



ネットワークの検出

- [ディスカバリについて](#) (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)
- [検出ジョブの管理](#) (24 ページ)

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。

ディスカバリ機能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行うこともできます（これらの設定がまだデバイスに存在しない場合）。デバイスの制御性については、[Cisco Digital Network Architecture Center 管理者ガイド](#)を参照してください。

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ます。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

Cisco DNA Center のホームページで、[Tools] > [Discovery] を選択して、[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。

- 「サポート対象デバイスのリスト」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 とデバイス間の最大ネットワーク遅延は 100 ミリ秒であることに注意してください。（最大遅延は 200 ミリ秒です）。

- Cisco DNA Center が使用できるように 1 つ以上の SNMP クレデンシャルがデバイス上で設定されていることを確認してください。少なくとも、これには SNMP v2C 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 2 つの基準のうち、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。
 - 匿名化を設定します。匿名化は、ホスト名とユーザ ID フィールドのスクランブルを実行します。詳細については、「[コレクタの設定情報の表示または更新](#)」を参照してください。



重要 ディスカバリを実行した後にデータを匿名化した場合、システムに投入される新しいデータは匿名になりますが、既存のデータは匿名にはなりません。

ディスカバリ クレデンシャル

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

- 標準シスコ デバイス : CLI および SNMP クレデンシャル。
- NFVIS デバイス : HTTP (HTTPS) クレデンシャル。
- 標準デバイスと NFVIS デバイスの両方 : CLI、SNMP、および HTTP (HTTPS) 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5つの保存済みクレデンシャルと1つのジョブ固有クレデンシャルを定義できます。

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 \(25 ページ\)](#)」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 クレデンシャルを編集し、ディスカバリ ジョブを再実行します。
- 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 クレデンシャルを編集し、ディスカバリ ジョブを再実行します。
 - 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。たとえば、クレデンシャルを削除してから 25 分後に、そのクレデンシャルを使用するディスカバリ ジョブが失敗します。

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。

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アルを設定します。
- 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アルを共有する 190 台のデバイス) の 1 つとグローバルクレデンシアル 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アル (クレデンシアル1、クレデンシアル2、クレデンシアル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 [インベントリ (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 は、デバイスを検出すると、そのデバイスのいずれかの IP アドレスをそのデバイスの優先管理 IP アドレスとしてログに記録します。IP アドレスは、デバイスの組み込み管理インターフェイス、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 アドレスとして記録するように Cisco DNA Center を設定できます (その IP アドレスが Cisco DNA Center から到達可能である場合)。

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

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

デバイスが検出された後に、[インベントリ (Inventory)] ウィンドウから管理 IP アドレスを更新できます。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 クレデンシャルが、TACACS サーバで定義されている TACACS クレデンシャル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。

ディスカバリの実行

CDP を使用したネットワークの検出

Cisco Discovery Protocol (CDP) IP アドレス範囲、または LLDP を使用してデバイスを検出できます。この手順では、CDP を使用してデバイスとホストを検出する方法を示します。ディスカバリ メソッドの詳細については、[Discover Your Network Using an IP Address Range \(13 ページ\)](#) および [LLDP を使用したネットワークの検出 \(18 ページ\)](#) 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 クレデンシャル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 デバイスで検出されます。

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の IP アドレスを設定します。(A host is an end-user device, such as a laptop computer or mobile device.)


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

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

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

- a) [ディスカバリ タイプ (Discovery Type)] で、[CDP] をクリックします。
- b) [IP アドレス (IP Address)] フィールドでシード IP アドレスを入力し、Cisco DNA Center でディスカバリ スキャンを開始します。
- c) (任意) [サブネットフィルタ (Subnet Filter)] フィールドで、ディスカバリ スキャンから除外する IP アドレスまたはサブネットを入力します。

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

- d)  をクリックします。

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

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

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

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

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

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

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

ステップ 4 [クレデンシヤル (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、[クレデンシヤルの追加 (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。 |
| 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もう一度入力します。 (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もう一度入力します。 (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 のクレデンシヤル

| フィールド | 説明 |
|--------------|--|
| Read | <ul style="list-style-type: none"> • [名前/説明 (Name/Description)] : 追加する SNMP v2c 設定の名前または説明。 • Read コミュニティ : デバイス上の SNMP 情報を表示するためにのみ使用される read-only コミュニティ ストリング 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"> • [名前/説明 (Name/Description)] : 追加する SNMP v2c 設定の名前または説明。 • Write コミュニティ : デバイス上の SNMP 情報を変更するために使用される write コミュニティ ストリング。 <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 3: SNMPv3 のクレデンシャル

| フィールド | 説明 |
|-------------------------|--|
| Name/Description | 追加した SNMPv3 設定の名前または説明。 |
| Username | SNMPv3 設定に関連付けられている名前。 |
| Mode | SNMP メッセージを必要とするセキュリティレベル。次のいずれかのモードを選択します。 <ul style="list-style-type: none"> • noAuthNoPriv : 認証または暗号を提供しません。 • AuthNoPriv : 認証を提供しますが、暗号は提供しません。 • AuthPriv : 認証と暗号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"> • DES : CBC DES-56 規格に基づく認証に DES 56-bit 暗号化を追加。 • AES128 : 暗号化の CBC モード AES。 • None : プライバシー設定なし。 |

| フィールド | 説明 |
|-------------------------|---|
| Privacy Password | <p>DES または AES128 暗号化をサポートしているデバイスで交換されるメッセージを暗号化するための秘密鍵を生成するために使用される SNMPv3 プライバシーパスワード。パスワード (またはパスフレーズ) は、8 文字以上にする必要があります。</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 プロパティ (SNMP PROPERTIES)] をクリックして、次のフィールドを設定します。

表 4: *SNMP Properties*

| フィールド | 説明 |
|----------------|---|
| 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 5 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"> • 名前/説明 : 追加する HTTPS ログイン情報の名前または説明です。 • ユーザ名 : HTTPS 接続の認証に使用される名前です。 • パスワード : HTTPS 接続の認証に使用されるパスワードです。 • ポート : HTTPS トラフィックに使用される TCP/UDP ポートの数です。デフォルトはポート番号 443 (HTTPS の既知のポート) です。 <p>(注) パスワードには、少なくとも1つの小文字、1つの大文字、1つの数字、1つの特殊文字が必要で、<>@',:;!およびスペースは使用できません。セキュリティ上の理由から、確認のためにパスワードをもう一度入力します。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。</p> |
| Write | <p>最大 5 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 : 追加する HTTPS ログイン情報の名前または説明です。 • ユーザ名 : HTTPS 接続の認証に使用される名前です。 • パスワード : HTTPS 接続の認証に使用されるパスワードです。 • ポート : HTTPS トラフィックに使用される TCP/UDP ポートの数です。デフォルトはポート番号 443 (HTTPS の既知のポート) です。 <p>(注) パスワードには、少なくとも1つの小文字、1つの大文字、1つの数字、1つの特殊文字が必要で、<>@',:;!およびスペースは使用できません。セキュリティ上の理由から、確認のためにパスワードをもう一度入力します。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。</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 830 に設定する必要があります。NETCONF は、ネットワークデバイスの設定をインストール、操作、削除するためのメカニズムです。

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

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

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

b) 使用する順序でプロトコルをドラッグアンドドロップします。

ステップ 6 [開始 (Start)] をクリックします。[検出 (Discover)] をクリックして、すぐにディスカバリを実行するか、または後で実行するためにディスカバリをスケジュールするかを選択します。

- 今すぐディスカバリを実行するには、[今すぐ (Now)] ラジオボタンをクリックし、[開始 (Start)] をクリックします。
- 後でディスカバリをスケジュールするには、[後で実行 (Later)] ラジオボタンをクリックして更新の日時を定義し、[開始 (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ディスカバリタスクを表示します。ディスカバリを開始する前にディスカバリタスクを編集するには、[編集 (Edit)] をクリックします。スケジュールされたディスカバリジョブを開始する前にキャンセルする場合は、[キャンセル (Cancel)] をクリックします。

[Discoveries] ウィンドウにスキャンの結果が表示されます。

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

Discover Your Network Using an IP Address Range

IP アドレス範囲、CDP、または LLDP を使用してデバイスを検出できます。この手順では、IP アドレス範囲を使用してデバイスとホストを検出する方法を示します。ディスカバリメソッドの詳細については、[CDP を使用したネットワークの検出 \(7 ページ\)](#) および [LLDP を使用したネットワークの検出 \(18 ページ\)](#) 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 \(2 ページ\)](#) 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 Cisco DNA Center のホームページで、[ディスカバリ (Discovery)] をクリックします。

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

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

- a) [ディスカバリ タイプ (Discovery Type)] で、[範囲 (Range)] をクリックします。
- b) [IP アドレス (IP Address)] フィールドに、Cisco DNA Center の最初と最後の IP アドレス (IP 範囲) を入力し、[追加 (Add)]  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) [優先管理 IP (Preferred Management IP)] で、次のいずれかのオプションを選択します。

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

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

ステップ 4 [クレデンシヤル (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、[クレデンシヤルの追加 (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もう一度入力します。 (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もう一度入力します。 (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"> • [名前/説明 (Name/Description)] : 追加する SNMP v2c 設定の名前または説明。 • Read コミュニティ : デバイス上の SNMP 情報を表示するためにのみ使用される read-only コミュニティストリングパスワード。 <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"> • [名前/説明 (Name/Description)] : 追加する SNMP v2c 設定の名前または説明。 • Write コミュニティ : デバイス上の SNMP 情報を変更するために使用される write コミュニティストリング。 <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 : 認証または暗号を提供しません。 • AuthNoPriv : 認証を提供しますが、暗号は提供しません。 • AuthPriv : 認証と暗号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"> • DES : CBC DES-56 規格に基づく認証に DES 56-bit 暗号化を追加。 • AES128 : 暗号化の CBC モード AES。 • None : プライバシー設定なし。 |
| Privacy Password | <p>DES または AES128 暗号化をサポートしているデバイスで交換されるメッセージを暗号化するための秘密鍵を生成するために使用されるSNMPv3プライバシーパスワード。パスワード（またはパスフレーズ）は、8文字以上にする必要があります。</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プロパティ（SNMP PROPERTIES）]をクリックして、次のフィールドを設定します。

表 9: *SNMP Properties*

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

| フィールド | 説明 |
|--------|-------------|
| タイムアウト | 再試行間隔を表す秒数。 |

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

表 10: HTTPS クレデンシヤル

| 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 5 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"> • 名前/説明 : 追加する HTTPS ログイン情報の名前または説明です。 • ユーザ名 : HTTPS 接続の認証に使用される名前です。 • パスワード : HTTPS 接続の認証に使用されるパスワードです。 • ポート : HTTPS トラフィックに使用される TCP/UDP ポートの数です。デフォルトはポート番号 443 (HTTPS の既知のポート) です。 <p>(注) パスワードには、少なくとも1つの小文字、1つの大文字、1つの数字、1つの特殊文字が必要で、<>@',:;!およびスペースは使用できません。セキュリティ上の理由から、確認のためにパスワードをもう一度入力します。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。</p> |
| Write | <p>最大 5 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"> • Name/Description : 追加する HTTPS ログイン情報の名前または説明です。 • ユーザ名 : HTTPS 接続の認証に使用される名前です。 • パスワード : HTTPS 接続の認証に使用されるパスワードです。 • ポート : HTTPS トラフィックに使用される TCP/UDP ポートの数です。デフォルトはポート番号 443 (HTTPS の既知のポート) です。 <p>(注) パスワードには、少なくとも1つの小文字、1つの大文字、1つの数字、1つの特殊文字が必要で、<>@',:;!およびスペースは使用できません。セキュリティ上の理由から、確認のためにパスワードをもう一度入力します。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。</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 830 に設定する必要があります。NETCONF は、ネットワークデバイス の設定をインストール、操作、削除するためのメカニズムです。

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

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

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

- b) 使用する順序でプロトコルをドラッグアンドドロップします。

ステップ 6 [開始 (Start)] をクリックします。[検出 (Discover)] をクリックして、すぐにディスカバリを実行す るか、または後で実行するためにディスカバリをスケジュールするかを選択します。

- 今すぐディスカバリを実行するには、[今すぐ (Now)] ラジオボタンをクリックし、[開始 (Start)] を クリックします。
- 後でディスカバリをスケジュールするには、[後で実行 (Later)] ラジオボタンをクリックして更新の 日時を定義し、[開始 (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ディスカバリタスクを表示します。ディスカバリを開 始する前にディスカバリタスクを編集するには、[編集 (Edit)] をクリックします。スケジュールされた ディスカバリジョブを開始する前にキャンセルする場合は、[キャンセル (Cancel)] をクリックします。

[Discoveries] ウィンドウにスキャンの結果が表示されます。

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

LLDP を使用したネットワークの検出

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



- (注)
- ディスカバリ機能では、正しい SNMP 読み取り専用 (RO) コミュニティストリングが必 要です。SNMP RO コミュニティストリングが指定されていない場合、ベストエフォート として、ディスカバリ機能はデフォルトの SNMP RO コミュニティストリングを公的に使 用します。
 - CLI クレデンシャル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 デバイスで検出されます。

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

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

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

- [ディスカバリ タイプ (Discovery Type)] で、[LLDP] 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。

-  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。

- (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。

- [優先管理 IP (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。
- **ループバック IP を使用 (Use Loopback IP)** : デバイスのループバック インターフェイスの IP アドレスを指定します。

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

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

ステップ 4 [クレデンシヤル (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。クレデンシヤルを設定する場合は、[グローバル設定として保存 (Save as global settings)] チェックボックスをオンにして、将来のジョブのためにそれらを保存できます。

- a) 使用するグローバル クレデンシ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、[クレデンシヤルの追加 (Add Credentials)] をクリックします。
- c) CLI クレデンシヤルの場合は、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もう一度入力します。 (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もう一度入力します。 (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 のクレデンシヤル

| フィールド | 説明 |
|-------------|--|
| Read | <ul style="list-style-type: none"> • [名前/説明 (Name/Description)] : 追加する SNMP v2c 設定の名前または説明。 • Read コミュニティ : デバイス上の SNMP 情報を表示するためにのみ使用される read-only コミュニティ ストリング パスワード。 (注) パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。 |

| フィールド | 説明 |
|--------------|---|
| Write | <ul style="list-style-type: none"> • [名前/説明 (Name/Description)] : 追加する SNMP v2c 設定の名前または説明。 • Write コミュニティ : デバイス上の SNMP 情報を変更するために使用される write コミュニティ ストリング。 <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 : 認証または暗号を提供しません。 • AuthNoPriv : 認証を提供しますが、暗号は提供しません。 • AuthPriv : 認証と暗号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。 |

| フィールド | 説明 |
|-------------------------|---|
| 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"> • DES : CBC DES-56 規格に基づく認証に DES 56-bit 暗号化を追加。 • AES128 : 暗号化の CBC モード AES。 • None : プライバシー設定なし。 |
| Privacy Password | <p>DES または AES128 暗号化をサポートしているデバイスで交換されるメッセージを暗号化するための秘密鍵を生成するために使用される SNMPv3 プライバシーパスワード。パスワード (またはパスフレーズ) は、8 文字以上にする必要があります。</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 プロパティ (SNMP PROPERTIES)] をクリックして、次のフィールドを設定します。

表 14: *SNMP Properties*

| フィールド | 説明 |
|----------------|---|
| 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 |
|-------|---|
| Read | <p>最大 5 つの HTTPS 読み取りクレデンシアルを設定できます。</p> <ul style="list-style-type: none"> • 名前/説明 : 追加する HTTPS ログイン情報の名前または説明です。 • ユーザ名 : HTTPS 接続の認証に使用される名前です。 • パスワード : HTTPS 接続の認証に使用されるパスワードです。 • ポート : HTTPS トラフィックに使用される TCP/UDP ポートの数です。デフォルトはポート番号 443 (HTTPS の既知のポート) です。 <p>(注) パスワードには、少なくとも1つの小文字、1つの大文字、1つの数字、1つの特殊文字が必要で、<>@',:;!およびスペースは使用できません。セキュリティ上の理由から、確認のためにパスワードをもう一度入力します。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。</p> |
| Write | <p>最大 5 つの HTTPS 書き込みクレデンシアルを設定できます。</p> <ul style="list-style-type: none"> • Name/Description : 追加する HTTPS ログイン情報の名前または説明です。 • ユーザ名 : HTTPS 接続の認証に使用される名前です。 • パスワード : HTTPS 接続の認証に使用されるパスワードです。 • ポート : HTTPS トラフィックに使用される TCP/UDP ポートの数です。デフォルトはポート番号 443 (HTTPS の既知のポート) です。 <p>(注) パスワードには、少なくとも1つの小文字、1つの大文字、1つの数字、1つの特殊文字が必要で、<>@',:;!およびスペースは使用できません。セキュリティ上の理由から、確認のためにパスワードをもう一度入力します。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。</p> |

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

- a) 使用するプロトコルの名前をクリックします。緑のチェックマークはプロトコルが選択されていることを示します。有効なプロトコルは、[SSH] (デフォルト) および [Telnet] です。
- b) 使用する順序でプロトコルをドラッグアンドドロップします。

ステップ 6 [開始 (Start)] をクリックします。[検出 (Discover)] をクリックして、すぐにディスカバリを実行するか、または後で実行するためにディスカバリをスケジュールするかを選択します。

- 今すぐディスカバリを実行するには、[今すぐ (Now)] ラジオボタンをクリックし、[開始 (Start)] をクリックします。
- 後でディスカバリをスケジュールするには、[後で実行 (Later)] ラジオボタンをクリックして更新の日時を定義し、[開始 (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ディスカバリタスクを表示します。ディスカバリを開始する前にディスカバリタスクを編集するには、[編集 (Edit)] をクリックします。スケジュールされたディスカバリジョブを開始する前にキャンセルする場合は、[キャンセル (Cancel)] をクリックします。

[Discoveries] ウィンドウにスキャンの結果が表示されます。

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

検出ジョブの管理

ディスカバリ ジョブの停止および開始

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

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

- [ディスカバリ (Discoveries)] ペインで、関連するディスカバリ ジョブを選択します。
- [Stop] をクリックします。

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

- [ディスカバリ (Discoveries)] ペインで、関連するディスカバリ ジョブを選択します。
- [Re-discover] をクリックして、選択した検出ジョブを再起動します。

ディスカバリ ジョブの編集

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。

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

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

ステップ 3 [Edit] をクリックします。

ステップ 4 次のフィールドを除き、ディスカバリのタイプに応じてディスカバリ 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 範囲 (IP Range)** : ディスカバリ名、ディスカバリタイプ、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す)。変更可能なフィールドの詳細については、[Discover Your Network Using an IP Address Range \(13 ページ\)](#) を参照してください。
- **LLDP** : 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、[LLDP を使用したネットワークの検出 \(18 ページ\)](#) を参照してください。

ステップ5 [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 Cisco DNA Center のホームページで、**[ディスカバリ (Discovery)]** をクリックします。

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

ステップ3 **[Edit]** をクリックします。

ステップ4 **[クレデンシャル (Credentials)]** エリアを展開します。

ステップ5 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6 使用するクレデンシャルを設定します。

- [クレデンシャルの追加 (Add Credentials)] をクリックします。
- 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 |
|-------------------------|---|
| 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もう一度入力します。 (注) パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。 |

| フィールド | 説明 |
|------------------------|--|
| Enable Password | <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が必要な場合にのみ、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もう一度入力します。</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> |

- 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 |
|--------------|--|
| Read | <ul style="list-style-type: none"> • [名前/説明 (Name/Description)] : 追加する SNMP v2c 設定の名前または説明。 • Read コミュニティ : デバイス上の SNMP 情報を表示するためにのみ使用される read-only コミュニティストリングパスワード。 <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"> • [名前/説明 (Name/Description)] : 追加する SNMP v2c 設定の名前または説明。 • Write コミュニティ : デバイス上の SNMP 情報を変更するために使用される write コミュニティストリング。 <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 |
|-------------------------|-------------------------|
| 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 : 認証または暗号を提供しません。 • AuthNoPriv : 認証を提供しますが、暗号は提供しません。 • AuthPriv : 認証と暗号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"> • DES : CBC DES-56 規格に基づく認証に DES 56-bit 暗号化を追加。 • AES128 : 暗号化の CBC モード AES。 • None : プライバシー設定なし。 |

| フィールド | 説明 |
|------------------|---|
| Privacy Password | <p>DES または AES128 暗号化をサポートしているデバイスで交換されるメッセージを暗号化するための秘密鍵を生成するために使用される SNMPv3 プライバシーパスワード。パスワード（またはパスフレーズ）は、8 文字以上にする必要があります。</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。 |

ステップ 7 [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、そのディスカバリ ジョブに定義されているすべての情報を保持できます。

始める前に

少なくとも 1 つのディスカバリ ジョブを実行する必要があります。

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

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

ステップ 3 [Clone & Edit] をクリックします。

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

ステップ 4 (任意) 検出ジョブの名前を変更します。

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

ディスカバリ ジョブの削除

アクティブまたは非アクティブに関係なく、検出ジョブを削除できます。

始める前に

少なくとも1つのディスカバリ ジョブを実行する必要があります。

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

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

ステップ3 [削除 (Delete)] をクリックします。

ステップ4 [OK] をクリックして確定します。

ディスカバリ ジョブ情報の表示

使用された設定やクレデンシヤルなどの、ディスカバリ ジョブに関する情報を表示できます。検出された、または検出に失敗した特定のデバイスに関する情報を含め、実行された各ディスカバリ ジョブに関する履歴情報も表示できます。

始める前に

少なくとも1つのディスカバリジョブを実行します。

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

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

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

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

