Type] で、[IP Address/Range] をクリックします。
- [From] フィールドと [To] フィールドに、スキャンする Cisco DNA Center 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 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。
- 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 [クレデンシヤル (Credentials)] エリアを展開し、ディスカバリ ジョブで使用するクレデンシヤルを設定します。

すでに作成されているグローバルクレデンシヤ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ヤルを設定します。独自のクレデンシヤルを設定する場合、[保存 (Save)] をクリックして現在のジョブにのみ保存できます。または、[グローバル設定として保存 (Save as global settings)] チェックボックスをクリックし、次に [保存 (Save)] をクリックして、現在または将来のジョブに保存できます。

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

表 6: CLI クレデンシヤル

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

d) [SNMP v2c] をクリックして、次のフィールドを設定します。

表 7: *SNMPv2c* のクレデンシャル

フィールド	説明
Read	<ul style="list-style-type: none"> • [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。 <p>(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。</p>
Write	<ul style="list-style-type: none"> • [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。 <p>(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。</p>

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

表 8: *SNMPv3* のクレデンシャル

フィールド	説明
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。 <ul style="list-style-type: none"> • [noAuthNoPriv] : 認証または暗号化を提供しません。 • [AuthNoPriv] : 認証を提供しますが、暗号化は提供しません。 • [AuthPriv] : 認証と暗号化の両方を提供します。
Auth Type	使用する認証タイプ (認証モードとして [AuthPriv] または [AuthNoPriv] を選択した場合に有効になります)。次のいずれかの認証タイプを選択します。 <ul style="list-style-type: none"> • [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	<p>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。</p> <p>(注)</p> <ul style="list-style-type: none"> 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	<p>プライバシータイプ。（認証モードとして [AuthPriv] を選択すると有効になります）。次のいずれかのプライバシータイプを選択します。</p> <ul style="list-style-type: none"> [AES128]：暗号化の CBC モード AES。 [None]：プライバシー設定はありません。
Privacy Password	<p>AES128 暗号化をサポートしているデバイスで交換されるメッセージを暗号化するための秘密鍵を生成するために使用される SNMPv3 プライバシーパスワード。パスワード（またはパスフレーズ）は、8 文字以上にする必要があります。</p> <p>(注)</p> <ul style="list-style-type: none"> 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 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	再試行間隔を表す秒数。

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

表 10: HTTPS クレデンシヤル

フィールド	説明
Type	設定している HTTPS クレデンシヤルのタイプを指定します。有効なタイプは、[読み取り (Read)] または [書き込み (Write)] です。
Read	<p>最大 10 つの HTTPS 読み取りクレデンシヤルを設定できます。</p> <ul style="list-style-type: none"> • [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。 <p>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。</p> <ul style="list-style-type: none"> • 小文字の英字 (a ~ z) • 大文字の英字 (A ~ Z) • 数字 (0 ~ 9) • 特殊文字 (: # _ * ?) - <p>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。</p>

フィールド	説明
Write	<p>最大 10 つの HTTPS 書き込みクレデンシャルを設定できます。</p> <ul style="list-style-type: none"> • [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。 <p>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。</p> <ul style="list-style-type: none"> • 小文字の英字 (a ~ z) • 大文字の英字 (A ~ Z) • 数字 (0 ~ 9) • 特殊文字 (: # _ * ?) - <p>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。</p>

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

(注) Cisco Catalyst 9800 シリーズワイヤレス コントローラ デバイスを検出するには、NETCONF を有効にし、ポートを次のいずれかに設定する必要があります。

- 830 (デフォルトのポート番号)
- 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)

NETCONF は、ネットワークデバイスの設定をインストール、操作、削除するメカニズムです。[Advanced] エリアで [Telnet] を選択すると、NETCONF は無効になります。

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

- 今すぐ検出を実行するには、[Now] ラジオボタンをクリックし、[Start] をクリックします。
- 後で検出をスケジュールするには、[Later] ラジオボタンをクリックして更新の日時を定義し、[Start] をクリックします。

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

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

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

LLDP を使用したネットワークの検出

Link Layer Discovery Protocol (LLDP)、CDP、または IP アドレス範囲を使用してデバイスを検出できます。この手順では、LLDP を使用してデバイスとホストを検出する方法を示します。ディスカバリ メソッドの詳細については、[CDP を使用したネットワークの検出 \(7 ページ\)](#) および [IP アドレス範囲を使用したネットワークの検出 \(14 ページ\)](#) 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 [IP Address/Range] 領域を展開し、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、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。
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が必要な場合にのみ、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	<ul style="list-style-type: none"> [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。 <p>(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。</p>
Write	<ul style="list-style-type: none"> [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。 <p>(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。</p>

- 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。 <ul style="list-style-type: none"> • [noAuthNoPriv] : 認証または暗号化を提供しません。 • [AuthNoPriv] : 認証を提供しますが、暗号化は提供しません。 • [AuthPriv] : 認証と暗号化の両方を提供します。
Auth Type	使用する認証タイプ (認証モードとして [AuthPriv] または [AuthNoPriv] を選択した場合に有効になります)。次のいずれかの認証タイプを選択します。 <ul style="list-style-type: none"> • [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。 <p>(注)</p> <ul style="list-style-type: none"> • 一部のシスコ ワイヤレス コントローラでは、パスワード (あるいはパスフレーズ) は少なくとも 12 文字以上である必要があります。ワイヤレス コントローラのパスワードの最小要件を必ず確認してください。パスワードに必要な最低限の文字数が守られないと、デバイスでは Cisco DNA Center による検出、監視、管理が行われなくなります。 • パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。
Privacy Type	プライバシータイプ。(認証モードとして [AuthPriv] を選択すると有効になります)。次のいずれかのプライバシータイプを選択します。 <ul style="list-style-type: none"> • [AES128] : 暗号化の CBC モード AES。 • [None] : プライバシー設定はありません。

フィールド	説明
Privacy Password	<p>AES128 暗号化をサポートしているデバイスで交換されるメッセージを暗号化するための秘密鍵を生成するために使用される SNMPv3 プライバシーパスワード。パスワード（またはパスフレーズ）は、8 文字以上にする必要があります。</p> <p>(注)</p> <ul style="list-style-type: none"> 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、[読み取り (Read)] または [書き込み (Write)] です。

フィールド	説明
<p>Read</p>	<p>最大 10 つの HTTPS 読み取りクレデンシャルを設定できます。</p> <ul style="list-style-type: none"> • [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。 <p>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。</p> <ul style="list-style-type: none"> • 小文字の英字 (a ~ z) • 大文字の英字 (A ~ Z) • 数字 (0 ~ 9) • 特殊文字 (: # _ * ?) - <p>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。</p>

フィールド	説明
Write	<p>最大 10 つの HTTPS 書き込みクレデンシャルを設定できます。</p> <ul style="list-style-type: none"> • [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。 <p>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。</p> <ul style="list-style-type: none"> • 小文字の英字 (a ~ z) • 大文字の英字 (A ~ Z) • 数字 (0 ~ 9) • 特殊文字 (: # _ * ?) - <p>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。</p>

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。

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

- 今すぐ検出を実行するには、[Now] ラジオボタンをクリックし、[Start] をクリックします。
- 後で検出をスケジュールするには、[Later] ラジオボタンをクリックして更新の日時を定義し、[Start] をクリックします。

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

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

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

ディスカバリ ジョブの管理

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]。
[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 [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) [Discoveries] ペインで、関連するジョブを選択します。
 - b) [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) [Discoveries] ペインで、関連するジョブを選択します。
 - b) [Re-discover] をクリックして、選択したジョブを再起動します。

ディスカバリ ジョブの複製

ディスカバリジョブを複製し、その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]。
[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 [View All Discoveries] をクリックします。
- ステップ 3 [Discovery] ペインで、検出ジョブを選択します。
- ステップ 4 [Copy & Edit] をクリックします。

Cisco DNA Center では、「Copy of Discovery_Job」という名前でディスカバリジョブのコピーが作成されます。
- ステップ 5 (任意) 検出ジョブの名前を変更します。
- 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]**。
[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** [View All Discoveries] をクリックします。
- ステップ 3** [ディスカバリ (Discovery)] ペインで、削除する検出ジョブを選択します。
- ステップ 4** [削除 (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]**。
[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** [View All Discoveries] をクリックします。
- ステップ 3** [Discovery] ペインで、検出ジョブを選択します。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]** : 実行された各ディスカバリジョブがリストされ、開始時刻やデバイス検出の有無などが表示されます。

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

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

ネットワーク階層の設計

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

新しいネットワーク インフラストラクチャの設計

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

これらのタスクは、[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。

ネットワーク階層について

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

ネットワーク階層は、次の事前設定された階層をもちます。

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

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、サイトマップ上の 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することはできません。

実行できるタスクのリストを以下に示します。

- 新しいネットワーク階層を作成する。詳細については、「[ネットワーク階層のサイトの作成 \(30 ページ\)](#)」を参照してください。
- Cisco Prime Infrastructure から既存のネットワーク階層をアップロードする。詳細については、「[既存のサイト階層をアップロード \(33 ページ\)](#)」を参照してください。

マップ内で使用するイメージファイルに関するガイドライン

- マップのイメージファイルを .jpg、.gif、.png、.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。
- イメージ画像の寸法が、キャンパスマップに追加する予定のすべてのビルディングと屋外領域の合計寸法よりも大きいことを確認します。
- マップのイメージファイルのサイズはさまざまです。Cisco DNA Center は元のイメージを完全な定義でデータベースにインポートしますが、表示中は、ワークスペースに合わせてサイズが自動的に変更されます。
- インポートする前に、サイトの縦と横の寸法をフィートまたはメートル単位で取得してください。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。

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]**。

結果：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]** をクリックし、**[Add Area]** を選択します。

(注) 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の名前を入力します。

(注) **[Area Name]** フィールドには、次の制限があります。

- エリア名は 40 文字までです。
- 特殊文字 (& > < ? ' " / []) は使用できません。

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。

(注) デフォルトでは、[グローバル (Global)] が親ノードです。

ステップ 5 [Add] をクリックします。

結果：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。

(注) 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] ポップアップ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。

(注) [Building Name] フィールドには、次の制限があります。

- 建物名は 40 文字までです。
- 特殊文字 (& > < ? ' " / []) は使用できません。

b) [Parent] ドロップダウンリストから、親ノードを選択します。

(注) デフォルトでは、[グローバル (Global)] が親ノードです。

c) [Address] フィールドにアドレスを入力します。

(注) 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。

結果：左側ペインの親サイトに建物が作成され、表示されます。

ビルディングへのフロアの追加

ビルディングを追加したら、そのビルディングのフロアを作成する必要があります。

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。

ビルディングへのフロアの追加

ステップ 2 左側のペインで、そのフロアのビルディングの横にある省略記号 **...** にカーソルを合わせ、[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。

(注) [Floor Name] フィールドには、次の制限があります。

- フロア名は 40 文字までです。
- 特殊文字 (& > < ? ' " / []) は使用できません。

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、フロアの特性に基ついて RF を計算する方法を決定します。

ステップ 5 [Floor Image] エリアで、フロアプランファイルをドラッグアンドドロップしてフロアプランをアップロードします。

(注) Cisco DNA Center では、フロアプランのファイルタイプとして DXF、DWG、JPG、GIF、PNG、および PDF がサポートされています。

図 2: フロアプランの例



(注) フロアプランをインポートしたら、オーバーレイの可視化を有効にしてください (フロアで [View Options] をクリックし、[Overlay Objects] のオーバーレイトグルをオンにします)。デフォルトでは、マップをインポートした後にオーバーレイは表示されません。

ステップ 6 CAD ファイル (DXF または DWG ファイルタイプ) をアップロードする場合は、[Floormap] ポップアップを使用して、マップにフロア要素として表示する CAD レイヤーを選択します。

- a) [2D] 列で、2D ビューに表示する CAD レイヤーのチェックボックスをオンにします。
- b) [3D Wall/Shelving Type] 列で、CAD レイヤーのドロップダウンリストを使用して、壁または棚のタイプを指定します。

(注) レイヤーを 3D ビューに表示するには、[3D Wall/Shelving Type] 値が必要です。壁/棚のタイプは、減衰とヒートマップの計算方法に影響します。

- c) [Use Selected Layers] をクリックします。

ステップ 7 [Width]、[Length]、および [Height] フィールドにフロアマップの寸法を入力します。

ステップ 8 [Add] をクリックします。

ネットワーク階層の管理

既存のサイト階層をアップロード

既存のネットワーク階層を含んでいる CSV ファイルまたはマップアーカイブ ファイルをアップロードすることができます。たとえば、Cisco Prime Infrastructure からエクスポートしたロケーション情報を含む CSV ファイルをアップロードできます。Cisco Prime Infrastructure からのマップのエクスポートについては、[マップアーカイブのエクスポート \(34 ページ\)](#) を参照してください。



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

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

ステップ 2 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 CSV ファイルをドラッグしてドロップするか、または、CSV ファイルがある場所に移動し、[Import] をクリックします。

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

ステップ 4 Cisco Prime Infrastructure マップ tar.gz アーカイブファイルをインポートするには [Import] > [Map Import] を選択します。

ステップ 5 [Import Site Hierarchy Archive] ダイアログボックスのボックスエリアにマップアーカイブファイルをドラッグしてドロップします。

ステップ 6 [保存] を選択してファイルをアップロードします。

結果 : [Import Preview] ウィンドウが表示され、インポートされたファイルが示されます。

マップアーカイブのエクスポート

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

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

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

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

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

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

結果 : tar ファイルが作成され、ローカルマシンに保存されます。

ステップ 5 [Done] をクリックします。

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。

ツリー階層を検索するには、左ペインの [階層の検索 (Find Hierarchy)] で、検索するサイト、ビルディング、フロア名の名称の一部または正式名称をのどちらかを入力します。

結果：ツリー階層が、検索フィールドに入力したテキストに基づいてフィルタ処理されます。

サイトの編集

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

ステップ 2 左側のペインで、サイトの横にある省略記号 ... にカーソルを合わせて、[Edit Area] を選択します。

ステップ 3 [Edit Area] ポップアップで、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] ポップアップで、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

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。

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

フロアの編集

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

- ステップ 1** [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。

フロアマップの要素とオーバーレイの編集

フロア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 (Access Points)
- Sensor

次のオーバーレイ オブジェクトを追加、編集、および削除します。

- カバレッジ エリア
- Location Regions
- 壁
- 柵
- マーカー
- GPS マーカー

アクセス ポイントの配置に関するガイドライン

フロア マップに AP を配置する際は、次の注意事項を考慮してください。

- 部屋や建物の屋外の近くにデバイスが置かれるように、カバレッジ領域の境界に沿って 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せん。
- 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、および削除

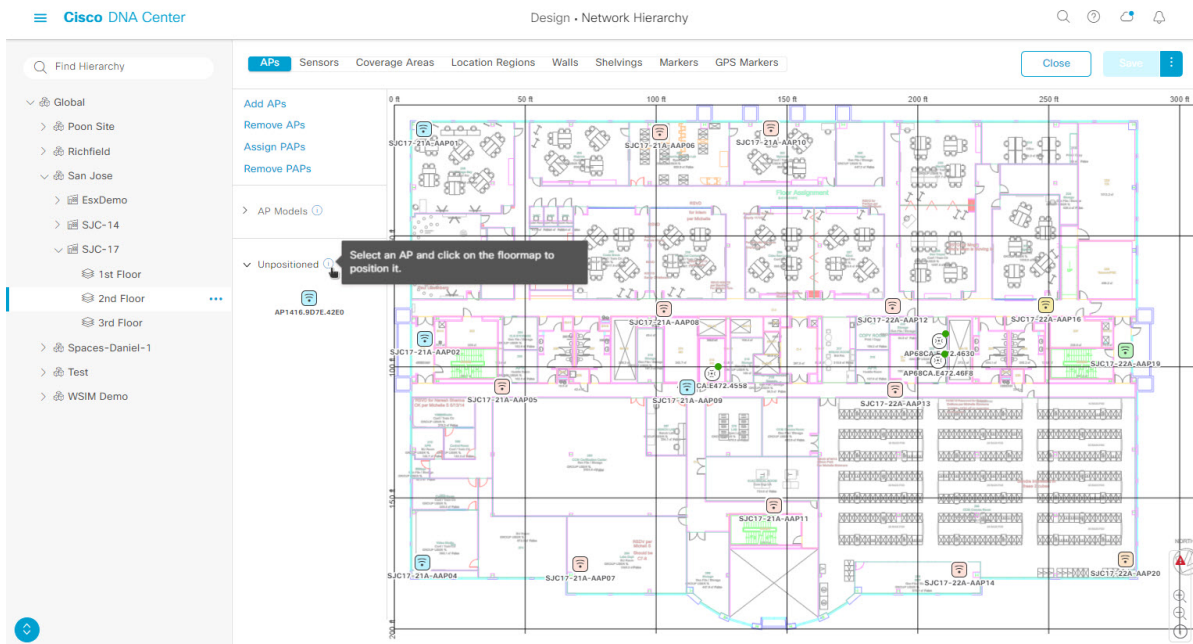
Cisco DNA Center Cisco DNA Center によって、カバレッジエリアの無線周波数 (RF) 信号の相対強度を表示する全体マップのヒートマップが計算されます。2D ワイヤレスマップの場合、このヒートマップは実際の RF 信号強度の近似値にすぎません。信号に影響を与える RF 信号の反射やその他の影響が考慮されていないためです。

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。「[ディスカバリについて](#)」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** 左側のペインでビルディングのフロアをクリックします。
- ステップ 3** マップツールバーから、**[Add/Edit]** をクリックします。
- ステップ 4** マップツールバーから **[AP]** トグルが有効になっていることを確認します。
- ステップ 5** マップの左側のペインで、**[Add APs]** をクリックします。
- ステップ 6** **[Add Aps]** スライドインペインから、アクセスポイントのチェックボックスをオンにして AP を一括で選択し、**[Add Selected]** をクリックします。または、アクセスポイントの横にある **[Add]** をクリックします。
- (注) 使用可能な検索オプションを使用して、アクセスポイントを検索できます。**[フィルタ (Filter)]** フィールドを使用し、AP 名、MAC アドレス、モデル、シスコワイヤレスコントローラのいずれかを使ってアクセスポイントを検索します。検索では大文字と小文字は区別されません。検索結果がテーブルに表示されます。**[追加 (Add)]** をクリックして、フロア領域に1つ以上の AP を追加します。
- 結果：新しく追加された AP 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せん。
- ステップ 7** フロア領域に AP を割り当てたら、**[AP の追加 (Add APs)]** ウィンドウを閉じます。
- ステップ 8** マップツールバーから、**[Add/Edit]** をクリックします。
- ステップ 9** マップの左側のペインから、**[Unpositioned]** カテゴリの AP をクリックして、AP を配置します。

図 3: 未配置の AP



ステップ 10 AP を配置するには、次のいずれかを実行します。

- AP を配置するフロアマップの場所をクリックします。
- [Edit AP] スライドインペインから、対応するフィールドに x 座標と y 座標を入力します。
- フロアマップに 3 つの点を描き、選択した点を使用して AP を配置できます。手順は次のとおりです。
 1. [Edit AP] スライドインペインで、[Position by 3 points] をクリックします。
 2. ポイントを定義するには、フロアマップの任意の場所をクリックして最初のポイントの描画を開始します。ポイントの描画を終了するには、再度をクリックします。最初の点までの距離を設定するためにダイアログボックスが表示されます。距離をメートル単位で入力し、[距離の設定 (Set Distance)] をクリックします。
 3. 2 番目と 3 番目の点を同様の方法で定義し、[保存 (Save)] をクリックします。
- フロアマップに 2 つの壁を定義し、定義した壁の間に AP を配置できます。これによって、2 つの壁の間の AP の位置を把握できるようになります。これは、壁の間の AP の位置を把握するのに役立ちます。
 1. [Edit AP] スライドインペインで、[Position by 2 walls] をクリックします。
 2. 最初の壁を定義するには、フロアマップの任意の場所をクリックして線の描画を開始します。線の描画を終了するには、再度をクリックします。最初の壁までの距離を設定するためにダイアログボックスが表示されます。距離をメートル単位で入力し、[Set Distance] をクリックします。
 3. 2 番目の壁を同様の方法で定義し、[保存 (Save)] をクリックします。

結果：壁の間で定義された距離に基づいて AP が自動的に配置されます。

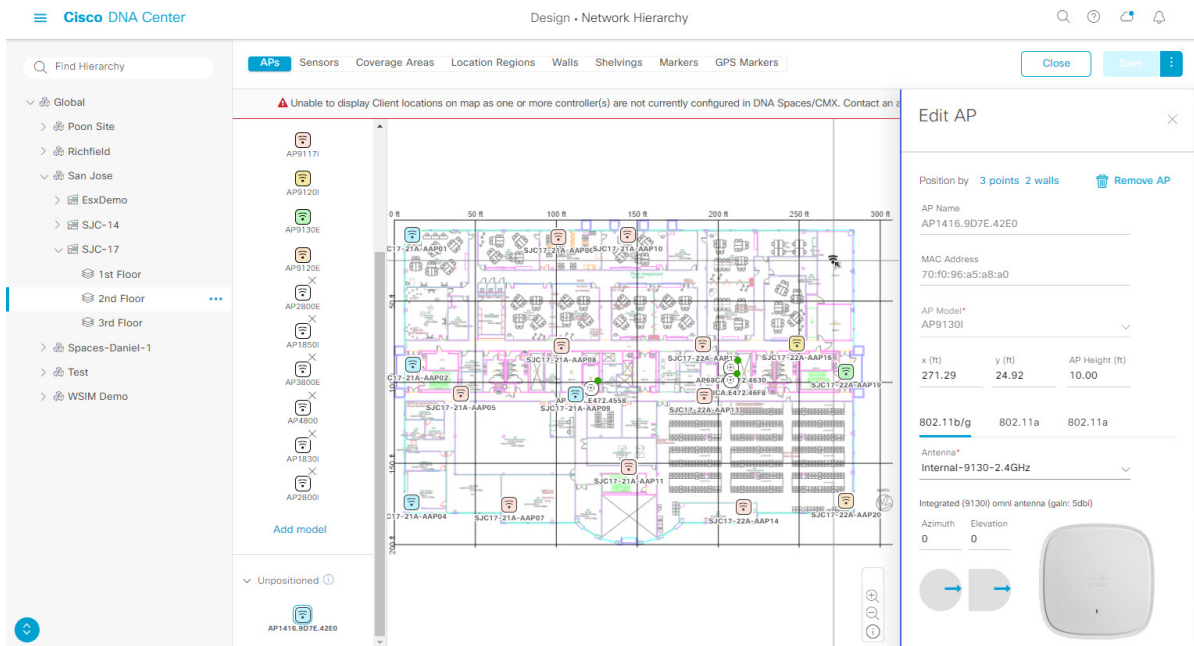
ステップ 11 [Edit AP] スライドインペインを使用して、次のような AP の詳細を設定します。

- [AP Name] : AP 名が表示されます。
- [MAC Address] : MAC アドレスが表示されます。
- [AP Model] : 選択したアクセスポイントの AP モデルを示します。
- [x] : AP の x 軸座標を示します。値は手動で入力できます。
- [y] : AP の y 軸座標を示します。値は手動で入力できます。
- [AP Height]] : アクセスポイントの高さを示します。値は手動で入力できます。
- [Antenna] : このアクセスポイントのアンテナタイプ。
 - (注) 外部の AP の場合は、アンテナを選択する必要があります。選択しないと、AP が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 ~ 360 です。Cisco DNA Center では、北は 0 または 360 度で、東は 90 度です。

値を手動で入力するか、フィールドの下の青色の矢印を使用して値を変更できます。

 - (注) 全方向アンテナのパターンでは方位角が存在しなくなるため、このオプションは表示されません。
- [Elevation] : 仰角を度数で表示します。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。

図 4: AP スライドインペインの編集



ステップ 12 アクセスポイントの配置と設定が完了したら、マップツールバーから [Save] をクリックします。

(注) Cisco Connected Mobile experience (CMX) が Cisco DNA Center と同期されている場合は、ヒートマップ上のクライアントの場所を表示できます。Cisco CMX 設定の作成を参照してください。

結果： AP の新しい位置に基づいてヒートマップが生成されます。

ステップ 13 フロアマップから AP を削除するには、編集モードの間に、マップの左側のペインから [Remove APs] をクリックします。

ステップ 14 [Delete APs] スライドインペインから、削除するアクセスポイントの横にあるチェックボックスをオンにし、[Delete Selected] をクリックします。

- すべてのアクセスポイントを削除するには、[Select All] をクリックし、[Delete Selected] をクリックします。
- フロアからアクセスポイントを削除するには、[削除 (Delete)] アイコンをクリックします。
- [Quick Filter] を使用し、AP 名、MAC アドレス、モデル、コントローラのいずれかで検索します。検索では大文字と小文字は区別されません。検索結果が表に表示されます。[削除 (Delete)] アイコンをクリックしてフロア領域から AP を削除します。

AP のクイック ビュー

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

- [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 のチャンネル番号。
 - [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 AP 名とともに表示されます。
- [Device 360] をクリックすると、特定のネットワーク要素（ルータ、スイッチ、AP、またはシスコワイヤレスコントローラ）の 360 度ビューが表示されます。[Cisco DNA Assurance ユーザガイド](#)の「デバイスの健全性のモニターとトラブルシューティング」トピックを参照してください。



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

センサーの追加、配置、および削除



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

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

-
- 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フロアをクリックします。
- ステップ 3** マップツールバーから、**[Add/Edit]** をクリックします。
- ステップ 4** マップツールバーから、**[Sensors]** トグルをクリックします。
- ステップ 5** **[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するか、またはセンサー行の横にある **[Add]** をクリックしてセンサーを追加します。
- (注) 検索オプションを使用して、特定のセンサーを検索できます。**[Filter]** フィールドを使用し、センサーの名前、MACアドレス、モデルのいずれかで検索します。検索では大文字と小文字は区別されません。検索結果がテーブルに表示されます。**[追加 (Add)]** をクリックして、フロア領域に 1 つ以上のセンサーを追加します。
- 結果：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 6** フロアマップへセンサーを割り当てたら、**[Add Sensors]** スライドインペインを閉じます。
- ステップ 7** マップツールバーから、**[Add/Edit]** をクリックします。
- ステップ 8** マップの左側のペインから、**[Unpositioned]** カテゴリのセンサーをクリックして、センサーを配置します。
- ステップ 9** センサーを配置するフロアマップの場所をクリックします。
- **[Sensor Details]** スライドインペインの **[x]**、**[y]**、および **[sensorHeight]** フィールドを使用して、センサーの正確な x、y、および z 座標を入力できます。
- ステップ 10** センサーの設定と調整が完了したら、**[保存 (Save)]** をクリックします。
- ステップ 11** フロアマップからセンサーを削除するには、編集モードの間に、マップの左側のペインから **[Remove APs]** をクリックします。
- ステップ 12** 削除するセンサーのチェックボックスをオンにし、**[Delete Selected]** をクリックします。
- すべてのセンサーを削除するには、**[すべて選択 (Select All)]** をクリックし、**[選択済みの削除 (Delete Selected)]** をクリックします。
 - フロアからセンサーを削除するには、そのセンサーの横にある **[削除 (Delete)]** アイコンをクリックします。
 - **[Quick Filter]** を使用して、名前、MAC アドレス、モデルのいずれかで検索します。検索では大文字と小文字は区別されません。検索結果がテーブルに表示されます。**[Delete]** アイコンをクリックして、フロア領域から 1 つ以上のセンサーを削除します。
-

カバレッジエリアの追加

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

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

-
- ステップ 1** 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フロアをクリックします。
- ステップ 3** マップツールバーから、**[Add/Edit]** をクリックします。
- ステップ 4** マップツールバーから、**[Coverage Areas]** トグルをクリックします。
- ステップ 5** マップの左側のペインから、**[Coverage Area]** アイコンをクリックします。
- ステップ 6** **[Coverage Area]** ポップアップウィンドウで、フィールドにカバレッジエリアの名前を入力し、**[Add Coverage]** をクリックします。
- ステップ 7** 描画ツールを使用して、カバレッジエリアの形状を作成します。
- マップをクリックしてポイントを作成し、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。
 - 任意のポイントを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。
 - 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 8** カバレッジエリアの作成が完了したら、マップツールバーの **[Save]** をクリックします。
- ステップ 9** 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。
- マップツールバーから、**[Add/Edit]** をクリックします。
 - マップツールバーから、**[Coverage Areas]** トグルをクリックします。
 - カバレッジエリアのポイントををクリックしてドラッグすると、形状を定義し直すことができます。
 - 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。
 - 編集が完了したら、マップツールバーの **[Save]** をクリックします。
- ステップ 10** 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。
- マップツールバーから、**[Add/Edit]** をクリックします。
 - マップツールバーから、**[Coverage Areas]** トグルをクリックします。
 - カバレッジエリアを右クリックし、**[Delete]** を選択します。
 - 削除が完了したら、マップツールバーの **[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作成

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

フロアマップ上に包含領域と除外領域を配置するためのガイドライン

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

フロア上の包含リージョンの定義

フロア上の包含リージョンの定義

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フロアをクリックします。

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

ステップ 4 マップツールバーから、**[Location Regions]** トグルをクリックします。

ステップ 5 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 6 描画ツールを使用して包含領域を作成します。

- マップをクリックしてポイントを作成し、包含領域の形状ができるまでポイントの作成を続けます。
- 形状を完成させるには、左側のペインで **[Inclusion]** アイコンをクリックして、描画モードを終了します。または、マップをダブルクリックして形状を確定することもできます。形状をキャンセルする場合は、マップ上で右クリックします。
- 既存の包含領域を移動するには、形状を新しい場所にドラッグアンドドロップします。
- 既存の包含領域を削除するには、形状を右クリックして **[Delete]** を選択します。

ステップ 7 包含領域の作成が完了したら、マップツールバーの **[Save]** をクリックします。

フロア上の除外リージョンの定義

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

ステップ 1 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フロアをクリックします。

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

ステップ 4 マップツールバーから、**[Location Regions]** トグルをクリックします。

ステップ 5 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 6 描画ツールを使用して除外領域を作成します。

- マップをクリックしてポイントを作成し、除外領域の形状ができるまでポイントの作成を続けます。
- 形状を完成させるには、左側のペインで **[Exclusion]** アイコンをクリックして、描画モードを終了します。または、マップをダブルクリックして形状を確定することもできます。形状をキャンセルする場合は、マップ上で右クリックします。
- 既存の除外領域を移動するには、形状を新しい場所にドラッグアンドドロップします。
- 既存の除外領域を削除するには、形状を右クリックして **[Delete]** を選択します。

ステップ 7 除外領域の作成が完了したら、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。

■ マーカーの配置

使用可能なル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ルール ラインがマップ上で強調表示されます。

ステップ 12 削除するル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。

■ マーカーの配置

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フロアをクリックします。

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

ステップ 4 マップツールバーから、[Markers] トグルをクリックします。

ステップ 5 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 描画ツールを使用してマーカーを配置します。

- マーカーを配置するにはマップをクリックします。
- マーカーを移動するには、
- 既存の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。
- 既存の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 7 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 のチャンネル番号または [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 [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] : チャン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、およびチャンネル使用率を含む)。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ンネル使用率。
 - [Assoc.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。

- **Issue Count**
- [Coverage Issues]
- [AP Down Issues]
- [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]
 - [APRSSI] : 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6時間です。ただし、この間隔は、ネットワーク環境の必要性に応じて、最高 24 時間まで変更できます。詳細については、[デバイスポーリング間隔の更新（52 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 [Update Polling Interval] をクリックします

ステップ 4 [Update Resync Interval] ダイアログボックスの [Status] フィールドで、[Enabled] をクリックしてポーリングを有効にするか、[Disabled] をクリックしてポーリングを無効にします。


ステップ 5 [Polling Time] フィールドには、継続的なポーリングサイクルの間隔（分単位）を入力します。有効な値は、25 ～ 1,440 分（24 時間）です。

(注) デバイス固有のポーリング時間は、グローバルなポーリング時間より優先されます。デバイス固有のポーリング時間を設定した後でグローバルなポーリング時間を変更した場合、Cisco DNA Center は引き続きデバイス固有のポーリング時間を使用します。

ステップ 6 [更新 (Update)] をクリックします。

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。

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 200 のエントリを表示できます。

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

始める前に

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


メニューアイコン () をクリックして、[Provision] > [Network Devices] > [Inventory] の順に選択します。[Inventory] ウィンドウには、検出プロセス中に収集されたデバイス情報が表示されます。次の表に、使用できる情報を記載します。

表 16: インベントリ

カラム	説明
Device Name	

カラム	説明
	<p>デバイスの名前。</p> <p>デバイス名をクリックすると、デバイスの次の詳細が表示されます。</p> <p>[Details] : デバイス名、到達可能性ステータス、管理性ステータス、IP アドレス、デバイスモデル、ロール、稼働時間、サイトなどの詳細が表示されます。</p> <ul style="list-style-type: none"> • [View Assurance 360] : [Assurance 360] ウィンドウが表示されます。360 を開くには、アシュアランスアプリケーションをインストールする必要があります。 <p>• Interfaces</p> <ul style="list-style-type: none"> • [Ethernet Ports] (すべてのデバイスが対象) : イーサネットポートの動作ステータスと管理ステータスが表示されます。 <p>Cisco Catalyst 4000 シリーズ、6000 シリーズ、および 9000 シリーズ スイッチとアグリゲーションサービスマルター (ASR) 1000 シリーズルターの場合、ポートビューにはラインカードとスーパーバイザカードの詳細が表示されます (使用可能な場合)。</p> <p>ラインカードには、プラットフォーム、アドレス、シリアル番号、ロール、およびスタックメンバー番号の詳細が含まれます。スーパーバイザカードには、部品番号、シリアル番号、スイッチ番号、およびスロット番号の詳細が含まれます。</p> <p>[Ports] テーブルには、動作ステータス、管理ステータス、タイプ、MAC アドレス、PoE ステータス、速度、MTU および説明が表示されます。このテーブルには、次のタイプの VLAN の ID も表示されます。</p> <ul style="list-style-type: none"> • 製造時提供のデフォルト VLAN の VLAN ID • 設定されたデフォルト VLAN の VLAN ID • 設定された VLAN の VLAN ID <p>Cisco Catalyst 2000、3000、および 9000 シリーズ スイッチの場合は、ポートビューでポートをクリックするか、[Ports] テーブルのポート名をクリックして、ポートの最大割り当て電力、および消費電力の詳細を表示します。</p> <ul style="list-style-type: none"> • [Color Code] ドロップダウンリストには、次のビューが用意されています。 <ul style="list-style-type: none"> • [Status] : イーサネットポートのデフォルトビューを表示します。 • [VLANs] : 特定のポートに割り当てられている VLAN を表示します。[VLANs] ビューでは、最大 5 つの VLAN を選択し、ポートに関連付けられている VLAN のみを一覧表示できます。 <p>[VLANs] ビューには、VLAN ポートマッピングの [Selected]、[Not Configured]、[Default]、および [VLAN] カラーコードが表示されま</p>

カラム	説明
	<p>す。</p> <ul style="list-style-type: none"> • [Port Channels] : デバイスで設定されている上位 5 つのポートチャネルを表示します。 <p>ポートチャネルビューには、デバイスで設定されているポートチャネルの [Selected] および [Port-channel] カラーコードが表示されます。</p> <ul style="list-style-type: none"> • [Port Actions] : <ul style="list-style-type: none"> • [Clear Mac Address] : ポートの MAC アドレスをクリアできます。ポートビューでポートをクリックします。次に、[Port Actions] ドロップダウンリストから [Clear Mac Address] を選択します。 • [Port Shut] : ポートをシャットダウンできます。ポートビューでポートをクリックします。次に、[Port Actions] ドロップダウンリストから [Port Shut] を選択します。警告メッセージには [OK] をクリックします。ポートの管理ステータスが [Down] になります。 <p>ポートの管理ステータスを [Up] にするには、[Port Actions] ドロップダウンリストから [Port No Shut] を選択します。警告メッセージには [OK] をクリックします。</p> <p>error-disabled ポートは黄色で表示されます。ポートビューで error-disabled ポートをクリックして、エラーの理由を表示します。error-disabled ポートをアクティブにするには、MAC アドレスをクリアして、ポートをシャットダウンします。</p> <ul style="list-style-type: none"> • [Port Description] : [PORT DESCRIPTION] の横にある [Edit] アイコンをクリックし、説明を入力して [Save] をクリックし、[Okay] をクリックしてポートに説明を追加します。説明を削除するには、[Delete] アイコンをクリックします。

カラム	説明
	<ul style="list-style-type: none"> • [Update VLAN] : [VLAN] の横にある編集アイコンをクリックし、[Edit VLAN] ドロップダウンリストから VLAN を選択し、[Save] をクリックして VLAN を更新します。2 つの VLAN が事前設定されているポートの VLAN を更新することはできません。 • VLAN の更新、ポートの説明の追加、MAC アドレスのクリア、およびポートのシャットダウンを行うには、デバイスソフトウェアタイプが IOS/IOS-XE である必要があります。 • ワイヤレスコントローラ (WLC) デバイスでは、VLAN の更新、MAC アドレスのクリア、およびポートのシャットはサポートされていません。 • VLAN の更新、MAC アドレスのクリア、およびポートのシャットは、アクセスポートでのみサポートされます。 • ポートをシャットダウンすると、ポートのトラフィックが中断されます。 • [VLANs] (スイッチとハブのみが対象) : VLAN のテーブルに、動作ステータス、管理ステータス、VLAN タイプ、および IP アドレスが表示されます。このテーブルには、次のタイプの VLAN の ID も表示されます。 <ul style="list-style-type: none"> • 製造時提供のデフォルト VLAN の VLAN ID • 設定されたデフォルト VLAN の VLAN ID • 設定された VLAN の VLAN ID • [Search] や [Filter] のオプションをクリックして、目的の VLAN の詳細を表示できます。 • [Virtual Ports] (ワイヤレスデバイス、コントローラ、ルータのみが対象) : ポートのテーブルに、動作ステータス、管理ステータス、タイプ、MAC アドレス、PoE ステータス、速度、および MTU が表示されます。[Search] や [Filter] のオプションをクリックして、目的のポートの詳細を表示できます。 • [Hardware and Software] : デバイスのハードウェアとソフトウェアの詳細が表示されます。 • [Configuration] : show running-config コマンドの出力で表示される内容に似た詳細な設定情報が表示されます。 <p>この機能は、アクセスポイント (AP) とワイヤレスコントローラにはサポートされていません。したがって、これらのデバイスタイプの場合は設定データは返されません。</p>

カラム	説明
	<ul style="list-style-type: none"> • [Power] : デバイスに割り当てられている電力、消費電力、および残りの電力に関する詳細が表示されます。 [Power Supplies] テーブルに、動作ステータス、シリアル番号、およびベンダー機器タイプの詳細が表示されます。 • [Fans] : ファンの動作ステータス、シリアル番号、およびベンダー機器タイプが表示されます。 • [SFP Modules] : プラットフォーム、シリアル番号、製造元、および Small Form-Factor Pluggable (SFP) モジュールの接続先ポートの詳細を表示します。 [Search] や [Filter] のオプションをクリックして、目的のポートの詳細を表示できます。 • [User Defined Fields] : デバイスに関連付けられているユーザー定義フィールドが表示されます。 • [Config Drift] : 構成の変更を表示し、同じデバイスの任意の2つのバージョンを選択して、各バージョンの実行中の構成データを比較できます。 (注) 実行中の構成データは、ワイヤレスコントローラやレガシーコントローラなどのデバイスではサポートされません。 • [Wireless Info] : プライマリとセカンダリの管理対象ロケーションが表示されます。 • [Mobility] : モビリティグループ名、RFグループ名、仮想IP、およびモビリティ MAC アドレスが表示されます。 <p>(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。</p>
IP Address	デバイスの IP アドレス。

コラム	説明
<p>Support Type</p>	<p>以下に示すデバイスのサポートレベルが表示されます。</p> <ul style="list-style-type: none"> • [Supported] : Cisco DNA Center のすべてのアプリケーションに対してデバイスパックがテスト済みです。これらのデバイスのいずれかの Cisco DNA Center 機能が動作しない場合は、サービスリクエストを開くことができます。 • [Unsupported] : Cisco DNA Center でテストおよび認定されていない他のすべてのシスコデバイスとサードパーティ製デバイス。これらのデバイスについて、Cisco DNA Center でさまざまな機能をベストエフォートとして試すことができます。ただし、Cisco DNA Center の機能が期待どおりに動作しない場合、サービスリクエストまたはバグを発生させることは求められていません。 • [Third Party] : デバイスパックは、お客様またはビジネスパートナーによって構築され、認定プロセスを経ています。サードパーティ製デバイスは、ディスカバリ、インベントリ、トポロジなどの基本自動化機能をサポートします。Cisco TAC は、これらのデバイスの初期レベルのサポートを提供します。ただし、デバイスパックに問題がある場合は、ビジネスパートナーに連絡する必要があります。
<p>Reachability</p>	<p>以下は、さまざまなステータスのリストです。</p> <ul style="list-style-type: none"> • [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。
<p>Manageability</p>	<p>デバイスのステータスが次のように示されます。</p> <ul style="list-style-type: none"> • [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。
<p>MAC Address</p>	<p>デバイスの MAC アドレス。</p>

カラム	説明
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、稼働している時間。
Device Role	<p>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。</p> <p>(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。</p> <p>必要に応じて、このカラムのドロップダウンリストを使用して、割り当てられたデバイス ロールを変更することができます。次のデバイス ロールを使用できます。</p> <ul style="list-style-type: none"> • Unknown • Access • Core • Distribution • Border Router
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、 ネットワーク階層について (29 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 (たとえば、Cisco Catalyst 4500 シリーズスイッチ)。
Resync Interval	デバイスのポーリング間隔。この間隔は、[Settings] でグローバルに設定するか、またはインベントリ内の特定のデバイスに対して設定できます。詳細については、 Cisco DNA Center 管理者ガイド を参照してください。

カラム	説明
Last Sync Status	<p>デバイス最終検出のスキャン状態。</p> <ul style="list-style-type: none"> • [Managed] : デバイスは完全に管理された状態です。 • [Partial Collection Failure] : デバイスは部分的に収集された状態で、すべてのインベントリ情報は収集されていません。障害の追加情報を表示するには、[Information] (i) アイコンにマウスを合わせます。 • [Unreachable] : デバイスの接続問題のため、デバイスに到達できず、インベントリ情報は収集されませんでした。この状態は、定期的な収集が行われたときに発生します。 • [Wrong Credentials] : デバイスをインベントリに追加した後にデバイスのログイン情報が変更された場合、この状態が表示されます。 • [In Progress] : インベントリ収集が実行されています。

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 Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックし、[Provision] > [Network Devices] > [Inventory] の順に選択します。
[Inventory] ウィンドウには、ディスクバリプロセス中に収集されたデバイス情報が表示されます。
- ステップ 2 サイトに割り当てるデバイスのチェックボックスをオンにします。
- ステップ 3 [Actions] メニューから、[Provision] > [Assign Device to Site] を選択します。
[Assign Device to Site] スライドインペインが表示されます。
- ステップ 4 [Assign Device To Site] スライドインペインで、デバイスの  アイコンの横にあるリンクをクリックします。
[Choose a floor] スライドインペインが表示されます。
- ステップ 5 [Choose a floor] スライドインペインで、デバイスに割り当てるフロアを選択します。
- ステップ 6 [Save] をクリックします。
- ステップ 7 (任意) 複数のデバイスを選択して同じ場所に追加した場合は、最初のデバイスで [Apply to All] チェックボックスをオンにすると、残りのデバイスに同じ場所を割り当てることができます。
- ステップ 8 [Assign] をクリックします。
- ステップ 9 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 サーバで Cisco DNA Center を登録します。これには、AAA サーバと Cisco DNA Center の共有秘密を定義することが含まれます。
 - AAA サーバで Cisco DNA Center の属性名を定義します。
 - Cisco DNA Center マルチホストクラスタの設定の場合は、AAA サーバのマルチホストクラスタに、すべての個別のホスト IP アドレスと仮想 IP アドレスを定義します。
- Cisco ISE を設定する前に、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。サポート対象の Cisco ISE バージョンの詳細については、「[Cisco DNA Center のサポート対象デバイス](#)」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ができますが、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 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、次のように [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 \(30 ページ\)](#)』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** [NMP Traps] 領域が表示されていない場合は展開し、次のいずれかを実行します。
- [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] 領域が表示されていない場合は展開し、次のいずれかを実行します。
- [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] 領域が表示されていない場合は展開し、次のいずれかを実行します。
- [Use Cisco DNA Center as NetFlow collector server] チェックボックスをオンにします。
デバイスインターフェースの 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 an external NetFlow collector server] チェックボックスをオンにし、NetFlow コレクタサーバーの IP アドレスとポート番号を入力します。
選択したサーバーがネットワークデバイスからの NetFlow エクスポートの宛先サーバーになります。NetFlow コレクタが選択されていない場合、アプリケーションテレメトリは有効になりません。
- ステップ 5** [Wired Client Data Collection] 領域を展開し、[Monitor wired clients] チェックボックスをオンにします。
この選択により、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) がオンになります。
デフォルトでは、サイトの IPDT は無効になっています。

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] 領域を展開し、[Enable Wireless Telemetry] チェックボックスをオンにします。

オンにすると、ネットワークのワイヤレスコントローラ、アクセスポイント、およびワイヤレスクライアントの正常性をモニターできます。

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

始める前に

- Cisco DNA Center 用の Cisco DNA Advantage ソフトウェアライセンスを保有していることを確認してください。**AI ネットワーク分析** アプリケーションは、Cisco DNA Advantage ソフトウェアライセンスに含まれています。
- **AI ネットワーク分析** アプリケーションがダウンロードおよびインストールされていることを確認します。[Cisco Digital Network Architecture Center 管理者ガイド](#)の「パッケージと更新のダウンロードとインストール」のトピックを参照してください。
- ネットワークまたは HTTP プロキシが、次のクラウドホストへのアウトバウンド HTTPS (TCP 443) アクセスを許可するように設定されていることを確認します。
 - [api.use1.prd.kairos.ciscolabs.com] (米国東部地域)
 - [api.euc1.prd.kairos.ciscolabs.com] (EU 中央地域)

ステップ 1 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] ウィンドウが表示されます。

AI Network Analytics

Using AI and Machine Learning, AI Network Analytics drives intelligence in the network, empowering administrators to accurately and effectively improve performance and issue resolution. AI Network Analytics eliminates noise and false positives significantly by learning, modeling and adapting to your specific network environment.

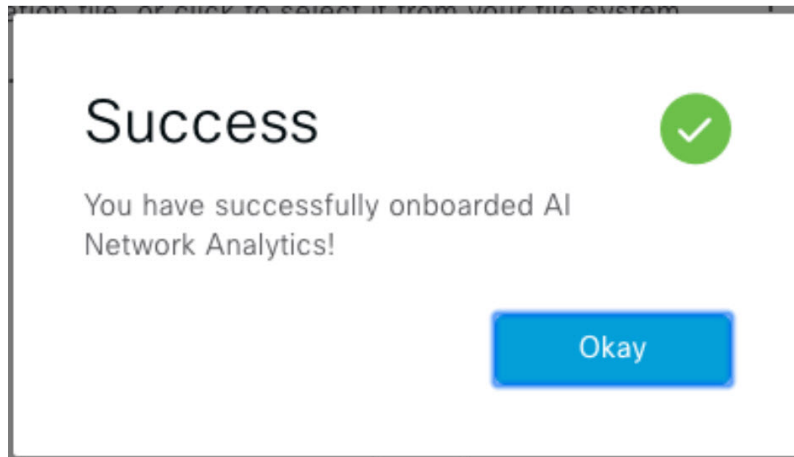
[Configure](#)

[Recover from a config file](#) ⓘ

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ます、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。

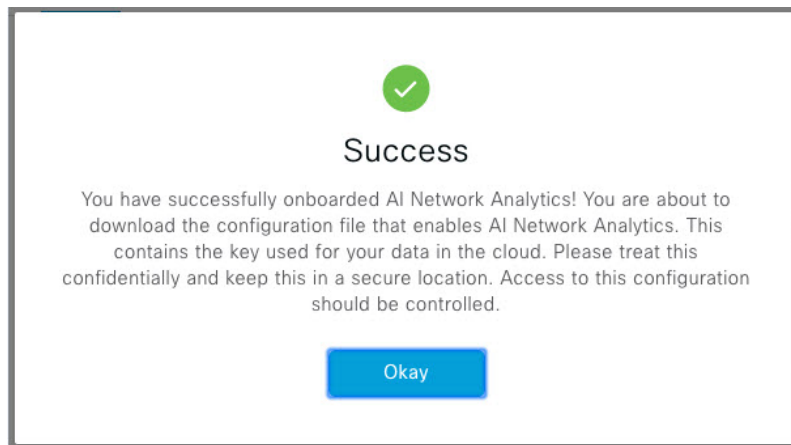
[Testing cloud connectivity...] タブで示されているように、システムはクラウド接続のテストを開始します。クラウド接続のテストが完了すると、[Testing cloud connectivity...] タブが [Cloud connection verified] に変わります。

3. [次へ (Next)] をクリックします。

[terms and conditions] ウィンドウが表示されます。

4. [Accept Cisco Universal Cloud Agreement] チェックボックスをオンにして契約条件に同意してから、[Enable] をクリックします。

Cisco AI Network Analytics が有効になるまでに数分かかる場合があります。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、[Cloud Connection] エリアに 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 データ収集を無効にするには、Cisco AI Network Analytics クラウドサービスへの接続をオフ（無効）にする必要があります。これにより、AI 駆動型の問題、ネットワークヒートマップ、サイトの比較、ピアの比較など、Cisco AI Network Analytics 関連のすべての機能が無効になります。

ステップ 1 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] ウィンドウが表示されます。

ステップ 3 [Cloud Connection] エリアで、 が表示されるように、ボタンをクリックしてオフにします。

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い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。
- 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。


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 5: ローカライズされたログイン画面の例



ロールベース アクセス コントロールのサポート アシュアランス

アシュアランスは、ロールベース アクセス コントロール (RBAC) をサポートしています。これにより、スーパー管理者ロールの権限を持つユーザーは、特定の アシュアランス 機能へのユーザーアクセスを許可または制限するカスタムロールを定義できます。

詳細については、『[Cisco DNA Center 管理者ガイド](#)』の「Manage Users」の章を参照してください。

カスタムロールを定義し、定義したロールにユーザーを割り当てるには、次の手順を実行します。

始める前に

SUPER-ADMIN-ROLE 権限を持つユーザのみがこの手順を実行することができます。

ステップ 1 カスタムロールを定義します。

- メニューアイコン (☰) をクリックして、[System] > [Users and Roles] > [Role Based Access Control] の順に選択します。

- b) [+ Create New Role] をクリックします。
[Create a Role] ウィンドウが表示されます。新しいロールを作成すると、新しいロールにユーザーを割り当てるように求められます。
- c) [Let's Do it] をクリックします。
今後この画面をスキップするには、[Don't show this to me again] チェックボックスをオンにします。
[Create a New Role] ウィンドウが表示されます。
- d) ロール名を入力し、[Next] をクリックします。
[Define the Access] ウィンドウにオプションのリストが表示されます。
- e) リストを展開するには、**アシユアランス** の横にある [>] をクリックします。
次のオプションが表示されます。このオプションを使用して、新しいロールに対して [Deny]、[Read] (デフォルト)、[Write] 権限を設定できます。
- [Monitor and Troubleshooting] : [Health]、[Issues]、[Sensors] ダッシュボードを使用してネットワークをモニターできます。また、360度ビューや問題の詳細からトレンドを分析し、洞察を得ることができます。
 - 権限レベルを [Deny] に設定すると、このロールを割り当てられたユーザーは、アシユアランスのどの機能も表示できません。
 - [Monitoring Settings] : データの保持と正常性の設定を管理できます。
データ保持の設定を管理するには、システム権限が必要です。
 - [Troubleshooting Tools] : センサーテストを作成およびスケジュールし、インテリジェントキャプチャの設定を管理できます。
- f) [Next] をクリックします。
[Summary] ウィンドウが表示されます。
- g) サマリーを確認します。情報が正しい場合は、[Create Role] をクリックします。誤りがある場合は、[Edit] をクリックして適切な変更を行います。
[Done, Role-Name] ウィンドウが表示されます。

ステップ 2 作成したカスタムロールにユーザーを割り当てるには、[Add Users] をクリックします。

[User Management] > [Internal Users] ウィンドウが表示されます。このウィンドウでは、カスタムロールを既存のユーザーまたは新規ユーザーに割り当てることができます。

- 既存のユーザーにカスタムロールを割り当てるには、次の手順を実行します。
 1. [Internal Users] ウィンドウで、カスタムロールを割り当てるユーザーの横にあるオプションボタンをクリックし、次に [Edit] をクリックします。
[Update Internal User] スライドインペインが表示されます。
 2. [Role List] ドロップダウンリストから、カスタムロールを選択し、[Save] をクリックします。
- カスタムロールを新規ユーザーに割り当てるには、次の手順を実行します。
 1. [+ Add] をクリックします。

[Create Internal User] スライドインペインが表示されます。

2. 表示されるフィールドに氏名とユーザー名を入力します。
3. [Role List] ドロップダウンリストから、新規ユーザーに割り当てるカスタムロールを選択します。
4. 新しいパスワードを入力し、確認のために再度入力します。
5. [Save] をクリックします。

ステップ 3 既存のユーザーがログイン中に、管理者がそのユーザーのアクセス権限を変更した場合、新しい権限設定を有効にするには、ユーザーが Cisco DNA Center からログアウトして、ログインし直す必要があります。

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。