

公共服务平台收集器 (CSPC)

自助服务 - 入门指南

2015 年 11 月

公司总部

思科系统公司。

170 West Tasman Drive
San Jose, CA 95134-1706
USA

<http://www.cisco.com>

© 2015 思科系统公司。版权所有。

目录

撰写人	2
审校者	2
CSPC 简介	3
必备条件	3
智能网络支持服务安全	3
智能网络支持服务支持社区	3
虚拟平台要求	3
下载虚拟机映像	3
配置设备 IP 地址	4
CSPC 注册	7
登录软件设备	9
收集器的运行	10
输入 CSPC 设备凭证	11
设备发现；资产数据收集和上传	15
通过 CDP、OSPF 和 ARP 等协议发现设备	17
通过扫描/Ping IP 地址范围发现设备	19
运行收集配置文件并上传数据	22

撰写人

姓名	邮件	职务
Josh Harpst	jharpst@cisco.com	SNTC 收集器支持工程师

审校者

姓名	邮件	职务
Lynden Price	jospri#@cisco.com	文档所有者/SNTC 收集器支持技术负责人

CSPC 简介

本文档介绍有关 CSPC 2.5.2 版本的信息。为了配置 CSPC 并确保成功完成设置，您应熟悉从命令行配置设备，并对网络管理系统有基本的了解。

CSPC 是基于 SNMP 的工具，用于发现思科设备和收集设备的信息。您应知道在设备上设置的 SNMP 只读团体字符串。本文档将指导您逐步完成 CSPC 的基本设置。

必备条件

首先，您需要先完成门户自注册过程，从而获得思科智能网络支持服务门户的访问权限，然后才能生成 CSPC 许可证文件。为此，请点击下方的链接。

<https://supportforums.cisco.com/document/12566021/new-smart-net-total-care>

智能网络支持服务安全

CSPC 使用多种协议从受支持的思科设备收集数据。在最低限度上，您只需 SNMP 只读访问权限，即可轮询网络中的设备并从设备收集资产详细信息。此外，您还可以启用 SSH 和/或 Telnet 访问权限补充您收集的数据。思科收集器使用 Telnet 和/或 SSH 收集设备配置数据、其他资产信息，以及关键事件后的异常数据。思科安全白皮书中列出了收集器能够执行的命令列表，点击此处可获取此白皮书：[思科安全白皮书](#)。

智能网络支持服务支持社区

有关智能网络支持服务的更多信息，请访问智能网络支持服务支持社区。在那里，您可以找到讨论组、常见问题解答、培训，以及智能网络支持服务的其他相关资源。

[智能网络支持服务支持社区](#)

虚拟平台要求

本节提供有关虚拟平台要求的信息。本指南不提供关于如何安装各种不同虚拟平台的指导。

要在 ESXi 4.x 或更高版本的虚拟平台上运行收集器映像，需满足以下系统要求：

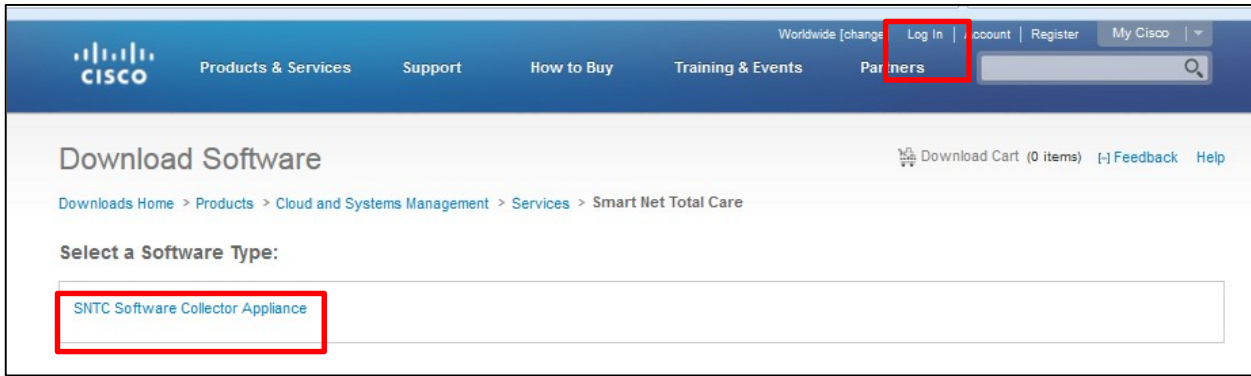
- 250 GB 硬盘驱动器空间
- 4 个 CPU 核心（虚拟 CPU）
- 1 个虚拟 NIC（所需 NIC 数量视网络拓扑而定）
- 4GB 虚拟 RAM

下载虚拟机映像

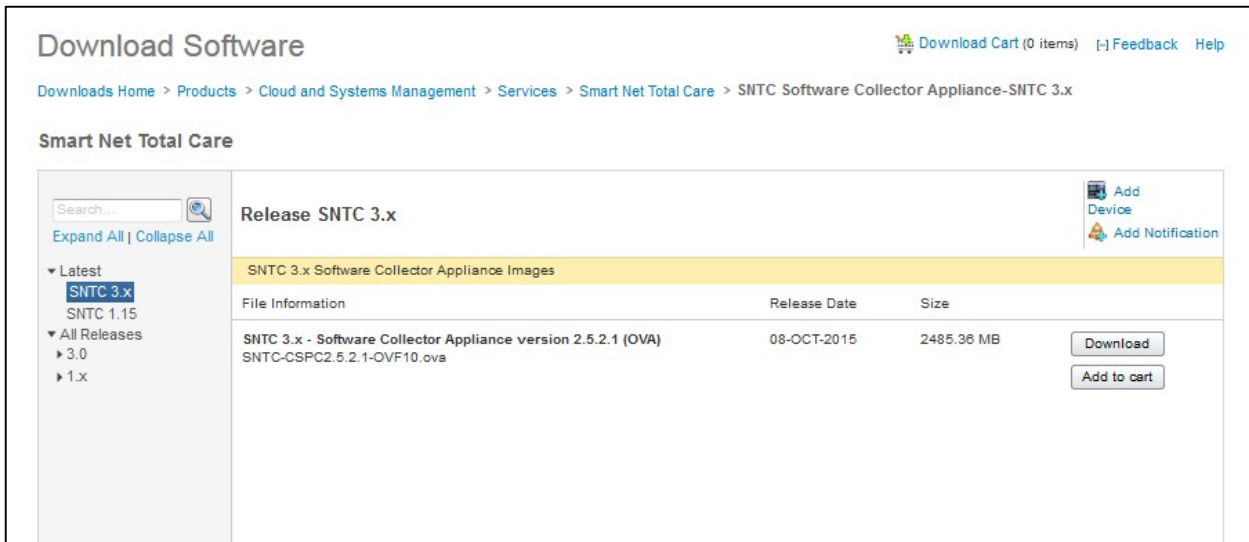
在确保您的虚拟环境可以提供所需的资源后，下一步是下载智能网络支持服务映像。此软件映像可以从下载中心获取。下载中心包括最新的软件映像。如需获取思科智能网络支持服务映像，请执行以下步骤：

- 访问如下 URL：<http://software.cisco.com/download/type.html?mdfid=283107976&catid=null>

- 点击屏幕右上角的**登录**链接，使用您的 CCO ID 和密码进行登录。



- 点击 **SNTC 软件收集器设备**，系统将显示“下载软件”窗口。



- 点击**下载**按钮。如果系统提示您接受“条款和条件”，请选择接受以开始下载映像。
- 将下载的映像部署到您的虚拟环境中。

配置设备 IP 地址

本节适用于收集器设备的虚拟机和硬件平台版本。要配置设备的 IP 地址，请执行以下步骤：

- 硬件设备：将显示器和键盘连接到服务器
- 软件设备：使用虚拟环境的工具连接到虚拟机控制台

打开收集器的电源后，系统会提示您按任意键。

- 按任意键

```
Press any key to continue.  
—
```

启动过程中显示“请按任意键”是正常情况，可能需要经过几分钟才会出现登录提示。

- 使用以下登录 ID/密码信息通过连接的控制台登录到软件设备：

admin/Admin!23

首次登录时，设备会强制要求您更改默认的 CLI 密码。

登录设备后，您会看到以下屏幕：

```
Last login: Thu Jun  5 08:28:00 2014
#####
#      This system is hardened and for the use of authorized users only.
#
#      Individuals using this computer system without authority, or in
#      excess of their authority, are subject to having all of their
#      activities on this system monitored and recorded by system
#      personnel.
#
#      In the course of monitoring individuals improperly using this
#      system, or in the course of system maintenance, the activities
#      of authorized users may also be monitored.
#
#      Anyone using this system expressly consents to such monitoring
#      and is advised that if such monitoring reveals possible
#      evidence of criminal activity, system personnel may provide the
#      evidence of such monitoring to law enforcement officials.
#####

=====
                Cisco Network Appliance Administration
=====

To see the list of all the commands press '?'
admin# ?
```

要分配静态 IP 地址，请使用 **conf ip** 命令。

- 在命令提示符中输入以下信息：

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

例如：conf ip eth0 192.168.1.100 255.255.255.0 192.168.1.1

```
admin# conf ip help

-----
Usage:
admin# conf ip <intf> <ipaddr> <netmask> <gateway>
Eg:
admin# conf ip eth0 192.168.155.2 255.255.255.0 192.168.150.1
-----
admin# conf ip eth0 192.168.155.2 255.255.255.0 192.168.150.1
```

要分配动态 IP 地址，请使用 **conf dhcp** 命令。

- 在命令提示符中输入以下信息：
conf dhcp <interface>

例如: conf dhcp eth0

```
conf dhcp <intf>
admin# conf dhcp eth0
```

配置 DNS 服务器:

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

要配置时区, 请运行以下命令并在提示符中输入相应的值:

```
# timezone
```

通过与 NTP 服务器同步配置时间。您也可以在提示符中按 Enter 键, 直接使用默认值:

```
# timesync
```

启用 Linux 用户登录 “collectorlogin” 并设置到期天数 (1-180)

```
# pwdreset collectorlogin 180
```

```
admin# pwdreset collectorlogin 180
Password for 'collectorlogin' reset to - Rtxjrr0+ successfully
Password expires in 180 days
Shell is enabled
passwd: all authentication tokens updated successfully
*** Please memorize the new password ***
Lost passwords cannot be recovered. The only alternative to recover is to reinstall the server.
admin#
```

记录此密码!

启用 Linux root 登录并设置到期天数 (1-180)

```
# pwdreset root 180
```

```
admin# pwdreset root 180
Password for 'root' reset to - Kqpbvm4@ successfully
Password expires in 180 days
Shell is enabled
passwd: all authentication tokens updated successfully
*** Please memorize the new password ***
Lost passwords cannot be recovered. The only alternative to recover is to reinstall the server.
admin#
```

记录此密码!

需要重新启动设备，更改的设置才会生效。

- 在命令提示符中输入以下命令：

```
# reboot
```

按 **y** 确认屏幕上的问题

设备重新启动后，确认该 IP 是正确的。

- 在命令提示符中输入以下命令：

```
# show ip
```

- 通过 SSH 连接到设备，确保您可以远程管理 CSPC。

CSPC 注册

要使收集器可用于思科智能网络支持服务门户，需要先执行 CSPC 注册流程。注册流程会执行验证，以便在 CSPC 收集器和思科数据中心之间建立连接。在注册流程中，您需要获取授权文件（一份安全证书和其他注册文件）。稍后，您需要使用这些注册文件/授权文件来完成 CSPC 安装。

在这一步，您需要访问智能网络支持服务门户，并完成自行激活和注册。要完成这些操作，请点击此链接：

<https://www.cisco.com/web/smartservices/sntc.html>

有关如何完成自助式自行激活的详细说明，请访问：

<https://supportforums.cisco.com/document/12566021/new-smart-net-total-care>

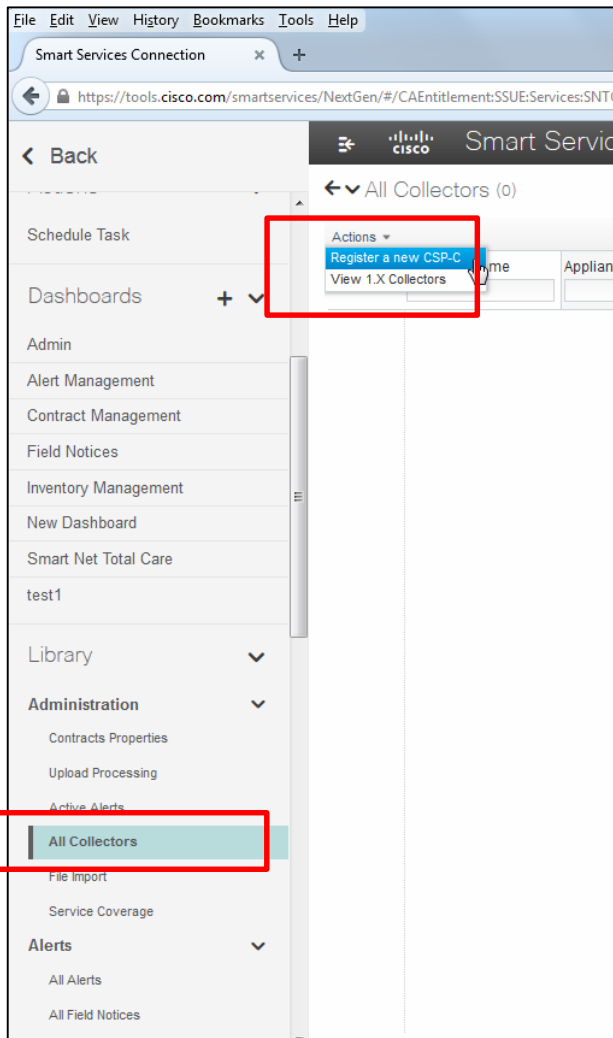
重要提示！

请勿解压授权文件！

只有智能网络支持服务客户管理员可以生成授权文件。登录智能网络支持服务门户：

<https://tools.cisco.com/smartservices/>

- 在左侧导航板中，依次选择**库 > 管理 > 所有收集器**
- 在显示的窗格中，依次选择**操作 > 注册新 CSPC** 选项



系统将显示“注册新 CSPC”屏幕：

Register a new CSP-C

* Required fields

* CSP-C Name:

* Entitled Company:

Entitled Company list:
CISCO SYSTEMS INC FOR US ▼

* Site ID:

Site ID list:

* Serial Number:

* Author name:

* Email id:

* Inventory Name:

按照如下要求填写必填字段：

- **CSPC 名称**应与服务器的主机名一致，也可以是用于在网上识别此收集器的任意名称
- 对于**已授权的公司**字段，请从下拉列表中选择您公司的名称
- 您可以在收集器的**站点 ID**中手动输入值。在此字段中可以输入您认为合适的任何内容
- 对于**序列号**，请从此处复制 Unix Epoch 时间：<http://www.epochconverter.com/>
- 对于**资产名称**，请使用“主机名-资产”的格式

点击**提交**按钮，然后等待系统弹出提示下载 zip 文件的对话框。将 zip 文件保存到便于查找的位置。请勿解压授权文件！

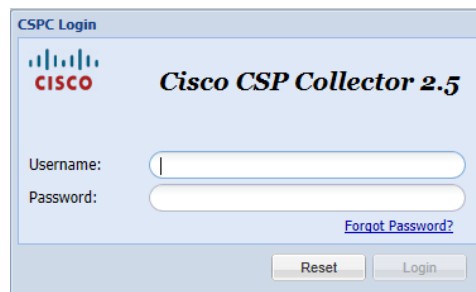
登录软件设备

要访问设备，请打开浏览器窗口并执行以下步骤：

- 使用以下 URL 格式访问设备：
`https://<your_appliance_ip_address>:8001/`

您将会在浏览器上看到安全证书警告，提醒您需要网站安全证书，或者浏览器无法确认安全连接。警告因浏览器的类型而异。

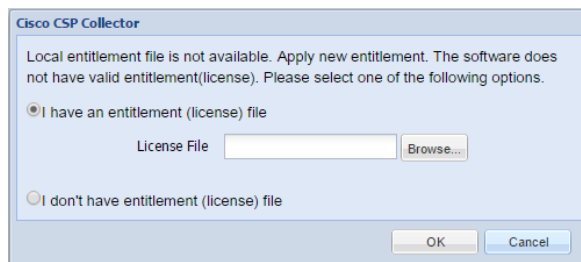
- 确认警告，然后继续登录设备。



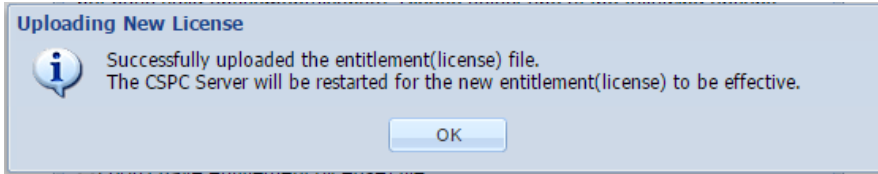
- 输入您的登录凭证。

默认的设备用户 ID/密码为：**admin/Admin#123**

首次登录收集器时，系统会提示您导入授权证书。执行此步骤后才能登录到 CSPC GUI。系统将显示如下消息框：

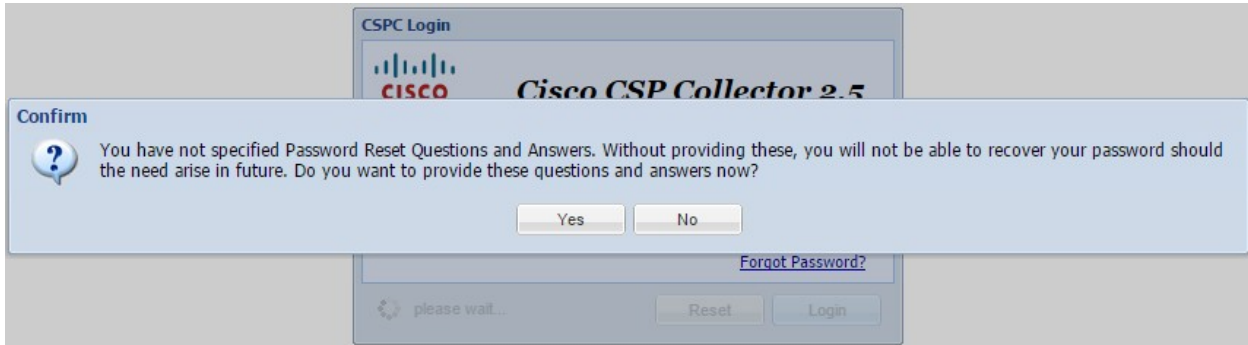


浏览至您的 .zip 授权文件，然后点击“确定”。



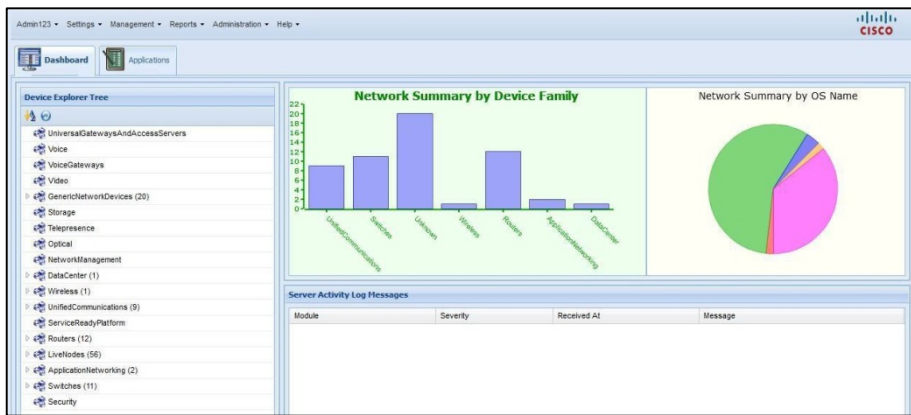
上传授权文件后点击“确定”，收集器将会重新启动。可能需要等待几分钟的时间才能重新登录。

使用 admin/Admin#123 凭证再次登录。系统将弹出“最终用户许可协议”。阅读该协议，点击“我接受”以继续。然后系统会提示您回答密码重置问题。



- 点击否，待稍后提供此信息。设备现已加载其软件项，可以正常运行。

所有软件加载完成后，系统将显示图形用户界面 (GUI)。



收集器的运行

收集器的运行涉及下列与收集器相关的任务：

- 输入 CSPC 设备凭证
- 设备发现；资产数据收集和上传

输入 CSPC 设备凭证

本节介绍指定设备凭证的过程。

要想发现网络设备并收集设备数据，您必须先输入设备凭证。

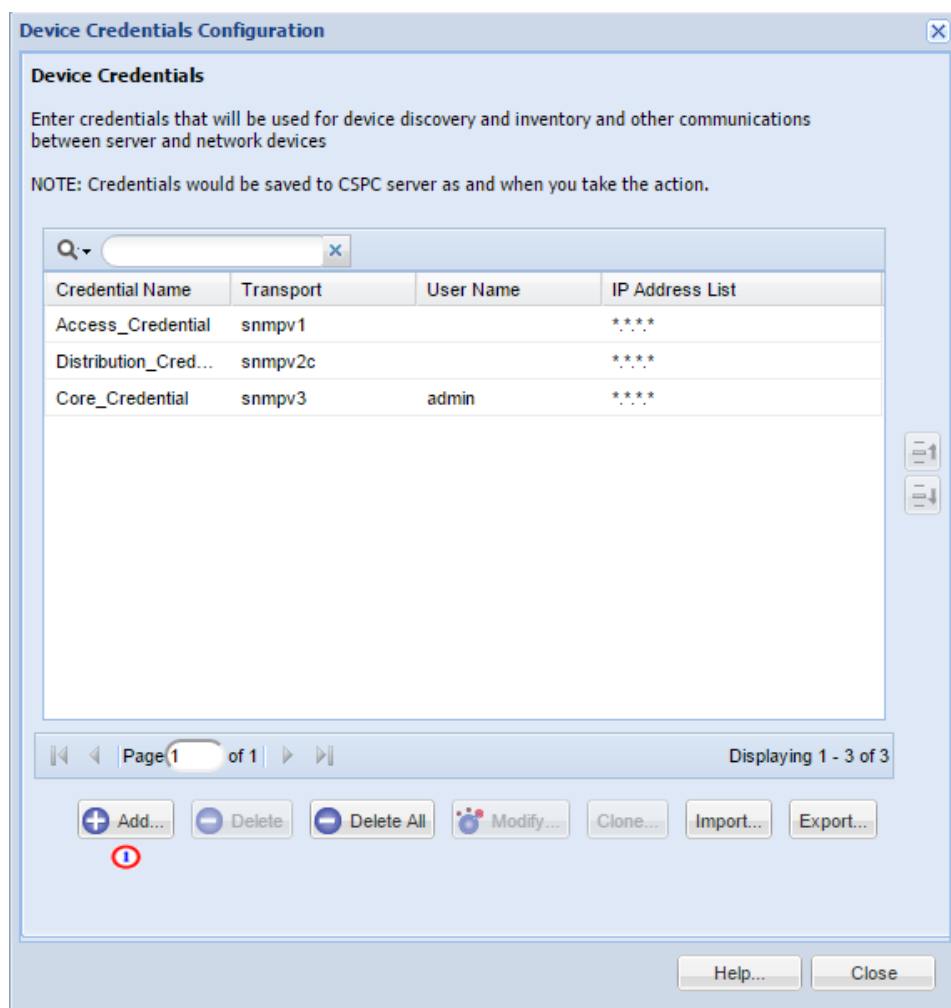
在 CSPC 中设置设备凭证是为了以下两个目的：

- SNMP 凭证用于首次发现设备和收集数据。
- 除 SNMP 凭证外，其余的凭证（telnet、SSH、HTTP 和 HTTPS 凭证）用于从发现的设备收集数据。

要设置使用 SNMP 协议的设备凭证，请执行以下步骤：

- 在 CSPC 菜单中，选择**设置 > 设备凭证**。

系统显示“设备凭证配置”窗口。



- 点击**添加**  创建凭证。

系统将显示设备凭证窗口，其中包含凭证标识、身份验证信息和 SNMP 只读团体字符串的详细信息。

Device Credentials

Credential Identification

* Name: UAT_Test (1)

Transport

Protocol: snmpv2c

Port: 161

Authentication

User Name: _____

Password: _____

Enable User Name: _____

Enable Password: _____

Pass Phrase: _____

Certificate: _____

SNMP V1/V2 Community Strings

Read Community: _____ (2)

Write Community: _____

SNMP V3 Authentication Details

* User Name: _____

Engine Id: _____

Auth Algorithm: _____

Auth Password: _____

Privacy Algorithm: _____

Privacy Password: _____

Include Ip Address Ranges/List (For Discovery and Data Collection)

* IP Address List: _____ (3)

Exclude Ip Address Ranges/List (For Data Collection only)

Exclude Ip List: _____

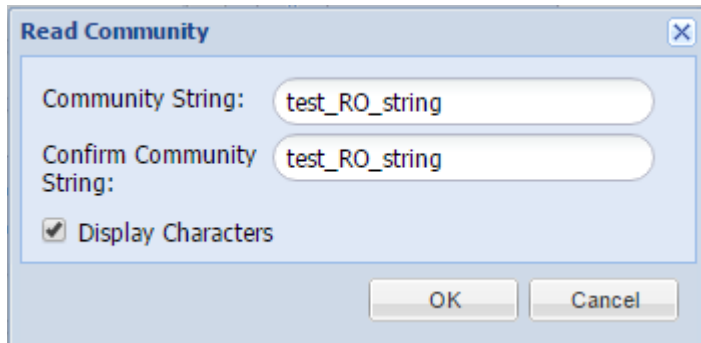
OK Cancel

填写所需数据：

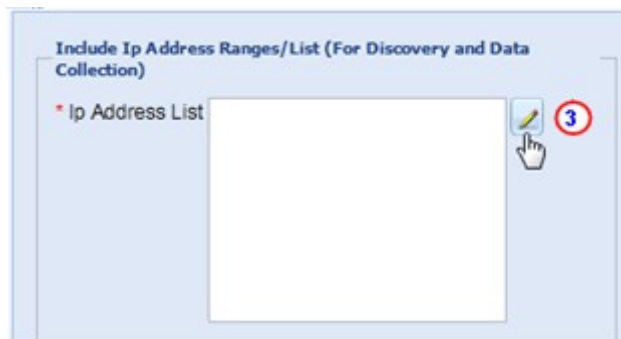
- 输入凭证名称（在本示例中，输入 UAT-Test）。(1)

凭证名称可以是您选择的任何名称，此名称应能代表您所在的组或区域。

- 在“传输”部分中，点击“协议”字段下拉列表，然后指定字符串的 SNMP 版本。
- 对于“SNMP V1/V2 社区字符串”部分，点击 ... 图标输入各自的读取社区字符串。② 系统将显示“输入读取团体字符串”窗口。




- 在“输入读取团体字符串”窗口中，输入读取社区字符串。
- 然后，点击“确定”。



- 在设备凭证窗口中点击“IP 地址列表”字段右侧的铅笔图标 ③。
- 然后输入 IP 地址列表。

需要提供多个 IP 地址或 IP 地址范围，以定义用于发现设备并从发现的设备中收集数据的 IP 地址。



- 在“IP 地址列表”字段中输入 IP 地址后，点击**添加** .

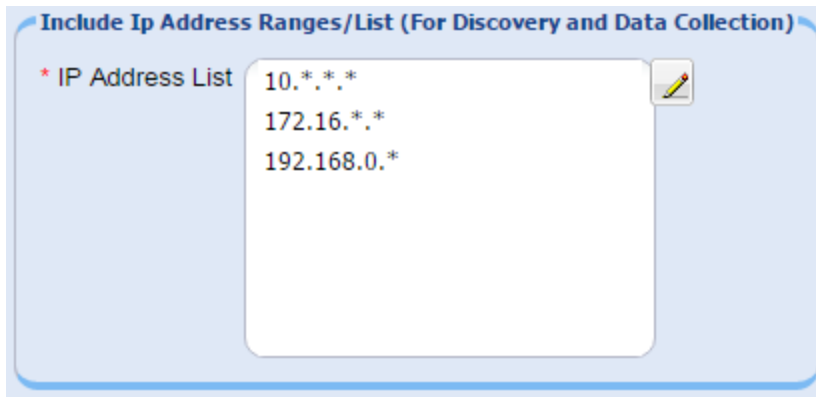
将输入的数据添加到 IP 地址列表中。

- 此列表用于指定 CSPC 可将该凭证用于哪些 IP 以与设备进行通信，从而执行设备发现或数据收集等操作。
- 您既可以提供特定 IP，也可以使用通配符替换 IP 的八位位组来创建 IP 地址范围。
- 对于此字段中不包括的 IP 或 IP 范围，CSPC 在尝试与拥有此类 IP 的设备进行通信时不会使用此凭证。
- 如果输入 *.*.*，CSPC 将会对所有 IP 使用该凭证。如果输入 172.16.*.*，则只允许将该凭证用于 172.16.0.0/16 子网中的设备。

引用的 IP 地址应尽可能严格或有限制，同时又能涵盖所有所需的设备。

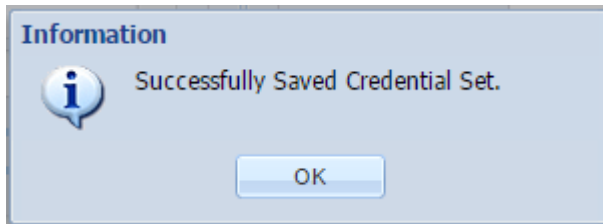
- 输入以上数据后，点击**确定**。

新 IP 将显示在“IP 地址列表”字段中。



- 点击**确定**。

保存成功后系统将显示“编辑凭证”窗口。



- 点击**确定**。

系统将关闭此窗口。

接下来的步骤用于执行设备发现、资产收集和上传。

要收集 show 命令信息，除了刚刚创建的 SNMP 凭证外，您还需要创建 SSH 和/或 Telnet 凭证。请遵循和上面相同的逻辑，但要将协议设为 SSH 或 Telnet，并使用相应的用户名/密码填充“身份验证”部分，而不是填充“SNMP V1/V2 社区字符串”部分。

设备发现；资产数据收集和上传

执行资产上传需要完成多个不同的程序，包括：

- 发现设备
- [运行收集配置文件并上传数据](#)

发现设备

本节介绍发现设备的三种方式以及如何运行发现作业：

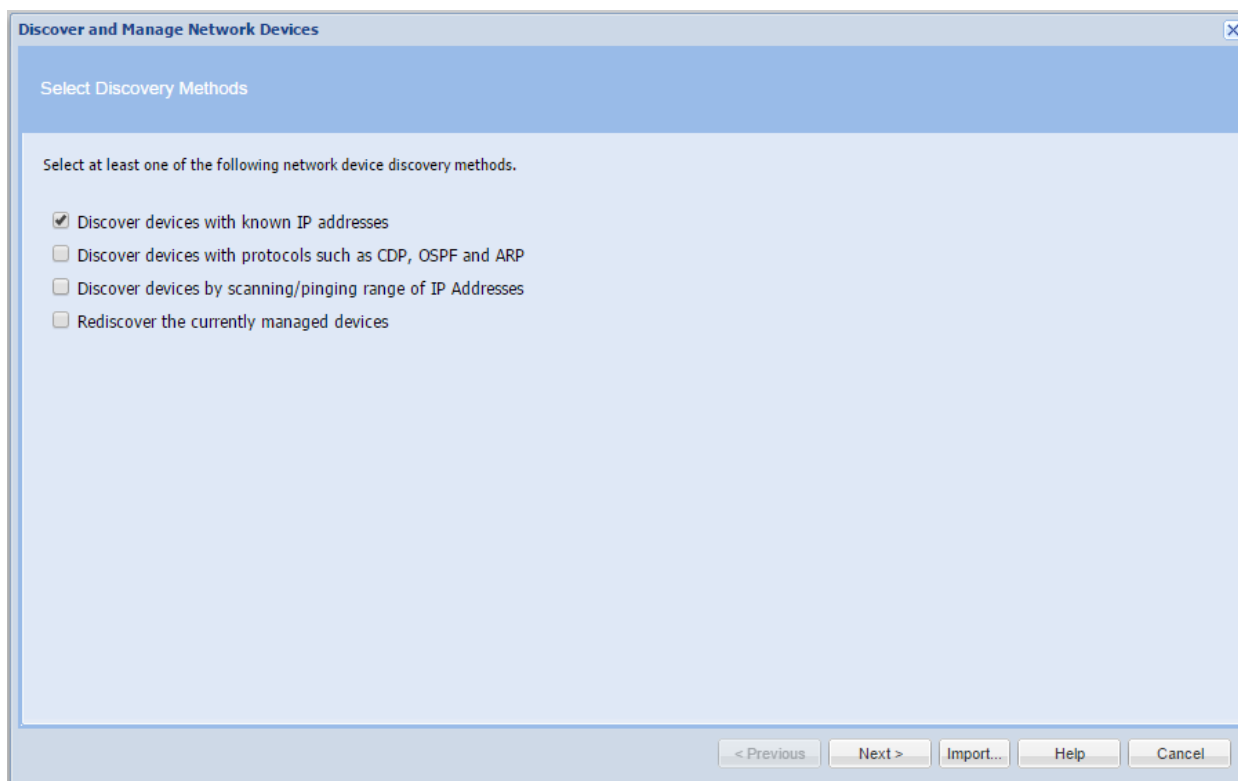
- [使用已知的 IP 地址发现设备](#)
- [通过 CDP、OSPF 和 ARP 等协议发现设备](#)
- [通过扫描/Ping IP 地址范围发现设备](#)
- [发现计划选项](#)

要使用上述 3 种发现方式之一发现设备，请选择**管理 > 发现并管理设备**。

系统将显示“发现和管理网络设备”窗口。

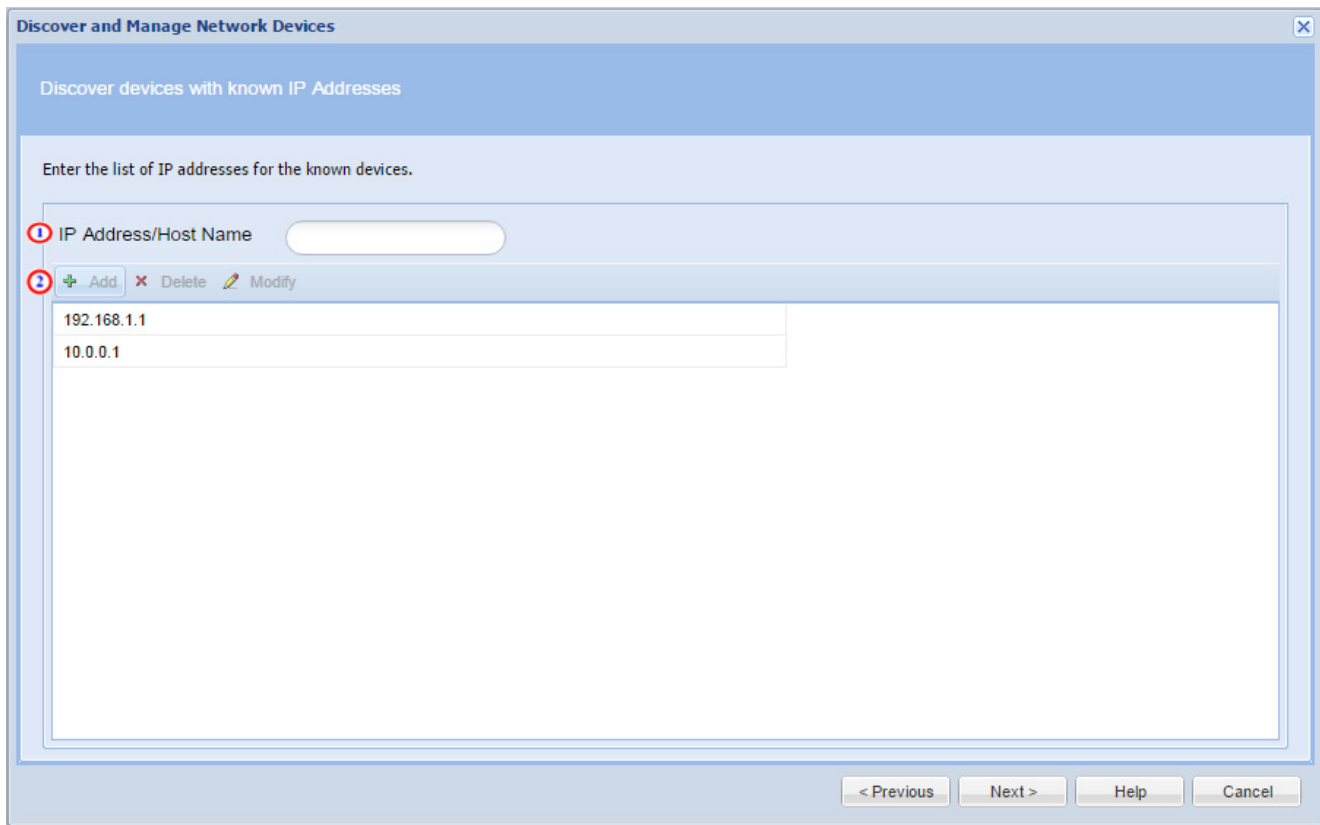
使用已知的 IP 地址发现设备

此发现过程将查找托管网络中的可用设备，其中设备的 IP 地址是已知的。要发现这些设备，请执行以下步骤：



- 选择要用于发现的方法。
- 然后点击**下一步**。

系统将显示与您选择的方法关联的窗格。



- 输入您希望从网络中发现的设备的 IP 地址。在“IP 地址/主机名称”字段中输入 IP 地址，**①** 然后点击 **+ 添加**，**②** 或按 Enter 键。

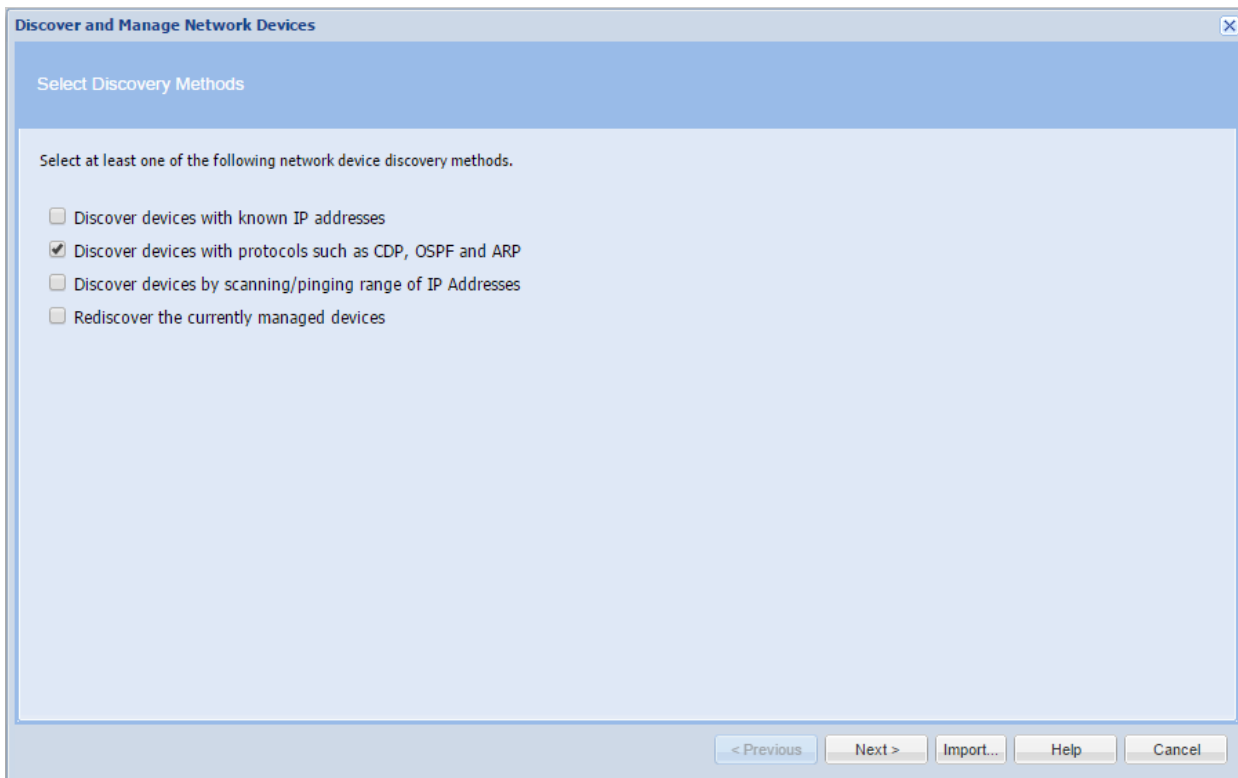
该 IP 地址即已添加到“IP 地址”列表中。

您可以在“IP 地址/主机名称”字段中的两个 IP 地址之间使用空格，同时添加多个 IP **①**。

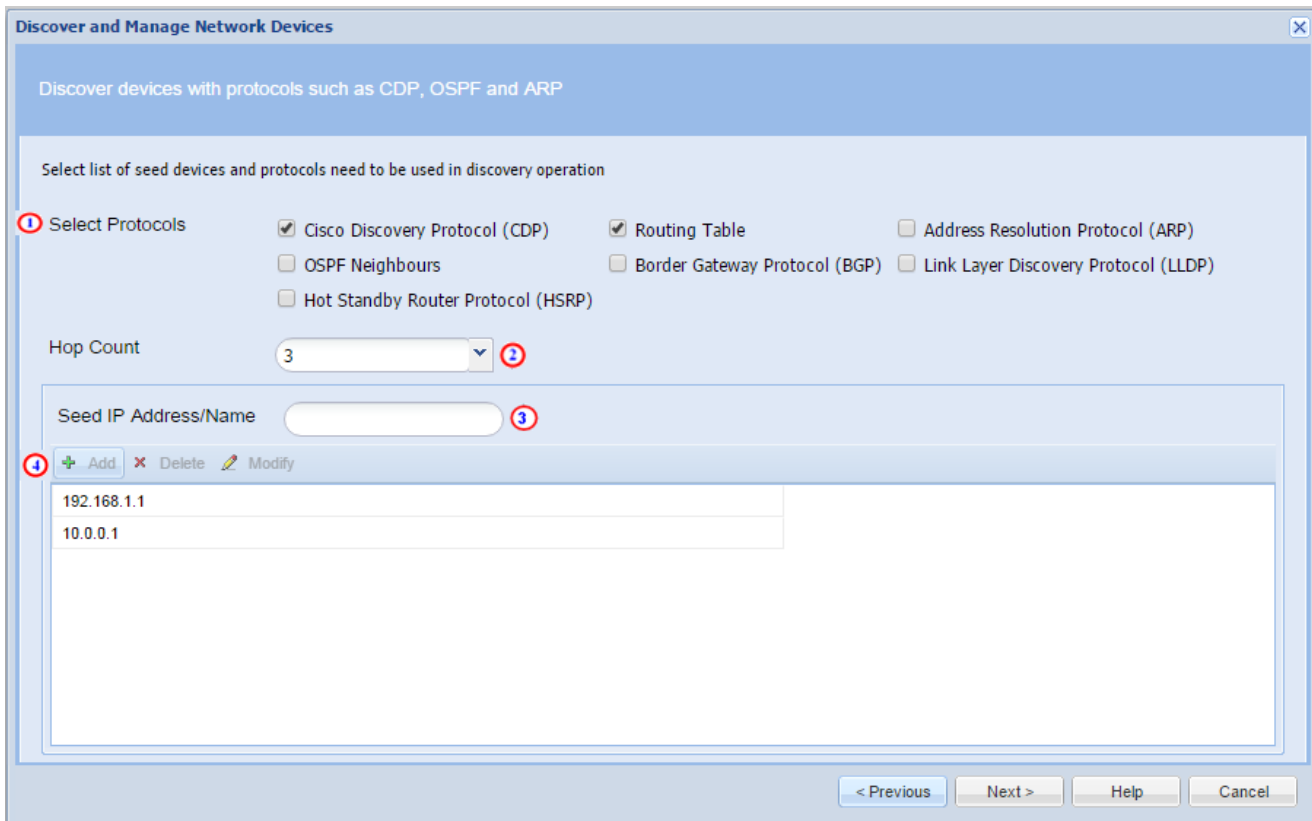
- 点击“下一步”继续设置[发现计划选项](#)。

通过 CDP、OSPF 和 ARP 等协议发现设备

此方法通过使用协议表（如思科发现协议 [CDP] 和地址解析协议 [ARP]）来发现网络设备。从发现的设备中收集的数据用于查找网络中的其他设备。



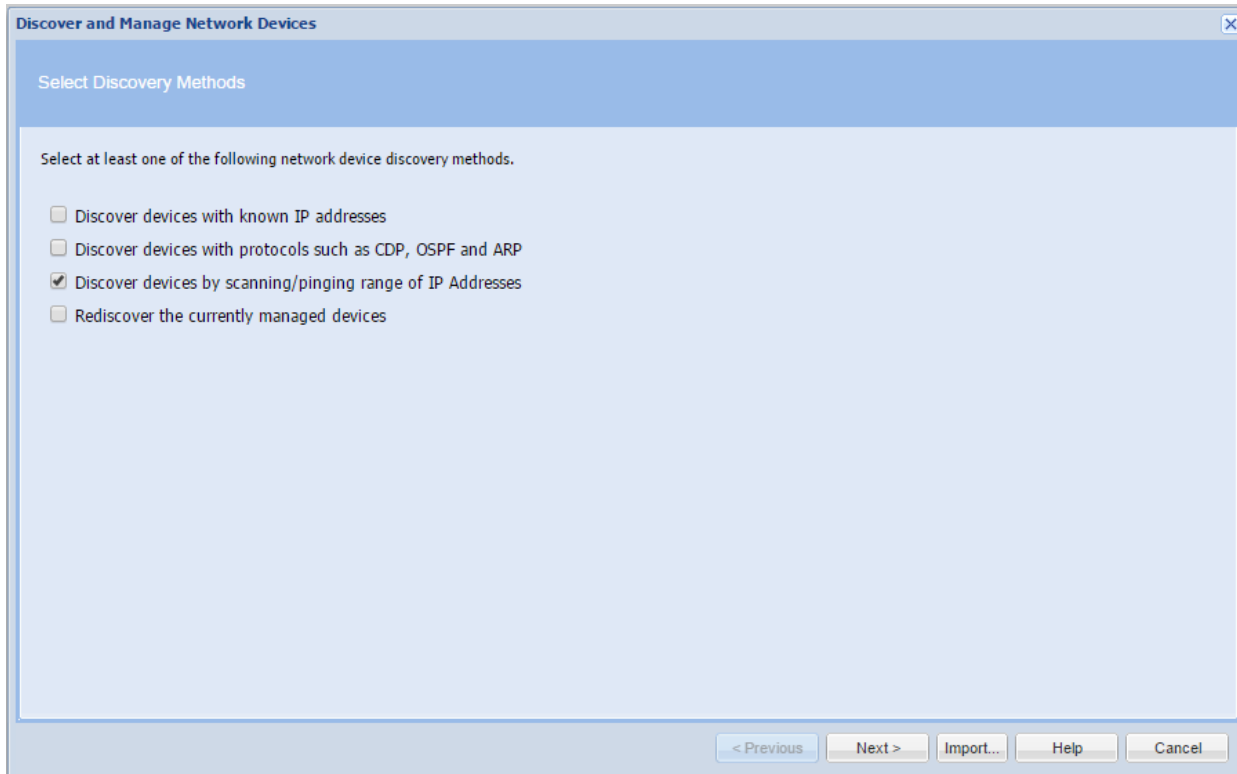
- 选择“通过 CDP、OSPF 和 ARP 等协议发现设备”。
- 然后点击下一步。



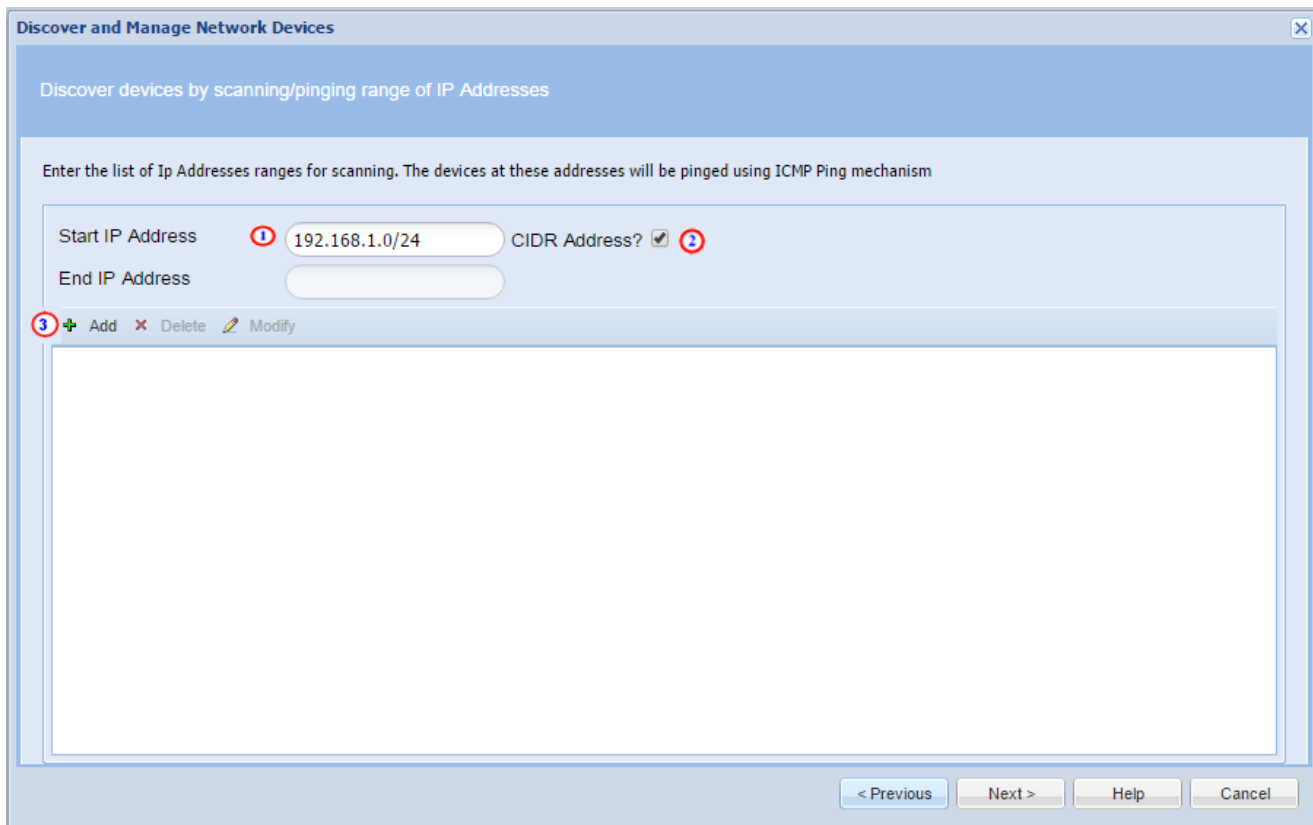
- 点击您希望 CSPC 考虑的协议旁边的复选框，以选择协议。收集器将查看设备中的相应表，在这些表中查找目标设备的 IP 地址。①
- 指定您希望 CSPC 超越种子设备的跳数值。②
- 输入您的种子设备 IP 地址 ③，然后点击 **+添加** ④ 将它们添加到种子设备列表。
- 点击“下一步”继续设置[发现计划选项](#)。

通过扫描/Ping IP 地址范围发现设备

此方法使用 SNMP 与您指定的范围内的所有 IP 地址联系。您可以提供该范围的起始 IP 地址和结束 IP 地址，或使用 CIDR 表示法指定特定子网。



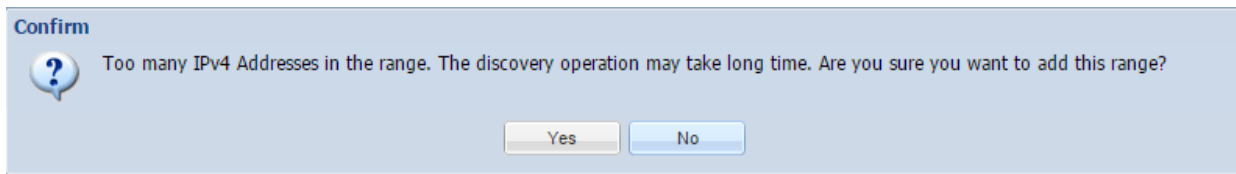
- 选择“通过扫描/Ping IP 地址范围发现设备”。
- 然后点击下一步。



您可以通过指定确切的起始和结束 IP 地址，或使用相应的 CIDR 表示法输入网络地址，来输入范围。
此例中突出显示了 CIDR 选项。

- 在“起始 IP 地址”字段中输入网络地址 **1**，然后输入斜线 (/) 以及相应的网络位数。然后，点击“CIDR 地址”复选框 **2** 并按 **+添加**。 **3**

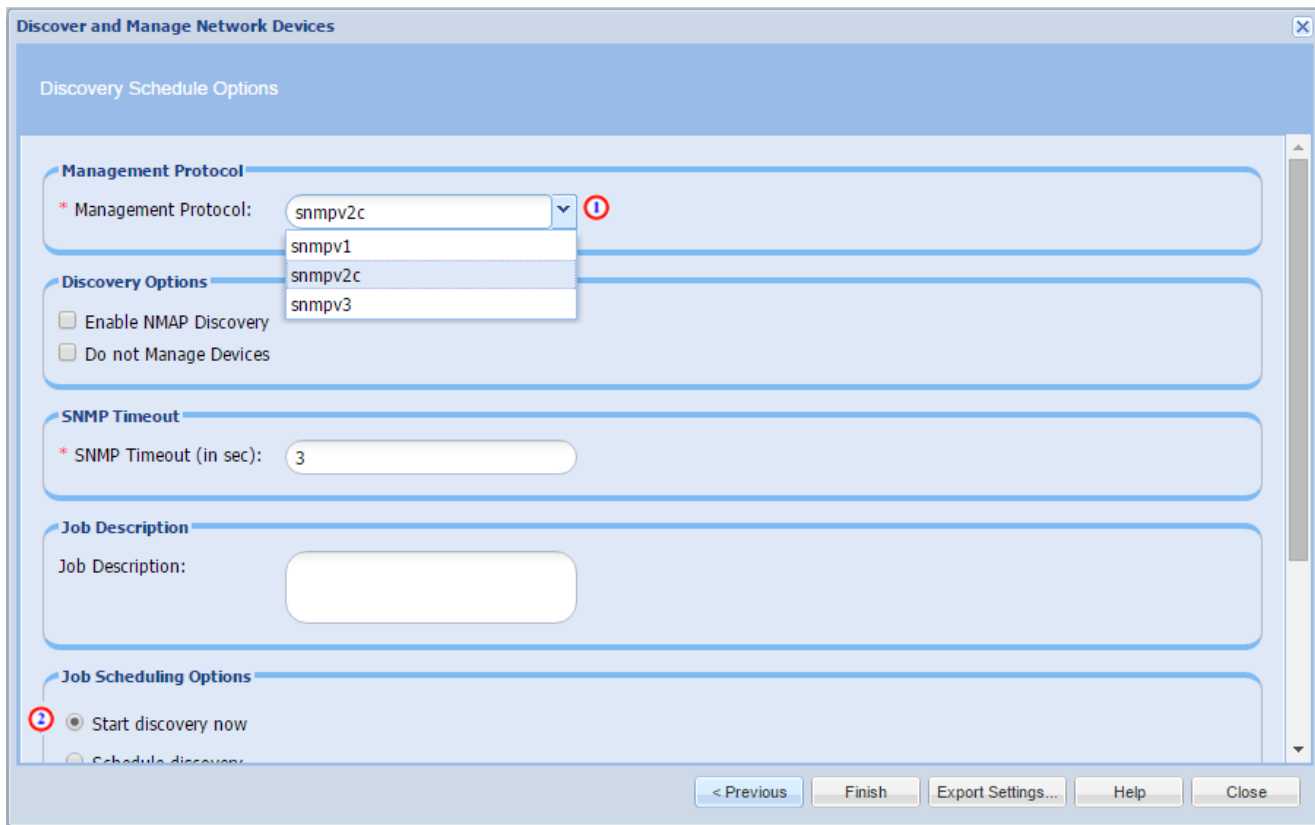
如果地址范围超过 255 个地址，系统将弹出以下消息。该消息通知您可能需要一些时间才能完成发现作业。



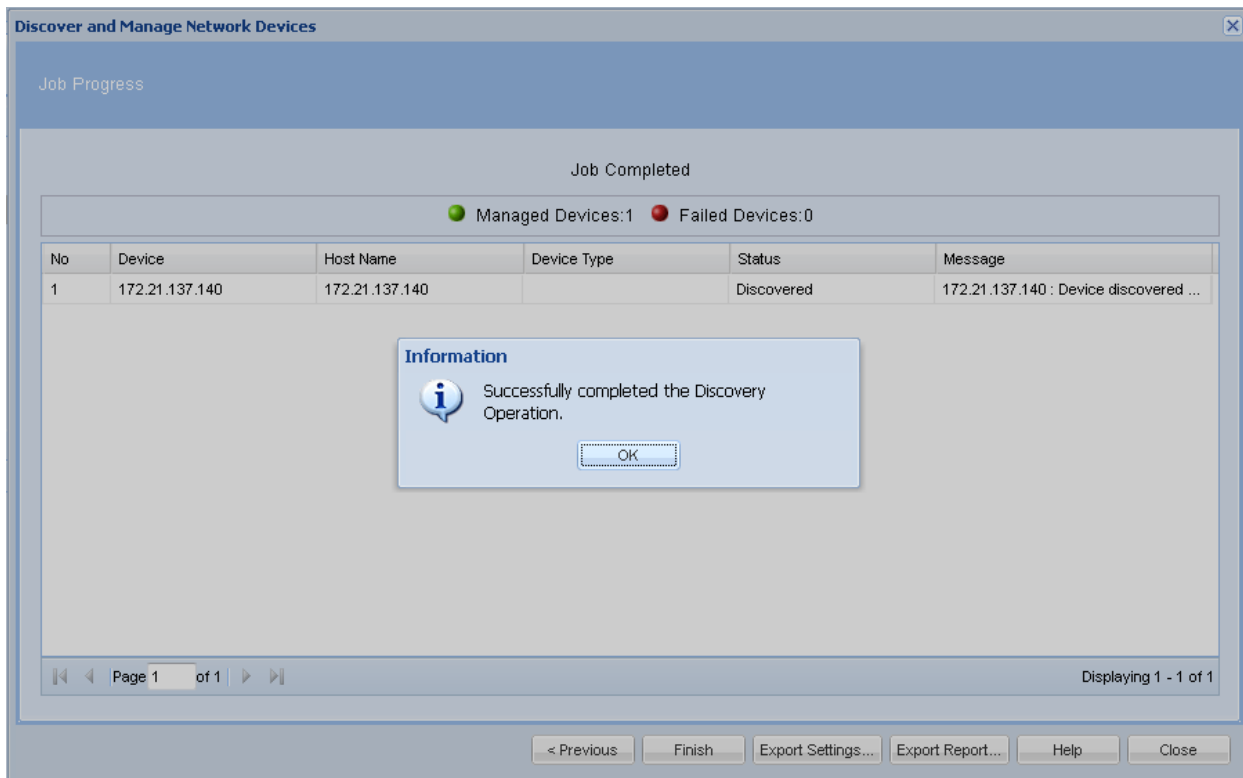
- 点击“是”并继续。

发现计划选项

选择上述三种发现选项之一并输入您的 IP 地址或 IP 地址范围后，决定您是想要立即运行设备发现操作，还是安排在稍后执行该操作。



- 在“管理协议”下，选择与设备凭证对应的 SNMP 版本。①
- 决定您是希望立即运行设备发现操作，还是安排在稍后执行该操作。② 在本示例中，我们将考虑使用立即发现选项。
- 点击**完成**后，系统将会运行发现作业。



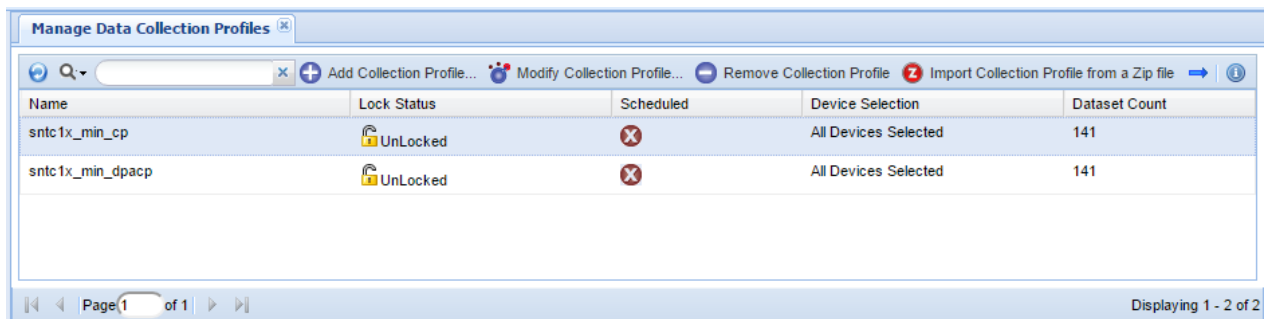
执行上述步骤后，系统会显示“已成功完成发现操作”消息。

- 点击**确定**。

运行收集配置文件并上传数据

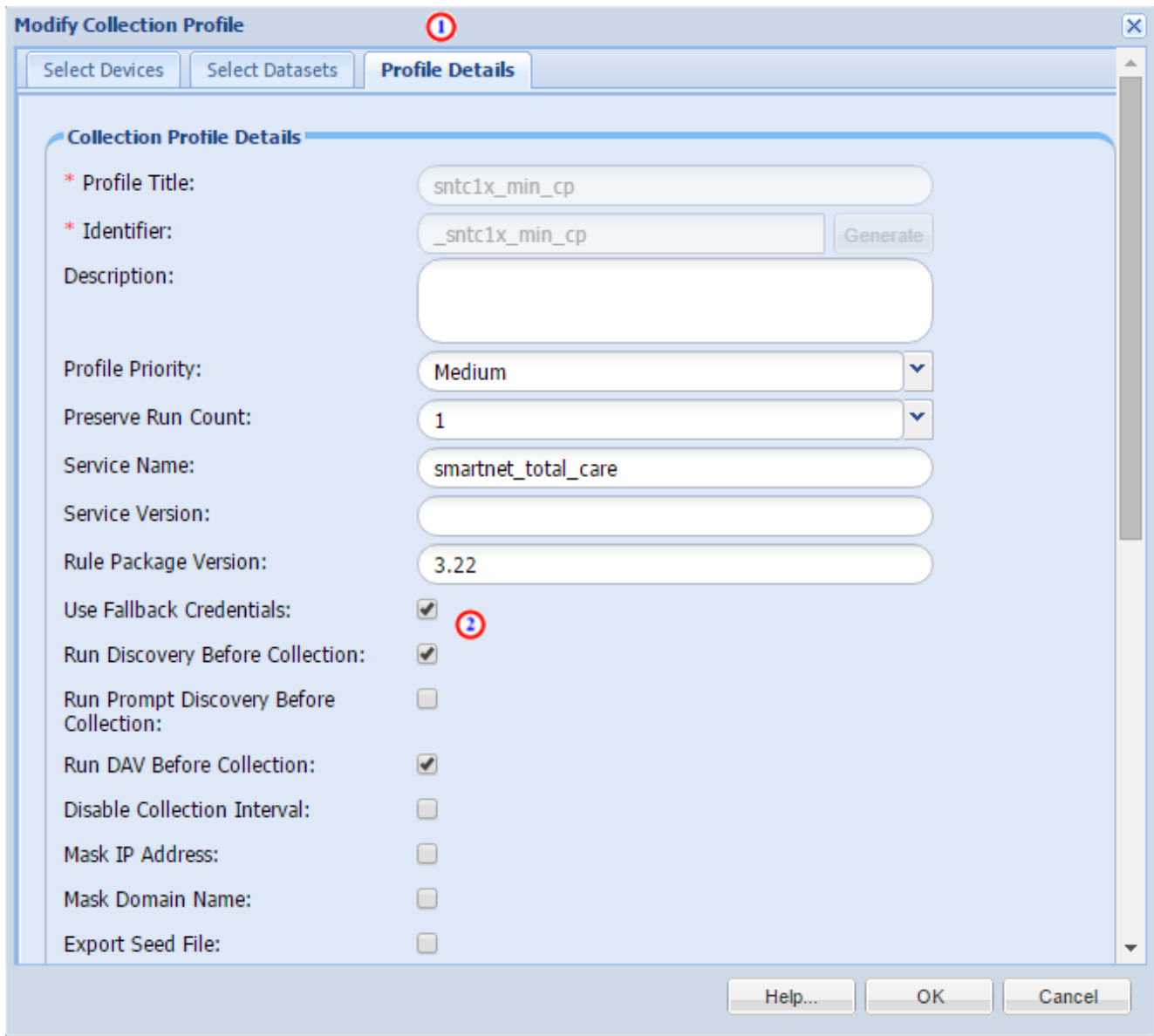
以下步骤将帮助您设置收集配置文件，让 CSPC 收集相关的设备数据，并在完成收集后向思科数据中心上传这些数据。

- 要管理您的收集配置文件，请转至**设置→管理数据收集配置文件...**。

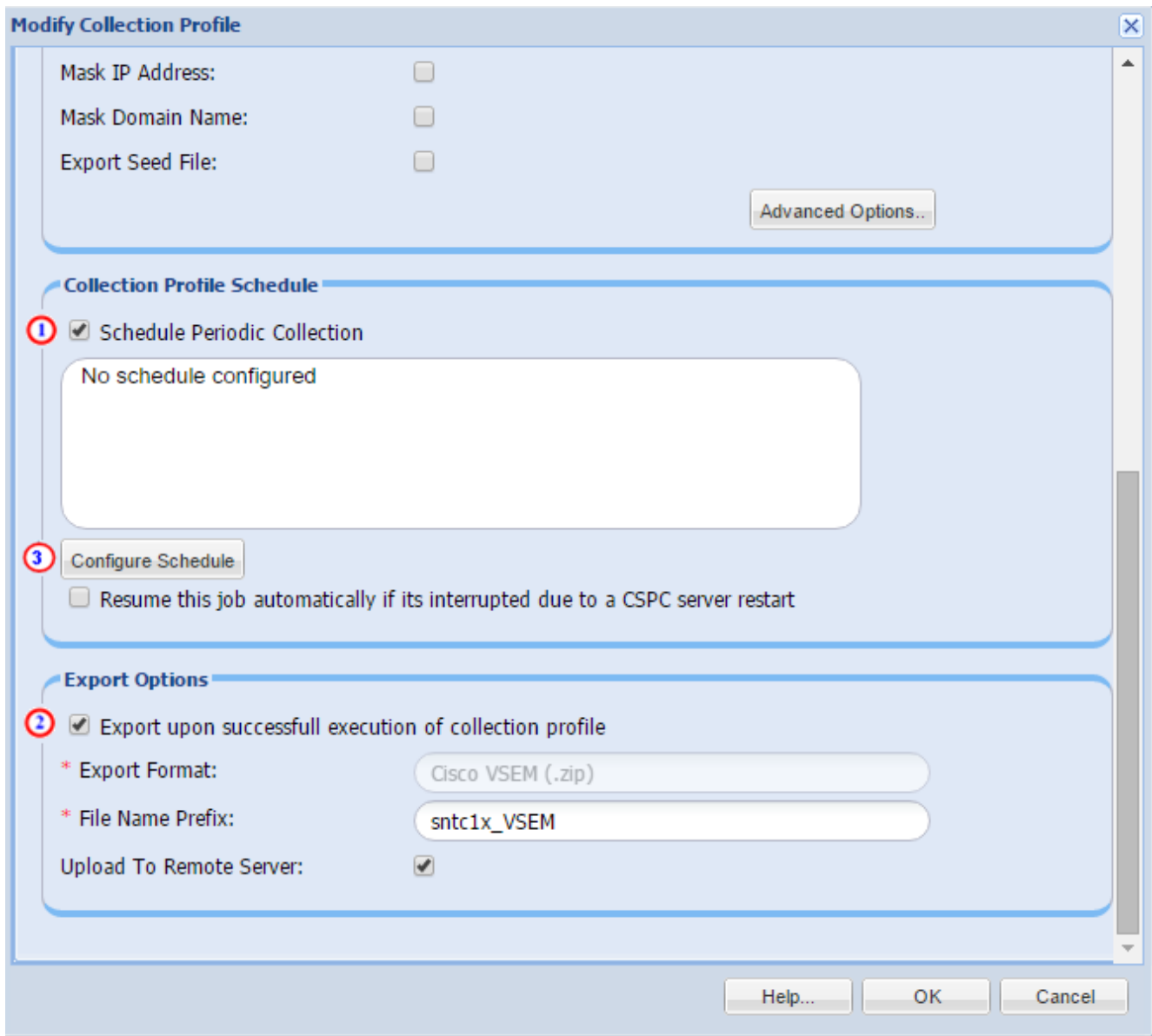


- 双击收集配置文件 **sntc 1x_min_cp**。系统将显示“修改收集配置文件”窗口。

该 CSPC 设备绑定了最低收集要求配置文件。最低收集要求配置文件包含每次收集/上传资产至少需要处理的强制收集命令。



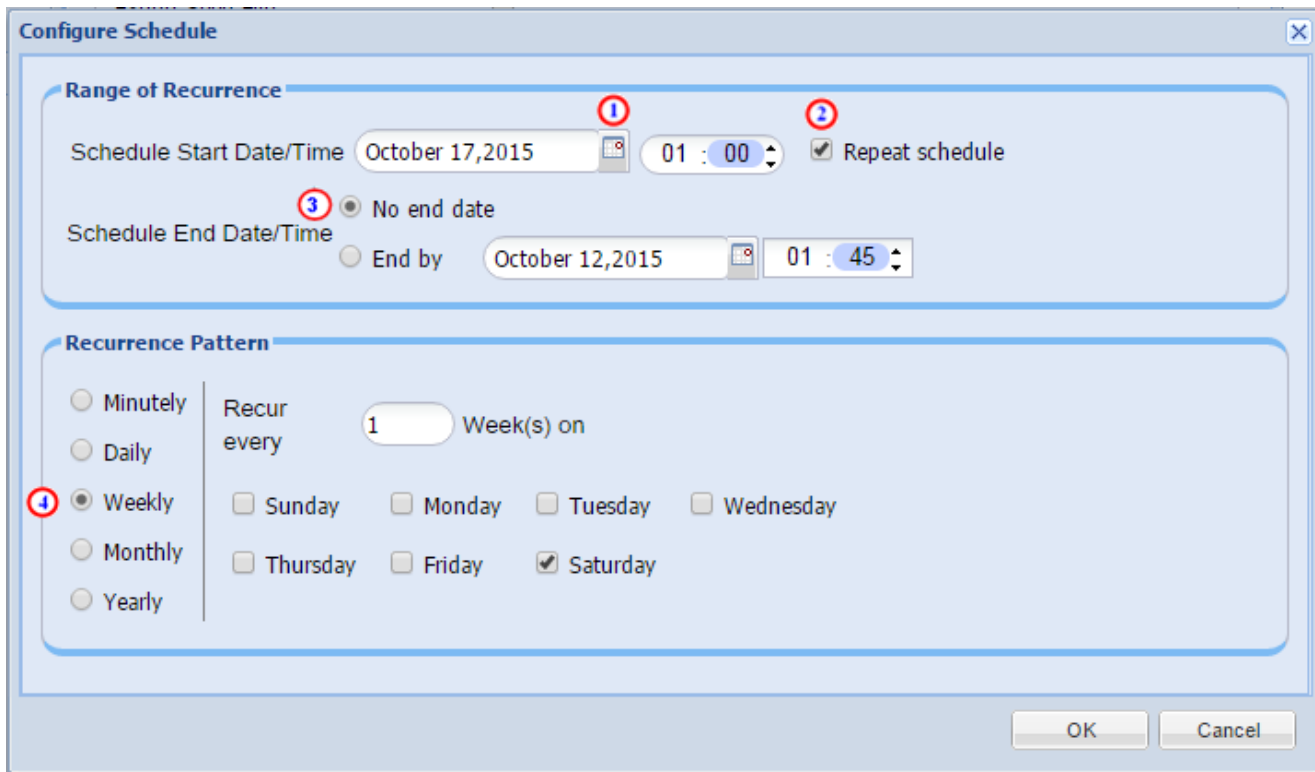
- 点击**配置文件详情**选项卡 **1**，然后选中“使用回退凭证”、“收集前运行发现”和“收集前运行 DAV”复选框。 **2**



- 向下滚动到窗口底部，并选中“计划定期收集”^①和“成功执行收集配置文件后导出”复选框。^②

通过选中“成功执行收集配置文件后导出”复选框上传数据。选中此复选框时，CSPC 完成收集后会将从收集配置文件收集的数据上传到思科。

- 点击“配置计划”^③继续转至“配置计划”屏幕。



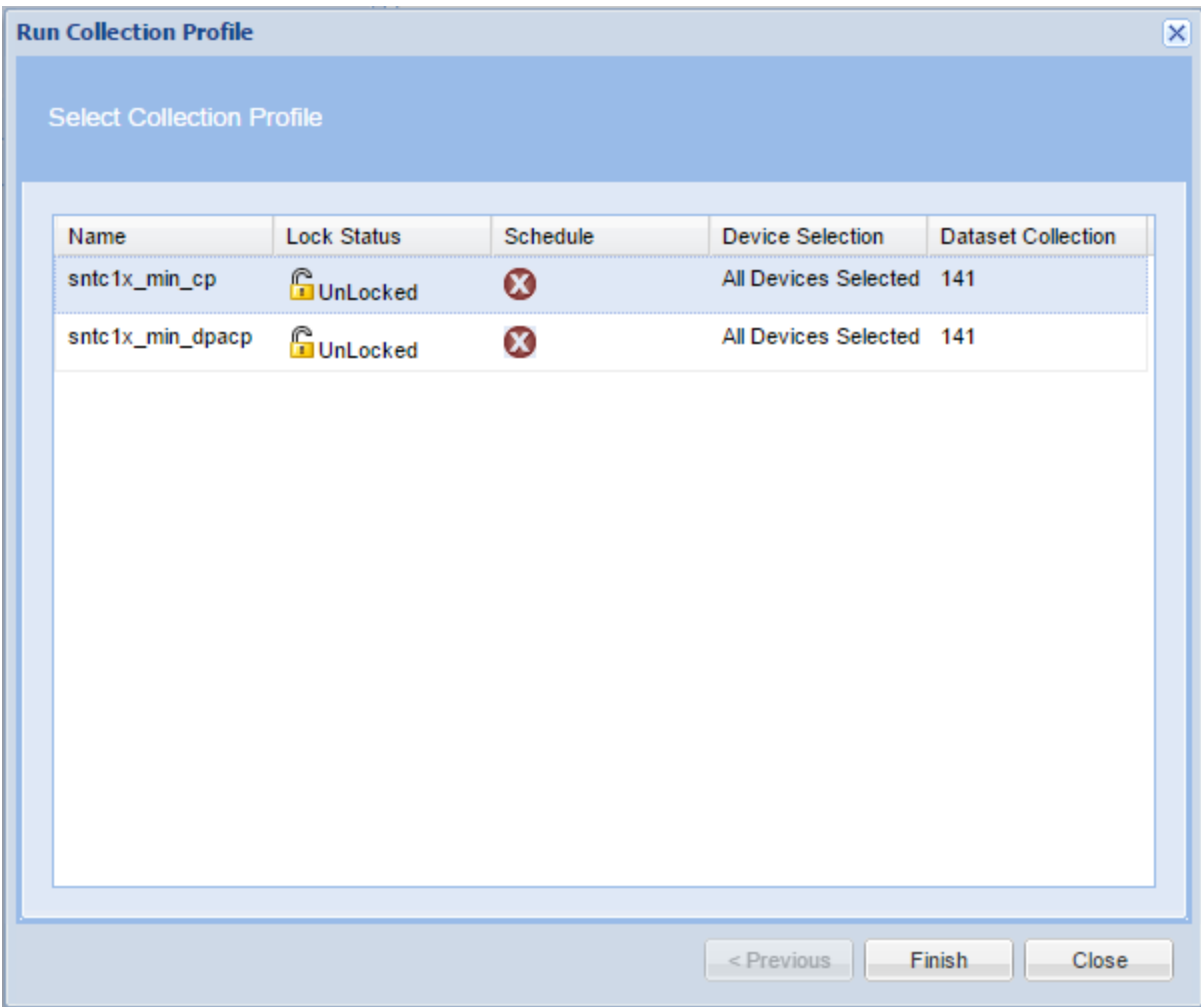
- 点击“日历”图标选择第一次收集的日期。①
- 系统将会弹出日历；请选择一个日期。

选择日期后，系统将返回“配置计划”窗口。

- 输入您希望执行收集的时间。
- 选中“重复计划”复选框。②
- 然后选择“无结束日期”单选按钮。③
- 现在，请选择“重复模式”。④
- 点击**确定**保存更改并返回到“修改收集配置文件”窗口。
- 点击**确定**关闭“修改收集配置文件”窗口。


系统将在您指定的日期和时间收集数据。



如果您希望运行按需收集，请转至**管理→运行收集配置文件**，选择 **sntc1x_min_cp**，然后点击**完成**。请参考下方的屏幕截图。








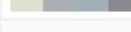

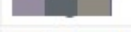


Run Collection Profile


Job Progress

Running Collection Profile Job(3%) 


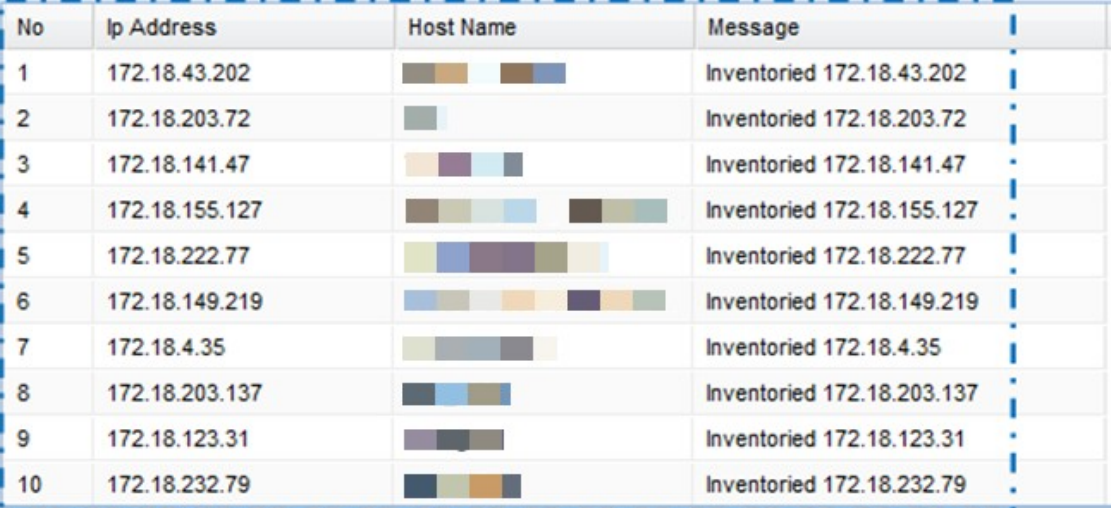
Selected Devices:1618  Completed Devices:69 


No	Ip Address	Host Name	Message
1	172.18.43.202		Inventoried 172.18.43.202
2	172.18.203.72		Inventoried 172.18.203.72
3	172.18.141.47		Inventoried 172.18.141.47
4	172.18.155.127		Inventoried 172.18.155.127
5	172.18.222.77		Inventoried 172.18.222.77
6	172.18.149.219		Inventoried 172.18.149.219
7	172.18.4.35		Inventoried 172.18.4.35
8	172.18.203.137		Inventoried 172.18.203.137
9	172.18.123.31		Inventoried 172.18.123.31
10	172.18.232.79		Inventoried 172.18.232.79

Page 1 of 2 Displaying 1 - 50 of 69

 **1**

< Previous Export Report... Finish Close

数据收集的详细信息已填妥。摘要显示在上方 ，详细信息显示在下方。 

- 收集过程完成后，可以导出上述报告，方法是点击**导出报告...**按钮。 
- 当您完成导出时，请点击**关闭**，或在后台运行收集。

收集作业完成时，上传的数据将发送至思科数据中心。最长 24 小时后，门户会处理您上传的数据。

您可以查看上传状态，方法是转至：<https://tools.cisco.com/smartservices>，然后点击**库**→**管理**→**上传处理**