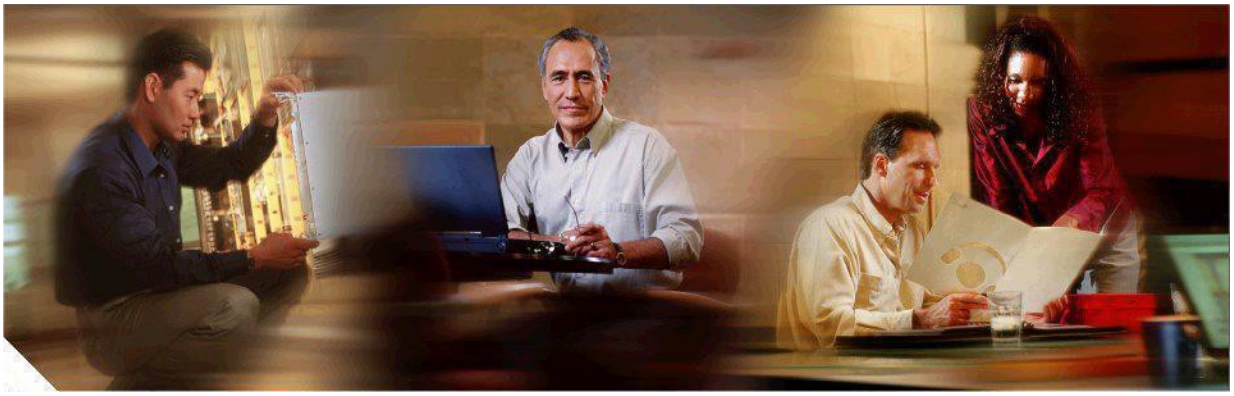


Common Services Platform Collector（CSPC）
セルフサービス - スタートアップ ガイド

2015 年 11 月

本社
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com/jp

目次

寄稿者

名前	電子メール	役職
ジョシュ・ハープスト	jharpst@cisco.com	SNTC コレクタ サポート エンジニア

校閲者

名前	電子メール	役職
リンデン・プライス	josprice#@cisco.com	ドキュメントの管理責任者および SNTC コレクタ サポート技術責任者

CSPC の概要

このマニュアルでは、CSPC 2.5.2 リリースに関する情報を示します。CSPC を設定し、正しくセットアップするには、コマンドラインによるデバイス設定の経験と、ネットワーク管理システムに関する基本的な知識が必要です。

CSPC は、SNMP ベースのツールであり、シスコ デバイスから情報を検出および収集します。ご使用のデバイスにセットアップされている SNMP 読み取り専用コミュニティ ストリングを把握しておくことが必要です。このマニュアルでは、CSPC の基本セットアップの手順を説明します。

前提条件

CSPC ライセンス ファイルを生成するには、Smart Net Total Care ポータルに対するアクセス権を取得するためのポータル オンボーディングを実行する必要があります。以下のリンクの指示に従ってください。
https://supportforums.cisco.com/document/12566021/new-smart-net-total-care

Smart Net Total Care のセキュリティ

CSPC は、さまざまなプロトコルを使用して、サポート対象のシスコ デバイスからデータを収集します。ネットワーク内のデバイスのポーリングを行い、デバイスからインベントリの詳細を収集するには、最低でも SNMP 読み取り専用アクセス権が必要になります。さらに、SSH または Telnet アクセス（あるいはその両方）を有効にして、収集に役立てることができます。シスコのコレクタは、Telnet または SSH（あるいはその両方）を使用して、デバイスの設定、インベントリの追加情報、および重大なイベント後に発生する例外ベースのデータを収集します。コレクタが実行できるコマンドの一覧は、シスコのセキュリティに関するホワイト ペーパーに記載されています。次のリンクからアクセスできます。シスコのセキュリティに関するホワイト ペーパー [英語]

Smart Net Total Care サポート コミュニティ

Smart Net Total Care の詳細については、Smart Net Total Care サポート コミュニティを参照してください。ディスカッション グループ、FAQ、トレーニング、およびその他の Smart Net Total Care 関連のリソースを利用できます。

Smart Net Total Care サポート コミュニティ

仮想プラットフォーム要件

このセクションでは、仮想プラットフォーム要件について説明します。このガイドでは、各種の仮想プラットフォームをインストールする方法については説明しません。

ESXi 4.x 以上の仮想プラットフォーム上で実行されるコレクタ イメージのシステム要件を次に示します。

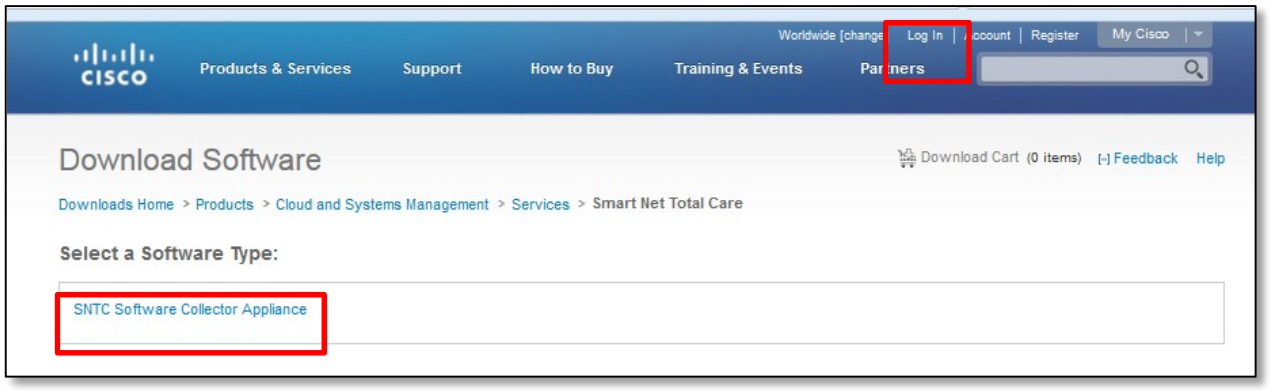
- 250 GB のハードドライブ空き容量
- CPU コア（仮想 CPU）X 4
- 仮想 NIC X 1（必要な NIC の数はネットワーク トポロジに応じて異なります）
- 4 GB の仮想 RAM

仮想マシン イメージのダウンロード

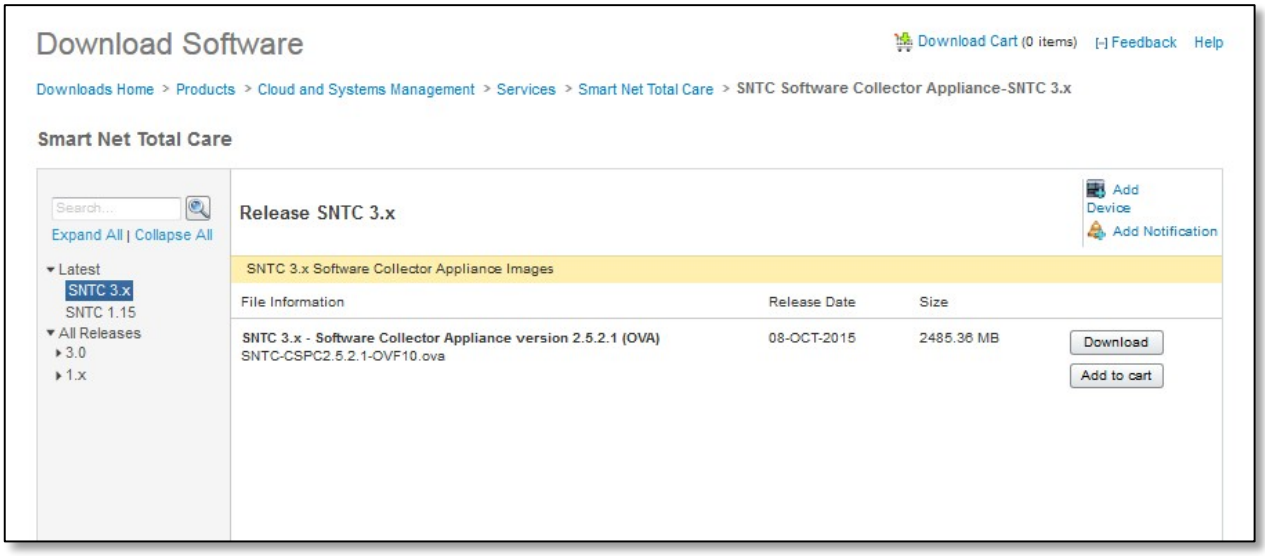
仮想環境で必要なリソースが提供されることを確認したら、次に Smart Net Total Care イメージをダウンロードします。ソフトウェア イメージはダウンロード センターから入手できます。ダウンロード センターには最新のソフトウェア イメージがあります。Cisco Smart Net Total Care イメージにアクセスするには、次の手順を実行します。

- 次の URL に移動します。
  http://software.cisco.com/download/type.html?mdfid=283107976&catid=null

- 画面右上隅の [ログイン（Log In）] リンクをクリックし、CCO ID とパスワードを使用してログインします。



- [SNTC ソフトウェア コレクタ アプライアンス（SNTC Software Collector Appliance）] をクリックします。[ソフトウェアのダウンロード（Download Software）] ウィンドウが表示されます。



- [ダウンロード（Download）] ボタンをクリックします。プロンプトが表示されたら、利用規約に同意します。これでイメージのダウンロードが開始されます。
- このイメージを仮想環境に導入します。

アプライアンス IP アドレスの設定

このセクションでは、仮想マシンとハードウェア プラットフォームの両方のアプライアンスについて説明します。

アプライアンスの IP アドレスを設定するには、次の手順を実行します。

- ハードウェア アプライアンスの場合：サーバにモニタとキーボードを接続します。
- ソフトウェア アプライアンスの場合：仮想環境のツールを使用して仮想マシンのコンソールに接続します。

コレクタの起動後、任意のキーを押すように求められます。

- 任意のキーを押します。

```
Press any key to continue.
_
```

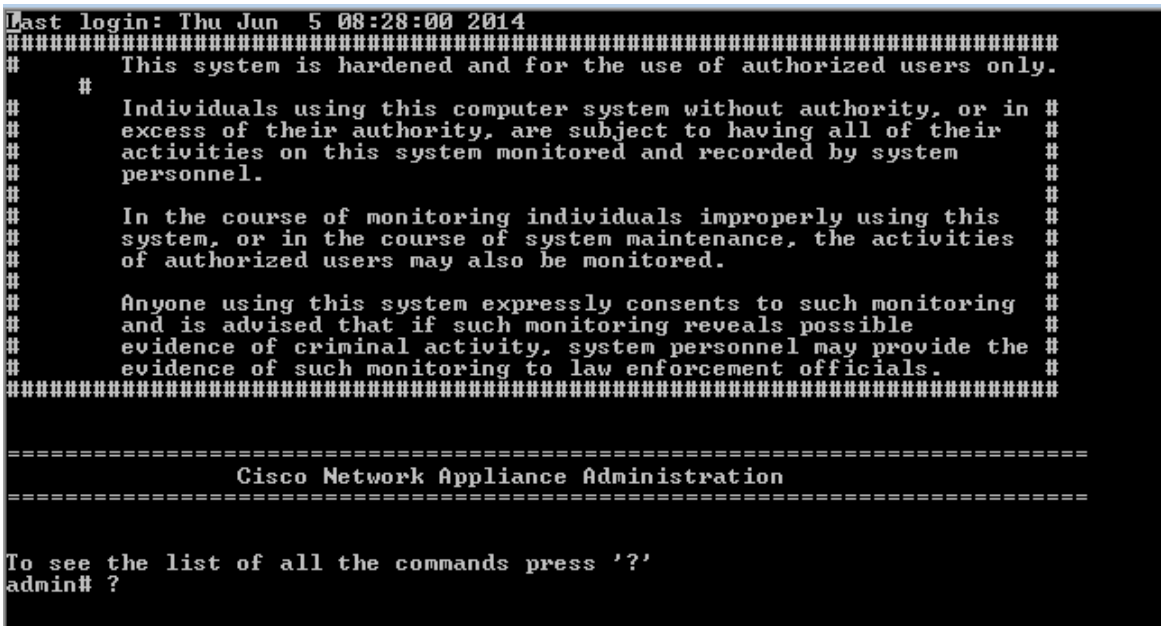
通常、ブート プロセス中に[任意のキーを押してください(Press any key)]と表示され、ログイン プロンプトが示されるまでに数分かかる場合があります。

- 次のログイン ID/パスワード情報を使用して、接続済みのコンソールを経由してソフトウェア アプライアンスにログインします。

  admin/Admin!23

アプライアンスに初めてログインする際、デフォルトの CLI パスワードを変更するように求められます。

アプライアンスにログインすると、次の画面が表示されます。

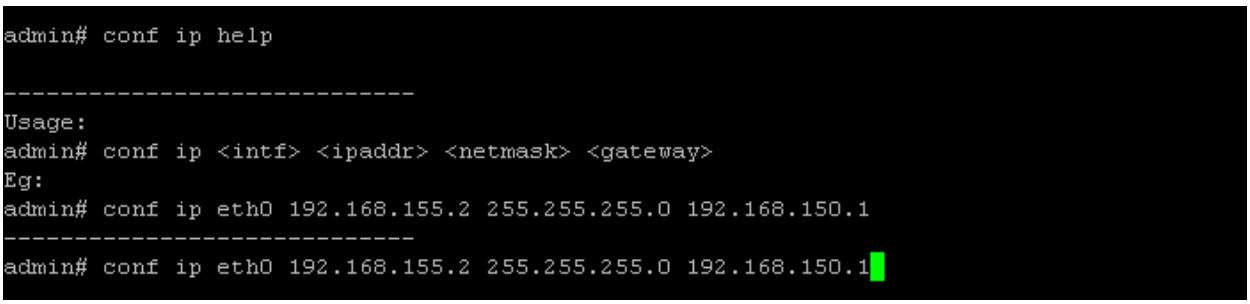


静的 IP アドレスを割り当てるには、**conf ip** コマンドを使用します。

- コマンド プロンプトで、次の情報を入力します。

  `# conf ip <interface> <IP address> <Netmask> <Default Gateway>`

  例:`conf ip eth0 192.168.1.100 255.255.255.0 192.168.1.1`

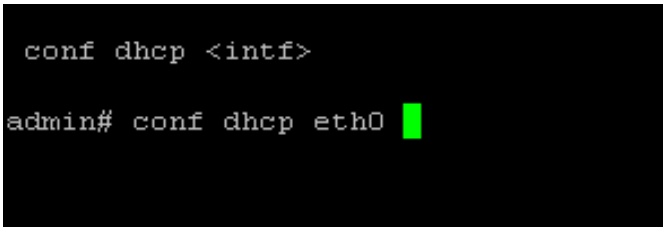


ダイナミック IP アドレスを割り当てるには、**conf dhcp** コマンドを使用します。

- コマンド プロンプトで、次の情報を入力します。

```
#  conf dhcp <interface>
```

例:`conf dhcp eth0`



次のコマンドを実行して DSN サーバを設定します。

```
#  conf dns -a <DNS IP address 1> <DNS IP address 2>
```

プロンプトで次のコマンドを実行し、適切な値を入力してタイムゾーンを設定します。

```
#  timezone
```

NTP サーバとの同期により時間を設定します。プロンプトで Enter を押して、デフォルトの設定を使用することもできます。

```
#  timesync
```

Linux ユーザ ログイン「collectorlogin」を有効にして、有効期限日数を設定します(1 ～ 180)。

```
#  pwdreset collectorlogin 180
```

```
admin# pwdreset collectorlogin 180

Password for 'collectorlogin' reset to - Rtxjrr0+ successfully
Password expires in 180 days
Shell is enabled
passwd: all authentication tokens updated successfully

*** Please memorize the new password ***
Lost passwords cannot be recovered. The only alternative to recover is to reinstall the server.

admin#
```

このパスワードは必ずメモしてください。

Linux root ログインを有効にして、有効期限日数を設定します(1 ～ 180)。

```
#  pwdreset root 180
```

```
admin# pwdreset root 180

Password for 'root' reset to - Kqpbvm4@ successfully
Password expires in 180 days
Shell is enabled
passwd: all authentication tokens updated successfully

*** Please memorize the new password ***
Lost passwords cannot be recovered. The only alternative to recover is to reinstall the server.

admin#
```

このパスワードは必ずメモしてください。

変更した設定を有効にするには、アプライアンスをリブートする必要があります。

- コマンド プロンプトで、次のように入力します。

```
#  reboot
```

画面の質問を確認し、**y** を入力します。

アプライアンスがリブートした後、IP が正しいことを確認します。

- コマンド プロンプトで、次のように入力します。

```
#  show ip
```

- CSPC をリモートで管理できるように、SSH を使用してアプライアンスに接続します。

CSPC 登録

CSPC の登録は、コレクタが Cisco Smart Net Total Care ポータルによって使用される前に実行する必要があります。この登録により、CSPC コレクタとシスコ データセンター間の接続を確立する検証が実施されるようになります。登録プロセスでは、権限付与ファイル（セキュリティ証明書やその他の登録ファイル）を取得する必要があります。これらの登録/権限付与ファイルは、CSPC のインストールを完了するために後で使用されます。

この手順を行うには、Smart Net Total Care ポータルにアクセスし、オンボーディングと登録を終了する必要があります。これを行うには、次のリンクの指示に従ってください。
https://www.cisco.com/web/smartservices/sntc.html

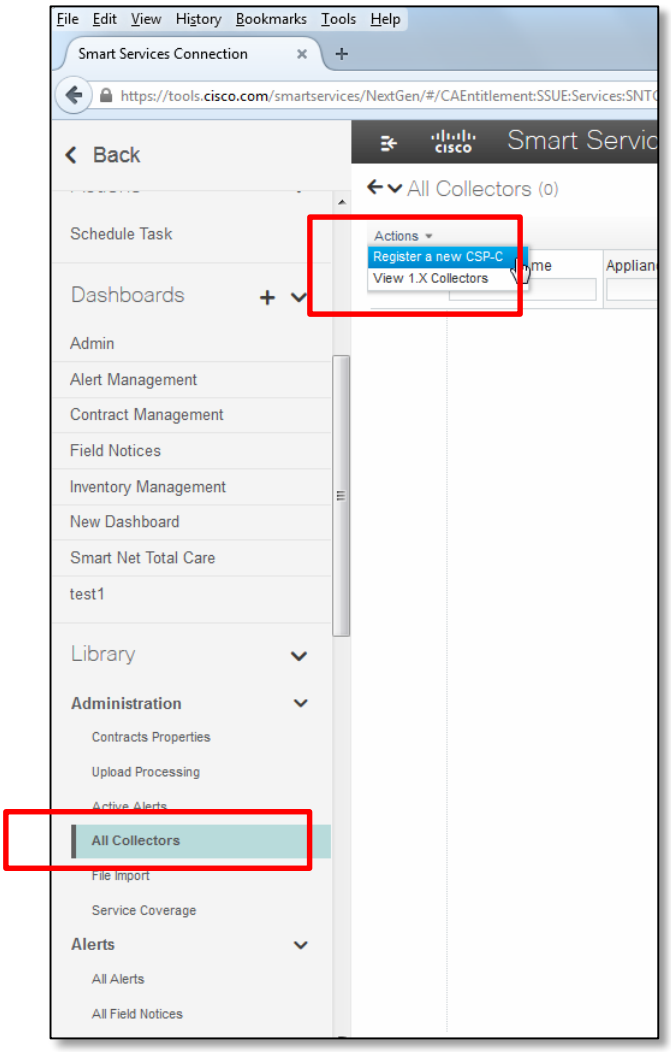
セルフサービスのオンボーディングを完了する方法の詳細については、次のリンクを参照してください。
https://supportforums.cisco.com/document/12566021/new-smart-net-total-care

重要

権限付与ファイルは解凍しないでください。

権限付与ファイルを作成できるのは Smart Net Total Care 顧客管理者だけです。Smart Net Total Care ポータル（https://tools.cisco.com/smartservices/）にログインします。

- 左側のナビゲーション ペインで [ライブラリ（Library）] > [管理（Administration）] > [すべてのコレクタ（All Collectors）] を選択します。
- 表示されるペインで [アクション（Actions）] > [新規 CSPC の登録（Register a New CSPC）] オプションを選択します。



[新規CSPCの登録（Register a New CSPC）] 画面が開きます。

次のように必須フィールドに入力します。

- [CSPC名（CSPC Name）] はサーバのホスト名と一致している必要があります。ネットワーク上でこのコレクタを特定するために使用する任意の名前にできます。
- ドロップダウンリストから貴社名を選択します。これが [権限付与された会社（Entitled Company）] フィールドに設定されます。
- コレクタの［サイトID（Site ID）］に手動で入力できます。このフィールドは、適切と思われる任意の ID にできます。
- ［シリアル番号（Serial Number）］には、http://www.epochconverter.com/ から Unix Epoch 時刻をコピーします。
- [インベントリ名（Inventory Name）] では「ホスト名-インベントリ」形式を使用します。

[送信（Submit）] ボタンをクリックし、zip ファイルをダウンロードするためのダイアログが表示されるまで待ちます。zip ファイルを見つけやすい場所に保存します。このファイルを解凍しないでください。

ソフトウェア アプライアンスへのログイン

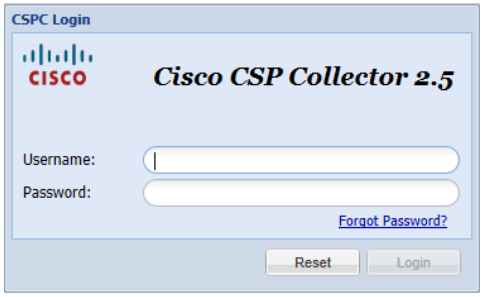
アプライアンスにアクセスするには、ブラウザ ウィンドウを開き、次の手順を実行します。

- アプライアンスにアクセスするには、次の URL 形式を使用します。

  https://<*アプライアンスの IP アドレス*>:8001/

Web サイトのセキュリティ証明書に関する警告や、ブラウザが安全な接続を確認できないことを通知する、セキュリティ証明書に関する警告が表示されます。警告の内容は、使用しているブラウザの種類によって異なります。

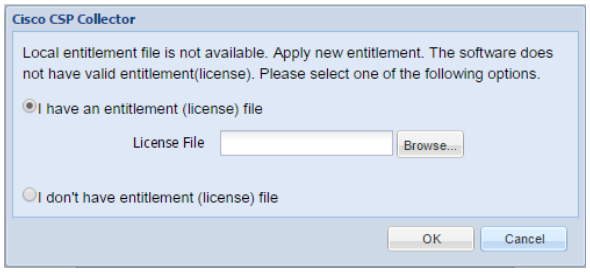
- 警告を確認し、アプライアンスのログインを続行します。



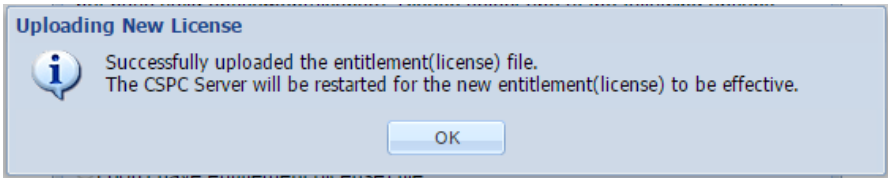
- ログイン情報を入力します。

デフォルトのアプライアンス ユーザ ID/パスワードは、**admin / Admin#123** です。

初めてコレクタにログインする場合、権限付与証明書のインポートを求めるプロンプトが表示されます。この手順が完了するまで、CSPC GUI にはログインできません。次のメッセージが表示されます。

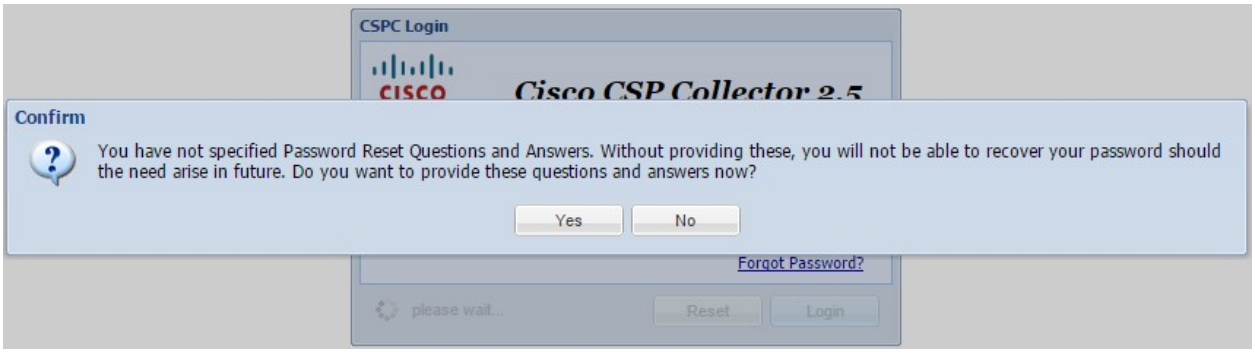


.zip 権限付与ファイルを参照し、[OK] をクリックします。



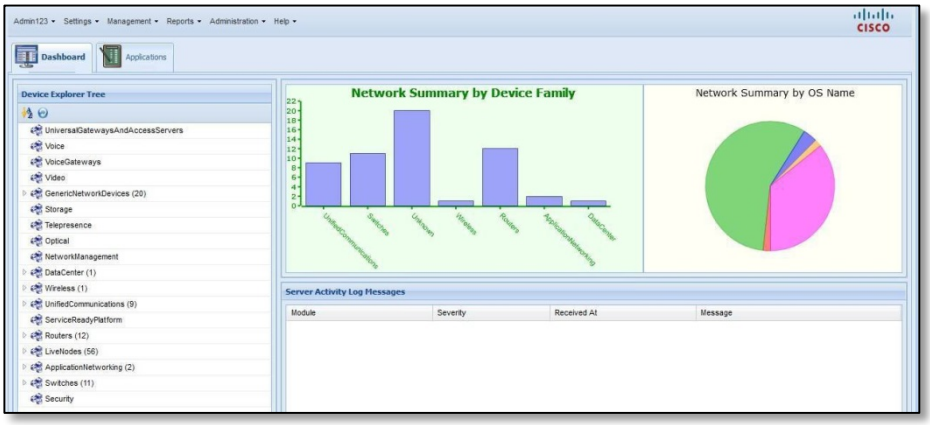
権限付与ファイルをアップロードして[OK]をクリックすると、コレクタがリブートします。再びログインできるようになるまでに、数分かかります。

admin/Admin#123 クレデンシャルを使用して再度ログインします。エンド ユーザ ライセンス契約書が表示されます。内容を確認し、[同意する(I Accept)]をクリックして続行します。パスワード リセットのための質問を求めるプロンプトが表示されます。



- この情報を後で設定する場合は [いいえ(No)] をクリックします。アプライアンスによって、操作用のソフトウェア アイテムがロードされます。

すべてのソフトウェアがロードされると、グラフィカル ユーザ インターフェイス(GUI)が表示されます。



コレクタの動作

コレクタを稼働させるには、次の関連タスクをコレクタで実行しておく必要があります。

- CSPC デバイス クレデンシャルの入力
- デバイスの検出、インベントリの収集およびアップロード

CSPC デバイス クレデンシャルの入力

このセクションでは、デバイスのクレデンシャルを指定する手順について説明します。

ネットワーク デバイスを検出し、デバイス データを収集するには、最初にデバイス クレデンシャルを入力する必要があります。

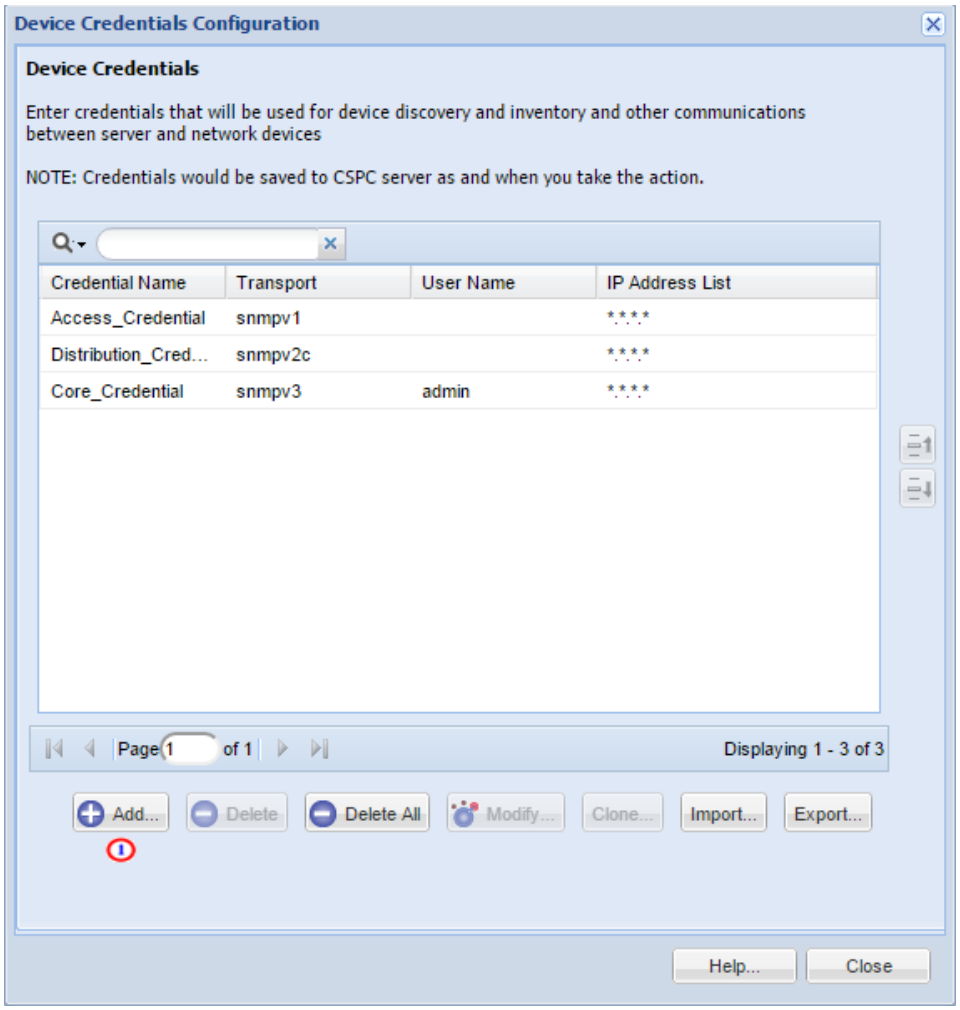
CSPC でのデバイス クレデンシャルのセットアップは、次の 2 つの目的のために行います。

- SNMP クレデンシャルは、デバイスの初期検出とデータ収集に使用されます。
- SNMP に加えて、残りのクレデンシャル（すなわち SSH、HTTP、HTTPS）は、検出されたデバイスからのデータ収集に使用されます。

SNMP プロトコルを使用してデバイス クレデンシャルを設定するには、次の手順を実行します。

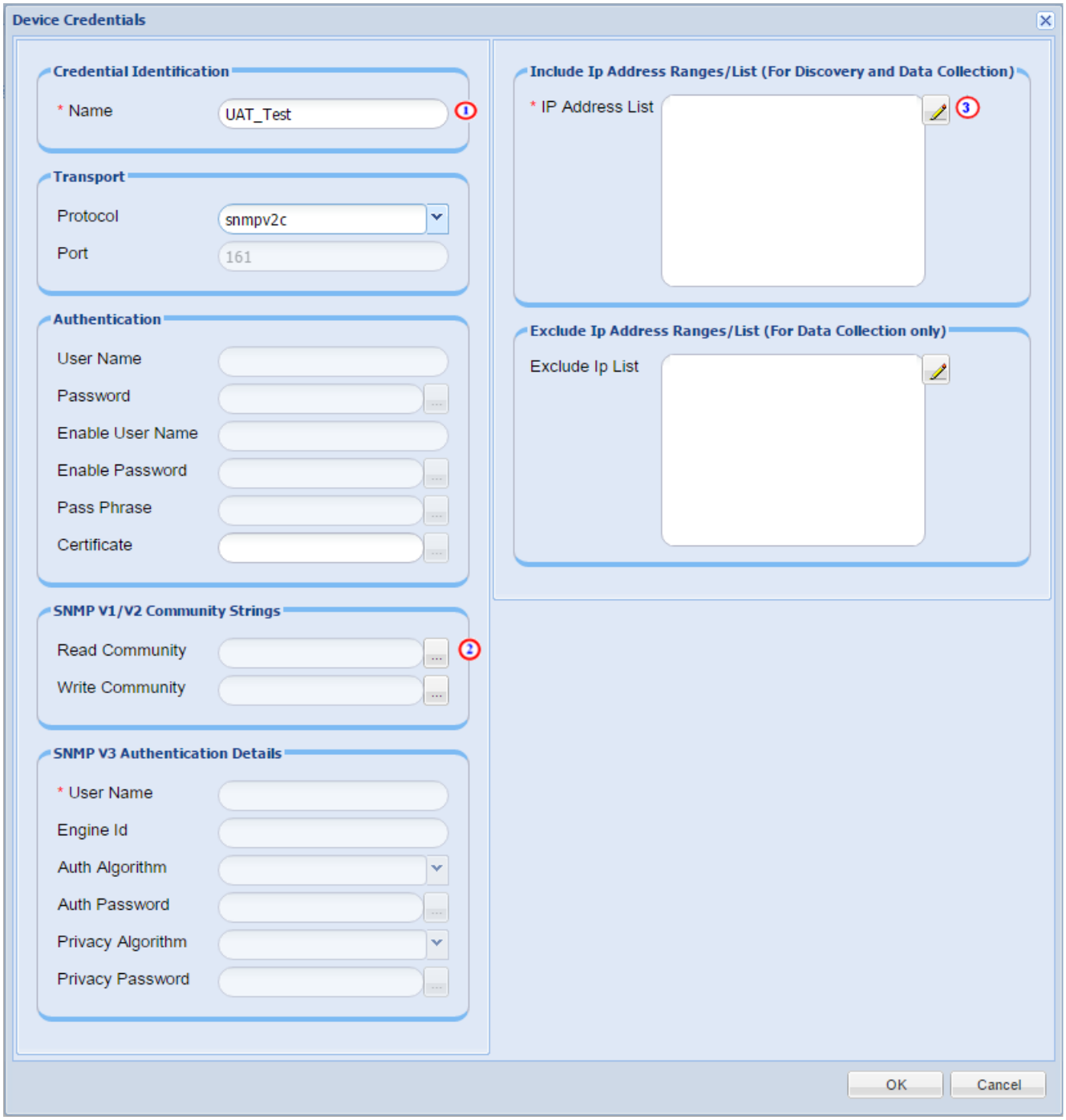
- CSPC メニューで、[設定（Settings）] > [デバイス クレデンシャル（Device Credentials）] を選択します。

[デバイスのクレデンシャルの設定（Device Credential Configuration）] ウィンドウが表示されます。



- [追加（Add）] (1) をクリックします。クレデンシャルが作成されます。

デバイス クレデンシャル ウィンドウが表示されます。ここにはクレデンシャルの ID、認証情報、および SNMP の read コミュニティ ストリングの詳細が表示されます。

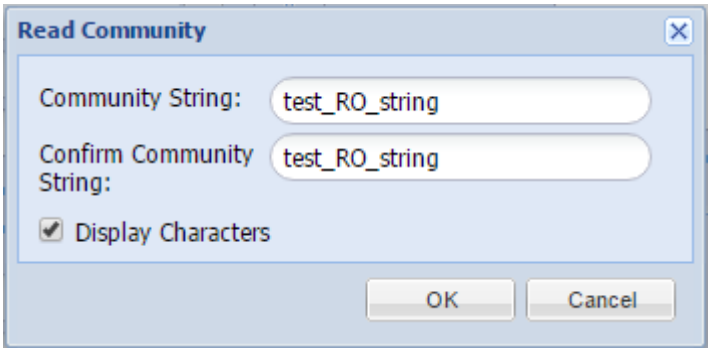


以下の必要なデータを入力します。

- クレデンシャル名（この例では UAT-Test）を入力します。1

クレデンシャル名は選択した任意の名前を使用できますが、作業しているグループまたは地域を示している必要があります。

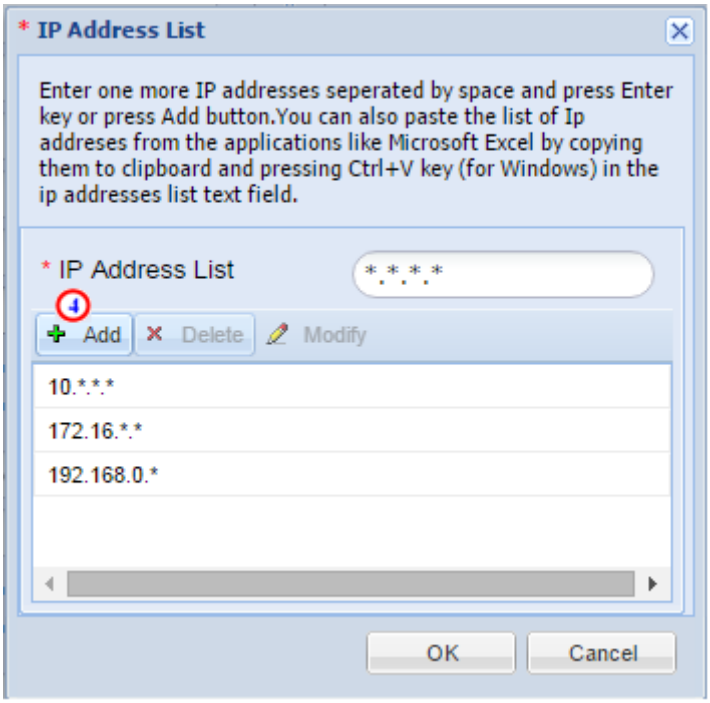
- [通信（Transport）] セクションにある [プロトコル（Protocol）]フィールドのドロップダウン リストをクリックし、SNMP バージョンのストリングを指定します。
- SNMP V1/V2[コミュニティ ストリング（Community Strings）]セクションについては、[…] アイコンをクリックしてそれぞれの読み取りコミュニティ ストリングを入力します。② [Read コミュニティ ストリングの入力（Enter Read Community String）] ウィンドウが表示されます。



- [Read コミュニティ ストリングの入力（Enter Read Community String）] ウィンドウで、read コミュニティ ストリングを入力します。
- 次に [OK] をクリックします。

- デバイス クレデンシャル ウィンドウの[IP アドレス リスト（IP Address List）]フィールドの右にある鉛筆アイコン ③ をクリックして、IP アドレス リストに入力します。
- IP アドレス リストを入力します。

デバイス検出、データ収集に使用する IP アドレスを、指定のデバイスに基づいて定義するには、IP アドレスまたは IP アドレスの範囲が必要です。



- [IPアドレスリスト(IP Address List)]フィールドに IP アドレスを入力した後、[追加(Add)] 4 をクリックします。

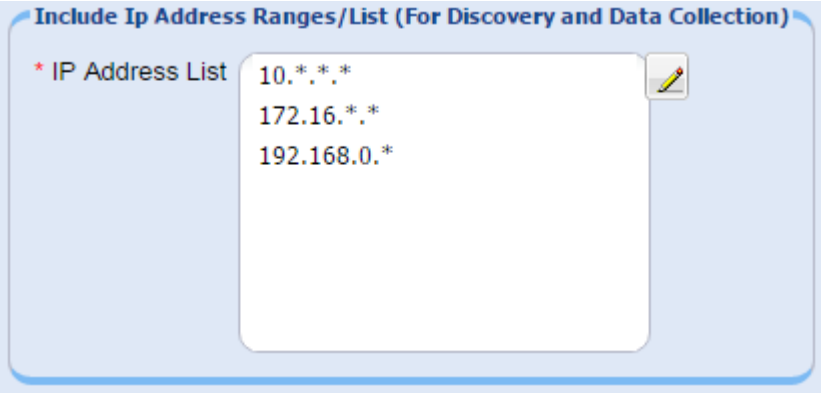
入力したデータが IP アドレス リストに追加されます。

- このリストは、どの IP の CSPC をこのクレデンシャルで使用して、検出やデータ収集などの操作のためにデバイスと通信するかを指定します。
- 特定の IP を指定したり、ワイルドカードを使用して IP のオクテットを置換して範囲を設定することもできます。
- このフィールドに IP も IP 範囲も含めないと、いずれかの IP を使用するデバイスと通信しようとするときに CSPC によってこのクレデンシャルが使用されません。
- 任意の IP のクレデンシャルを使用するために、CSPC では *.*.*.* と入力できます。172.16.*.* と入力すると、172.16.0.0/16 サブネット内のデバイスでのみクレデンシャルの使用が許可されます。

参照される IP アドレスは、すべての必要なデバイスを網羅するとはいえ、可能な限り、厳密または限定的にする必要があります。

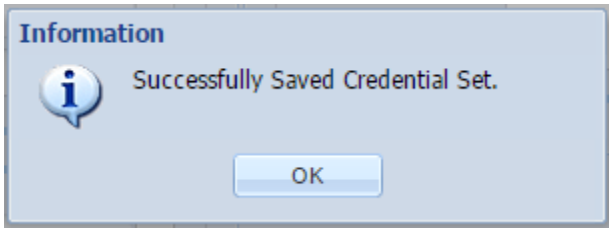
- 前述のデータを入力した後、[OK] をクリックします。

[IPアドレスリスト(IP Address List)]フィールドに新しい IP が表示されます。



- [OK] をクリックします。

保存に成功したことを伝えるメッセージとともに [クレデンシャルの編集（Edit Credentials）] ウィンドウが表示されます。



- [OK] をクリックします。

これでウィンドウが閉じます。

次のステップでは、デバイスの検出、インベントリ、アップロードを実行します。

show コマンドの情報を収集するには、先ほど作成した SNMP クレデンシャルに加えて、Telnet または SSH クレデンシャル（あるいはその両方）を作成する必要があります。前述と同じロジックに従いますが、プロトコルを SSH または Telnet に設定し、SNMP V1/V2 の [コミュニティ ストリング（Community Strings）] セクションではなく、[認証（Authentication）] セクションに該当するユーザ名/パスワードを入力します。

デバイスの検出、インベントリの収集およびアップロード

インベントリのアップロードを実行するには、以下の複数の手順が必要です。

- デバイスの検出
- 収集プロファイルの実行とデータのアップロード

デバイスの検出

このセクションでは、デバイスの検出を実行できる 3 つの方法、およびそれらの検出ジョブの実行方法を示します。

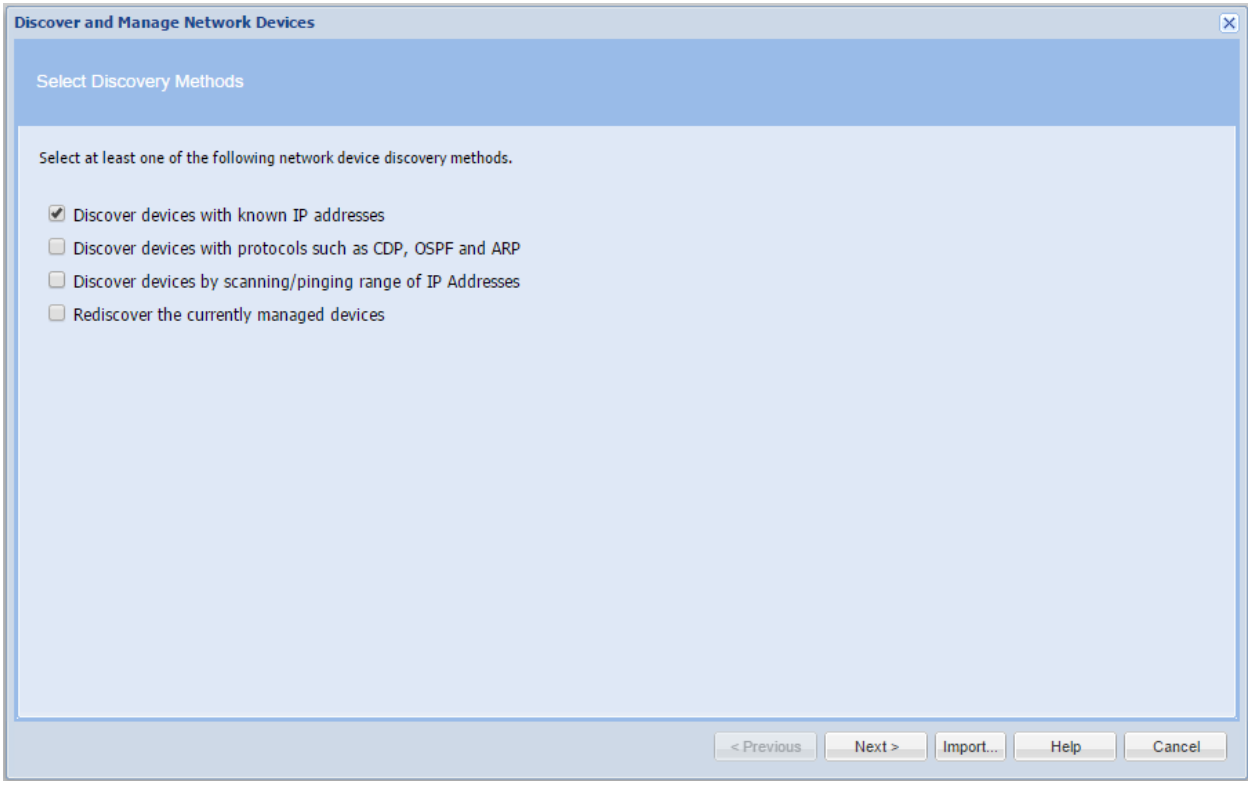
- 既知の IP アドレスを使用したデバイスの検出
- CDP、OSPF、ARP などのプロトコルを使用したデバイスの検出
- IP アドレスの範囲のスキャンおよび Ping によるデバイスの検出
- 検出スケジュールのオプション

3 つの検出オプションのいずれかでデバイスを検出するには、[管理(Management)]>[デバイスの検出と管理(Discover and Manage Devices)]を選択します。

[ネットワーク デバイスの検出と管理(Discover and Manage Network Devices)]ウィンドウが表示されます。

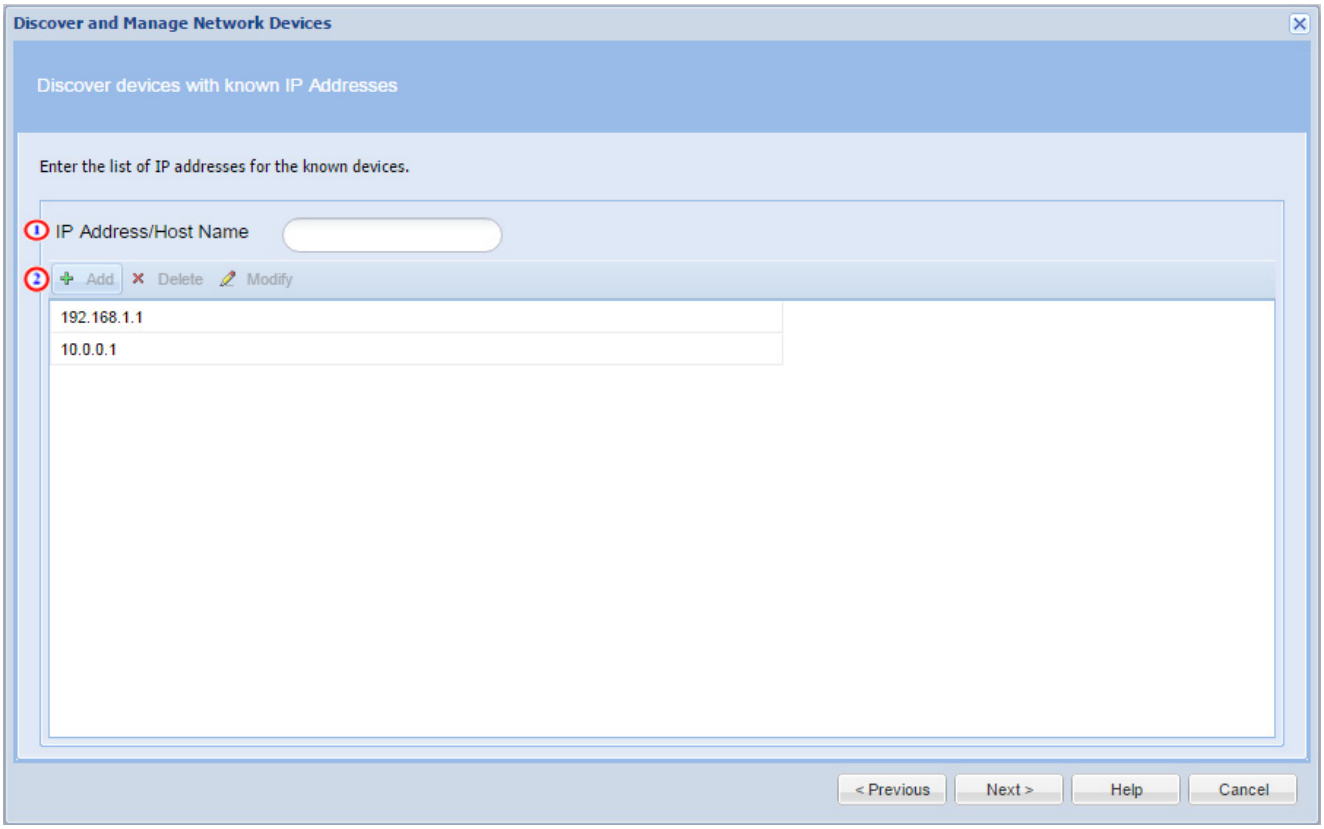
既知の IP アドレスを使用したデバイスの検出

この検出プロセスでは、デバイスの IP アドレスが既に判明している、管理対象ネットワークで使用可能なデバイスが検出されます。こうしたデバイスを検出するには、次の手順を実行します。



- 検出に使用する方法を選択します。
- [次へ(Next)] をクリックします。

選択した方法に関連するペインが表示されます。



- ネットワークから検出するデバイスの IP アドレスを入力します。[IPアドレス/ホスト名（IP Address/Host Name）]フィールド ① に IP アドレスを入力し、[+追加（+ Add）] ② をクリックするか、Enter キーを押します。

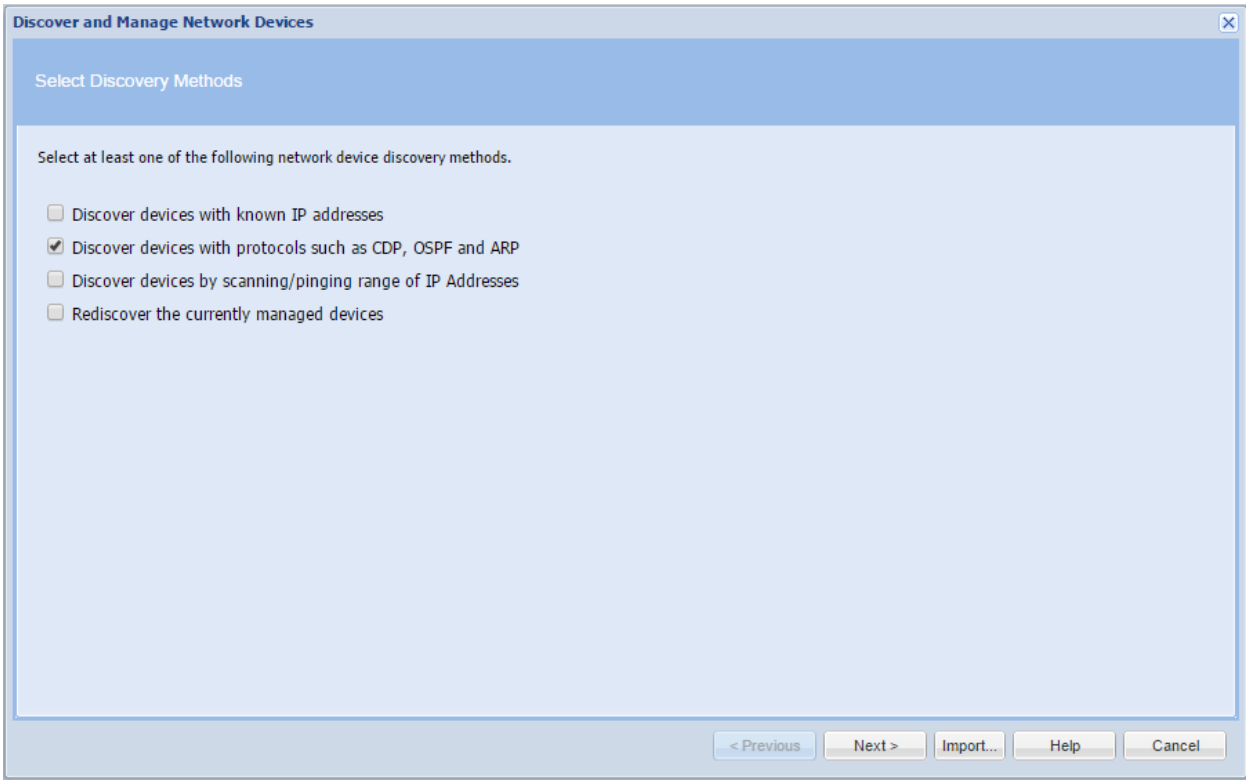
IP アドレスが[IPアドレスリスト（IP Address List）]に追加されます。

同時に複数の IP を追加できます。その場合には、[IPアドレス/ホスト名（IP Address Host Name）]フィールド ① に入力する IP をスペースで区切ります。

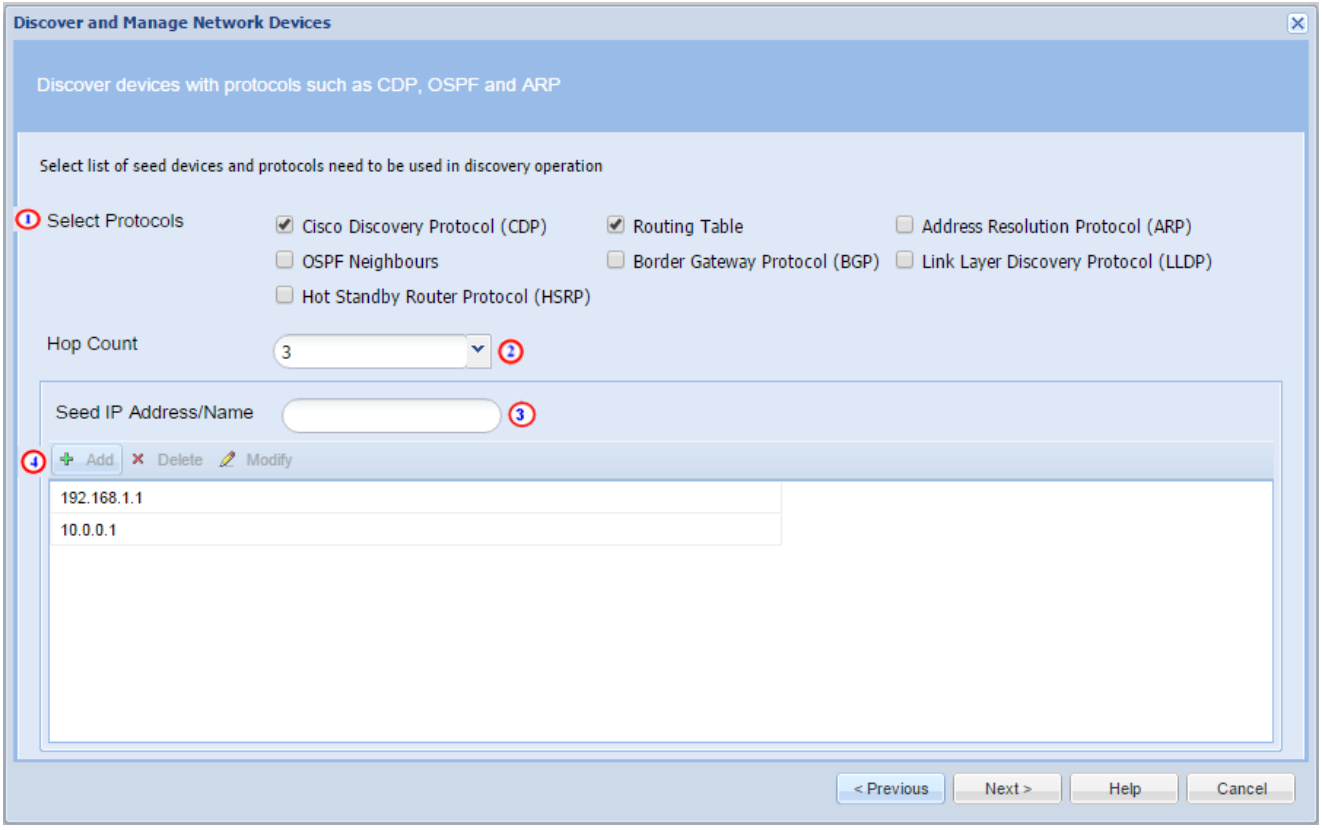
- [次へ（Next）]をクリックして、検出スケジュールのオプションに進みます。

CDP、OSPF、ARP などのプロトコルを使用したデバイスの検出

Cisco Discovery Protocol（CDP）、Address Resolution Protocol（ARP）などのプロトコル テーブルを使用して、ネットワーク デバイスを検出します。検出されたデバイスから収集されたデータは、ネットワーク内に追加されたデバイスを見つけるために使用されます。



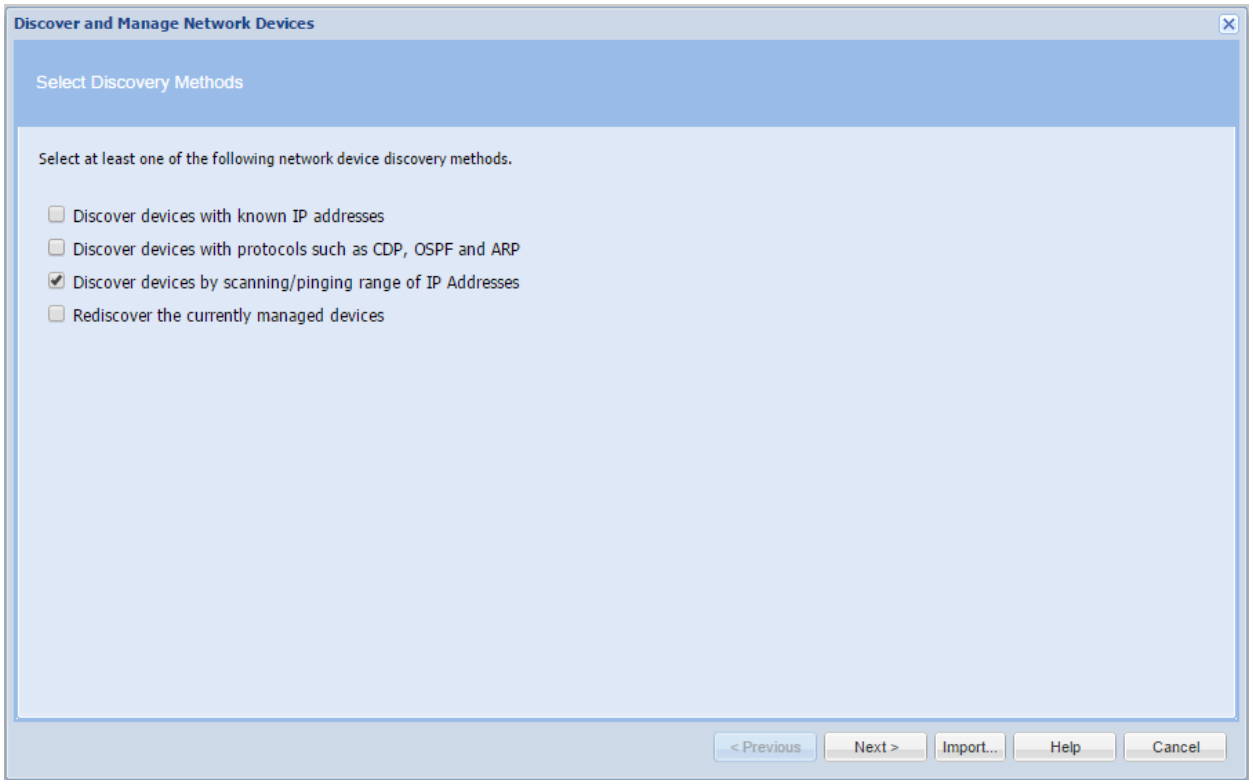
- [CDP、OSPF、ARPなどのプロトコルを使用したデバイスの検出（Discover devices with protocols such as CDP, OSPF and ARP）]を選択します。
- [次へ（Next）] をクリックします。



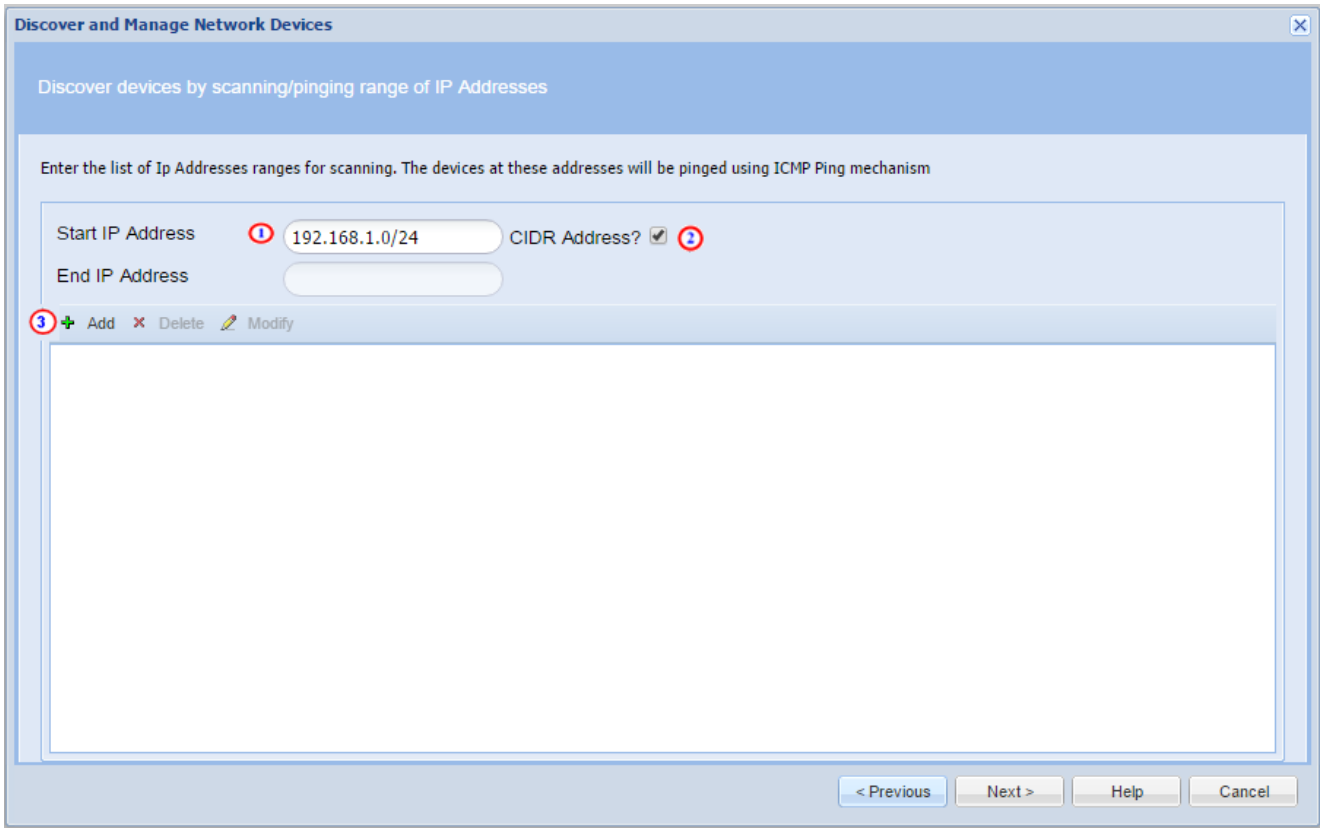
- CSPC で使用するプロトコルの隣にあるボックスをクリックして、プロトコルの選択を行います。コレクタはデバイス内の対応するテーブルを調べて、これらのテーブル内のデバイスの IP アドレスの検出を行います。①
- CSPS がシード デバイスを超えて到達するホップカウント値 ② を指定します。
- シード デバイスの IP アドレス ③ を入力し、[+追加(+Add)] ④ をクリックしてシード デバイス リストに追加します。
- [次へ(Next)]をクリックして、検出スケジュールのオプションに進みます。

IP アドレスの範囲のスキャンおよび Ping によるデバイスの検出

この方法では、ユーザが指定した範囲内のすべての IP アドレスを SNMP を使用して収集します。範囲の開始 IP アドレスと終了 IP アドレスを提供するか、CIDR 表記を使用して特定のサブネットを指定します。



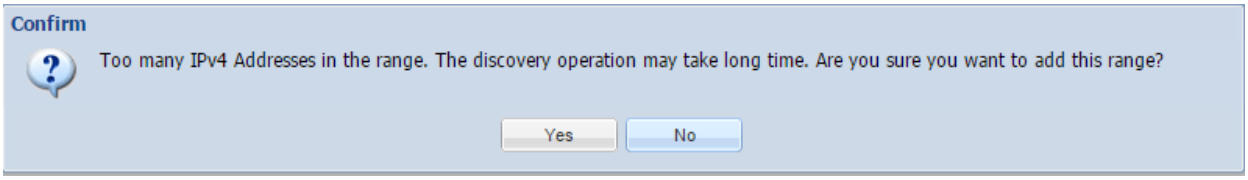
- [IPアドレスの範囲のスキャンおよびPingによるデバイスの検出(Discover Devices by scanning/pinging range of IP Addresses)]を選択します。
- [次へ(Next)] をクリックします。



範囲の正確な開始 IP アドレスと終了 IP アドレスを指定するか、対応する CIDR 表記を使用してネットワーク アドレスを入力して、範囲を指定できます。
この例では、CIDR オプションが強調表示されています。

- [開始IPアドレス(Start IP Address)]フィールド (1) に適切なネットワーク アドレス、スラッシュ(/)、該当するネットワーク ビット数の順で入力します。次に、[CIDRアドレス(CIDR アドレス)]ボックス (2) をクリックして、[+追加(+Add)] (3) を押します。

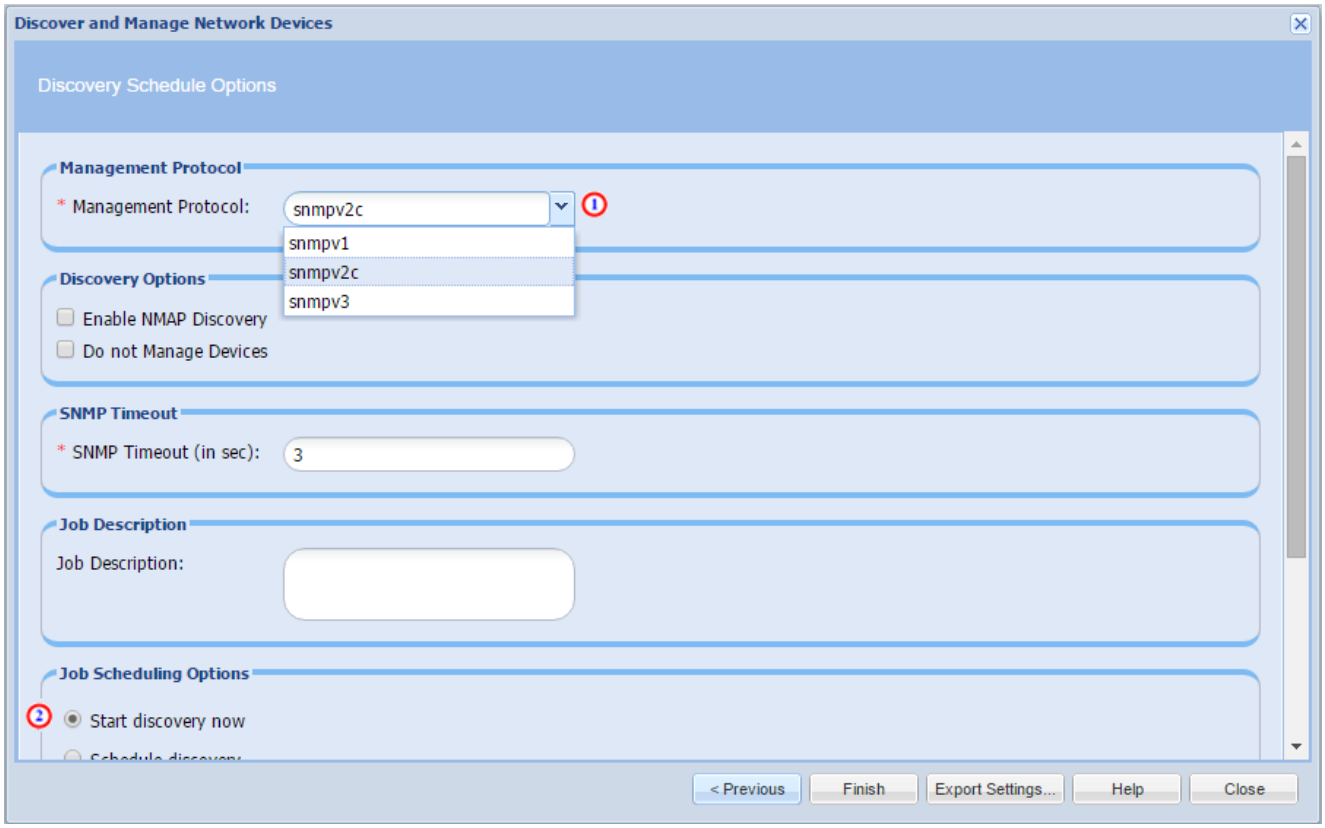
255 アドレスを超える範囲のアドレスの場合、次のポップアップ メッセージが表示されます。これは、検出ジョブの完了に時間がかかる可能性があることを知らせるメッセージです。



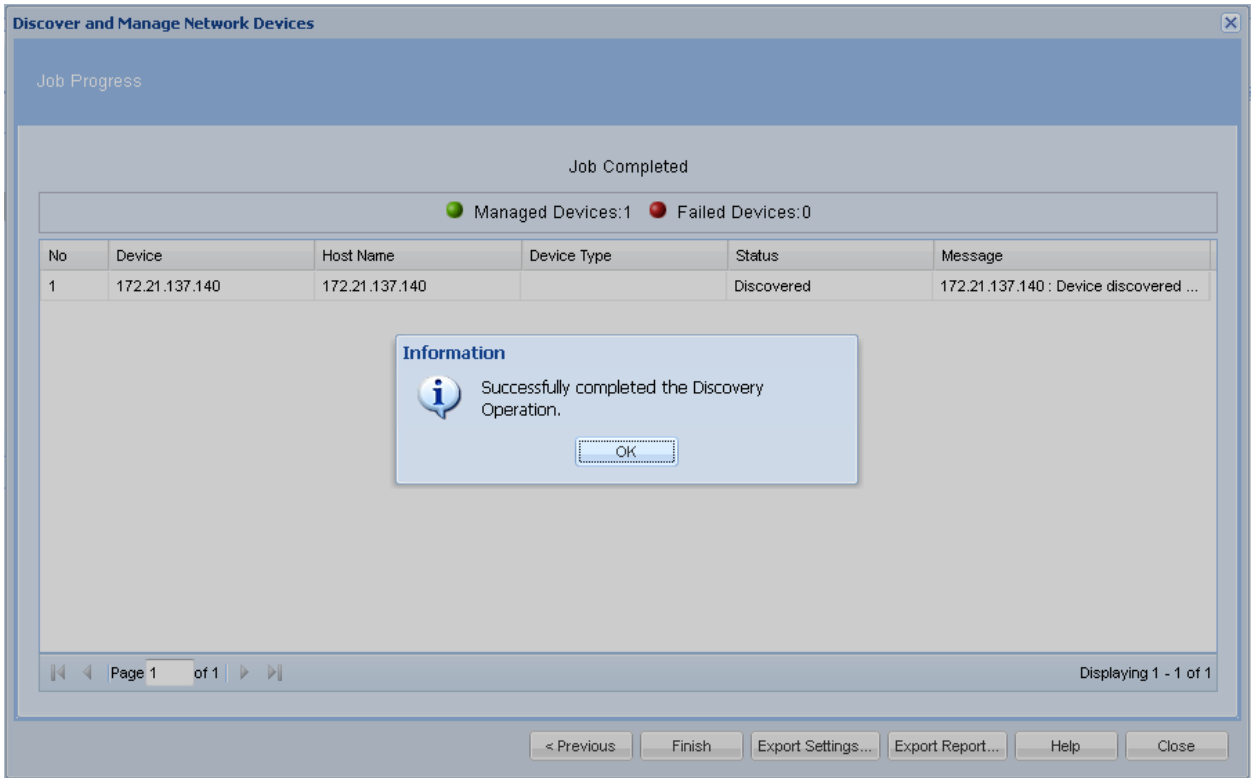
- [はい(Yes)]をクリックして続行します。

検出スケジュールのオプション

前述の 3 つの検出オプションのいずれかを選択し、IP アドレスまたは IP アドレスの範囲を設定した後、検出をすぐに実行するのか、将来のある時点で実行するのかを決定します。



- [管理プロトコル(Management Protocol)]で、使用しているデバイス クレデンシャルに対応する SNMP のバージョンを選択します。①
- すぐに検出を実行するか、将来行うためにスケジュール設定するかを決定します。② この例では、すぐに検出するオプションを選択します。
- [完了(Finish)] をクリックし、検出ジョブを実行します。



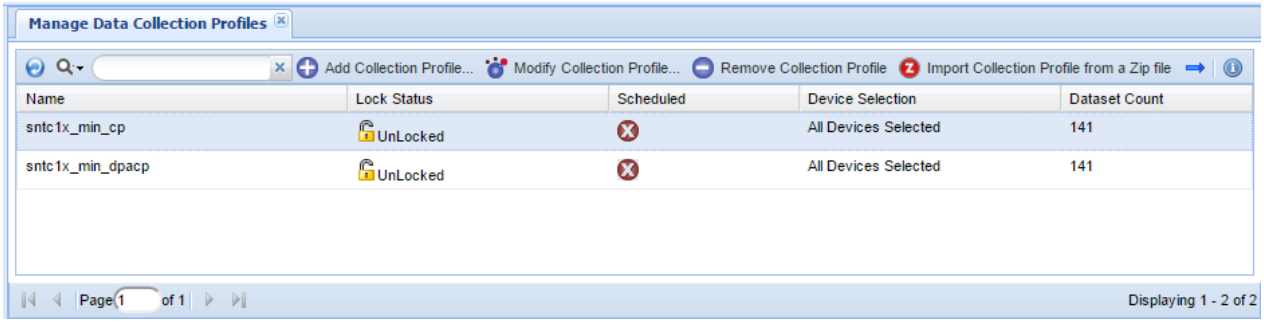
前述の手順を実行後、[正常に検出操作が完了しました(Successfully completed the Discovery Operation)] というメッセージが表示されます。

- [OK] をクリックします。

収集プロファイルの実行とデータのアップロード

次のステップを実行すると、収集プロファイルをセットアップできます。このプロファイルを使用すると、CSPC で関連デバイス データを収集したり、完了時にシスコ データセンターに対するアップロードを開始したりできます。

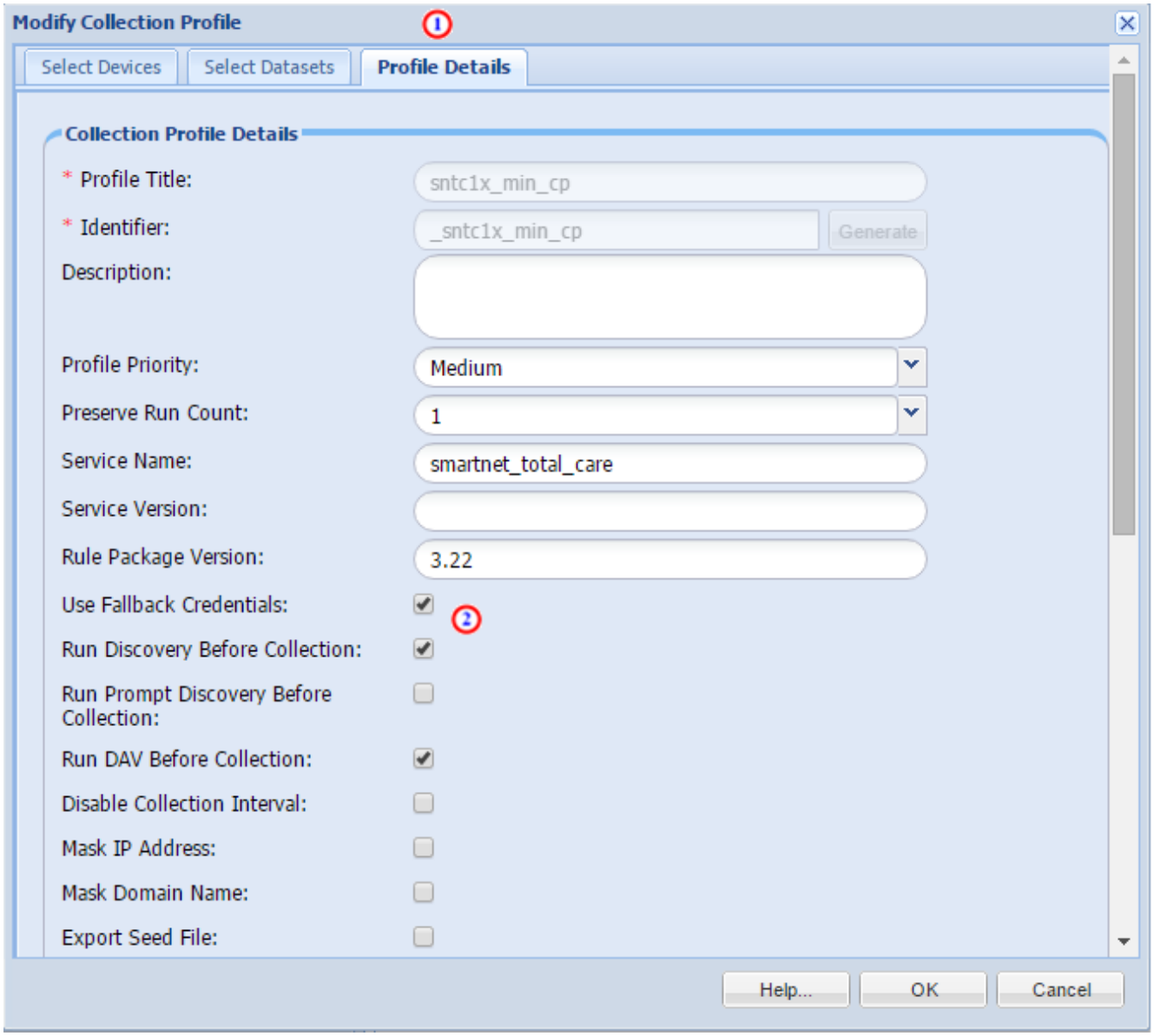
- 収集プロファイルを管理するには、[設定(Settings)]→[データ収集プロファイルの管理... (Manage Data Collection Profiles...)]と進みます。



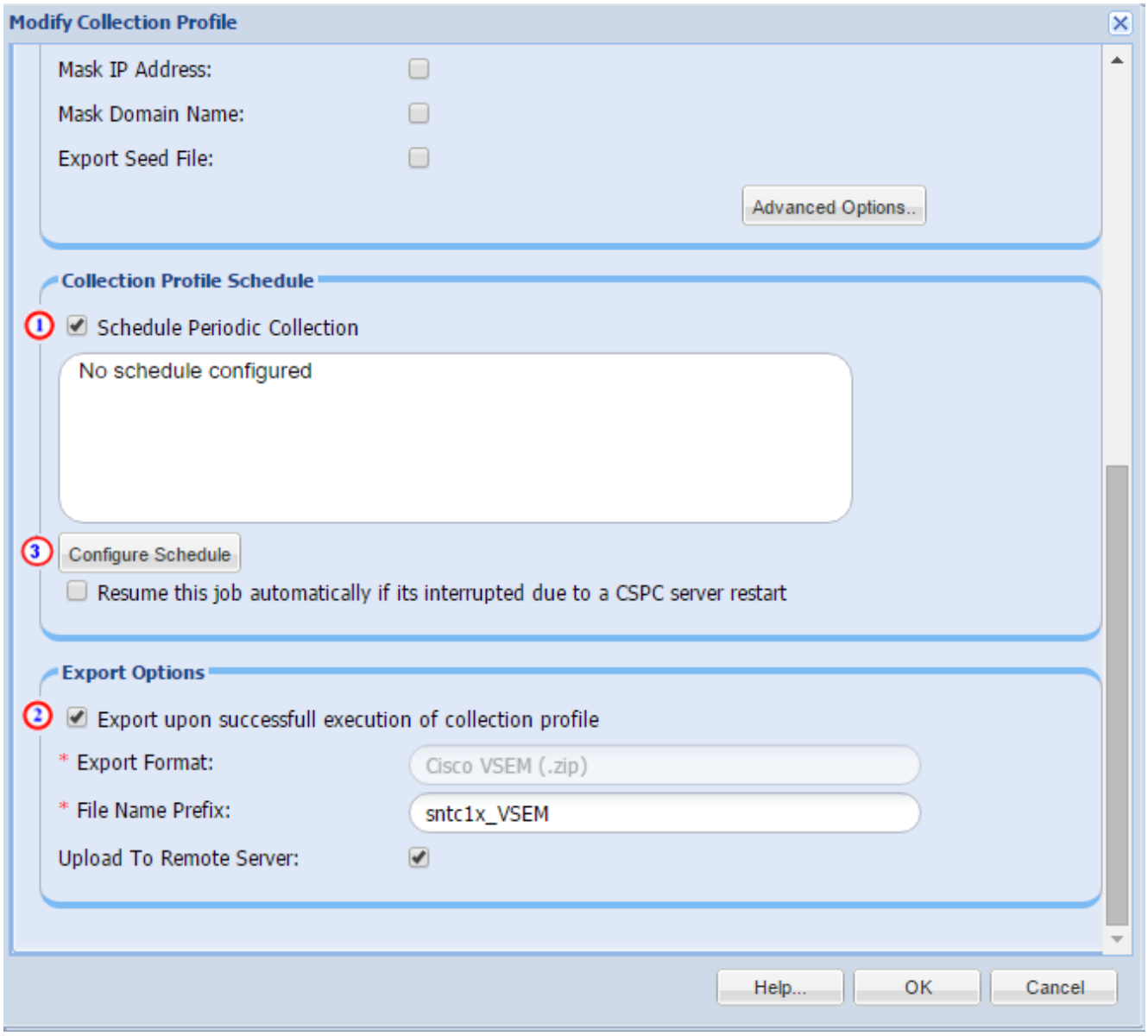
- 収集プロファイル **sntc 1x_min_cp** をダブルクリックします。

[収集プロファイルの変更(Modify Collection Profile)]ウィンドウが表示されます。

CSPC アプライアンスには、最小限の収集プロファイルがバンドルされています。最小限の収集プロファイルには、各インベントリ収集/アップロードのために処理する必要のある必須収集コマンドの最小限のセットが含まれています。



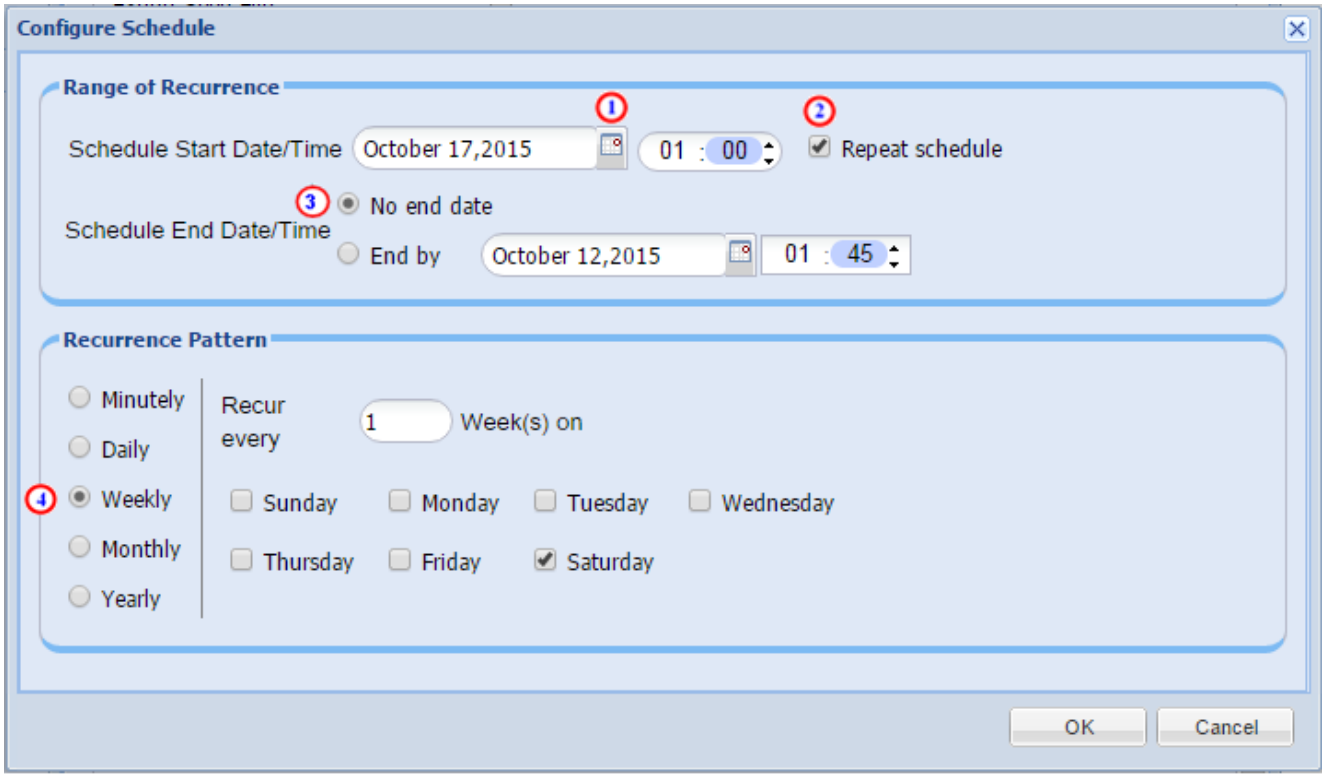
- [プロファイルの詳細(Profile Details)] タブ 1 をクリックしてから、[フォールバッククレデンシャルの使用(Use Fallback Credentials)]、[収集の前に検出を実行(Run Discovery Before Collection)]、[収集の前に DAV を実行(Run DAV Before Collection)]の各ボックスを選択します。2



- ウィンドウ下部までスクロールし、[定期的収集をスケジュール設定（Schedule Periodic Collection）] ① と、[収集プロファイルの実行が正常に行われた後にエクスポート（Export upon successful execution of collection profile）] ② の両方のボックスを選択します。

[収集プロファイルが正常に行われた後にエクスポート（Export upon successful execution of collection profile）] チェックボックスを選択すると、アップロードが有効になります。このチェックボックスを選択すると、収集完了後、CSPC によって、収集プロファイルから収集されたデータがシスコにアップロードされます。

- [スケジュールの設定（Configure Schedule）] ③ をクリックし、[スケジュールの設定（Configure Schedule）] 画面に進みます。



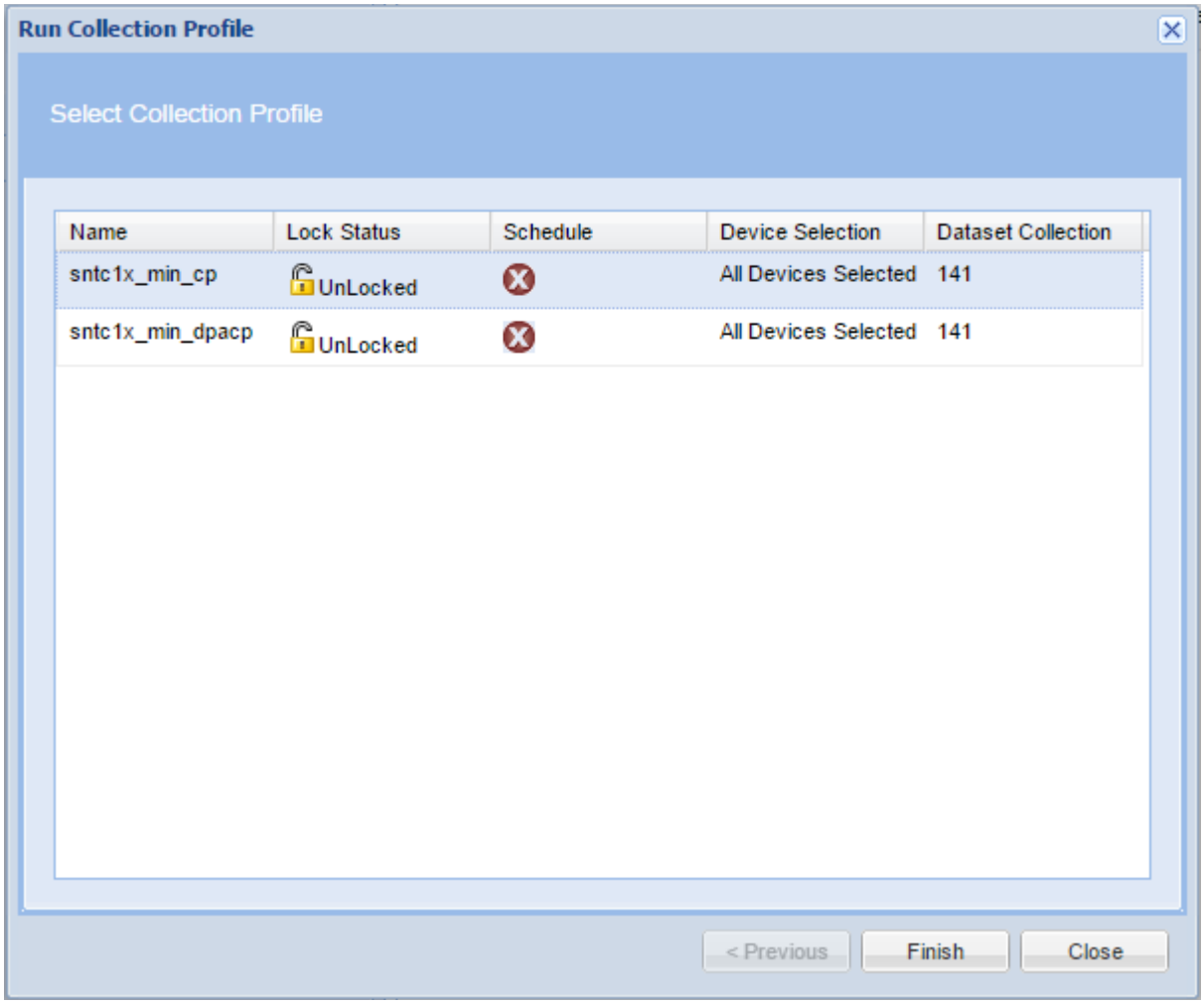
- カレンダー アイコンをクリックして、最初の収集の日付を選択します。①
- カレンダーが表示されるので、日付を選択します。

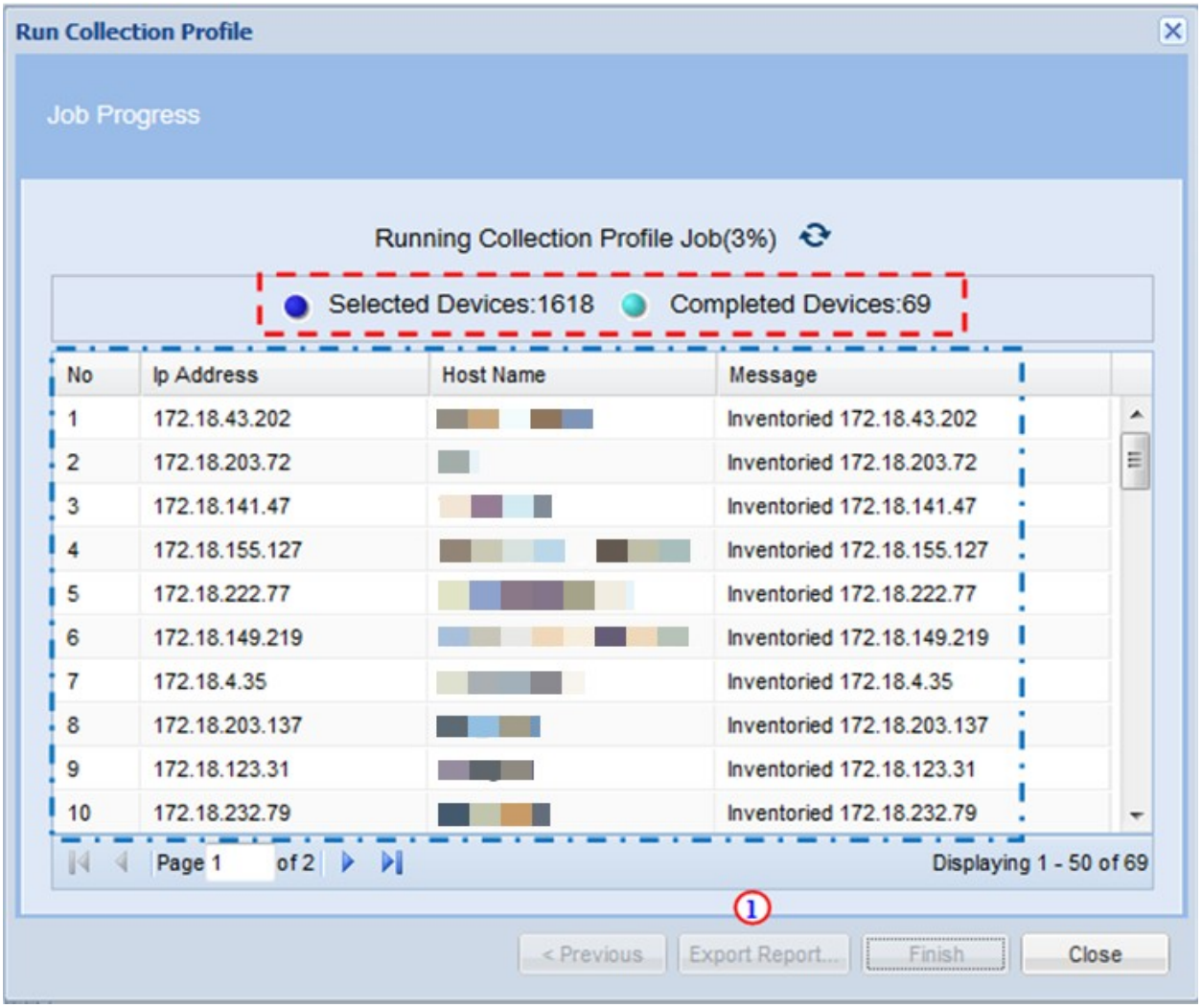
日付を選択すると、[スケジュールの設定（Configure Schedule）] ウィンドウに切り替わります。

- 収集を行う時刻を入力します。
- [スケジュールを繰り返す（Repeat schedule）] ② ボックスを選択します。
- 次に、[終了日なし（No end date）] ボタンを選択します。③
- [反復パターン（Recurrence Pattern）]を選択します。④
- [OK] をクリックして変更を保存し、[収集プロファイルの変更（Modify Collection Profile）]ウィンドウに戻ります。
- [OK]をクリックし、[収集プロファイルの変更（Modify Collection Profile）]ウィンドウを閉じます。

収集は指定した日時に行われます。

オンデマンド収集を実行する場合には、[管理（Management）]→[収集プロファイルの実行（Run Collection Profile）]と移動し、sntc1x_min_cp を選択してから [終了（Finish）] をクリックします。次のスクリーン ショットを参照してください。


Run Collection Profile
Select Collection Profile
Name
Lock Status
Schedule
Device Selection
Dataset Collection
sntc1x_min_cp
UnLocked
All Devices Selected
141
sntc1x_min_dpacp
UnLocked
All Devices Selected
141
< Previous
Finish
Close



データ収集の詳細が入力されています。概要は上、詳細は下に表示されます。

- 収集プロセスの完了後、前述のレポートは、[レポートのエクスポート（Export Report)…]ボタン ① をクリックしてエクスポートできます。
- 収集が終了した時点で、または収集をバックグラウンドで実行するときに[閉じる(Close)] をクリックします。

収集ジョブが完了すると、シスコ データセンターにアップロードされます。アップロードがポータルで処理されるまでには、最大で 24 時間かかる場合があります。

https://tools.cisco.com/smartservices にアクセスし、[ライブラリ(Library)]→[管理(Management)]→[アップロード処理(Upload Processing)]の順にクリックすると、アップロード状況を確認できます。