Cisco Common Services Platform Collector ユーザ ガイド

バージョン 2.7
2017 年 3 月

Text Part Number:

Cisco Common Services Platform Collector ユーザ ガイド

目次

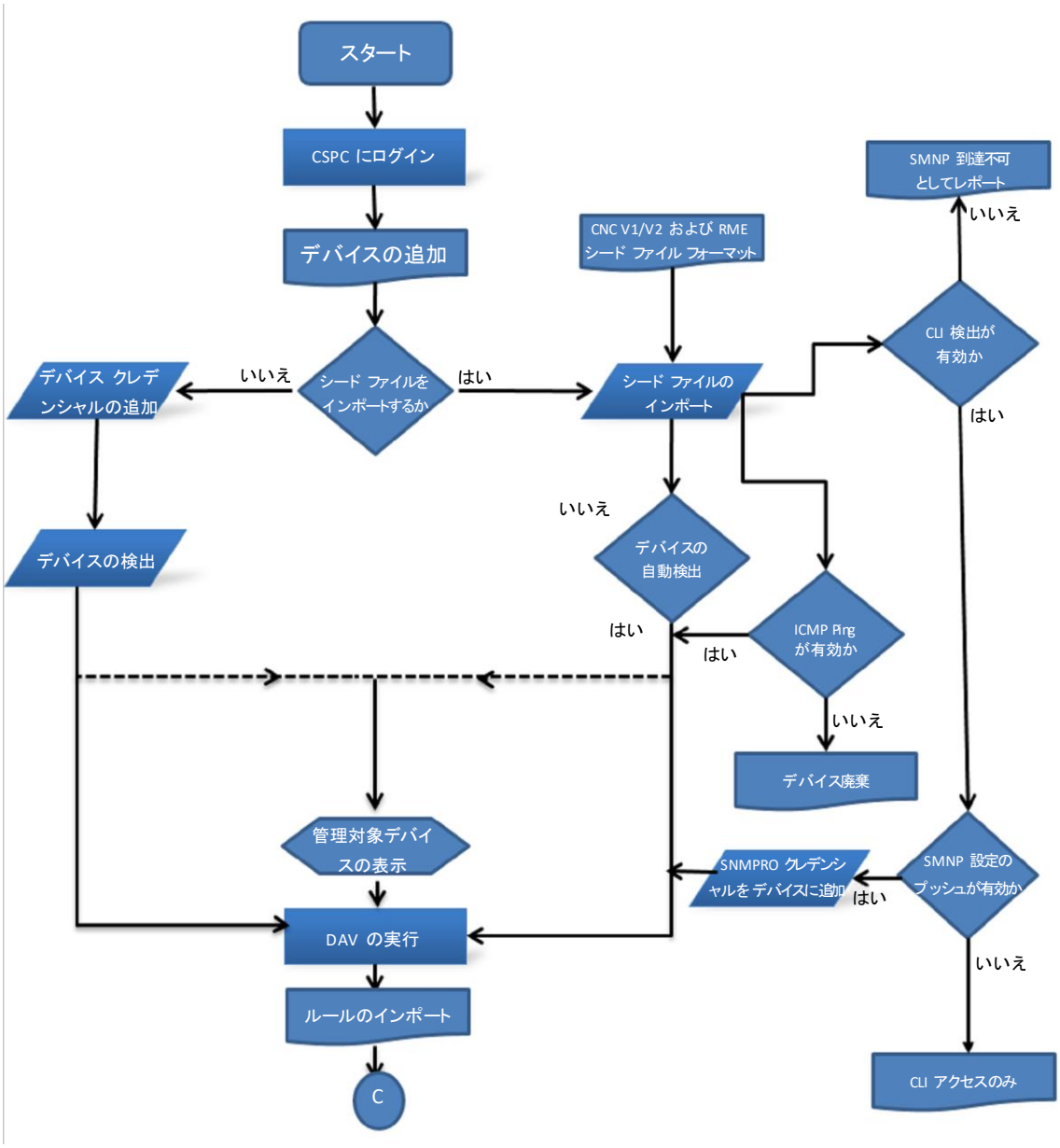
付録 F

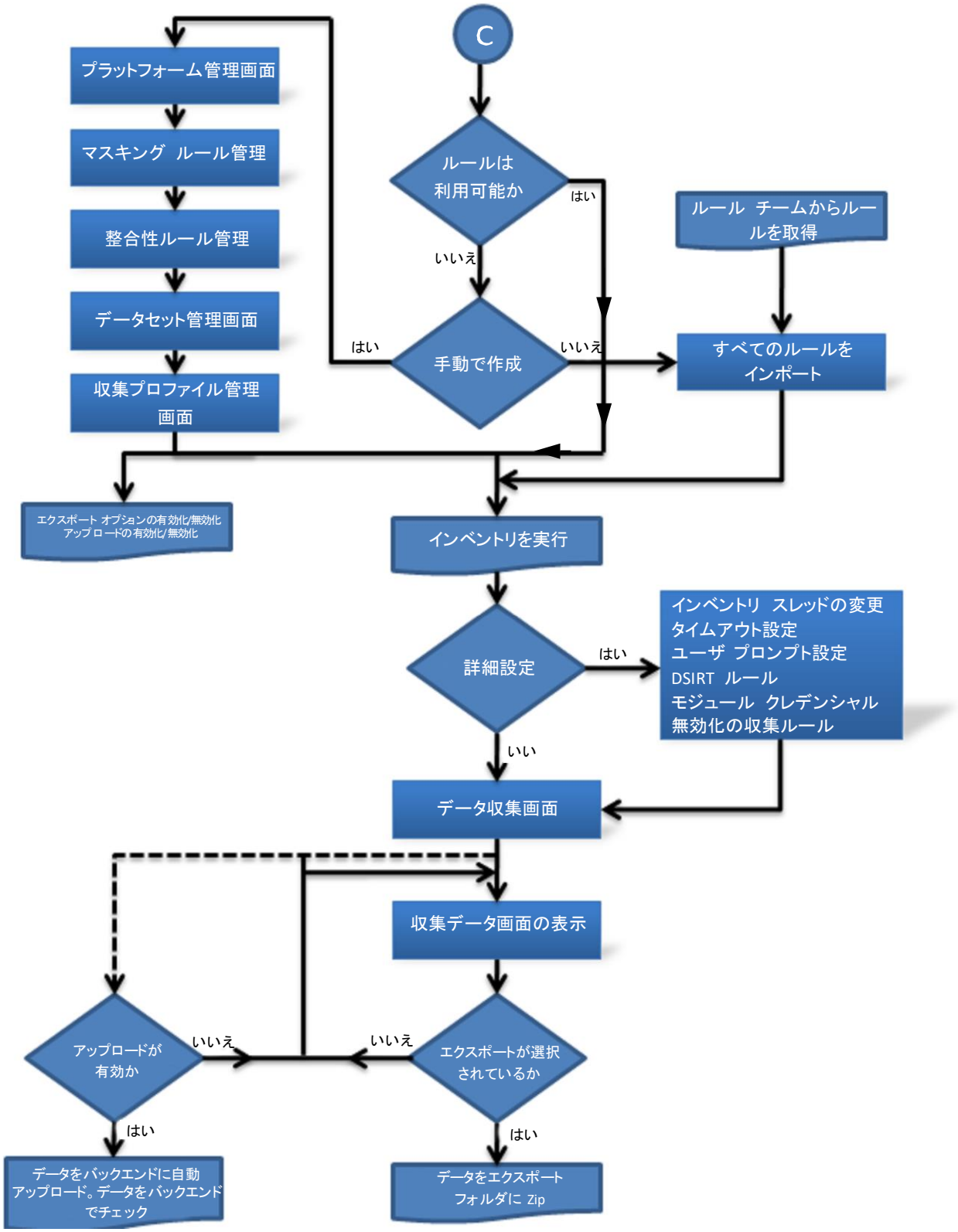
付録 G

付録 H

1

CSPC フローチャート




C
プラットフォーム管理画面
マスキング ルール管理
整合性ルール管理
データセット管理画面
収集プロファイル管理画面
ルールは利用可能か
はい
いいえ
手動で作成
はい
いいえ
ルール チームからルールを取得
すべてのルールをインポート
エクスポート オプションの有効化/無効化
アップロードの有効化/無効化
インベントリを実行
詳細設定
はい
インベントリ スレッドの変更
タイムアウト設定
ユーザ プロンプト設定
DSIRT ルール
モジュール クレデンシャル
無効化の収集ルール
いい
データ収集画面
収集データ画面の表示
アップロードが有効か
いいえ
いいえ
エクスポートが選択されているか
はい
はい
データをバックエンドに自動アップロード。データをバックエンドでチェック
データをエクスポートフォルダに Zip

2

はじめに

CSPC 収集プラットフォーム ソフトウェアの概要

CSPC 収集プラットフォーム ソフトウェアは、カスタマー ネットワーク情報のさまざまな側面を収集するための広範な収集メカニズムとして機能します。CSPC は検出されたデバイスに接続し、ネットワーク管理者やネットワーク エンジニアにネットワーク情報を提供します。CSPC によって収集されたデータはネットワーク管理アプリケーションによって使用され、ハードウェアとソフトウェア双方の詳細なレポート（インベントリ レポートなど）および分析が提供されます。

このユーザ ガイドでは、CSPC ソフトウェア バージョン 2.7 の使用方法について説明します。プログラムの更新、重要な注意事項、イメージの場所などの情報については、『**CSPC Release Notes（CSPC リリース ノート）**』を参照してください。

このガイドの対象ユーザ

このガイドは、ルータ、スイッチ、ファイアウォール、ワイヤレス デバイス、侵入防御システムなどのネットワーク デバイスで構成される異種ネットワークの情報を収集する、ネットワーク管理者、セキュリティ管理者、およびシスコ ネットワーク エンジニアを対象としています。

ネットワークの基本、接続性、ネットワーク デバイスの設定、およびネットワーク上で実行する管理タスクを理解している必要があります。

このガイドについて

『*CSPC ユーザ ガイド*』では、CSPC ユーザ インターフェイスで利用可能なすべての機能を説明します。

CSPC コレクタへのアクセス

CSPC 2.7 は Web ベースのアプリケーションで、URL からアクセスします。

注　推奨されるブラウザは、Microsoft Internet Explorer 9.0 ～ 11.0、および Mozilla Firefox 27 ～ 49 です。

CSPC アプリケーションにアクセスするには、以下の手順に従います。

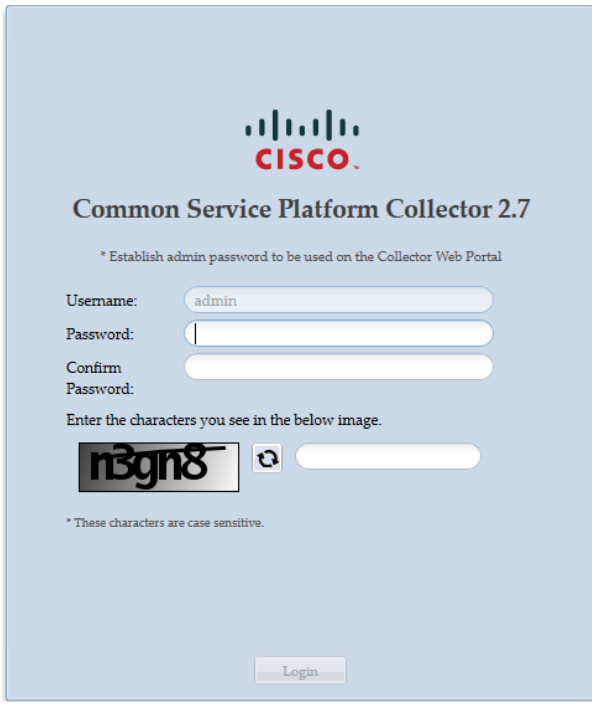
ステップ 1　Web ブラウザで次の URL を開きます。

https://<cspc-server-ip>:8001/cspcgxt

注
- 上記の URL の cspc-server-ip は、CSPC がインストールされているマシンの IP アドレスです。
- 上記の URL にアクセスすると、Web サイトのセキュリティ証明書メッセージを示す証明書エラーが表示されます。[続行（Continue）] をクリックしてこの Web サイト リンクにアクセスするか、SSL 証明書をアップロードしてログインに進みます。「有効な SSL 証明書のアップロード」を参照してください。
- デフォルトのユーザ名を使用できます。デフォルトのユーザ名は **admin** です。最初のログインでパスワードを設定します。
- ユーザ アカウントのパスワードは、3 ～ 12 ヵ月で有効期限切れになります。デフォルトは 6 ヵ月です。パスワードの最長リセット期間は 12 ヵ月です。
- 失敗したログインはすべて検出され、監査されます。
- ユーザ パスワードの入力失敗回数は、ユーザ アカウントまたは IP アドレスがロックされるまでに試行できる回数で、デフォルト値は 5 回です。
- [ロックアウト リセット期間（Lockout Reset Duration）] 属性で指定された時間内にログインを複数回失敗した場合にユーザ アカウントまたは IP アドレスがロックされアクセス不可のままとなる時間（分）のデフォルト値は 60 分です。
- 無効なログイン試行によりユーザ アカウントをロックする場合、その試行は特定の時間枠内で行われる必要があり、そのデフォルト値は 5 分です。

ステップ 2　admin ユーザのパスワードを設定し、イメージの文字を入力します。これは初めてログインする場合だけで、次のような画面が表示されます。

図 2-1　　パスワードの設定



パスワードにおける推奨事項

パスワードの作成

- すべてのパスワード、パスフレーズ、および PIN（「パスワード」）は、パスワード構成基準に準拠する必要があります。
- ユーザは、シスコのアカウントとシスコ以外のアクセス用に同じパスワードを使用してはなりません（たとえば、シスコのアカウントと、シスコ以外のアクセス用（個人のアカウント、オプション取引、銀行取引など）に同じパスワードを使用してはなりません）。ユーザは、クラウド サービス プロバイダーなどの外部の場所にシスコ アカウントのパスワードを保存してはなりません（たとえば、個人の銀行取引、電子メール、ソーシャル メディアなど）。
- グループ メンバーシップやプログラム（「Sudo」など）を通じて付与されたシステムレベルの特権を使用する管理用のアカウントには、システムレベルの特権にアクセスするそのユーザが保有する他のどのアカウントとも異なるパスワードを設定する必要があります。

パスワードの変更

- すべてのユーザレベルのパスワード（CSPC UI、SSH、CLI など）は、少なくとも 6 ヵ月ごとに変更する必要があります。
- すべてのシステムレベル パスワード（特権を持つ管理者アカウント、または特権を持った管理者としてアクセス可能なユーザレベルのアカウント）は少なくとも 90 日ごとに変更する必要があります。

- すべての本稼働システムレベルのパスワードは、企業情報セキュリティによって管理されるグローバル パスワード管理データベースに格納する必要があります。
- 定期スキャンや不定期スキャン時に推測または解読されたパスワードは、このポリシーを遵守するように変更する必要があります。

パスワード保護

- パスワードは、管理アシスタント、マネージャ、同僚、家族を含め、誰とも共有してはなりません。すべてのパスワードは、シスコの社外秘データに分類し、データ保護基準に従って処理する必要があります。
- システム、アプリケーション、デバイス、およびサービスにおいて、クリア テキストや簡単に復元できる形式でパスワードを格納したり、送信したりしてはなりません。
- 電子メール メッセージ、サポート ケース、またはその他の形式の電子的なコミュニケーションにパスワードを含めてはなりません。
- パスワードを書き留めてオフィス内に保管することは避けてください。コンピューティング デバイス、携帯電話、タブレットなどで、暗号化されていないファイルにパスワードを保存しないでください。
- 信頼できないデバイスでアプリケーション（Web ブラウザなど）の「パスワードを保存する」機能を使用しないでください。
- パスワードの漏洩が疑われる場合は、ただちに報告してすべてのパスワードをリセットしなければなりません。

パスワードの復旧

- パスワードを復旧するための質問は、初回ログイン時に入力する必要があります。
- 20 個の質問の中から、少なくとも 3 つの秘密の質問に回答する必要があります。
- 紛失したパスワードは、秘密の質問に回答しないと復旧できません。

デフォルト パスワード

- デフォルト ユーザ/パスワードの数は、アプリケーションのニーズに応じて最小限に限定します。
- デフォルト パスワード（必要な場合）は動的に設定します。つまり、インストールごとに固有のデフォルト パスワードを生成し、複数のシステムが一度に侵害されないようにします。
- デフォルトのユーザ ID とパスワードも、上記の Cisco InfoSec ポリシーに準拠する必要があります。
- 強力なパスワードやパスフレーズにするには次の要件を満たさなければなりません。
- 8 つ以上の英数字を含む。
- 大文字小文字を両方含む。
- 1 つ以上の数字を含む（例：0 ～ 9）。
- 1 つ以上の特殊文字を含む（例：!$%^&*()_+|~-=¥`{}[]:";'<>?,./）。
- CLI では、エスケープ文字（例：¥!）を次の文字の前に付けます（!$&()|¥;'>）。
- CLI では次の文字（"　<　'　?）は使用できません。

禁止文字

次の文字は、シスコ アプリケーションと競合する可能性があるため使用できません。

- 特殊な 8 ビット文字（例： £, Á ë, ô, Ñ, ¿, ß ）
- スペース

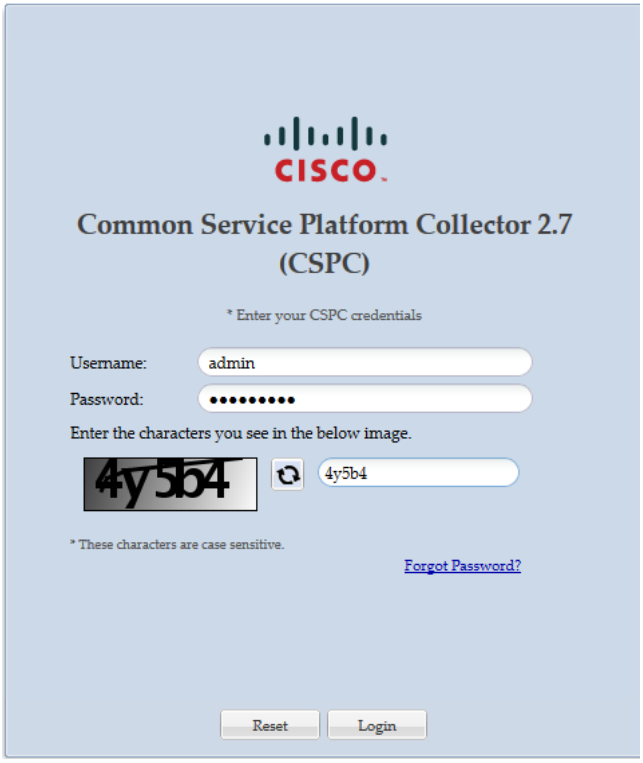
禁止パスワード、パスフレーズ

次のパスワードやパスフレーズ文字は使用できません。

- 過去 10 回分のパスワード、パスフレーズ。
- 8 文字未満であるもの。
- 外国語も含め辞書に登録されているもの。または、俗語、方言、専門用語に含まれるもの。
- 家族、ペット、友人、キャラクタの生年月日、住所、電話番号、名前などの個人情報を含むもの。
- ビルの名前、システム コマンド、サイト、企業、ハードウェア、ソフトウェアなどの仕事関連の情報を含むもの。
- cisco、sanjose、sanfran、またはその派生語を含むもの。
- aaabbb、qwerty、zyxwvuts、123321 などの数字パターンを含むもの。
- スペルを逆にした一般用語、または、一般用語の前後に数字をつけたもの（例： terces, secret1 or 1secret ）

ステップ 3　クレデンシャルとイメージの文字を入力し、[ログイン（Login）] をクリックします。

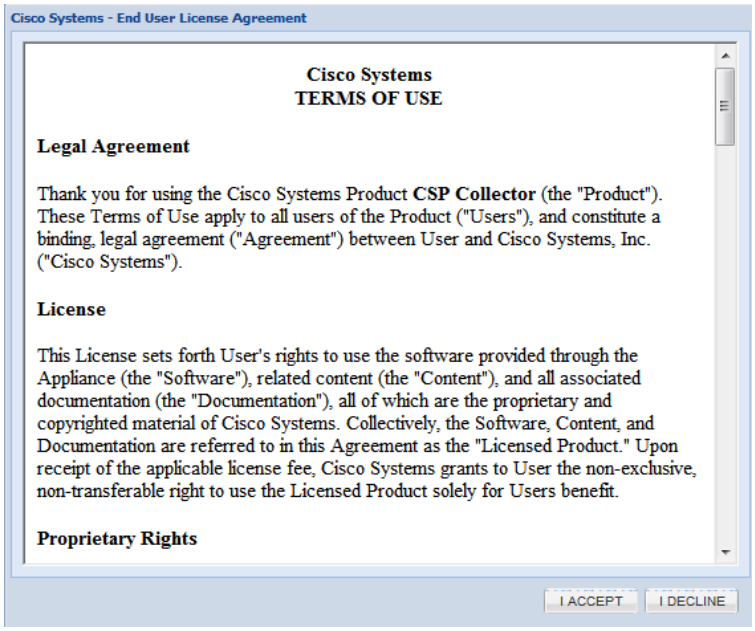
図 2-2　　CSPC コレクタ



ステップ 4　質問に回答し、[OK] をクリックしてパスワード リセットの質問を保存します。

図 2-3　　パスワード リセットの質問（Password Reset Questions）

図 2-4　　エンド ユーザ ライセンス契約（End User License Agreement）



ステップ 5　[同意する（Accept）] ボタンをクリックして利用条件に同意します。

ステップ 6　CSPC でデバイスを収集するために設定が必要なフィールドに入力します。[次へ（Next）] をクリックします。

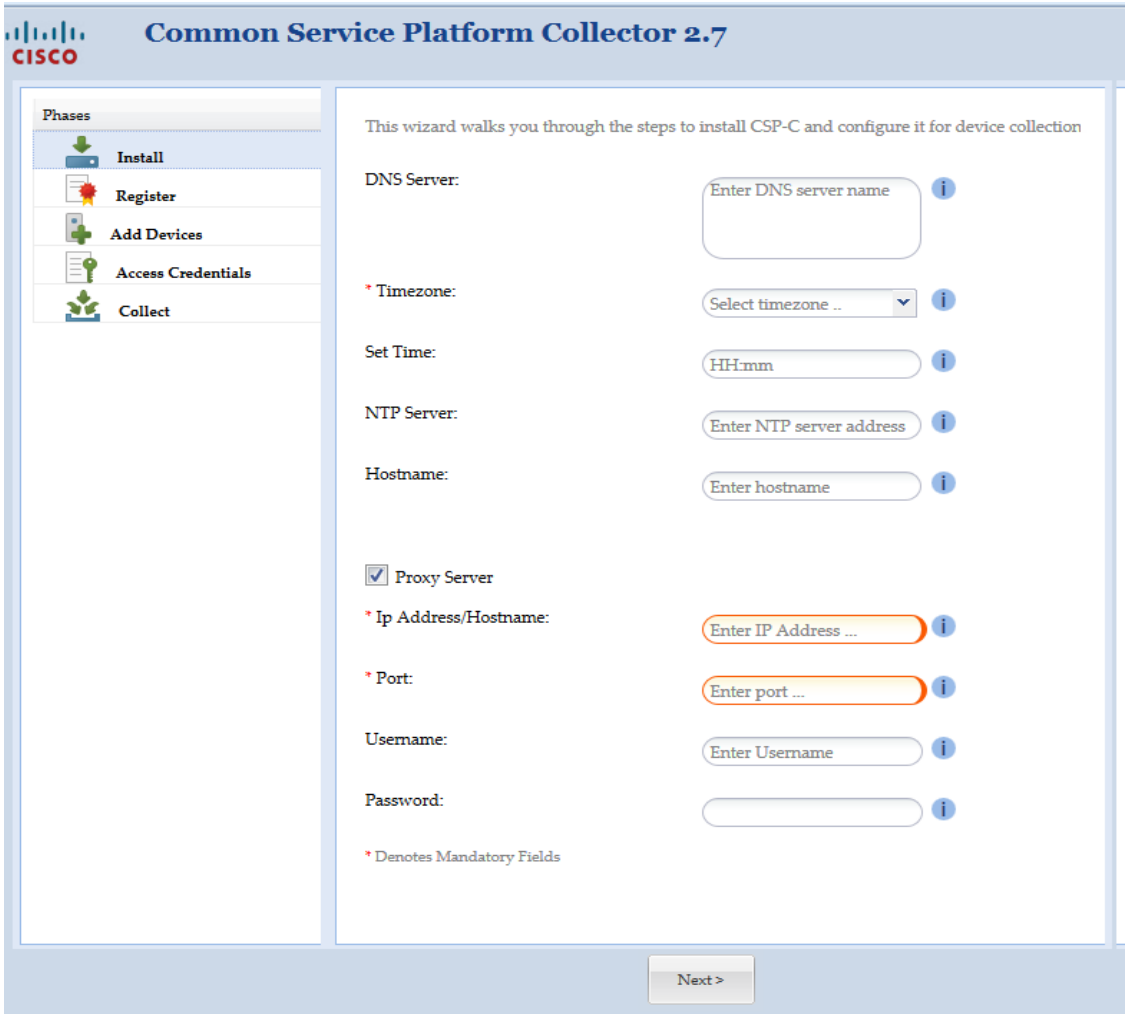
表 2-1　　*ウィザード パラメータ*

パラメータ	説明
[DNS サーバ（DNS Server）]	DNS サーバの IP アドレス
[NTP サーバ（NTP Server）]	NTP サーバの IP アドレス
[タイムゾーン（Timezone）]	コレクタのタイム ゾーン
[設定時間（Set Time）]	アプライアンスの時間を設定します。時間は、選択したタイム ゾーンの実際の時間と一致させる必要があります。
[ホスト名（Host Name）]	ホストの名前
[IP アドレス/ホスト名（IP Address/Host Name）]	プロキシ サーバの IP アドレスまたはホスト名
[ポート（Port）]	プロキシ サーバのポート番号
[ユーザ名（Username）]	プロキシ サーバのクレデンシャル
[パスワード（Password）]	

表 2-1　　ウィザード パラメータ

注　プロキシサーバはオプションです。設定には 30 秒かかります。

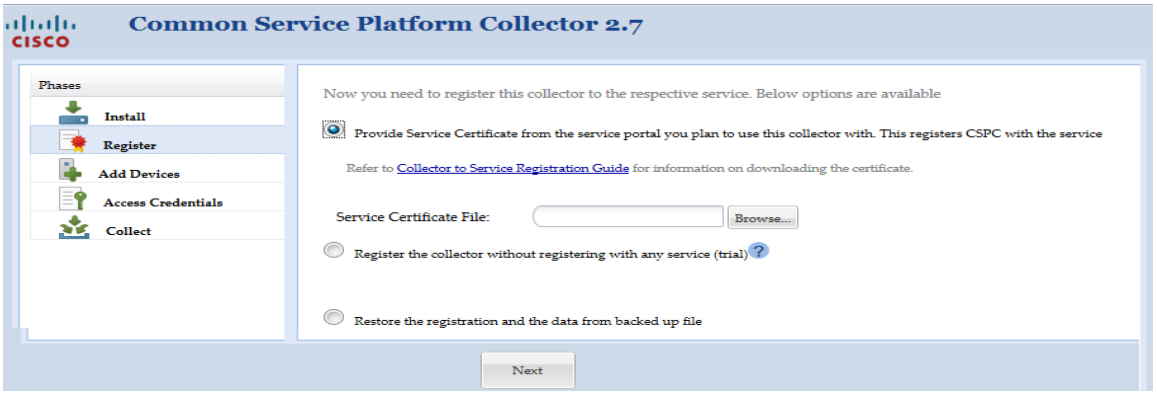
図 2-5　　CSPC のインストール



ステップ 7　次のいずれかの方法で登録できます。

- ブラウザから**サービス証明書ファイル**をアップロードします。

図 2-6　　サービス証明書ファイル

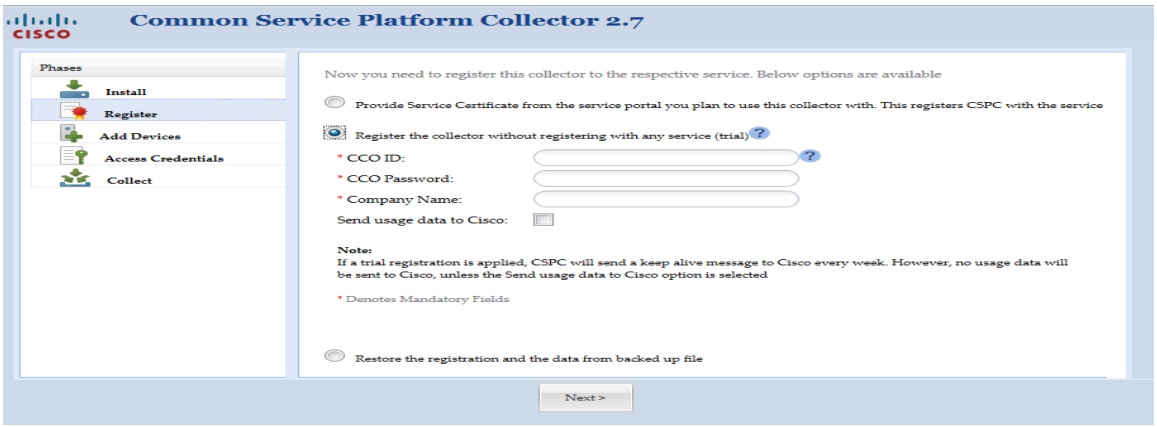


または

- CCO のクレデンシャルを入力してトライアル ライセンスを取得します。必要に応じて、[使用状況データをシスコに送信（Send Usage Data to Cisco）] を選択し、[次へ（Next）] をクリックします。

注
- CSPC をダウンロードし、トライアル ライセンスを使用してインストールできます。ただし、CSPC は使用開始前にシスコ（RMC）に登録する必要があります。最初のオプションとして、ウィザードを使用して CSPC を設定することができます。CSPC は、少なくとも週に 1 度は RMC で更新する必要があります。アップロードが無効になっている場合、シスコに収集したデータを送信することはできません。
- シスコのページにログインしてメリットを得るには、Cisco.com ID（CCO ID）を作成する必要があります。これがユーザ ID になります。

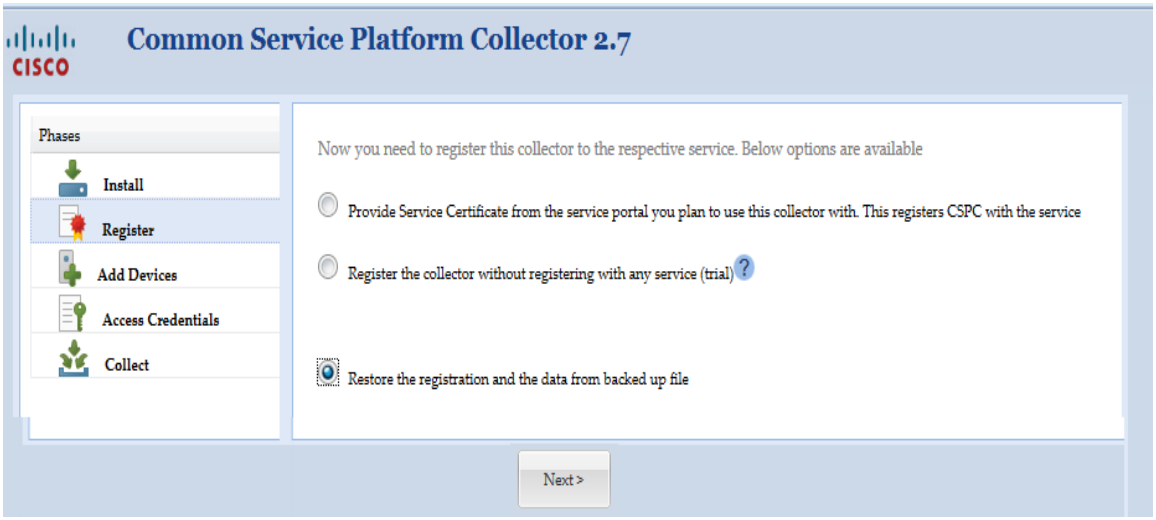
図 2-7　　CCO クレデンシャル



または

- [バックアップ ファイルから登録およびデータを復元（Restore the registration and the data from backed up file）] を選択し、バックアップを復元します。

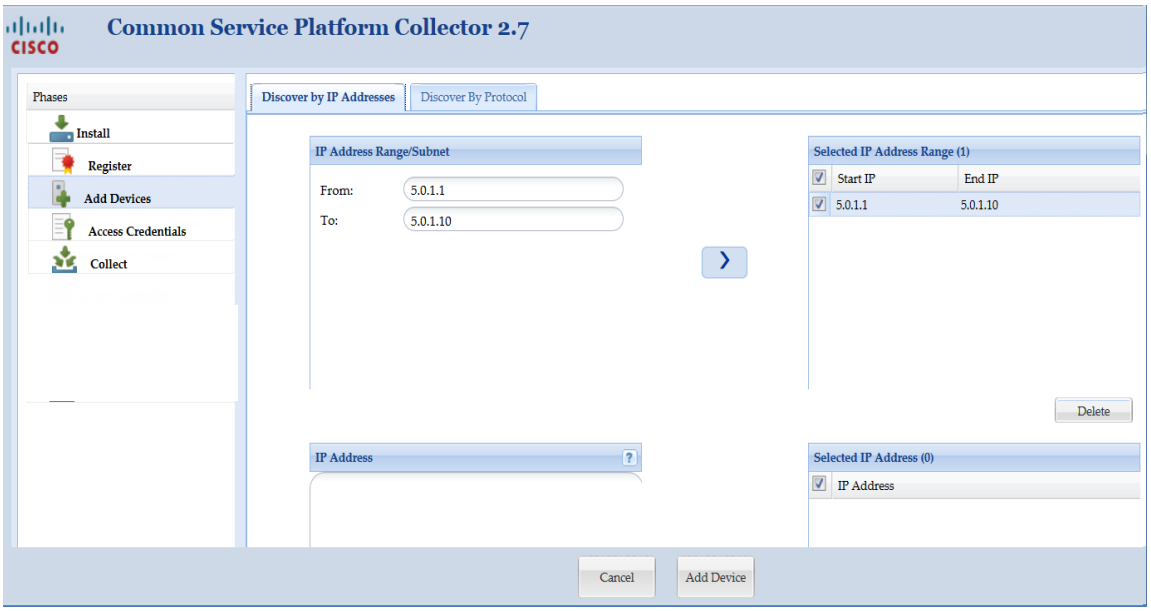
図 2-8　　バックアップの復元



ステップ 8　次のいずれかの方法でデバイスを追加できます。[デバイスの追加（Add Device）] をクリックします。

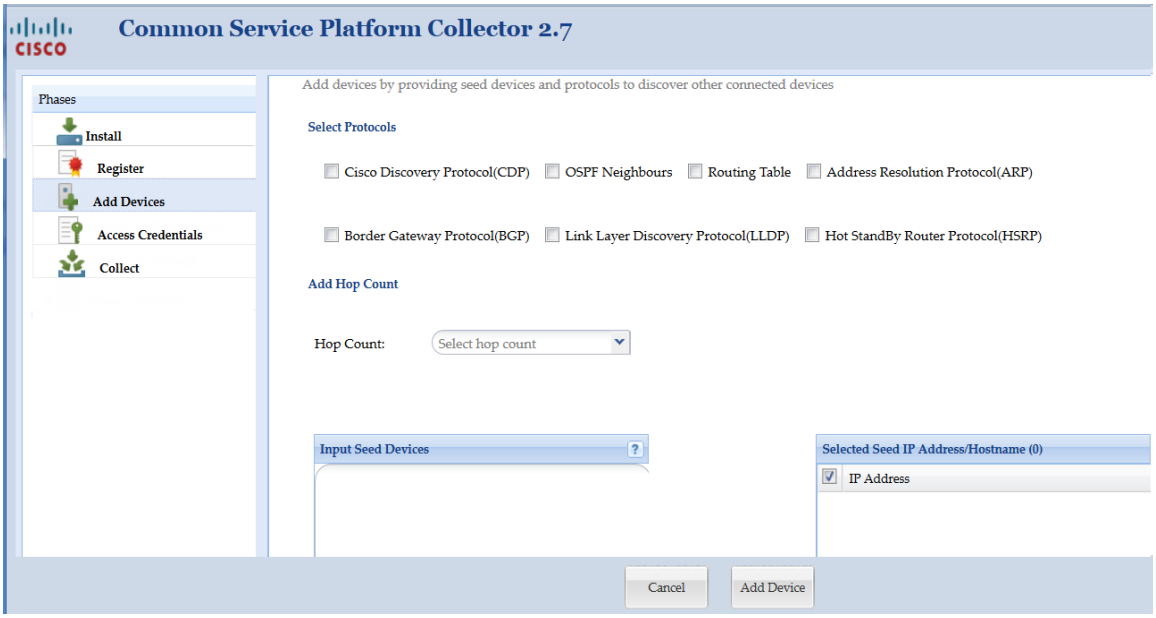
- [IP アドレス（IP Address）] を入力し、> を使用して、特定の IP アドレス、または IP アドレスの範囲を選択します。

図 2-9　　[IP アドレスによる検出（Discovery By IP Address）]



- 必要な [プロトコル（Protocol(s)）]、[ホップ数（HOP Count）]、[シード IP アドレス（Seed IP Address）] を選択します。> を使用してシード IP アドレスを選択します。

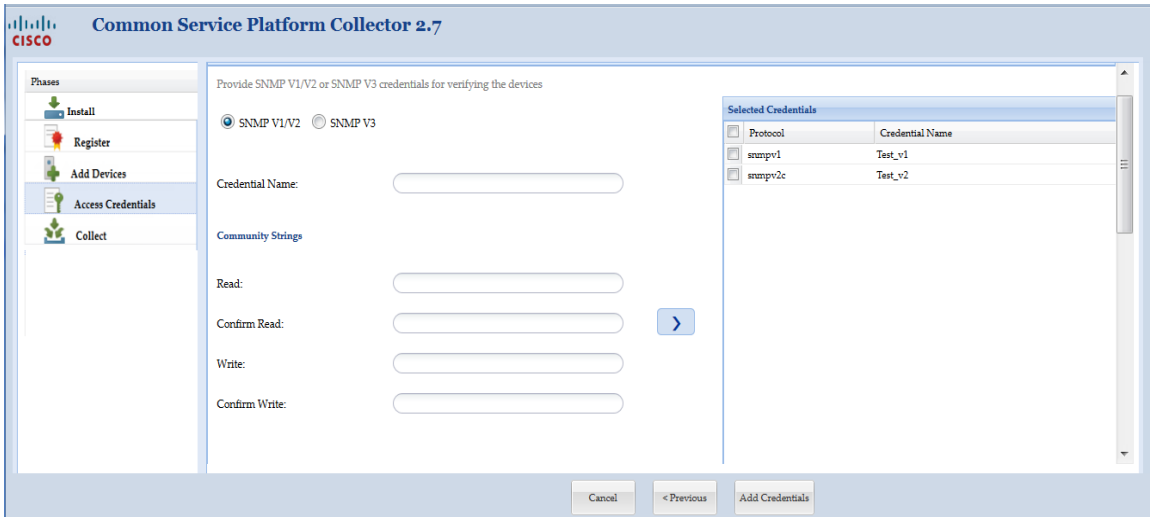
図 2-10　　[プロトコルによる検出（Discovery By Protocol）]



ステップ 9　次のいずれかの方法でクレデンシャルを追加できます。[クレデンシャルの追加（Add Credential）] をクリックします。

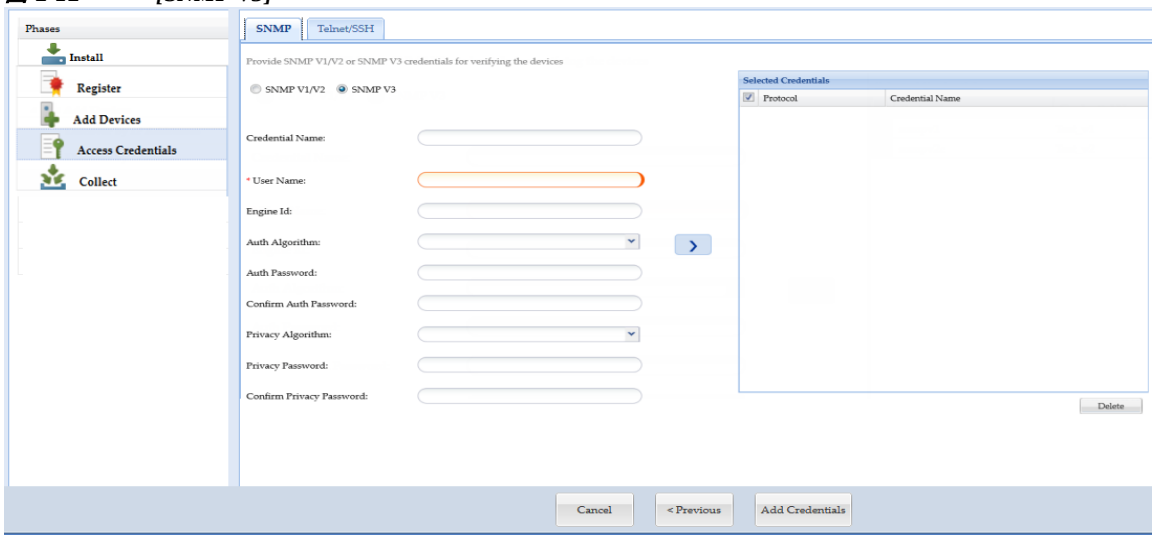
- [SNMPV1/V2] を選択した場合は、[クレデンシャル名（Credential Name）]、および [コミュニティ ストリング（Community Strings）] の [読み込み（Read）] と [書き込み（Write）] を入力します。> を使用してクレデンシャルを選択します。

図 2-11　　[SNMP V1/V2]



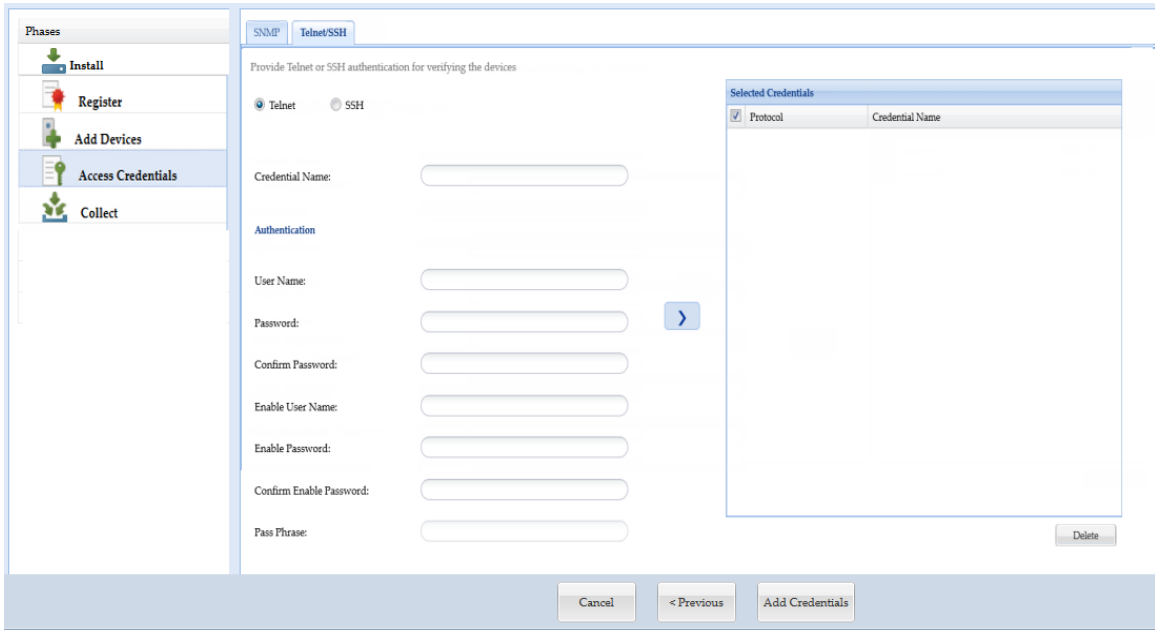
- [SNMP V3] を選択した場合は、[クレデンシャル名（Credential Name）、[ユーザ名（User Name）]、[エンジン ID（Engine Id）]、[認証アルゴリズム（Auth Algorithm）]、[認証パスワード（Auth Password）]、[プライバシー アルゴリズム（Privacy Algorithm）]、[プライバシー パスワード（Privacy Password）] を入力します。> を使用してクレデンシャルを選択します。

図 2-12　　[SNMP V3]



- [Telnet] を選択した場合は、[クレデンシャル名（Credential Name）]、[ユーザ名（User Name）]、[パスワード（Password）]、[ユーザ名の有効化（Enable User Name）]、[パスワードの有効化（Enable Password）]、[パスフレーズ（Pass Phrase）] を入力します。> を使用してクレデンシャルを選択します。
- [SSH] を選択した場合は、[クレデンシャル名（Credential Name）]、[ユーザ名（User Name）]、[パスワード（Password）]、[ユーザ名の有効化（Enable User Name）]、[パスワードの有効化（Enable Password）]、[パスフレーズ（Pass Phrase）] を入力します。> を使用してクレデンシャルを選択します。

図 2-13　　[Telnet] および [SSH]



ステップ 10　[すぐに収集を開始（Start Collection now）] を選択後、[すぐに収集（Collect Now）] をクリックしてその時点で収集を開始するか、[定期的な収集をスケジュール（Schedule Periodic Collection）] をクリック後、[スケジュール（Schedule）] をクリックして後で収集します。図 2-15 に示すように、スケジュールの開始日時と終了日時を設定するか、定期的なパターンとして [毎分（Minutely）]、[毎日（Daily）]、[毎週（Weekly）]、[毎月（Monthly）]、または [年に 1 回（Yearly）] を選択することができます。

図 2-14　　[すぐに収集（Collect Now）]

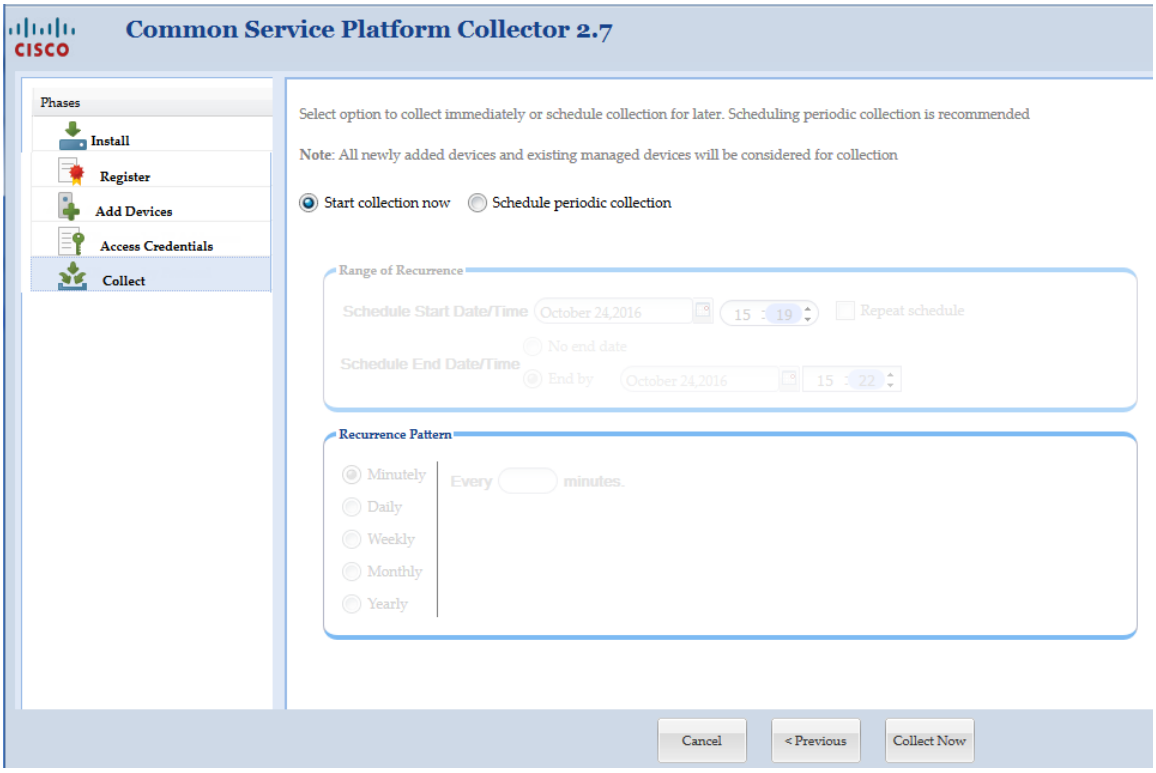
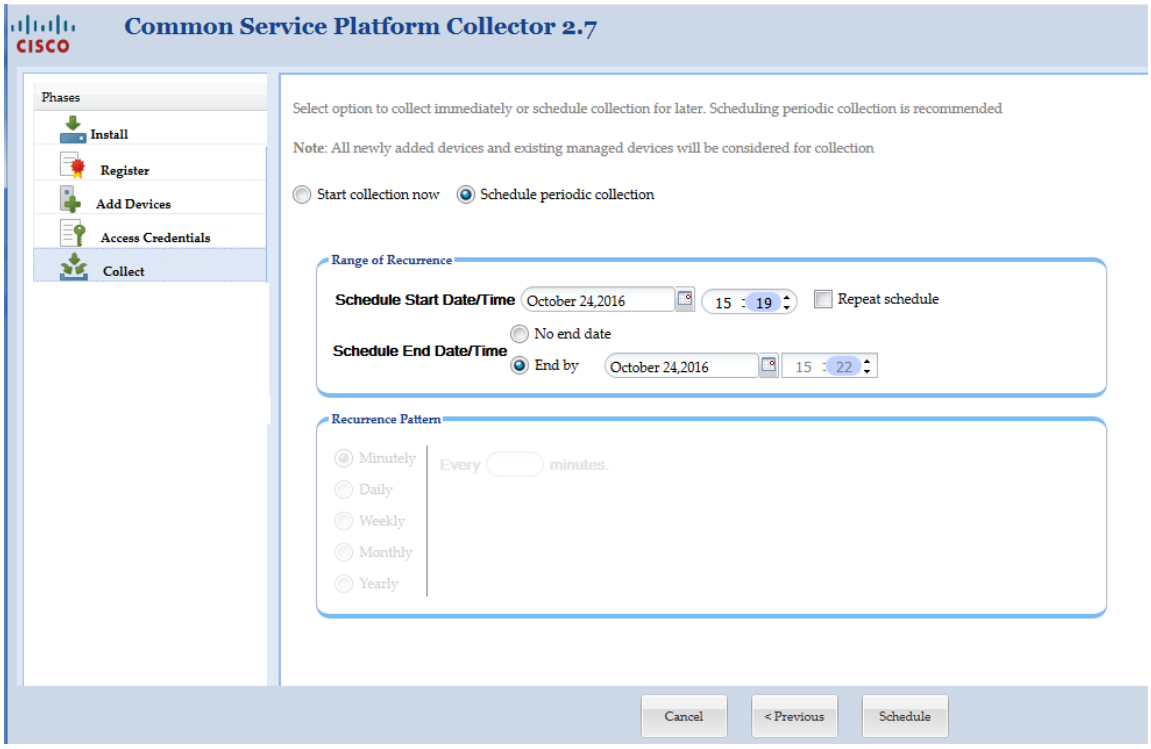


図 2-15　　[定期的な収集をスケジュール（Schedule Periodic Collection）]



CSPC コレクタにログインすると、[ダッシュボード（Dashboard）] 画面が表示されます

注　セッションが 15 分以上アイドル状態になると、ユーザはアプリケーションからログアウトされます。

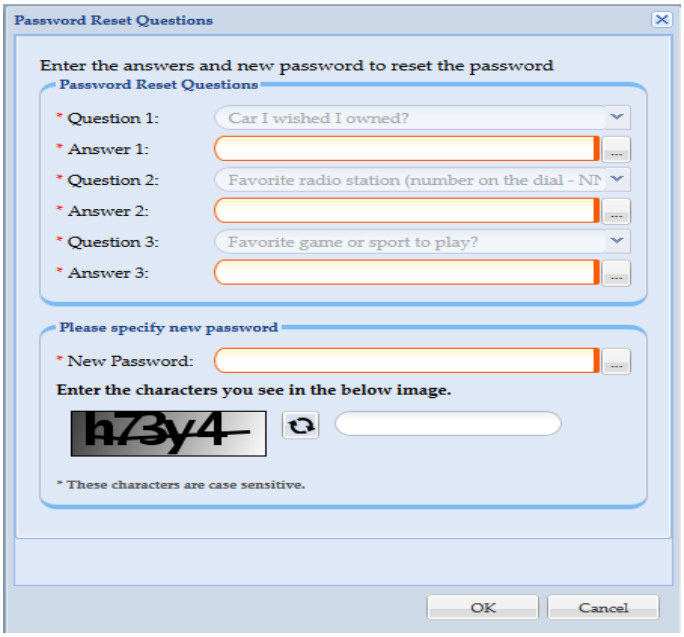
CSPC フローチャートに戻る

パスワードを忘れた場合

パスワードを忘れた場合は、ログイン画面の [パスワードを忘れた場合（Forgot password?）] リンクをクリックします。次に示すダイアログボックスが開き、一連の質問が表示されます。一連の質問に解答し、[新しいパスワード（New Password）] テキスト ボックスに新しいパスワードを入力します。イメージの文字を入力します。

[OK] ボタンをクリックします。パスワードがリセットされます。

図 2-16　　パスワードのリセット（Password Reset）



サーバとパッケージのバージョン

[サーバ バージョンの表示（View Server Versions）] 画面では、CSPC にインストールされている CSPC 基本コレクタ、アドオン、およびその他のオプショナル パッケージのバージョンを確認できます。

CSPC にログインした後、[ヘルプ（Help）] メニュー >[バージョン情報（About）]>[バージョンの表示（View Versions）] の順にクリックします。

バージョン情報を示す画面（図 2-18）が表示されます。

図 2-17　View Server Versions

図 2-18　サーバ バージョンの表示

View Server Versions

Title	Version	Description
CSPC Base Collector	2.7	
Rules Package	4.0	
PoP	4.0	Collection Profile Package Patch of …
DSIRT1.2		DSIRT Package. DSIRT avoid collec…
RP4.0	4.0	Collection Rules Package
RP4.0_SNTC_CP	4.0	Collection Profile Package
Agent	1.0	

3

CSPC ダッシュボード

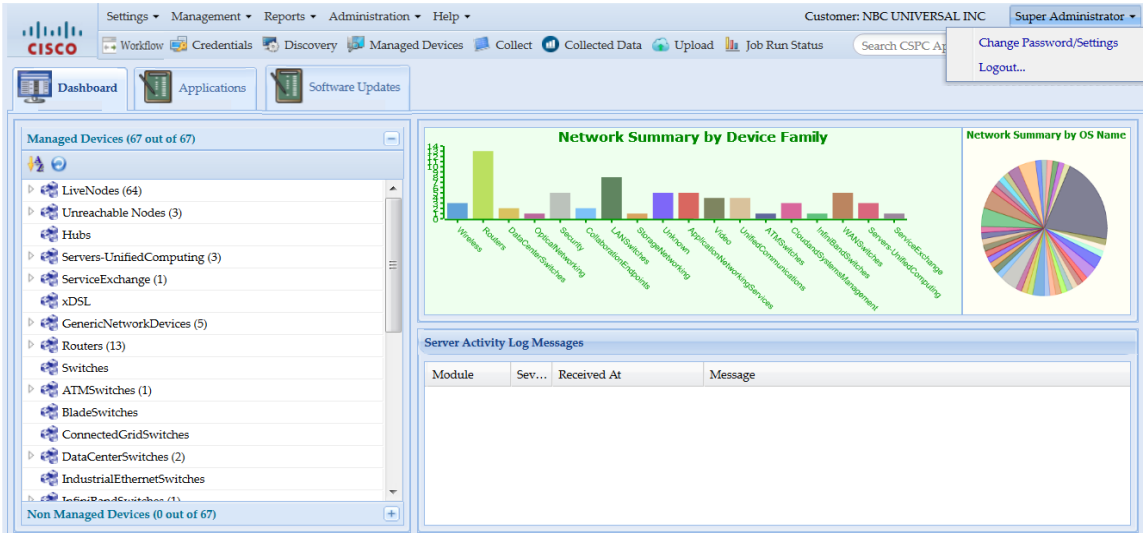
ダッシュボード

ダッシュボードは、CSP Collector のプライマリ画面です。この画面は、それぞれのユーザに合わせてカスタマイズすることができます。レイアウト指定後に保存でき、次回ログイン時には、カスタマイズしたレイアウトが表示されます。

メニュー オプション、[デバイス エクスプローラ ツリー（Device Explorer Tree）]、[サーバ アクティビティ ログ メッセージ（Server Activity Log Messages）]、およびグラフにアクセスするには、ダッシュボードを使用します。ダッシュボードは、メニュー バー（[ユーザ（User）]、[設定（Settings）]、[運用（Management）]、[レポート（Reports）]、[管理（Administration）]、[ヘルプ(Help)]）や、重要な機能にすぐにアクセスできるクイック メニュー バー、2 つのタブ（[ダッシュボード(Dashboard)] と [アプリケーション（Applications）]）で構成されています。検索オプションが用意されているため、CSPC アプリケーションに簡単に移動できます。右上隅にある CSPC 通知コミュニケータは、検出、収集、DAV、アップロードなどを含むジョブの完了といった各種イベントを検出します。イベントが検出されると、CSPC は UI と設定された 1 人または複数の電子メール受信者にイベント完了通知を送信します。各イベントには個別の受信者グループを設定できます。イベントの履歴は保持されません。[サーバ アクティビティ ログ メッセージ（Server Activity Log Messages）] を表示することもできます。[CSPC のセキュアなブラウジングを無効にする（Disable Secure Browsing for CSPC）] をオンにすると、ブラウザとサーバ間の暗号化通信が無効になります。これをオンにすると、アプリケーションのセキュリティが脆弱になる可能性があるので、必要な場合以外はオンにしないでください。

画面の左側にあるノード エクスプローラには、CSPC の管理下にあるデバイスがすべて表示されます。いずれかのデバイスを右クリックすると、ポップアップ メニューが開き、選択したデバイスのプロパティが表示されます。[サーバ アクティビティ ログ メッセージ（Server Activity Log Messages）] ウィンドウには、検出とデータ収集の双方についてのステータス メッセージが表示されます。

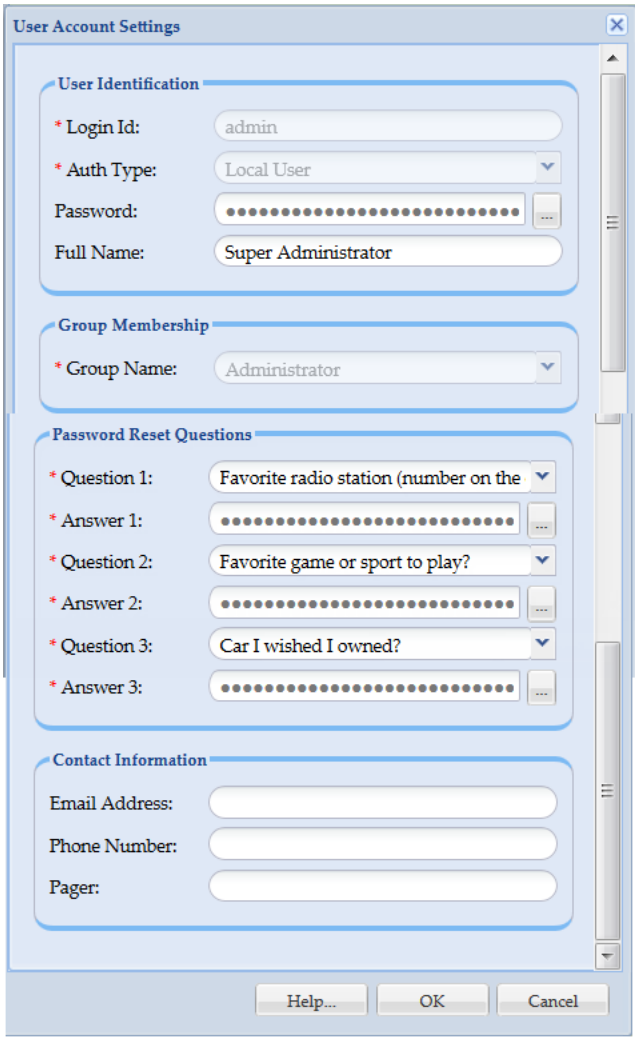
図 3-1　　CSPC ダッシュボード



ダッシュボード

パスワードを変更するには、ダッシュボードの右上のドロップダウンから [パスワードの変更/設定（Change Password/setting）] をクリックします。すべての必須フィールドを変更して [OK] をクリックします。

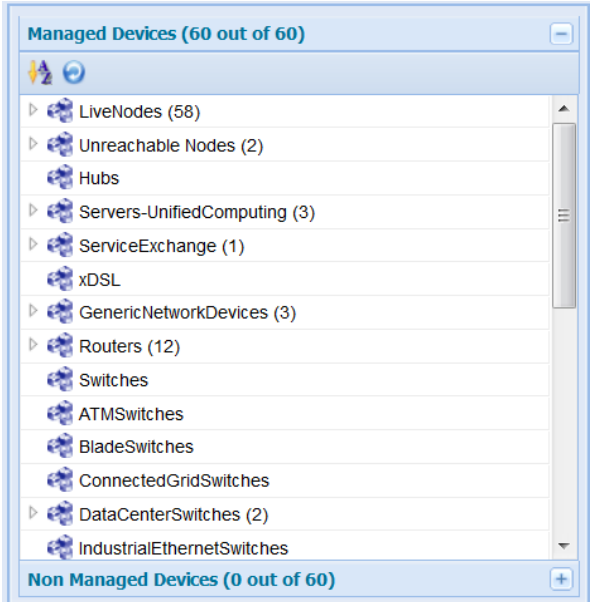
図 3-2　　パスワードの変更



管理対象デバイス

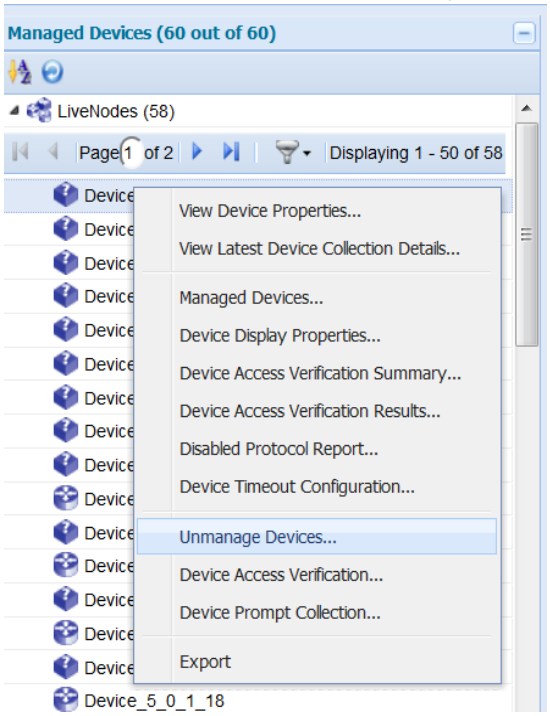
[管理対象デバイス（Managed Devices）] には、CSPC によってデータが収集されている管理対象ネットワーク デバイスの一覧が表示されます。デバイス名の横にある矢印をクリックすると、一覧が展開されます。[管理対象デバイス ツリー（Managed Device Tree）] では、リスト内の各ネットワーク デバイスの下に最大 50 台のデバイスしか表示されません。追加のデバイスを表示するには、[次へ（Next）] ボタン アイコンをクリックします。

図 3-3　　管理対象デバイス ツリー（Managed Device Tree）



デバイスを右クリックすると、図 3-4 に示すメニューが表示されます。

図 3-4　　[管理対象デバイス（Managed Devices）] メニュー



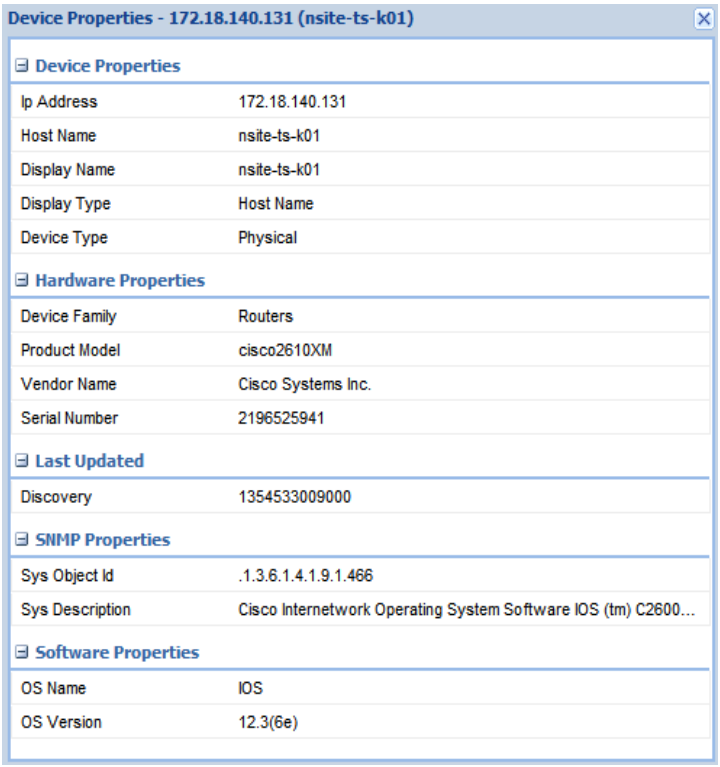
メニュー オプションには次のオプションが表示されます。

-
- 最新の収集の詳細を表示
- [検出されたデバイスの表示（View Discovered Devices）]
- [デバイス アクセス検証のサマリー（Device Access Verification Summary）]
- デバイス アクセス検証のサマリー（Device Access Verification Summary）
- [アクセス検証結果の表示（View Access Verification Results）]
- [無効プロトコル レポート（Disabled Protocol Report）]
- [デバイスのタイムアウト設定（Device Timeout Configuration）]
- [デバイスを管理対象外にする（Unmanage Devices）]
- [デバイス アクセスの検証（Verify Device Access）]
- [デバイス プロンプトの収集（Device Prompt Collection）]
- エクスポート

デバイスのプロパティの表示

デバイスのプロパティを表示するには、デバイスをダブルクリックまたは右クリックして、[デバイスのプロパティの表示（View Device Properties）] を選択します。図 3-5 に示す [デバイスのプロパティ（Device Properties）] 画面が表示されます。

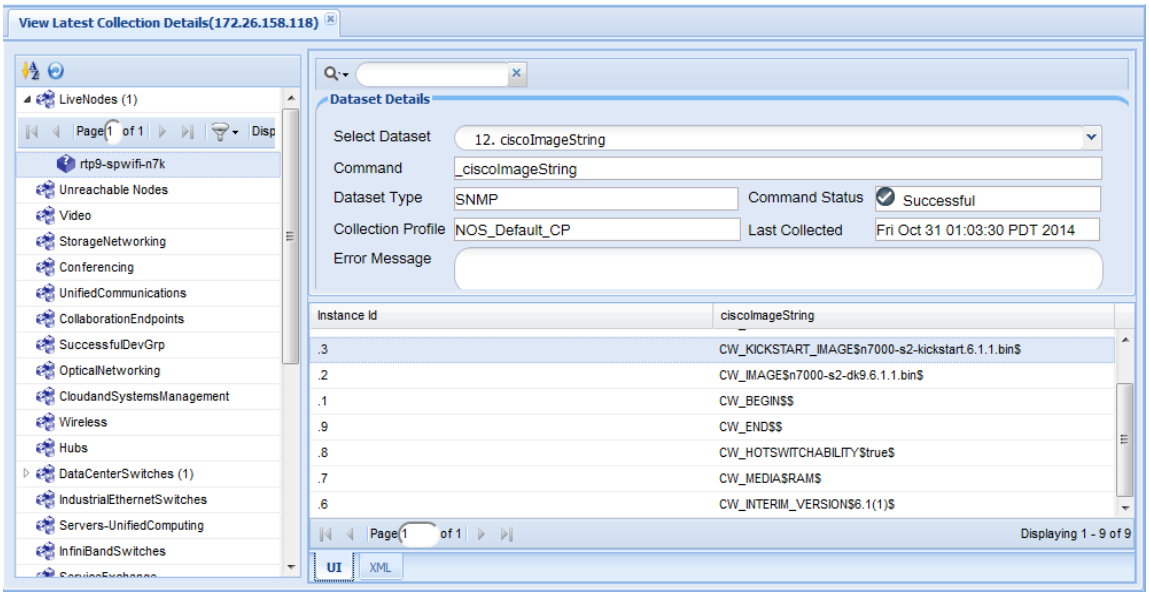
図 3-5　デバイスのプロパティ



最新の収集の詳細を表示

最新の収集データの詳細を表示するには、コレクションを右クリックして、[最新の収集の詳細（Latest Collection Details）] オプションを選択します。図 3-6 に示す [最新の収集の詳細（Latest Collection Details）] 画面が表示されます。[データセットの選択（Select Dataset）] ドロップダウンからデータセット名を選択すると、[コマンド（Command）]、[データセット タイプ（Dataset Type）]、[コマンドのステータス（Command Status）]、[収集プロファイル（Collection Profile）]、[最終収集日時（Last Collected）]、[エラー メッセージ（Error Message）] などの詳細が表示されます。UI コマンドの場合は [UI] タブと [XML] タブの両方が、CLI コマンドの場合は [CLI] タブのみがページの下部に表示されます。検索を使用してデータセットの詳細を表示することもできます。

図 3-6　　[最新の収集の詳細（Latest Collection Details）]



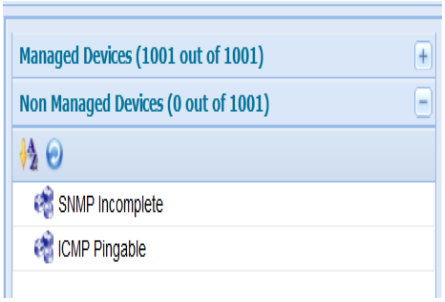
エクスポート

管理対象デバイスの DAV 結果ファイルをダウンロードするには、図 3-4 に示すようにフォルダまたはデバイスを右クリックして [エクスポート（Export）] オプションを選択します。ManagedDevicesCredentials.csv ファイルがシステムにダウンロードされます。このファイルは、Microsoft Excel または類似のアプリケーションで表示できます。

[管理対象外デバイス（Non Managed Devices）]

[管理対象外デバイス（Non Managed Devices）] には、CSPC によってデータが収集されている管理対象外ネットワーク デバイスが一覧表示されます。デバイス名の横にある矢印をクリックすると、一覧が展開されます。

図 3-7　　[管理対象外デバイス（Non Managed Devices）]



4

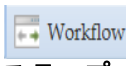
CSPC ワークフロー

CSPC ワークフローは、デバイスの検出から、クレデンシャルの追加、デバイスの収集まで 1 度にできる強力な機能です。デバイスを追加するには、IP アドレスによる検出とプロトコルによる検出の 2 種類の方法があります。SNMP V1/V2、V3、Telnet、SSH を使用してクレデンシャルを追加し、すぐに収集するか、スケジュールして後で収集するかのいずれかを実行できます。

ワークフローを開始するには、次の手順を実行します。

ステップ 1　メニュー バーから [ワークフロー（Workflow）] をクリックします。

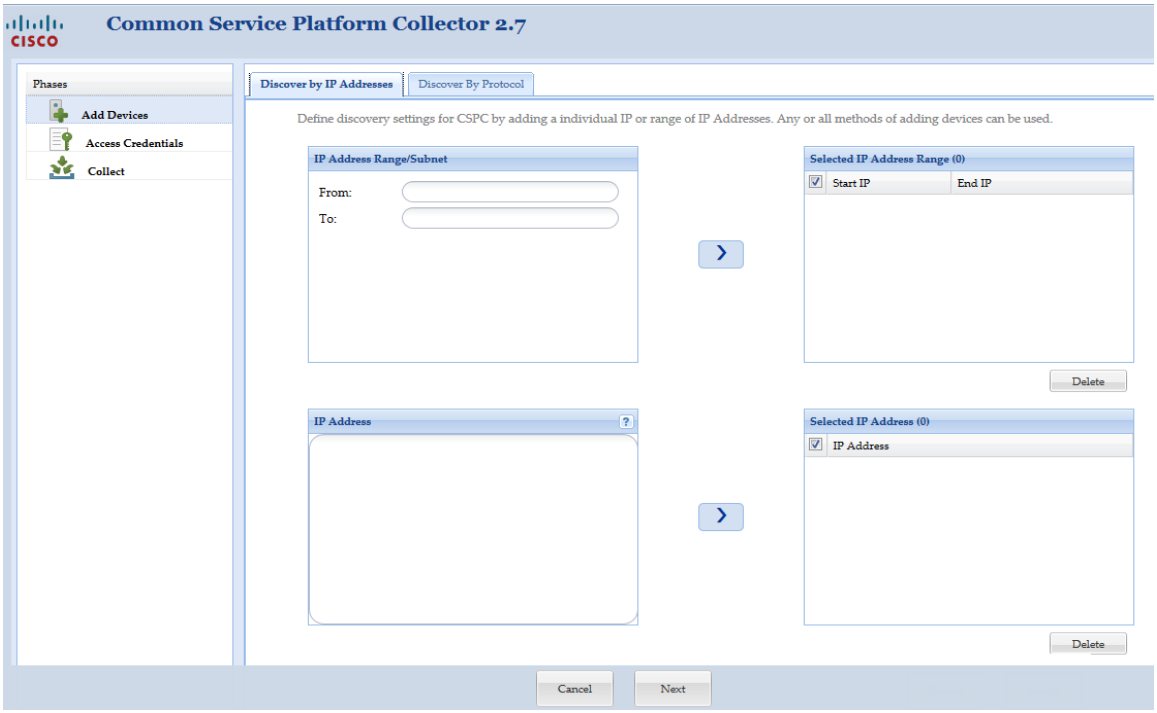
図 4-1　　[ワークフロー（Workflow）] メニュー



ステップ 2　次のいずれかの方法でデバイスを追加し、[次へ（Next）] をクリックします。

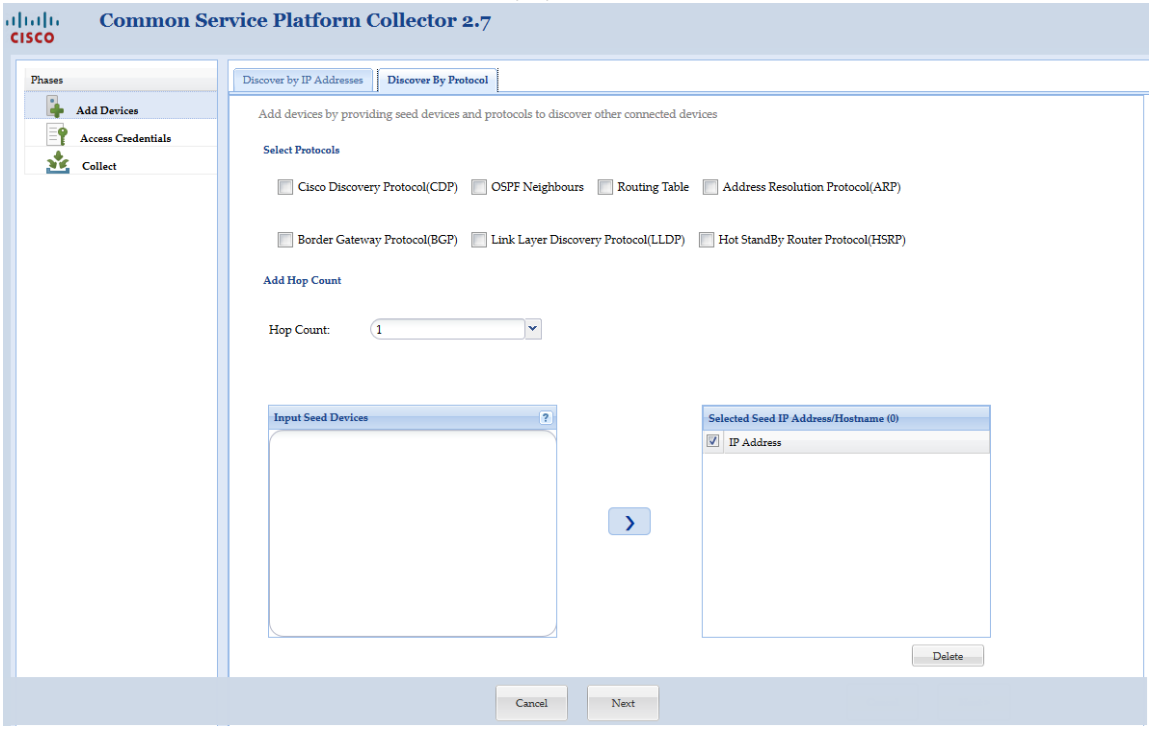
- [IP アドレス（IP Address）] を入力し、> を使用して、IP アドレスを選択します。IP アドレスの範囲を選択することもできます。

図 4-2　　[IP アドレスによる検出（Discovery By IP Address）]



- 必要な [プロトコル（Protocol(s)）]、[ホップ数（HOP Count）]、[シード IP アドレス（Seed IP Address）] を選択します。> を使用してシード IP アドレスを選択します。

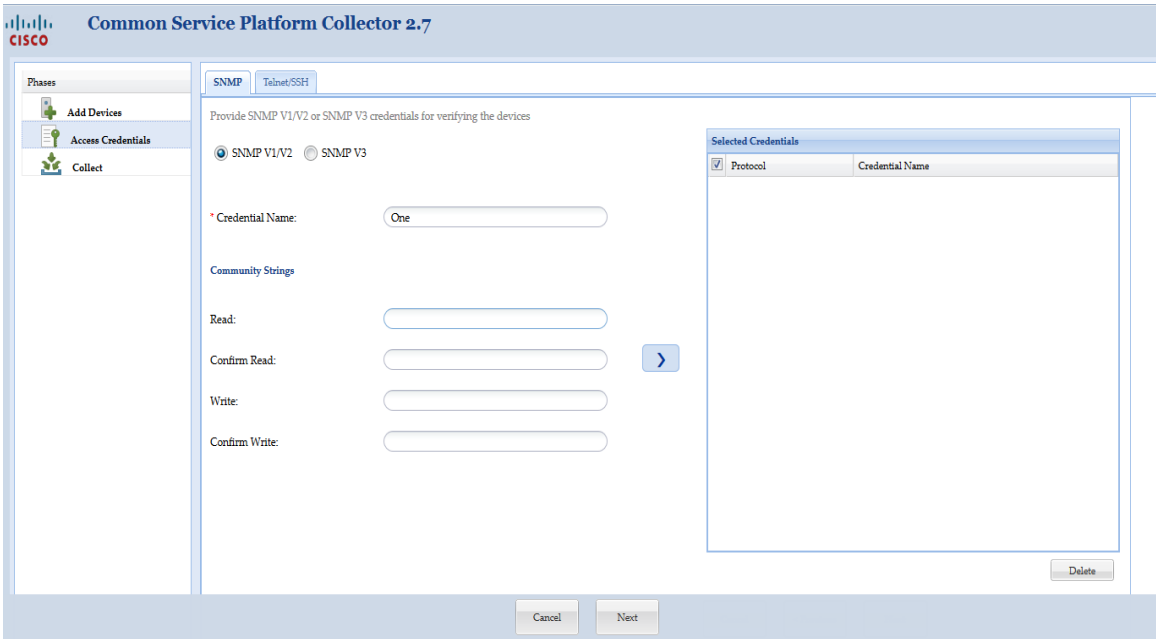
図 4-3　　[プロトコルによる検出（Discovery By Protocol）]



ステップ 3　　次のいずれかの方法でクレデンシャルを追加できます。[クレデンシャルの追加（Add Credential）] をクリックします。

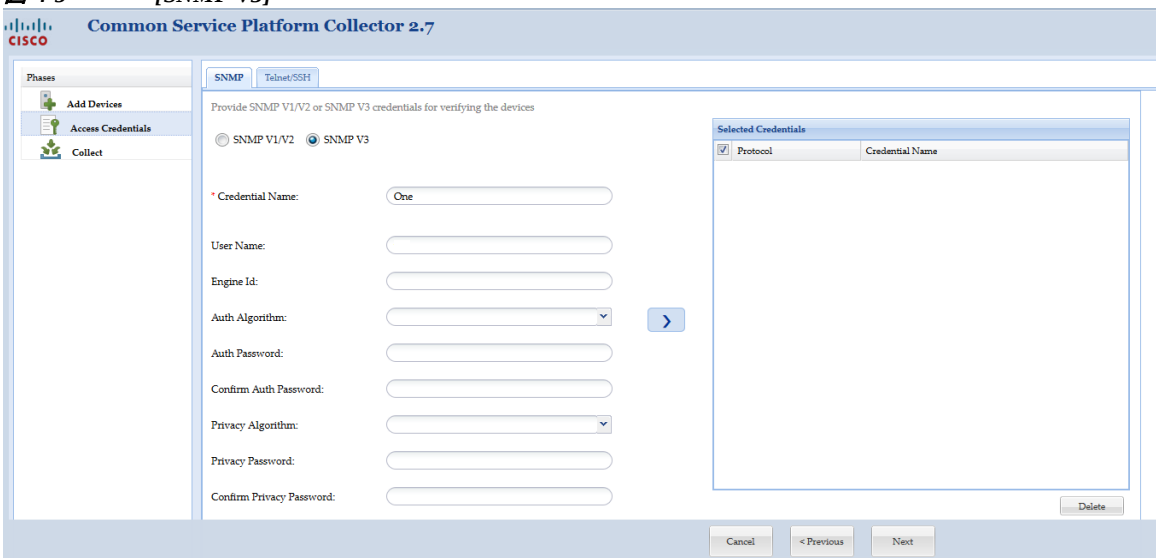
- [SNMPV1/V2] を選択した場合は、[クレデンシャル名（Credential Name）]、および [コミュニティ ストリング（Community Strings）] の [読み込み（Read）] と [書き込み（Write）] を入力します。> を使用してクレデンシャルを選択します。

図 4-4　　[SNMP V1/V2]



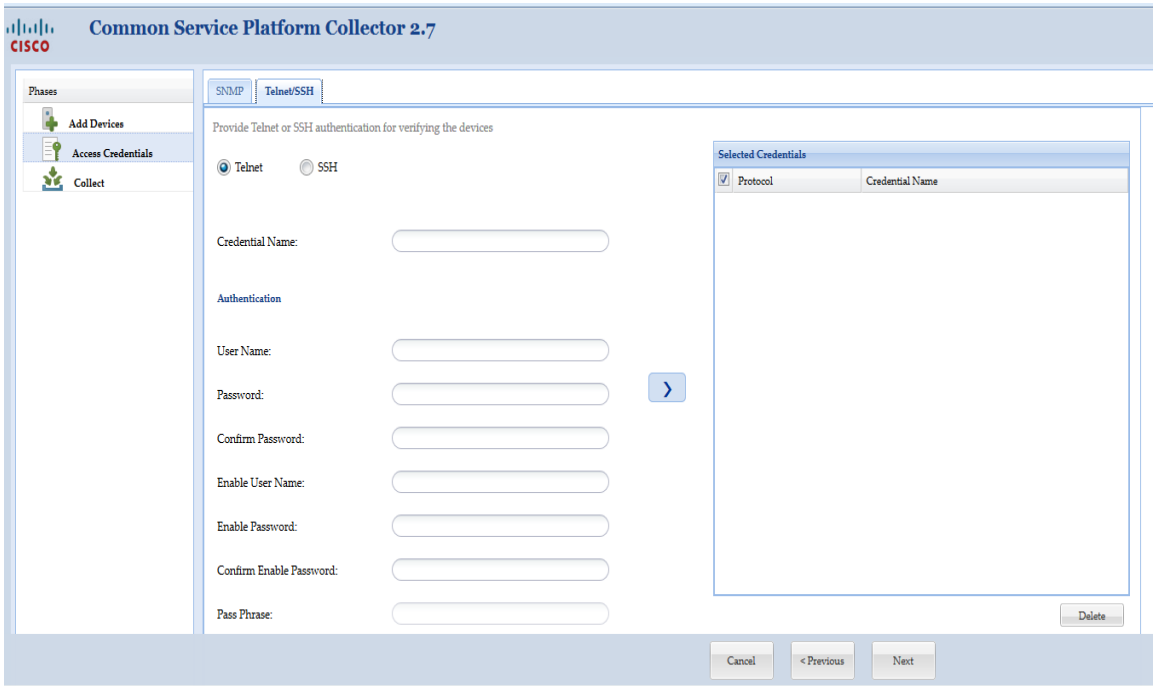
- [SNMP V3] を選択した場合は、[クレデンシャル名（Credential Name）、[ユーザ名（User Name）]、[エンジン ID（Engine Id）]、[認証アルゴリズム（Auth Algorithm）]、[認証パスワード（Auth Password）]、[プライバシー アルゴリズム（Privacy Algorithm）]、[プライバシー パスワード（Privacy Password）] を入力します。> を使用してクレデンシャルを選択します。

図 4-5　　[SNMP V3]



- [Telnet] を選択した場合は、[クレデンシャル名（Credential Name）]、[ユーザ名（User Name）]、[パスワード（Password）]、[ユーザ名の有効化（Enable User Name）]、[パスワードの有効化（Enable Password）]、[パスフレーズ（Pass Phrase）] を入力します。> を使用してクレデンシャルを選択します。
- [SSH] を選択した場合は、[クレデンシャル名（Credential Name）]、[ユーザ名（User Name）]、[パスワード（Password）]、[ユーザ名の有効化（Enable User Name）]、[パスワードの有効化（Enable Password）]、[パスフレーズ（Pass Phrase）] を入力します。> を使用してクレデンシャルを選択します。

図 4-6　　[Telnet] および [SSH]



ステップ 4　[すぐに収集を開始（Start Collection now）] を選択後、[すぐに収集（Collect Now）] をクリックしてその時点で収集を開始するか、[定期な収集をスケジュール（Schedule Periodic Collection）] をクリック後、[スケジュール（Schedule）] をクリックして後で収集します。図 4-8 に示すように、スケジュールの開始日時と終了日時を設定するか、定期的なパターンとして [毎分（Minutely）]、[毎日（Daily）]、[毎週（Weekly）]、[毎月（Monthly）]、または [年に 1 回（Yearly）] を選択することができます。

図 4-7　　[すぐに収集（Collect Now）]

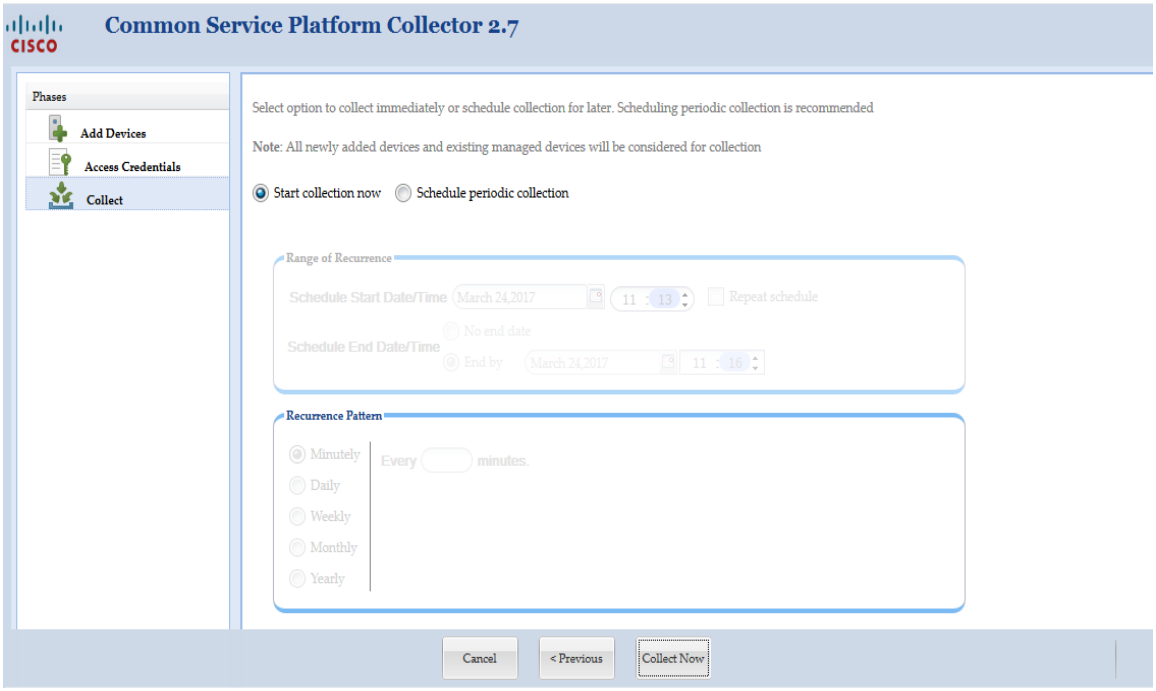
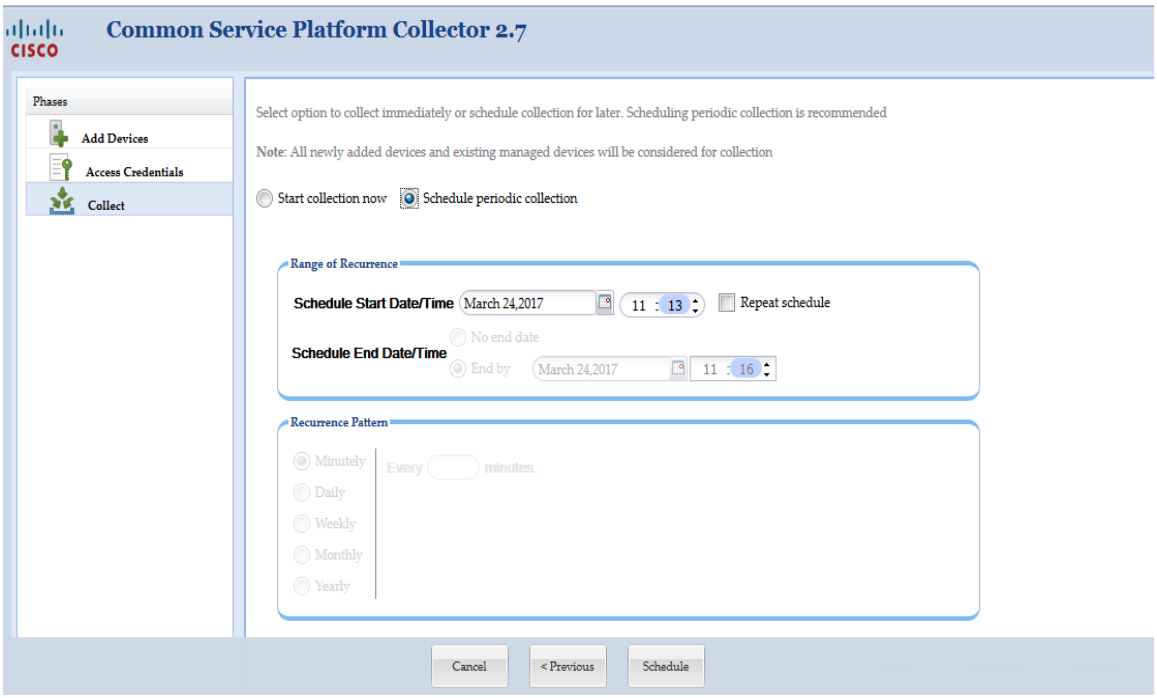


図 4-8　　[定期的な収集をスケジュール（Schedule Periodic Collection）]



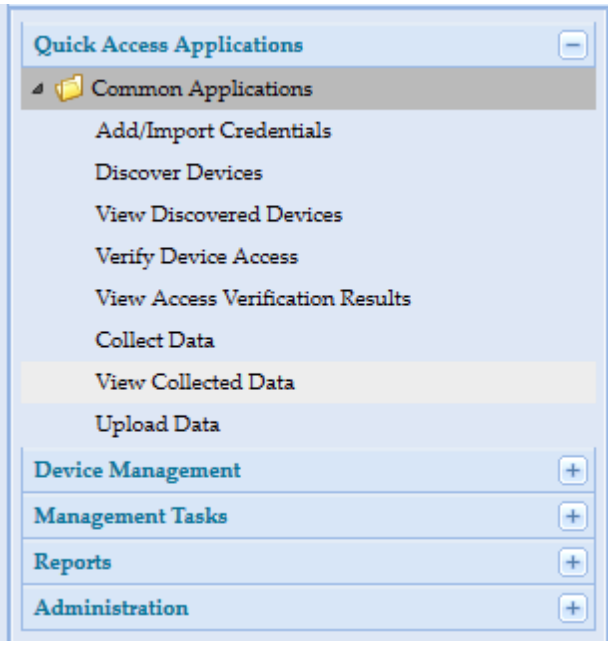
5

クイック アクセス アプリケーション - デバイス管理

共通アプリケーション

[共通アプリケーション（Common Application）] タブでは、ネットワーク デバイスに関するソフトウェアとハードウェア情報の指定/収集/保存が可能なツールにアクセスできます。

図 5-1　　デバイス管理



この項では、共通アプリケーション ツールの以下の項目について説明します。

- [クレデンシャルの追加/インポート（Add/Import Credentials）]
- [デバイスの検出（Discover Devices）]
- [検出されたデバイスの表示（View Discovered Devices）]
- [デバイス アクセスの検証（Verify Device Access）]
- [データの収集（Collect Data）]
- [収集されたデバイスの表示（View Collected Devices）]
- [データのアップロード（Upload Data）]

リンクを使用して移動します。

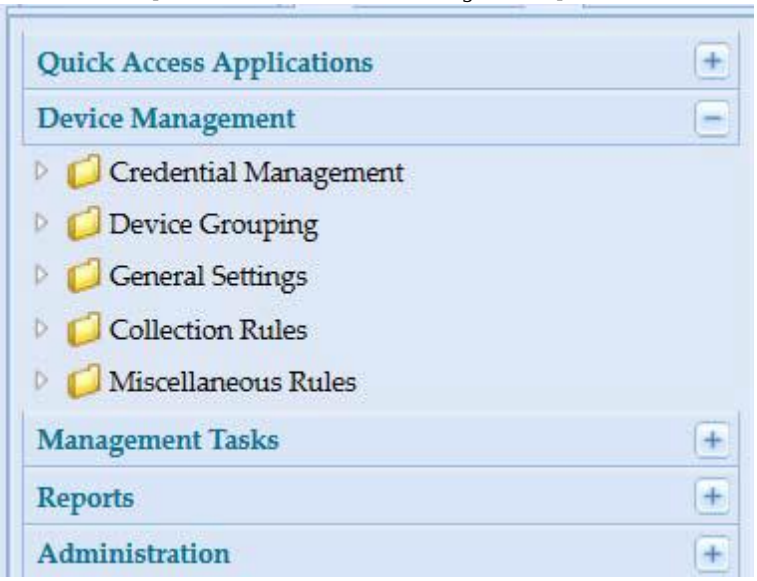
6

アプリケーション - デバイス管理

[デバイス管理（Device Management）]

[共通アプリケーション（Common Application）] タブでは、ネットワーク デバイスに関するソフトウェアとハードウェア情報の指定、収集、保存が可能なツールにアクセスできます。

図 6-1　　[デバイス管理（Device Management）]



この項では、[デバイス管理（Device Management）] ツールの以下の項目について説明します。

- [クレデンシャル管理（Credential Management）]
- [デバイスのグループ化（Device Grouping）]
- [全般設定（General Settings）]
- [収集ルール（Collection Rules）]
- [その他のルール（Miscellaneous Rules）]

[クレデンシャル管理（Credential Management）]

[デバイス管理（Device Management）] タブの [クレデンシャル管理（Credential Management）] サブ タブを使用して、デバイスまたはモジュールのクレデンシャルを設定し、シード ファイルを管理します。

この項では、[クレデンシャル管理（Credential Management）] オプションの以下の項目について説明します。

- [クレデンシャルの追加/インポート（Add/Import Credentials）]
- [サブ モジュール クレデンシャルの管理（Manage Sub Module Credentials）]
- [シード ファイルの管理（Manage Seed File）]
- [インポートされたシード ファイル（Imported Seed file）]
- [管理対象外デバイス リスト（Do Not Manage Device List）]

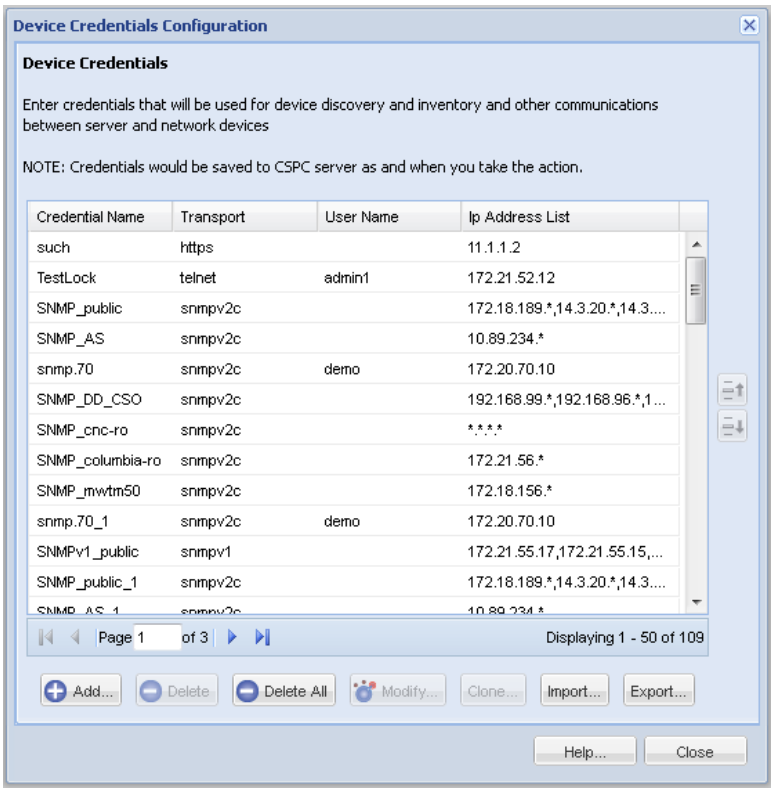
[クレデンシャルの追加/インポート（Add/Import Credentials）]

ネットワーク デバイスを検出して、デバイスからデータを収集するためには、まずクレデンシャルを入力する必要があります。CSPC に設定するデバイス クレデンシャルは、2 つの目的のために使用されます。SNMP クレデンシャルは、デバイスの初期検出にのみ使用されます。

Telnet、SSH、HTTP、HTTPS、WMI、TL1、IIOP などのその他のクレデンシャルは、検出されたデバイスからのデータ収集に使用されます。

クレデンシャルを追加するには、デバイス クレデンシャルの構成ウィザードを使用します。ウィザードの手順に従って、クレデンシャルのパラメータを選択します。

図 6-2　　デバイス クレデンシャルの設定



クレデンシャルを追加したり、既存のクレデンシャルを変更、削除、または複製したりできます。CSPC サーバからすべてのクレデンシャルを削除するには、[すべて削除（Delete All）] ボタンをクリックします。

クレデンシャルは次のようなアプリケーションからインポートできます。

- Cisco Works DCR XML ファイル（.xml）
- Pari Networks クレデンシャル リポジトリ（.xml）
- Cisco Works DCR CSV ファイル（.csv）
- CNC CSV ファイル（.csv）
- 通常の CSV ファイル（.csv）

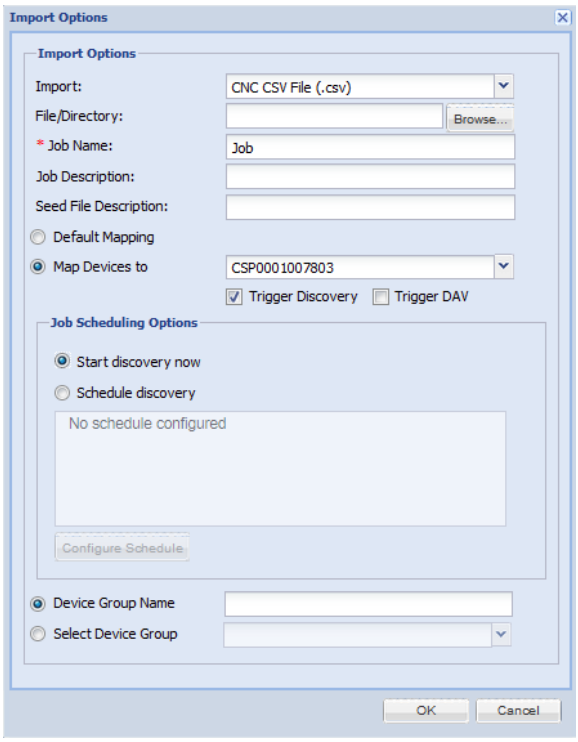
シード ファイルのインポート

シード ファイルはジョブとしてインポートできます。インポートするシード ファイルに含まれている各デバイス エントリのエラーまたは情報メッセージは、ジョブ ログの詳細の一部としてキャプチャされます。これらのメッセージは、ジョブ ログを表示することで確認できます。

シード ファイルをインポートする際には、元のシード ファイルに名前を付けて保存してください。これにより、必要に応じてデータベースからファイルを取得できます。

シード ファイルのインポート検出プロセスの中で、新しいデバイス グループを作成するか、既存のデバイス グループを選択し、検出されたデバイスをそのデバイス グループに追加します。デバイスはデフォルトの権限またはドロップダウンの権限にマッピングできます。検出および DAV はオプションであり、DCR CSV および CNC CSV 形式の場合にのみ指定できます。DAV は、検出オプションをオンにした場合にのみトリガーできます。

図 6-3　　[インポート オプション（Import Option）]



シード ファイルをインポートするには、以下の手順に従います。

ステップ 1 [デバイス クレデンシャルの設定（Device Credentials Configuration）] ウィンドウで、[インポート（Import）] ボタンをクリックします。

ステップ 2 [インポート（Import）] ドロップダウン ボックスから、次のいずれかのファイルを選択します。

- Cisco Works DCR XML ファイル（.xml）
- Pari Networks クレデンシャル リポジトリ（.xml）
- Cisco Works DCR CSV ファイル（.csv）
- CNC CSV ファイル（.csv）
- 通常の CSV ファイル（.csv）

ステップ 3 [参照（Browse）] ボタンをクリックして、インポートするシード ファイルを選択します。

ステップ 4 ジョブ名、ジョブの説明、シード ファイルの説明を、それぞれのフィールドに入力します。

ステップ 5 [デフォルトのマッピング（Default Mapping）] または [デバイスのマッピング先（Map Devices To）] を選択します。[デバイスのマッピング先（Map Devices To）] を選択した場合は、権限をドロップダウンから選択します。

注 [ジョブ名（Job Name）] は必須フィールドです。

ステップ 6 [OK] ボタンをクリックします。シード ファイルがインポートされます。

エクスポート

エクスポート オプションを使用して、既存のクレデンシャルをエクスポートできます。

図 6-4　　[エクスポート オプション（Export Options）]

コンテンツをエクスポートするには、以下の手順に従います。

ステップ 1 [デバイス クレデンシャルの設定（Device Credentials Configuration）] ウィンドウで、[エクスポート（Export）] ボタンをクリックします。

ステップ 2 パスワードの確認を促すメッセージが表示されます。

ステップ 3 CSPC へのログインに使用しているパスワードを入力します。

ステップ 4 [エクスポート形式（Export Format）] ドロップダウン ボックスから、次のいずれかの形式を選択します。

- Pari Networks クレデンシャル リポジトリ（.xml）
- CNC CSV ファイル（.csv）

ステップ 5 [OK] ボタンをクリックします。

ステップ 6 システムにファイルを保存します。

注・インポートしたシード ファイルに含まれているデバイスはすべて、CSPC の検出時に到達不能であっても管理対象デバイスとみなされます。

- 到達不能デバイスを含むシード ファイルをエクスポートできます。到達不能デバイスのステータスは、このシード ファイル *ManageDevicesCredentials.cvs* で「*Valid_Unreachable:Status*」と表示されます。

検出および DAV ジョブのトリガー

シード ファイルをインポートする際には、検出および DAV ジョブをトリガーすることもできます。これを行うには、以下の手順に従います。

ステップ 1 上の説明に従ってシード ファイルをインポートするための詳細を入力します。

ステップ 2 [インポート（Import）] ドロップダウン ボックスから、次の 2 つのオプションのいずれかを選択します。

- Cisco Works DCR CSV ファイル（.csv）
- CNC CSV ファイル（.csv）

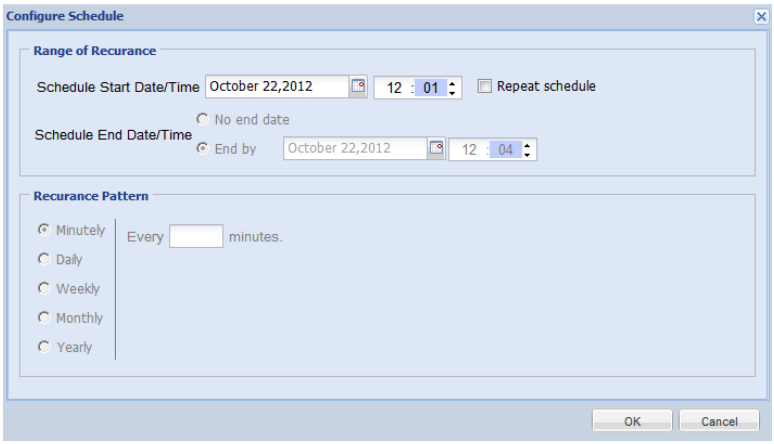
ステップ 3 [検出のトリガー（Trigger Discovery）] や [DAV のトリガー（Trigger DAV）] チェックボックスをオンにします。

ステップ 4 検出は今すぐ開始することも、後で開始するようにスケジュールすることもできます。後で開始するには、[検出のスケジュール（Schedule Discovery）] オプションを選択し、[スケジュールの設定

（Configure Schedule）] ボタンをクリックします。

ステップ 5 図 6-5 に示すように、スケジュールの開始日時と終了日時を設定するか、定期的なパターンとして [毎分（Minutely）]、[毎日（Daily）]、[毎週（Weekly）]、[毎月（Monthly）]、または [年に 1 回（Yearly）] を選択することができます。

図 6-5　　[スケジュールの設定（Configure Schedule）]



ステップ 6 [デバイス グループ名（Device Name）] フィールドにデバイス グループ名を入力します。

ステップ 7 または [デバイス グループ名の選択（Select Device Group Name）] オプション ボタンをクリックし、
ドロップダウン ボックスからデバイス グループ名を選択します。

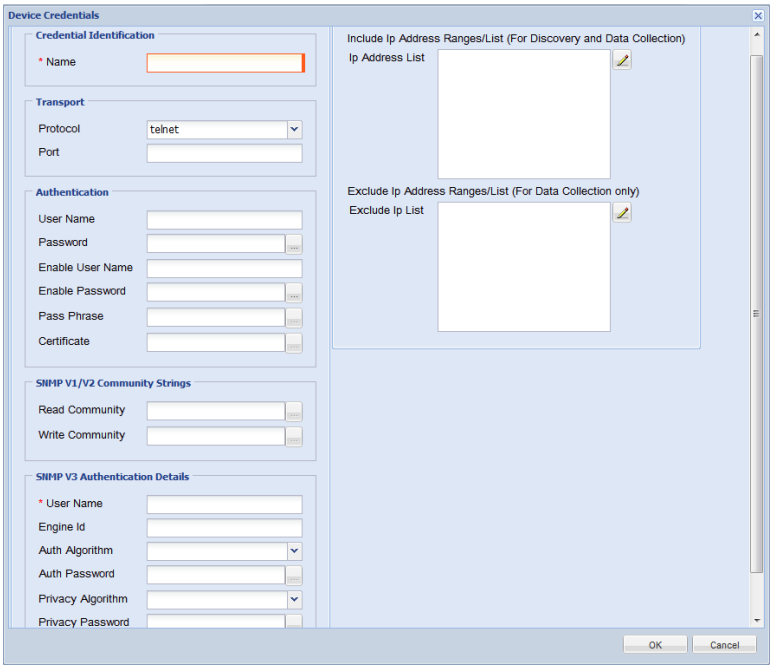
ステップ 8 [OK] ボタンをクリックします。

CSPC フローチャートに戻る

クレデンシャルの追加

クレデンシャルを追加するには、[デバイス クレデンシャル（Device Credentials）] 画面で [追加（Add）] をクリックします。

図 6-6　　クレデンシャルの追加



クレデンシャルを追加するには、以下の手順に従います。

ステップ 1 新しいクレデンシャルを作成するために次の情報を入力します。

- クレデンシャルの名前（クレデンシャルを識別するためにユーザが選択した名前）。
- 転送プロトコル（CSPC は、Telnet、SSHv1、SSHv2、HTTP、HTTPS、SNMPv1、SNMPv2c、SNMPv3、WMI、TL1、IIOP など、データ収集のためのさまざまなプロトコルをサポートしています）。
- 認証（選択したプロトコルに応じて、以下の認証メカニズムを使用します）。
  - Telnet、SSH、HTTP、HTTPS プロトコルの場合は、[ユーザ名（User Name）]、[パスワード（Password）]、[ユーザ名の有効化（Enable User Name）]、および [パスワードの有効化（Enable Password）] を入力します。
  - SSH プロトコル証明書ベースの認証の場合は、[ユーザ名（User Name）] と [証明書（Certificate）]（パス フレーズあり、またはパス フレーズなし）を入力します。
  - WMI プロトコルの場合は、[ユーザ名（User Name）] と [パスワード（Password）] を入力します。
  - SNMP V1 および V2 の場合は、[読み取りコミュニティ（Read Community）] 文字列と [書き込みコミュニティ（Write Community）] 文字列を入力します。
  - SNMP V3 の場合は、[ユーザ名（User Name）]、[エンジン ID（Engine ID）]、使用する [認証アルゴリズム（Auth Algorithm）]、[認証パスワード（Auth Password）]、[プライバ

シー アルゴリズム（Privacy Algorithm）]、および [プライバシー パスワード（Privacy Password）] を入力します。

- TL1 プロトコルの場合は、[ユーザ名（User Name）] と [パスワード（Password）] を入力します。

- [IP アドレス範囲を含める（Include IP Address Range）] および [IP アドレス範囲を除外する（Exclude IP Address Range）]。

  [IP アドレス範囲を含める（Include IP Address Range）] オプションを使用すると、一連の IP アドレス、または 10 で始まるすべての IP アドレスを示す、10.*.*.* のようなワイルドカード IP アドレスを入力できます。[IP アドレス範囲を除外する（Exclude IP Address Range）] は、データ収集においてのみ有効です。

  IP アドレスを入力するには、[IP アドレス リスト（IP Address List）] のエディタをクリックし、[IP アドレス リスト（IP Address List）] フィールドに複数の IP アドレスをカンマ区切りで入力します。

ステップ 2 [OK] をクリックします。

[変更（Modify）] をクリックして、既存のクレデンシャルを編集することもできます。選択したクレデンシャルを削除するには [削除（Delete）] をクリックします。選択したクレデンシャルのコピーを作成して変更するには、[複製（Clone）] をクリックします。

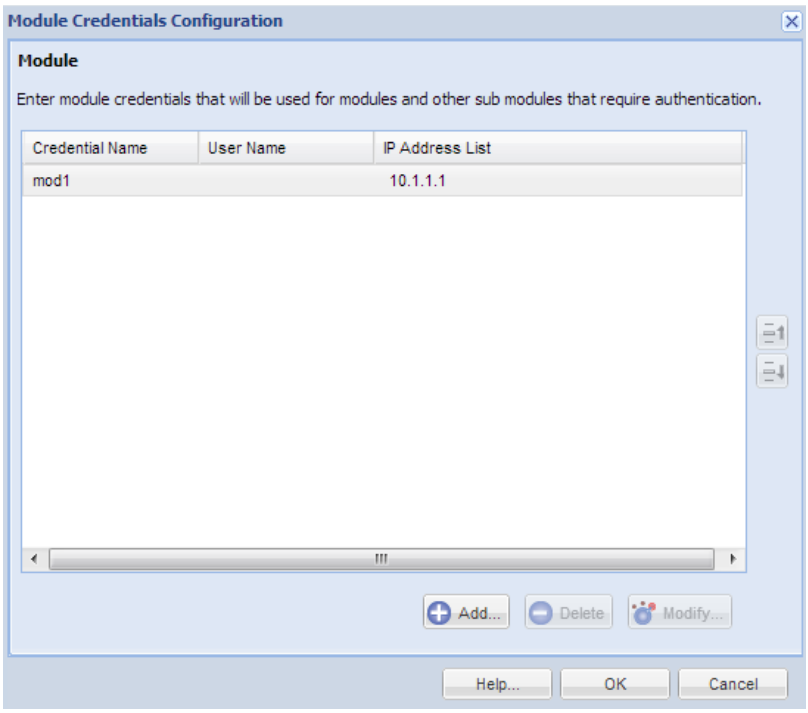
CSPC フローチャートに戻る

[サブ モジュール クレデンシャルの管理（Manage Sub Module Credentials）]

モジュールからデータを収集するためには、まずクレデンシャルを入力する必要があります。モジュール クレデンシャルは、モジュール、または追加の認証が必要なサブ モジュールからデータを収集するために使用されます。

クレデンシャルを追加するには、モジュール クレデンシャル ウィザードを使用します。ウィザードの手順に従って、クレデンシャルのパラメータを選択します。

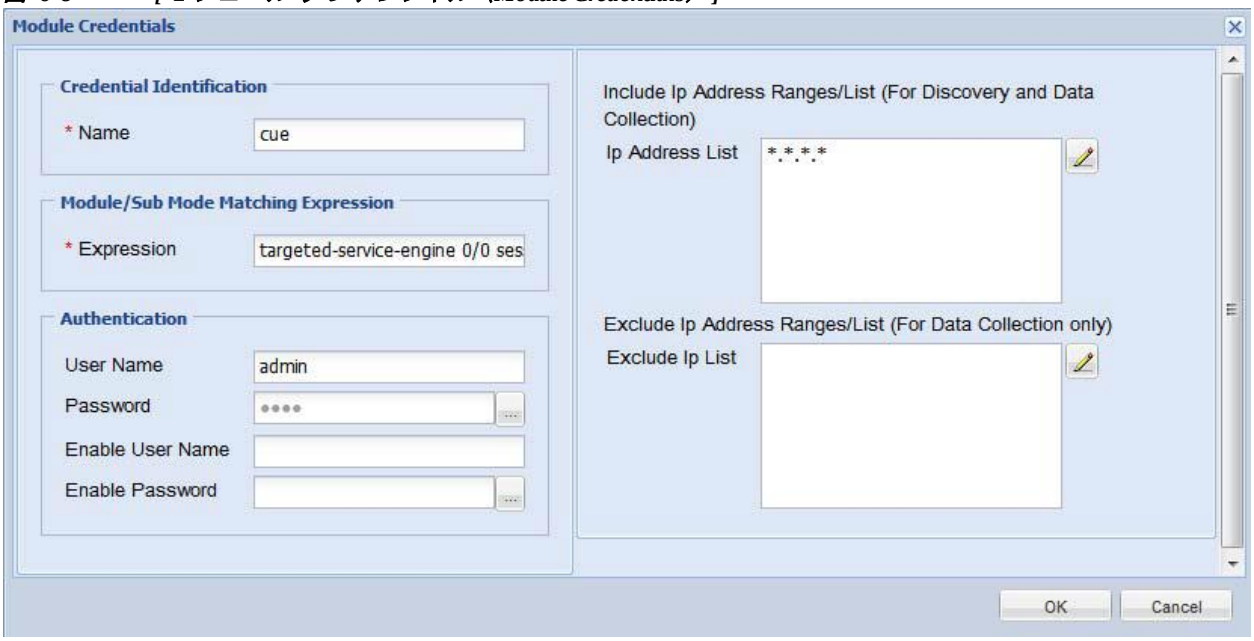
図 6-7　　モジュール クレデンシャルのメイン ウィンドウ



クレデンシャルを追加したり、既存のクレデンシャルを変更または削除したりできます。縦方向のスクロール バーを使用すると、表内の前後のクレデンシャルに移動できます。

クレデンシャルを追加するには、図 6-8 に示す [モジュール クレデンシャル（Module Credentials）] 画面で
[追加（Add）] をクリックします。

図 6-8　　[モジュール クレデンシャル（Module Credentials）]



モジュール クレデンシャルを追加するには、以下の手順に従います。

ステップ 1 新しいクレデンシャルを作成するために次の情報を入力します。

- クレデンシャルの名前（クレデンシャルを識別するためにユーザが選択した名前）。
- [モジュール/サブモード マッチング表現（Module/Sub Mode Matching Expression）]（このクレデンシャルをモジュールに使用するかしないか、マッチングするために使用される表現）。
- 認証（選択したプロトコルに応じて、以下の認証メカニズムを使用します）。
  - モジュールにアクセスするための [ユーザ名（User Name）]、[パスワード（Password）]、[ユーザ名の有効化（Enable User Name）]、および [パスワードの有効化（Enable Password）] を入力します。
- [IP アドレス範囲を含める（Include IP Address Range）] および [IP アドレス範囲を除外する（Exclude IP Address Range）]。

  [IP アドレス範囲を含める（Include IP Address Range）] オプションを使用すると、一連の IP アドレス、または 10 で始まるすべての IP アドレスを示す、10.*.*.* のようなワイルドカード IP アドレスを入力できます。[IP アドレス範囲を除外する（Exclude IP Address Range）] は、データ収集においてのみ有効です。

  IP アドレスは、[IP アドレス リスト（IP Address List）] のエディタをクリックして入力します。

ステップ 2 [OK] をクリックします。

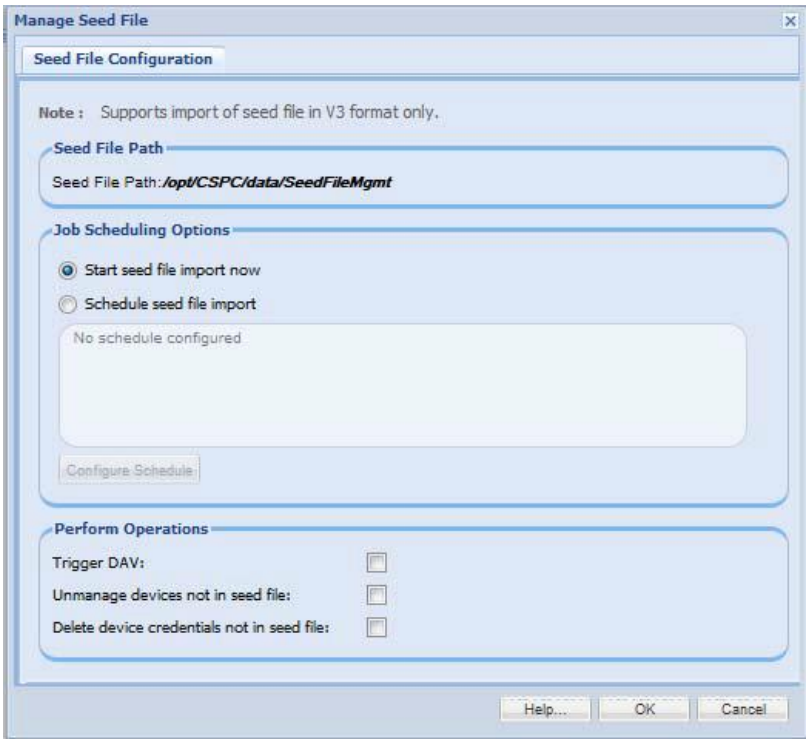
[変更（Modify）] をクリックして、既存のクレデンシャルを編集することもできます。クレデンシャルを削除するには [削除（Delete）] をクリックします。

CSPC フローチャートに戻る

[シード ファイルの管理（Manage Seed File）]

最新のクレデンシャルとデバイスを含むシード ファイルをインポートできます。これを行うには、目的のシード ファイルを手動でデフォルト パスに配置します。削除、更新、または追加されるデバイスが決定され、必要なアクションが実行されます。シード ファイルに存在せず、CSPC に含まれているデバイスは削除されます。

図 6-9　　シード ファイルの設定



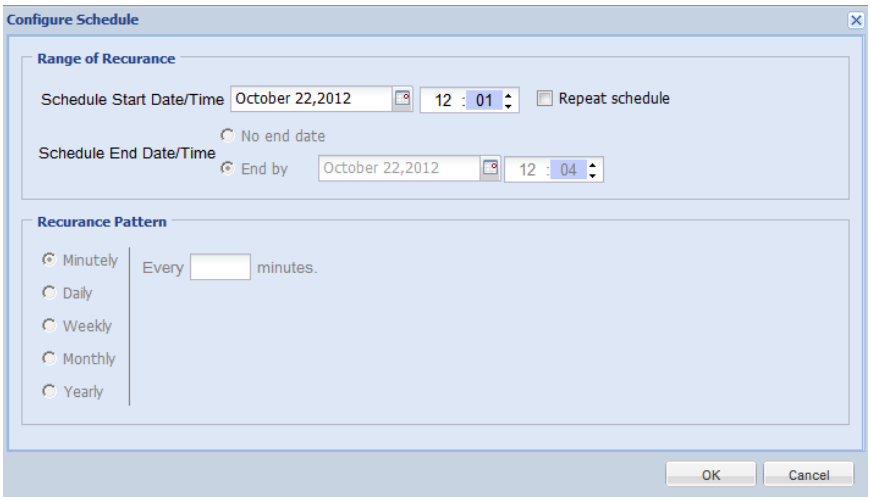
シード ファイルをインポートするには、以下の手順を実行します。

ステップ 1　画面に表示されるデフォルトの場所に CNC V3 形式のシード ファイルを配置します。シード ファイルは必ず画面に表示される場所に配置し、CSPC ユーザに対してファイルの読み取り権限を許可する必要があります。

ステップ 2　シード ファイルのインポートはすぐに開始することも、後で開始するようにスケジュールすることもできます。後で開始するには、[シード ファイルのインポートのスケジュール（Schedule Seed file import）] オプションを選択し、[スケジュールの設定（Configure Schedule）] ボタンをクリックします。

ステップ 3　スケジュールの開始日時と終了日時を設定するか、定期的なパターンとして [毎分（Minutely）]、
[毎日（Daily）]、[毎週（Weekly）]、[毎月（Monthly）]、または [年に 1 回（Yearly）] を選択することができます（図 6-10 参照）。

図 6-10　　[スケジュールの設定（Configure Schedule）]



ステップ 4 必要な操作をチェックし、[OK] をクリックします。

図 6-11 操作

オプション	説明
DAV をトリガーする（Trigger DAV）	デバイス アクセス検証をトリガーします。
シード ファイルに含まれていないデバイスを管理対象外にする（Unmanage devices not in seed file）	シード ファイルに含まれていないデバイスを管理対象外にします。
シード ファイルに含まれていないデバイスを削除する（Delete device credentials not in seed file）	シード ファイルに含まれていないデバイス クレデンシャルのみを削除します。

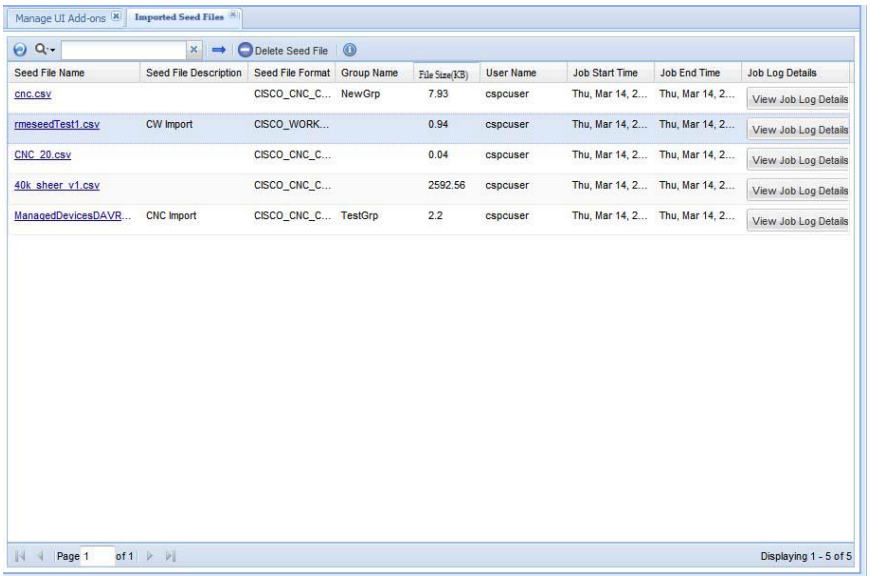
[インポートされたシード ファイル（Imported Seed file）]

シード ファイルをインポートすると、情報は [インポートされたシード ファイル（Imported Seed file）] 画面に表示されます。画面の各行は 1 つのインポートに対応します。

図 6-12 に示すように、[シード ファイル名（Seed File Name）] フィールドはハイパーリンクとして機能します。このリンクをクリックすると、システムに保存されている元のシード ファイルをダウンロード（またはエクスポート）できます。画面には、ファイル形式、ユーザ情報、ファイル サイズなどインポートに関連するすべての詳細とインポート実行のジョブ ログの詳細がキャプチャされます。

画面から 1 つまたは複数の行を削除することができます。

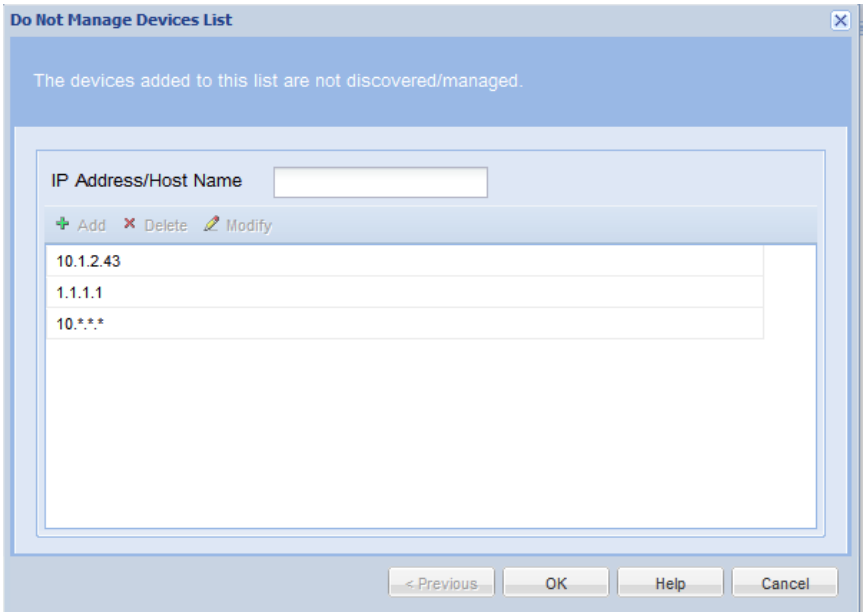
図 6-12　　インポートされたシード ファイル



[管理対象外デバイス リスト（Do Not Manage Device List）]

このリストには、コレクタの管理対象外とする一連のデバイスを選択するためのオプションがあります。デバイスを [管理対象外デバイス リスト（Do Not Manage Device List）] に追加した場合、そのデバイスは検出されず、CSPC に追加されません。

図 6-13　　[管理対象外デバイス リスト（Do Not Manage Device List）]



上の画面に示すように、IP アドレスが *10.*.*.**、*1.1.1.1*、および *10.1.2.43* の 3 台のデバイスは、すべて検出されたとしても、インベントリは実行されません。

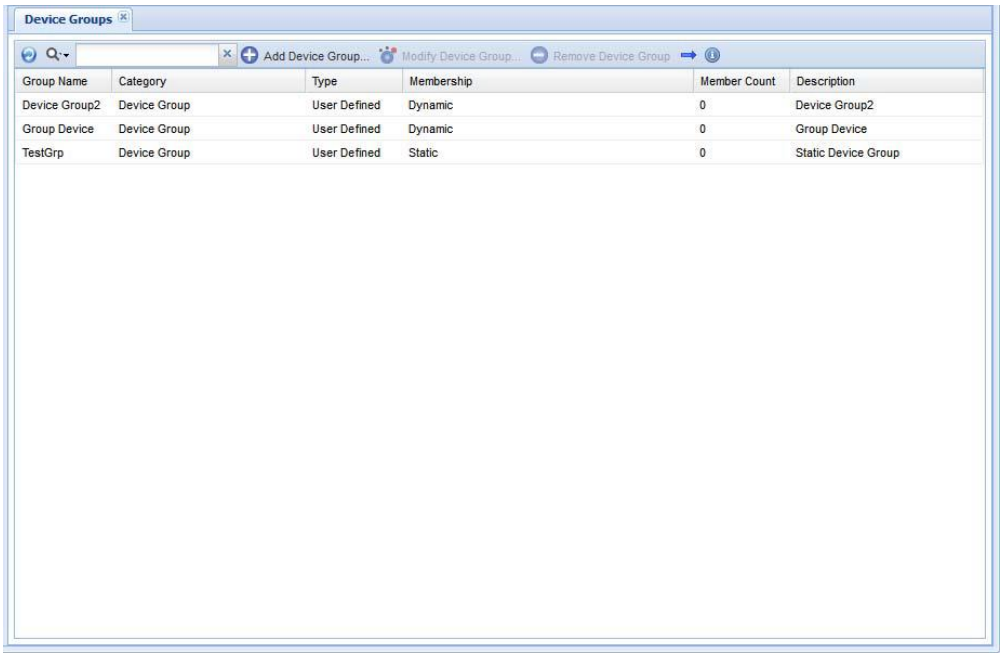
[デバイスのグループ化（Device Grouping）]

[デバイス管理（Device Management）] タブの [デバイス グループ（Device Groups）] サブ タブを使用して、デバイス グループの作成と管理を行います。

[デバイス グループ（Device Groups）]

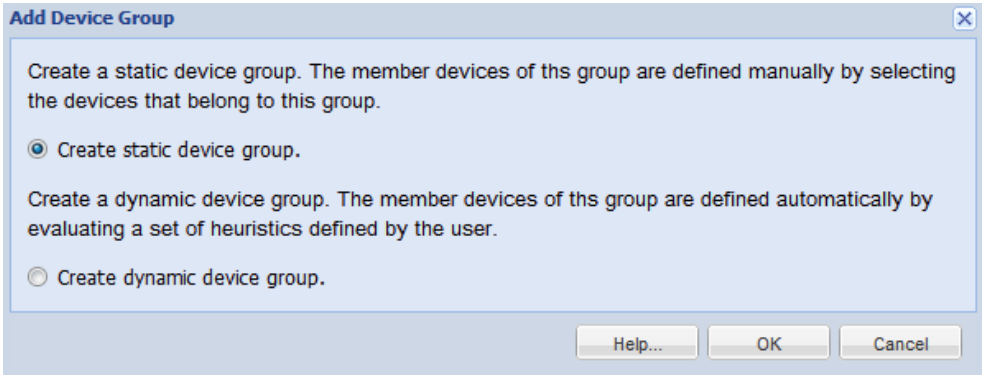
[デバイス グループ（Device Groups）] オプションは、デバイス グループを追加、変更、または削除する場合に使用します。CSPC には、システムによって生成された特定のデフォルト グループがあります。また、デバイス グループを作成する場合は、以下の設定を使用できます。デバイス グループは、静的または動的にできます。静的デバイス グループでは、特定のグループに属するデバイスを手動で選択する必要があります。動的グループでは、条件を定義します。その条件（現在管理対象か管理対象外か）に一致するすべてのデバイスが自動的にこのグループに表示されます。

図 6-14　　デバイス グループのメイン ウィンドウ



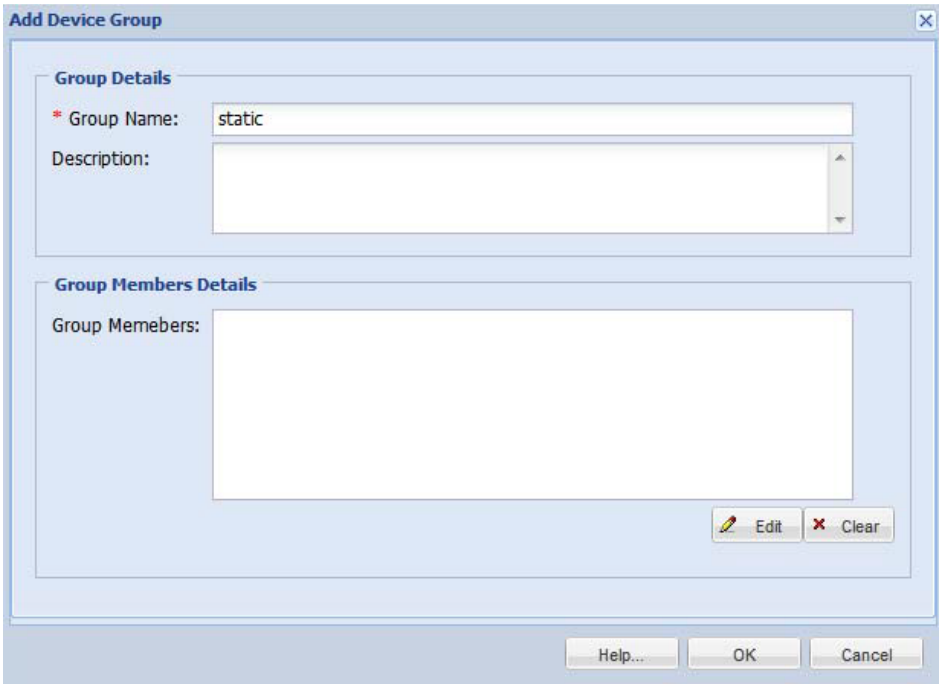
[デバイス グループの追加（Add Device Group）] を選択したら、静的グループを作成するか、動的グループを作成するかを選択します。

図 6-15　　[デバイス グループの追加（Add Device Group）]



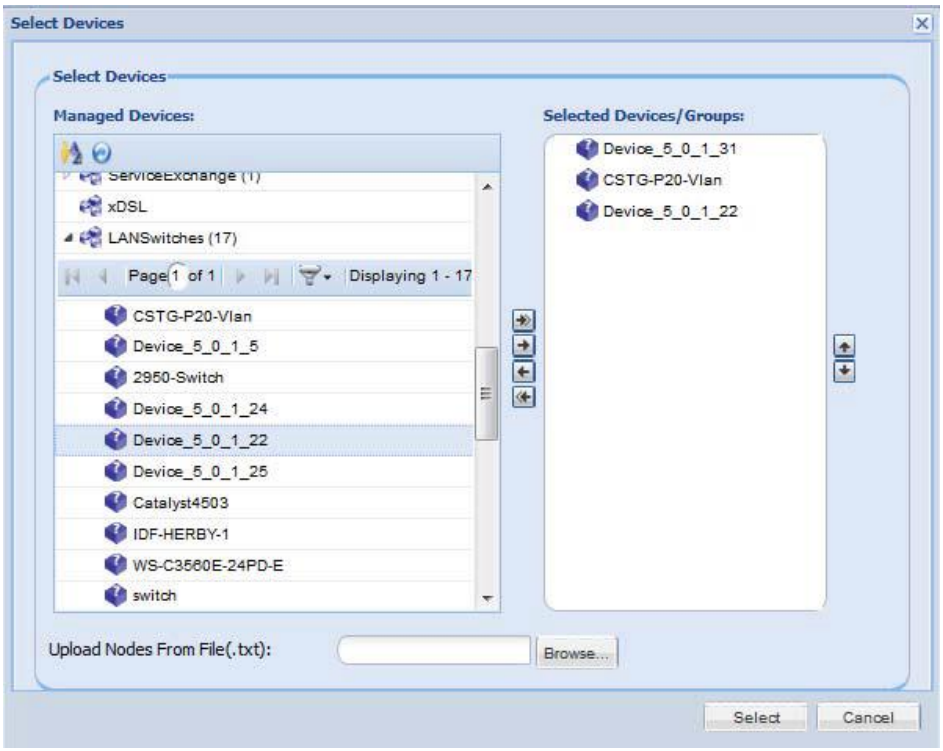
静的グループの作成については、以下を参照してください。

図 6-16　　静的グループの作成



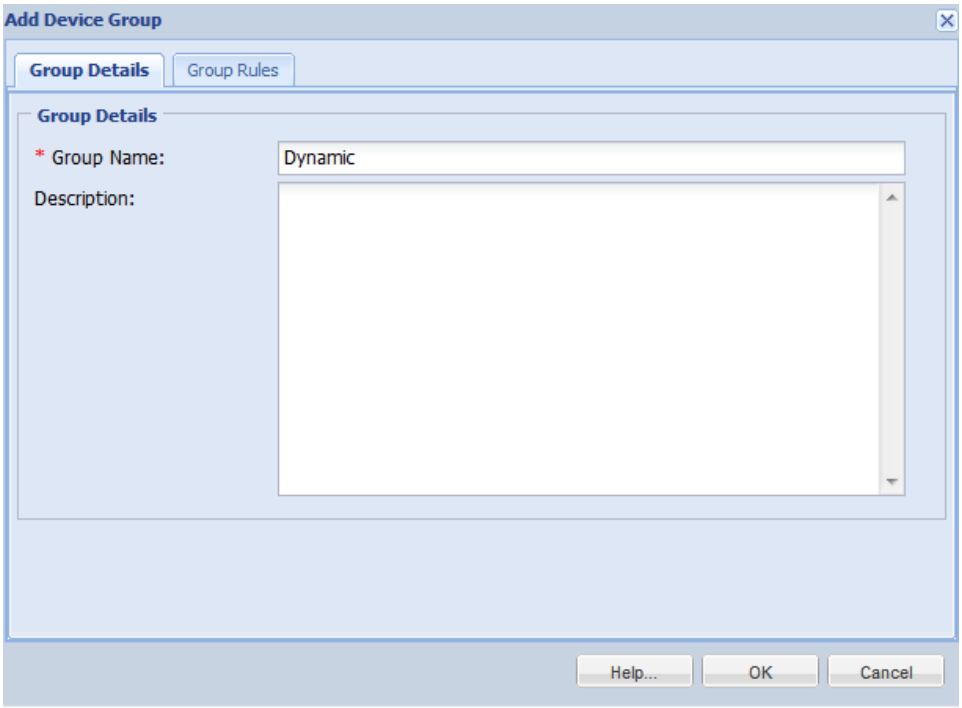
グループ名と説明を入力します。ウィンドウ内の [編集（Edit）] をクリックしてグループ メンバーを選択します。
デバイスを選択するか、[参照（Browse）] をクリックしてデバイスを含む .txt ファイルをアップロードしたら、[OK] をクリックして静的デバイス グループを作成します。

図 6-17　　[管理対象デバイス（Managed Devices）]



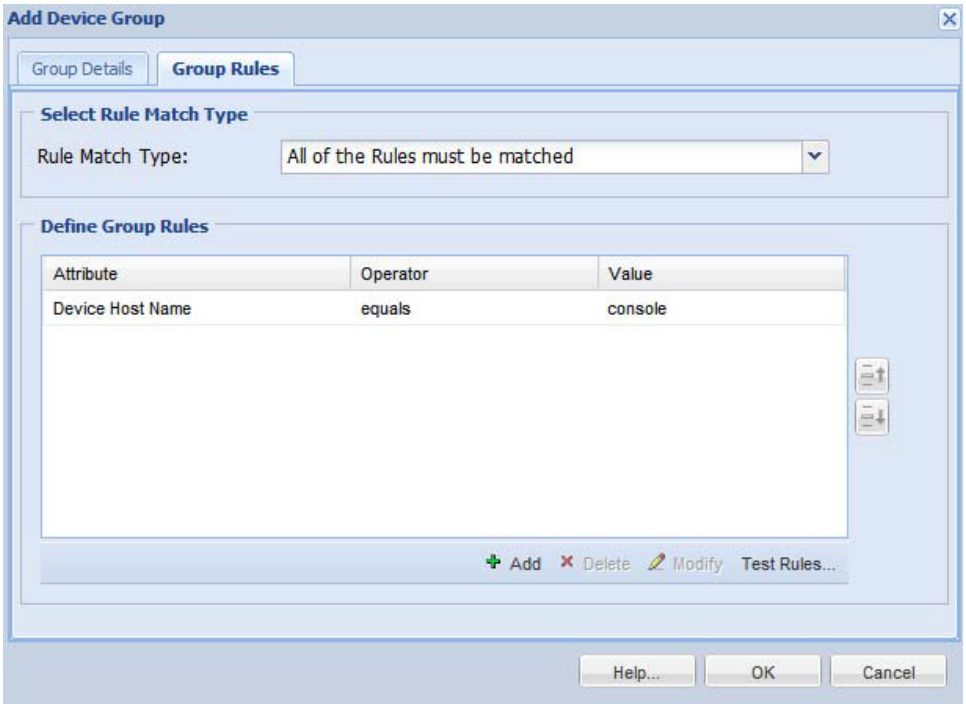
同様に、新規デバイス グループの作成時に動的グループ オプションを選択する場合は、ヒューリスティックを定義してその特定のグループに属するデバイスを指定できます。これを示しているのが図 6-18 です。

図 6-18　　動的グループの追加



グループ名と説明を定義したら、次に示すようにグループ ルールを定義できます。

図 6-19　　グループ ルールの追加



属性や値に基づき一致する必要がある、または一致しない条件またはルールを定義します。

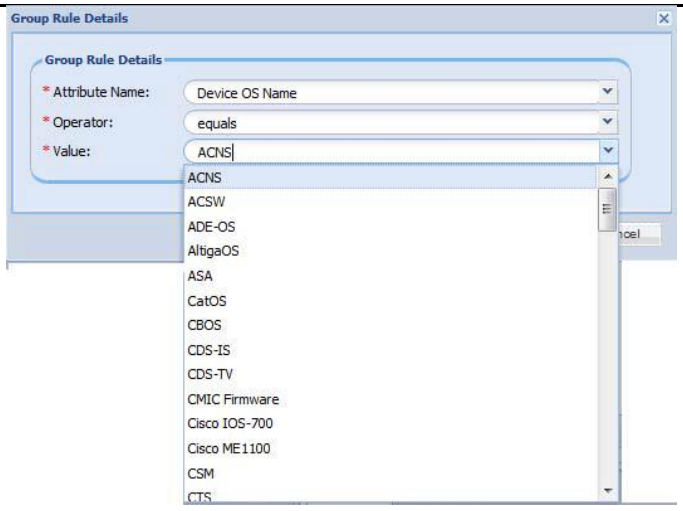
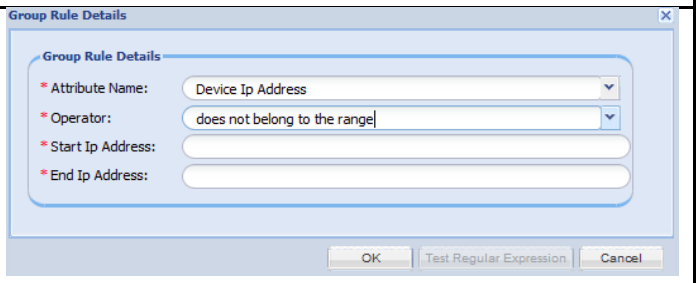
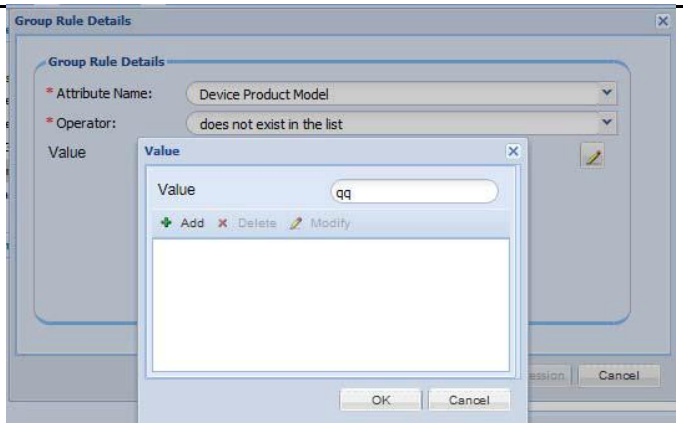
[追加（Add）] をクリックして、それらの条件を追加します。

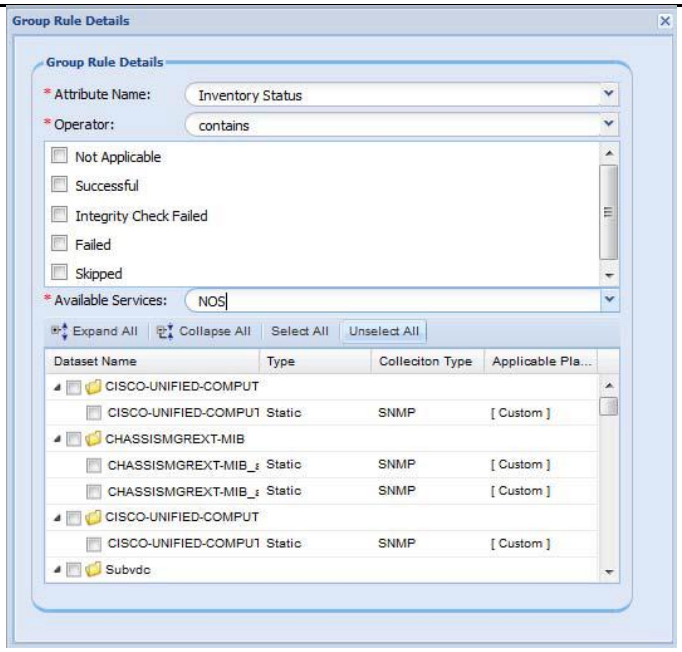
図 6-20 [グループ ルール詳細（Group Rule Details）]

[デバイスのホスト名（Device Host Name）]、[デバイスの OS バージョン（Device OS Version）]、[デバイスのベンダー名（Device Vendor Name）]、[デバイスの製品モジュール（Device Product Module）]、または [デバイスの IP アドレス（Device IP Address）] などの属性を選択し、[等しい（equals）]、[リストに含まれている（contains in the list）] などの演算子を使用して、値を入力します。ルールはいくつでも作成できます。

新たに検出されるデバイスは、自動的にこれらの条件と一致し、動的グループに追加されます。

表 6-1 グループ ルールの特殊なケース

特殊ケース	図
[デバイスの OS 名（Device OS Name）] を [属性名（Attribute Name）] として選択した場合は、ドロップダウンから値を選択する必要があります。	
[デバイスの IP アドレス（Device IP Address）] を [属性名（Attribute Name）] として選択し、[範囲に属さない（does not belong to the range）] を [演算子（Operator）] として選択した場合は、[開始 IP アドレス（Start Ip Address）] と [終了 IP アドレス（End Ip Address）] を入力する必要があります。	
任意の [属性名（Attribute Name）] を選択し、[リストに存在しない（does not exist in the list）] を [演算子（Operator）] として選択した場合は、画面の編集アイコンを使用して、手動で [値（Value）] を追加する必要があります。	

特殊ケース	図
[インベントリ ステータス（Inventory Status）] または [設定ステータス（Config Status）] を [属性名（Attribute Name）] として選択し、 [含む（contains）] または [含まない（does not contain）] を [演算子（Operator）] として選択した場合は、画面で必要なステータスを選択し、ドロップダウンから [使用可能なサービス（Available Services）] を選択します。[インベントリ ステータス NOS（Inventory Status NOS）] を選択した場合のみ、すべてのデータセット名が表示され、リストに選択できます。 インベントリ ステータスには詳細な情報が表示されます。データセットの仕様に基づいてグループを作成する場合は、インベントリ ステータスに基づいてルールを作成することを推奨します。	

[全般設定（General Settings）]

[デバイス管理（Device Management）] タブの [全般設定（General Settings）] サブ タブを使用して、アプリケーション、検出、インベントリ、ジョブ詳細を設定します。

この項では、[全般設定（General Settings）] オプションの以下の項目について説明します。

- [アプリケーション設定（Application Settings）]
- [検出設定（Discovery Settings）]
- [インベントリ設定（Inventory Settings）]
- [ジョブ詳細設定（Advanced Job Settings）]

[アプリケーション設定（Application Settings）]

[アプリケーション設定（Application Settings）] では、デバイス プロンプト、サブモード、データ エクスポート設定などデバイスのインベントリ データの収集設定を設定できます。

全般設定：

[IP ホスト マスク設定（IP Host Mask Settings）]：デバイスの IP アドレスとホスト名のデータ プライバシーが有効になっている場合、シスコに送信される顧客デバイスの IP アドレスとホスト名はユーザ定義の IP アドレスとホスト名のセットに置き換えられます。

[IP アドレス マスク（IP Address Mask）] フィールドでは顧客の実際の IP アドレスの置換に使用する IP アドレス範囲を定義でき、[ホスト名マスク（Hostname Mask）] フィールドでは顧客の実際のホスト名の置換に使用するプレフィックスを定義できます。

図 6-21　　[全般設定（General Settings）]

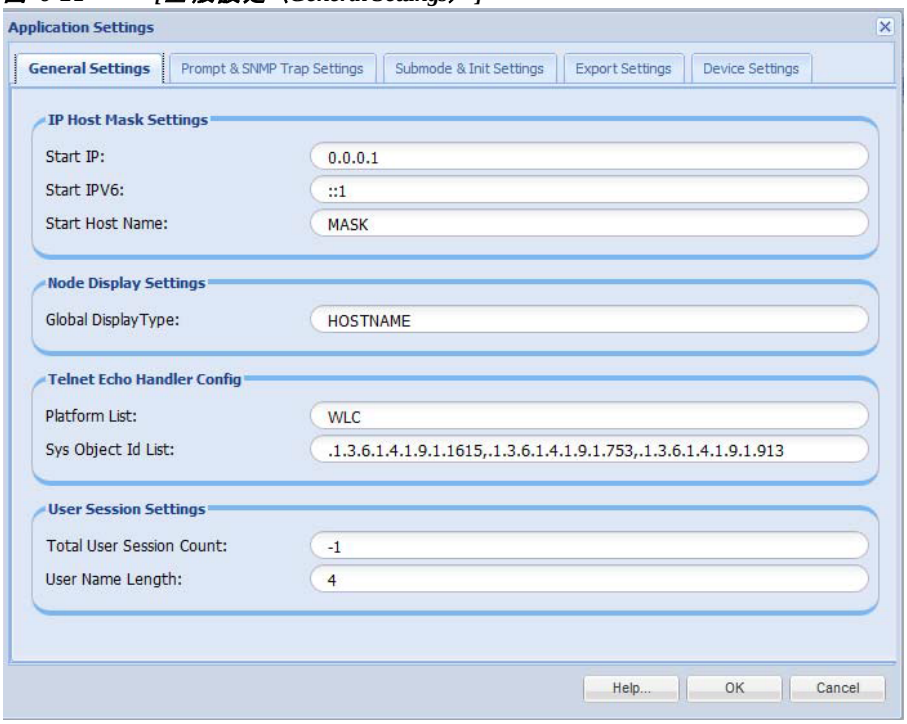


表 6-2 [全般設定（General Settings）]

フィールド名	説明
開始 IP（Start IP）	IPv4 データのマスキングにおいて開始値として設定するIPアドレスマスクされる各IPアドレスはこの値から 1 ずつ増加します。
開始 IPv6（Start IPv6）	IPv6 データのマスキングにおいて開始値として設定するIPアドレスマスクされる各 IPアドレスはこの値から 1 ずつ増加します。
開始ホスト名（Start Hostname）	ホスト名のマスクに使用するプレフィックス。
グローバル表示タイプ（Global Display Type）	デバイスごとに表示されるデバイス属性。
プラットフォーム リスト（Platform List）	Telnet エコーが有効になっているプラットフォームのリスト。

SysObject ID リスト（SysObject ID List）	Telnet エコーが有効になっているデバイスの SystemObject ID。
合計ユーザ セッション数（Total User Session Count）	固有の CSPC ユーザ セッションの最大数。

プロンプト設定：

図 6-22　　[プロンプト設定（Prompt Settings）]

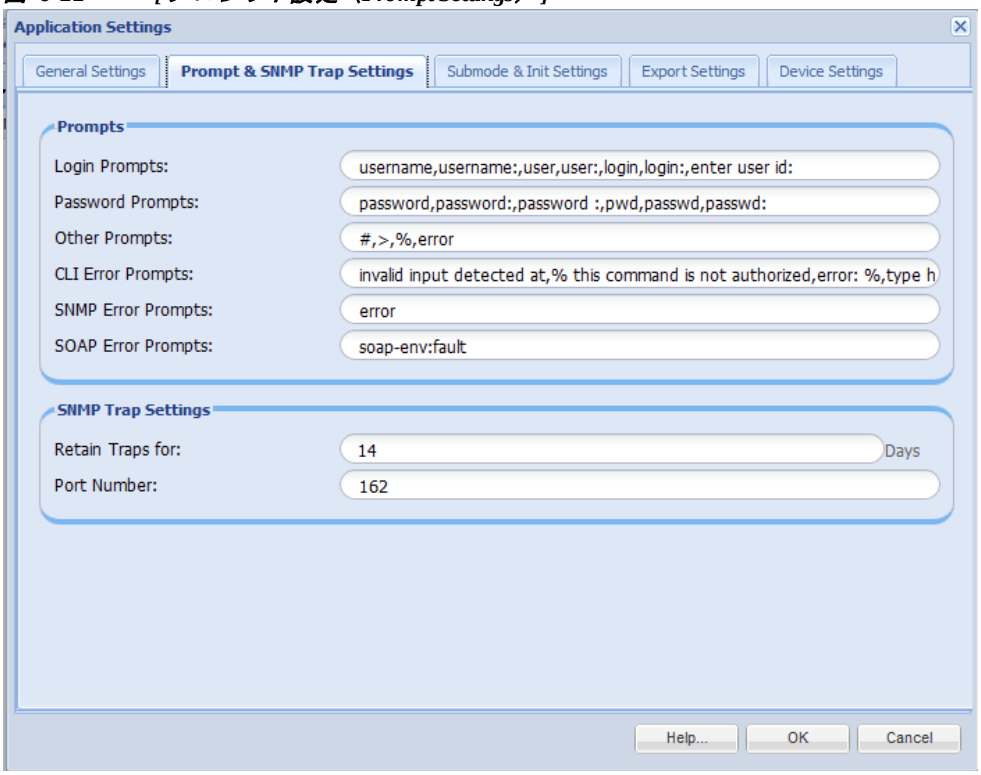


表 6-3 [プロンプト設定（Prompt Settings）]

フィールド名	説明
プロンプト（Prompts）	
ログイン プロンプト（Login Prompts）	CSPC で処理する必要がある追加のログイン プロンプトに使用されます。
パスワード プロンプト（Password Prompts）	CSPC で処理する必要がある追加のパスワード プロンプトに使用されます。
その他のプロンプト（Other Prompts）	その他に使用されます。
CLI エラー プロンプト（CLI Error Prompts）	CSPC で処理する必要がある追加の CLI エラー プロンプトに使用されます。
SNMP エラー プロンプト（SNMP Error Prompts）	CSPC で処理する必要がある追加の SNMP エラー プロンプトに使用されます。
SOAP エラー プロンプト（SOAP Error Prompts）	CSPC で処理する必要がある追加の SOAP エラー プロンプトに使用されます。
SNMP トラップ設定（SNMP Trap Settings）	
トラップの保持期間（Retain Traps for）	トラップを保持する日数を指定します。
SNMP トラップ メッセージを受信するポートを設定します。デフォルト ポートは 162 です。 注 SNMP トラップ メッセージをリッスンする新しい着信ポートを設定する場合は、対応する IP テーブル ルールと NAT ルータ設定を手動で更新する必要があります。	SNMP トラップ メッセージを受信するポートを設定します。デフォルト ポートは 162 です。 注 SNMP トラップ メッセージをリッスンする新しい着信ポートを設定する場合は、対応する IP テーブル ルールと NAT ルータ設定を手動で更新する必要があります。

[サブモードおよび初期設定（Submode & Init Settings）]

図 6-23　　[サブモードおよび初期設定（Submode & Init Settings）]

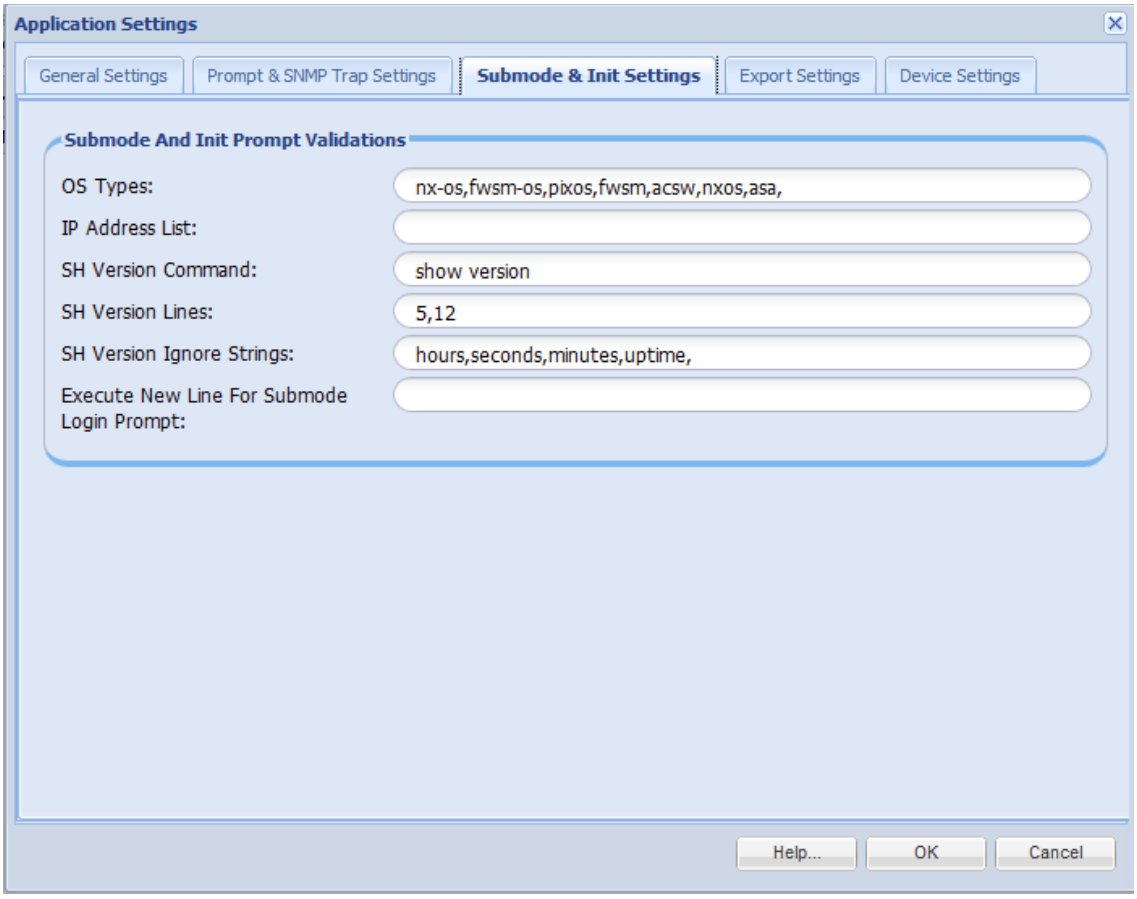


表 6-4 [サブモードおよび初期設定（Submode & Init Settings）]

フィールド名	説明
OS タイプ（OS Type）	OS のタイプ。
IP アドレス リスト（IP Address List）	IP アドレスのリスト。
SH Version コマンド（SH Version Command）	サブモード中に show version を実行する必要があるかどうかを指定します。
SH Version の行数（SH Version Lines）	show version の出力から取得する必要がある行数。
SH Version の無視設定（SH Version Ignore Strings）	show version 設定を考慮するか無視するかを指定します。
サブモード ログイン プロンプトでニューラインを実行（Execute New Line for Submode Login Prompt）	サブモード ログイン プロンプトの終了時にニューラインを実行する必要があるかどうかを指定します。

エクスポート設定 :

図 6-24　　[エクスポート設定（Export Settings）]

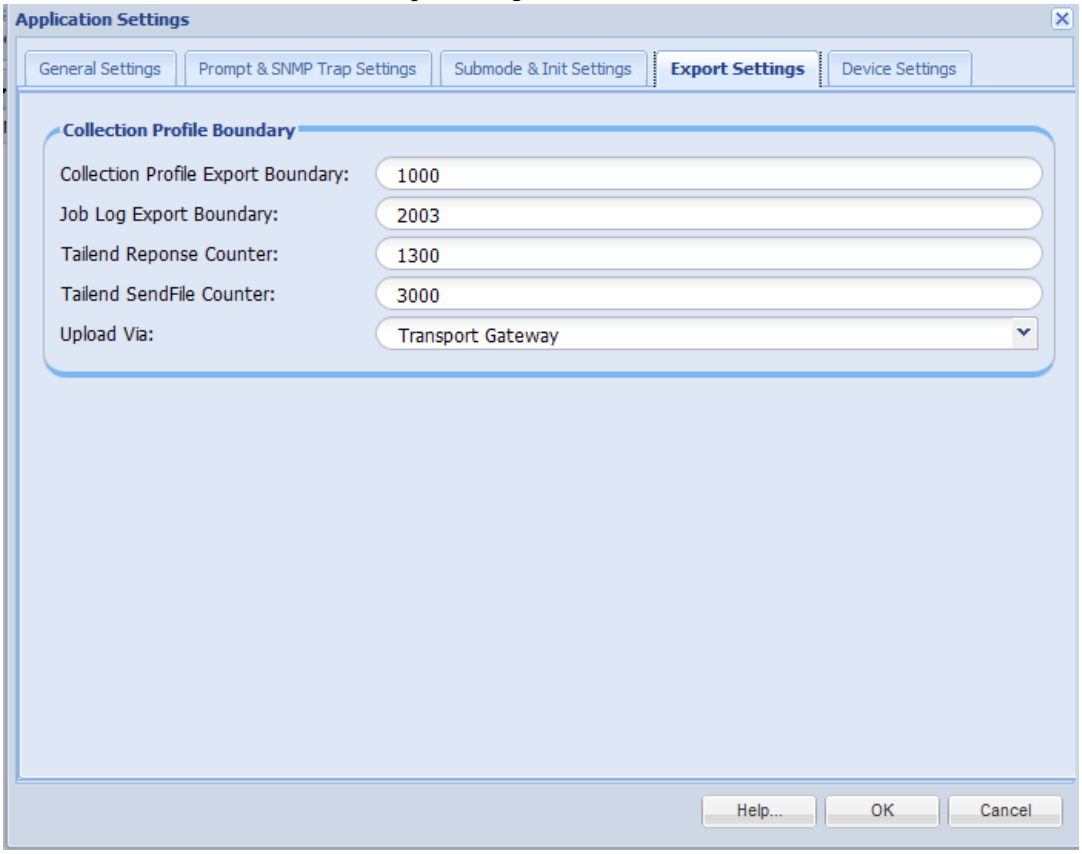


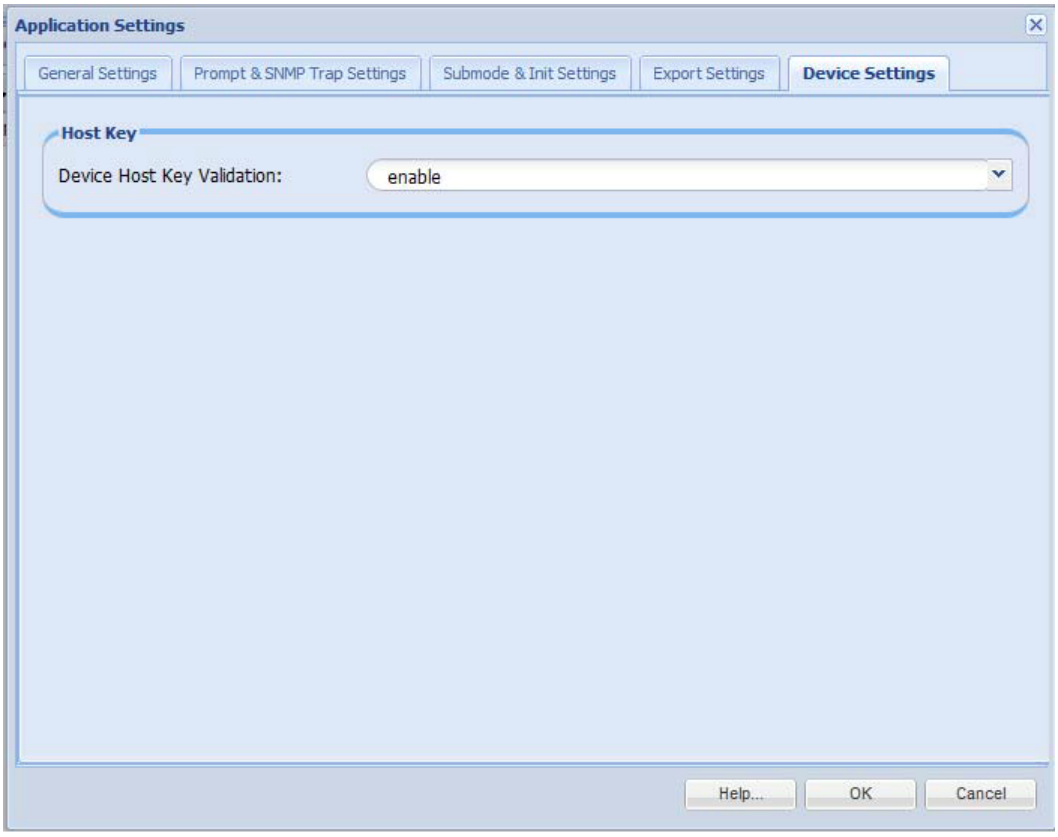
表 6-5 [エクスポート設定（Export Settings）]

フィールド名	説明
収集プロファイルのエクスポート境界（Collection Profile Export Boundary）	VSEM のエクスポート境界設定。
ジョブ ログのエクスポート境界（Job Log Export Boundary）	ジョブ ログのエクスポート境界。
TailEnd 応答カウンタ（TailEnd Response Counter）	TailEnd の応答カウンタ。
TailEnd シード ファイル カウンタ（TailEnd SeedFile Counter）	TailEnd のシード ファイル カウンタ。
アップロード方法（Upload Via）	アップロード方法オプションを次のいずれかに設定します。 • [トランスポート ゲートウェイ（Transport Gateway）] • [接続（Connectivity）] • [NetAuth-SSL] • [無効（Disabled）]

デバイス設定：

SSH 通信時にデバイスでキーを有効または無効にします。無効にした場合、同じキーが繰り返し使用されるか、新しいキーが生成されます。

図 6-25　　[デバイス設定（DeviceSettings）]



[検出設定（Discovery Settings）]

[検出設定（Discovery Settings）] では、デバイス検出の設定を変更できます。検出タイムアウト、含めるプラットフォーム、除外するプラットフォームを設定できます。

[設定（Preferences）] タブで、図 6-26 に示すように値を入力します。

図 6-26　　[検出設定（Discovery Settings）]

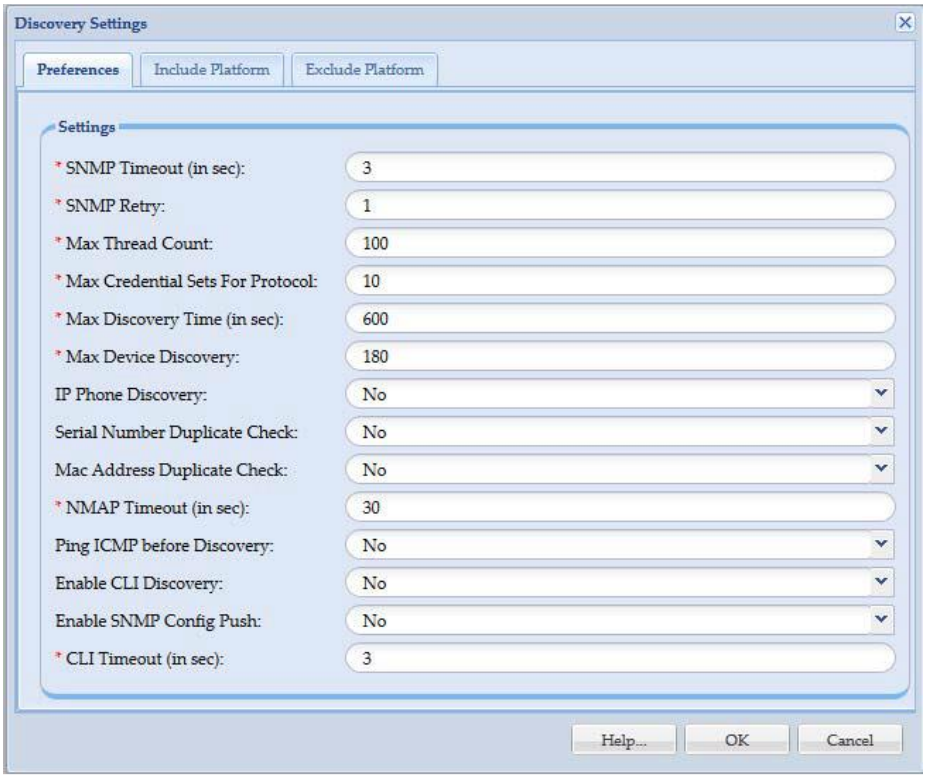


表 6-6 検出タイムアウト

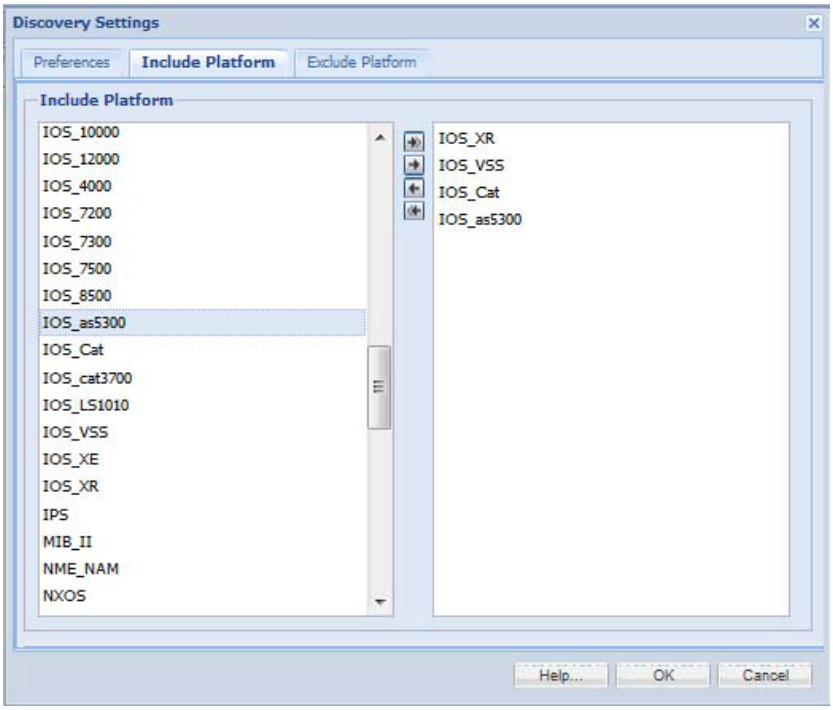
フィールド名	説明
SNMP タイムアウト（秒）（SNMP Timeout (in sec)）	SNMP 接続のタイムアウト値（秒単位）。デフォルト値は 3 秒です。
SNMP 再試行（SNMP Retry）	SNMP 接続の再試行回数。デフォルト値は 1 です。
最大スレッド数（MaxThread Count）	各検出ジョブのスレッド プールのサイズ。デフォルト値は 100 です。
プロトコルに使用するクレデンシャル セットの最大数（MaxCredential Sets For Protocol）	各プロトコルに使用するクレデンシャル セットの最大数。 デフォルト値は 50 です。
最大検出時間（秒）　（MaxDiscovery Time (in sec)）	各検出ジョブの最大検出時間（秒単位）。 デフォルト値は 600 秒です。有効な値は 0 または 60 以上です。0 を指定した場合、猶予時間は適用されません。0 ～ 60 の値を設定すると、デフォルト値の 600 が使用されます。
最大デバイス検出時間（MaxDevice Discovery）	一つのデバイスの最大検出時間（秒単位）。デフォルト値は 180 秒です。有効な値 : 5 秒以上。値が

フィールド名	説明
	5 未満の場合は、5 が適用されます。
IP Phone の検出（IP Phone Discovery）	IP Phone の検出を有効または無効にできます。
シリアル番号重複チェック（Serial Number Duplicate Check）	シリアル番号が重複していないかチェックします。
[MAC アドレスの重複チェック（Mac Address Duplicate Check）]	MAC アドレスが重複していないかチェックします。
NMAP タイムアウト（秒）（NMAP Timeout (in sec)）	Nmap アプリケーションを使用したデバイス検出のタイムアウト値（秒単位）。デフォルト値は 30 秒です。有効な値は 0 以上です。値が 0 未満の場合は、デフォルト値が適用されます。
検出前に ICMP を ping（Ping ICMP before Discovery）	有効または無効にできます。有効にした場合、検出前にデバイスに対して ping を実行します。
CLI 検出の有効化（Enable CLI Discovery）	有効（オン）にした場合、検出は SNMP に失敗したデバイスのみを対象に CLI から Telnet または SSH を使用して行われます。
SNMP 設定のプッシュの有効化（Enable SNMP Config Push）	CLI 検出を有効にした場合は、RO 文字列に対する SMNP 設定のプッシュが必要です。
CLI タイムアウト（CLI Timeout）	CLI 接続のタイムアウト値（秒単位）。デフォルト値は 3 秒です。

プラットフォームを含める（オプション）：

[プラットフォームを含める（Include Platform）] リストにプラットフォームを指定した場合、それらの特定のプラットフォームのみが検出されます。

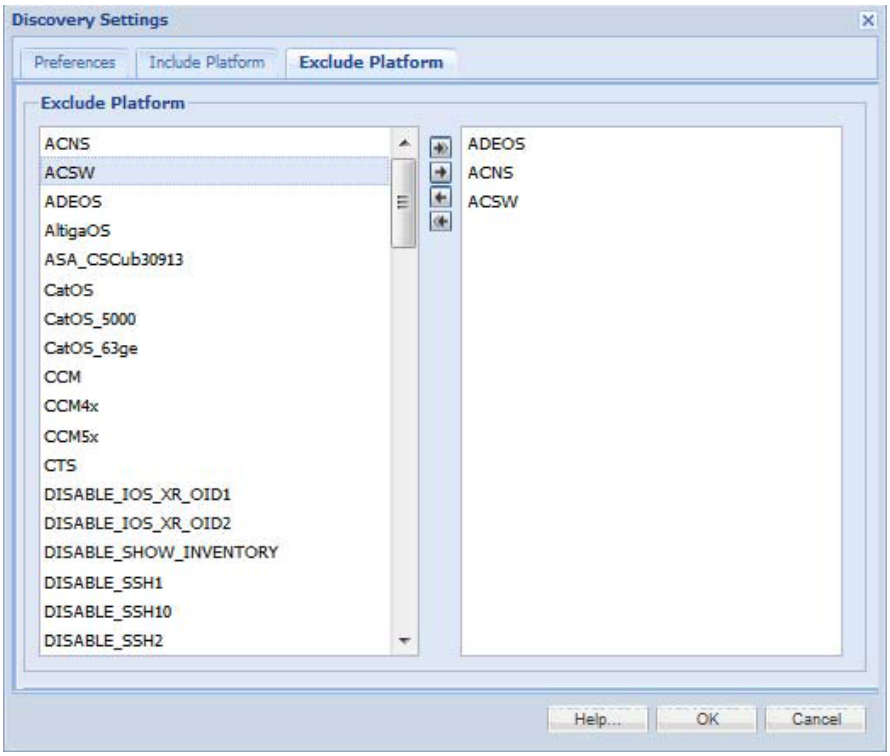
図 6-27　　[プラットフォームを含める（Include Platform）]



プラットフォームを除外する（オプション）：

[プラットフォームを除外する（Exclude Platform）] リストにプラットフォームを指定した場合、そのプラットフォームに属するデバイスはすべて無視されます。

図 6-28　　[プラットフォームを除外する（Exclude Platform）]



[インベントリ設定（Inventory Settings）]

[インベントリ設定（Inventory Settings）] では、いくつかの詳細な収集設定を設定できます。

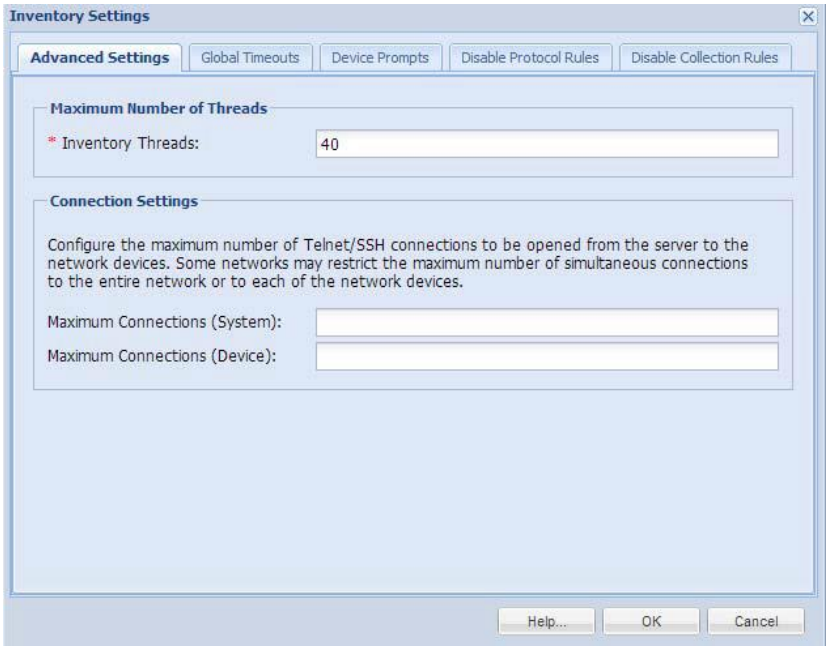
それらの設定には、インベントリ スレッド、デバイスの接続性オプション、タイムアウト オプション、デバイス プロンプト、無効化のプロトコル ルール、および無効化の収集ルールなどがあります。

詳細設定：

[インベントリ設定（Inventory Settings）] 画面の [詳細設定（Advanced Settings）] タブには次のオプションがあります。

- [インベントリ スレッド（Inventory Threads）]：コレクタが使用するインベントリ スレッドの最大数を設定します。デフォルトでは、Microsoft Windows の値は 40 で、Linux の値はハードウェア構成に応じて 40 ～ 100 です。設定可能な最大値は、Microsoft Windows も Linux も 200 です。
- [接続設定（Connection Settings）]：1 台のデバイスに設定できる最大接続数、またはコレクタ全体の最大接続数を設定します。これらの設定は、Telnet または SSH クレデンシャルにのみ適用されます。一部のネットワークでは、認証サーバによるアプリケーションまたはデバイスの接続数の制限があるため、この設定を行う必要があります。デフォルトでは、デバイスごとに 1 つの接続のみであり、コレクタ全体に対する接続制限はありません。

図 6-29　　[インベントリ設定（Inventory Settings）]



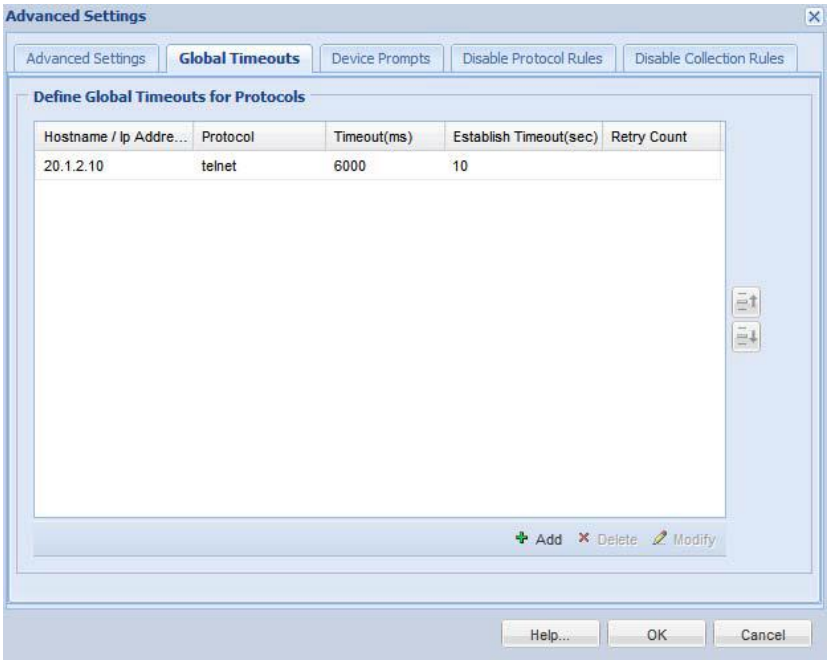
CSPC フローチャートに戻る

[グローバル タイムアウト（Global Timeouts）]

[グローバル タイムアウト（Global Timeouts）] タブでは、特定の IP アドレスまたは IP アドレスの範囲に対するタイムアウト オプションを選択できます。このタブでは、Telnet、SSH、SNMP、HTTP などの特定のプロトコル用のタイムアウト オプションを指定できます。

縦方向のスクロール バーを使用すると、ウィンドウの前後のタイムアウト オプションに移動できます。

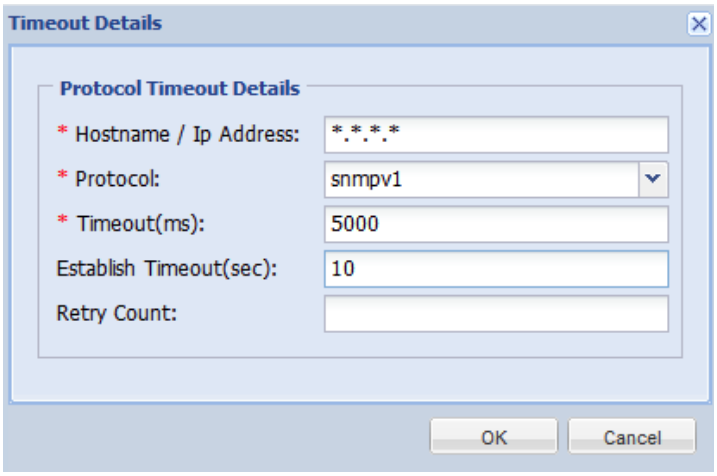
図 6-30　　[グローバル タイムアウト（Global Timeouts）]



タイムアウトを入力するには、[追加（Add）] ボタンをクリックします。[タイムアウトの詳細（Timeout Details）] 画面では、次の情報を入力できます。

- [ホスト名/IP アドレス（Hostname / IP Address）] : 10.*.*.*（10 で始まるすべての IP アドレスを表す）などの IP アドレス表現を選択できます。
- [プロトコル（Protocol）] : プロトコル（Telnet、SSHv1、SSHv2、HTTP、HTTPS、TL1、SNMPv1、SNMPv2、SNMPv3、WMI、IIOP）を選択します。
- [タイムアウト（ミリ秒）（Timeout (ms)）] : ミリ秒単位のタイムアウトを 1,000 ミリ秒（1 秒）～ 600,000 ミリ秒（10 分）の範囲で入力します。
- [確立タイムアウト（秒）（Establish Timeout (sec)）] : デバイスの接続を確立するのにかかる時間を設定します。デフォルトは 10 秒です。
- [再試行回数（Retry Count）] : 「再試行」回数も選択できます。

図 6-31　　[グローバル タイムアウト（Global Timeouts）]



グローバル タイムアウト値を変更するには、[変更（Modify）] ボタンを使用します。タイムアウト値を削除するには、[削除（Delete）] ボタンを使用します。

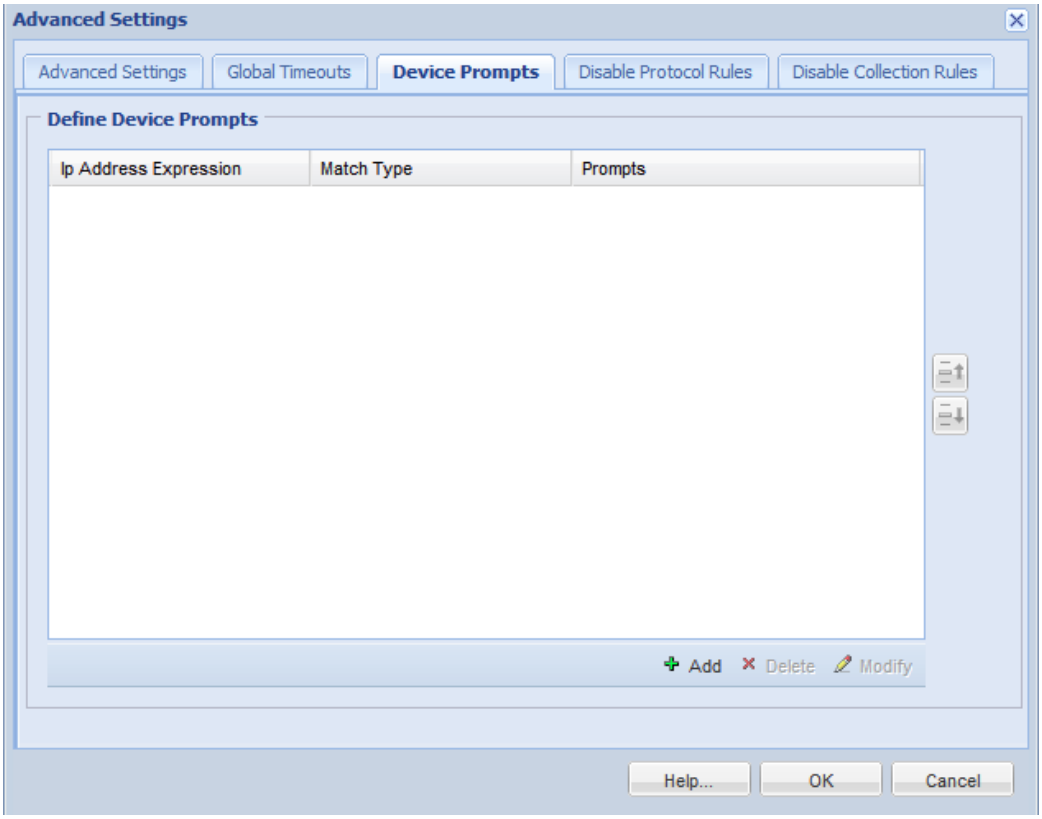
CSPC フローチャートに戻る

[デバイス プロンプト（Device Prompts）]

[デバイス プロンプト（Device Prompts）] タブでは、特定のデバイスまたはデバイス グループに固有のプロンプト オプションを選択できます。デバイス プロンプトは、セキュリティ上の理由で認証サーバ経由でプロンプトが変更されたり、デバイスまたはデバイス グループのデータ収集が完了した際に使用されます。デバイス プロンプトが変更された場合、コレクタは、データ収集を正常に実行するために、それらのプロンプトに対応可能である必要があります。

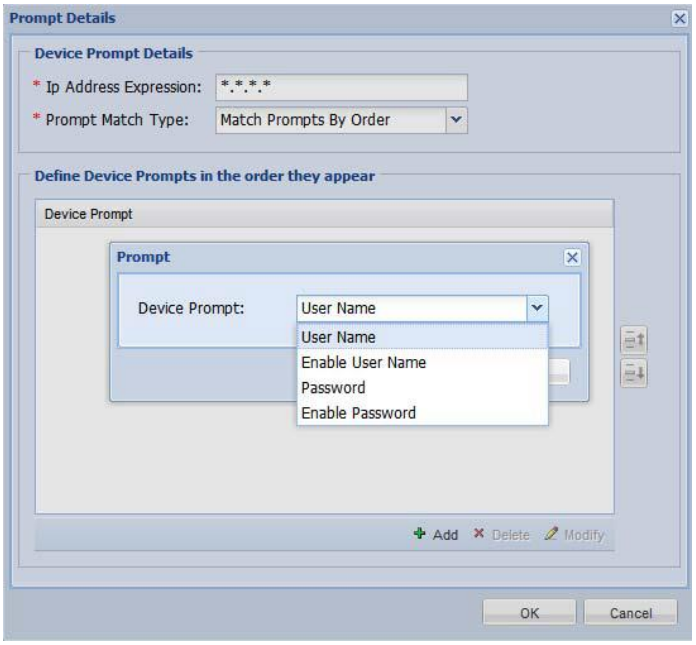
これらのオプションを設定する方法は 2 つあります。1 つは順序に基づいてプロンプトを一致させる方法で、もう 1 つは特定の文字列や正規表現に一致させる方法です。

図 6-32　　[デバイス プロンプト（Device Prompts）]



*順序*と*正規表現*については、以下で説明します。

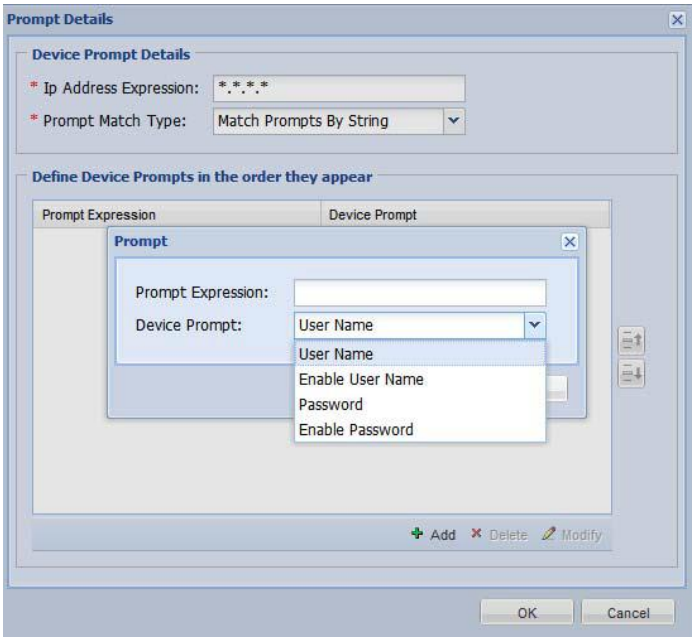
図 6-33　　順序に基づくプロンプトの詳細



1 つめの方法の場合、デバイスまたはデバイス グループにおいて、コレクタが特定の順序でクレデンシャル情報を送信してくると想定されています。たとえば、[パスワード（Password）]、[ユーザ名の有効化（Enable User Name）]、[パスワードの有効化（Enable Password）] の順序で送信されてくると想定されている場合、そのとおりの順序に変更できます（図 6-33 を参照）。

同様に、図 6-34 に示すように、プロンプトの文字列が一致していることが想定されている場合、プロンプトに表示したい文字列を指定することができます。

図 6-34　　文字列に基づくプロンプトの詳細



IP アドレスが 1.1.1.1 のこのデバイスの例では、[ユーザ名（User Name）] にデバイス プロンプトとして「*user:*」の表現が含まれている必要があります。

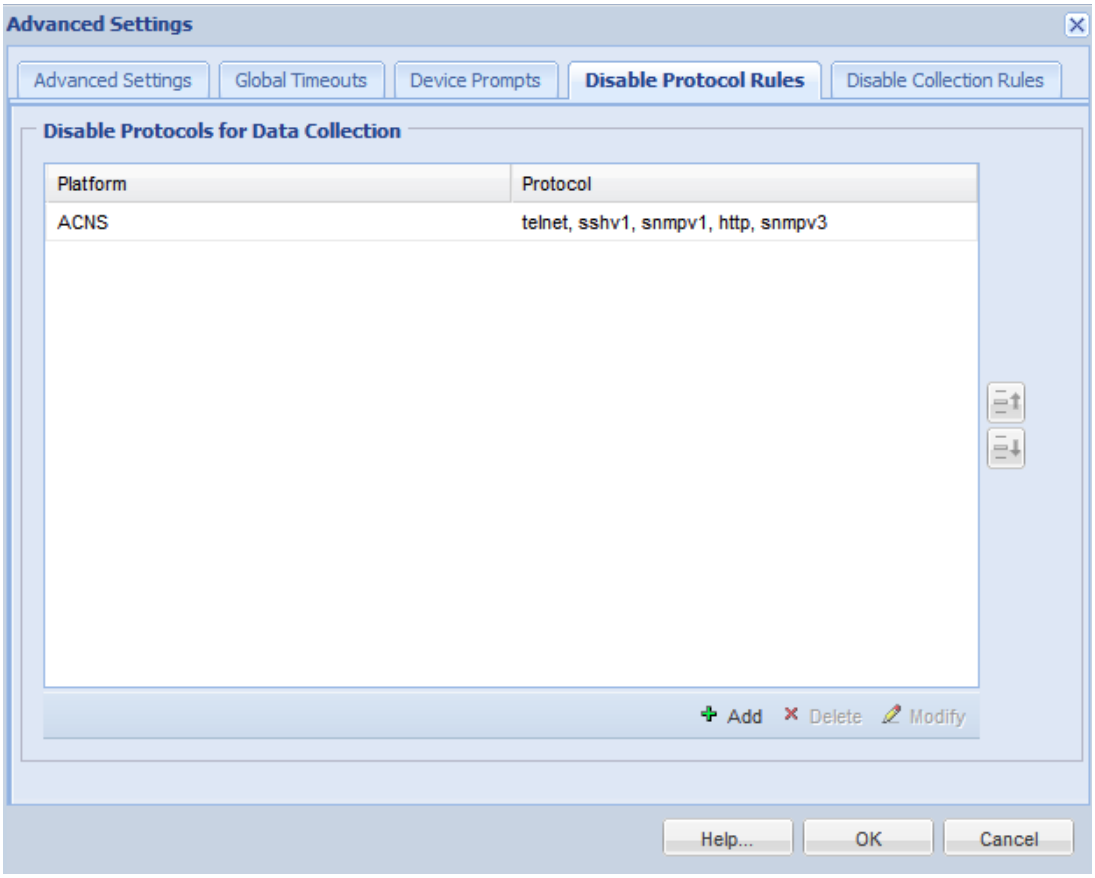
プロンプトの値を変更するには、[変更（Modify）] ボタンを使用します。プロンプトを削除するには、[削除（Delete）] ボタンを使用します。

CSPC フローチャートに戻る

[プロトコルの無効化ルール（Disable Protocol Rules）]

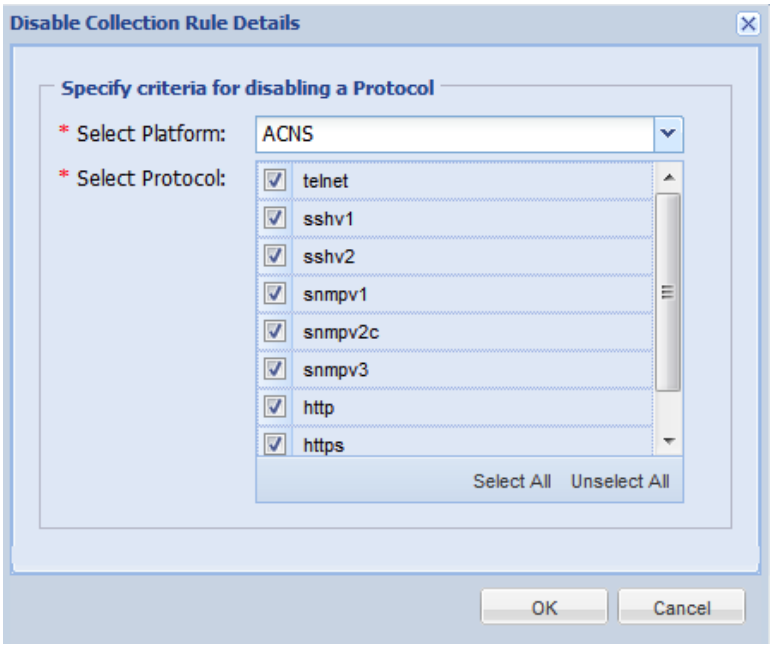
[プロトコルの無効化ルール（Disable Protocol Rules）] タブでは、特定のプラットフォームに対して無効化する必要があるプロトコルを設定できます。指定したプラットフォームの無効化されたプロトコルに対して、インベントリおよびデバイス アクセスの検証は実行されません。そのため、データセットを変更することなく、プロトコルを有効化または無効化できます。

図 6-35　　[デバイス プロトコル ルール（Device Protocol Rules）]



プロトコルの無効化ルールを追加したり、既存のプロトコルの無効化ルールを変更または削除したりできます。縦方向のスクロール バーを使用すると、表内の前後のルールに移動できます。プロトコルの無効化ルールを追加するには、[プロトコルの無効化ルール（Disable Protocol Rules）] 画面で [追加（Add）] をクリックします。

図 6-36　　[プロトコルの無効化ルール（Disable Protocol Rules）] 詳細



プロトコルの無効化ルールを新規作成するには、以下の手順に従います。

ステップ 1　次の情報を入力します。

- [プラットフォームの選択（Select Platform）]：プロトコルを無効化する必要があるプラットフォームをコンボ リストから選択します。コンボ リストには、システム定義とカスタム定義のすべての設定済みプラットフォームが表示されます。
- [プロトコルの選択（Select Protocols）]：[プラットフォームの選択（Select Platform）] で選択したプラットフォームに対して無効化する必要があるプロトコルを選択します。コンボ リストには、サポートされているすべてのプロトコル（Telnet、SSHv1、SSHv2、SNMPv1、SNMPv2、SNMPv3、HTTP、HTTPS、TL1、WMI、IIOP）が表示されます。

ステップ 2　[すべて選択（Select All）] ボタンまたは [すべて選択解除（Unselect All）] ボタンを使用して、すべてのプロトコルを選択または選択解除することもできます。

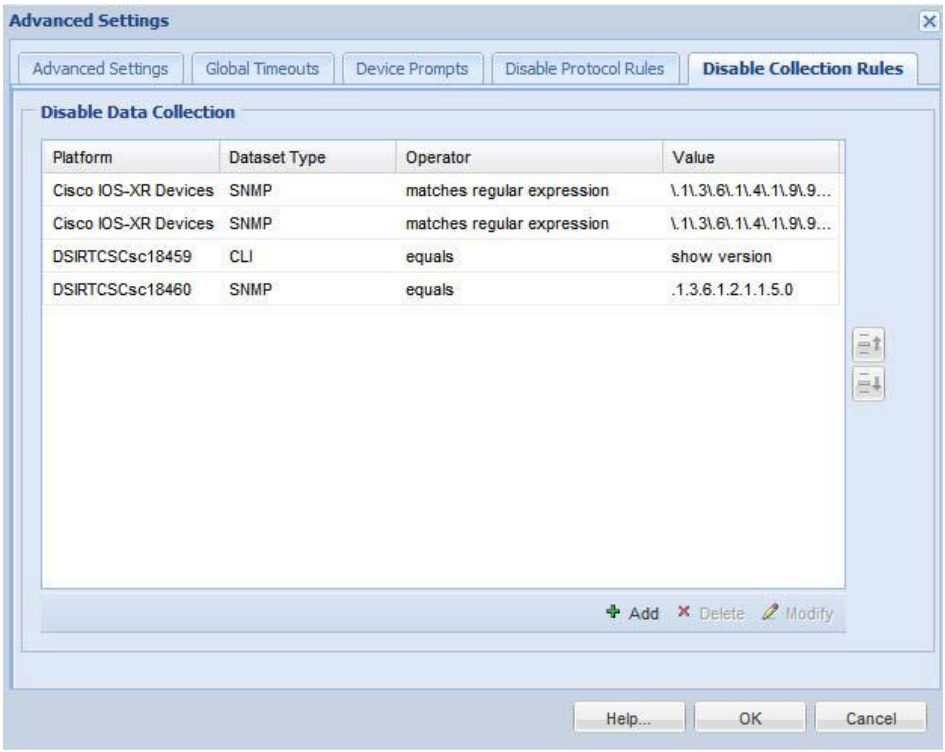
ステップ 3　[OK] をクリックして、設定したルールを CSPC に追加します。

[収集の無効化ルール（Disable Collection Rules）]

[収集の無効化ルール（Disable Collection Rules）] タブでは、特定のプラットフォームに対して特定のコマンドまたは OID を無効化できます。インベントリは、無効化されたコマンドまたは OID に対しては実行されません。

あるデータセットに複数の OID が存在する場合、インベントリはそのデータセットに対して実行され、無効化されていない OID の結果が表示されますが、無効化された OID の収集は行われません。

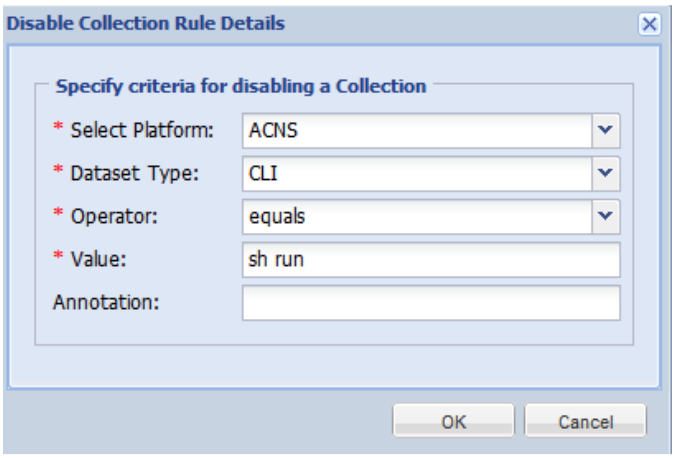
図 6-37　　[収集の無効化ルール（Disable Collection Rules]）



収集の無効化ルールを追加したり、既存の収集の無効化ルールを変更または削除したりできます。縦方向のスクロール バーを使用すると、表内の前後のルールに移動できます。

収集の無効化ルールを追加するには、[収集の無効化ルール（Disable Collection Rules）] 画面で [追加（Add）] をクリックします。

図 6-38　　[収集の無効化ルール（Disable Collection Rules）] 詳細


Disable Collection Rule Details
Specify criteria for disabling a Collection
* Select Platform:
ACNS
* Dataset Type:
CLI
* Operator:
equals
* Value:
sh run
Annotation:
OK
Cancel

収集の無効化ルールを新規作成するには、以下の手順に従います。

ステップ 1 次の情報を入力します。

- [プラットフォームの選択（Select Platform）]：プロトコルを無効化する必要があるプラットフォームをコンボ リストから選択します。コンボ リストには、システム定義とカスタム定義のすべての設定済みプラットフォームが表示されます。
- [データセット タイプの選択（Select Dataset Type）]：サポートされているデータセット タイプは CLI または SNMP です。
- [演算子（Operator）]：[等しい（equals）]、[等しくない（does not equal）]、[正規表現に一致する（matches regular expression）]、[正規表現に一致しない（does not match regular expression）] のいずれかを選択します。
- [値（Value）]：無効化する正確な CLI コマンドまたは OID。
- [注釈（Annotation）]：メモを追加できます。

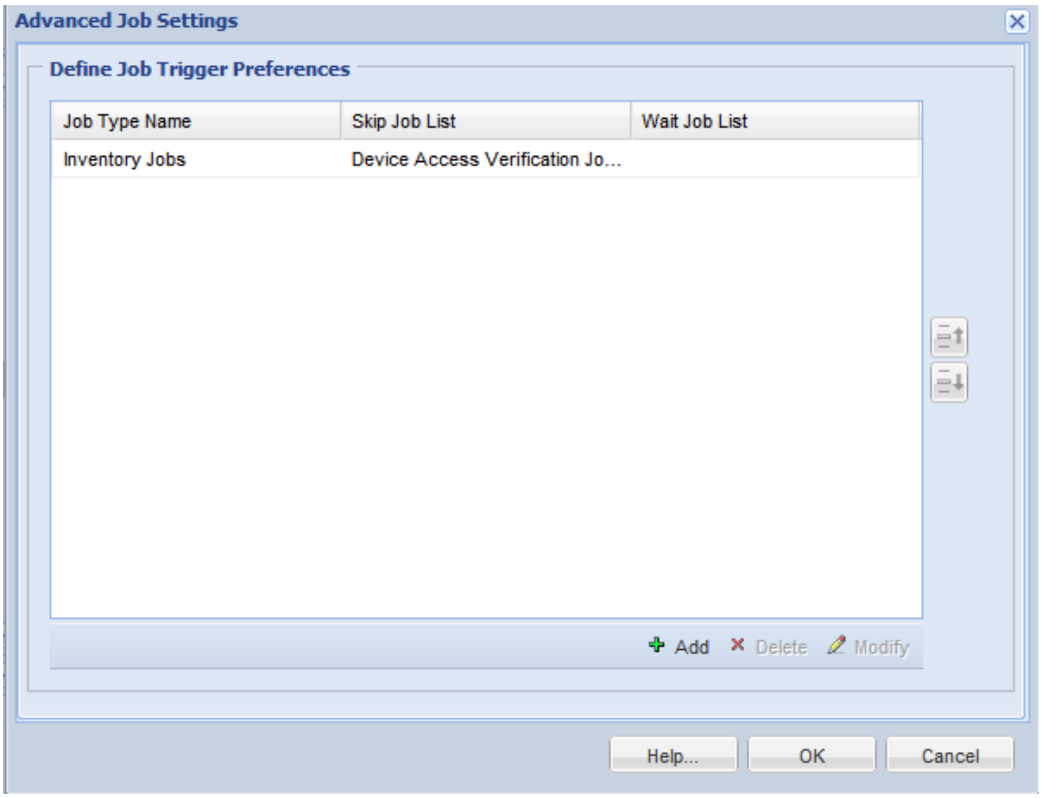
ステップ 2 [OK] をクリックして、設定したルールを CSPC に追加します。

CSPC フローチャートに戻る

[ジョブ詳細設定（Advanced Job Settings）]

この設定には、さまざまなジョブを設定するためのオプションがあります。ジョブをトリガーするための設定、スキップ可能なジョブ、およびトリガーの設定に基づき待機する必要があるジョブを定義できます。新しいジョブ トリガー設定は、[ジョブ詳細設定（Advanced Job Settings）] ウィンドウで [追加（Add）] ボタンを選択して追加できます。

図 6-39　　[ジョブ詳細設定（Advanced Job Settings）]

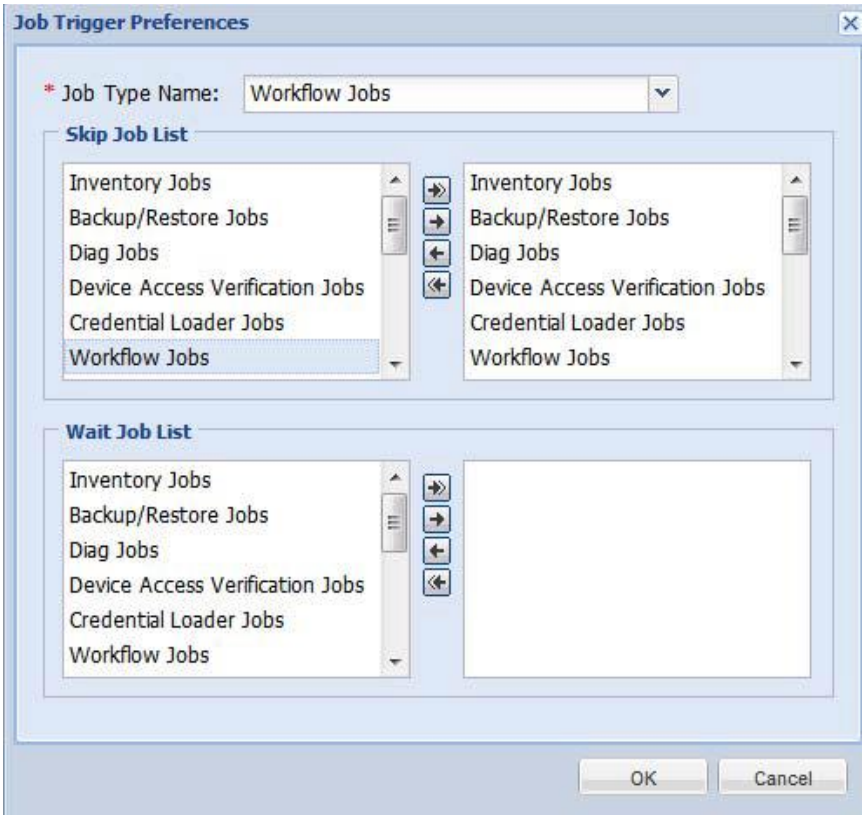


[待機ジョブ リスト（Wait Job List）] と [スキップ ジョブ リスト（Skip Job List）] にジョブを追加できます。

[待機ジョブ リスト（Wait Job List）] : [ジョブ タイプ名（Job Type Name）] に指定したジョブは、[待機ジョブ リスト（Wait Job List）] に指定したジョブが完了した後にのみ開始します。

[スキップ ジョブ リスト（Skip Job List）] : [ジョブ タイプ名（Job Type Name）] に指定したジョブは、[スキップ ジョブ リスト（Skip Job List）] に指定したジョブが実行されている場合には開始しません。

図 6-40　　[ジョブ トリガー設定（Job Trigger Preferences）] の追加



[収集ルール（Collection Rules）]

[デバイス管理（Device Management）] タブの [収集ルール（Collection Rules）] サブ タブでは、データ収集プロファイルの設定、新しいデータセットの作成、およびデータ整合性ルールとデータ マスキング ルールの管理を行うことができます。

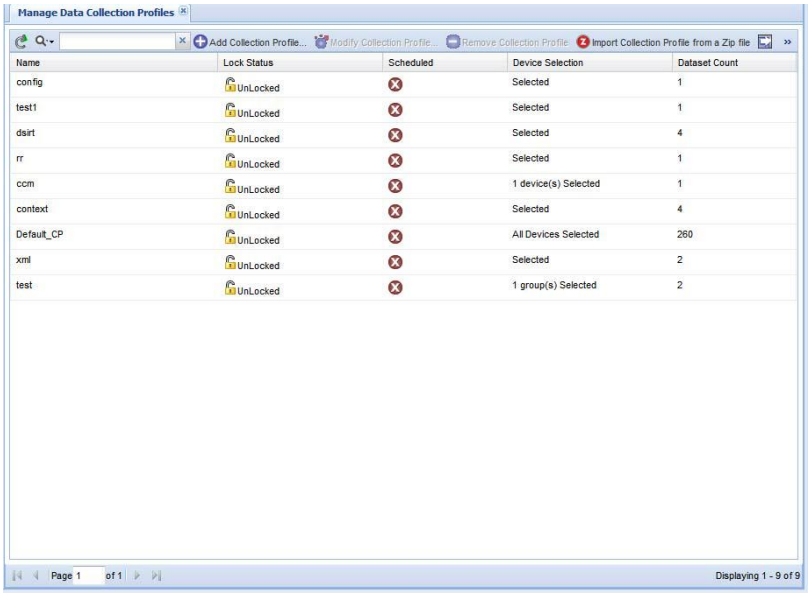
この項では、[収集ルール（Collection Rules）] オプションの以下の項目について説明します。

- [データ収集プロファイルの管理（Manage Data Collection Profiles）]
- [アップロード プロファイルの管理（Manage Upload Profiles）]
- [データセットの管理（Manage Datasets）]
- [プラットフォーム定義の管理（Manage Platform Definitions）]
- [データ整合性ルールの管理（Manage Data Integrity Rules）]
- [データ マスキング ルールの管理（Manage Data Masking Rules）]
- [Syslog ソース ファイルの管理（Manage Syslog Source Files）]

[データ収集プロファイルの管理（Manage Data Collection Profiles）]

収集プロファイルでは、収集するデータの種類、データの収集元となるデバイス、およびデータの収集頻度を定義します。

図 6-41　　収集プロファイルのメイン ウィンドウ



収集プロファイルが 1 つも作成されていない場合、CSPC はどのデバイスからもデータを収集しません。

新しいデータ収集プロファイルを作成するには、[データ収集プロファイルの管理（Manage Data Collection Profiles）] ウィンドウの [収集プロファイルの追加（Add Collection Profile）] アイコンをクリックします。

システムにローカルに保存されている zip ファイルから収集プロファイルをインポートすることもできます。これを行うには、[Zip ファイルから収集プロファイルをインポート（Import Collection Profile from Zip File）] ボタンをクリックし、収集プロファイルを含む zip ファイルを選択します。

新しいデータ収集プロファイルを追加するには、以下の手順に従います。

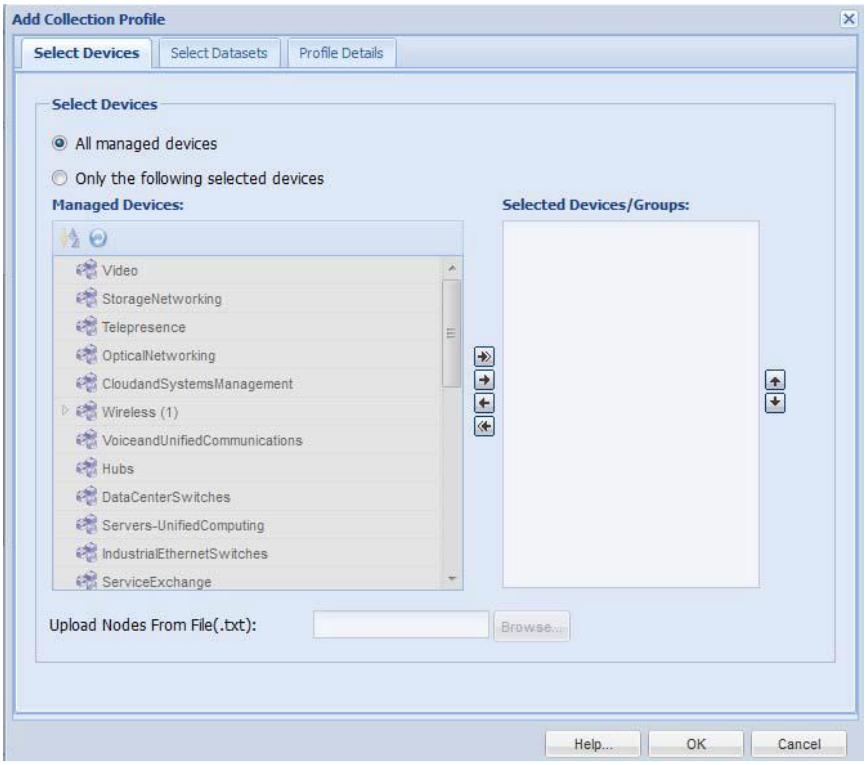
ステップ 1 デバイスを選択します。

ステップ 2 データセットを選択します。

ステップ 3 プロファイルの詳細を選択します。

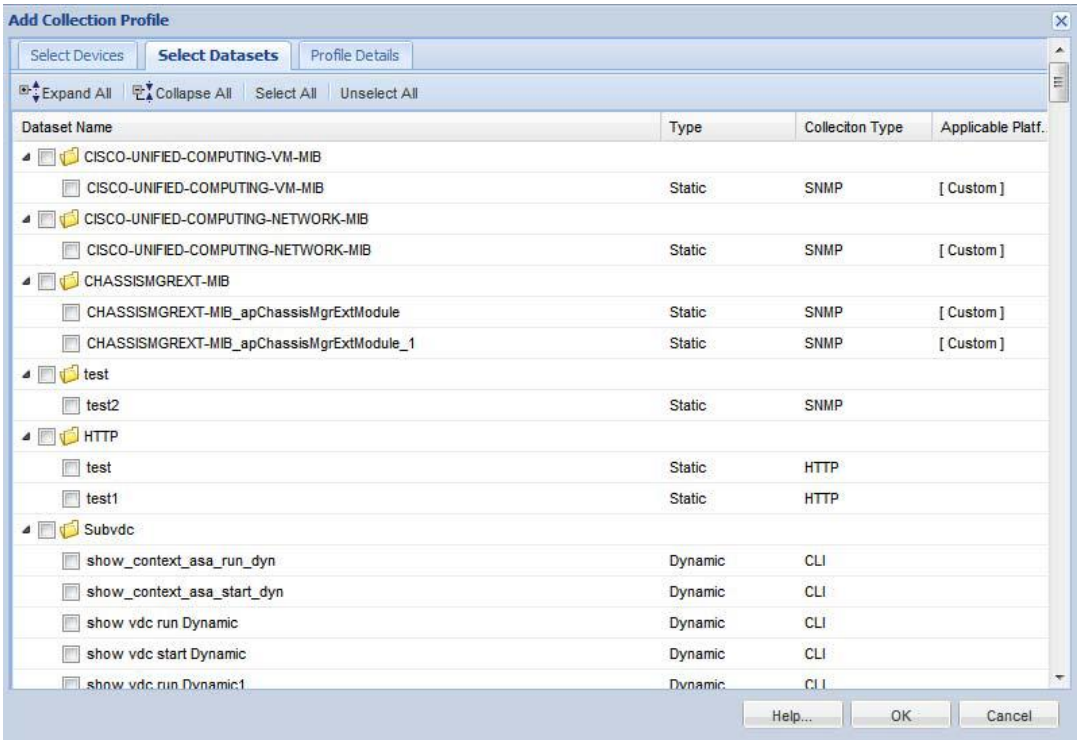
ステップ 4 [OK] をクリックします。

図 6-42　　収集プロファイル用のデバイスの選択



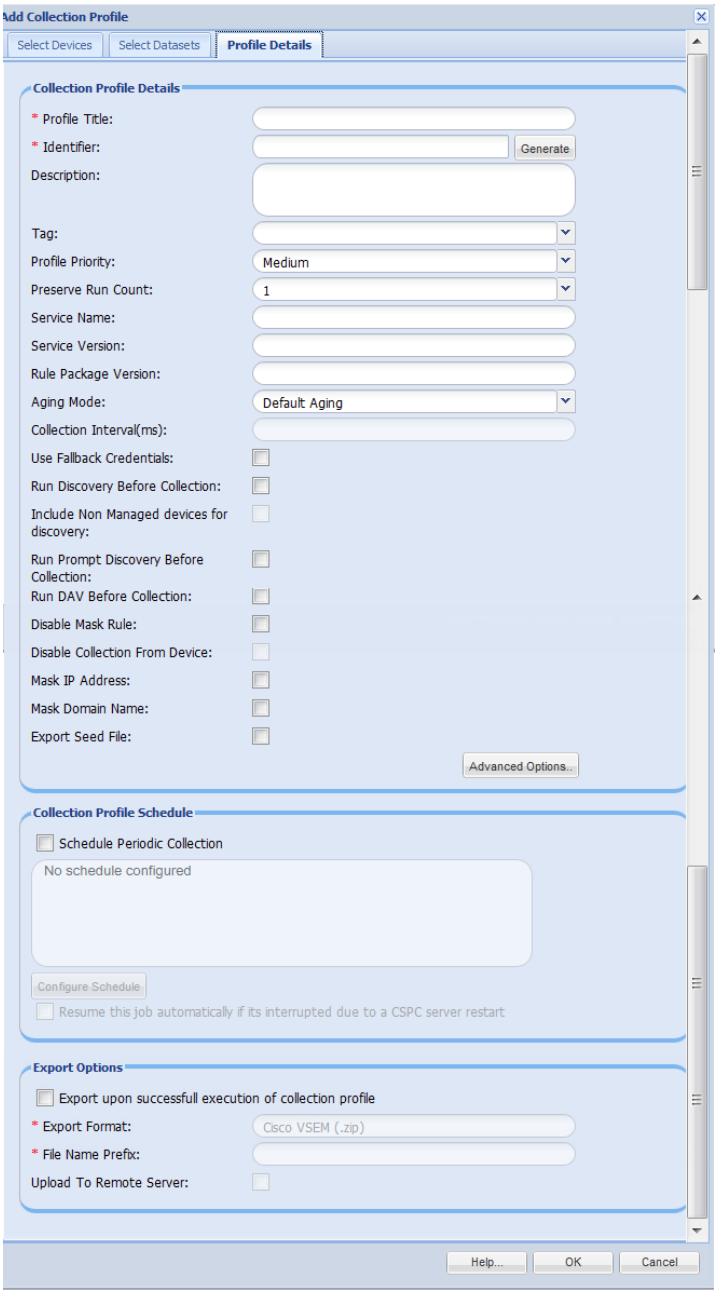
収集を開始するには、上の図に示すように、データを収集するデバイスまたは一連のデバイスを選択するか、デバイスの各 IP アドレスが連続する行に入力されている .txt ファイルをインポートします。デバイスを選択したら、プロファイル作成の次のステップはデータセットの選択です。CSPC 内のデータセットは、CLI コマンド、SNMP 要求、SOAP/XML 要求、またはファイルの出力です。*データセット*の詳細については、「*データセットの管理*」の章を参照してください。

図 6-43　　[データセットの選択（Select Datasets）]



必要なデータセットを選択したら、次に示すように、データの収集頻度を定義するプロファイル オプションを選択します。

図 6-44　　[プロファイル詳細（Profile Details）]



このウィンドウには、プロファイル自体の優先度、保存する必要があるプロファイル実行データのバージョン数、データ収集のためにプロファイルを実行する頻度を選択するためのオプションがあります。プロファイルを識別するタイトル、および識別情報を入力する必要があります。識別情報は、プロファイルを一意に特定するために XML API によって使用されます。識別情報が指定されていない場合、システムによってプロファイルの自動識別情報が生成されます。

タグは VSEM ファイルに付加される情報です。ドロップダウンからオプションを選択するか、プロファイルに付けるタグを手動で入力します。

各プロファイルは、個別の優先度を指定して設定します。リソースの競合がある場合、優先度が高いプロファイルが常に優先されます。

作成したプロファイルの [サービス名（Service Name）] と [サービス バージョン（Service Version）] を指定できます。サービス バージョンは、データを収集してアップロードする特定のサービス プログラムのバージョンです。

[ルール パッケージ バージョン（Rule package version）] を指定します。

ドロップダウンからデータの [エージング モード（Aging Mode）] を選択します。

[デフォルトのエージング（Default Aging）] を選択すると、設定可能な時間間隔が使用されます。このオプションはデフォルトで有効になっており、データセットで指定したエージング間隔が使用されます。

[エージングの無効化（Disable Aging）] を選択すると、データ エージングは無効になります。このオプションはデータ エージングを無効するもので、収集はデバイスから直接行われます。

[カスタム エージング（Custom Aging）] を選択する場合は、収集間隔をミリ秒単位で指定する必要があります。
このオプションでは、CP レベルのデータ エージング（ミリ秒）を指定します。このオプションを指定すると、データセットで定義されたエージングがオーバーライドされるとともに、[デバイスからの収集を無効にする（Disable Collection From Device）] オプションを使用できるようになります。

デバイスからの収集を無効にするには、[デバイスからの収集を無効にする（Disable Collection From Device）] オプションを使用します。このオプションをオンにすると、見つからない/期限切れのデータセットのデータはデバイスからは直接収集されません。これらのデータセットのデータは、CP サマリー レポートで「省略」と表示されます。
オフにすると、見つからない/期限切れのデータセットのデータがデバイスから収集されます。

[フォールバック クレデンシャルの使用（Use Fallback Credentials）] オプションは、データ収集に使用されているクレデンシャルが機能しない場合のために用意されています。一般的に、データ収集にも検出クレデンシャルを使用している場合、そのクレデンシャルは必ずしもすべてのデバイスに対しては機能しません。CSPC は、データ収集のためのフォールバック クレデンシャルとして、デバイス アクセスの検証にパスした次のクレデンシャルを選択します。

[収集前に検出を実行（Run Discovery Before Collection）] オプションを使用して、インベントリを実行する前にデバイスを再検出します。

管理対象外のデバイスを検出するには、[管理対象外のデバイスを検出に含める（Include Non Managed devices for discovery）] オプションを使用します。

インベントリを実行する前にプロンプトを収集するには、[収集前にプロンプト検出を実行（Run Prompt Discovery before Collection）] オプションを使用します。

インベントリを実行する前にクレデンシャルを検証するには、[収集前に DAV を実行（Run DAV Before Collection）] オプションを使用します。

ルール セットに従ってデータ収集をマスクしない場合は、[マスク ルールを無効にする（Disable Mask Rule）] オプションを使用します。

顧客から収集した IP アドレスをシスコにアップロードする前にマスクするには、[IP アドレスのマスク（Mask IP Address）] オプションを使用します。

顧客から収集したドメイン名をシスコにアップロードする前にマスクするには、[ドメイン名のマスク（Mask Domain Name）] オプションを使用します。

[IP アドレスのマスク（Mask IP Address）] オプションと [ドメイン名のマスク（Mask Domain Name）] オプションを使用すれば、データのプライバシーと用途を、顧客のニーズに合わせることができます。マスク設定は、[設定（Settings）] メニューの [詳細設定（Advanced Settings）] オプションで指定できます。

システムに保存されているすべてのオリジナル シード ファイルを収集プロファイルと一緒にアップロードする場合は、[シード ファイルのエクスポート（Export Seed File）] オプションを使用します。到達不能デバイスをエクスポートすることもできます。このオプションは、マスキング/DPA が有効になっている場合には使用できません。

収集プロファイルの実行が成功した後に、収集プロファイル データをエクスポートする場合は、[エクスポート オプション（Export Options）] を使用します。データは次の形式でエクスポートできます。

- Cisco VSEM（.zip）

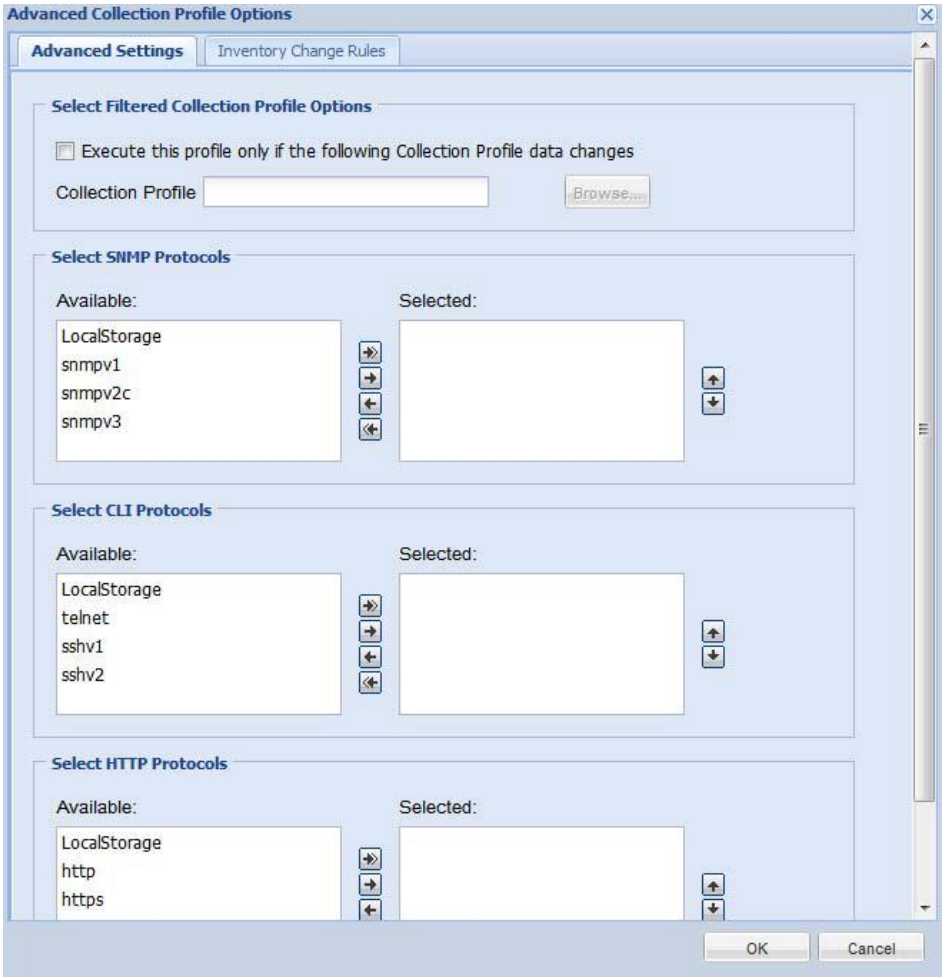
収集プロファイルの詳細をリモート サーバにアップロードする場合は、[リモート サーバにアップロード（Upload to Remote Server）] チェックボックスをオンにします。[リモート サーバにアップロード（Upload to Remote Server）]チェックボックスをオフのままにすると、収集プロファイル データはリモート サーバにアップロードされません。

すべてのステップを完了し、[OK] をクリックすると、データ収集プロファイルが作成されて使用できるようになります。

収集プロファイルを後で実行するようにスケジュールしている場合、[このジョブが CSPC サーバの再起動によって中断した場合は自動的に再開する（Resume this job automatically if it is interrupted due to a CSPC Server restart）] オプションが選択可能になります。収集プロファイルを実行中に、CSPC が何らかの理由で再起動した場合、CSPC は再起動後に該当ジョブを再開します。

[プロファイル詳細（Profile Details）] ウィンドウの [詳細オプション（Advanced Options）] をクリックすると、次のウィンドウが表示されます。

図 6-45　　[収集プロファイル詳細オプション（Advanced Collection Profile Options）]



[収集プロファイル詳細オプション（Advanced Collection Profile Options）] ウィンドウには、使用可能な SNMP、CLI、および HTTP プロトコルが表示されます。一覧から目的のプロトコルを選択し、矢印をクリックして追加できます。または、二重矢印をクリックしてすべてのプロトコルを追加することもできます。

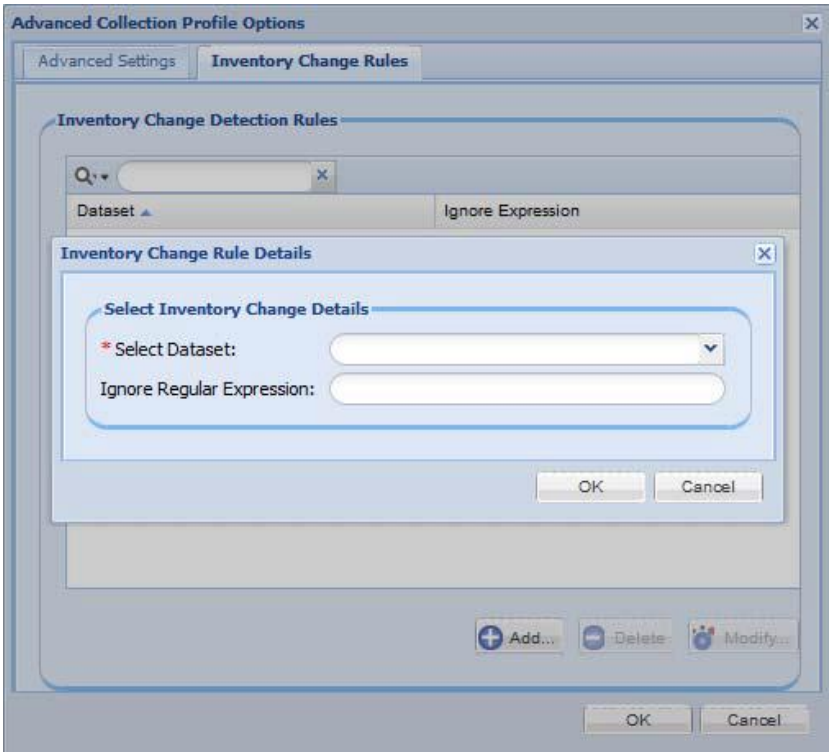
[選択済み（Selected）] ボックスの横にある矢印キーを使用すると、プロトコルを上下に移動できます。[選択済み（Selected）] ボックスの一番上のプロトコルが優先され、それより下のプロトコルよりも先に実行されます。

[LocalStorage] を選択すると、特定のデバイスまたはデータセットに対して実行するたびにそのデバイスまたはデータセットがローカル データベースに存在するかどうかがまずチェックされ、見つからない場合には選択したプロトコル順序に基づいて次のプロトコルが実行されます。

特定の収集プロファイルが変更された場合にのみプロファイルを実行するフィルタを設定できます。フィルタを設定するには、[次の収集プロファイル データが変更された場合にのみこのプロファイルを実行する（Execute this profile only if the following collection profile data changes）] の横にあるチェックボックスをオンにし、[参照（Browse）] ボタンをクリックして収集プロファイルを選択します。

ルールを追加または変更するには、[インベントリ変更ルール（Inventory Change Rules）] をクリックします。データセットを選択し、[正規表現を無視（Ignore Regular Expression）] を入力して、[OK] をクリックします。

図 6-46　　[インベントリ変更ルール詳細（Inventory Change Rule Details）]



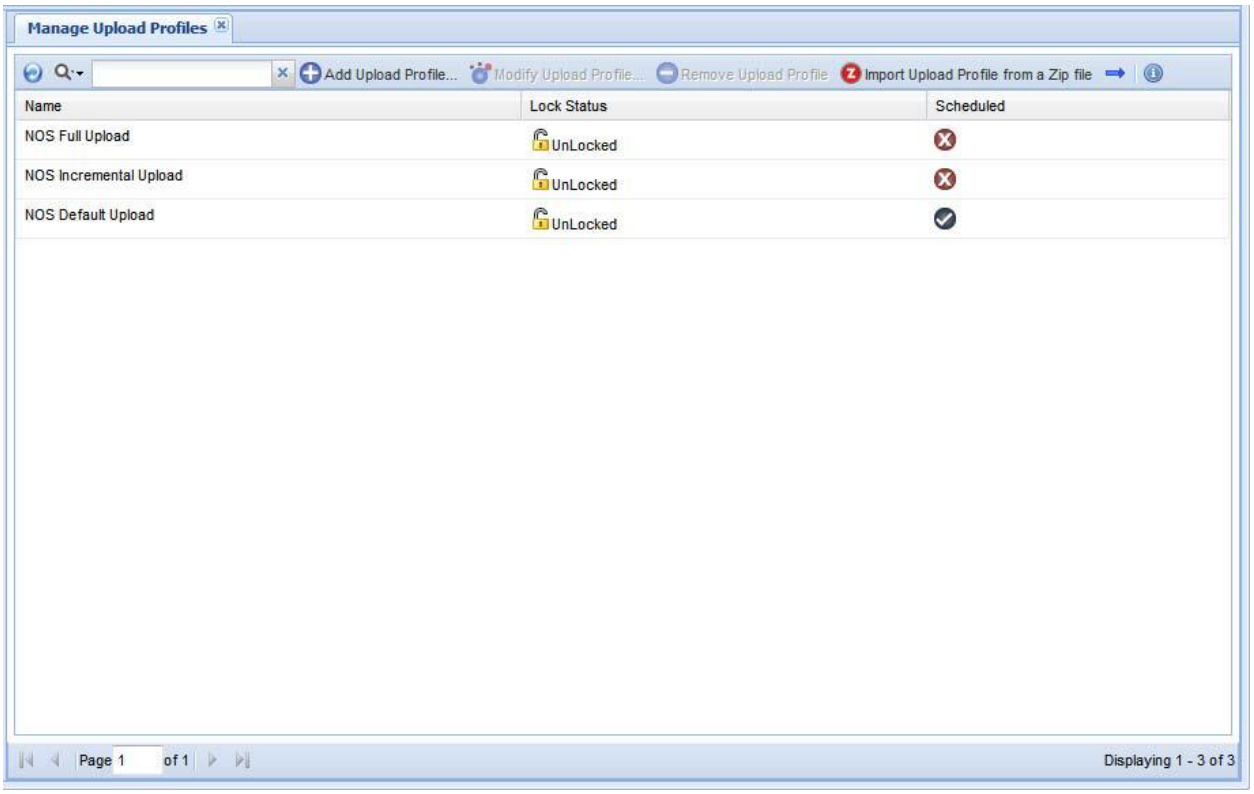
[OK] ボタンをクリックして、選択内容を保存します。

CSPC フローチャートに戻る

[アップロード プロファイルの管理（Manage Upload Profiles）]

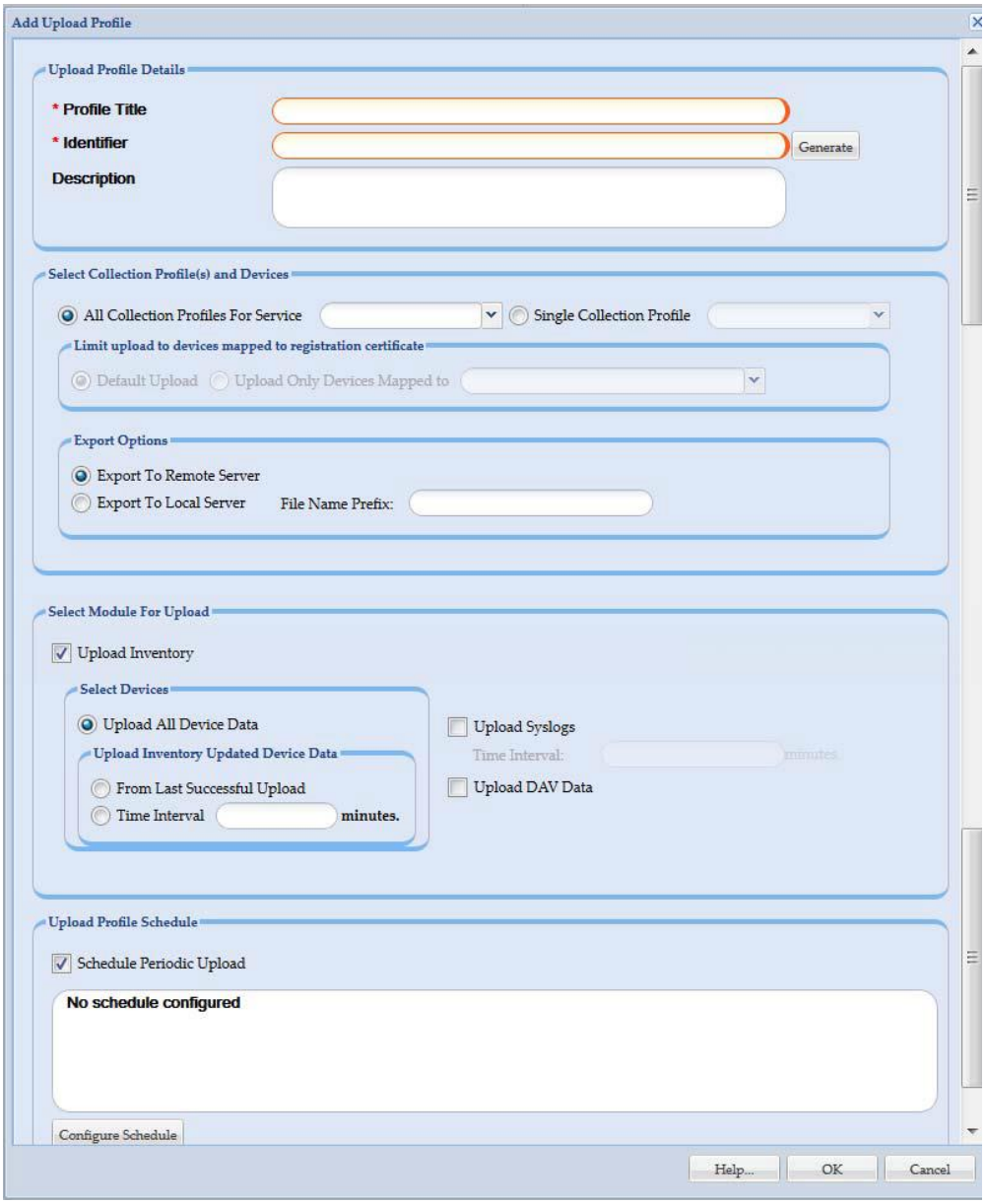
[アップロード プロファイルの管理（Manage Upload Profiles）] では、ローカルまたはバックエンドにアップロードする必要がある Syslog、インベントリ、DAV を含むデータのタイプを指定できます。

図 6-47　　[アップロード プロファイルの管理（Manage Upload Profiles）]



システムに保存されている zip ファイルからアップロード プロファイルをインポートできます。これを行うには、[アップロード プロファイルの管理（Manage Upload Profiles）] 画面の [zip ファイルからアップロード プロファイルをインポート（Import Upload Profile from a Zip file）] アイコンをクリックします。[ファイルのアップロード（Upload File）] ダイアログボックスで、目的のファイルを参照し、[送信（Submit）] ボタンをクリックしてファイルのアップロードを開始します。

図 6-48　　[アップロード プロファイルの追加（Add Upload Profiles）]



[サービスのすべての収集プロファイル（All Collection Profiles For Service）] または [単一の収集プロファイル（Single Collection Profile）] のいずれかを選択して、ドロップ ダウンから対応する登録証明書を選択することができます。

[デフォルトのアップロード（Default Upload）] を選択してデフォルトの登録証明書にデバイスをアップロードするか、[一致したデバイスのみアップロード（Upload only devices mappedto）] を選択して、ドロップダウンで指定した登録証明書にアップロードすることができます。

[インベントリのアップロード（Upload Inventory）] を選択してアップロードするモジュールを指定することができます。[すべてのデバイス データのアップロード（Upload All Device Data）] を選択し、[時間間隔（Time Interval）]（分）、または、[最後に成功したアップロード以降（From Last Successful Upload）] オプションを指定して、更新されたデバイス データをアップロードすることができます。

DAV データまたは Syslog をアップロードするには、[DAV データのアップロード（Upload DAV Data）]、または [Syslog のアップロード（Upload Syslog）] を選択します。Syslog の場合は、時間間隔を分で指定します。

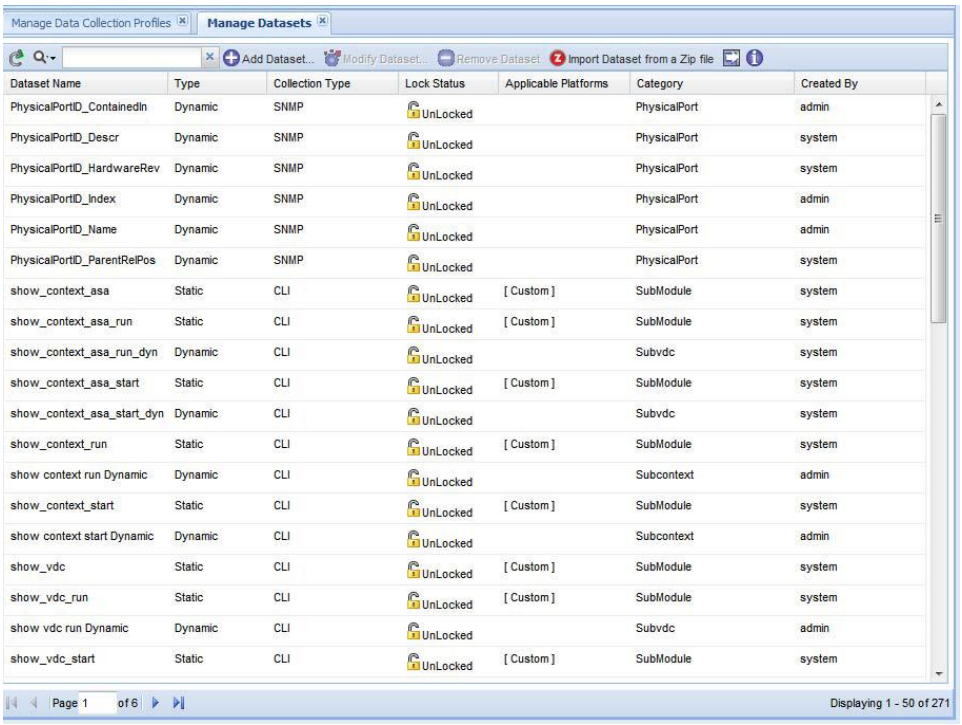
[スケジュールの設定（Configure Schedule）] オプションを使用してデータの定期的なアップロードをスケジュールすることもできます。このデータは、リモート サーバまたはサーバにローカルにエクスポートできます。

[データセットの管理（Manage Datasets）]

[データセットの管理（Manage Datasets）] は、新しいデータ収集ポイントの作成に使用します。データセットは、CSPC 収集プロファイルのビルディング ブロックです。データセットには、プラットフォームの定義、データ/マスキング ルールが含まれています。データセットは、追加、変更、または削除できます。

CSPC 内のデータセットは、CLI コマンド、SNMP 要求（SNMP）、または XML 出力（SOAP/XML）の出力です。

図 6-49　　[データセットの管理（Manage Datasets）]



新規のデータセットを作成する準備ができたら、[データセットの追加（Add Dataset）] オプションを選択します。静的および動的データセットを作成できます。

zip ファイルからデータをインポートすることもできます。これを行うには、[データセットの管理（Manage Datasets）] ウィンドウの [zip ファイルからデータセットをインポート（Import Dataset from a zip file）] ボタンをクリックし、インポートする zip ファイルを選択します。

静的データセット

静的データセットで指定された収集メカニズムは、コマンドまたは SNMP 要求として定義されます。次の手順に従って新しい静的データセットを追加します。

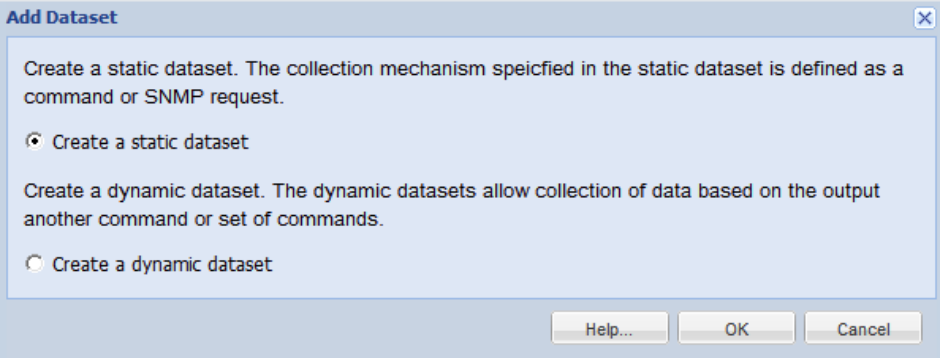
ステップ 1 データセットの詳細を入力します。

ステップ 2 データセットのプラットフォームを入力します。

ステップ 3 [OK] をクリックします。

下の図に示すように、[静的データセットの作成（Create static dataset）] オプションを選択し、[OK] ボタンをクリックして静的データセットを作成します。

図 6-50　　[データセットの追加（Add Dataset）]



[データセットの追加/変更（Add/Modify Dataset）] は、データセットの追加/作成に使用します。データセットの追加は、ロックされた状態でもロック解除された状態でも可能です。

データセットを追加するには、以下の手順に従います。

ステップ 1 次のデータセットの詳細を入力します。

[タイトル（Title）]：データセットの名前。これは必須フィールドです。

[識別情報（Identifier）]：これはユーザが定義することができます。ユーザが定義しない場合は、システムによって生成されます。

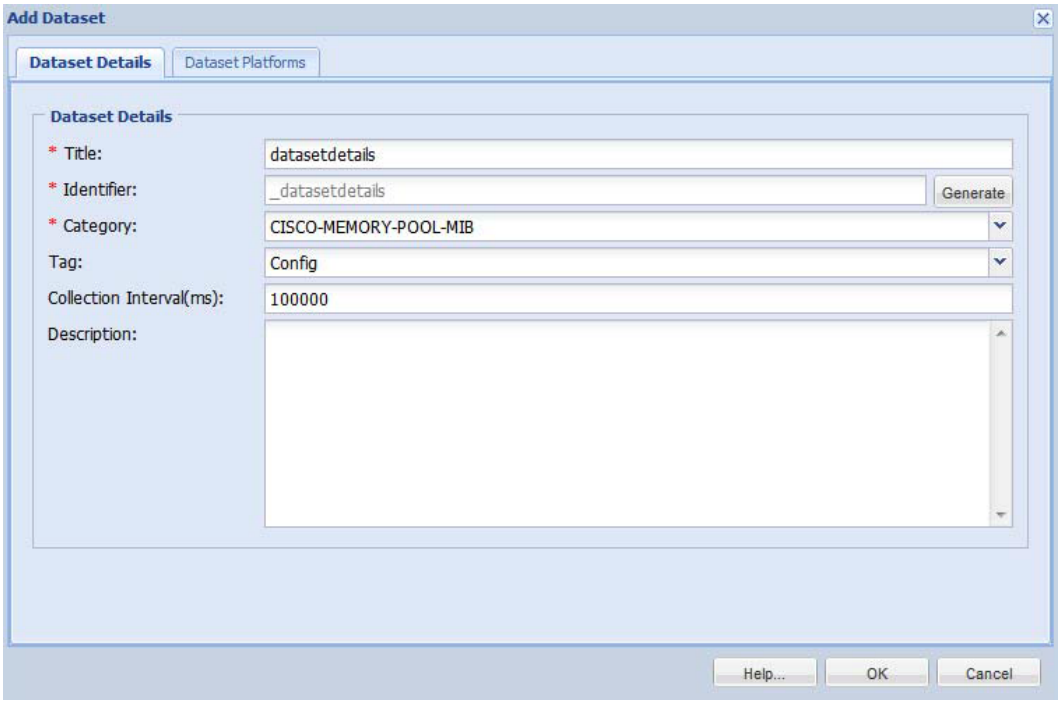
[カテゴリ（Category）]：これは必須フィールドです。これはユーザによってカスタム定義されます。存在しないカテゴリを入力すると、新しいカテゴリが作成されます。

[収集間隔（Collection Interval）]：収集間隔をミリ秒単位で指定できます。

[タグ（Tag）]：ドロップダウン リストからタグを選択します。

[説明（Description）]：データセットの説明。

図 6-51　　[データセットの詳細（Dataset Details）] の入力



ステップ 2　これらの情報を入力したら、このデータセットに適用可能なプラットフォームと収集方法を次のオプションから選択できます。

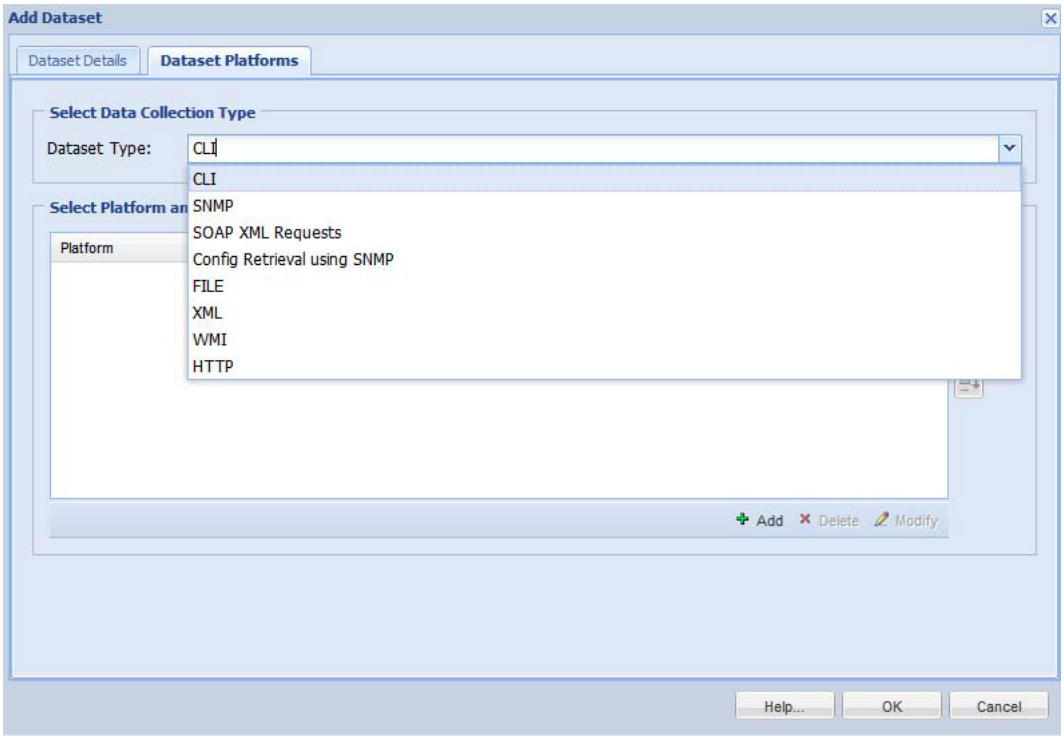
[データセット タイプ（Dataset Type）]

- CLI
- SNMP
- SOAP XML 要求（SOAP XML Requests）
- SNMP による設定の取得（Config Retrieval using SNMP）
- FILE
- XML
- WMI
- HTTP
- TL1
- IIOP

[CLI]

この例では、CLI が選択されています。CLI は、デバイスで実行するコマンドを含むデータセットです。

図 6-52　　[データセット プラットフォーム（Dataset Platforms）] オプション（[CLI] を選択）



データセットを適用する特定のプラットフォームを選択します。プラットフォームの一覧には多数のプラットフォームがあり、一致するオペレーティング システム、一致するデバイス グループ、またはその他の形式に基づきプラットフォームを選択できます。「プラットフォーム定義の管理」の章の説明に従い、独自のプラットフォーム定義を作成することもできます。

図 6-53　　[データセット エントリ詳細（Dataset Entry Details）]（CLI）

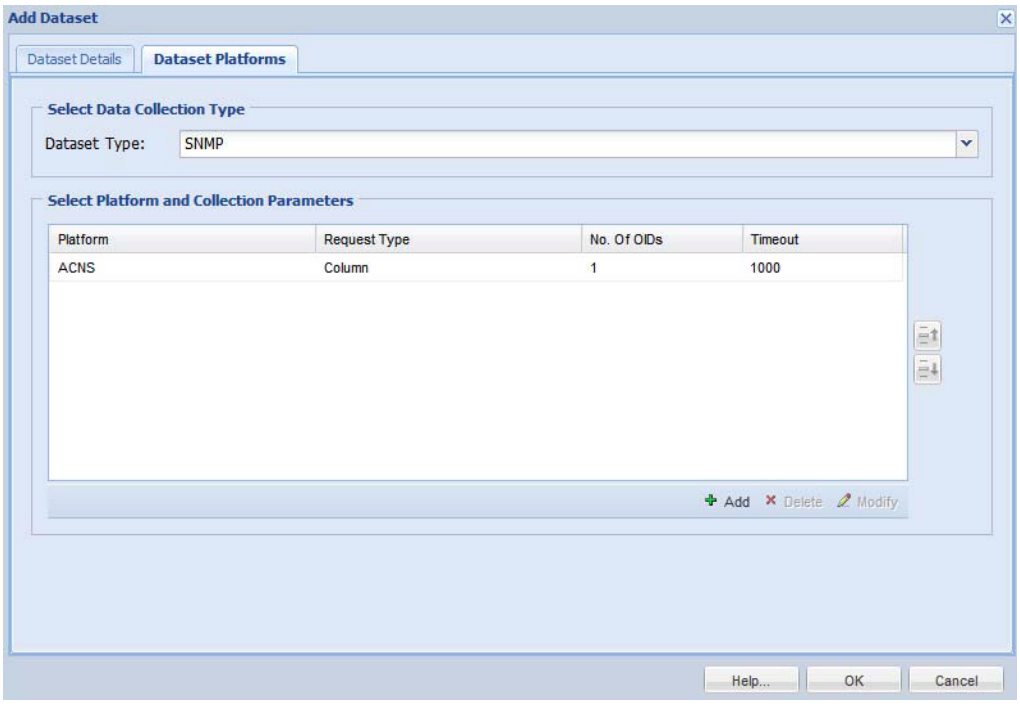
プラットフォームを選択したら、ネットワークアドレス変換(NAT)アプライアンスの場合は、「ネットワーク アドレス変換（NAT）アプライアンスのオプション パラメータ、ページ D-1」で説明されているように、コマンド文字列を入力します（CLI に基づきデータセットを作成しているため）。さらに、以下のようなその他の詳細情報を入力します。

- 設定の [サブモード（Sub Mode）] オプション（管理モードでコマンドを実行する IOS-XR プラットフォームにのみ適用可能）
- [最大行数（Maximum Lines）]（一部のコマンドの出力は数千行になることがあるため、このオプションを使用すると、選択した行数に情報を切り詰めることができます）
- [整合性ルール（Integrity Rule）]（デバイスから戻されたコマンド出力が、コマンドの実行が正常終了したときの適切な出力であるか、戻された出力がエラー メッセージであるかを判断するのに役立ちます。独自の整合性ルールを定義することができます。整合性ルールの詳細については、[アプリケーション（Applications）]>[デバイス管理（Device Management）]>[データ収集設定（Data Collection Settings）] タブを選択して確認してください）
- [マスキング ルール（Masking Rule）]（マスクする必要があるコマンド出力内の個別のフィールド）
- [データセット タイムアウト（Dataset Timeout）]（コレクタがデータ出力を待つ時間）

[SNMP]

[データセット タイプ（Dataset Type）] から [SNMP] オプションを選択し、[追加（Add）] ボタンをクリックします。

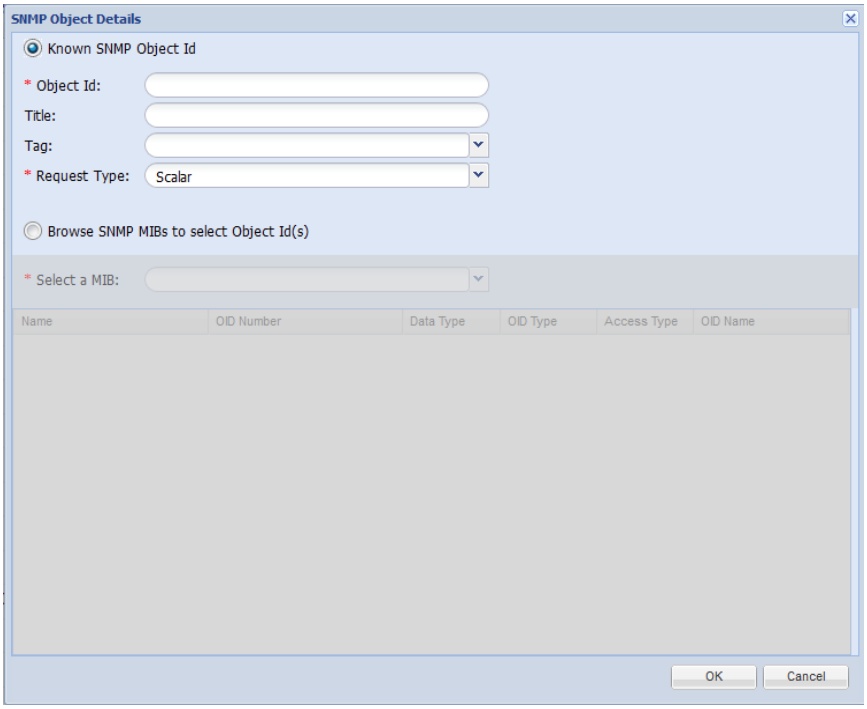
図 6-54　　[データセット プラットフォーム（Dataset Platforms）] オプション（[SNMP] を選択）



以下のスクリーンショットは、SNMP データセットの追加を示しています。図 6-55 に示すように、[データセット プラットフォーム（Dataset Platforms）] オプションで [SNMP] を選択したら、MIB 変数を追加します。事前にロードされているすべての MIB が表示されるので、自分のデータセットに追加する MIB

と変数を選択できます。

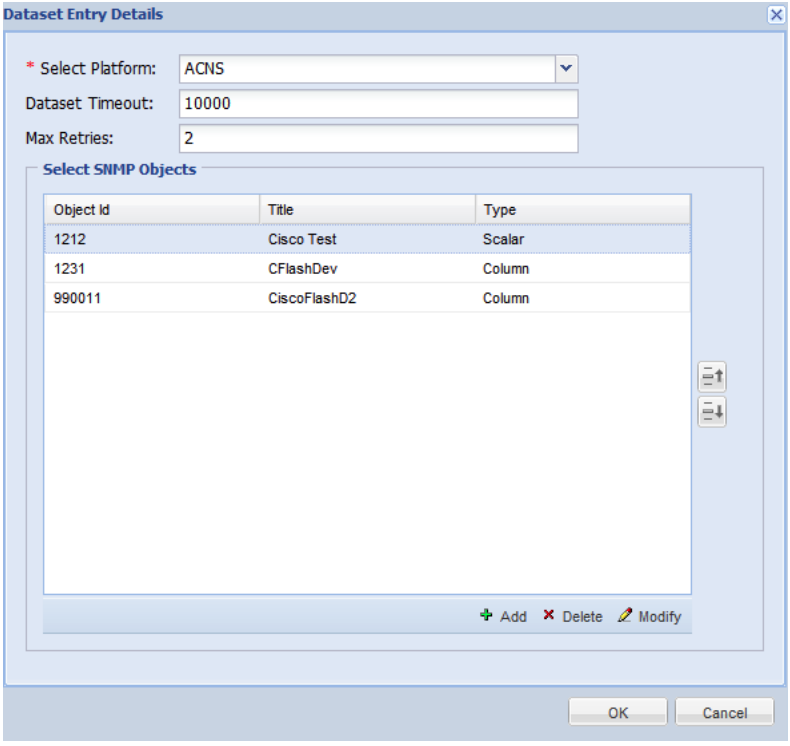
図 6-55　　[データセット エントリ詳細（Dataset Entry Details）] ([SNMP] - MIB 変数を選択）



選択を完了したら、[OK] をクリックします。

次に示すように、SNMP 変数が新しいデータセットに追加されます。

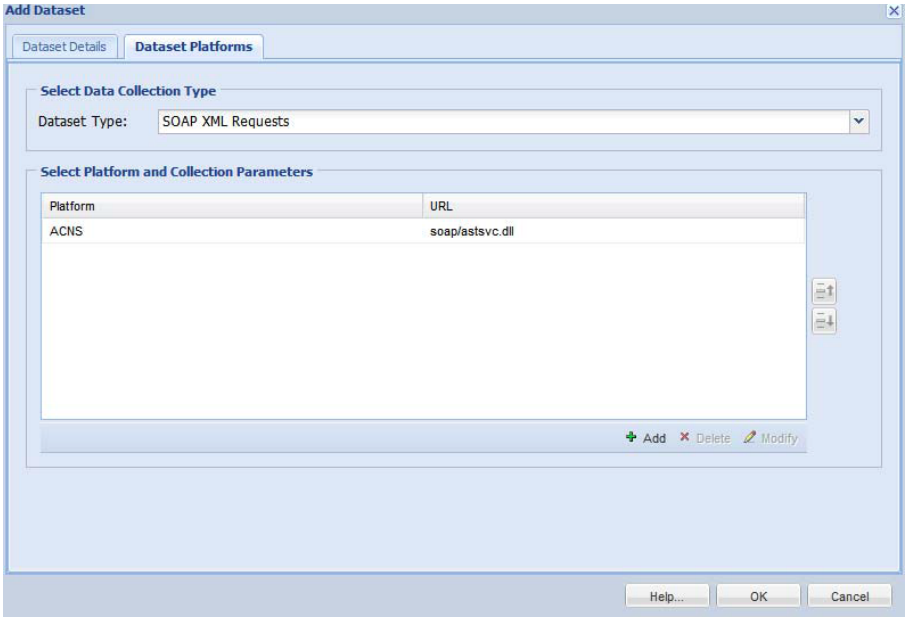
図 6-56　　[データセット エントリ詳細（Dataset Entry Details）] - SNMP



[SOAP XML 要求（SOAP XML Request）]

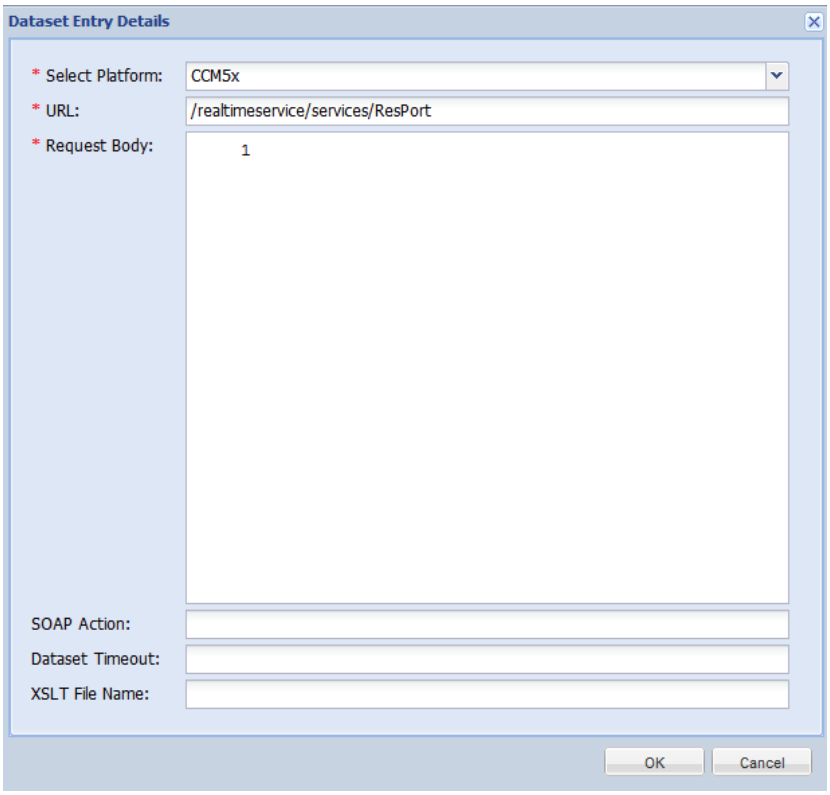
[データセット タイプ（Dataset Type）] から [SOAP XML 要求（SOAP XML Request）] オプションを選択し、
[追加（Add）] ボタンをクリックします。

図 6-57　　[データセット プラットフォーム（Dataset Platforms）]（[SOAP XML 要求（SOAP XML Requests）] を選択）



以下で定義されているように、*SOAP XML* の詳細を入力します。すべてのデータを入力すると、新しい SOAP *XML* データセットを追加できます。

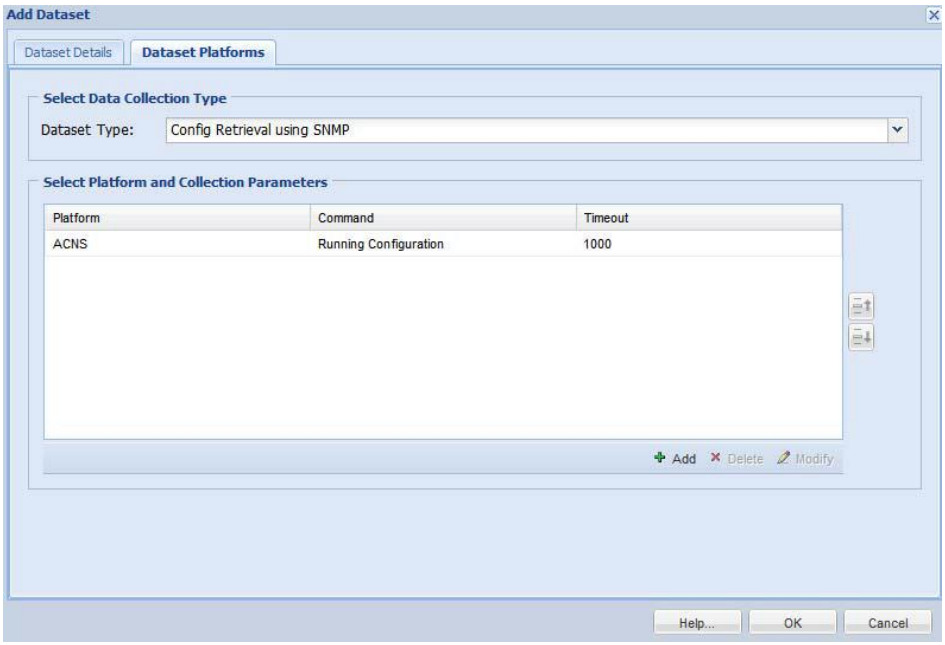
図 6-58　　[データセット エントリ詳細（Dataset Entry Details）] - SOAP XML



[SNMP による設定の取得（Config Retrieval using SNMP）]

[設定の取得（Config Retrieval）] オプションを選択し、[追加（Add）] ボタンをクリックすると、SNMP を使用して、設定（実行または起動）の収集を開始できます。選択したプロトコルに基づき作成するデータセットのタイプを選択したら、[追加（Add）] ボタンをクリックして、データセットの詳細を入力します。

図 6-59　　[データセット プラットフォーム（Dataset Platforms）]（[SNMP による設定の取得（Config Retrieval using SNMP）] を選択）



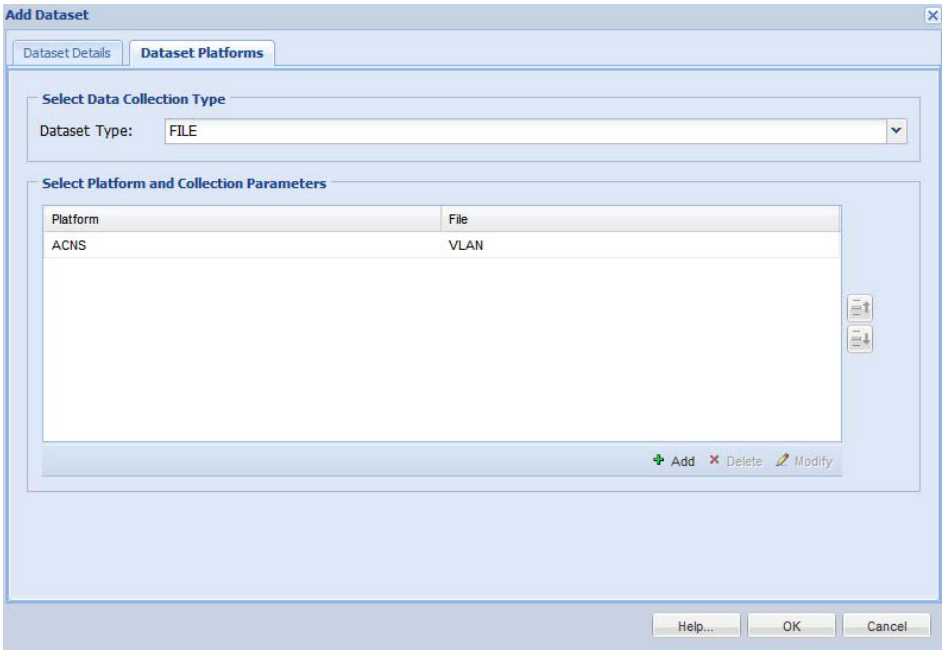
SNMP による*設定の取得*の詳細を入力します。すべてのデータを入力すると、SNMP による*設定の取得*を新しく追加できます。

図 6-60　　[SNMP による設定の取得（Config Retrieval using SNMP）] の詳細

[ファイル（FILE）]

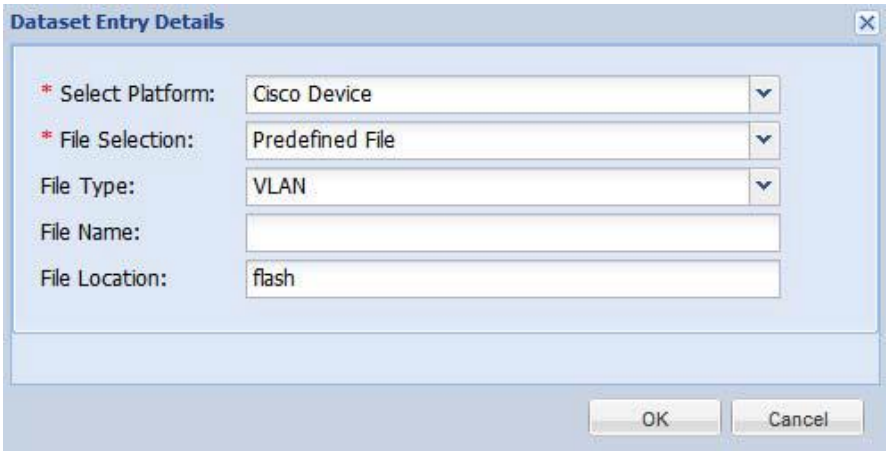
[ファイル（FILE）] オプションを選択し、[追加（Add）] ボタンをクリックすると、[事前定義ファイル（predefined file）] または [ユーザ定義ファイル（user defined file）] に基づきデータの収集を開始できます。

図 6-61　　[データセット プラットフォーム（Dataset Platforms）]（[ファイル（FILE）] を選択）



[ファイル（File）] オプションの詳細（[事前定義ファイル（Predefined File）] または [ユーザ定義ファイル（User Defined File）]）を入力します。すべてのデータを入力すると、新しいファイル（FILE）データセットを追加できます。

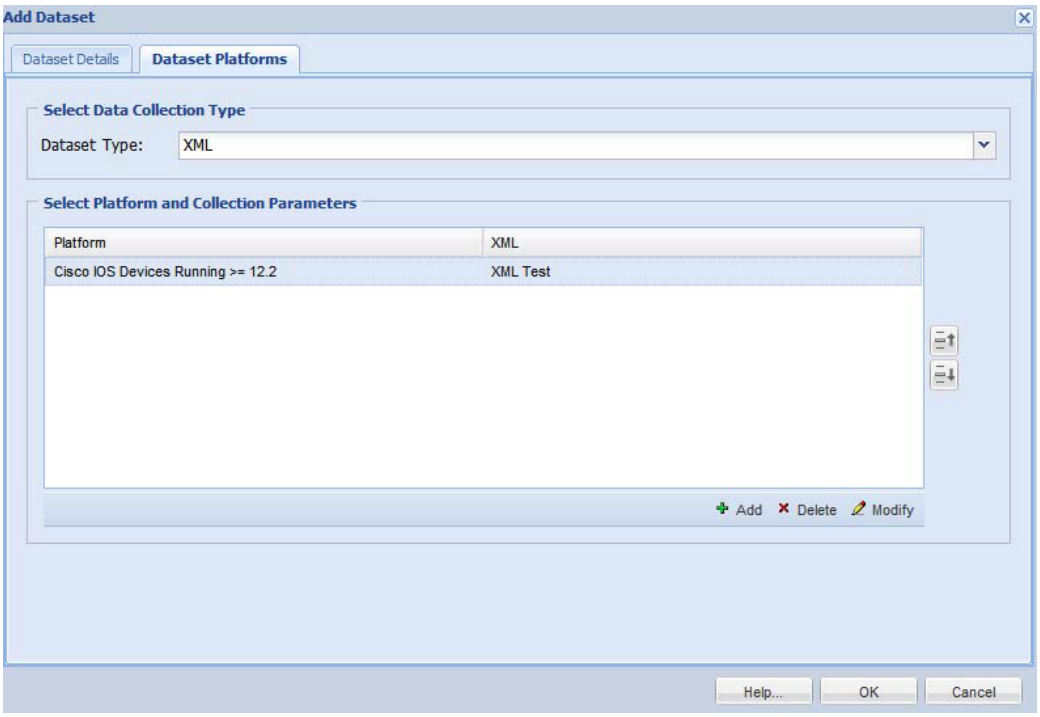
図 6-62　　[データセット エントリ詳細（Dataset Entry Details）] - [ファイル（FILE）]



[XML]

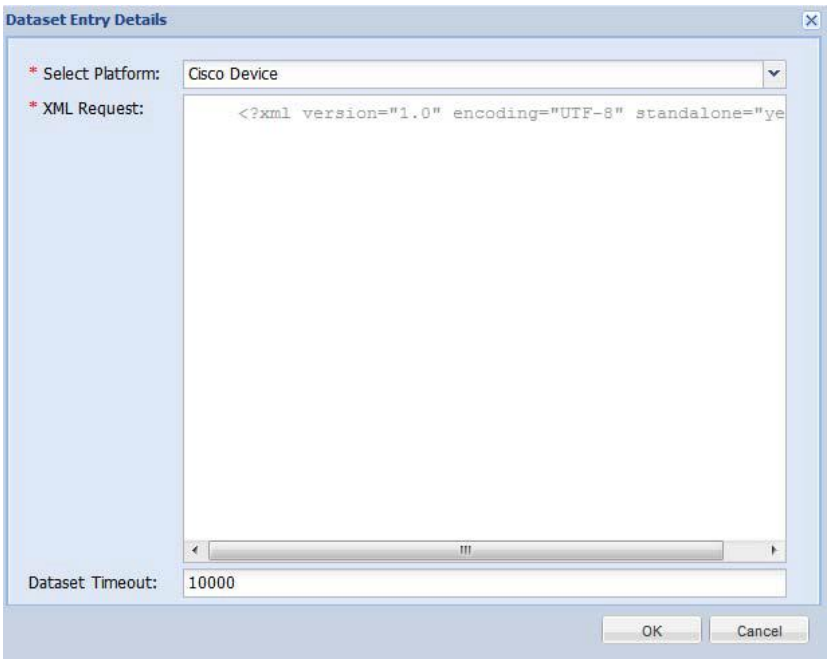
[XML] データセット オプションを選択し、[追加（Add）] ボタンをクリックすると、サポートされているプラットフォームの XML 形式でのデータ収集を開始できます。選択したプロトコルに基づき作成するデータセットのタイプを選択したら、[追加（Add）] ボタンをクリックして、データセットの詳細を入力します。

図 6-63　　[データセット プラットフォーム（Dataset Platforms）]（[XML] を選択）



XML 選択の詳細を入力します。すべてのデータを入力すると、新しい XML データセットを追加できます。

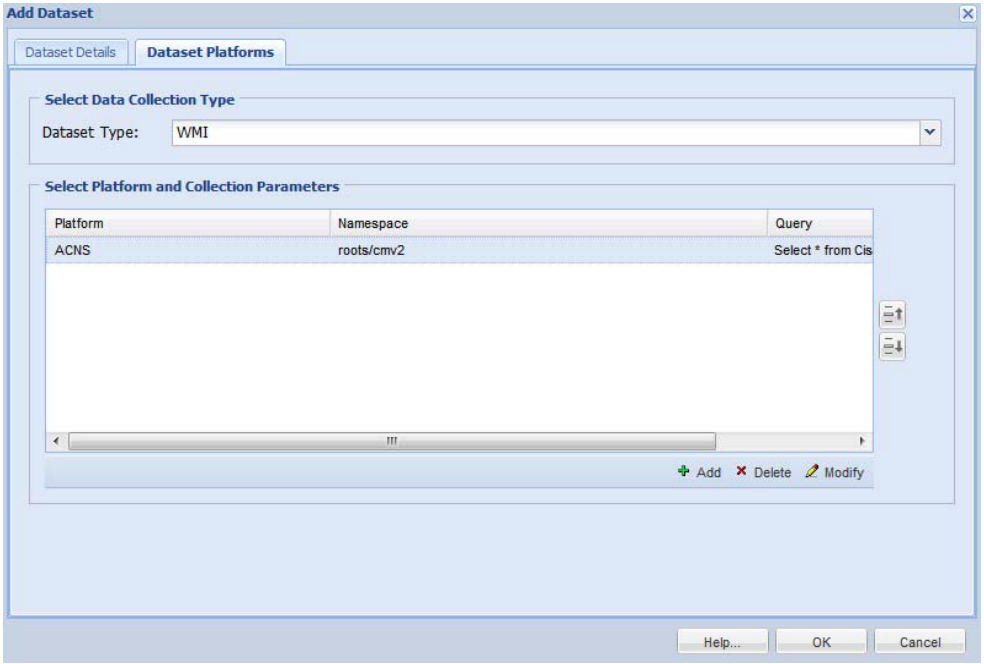
図 6-64　　[データセット エントリ詳細（Dataset Entry Details）] - [XML]



[WMI]

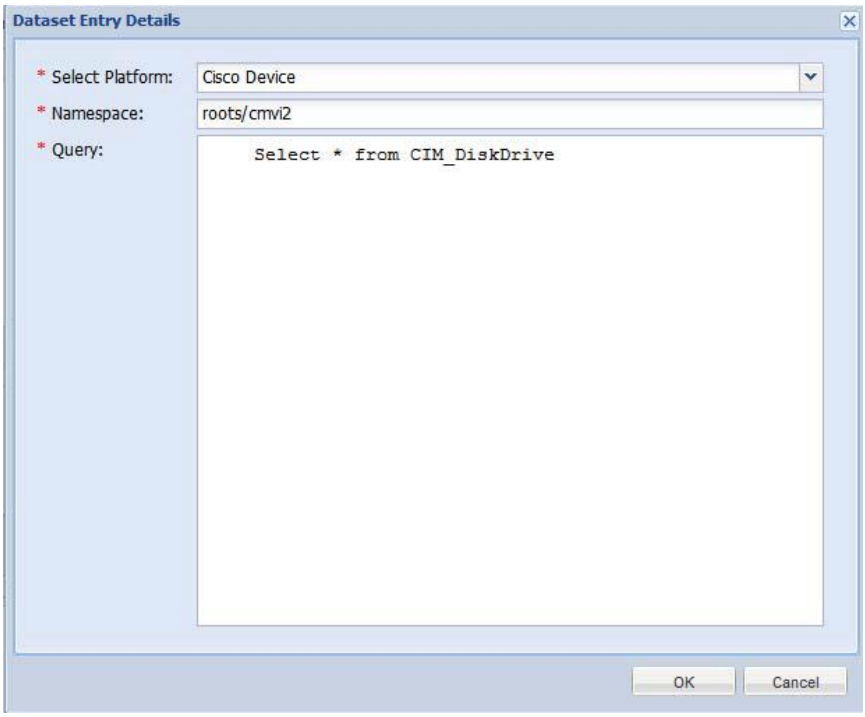
[WMI] データセット オプションを選択し、[追加（Add）] ボタンをクリックすると、サポートされているプラットフォームの WMI データの収集を開始できます。選択したプロトコルに基づき作成するデータセットのタイプを選択したら、[追加（Add）] ボタンをクリックして、データセットの詳細を入力します。

図 6-65　　[データセット プラットフォーム（Dataset Platforms）]（[WMI] を選択）



WMI 選択の詳細を入力します。すべてのデータを入力すると、新しい WMI データセットを追加できます。

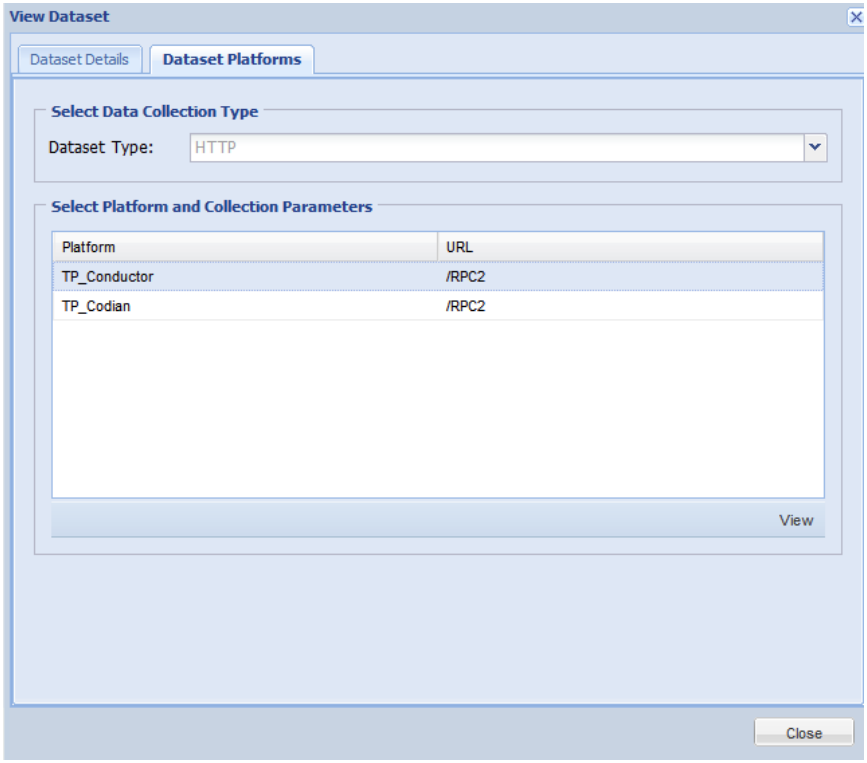
図 6-66　　[データセット エントリ詳細（Dataset Entry Details）] - [WMI]



[HTTP]

[HTTP] オプションを選択し、[追加（Add）] ボタンをクリックしたら、プラットフォームを選択して URL を指定します。これらは必須フィールドです。完了したら、データ収集を開始できます。

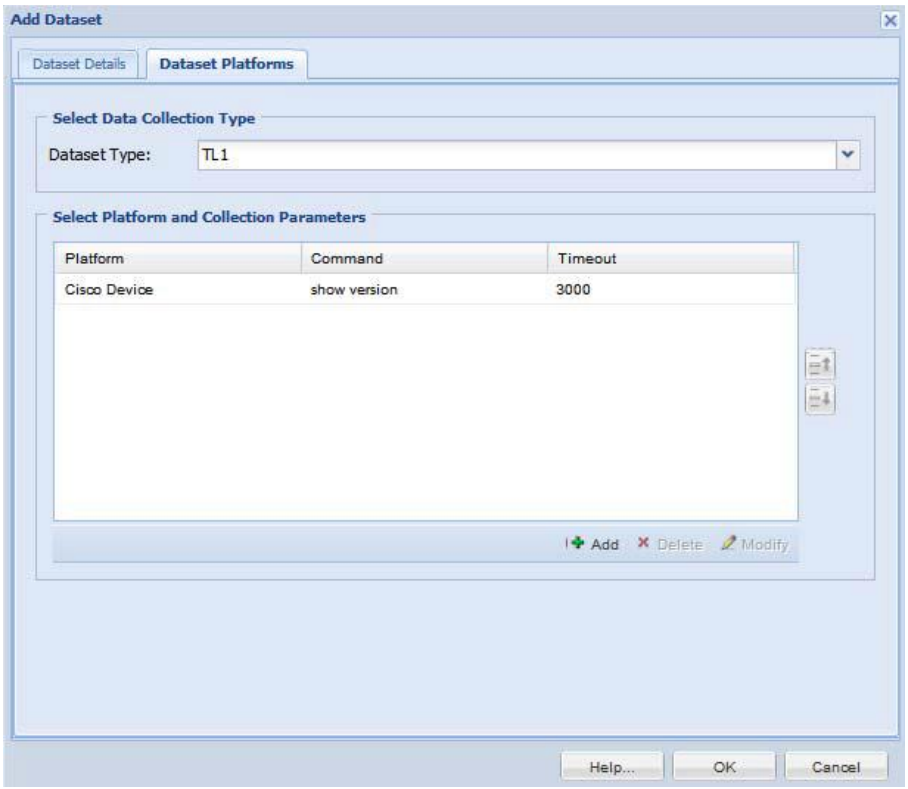
図 6-67　　[データセット プラットフォーム（Dataset Platforms）]（[HTTP] を選択）



[TL1]

[TL1] オプションを選択し、[追加（Add）] ボタンをクリックしたら、プラットフォームとコマンド文字列を選択します。これらは必須フィールドです。[最大行数（Maximum Lines）]、[整合性ルール（Integrity Rule）]、[マスキング ルール（Masking Rule）]、[データセット タイムアウト（Dataset Timeout）] を入力することもできます。[OK] ボタンをクリックして、データを追加します。

図 6-68　　[データセット プラットフォーム（Dataset Platforms）]（[TL1] を選択）



[IIOP]

[IIOP] オプションを選択し、[追加（Add）] ボタンをクリックしたら、プラットフォームを選択します。これは必須フィールドです。[データセット タイムアウト（Dataset Timeout）] を入力し、API またはすべての API を選択することもできます。[OK] ボタンをクリックして、データを追加します。

図 6-69　　[データセット プラットフォーム（Dataset Platforms）]（[IIOP] を選択）

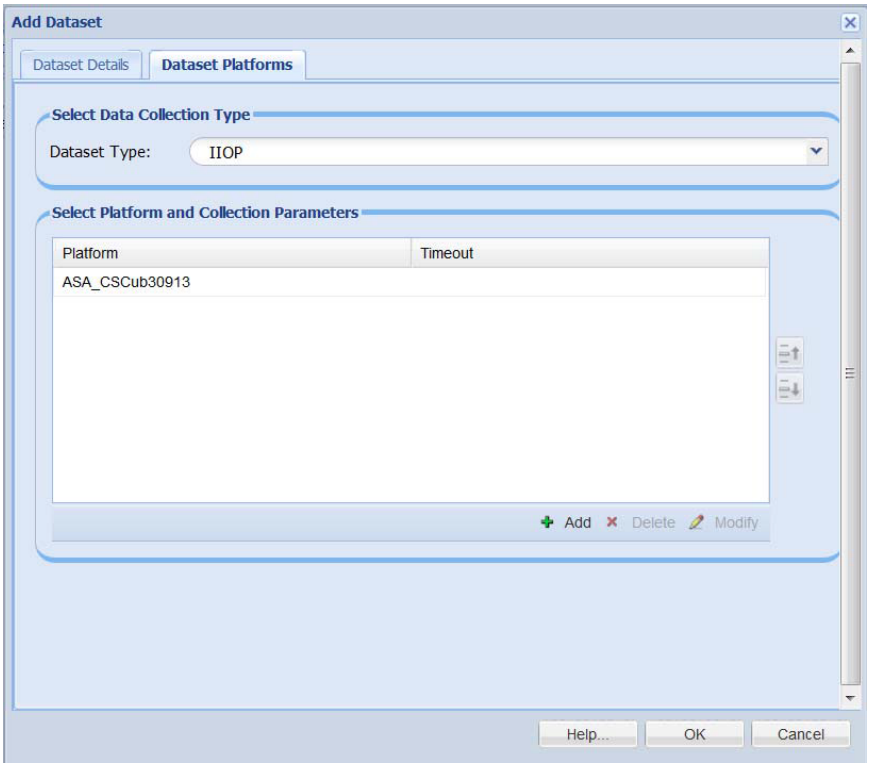
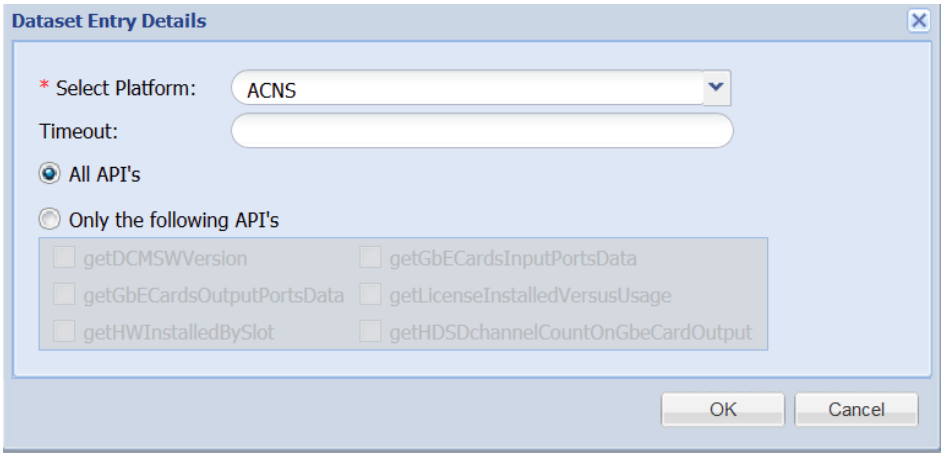


図 6-70　　[データセット エントリ詳細（Dataset Entry Details）]



CSPC フローチャートに戻る

動的データセット

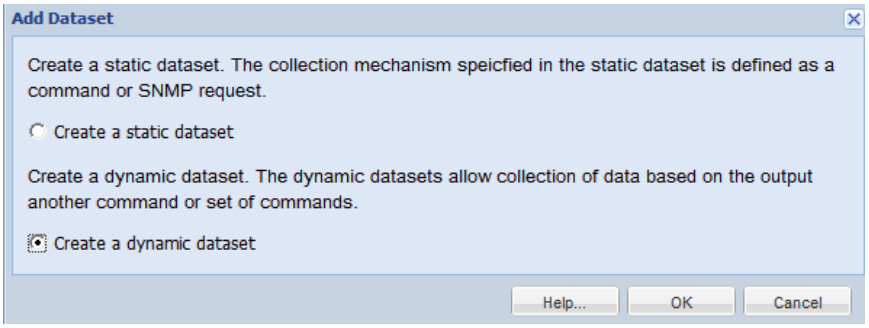
動的データセットを使用すると、別のコマンドまたはコマンド セットの出力に基づいてデータを収集できます。

動的データセットを作成するには、以下の手順に従います。

ステップ 1 [収集ルール（Collection Rules）] で [データセットの管理（Manage Datasets）] をクリックします

ステップ 2 [データセットの追加（Add Dataset）] ボタンをクリックします。

図 6-71　　[データセットの追加（Add Dataset）]



ステップ 3 [動的データセットの作成（Create Dynamic Dataset）] を選択し、[OK] をクリックします。

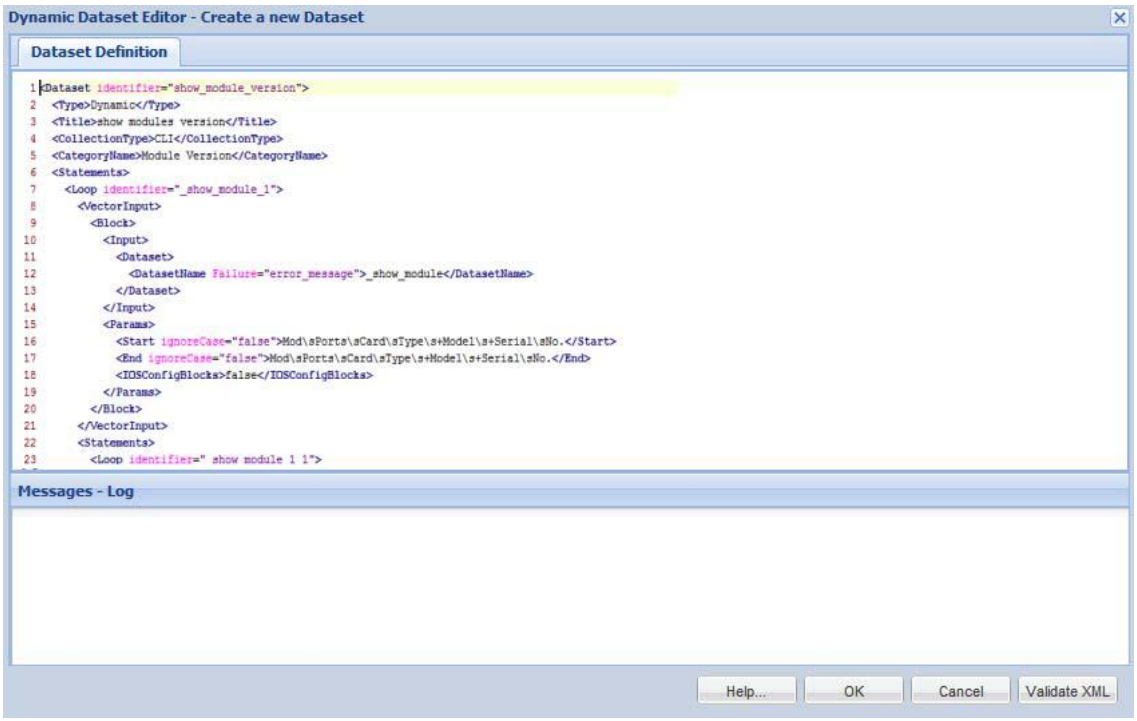
ステップ 4 [データセット定義（Dataset Definition）] ボックスで、動的データセットの XML を指定します。

XML ファイルでは API Pari XML スキーマが使用されます。

ステップ 5 [OK] をクリックします。

動的データセットが作成され、[データセットの管理（Manage Datasets）] に追加されます。

図 6-72　　動的データセットの作成

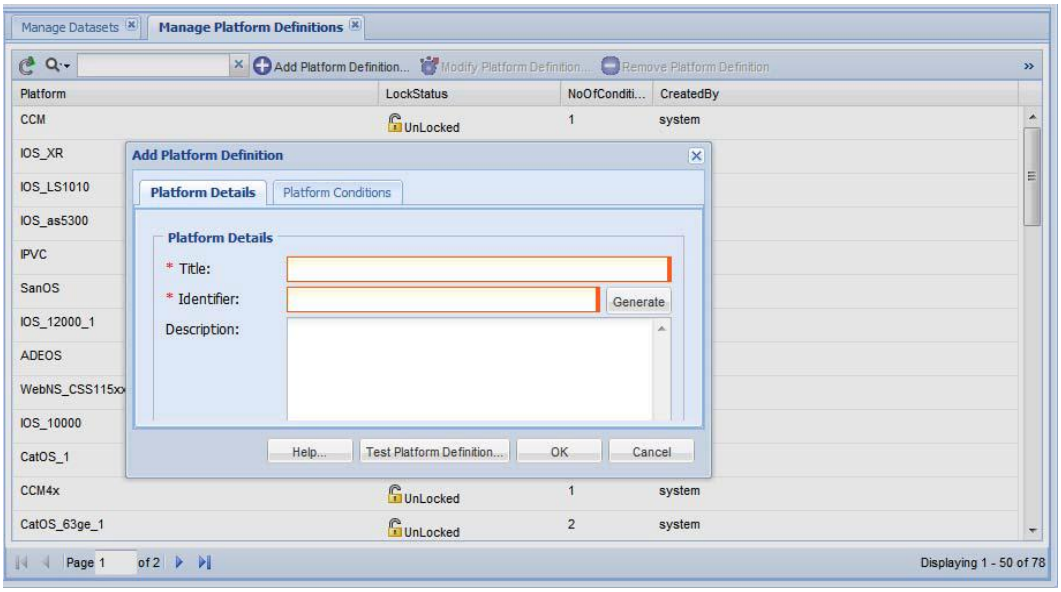

Dynamic Dataset Editor - Create a new Dataset
Dataset Definition
<Dataset identifier="show_module_version">
<Type>Dynamic</Type>
<Title>show modules version</Title>
<CollectionType>CLI</CollectionType>
<CategoryName>Module Version</CategoryName>
<Statements>
<Loop identifier="_show_module_1">
<VectorInput>
<Block>
<Input>
<Dataset>
<DatasetName failure="error_message">_show_module</DatasetName>
</Dataset>
</Input>
<Params>
<Start ignoreCase="false">Mod\sPorts\sCard\sType\s+Model\s+Serial\sNo.</Start>
<End ignoreCase="false">Mod\sPorts\sCard\sType\s+Model\s+Serial\sNo.</End>
<IOSConfigBlocks>false</IOSConfigBlocks>
</Params>
</Block>
</VectorInput>
<Statements>
<Loop identifier=" show module 1 1">
Messages - Log
Help...
OK
Cancel
Validate XML

[プラットフォーム定義の管理（Manage Platform Definitions）]

[プラットフォーム定義の管理（Manage Platform Definitions）] では、一定の条件に一致するデバイスのグループを選択できます。[データセットの管理（Manage Datasets）] を使用してこのデバイスのグループから収集するデータを選択できます。その一定の条件に一致する新しいデバイスが検出されると、そのデバイスは自動的にこのプラットフォームの一部になります。そのため、このプラットフォーム定義内の他のデバイスに対して収集された同じデータが新しいデバイスから収集されます。

新しいプラットフォーム定義を作成するには、以下の手順に従います。

図 6-73　　プラットフォーム定義の作成

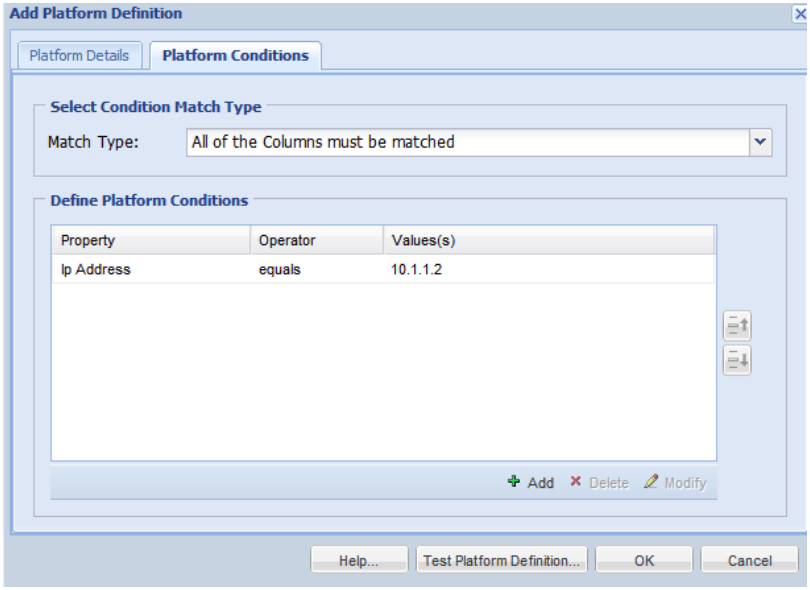


ステップ 1 [プラットフォーム定義の追加（Add Platform Definition）] ボタンをクリックします。

ステップ 2 図 6-73 に示すように、新しいプラットフォーム定義の [タイトル（Title）]、[識別情報（Identifier）]、および [説明（Description）] を入力します。

ステップ 3 基本データを入力したら、次に示すように、このプラットフォーム定義を構成する条件を入力します。

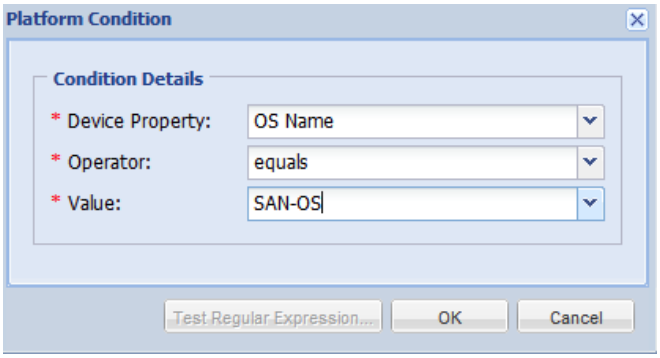
図 6-74　　[プラットフォーム条件（Platform Conditions）] の追加



ステップ 4　このプラットフォームの定義にデバイスを含めるためには、定義するすべての条件に一致する必要があるか、または条件の一部を満たすだけでよいかを選択します。

ステップ 5　[追加（Add）] をクリックして、条件の追加を開始します。

図 6-75　　[プラットフォーム条件（Platform Conditions）]



ステップ 6　条件を入力するときには、以下のオプションを指定します。

- [OS 名（OS Name）]、[OS バージョン（OS Version）]、[製品モデル（Product Model）]、[SNMP システムのオブジェクト ID（SNMP Sys Object ID）]、および [SNMP システムの説明（SNMP Sys Description）] を選択できます。
- [デバイス プロパティ（Device Property）] の選択内容に応じて（つまり、リストから [OS 名（OS Name）] を選択しているか、または [OS バージョン（OS Version）]、[製品モデル（Product Model）]、[SNMP システムのオブジェクト ID（SNMP Sys Object ID）] を選択しているか）、[値（Value）] フィールドは変わります。[演算子（Operator）] はこの 2 つのフィールドを比較するために使用します。
- [演算子（Operator）] には、[等しい（equals）]、[等しくない（does not equal）]、[リストに含まれている（in the list）]、[リストに含まれていない（not in the list）]、[正規表現に一致しない（does not match regular expression）]、および [正規表現に一致する（matches regular expression）] の 6 つのオプションがあります。

CSPC フローチャートに戻る

プラットフォームの定義を作成したら、次に示すように、[プラットフォーム定義のテスト（Test Platform Definition）] を使用して、この定義と一致するプラットフォームがあるかどうかを確認します。

図 6-76　　プラットフォーム定義のテスト

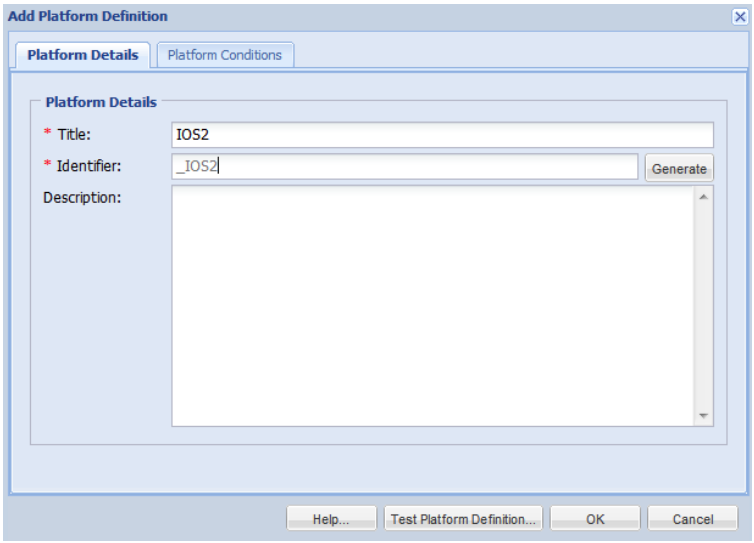


図 6-77　　カスタム プラットフォーム定義のテスト

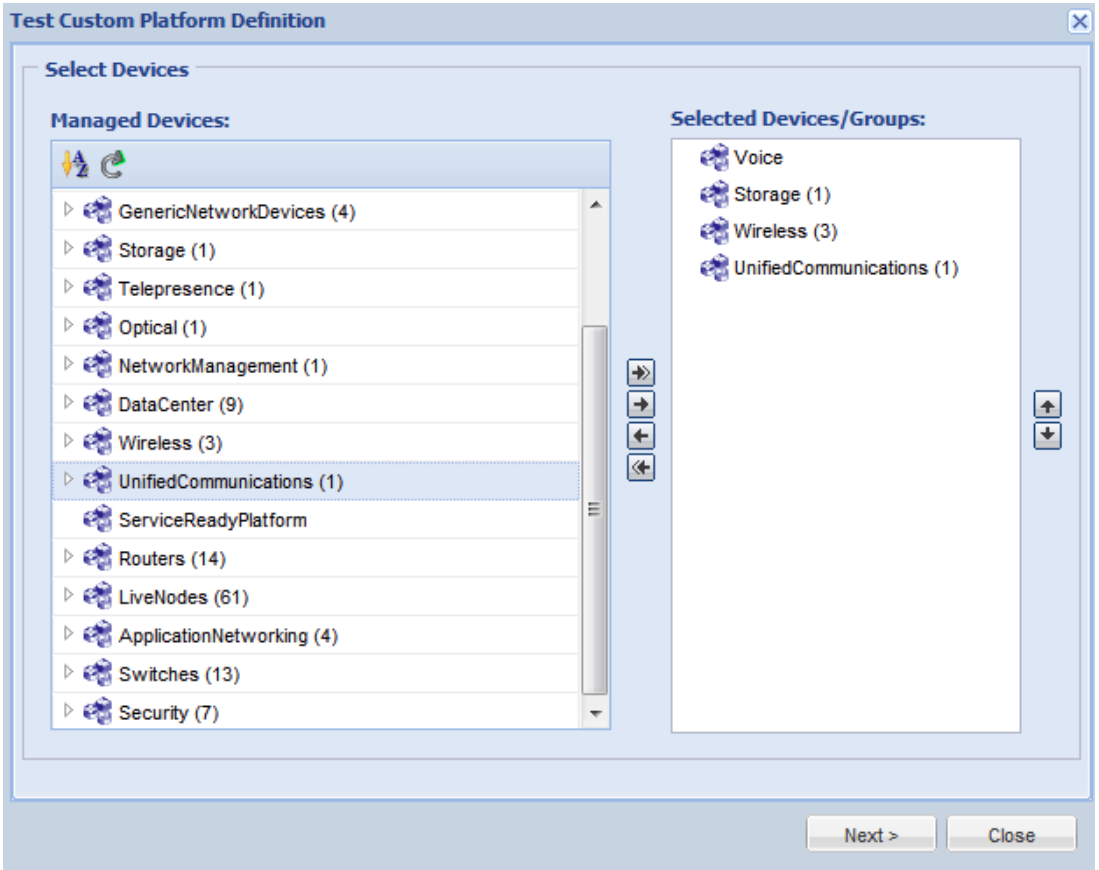
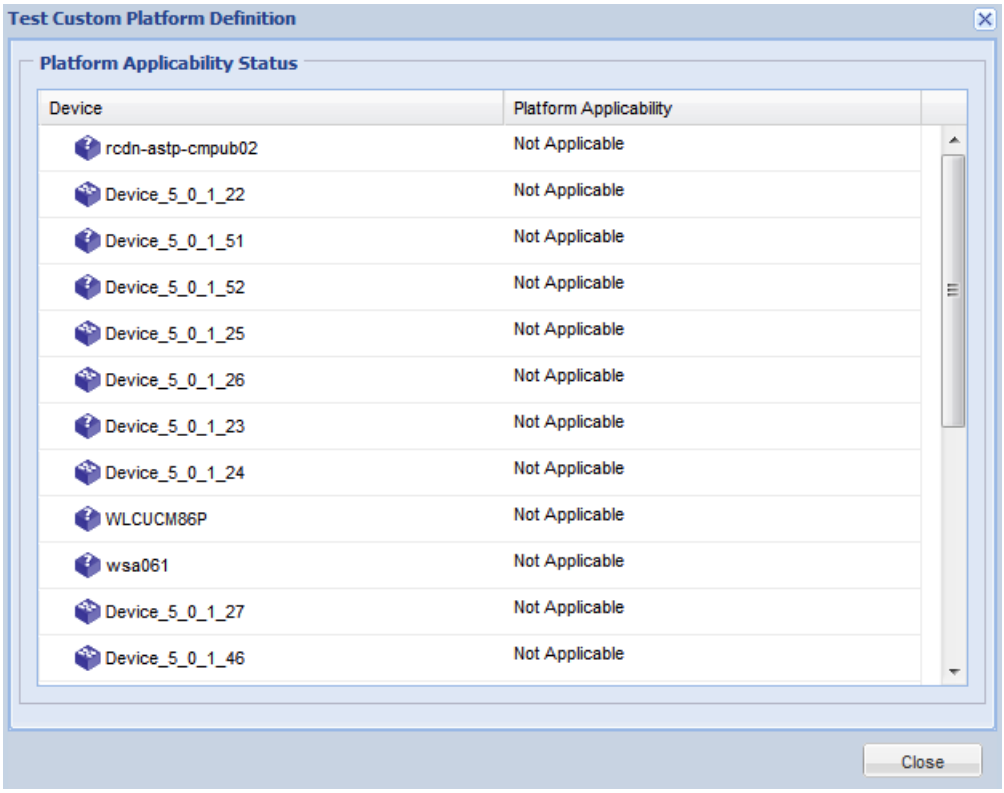
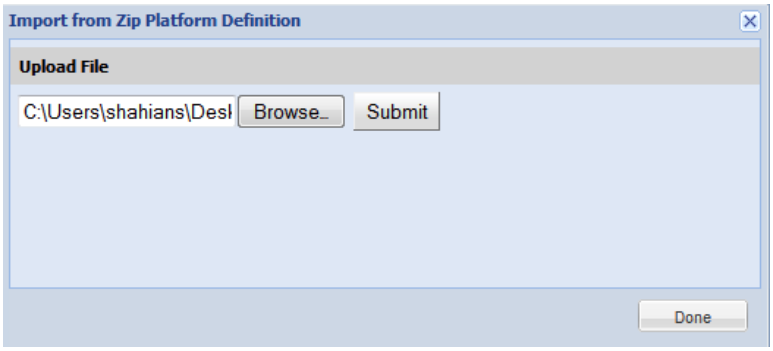


図 6-78　　[プラットフォーム適用状況（Platform Applicability Status）]



システムにローカルに保存されている zip ファイルからプラットフォーム定義をインポートすることもできます。これを行うには、[プラットフォーム定義の管理（Manage Platform Definitions）] ウィンドウで右クリックし、[zip ファイルからプラットフォーム定義をインポート（Import Platform Definition from Zip File）] オプションを選択します。次に、
図 6-79 に示すように、システム上にあるプラットフォーム定義を含む zip ファイルを参照して [送信（Submit）] をクリックします。

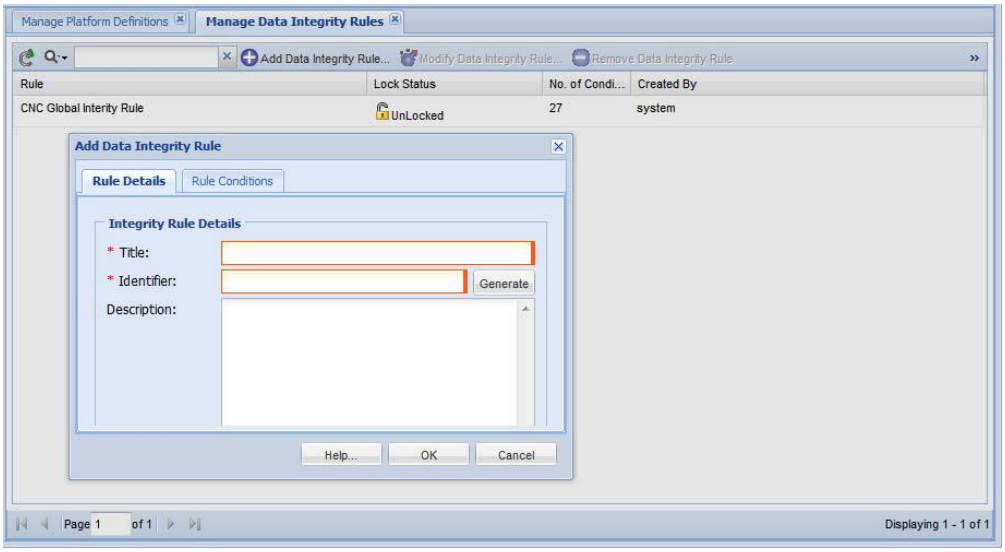
図 6-79　　zip ファイルからインポート



[データ整合性ルールの管理（Manage Data Integrity Rules）]

データ整合性ルールは、実行したコマンドが正しい応答を戻しているか、エラー メッセージを戻しているかを確認するために定義されます。次に示すように、新規のデータ整合性ルールを作成できます。

図 6-80　　新しいデータ整合性ルールの作成

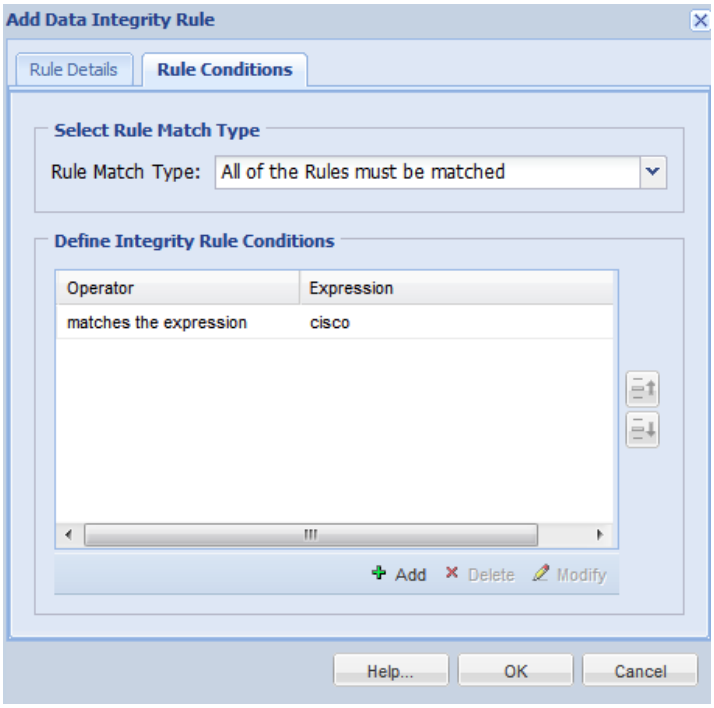


ステップ 1 [データ整合性ルールの追加（Add Data Integrity Rules）] をクリックします。

ステップ 2 新しいデータ整合性ルールの [タイトル（Title）]、「識別情報（Identifier）]、[説明（Description）] を入力します。

ステップ 3 基本データを入力したら、次に示すように、そのルールを構成するルール条件を入力します。

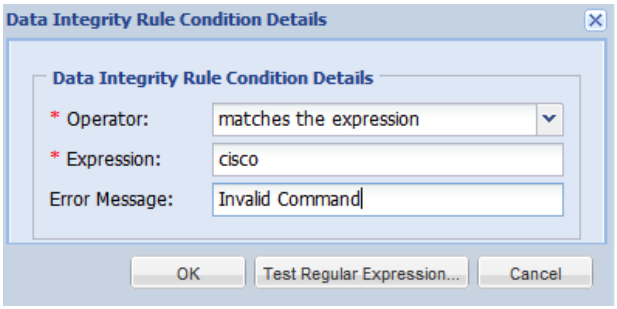
図 6-81　　データ整合性ルールのルール条件



ステップ 4　この整合性ルールにデバイスを含めるためには、定義するすべての条件に一致する必要があるか、または条件の一部を満たすだけでよいかを選択します。

ステップ 5　[追加（Add）] をクリックして、条件の追加を開始します。

図 6-82　　[ルール条件（Rule Conditions）]



ステップ 6　条件入力時には、[演算子（Operator）]（[正規表現に一致する（matches the expression）] または [正規表現に一致しない（does not match the expression）]）、正規表現（[Expression]）の値、および表示する [エラー メッセージ（Error Message）] を指定します。

システムにローカルに保存されている zip ファイルからプラットフォーム定義をインポートすることもできます。これを行うには、[データ整合性ルールの管理（Manage Data Integrity Rules）] ウィンドウを右クリックし、[zip ファイルからデータ整合性ルールをインポート（Import Data Integrity Rules from a Zip File）] オプションを選択します。次に、システム上にある整合性ルールを含む zip ファイルを参照して [送信（Submit）] をクリックします。

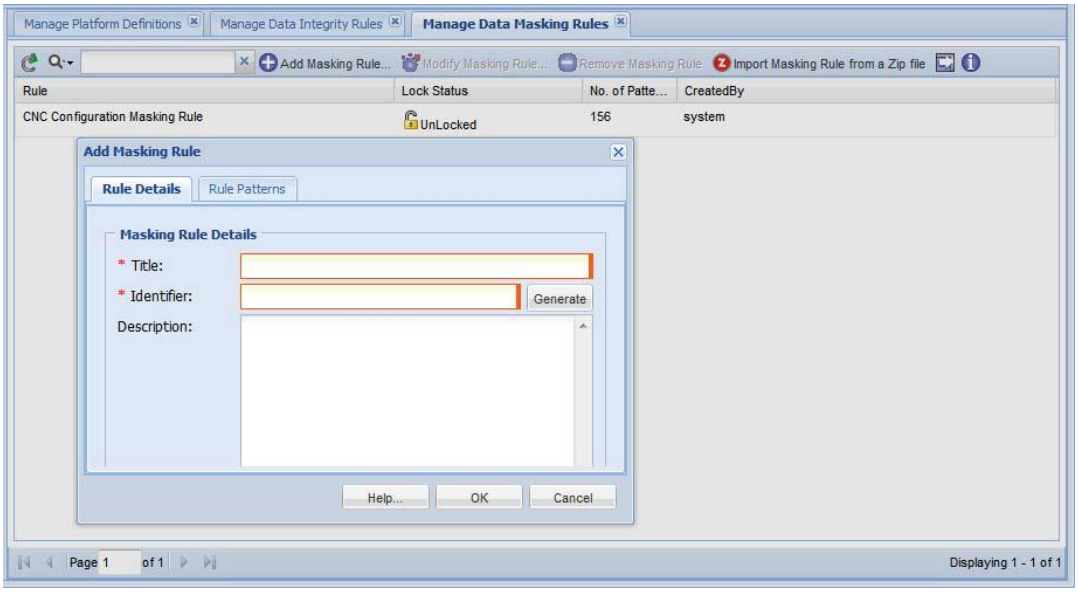
CSPC フローチャートに戻る

[データ マスキング ルールの管理（Manage Data Masking Rules）]

マスキング オプションは、コンフィギュレーション ファイル内の一定の機密情報（ユーザ名とパスワードなど）を、より高いレベルのアプリケーションにエクスポートする前に、マスクするために用意されています。データをエクスポートする前にコレクタがマスクする必要があるデータを指示するデータ マスキング ルールを作成できます。

以下の手順に従って新規のマスキング ルールを作成します。

図 6-83　　新しいデータ マスキング ルールの作成

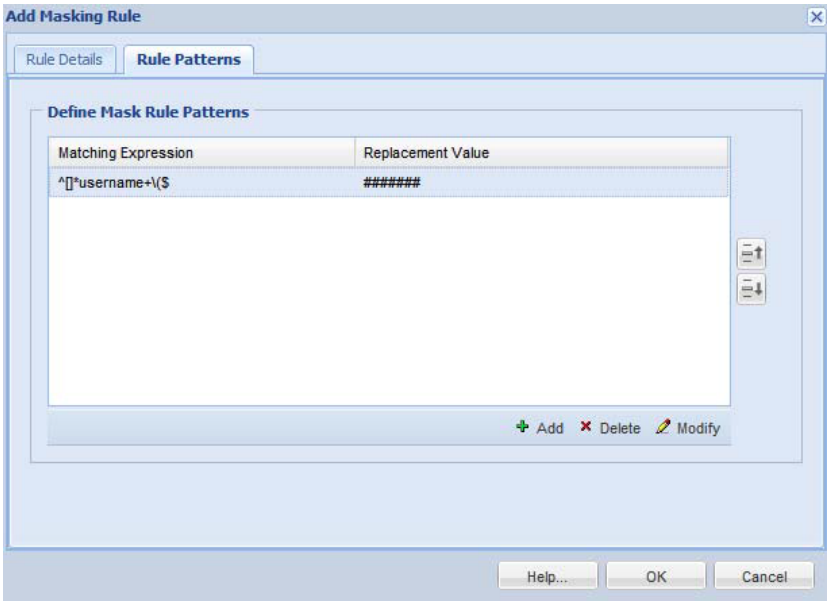


ステップ 1 [マスキング ルールの追加（Add Masking Rules）] ボタンをクリックします。

ステップ 2 [マスキング ルールの追加（Add Masking Rules）] ウィンドウで、新しいマスキング ルールの [タイトル（Title）]、「識別情報（Identifier）]、[説明（Description）] を入力します。

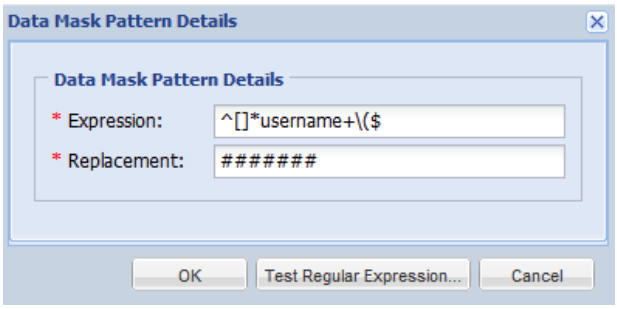
ステップ 3 基本データを入力したら、次に示すように、そのルールを構成するルール パターンを入力します。

図 6-84　　データ マスキング ルールの [ルール パターン（Rule Patterns）]



ステップ 4　[追加（Add）] をクリックして、条件の追加を開始します。

図 6-85　　ルール パターン条件



ステップ 5　ここで示すように、コンフィギュレーション ファイルにユーザ名に続き、パスワードが含まれている場合、文字列 xxxxxx　で置き換えられます。

システムにローカルに保存されている zip ファイルからマスキング ルールをインポートすることもできます。これを行うには、[データ マスキング ルールの管理（Manage Data Masking Rules）] ウィンドウで右クリックし、[zip ファイルからマスキング ルールをインポート（Import Masking Rules from a Zip File）] オプションを選択します。次に、システム上にあるマスキング ルールを含む zip ファイルを参照して [送信（Submit）] をクリックします。

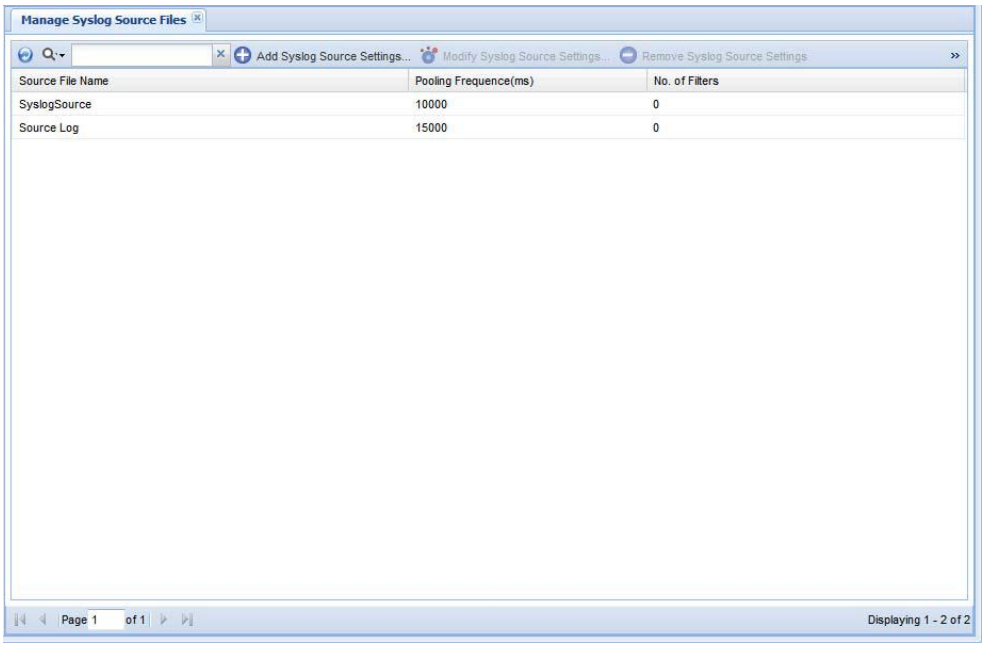
CSPC フローチャートに戻る

[Syslog ソース ファイルの管理（Manage Syslog Source Files）]

[Syslog ソース ファイル（Syslog Source Files）] オプションを使用すると、デバイスからの Syslog 収集を定義できます。Syslog ソースの新しい設定を追加できます。

サポート対象の Syslog 形式や例については、「付録 C サポート対象の Syslog 形式」を参照してください。

図 6-86　　[Syslog ソース ファイルの管理（Manage Syslog Source Files）]



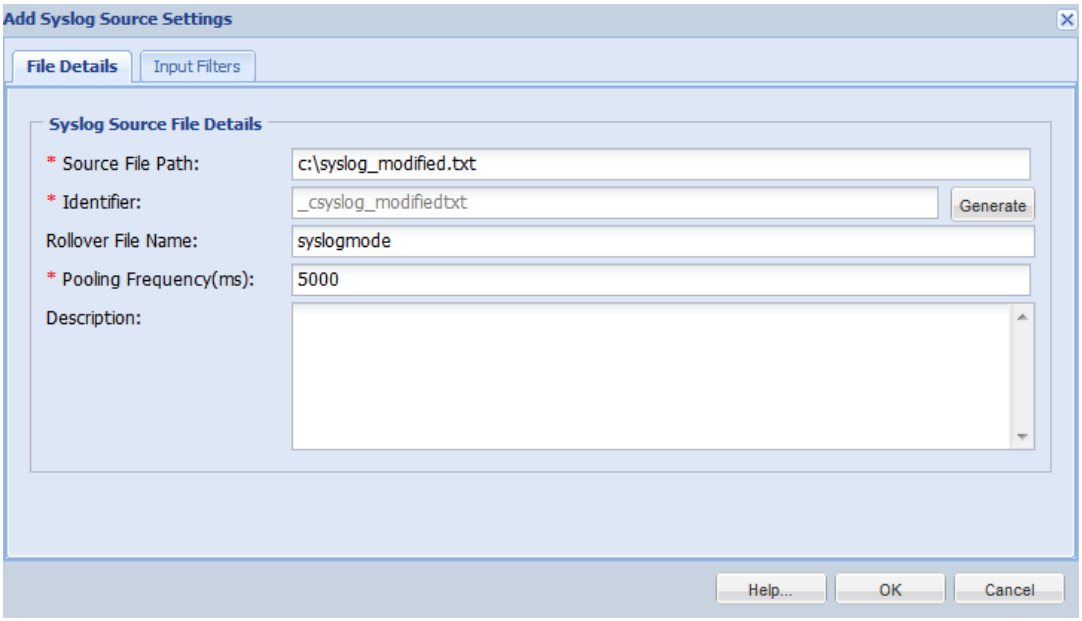
[追加（Add）] ボタンをクリックして、新規の Syslog ソース ファイルを作成します。

[Syslog ソースの追加（Add Syslog Source）] オプションを使用すると、新規の Syslog ソースを追加することができます。Syslog ソースの追加の画面には、2 つのタブがあります。

1 つ目のタブは図 6-87 に示すように、[ファイルの詳細（File Details）] です。このウィンドウでは以下の情報を入力する必要があります。

- [ソース ファイルのパス（Source File Path）]：Syslog ソースがあるパスです。
- [識別情報（Identifier）]：ユーザ定義またはシステム生成の識別情報です。
- [ロールオーバー ファイルの名前（Roll Over File Name）]：プライマリ ファイルがロールオーバーした場合に、スプールする必要があるファイルの名前です。
- [ポーリング頻度（Polling Frequency）]：Syslog メッセージをポーリングするポーリング頻度です。値の範囲は 5,000 ～ 3,600,000 ミリ秒です。
- [説明（Description）]：ファイルの説明です。

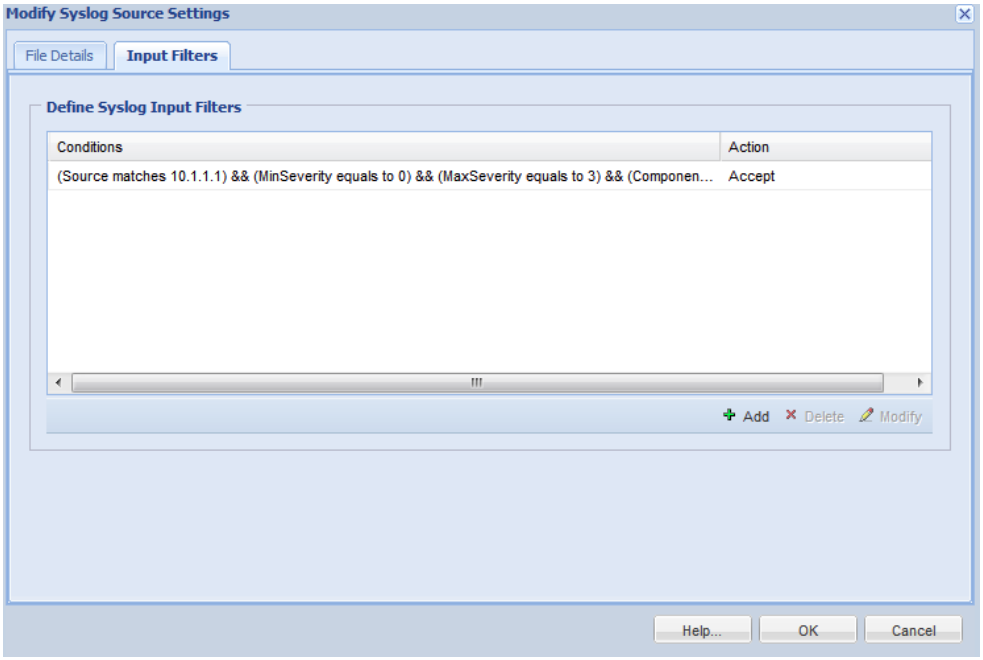
図 6-87　　Syslog ソースの追加



2 つ目のタブは [入力フィルタ（Input Filters）] です。[追加（Add）] ボタンを選択すると、[入力フィルタの詳細（Input Filter Details）] ウィンドウが開きます。このウィンドウでは以下の情報を入力する必要があります。

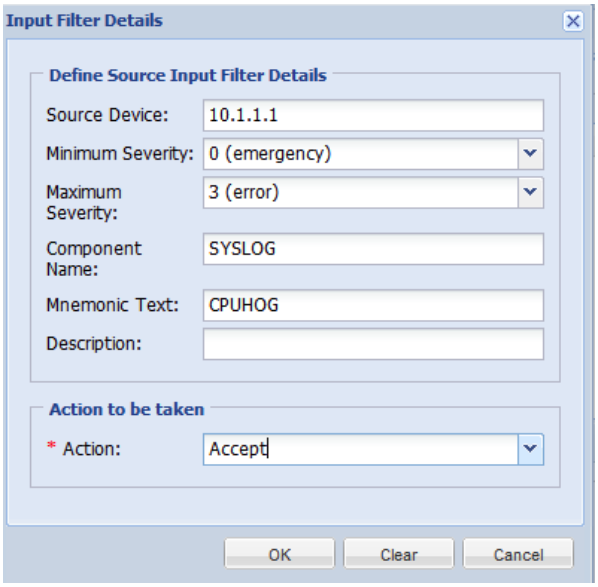
- [送信元デバイス（Source Device）]：スプールするメッセージを出力するデバイスです。
- [最小の重大度（Minimum Severity）]：表示する必要がある最小の重大度です。
- [最大の重大度（Maximum Severity）]：表示する必要がある最大の重大度です。
- [コンポーネント名（Component Name）]：メッセージ内のコンポーネントの名前です。
- [ニーモニック テキスト（Mnemonic Text）]：メッセージ内のニーモニック テキストです。
- [説明（Description）]：メッセージ内の説明です。
- [実行するアクション（Action to be taken）]：Syslog を [承認（Accept）] するか [廃棄（Drop）] するかを選択します。

図 6-88　　入力フィルタの追加



[追加（Add）] ボタンをクリックすると、図 7-89 に示す画面が表示されます。次に示すように詳細を入力します。

図 6-89　　[入力フィルタの詳細（Input Filter Details）] の追加



[その他のルール（Miscellaneous Rules）]

[デバイス管理（Device Management）] タブの [その他のルール（Miscellaneous Rules）] サブ タブでは、ルール、プロファイルの設定、ワークフローの管理ができます。

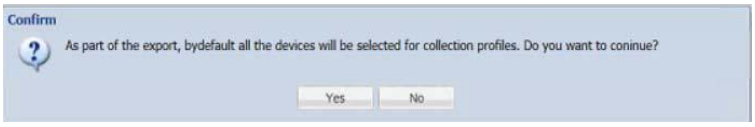
この項では、[その他のルール（Miscellaneous Rules）] オプションの以下の項目について説明します。

- [すべてのルールのエクスポート（Export All Rules）]
- [すべてのルールのインポート（Import All Rules）]
- [DSIRT ファイルのインポート（Import DSIRT Files）]
- [アプリケーション検出プロファイルの管理（Manage Application Discovery Profiles）]
- [SNMP トラップ プロファイルの管理（Manage SNMP Trap Profiles）]
- [ジャンプ サーバの管理（Manage Jump Server）]
- [クレデンシャルのロック設定（Credential Lock Settings）]
- [ワークフローの管理（Manage WorkFlow）]

[すべてのルールのエクスポート（Export All Rules）]

すべてのルールをエクスポートするには、[データ収集設定（Data Collection Settings）] の [すべてのルールをエクスポート（Export All Rules）] オプションを使用します。[はい（Yes）] をクリックしてすべてのルールをエクスポートします。zip ファイルがダウンロードされます。

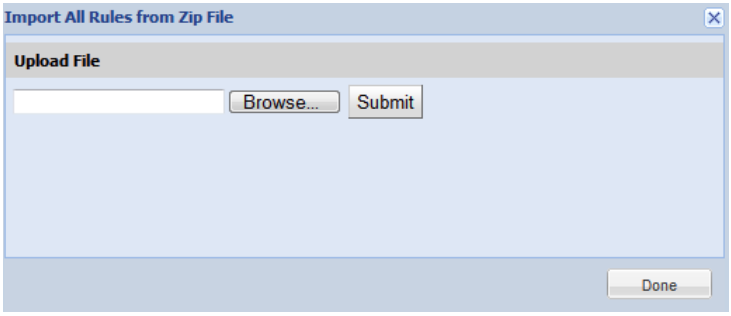
図 6-90　　[すべてのルールのエクスポート（Export All Rules）]



[すべてのルールのインポート（Import All Rules）]

すべてのルールをインポートするには、[データ収集設定（Data Collection Settings）] の [すべてのルールをインポート（Import All Rules）] オプションを使用します。表示されるダイアログボックスで、[参照（Browse）] ボタンをクリックして zip 形式のルール ファイルを選択し、[OK] をクリックしてすべてのルールのインポートを開始します。

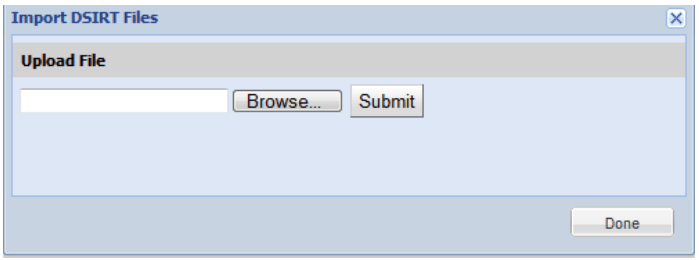
図 6-91　　[すべてのルールのインポート（Import All Rules）]



[DSIRT ファイルのインポート（Import DSIRT Files）]

[DSIRT ファイルのインポート（Import DSIRT Files）] では、DSIRT（Device Software Issues Reporting Tool）ファイルを選択してツールにインポートできます。

図 6-92　　[DSIRT ファイルのインポート（Import DSIRT Files）]

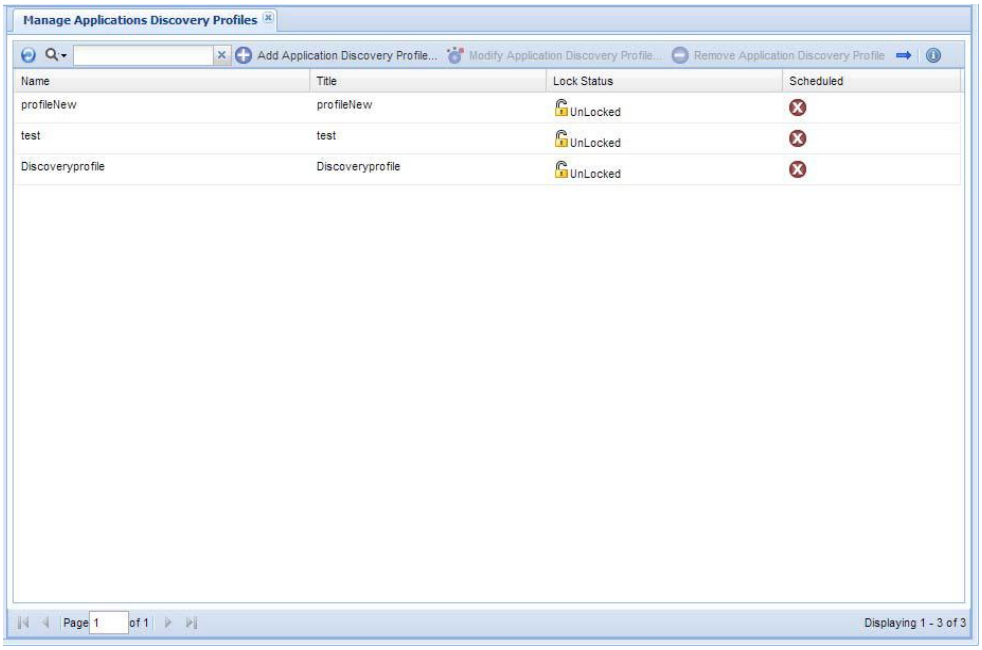


CSPC フローチャートに戻る

[アプリケーション検出プロファイルの管理（Manage Application Discovery Profiles）]

[アプリケーション検出プロファイルの管理（Manage Application Discovery Profiles）] では、アプリケーション検出プロファイルを追加または編集したり、データを収集するデバイスとデータの収集頻度を定義したりできます。アプリケーション検出では、デバイス（通常はコンピューティング サーバ）から情報を収集することにより、デバイスにインストールされているアプリケーションとデバイスで実行されているアプリケーションを検出します。

図 6-93　　[アプリケーション検出プロファイルの管理（Manage Application Discovery Profiles）]



新しいアプリケーション検出プロファイルを作成するには、[アプリケーション検出プロファイルの管理（Manage Application Discovery Profiles）] ウィンドウの [アプリケーション検出プロファイルの追加（Add Application Discovery Profiles）] アイコンをクリックします。

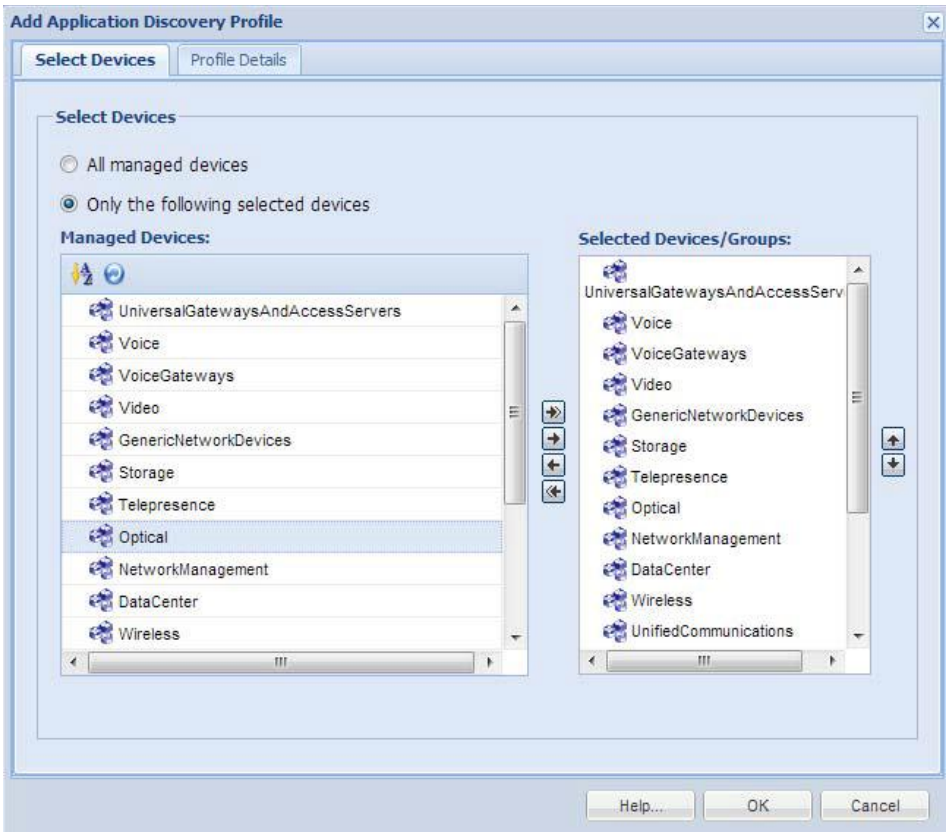
新しいアプリケーション検出プロファイルを追加するには、以下の手順に従います。

ステップ 1　デバイスを選択します。

ステップ 2　[プロファイルの詳細（Profile Details）] を選択します。

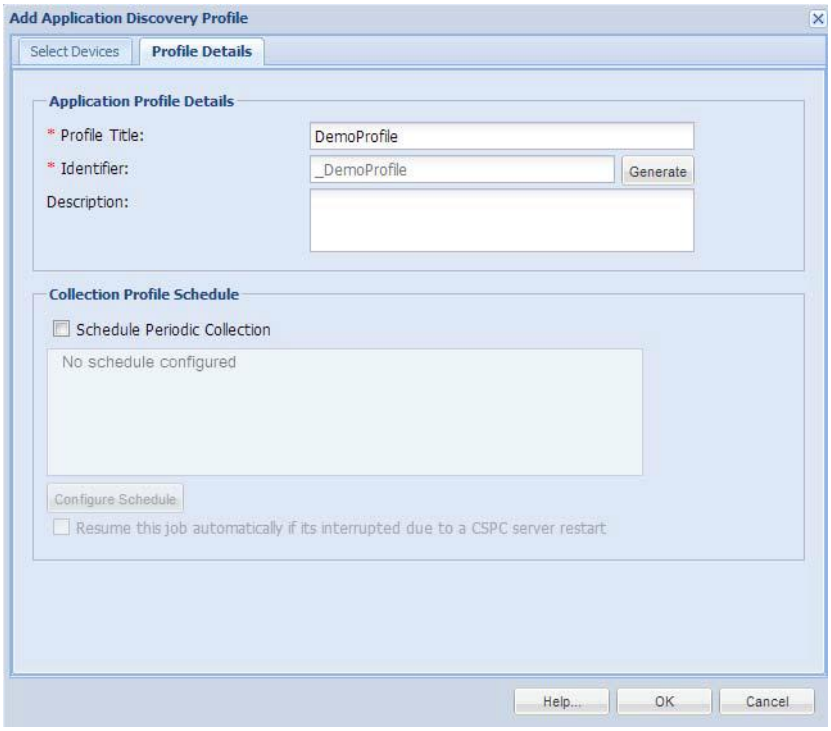
ステップ 3　[OK] をクリックします。

図 6-94　　アプリケーション検出プロファイルの [デバイスの選択（Select Devices]）



収集を開始するには、図 6-94 に示すように、データを収集するデバイスまたは一連のデバイスを選択します。
デバイスを選択したら、図 6-95 に示すように、データの収集頻度を定義するプロファイル オプションを選択します。

図 6-95　　[プロファイル詳細（Profile Details）]

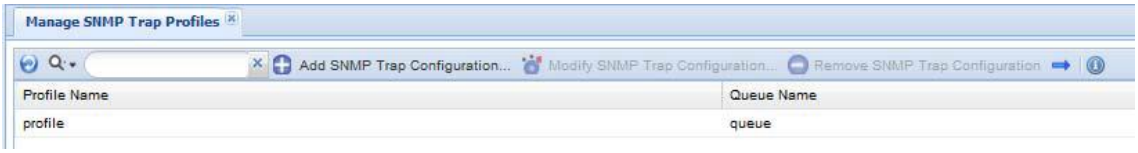


定期的に収集するジョブをスケジュールしている場合、[このジョブが CSPC サーバの再起動によって中断した場合は自動的に再開する（Resume this job automatically if it is interrupted due to a CSPC Server restart）] オプションを選択すると、CSPC サーバが再起動した場合でもジョブを再開できます。

[SNMP トラップ プロファイルの管理（Manage SNMP Trap Profiles）]

この画面では、新しい SNMP トラップ プロファイルを追加したり、設定したフィルタに応じてプロファイルを保存したりできます。1 つのトラップを複数のフィルタに適用できます。トラップを受信すると通知されます。

図 6-96　　[SNMP トラップ プロファイルの管理（Manage SNMP Trap Profiles）]



新しい SNMP トラップ プロファイルを作成するには、[SNMP トラップ プロファイルの管理（Manage SNMP Trap Profiles）] ウィンドウの [SNMP トラップ設定の追加（Add SNMP Trap Configuration）] アイコンをクリックします。

新しい SNMP トラップ プロファイルを追加するには、以下の手順に従います。

ステップ 1　[プロファイルの詳細（Profile Details）] を選択します。

a. [プロファイル名（Profile name）] と [キュー名（Queue name）] を入力します。キュー名は、アドオン

プロセスが特定の JMF キューにサブスクライブする必要がある JMF キューの名前です。

b. 矢印をクリックして 通知タイプを選択します。デフォルトでは、通知タイプは 2 つしかありません。
必要に応じて、XML 要求を実行して通知をいくつでも追加できます。「XML API」を参照してください。

ステップ 2　デバイスを選択します。

ステップ 3　[OK] をクリックします。

図 6-97　　[プロファイル詳細（Profile Details）]

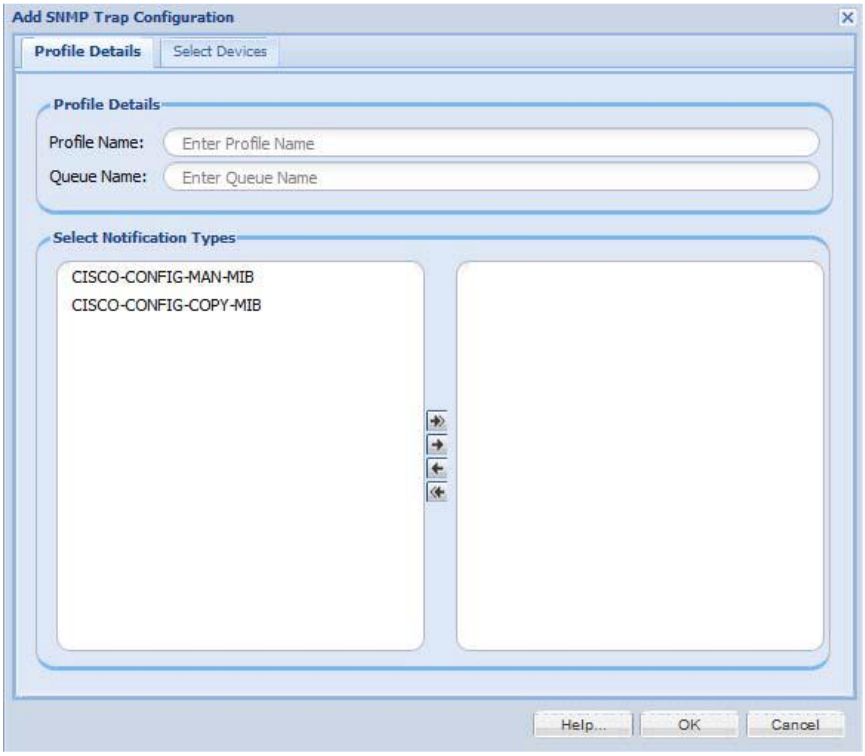
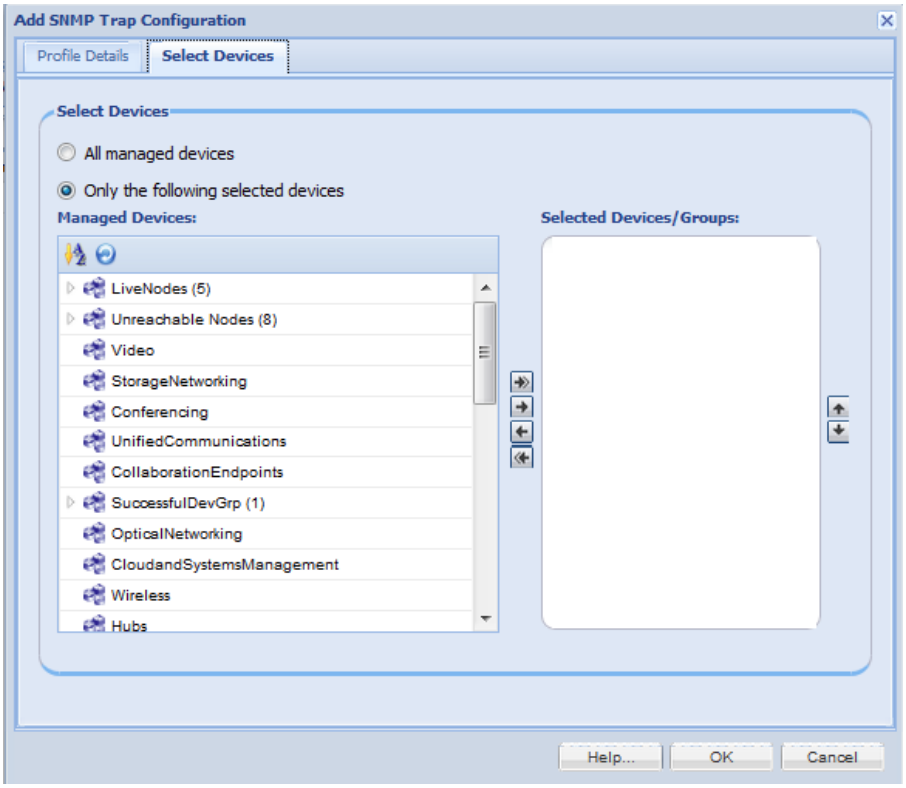


図 6-98 に示す [デバイスの選択（Select Devices）] タブでは、デバイスを特定のトラップ プロファイルにマッピングできます。

デバイスをトラップ プロファイルにマッピングするには、次の 2 つのオプションがあります。

- [すべての管理対象デバイス（All managed devices）]：すべてのデバイスを指定したトラップ プロファイルにマッピングします。
- [次の選択したデバイスのみ（Only the following selected devices）]：選択したデバイスのみを指定したトラップ プロファイルにマッピングします。

図 6-98　　[デバイスの選択（Select Devices）]



[ジャンプ サーバの管理（Manage Jump Server）]

ジャンプ サーバのサポートにより、CSPC はジャンプ サーバ経由で任意のデバイス CLI に接続できます。これにより、デバイス CLI への直接アクセスが防止されます。ジャンプ サーバの設定では、ジャンプ サーバの機能を設定できます。[ジャンプ サーバの管理（Manage Jump Server）] では、ジャンプ サーバを追加または編集できます。また、デバイスと接続タイプを管理したり、接続をテストしたりすることもできます。

図 6-99 [ジャンプ サーバの管理（Manage Jump Server）]

新しいジャンプ サーバを作成するには、[ジャンプ サーバの管理（Manage Jump Server）] ウィンドウの [ジャンプ サーバの追加（Add Jump Server）] アイコンをクリックします。

新しいジャンプ サーバを追加するには、以下の手順に従います。

ステップ 1　[プロファイルの詳細（Profile Details）] を選択します。

ステップ 2　デバイスを選択します。

ステップ 3　[OK] をクリックします。

図 6-100　[プロファイル詳細（Profile Details）]

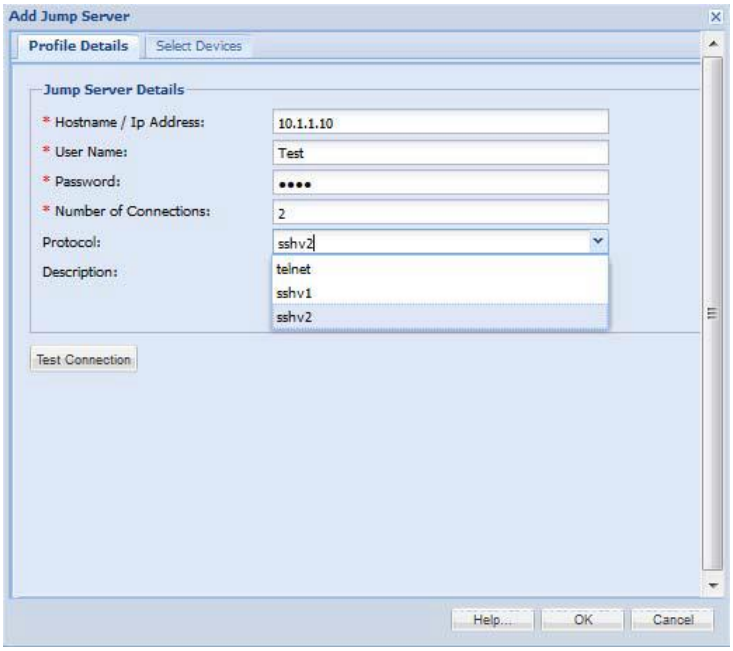


表 6-7　　ジャンプ サーバのパラメータ

フィールド名	説明
[ホスト名（Host Name）]	サーバの定義名。
[ユーザ名（User Name）]	ログイン ユーザ名。
[パスワード（Password）]	ログイン パスワード。
[コネクション数（Number of Connections）]	ジャンプ サーバへの接続の数。
[プロトコル（Protocol）]	使用されるプロトコルを選択します。
[説明（Description）]	サーバの説明。
[接続のテスト（Test Connection）]	ジャンプ サーバのクレデンシャルを確認します。

図 6-101 に示す [デバイスの選択（Select Devices）] タブでは、デバイスを特定のジャンプ サーバにマッピングできます。

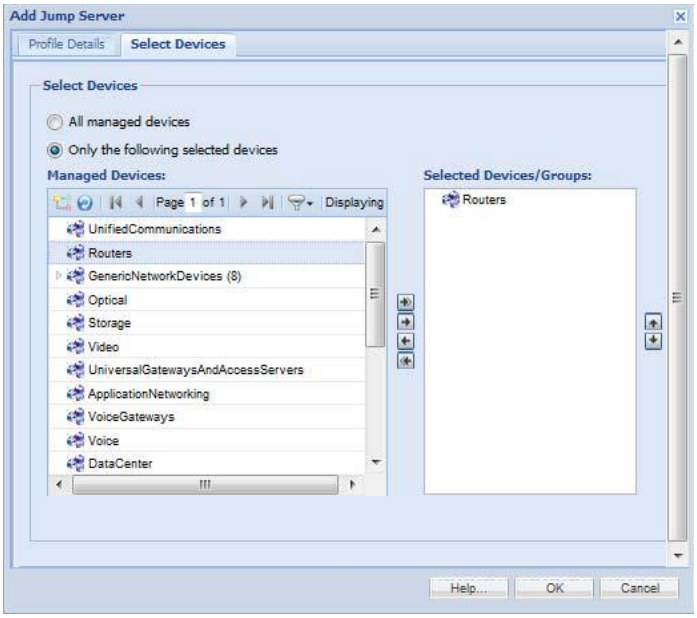
デバイスをジャンプ サーバにマッピングするには、次の 2 つのオプションがあります。

- [すべての管理対象デバイス（All managed devices）]: すべてのデバイスをジャンプ サーバにマッピングします。
- [次の選択したデバイスのみ（Only the following selected devices）]: 選択したデバイスのみを指定したジャンプ サーバにマッピングします。

[すべての管理対象デバイス（All managed devices）] オプションを選択すると、すべてのデバイスが指定したジャンプ サーバにマッピングされます。指定したサーバにすべてのデバイスをマッピングする場合は、その他のデバイスが別のジャンプ サーバにマッピングされていないことを確認する必要があります。

[次の選択したデバイスのみ（Only the following selected devices）] オプションを選択すると、選択したデバイスのみが指定したジャンプ サーバにマッピングされます。指定したジャンプ サーバにマッピングしようとしているデバイスの一部がすでに別のジャンプ サーバにマッピングされている場合、ジャンプ サーバの作成中にそれらのデバイスがマッピングから除外され、固有のデバイスがマッピングされます。

図 6-101　[デバイスの選択（Select Devices）]

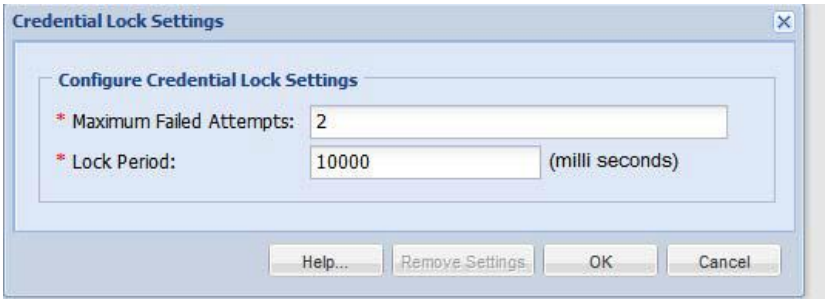


[クレデンシャルのロック設定（Credential Lock Settings）]

[クレデンシャルのロック設定（Credential Lock Settings）] では、特定のクレデンシャルの最大試行失敗回数を設定できます。クレデンシャルのロック期間を指定することもできます。ロック期間が設定されている場合、そのクレデンシャルはロック期間が終了するとロック解除されます。

ユーザが手動でクレデンシャルをロック解除するためのオプションもあります。このオプションにより、デバイスが特定のクレデンシャルに応答できなかった場合でも検出またはインベントリ処理を続行できます。

図 6-102　[クレデンシャルのロック設定（Credential Lock Settings）]



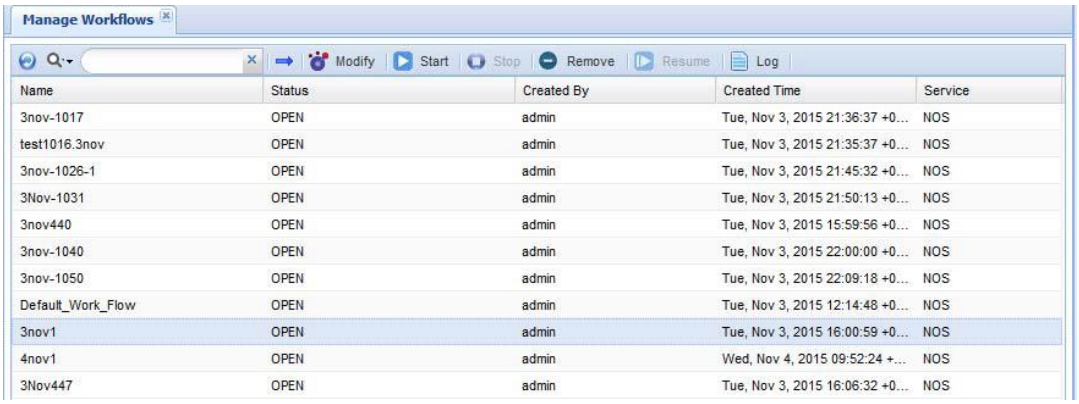
[設定の削除（Remove Settings）] ボタンを使用して、以前追加したロック設定を削除することもできます。

[ワークフローの管理（Manage WorkFlow）]

[ワークフローの管理（Manage WorkFlow）] で、ログの変更、開始、停止、削除、再開、表示ができます。ログには、[名前（Name）]、[ステータス（Status）]、[作成者（Created By）]、[作成日時（Created Time）]、[サービス（Service）] が表示されます。

- [変更（Modify）] をクリックすると、ワークフローを変更できます。
- [開始（Start）] をクリックすると、[オープン（open）] および [停止（stop）] ステータスのワークフローを開始できます。
- [停止（Stop）] をクリックすると、ワークフローが停止し、[再開（Resume）] をクリックすると、ワークフローが再開します。

図 6-103　　[ワークフローの管理（Manage WorkFlow）]



7

アプリケーション - 管理タスク

管理タスク

管理タスクを利用してツールにアクセスし、検出、プロファイルの収集、ジョブ ステータスの取得を実行できます。

この項では、[管理タスク（Management Tasks）] オプションの以下の項目について説明します。

- [デバイス タスク（Device Tasks）]
- [共通タスク（Common Tasks）]
- [ジョブの実行状況（Job Run Status）]
- ジョブ管理

[デバイス タスク（Device Tasks）]

[管理タスク（Management Tasks）] タブの [デバイス タスク（Device Tasks）] サブ タブを使用して、デバイス検出とデータ収集プロセスを設定します。

この項では、[デバイス タスク（Device Tasks）] オプションの以下の項目について説明します。

- [デバイスの検出（Discover Devices）]
- [デバイスを管理対象外にする（Unmanage Devices）]
- [デバイス アクセスの検証（Verify Device Access）]
- [デバイス プロンプトの収集（Device Prompt Collection）]

[デバイスの検出（Discover Devices）]

[デバイスの検出（Discover Devices）] 機能を使用すると、デバイスを検出して管理することができます。[デバイスの検出（Discover Devices）] をダブルクリックすると、[ネットワーク デバイスの検出および管理（Discover and Manage Network Devices）] ウィザードが表示されます。このウィザードでは、検出方法を選択し、デバイスの IP アドレスまたはホスト名を入力して、検出対象のデバイスを選択できます。

注 IP 範囲内のすべてのホストにクレデンシャルがさらされないようにするには：

- IP 範囲に基づく検出に信頼できるネットワークを使用します。
- 個別の IP アドレスを使用してデバイスを追加することを推奨します。

デバイスの検出には、次のような複数の方法があります。

- 既知のデバイス リスト
- プロトコル ベースの検出（CDP、OSPF、ARP、BGP など）。UC 検出ではサポートされません。

- IP アドレス範囲のスキャン
- 現在の管理対象デバイスの再検出

注　検出方法を選択せずに [次へ（Next）] ボタンをクリックすると、「少なくとも 1 つの検出方法を選択してください」というメッセージ ボックスが表示されます。

図 7-1　　既知の IP と再検出

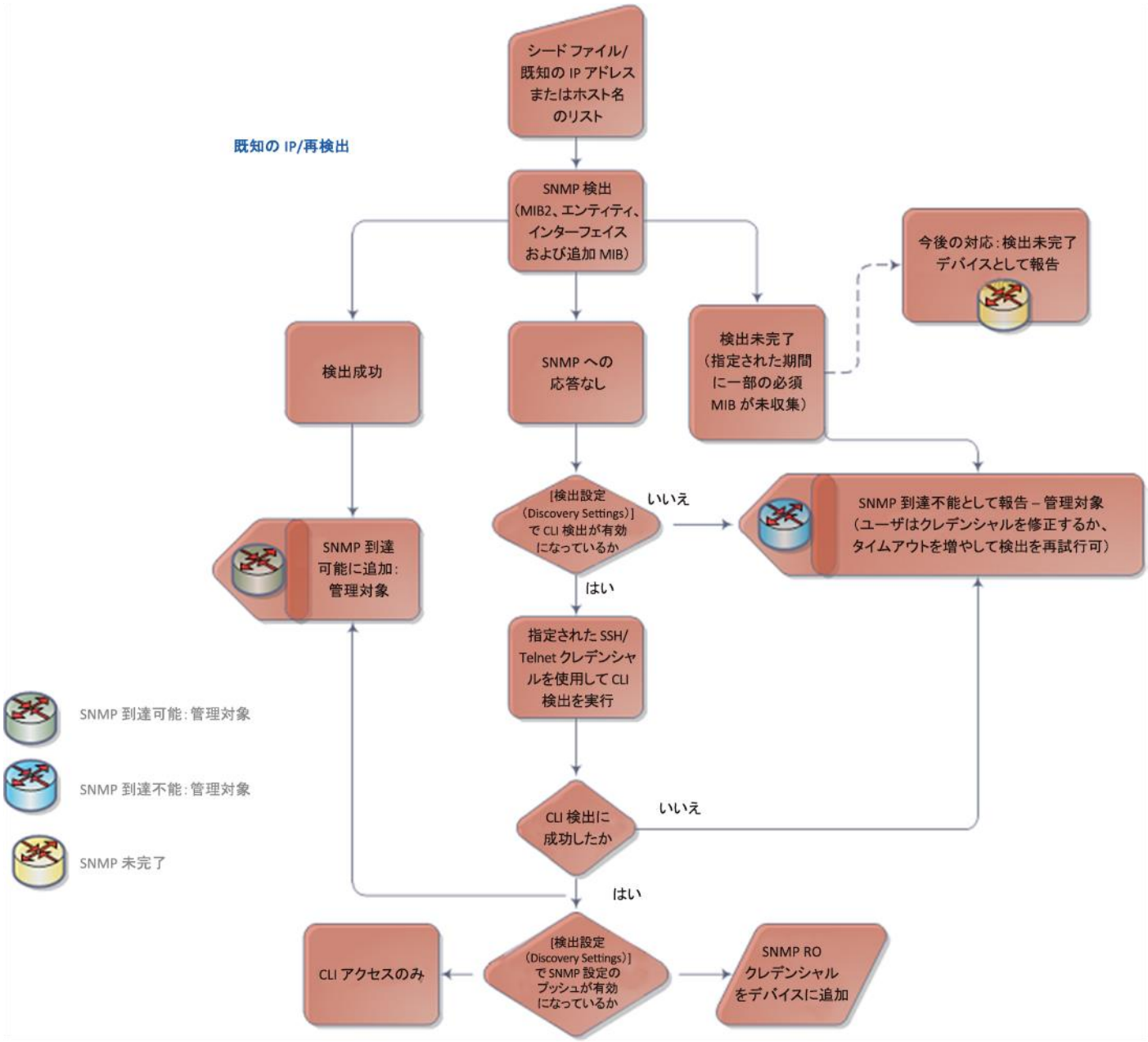


図 7-2　　範囲検出

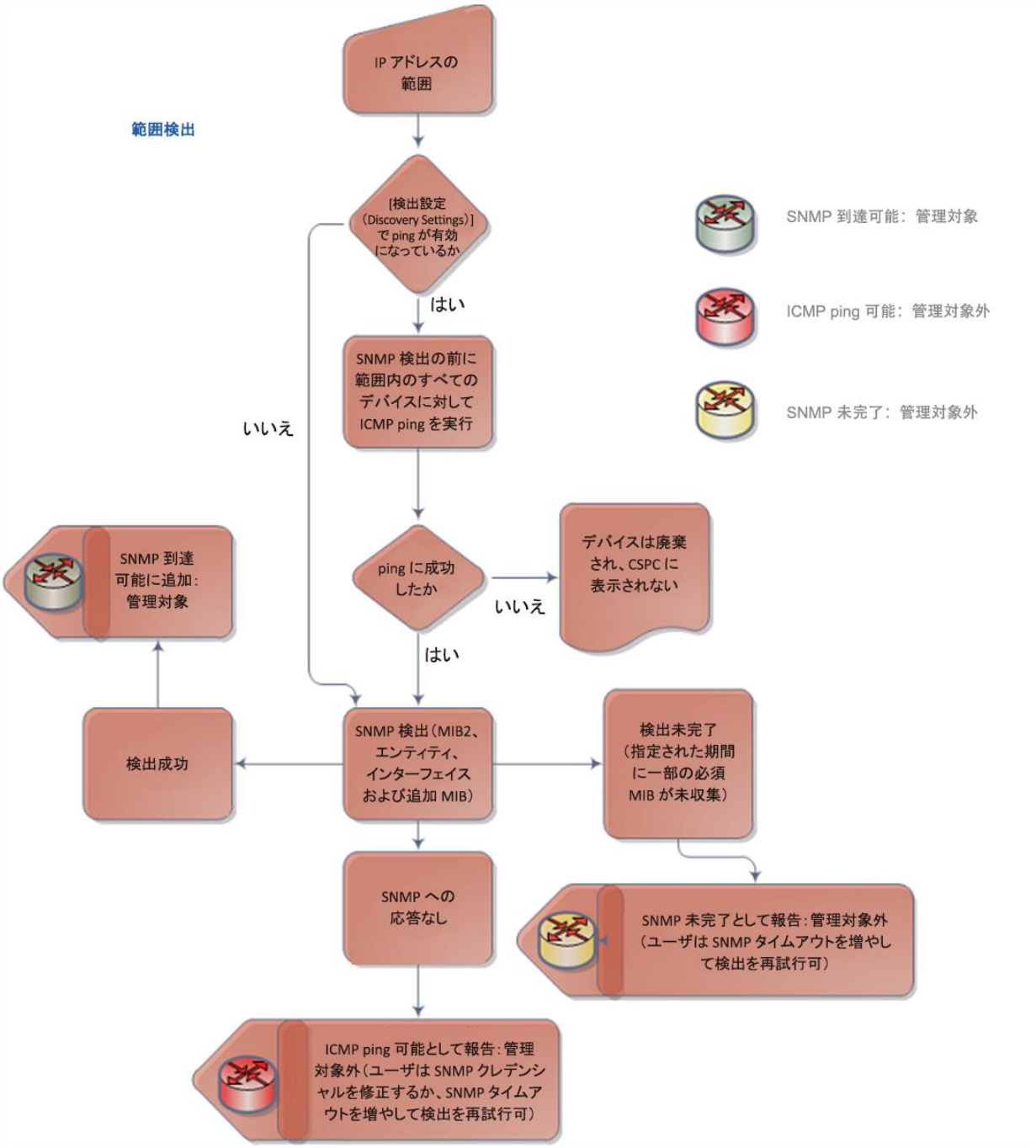

範囲検出
IP アドレスの範囲
[検出設定（Discovery Settings）] で ping が有効になっているか
はい
いいえ
SNMP 検出の前に範囲内のすべてのデバイスに対して ICMP ping を実行
ping に成功したか
いいえ
デバイスは廃棄され、CSPC に表示されない
はい
SNMP 到達可能に追加：管理対象
検出成功
SNMP 検出（MIB2、エンティティ、インターフェイスおよび追加 MIB）
検出未完了（指定された期間に一部の必須 MIB が未収集）
SNMP への応答なし
SNMP 未完了として報告：管理対象外（ユーザは SNMP タイムアウトを増やして検出を再試行可）
ICMP ping 可能として報告：管理対象外（ユーザは SNMP クレデンシャルを修正するか、SNMP タイムアウトを増やして検出を再試行可）
SNMP 到達可能：管理対象
ICMP ping 可能：管理対象外
SNMP 未完了：管理対象外

図 7-3　　シード IP と プロトコル ベースの検出

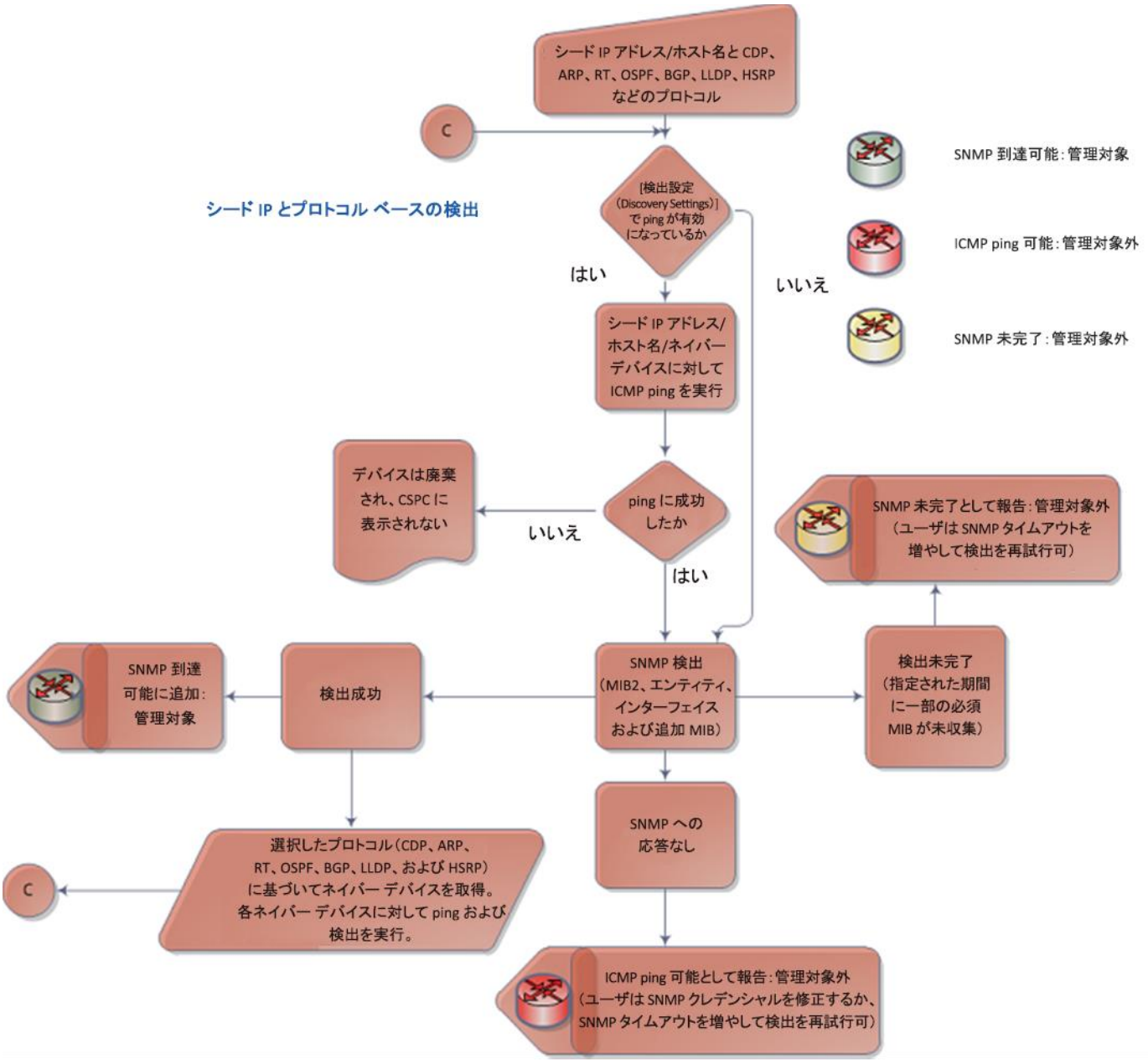
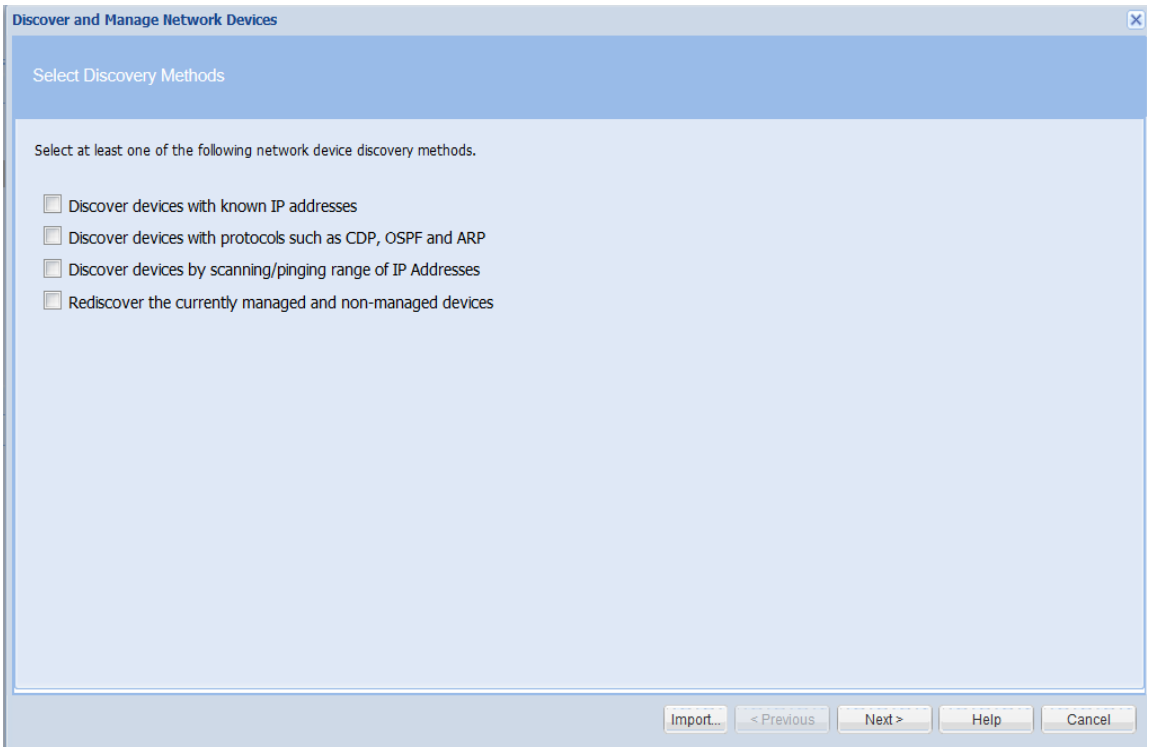


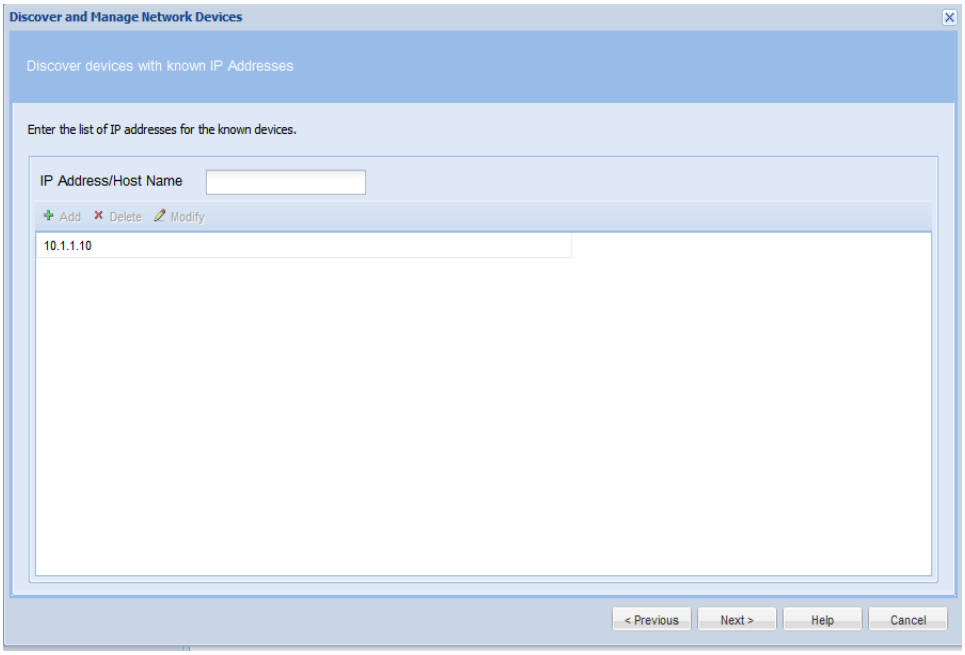
図 7-4　　[ネットワーク デバイスの検出および管理（Discover and Manage Network Devices）]



CiscoWorks DCR ファイルや Pari Discovery Options XML ファイルからデバイス リストをインポートすることもできます。

既知のデバイス リストでの検出の場合は、図 7-5 に示すように、IP アドレスまたはホスト名を入力します。

図 7-5　　[既知の IP アドレスを使用したデバイスの検出（Discover Devices using Known IP Addresses）]



CSPC では、SNMP クレデンシャルが間違っているか、デバイスで SNMP がサポートされていないために SNMP プロトコルを使用してデバイスに到達できない場合には、Nmap（ネットワーク マッパー）ベースの検出が使用されます。Nmap は、IP パケット データをこれまでにないやり方で使用して、ネットワー

ク上の利用可能なホスト、それらのホストが提供しているサービス、それらのホストで実行されているオペレーティング システム（および OS バージョン）などのさまざまな特性を判断します。

Nmap 検出は、CDP、OSPF、ARP などの検出オプションのいずれか、または IP アドレス範囲を使用してデバイスを検出するようにスケジュールする場合に有効にできます。[検出スケジュールのオプション（Discovery Options）] 画面の [Nmap] チェックボックスをオンにすると、指定した検出プロトコルによって検出された各 IP アドレス、または指定したアドレス範囲内の各 IP アドレスに対して NMAP 検出が実行されます。

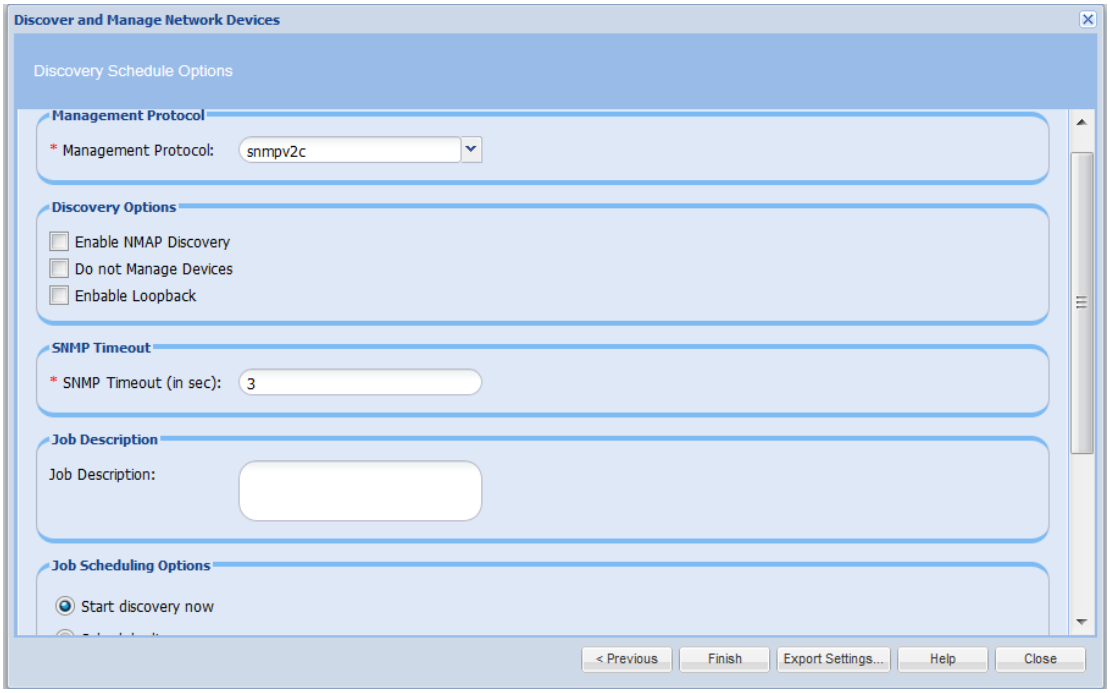
非 SNMP デバイス（SNMP エージェントが実行されていないデバイス）を検出する場合は、[NMAP 検出の有効化（Enable NMAP discovery）] オプションを選択します。検出された非 SNMP デバイスは「**非 SNMP デバイス**」レポートに表示されます。

[管理対象外デバイス（Do not Manage Devices）] オプションを選択した場合、デバイスは管理されませんが、検出されます。これらのデバイスは、検出されたデバイスと到達不能デバイスの *.csv* ファイルを含む zip ファイルとしてエクスポートできます。検出されたデバイスの *csv* ファイルは *CNC CSV* 形式です。このエクスポート オプションは、[検出ジョブ（Discovery Jobs）] にあります。

[ループバックの有効化（Enable Loopback）] オプションを選択した場合、検出ではループバック IP アドレスが優先され、ループバックが見つからない場合にはそれ以外のアドレスが使用されます。

必要に応じて、ジョブ固有の SNMP タイムアウト値を [SNMP タイムアウト（秒）（SNMP Timeout (in sec)）] フィールドに入力します。

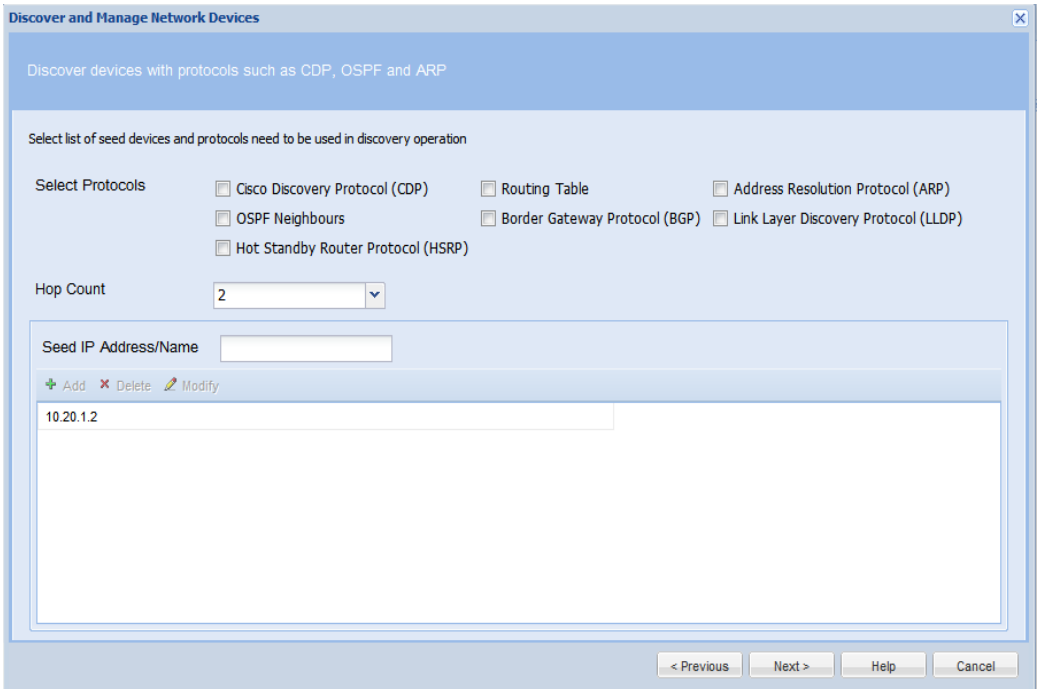
図 7-6　　Nmap Discovery



プロトコル ベースの検出の場合は、以下の情報を入力します。

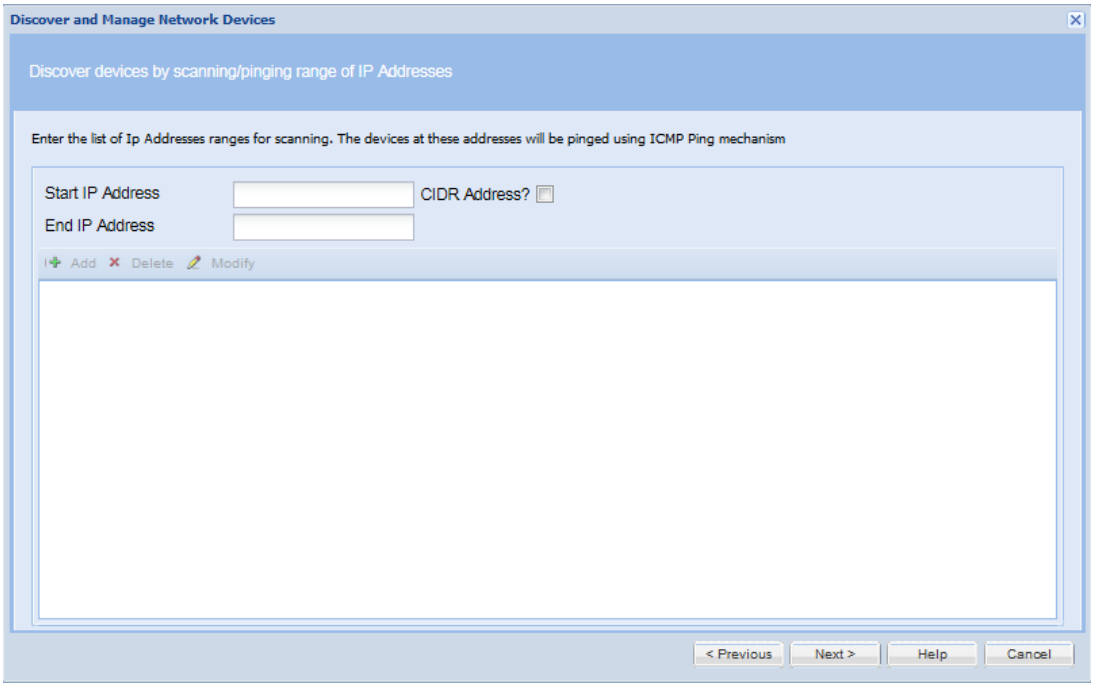
- プロトコル（CDP、ルーティング テーブル、ARP、OSPF ネイバー、BGP、HSRP、LLDP など）
- ホップ カウント（検出プロセスが通過するホップ数）
- シード IP アドレス（1 台または複数の初期シード デバイス）

図 7-7　　プロトコル ベースの検出



IP 範囲のスキャン ベースの検出の場合は、開始 IP アドレスと終了 IP アドレスを入力します。開始 IP アドレスは、「*IP アドレス/サブネット マスク（x.x.x.x/x）*」のように CIDR 形式で入力することもできます。この場合、終了アドレスは自動的に設定されます。CIDR アドレスは、開始 IP アドレスを入力する前に選択します。

図 7-8　　IP Scanning

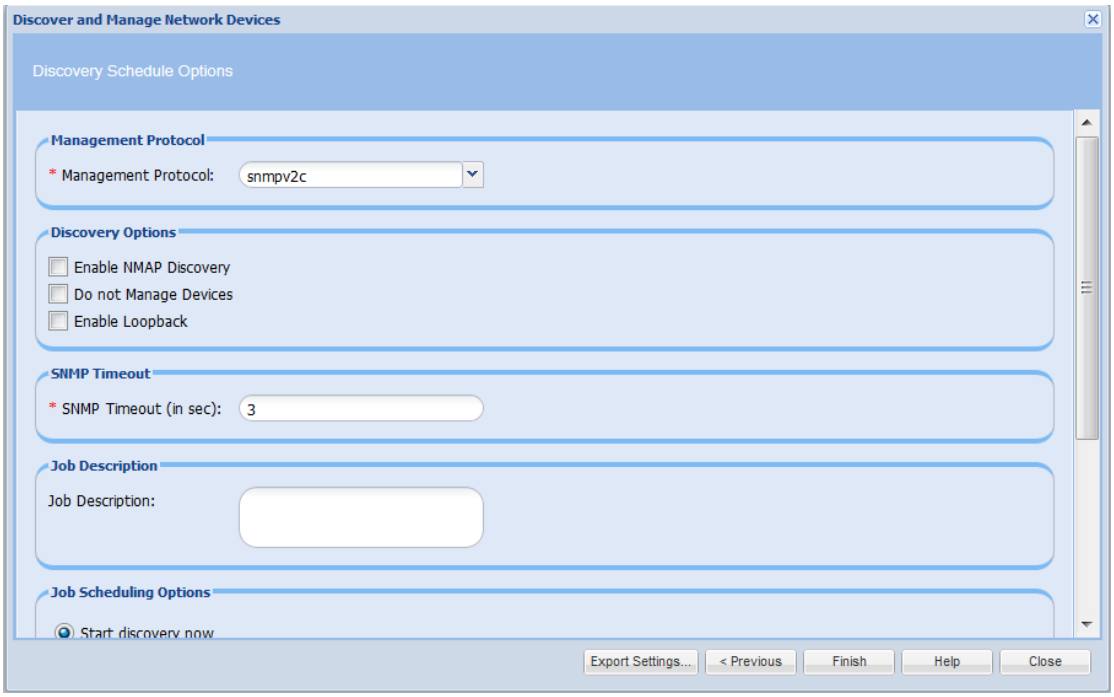


[現在の管理対象デバイスを再検出（Rediscover the currently managed devices）] オプションを選択すると、検出プロセスによって現在管理されているすべてのデバイスが再検出されます。

検出プロセスに使用する管理プロトコルを選択します。現在選択可能なオプションは、SNMPv1、SNMPv2、または SNMPv3 です。

検出のタイプを指定したら、デバイスの検出を実行できます。検出プロセスのスケジュールは、すぐに設定することも、後で設定することもできます。

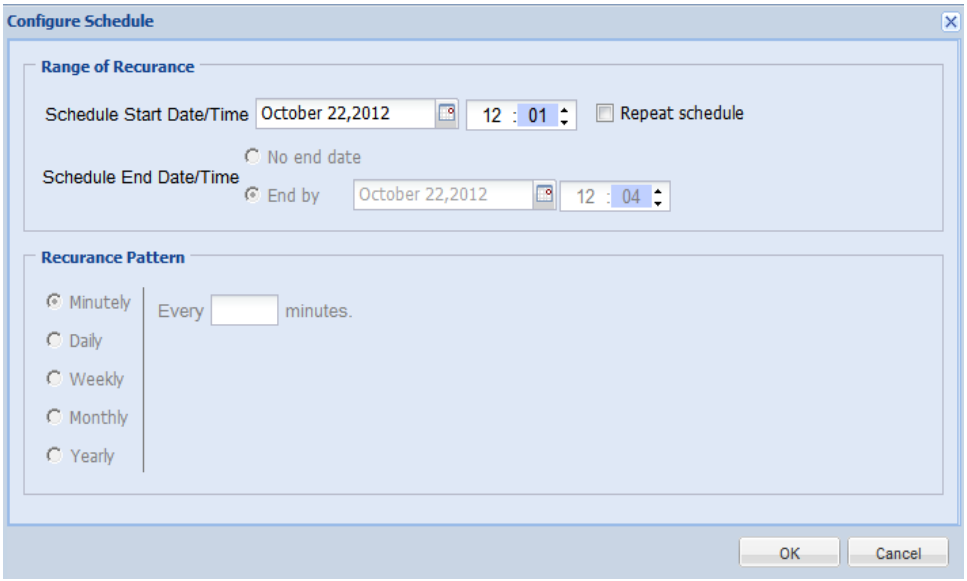
図 7-9　　Discovery Schedule Options



検出を後で実行するようにスケジュールするには、[検出のスケジュール（Schedule Discovery）] オプションを選択し、[スケジュールの設定（Configure Schedule）] ボタンをクリックします。

図 7-10 に示すように、スケジュールの開始日時と終了日時を設定するか、定期的なパターンとして [毎分（Minutely）]、[毎日（Daily）]、[毎週（Weekly）]、[毎月（Monthly）]、または [年に 1 回（Yearly）] を選択することができます。

図 7-10　　[スケジュールの設定（Configure Schedule）]

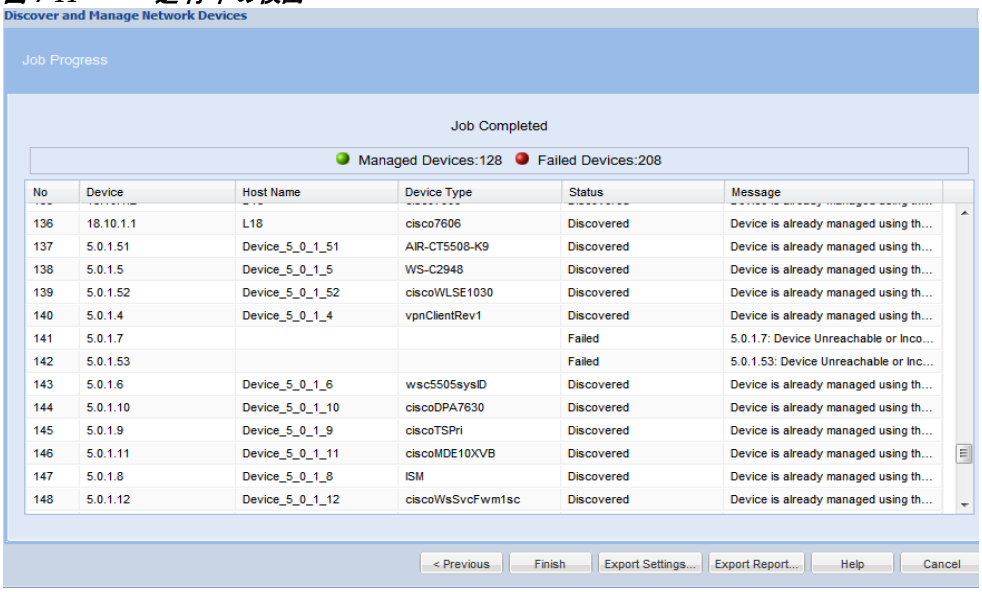


*検出および管理*の操作が終了すると、選択したデバイスの [IP アドレス（IP Address）]、[ホスト名（Host Name）]、[デバイス タイプ（Device Type）]、[ステータス（Status）]（デバイスが管理対象か対象でないかを示す）、および [メッセージ（Message）] を含む結果が表示されます。検出プロセスは、画面を閉じてバックグラウンドで実行することができます。バックグラウンド処理の結果を確認するには、[ジョブ ログ レポート（Job Log Reports）] > [検出ジョブ（Discovery Jobs）] を選択します。

古い検出ジョブのクローンを作成して、新しい検出ジョブとして使用することもできます。検出処理のクローン作成の詳細については、[ジョブ ログ レポート（Job Log Reports）] > [検出ジョブ（Discovery Jobs）] を選択して確認してください。

検出ジョブ レポートでは、検出されたジョブを右クリックして [このジョブのクローンを作成して新規検出を作成（Create new discovery by cloning this job）] を選択することで新しい検出ジョブを作成できます。

図 7-11　　進行中の検出



検出の設定は XML ファイルにエクスポートでき、検出されたデバイスのレポートをエクスポートすること

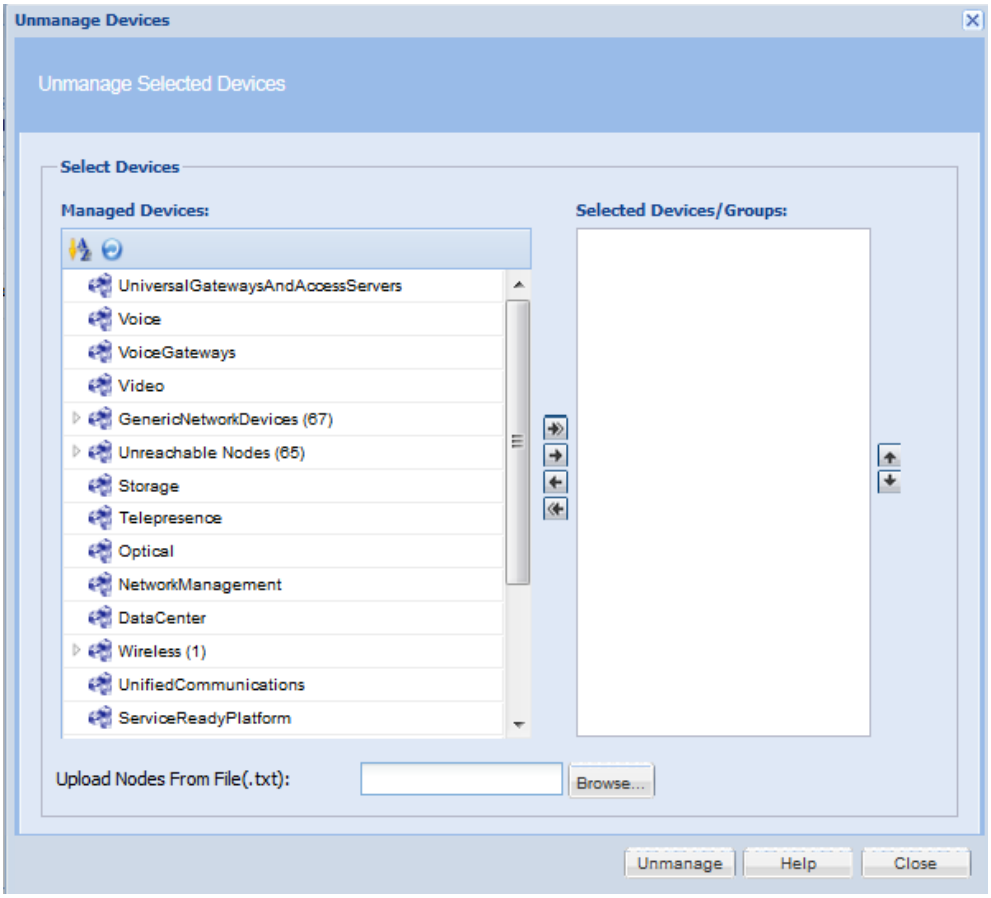
もできます。

CSPC フローチャートに戻る

[デバイスを管理対象外にする（Unmanage Devices）]

[デバイスを管理対象外にする（Unmanage Devices）] をダブルクリックすると、新しいウィンドウが開きます。このウィンドウには、すでに管理対象であるデバイスの一覧が表示されていて、管理対象外にするデバイスを選択できます。デバイスまたはグループを選択すると、選択したデバイスまたはグループがウィンドウの右側に表示されます。次に、[管理対象外にする（Unmanage）] をクリックして、次に示すように、選択したデバイスまたはグループを削除します。*.txt* ファイルからノードのリストを参照してアップロードすることもできます。

図 7-12　　[デバイスを管理対象外にする（Unmanage Devices）]



この操作を終了すると、CSPC は、管理対象外デバイスと対応するすべてのデータ（収集プロファイルデータなど）をそのデータベースから削除します。

[デバイス アクセスの検証（Verify Device Access）]

[デバイス アクセスの検証（Device Access Verification）] は、次に示すように、あるデバイスに特定のクレデンシャルを使用してアクセスできるかどうかを確認する場合に使用します。

デバイス アクセスの検証を実行するには、以下の手順に従います。

ステップ 1 データ アクセスを検証する必要があるデバイスを選択します。*.txt* ファイルからノードのリストを参照してアップロードすることもできます。

ステップ 2 検証に使用するプロトコルを選択します。すべてのプロトコルが失敗した場合は、ICMP を使用してデバイスの到達可能性を確認できます。

ステップ 3 今すぐに検証処理を開始するか、後で開始するようにスケジュールします。

図 7-13　　[デバイス アクセスの検証（Device Access Verification）] - [デバイスの選択（Device Selection）]

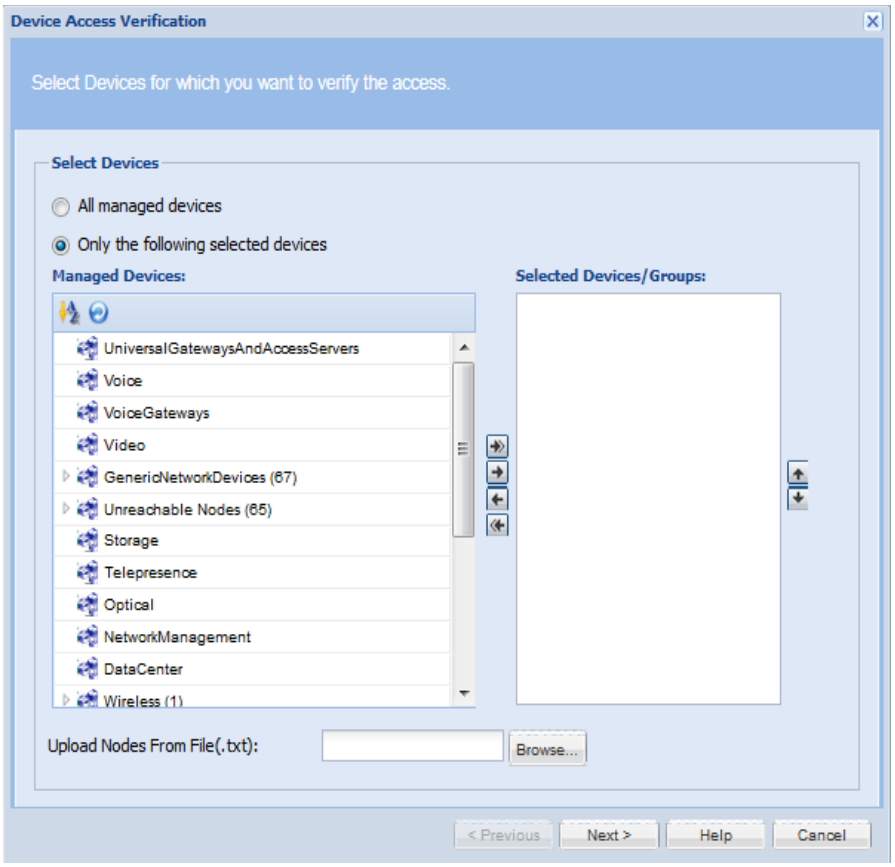
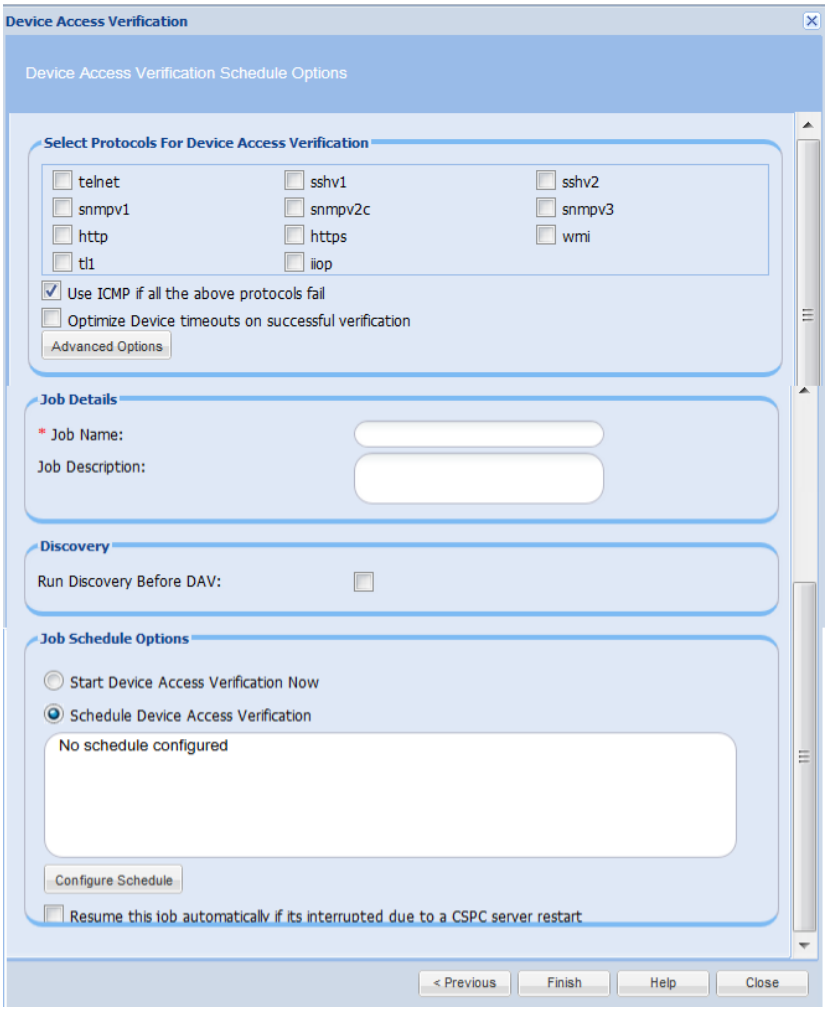


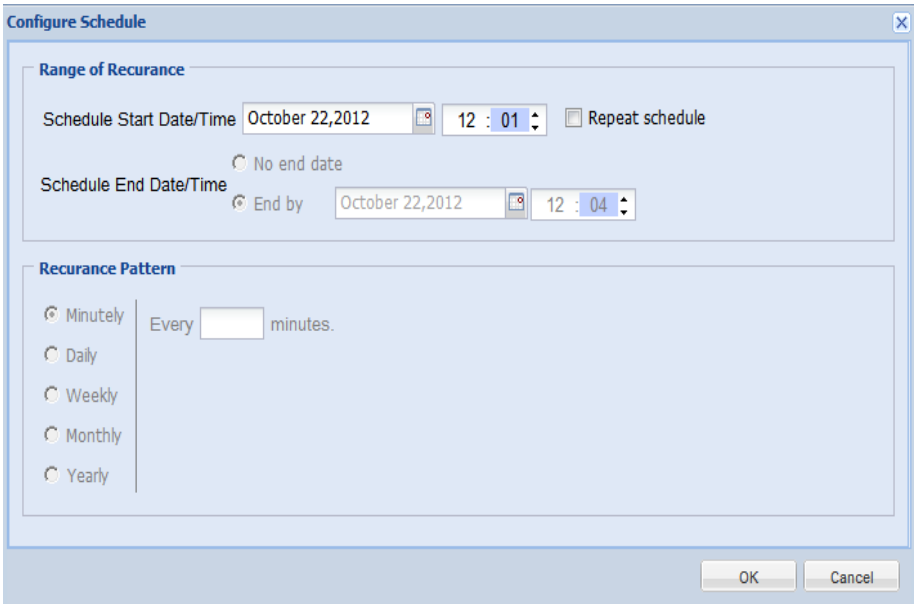
図 7-14　　Device Access Verification - Protocol Selection



[DAV の前に検出を実行（Run Discovery before DAV）] オプションを使用して、DAV を実行する前にデバイスを再検出します。

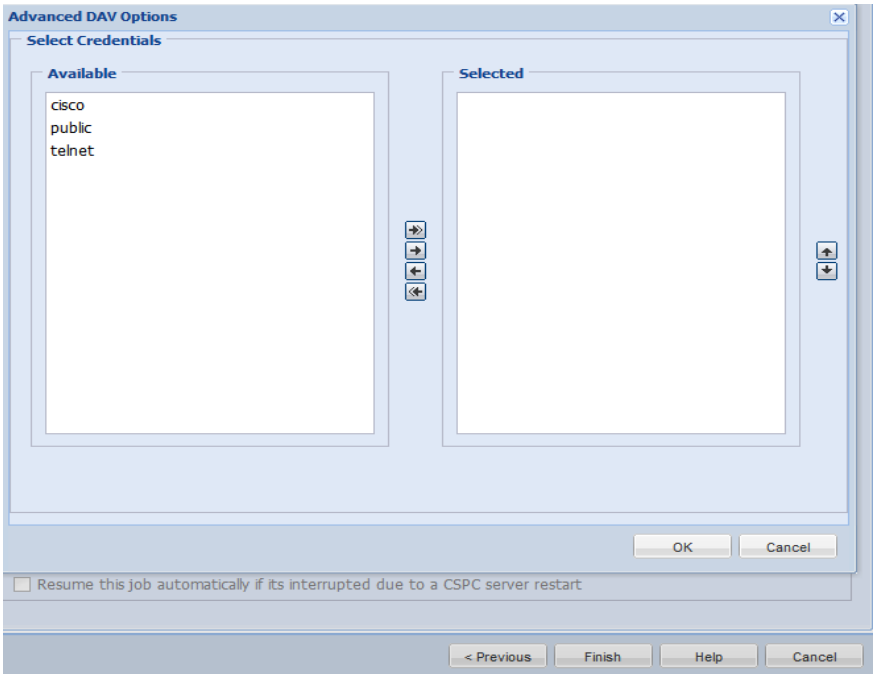
デバイス アクセスの検証を後で実行するようにスケジュールするには、[デバイス アクセスの検証のスケジュール（Schedule Device Access Verification）] オプションを選択し、[スケジュールの設定（Configure Schedule）] ボタンをクリックします。図 7-15 に示すように、スケジュールの開始日時と終了日時を設定するか、定期的なパターンとして [分単位（Minutely）]、[毎日（Daily）]、[毎週（Weekly）]、[毎月（Monthly）]、または [年に 1 回（Yearly）] を選択することができます。

図 7-15　　[スケジュールの設定（Configure Schedule）]



[詳細オプション（Advanced Options）] ボタンをクリックすると、図 7-16 に示すように DAV の実行に使用するクレデンシャルを選択できます。

図 7-16　　[DAV の詳細オプション（Advanced DAV Options）]



ジョブが起動すると、次に示すように、特定のデバイスに対して成功および失敗したクレデンシャルとプロトコルを確認できます。

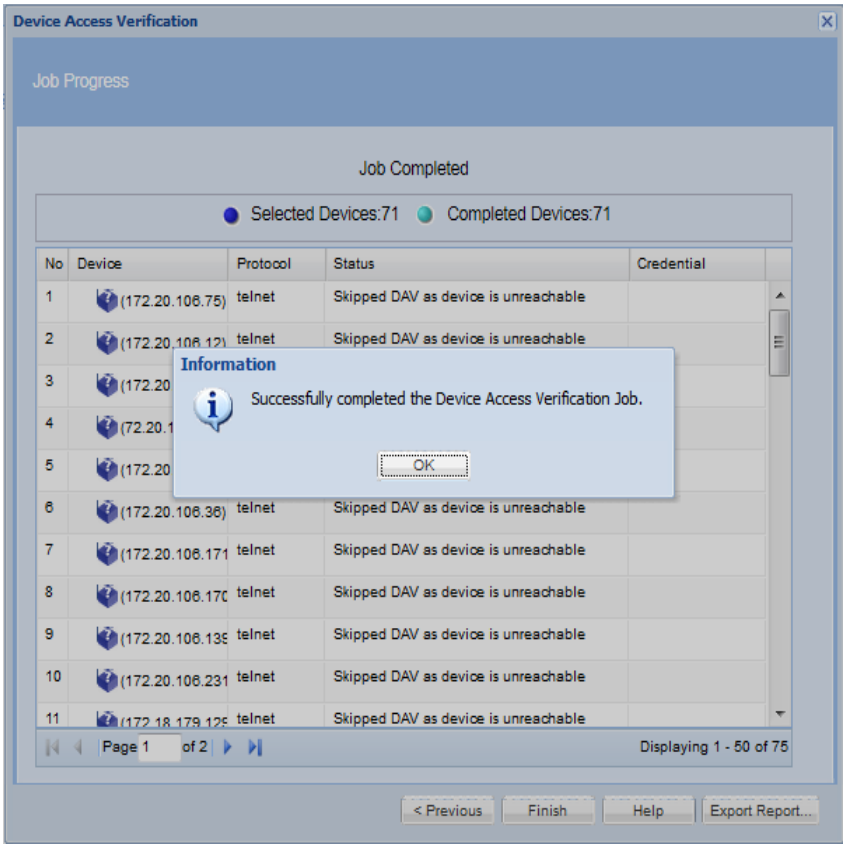
検証成功時にデバイス タイムアウトを最適化するためのオプションもあります。このオプションは、SNMP にのみ適用できます。このオプションを有効にすると、特定のデバイスのタイムアウトが自動的に計算されて、[詳細設定（Advanced Settings）] の [グローバル タイムアウト（Global Timeouts）] に追加されます。

デバイス アクセスの検証ジョブを後で実行するようスケジュールされている場合、[このジョブが CSPC サーバの再起動によって中断した場合は自動的に再開する（Resume this job automatically if it is interrupted due to a CSPC Server restart）] オプションが選択可能になります。デバイス アクセスの検証ジョブを実行中に、CSPC が何らかの理由で再起動した場合、CSPC は再起動後に該当ジョブを再開します。

デフォルトでは、CSPC はデバイスに ping を送信し、そのデバイスが追加の ping で応答するかどうかを確認します。

選択したすべてのルーティング プロトコルが DAV に失敗した場合、デフォルトでは、デバイスが応答するかどうかを確認するために追加の ping 機能がトリガーされます。

図 7-17　　[デバイス アクセスの検証（Device Access Verification）] - 結果



CSPC フローチャートに戻る

[デバイス プロンプトの収集（Device Prompt Collection）]

[デバイス プロンプトの収集（Device Prompt Collection）] オプションを使用して、選択したデバイスのデバイス プロンプトと DNS 名を収集できます。

デバイス プロンプトの収集を実行するには、以下の手順に従います。

ステップ 1 デバイス プロンプトを収集する必要があるデバイスを選択します。

ステップ 2 収集ジョブを作成します。

ステップ 3 今すぐにジョブを開始するか、後で開始するようにスケジュールします。

図 7-18　　プロンプトを収集するデバイスの選択

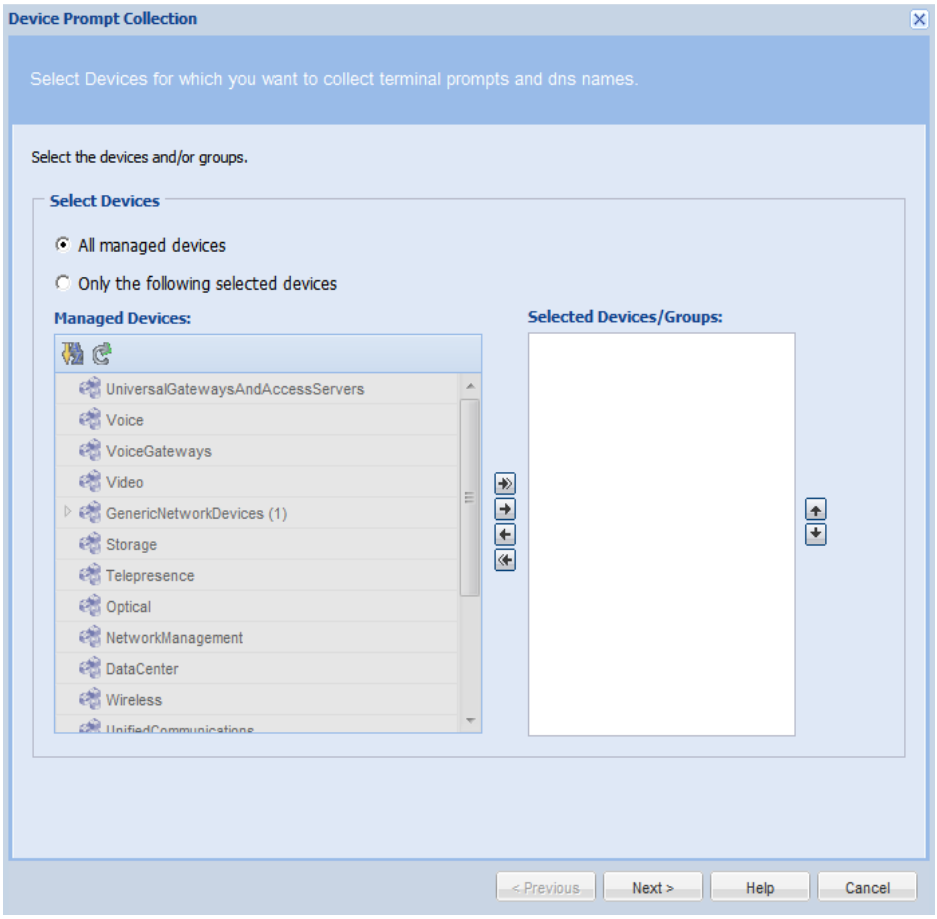
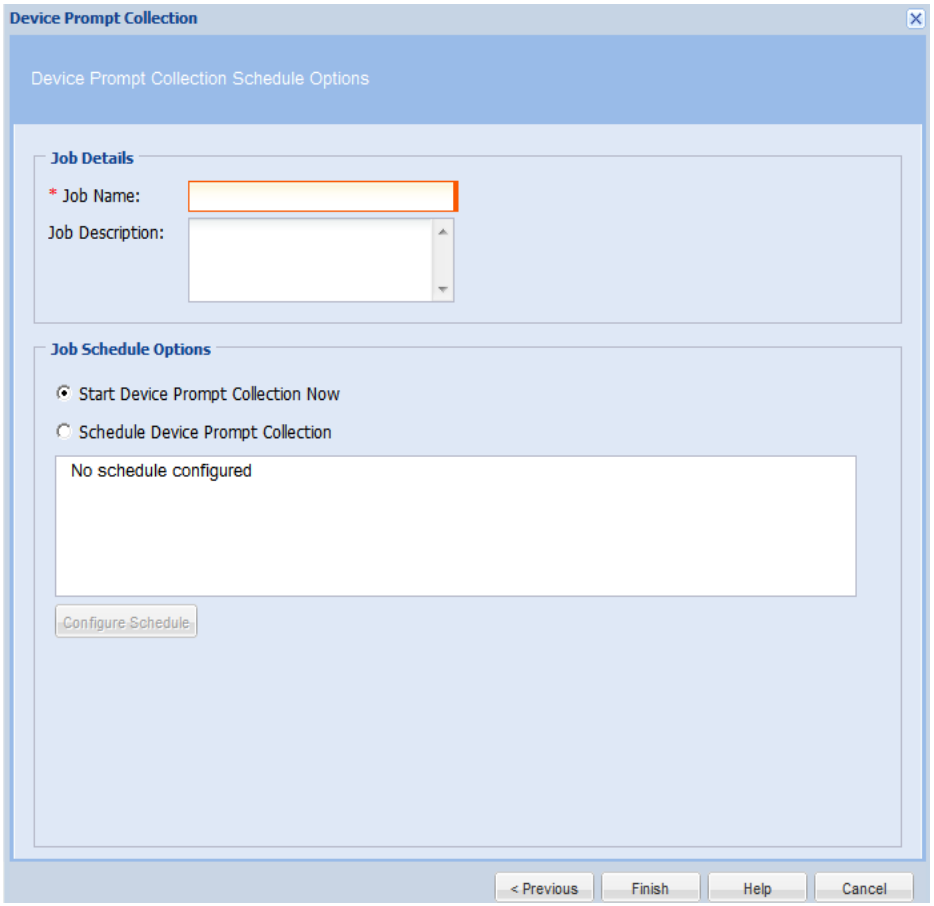
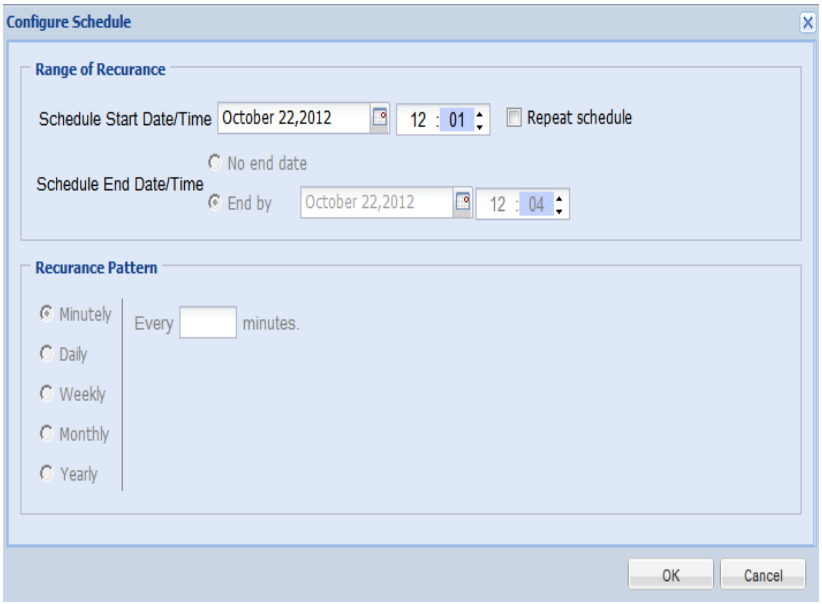


図 7-19　　プロンプト収集ジョブの作成



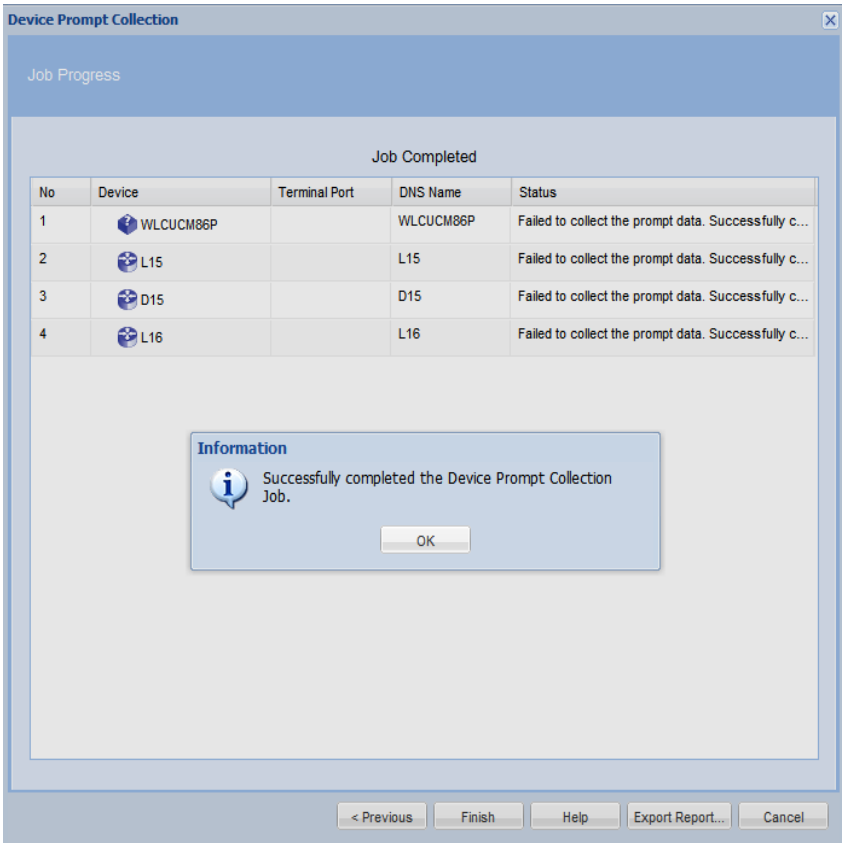
デバイス プロンプトの収集を後で実行するようにスケジュールするには、[デバイス プロンプトの収集のスケジュール（Schedule Device Prompt Collection）] オプションを選択し、[スケジュールの設定（Configure Schedule）] ボタンをクリックします。図 7-20 に示すように、スケジュールの開始日時と終了日時を設定するか、定期的なパターンとして [分単位（Minutely）]、[毎日（Daily）]、[毎週（Weekly）]、[毎月（Monthly）]、または [年に 1 回（Yearly）] を選択することができます。

図 7-20　　[スケジュールの設定（Configure Schedule）]



ジョブが起動すると、図 7-21 に示すように、特定のデバイスに対して成功および失敗した収集を確認できます。

図 7-21　　実行中のプロンプト収集ジョブ



[共通タスク（Common Tasks）]

[管理タスク（Management Tasks）] タブの [共通タスク（Common Tasks）] サブ タブでは、選択した収集プロファイルを実行できます。収集プロファイルについては、「収集ルール」と「その他のルール」の章で説明しています。

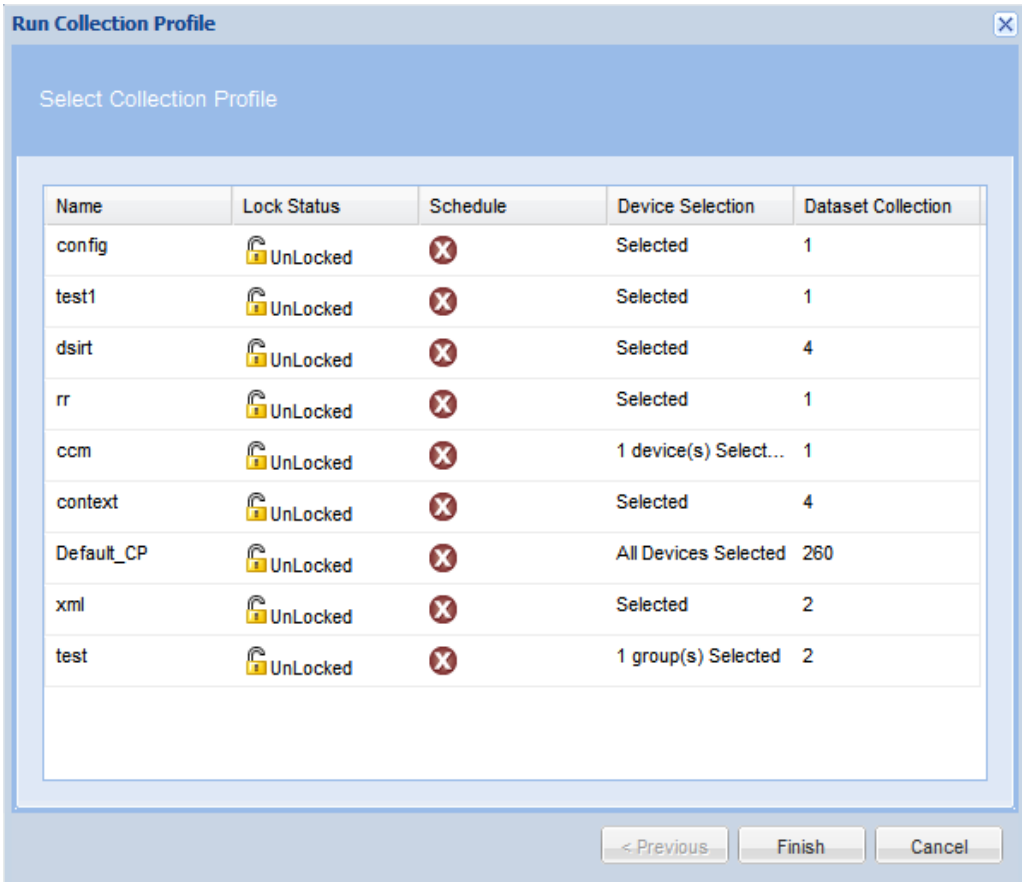
この項では、[データ収集（Data Collection）] オプションの以下の項目について説明します。

- [データの収集（Collect Data）]
- [データのアップロード（Upload Data）]
- [アドホック データ収集（Adhoc Data Collection）]
- [アプリケーション データの収集（Collect Application Data）]

[データの収集（Collect Data）]

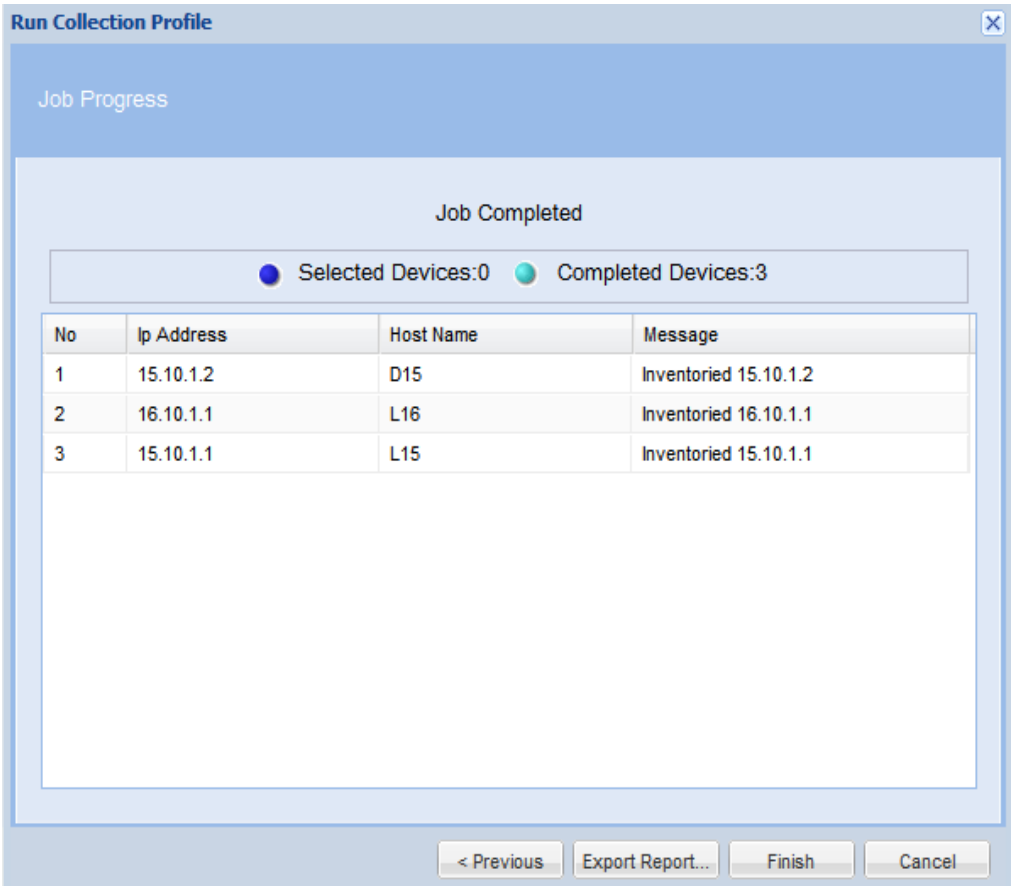
定義済みの収集プロファイルの一覧から任意の収集プロファイルを選択し、必要に応じて実行できます。プロファイルを実行するには、プロファイルを選択して [完了（Finish）] ボタンをクリックします。

図 7-22　　[収集プロファイルの選択（Select the Collection Profile）]



ジョブを起動すると、次に示すように、デバイス名、IP アドレス、および成功または失敗を含む結果が表示されます。

図 7-23　　データ収集プロファイルの実行結果



[データのアップロード（Upload Data）]

[アップロード プロファイルの実行（Run Upload Profile）] 画面には、[アップロード プロファイルの管理（Manage Upload Profiles）] で作成したプロファイルの一覧が表示されます。アップロード プロファイルを開始するには、[アップロード プロファイルの実行（Run Upload Profile）] 画面からプロファイルを選択して [完了（Finish）] をクリックします。

図 7-24　　[アップロード プロファイルの実行（Run Upload Profile）]

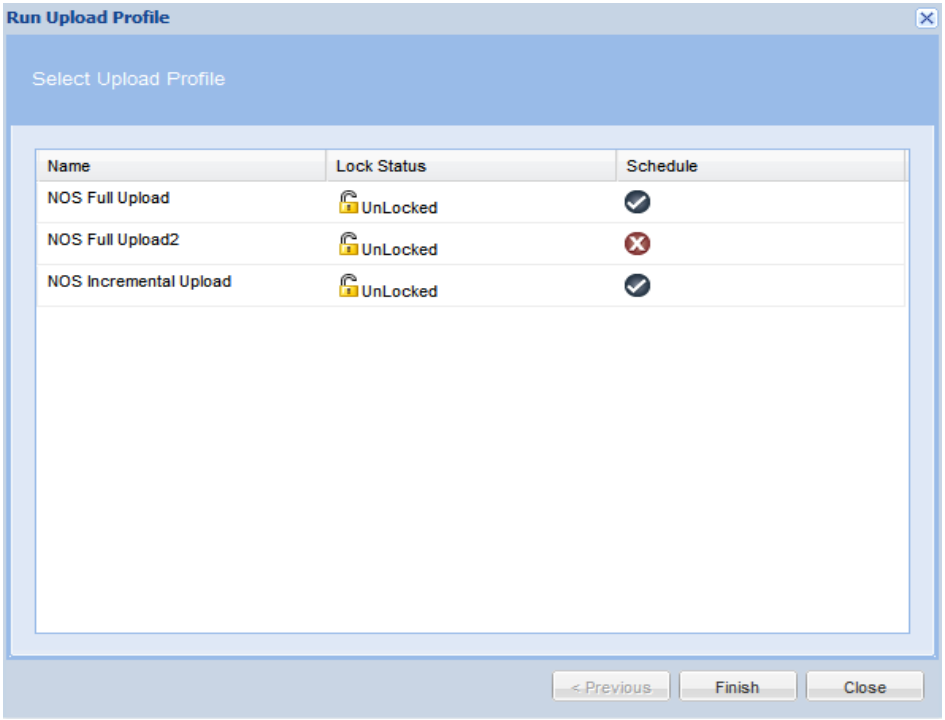
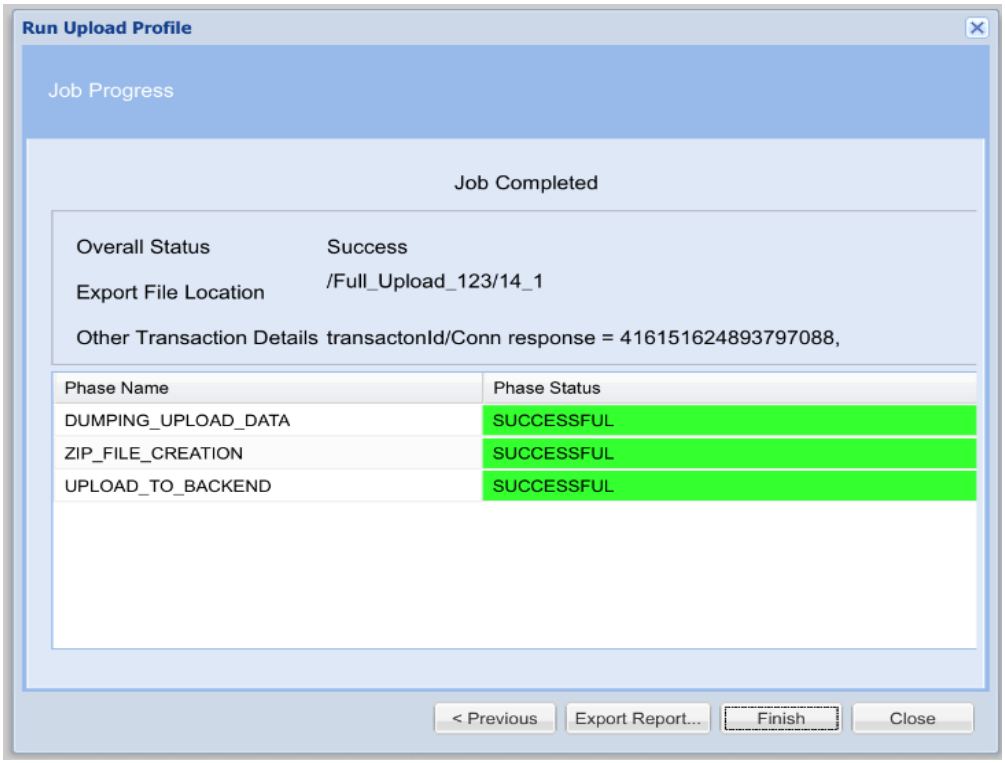


図 7-25 に示すように、アップロード プロファイルのステータスを示す [ジョブの進捗状況（Job Progress）] 画面が表示されます。

図 7-25　　ジョブ実行結果



アップロードが実行中のジョブはオレンジ色、アップロードに成功したジョブは緑色、アップロードに失敗したジョブは赤色でそれぞれ表示されます。

これらのフェーズ ステータスのいずれかにエラーが発生した場合は、アップロード プロファイルを再実行する必要があります。

CSPC フローチャートに戻る

[アドホック データ収集（Adhoc Data Collection）]

データセットに基づいてデータを収集するように設定したいデバイスがある場合は、アドホック収集プロファイルを作成できます。

一般に、収集プロファイルはデバイス セットに関連付けられます。つまり、収集プロファイルを実行する際には、
この収集プロファイル定義に関連付けられているデバイスに対して収集が実行されます。

プロファイル定義に存在するデバイス セット以外のデバイス セットに対して収集プロファイルを実行したい場合は、アドホック収集プロファイルを使用してこれを実現できます。

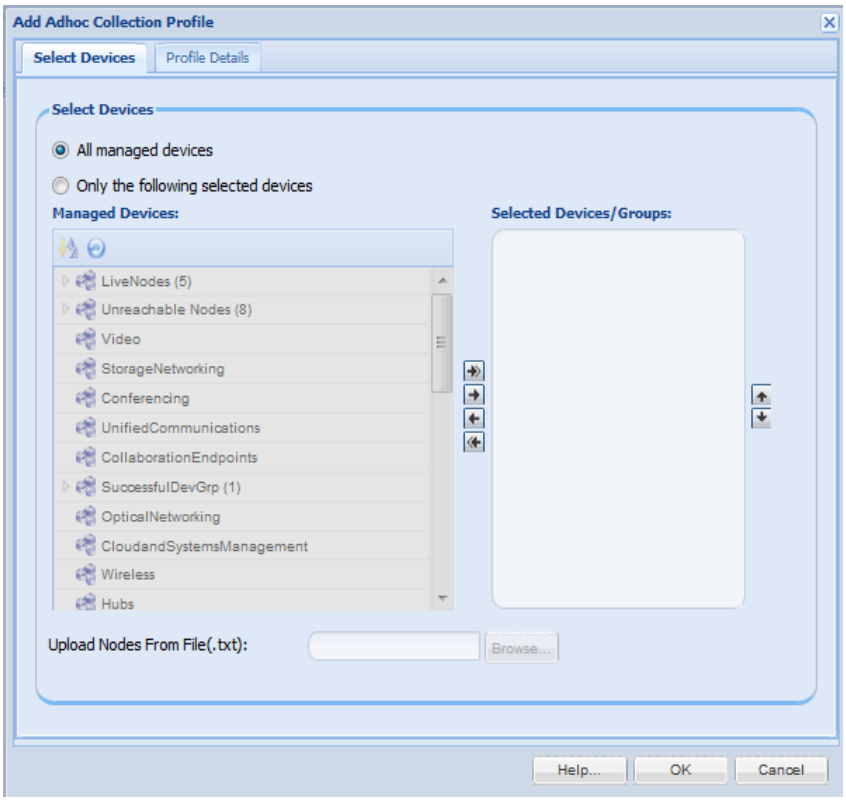
アドホック収集プロファイルを作成する場合は、以下を選択します。

- 基本収集プロファイル
- デバイスの詳細
- スケジュール情報

アドホック収集プロファイルは、指定された基本収集プロファイルから収集の詳細（データセットなど）を検証します。各デバイスの詳細とスケジュール情報以外のすべての詳細を継承します。

[アドホック データ収集プロファイルの作成（Create Adhoc Data Collection Profiles）] をクリックすると、図 7-26 に示す画面が表示されます。

図 7-26　　アドホック収集の [デバイスの選択（Select Devices）]

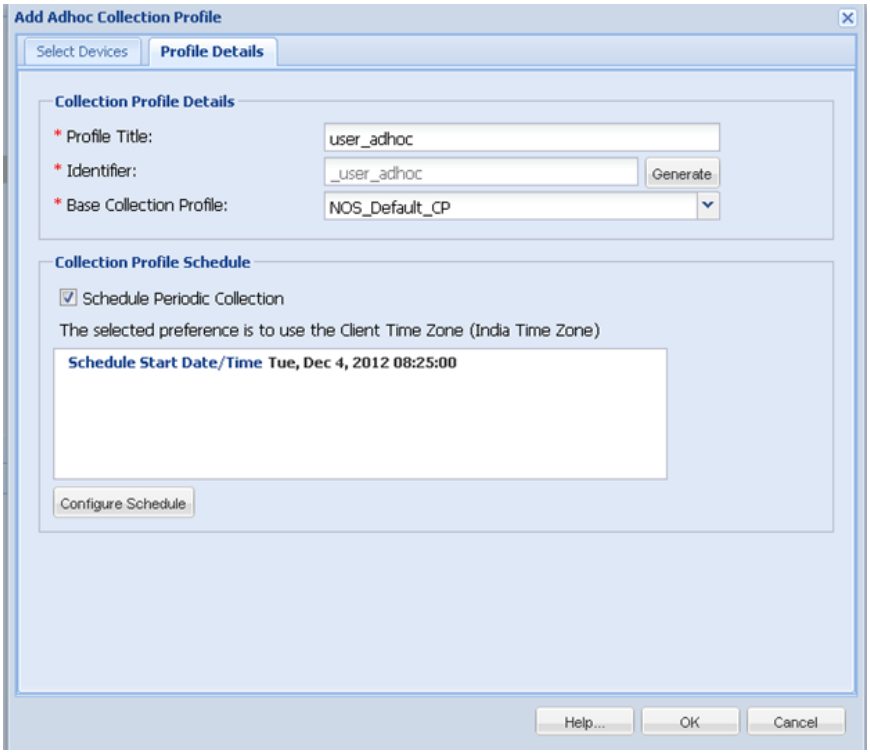


次の 2 つのセクションで必要な詳細を入力します。

- デバイスの選択（Select Devices）
- プロファイル詳細（Profile Details）

[デバイスの選択（Select Devices）] では、すべての管理対象デバイスを選択することも、少数のデバイスのみを選択することもできます。.txt ファイルからノードのリストを参照してアップロードすることもできます。[プロファイル詳細（Profile Details）] では、図 7-27 に示すように、必要な詳細を追加できます。

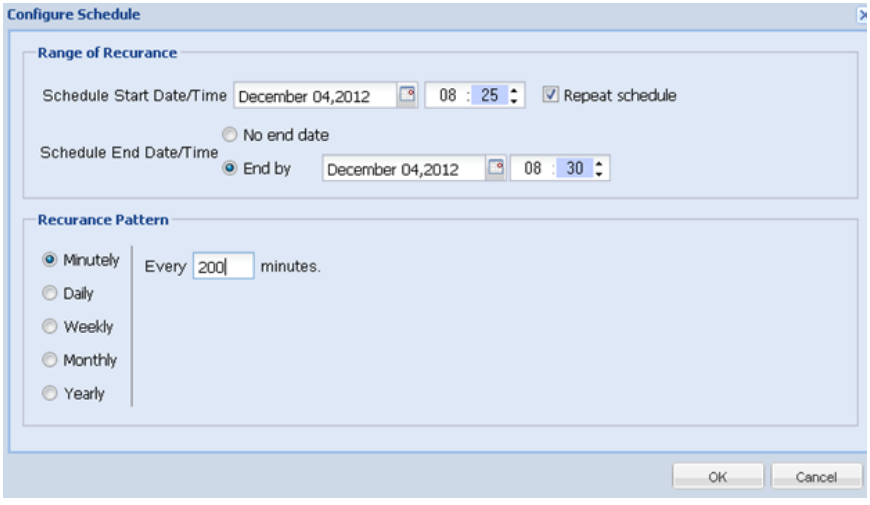
図 7-27　　アドホック収集の [プロファイル詳細（Profile Details）]



[基本収集プロファイル（Base Collection Profile）] ドロップダウン ボックスには、CSPC に存在するすべての収集プロファイルが表示されます。基本収集プロファイルとして使用する収集プロファイルを選択する必要があります。基本収集プロファイルの選択は必須です。

[スケジュールの設定（Configure Schedule）] では、必要な詳細を入力することにより、アドホック収集を指定した時刻にスケジュールし、特定の間隔で繰り返し実行するように設定できます。

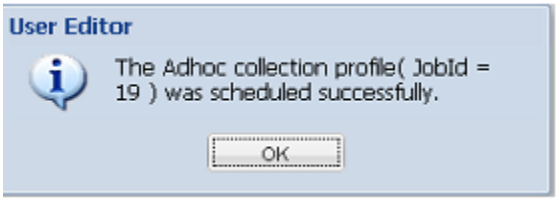
図 7-28　　[スケジュールの設定（Configure Schedule）]



[OK] をクリックして、プロファイルとデバイス詳細をアドホック収集プロファイルに保存します。正常

に完了すると、図 7-29 に示すメッセージが表示されます。

図 7-29　　確認メッセージ

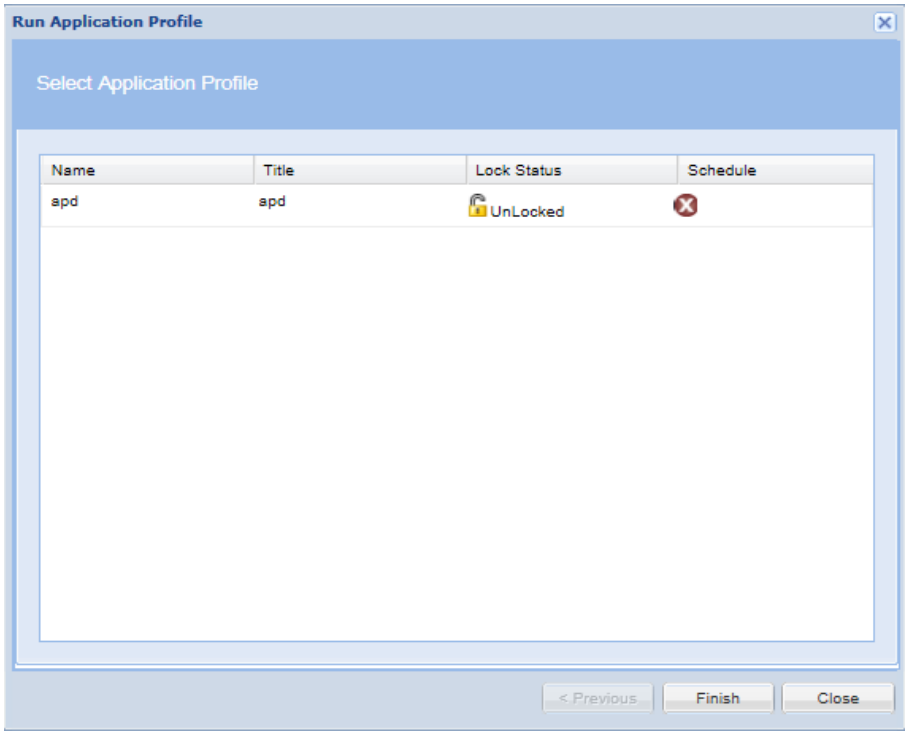


作成したアドホック収集プロファイルは、[データ収集プロファイルの管理（Manage Data Collection Profiles）] タブに表示されます。

[アプリケーション データの収集（Collect Application Data）]

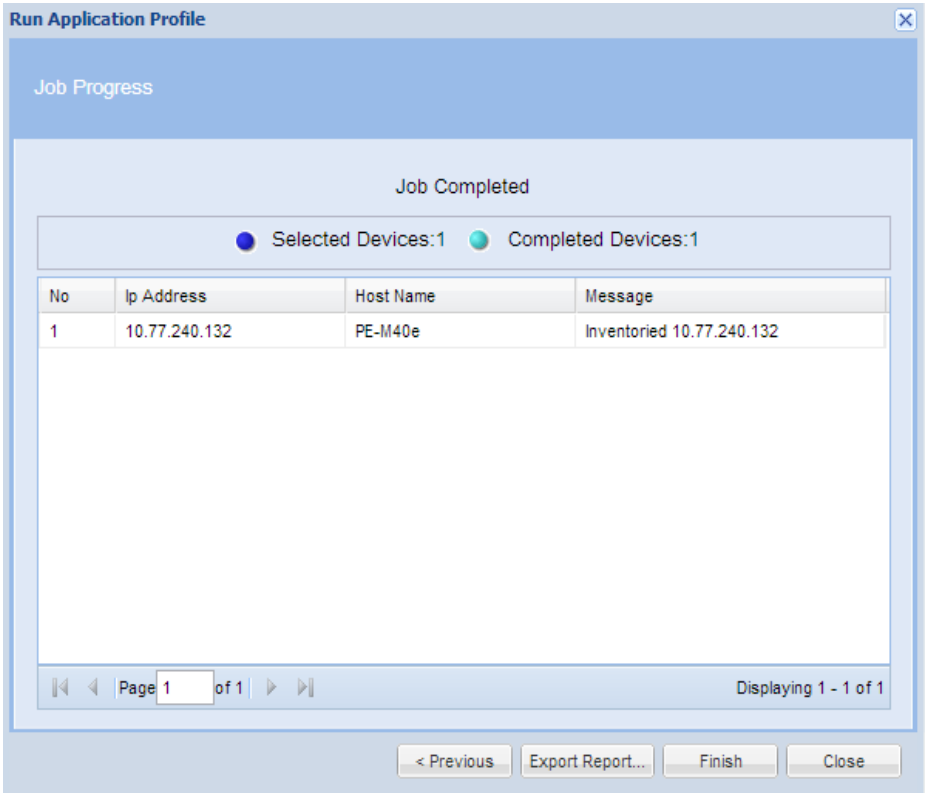
[アプリケーション プロファイルの実行（Run Application Profile）] には、アプリケーション プロファイルの一覧が表示されます。定義済みのアプリケーション プロファイルの一覧から任意のアプリケーション プロファイルを選択し、必要に応じて実行できます。プロファイルを実行するには、プロファイルを選択して [完了（Finish）] をクリックします。

図 7-30　　[アプリケーション プロファイルの実行（Run Application Profile）]



ジョブを起動すると、図 7-31 に示すように、IP アドレス、ホスト名、および成功または失敗を含む結果が表示されます。

図 7-31　　アプリケーション収集プロファイルの実行結果

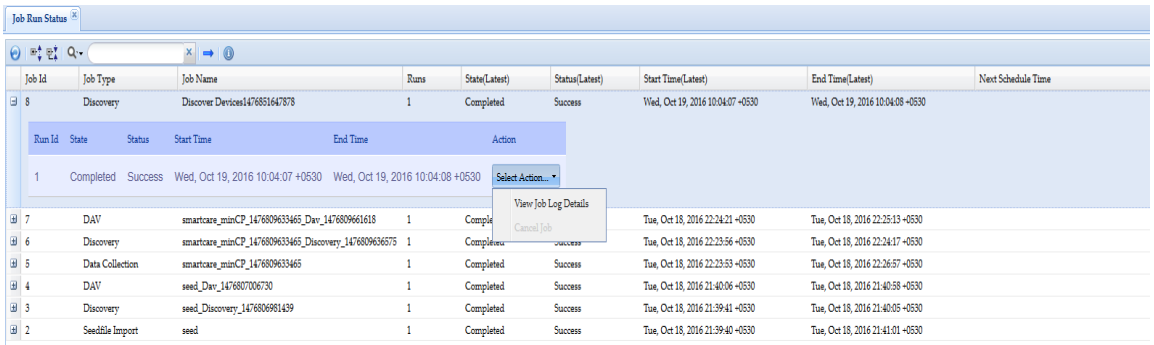


[ジョブの実行状況（Job Run Status）]

[ジョブの実行状況（Job Run Status）]

[ジョブの実行状況（Job Run Status）] で、実行したすべてのジョブの状況を把握できます。また、[ジョブ ID（Job ID）] の隣にある [+] 記号をクリックして、各ジョブの説明を確認できます。[+] 記号をクリックすると、図 7-32 に示すように、そのジョブの [実行 ID（Run Id）]、[状態（State）]（[成功（Successful）]/[中止（Aborted）]）、[ステータス（Status）]（[完了（Completed）]/[未完了（Not Completed）]）、[開始時刻（Start Time）]、[終了時刻（End Time）]、
および [ジョブ ログの詳細（Job Log Details）] が表示されます。

図 7-32　　[ジョブの実行状況（Job run Status）]

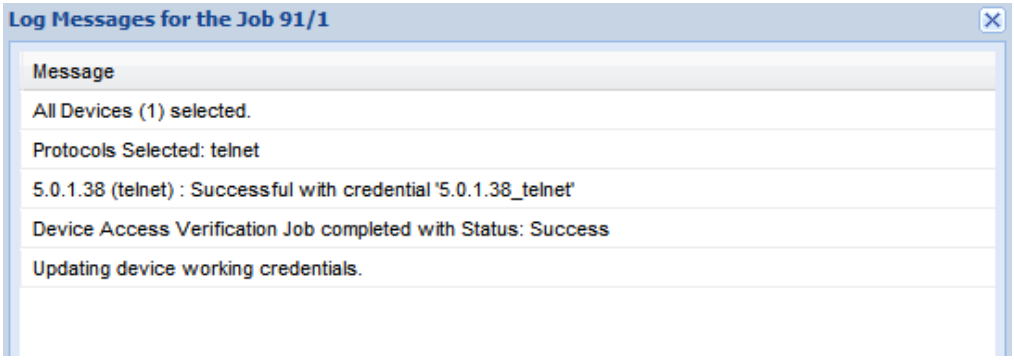


レポート内にある [アクション（Action）] ボタンを選択して、そのジョブのジョブ ログの詳細を表示す

るか、または実行中のジョブをキャンセルします。

図 7-33 にジョブ ログの詳細を示します。

図 7-33　　ジョブ ログの詳細



ジョブ管理

ジョブ情報を取得するには、[管理タスク（Management tasks）] タブの [ジョブ管理（Job Management）] サブ タブを使用します。ジョブ情報は、出力ファイルにエクスポートすることもできます。現在サポートされているファイル形式は、PDF、HTML、DOC、CSV（カンマ区切り）、TXT（タブ区切り）です。

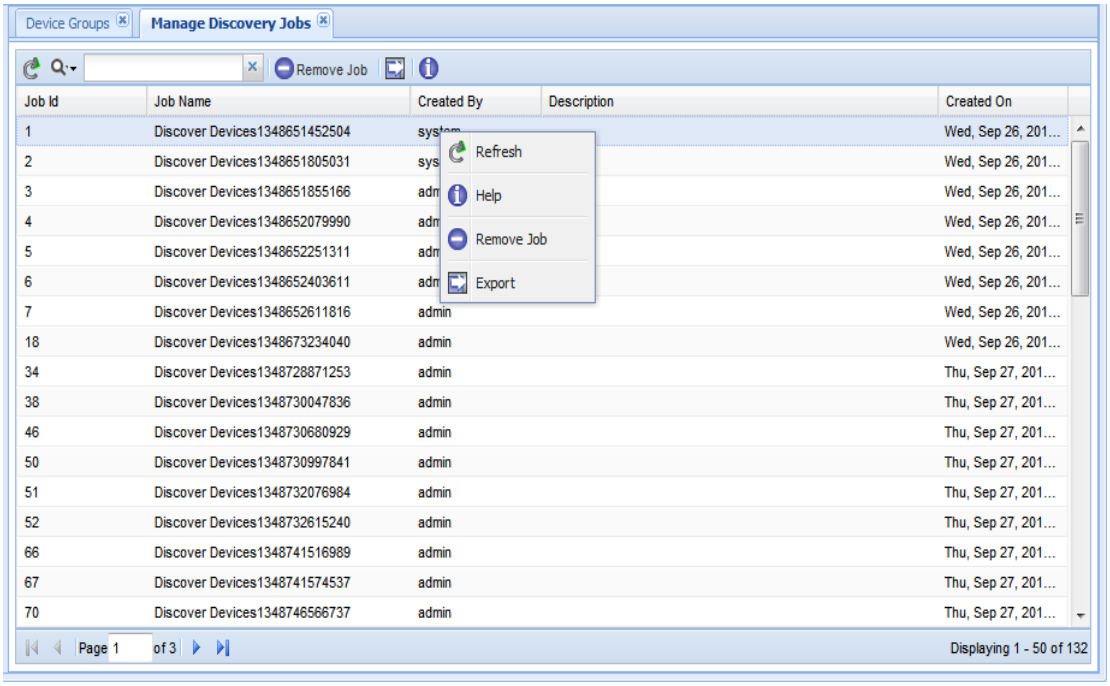
この項では、[ジョブ管理（Job Management）] オプションの以下の項目について説明します。

- [検出ジョブの管理（Manage Discovery Jobs）]
- [デバイス アクセスの検証ジョブの管理（Manage Device Access Verification Jobs）]
- [ワークフロー ジョブの管理（Manage Workflow Jobs）]
- [設定ジョブの管理（Manage Configuration Jobs）]
- [デバイス プロンプト収集ジョブの管理（Manage Device Prompt Collection Jobs）]
- [ヘルス モニタ ジョブの管理（Manage Health Monitor Jobs）]

[検出ジョブの管理（Manage Discovery Jobs）]

次に示すように、[検出ジョブの管理（Manage Discovery Jobs）] には、すでに実行したすべての検出ジョブの一覧があり、ジョブ情報をエクスポートするか、ジョブ情報をデータベースから削除するためのオプションがあります。

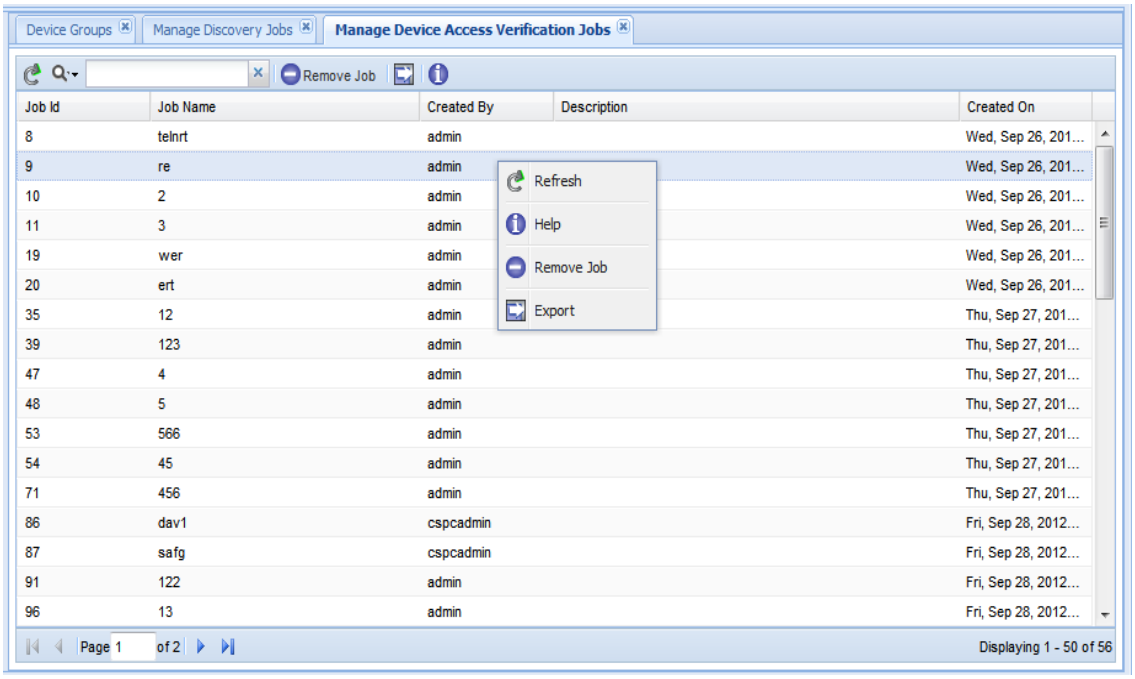
図 7-34　　[検出ジョブの管理（Manage Discovery Jobs）]



[デバイス アクセスの検証ジョブの管理（Manage Device Access Verification Jobs）]

次に示すように、[デバイス アクセスの検証ジョブの管理（Manage Device Access Verification Jobs）] には、すでに実行したすべてのデバイス検証ジョブの一覧があり、ジョブ情報をエクスポートするか、ジョブ情報をデータベースから削除するためのオプションがあります。

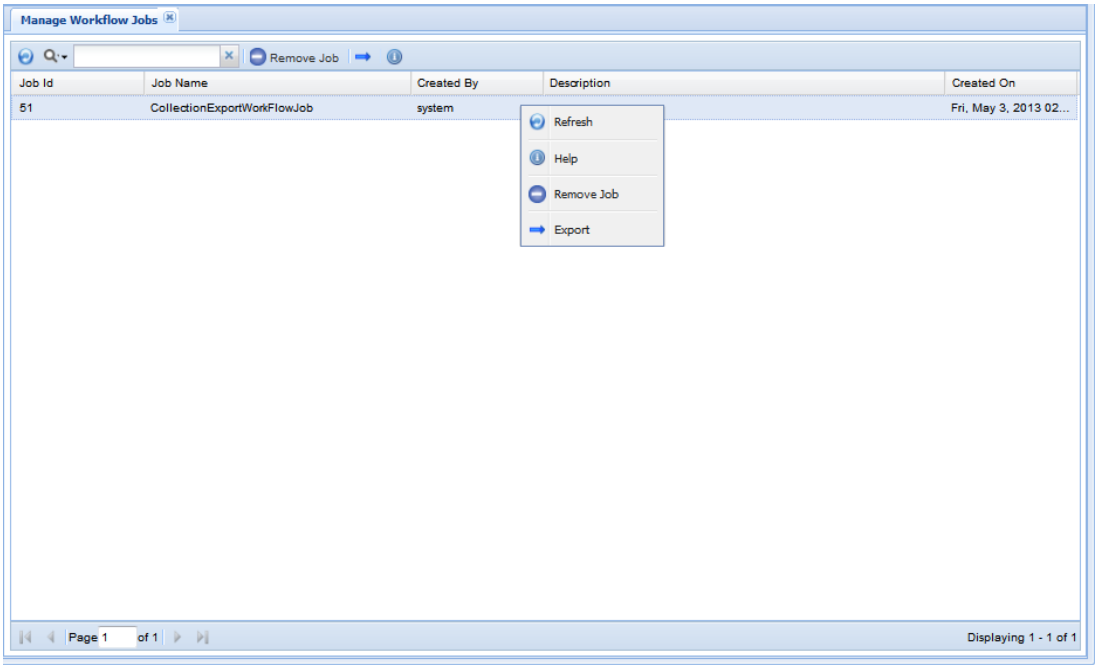
図 7-35　　[デバイス アクセスの検証ジョブの管理（Manage Device Access Verification Jobs）]



[ワークフロー ジョブの管理（Manage Workflow Jobs）]

次に示すように、[ワークフロー ジョブの管理（Manage Workflow Jobs）] には、すでに実行したワークフロー ジョブの一覧があり、ジョブ情報をエクスポートするか、ジョブ情報をデータベースから削除するためのオプションがあります。

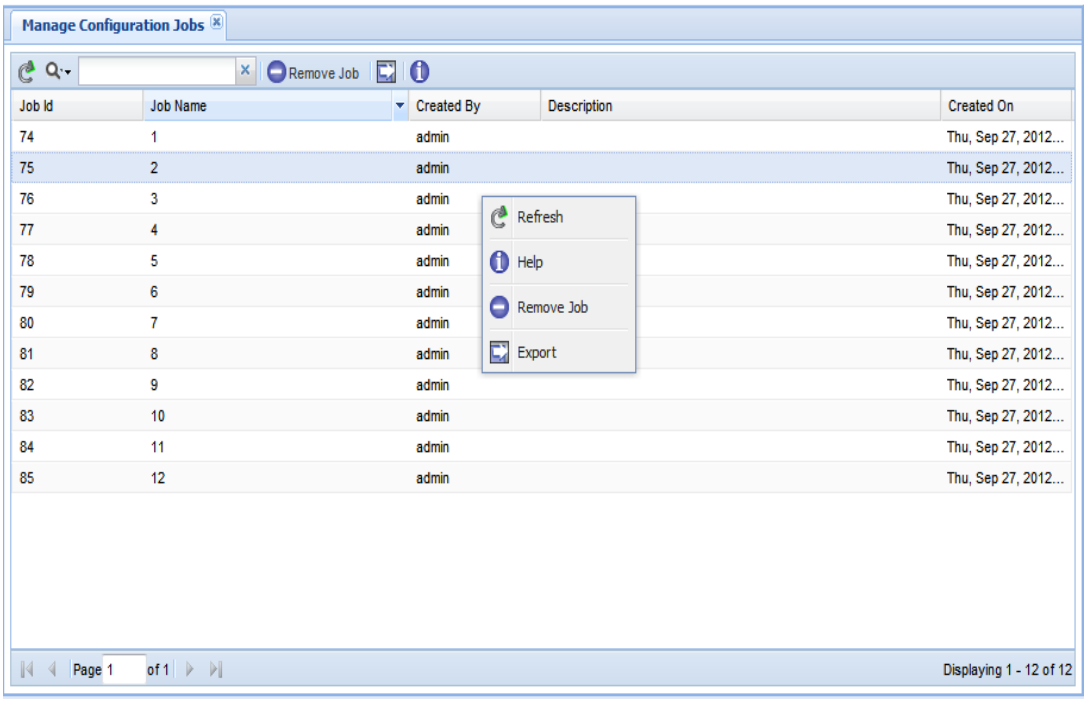
図 7-36　　[ワークフロー ジョブの管理（Manage Workflow Jobs）]



[設定ジョブの管理（Manage Configuration Jobs）]

次に示すように、[設定ジョブの管理（Manage Configuration Jobs）] には、すでに実行したすべてのデバイス設定ジョブの一覧があり、ジョブ情報をエクスポートするか、ジョブ情報をデータベースから削除するためのオプションがあります。

図 7-37　　[設定ジョブの管理（Manage Configuration Jobs）]

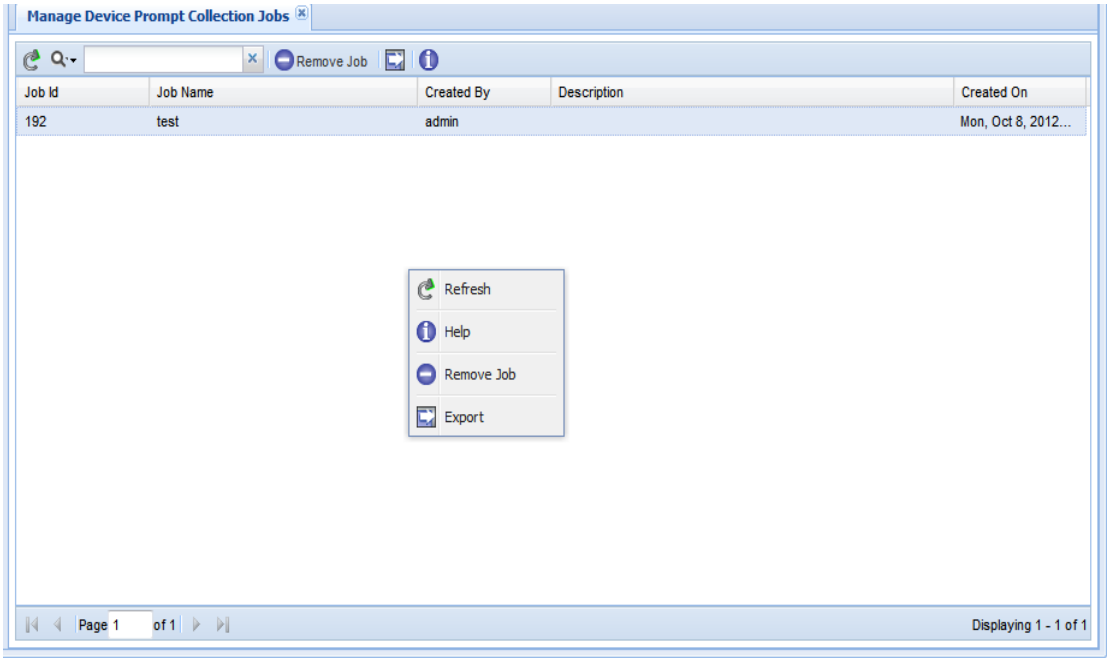


[デバイス プロンプト収集ジョブの管理（Manage Device Prompt Collection Jobs）]

図 7-38 に示すように、[デバイス プロンプト収集ジョブの管理（Manage Device Prompt Collection Jobs）] には、すでに実行したすべてのデバイス プロンプト収集ジョブの一覧があり、ジョブ情報をエクスポートするか、ジョブ情報をデータベースから削除するためのオプションがあります。

ジョブ情報は、出力ファイルにエクスポートすることもできます。現在サポートされているファイル形式は、PDF、HTML、DOC、CSV（カンマ区切り）、TXT（タブ区切り）です。

図 7-38　　[デバイス プロンプト収集ジョブ（Device Prompt Collection Jobs）]

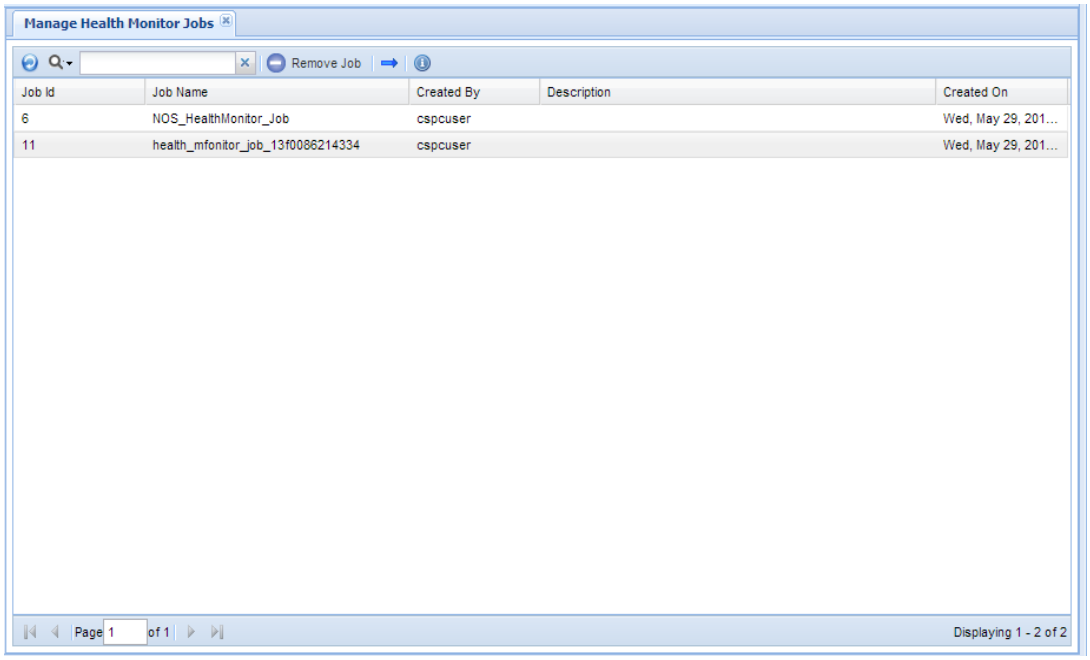


[ヘルス モニタ ジョブの管理（Manage Health Monitor Jobs）]

[ヘルス モニタ ジョブの管理（Manage Health Monitor Jobs）] には、すでに実行したすべてのモニタ ジョブの一覧があり、ジョブ情報をエクスポートするか、ジョブ情報をデータベースから削除するためのオプションがあります。

ヘルス モニタ ジョブは NOS 構成の一部としてインストールされます。これは毎日スケジュールされるジョブです。ユーザは、スケジュールされたヘルス モニタ ジョブを GUI/CLI から変更または作成することはできません。インストール後のヘルス モニタ ジョブのスクリーンショットを図 7-39 に示します。ジョブ情報は、出力ファイルにエクスポートすることもできます。現在サポートされているファイル形式は、PDF、HTML、DOC、CSV（カンマ区切り）、TXT（タブ区切り）です。

図 7-39　　[ヘルス モニタ ジョブ（Health Monitor Jobs）]



ジョブ実行の詳細は、[レポート（Reports）] -> [ジョブ管理レポート（Job Management Reports）] から表示することもできます。図 7-40 に示すように、ドロップダウンから [ヘルス収集ジョブ（Health Collection Jobs）] を選択し、[OK] をクリックします。

図 7-40　　[ジョブ レポート フィルタ（Job Report Filter）]

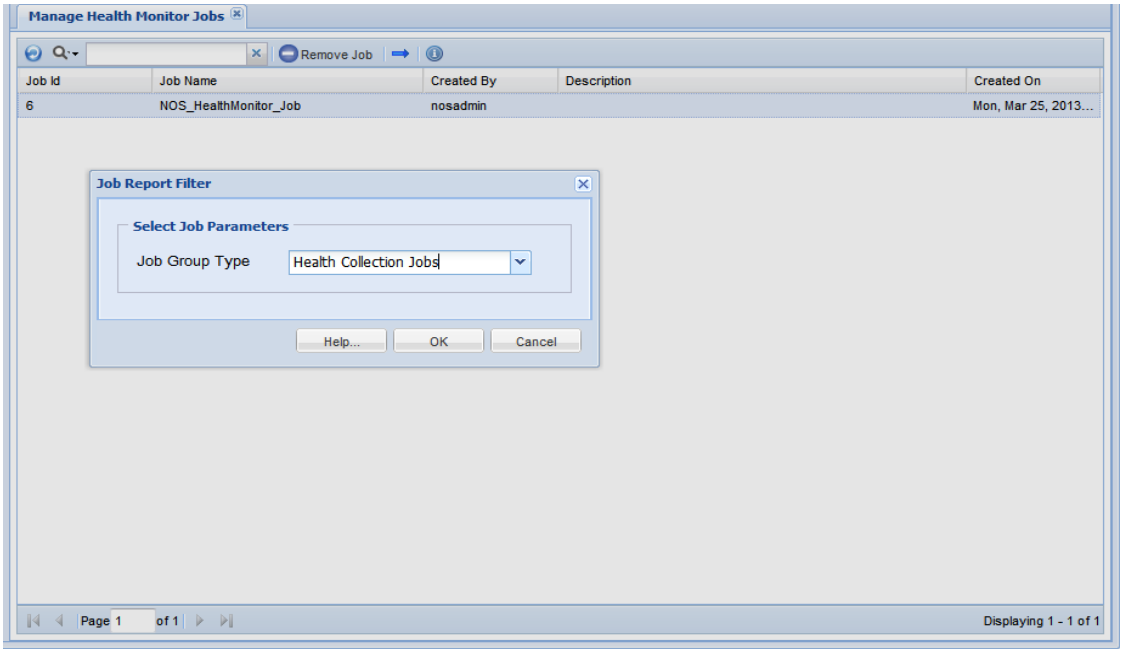


図 7-41　　[ヘルス収集ジョブ（Health Collection Jobs）]

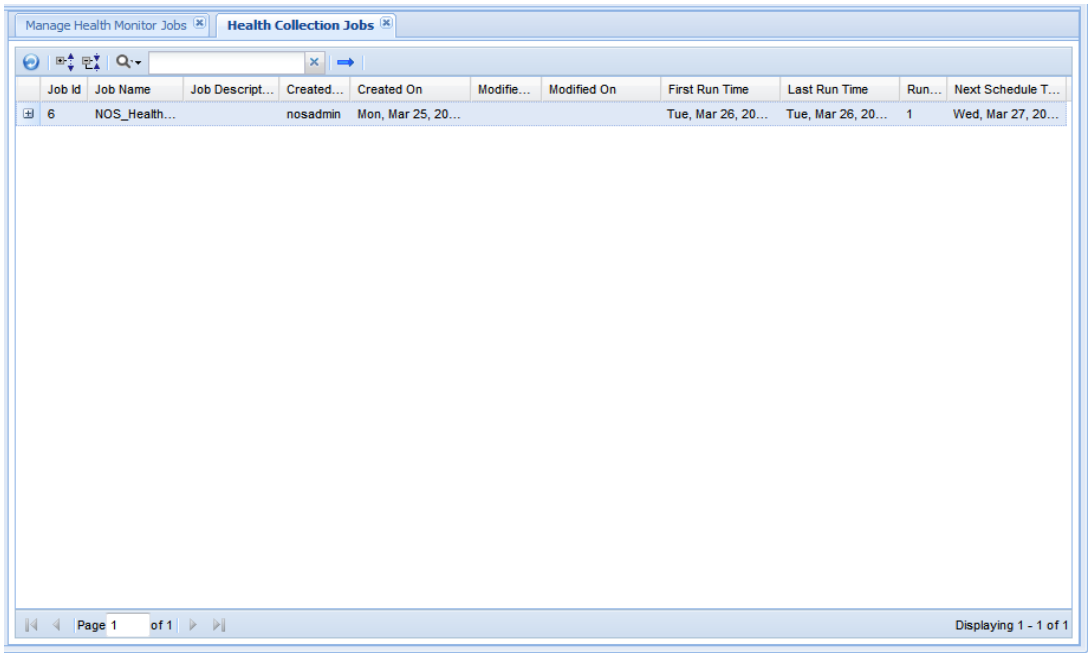


図 7-41 では、[ジョブ ID（Job Id）]、[ジョブ名（Job Name）]、[作成者（Created By）]、[作成日時（Created On）]、[変更者（Modified By）]、[変更日時（Modified On）]、[最初の実行時刻（First Run Time）]、[最後の実行時刻（Last Run Time）]、[実行回数（Run Count）]、[次のスケジュール時刻（Next Scheduled Time）] を確認できます。画面には、ジョブを手動で起動するオプションはありません。

これを達成できる CLI が 2 つあります。CLI は次のとおりです。

- job_schedule_healthMonitor_runnow.sh
- show_settings_healthMonitor_jobparameters.sh

show_settings_healthMonitor_jobparameters.sh を使用すると、ヘルス モニタ ジョブのすべてのパラメータを表示できます。1 つ目の job_schedule_healthMonitor_runnow.sh を使用すると、今すぐ実行ジョブを作成できます。これには 4 つのパラメータが必要です。図 7-42 に、CLI からヘルス モニタ ジョブを表示するためのパラメータを示します。

図 7-42　　CLI コマンド

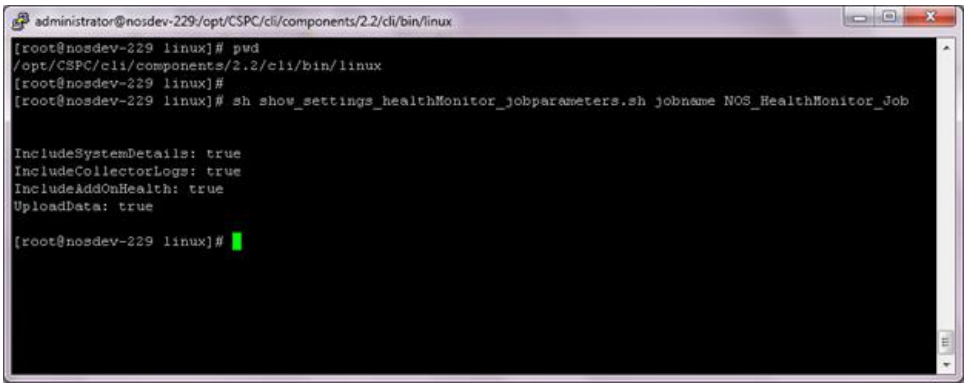
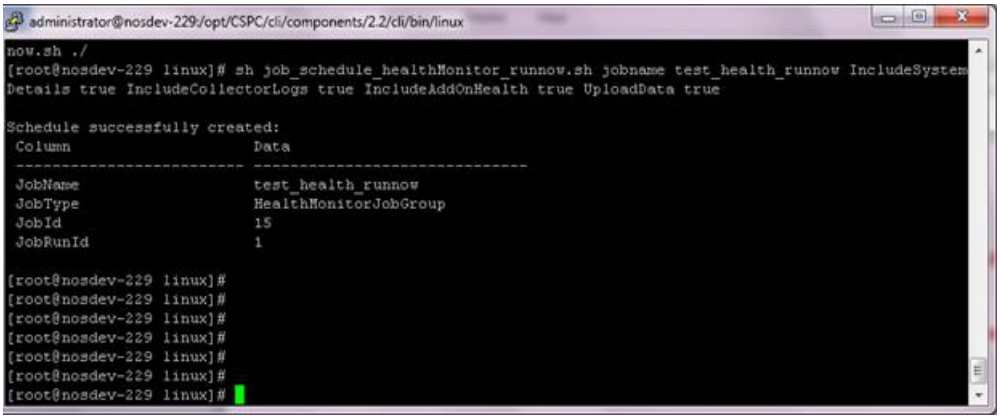


図 7-42 に示すように、CLI から新しいヘルス モニタの今すぐ実行ジョブをスケジュールできます。

CLI コマンド



8

アプリケーション - レポート

レポート

[レポート（Reports）] タブを使用して、収集されたデータと、検出、インベントリ、収集、およびバックアップ ジョブのジョブ ログの詳細を確認します。

この項では、[レポート（Reports）] オプションの以下の項目について説明します。

- [デバイス レポート（Device Reports）]
- [デバイス アクセス検証レポート（Device Access Verification Reports）]
- [データ収集レポート（Data Collection Reports）]
- [サービス レポート（Services Reports）]
- [監査証跡（Audit Trails）]
- [その他（Miscellaneous）]

レポートはすべて、多様なグラフ作成オプションとともに、HTML、Microsoft Word、PDF、CSV、TXT などのさまざまな形式でエクスポートできます。各レポートは、フィルタリング オプションとレポート フォーマット オプションを使用して簡単にナビゲートできます。

[デバイス レポート（Device Reports）]

[デバイス レポート（Device Reports）] サブ タブを使用して、選択したデバイスの収集データを確認します。この項では、[レポート（Reports）] オプションの以下の項目について説明します。

- [検出されたデバイスの表示（View Discovered Devices）]
- [到達不能デバイスの表示（View Unreachable Devices）]
- [重複デバイスの表示（View Duplicate Devices）]
- [検出レポート（Discovery Report）]
- [デバイスの表示プロパティ（Device Display Properties）]
- [非 SNMP デバイス（Non SNMP Devices）]
- [インターフェイスの概要（IOS、PIX、ASA、IOS-XR）（Interface Summary (IOS, PIX, ASA, IOS-XR)）]

[検出されたデバイスの表示（View Discovered Devices）]

[検出されたデバイス（Discovered Devices）] レポートには、検出および管理されているすべてのデバイスとそれらのデバイスの [IP アドレス（IP Address）]、[ホスト名（Host Name）]、[システム オブジェクト ID（Sys Object Id）]、[デバイス ファミリ（Device Family）]、[製品モデル（Product Model）]、[シリアル番号（Serial Number）]、[ベンダー名（Vendor Name）]、[OS 名（OS Name）]、[OS バージョン（OS Version）]、[検出日時（Discovery Date/Time）]、[ソース（Source）]、[到達可能（Reachable）] かどうか、などの詳細情報が表示されます。HTML、Microsoft Word、PDF、CSV、TXT などのさまざまな形式でエクスポートでき、多様なグラフ作成オプションを利用できます。また、フィルタリングとフォーマットのオプションにより、見やすく表示することができます。

図 8-1　　[検出されたデバイスの表示（View Discovered Devices）]

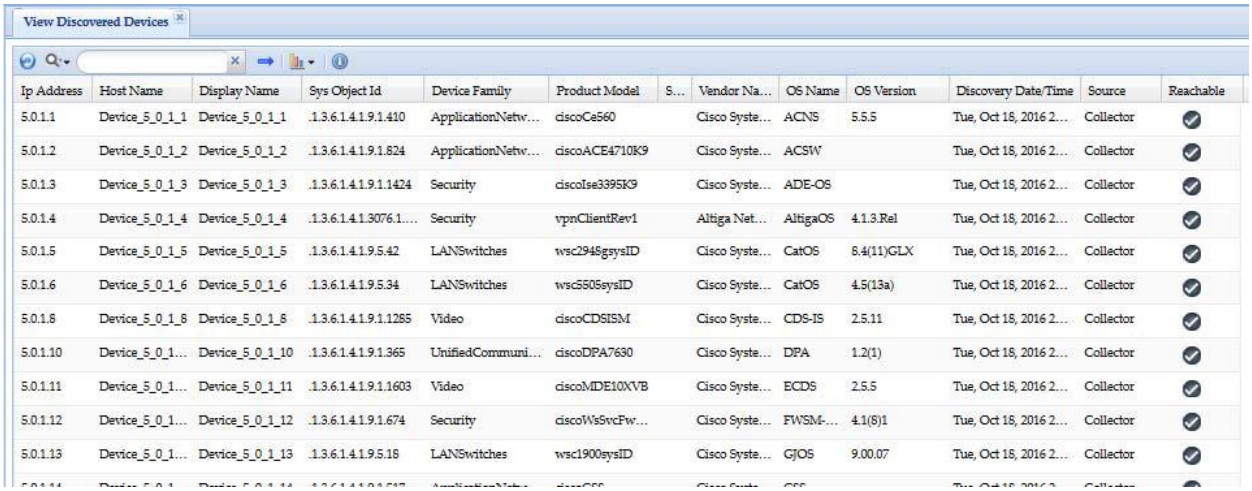


図 8-2 に示すように各レポートにはすべて、デバイス製品ファミリのグラフとともに、さまざまなグラフ作成オプションが用意されています。

図 8-2　　[グラフ作成オプション（Graphing Options）]

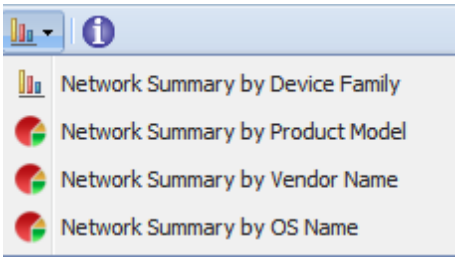
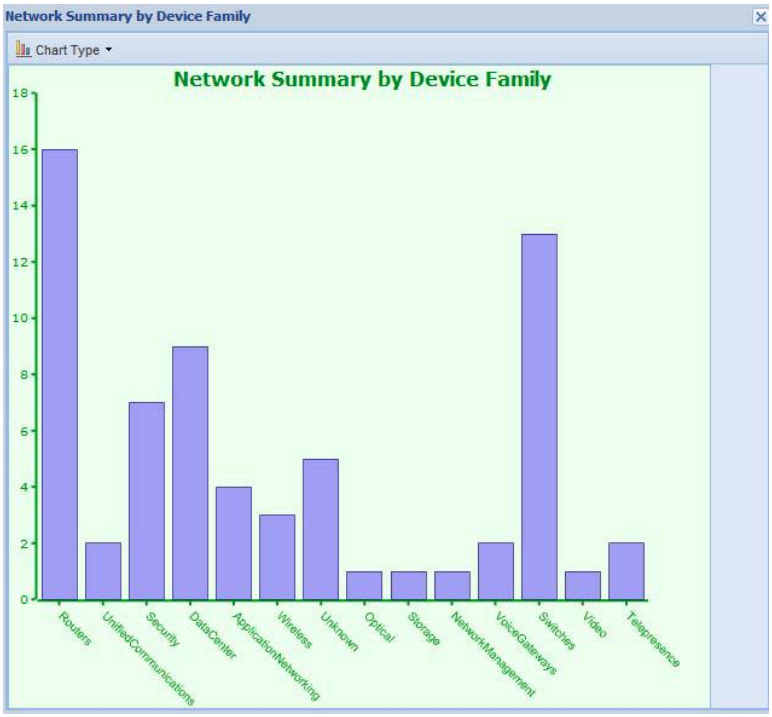


図 8-3　　[製品モデル別ネットワーク サマリー（Network Summary by Product Model）]



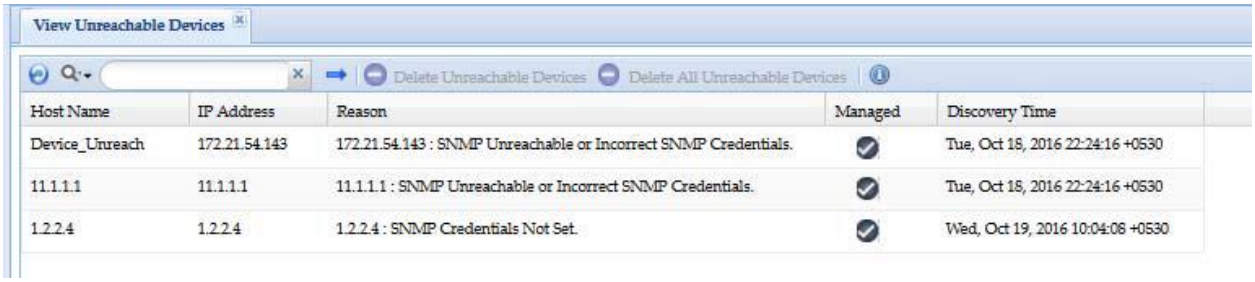
CSPC フローチャートに戻る

[到達不能デバイスの表示（View Unreachable Devices）]

このレポートには、到達不能デバイスと検出の実行中に検出されなかったデバイスがすべて表示されます。各到達不能デバイスのホスト名、IP アドレス、理由、管理ステータス、検出時刻などの情報が表示されます。

デバイスの再検出を実行するには、デバイスを右クリックして [検出ジョブを開始（Start Discovery Job）] オプションを選択します。また、[到達不能デバイスを削除（Delete Unreachable Device）] をクリックして任意の到達不能デバイスを削除したり、[すべての到達不能デバイスを削除（Delete All Unreachable Device）] をクリックしてすべての到達不能デバイスを削除したりすることもできます。

図 8-4　　[到達不能デバイスの表示（View Unreachable Devices）]

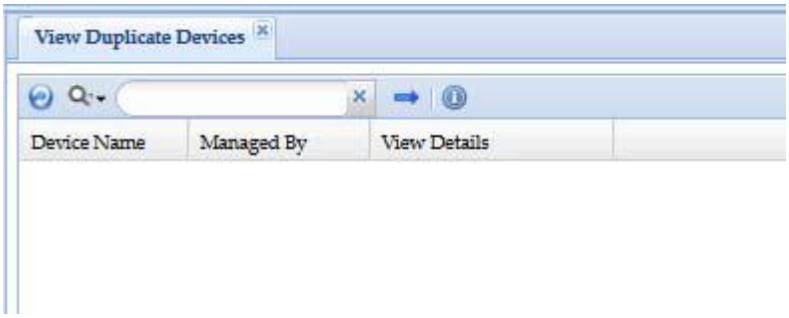


[重複デバイスの表示（View Duplicate Devices）]

このレポートには、図 8-5 に示すようにすべての重複デバイスが表示されます。[デバイス名（Device

Name）]、
[管理者（Managed By）]、[デバイスの詳細（View Details）] などの情報が表示されます。

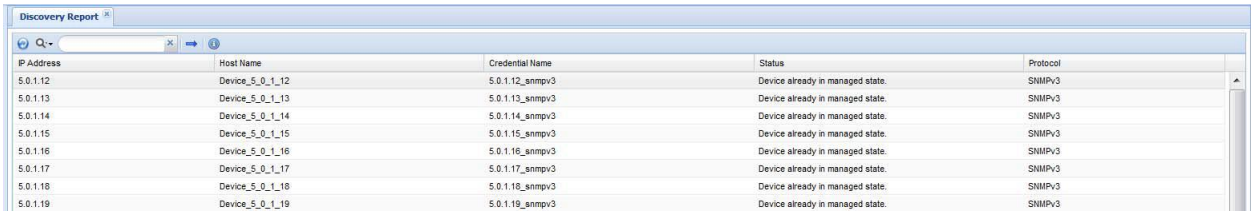
図 8-5　　重複デバイス



[検出レポート（Discovery Report）]

このレポートには、検出されたすべてのデバイスが表示されます。検出された各デバイスのホスト名、IP アドレス、クレデンシャル名、ステータス、プロトコルなどの情報が表示されます。

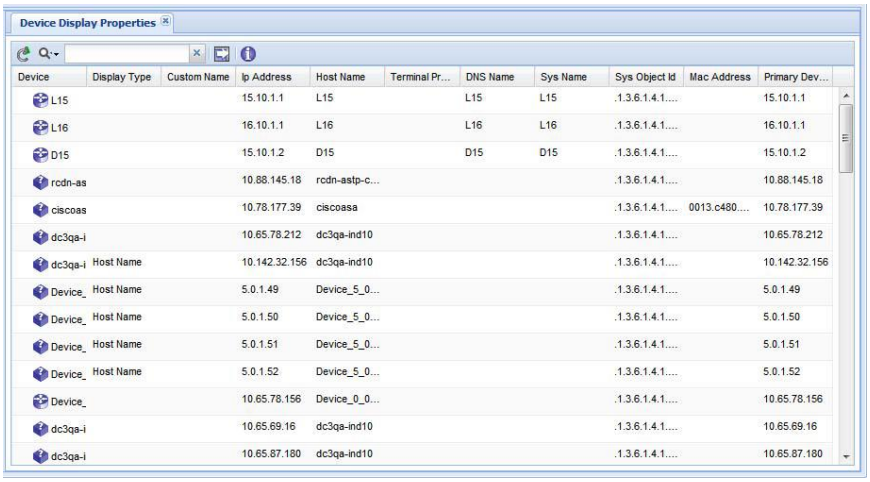
図 8-6　　[検出レポート（Discovery Report）]



[デバイスの表示プロパティ（Device Display Properties）]

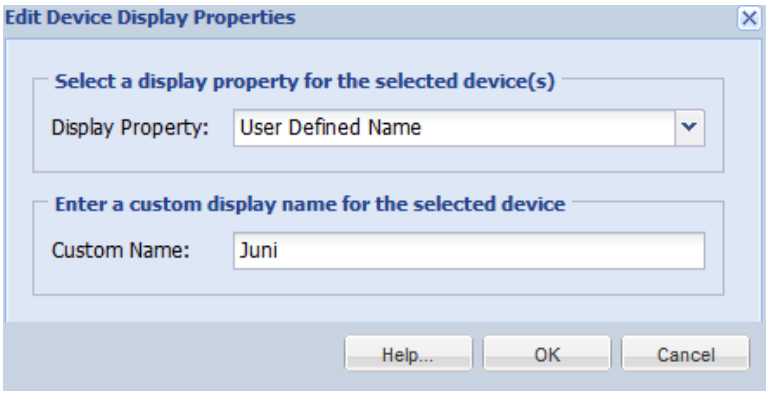
[デバイスの表示プロパティ（Device Display Properties）] レポートには、すべてのデバイスに設定されているプロパティが表示されます。また、このウィンドウでは、特定のデバイスまたはデバイス グループの表示プロパティを設定することもできます。ホスト名、IP アドレス、DNS 名などのデバイス プロパティに固有の名前を割り当てることができます。

図 8-7　　[デバイスの表示プロパティ（Device Display Properties）]



デバイスの表示プロパティにカスタム名を付けるには、一覧の任意のデバイスを右クリックして [プロパティの編集（Edit Properties）] オプションを選択します。ローカル設定はグローバル設定よりも優先されます。

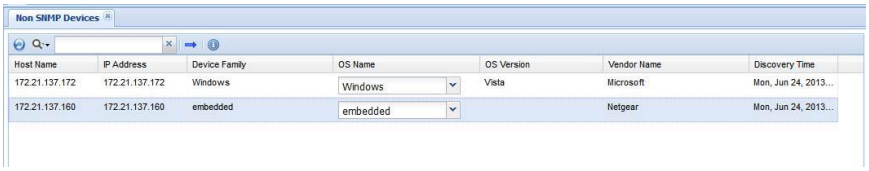
図 8-8　　[デバイスの表示プロパティの編集（Edit Device Display Properties）]



[非 SNMP デバイス（Non SNMP Devices）]

[非 SNMP デバイス（Non SNMP Devices）] レポートには、「Nmap」メカニズムによって検出された、SNMP エージェントが動作していないデバイスの一覧が表示されます。これらのデバイスは管理対象状態に移行できます。
これを行うには、デバイスを選択し、右クリックして [デバイスの管理（Manage Devices）] を選択します。

図 8-9　　[非 SNMP デバイス（Non SNMP Devices）]

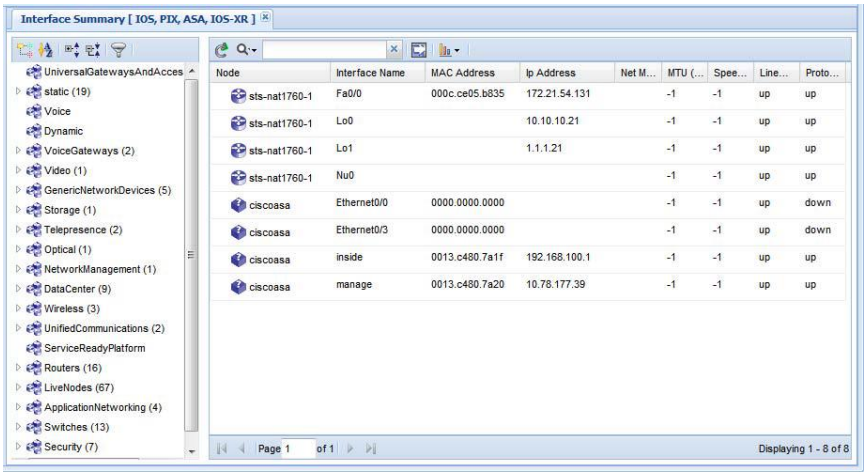


Nmap によって検出されたデバイスの OS が正しくない場合は、ドロップダウン リストから適切な OS 名を選択できます。

[インターフェイスの概要（IOS、PIX、ASA、IOS-XR）（Interface Summary (IOS, PIX, ASA, IOS-XR)）]

[インターフェイスの概要（Interface Summary）] レポートには、CSPC で使用可能なすべてのインターフェイスの一覧が表示されます。

図 8-10　　[インターフェイスの概要（Interface Summary）]



インターフェイスの概要データは、グラフィック アイコンをクリックしてグラフィック形式で表示することもできます。次のオプションが表示されます。

- インターフェイス ステータスの概要
- インターフェイス IP アドレスの概要
- インターフェイス タイプの概要

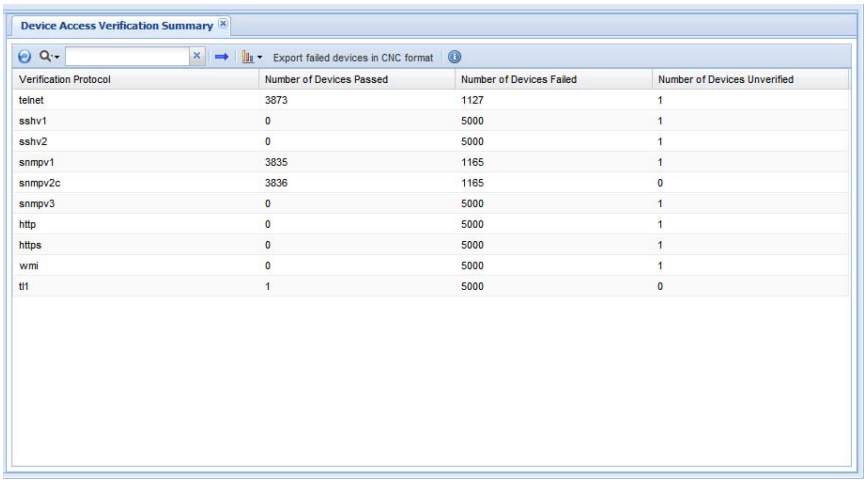
[デバイス アクセス検証レポート（Device Access Verification Reports）]

- [デバイス アクセス検証のサマリー（Device Access Verification Summary）]
- [データセット タイプ別のデバイス アクセス検証（Device Access Verification By Dataset Type）]
- [アクセス検証結果の表示（View Access Verification Results）]

[デバイス アクセス検証のサマリー（Device Access Verification Summary）]

[デバイス アクセス検証のサマリー（Device Access Verification Summary）] レポートには、アクセス検証のサマリーが表示されます。このレポートには、使用したプロトコルのタイプ、成功または失敗したデバイス数、および検証されていないデバイス数の詳細な概要が示されます。これを示しているのが図 8-11 です。

図 8-11　　[デバイス アクセス検証のサマリー（Device Access Verification Summary）]



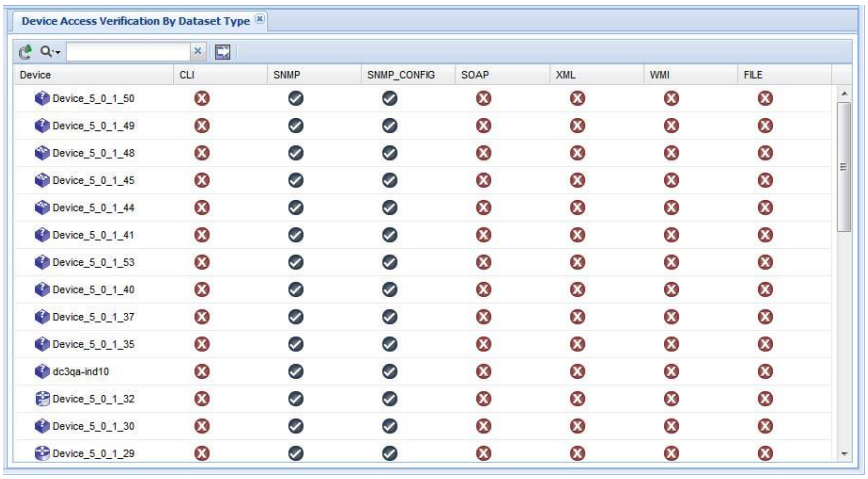
Verification Protocol	Number of Devices Passed	Number of Devices Failed	Number of Devices Unverified
telnet	3873	1127	1
sshv1	0	5000	1
sshv2	0	5000	1
snmpv1	3835	1165	1
snmpv2c	3836	1165	0
snmpv3	0	5000	1
http	0	5000	1
https	0	5000	1
wmi	0	5000	1
tl1	1	5000	0

[デバイス アクセス検証のサマリー（Device Access Verification Summary）] では、障害が発生したデバイスを CNC 形式でエクスポートできます。選択したフィルタ タイプ（デバイス、プロトコル、ステータスなど）に関連するデータと失敗したクレデンシャルのみがシード ファイルの一部としてエクスポートされます。このエクスポート オプションは、手動で追加したデバイスとシード ファイルのインポートによって追加したデバイスの両方でサポートされます。

[データセット タイプ別のデバイス アクセス検証（Device Access Verification By Dataset Type）]

[データセット タイプ別のデバイス アクセス検証（Device Access Verification by Dataset Type）] には、デバイスの一覧とそれらのデバイスで CLI、SNMP、SNM 設定、SOAP、XML、WMI、FILE タイプのプロトコルとファイルがサポートされているかどうかが表示されます。

図 8-12　　[データセット タイプ別のデバイス アクセス検証（Device Access Verification By Dataset Type）]

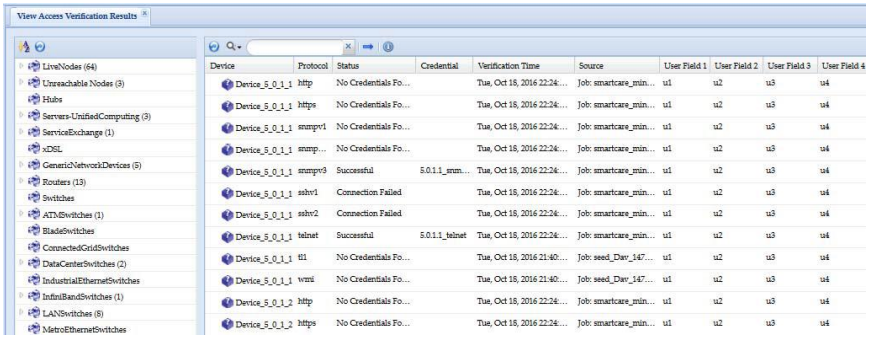


Device	CLI	SNMP	SNMP_CONFIG	SOAP	XML	WMI	FILE
Device_5_0_1_50	✗	✓	✓	✗	✗	✗	✗
Device_5_0_1_49	✗	✓	✓	✗	✗	✗	✗
Device_5_0_1_48	✗	✓	✓	✗	✗	✗	✗
Device_5_0_1_45	✗	✓	✓	✗	✗	✗	✗
Device_5_0_1_44	✗	✓	✓	✗	✗	✗	✗
Device_5_0_1_41	✗	✓	✓	✗	✗	✗	✗
Device_5_0_1_53	✗	✓	✓	✗	✗	✗	✗
Device_5_0_1_40	✗	✓	✓	✗	✗	✗	✗
Device_5_0_1_37	✗	✓	✓	✗	✗	✗	✗
Device_5_0_1_35	✗	✓	✓	✗	✗	✗	✗
dc3qa-ind10	✗	✓	✓	✗	✗	✗	✗
Device_5_0_1_32	✗	✓	✓	✗	✗	✗	✗
Device_5_0_1_30	✗	✓	✓	✗	✗	✗	✗
Device_5_0_1_29	✗	✓	✓	✗	✗	✗	✗

[アクセス検証結果の表示（View Access Verification Results）]

[アクセス検証結果の表示（View Access Verification Results）] レポートには、最新のデバイス アクセス検証の結果が表示されます。このレポートには、検証時間および検証のソース（検出の一部または独立した検証ジョブ）と成功または失敗したプロトコル、デバイスの組み合わせ、およびユーザ定義フィールドの詳細が表示されます。これを示しているのが図 8-13 です。

図 8-13　　[アクセス検証結果の表示（View Access Verification Results）] レポート



このレポートには、インテリジェント検索オプションも表示されています。「tel」と入力すると、Telnet クレデンシャルのみリストされ、レポートには、入力した「tel」と一致するエントリのみ表示されます。上のスクリーンショットに示されているように、検索オプションは非常に広範なものなので、レポート内の任意のフィールドまたは値に基づき検索できます。ワイルドカード、正規表現、マッチング パターンなども指定できます。これらを指定すると、探しているデータを迅速かつ容易にピンポイントで検索できます。

CSPC フローチャートに戻る

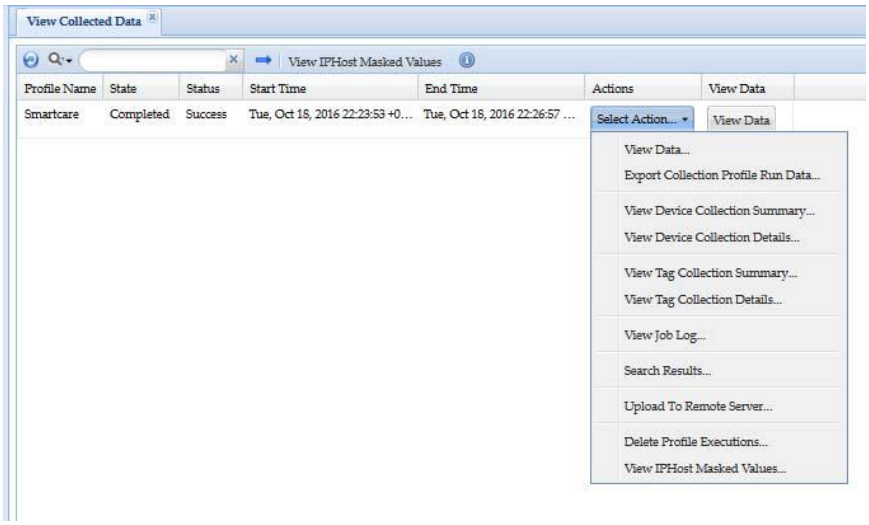
[データ収集レポート（Data Collection Reports）]

- [収集されたデバイスの表示（View Collected Devices）]
- [収集実行結果サマリーの表示（View Collection Run Summary）]
- [設定収集済みデバイス（Config Collected Devices）]
- [デバイスごとの設定データ（Config Data Per Device）]

[収集されたデバイスの表示（View Collected Devices）]

このレポートには、完了した収集プロファイルのサマリー、およびそれらの収集プロファイルを入力している間に収集されたデータが表示されます。特定の完了した収集プロファイル データを確認したり、データをレポートにエクスポートしたりできます。また、ジョブ ログのステータスを確認したり、収集データを削除したりすることもできます。

図 8-14　　[収集プロファイル実行結果サマリー（Collection Profile Run Summary）] メイン ウィンドウ

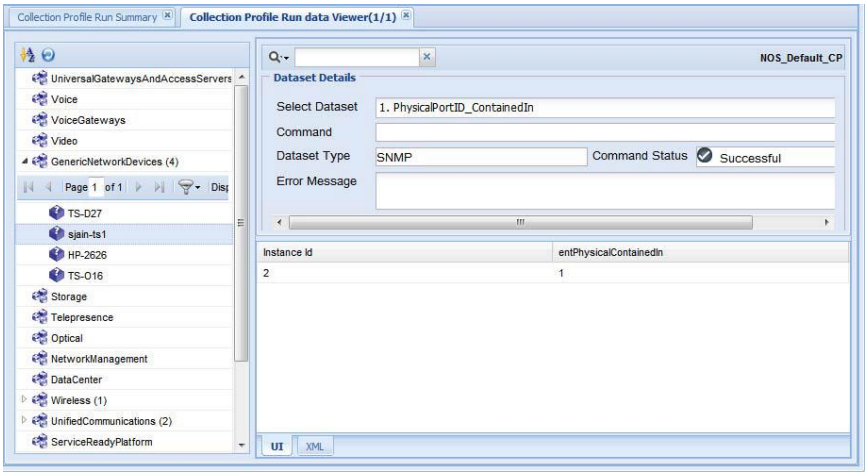


レポート内の任意の行を選択して右クリックすると、その行に関連付けられているすべてのオプションを表示できます。

- [データを表示（View Data）]
- [収集プロファイル実行データをエクスポート（Export Collection Profile Run Data）]
- [デバイス収集のサマリーを表示（View Device Collection Summary）]
- [デバイス収集の詳細を表示（View Device Collection Details）]
- [タグ収集のサマリーを表示（View Tag Collection Summary）]
- [タグ収集の詳細を表示（View Tag Collection Details）]
- [ジョブ ログを表示（View Job Log）]
- [結果を検索（Search Results）]
- [リモート サーバにアップロード（Upload to Remote Server）]
- [プロファイルの実行を削除（Delete Profile Executions）]
- [IP ホストのマスク値を表示（View IP Host Masked Values）]

図 8-15 に示すように [データを表示（View Data）] を選択すると、[収集プロファイル実行データ ビューア（Collection Profile Run Data Viewer）] にデータが表示されます。

図 8-15　　[収集プロファイル実行データ ビューア（Collection Profile Run Data Viewer）]



特定のデータセットを選択すると、そのデータセットの出力とデータ収集の成功または失敗のステータス（[コマンド ステータス（Command Status）]）が表示されます。[コマンド ステータス（Command Status）] には次のいずれかの状態が表示されます。

- 成功（Successful）
- 失敗（Failed）
- 該当なし（Not Applicable）

[収集のサマリーを表示（View Collection Summary）] と [収集の詳細を表示（View Collection Details）] には、
選択した収集プロファイルの収集のサマリーと詳細が表示されます。これを示しているのが図 8-16 です。

図 8-16　　[デバイス収集プロファイル実行結果サマリー（Collection Profile Device Run Summary）]

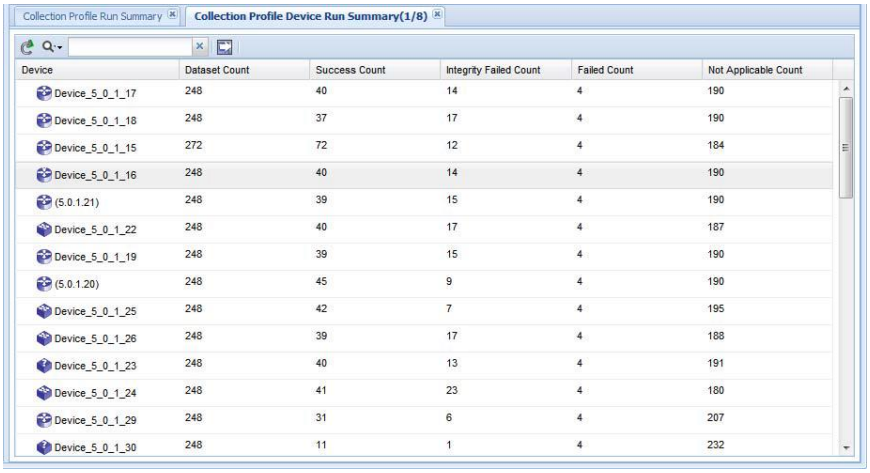
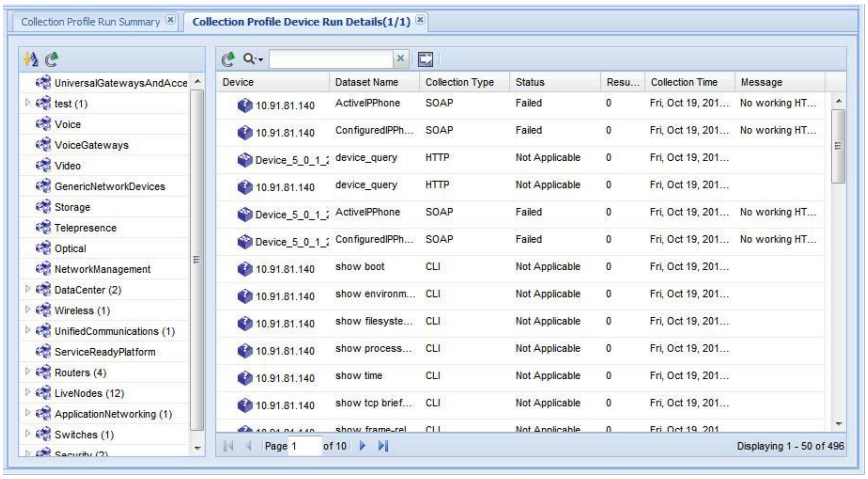
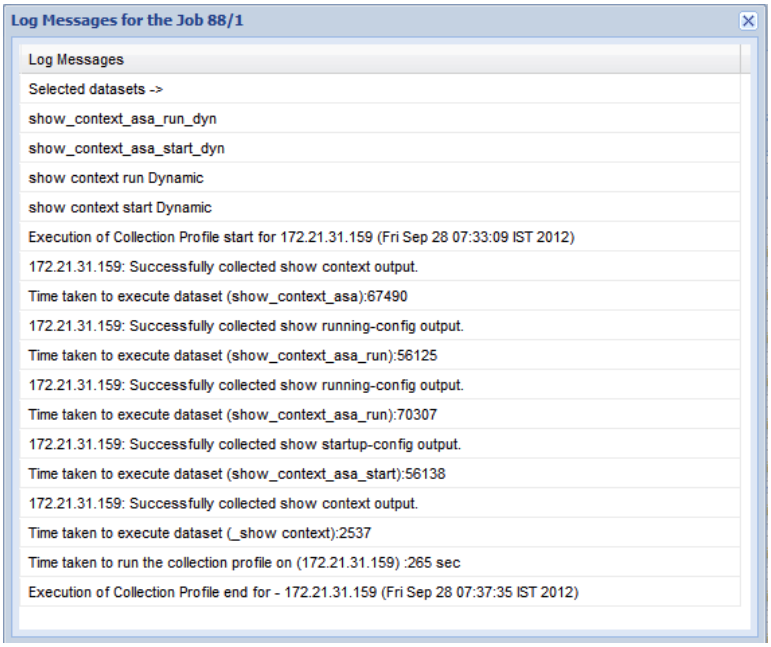


図 8-17　　[収集プロファイル実行結果詳細（Collection Profile Run Details）]



次に示すように、特定の実行ジョブのログ メッセージ、および選択したデバイスの各データセットの収集ステータスを確認できます。

図 8-18　　[収集プロファイル実行結果サマリー ログ メッセージ（Collection Profile Run Summary Log Messages）]



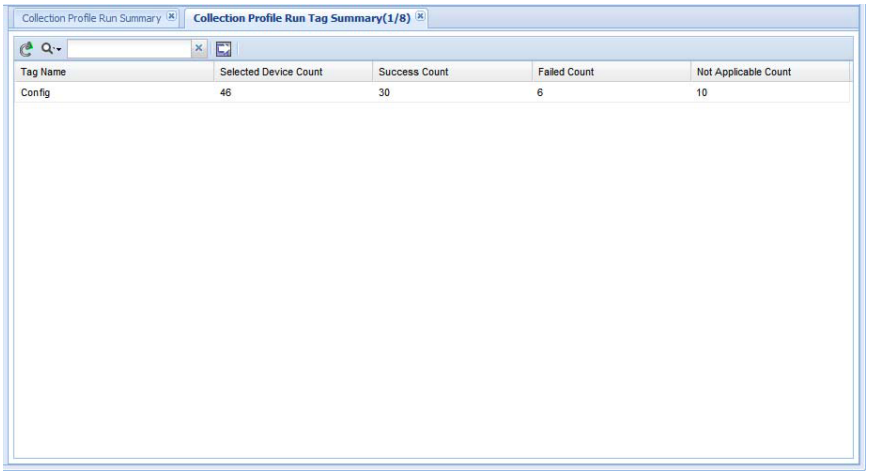
[プロファイル実行対象の削除（Delete Profile Executions）] を選択して、収集プロファイルの実行の特定のインスタンスを削除することもできます。

次に示すように、選択した 2 つの実行間の相違点を確認するには、[選択した実行間の相違点表示（Show Differences between selected Runs）] オプションを選択します。

以前にタグ付けされたコマンドのサマリーを表示するには、[タグ収集のサマリーを表示（View Tag

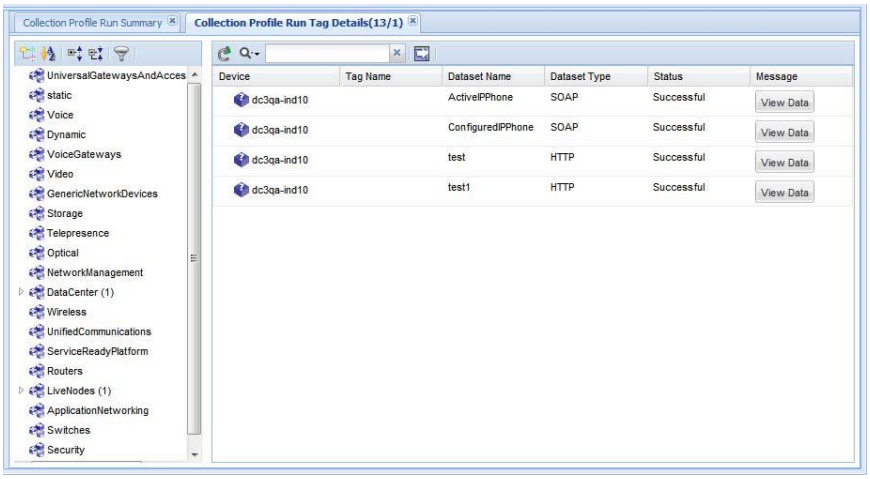
Collection Summary）] オプションを使用します。図 8-19 に示すようにタグ収集のサマリー画面には、タグ付けされたデバイスの数と成功数、失敗数、および該当しないデバイスの数が表示されます。

図 8-19　　[タグ収集のサマリーを表示（View Tag Collection Summary）]



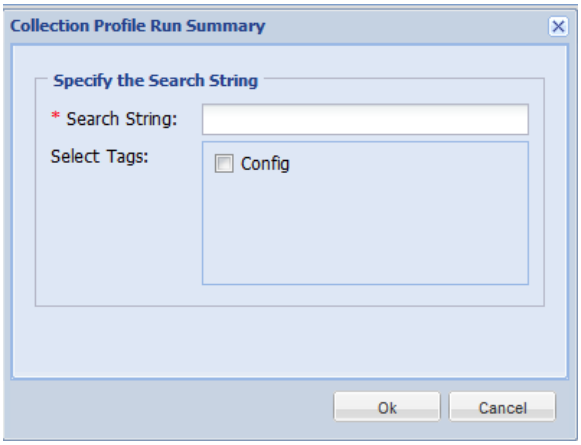
タグ付けされたコマンドの詳細を表示するには、[タグ収集の詳細を表示（View Tag Collection Details）] オプションを使用します。この画面には、[デバイス名（Device）]、[タグ名（Tag Name）]、[データセット名（Dataset Name）]、[データセット タイプ（Dataset Type）]、[ステータス（Status）]、および [メッセージ（Message）] が表示されます。

図 8-20　　[タグ収集の詳細を表示（View Tag Collection Details）]



結果を検索するには、[結果を検索（Search Results）] オプションを使用します。図 8-21 に示すように検索文字列を指定し、結果の検索に使用するタグを選択します。

図 8-21　　[収集プロファイル実行結果サマリー（Collection Profile Run Summary）]



収集プロファイルの詳細をリモート サーバにアップロードするには、[リモート サーバにアップロード（Upload to Remote Server）] オプションを使用します。

図 8-22　　リモート サーバへのアップロード中

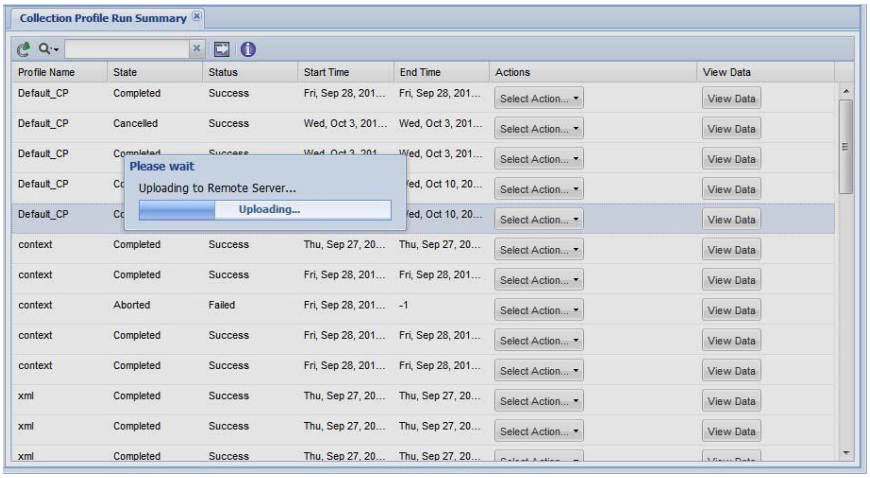
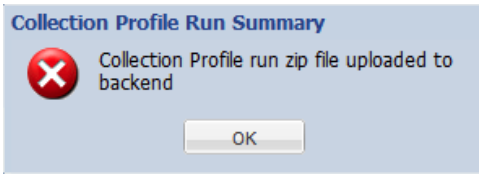


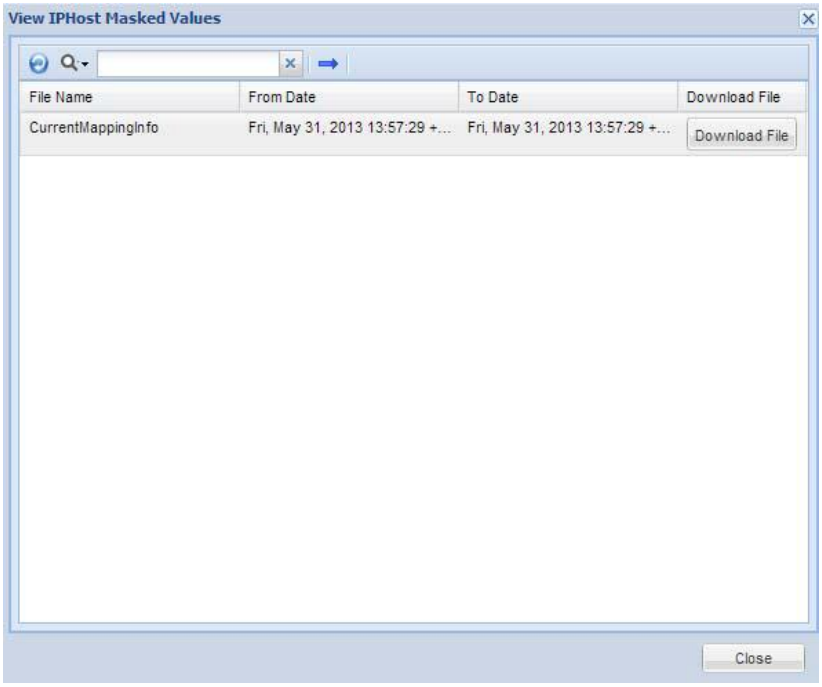
図 8-23 に示すように、アップロードが成功したことを確認するメッセージが表示されます。

図 8-23　　リモート サーバへのアップロード メッセージ



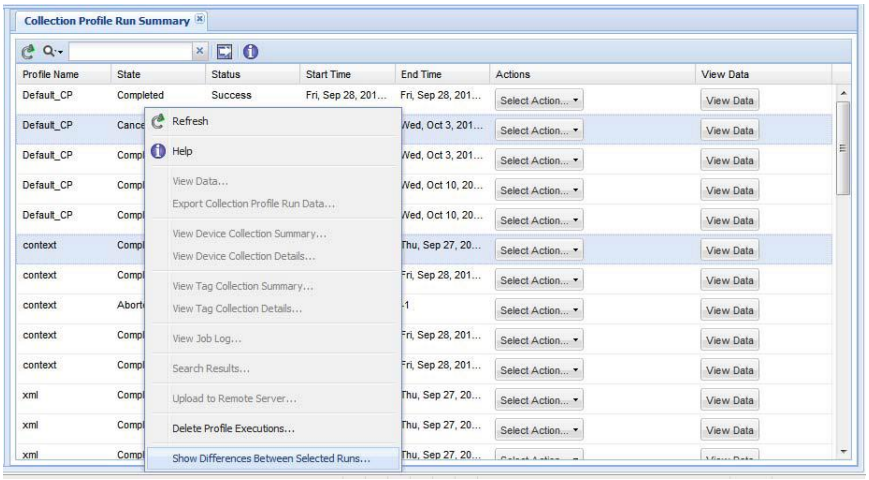
IP ホストのマスク値を表示するには、[IP ホストのマスク値を表示（View IP Host Masked Values）] オプションを表示します。[ダウンロード（Download）] ボタンをクリックして、ファイルをテキスト形式でダウンロードすることもできます。

図 8-24　　[IP ホストのマスク値を表示（View IP Host Masked Values）]



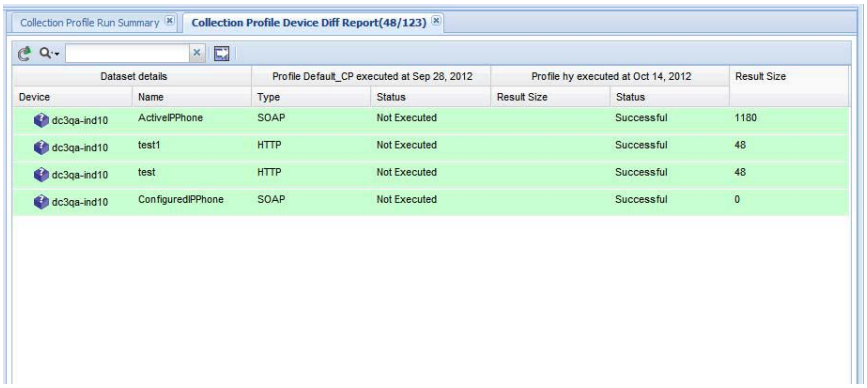
選択した実行間の相違点を表示するには、図 8-25 に示すように [選択した実行間の相違点を表示（Show Differences between selected Runs）] オプションを選択します。

図 8-25　　[選択した実行間の相違点表示（Show Differences between selected Runs）]



2 つの異なる実行を選択すると、それぞれの実行間で変化した内容を差異レポートで確認できます。このレポートでは、変更点が（緑：追加、赤：削除、青：変更）に色分けされて正確に表示されます。

図 8-26　　2 つの収集プロファイル実行間の相違点

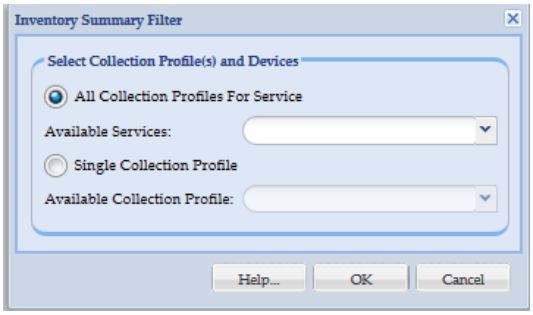


CSPC フローチャートに戻る

[収集実行結果サマリーの表示（View Collection Run Summary）]

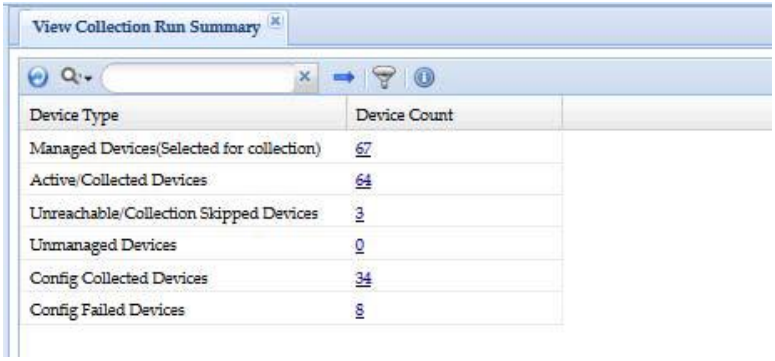
[収集実行結果サマリー（Collection Run Summary）] レポートには、インベントリのサマリーが表示されます。[サービスのすべての収集プロファイル（All Collection Profiles for Service）] または [単一の収集プロファイル（Single Collection Profile）] を表示できます。収集プロファイルとデバイスを表示するにはオプションを選択します。図 8-27 に示すように、[利用可能なサービス（Available Services）] と [利用可能な収集プロファイル（Available Collection Profile）] ドロップ ダウン ボックスで、利用可能なサービスを選択して [OK] をクリックします。

図 8-27　　[インベントリ サマリー フィルタ（Inventory Summary Filter）] の表示



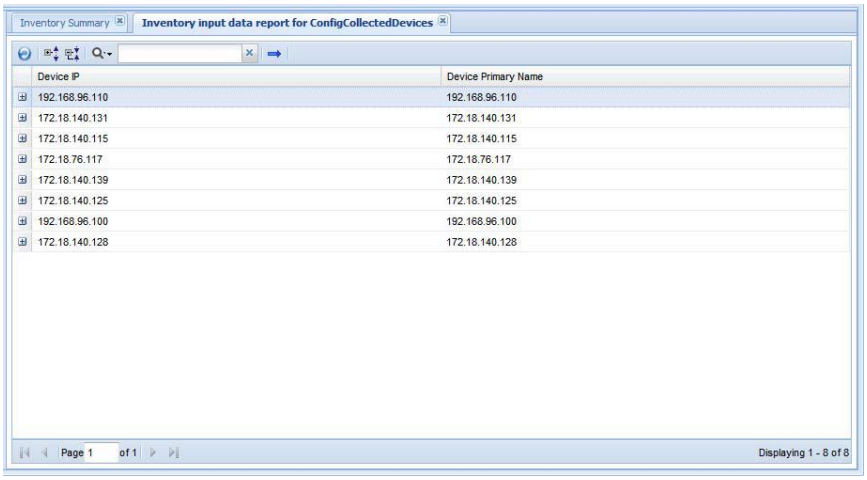
[収集実行結果サマリーの表示（View Collection Run Summary）] 画面が表示されます。この画面には、図 8-28 に示すように [デバイス タイプ（Device Type）] と [デバイス数（Device Count）] の一覧が表示されます。

図 8-28　　[収集実行結果サマリーの表示（View Collection Run Summary）]



[デバイス数（Device Count）] をクリックすると、図 8-29 に示すように、該当するデバイスの [インベントリ入力データ レポート（Inventory Input Data Report）] が表示されます。

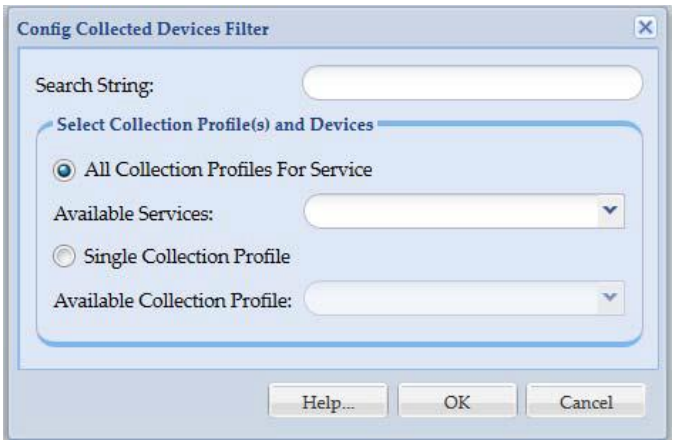
図 8-29　　[インベントリ入力データ レポート（Inventory Input Data Report）]



[設定収集済みデバイス（Config Collected Devices）]

収集プロファイルとデバイスをフィルタリングして表示できます。[検索文字列（Search String）] にフィルタ値を入力して設定収集済みデバイスを表示することもできます。

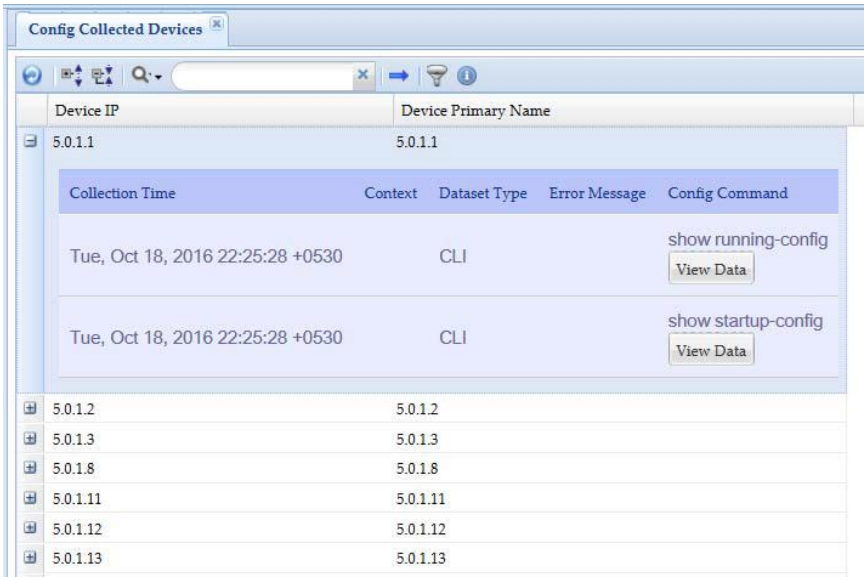
図 8-30　　[設定収集済みデバイス フィルタ（Config Collected Devices Filter）] の表示



[設定収集済みデバイス（Config Collected Devices）] 画面が表示されます。この画面には、図 8-31 に示すように [デバイス IP（Device IP）] と [デバイス プライマリ名（Device Primary Name）] の一覧が表示されます。

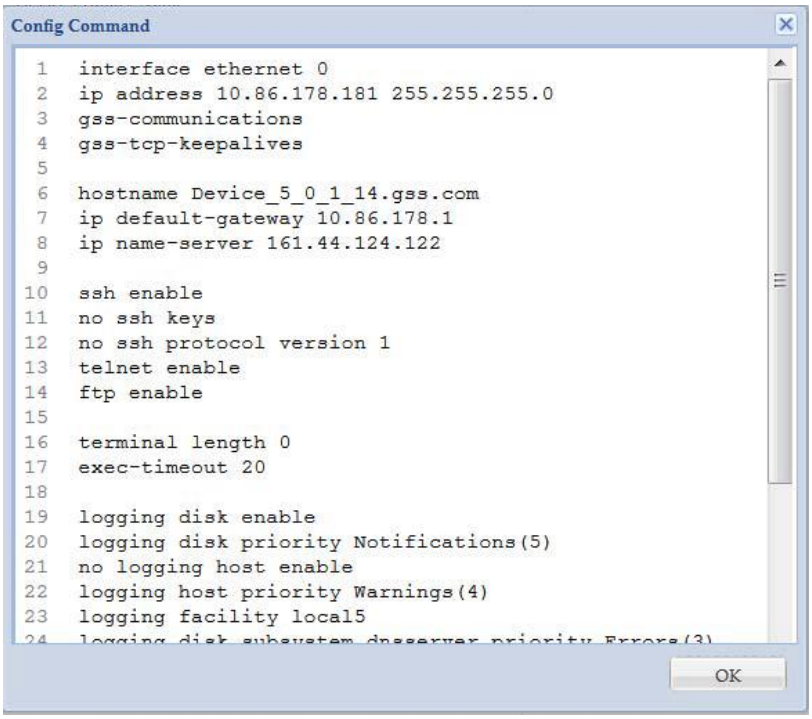
また、[デバイス IP（Device IP）] の横にある [+] 記号をクリックすれば、各デバイスの詳細を表示できます。詳細には、選択したデバイスの [収集日時（Collection Time）]、[コンテキスト（Context）]、[データセット タイプ（Dataset Type）]、[エラー メッセージ（Error Message）]、[設定コマンド（Config Command）] が表示されます。

図 8-31　　[設定収集済みデバイス（Config Collected Devices）]



レポートの [データの表示（View Data）] をクリックすると、選択したデバイスの [設定コマンド（Config Command）] が表示されます。図 8-32 には [設定コマンド（Config Command）] の詳細が示されています。

図 8-32　　[設定コマンド（Config Command）]



[デバイスごとの設定データ（Config Data Per Device）]

[デバイスごとの設定データ（Config Data Per Devices）] レポートには、CSP Collector によって収集された設定が表示されます。収集プロファイルに基づいて設定を選択できます。次に示すように、必要な情報を指定することで [デバイスごとの設定データ フィルタ（Config Data Per Device Filter）] を設定できます。

図 8-33　　[デバイスごとの設定データ フィルタ（Config Data Per Device Filter）]

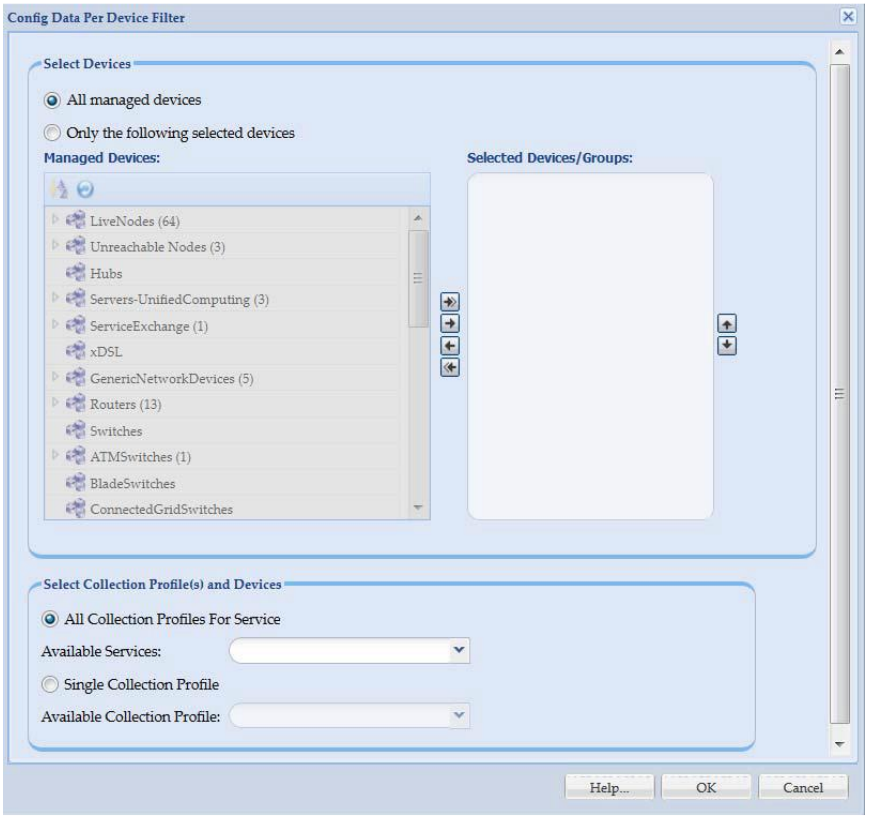


図 8-34 に示すように、指定したデバイスの設定データが処理されます。[データを表示（View Data）] をクリックすると、指定したデバイスの収集済み設定データが表示されます。

図 8-34 収集された設定データ

[サービス レポート（Services Reports）]

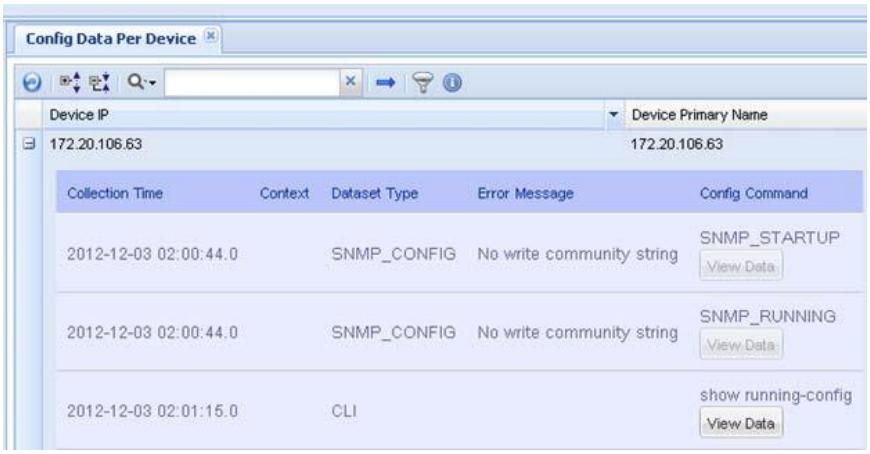
[アラート（Alerts）]

このレポートには、すべてのアラートの一覧が表示されます。イベント ID、モジュール、イベントの時刻、重大度、およびメッセージと [詳細を表示（View Details）] ボタンが表示されます。CSPC システムで 14 日以上経過したアラートは消去されます。

アラートには、UI 通知アラートと電子メール アラートの 2 種類があります。

- UI 通知アラートは、通知を受信すると UI として表示されます。
- 電子メール アラートは、登録済みの電子メール アドレスに電子メールで送信されるアラートです。

図 8-35　　[アラート（Alerts）]



[SNMP トラップ レポート（SNMP Trap Report）]

このレポートには、トラップの一覧がデバイス、通知タイプ、トラップ データ、および受信時刻別にソートされて表示されます。[SNMP トラップ レポート（SNMP Trap Report）] を生成するには、次の手順を実行します。

ステップ 1 ドロップダウンから [トラップの受信時刻（Trap Received Time）] を選択します。

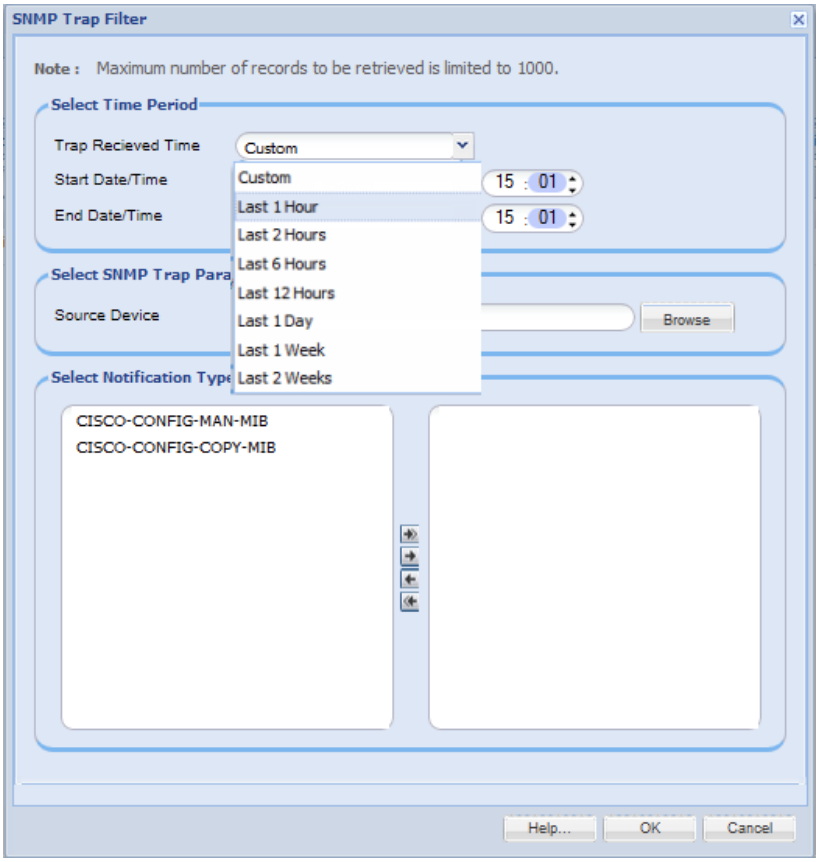
- [カスタム（Custom）] を選択した場合は、[開始日時（Start Date/Time）] と [終了日時（End Date/Time）] を入力します。

ステップ 2 [送信元デバイス（Source Device）] を参照して選択します。

ステップ 3 [通知タイプ（Notification Types）] を選択します。

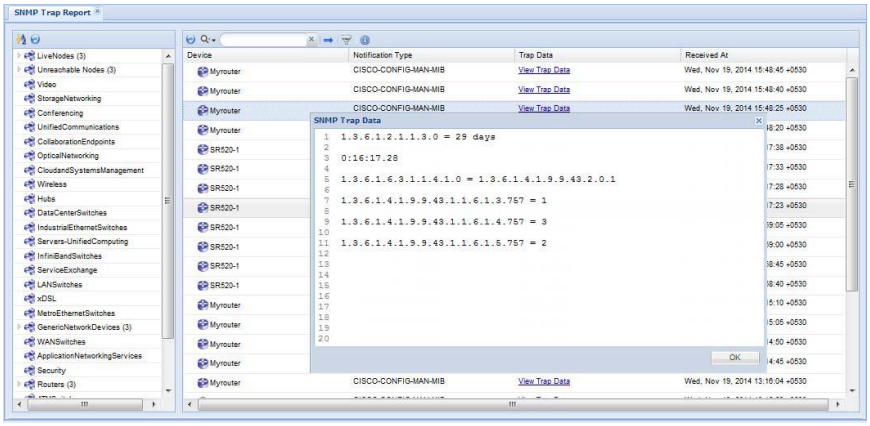
ステップ 4 [OK] をクリックします。

図 8-36　　[SNMP トラップ フィルタ（SNMP Trap Filter）]



トラップ データを表示するには、[トラップ データの表示（View Trap Data）] をクリックします。

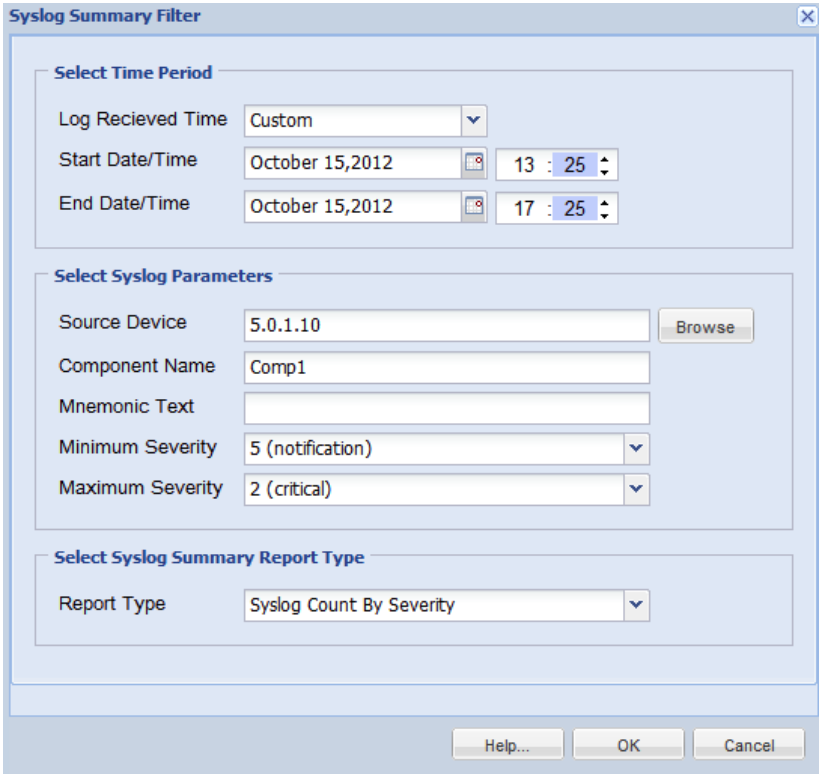
図 8-37　　SNMP レポート



[Syslog サマリー（Syslog Summary）]

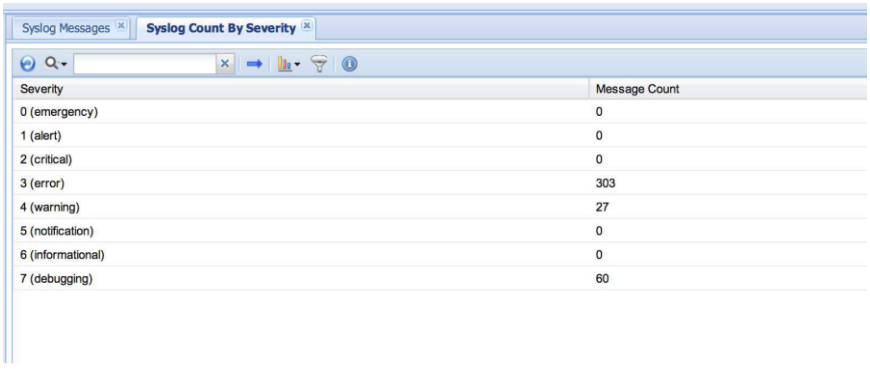
[Syslog サマリー（Syslog Summary）] レポートには、CSPC によって収集されたすべての Syslog のサマリーが表示されます。図 8-38 に示すように、ログの受信日時、重大度に基づくサマリーを表示するかどうかなどのフィルタリング情報を入力する必要があります。

図 8-38　　[Syslog サマリー フィルタ（Syslog Summary Filter）]



フィルタを選択すると、フィルタと一致するサマリー レポートが表示されます。

図 8-39　　[Syslog サマリー（Syslog Summary）]



[Syslog メッセージ（Syslog Messages）]

[Syslog メッセージ（Syslog Messages）] レポートには、CSPC によって収集されたすべての Syslog が表示されます。[Syslog サマリー（Syslog Summary）] レポートと同様、詳細な Syslog メッセージ レポートを作成する前に適用する必要があるフィルタを指定する必要があります。

図 8-40　　[Syslog フィルタ（Syslog Filter）]

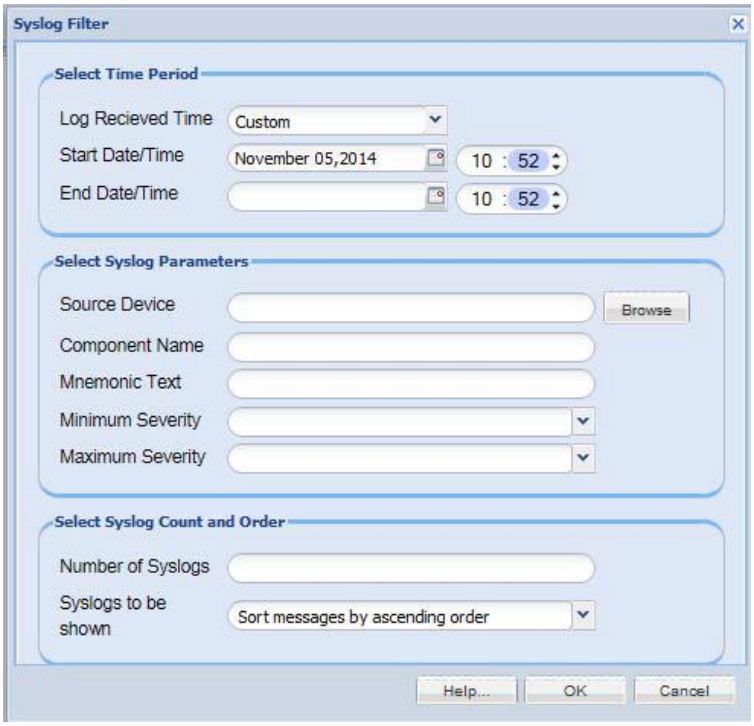
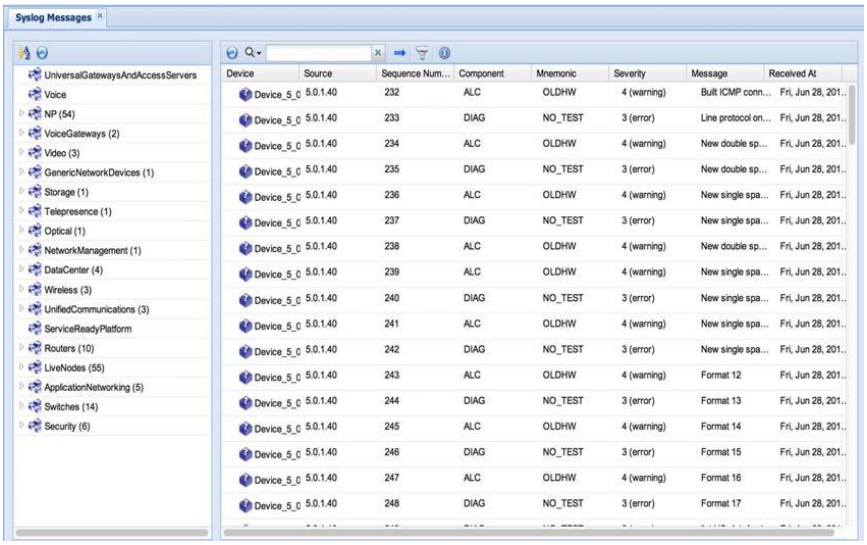


図 8-41　　[Syslog メッセージ（Syslog Messages）]



ジョブ レポート

[ジョブ ログ レポート（Job Log Reports）] サブ タブでは、CSP Collector を使用して実行したさまざまな操作に関する収集済みのログを表示できます。

この項では、[レポート（Reports）] オプションの以下の項目について説明します。

- [検出ジョブ（Discovery Jobs）]
- [インベントリ ジョブ（Inventory Jobs）]
- [ジョブ管理レポート（Job Management Reports）]

[検出ジョブ（Discovery Jobs）]

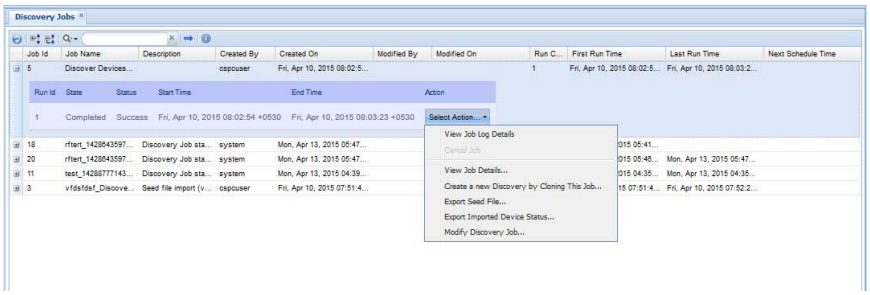
[検出ジョブ（Discovery Jobs）] レポートには、実行したすべてのネットワーク デバイス検出ジョブに関する情報が含まれています。

また、[ジョブ ID（Job ID）] の隣にある [+] 記号をクリックして、各ジョブの説明を確認できます。[+] 記号をクリックすると、そのジョブの [実行 ID（Run Id）]、[状態（State）]（[成功（Successful）]/[中止（Aborted）]）、[ステータス（Status）]（[完了（Completed）]/[未完了（Not Completed）]）、[開始時刻（Start Time）]、[終了時刻（End Time）]、
および [ジョブ ログの詳細（Job Log Details）] が表示されます。

[ジョブの詳細を表示（View Job Details）]->[ジョブをキャンセル（Cancel Job）] ボタンを使用して、ジョブをキャンセルできます。

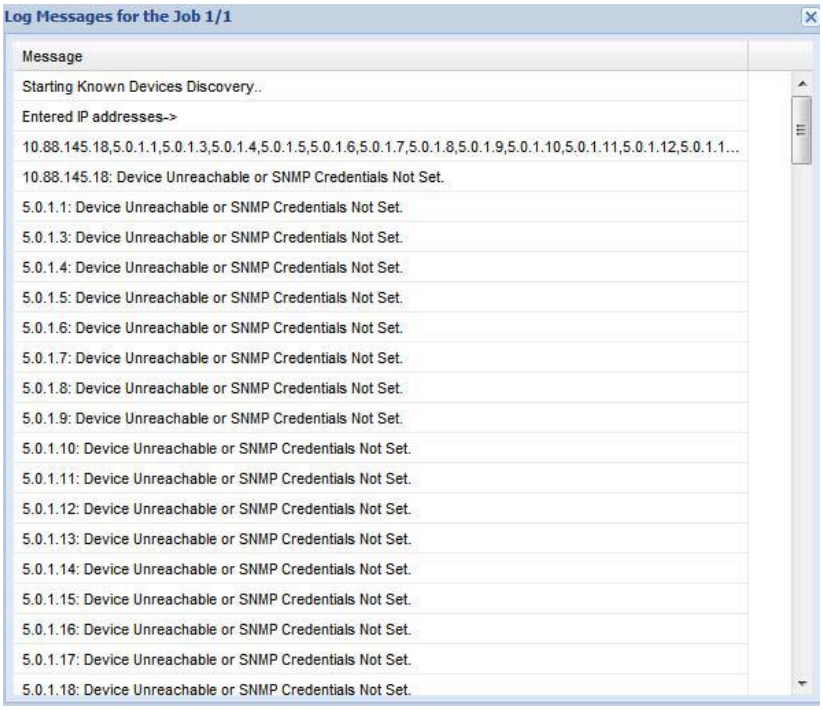
これらの詳細情報は、すべての*ジョブ レポート*に共通です。

図 8-42　　[検出ジョブ（Discovery Jobs）]



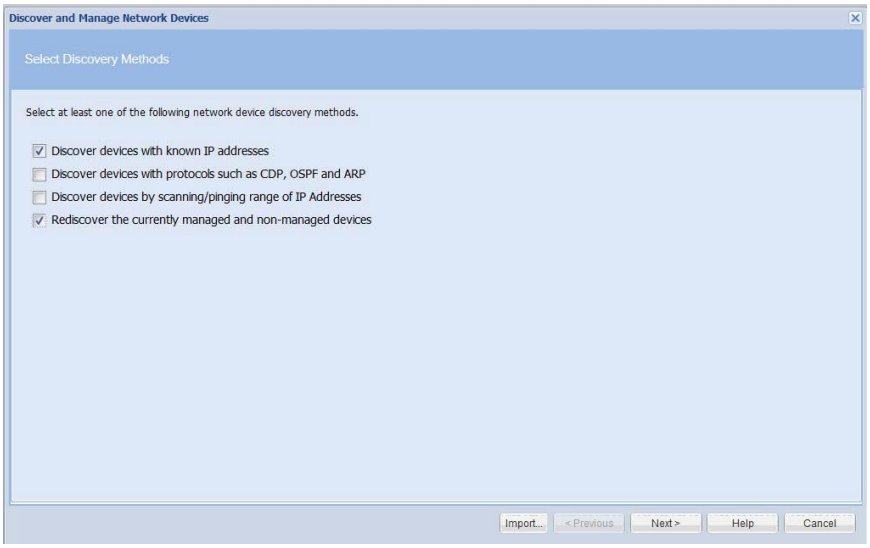
レポート内にある [アクション（Action）] ボタンを選択して、そのジョブのジョブ ログの詳細を表示するか、またはジョブ自体（検出に指定されていたオプションなど）を表示します。また、この検出ジョブのクローンを作成して、新しいジョブを作成することができます。図 8-43 はジョブ ログの詳細を示しています。また、シード ファイルをエクスポートしたり、インポートされたデバイスのステータスをエクスポートしたりすることもできます。インポートされたデバイスのステータスを確認するには、検出ジョブの ID とジョブの実行 ID に基づいてレポートの生成やエクスポートを行います。インポートされたデバイスのステータスを「*ImportedDeviceStatus_jobid_jobrunid.csv*」という名前の *.csv* ファイルにエクスポートするには、[インポートされたデバイスのステータスをエクスポート（Export Imported Devices Status）] をクリックします。

図 8-43　　ジョブ ログの詳細



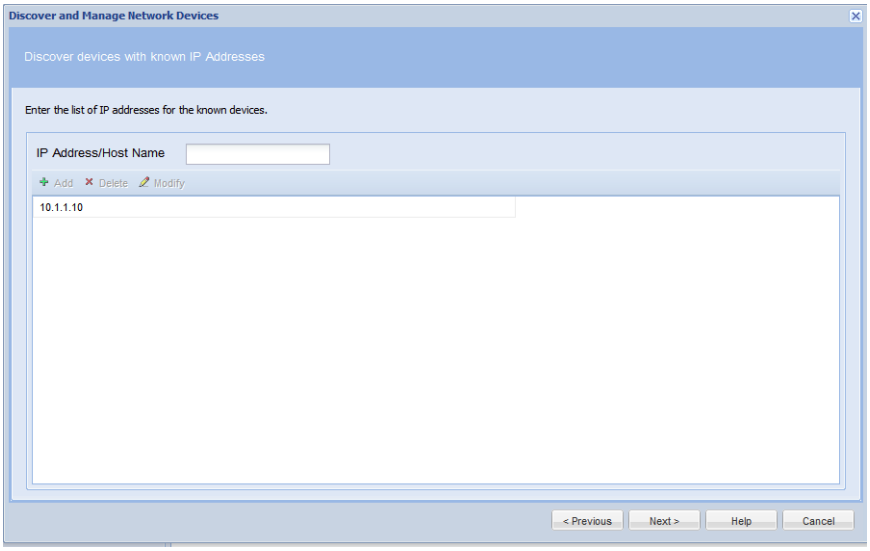
[クローンを作成（Cloning）] または [検出ジョブを変更（Modify Discovery Job）] オプションを選択すると、すでに完了している実際のジョブが表示され、そのジョブを変更して別のジョブを作成することができます。

図 8-44　　この検出ジョブのクローンを作成



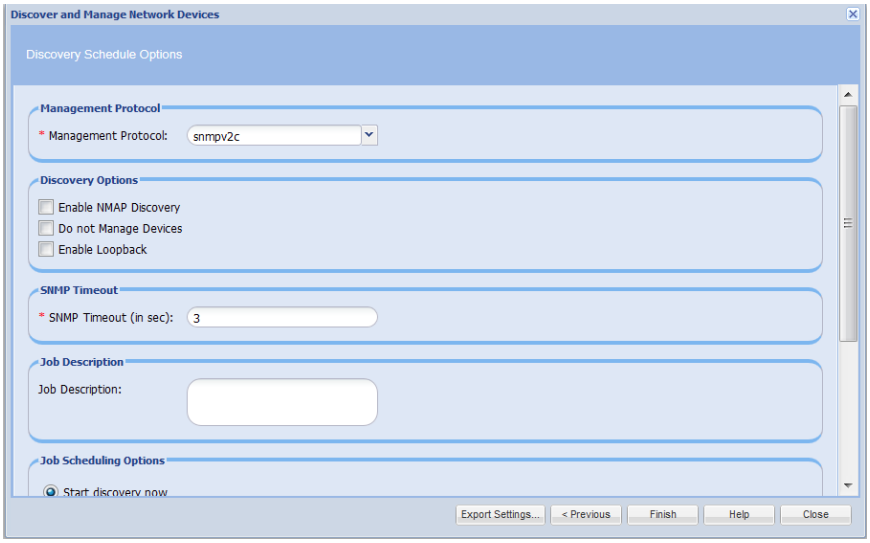
[次へ（Next）] ボタンをクリックして、[IP アドレス/ホスト名（IP Address/Host Name）] を入力します。

図 8-45　　[既知の IP アドレスを使用したデバイスの検出（Discover Devices using Known IP Addresses）]



検出スケジュール オプションを設定するには、[次へ（Next）] ボタンをクリックします。

図 8-46　　[検出スケジュール オプション（Discovery Schedule Options）]

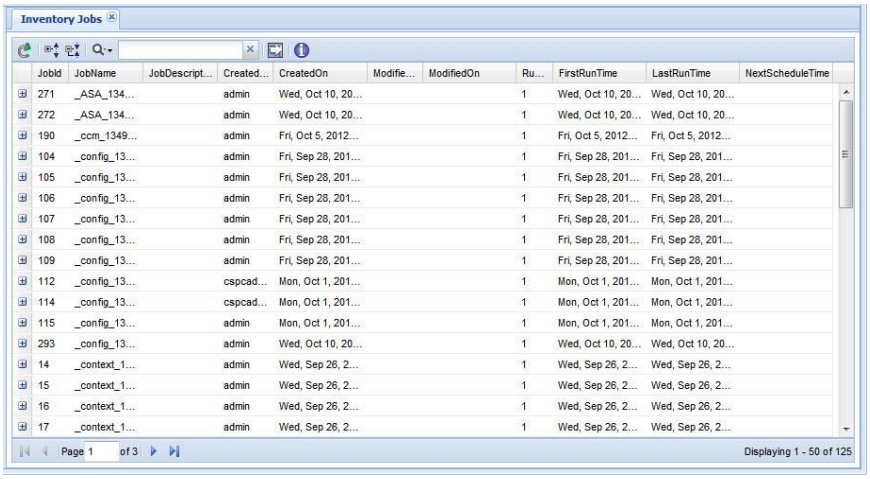


[インベントリ ジョブ（Inventory Jobs）]

このレポートには、実行したすべてのネットワーク デバイス インベントリ ジョブが含まれています。

また、[ジョブ ID（Job ID）] の隣にある [+] 記号をクリックして、各ジョブの説明を確認できます。[+] 記号をクリックすると、次の図に示すように、そのジョブの [実行 ID（Run Id）]、[状態（State）]（[成功（Successful）]/[中止（Aborted）]）、[ステータス（Status）]（[完了（Completed）]/[未完了（Not Completed）]）、[開始時刻（Start Time）]、[終了時刻（End Time）]、および [ジョブ ログの詳細（Job Log Details）] が表示されます。

図 8-47　　[インベントリ ジョブ（Inventory Jobs）] のメイン ウィンドウ

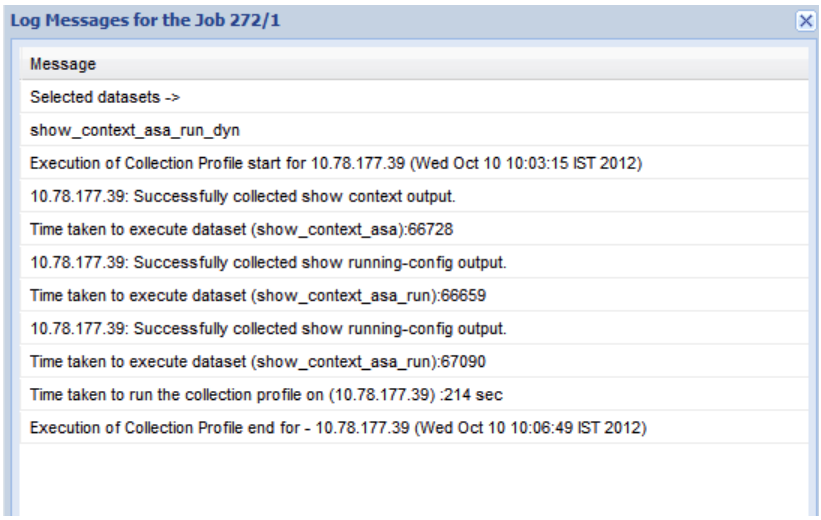


レポート内にある [アクション（Action）] ボタンを選択して、そのジョブのジョブ ログの詳細を表示するか、または実行中のジョブをキャンセルします。[ジョブを一時停止（Pause Job）] オプションと [ジョブを再開（Resume Job）] オプションを使用すると、実行中のジョブを一時停止して後で再開できます。

[失敗したデータセットを再収集（Recollect Failed Datasets）] オプションを選択すると、以前にエラーが表示されたデバイスのデータのみが収集されます。データの収集が完了すると、他のデータとマージされてからシスコに送信されます。

図 8-48 はジョブ ログの詳細を示しています。

図 8-48　　ジョブ ログの詳細



[ジョブ管理レポート（Job Management Reports）]

[ジョブ管理レポート（Job Management Reports）] オプションには、検出ジョブとインベントリ ジョブを除く、サポートされているすべてのジョブが含まれていて、それらのジョブを選択できます。

[ジョブ管理レポート（Job Management Reports）] では、サポートされているすべてのジョブ レポートを選択できます。[ジョブ グループ タイプ（Job Group Type）] ドロップダウン リストから任意のジョブを選択して指定したジョブ レポートを表示できます。また、[ジョブ ID（Job ID）] の隣にある [+] 記号をクリックして、各ジョブの説明を確認できます。[+] 記号をクリックすると、そのジョブの [実行 ID（Run Id）]、[状態（State）]（[成功（Successful）]/[中止（Aborted）]）、[ステータス（Status）]（[完了（Completed）]/[未完了（Not Completed）]）、[開始時刻（Start Time）]、[終了時刻（End Time）]、および [ジョブ ログの詳細（Job Log Details）] が表示されます。

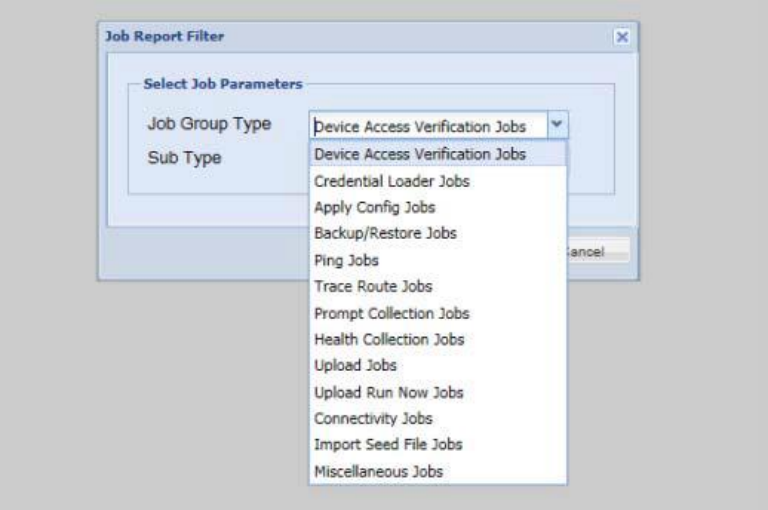
レポート内にある [アクション（Action）] ボタンを選択して、そのジョブのジョブ ログの詳細を表示するか、または実行中のジョブをキャンセルします。

現在サポートされているジョブは次のとおりです。

- [デバイス アクセス検証ジョブ（Device Access Verification Jobs）]
- [クレデンシャル ローダー ジョブ（Credential Loader Jobs）]
- [設定の適用ジョブ（Apply Config Jobs）]
- [バックアップおよび復元ジョブ（Backup and Restore Jobs）]
- [ping ジョブ（Ping Jobs）]
- [トレース ルート ジョブ（Trace Route Jobs）]
- [プロンプト収集ジョブ（Prompt Collection Jobs）]
- [ヘルス収集ジョブ（Health Collection Jobs）]
- [アップロード ジョブ（Upload Jobs）]
- [直ちにアップロードを実行ジョブ（Upload Run Now Jobs）]
- [接続ジョブ（Connectivity Jobs）]
- [シード ファイルのインポート ジョブ（Import Seed File Jobs）]
- [その他のジョブ（Miscellaneous Jobs）]

[ジョブ管理レポート（Job Management Reports）] ウィンドウを開いたら、表示するジョブを選択して [OK] をクリックします。各ジョブの詳細については、以下を参照してください。ジョブには、スケジュール ジョブと未スケジュール ジョブがあります。ジョブを編集するには、目的のジョブを右クリックして [ジョブ スケジュールを編集（Edit Job Schedule）] オプションを選択します。

図 8-49　　[ジョブ管理レポート（Job Management Reports）]

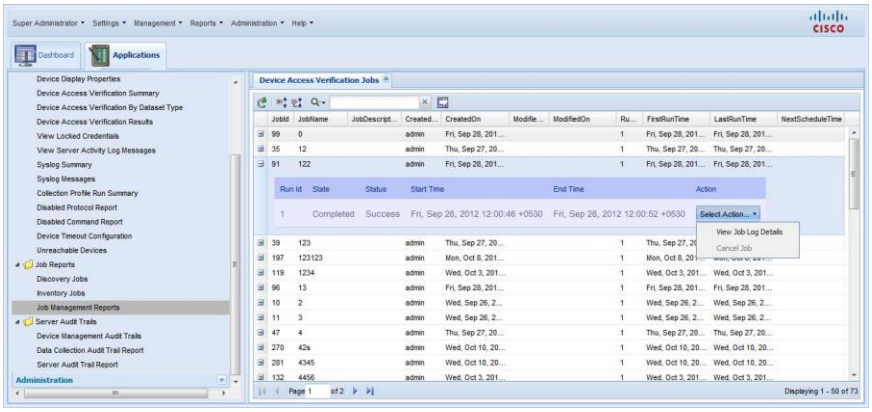


[デバイス アクセス検証ジョブ（Device Access Verification Jobs）]

[デバイス アクセス検証ジョブ（Device Access Verification Jobs）] レポートには、実行したすべてのネットワーク デバイス検証ジョブが含まれています。

また、[ジョブ ID（Job ID）] の隣にある [+] 記号をクリックして、各ジョブの説明を確認できます。図 8-50 に示すように、[+] 記号をクリックすると、そのジョブの [実行 ID（Run Id）]、[状態（State）]（[成功（Successful）]/[中止（Aborted）]）、[ステータス（Status）]（[完了（Completed）]/[未完了（Not Completed）]）、[開始時刻（Start Time）]、[終了時刻（End Time）]、および [ジョブ ログの詳細（Job Log Details）] が表示されます。

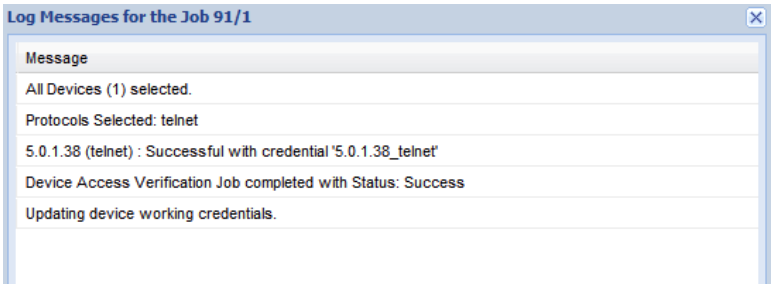
図 8-50　　[デバイス アクセス検証ジョブ（Device Access Verification Jobs）] メイン ウィンドウ



レポート内にある [アクション（Action）] ボタンを選択して、そのジョブのジョブ ログの詳細を表示するか、または実行中のジョブをキャンセルします。

図 8-51 はジョブ ログの詳細を示しています。

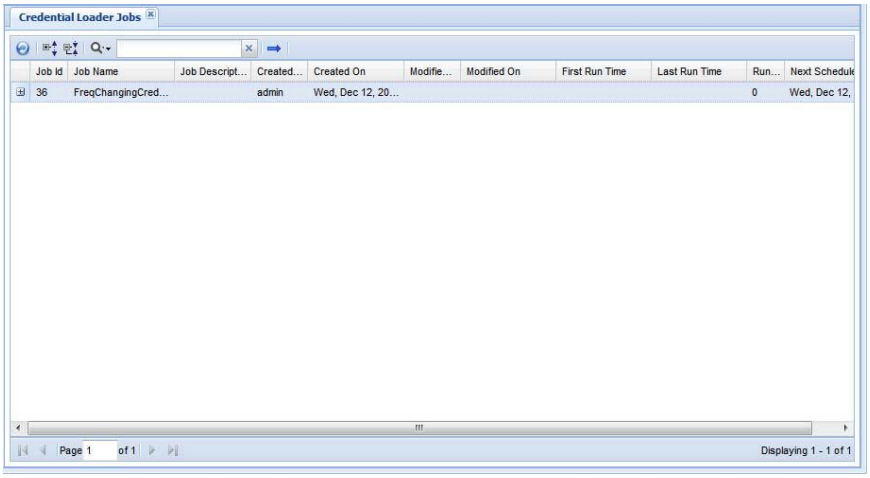
図 8-51　　ジョブ ログの詳細



[クレデンシャル ローダー ジョブ（Credential Loader Jobs）]

[クレデンシャル ローダー ジョブ（Credential Loader Jobs）] では、[変更されているクレデンシャルのインポート（Changing Credential Import）] を使用して実行または作成したすべてのジョブを確認できます。

図 8-52　　[クレデンシャル ローダー ジョブ（Credential Loader Jobs）]



ジョブには、スケジュール ジョブと未スケジュール ジョブがあり、ジョブ名を右クリックすると編集できます。

また、[ジョブ ID（Job ID）] の隣にある [+] 記号をクリックして、各ジョブの説明を確認できます。[+] 記号をクリックすると、そのジョブの [実行 ID（Run Id）]、[状態（State）]（[成功（Successful）]/[中止（Aborted）]）、[ステータス（Status）]（[完了（Completed）]/[未完了（Not Completed）]）、[開始時刻（Start Time）]、[終了時刻（End Time）] が表示されます。

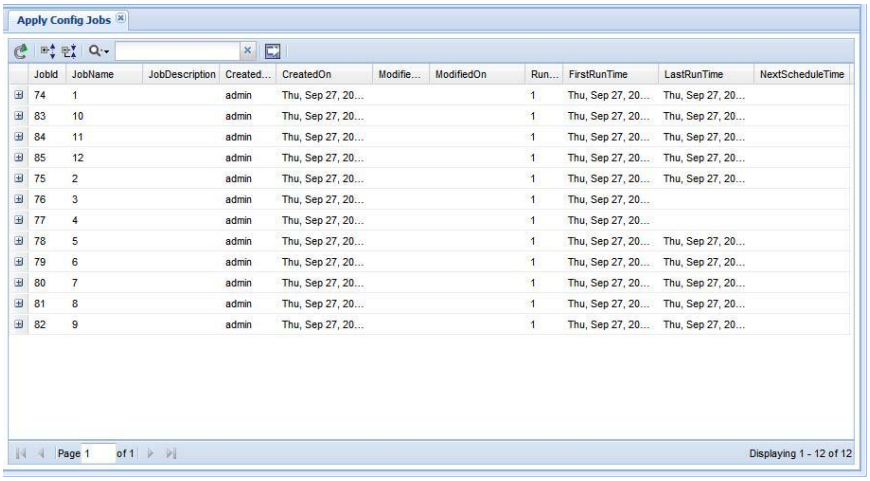
[設定の適用ジョブ（Apply Config Jobs）]

[設定の適用ジョブ（Apply Config Jobs）] レポートでは、CSP Collector から適用された設定ジョブを確認できます。すべてのジョブ、ジョブ作成者などを確認できます。

また、[ジョブ ID（Job ID）] の隣にある [+] 記号をクリックして、各ジョブの説明を確認できます。図 8-53 に示すように、[+] 記号をクリックすると、そのジョブの [実行 ID（Run Id）]、[状態（State）]（[成功（Successful）]/[中止（Aborted）]）、[ステータス（Status）]（[完了（Completed）]/[未完了（Not Completed）]）、[開始時刻（Start Time）]、[終了時刻（End Time）]、および [ジョブ ログの詳細（Job Log Details）] が表示されます。

ジョブには、スケジュール ジョブと未スケジュール ジョブがあり、ジョブ名を右クリックすると編集できます。

図 8-53　　[設定の適用ジョブ（Apply Config Jobs）]



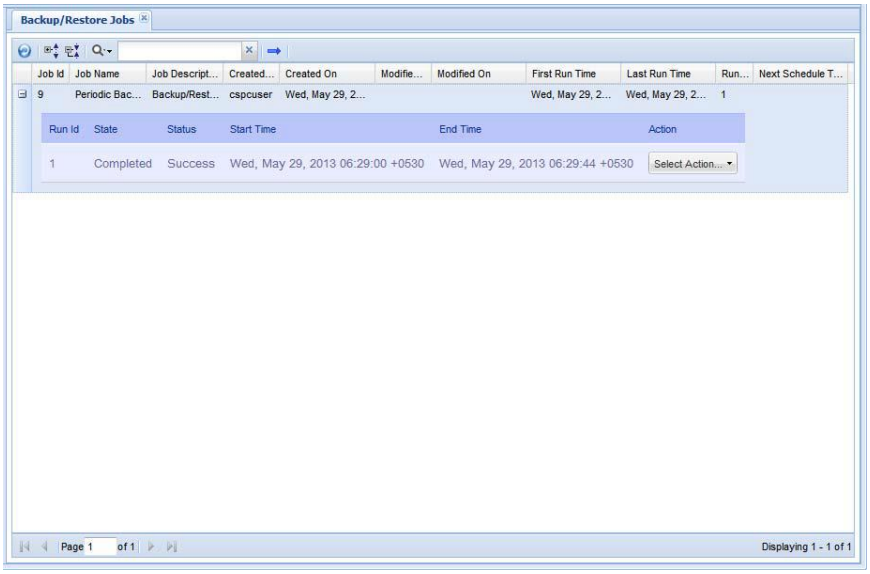
[バックアップおよび復元ジョブ（Backup and Restore Jobs）]

[バックアップおよび復元ジョブ（Backup and Restore Jobs）] レポートでは、CSP Collector に適用されたバックアップ ジョブと復元ジョブを確認できます。すべてのジョブ、ジョブ作成者などを確認できます。

また、[ジョブ ID（Job ID）] の隣にある [+] 記号をクリックして、各ジョブの説明を確認できます。[+] 記号をクリックすると、次の図に示すように、そのジョブの [実行 ID（Run Id）]、[状態（State）]（[成功（Successful）]/[中止（Aborted）]）、[ステータス（Status）]（[完了（Completed）]/[未完了（Not Completed）]）、[開始時刻（Start Time）]、[終了時刻（End Time）]、および [ジョブ ログの詳細（Job Log Details）] が表示されます。

ジョブには、スケジュール ジョブと未スケジュール ジョブがあり、ジョブ名を右クリックすると編集できます。

図 8-54　　[バックアップおよび復元ジョブ（Backup and Restore Jobs）]



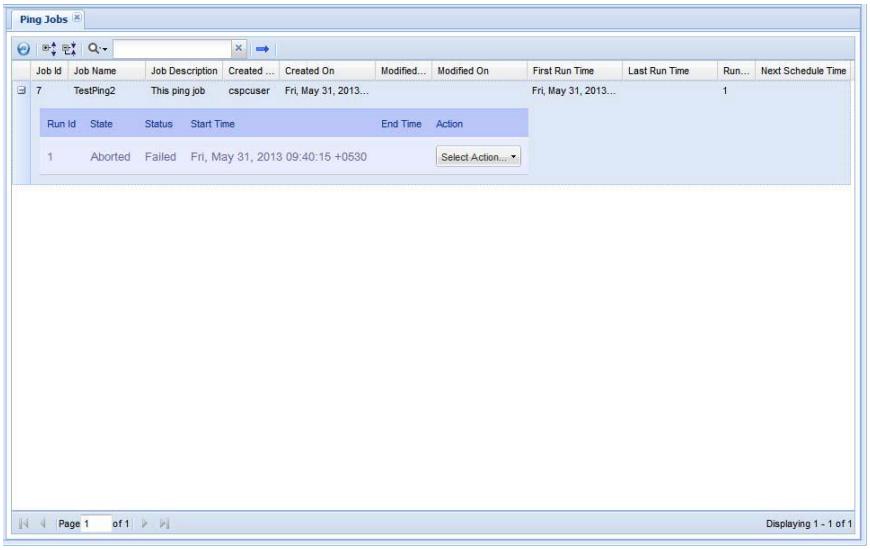
[ping ジョブ（Ping Jobs）]

[ping ジョブ（Ping Jobs）] では、XML API インターフェイスから CSP Collector に適用された ping ジョブを確認できます。

また、[ジョブ ID（Job ID）] の隣にある [+] 記号をクリックして、各ジョブの説明を確認できます。[+] 記号をクリックすると、次の図に示すように、そのジョブの [実行 ID（Run Id）]、[状態（State）]（[成功（Successful）]/[中止（Aborted）]）、[ステータス（Status）]（[完了（Completed）]/[未完了（Not Completed）]）、[開始時刻（Start Time）]、[終了時刻（End Time）]、および [ジョブ ログの詳細（Job Log Details）] が表示されます。

ジョブには、スケジュール ジョブと未スケジュール ジョブがあり、ジョブ名を右クリックすると編集できます。

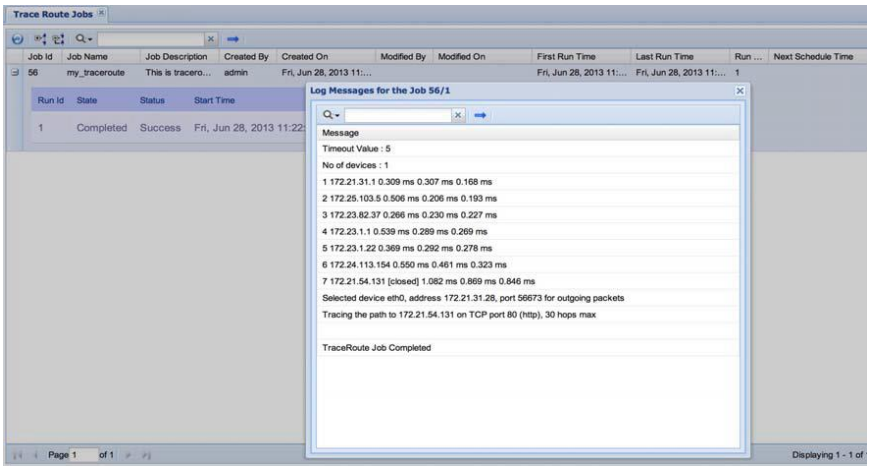
図 8-55　　[ping ジョブ（Ping Jobs）]



[トレース ルート ジョブ（Trace Route Jobs）]

[トレース ルート ジョブ（Trace Route Jobs）] では、CSP Collector で実行されたすべてのトレース ルート ジョブを確認できます。

図 8-56　　[トレース ルート ジョブ（Trace Route Jobs）]



[ジョブ ID（Job ID）] の隣にある [+] 記号をクリックして、各ジョブの説明を確認できます。[+] 記号をクリックすると、そのジョブの [実行 ID（Run Id）]、[状態（State）]（[成功（Successful）]/[中止（Aborted）]）、[ステータス（Status）]（[完了（Completed）]/[未完了（Not Completed）]）、[開始時刻（Start Time）]、[終了時刻（End Time）]、および [ジョブ ログの詳細（Job Log Details）] が表示されます。

ジョブには、スケジュール ジョブと未スケジュール ジョブがあり、ジョブ名を右クリックすると編集できます。

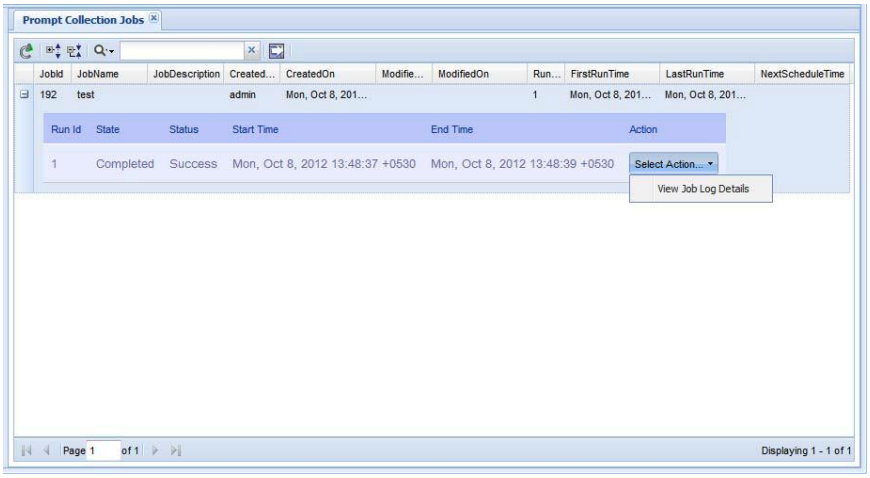
[プロンプト収集ジョブ（Prompt Collection Jobs）]

[プロンプト収集ジョブ（Prompt Collection Jobs）] レポートには、実行したすべてのプロンプト収集ジョブが含まれています。

また、[ジョブ ID（Job ID）] の隣にある [+] 記号をクリックして、各ジョブの説明を確認できます。[+] 記号をクリックすると、次の図に示すように、そのジョブの [実行 ID（Run Id）]、[状態（State）]（[成功（Successful）]/[中止（Aborted）]）、[ステータス（Status）]（[完了（Completed）]/[未完了（Not Completed）]）、[開始時刻（Start Time）]、[終了時刻（End Time）]、および [ジョブ ログの詳細（Job Log Details）] が表示されます。

ジョブには、スケジュール ジョブと未スケジュール ジョブがあり、ジョブ名を右クリックすると編集できます。

図 8-57　　[プロンプト収集ジョブ（Prompt Collection Jobs）]



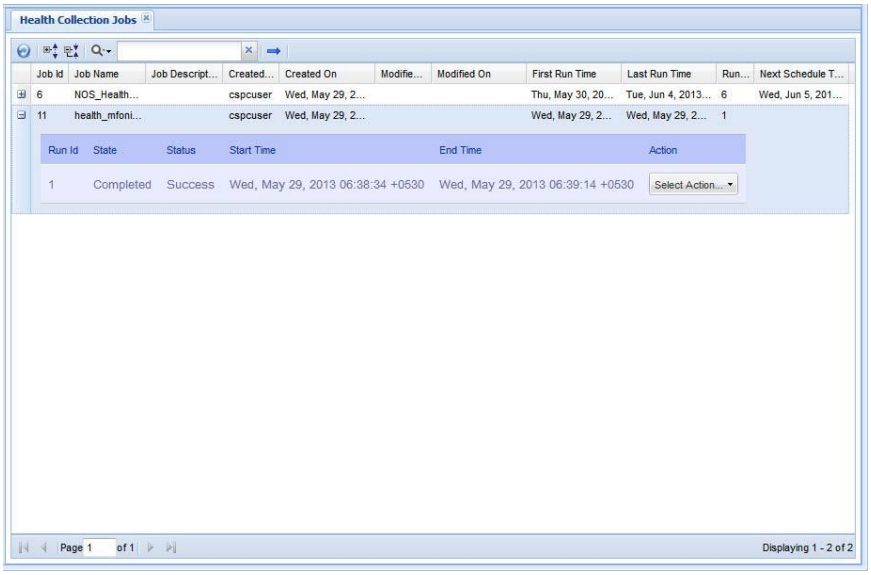
[ヘルス収集ジョブ（Health Collection Jobs）]

[ヘルス収集ジョブ（Health Collection Jobs）] レポートには、CSPC で実行された [ヘルス モニタ ジョブ（Health Monitor jobs）] がすべて含まれています。また、[ジョブ ID（Job ID）] の隣にある [+] 記号をクリックして、各ジョブの説明を確認できます。[+] 記号をクリックすると、そのジョブの [実行 ID（Run Id）]、[状態（State）]（[成功（Successful）]/[中止（Aborted）]）、[ステータス（Status）]（[完了（Completed）]/[未完了（Not Completed）]）、[開始時刻（Start Time）]、

[終了時刻（End Time）]、および [ジョブ ログの詳細（Job Log Details）] が表示されます（図 8-58 参照）。

ジョブには、スケジュール ジョブと未スケジュール ジョブがあり、ジョブ名を右クリックすると編集できます。

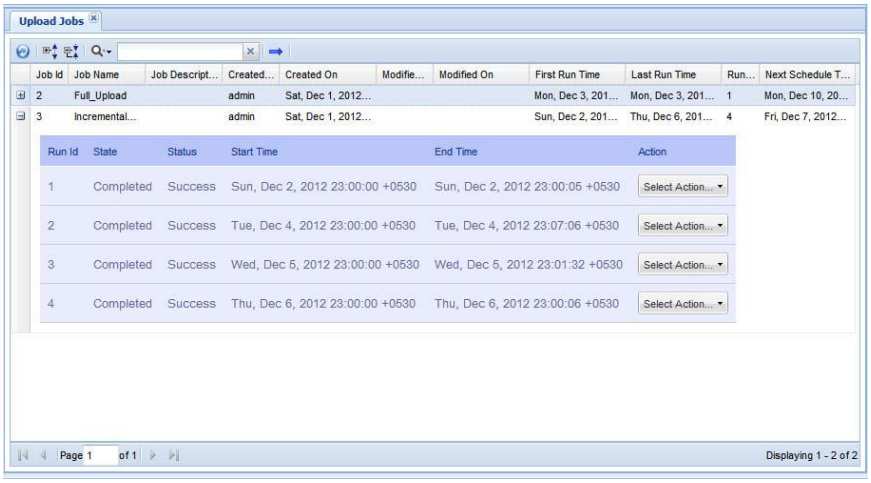
図 8-58　　[ヘルス収集ジョブ（Health Collection Jobs）]



[アップロード ジョブ（Upload Jobs）]

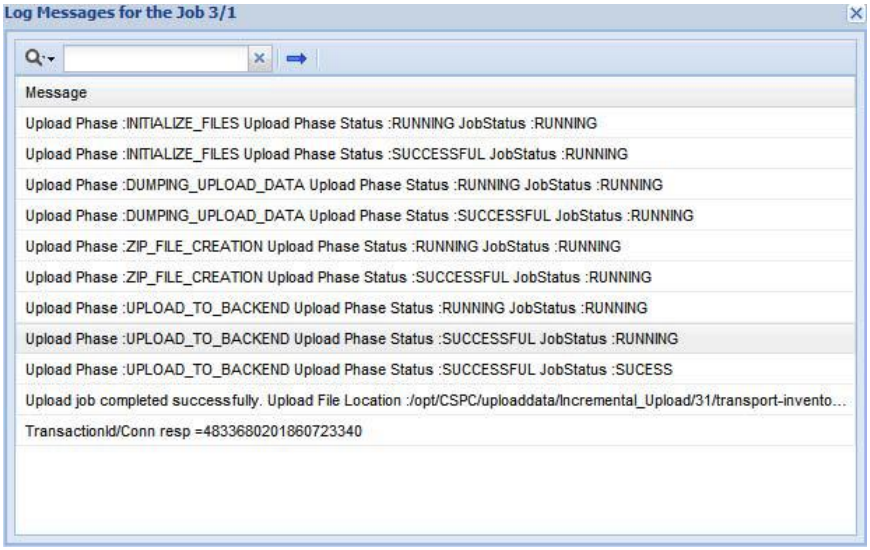
[アップロード ジョブ（Upload Jobs）] レポートでは、アップロード プロファイルでスケジュールされているすべてのジョブと、ユーザが定義し、システムによって作成されたアップロード ジョブを確認できます。ジョブのスケジュールを解除したり、既存のジョブ スケジュールを編集したりできます。また、アップロードされたジョブのステータスを確認したり、ジョブ ログの詳細を表示したり、実行中のジョブをキャンセルしたりすることもできます。

図 8-59　　[アップロード ジョブ（Upload Jobs）]



アップロードされたジョブのステータスを確認するには、[ジョブ ID（Job ID）] の隣にある [+] 記号をクリックします。ジョブのステータスは、上の図に示すようにデータや時刻と一緒に表示されます。図 8-60 に示したジョブ ログの詳細を表示するには、[アクションの選択（Select Action）] ボタンをクリックし、[ジョブ ログの詳細を表示（View Job Log Details）] をクリックします。

図 8-60　　[ジョブ ログの詳細を表示（View Job Log Details）]



スケジュールされたアップロードを実行しない場合は、ジョブを右クリックして [ジョブのスケジュール

を解除（Unschedule Job）] ボタンをクリックします。

図 8-61　　[ジョブのスケジュールを解除（Unschedule Job）]/[ジョブ スケジュールの編集（Edit Job Schedule）]

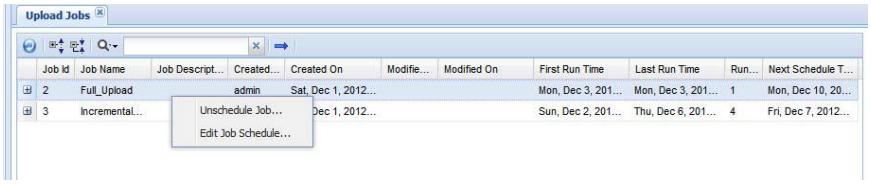
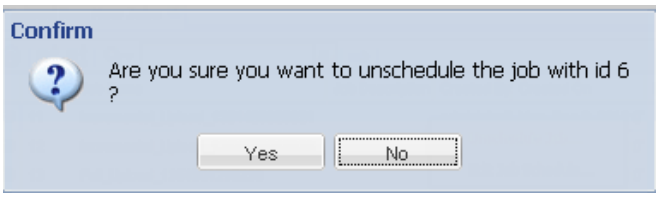


図 8-62 に示すような、確認用のダイアログボックスが表示されます。

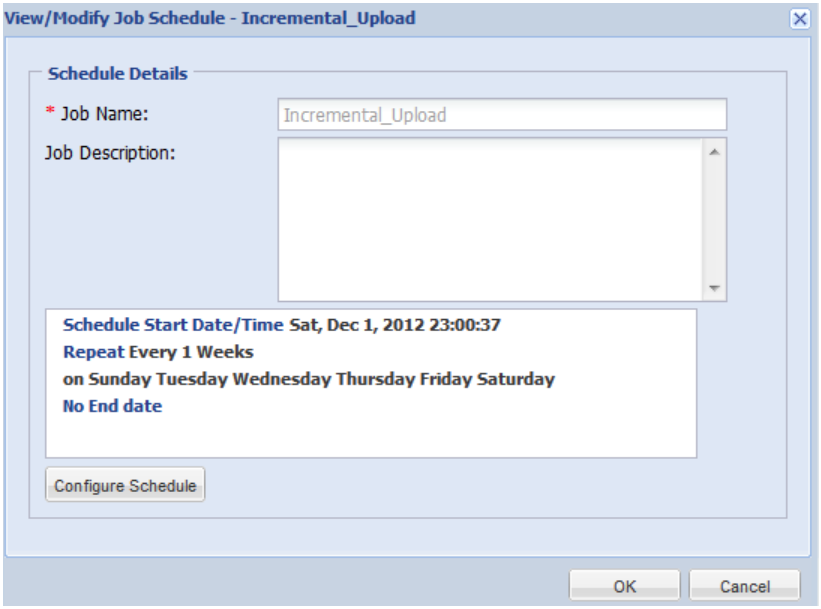
図 8-62　　ジョブのスケジュール解除



[はい（Yes）] をクリックしてジョブのスケジュールを解除します。

既存のアップロード ジョブのスケジュールを編集する場合は、ジョブを右クリックして [ジョブのスケジュールを編集（Edit Job Schedule）] ボタンをクリックします。次に示す [ジョブ スケジュールの変更（Modify Job Schedule）] 画面が表示されます。

図 8-63　　[ジョブ スケジュールの変更（Modify Job Schedule）]

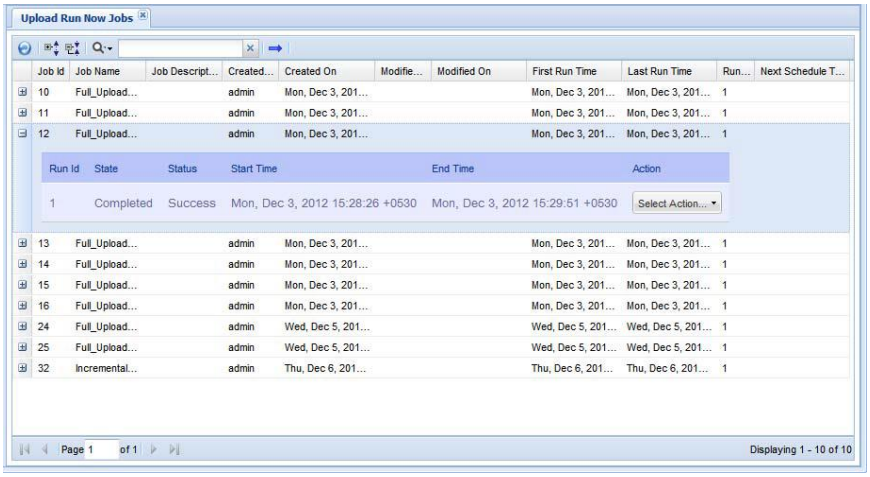


[スケジュールの設定（Configure Schedule）] ボタンをクリックして、スケジュールを再設定できます。ジョブ名以外のすべての詳細を変更できます。

[直ちにアップロードを実行ジョブ（Upload Run Now Jobs）]

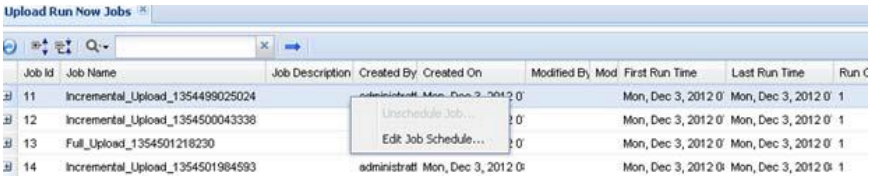
[直ちにアップロードを実行ジョブ（Upload Run Now Jobs）] では、アップロード プロファイルを使用して実行されたすべての「直ちに実行」ジョブを確認できます。直ちにアップロードを実行ジョブは、システムによりシステム生成のジョブ スケジュールを使用して作成されたシステム アップロード ジョブです。

図 8-64　　[直ちにアップロードを実行ジョブ（Upload Run Now Jobs）]



すでに完了済みで繰り返しスケジュールのないユーザ ジョブの場合は、ジョブ スケジュールの変更のみ行うことができます。これを行うと、今後のシステム アップロードの実行が変更されます。

図 8-65　　[ジョブ スケジュールの編集（Edit Job Schedule）]

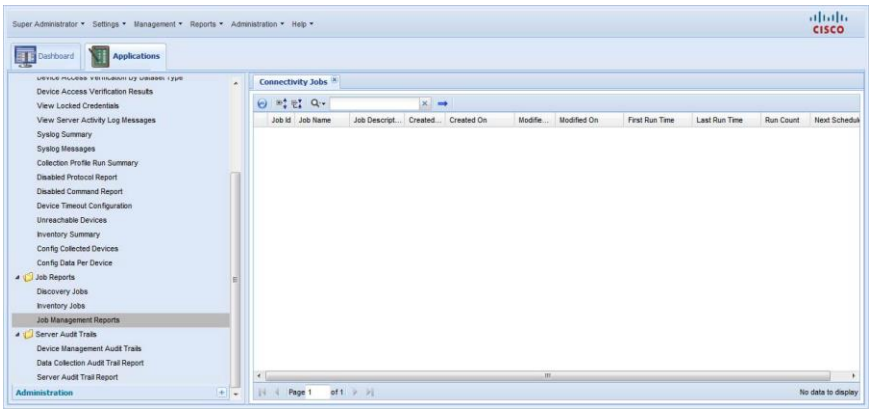


スケジュールの変更は、[直ちにアップロードを実行ジョブ（Upload Run Now Jobs）] の [次のスケジュール時刻（Next Schedule Time）] に反映されます。

[接続ジョブ（Connectivity Jobs）]

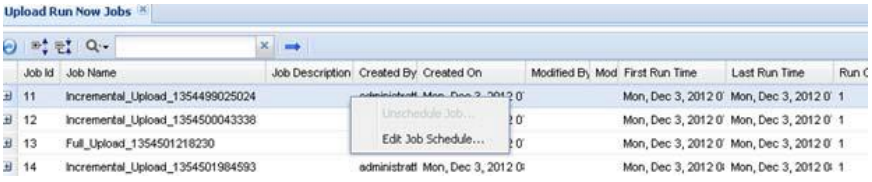
[接続ジョブ（Connectivity Jobs）] レポートには、接続関連の情報、実行回数、および最初と最後の実行時刻が表示されます。

図 8-66　　[接続ジョブ（Connectivity Jobs）]



すでに完了済みで繰り返しスケジュールのないユーザ ジョブの場合は、ジョブ スケジュールの変更のみ行うことができます。これを行うと、今後のシステム アップロードの実行が変更されます。

図 8-67　　[ジョブ スケジュールの編集（Edit Job Schedule）]

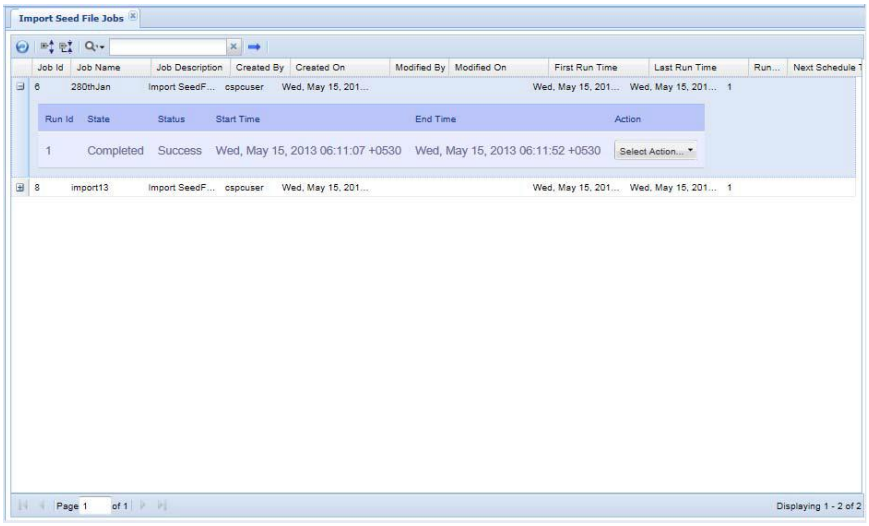


スケジュールの変更は、[接続ジョブ（Connectivity Jobs）] の [次のスケジュール時刻（Next Schedule Time）] に反映されます。

[シード ファイルのインポート ジョブ（Import Seed File Jobs）]

[シード ファイルのインポート ジョブ（Import Seed File Jobs）] レポートには、シード ファイルのインポート ジョブの一覧が表示されます。[ジョブ ID（Job ID）] の隣にある [+] 記号をクリックして、各ジョブの説明を確認できます。[実行 ID（Run Id）]、[状態（State）]（[完了（Completed）]/[未完了（Not Completed）]）、[ステータス（Status）]（[成功（Successful）]/[中止（Aborted）]）、[開始時刻（Start Time）]、[終了時刻（End Time）] が表示されます。レポート内にある [アクション（Action）] ボタンを選択して、そのジョブのジョブ ログの詳細を表示するか、または実行中のジョブをキャンセルします。

図 8-68　　[シード ファイルのインポート ジョブ（Import Seed File Jobs）]



[その他のジョブ（Miscellaneous Jobs）]

[その他のジョブ（Miscellaneous Jobs）] には、比較的小さな 1 回限りの非同期ジョブの一覧が表示されます。このようなジョブの例として、収集プロファイルのエクスポート ジョブがあります。

図 8-69　　[その他のジョブ（Miscellaneous Jobs）]

[監査証跡（Audit Trails）]

[監査証跡レポート（Audit Trail Report）] には、すべてのサーバ関連のログが含まれています。[サーバ監査証跡レポート（Server Audit Trails Reports）] サブ タブを使用して、サーバの監査証跡、データ収集、およびデバイス管理の情報を確認します。表示される列は、[ユーザ名（User Name）]、[モジュール（Module）]、[サブ モジュール（Sub Module）]、[ログ時刻（Log Time）]、[ジョブ ログの詳細（Job Log Detail）] です。

サブ モジュールには、セッション管理、パッチ管理、ユーザ管理、グループへの変更が表示されます。また、他のホストからの許可されない接続試行も表示されます。このレポートは、PDF、HTML、DOC、CSV（カンマ区切り）、TXT（タブ区切り）形式でエクスポートできます。

この項では、[レポート（Reports）] オプションの以下の項目について説明します。

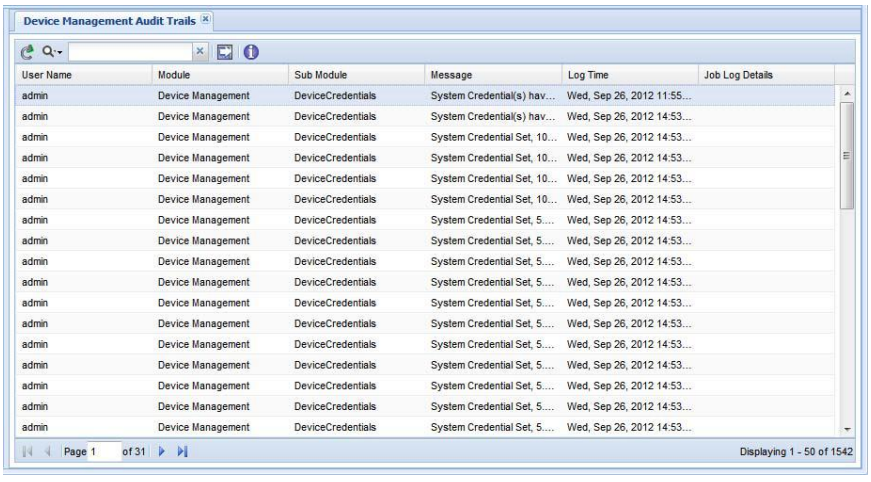
- [デバイス管理監査証跡（Device Management Audit Trails）]
- [データ収集監査証跡レポート（Data Collection Audit Trail Report）]
- [サーバ監査証跡レポート（Server Audit Trail Report）]

[デバイス管理監査証跡（Device Management Audit Trails）]

[デバイス管理監査証跡（Device Management Audit Trails）] レポートには、すべてのデバイス管理ログが含まれています。また、さまざまなジョブのジョブ ログの詳細も表示されます。表示される列は、[ユーザ名（User Name）]、[モジュール（Module）]、[サブ モジュール（Sub Module）]、[ログ時刻（Log Time）]、[ジョブ ログの詳細（Job Log Detail）] です。一部のジョブについては、[ジョブ ログの詳細（Job Log Details）] ボタンが表示されます。このボタンをクリックすると、該当するジョブ ログが表示されます。

サブ モジュールには、デバイス クレデンシャル、検出サブシステム、デバイス アクセス検証、デバイスの状態の変更、インベントリ サブシステム、サーバ設定への変更が表示されます。このレポートのコンテンツは、PDF、HTML、DOC、CSV（カンマ区切り）、TXT（タブ区切り）形式でエクスポートできます。

図 8-70　　[デバイス管理監査証跡（Device Management Audit Trails）]



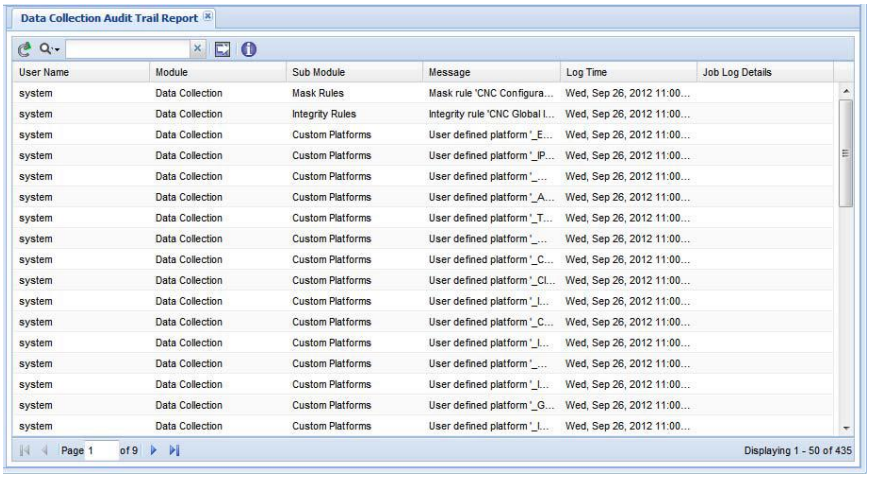
[データ収集監査証跡レポート（Data Collection Audit Trail Report）]

[データ収集監査証跡レポート（Data Collection Audit Trail Report）] には、すべてのデータ収集プロファイルの監査証跡が表示されます。表示される列は、[ユーザ名（User Name）]、[モジュール（Module）]、[サブ モジュール（Sub Module）]、[ログ時刻（Log Time）]、[ジョブ ログの詳細（Job Log Detail）] です。

このレポートには、収集プロファイル、データセット、プラットフォーム、整合性ルール、およびマスキング ルールを含むデータ収集設定への変更がすべて表示されます。

このレポートは、PDF、HTML、DOC、CSV（カンマ区切り）、TXT（タブ区切り）形式でエクスポートできます。

図 8-71　　[データ収集監査証跡レポート（Data Collection Audit Trail Report）]



[サーバ監査証跡レポート（Server Audit Trail Report）]

[サーバ監査証跡レポート（Server Audit Trail Report）] には、すべてのサーバ関連のログが含まれています。
表示される列は、[ユーザ名（User Name）]、[モジュール（Module）]、[サブ モジュール（Sub Module）]、[ログ時刻（Log Time）]、[ジョブ ログの詳細（Job Log Detail）] です。

サブ モジュールには、セッション管理、パッチ管理、ユーザ管理、グループへの変更が表示されます。また、他のホストからの許可されない接続試行も表示されます。

このレポートは、PDF、HTML、DOC、CSV（カンマ区切り）、TXT（タブ区切り）形式でエクスポートできます。

図 8-72 [サーバ監査証跡レポート（Server Audit Trail Report）]

[その他（Miscellaneous）]

[デバイス ラウンチ パッド（Device Launch Pad）]

[デバイス ラウンチ パッド（Device Launch Pad）] レポートには、すべてのデバイスの一覧が表示されます。それぞれのデバイスに対して起動するアプリケーションを選択できます。

レポート生成のプロセスには 2 つのステップがあります。まずデバイスを選択し、次にアプリケーションを選択します。選択した特定のアプリケーション レポートが、選択したデバイスに対して起動されます。

図 8-73　　[デバイスの選択（Select Devices）]

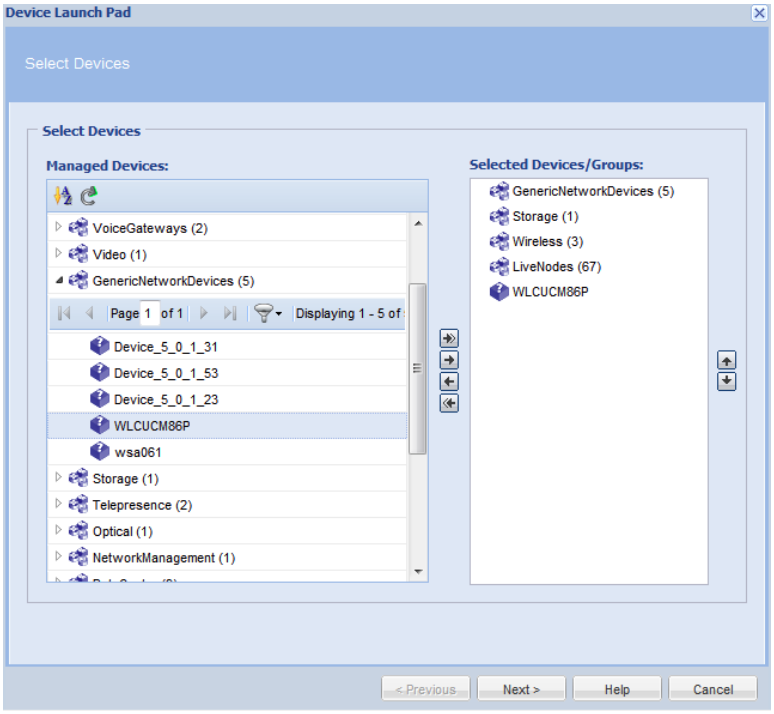
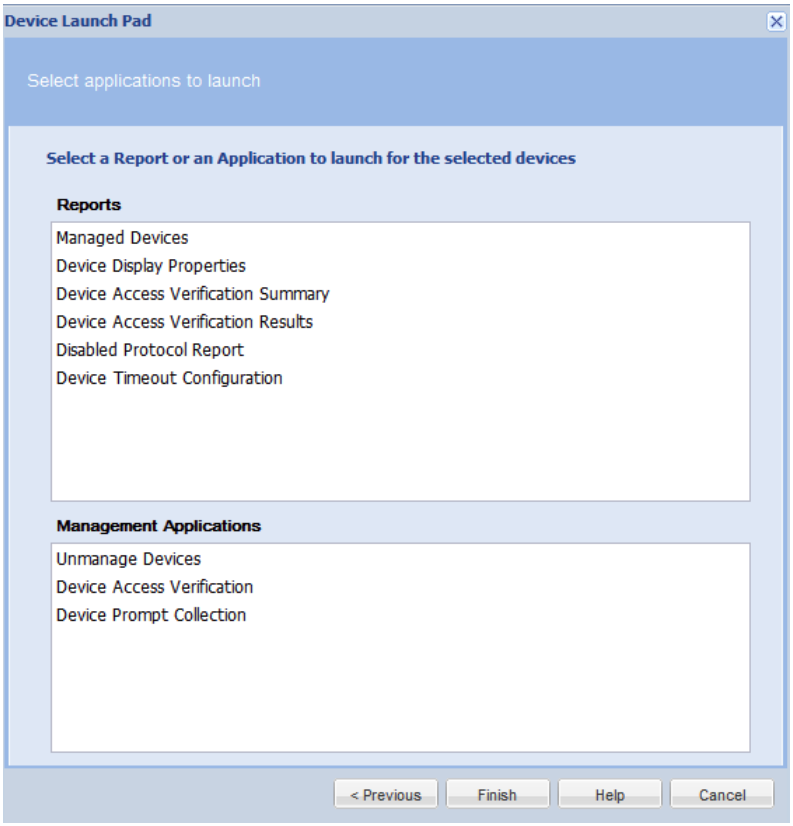


図 8-74　　[起動するアプリケーションの選択（Select application to Launch]）

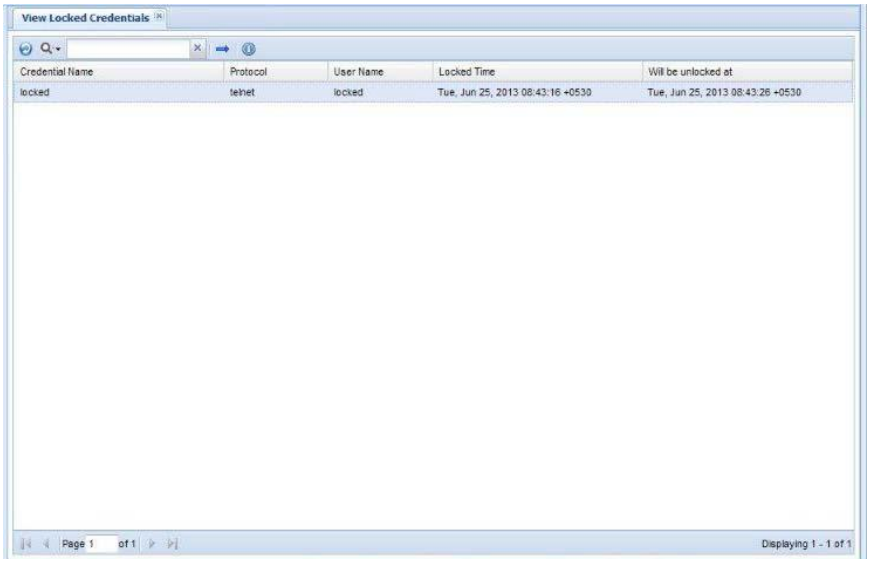


選択が完了すると、選択したアプリケーションが選択したデバイスに対して起動されます。

[ロックされているクレデンシャルの表示（View Locked Credentials）]

このレポートには、ロックされているすべてのクレデンシャルの一覧が表示されます。クレデンシャル名、プロトコル、ユーザ名、ロックされた時刻、および（設定済みのロック期間に基づいて）ロックが解除される時刻が表示されます。

図 8-75　　[ロックされているクレデンシャルの表示（View Locked Credentials）]

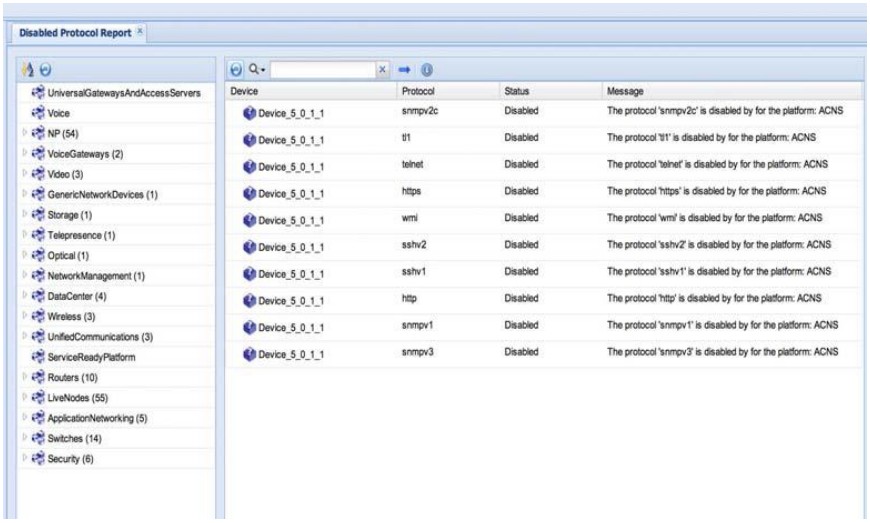


クレデンシャルのロックを解除するには、ロックを解除するクレデンシャルを右クリックし、[クレデンシャルのロックを解除...（Unlock the Credential...）] オプションを選択します。

[無効プロトコル レポート（Disabled Protocol Report）]

[無効プロトコル レポート（Disabled Protocol Report）] には、特定のデバイスやグループで無効になっているすべてのプロトコルが表示されます。このレポートのコンテンツは、サポートされているいずれかの形式でエクスポートできます。サポートされている形式は、HTML、PDF、Microsoft Word、CSV、および TXT です。

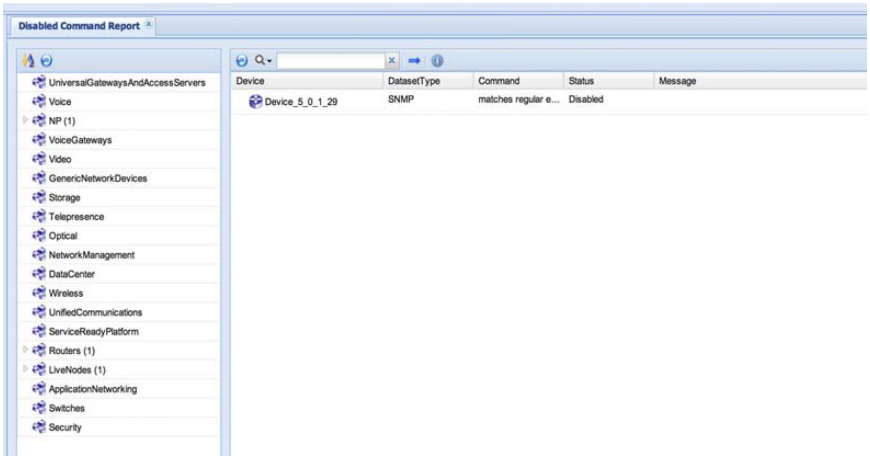
図 8-76　　[無効プロトコル レポート（Disabled Protocol Report）]



[無効コマンド レポート（Disabled Command Report）]

[無効コマンド レポート（Disabled Command Report）] には、特定のデバイスやグループで無効になっているコマンドの詳細が表示されます。

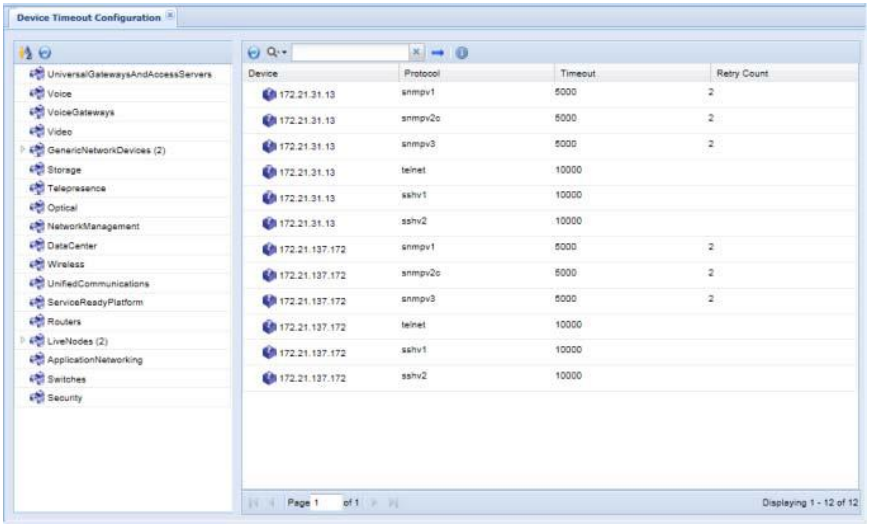
図 8-77　　[無効コマンド レポート（Disabled Command Report）]



[デバイスのタイムアウト設定（Device Timeout Configuration）]

[デバイスのタイムアウト設定（Device Timeout Configuration）] レポートには、それぞれのデバイスに指定されているすべてのタイムアウト設定、および再試行回数が表示されます。これらの値は、[詳細設定（Advanced Settings）] の [グローバル タイムアウト（Global Timeouts）] に設定されているタイムアウトから設定されます。このレポートは、PDF、HTML、DOC、CSV（カンマ区切り）、TXT（タブ区切り）形式でエクスポートできます。

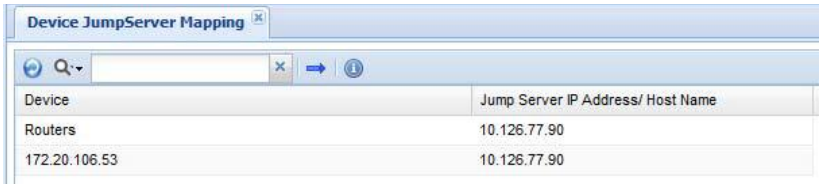
図 8-78　　[デバイスのタイムアウト設定（Device Timeout Configuration）]



[デバイスとジャンプ サーバのマッピング（Device Jump Server Mapping）]

このレポートには、図 8-79 に示すようにジャンプ サーバにマッピングされているすべてのデバイスまたはグループが表示されます。デバイスのデバイス/グループ名または IP アドレス、デバイスがマッピングされているジャンプ サーバの IP アドレスなどの情報が表示されます。

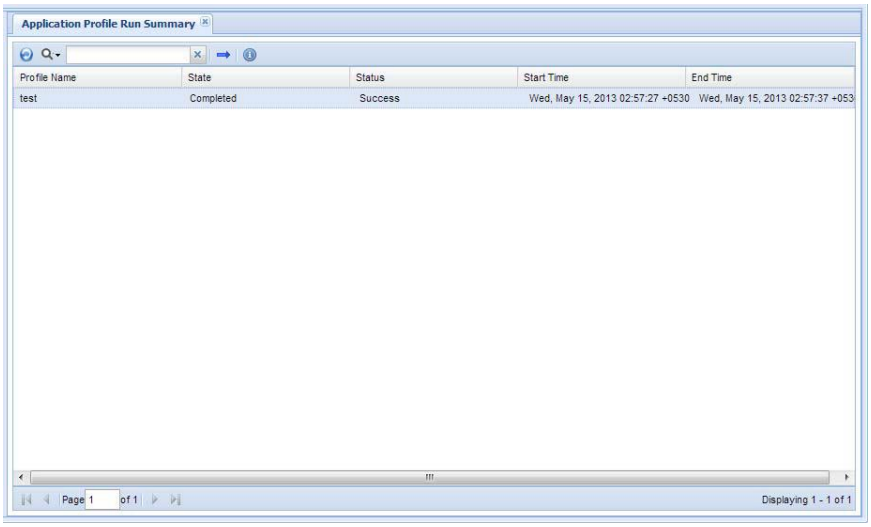
図 8-79　　ジャンプ サーバのマッピング



[アプリケーション プロファイルの実行のサマリー（Application Profile Run Summary）]

[アプリケーション プロファイルの実行のサマリー（Application Profile Run Summary）] レポートには、図 8-80 に示すように、完了したアプリケーション プロファイルのサマリーが表示されます。

図 8-80　　[アプリケーション プロファイルの実行のサマリー（Application Profile Run Summary）]



[アプリケーション検出レポート（Application Discovery Report）]

[アプリケーション検出レポート（Application Discovery Report）] には、サーバにインストールされている検出アプリケーションの一覧が表示されます（以下のリストを参照）。図 8-81 に示すように、インストールされている各アプリケーションについて、[OS タイプ（OS Type）]、[OS バージョン（OS Version）]、[CPU タイプ（CPU Type）]、搭載されている [メモリの総容量（Total Memory）] などのシステム レベルの情報が表示されます。

図 8-81　　[アプリケーション検出レポート（Application Discovery Report）]

各行を展開すると、図 8-82 に示すように、インストールされているアプリケーションの一覧と、[アプリケーション名（Name）]、[バージョン（Version）]、[ベンダー（Vendor）]、アプリケーションがインストールされている [パス（Path）]、[インストールされた日付（Installed date）]、[実行状態（Status）] などの各アプリケーションの詳細が表示されます。

インストールされている検出アプリケーション

Microsoft Windows および Linux プラットフォームで検出できるアプリケーションは次のとおりです。

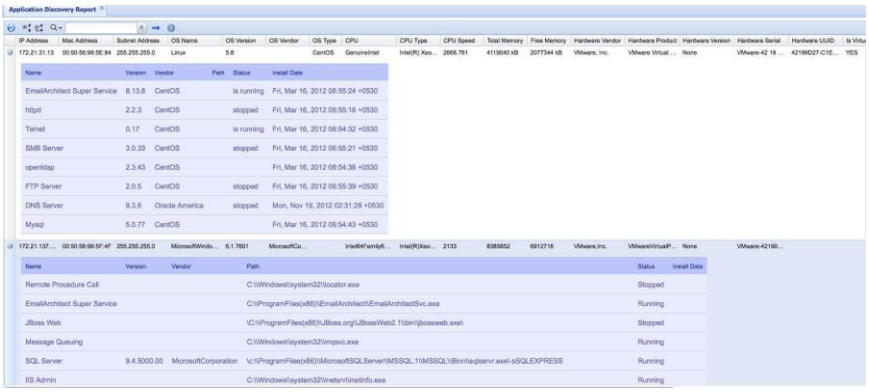
Microsoft Windows：

Tomact、MySQL、ArgoSoft、DB2、SQL Server、OpenLDAP、NetBIOS Session Service、EmailArchitect Super Service、JBOSS、DNS サーバ、MSMQ、VMWare Workstation、WebSphere、Oracle、RPC、IIS Admin、SANSurfer。

Linux :

Tomcat、MySQL、httpd、OpenLDAP、FTP サーバ、SendMail、Telnet、DNS サーバ。

図 8-82　　[アプリケーション検出レポート（Application Discovery Report）]（展開時）



9

アプリケーション - 管理

管理

[管理（Administration）] タブを使用して、CSPC サーバのユーザの作成、収集データのバックアップの作成、サーバ パッチの確認などを行います。

この項では、[レポート（Reports）] オプションの以下の項目について説明します。

- [ユーザ管理（User Management）]
- [ユーザ設定（User Preferences）]
- [アラート管理（Alert Management）]
- [バックアップと復元（Backup and Restore）]
- [ログ設定（Log Preferences）]
- [その他のアプリケーション（Miscellaneous Applications）]

[ユーザ管理（User Management）]

[ユーザ管理（User Management）] サブ タブは、特定の CSPC サーバのユーザを作成し、ユーザ設定を変更するために使用します。

この項では、各オプションの以下の項目について説明します。

- [ユーザ管理（Manage Users）]
- [リモート認証サーバの管理（Manage Remote Authentication Servers）]
- [ユーザ セッション レポート（User Session Report）]

[ユーザ管理（Manage Users）]

[ユーザ管理（Manage Users）] をダブルクリックすると、次に示すような [ユーザ管理（Manage Users）] ウィンドウが開きます。このウィンドウでは、コレクタ ユーザの作成と管理ができます。

図 9-1　　[ユーザ管理（Manage Users）]

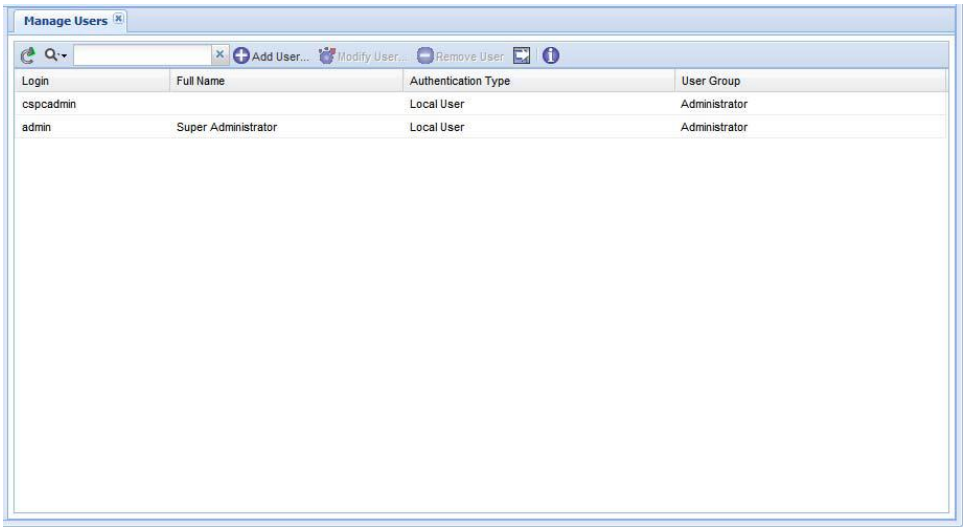
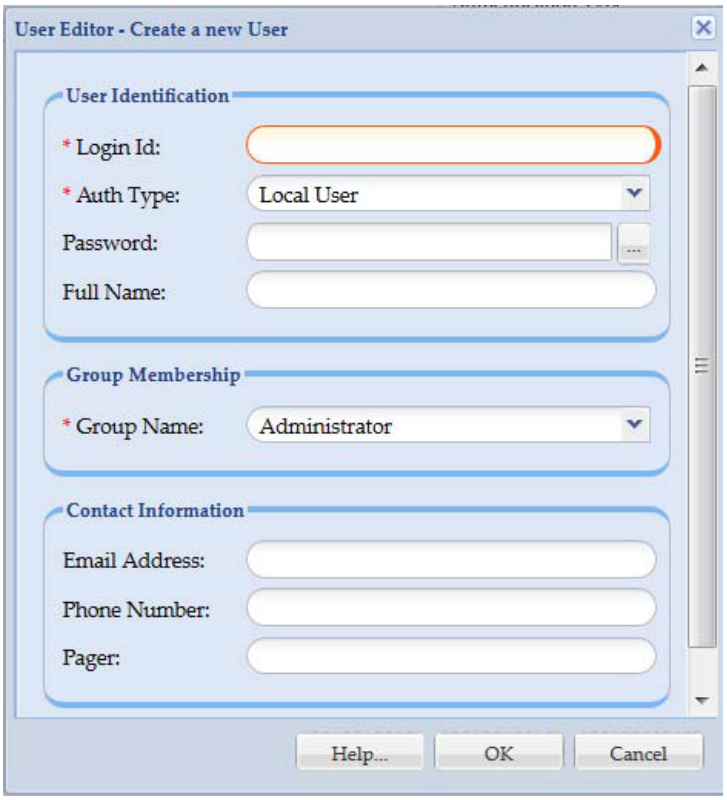


図 9-2　　コレクタ ユーザの管理



新規ユーザを追加するには、[ユーザの追加（Add User）] をクリックします。このウィンドウには、システムで定義されている各ユーザの以下の情報が表示されます。

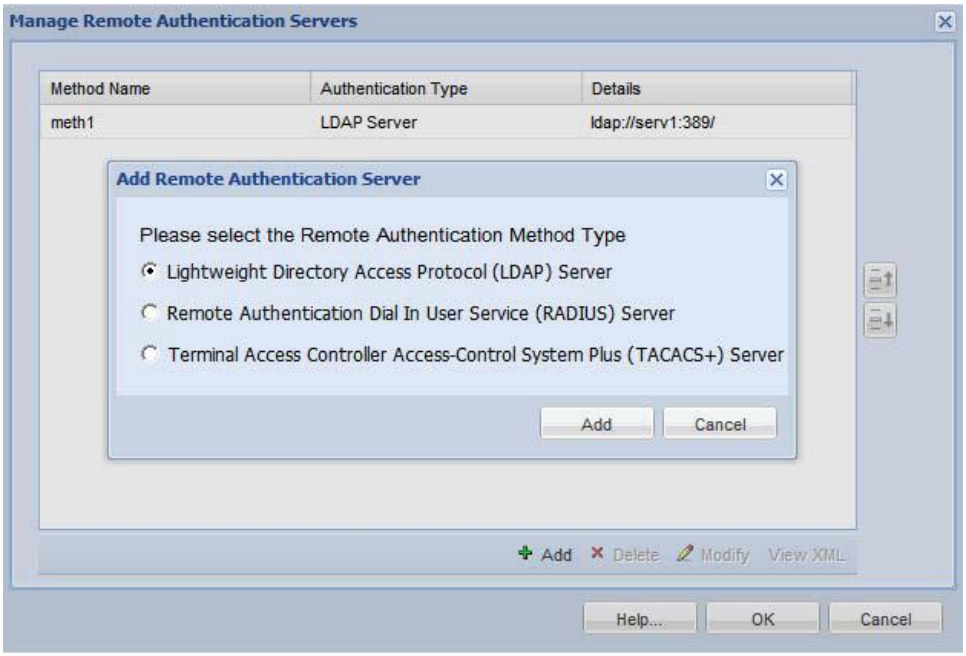
- ログイン ID
- 認証タイプ（ローカル、リモート ユーザ認証）
- パスワード（マスク済み）
- 名前
- グループ名
- 電子メール アドレス
- 電話番号
- ポケベル

既存のユーザの詳細を変更するには、[ユーザの変更（Modify User）] ボタンをクリックします。既存のユーザを削除するには、[ユーザの削除（Remove User）] ボタンをクリックします。

[リモート認証サーバの管理（Manage Remote Authentication Servers）]

ユーザ認証タイプがリモート認証の場合、CSPC はリモート認証サーバからユーザ クレデンシャルを取得します。次に示すように、リモート認証サーバは、クレデンシャルにアクセスするようにセットアップする必要があります。

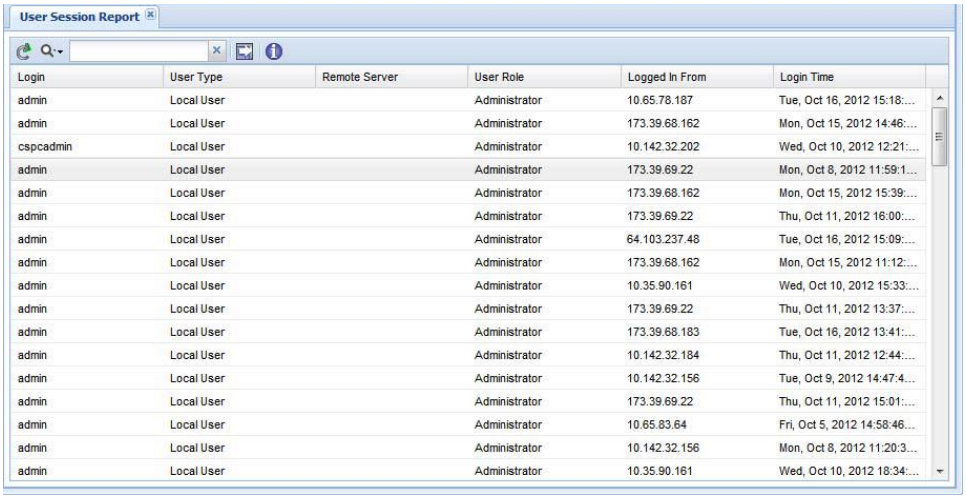
図 9-3　　リモート認証サーバのセットアップ



[ユーザ セッション レポート（User Session Report）]

[ユーザ セッション レポート（User Session Report）] ウィンドウには、サーバに現在接続しているユーザの一覧が表示されます。

図 9-4　　[ユーザ セッション レポート（User Session Report）]



[ユーザ設定（User Preferences）]

[ユーザ設定（User Preferences）] サブ タブは、特定の CSPC サーバのユーザ設定を変更するために使用します。

この項では、各オプションの以下の項目について説明します。

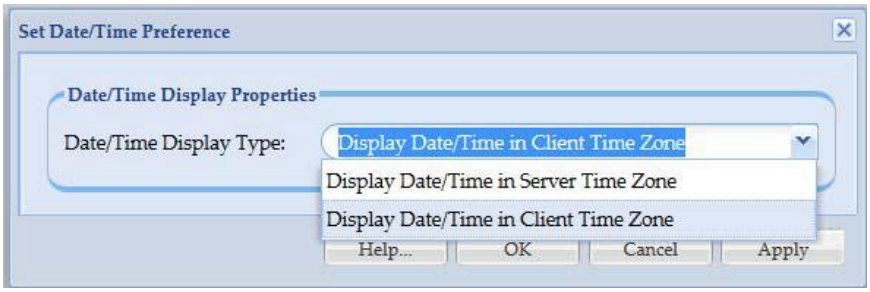
- [日時設定の変更（Modify Data/Time Preference）]
- [デフォルトのデバイス表示プロパティの設定（Configure Default Device Display Property）]

[日時設定の変更（Modify Data/Time Preference）]

[日時設定の変更（Modify Data/Time Preference）] では、日付と時刻を設定できます。図 9-5 に示すように、
日付と時刻をクライアントのタイム ゾーンで表示するか、サーバのタイム ゾーンで表示するかを選択できます。

変更を終えると、設定はその特定のユーザ アカウント用に保存されます。

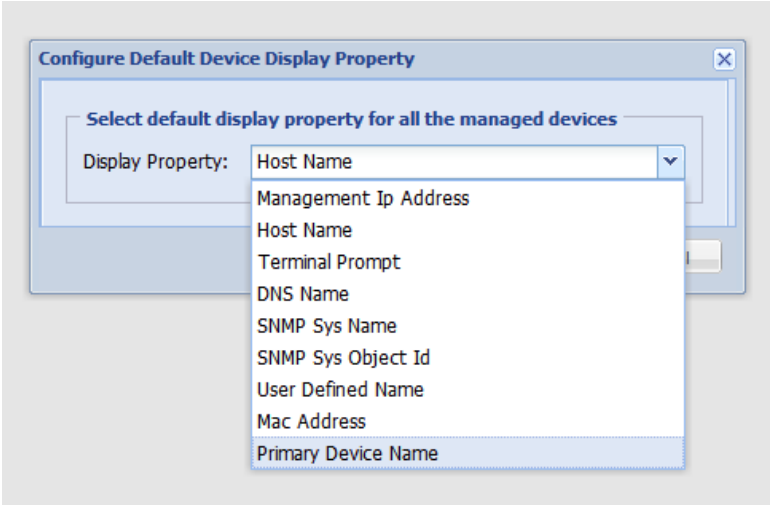
図 9-5　　[ユーザ設定の変更（Modify User Preferences）]



[デフォルトのデバイス表示プロパティの設定（Configure Default Device Display Property）]

[デフォルトのデバイス表示プロパティの設定（Configure Default Device Display Property）] では、すべての管理対象デバイスのデフォルトとなるデバイス プロパティを選択できます。

図 9-6　　[デフォルトのデバイス表示プロパティの設定（Configure Default Device Display Property）]



[アラート管理（Alert Management）]

[アラート管理（Alert Management）] サブ タブは、特定の CSPC サーバの電子メール設定やアラートを定義するために使用します。

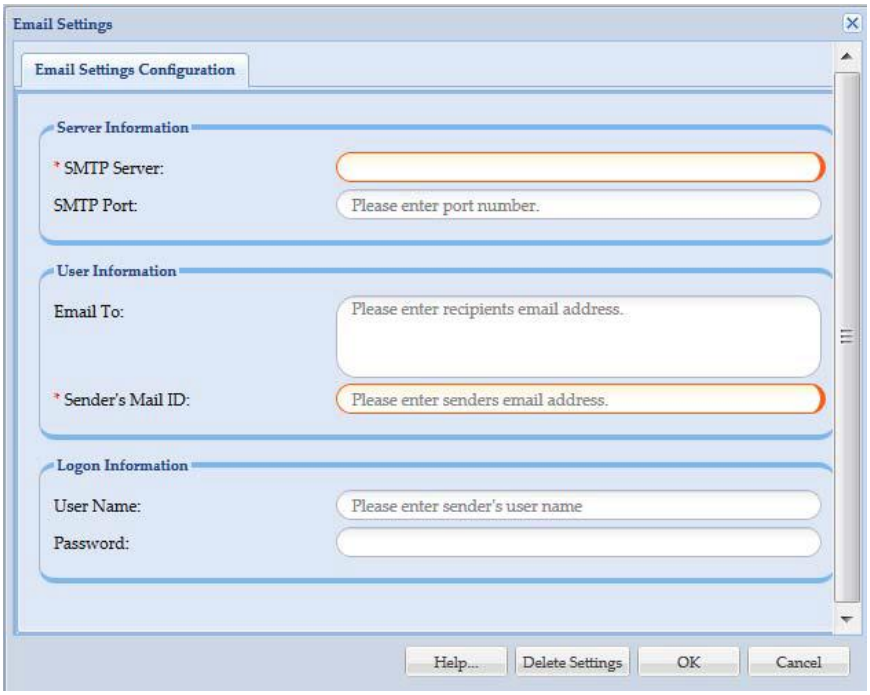
この項では、各オプションの以下の項目について説明します。

- [電子メール設定（Email Settings）]
- [サブスクライバの管理（Manage Subscribers）]
- [アラート設定（Alert Configuration）]

[電子メール設定（Email Settings）]

この設定には、メール交換のために SMTP サーバを設定するオプションがあります。

図 9-7　　[電子メール設定（Email Settings）]



すべての必須フィールドに入力して [OK] をクリックします。

表 9-1　　SMTP サーバ パラメータ

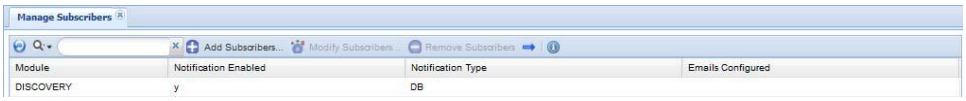
フィールド名	内容
[SMTP サーバ（SMTP Server）]	サーバ名またはサーバの ID。
[SMTP ポート（SMTP Port）]	サーバに使用されるポート番号。
[メール宛先（Email To）]	受信者のメール アドレス。
[送信者のメール ID（Sender's Mail ID）]	送信者のメール アドレス。
[ユーザ名（User Name）]	ログイン名。
[パスワード（Password）]	ログイン パスワード。

SMTP 設定をデフォルト値にリセットするには、[デフォルト設定（Default Settings）] をクリックします。

[サブスクライバの管理（Manage Subscribers）]

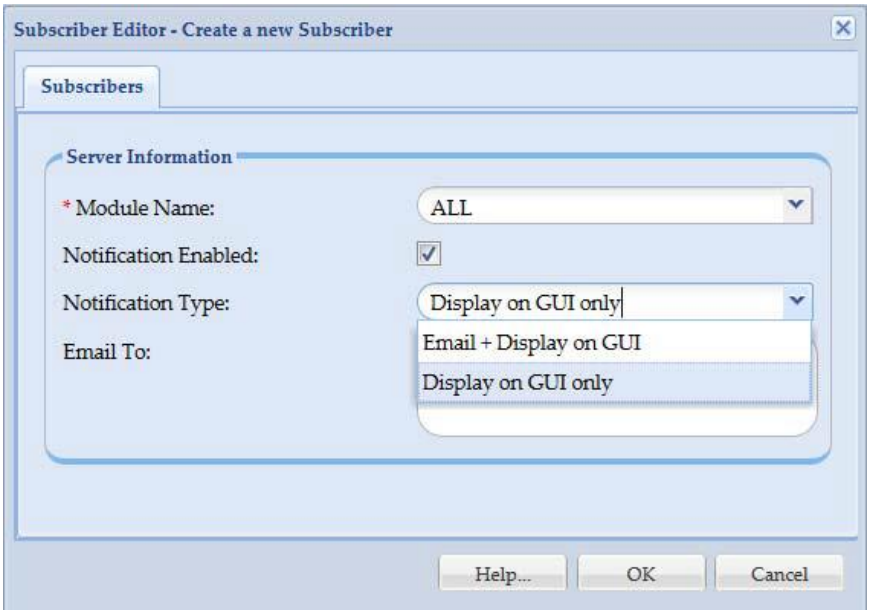
このオプションでは、すべてのサブスクライバを管理できます。

図 9-8 [サブスクライバの管理（Manage Subscribers）]



ステップ 1　サブスクライバを追加するには、[サブスクライバの追加（Add Subscribers）] をクリックします。図 9-9 に示す画面が表示されます。

図 9-9　　[サブスクライバの追加（Add Subscribers）]

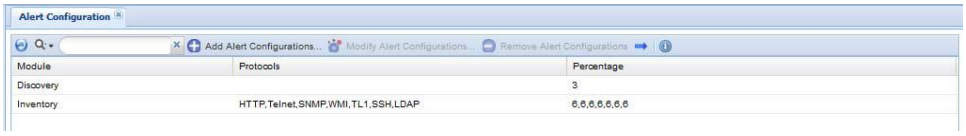


ステップ 2 [モジュール名（Module Name）] を入力して [通知を有効にする（Notification Enabled）] をオンにし、必要に応じて[通知タイプ（Notification Type）] と [メール宛先（Email To）] を入力して [OK] をクリックします。

[アラート設定（Alert Configuration）]

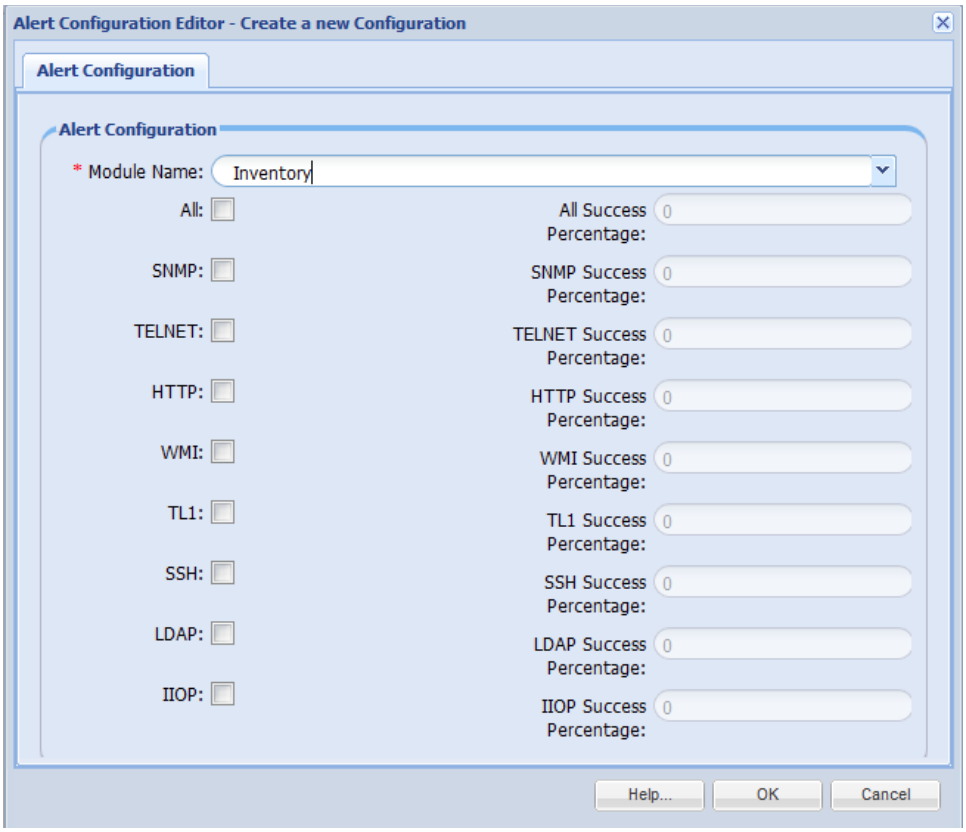
ワークフロー CSPC サービスにアラートを出し、ユーザに通知をプッシュします。ジョブのステータスを確認するために毎回ログインする必要はありません。

図 9-10　　[アラート設定（Alert Configuration）]



ステップ 1　アラートを追加するには、[アラート追加設定（Add Alert Configurations）] をクリックします。図 9-11 に示す画面が表示されます。

図 9-11　　[アラート追加設定（Add Alert Configurations）]



ステップ 2　[モジュール名（Module Name）] をドロップダウンから選択します。

- [検出（Discovery）] を選択した場合は、[検出の成功率（%）（Discovery success Percentage）] の値を入力します。
- [インベントリ（Inventory）] または [DAV] を選択した場合は、プロトコルを選択し、そのプロトコルの [成功率（Success Percentage）] の値を入力します。

ステップ 3　[OK] をクリックします。

注　[すべて（All）] または任意のプロトコルを選択できます。

[バックアップと復元（Backup and Restore）]

[バックアップと復元（Backup and Restore）] サブ タブは、収集データのバックアップ作成、および障害発生時にバックアップ データを復元するために使用します。

注　ファイルをより安全に転送するには：

- FTP や TFTP のような安全でないプロトコルの代わりに安全な SFTP や SCP プロトコルを使用することを推奨します。

この項では、各オプションの以下の項目について説明します。

- [バックアップ（Backup）]

- [バックアップの復元（Restore Backup）]

[バックアップ（Backup）]

[バックアップ（Backup）] オプションでは、任意の時点でのデータベース バックアップを選択したり、定期的なデータベース バックアップのオプションを指定したりできます。

バックアップ ジョブを実行するには、以下の手順に従います。

ステップ 1 [FTP サーバ（FTP Server）] または [ローカル サーバ（Local Server）] を選択します。

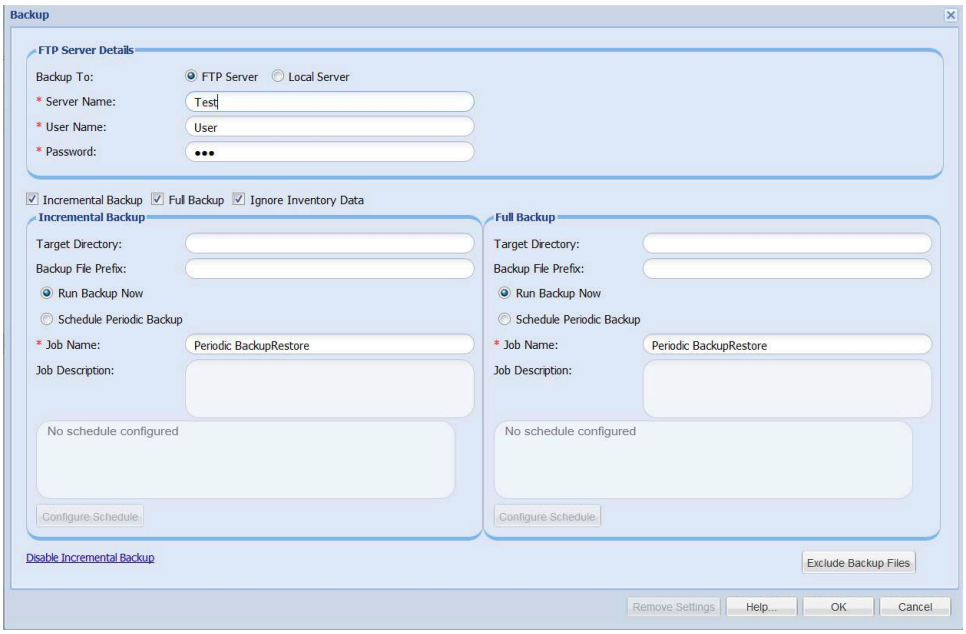
- [FTP サーバ（FTP Server）] を選択した場合は、次の情報を入力します。
  - [サーバ名（Server Name）]：FTP サーバの IP アドレス/ホスト名
  - [ユーザ名（User Name）]：FTP サーバのユーザ名
  - [パスワード（Password）]：FTP サーバのパスワード
- [ローカル サーバ（Local Server）] を選択した場合は、そのまま続行します。

ステップ 2 [増分バックアップ（Incremental Backup）]、[完全バックアップ（Full Backup）]、[インベントリ データを除く（Ignore Inventory Data）] オプションの必要なものを選択し、次の情報を入力します。

- [ターゲット ディレクトリ（Target Directory）]：バックアップ ファイルを保存する必要があるディレクトリ
- [バックアップ ファイルのプレフィックス（Backup File prefix）]：バックアップされたファイルに追加されるタグ
- すぐにバックアップを開始する場合は、[直ちにバックアップを実行（Run Backup Now）] を選択します。ジョブを後で実行するようにスケジュールする場合は、[定期的なバックアップをスケジュール（Schedule Periodic Backup）] を選択します。定期的なバックアップのスケジュール設定では、データ バックアップの [繰り返しの範囲（Range of Recurrences）]、[スケジュールの開始日時（Schedule Start Date/Time）]、[スケジュールの終了日時（Schedule End Date/Time）]、[反復パターン（Recurrence Pattern）] を指定できます。これを示しているのが図 9-13 です。
- [ジョブ名（Job Name）]：ジョブ名を入力します。
- [ジョブの説明（Job Description）]：ジョブの説明を入力します。

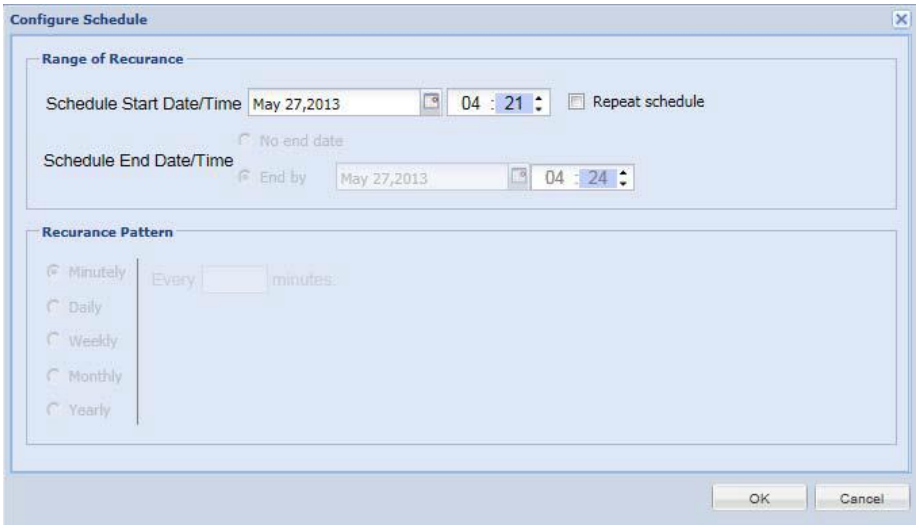
注 インベントリ データをバックアップから除外するには、[インベントリ データを除く（Ignore Inventory Data）] を選択します。

図 9-12　　[バックアップ（Backup）]



注 増分バックアップを無効にするには、[増分バックアップを無効にする（Disable Incremental Backup）] をクリックします。CSPC を再起動するように求められます。同様に、増分バックアップを有効にするには、[増分バックアップを有効にする（Enable Incremental Backup）] をクリックします。これもまた再起動が必要です。

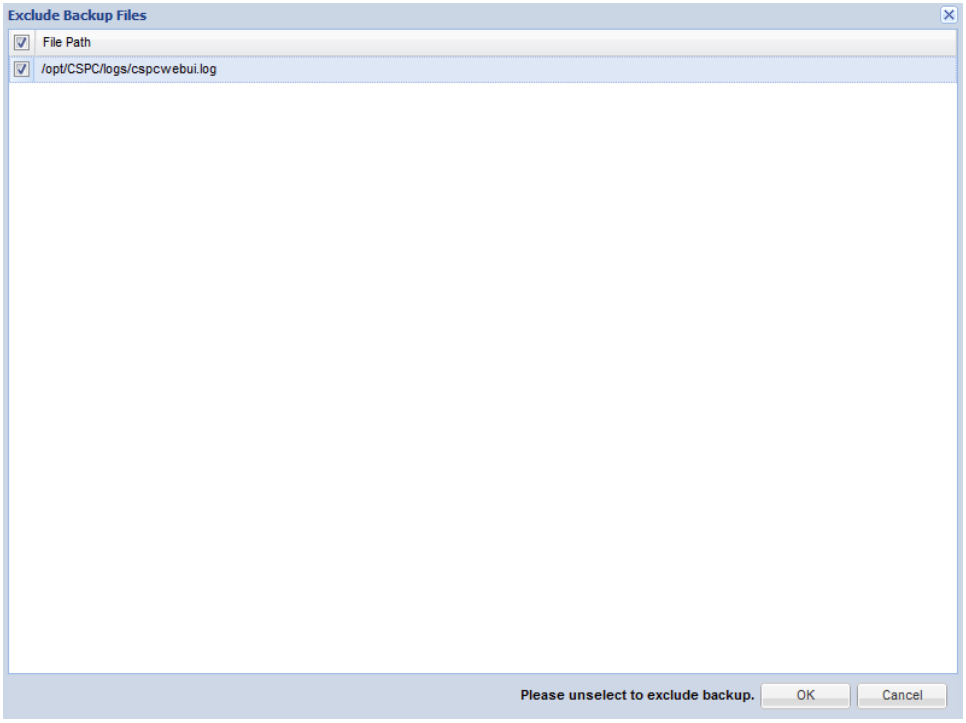
図 9-13　　[スケジュールの設定（Configure Schedule）]



ステップ 3 バックアップからファイルを除くには、図 9-14 に示すように、ファイルの選択を解除します。

この画面にファイルを表示するには、プロパティ ファイルにファイル パスを入力します。

図 9-14　　[バックアップからファイルを除く（Exclude Backup Files）]



[バックアップの復元（Restore Backup）]

[バックアップの復元（Restore Backup）] オプションでは、すでに保存されているデータ バックアップを復元できます。サーバ情報（バックアップ ファイルの保存場所など）、およびシステムにバックアップされる CSPC ロードを指定する必要があります。これを示しているのが図 9-15 です。

バックアップ ファイルを復元するには、以下の手順に従います。

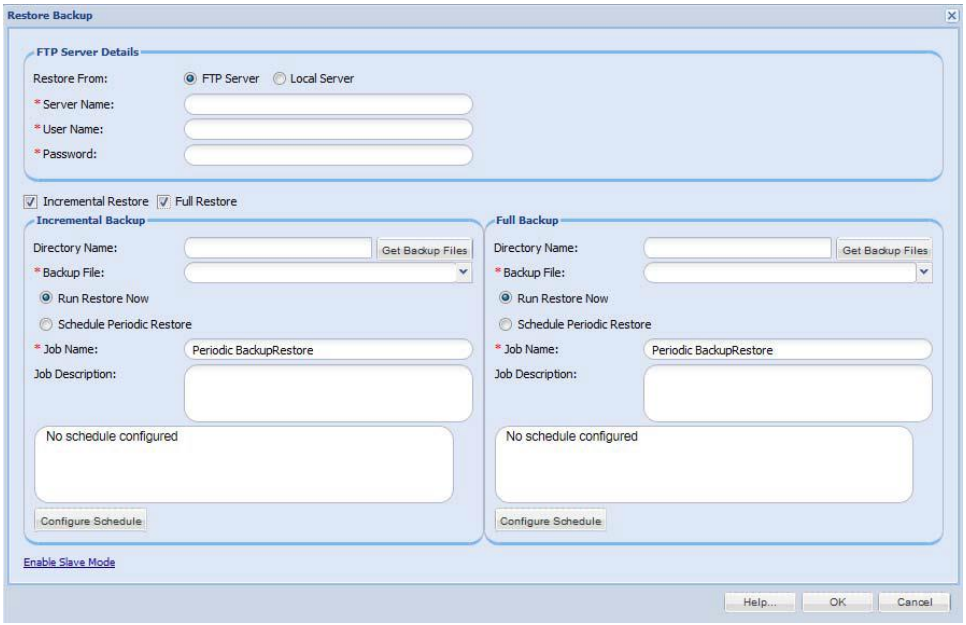
ステップ 1 [FTP サーバ（FTP Server）] または [ローカル サーバ（Local Server）] を選択します。

- [FTP サーバ（FTP Server）] を選択した場合は、次の情報を入力します。
  - [サーバ名（Server Name）]：FTP サーバの IP アドレス/ホスト名
  - [ユーザ名（User Name）]：FTP サーバのユーザ名
  - [パスワード（Password）]：FTP サーバのパスワード
- [ローカル サーバ（Local Server）] を選択した場合は、そのまま続行します。

ステップ 2 [増分復元（Incremental Restore）] や [完全復元（Full Restore）] を選択し、次の情報を入力します。

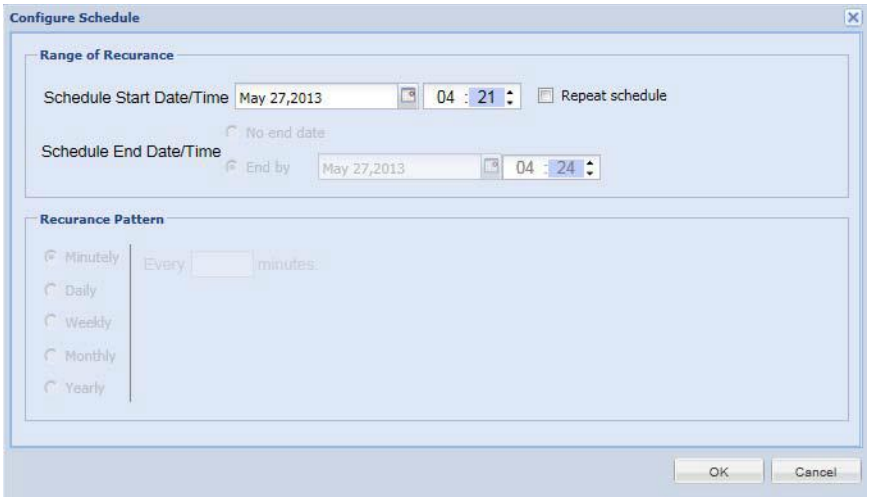
- [ディレクトリ名（Directory Name）]：バックアップ ファイルを復元する必要があるディレクトリ
- [バックアップ ファイル（Backup File）]：バックアップ ファイル名
- すぐに復元を開始する場合は、[直ちに復元を実行（Run Restore Now）] を選択します。ジョブを後で実行するようにスケジュールする場合は、[定期的な復元をスケジュール（Schedule Periodic Restore）] を選択します。定期的な復元のスケジュール設定では、データ復元の [繰り返しの範囲（Range of Recurrences）]、[スケジュールの開始日時（Schedule Start Date/Time）]、[スケジュールの終了日時（Schedule End Date/Time）]、[反復パターン（Recurrence Pattern）] を指定できます。これを示しているのが図 9-16 です。
- [ジョブ名（Job Name）]：ジョブ名を入力します。
- [ジョブの説明（Job Description）]：ジョブの説明を入力します。

図 9-15　　サーバ バックアップの復元



注 スレーブ モードを有効にするには、[スレーブ モードを有効にする（Enable Slave Mode）] をクリックします。CSPC の再起動が必要です。これにより、CSPC でバックアップと復元以外のジョブがすべて無効になります。
同様に、スレーブ モードを無効にするには、[スレーブ モードを無効にする（Disable Slave Mode）] をクリックします。これもまた再起動が必要です。

図 9-16　　[スケジュールの設定（Configure Schedule）]



[ログ設定（Log Preferences）]

[サーバ ログの設定（Server Log Preference）] サブ タブは、サポートの問題を特定および修正するのに役立つサーバ ログを管理するために使用します。

この項では、各オプションの以下の項目について説明します。

- [ログ設定（Log Preferences）]
- [ログ ファイルのエクスポート（Export Log Files）]

[ログ設定（Log Preferences）]

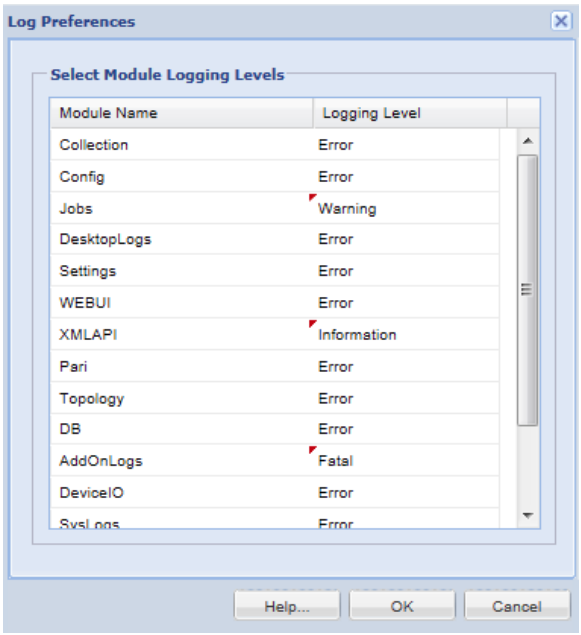
[ログ設定（Log Preferences）] では、CSPC の各モジュールの詳細なログ レベルを選択できます。サーバと UI コンポーネントのログ設定を変更できます。

ログ レベルには、次のいずれかを指定できます。

- 致命的
- エラー
- 警告
- 情報
- デバッグ
- トレース

ログ レベルを変更するには、ログ レベルをクリックして該当するレベルを選択します。[なし（none）] を選択して、特定のモジュールのログを無視することもできます。この設定は、CSPC ログでのログ メッセージの表示に使用されます。

図 9-17　　[ログ設定（Log Preferences）]



[ログ ファイルのエクスポート（Export Log Files）]

ログ ファイルのエクスポート機能を使用すると、エラーが発生して、Cisco CSP のサポート スタッフがサーバ ログを必要とする場合に、すべてのサーバ ログ ファイルをエクスポートしてサポート スタッフに渡すことができます。ログ ファイルは、ファイル名またはタイムスタンプに基づいてエクスポートできます。次のスクリーンショットを参照してください。

図 9-18　　ファイルに基づくログ ファイルのエクスポート

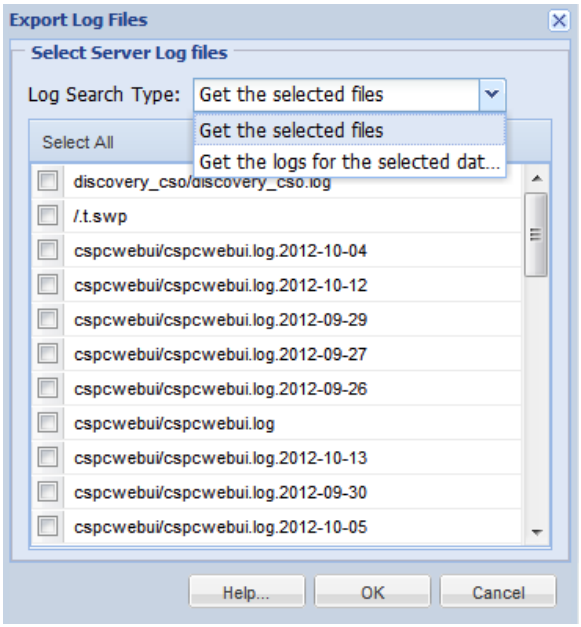
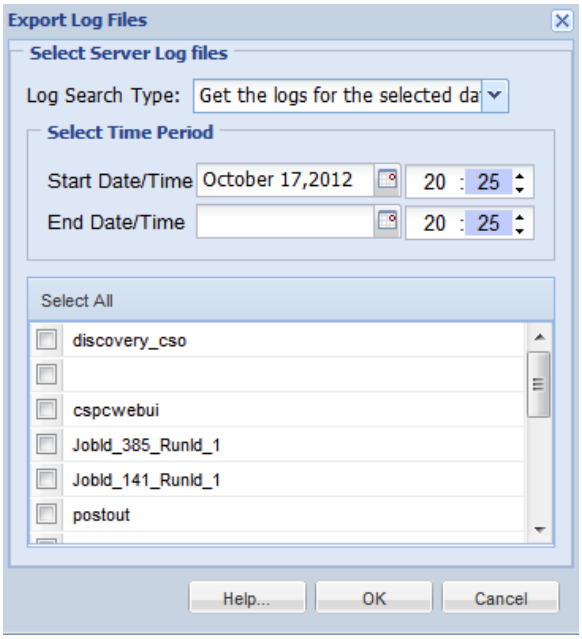


図 9-19　　タイムスタンプに基づくログ ファイルのエクスポート



[その他のアプリケーション（Miscellaneous Applications）]

[その他のアプリケーション（Miscellaneous Applications）] サブ タブには、サーバ情報が表示されます。また、クライアントとサーバの再同期が可能で、複数の診断ツールも用意されています。

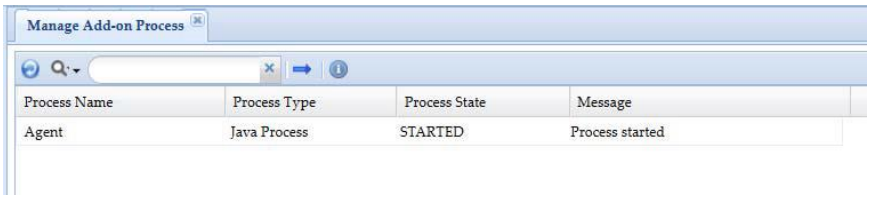
この項では、各オプションの以下の項目について説明します。

- [アドオン プロセスの管理（Manage Add-on Process）]
- [UI アドオンの管理（Manage UI Add-Ons）]
- [サーバのプロパティ（Server Properties）]
- [診断ツール（Diagnostic Tools）]
- [XML API コンソール（XML API Console）]

[アドオン プロセスの管理（Manage Add-on Process）]

[アドオン プロセスの管理（Manage Add-on Process）] には、CSPC 用のアドオン プロセスを含むサーバ プロセスの詳細が表示されます。このレポートには、図 9-20 に示すように、[プロセス名（Process Name）]、[プロセス タイプ（Process Type）]、[プロセスの状態（Process State）]、そのプロセスに関連付けられている [メッセージ（Message）] が表示されます。

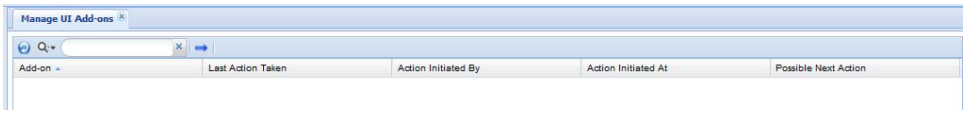
図 9-20　　サーバ プロセス サマリーの表示



[UI アドオンの管理（Manage UI Add-Ons）]

[UI アドオンの管理（Manage UI Add-Ons）] 画面には、アドオン、アドオンで実行されているアクション、アクションを開始したユーザ、アクションの時刻、次に実行可能なアクションの一覧が表示されます。

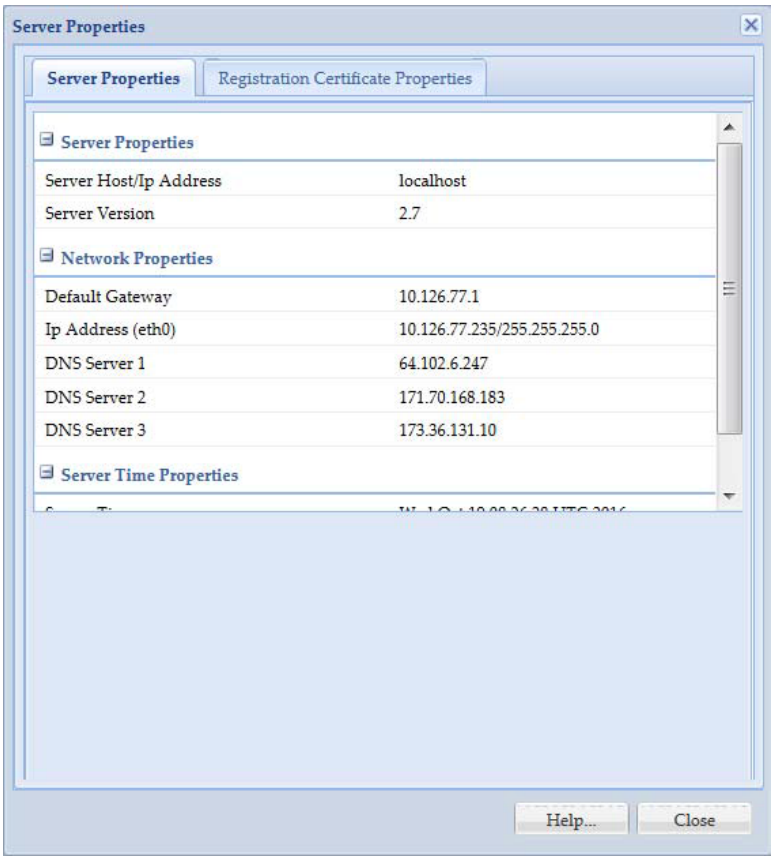
図 9-21 [UI アドオンの管理（Manage UI Add-Ons）]



[サーバのプロパティ（Server Properties）]

[サーバのプロパティ（Server Properties）] ウィンドウには、サーバ自体の情報が表示されます。このウィンドウに表示されるデータは、[サーバのプロパティ（Server Properties）] と [登録証明書のプロパティ（Registration Certificate Properties）] です。図 9-22 に示すように、サーバの IP アドレス、サーバ バージョン、デフォルト ゲートウェイ、サーバのタイム ゾーンなどの情報が表示されます。

図 9-22　　[サーバのプロパティ（Server Properties）]



[登録証明書のプロパティ（Registration Certificate Properties）] をクリックすると、サーバの証明書情報を確認できます。各登録証明書を展開してプロパティを表示後、[新規登録証明書の追加（Add new registration certificate）] をクリックし、証明書ファイルを参照して [更新（Update）] をクリックすると、図 9-23 に示すように、証明書をアップグレードすることができます。

図 9-23 [登録証明書のプロパティ（Registration Certificate Properties）]

注 CSPC は、1 つのコレクタで複数のサービスをサポートし、10,000 台以上のデバイスをアップロードできます。証明書は随時インストールできます。最初の証明書はインストール時に適用されます。1 つのサービスに複数の登録証明書を追加する場合、会社名はすべての証明書で同じにする必要があります。また、同じコレクタ上でサービスが異なる場合は、企業名は同じでなくてもかまいません。同じコレクタの別のサービス用に複数の登録証明書をアップロードして、証明書に基づいて設定することができます。サービス名は登録証明書と合わせる必要があります。2.7 より前に作成された古い証明書は、新規インストールでは機能しませんが、アップグレードすることは可能です。サービス固有の登録証明書は、特定のサービスのバックエンドにデータをアップロードするために使用されます。

[診断ツール（Diagnostic Tools）]

このオプションでは、デバイスが利用可能か、またはデバイスへの接続が確立されているかを確認するための *ping* や *traceroute* などのシンプルな診断ツールを利用できます。使用するコマンドを選択し、診断を実行するデバイスを選択して、[コマンドの実行（Run Command）] をクリックします。結果は、ウィンドウの [コマンドの結果（Command Result）] セクションに表示されます。

図 9-24　　診断ツール - ping ユーティリティ

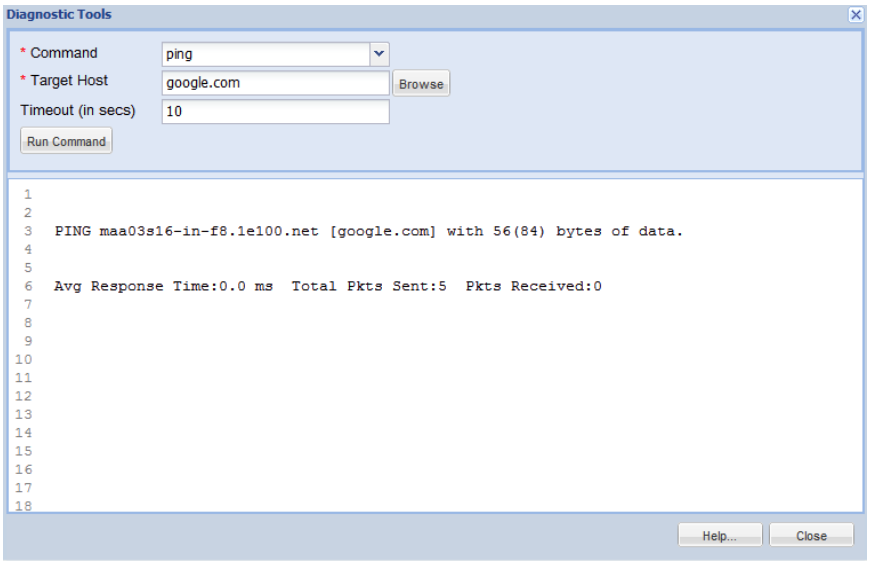
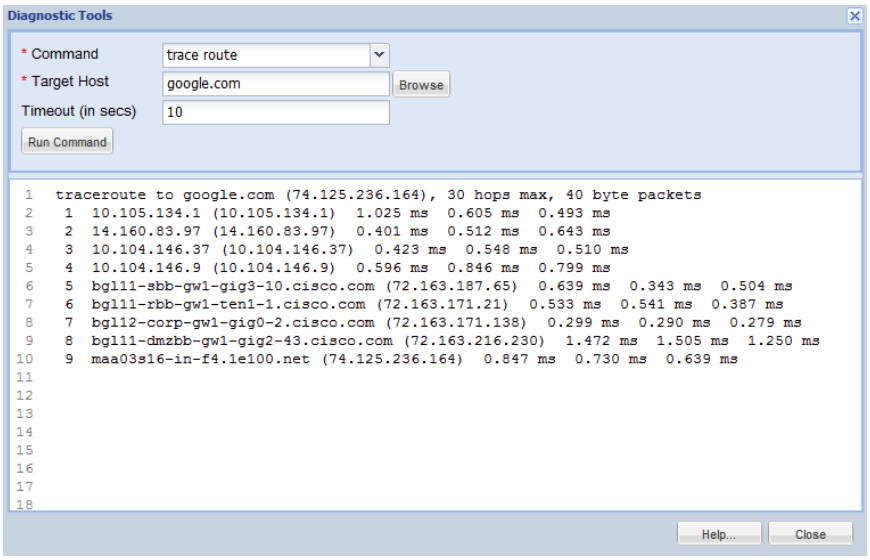


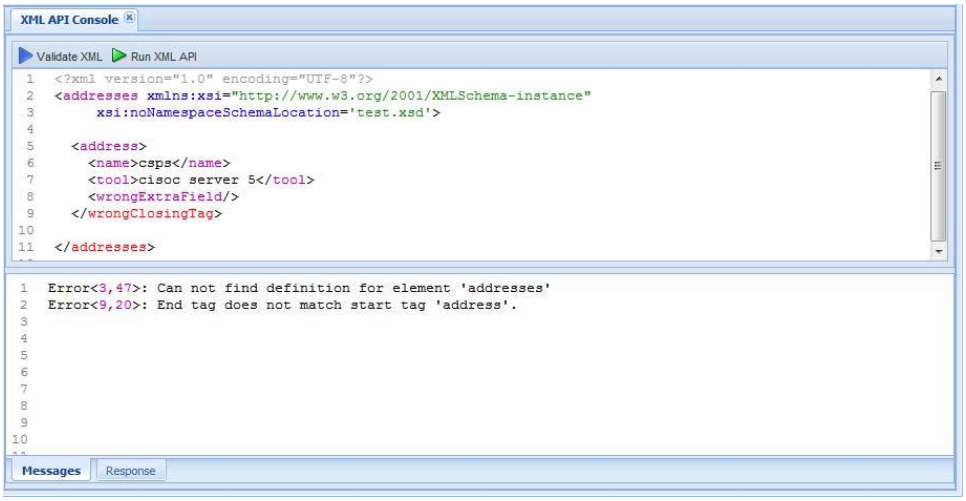
図 9-25　　診断ツール - Trace Route ユーティリティ



[XML API コンソール（XML API Console）]

[XML API コンソール（XML API Console）] オプションでは、CSPC サーバ上で XML API を実行することができます。このオプションを使用すると、サードパーティ アプリケーションを CSPC と統合させることができます。これを示しているのが図 9-26 です。

図 9-26　　[XML API コンソール（XML API Console）]



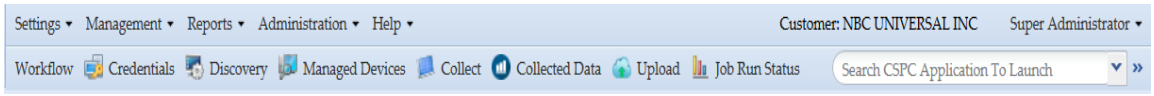
10

メニュー オプション

メニュー

メニュー オプションは、アプリケーションに迅速にアクセスするための手段です。

図 10- 1　　メニュー オプション



CSPC のメニュー オプションは以下のとおりです。

- [ユーザ名（User Name）]
- [設定（Settings）]
- [管理（Management）]
- [レポート（Reports）]
- [管理（Administration）]
- [ヘルプ（Help）]
- クイック メニュー

[ユーザ名（User Name）]

CSPC アプリケーションにログインしているユーザの氏名/ユーザ名が表示されます。図 10-1 では、スーパー管理者がログインしています。

次のオプションがあります。

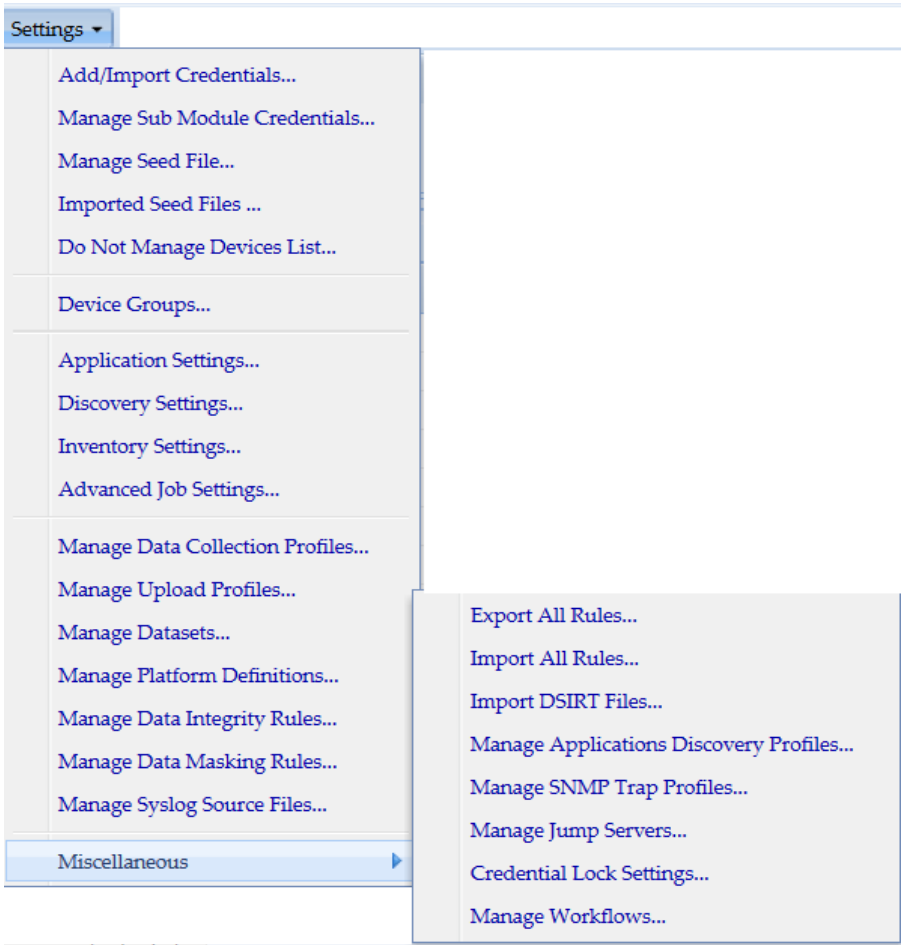
- [ログアウト（Logout）]：ログアウトして、CSPC クライアント アプリケーションを終了します。
- [パスワードの変更/設定（Change Password/settings）]：パスワードをリセットします。

メニュー

[設定（Settings）]

次に示すように、メニュー バーの [設定（Settings）] には、デバイス クレデンシャルやデバイスの固有情報を収集するための収集プロファイルを設定するための各種オプションがあります。各オプションの詳細については、[アプリケーション（Applications）]>[デバイス管理（Device Management）] タブを選択して確認してください。

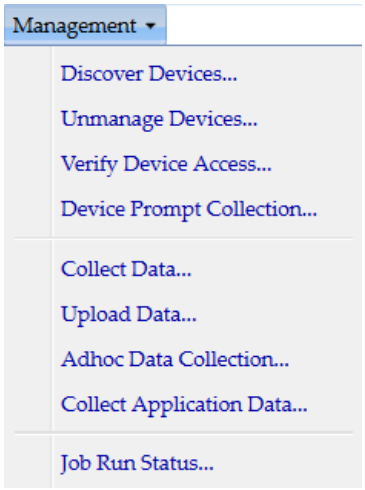
図 10- 2　　メニュー オプション - [設定（Settings）]



[管理（Management）]

次に示すように、メニュー バーの [管理（Management）] には、デバイスの検出と管理や収集プロファイル実行のための各種オプションがあります。各オプションの詳細については、[アプリケーション（Applications）] > [デバイス管理（Device Management）] タブを選択して確認してください。

図 10- 3　　メニュー オプション - [管理（Management）]

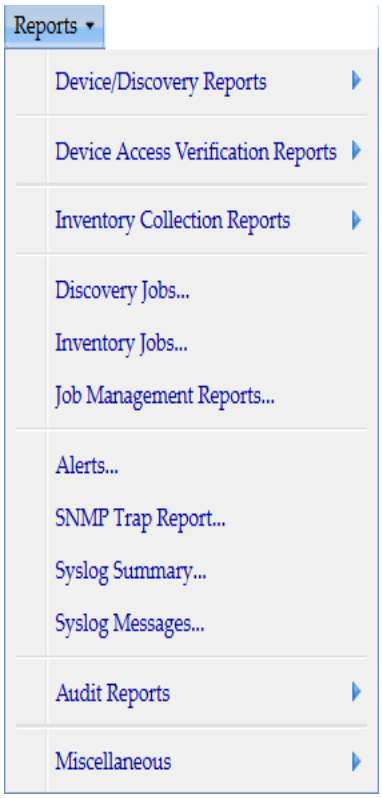


メニュー

[レポート（Reports）]

次に示すように、メニュー バーの [レポート（Reports）] には、収集したデータを表示するための各種レポート作成オプションがあります。各オプションの詳細については、[アプリケーション（Applications）] > [レポート（Reports）] タブを選択して確認してください。

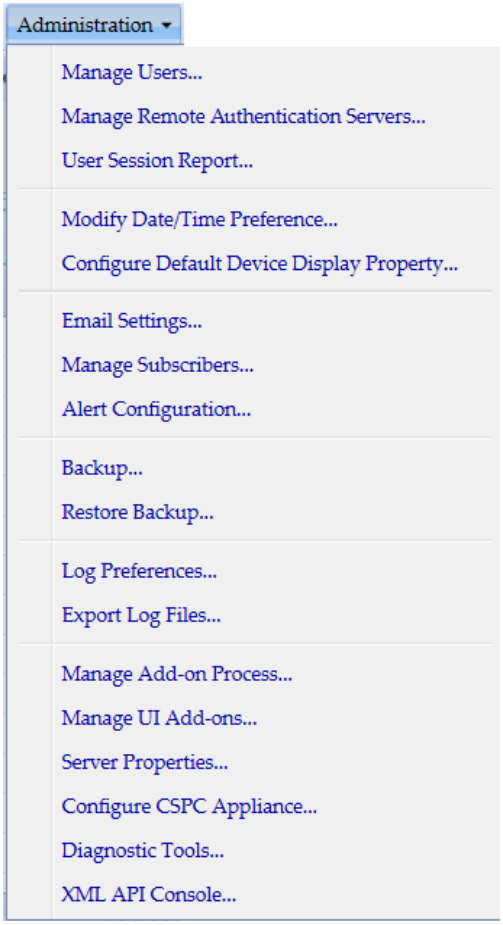
図 10- 4　　メニュー オプション - [レポート（Reports）]



[管理（Administration）]

次に示すように、メニュー バーの [管理（Administration）] には、サーバ、デバイス、および収集プロファイルを管理するための各種オプションがあります。各オプションの詳細については、[アプリケーション（Applications）]>[管理（Administration）] タブを選択して確認してください。

図 10- 5　　メニュー オプション - [管理（Administration）]



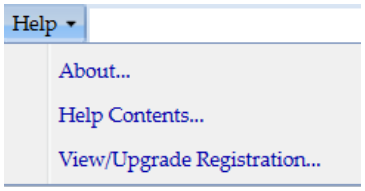
メニュー

[ヘルプ（Help）]

[ヘルプ（Help）] メニューには次のオプションが表示されます。

- [バージョン情報（About）]
- [ヘルプ コンテンツ（Help Contents）]
- [表示/アップグレード登録（View/Upgrade Registration）]

図 10- 6　　メニュー オプション - [ヘルプ（Help）]

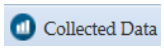
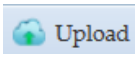


クイック メニュー

このメニューでは、CSPC の重要な機能に迅速かつ簡単にアクセスできます。

表 10-1　クイック メニュー

メニュー オプション	説明
Credentials	このメニューは、[デバイス クレデンシャル（Device Credentials）] ページにアクセスします。詳細については、[クレデンシャルの追加/インポート（Add/Import Credentials）] を参照してください。
Discovery	このメニューは、[検出方式の選択（Select Discovery Methods）] ページにアクセスします。詳細については、[デバイスの検出（Discover Devices）] を参照してください。
Managed Devices	このメニューは、[検出されたデバイスの表示（View Discovered Devices）] ページにアクセスします。詳細については、[検出されたデバイスの表示（View Discovered Devices）] を参照してください。
Collect	このメニューは、[収集プロファイルの選択（Select Collection Profile）] ページにアクセスします。詳細については、[データの収集（Collect Data）] を参照してください。

メニュー	
	このメニューは、[収集されたデータの表示（View Collected Data）] ページにアクセスします。詳細については、[収集されたデバイスの表示（View Collected Devices）] を参照してください。
	このメニューは、[アップロード プロファイルの選択（Select Upload Profile）] ページにアクセスします。詳細については、[データのアップロード（Upload Data）] を参照してください。
	このメニューは、[ジョブの実行状況（Job Run Status）] ページにアクセスします。詳細については、[ジョブの実行状況（Job Run Status）] を参照してください。

A

CSPC へのデバイスの追加

概要

CSPC にデバイスを追加するには、2 つのステップを続けて実行します。まず、デバイス クレデンシャルを追加します。ただし、デバイス クレデンシャルを追加してもデバイスは追加されません。クレデンシャルを追加したら、追加でデバイス管理の手順を行う必要があります。デバイスの管理ではクレデンシャルを使用して、SNMP 経由でデバイスに接続し、デバイスの分類データを収集します。

クレデンシャルの追加方法は 2 つあります。個別に追加する方法と、インポートを使用して追加する方法です。クレデンシャルは次のようなアプリケーションからインポートできます。

- Cisco Works DCR XML ファイル（.xml）
- Pari Networks クレデンシャル リポジトリ（.xml）
- Cisco Works DCR CSV ファイル（.csv）
- CNC CSV ファイル（.csv）
- 通常の CSV ファイル（.csv）

クレデンシャルの追加は、方法に関わらずすべて [クレデンシャル（Credentials）] 画面上で行います。

CSPC では、クレデンシャルとデバイス間に 1 対多の関係があります。1 つのクレデンシャルに対して複数のデバイスが保存されます。複数のデバイスは、IP アドレスが一致するワイルドカードを指定して、または IP アドレスを列挙して指定できます。IP アドレスが一致するワイルドカードを指定することを推奨します。

1 回目の収集で、最初のワイルドカードに一致するデバイスでの収集が失敗した場合、2 番目のワイルドカードに一致するデバイスが試されます。その後の収集では、前回成功したクレデンシャルが最初に試されます。

また、データセット タイプのプロトコルは、クレデンシャルの順序で判断されます。たとえば、SSH と Telnet 間の選択は、SSH と Telnet のクレデンシャルの順序で制御されます。

そのため、クレデンシャルの順序は重要であり、変更することができます。

クレデンシャルはエクスポートできますが、対応形式は Pari Credentials ファイル形式だけです。

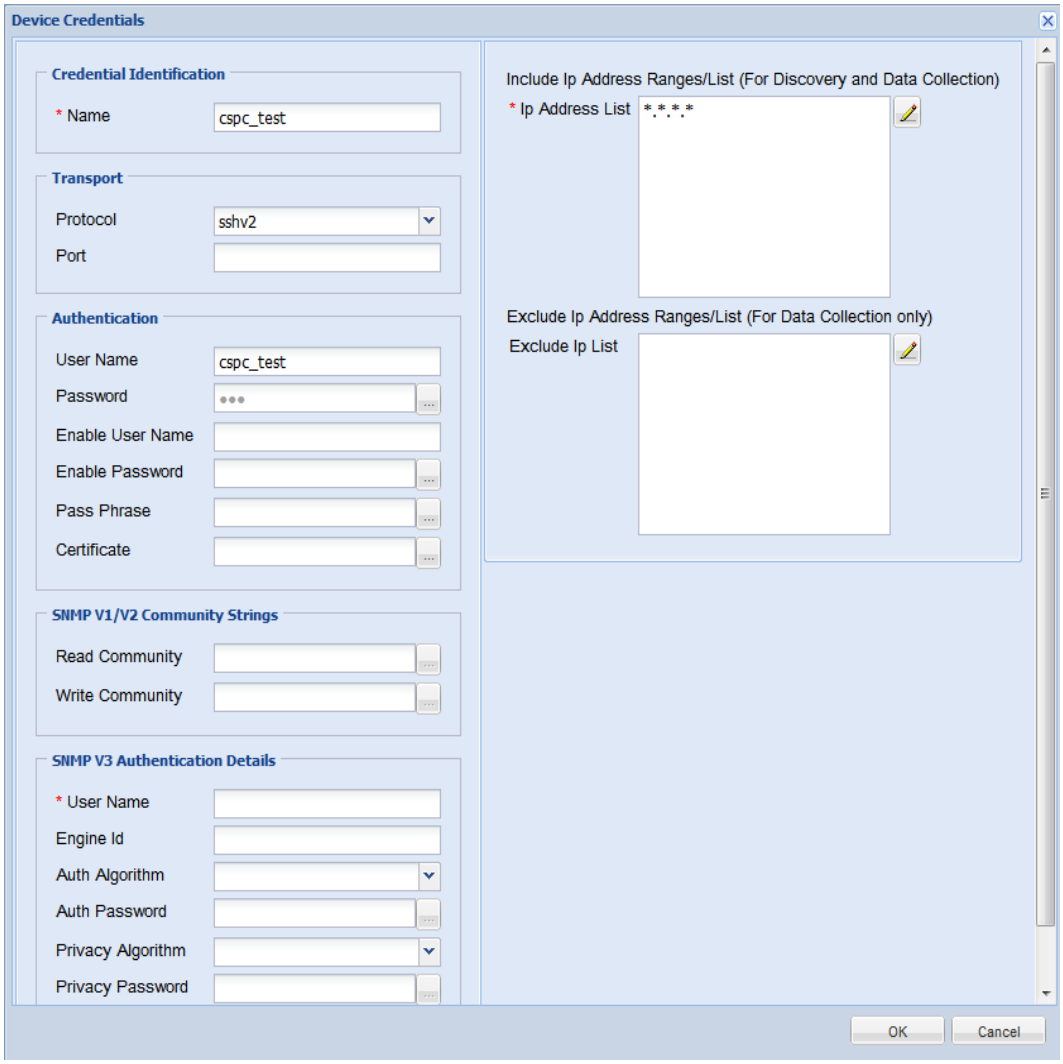
クレデンシャルを追加すると、デバイスを管理できます。クレデンシャルは、IP アドレスが一致するワイルドカード、または IP アドレス自体を指定して入力する必要がありますが、デバイスは IP アドレスまたは DNS 名で管理できます。

概要

例

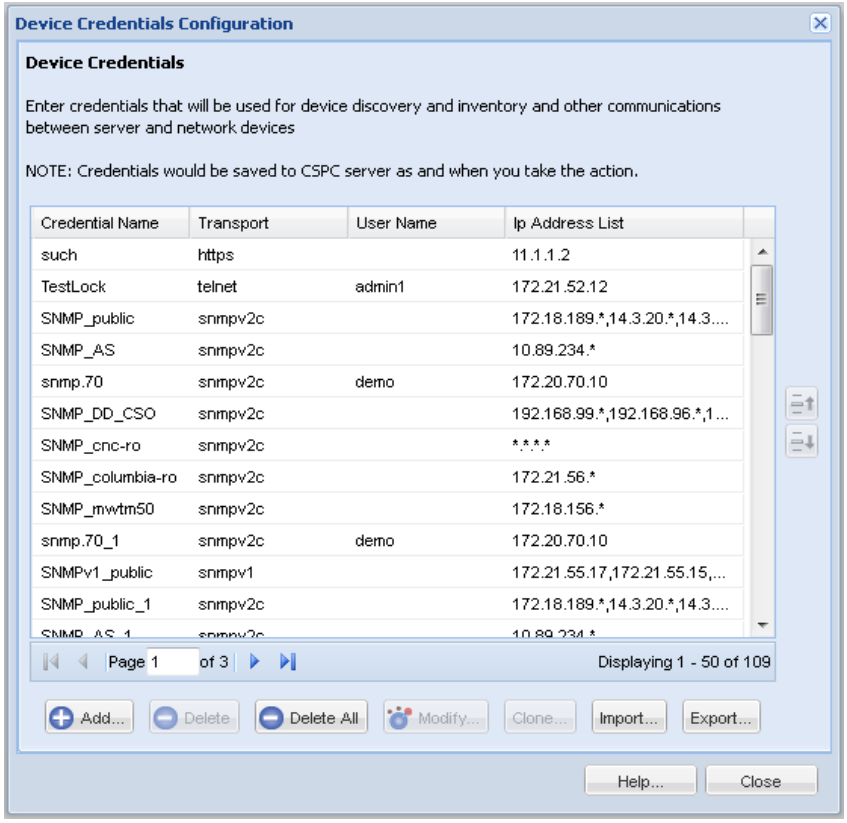
次の例では、ワイルドカードに対して SSH クレデンシャルが追加されています。

図 A-1　　[デバイス クレデンシャル（Device Credentials）]



結果を図 A-2 に示します。

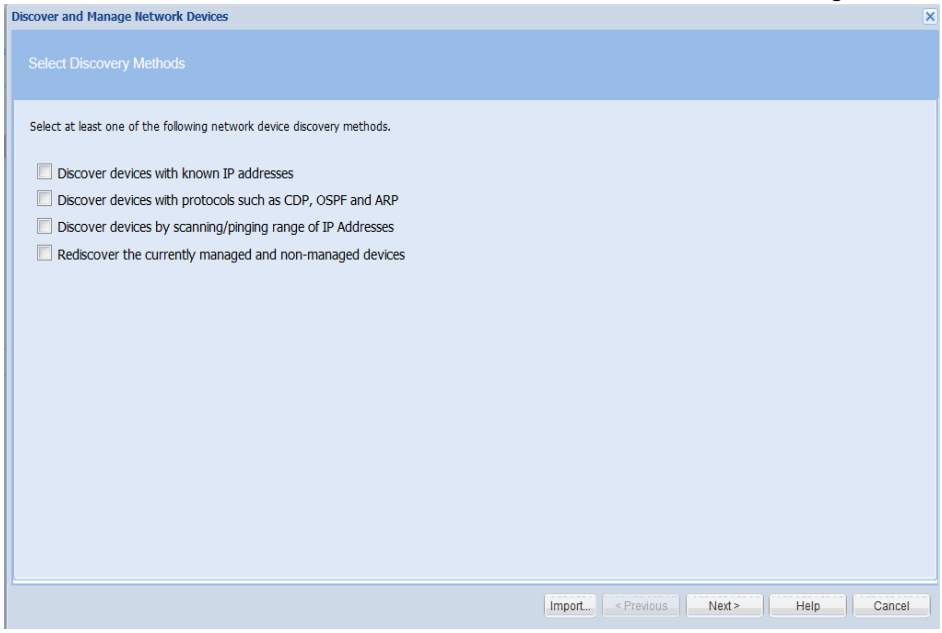
図 A-2　　[デバイス クレデンシャルの設定（Device Credential Configuration）]



これで、デバイスは管理可能になりました。デバイスは、既知のデバイスの再認識によって管理されます。これは何もデバイスを検出しない特別なディスカバリー（収集）です。

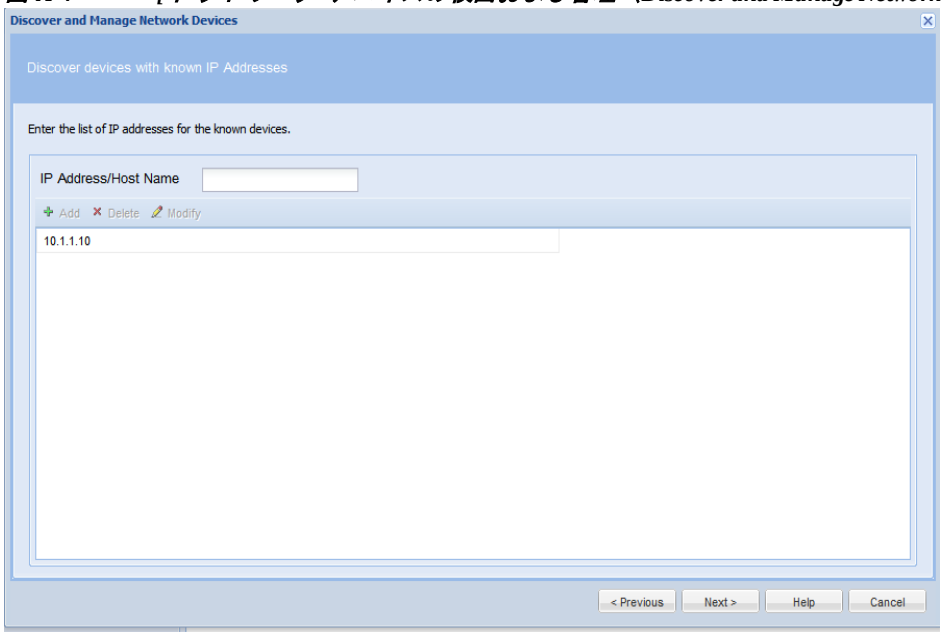
概要

図 A-3　　[ネットワーク デバイスの検出および管理（Discover and Manage Network Devices）]



IP アドレスまたは DNS 名のいずれかです。

図 A-4　　[ネットワーク デバイスの検出および管理（Discover and Manage Network Devices）]



B

シード ファイルの形式

CSPC では、次のシード ファイル形式がサポートされます。

1. CNC シード ファイル形式
2. Cisco Works シード ファイル形式
3. 簡易シード ファイル形式

CNC シード ファイル形式には次の 3 つの形式があります。

1. CNC 20 フィールド形式
2. CNC 30 フィールド形式
3. CNC 36 フィールド形式

Cisco Works には次の 2 つの形式があります。

1. Cisco Works 30 フィールド形式
2. Cisco Works 34 フィールド形式

注 上記のシード ファイル形式はすべて *.csv* タイプです。

簡易シード ファイル形式では、ワイルド カードを使用してすべてのデバイスまたはデバイス セットのクレデンシャルを簡単に指定できます。

簡易形式とそれ以外の形式の基本的な違いは、同じデバイスに対して複数のエントリがあり、各エントリが 1 つのプロトコルに対応していることです。その他の形式では、すべてのデバイスに対して同じエントリを使用します。

ヘッダー情報

CNC シード ファイル形式

CNC 20 フィールド形式のヘッダーには次のフィールドが含まれています。

; Col# = 1: Name (including domain or simply an IP),
; Col# = 2: RO community string,
; Col# = 3: RW community string,
; Col# = 4: Serial Number,
; Col# = 5: User Field 1,
; Col# = 6: User Field 2,
; Col# = 7: User Field 3,
; Col# = 8: User Field 4,
; Col# = 9; Name = Telnet password,
; Col# = 10; Name = Enable password,
; Col# = 11; Name = Enable secret,
; Col# = 12; Name = Tacacs user,
; Col# = 13; Name = Tacacs password,
; Col# = 14; Name = Tacacs enable user,
; Col# = 15; Name = Tacacs enable password,
; Col# = 16; Name = Local user,
; Col# = 17; Name = Local password,
; Col# = 18; Name = Rcp user,
; Col# = 19; Name = Rcp password,
; Col# = 20; Name = Enable User,

CNC 30 フィールド形式のヘッダーには次のフィールドが含まれています。

; Col# = 1: IP Address (including domain or simply an IP),
; Col# = 2: Host Name,
; Col# = 3: Domain Name,
; Col# = 4: Device Identity,
; Col# = 5: Display Name,
; Col# = 6: SysObjectID,
; Col# = 7: DCR Device Type,
; Col# = 8: MDF Type,
; Col# = 9; Snmp RO
; Col# = 10; Snmp RW

; Col# = 11; SnmpV3 User Name
; Col# = 12; Snmp V3 Auth Pass
; Col# = 13; Snmp V3 Engine ID
; Col# = 14; Snmp V3 Auth Algorithm
; Col# = 15; RX Boot Mode User
; Col# = 16; RX Boot Mode Pass
; Col# = 17; Primary User (Tacacs User)
; Col# = 18; Primary Pass (Tacacs Pass)
; Col# = 19; Primary Enable Pass
; Col# = 20; Http User
; Col# = 21; Http Pass
; Col# = 22; Http Mode
; Col# = 23; Http Port
; Col# = 24; Https Port
; Col# = 25; Cert Common Name,
; Col# = 26; Secondary User,
; Col# = 27; Secondary Pass,
; Col# = 28; Secondary Enable Pass,
; Col# = 29; Secondary Http User,
; Col# = 30; Secondary Http Pass,

CNC 36 フィールド形式のヘッダーには次のフィールドが含まれています。

; Col# = 1: IP Address (including domain or simply an IP),
; Col# = 2: Host Name,
; Col# = 3: Domain Name,
; Col# = 4: Device Identity,
; Col# = 5: Display Name,
; Col# = 6: SysObjectID,
; Col# = 7: DCR Device Type,
; Col# = 8: MDF Type,
; Col# = 9; Snmp RO
; Col# = 10; Snmp RW
; Col# = 11; SnmpV3 User Name
; Col# = 12; Snmp V3 Auth Pass
; Col# = 13; Snmp V3 Engine ID
; Col# = 14; Snmp V3 Auth Algorithm
; Col# = 15; RX Boot Mode User

; Col# = 16; RX Boot Mode Pass
; Col# = 17; Primary User (Tacacs User)
; Col# = 18; Primary Pass (Tacacs Pass)
; Col# = 19; Primary Enable Pass
; Col# = 20; Http User
; Col# = 21; Http Pass
; Col# = 22; Http Mode
; Col# = 23; Http Port
; Col# = 24; Https Port
; Col# = 25; Cert Common Name,
; Col# = 26; Secondary User,
; Col# = 27; Secondary Pass,
; Col# = 28; Secondary Enable Pass,
; Col# = 29; Secondary Http User,
; Col# = 30; Secondary Http Pass,
; Col# = 31; Snmp V3 Priv Algorithm,
; Col# = 32; Snmp V3 Priv Pass,
; Col# = 33; User Field 1,
; Col# = 34; User Field 2,
; Col# = 35; User Field 3,
; Col# = 36; User Field 4,

Cisco Works シード ファイル形式

Cisco Works 30 シード ファイルのヘッダーには次のフィールドが含まれています。

- management_ip_address
- host_name
- domain_name
- device_identity
- display_name
- sysObjectID
- dcr_device_type　mdf_type　snmp_v2_ro_comm_string
- snmp_v2_rw_comm_string
- snmp_v3_user_id　snmp_v3_password　snmp_v3_engine_id
- snmp_v3_auth_algorithm
- rxboot_mode_username

- rxboot_mode_password
- primary_username
- primary_password
- primary_enable_password
- http_username
- http_password
- http_mode
- http_port
- https_port
- cert_common_name
- secondary_username
- secondary_password
- secondary_enable_password
- secondary_http_username
- secondary_http_password

Cisco Works 34 シード ファイルのヘッダーには次のフィールドが含まれています。

- management_ip_address
- host_name
- domain_name
- device_identity
- display_name
- sysObjectID
- dcr_device_type
- mdf_type
- sysContact
- sysLocation
- snmp_v2_ro_comm_string
- snmp_v2_rw_comm_string
- snmp_v3_user_id
- snmp_v3_password
- snmp_v3_engine_id
- snmp_v3_auth_algorithm
- snmp_v3_priv_password
- snmp_v3_priv_algorithm
- rxboot_mode_username
- rxboot_mode_password

- primary_username
- primary_password
- primary_enable_password
- http_username
- http_password
- http_mode
- http_port
- https_port
- cert_common_name
- secondary_username
- secondary_password
- secondary_enable_password
- secondary_http_username
- secondary_http_password

簡易シード ファイル形式

簡易シード ファイルのヘッダーには次のフィールドが含まれています。

- IPAddress
- protocol
- port
- username
- password
- enableusername
- enablepassword
- SnmpRO
- SnmpRW
- SnmpV3Id
- SnmpV3Password
- SnmpV3EngineId
- Snmpv3AuthAlogorithm
- SnmpV3PrivAlgorithm
- SnmpVPrivPassword

エクスポートファイル形式

Service Appliance 1.0 のエクスポート ユーティリティによって生成されるファイルのコンテンツは以下のとおりです。

; Col# = 1: IP Address (including domain or simply an IP)

; Col# = 2: Host Name
; Col# = 3: Domain Name
; Col# = 4: Device Identity
; Col# = 5: Display Name
; Col# = 6: SysObjectID
; Col# = 7: DCR Device Type
; Col# = 8: MDF Type
; Col# = 9; Snmp RO
; Col# = 10; Snmp RW
; Col# = 11; SnmpV3 User Name
; Col# = 12; Snmp V3 Auth Pass
; Col# = 13; Snmp V3 Engine ID
; Col# = 14; Snmp V3 Auth Algorithm
; Col# = 15; RX Boot Mode User
; Col# = 16; RX Boot Mode Pass
; Col# = 17; Primary User(Tacacs User)
; Col# = 18; Primary Pass(Tacacs Pass)
; Col# = 19; Primary Enable Pass
; Col# = 20; Http User
; Col# = 21; Http Pass
; Col# = 22; Http Mode
; Col# = 23; Http Port
; Col# = 24; Https Port
; Col# = 25; Cert Common Name
; Col# = 26; Secondary User
; Col# = 27; Secondary Pass
; Col# = 28; Secondary Enable Pass
; Col# = 29; Secondary Http User
; Col# = 30; Secondary Http Pass
; Col# = 31; Snmp V3 Priv Algorithm
; Col# = 32; Snmp V3 Priv Pass
; Col# = 33; User Field 1
; Col# = 34; User Field 2
; Col# = 35; User Field 3
; Col# = 36; User Field 4
; Col# = 37; Status_Msg

C

サポートされる Syslog の形式

CSPC は次の Syslog 形式をサポートします。

- Nov 26 17:44:42 *customer* evlogd: [local-60sec42.542] [sessmgr 12988 unusual] [7/1/4486 <sessmgr:28> ssmgr_gr_sess.c:1379] [callid 082be77b] [context: PGWin, contextID: 2] [software internal system critical-info syslog] ucheck-point failed for the cmd: 43
- Nov 26 17:42:21 [x.x.x.x.x.x] evlogd: [local-60sec21.785] [sessmgr 12988 unusual] [10/0/5440 <sessmgr:246> ssmgr_gr_sess.c:1379] [callid 4571e772] [context: XGWin, contextID: 6] [software internal system critical-info syslog] ucheck-point failed for the cmd: 43
- x.x.x.x x: RP/0/RP0/CPU0:Dec 15 20:34:47.343 UTC: exec[65724]: %SECURITY-login-4-AUTHEN_FAILED : Failed authentication attempt by user 'lab' from '172.21.31.17' on 'vty0'
- Apr 12 01:51:22 x.x.x.x x: RP/0/RP0/CPU0:Apr 12 02:09:47.690 UTC: exec[65741]: %SECURITY-login-4-AUTHEN_FAILED : Failed authentication attempt by user 'lab' from '10.142.36.103' on 'vty0'
- x.x.x.x x: 001604: *Jun 24 06:09:16.102 PST: %LINK-5-CHANGED: Interface Loopback123, changed state to administratively down
- x.x.x.x x: 22w1d: %SYS-5-CONFIG_I: Configured from console by vty1 (64.103.247.104)

注 CSPC は、CNC でサポートされるすべての Syslog 形式もサポートします。

D

ネットワークアドレス変換アプライアンスのオプション パラメータ

この機能によって、CSPC サーバの IP アドレスを設定したコマンドで、TFTP データセット/CLI データセット/ApplyIPSsignature/ApplyConfig を作成/実行することができます。CSPC サーバの IP アドレスは、TFTP データセット/CLI データセット/ApplyIPSsignature/ApplyConfig の実行時に動的に追加される必要があります。CLI データセット/ApplyIPSsignature/ApplyConfig でこの機能を使用するには、CSPC サーバの IP アドレスを置き換える必要があるコマンドに <#SERVERIP#> という独自のタグを追加しなければなりません。TFTP データセットは、更新する必要はありません。デフォルトでは、CSPC は自分自身の IP に置き換えますが、外部から参照可能な IP が、内部の CSPC IP と違う場合は、次の XML を使用して、<#SERVERIP#> タグを置き換える IP を追加/変更します。

CSPC サーバの IP アドレスを追加/変更するには、次の XML API を使用します。

<Request requestId="" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"

xsi:schemaLocation="http://www.parinetworks.com/api/schemas/1.1 pari_api.xsd"

xmlns="http://www.parinetworks.com/api/schemas/1.1">

<Manage>

<Add operationId="1">

<ServerDetails>

<IPAddress>x.x.x.x</IPAddress>

</ServerDetails>

</Add>

</Manage>

</Request>

E

条件付き収集

条件付き収集についての説明

「条件付き収集」という用語は一般に、一連の条件または別のデータ収集の結果に基づいて行われる、収集に関するあらゆる判断（収集するかどうか、何を収集するか、何回収集するか）を表します。これと同じ意味を表す用語として、「複合収集」、「動的収集」、「後続収集」があります。

サポート対象

監査の使用例

- データセット（SNMP または CLI）の実行
- 出力の解析と一連の値の取得
- 上で取得した各値に対する別のコマンドの実行

Cisco CallManager の使用例

Cisco CallManager 検出では、SysOID が一連の設定可能な OID の 1 つで、追加の OID が値を返す場合、デバイスは Cisco CallManager と見なされ、CCM CallManager プラットフォームが適用されます。

サポートの詳細：

これは条件付き収集でサポートされます。ただし、CSPC における「プラットフォーム定義」は検出操作の結果のみに依存し、
インベントリ収集の結果には依存しません。

つまり、プラットフォーム定義は次のように実装する必要があります。

1. 一連の SysOID を指定してプラットフォームの「対象の CallManager」を定義する
2. 「対象の CallManager」プラットフォームにのみ適用される条件付き収集を定義する
3. この条件付き収集では、追加の OID を実行し、その戻り値に基づいて収集したい最終的なデータセットを収集する

SNMP/CLI 設定のフォールバック収集

デバイスからの設定の収集を制御する設定は 4 つあります。CLI のみの場合と SNMP のみの場合、後続収集は必要ありません。ただし、SNMP への CLI フォールバック設定と CLI への SNMP フォールバック設定では、最初に試みたプロトコルが失敗した場合には、後続収集が実行されます。

サポートの詳細：

これは条件付き収集でサポートされます。ただし、これは設定を収集する場合には有効ですが、それ以外の収集にはそれほど役立たない可能性があります。

例：インターフェイスの統計情報は、SNMP で収集したか、CLI で収集したかによって出力がまったく異なるものになる場合があります。

後続収集に基づいて収集された値

これはインベントリよりも監査でよく見られる例です。これは RBML の「条件」ブロックで制御される後続収集の例です。そのため、「真」の条件付き収集と見なすことができます。

サポートの詳細：

この使用例は、上記の監査の使用例の一部としてサポートされます。

再ログインが必要なコマンド

異なるスロットのカードにアクセスするためにコミュニティ ストリングを変えて同じデバイスに複数回ログインする必要があるコマンド

この例では、同じ OID が同じデバイスに対して複数回（異なるスロットの異なるカードにログインするたびに）発行されます。ここでは、変えるのはコマンドではなく、コミュニティ ストリングです。パスワード *public@SM_1* を使用してログインし、スロット モジュール 1 のカードにアクセスします。これらは WAN スイッチに対して発行されます。

サポートの詳細：

これは条件付き収集でサポートされます。ただし、サポートはコミュニティ ストリングの動的な変更に制限されます（ユーザ名/パスワードやデバイスの IP アドレスなどのその他のクレデンシャルの動的な変更はサポートされません。このような要件がある場合は、追加モジュールで処理する必要があります）。

条件付き収集の詳細

CSPC の条件付き収集は再帰アルゴリズムに基づいており、最後の処理が完了するまで各処理単位からの出力が次の処理単位への入力として渡されます。

ステートメント

ステートメントは条件付き収集における基本的な処理単位です。ステートメントは各処理単位の開始点を示します。各ステートメントは「ID」で識別され、オプションでタイトルを入力することができます。ステートメントは <Statement> タグで表されます。

ステートメントには次の 2 つのタイプがあります。

1. 条件
2. ループ

各ステートメントの入力はステートメントタイプによって異なります。入力は、条件ステートメントの場合はスカラー入力、ループ ステートメントの場合はベクトル入力です。

条件ステートメント

条件ステートメントは <Condition> タグで表され、ステートメント ID で識別されます。条件ステートメントの各入力はベクトル入力です。入力の出力を処理するには、<Operation> タグを使用します。<Operation> タグでは、ユーザが出力に対する操作を選択します。実行した操作に基づいて、<Match> タグと <NonMatch> タグを使用して単一の処理単位を続行するか、次の処理に移るかを決定できます。

<Match> タグと <NonMatch> タグでは、ユーザは値を変数に保存できます。この変数はそれ以降の処理に使用できます。値を保存するには、<Match> タグの下で <Assignment> タグを使用します。実行した操作に基づき、エンジンを使用して次の操作を実行できます。

a. 次のステートメントを実行する（<Goto> を使用）
b. 処理から取得した次の値を使用する（<Continue> を使用）
c. プロセスを終了する（<Exit> を使用）
d. 特定のマッチング状況で再帰を中断する（<Break> を使用）

条件ステートメントが、条件付き収集の出力が行われる最後の実行プログラムである場合は、<Output> タグを使用します。CSPC では、次の 2 つのタイプの出力処理が現在サポートされています。

1. **Dataset**：前の手順で得られた変数を使用して別のデータセットを実行します。データセットでは、割り当てに使用した変数文字列（大文字と小文字は区別されます）を使用する必要があります。

   例：変数名が "name" で、出力データセットが各スロットへのログインである場合、コマンドは **`session slot <`*`name`*`> processor 1`** になります。
2. **AddOutput**：このタイプの出力を使用すると、処理した出力をユーザが希望する形式で表示できます。

スカラー入力

スカラー入力は条件ステートメントの必須要素であり、条件ステートメントでのみ使用できます。条件ステートメントでの処理には、次の 5 つのタイプのスカラー入力を使用できます。

1. **デバイスのプロパティ**：デバイスのプロパティの確認に使用します。
2. **変数**：初期化で使用します。
3. **データセット**：デバイスで何らかのコマンドを実行する場合に必要となるデータセットの名前。
4. **ループ コンテキスト**：現在のループから入力を取得する必要がある場合にエンジンと通信する入力データ タイプ。

5. **SNMPIndex/SNMPOid/SNMPValue**：SNMP データの処理に使用します。

操作

スカラー入力の出力を処理するには、<Operation> タグを使用します。操作には、次の 2 つのタイプがあります。

1. **文字列操作**：Java の正規表現で使用します。各マッチング パターンが Java 文字列と比較され、matches（一致する）、doesnotmatch（一致しない）、contains（含む）、doesnotcontain（含まない）、isEmpty（空かどうか）、equals（等しい）、notEquals（等しくない）のチェックが行われます。
2. **ベクトル操作**：通常の Java ベクトルとして使用します。出力を変数に追加し、それ以降の処理に使用できます。

割り当て

条件ステートメントの割り当てでは、各操作の最後に、得られた変数に値が割り当てられます。変数に値を割り当てるには、<Variable> タグの割り当ての下に変数を作成します。変数は、次の重要なタグに基づいて結果として得られた値が割り当てられます。

a. **append**：一致する結果を、得られた変数に追加する必要があるかどうかを示します。
b. **onlyIfNotNull**：結果が null でない場合にのみ、結果を変数に追加します。
c. **trim**：結果の文字列をトリミングしてから変数に追加します。
d. **vectorType**：List/Set/OrderedList。結果を結果のリストに追加します。デフォルトでは、結果はリストに追加されます。ただし、挿入順序を保持する必要がある場合は、OrderedList を使用する必要があります。Set は、変数に対して、一意の結果文字列が必要な場合にのみ使用します。
e. **Operation**：Add/Remove。Add は結果を結果リストに追加し、Remove は結果リストに存在する文字列を削除します。

ループ ステートメント

ループは、while ループのように終了条件が満たされるまで各ステートメントが再帰的に実行されます。ループ ステートメントは <Loop> タグで表され、ステートメント識別子で識別されます。ループ ステートメントは、どの条件付き収集データセットにおいても、最初のステートメントになります。

ループ ステートメントの各入力はベクトル入力です。各ループ ステートメントは条件ステートメントで終了する必要があります。ベクトル入力から収集されたデータは、特定の一致条件と条件ステートメントによってさらに処理されます。

ベクトル入力

条件付き収集では、4 つのタイプのベクトル入力が使用されます。各ベクトル入力には、複合収集のニーズを達成するうえで個別の重要性があります。4 つのタイプのベクトル入力は次のとおりです。

1. **ブロック ベクトル入力**：ブロック ベクトル入力は、デバイス応答からの応答ブロックを処理する必要がある場合に使用します。各ブロック入力には、必須の <Input> フィールドと <Params> フィールドがあります。ブロック内の入力には、SNMP 以外の任意のスカラー入力を使用できます。<Params> フィールドには、ブロックの開始と終了を示す開始文字列と終了文字列があります。また、開始文字列と終了文字列には、Java のパターン マッチングが適用されます。一致したパターンの結果は、条件ステートメントまたはループ ステートメントでさらに処理されます。

2. **行ベクトル入力**：行ベクトル入力は、デバイスからの応答を 1 行ずつ処理する必要がある場合に使用します。各行入力には、必須の <Input> フィールドと <Params> フィールドがあります。行内の入力には、SNMP 以外の任意のスカラー入力を使用できます。<Params> フィールドには文字列の <Match> タグ一致条件があり、Java のパターン マッチングが結果に適用されます。一致したパターンの結果は、条件ステートメントまたはループ ステートメントでさらに処理されます。
3. **SNMP テーブル**：SNMP テーブルからの SNMP 応答の処理に使用します。各 SNMP 入力には、必須の <Input> フィールドと <Rows> フィールドがあります。SNMP の入力には、SNMP スカラー入力を使用する必要があります。
4. **変数ベクトル入力**：Java の配列リストに似ています。入力リストが生成され、さらなる処理のために後続の処理単位に渡されます。

アクション

アクションは、条件付き収集でリクエストの処理前、処理中、または処理後に特定のアクションを実行する必要がある場合に使用します。ほとんどの場合、アクションでは変数への割り当てを実行します。この変数はそれ以降の処理に使用されます。

例

CLI 複合収集

デバイスから Show インターフェイスを収集し、その後に「FastEthemet」文字列を含むインターフェイスのインターフェイス ステータスを取得します。

```
<Dataset identifier="ios_show_int_accounting_dynamic">
<Type>Dynamic</Type>
<Title>ios_show_int_accounting_dynamic</Title>
<CollectionType>CLI</CollectionType>
<CategoryName> show_int_accounting</CategoryName>
<Statements>
<Loop identifier="_show_interface_1">
<VectorInput>
<Line>
<Input>
<Dataset>
<DatasetName Failure="error_message">_show interface</DatasetName>
</Dataset>
</Input>
<Params>
<Match ignoreCase="false">FastEthernet[^A-Za-z_]*</Match>
```

```
</Params>
</Line>
</VectorInput>
<Statements>
<Condition identifier="output_cond">
<Input>
<LoopContext></LoopContext>
</Input>
<Operation>
<NotEquals ignoreCase="true"></NotEquals>
</Operation>
<Match>
<Assignment>
<Variable append="false" onlyIfNotNull="true" trim="true" vectorType="List" operation="add">interface</Variable>
<Value></Value>
</Assignment>
<Output>
<Dataset>
<DatasetName>ios_show_interface accounting</DatasetName>
<Variables>
<Variable>interface</Variable>
</Variables>
</Dataset>
</Output>
<Continue></Continue>
</Match>
<NonMatch>
<Continue></Continue>
</NonMatch>
</Condition>
</Statements>
</Loop>
</Statements>
</Dataset>
```

SNMP 複合収集

<Dataset identifier="ifHCOutOctets_all_interfaces_9089">

<Type>Dynamic</Type>

<Title>ifHCOutOctets_all_interfaces For AIF: 9089 Created at Dec 20, 2011 9:48:06 PM</Title>

<CollectionType>SNMP</CollectionType>

<CategoryName>AIF_9089</CategoryName>

<Statements>

<Loop identifier="loop1">

<Title>Get SNMP Interface Types</Title>

<VectorInput>

<SNMPTable>

<Input>

<Dataset>

<DatasetName>ifType_9089_internal</DatasetName>

</Dataset>

</Input>

<Rows>

</Rows>

</SNMPTable>

</VectorInput>

<Actions>

<Assignment>

<Variable append="false" onlyIfNotNull="false" trim="false" vectorType="Set" Operation="add">ifTypes</Variable>

<Values>

<Value>6</Value><Value>62</Value><Value>5</Value><Value>6</Value><Value>9</Value><Value>15</Value><Value>17</Value><Value>18</Value><Value>19</Value><Value>22</Value><Value>28</Value><Value>30</Value><Value>32</Value><Value>37</Value><Value>39</Value><Value>49</Value><Value>63</Value><Value>73</Value><Value>76</Value><Value>77</Value><Value>81</Value><Value>100</Value><Value>101</Value><Value>102</Value><Value>103</Value><Value>107</Value><Value>108</Value><Value>131</Value><Value>134</Value><Value>166</Value><Value>171</Value></Values>

</Assignment>

</Actions>

<Statements>

<Condition identifier="loop1_cond1">

<Title>Check to see if Interface is require type</Title>

<Input>

<SNMPValue>

<LoopContext></LoopContext>
</SNMPValue>
</Input>
<Operation>
<IsMemberOf><VariableName>ifTypes</VariableName>
</IsMemberOf>
</Operation>
<Match>
<Goto></Goto>
</Match>
<NonMatch>
<Continue></Continue>
</NonMatch>
</Condition>
<Condition identifier="loop1_cond_last">
<Title>Save the ifIndex</Title>
<Input>
<SNMPIndex>
<LoopContext></LoopContext>
</SNMPIndex>
</Input>
<Operation>
<Matches ignoreCase="false">^.*¥.([0-9]+)$</Matches>
</Operation>
<Match>
<Assignment>
<Variable append="true" onlyIfNotNull="true" trim="true" vectorType="Set" Operation="add">interfaceList</Variable>
<Value><loop1_cond_last.1></Value></Assignment>
<Goto></Goto>
</Match>
<NonMatch>
<Continue></Continue>
</NonMatch>
</Condition>
</Statements>
</Loop>
<Loop identifier="loop2">

```
<Title>Get SNMP Interface Oper Status</Title>
<VectorInput>
<SNMPTable>
<Input>
<Dataset>
<DatasetName>ifOperStatus_9089_internal</DatasetName>
</Dataset>
</Input>
<Rows>
</Rows>
</SNMPTable>
</VectorInput>
<Statements>
<Condition identifier="loop2_cond1">
<Input>
<SNMPValue>
<LoopContext></LoopContext>
</SNMPValue>
</Input>
<Operation>
<Equals ignoreCase="false">1</Equals>
</Operation>
<Match>
<Continue></Continue>
</Match>
<NonMatch>
<Goto></Goto>
</NonMatch>
</Condition>
<Condition identifier="loop2_cond2">
<Title>Remove If Interface is not up</Title>
<Input>
<SNMPIndex>
<LoopContext></LoopContext>
</SNMPIndex>
</Input>
<Operation>
```

<Matches ignoreCase="false">^.*¥.([0-9]+)$</Matches>
</Operation>
<Match>
<Assignment>
<Variable append="false" onlyIfNotNull="false" trim="false" vectorType="List"
Operation="add">interfaceList</Variable>
<Value><loop2_cond2.1></Value></Assignment>
<Goto></Goto>
</Match>
<NonMatch>
<Continue></Continue>
</NonMatch>
</Condition>
</Statements>
</Loop>
<Loop identifier="last">
<Title>Collect the output</Title>
<VectorInput>
<SNMPTable>
<Input>
<Dataset>
<DatasetName>ifHCOutOctets_all_interfaces_9089_ifHCOutOctets</DatasetName>
</Dataset>
</Input>
<Rows>
</Rows>
</SNMPTable>
</VectorInput>
<Statements>
<Condition identifier="last_cond1">
<Input>
<SNMPIndex>
<LoopContext></LoopContext>
</SNMPIndex>
</Input>
<Operation>
<Matches ignoreCase="false">^.*¥.([0-9]+)$</Matches>

```
</Operation>
<Match>
<Assignment>
<Variable append="false" onlyIfNotNull="true" trim="true" vectorType="List" Operation="add">oid</Variable>
<Value></Value></Assignment>
<Goto></Goto>
</Match>
<NonMatch>
<Continue></Continue>
</NonMatch>
</Condition>
<Condition identifier="last_cond2">
<Title>Check to see if this is in the final List</Title>
<Input>
<Variable>last_cond1.1</Variable>
</Input>
<Operation>
<IsMemberOf><VariableName>interfaceList</VariableName>
</IsMemberOf>
</Operation>
<Match>
<Goto></Goto>
</Match>
<NonMatch>
<Continue></Continue>
</NonMatch>
</Condition>
<Condition identifier="last_cond3">
<Title>Add the value to the final output</Title>
<Input>
<SNMPValue>
<LoopContext></LoopContext>
</SNMPValue>
</Input>
<Operation>
<Matches ignoreCase="false">^(.*)$</Matches>
</Operation>
```

条件付き収集についての説明

```
<Match>
<Assignment>
<Variable append="false" onlyIfNotNull="true" trim="true" vectorType="List" Operation="add">interface</Variable>
<Value><last_cond1.1></Value></Assignment>
<Output>
<AddOutput>
<Value><SnmpDatasetResponse><SNMPRequest><RequestType>Column</RequestType><ObjectList><Object><oid></Object></ObjectList></SNMPRequest><SnmpResponse><Row><InstanceId><last_cond1.1></InstanceId><Columns><Column><last_cond3.1></Column></Columns></Row></SnmpResponse></SnmpDatasetResponse></Value>
<Variables>
<Variable>interface</Variable>
</Variables>
</AddOutput>
</Output>
<Goto></Goto>
</Match>
<NonMatch>
<Continue></Continue>
</NonMatch>
</Condition>
</Statements>
</Loop>
</Statements>
</Dataset>
```

F

XML API

シード ファイル ジョブ（すぐに実行用）

```
<Request requestId="" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                    xsi:schemaLocation="http://www.parinetworks.com/api/schemas/1.1
../../../../CSPC2.3Dev/pari/dash/resources/server/schema/pari_api.xsd"
                    xmlns="http://www.parinetworks.com/api/schemas/1.1">
          <Job>
            <Schedule operationId="1">
              <JobSchedule runnow="true">
              </JobSchedule>
              <RegressiveSeedFileJob>
                <TriggerDav>true</TriggerDav>
                <DeleteCreds>true</DeleteCreds>
                <DeleteDevices>true</DeleteDevices>
              </RegressiveSeedFileJob>
            </Schedule>
          </Job>
        </Request>
```

シード ファイル ジョブ（スケジュール実行用）

```
<Request requestId="" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                    xsi:schemaLocation="http://www.parinetworks.com/api/schemas/1.1
../../../../CSPC2.3Dev/pari/dash/resources/server/schema/pari_api.xsd"
                    xmlns="http://www.parinetworks.com/api/schemas/1.1">
          <Job>
            <Schedule operationId="1">
              <JobSchedule runnow="false">
                <Start>1409607000000</Start>
                <Repeat>
                  <IntervalMilliSeconds>600000</IntervalMilliSeconds>
```

```
            <!- <End>1254316663640</End>->
          </Repeat>
        </JobSchedule>
        <RegressiveSeedFileJob>
          <TriggerDav>true</TriggerDav>
          <DeleteCreds>true</DeleteCreds>
          <DeleteDevices>true</DeleteDevices>
        </RegressiveSeedFileJob>
      </Schedule>
    </Job>
  </Request>
```

通知の追加

```
<Request xmlns="http://www.parinetworks.com/api/schemas/1.1" requestId="4444">
  <Manage>
    <Add operationId="1">
      <NotificationList>
       <Notification>
       <TrapOID></TrapOID>
       <NotificationType></NotificationType>
       </Notification>
      </NotificationList>
    </Add>
  </Manage>
</Request>
```

すべての通知の削除

```
<Request xmlns="http://www.parinetworks.com/api/schemas/1.1" requestId="4444">
  <Manage>
    <Delete operationId="1">
      <NotificationList all="true">
      </NotificationList>
    </Delete>
  </Manage>
</Request>
```

1 つの通知の削除

```
<Request xmlns="http://www.parinetworks.com/api/schemas/1.1" requestId="4444">
  <Manage>
    <Delete operationId="1">
      <NotificationList>
        <Notification>
<TrapOID></TrapOID>
        </Notification>
      </NotificationList>
    </Delete>
  </Manage>
</Request>
```

すべての通知タイプの取得

```
<Request xmlns="http://www.parinetworks.com/api/schemas/1.1" requestId="4444">
  <Manage>
    <Get operationId="1">
      <NotificationList all="true">
      </NotificationList>
    </Get>
  </Manage>
</Request>
```

通知の変更

```
<Request xmlns="http://www.parinetworks.com/api/schemas/1.1" requestId="4444">
  <Manage>
    <Modify operationId="1">
      <NotificationList>
       <Notification>
       <TrapOID></TrapOID>
       <NotificationType></NotificationType>
       </Notification>
      </NotificationList>
    </Modify>
```

```
  </Manage>
</Request>
```

SNMP トラップ プロファイルの追加

```
<Request xmlns="http://www.parinetworks.com/api/schemas/1.1" requestId="44444">
  <Manage>
    <Add operationId="1">
      <SNMPTrapProfileList>
        <SNMPTrapProfile>
          <ProfileName>profile1</ProfileName>
 <QueueName>queue1</QueueName>
 <NotificationList>
 <Notification>
 <NotificationType>config</NotificationType>
</Notification>
 </NotificationList>
 <DeviceSelection all="true">
            </DeviceSelection>
        </SNMPTrapProfile>
      </SNMPTrapProfileList>
    </Add>
  </Manage>
</Request>
```

すべての SNMP トラップ プロファイルの削除

```
<Request xmlns="http://www.parinetworks.com/api/schemas/1.1" requestId="4444">
  <Manage>
    <Delete operationId="1">
      <SNMPTrapProfileList all="true" />
    </Delete>
  </Manage>
</Request>
```

1 つの SNMP トラップ プロファイルの削除

```
<Request xmlns="http://www.parinetworks.com/api/schemas/1.1" requestId="4444">
  <Manage>
    <Delete operationId="1">
      <SNMPTrapProfileList>
        <SNMPTrapProfile>
<ProfileName>profile</ProfileName>
        </SNMPTrapProfile>
      </SNMPTrapProfileList>
    </Delete>
  </Manage>
</Request>
```

すべての SNMP トラップ プロファイルの取得

```
<Request xmlns="http://www.parinetworks.com/api/schemas/1.1" requestId="4444">
  <Manage>
    <Get operationId="1">
      <SNMPTrapProfileList all="true" />
    </Get>
  </Manage>
</Request>
```

1 つの SNMP トラップ プロファイルの取得

```
<Request requestId="4444" xmlns="http://www.parinetworks.com/api/schemas/1.1">
  <Manage>
    <Get operationId="1">
      <SNMPTrapProfileList>
        <SNMPTrapProfile> <ProfileName>profile</ProfileName>
        </SNMPTrapProfile>
      </SNMPTrapProfileList>
    </Get>
  </Manage>
</Request>
```

SNMP トラップ プロファイルの変更

```
<Request xmlns="http://www.parinetworks.com/api/schemas/1.1" requestId="44444">
   <Manage>
      <Modify operationId="1">
         <SNMPTrapProfileList>
            <SNMPTrapProfile>
               <ProfileName>profile1</ProfileName>
 <QueueName>queue1</QueueName>
 <NotificationList>
 <Notification>
 <NotificationType>config</NotificationType>
</Notification>
 </NotificationList>
 <DeviceSelection all="false">
                  <DeviceList>
                     <Device>
                        <IPAddress>x.x.x.x</IPAddress>
                     </Device>
                  </DeviceList>
               </DeviceSelection>
            </SNMPTrapProfile>
         </SNMPTrapProfileList>
      </Modify>
   </Manage>
</Request>
```

SNMP トラップ レポート

カスタム レポート XML

```
<Request xmlns="http://www.parinetworks.com/api/schemas/1.1 "requestId="44444">
<Report>
 <Get operationId="1">
   <SnmpTrapReport>
    <TimePeriod>
     <Custom>
      <FromTime></FromTime>
```

```
      <ToTime></ToTime>
     </Custom>
    </TimePeriod>
     <Source>
     </Source>
    <NotificationList>
    <Notification></Notification>
    </NotificationList>
   </SnmpTrapReport>
 </Get>
</Report>
</Request>
```

時間間隔ベースのレポート

```
<Request xmlns="http://www.parinetworks.com/api/schemas/1.1 "requestId="44444">
<Report>
 <Get operationId="1">
   <SnmpTrapReport>
   <TimePeriod>
    <SinceTime>
    </SinceTime>
   </TimePeriod>
   <Source>
   </Source>
   <NotificationList>
   <NotificationType></NotificationType>
   </NotificationList>
   </SnmpTrapReport>
 </Get>
</Report>
</Request>
<SinceTime><!-- /* Style Definitions */ table.MsoNormalTable
Unknown macro: {mso-style-name}
```

SNMP トラップ ポートの変更および設定の消去

```
<Request requestId="4444" xmlns="http://www.parinetworks.com/api/schemas/1.1">
  <Manage>
    <Modify operationId="1">
     <ApplicationPreferencesSettings>
       <SnmpTrapSettings>
       <PurgeSettings>15</PurgeSettings>
       <SnmpTrapPort>162</SnmpTrapPort>
        </SnmpTrapSettings>
    </ApplicationPreferencesSettings>
    </Modify>
  </Manage>
  </Request>
```

この変更実行後、表示に反映するためには、ユーザによる CSPC の再起動が必要

CSPC DB バックアップおよび復元用 XML API

バックアップ ジョブ XML API

```
<Request xmlns="http://www.parinetworks.com/api/schemas/1.1" requestId="3333">
<Job>
<Schedule operationId="123">
<JobSchedule runnow="true">
</JobSchedule>
<BackupJob jobName="Backup_Scheduled1">
<IgnoreRunningJobs>false</IgnoreRunningJobs>
<FTPServerOptions>
<ServerHost>10.126.77.129</ServerHost>
<UserName>root</UserName>
<Password>XXXXX</Password>
<Directory>resources</Directory>
<FileName>file_temp_1</FileName>
</FTPServerOptions>
<PropertiesConfigFile>resources/server/backup_resource_config.properties</PropertiesConfigFile>
</BackupJob>
```

```
</Schedule>
</Job>
</Request>
```

復元ジョブ XML API

```
<Request xmlns="http://www.parinetworks.com/api/schemas/1.1" requestId="3333">
  <Job>
    <Schedule operationId="123">
      <JobSchedule runnow="true" />
      <RestoreJob jobName="Backup">
        <FTPServerOptions>
          <ServerHost>10.126.77.129</ServerHost>
          <UserName>user</UserName>
          <Password>xxxx</Password>
          <Directory>resources</Directory>
          <FileName>_1391384366427.pbx</FileName>
        </FTPServerOptions>
      </RestoreJob>
    </Schedule>
  </Job>
</Request>
```

CLI チャネル XML API

CSPC CLI チャネルはデバイスを動的にサポートし、XML を使用して必要な情報を取得し、今後の使用のために DB に保存します。

新しいデバイス入力用 XML

```
<?xml version="1.0"?>
<Request xmlns="http://www.parinetworks.com/api/schemas/1.1" requestId="12">
  <Manage>
    <Add operationId="1" replace="true">
    <ChannelType channelId = "StarOS">    <!-- Provide unique name for new channel -->
    <ChannelTypeRules>
      <Rules>
```

```
        <MatchType>ANY</MatchType>          <!-- MatchType is based on rules provided, ANY or ALL -->
          <Rule>
                <Attribute><![CDATA[OSTYPE]]></Attribute> <!-- Provide the attribute which needs to be matched with device OSTYPE, SYSOBJID, VERSIONTYPE -->
                <Operator>EQUALS</Operator>                <!-- Provide operator used to match with attribute EQUALS, INDEXOF, STARTSWITH, ENDSWITH, CONTAINS, GREATERTHAN,
                                                                                                                                LESSTHAN -->
                <Operands>
                <Operand><![CDATA[Star OS]]></Operand>  <!-- Operand depend on attribute and operator values -->
                </Operands>
          </Rule>
      </Rules>
    </ChannelTypeRules>

    <CLIRules>
      <MorePromptRules>
        <Rules>
              <MatchType>ANY</MatchType>                    <!-- MatchType is based on rules provided, ANY or ALL -->
                    <Rule>
                        <Attribute><![CDATA[OUTPUT]]></Attribute>
                        <Operator>INDEXOF</Operator>        <!-- Provide operator used to match with attribute EQUALS, INDEXOF, STARTSWITH, ENDSWITH, CONTAINS -->
                        <Operands>
                        <Operand><![CDATA[--More--]]></Operand>          <!-- Provide more prompts available for the device -->
                        </Operands>
                  </Rule>
                </Rules>
                <ContinueChar><![CDATA[32]]></ContinueChar>          <!-- Provide character needs to be entered if more prompt available -->
      </MorePromptRules>

        <OtherPromptRules>
              <Rules>                                       <!-- This OtherPromptRules are used when the device is having prompts other than more prompts -->
                <MatchType>ANY</MatchType>
                <Rule>
                  <Attribute><![CDATA[OSTYPE]]></Attribute>
```

```
                    <Operator>EQUALS</Operator>
                    <Operands>
                      <Operand><![CDATA[AsyncOS]]></Operand>
                    </Operands>
                  </Rule>
                  <Rule>
                    <Attribute><![CDATA[OUTPUT]]></Attribute>
                    <Operator>INDEXOF</Operator>
                    <Operands>
                      <Operand><![CDATA[Do you want to mask the password]]></Operand> <!-- The prompt appears on the
device -->
                    </Operands>
                  </Rule>
                </Rules>
                <ContinueChar><![CDATA[Y]]></ContinueChar>  <!-- ContinueChar is used if we need to input any data/char-
acter to continue further from the prompt -->
        </OtherPromptRules>


      <EnableRules>
              <EnableCommand>enable</EnableCommand>    <!-- Provide command used to enter into enable mode -->
              <EnableUserPrompts><![CDATA[Username:&login:&user:]]></EnableUserPrompts>      <!-- Provide user
prompts -->
               <EnablePwdPrompts><![CDATA[Password:]]></EnablePwdPrompts>
                      <!-- Provide password prompts -->
        </EnableRules>


      <ClearTerminalLengthDefinition>
        <Command>terminal length 0</Command>    <!-- Provide commands used to set terminal length for the device -->
        <Command>terminal width 0</Command>
      </ClearTerminalLengthDefinition>
      <AfterLoginCommand>
        <Command>clish</Command>                    <!-- some devices required commands after login to the device
and before entering into the enable mode, provide those
                    commands here -->
      </AfterLoginCommand>
      <ReplaceEscChar>[j</ReplaceEscChar>        <!-- Provide escape characters to be replaced -->
          <ClearLineDef>3</ClearLineDef>                <!-- This will clear the buffer before executing the command
while collecting the data from the device -->
          <ControlChar>¥n</ControlChar>
```

```
        <Priority>100</Priority>
        <UsePariPatentEndOfCommand>true</UsePariPatentEndOfCommand>
    </CLIRules>
</ChannelType>
</Add>
</Manage>
</Request>
```

チャネル変更 XML

```
<?xml version="1.0"?>
<Request xmlns="http://www.parinetworks.com/api/schemas/1.1" requestId="12">
  <Manage>
    <Modify operationId="1">
    <ChannelType channelId = "ACNS">    <!-- Provide unique name for new channel -->
    <ChannleTypeRules>
      <Rules>
        <MatchType>ANY</MatchType>          <!-- MatchType is based on rules provided, ANY or ALL -->
          <Rule>
              <Attribute><![CDATA[OSTYPE]]></Attribute> <!-- Provide the attribute which needs to be matched with device
OSTYPE, SYSOBJID, VERSIONTYPE    -->
              <Operator>EQUALS</Operator>          <!-- Provide operator used to match with attribute EQUALS,
INDEXOF, STARTSWITH, ENDSWITH, CONTAINS, GREATERTHAN,
                                                                                LESSTHAN    -->
              <Operands>
              <Operand><![CDATA[Star OS]]></Operand>  <!-- Operand depend on attribute and operator values -->
              </Operands>
          </Rule>
      </Rules>
    </ChannleTypeRules>

    <CLIRules>
      <MorePromptRules>
        <Rules>
            <MatchType>ANY</MatchType>                  <!-- MatchType is based on rules provided, ANY
or ALL -->
                <Rule>
                    <Attribute><![CDATA[OUTPUT]]></Attribute>
```

```
                    <Operator>INDEXOF</Operator>        <!-- Provide operator used to match with attribute
EQUALS, INDEXOF, STARTSWITH, ENDSWITH, CONTAINS, GREATERTHAN,
                                                                                    LESSTHAN    -->
                    <Operands>
                    <Operand><![CDATA[--More--]]></Operand>        <!-- Provide more prompts available
for the device -->
                    <Operand><![CDATA[<--- More --->]]></Operand>
                    </Operands>
                 </Rule>
               </Rules>
               <ContinueChar><![CDATA[32]]></ContinueChar>          <!-- Provide character needs to be entered if
more prompt available -->
        </MorePromptRules>


          <OtherPromptRules>
               <Rules>                                                <!-- This OtherPromptRules are used when the de-
vice is having prompts other than more prompts -->
                 <MatchType>ANY</MatchType>
                 <Rule>
                   <Attribute><![CDATA[OSTYPE]]></Attribute>
                   <Operator>EQUALS</Operator>
                   <Operands>
                     <Operand><![CDATA[AsyncOS]]></Operand>
                   </Operands>
                 </Rule>
                 <Rule>
                   <Attribute><![CDATA[OUTPUT]]></Attribute>
                   <Operator>INDEXOF</Operator>
                   <Operands>
                     <Operand><![CDATA[Do you want to mask the password]]></Operand> <!-- The prompt appears on the
device -->
                   </Operands>
                 </Rule>
               </Rules>
               <ContinueChar><![CDATA[Y]]></ContinueChar>   <!-- ContinueChar is used if we need to input any data/char-
acter to continue further from the prompt -->
        </OtherPromptRules>


          <EnableRules>
```

```
                <EnableCommand>enable</EnableCommand>    <!-- Provide command used to enter into enable mode -->
                <EnableUserPrompts><![CDATA[Username:&Password:&login:&user:]]></EnableUserPrompts>    <!-- Pro-
vide user prompts -->
                  <EnablePwdPrompts><![CDATA[Password:]]></EnablePwdPrompts>
                        <!-- Provide password prompts -->
        </EnableRules>

      <ClearTerminalLengthDefinition>
        <Command>terminal length 0</Command>    <!-- Provide commands used to set terminal length for the device -->
        <Command>terminal width 0</Command>
      </ClearTerminalLengthDefinition>

          <AfterLoginCommand>
        <Command>Clish</Command>                    <!-- some devices required commands after login to the device
and before entering into the enable mode, provide those
                                commands here -->
      </AfterLoginCommand>

      <ReplaceEscChar>[j</ReplaceEscChar>        <!-- Provide escape characters to be replaced -->
          <ClearLineDef>3</ClearLineDef>                <!-- This will clear the buffer before executing the command
while collecting the data from the device -->
          <ControlChar>¥n</ControlChar>
          <Priority>100</Priority>
        <UsePariPatentEndOfCommand>true</UsePariPatentEndOfCommand>
    </CLIRules>
</ChannelType>
</Modify>
</Manage>
</Request>
```

CLI チャネルでレポートを取得する XML

```
<Request xmlns="http://www.parinetworks.com/api/schemas/1.1" requestId="CLIChannelReport">
    <Manage>
        <Get operationId="1">
            <CLIChannelReport all = "false">    <!-- all equals true will get the all channels Channel Type rules only not CLI rules -->
                <ChannelId>IOS</ChannelId>    <!-- if all equals false we need to provide channle id to get that particular channel channel type rulas and cli
                rules    -->
            </CLIChannelReport>
        </Get>
    </Manage>
</Request> ?
```

チャネル削除 XML

```
- <Request xmlns="http://www.parinetworks.com/api/schemas/1.1" requestId="ChannelList">
- <Manage>
- <Delete operationId="1">
  <ChannelType channelId="Acsw" />
- <!--  This Xml deletes channel defintions which is provided here as channelId
  -->
  </Delete>
  </Manage>
  </Request>
```

CLI チャネル リスト レポート取得用 XML

```
Request xmlns="http://www.parinetworks.com/api/schemas/1.1" requestId="ChannelList">
    <Manage>
        <Get operationId="1">
            <ChannelList all = "true"/> <!-- This report lists all the existing channel ids list  -->
        </Get>
    </Manage>
</Request>?
```

インポートされたデバイスのステータス レポート取得

```
<Request xmlns="http://www.parinetworks.com/api/schemas/1.1" requestId="44444">
 <Manage>
    <Get operationId="1">
       <ImportedDeviceStatusReport>
      <DiscoveryJobId>32</DiscoveryJobId>
      <DiscoveryJobRunId>1</DiscoveryJobRunId>
       </ImportedDeviceStatusReport>
    </Get>
 </Manage>
</Request>
```

CSPC バックアップ（PSS）

```
<Request xmlns="http://www.parinetworks.com/api/schemas/1.1" requestId="3333">
<Job>
<Schedule operationId="123">
<JobSchedule runnow="true">
</JobSchedule>
<BackupJob jobName="Backup_RunNow">
<BackupJobType>Full_Backup</BackupJobType>
<IgnoreRunningJobs>true</IgnoreRunningJobs>
<FTPServerOptions>
<ServerHost>10.126.77.129</ServerHost>
<UserName>root</UserName>
<Password>cspc*123</Password>
<Directory>CSPC_Backup</Directory>
<FileName>backup</FileName>
</FTPServerOptions>
<IgnoreInventoryData>true</IgnoreInventoryData>
</BackupJob>
</Schedule>
</Job>
</Request>
```

CSPC バックアップ（PSS）- スケジュール

```
<Request xmlns="http://www.parinetworks.com/api/schemas/1.1" requestId="3333">
<Job>
<Schedule operationId="123">
<JobSchedule runnow="false">
<Start>1450692900000</Start>
</JobSchedule>
<BackupJob jobName="Backup_RunNow">
<BackupJobType>Full_Backup</BackupJobType>
<IgnoreRunningJobs>true</IgnoreRunningJobs>
<FTPServerOptions>
<ServerHost>10.127.152.54</ServerHost>
<UserName>admin</UserName>
<Password>Admin123</Password>
<FileName>xml</FileName>
</FTPServerOptions>
<IgnoreInventoryData>true</IgnoreInventoryData>
</BackupJob>
</Schedule>
</Job>
</Request>
```

ループバック インターフェイスの IP アドレス収集（NOS）

```
<Request xmlns="http://www.parinetworks.com/api/schemas/1.1" requestId="3333">
  <Job>
    <Schedule operationId="1">
      <JobSchedule runnow="true" />
      <DiscoveryJob identifier="my_discovery123">
        <DiscoveryOptionsList>
          <DiscoveryOptions>
            <IPAddressList>
              <IPAddress>6.0.1.1</IPAddress>
            </IPAddressList>
            <useLoopBackIp>true</useLoopBackIp>
          </DiscoveryOptions>
```

```
        </DiscoveryOptionsList>
      </DiscoveryJob>
    </Schedule>
  </Job>
</Request>
```

オプションのメタデータ ラベルをカスタム データセットの OID に追加（PSS）

```
<Request xmlns="http://www.parinetworks.com/api/schemas/1.1" requestId="44444">
  <Manage>
    <Add operationId="1">
      <DatasetList>
        <Dataset identifier="_snmp_XML_SNTest2">
          <Title>_snmp_XML_SNTest2</Title>
          <Description/>
          <CategoryName>1</CategoryName>
          <CreatedUser>XML</CreatedUser>
          <Locked>false</Locked>
          <CollectionType>SNMP</CollectionType>
          <VersionedDatasetList>
            <VersionedDataset identifier="cisco">
              <SNMP>
                <SNMPRequest>
                  <RequestType>Scalar</RequestType>
                  <ObjectList>
                    <Object>
                      <Id>.1.3.6.1.4.1.9.2.1.3</Id>
                      <Title>hostName</Title>
                      <Tag>!@#$%^&*()":.,</Tag>
                      <Type>Scalar</Type>
                    </Object>
                  </ObjectList>
                </SNMPRequest>
              </SNMP>
            </VersionedDataset>
          </VersionedDatasetList>
```

```
        </Dataset>
      </DatasetList>
    </Add>
  </Manage>
</Request>
```

収集プロファイルのエクスポートおよびインポート（PSS）

すべてのルールをエクスポートする API

```
<Request>
  <Export>
    <ExportAllRules>
    <ExportLocation></ExportLocation>
    </ExportAllRules>
    </Export>
  </Request>
```

すべてのルールをインポートする API

```
  <Request>
  <Execute>
    <ImportAllRulesFromZipFile>
    <AllRuleZipFileLocation>/opt/CSPC/data/ruleExport/CSPCRules_1450433792272.Zip</AllRuleZipFileLocation>

    </ImportAllRulesFromZipFile>
    </Execute>
  </Request>
```

カスタム プロファイル用署名のアップロード（PSS）

```
<CollectionProfile identifier="_ASA_Test">
  <Title>ASA Test</Title>
  <CreatedUser>admin</CreatedUser>
  <CreationTime>1439385708000</CreationTime>
  <Locked>false</Locked>
  <Tag>DONOTPROCESS</Tag>
  <ExportSeedFile>false</ExportSeedFile>
```

```
    <ApplicationDiscoveryProfile>false</ApplicationDiscoveryProfile>
    <DisableCollectionInterval>false</DisableCollectionInterval>
    <Priority>Medium</Priority>
    <PreserveRunCount>1</PreserveRunCount>
    <CredentialFallback>false</CredentialFallback>
    <RunDiscoveryBeforeExecution>false</RunDiscoveryBeforeExecution>
    <RunDAVBeforeExecution>false</RunDAVBeforeExecution>
    <RunPromptCollectionBeforeExecution>false</RunPromptCollectionBeforeExecution>
    <DeviceSelection all="true" />
    <DatasetList>
      <Dataset>_show running_config</Dataset>
    </DatasetList>
    <DataPrivacy>
      <IsIPPrivacyEnabled>false</IsIPPrivacyEnabled>
      <IsHostPrivacyEnabled>false</IsHostPrivacyEnabled>
    </DataPrivacy>
</CollectionProfile>
```

検出分類

```
<Request requestId="123">
<Manage>
<Modify operationId="11">
  <ApplicationPreferencesSettings>
          <Discovery>
            <SnmpTimeout>3</SnmpTimeout>
            <SnmpRetry>1</SnmpRetry>
            <MaxThreadCount>100</MaxThreadCount>
            <MaxCredentialSets>10</MaxCredentialSets>
            <MaxDiscoveryTime>600</MaxDiscoveryTime>
            <MaxDeviceDiscoveryTime>180</MaxDeviceDiscoveryTime>
            <IpPhoneDiscovery>false</IpPhoneDiscovery>
            <NmapTimeout>30</NmapTimeout>
            <SerialNumDuplicateCheckEnabled>false</SerialNumDuplicateCheckEnabled>
            <IncludePlatformList>[]</IncludePlatformList>
            <TryPingFirst>true</TryPingFirst>
            <ExcludePlatformList>[_EXCLUDE_CSCus90617]</ExcludePlatformList>
```

```
            <EnableCLIdiscovery>false</EnableCLIdiscovery>
            <CLIDiscoveryTimeOut>3</CLIDiscoveryTimeOut>
            <EnableSnmpConfigPush>false</EnableSnmpConfigPush>
          </Discovery>
        </ApplicationPreferencesSettings>
</Modify>
</Manage>
</Request>
```

G

有効な SSL 証明書のアップロード

CSPC キーストアに SSL 証明書をアップロードするには、次を実行します。

ステップ 1　次のいずれか 1 つを選択します。

- お客様自身が選択し、信頼できる認証局から購入した SSL 証明書をアップロードする。

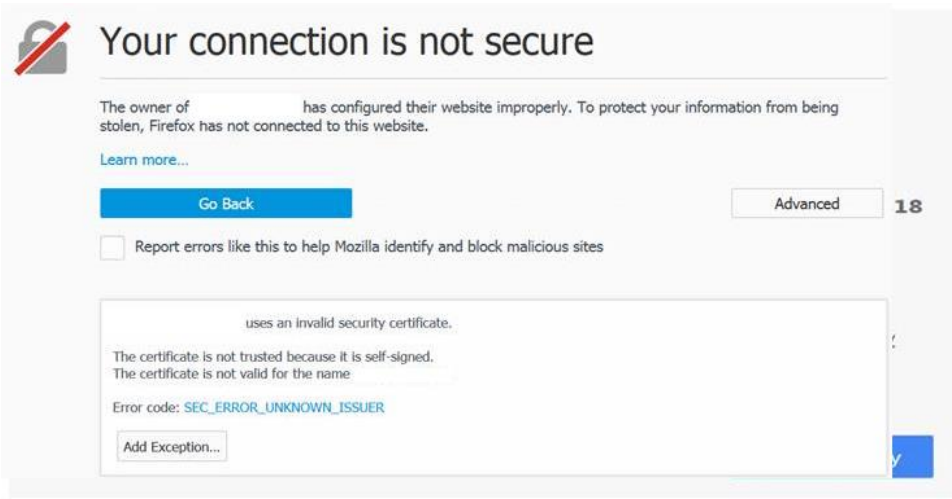
または

- お客様が自己署名した自社の証明書をアップロードする。

上記の 1 番目のシナリオの場合は、直接次のコマンドを使用してキーストアを作成しますから開始できます。

注　自己署名証明書の場合は必ずブラウザの警告メッセージが表示されます。

図 G-1　　警告メッセージ



Symantec（VeriSign）や Digicert などの信頼された署名機関から提供される SSL 証明書を使用している場合はこの警告メッセージは表示されません。

自己署名証明書の生成

自己署名証明書では、秘密キーと証明書署名要求（CSR）が必要です。

ステップ 2CSPC CLI で次のコマンドを使用して、秘密キーと証明書署名要求（CSR）を生成します。お客様は入力フィールドの詳細情報を提供する必要があります。

```
#openssl req -new -newkey rsa:2048 -nodes -keyout localhost.key -out localhost.csr

Generating a 2048 bit RSA private key
..................+++
.....................................................................................
```

```
...+++
writing new private key to 'localhost.key'
-----
```

お客様の証明書要求に組み込まれる情報を

入力するように求められます。

入力するのは、「識別名」、または「DN」と呼ばれる情報です。

入力するフィールドはごく限られており、一部は空白のままにすることもできます。

デフォルト値が入っているフィールドもあります。

「.」を入力すると空白のままになります。

```
-----
Country Name (2 letter code) [XX]:IN
State or Province Name (full name) []:TN
Locality Name (eg, city) [Default City]:Trichy
Organization Name (eg, company) [Default Company Ltd]:KSKTech
Organizational Unit Name (eg, section) []:IT
Common Name (eg, your name or your server's hostname) []:cspc
Email Address []:ksk@wxyz.com
```

次の「追加」属性を入力してください。

証明書要求と合わせて送信されます。

```
A challenge password []:password
An optional company name []:AEY
```

上記のコマンドで、localhost.key（キー ファイル）と localhost.csr（CSR ファイル）の 2 つのファイルが生成されます。

- シナリオ 1：お客様は、CSPC でキーと CSR ファイルのみを生成するよう要求できます。その場合、生成されたキー/CSR ファイルを使用して自分で証明書を作成することになります。上記ファイル（localhost.csr および localhost.key）が生成されたら、お客様は証明書を作成して、提供します。証明書ファイルは、.cer または .crt です（Microsoft プラットフォームでは通常 .cer ファイル）。ステップ 4 に進みます。
- シナリオ 2：お客様は CSPC で、生成されたキーと CSR ファイル（localhost.csr および localhost.key）から証明書を作成するよう要求できます。この場合は、ステップ 3 に進みます。

ステップ 3 次のコマンドを使用して証明書を作成します。

```
# openssl x509 -req -days 500 -in localhost.csr -signkey localhost.key -out localhost.crt
Signature ok
subject=/C=IN/ST=TN/L=Trichy/O=KSKTech/OU=IT/CN=cspc/emailAddress= ksk@wxyz.com
Getting Private key
```

上記コマンドで自己署名証明書ファイル（localhost.crt）が生成されます。

このステップは任意です。

次のコマンドを使用して、キーストアを作成する前に、お客様が提供した証明書を確認します。

```
/opt/cisco/ss/adminshell/applications/CSPC/jreinstall/bin/keytool  -printcert  -v  -
file localhost.crt
```

ステップ 4次のコマンドを使用してキーストアを作成します。

```
#openssl pkcs12 -export -in localhost.crt -inkey localhost.key > localhost.p12
Enter ExportPassword:cspcgxt
Verifying - Enter Export Password:cspcgxt
```

上記コマンドで .p12 ファイルが生成されます。

注　パスワードとして「cspcgxt」を使用します（他のパスワードを使用する場合、別のキーストアを作成し、server.xml ファイルの「keystoreFile」と「keystorePass」を編集する必要があります）。

ステップ 5次のコマンドを使用して、作成されたキーストアを CSPC キーストアにインポートします。

```
/opt/cisco/ss/adminshell/applications/CSPC/jreinstall/bin/keytool -importkeystore -
srckeystore localhost.p12 -srcstoretype pkcs12 -destkeystore $CSP-
CHOME/webui/tomcat/conf/cspcgxt -deststoretype jks
Enter destination keystore password:cspcgxt
Enter source keystore password:cspcgxt
Entry for alias 1 successfully imported.
Import command completed: 1 entries successfully imported, 0 entries failed or canceled
```

ステップ 6CSPC キーストアから既存のエイリアスを削除します。

* 次のコマンドを使用して、CSPC キーストアの詳細を確認します。

```
/opt/cisco/ss/adminshell/applications/CSPC/jreinstall/bin/keytool -list -v -keystore
$CSPCHOME/webui/tomcat/conf/cspcgxt
Your keystore contains 2 entries
Alias name: tomcat
Alias name: 1
```

tomcat のエイリアスには CSPC の自己署名証明書が含まれているため、次のコマンドを使用して削除する必要があります。

```
/opt/cisco/ss/adminshell/applications/CSPC/jreinstall/bin/keytool   -delete   -alias
tomcat -keystore   $CSPCHOME/webui/tomcat/conf/cspcgxt
Enter keystore password:cspcgxt
/opt/cisco/ss/adminshell/applications/CSPC/jreinstall/bin/keytool -list -v -keystore
$CSPCHOME/webui/tomcat/conf/cspcgxt
Enter keystore password:cspcgxt
```

これで CSPC キーストアのエイリアスは 1 つだけになりました。

```
Keystore type: JKS
Keystore provider: SUN Your keystore contains 1 entry
Alias name: 1
```

次のコマンドを使用してエイリアス名を tomcat に変更します（このステップは任意です）。

```
/opt/cisco/ss/adminshell/applications/CSPC/jreinstall/bin/keytool -changealias -alias
1 -destalias tomcat -keystore  $CSPCHOME/webui/tomcat/conf/cspcgxt
Enter keystore password: cspcgxt
```

ステップ 7エイリアス名が変更されたことを確認します。

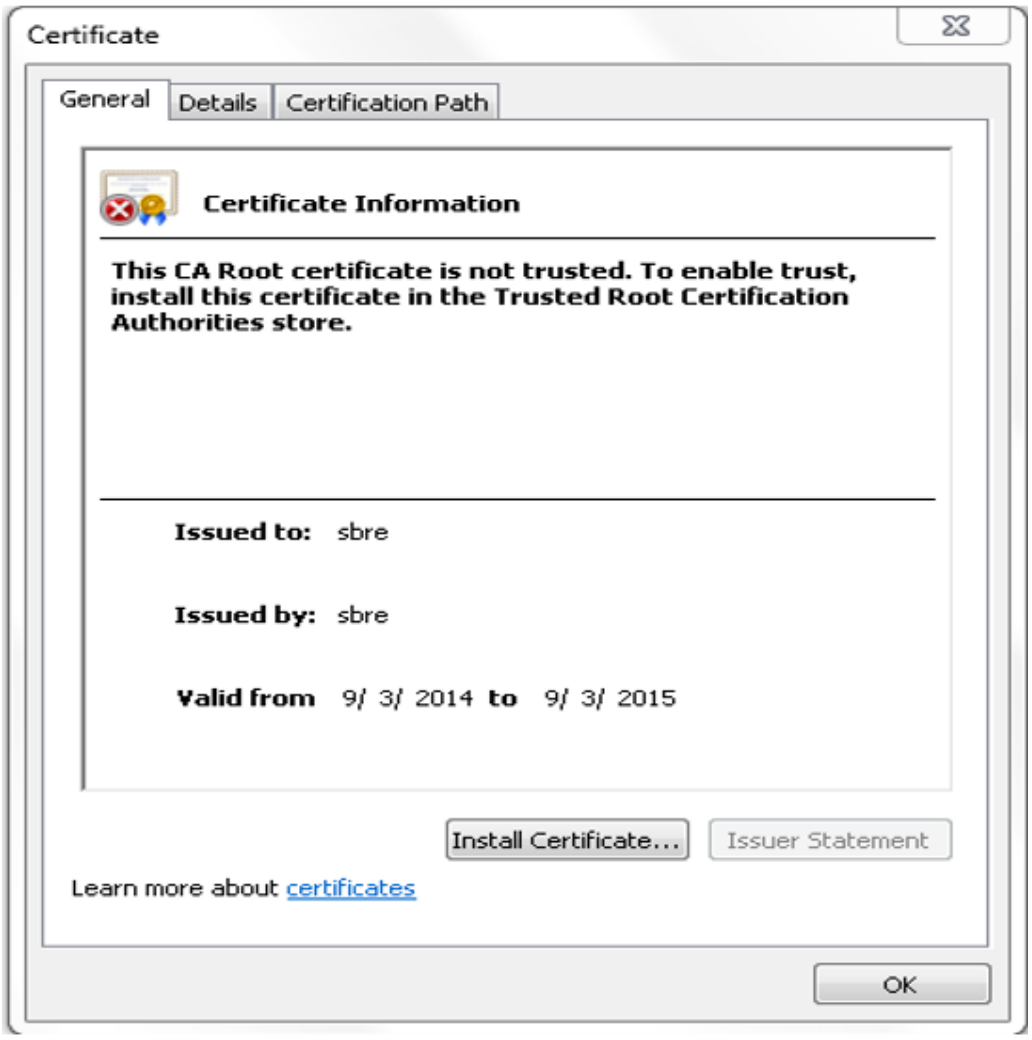
```
/opt/cisco/ss/adminshell/applications/CSPC/jreinstall/bin/keytool -list -v -keystore
$CSPCHOME/webui/tomcat/conf/cspcgxt
Enter keystore password: cspcgxt
Keystore type: JKS
Keystore provider: SUN.Your keystore contains 1 entry
Alias name: tomcat
```

ステップ 8次のコマンドで CSPC サービスを再起動します。

```
# service cspc restart
```

ステップ 9アップロードされた SSL 証明書が、次の画面のようにブラウザに表示されることを確認します。

図 G-2　　証明書情報


Certificate
General
Details
Certification Path
Certificate Information
This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.
Issued to: sbre
Issued by: sbre
Valid from 9/ 3/ 2014 to 9/ 3/ 2015
Install Certificate...
Issuer Statement
Learn more about certificates
OK