



## ネットワークの検出

- [検出の概要 \(1 ページ\)](#)
- [検出ダッシュボード \(2 ページ\)](#)
- [ディスカバリの前提条件 \(2 ページ\)](#)
- [ディスカバリ クレデンシヤル \(3 ページ\)](#)
- [優先管理 IP アドレス \(6 ページ\)](#)
- [設定のガイドラインと制限事項のディスカバリ \(6 ページ\)](#)
- [ディスカバリの実行 \(7 ページ\)](#)
- [ディスカバリ ジョブの管理 \(30 ページ\)](#)
- [すべてのディスカバリの表示 \(36 ページ\)](#)

### 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 アシユアランスについては、デバイスのループバックアドレスを指定することをお勧めします。

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



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

## 検出ダッシュボード

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

## ディスカバリの前提条件

ディスカバリを実行する前に、次の最小要件を満たしてください。

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

- Cisco DNA Center が使用できるように 1 つ以上の SNMP クレデンシャルがデバイス上で設定されていることを確認してください。少なくとも、これには SNMPv2C 読み取りクレデンシャルを使用できます。詳細については、[ディスカバリ クレデンシャル \(3 ページ\)](#) を参照してください。
- Cisco DNA Center に検出させ、管理委させるデバイスの SSH クレデンシャルを設定します。以下の基準のうち、少なくとも 1 つが満たされる場合、Cisco DNA Center はデバイスを検出し、そのインベントリに追加します。
  - デバイスへの SSH アクセスのために Cisco DNA Center が使用するアカウントが、特権 EXEC モード (レベル 15) である。
  - ディスカバリ ジョブで設定される CLI クレデンシャルの一部としてデバイスのイン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。

## ディスカバリ クレデンシャル

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

- ネットワークデバイス : CLI と SNMP のクレデンシャル。



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

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

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

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

## クレデンシャルと Cisco ISE のディスカバリ

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

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

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

## ディスカバリ クレデンシャルのガイドラインと制約事項

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

- ディスカバリ ジョブで使用されるデバイス クレデンシャルを変更するには、ディスカバリ ジョブを編集し、使用しなくなったクレデンシャルの選択を解除する必要があります。その後、新しいクレデンシャルを追加してディスカバリを開始する必要があります。詳細については、「[ディスカバリ ジョブでクレデンシャルを変更 \(31 ページ\)](#)」を参照してください。
- デバイスが正常に検出された後にデバイスのクレデンシャルを変更すると、そのデバイスのその後のポーリングサイクルは失敗します。この状況を修正するには、次のいずれかのオプションを使用します。
  - ディスカバリ ツールを使用します：
    - デバイスの新しいクレデンシャルと一致する、ジョブ固有のクレデンシャルを使用して、新しいディスカバリ ジョブを実行します。
    - 既存のディスカバリ ジョブを編集し、ディスカバリを再実行します。
  - 設計ツールを使用します：
    - 新しいグローバル クレデンシャルを作成し、適切なグローバル クレデンシャルを使用して新しいディスカバリ ジョブを実行します。

- 既存のグローバルログイン情報を編集し、[Copy & Edit] を使用してディスカバリ ジョブを再作成します。または、新しいディスカバリ ジョブを作成します。
- デバイス認証に失敗するために進行中のディスカバリ ポーリング サイクルが失敗する場合は、次のいずれかのオプションを使用して状況を修正できます。
  - ディスカバリ ツールを使用します：
    - 現在のディスカバリ ジョブを停止または削除し、デバイスのクレデンシャルと一致する、ジョブ固有のクレデンシャルを使用して、新しいディスカバリ ジョブを実行します。
    - 現在のディスカバリ ジョブを停止または削除し、既存のディスカバリ ジョブを編集して、ディスカバリ を再実行します。
  - 設計ツールを使用します：
    - 新しいグローバル クレデンシャルを作成し、適切なグローバル クレデンシャルを使用して新しいディスカバリ ジョブを実行します。
    - 既存のグローバルログイン情報を編集し、[Copy & Edit] を使用してディスカバリ ジョブを再作成します。または、新しいディスカバリ ジョブを作成します。
- グローバル クレデンシャルを削除しても、以前に検出されたデバイスは影響を受けません。以前に検出されたデバイスのステータスは、認証の失敗を示しません。ただし、削除されたクレデンシャルの使用を試みる次のディスカバリ は失敗します。ディスカバリ は、いずれかのデバイスへの接続を試みる前に失敗します。

## ディスカバリ クレデンシャルの例

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

FIPS モードの展開の場合、ディスカバリパスワードの最小文字数は8です。

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

- 
- ステップ1** クレデンシャル0としてCLIグローバルクレデンシャルを設定します。
  - ステップ2** SNMP (v2c または v3) グローバルクレデンシャルを設定します。
  - ステップ3** 190 台のデバイスの IP アドレス (グローバルクレデンシャルを共有する 190 台のデバイス) の1つとグローバルクレデンシャル0を使用してディスカバリ ジョブを実行します。

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

ステップ5 [Inventory] ウィンドウで結果を確認します。

## 優先管理 IP アドレス

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

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

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

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

## 設定のガイドラインと制限事項のディスカバリ

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

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

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

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

## ディスカバリの実行

ここでは、ディスカバリの実行方法について説明します。

### CDP を使用したネットワークの検出

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



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

#### 始める前に

- ネットワークデバイスで CDP を有効にします。
- [ディスカバリの前提条件 \(2 ページ\)](#) で説明されているように、ネットワークデバイスを設定します。
- クライアント IP アドレスとしてネットワークデバイスのホスト IP アドレスを設定します。(A host is an end-user device, such as a laptop computer or mobile device.)

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

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

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



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

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

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

- [CDP Level] : スキャンするシードデバイスからのホップ数を入力します。  
有効値は 1 ~ 16 です。デフォルト値は 16 です。たとえば、CDP レベル 3 は、CDP がシードデバイスから最大 3 つのホップまでスキャンすることを意味します。
- [Preferred Management IP Address] : 次のいずれかのオプションボタンをクリックします。
  - [None] : デバイスが任意の IP アドレスを使用できるようにします。
  - [Use Loopback IP] : デバイスのループバック インターフェイスの IP アドレスを指定します。
    - (注) [Use Loopback IP] の使用を選択し、デバイスにループバック インターフェイスがない場合、Cisco DNA Center は優先管理 IP アドレス (6 ページ) で説明されているロジックを使用して、管理 IP アドレスを選択します。
    - (注) ループバック インターフェイスの IP アドレスを優先管理 IP アドレスとして使用するには、CDP ネイバーの IP アドレスが Cisco DNA Center から到達可能であることを確認します。

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

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

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

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

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

**ステップ 8** CLI クレデンシャルの場合は、次の手順を実行します。

- a) 次のフィールドを設定します。



表 1: CLI クレデンシャル

| フィールド                   | 説明   |
|-------------------------|--|
| <b>Name/Description</b> | CLI クレデンシャルを説明する名前または語句。   |
| <b>Username</b>         | 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。  |
| <b>Password</b>         | 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。<br>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。<br><br>(注) パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。                     |
| <b>Enable Password</b>  | 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。<br>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。<br><br>(注) パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。 |

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

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

- a) 次のフィールドを設定します。

表 2: SNMPv2c のクレデンシャル

| フィールド        | 説明  |
|--------------|---|
| <b>Read</b>  | <ul style="list-style-type: none"> <li>• [Name/Description] : 追加している SNMPv2c 設定の名前または説明。</li> <li>• [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。</li> </ul> <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> |
| <b>Write</b> | <ul style="list-style-type: none"> <li>• [Name/Description] : 追加している SNMPv2c 設定の名前または説明。</li> <li>• [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。</li> </ul> <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>         |

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

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

- a) 次のフィールドを設定します。

表 3: SNMPv3 のクレデンシャル

| フィールド                   | 説明   |
|-------------------------|--|
| <b>Name/Description</b> | 追加した SNMPv3 設定の名前または説明。  |
| <b>Username</b>         | SNMPv3 設定に関連付けられている名前。   |
| <b>Mode</b>             | 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"> <li>• [noAuthNoPriv] : 認証または暗号化を提供しません。</li> <li>• [AuthNoPriv] : 認証を提供しますが、暗号化は提供しません。</li> <li>• [AuthPriv] : 認証と暗号化の両方を提供します。</li> </ul> |

| フィールド                | 説明   |
|----------------------|--|
| <b>Auth Type</b>     | <p>使用する認証タイプ（[Mode] として [AuthPriv] または [AuthNoPriv] を選択した場合に有効になります）。次のいずれかの認証タイプを選択します。</p> <ul style="list-style-type: none"> <li>• [SHA] : HMAC-SHA に基づく認証。</li> <li>• [MD5] : HMAC-MD5 に基づく認証。</li> </ul>  |
| <b>Auth Password</b> | <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"> <li>• 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。</li> <li>• 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。</li> </ul>   |
| <b>Privacy Type</b>  | <p>プライバシータイプ。（[Mode] として [AuthPriv] を選択した場合に有効になります）。次のいずれかのプライバシータイプを選択します。</p> <ul style="list-style-type: none"> <li>• [AES128] : 暗号化の 128 ビット CBC モード AES。</li> <li>• <b>CISCOAES192</b> : シスコのデバイス上での暗号化の 192 ビット CBC モード AES。</li> <li>• <b>CISCOAES256</b> : シスコのデバイス上での暗号化の 256 ビット CBC モード AES。</li> </ul> <p>(注)</p> <ul style="list-style-type: none"> <li>• 検出機能とインベントリ機能の使用は、プライバシータイプ CISCOAES192 および CISCOAES256 のみでサポートされています。アシュアランス機能はサポートされていません。</li> <li>• プライバシータイプ AES128 は、検出、インベントリ、およびアシュアランスでサポートされています。</li> </ul> |

| フィールド                   | 説明   |
|-------------------------|--|
| <b>Privacy Password</b> | <p>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。</p> <p>(注)</p> <ul style="list-style-type: none"> <li>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。</li> <li>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。</li> </ul> |

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

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

- a) 次のフィールドを設定します。

表 4: SNMP のプロパティ

| フィールド          | 説明   |
|----------------|--|
| <b>Retries</b> | 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。 |
| <b>Timeout</b> | 再試行の時間間隔（秒単位）。                                     |

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

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

- a) 次のフィールドを設定します。

表 5: HTTPS クレデンシャル

| フィールド      | 説明  |
|------------|---|
| Type       | 設定している HTTPS クレデンシャルのタイプを指定します。有効なタイプは、 <b>[Read]</b> または <b>[White]</b> です。  |
| Read/Write | <p>最大 10 個の HTTPS 読み取りまたは書き込みクレデンシャルを設定できます。</p> <ul style="list-style-type: none"> <li>• <b>[Name/Description]</b> : 追加している HTTPS ログイン情報の名前または説明。</li> <li>• <b>[Username]</b> : HTTPS 接続の認証に使用される名前です。</li> <li>• <b>[Password]</b> : 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。</li> <li>• <b>[Port]</b> : 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。</li> </ul> <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"> <li>• 小文字の英字 (a ~ z)</li> <li>• 大文字の英字 (A ~ Z)</li> <li>• 数字 (0 ~ 9)</li> <li>• 特殊文字 (: # _ * ?) -</li> </ul> <p>パスワードにスペースや山カッコ (&lt;&gt;) 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> |

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

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

- a) [Port] フィールドに、ポート番号を入力します。次のいずれかのポートを使用できます。
- ポート 830 (デフォルト)
  - デバイスで使用可能なその他のポート
  - Cisco DNA Center で設定されたカスタムポート (デバイスの可制御性が有効な場合のみカスタムポートを使用できます。詳細については、[Cisco DNA Center 管理者ガイド](#)の「Device Controllability」の項を参照してください)
- )。
- (注) [Add Discovery] ウィンドウの [Advanced] エリアで [Telnet] プロトコルを選択すると、NETCONF は無効になります。
- (注) Cisco Catalyst 9800 シリーズワイヤレス コントローラ デバイスを検出するには、NETCONF を有効にする必要があります。
- b) これらのログイン情報を後で使用するために保存する場合は、[Save as global settings] チェックボックスをオンにします。このチェックボックスをオンにしない場合、ログイン情報は現在の検出ジョブにのみ使用できます。
- c) [Save] をクリックします。

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

- a) 使用するプロトコルの名前をクリックします。緑のチェックマークはプロトコルが選択されていることを示します。
- 有効なプロトコルは、[SSH] (デフォルト) および [Telnet] です。
- b) 使用する順序でプロトコルをドラッグ アンド ドロップします。
- (注) [Add Discovery] ウィンドウの [Advanced] エリアで [Telnet] プロトコルを選択すると、NETCONF は無効になります。

**ステップ 15** [Discover] をクリックします。

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

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

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

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

- [Daily] : [Run at Interval (Days) ] フィールドに間隔を日単位で入力します。
  - [Weekly]:[Run at Interval (Weeks) ] フィールドに間隔を週単位で入力します。
5. 繰り返しに [Daily] または [Weekly] を選択した場合は、[Set Schedule End] チェックボックスをオンにして終了日時を定義します。
- (注) 繰り返しでは、新しいデバイスのみを検出できます。上部に表示される [Discover only new devices] トグルボタンは、デフォルトで有効になっています。
6. [End Date] または [End After] をクリックします。
- [End Date] : 繰り返しを終了する月、日付、年を入力します。
  - [End After] : 繰り返しを終了するまでの回数を入力します。
7. [Start] をクリックします。

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

[Discoveries] ウィンドウにスキャンの結果が表示されます。

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

## IP アドレス範囲を使用したネットワークの検出

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

### 始める前に

[ディスカバリの前提条件 \(2 ページ\)](#) で説明されているように、デバイスには必須のデバイス設定が存在する必要があります。

- ステップ 1** メニューアイコン (☰) をクリックして、[Tools] > [Discovery]。
- ステップ 2** [Discovery] ウィンドウで、[Add Discovery] をクリックします。
- ステップ 3** [New Discovery] ウィンドウの [Discovery Name] フィールドに、名前を入力します。
- ステップ 4** まだ表示されていない場合は [IP Address/Ranges] エリアを展開し、次のフィールドを設定します。
- [Discovery Type] : [IP Address/Range] オプションボタンをクリックし、IP アドレスまたはアドレス範囲を使用してデバイスを検出します。
  - [From] および [To] フィールド : [From] フィールドに開始 IP アドレスを入力し、[To] フィールドに終了 IP アドレスを入力します。



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

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

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

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

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

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

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

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

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

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

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

**ステップ 8** CLI クレデンシャルの場合は、次の手順を実行します。

a) 次のフィールドを設定します。

表 6: CLI クレデンシャル

| フィールド                   | 説明                                  |
|-------------------------|-------------------------------------|
| <b>Name/Description</b> | CLI クレデンシャルを説明する名前または語句。            |
| <b>Username</b>         | 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  |
|------------------------|---|
| <b>Password</b>        | <p>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。</p> <p>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。</p> <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>                     |
| <b>Enable Password</b> | <p>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。</p> <p>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。</p> <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> |

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

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

- a) 次のフィールドを設定します。

表 7: *SNMPv2c* のクレデンシャル

| フィールド        | 説明  |
|--------------|---|
| <b>Read</b>  | <ul style="list-style-type: none"> <li>• [Name/Description] : 追加している SNMPv2c 設定の名前または説明。</li> <li>• [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。</li> </ul> <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> |
| <b>Write</b> | <ul style="list-style-type: none"> <li>• [Name/Description] : 追加している SNMPv2c 設定の名前または説明。</li> <li>• [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。</li> </ul> <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>         |

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

c) [Save] をクリックします。

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

a) 次のフィールドを設定します。

表 8: SNMPv3 のクレデンシャル

| フィールド                   | 説明   |
|-------------------------|--|
| <b>Name/Description</b> | 追加した SNMPv3 設定の名前または説明。  |
| <b>Username</b>         | SNMPv3 設定に関連付けられている名前。   |
| <b>Mode</b>             | 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"> <li>• [noAuthNoPriv] : 認証または暗号化を提供しません。</li> <li>• [AuthNoPriv] : 認証を提供しますが、暗号化は提供しません。</li> <li>• [AuthPriv] : 認証と暗号化の両方を提供します。</li> </ul>  |
| <b>Auth Type</b>        | 使用する認証タイプ ([Mode] として [AuthPriv] または [AuthNoPriv] を選択した場合に有効になります)。次のいずれかの認証タイプを選択します。 <ul style="list-style-type: none"> <li>• [SHA] : HMAC-SHA に基づく認証。</li> <li>• [MD5] : HMAC-MD5 に基づく認証。</li> </ul>  |
| <b>Auth Password</b>    | 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"> <li>• 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。</li> <li>• 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。</li> </ul> |

| フィールド                   | 説明   |
|-------------------------|--|
| <b>Privacy Type</b>     | <p>プライバシータイプ。 ([Mode] として [AuthPriv] を選択した場合に有効になります) 。次のいずれかのプライバシータイプを選択します。</p> <ul style="list-style-type: none"> <li>• [AES128] : 暗号化の 128 ビット CBC モード AES。</li> <li>• <b>CISCOAES192</b> : シスコのデバイス上での暗号化の 192 ビット CBC モード AES。</li> <li>• <b>CISCOAES256</b> : シスコのデバイス上での暗号化の 256 ビット CBC モード AES。</li> </ul> <p>(注)</p> <ul style="list-style-type: none"> <li>• 検出機能とインベントリ機能の使用は、プライバシータイプ CISCOAES192 および CISCOAES256 のみでサポートされています。アシュアランス機能はサポートされていません。</li> <li>• プライバシータイプ AES128 は、検出、インベントリ、およびアシュアランスでサポートされています。</li> </ul> |
| <b>Privacy Password</b> | <p>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。</p> <p>(注)</p> <ul style="list-style-type: none"> <li>• 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。</li> <li>• 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。</li> </ul>   |

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

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

- a) 次のフィールドを設定します。

表 9: SNMP のプロパティ

| フィールド          | 説明   |
|----------------|--|
| <b>Retries</b> | 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。 |
| <b>Timeout</b> | 再試行の時間間隔（秒単位）。                                     |

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

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

- a) 次のフィールドを設定します。

表 10: HTTPS クレデンシャル

| フィールド       | 説明   |
|-------------|--|
| <b>Type</b> | 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。  |
| <b>Read</b> | <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"> <li>• [Name/Description] : 追加している HTTPS ログイン情報の名前または説明。</li> <li>• [Username] : HTTPS 接続の認証に使用される名前です。</li> <li>• [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。</li> <li>• [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。</li> </ul> <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"> <li>• 小文字の英字 (a ~ z)</li> <li>• 大文字の英字 (A ~ Z)</li> <li>• 数字 (0 ~ 9)</li> <li>• 特殊文字 (: # _ * ?) -</li> </ul> <p>パスワードにスペースや山カッコ (&lt;&gt;) 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"> <li>• [Name/Description] : 追加している HTTPS ログイン情報の名前または説明。</li> <li>• [Username] : HTTPS 接続の認証に使用される名前です。</li> <li>• [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。</li> <li>• [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。</li> </ul> <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"> <li>• 小文字の英字 (a ~ z)</li> <li>• 大文字の英字 (A ~ Z)</li> <li>• 数字 (0 ~ 9)</li> <li>• 特殊文字 (: # _ * ?) -</li> </ul> <p>パスワードにスペースや山カッコ (&lt;&gt;) 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> |

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

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

- a) [Port] フィールドに、ポート番号を入力します。次のいずれかのポートを使用できます。
  - ポート 830 (デフォルト)
  - デバイスで使用可能なその他のポート
  - Cisco DNA Center で設定されたカスタムポート (デバイスの可制御性が有効な場合のみカスタムポートを使用できます。詳細については、[Cisco DNA Center 管理者ガイド](#) の「Device Controllability」の項を参照してください)

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

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

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

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

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

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

- b) 使用する順序でプロトコルをドラッグ アンド ドロップします。

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

**ステップ 15** [Discover] をクリックします。

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

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

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

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

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



7. [Start] をクリックします。

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

[Discoveries] ウィンドウにスキャンの結果が表示されます。

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

## LLDP を使用したネットワークの検出

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



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

### 始める前に

- ネットワークデバイスで LLDP を有効にします。
- [ディスカバリの前提条件（2 ページ）](#) で説明されているように、ネットワークデバイスを設定します。
- クライアント IP アドレスとしてネットワークデバイスのホストの IP アドレスを設定します。(A host is an end-user device, such as a laptop computer or mobile device.)

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

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

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

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

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

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

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

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

- [Preferred Management IP Address] : 次のいずれかのオプションボタンをクリックします。

- [None] : デバイスが任意の IP アドレスを使用できるようにします。
- [Use Loopback IP] : デバイスのループバック インターフェイスの IP アドレスを指定します。  
(注) [Use Loopback IP] の使用を選択し、デバイスにループバック インターフェイスがない場合、Cisco DNA Center は **優先管理 IP アドレス (6 ページ)** で説明されているロジックを使用して、管理 IP アドレスを選択します。  
(注) ループバック インターフェイスの IP アドレスを優先管理 IP アドレスとして使用するには、LLDP ネイバーの IP アドレスが Cisco DNA Center から到達可能であることを確認します。

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

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

- 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。
- 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。
- 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   |
|-------------------------|--|
| <b>Name/Description</b> | CLI クレデンシャルを説明する名前または語句。   |
| <b>Username</b>         | 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。  |
| <b>Password</b>         | 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。<br>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。<br>(注) パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。 |

| フィールド                  | 説明  |
|------------------------|---|
| <b>Enable Password</b> | <p>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。</p> <p>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。</p> <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> |

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  |
|--------------|---|
| <b>Read</b>  | <ul style="list-style-type: none"> <li>• [Name/Description] : 追加している SNMPv2c 設定の名前または説明。</li> <li>• [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。</li> </ul> <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> |
| <b>Write</b> | <ul style="list-style-type: none"> <li>• [Name/Description] : 追加している SNMPv2c 設定の名前または説明。</li> <li>• [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。</li> </ul> <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  |
|-------------------------|---|
| <b>Name/Description</b> | 追加した SNMPv3 設定の名前または説明。   |
| <b>Username</b>         | SNMPv3 設定に関連付けられている名前。  |
| <b>Mode</b>             | <p>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。</p> <ul style="list-style-type: none"> <li>• [noAuthNoPriv] : 認証または暗号化を提供しません。</li> <li>• [AuthNoPriv] : 認証を提供しますが、暗号化は提供しません。</li> <li>• [AuthPriv] : 認証と暗号化の両方を提供します。</li> </ul> |

| フィールド                | 説明   |
|----------------------|--|
| <b>Auth Type</b>     | <p>使用する認証タイプ（[Mode]として [AuthPriv] または [AuthNoPriv] を選択した場合に有効になります）。次のいずれかの認証タイプを選択します。</p> <ul style="list-style-type: none"> <li>• [SHA] : HMAC-SHA に基づく認証。</li> <li>• [MD5] : HMAC-MD5 に基づく認証。</li> </ul>   |
| <b>Auth Password</b> | <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"> <li>• 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。</li> <li>• 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。</li> </ul>  |
| <b>Privacy Type</b>  | <p>プライバシータイプ。（[Mode]として [AuthPriv] を選択した場合に有効になります）。次のいずれかのプライバシー タイプを選択します。</p> <ul style="list-style-type: none"> <li>• [AES128] : 暗号化の 128 ビット CBC モード AES。</li> <li>• <b>CISCOAES192</b> : シスコのデバイス上での暗号化の 192 ビット CBC モード AES。</li> <li>• <b>CISCOAES256</b> : シスコのデバイス上での暗号化の 256 ビット CBC モード AES。</li> </ul> <p>(注)</p> <ul style="list-style-type: none"> <li>• 検出機能とインベントリ機能の使用は、プライバシータイプ CISCOAES192 および CISCOAES256 のみでサポートされています。アシュアランス 機能はサポートされていません。</li> <li>• プライバシー タイプ AES128 は、検出、インベントリ、およびアシュアランスでサポートされています。</li> </ul> |

| フィールド                   | 説明  |
|-------------------------|---|
| <b>Privacy Password</b> | <p>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。</p> <p>(注)</p> <ul style="list-style-type: none"> <li>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。</li> <li>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。</li> </ul> |

- 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  |
|----------------|---|
| <b>Retries</b> | 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。 |
| <b>Timeout</b> | 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   |
|-------------|--|
| <b>Type</b> | 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、 <b>[Read]</b> または <b>[White]</b> です。 |

| フィールド       | 説明   |
|-------------|--|
| <b>Read</b> | <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"> <li>• [Name/Description] : 追加している HTTPS ログイン情報の名前または説明。</li> <li>• [Username] : HTTPS 接続の認証に使用される名前です。</li> <li>• [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。</li> <li>• [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。</li> </ul> <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"> <li>• 小文字の英字 (a ~ z)</li> <li>• 大文字の英字 (A ~ Z)</li> <li>• 数字 (0 ~ 9)</li> <li>• 特殊文字 (: # _ * ?) -</li> </ul> <p>パスワードにスペースや山カッコ (&lt;&gt;) 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ヤルを設定できます。</p> <ul style="list-style-type: none"> <li>• [Name/Description] : 追加している HTTPS ログイン情報の名前または説明。</li> <li>• [Username] : HTTPS 接続の認証に使用される名前です。</li> <li>• [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。</li> <li>• [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。</li> </ul> <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"> <li>• 小文字の英字 (a ~ z)</li> <li>• 大文字の英字 (A ~ Z)</li> <li>• 数字 (0 ~ 9)</li> <li>• 特殊文字 (: # _ * ?) -</li> </ul> <p>パスワードにスペースや山カッコ (&lt;&gt;) 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] をクリックします。

[Discover Devices] スライドインペインが表示されます。

- ステップ 8** 今すぐ検出を実行するには、[Now] ラジオボタンをクリックし、[Start] をクリックします。
- 新しいデバイスのみを検出する場合は、[Discover only new devices] トグルボタンをクリックします。

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

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



- [Daily] : [Run at Interval (Days) ] フィールドに間隔を日単位で入力します。
  - [Weekly]:[Run at Interval (Weeks) ] フィールドに間隔を週単位で入力します。
5. 繰り返しに [Daily] または [Weekly] を選択した場合は、[Set Schedule End] チェックボックスをオンにして終了日時を定義します。
    - (注) 繰り返しでは、新しいデバイスのみを検出できます。上部に表示される [Discover only new devices] トグルボタンは、デフォルトで有効になっています。
  6. [End Date] または [End After] をクリックします。
    - [End Date] : 繰り返しを終了する月、日付、年を入力します。
    - [End After] : 繰り返しを終了するまでの回数を入力します。
  7. [Start] をクリックします。

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

[Discoveries] ウィンドウにスキャンの結果が表示されます。

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

## ディスカバリ ジョブの管理

ここでは、ディスカバリジョブの管理方法について説明します。

### ディスカバリ ジョブの停止および開始

- ステップ 1 メニューアイコン (☰) をクリックして、[Tools] > [Discovery]。
- ステップ 2 [Discovery] ウィンドウで、[All discoveries page from previous release] をクリックします。
- ステップ 3 アクティブなディスカバリ ジョブを停止するには、次の手順を実行します。
  - a) 左側の [Discoveries] ペインで、ディスカバリジョブをクリックします。
  - b) 下部ペインの右側で、[Stop] をクリックします。
- ステップ 4 非アクティブなディスカバリ ジョブを再起動するには、次の手順を実行します。
  - a) 左側の [Discoveries] ペインで、ディスカバリジョブをクリックします。
  - b) 下部ペインの右側で、[Re-discover] をクリックします。

## ディスカバリ ジョブの編集

既存のディスカバリジョブを編集して、ジョブを再実行できます。

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

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

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

**ステップ 4** [Edit] をクリックします。

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

- **[CDP]** : ディスカバリ名、ディスカバリタイプ、IP アドレス。変更可能なフィールドの詳細については、[CDP を使用したネットワークの検出 \(7 ページ\)](#) を参照してください。
- **[IP Range]** : ディスカバリ名、タイプ、IP アドレス範囲 (ただし別の IP アドレス範囲を追加できません)。変更可能なフィールドの詳細については、[IP アドレス範囲を使用したネットワークの検出 \(15 ページ\)](#) を参照してください。
- **[LLDP]** : ディスカバリ名、タイプ、IP アドレス。変更可能なフィールドの詳細については、[LLDP を使用したネットワークの検出 \(23 ページ\)](#) を参照してください。

**ステップ 6** [Start] をクリックします。

## ディスカバリ ジョブでクレデンシャルを変更

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

始める前に

少なくとも 1 つのディスカバリ ジョブが必要です。

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

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

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

**ステップ 4** [Edit] をクリックします。

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

**ステップ 6** 使わないクレデンシャルを非選択状態にします。

**ステップ 7** 使用するクレデンシャルを設定します。

- a) [クレデンシャルの追加 (Add Credentials) ] をクリックします。
- b) CLI クレデンシャルを設定するには、次のフィールドを設定します。

表 16: CLI クレデンシャル

| フィールド                   | 説明   |
|-------------------------|--|
| <b>Name/Description</b> | CLI クレデンシャルを説明する名前または語句。   |
| <b>Username</b>         | 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。  |
| <b>Password</b>         | 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。<br>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。<br>(注) パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。                     |
| <b>Enable Password</b>  | 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。<br>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。<br>(注) パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。 |

- c) [SNMP v2c] をクリックして、次のフィールドを設定します。

表 17: SNMPv2c のクレデンシャル

| フィールド        | 説明  |
|--------------|---|
| <b>Read</b>  | <ul style="list-style-type: none"> <li>[Name/Description] : 追加している SNMPv2c 設定の名前または説明。</li> <li>[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。</li> </ul> <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> |
| <b>Write</b> | <ul style="list-style-type: none"> <li>[Name/Description] : 追加している SNMPv2c 設定の名前または説明。</li> <li>[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。</li> </ul> <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>         |

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

表 18: SNMPv3 のクレデンシャル

| フィールド                   | 説明   |
|-------------------------|--|
| <b>Name/Description</b> | 追加した SNMPv3 設定の名前または説明。  |
| <b>Username</b>         | SNMPv3 設定に関連付けられている名前。   |
| <b>Mode</b>             | 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"> <li>• [noAuthNoPriv] : 認証または暗号化を提供しません。</li> <li>• [AuthNoPriv] : 認証を提供しますが、暗号化は提供しません。</li> <li>• [AuthPriv] : 認証と暗号化の両方を提供します。</li> </ul>   |
| <b>Auth Type</b>        | 使用する認証タイプ ([Mode] として [AuthPriv] または [AuthNoPriv] を選択した場合に有効になります)。次のいずれかの認証タイプを選択します。 <ul style="list-style-type: none"> <li>• [SHA] : HMAC-SHA に基づく認証。</li> <li>• [MD5] : HMAC-MD5 に基づく認証。</li> </ul>  |
| <b>Auth Password</b>    | 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"> <li>• 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。</li> <li>• 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。</li> </ul> |

| フィールド                   | 説明  |
|-------------------------|---|
| <b>Privacy Type</b>     | <p>プライバシータイプ。 ([Mode] として [AuthPriv] を選択した場合に有効になります)。 次のいずれかのプライバシータイプを選択します。</p> <ul style="list-style-type: none"> <li>• [AES128] : 暗号化の 128 ビット CBC モード AES。</li> <li>• <b>CISCOAES192</b> : シスコのデバイス上での暗号化の 192 ビット CBC モード AES。</li> <li>• <b>CISCOAES256</b> : シスコのデバイス上での暗号化の 256 ビット CBC モード AES。</li> </ul> <p>(注)</p> <ul style="list-style-type: none"> <li>• 検出機能とインベントリ機能の使用は、プライバシータイプ CISCOAES192 および CISCOAES256 のみでサポートされています。 アシユアランス機能はサポートされていません。</li> <li>• プライバシータイプ AES128 は、検出、インベントリ、およびアシユアランスでサポートされています。</li> </ul> |
| <b>Privacy Password</b> | <p>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 (またはパズフレーズ) 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"> <li>• 一部のシスコワイヤレスコントローラでは、パスワード (あるいはパズフレーズ) 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。</li> <li>• 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。</li> </ul>   |

ステップ 8 [Start] をクリックします。

## ディスカバリ ジョブの複製

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

始める前に

少なくとも 1 つのディスカバリ ジョブを実行する必要があります。

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

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

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

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

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

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

ステップ6 新しいディスカバリ ジョブのパラメータを定義または更新します。

---

## ディスカバリ ジョブの削除

アクティブまたは非アクティブに関係なく、検出ジョブを削除できます。

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

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

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

ステップ4 下部ペインの右側で、[Delete] をクリックします。

ステップ5 [OK] をクリックして確定します。

---

## ディスカバリ ジョブ情報の表示

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

### 始める前に

少なくとも1つのディスカバリジョブを実行します。

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

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

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

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

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

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

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

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

## すべてのディスカバリの表示

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

---





## 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。