Cisco CSPC 2.6 Collector

Quick Start Guide

August 2016

Contents

1. Introduction to CSPC

This document provides information about the CSPC release. In order to configure CSPC and ensure a successful setup, you should have experience configuring devices from a command line as well as a basic understanding of network management systems.

CSPC is an SNMP-based tool that discovers and collects information from your Cisco devices. You should know the SNMP Read Only community string(s) that are set up on your devices. This document will walk you through the steps for a basic CSPC setup.

Prerequisites

Before you'll have the ability to generate the CSPC's license file, you'll first need to complete your portal onboarding to gain access to your service portal. To do that follow the link below.

https://tools.cisco.com/smartservices

(portal Registration Required)

Browsers

CSPC supported browsers are Firefox version 27 to 42 and Internet Explorer (IE) version 9 to 11.

2. Virtual Platform Requirements

This section provides information about the virtual platform requirements. This guide does not provide directions on how to install the different virtual platforms.

These are the system requirements for the collector image that runs on a ESXi 4.x or higher virtual platform:

- 250 GB of hard drive space
- 4 CPU cores (virtual CPUs)
- 1 virtual NIC (number of NICs required is dependent upon the network topology)
- 4GB of virtual RAM

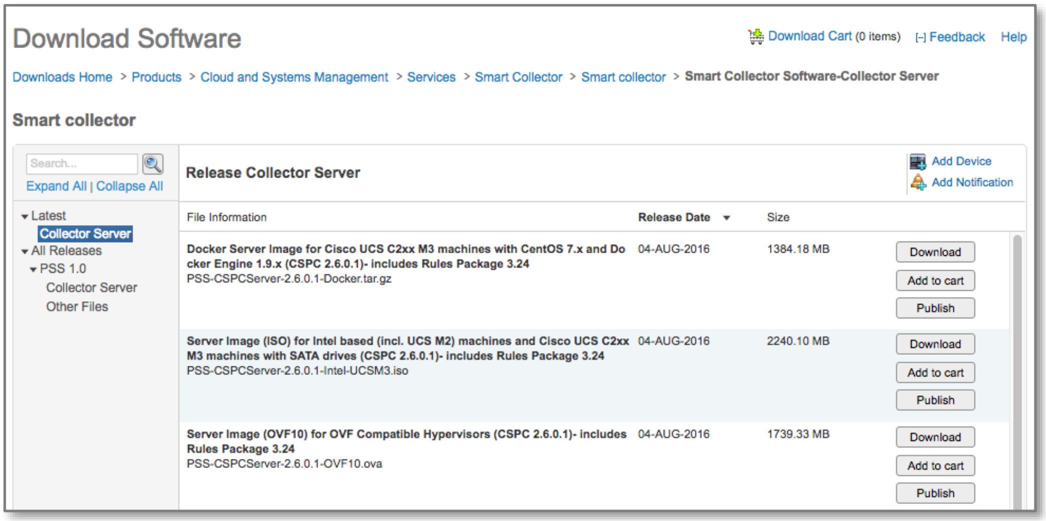
3. Download the Virtual Machine Image

After ensuring that your virtual environment can provide the needed resources, the next step is to download the CSPC collector image. The software image can be obtained from the download center. The download center contains the most recent software image. To access the CSPC collector image, perform the following steps:

- Go to the following URL:

https://software.cisco.com/download/release.html?mdfid=283114009&flowi d=17761&softwareid=283308 676&release=Collector%20Server&relind=AVAILABLE&rellifecycle=&reltype=latest

- Login with your CCO ID and password if requested.



Download Software

Downloads Home > Products > Cloud and Systems Management > Services > Smart Collector > Smart collector > Smart Collector Software-Collector Server

Smart collector

Release Collector Server

File Information	Release Date	Size
Docker Server Image for Cisco UCS C2xx M3 machines with CentOS 7.x and Docker Engine 1.9.x (CSPC 2.6.0.1)- includes Rules Package 3.24 PSS-CSPCServer-2.6.0.1-Docker.tar.gz	04-AUG-2016	1384.18 MB
Server Image (ISO) for Intel based (incl. UCS M2) machines and Cisco UCS C2xx M3 machines with SATA drives (CSPC 2.6.0.1)- includes Rules Package 3.24 PSS-CSPCServer-2.6.0.1-Intel-UCSM3.iso	04-AUG-2016	2240.10 MB
Server Image (OVF10) for OVF Compatible Hypervisors (CSPC 2.6.0.1)- includes Rules Package 3.24 PSS-CSPCServer-2.6.0.1-OVF10.ova	04-AUG-2016	1739.33 MB

- Click the **Download** button for the version you need. If you are prompted, accept the Terms and Conditions to start the image download.

- Deploy this image to your environment.

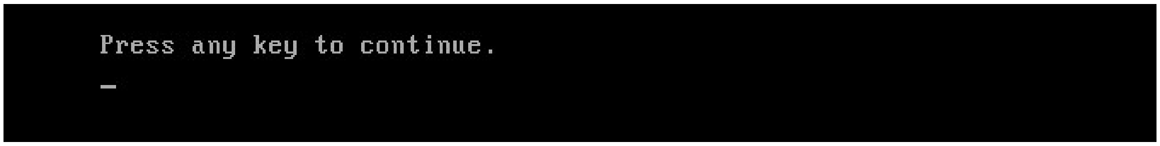
4. Configure Appliance IP Address

This section applies to both the virtual machine and hardware platform versions of the appliance. To configure the IP address of the appliance, perform the following steps:

- For hardware appliances: connect a monitor and keyboard to the server.
- For software appliances: connect to the virtual machine console using your virtual environment'stools.

After powering on the collector, you should see a request to press any key.

- Press any key



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

The "Press any key" display is normal during the boot up process and may take several minutes before you will see a login prompt.

- Log into the software appliance via connected console using the following login id/pw information:

admin/Admin!23

By default, the following user accounts are created:

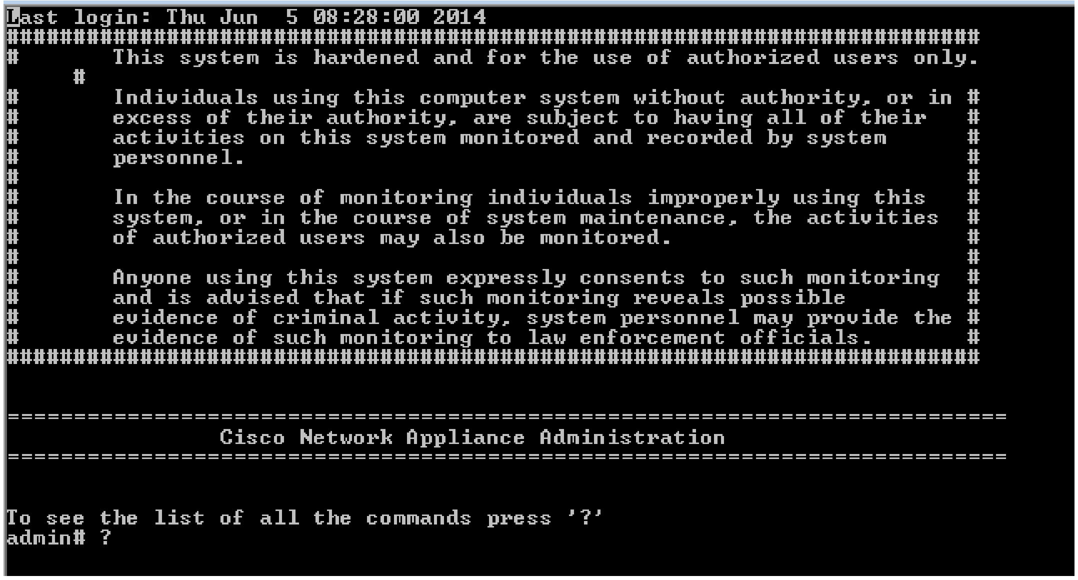
User-ID	Password	Shell
admin	Admin!23	Admin Shell (CLI)
Admin123	Admin123	CSPC Web GUI
collectorlogin	<Disabled by default>	Linux (Bash)
root	<Disabled by default>	Linux (Bash)

By default, the only user enabled for CLI access is 'admin'

To enable **collectorlogin** and **root** User IDs, use the `pwdreset` command. [Refer to CLI Commands section]

On the first login, the appliance forces a password change from the default CLI password.

After logging in to the appliance you will see the following screen:



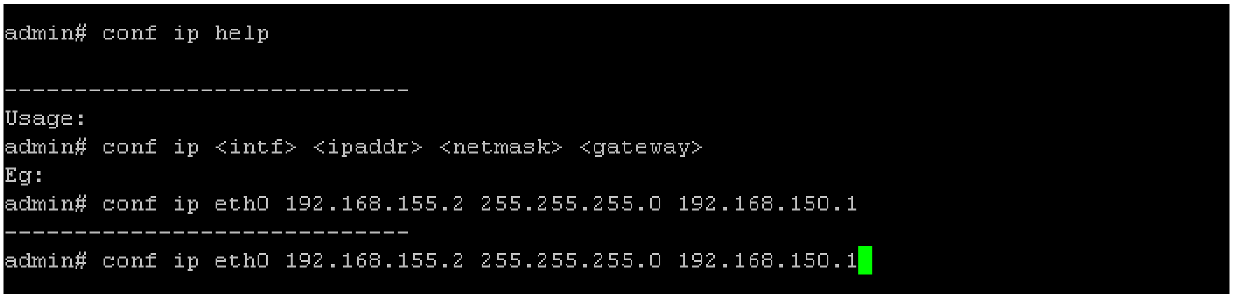
```
Last login: Thu Jun  5 08:28:00 2014
#########################################################################
#       This system is hardened and for the use of authorized users only.
     #
#       Individuals using this computer system without authority, or in #
#       excess of their authority, 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# ?
```

To assign a static IP address, the command **conf ip** is used.

- At the command prompt enter the following information:

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

For example: conf ip eth0 192.168.1.100 255.255.255.0 192.168.1.1



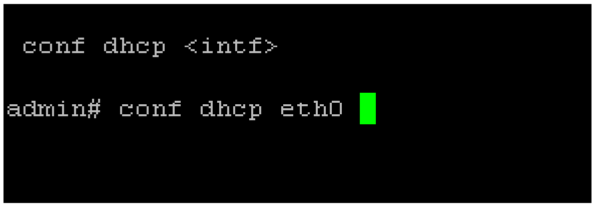
```
admin# conf ip help

----------------------------
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
```

To assign a dynamic IP address, the command **conf dhcp** is used.

- At the command prompt enter the following information:

  # conf dhcp <interface>

For example: conf dhcp eth0



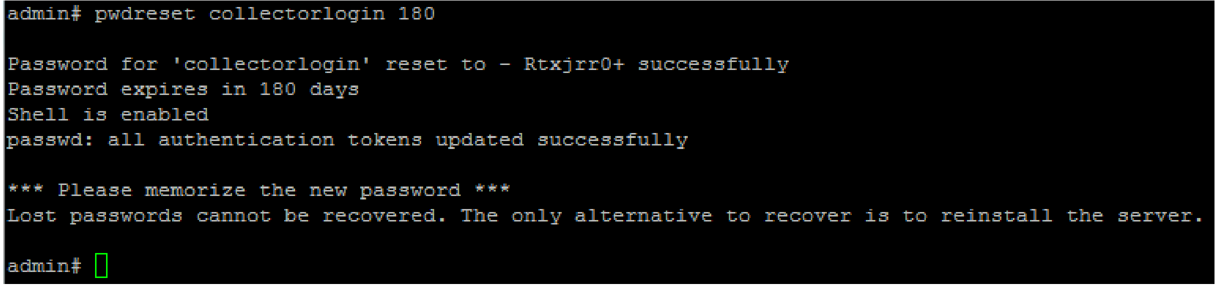
```
 conf dhcp <intf>

admin# conf dhcp eth0
```

Configure the DNS servers:
# conf dns –a <DNS IP address 1> <DNS IP address 2>

Configure the timezone by running this command and entering the appropriate value at the prompt:
# timezone

Configure the time by syncing with your NTP server. You can also press enter at the prompt to use the default:
# timesync

Enable the Linux user login “collectorlogin” and set in how many days it should expire (1-180)
# pwdreset collectorlogin 180

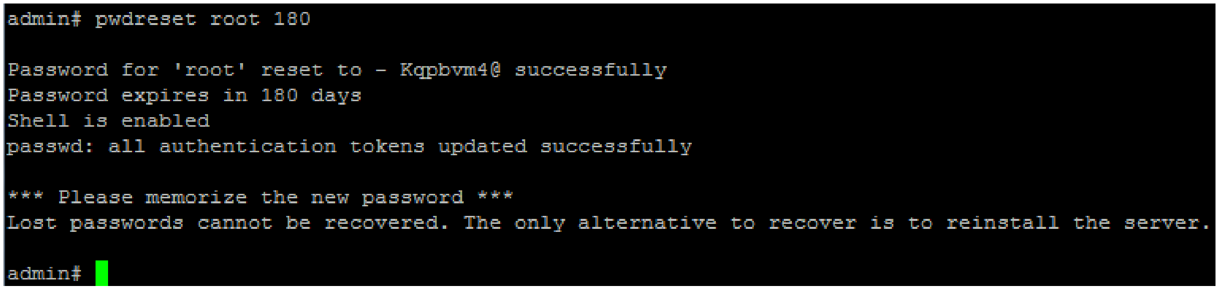


```
admin# pwdreset collectorlogin 180

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#
```

Record this password!

Enable the Linux root login and set in how many days it should expire (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#
```

Record this password!

To make the changed settings effective, the appliance needs to be rebooted.

- At the command prompt enter:

  # reboot

confirm the question on the screen with **y**

After the appliance has rebooted, confirm that the IP is correct.

- At the command prompt enter:

  # show ip

- Connect to the appliance via SSH to ensure you can manage the CSPC remotely.

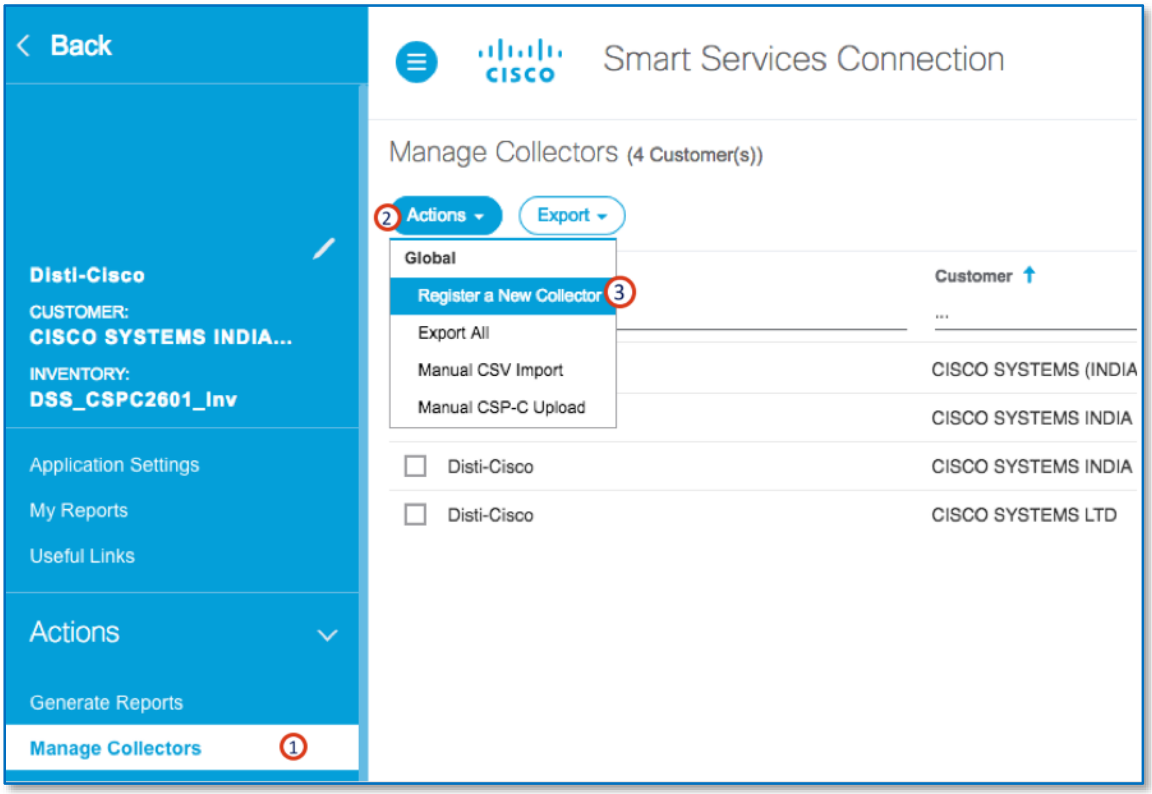
5. CSPC Registration

A CSPC registration needs to be performed before the collector can be utilized by the portal. The registration allows a validation to occur that creates a connection between the CSPC collector and the Cisco data center. The registration process requires you to obtain the entitlement files (a security certificate and other registration files). These registration/entitlement files are used later to complete the CSPC installation.

Important!
Do not unzip the entitlement file!

Log in to the service portal at https://tools.cisco.com/smartservices/

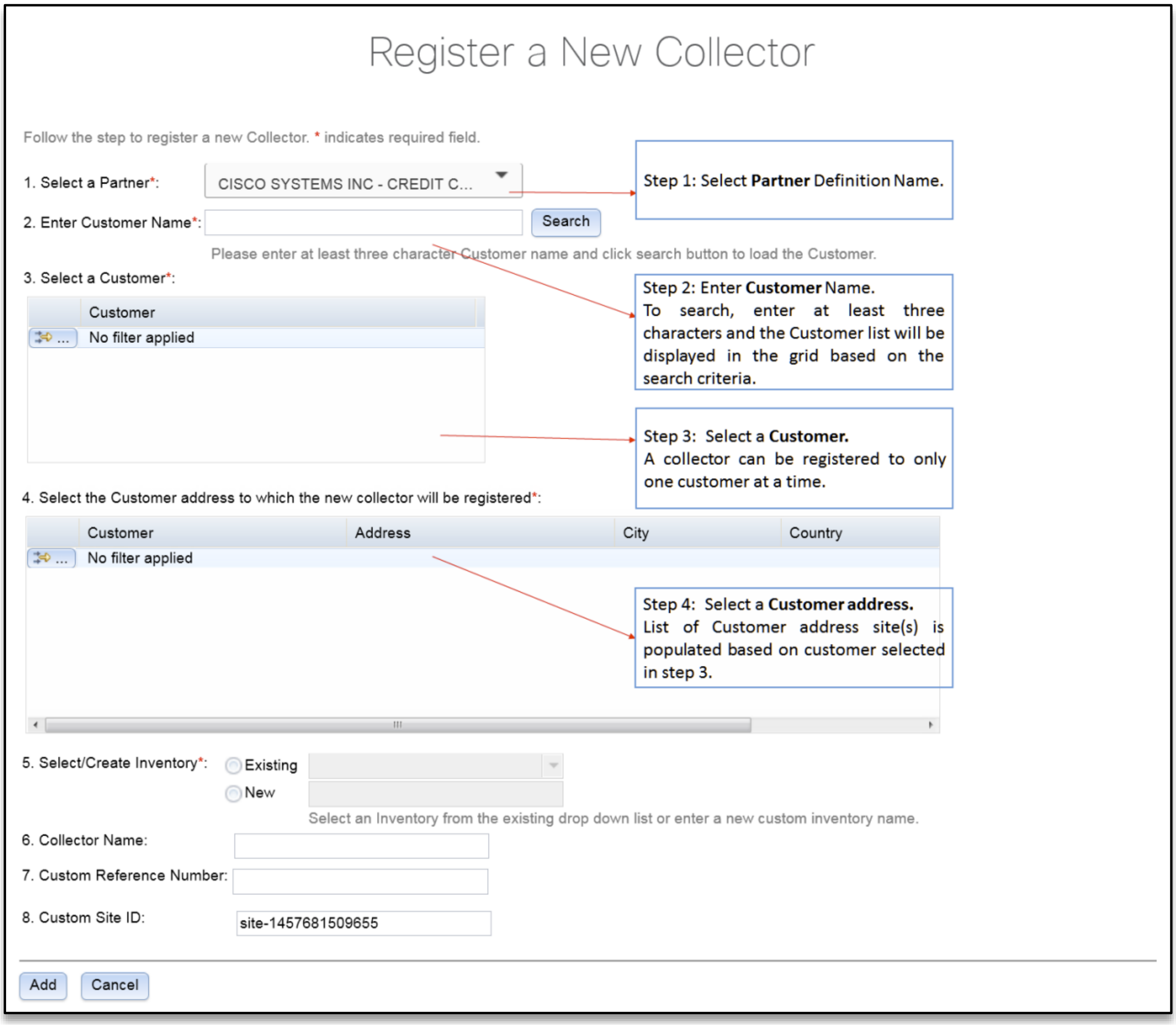
- From the left navigation pane, select **Actions > Manage Collectors**
- In the pane displayed, select the **Actions > Register a New Collector** option



Disti-Cisco
CUSTOMER:
CISCO SYSTEMS INDIA...
INVENTORY:
DSS_CSPC2601_Inv

	Customer
	CISCO SYSTEMS (INDIA
	CISCO SYSTEMS INDIA
□ Disti-Cisco	CISCO SYSTEMS INDIA
□ Disti-Cisco	CISCO SYSTEMS LTD

The Register a New Collector screen opens:



Register a New Collector

Follow the step to register a new Collector. * indicates required field.

1. Select a Partner*: CISCO SYSTEMS INC - CREDIT C...

2. Enter Customer Name*:

Please enter at least three character Customer name and click search button to load the Customer.

3. Select a Customer*:

Customer
No filter applied

4. Select the Customer address to which the new collector will be registered*:

Customer	Address	City	Country
No filter applied			

5. Select/Create Inventory*: ○ Existing ○ New

Select an Inventory from the existing drop down list or enter a new custom inventory name.

6. Collector Name:

7. Custom Reference Number:

8. Custom Site ID: site-1457681509655

Step 1: Select **Partner** Definition Name.

Step 2: Enter **Customer** Name.
To search, enter at least three characters and the Customer list will be displayed in the grid based on the search criteria.

Step 3: Select a **Customer.**
A collector can be registered to only one customer at a time.

Step 4: Select a **Customer address.**
List of Customer address site(s) is populated based on customer selected in step 3.

Complete the required fields as follows:

- The **Enter Customer Name** should be input into the form. This searches for all customers with valid contracts to register a collector for.
- **Select a Customer**, based on the search results, select the customer name to be registered.
- **Select the Customer Address**, Click the radio button to select the Customer with the address to which the new collector will be registered.

- **Select the Inventory**, from the drop down list of Existing Inventories or select New and enter a name for the new inventory.

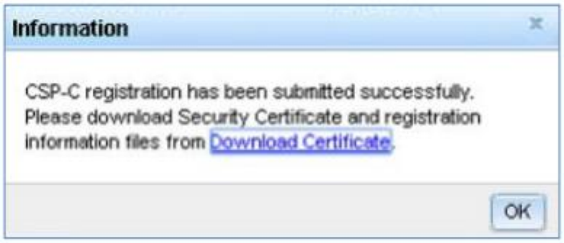
- **Enter a Collector Name** and **Custom Reference Number.** Provide a meaningful name for your collection and reference number.

- **Custom Site ID** is an auto-populated field. You may change it to more clearly describe the location of the collector you are registering. The allowed characters include alphanumeric, #, &, _ and - characters.

Click the **Add** button and wait for the dialogue to popup that will allow you to download the zip file. Save the zip file to a location where you will be able to find it. Do not unzip the file!

Downloading a Certificate

Downloading a certificate provides you entitlement files, a security certificate and other registration related files that are used when installing the Collector entitlement file. To download a certificate, click the Download Certificate link in the registration success message dialog box.



Information

CSP-C registration has been submitted successfully. Please download Security Certificate and registration information files from Download Certificate.

- A zip file window appears requesting you to either save or open the entitlement file, which contains the certificate (license file) and other registration files.

- Save the zip file in your local system.

- An email notification is also sent to the user who registered the collector that includes a link to download the certificate.

6. Log into the Software Appliance

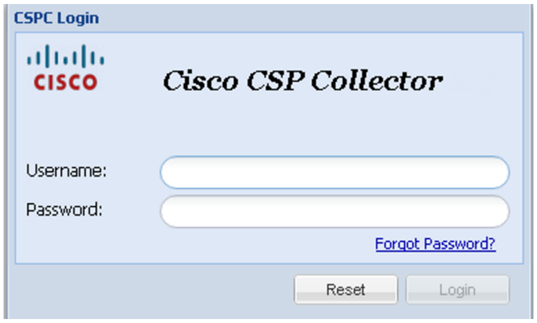
To access the appliance, open a browser window and perform the following steps:

- Use the following URL format to access the

appliance: https://<*your_appliance_ip_address*>:8001/

You will see some type of security certificate warning on your browser that alerts you about the websites security certificate or that the browser cannot confirm a secure connection. The warning will be different depending upon the type browser you have.

- Acknowledge the warning and then continue with the appliance login.

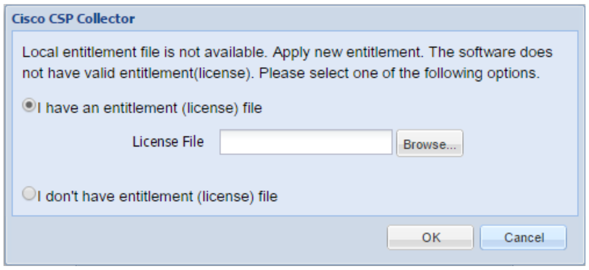


- Enter your login credentials.

The default appliance user id/password is: **Admin123 / Admin123**

Upload New License File to collector:

The very first time you log into the collector you will be prompted to import an entitlement certificate. You will not be able to login to the CSPC GUI until this step is performed. This message will appear:



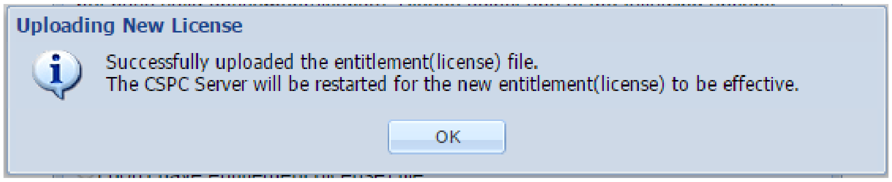
Local entitlement file is not available. Apply new entitlement. The software does not have valid entitlement(license). Please select one of the following options.

● I have an entitlement (license) file

License File

○ I don't have entitlement (license) file

Browse to your .zip entitlement file and then click OK.

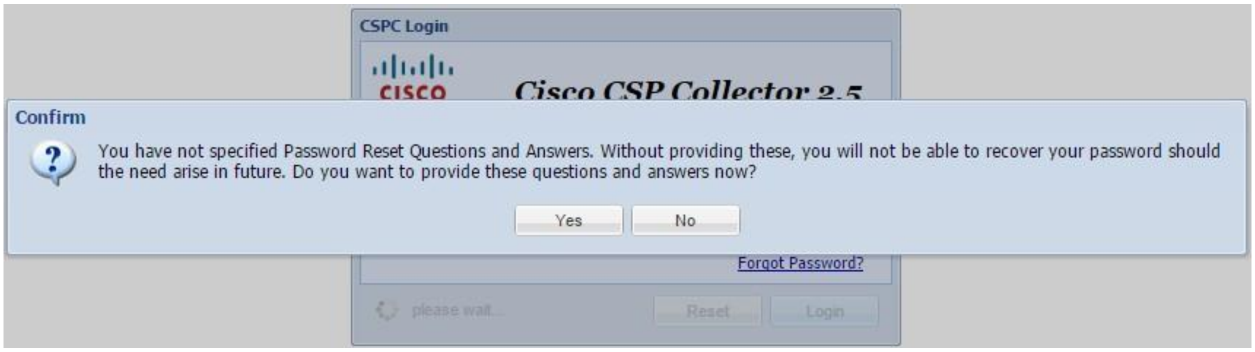


Uploading New License

Successfully uploaded the entitlement(license) file.
The CSPC Server will be restarted for the new entitlement(license) to be effective.

After you upload the entitlement and click OK, the collector will reboot. It will take a couple minutes before you'll be able to log back in.

Log in again using the admin/Admin123 credentials. An End User License Agreement will pop up. Read it and click "I Accept" to proceed. You will then be prompted for Password Reset Questions.

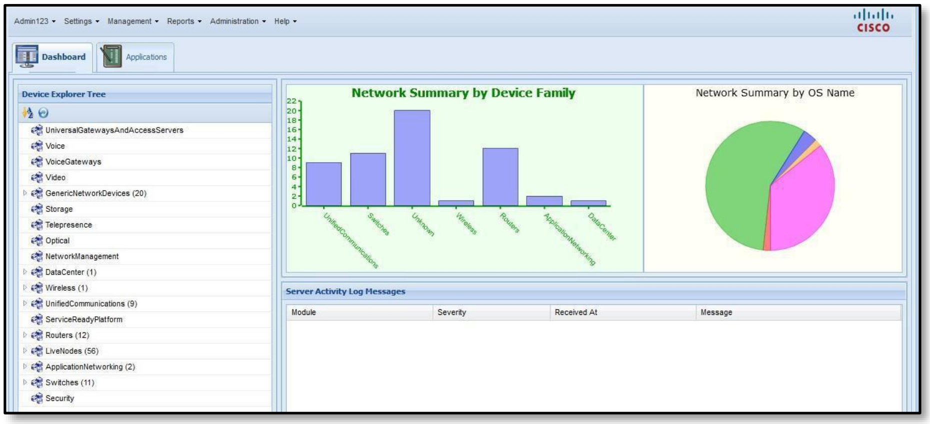


Confirm

You have not specified Password Reset Questions and Answers. Without providing these, you will not be able to recover your password should the need arise in future. Do you want to provide these questions and answers now?

- Click **No** to provide this information at a later time. The appliance now loads its software items for operation.

After all software is loaded, the graphical user interface (GUI) appears.



7. Collector Operation

The collector operation requires that the collector have these related tasks performed:

- Entering CSPC Device Credentials
- Device Discovery, Inventory Collection and Upload

Entering CSPC Device Credentials

This section describes the process for specifying the device credentials.

In order to discover network devices and collect device data, you must first enter the device credentials.

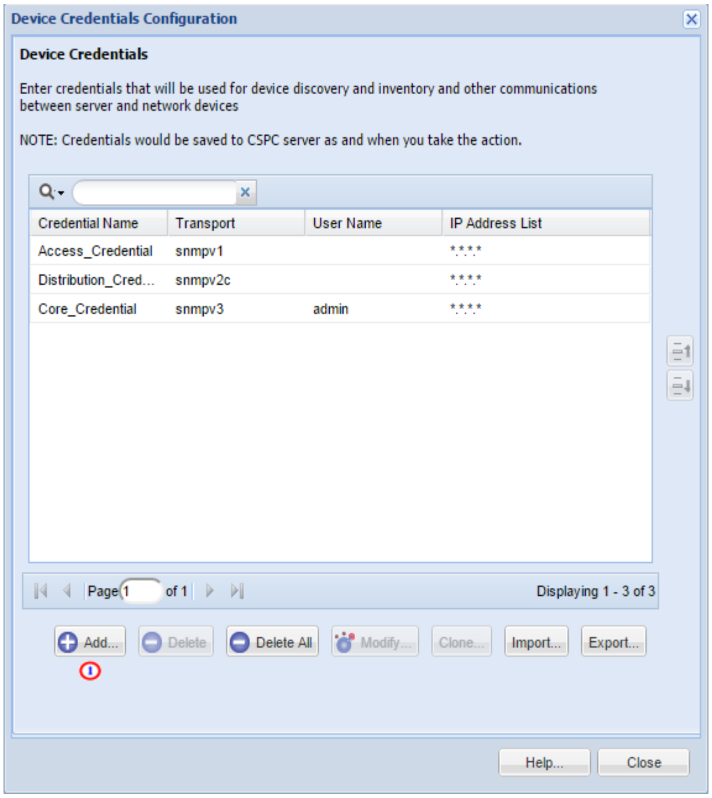
The setup of device credentials in CSPC is used for two purposes:

- SNMP credentials are used for the initial discovery of the devices, and for data collection.
- In addition to SNMP, the remaining credentials (telnet, SSH, HTTP, HTTPS) are used for data collection from the discovered devices.

To set the device credentials using the SNMP protocol, perform the following steps:

- On the CSPC menu, choose **Settings > Device Credentials**

The Device Credential Configuration window appears.



Device Credentials Configuration

Device Credentials

Enter credentials that will be used for device discovery and inventory and other communications between server and network devices

NOTE: Credentials would be saved to CSPC server as and when you take the action.

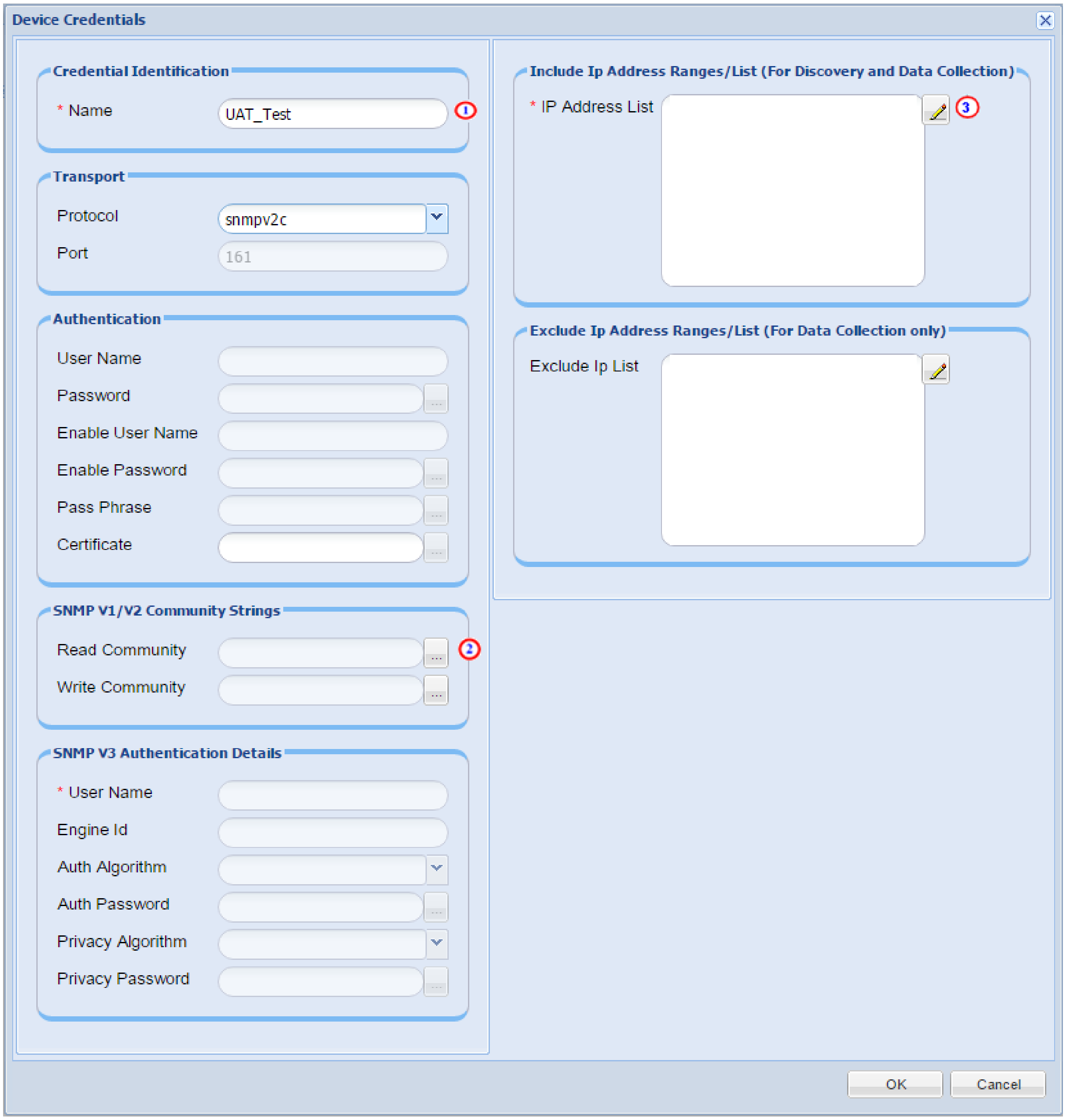
Credential Name	Transport	User Name	IP Address List
Access_Credential	snmpv1		*.*.*.*
Distribution_Cred...	snmpv2c		*.*.*.*
Core_Credential	snmpv3	admin	*.*.*.*

Page 1 of 1

Displaying 1 - 3 of 3

Click ① to create a credential.

The device credentials window appears, which contains credential identification, authentication information, and SNMP Read community string details.



Device Credentials

Credential Identification

* Name: UAT_Test

Transport

Protocol: snmpv2c

Port: 161

Authentication

User Name

Password

Enable User Name

Enable Password

Pass Phrase

Certificate

SNMP V1/V2 Community Strings

Read Community

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

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

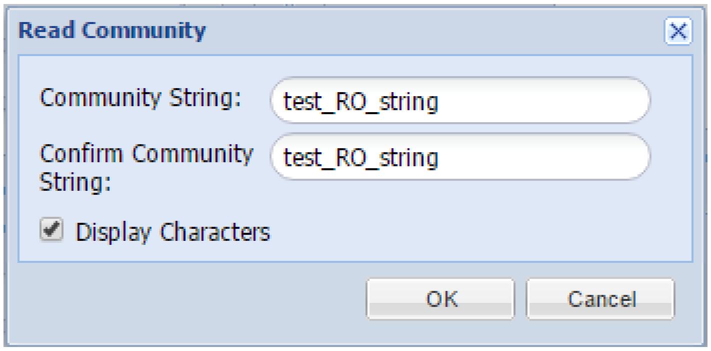
Exclude Ip List

Fill out the required data:

- Enter a credential name (in example, UAT-Test). ①

The credential name can be any name you choose and should be representative of the group or area you are working with.

- In the Transport section click the Protocol field drop-down list and specify the SNMP version of your string.
- For the SNMP V1/V2 Community Strings section, enter the respective Read community string by clicking the … icon. ② The Enter Read Community String window appears.

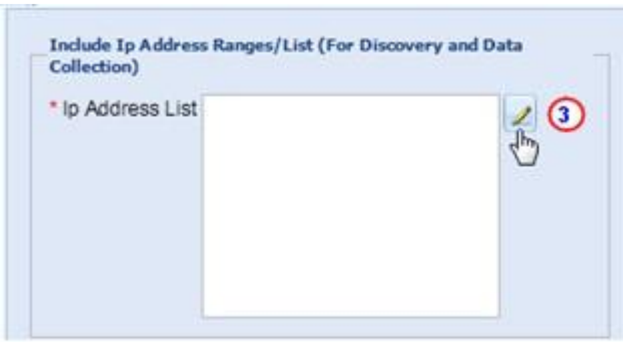

Read Community

Community String: test_RO_string

Confirm Community String: test_RO_string

☑ Display Characters

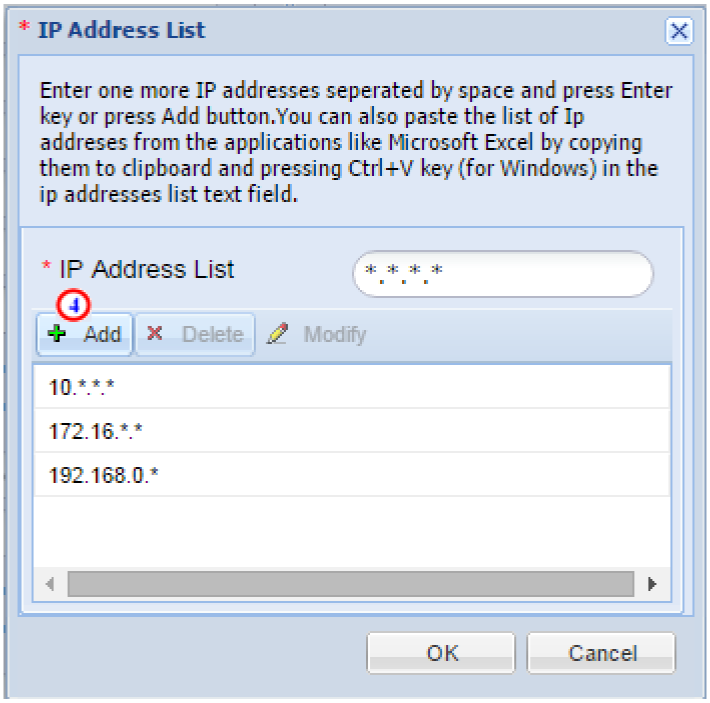
- In the Enter Read Community String window, enter the read community string.
- Then click OK.


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

* Ip Address List

- Enter an IP Address list by clicking the pencil icon ③ to the right of the IP Address List field in the device credentials window.
- Then enter the IP address list.

The IP addresses or IP address ranges are required to define the IP addresses that will be used for the device discovery and data collection, from those identified devices.



* IP Address List

Enter one more IP addresses seperated by space and press Enter key or press Add button.You can also paste the list of Ip addreses from the applications like Microsoft Excel by copying them to clipboard and pressing Ctrl+V key (for Windows) in the ip addresses list text field.

* IP Address List: *.*.*.*

10.*.*.*

172.16.*.*

192.168.0.*

- After entering the IP Address in the IP Address list field, click **Add**

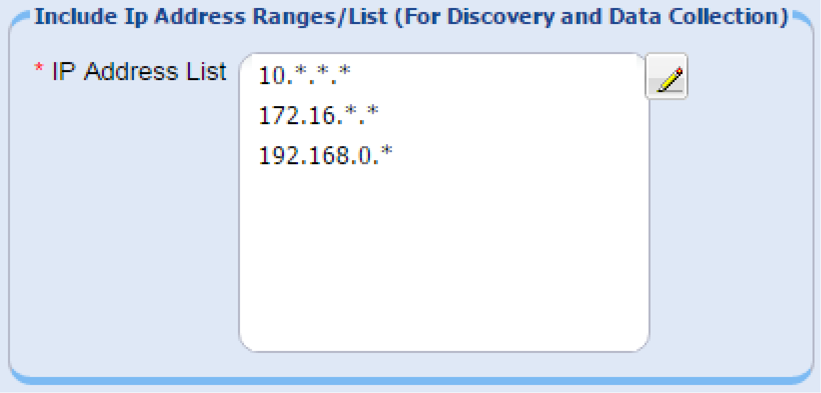
④. The entered data is added to the IP address list.

- ➢ This list specifies which IPs CSPC may use with this credential to communicate with devices for operations such as discoveries or data collection.
- ➢ Specific IPs can be provided or wildcards can be used to replace octets of an IP to create a range.
- ➢ If an IP or range of IPs is not included in this field, CSPC will not use this credential when trying to communicate with a device that has such an IP.
- ➢ Entering *.*.*.* will allow CSPC to use the credential with any IP. 172.16.*.* would only allow the credentials to be used for devices in the 172.16.0.0/16 subnet.

The IP addresses that are referenced should be as tight or as restrictive as possible, while allowing coverage for all required devices.

- After entering the above data, click **OK**.

The new IP(s) appear in the IP Address List field.



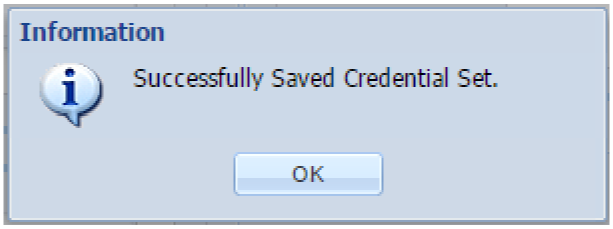
Include Ip Address Ranges/List (For Discovery and Data Collection)

* IP Address List

```
10.*.*.*
172.16.*.*
192.168.0.*
```

- Click **OK**.

The Edit Credentials window appears with a successful saved message.



Information

Successfully Saved Credential Set.

- Click **OK**.

The window closes.

The next steps are used to perform the steps for device discovery, inventory and upload.

To collect show command information, you will need to create an SSH and/or Telnet credential in addition to the SNMP credential you just created. Follow the same logic as above, but set the Protocol to SSH or Telnet and fill out the Authentication section with the appropriate username/password, instead of the SNMP V1/V2 Community Strings section.

Device Discovery, Inventory Collection and Upload

There are several different processes that are required to perform an inventory upload. Those processes are:

- Discover the Devices
- Run Collection Profile and Upload Data

Discover the Devices

This section shows the three ways you can discover your devices as well as how to run the discovery job:

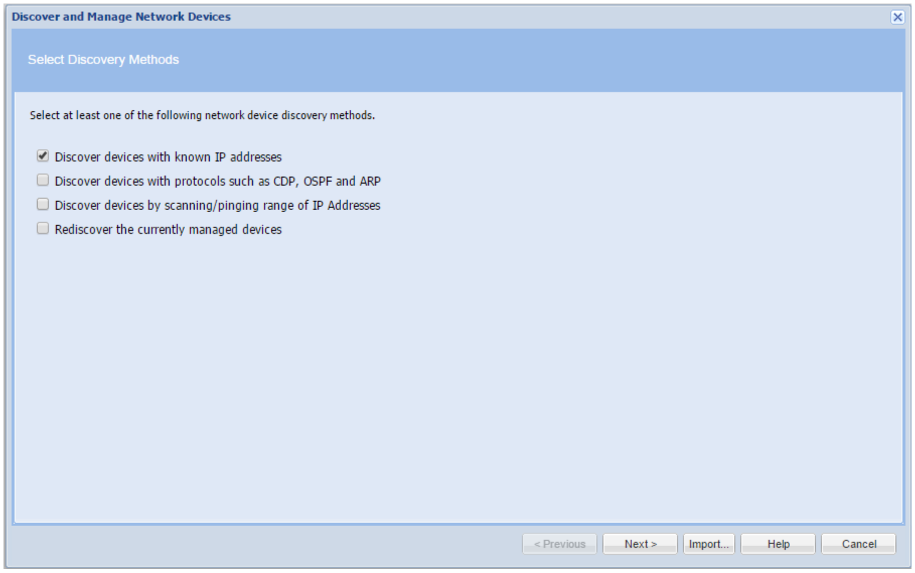
- Discover devices using Known IP Addresses
- Discover devices with protocols such as CDP, OSPF and ARP
- Discover devices by scanning/pinging a range of IP Addresses
- Discovery Schedule Options

To discover your devices for any of the 3 discovery options, choose **Management > Discover and Manage Devices**.

The Discover and Manage Network Devices window appears.

Discover Devices using Known IP Addresses

This discovery process finds the available devices in a managed network, where the IP addresses of the devices are already known. To discover these devices, perform the following steps:



Discover and Manage Network Devices

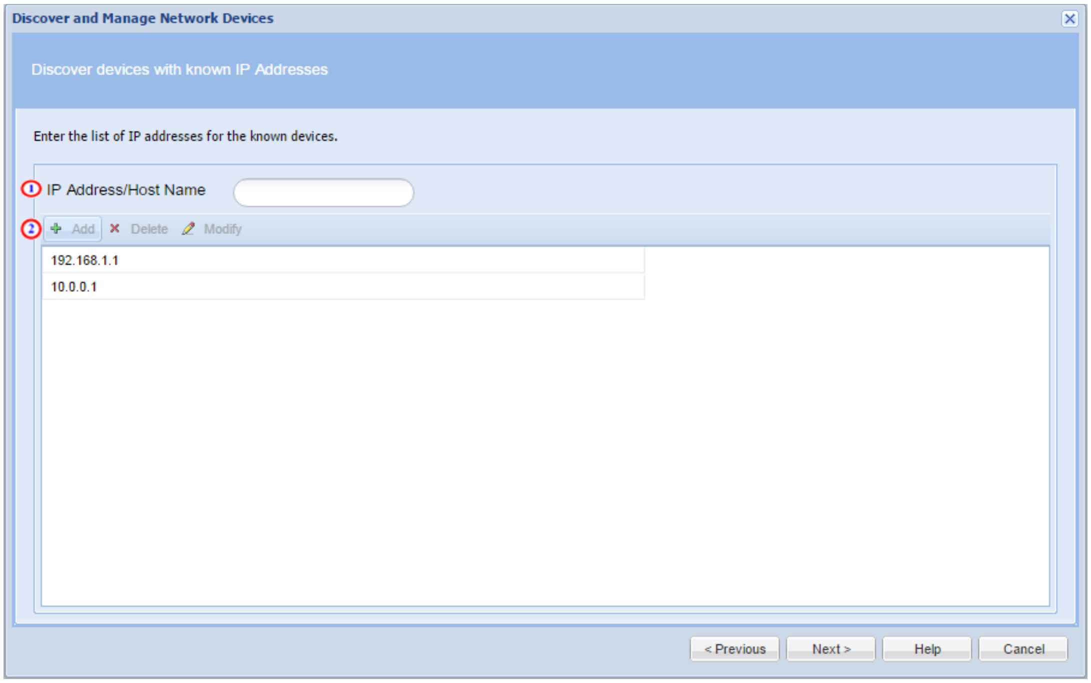
Select Discovery Methods

Select at least one of the following network device discovery methods.

☑ Discover devices with known IP addresses
☐ Discover devices with protocols such as CDP, OSPF and ARP
☐ Discover devices by scanning/pinging range of IP Addresses
☐ Rediscover the currently managed devices

- Select the method you want to use for discovery.
- Then click **Next**.

The pane associated to the method you selected appears.


Discover and Manage Network Devices
Discover devices with known IP Addresses
Enter the list of IP addresses for the known devices.
1 IP Address/Host Name
2 Add Delete Modify
< Previous
Next >
Help
Cancel

192.168.1.1
10.0.0.1

- Enter the IP Addresses for the devices that you want to discover from your network.

Place the IP Address in the IP Address/Host Name field 1 then click **+ Add** 2 or press the enter key.

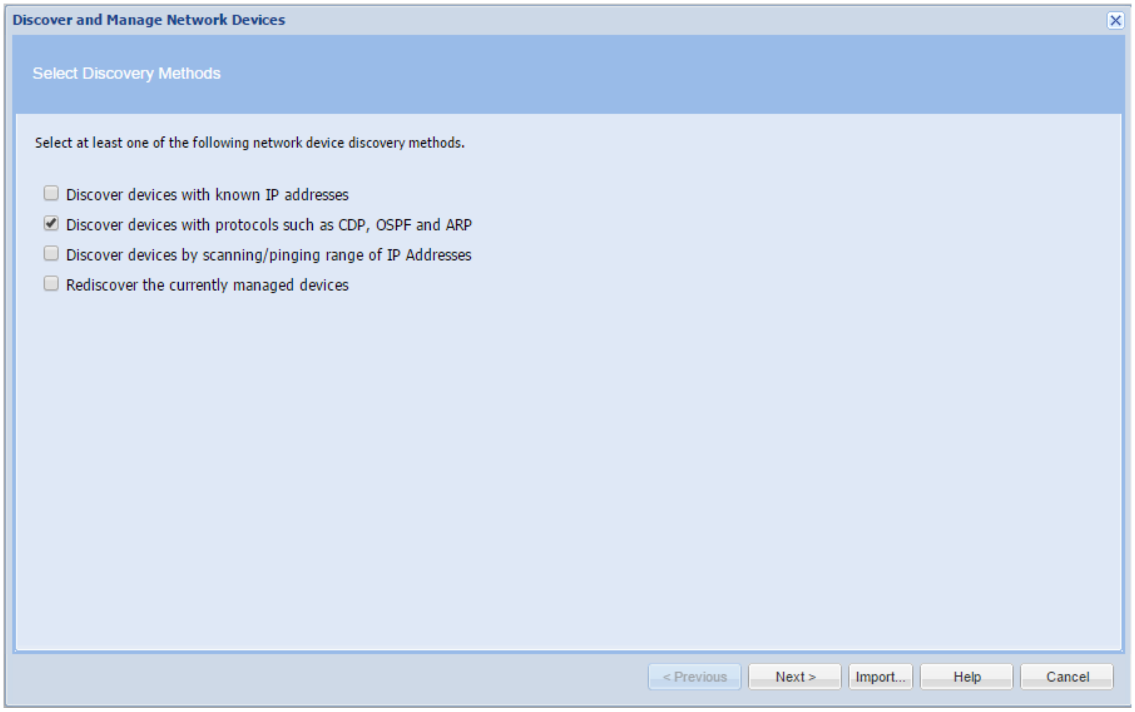
The IP Address is added to the IP Address list.

You can add multiple IPs at once by using a space in between IPs in the IP Address/Host name field 1 .

- Click Next to proceed to the Discovery Schedule Options

Discover devices with protocols such as CDP, OSPF and ARP

This discovers the network devices by using protocol tables such as Cisco Discovery Protocol (CDP), and Address Resolution Protocol (ARP). Data collected from discovered devices is used to find additional devices in the network.



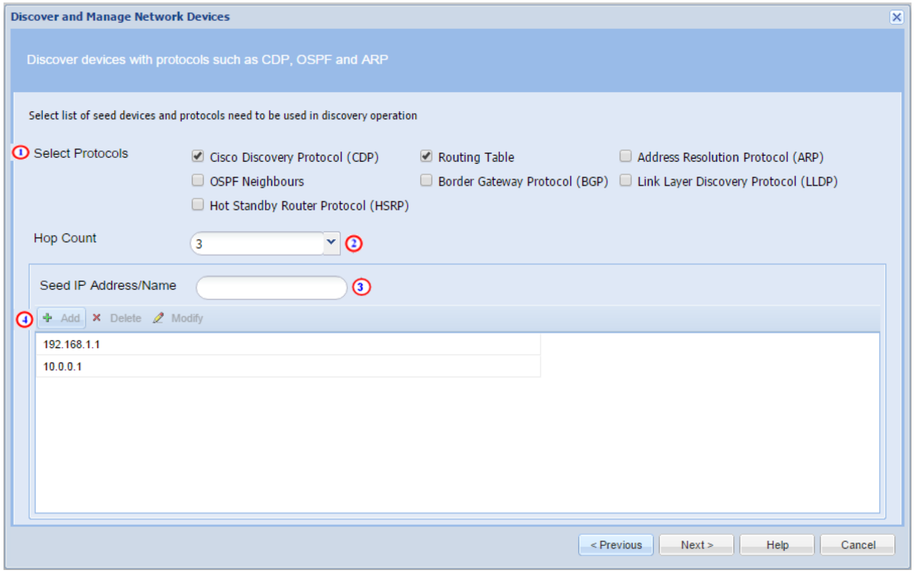
Discover and Manage Network Devices

Select Discovery Methods

Select at least one of the following network device discovery methods.

- □ Discover devices with known IP addresses
- ☑ Discover devices with protocols such as CDP, OSPF and ARP
- □ Discover devices by scanning/pinging range of IP Addresses
- □ Rediscover the currently managed devices

- Select Discover devices with protocols such as CDP, OSPF and ARP.
- Then click **Next**.



Discover and Manage Network Devices

Discover devices with protocols such as CDP, OSPF and ARP

Select list of seed devices and protocols need to be used in discovery operation

1 Select Protocols

- ☑ Cisco Discovery Protocol (CDP)
- □ OSPF Neighbours
- □ Hot Standby Router Protocol (HSRP)
- ☑ Routing Table
- □ Border Gateway Protocol (BGP)
- □ Address Resolution Protocol (ARP)
- □ Link Layer Discovery Protocol (LLDP)

Hop Count: 3 2

Seed IP Address/Name: 3

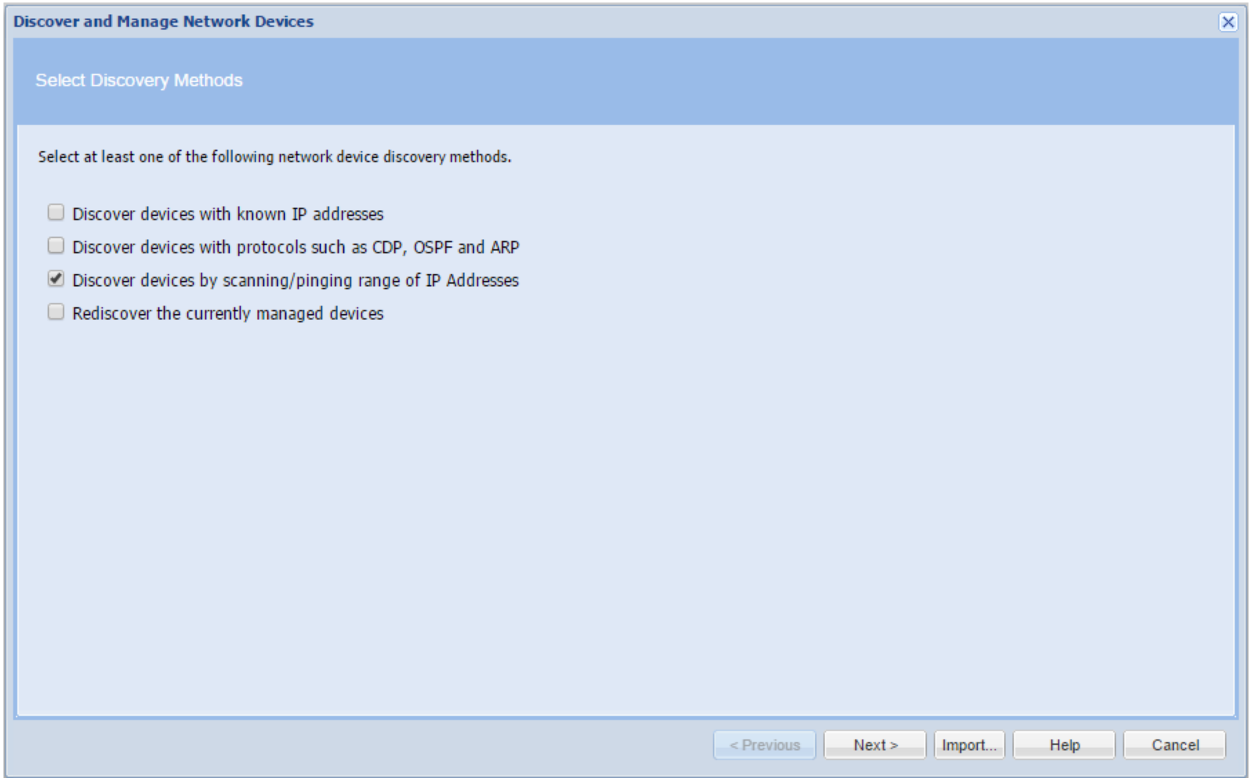
4 Add Delete Modify

192.168.1.1
10.0.0.1

- Select the protocols by clicking the boxes next to the protocol(s) you would like the CSPC to consider. The collector will look at the corresponding tables within a device to find IP addresses for devices within those tables to discover. ①
- Specify the Hop Count value ② that you would like the CSPC to go, beyond the seed device
- Enter your seed device IP Address(es) ③ and then click **+Add** ④ to add them to the seed device list.
- Click Next to proceed to the Discovery Schedule Options

Discover devices by scanning/pinging a range of IP Addresses

This method uses SNMP to contact all the IP addresses in the range you specify.
You provide the starting IP address and the ending IP address of the range or specify a particular subnet using CIDR notation.



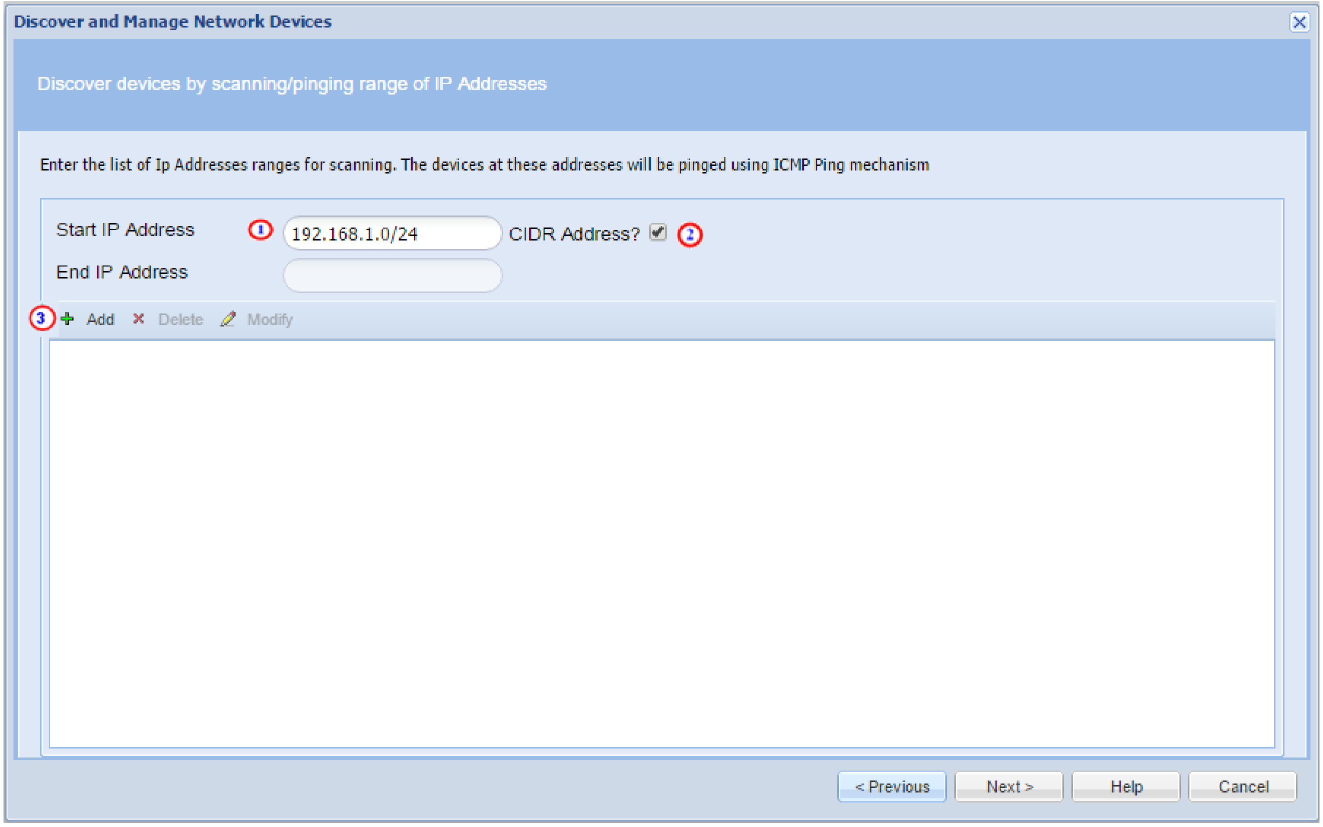
Discover and Manage Network Devices

Select Discovery Methods

Select at least one of the following network device discovery methods.

☐ Discover devices with known IP addresses
☐ Discover devices with protocols such as CDP, OSPF and ARP
☑ Discover devices by scanning/pinging range of IP Addresses
☐ Rediscover the currently managed devices

- Select Discover Devices by scanning/pinging range of IP Addresses.
- Then click **Next**.



Discover and Manage Network Devices

Discover devices by scanning/pinging range of IP Addresses

Enter the list of Ip Addresses ranges for scanning. The devices at these addresses will be pinged using ICMP Ping mechanism

Start IP Address (1) 192.168.1.0/24 CIDR Address? ☑ (2)

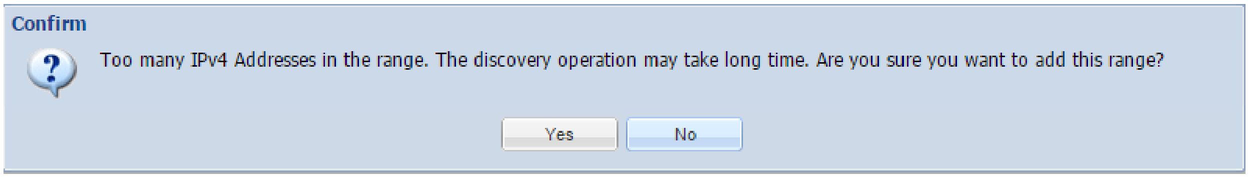
End IP Address

You can enter ranges by specifying the exact starting and ending IP address for a range or by entering in a network address with its corresponding CIDR notation.

For this example the CIDR option is highlighted.

- Enter the network address in the Start IP Address field (1) followed by a slash (/) and the appropriate network bit number. Then click the CIDR Address box (2) and press **+Add** (3)

Any range larger than 255 addresses will yield the following pop-up message. This is informing you that it may take some time for the Discovery Job to complete.



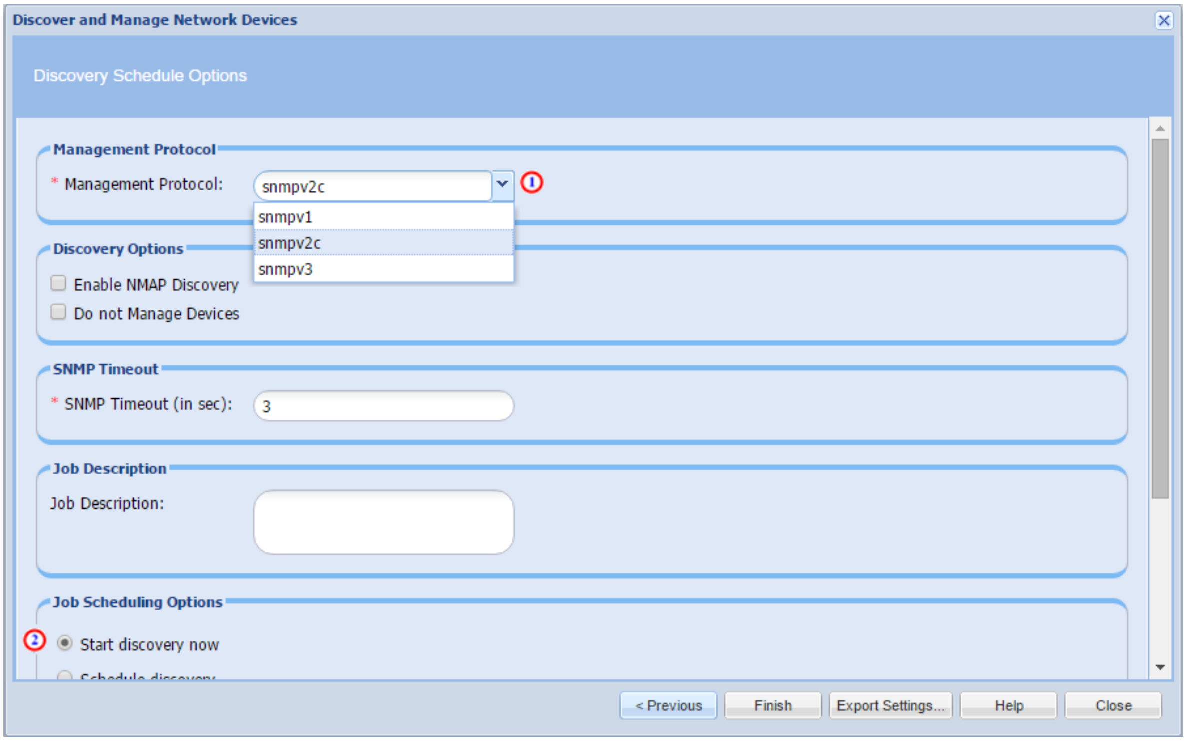
Confirm

Too many IPv4 Addresses in the range. The discovery operation may take long time. Are you sure you want to add this range?

- Click Yes and proceed.

Discovery Schedule Options

After you select one of the three discovery options mentioned above and put in your IP Addresses or ranges of IP Addresses, decide if you want to run that discovery now or schedule it for some time in the future.



Discover and Manage Network Devices

Discovery Schedule Options

Management Protocol

* Management Protocol: snmpv2c ①

Discovery Options

☐ Enable NMAP Discovery

☐ Do not Manage Devices

SNMP Timeout

* SNMP Timeout (in sec): 3

Job Description

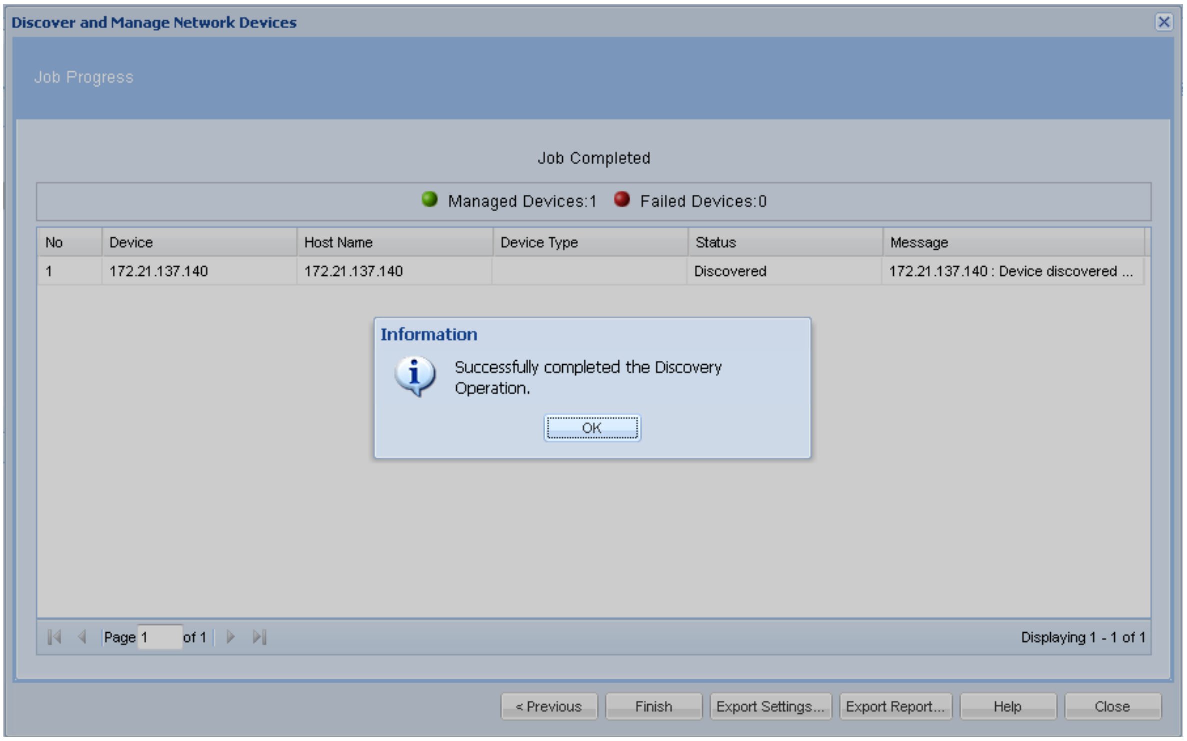
Job Description:

Job Scheduling Options

② ● Start discovery now

○ Schedule discovery

- Under Management Protocol, select the version of SNMP that corresponds with your Device Credentials. ①
- Decide if you want the discovery to run now or schedule for the future. ② For this example, we will consider the option to discover now.
- Click **Finish** and your discovery job will run.



Job Completed

🟢 Managed Devices:1 🔴 Failed Devices:0

No	Device	Host Name	Device Type	Status	Message
1	172.21.137.140	172.21.137.140		Discovered	172.21.137.140 : Device discovered ...

Information

Successfully completed the Discovery Operation.

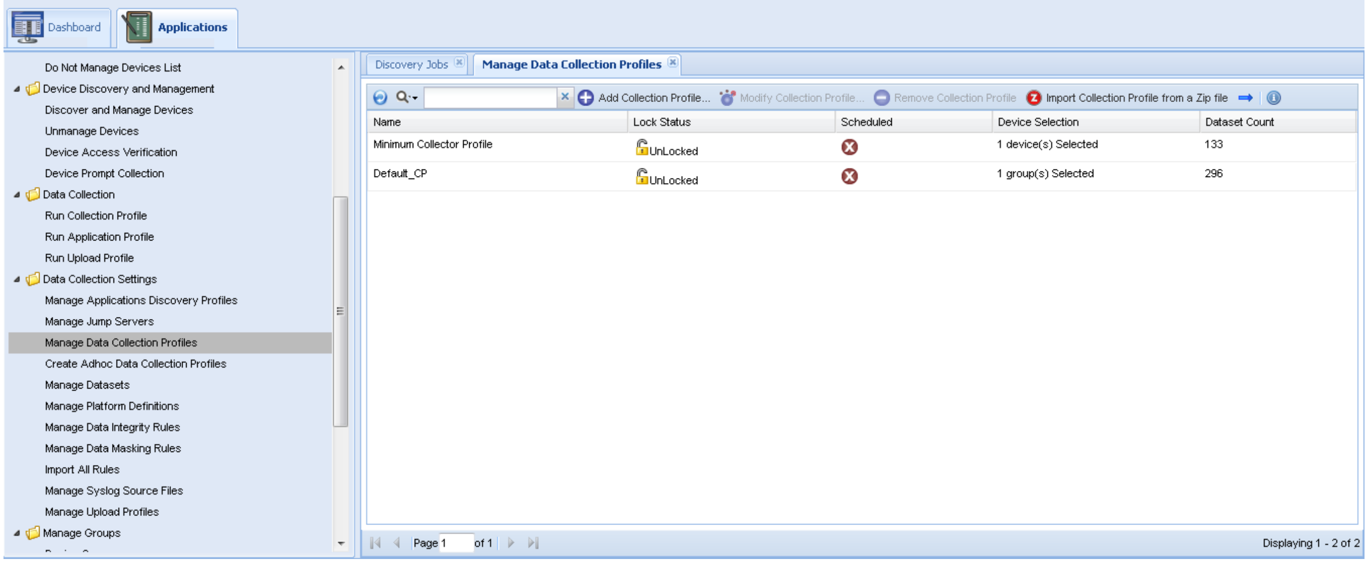
After performing the above steps, the “Successfully completed the Discovery Operation” message is displayed.

- Click **OK**.

Run Collection Profile and Upload Data

The below steps will help you set up the Collection Profile that will enable CSPC to collect relevant device data, as well as initiate an upload to the Cisco Data Center upon completion.

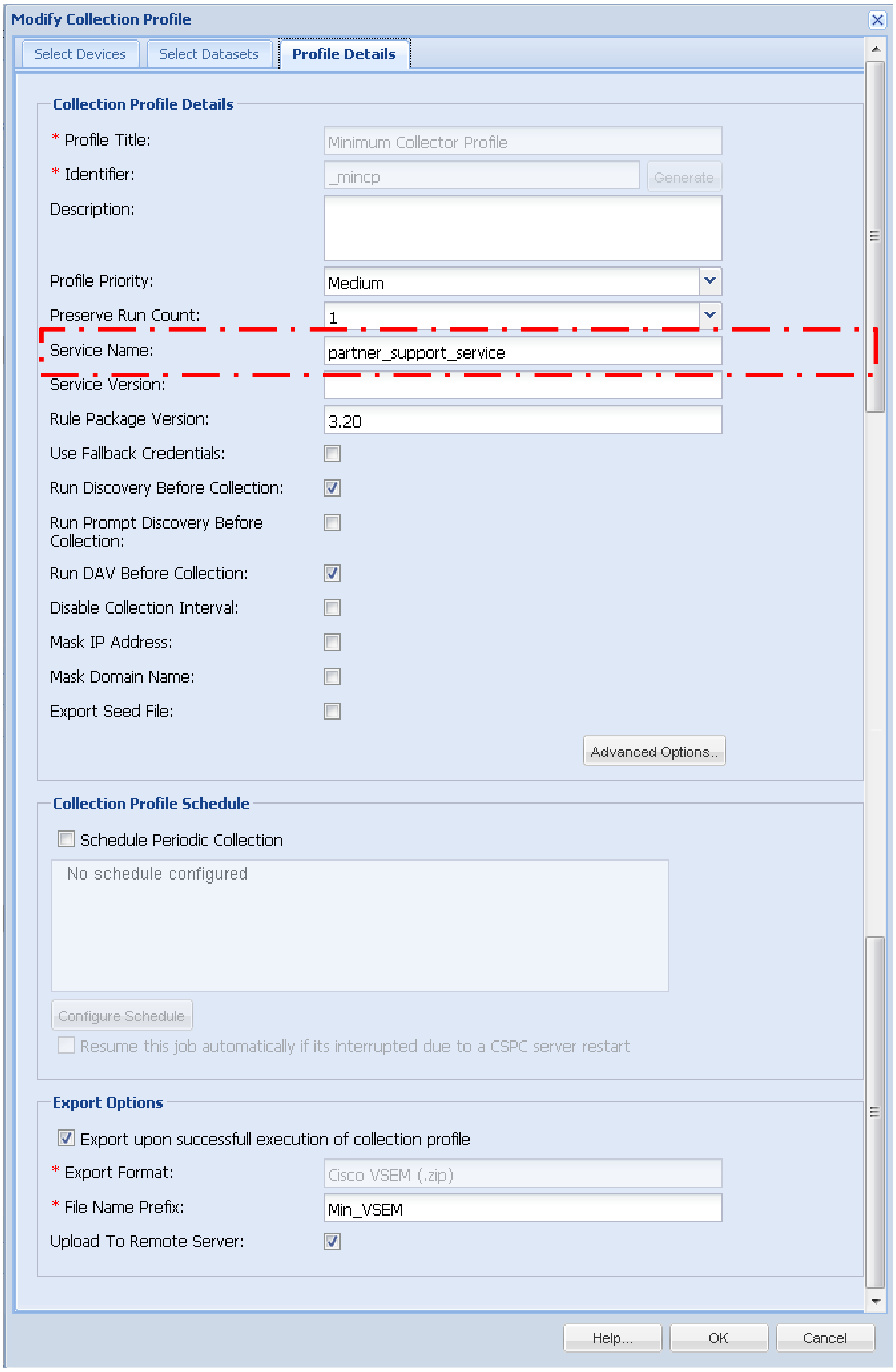
- To manage your Collection Profile, Click the **Applications** tab and choose **Data Collection Settings > Manage Data Collection Profile.** The data Collection Profiles pane appears.


Dashboard
Applications
Do Not Manage Devices List
Device Discovery and Management
Discover and Manage Devices
Unmanage Devices
Device Access Verification
Device Prompt Collection
Data Collection
Run Collection Profile
Run Application Profile
Run Upload Profile
Data Collection Settings
Manage Applications Discovery Profiles
Manage Jump Servers
Manage Data Collection Profiles
Create Adhoc Data Collection Profiles
Manage Datasets
Manage Platform Definitions
Manage Data Integrity Rules
Manage Data Masking Rules
Import All Rules
Manage Syslog Source Files
Manage Upload Profiles
Manage Groups
Discovery Jobs
Manage Data Collection Profiles
Add Collection Profile...
Modify Collection Profile...
Remove Collection Profile
Import Collection Profile from a Zip file
Page 1 of 1
Displaying 1 - 2 of 2

Name	Lock Status	Scheduled	Device Selection	Dataset Count
Minimum Collector Profile	UnLocked	☒	1 device(s) Selected	133
Default_CP	UnLocked	☒	1 group(s) Selected	296

- Double-click the collection profile **Minimum Collection Profile**. The Modify Collection Profile window appears.

The Minimum Collection Profile is bundled with the CSPC appliance. The Minimum Collection Profile contains a minimum set of mandatory collection commands that are required to be processed for each inventory collection/upload.



Modify Collection Profile

Collection Profile Details

* Profile Title:	Minimum Collector Profile
* Identifier:	_mincp
Description:	
Profile Priority:	Medium
Preserve Run Count:	1
Service Name:	partner_support_service
Service Version:	
Rule Package Version:	3.20
Use Fallback Credentials:	□
Run Discovery Before Collection:	☑
Run Prompt Discovery Before Collection:	□
Run DAV Before Collection:	☑
Disable Collection Interval:	□
Mask IP Address:	□
Mask Domain Name:	□
Export Seed File:	□

Collection Profile Schedule

□ Schedule Periodic Collection

No schedule configured

□ Resume this job automatically if its interrupted due to a CSPC server restart

Export Options

☑ Export upon successfull execution of collection profile

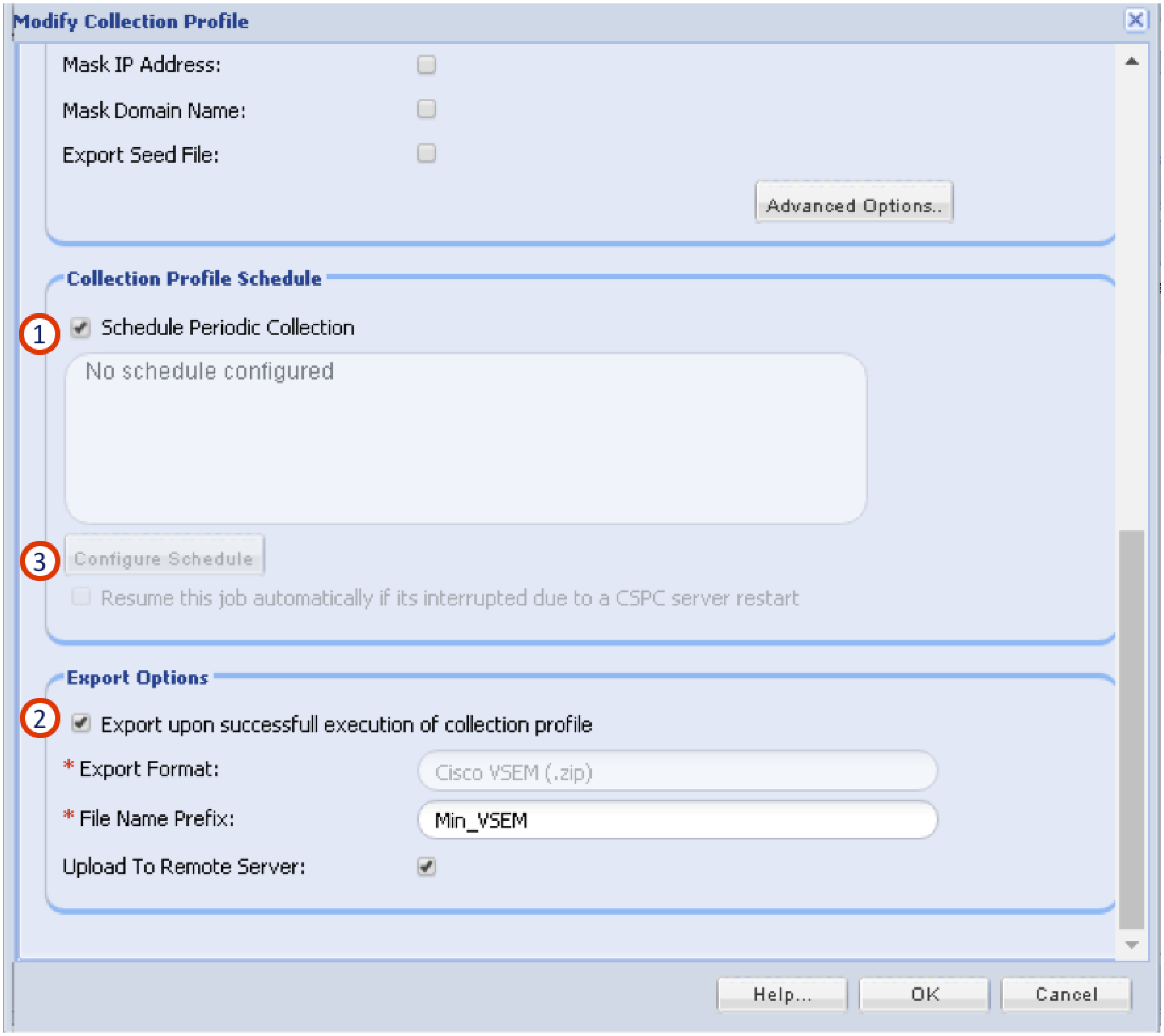
* Export Format:	Cisco VSEM (.zip)
* File Name Prefix:	Min_VSEM
Upload To Remote Server:	☑

The Modify Collection Profile panel lets you perform the same profile functions as noted in Profile Details tab of the Add Collection Profile section:

- Provide collection profile details.
- Set profile running parameters.
- Set a collection schedule for the Collection to run periodically.
- Set export options.

Do NOT change the service name (in example, partner_support_service) that is in the service name field. The field is allowed to be modified; however, if you change the name to something else, when inventory data gets sent to the Cisco Data Center, the data repository will not recognize the different service name and the data will not get routed correctly.

- Click the Profile Details tab ① and then check the boxes for, 'Run Discovery Before Collection,' and 'Run DAV Before Collection' ②



Mask IP Address: □

Mask Domain Name: □

Export Seed File: □

☑ Schedule Periodic Collection

No schedule configured

□ Resume this job automatically if its interrupted due to a CSPC server restart

☑ Export upon successfull execution of collection profile

* Export Format: Cisco VSEM (.zip)

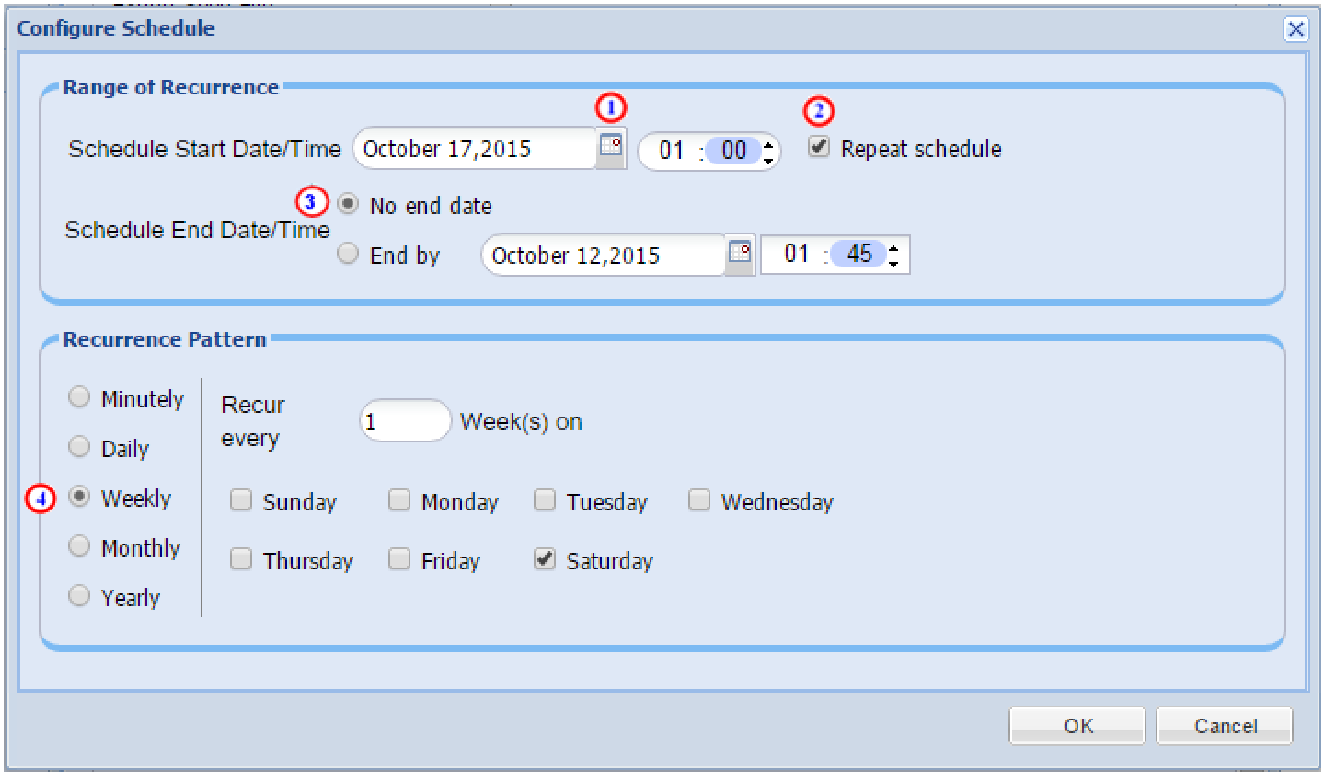
* File Name Prefix: Min_VSEM

Upload To Remote Server: ☑

- Scroll down to the bottom of the window and check the boxes for Schedule Periodic Collection (1) and 'Export upon successful execution of collection profile' (2)

The 'Export upon successful execution of collection profile' checkbox enables uploads. With this checkbox checked, after the collection completes, CSPC will upload the collected data from the Collection Profile to Cisco.

- Click Configure Schedule (3) to proceed to the Configure Schedule Screen



Configure Schedule

Range of Recurrence

① ②

Schedule Start Date/Time: October 17,2015 — 01 : 00 — ☑ Repeat schedule

③

Schedule End Date/Time: ● No end date

○ End by: October 12,2015 — 01 : 45

Recurrence Pattern

○ Minutely
○ Daily
④ ● Weekly
○ Monthly
○ Yearly

Recur every 1 Week(s) on

□ Sunday □ Monday □ Tuesday □ Wednesday
□ Thursday □ Friday ☑ Saturday

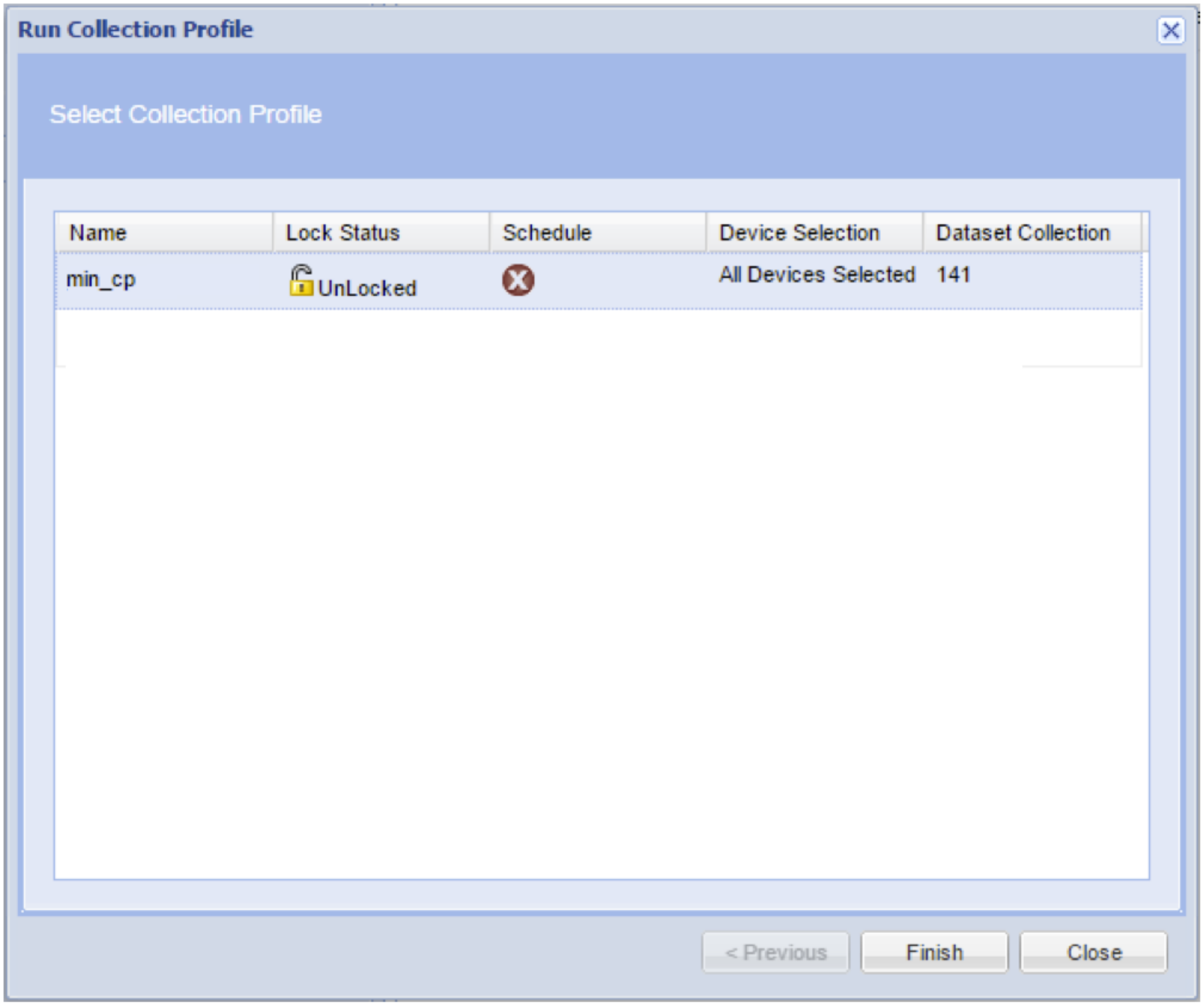
- Begin by selecting the date of the first collection by clicking the Calendar icon.①
- A calendar will pop up; select a date.

After you select your date you will be brought back to the Configure Schedule window.

- Enter the time of day you would like the collection to take place.
- Check the box for Repeat schedule.②
- Then select the No end date radio button.③
- Now choose the Recurrence Pattern. ④
- Click **OK** to save your changes and return to the Modify Collection Profile window.
- Click **OK** to close out the Modify Collection Profile window.

Your collection will occur at the date and time you specified.

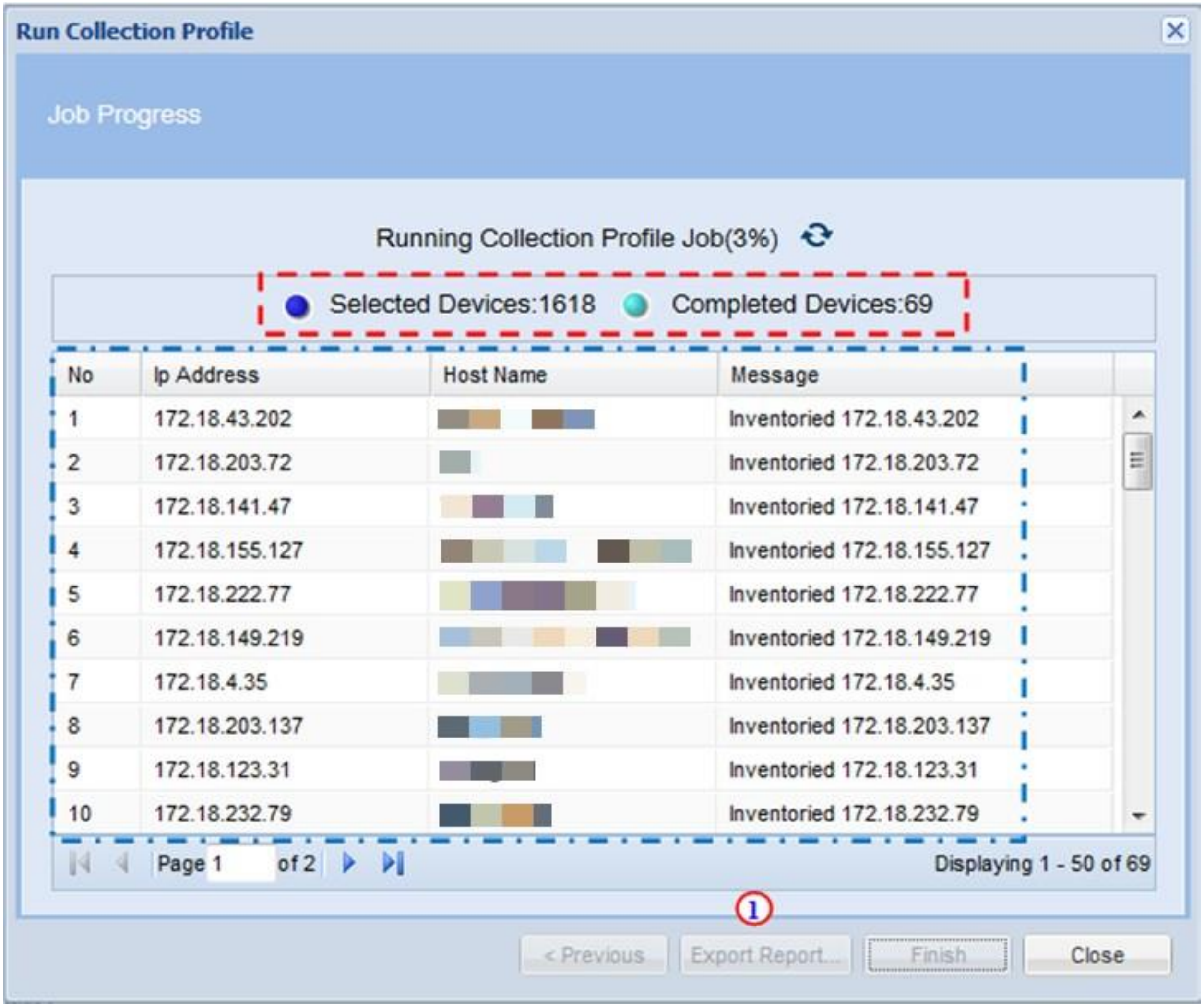
If you want to run an On Demand collection, go to **Management > Run Collection Profile**, select **min_cp** and then click **Finish**. Please refer to the screen shots below.



Run Collection Profile

Select Collection Profile

Name	Lock Status	Schedule	Device Selection	Dataset Collection
min_cp	UnLocked	☒	All Devices Selected	141



Running Collection Profile Job(3%)

● Selected Devices:1618 ● Completed Devices:69

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

Displaying 1 - 50 of 69

The details of the data collection are filled in. A summary is above and the details are below.

- After the collection process finishes, the above report can be exported by clicking the **Export Report...** button. ①
- Click **Close** when you are finished or to let the Collection run in the background.

When the collection job completes, the upload will be sent to the Cisco Data Center. It may take up to 24 hours before your upload will be processed by the portal.

You can view the upload status by going to: https://tools.cisco.com/smartservices and clicking **Library** > **Inventory** > **Inventory Collection**

Appendix A: Manual Import

A partner can also import inventory manually to the portal in one of the following conditions:

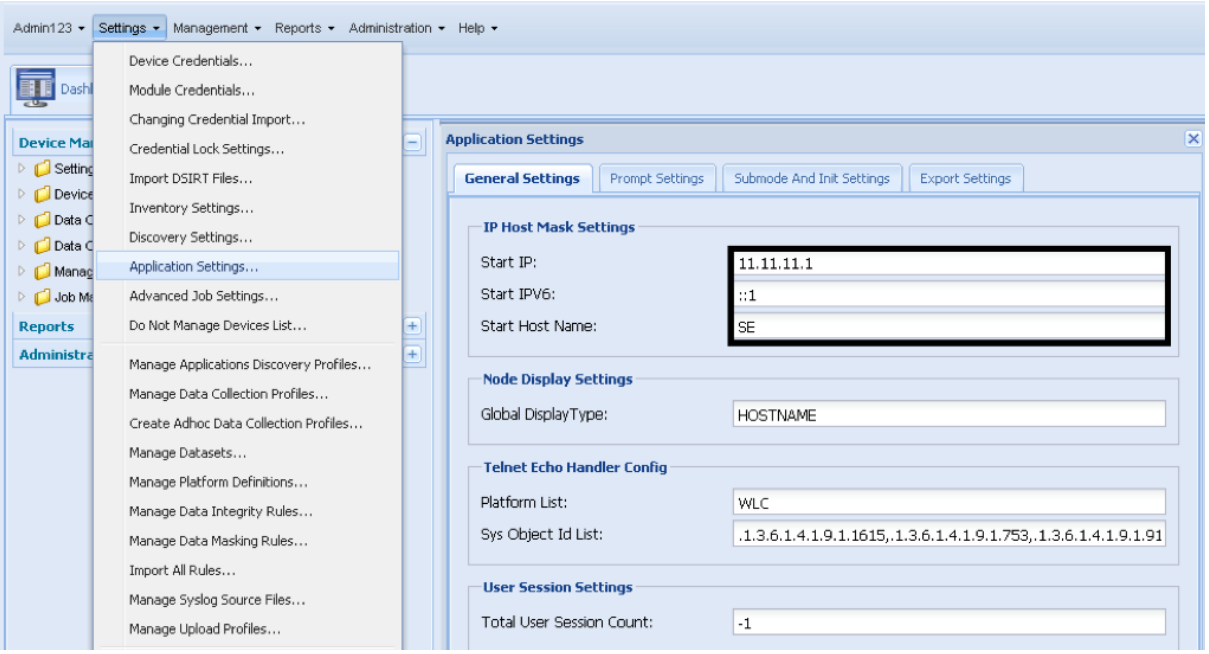
- A customer does not need a collector in the deployment environment.
- A customer does not want the partner to collect information of all the devices from their network.

For more information on importing the inventory manually into the portal, refer to your portal user guide.

Note: The mutual relationship is not established between the device information that is uploaded using the CSV file. For instance, if you upload the information for a router chassis and the cards installed within that chassis, then the application might not be able to discern that those cards are installed in the chassis. Also, knowledge about the chassis support contract that actually covers the installed cards is not known. (For example, a card that is covered under a chassis contract will be reported as uncovered in the reports).

Appendix B: DPA Masking

The CSPC does support IP Address and Hostname masking.


Admin123 ▾
Settings ▾
Management ▾
Reports ▾
Administration ▾
Help ▾
Device Credentials...
Module Credentials...
Changing Credential Import...
Credential Lock Settings...
Import DSIRT Files...
Inventory Settings...
Discovery Settings...
Application Settings...
Advanced Job Settings...
Do Not Manage Devices List...
Manage Applications Discovery Profiles...
Manage Data Collection Profiles...
Create Adhoc Data Collection Profiles...
Manage Datasets...
Manage Platform Definitions...
Manage Data Integrity Rules...
Manage Data Masking Rules...
Import All Rules...
Manage Syslog Source Files...
Manage Upload Profiles...
Dashl
Device Ma
Setting
Device
Data C
Data C
Manag
Job Ma
Reports
Administra
General Settings
Prompt Settings
Submode And Init Settings
Export Settings

Application Settings

IP Host Mask Settings

Start IP: 11.11.11.1

Start IPV6: ::1

Start Host Name: SE

Node Display Settings

Global DisplayType: HOSTNAME

Telnet Echo Handler Config

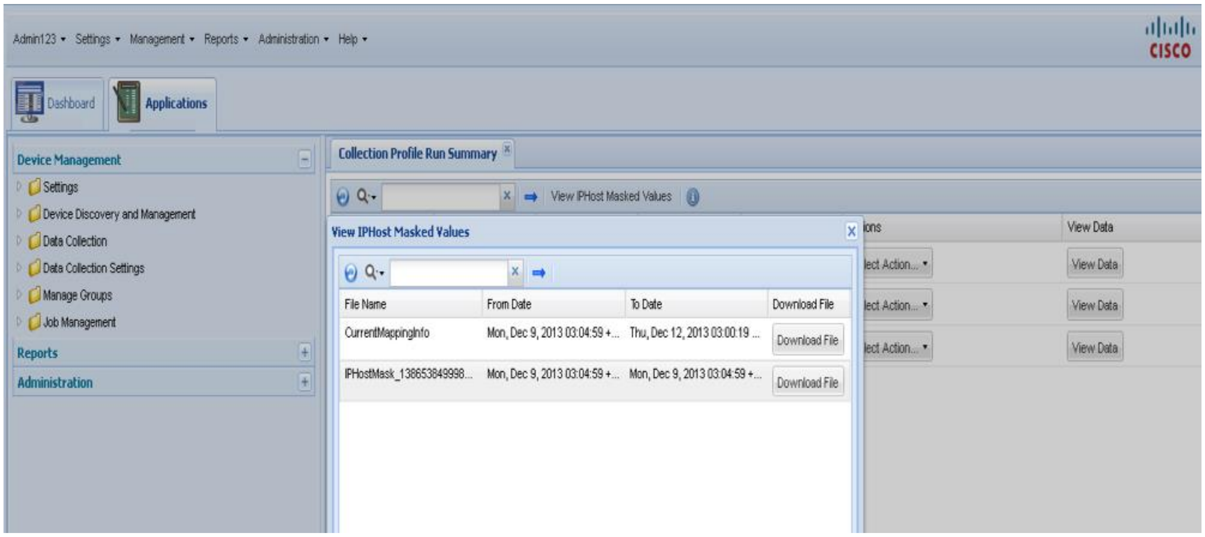
Platform List: WLC

Sys Object Id List: .1.3.6.1.4.1.9.1.1615,.1.3.6.1.4.1.9.1.753,.1.3.6.1.4.1.9.1.91

User Session Settings

Total User Session Count: -1

- Click **View IPHost Masked Values** to download/save it in your local machine "CurrentMappingInfo" file with the extension of ".txt" file



View IPHost Masked Values

File Name	From Date	To Date	Download File
CurrentMappingInfo	Mon, Dec 9, 2013 03:04:59 +...	Thu, Dec 12, 2013 03:00:19 ...	Download File
IPHostMask_138653849998...	Mon, Dec 9, 2013 03:04:59 +...	Mon, Dec 9, 2013 03:04:59 +...	Download File

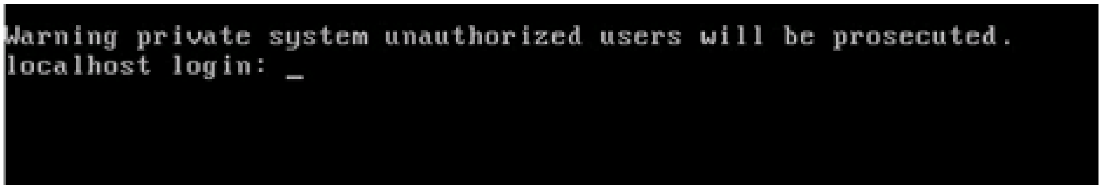
Appendix C: LifeCycle Management (LCM)

Collection Platform Software upgrades are released on a regular Cadence. These upgrades provide several new features or support for new devices or improve performance or improve the security of the already deployed collectors at the Customer/Partner locations.

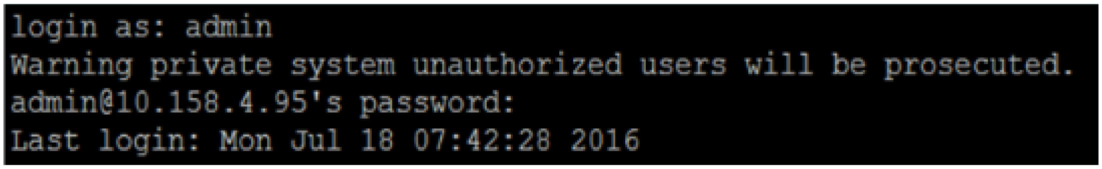
We highly recommend partners upgrade their Collection software to the latest version by following the below **6 simple steps**.

Note: The user shall be able to upgrade their collectors from CSPC version 2.3.x and above to the latest version **using a single patch** .

1. Login: Login to adminshell using admin credentials



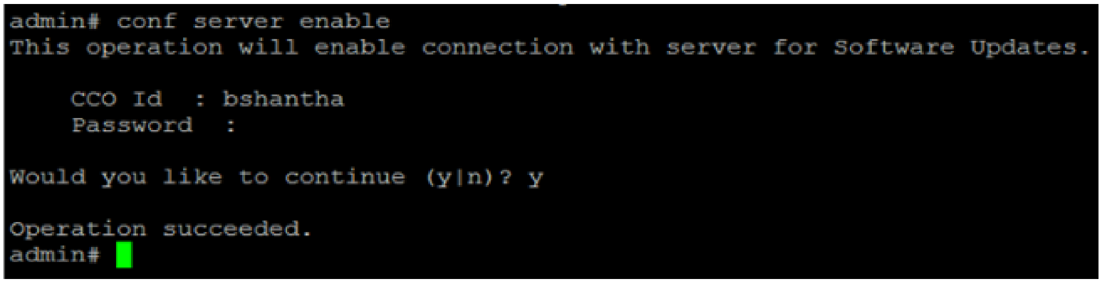
```
Warning private system unauthorized users will be prosecuted.
localhost login: _
```



```
login as: admin
Warning private system unauthorized users will be prosecuted.
admin@10.158.4.95's password:
Last login: Mon Jul 18 07:42:28 2016
```

2. Establish connection: After login at the prompt, enter the **"conf server enable"** command to enable connection with the Cisco's upgrade server. At the prompt provide your registered CCO credentials. This shall-

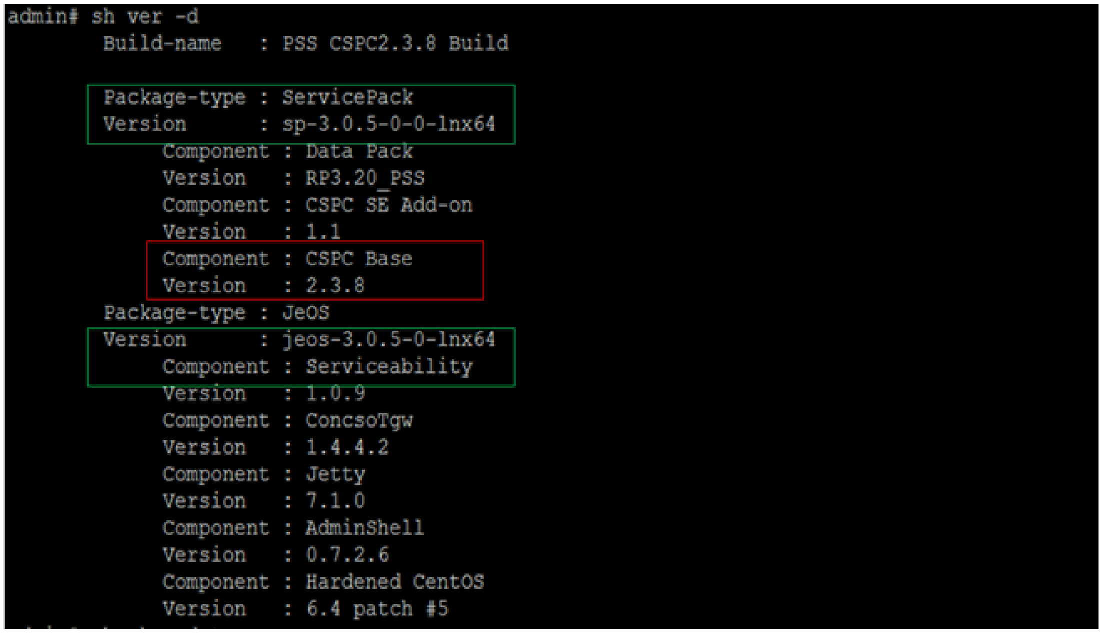
- validate that you have a valid contract and are eligible to receive upgrades to your Collector
- enable connection with the Cisco's Collection Platform Software upgrade server



```
admin# conf server enable
This operation will enable connection with server for Software Updates.

    CCO Id   : bshantha
    Password  :

Would you like to continue (y|n)? y

Operation succeeded.
admin# █
```

You may notice the message "Operation succeeded" on successful login

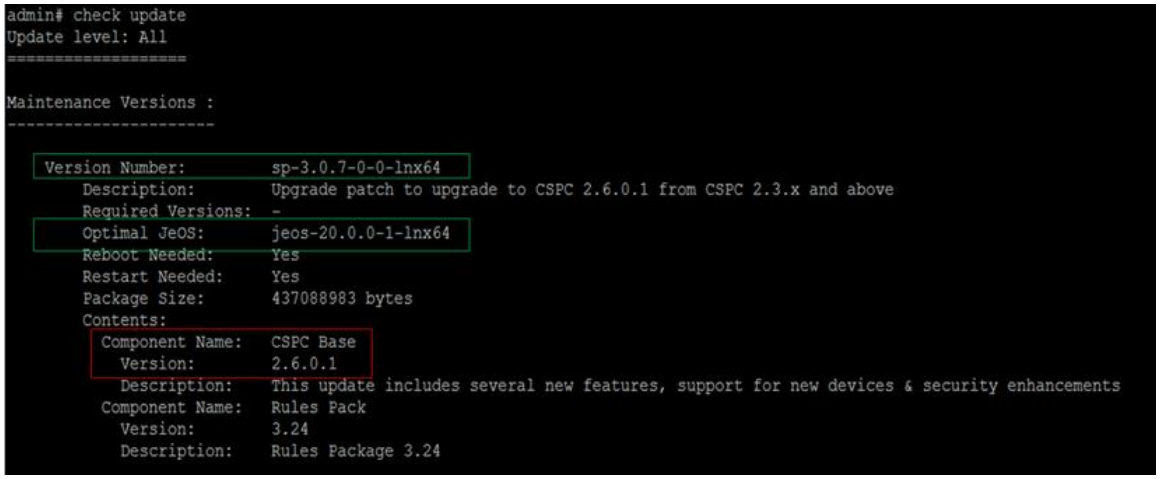
3. Current Version details: View details of your current Collector Platform Software version by using the **"sh version"** command



```
admin# sh ver -d
        Build-name    : PSS CSPC2.3.8 Build

        Package-type : ServicePack
        Version      : sp-3.0.5-0-0-lnx64
             Component : Data Pack
             Version   : RP3.20_PSS
             Component : CSPC SE Add-on
             Version   : 1.1
             Component : CSPC Base
             Version   : 2.3.8
        Package-type : JeOS
        Version      : jeos-3.0.5-0-lnx64
             Component : Serviceability
             Version   : 1.0.9
             Component : ConcsoTgw
             Version   : 1.4.4.2
             Component : Jetty
             Version   : 7.1.0
             Component : AdminShell
             Version   : 0.7.2.6
             Component : Hardened CentOS
             Version   : 6.4 patch #5
```

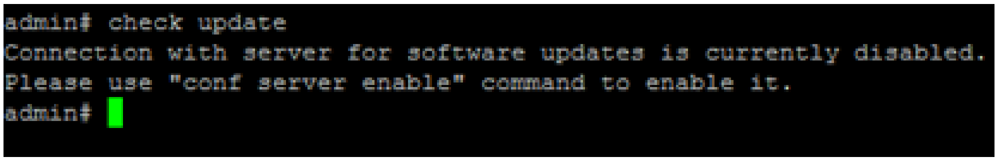
In this example you notice the details of all the components of your Collection Platform Software. CSPC version is shown as CSPC 2.3.8; You also notice the Service Pack(SP) & JeOS versions as well.

4. Check for Updates: Check whether your collector has any new updates by running **"check update"** command at the prompt.



```
admin# check update
Update level: All
===================

Maintenance Versions :
----------------------

   Version Number:          sp-3.0.7-0-0-lnx64
       Description:         Upgrade patch to upgrade to CSPC 2.6.0.1 from CSPC 2.3.x and above
       Required Versions:   -
       Optimal JeOS:        jeos-20.0.0-1-lnx64
       Reboot Needed:       Yes
       Restart Needed:      Yes
       Package Size:        437088983 bytes
       Contents:
         Component Name:    CSPC Base
           Version:         2.6.0.1
           Description:     This update includes several new features, support for new devices & security enhancements
         Component Name:    Rules Pack
           Version:         3.24
           Description:     Rules Package 3.24
```

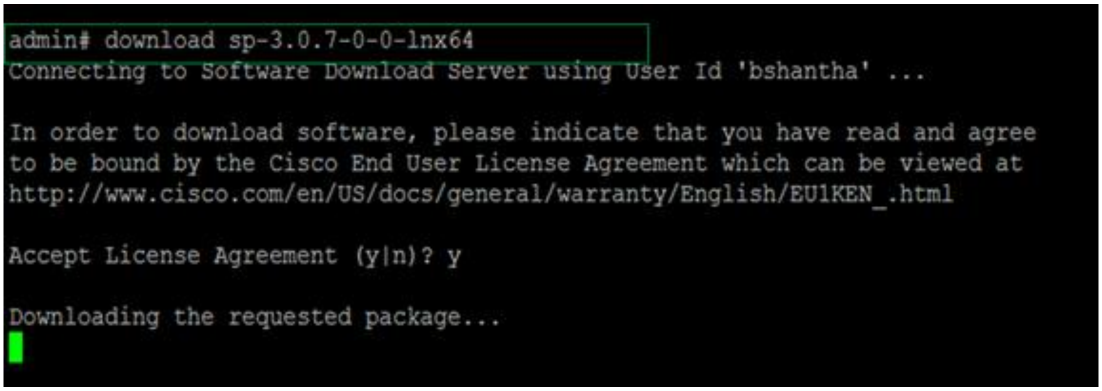
In case your connection to the Server is not enabled you shall see a message as shown below –



```
admin# check update
Connection with server for software updates is currently disabled.
Please use "conf server enable" command to enable it.
admin#
```

5. Download Patch:

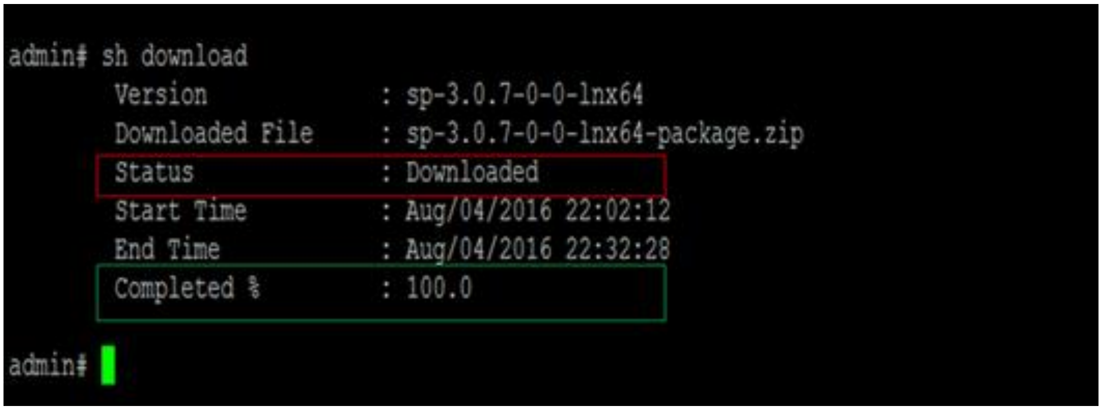
Download the patch by running "**download sp<ver>**" command as shown below.



```
admin# download sp-3.0.7-0-0-lnx64
Connecting to Software Download Server using User Id 'bshantha' ...

In order to download software, please indicate that you have read and agree
to be bound by the Cisco End User License Agreement which can be viewed at
http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html

Accept License Agreement (y|n)? y

Downloading the requested package...
```

View the license agreement and download shall start only **after you accept the license agreement by saying "y".**

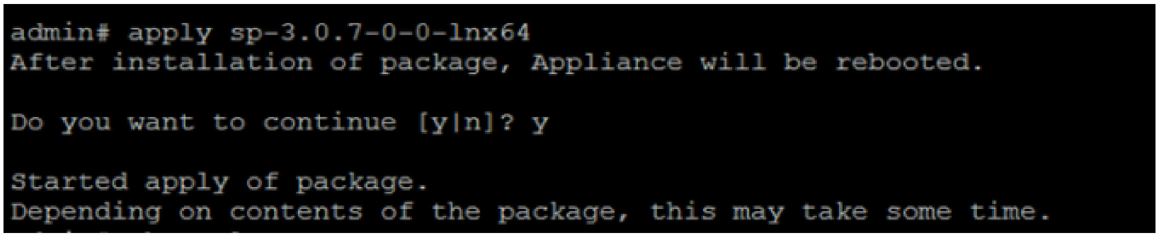
You may review the status of download by running the "sh download" command as shown below.



```
admin# sh download
        Version               : sp-3.0.7-0-0-lnx64
        Downloaded File       : sp-3.0.7-0-0-lnx64-package.zip
        Status                : Downloaded
        Start Time            : Aug/04/2016 22:02:12
        End Time              : Aug/04/2016 22:32:28
        Completed %           : 100.0

admin#
```

You notice the status as "Downloaded" and 100% completed on completion. The download might take several minutes, depending on several factors such as size of the patch, network speed/latency etc. In our example the download took around 30 minutes

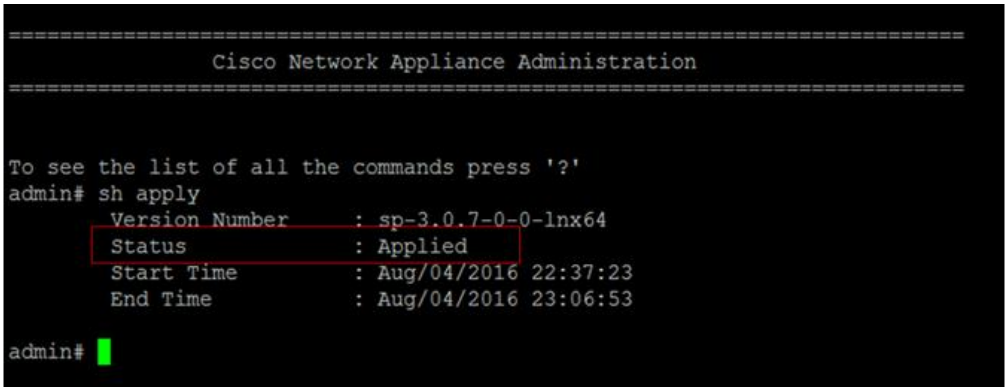
6. Apply Patch: After completing the download, apply the patch on to your collector by running the **"apply sp<ver>"** command



```
admin# apply sp-3.0.7-0-0-lnx64
After installation of package, Appliance will be rebooted.

Do you want to continue [y|n]? y

Started apply of package.
Depending on contents of the package, this may take some time.
```

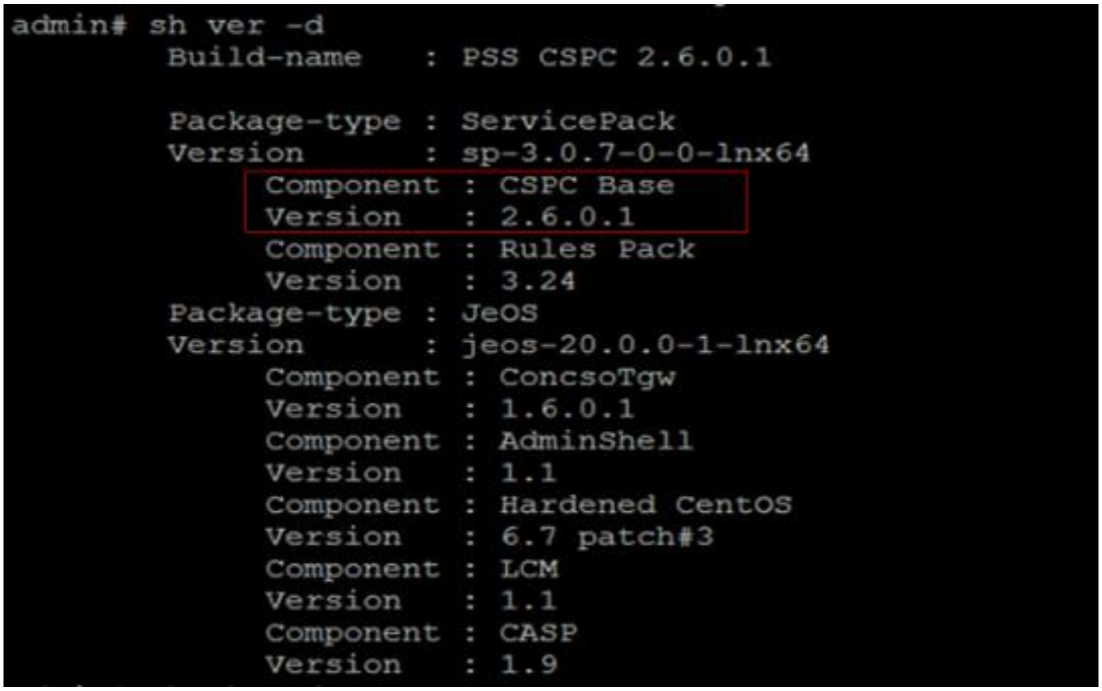
If the patch requires the collector appliance to be rebooted, you shall be a shown a message for the same. The patch shall be applied only after the user confirms to continue.

You may review the status of patch application by running the "**sh apply**" command



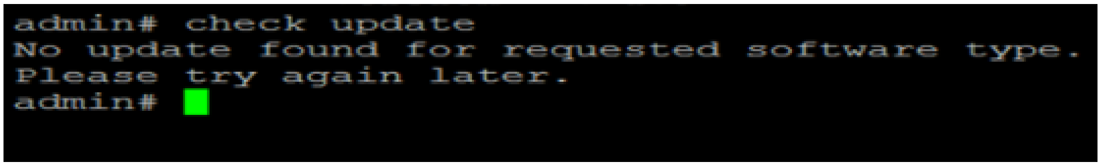
```
===========================================================================
                Cisco Network Appliance Administration
===========================================================================


To see the list of all the commands press '?'
admin# sh apply
        Version Number     : sp-3.0.7-0-0-lnx64
        Status             : Applied
        Start Time         : Aug/04/2016 22:37:23
        End Time           : Aug/04/2016 23:06:53

admin#
```

Review/Verify: After applying the patch (and on appliance reboot if required), you may again run "sh version" command to view the latest Collector Platform Software version by using the **"sh version"** command and verify your appliance is up to date.



```
admin# sh ver -d
        Build-name   : PSS CSPC 2.6.0.1

        Package-type : ServicePack
        Version      : sp-3.0.7-0-0-lnx64
             Component : CSPC Base
             Version   : 2.6.0.1
             Component : Rules Pack
             Version   : 3.24
        Package-type : JeOS
        Version      : jeos-20.0.0-1-lnx64
             Component : ConcsoTgw
             Version   : 1.6.0.1
             Component : AdminShell
             Version   : 1.1
             Component : Hardened CentOS
             Version   : 6.7 patch#3
             Component : LCM
             Version   : 1.1
             Component : CASP
             Version   : 1.9
```

You may again run "check update" command to confirm that your appliance is up to date and has the latest patches.



```
admin# check update
No update found for requested software type.
Please try again later.
admin# 
```

Appendix D: CSPC CLI Commands

This section lists all the CLI commands, and a brief explanation of each command. The table also identifies which default user accounts have authority to use each command.

Note A user can connect to the 'target hardware' using SSH to shell, which is part of installed ISO/CSPC image, using the standard ssh client, and can then configure the CSPC.

CLI Command	Explanation	User IDs (Privilege)
?	Displays available commands	cisco, admin, user
about	Provides detailed information about appliance hardware and software configuration of interest to Cisco support personnel. This command is synonymous with show version [destination_file] Destination file: Located in a directory local to the partner's/customers laptop. Full path specified. The 'about'/'show version' command rejected if there is a naming conflict -- with appropriate screen message.	All (cisco, admin, user, viewer)
clear history *	Clears the command history for the current user, if command is invoked without user id; clears the command history for the specified user if specified with a user id.	*'cisco' can clear histories for all user ids. * 'admin' can clear histories for 'admin', 'viewer' and 'user' * 'viewer' and 'user' can clear their own histories
collector <options>	The smart collector options are: start / stop / status / restart.	cisco, admin, user
conf date *	Manually set the date and time	cisco, admin, user
conf dhcp <intf>	DHCP configuration	cisco, admin, user
conf dns [-ad] *	Configure the domain name server (DNS) (* means "one or	cisco, admin, user

	more") admin# conf dns [-ad] aa.bb.cc.dd … For example: To add the dns name server IP use: admin# conf dns -a 192.168.1.1 192.168.2.1 To delete the dns name server IP use: admin# conf dns -d 192.168.1.1 192.168.2.1	
conf ip *	Static IP Configuration, lets you configure: <intf> <ipaddr> <netmask> <gateway>	cisco, admin, user
conf proxy *	conf proxy <ipaddr> [<port>][<user> <passwd>] The Conf proxy command allows the user to set the proxy server, which enables intranet/internet traffic to be routed from the configured proxy server originating from the Smart Services Appliance. The Conf Proxy command supports only HTTP traffic. This means if the appliance needs to access the internet via a NON-HTTP protocol like – XMPP, then the traffic will not be routed via the proxy servers. Smart services appliances use outbound traffic to communicate with Cisco. The specific ports for outbound communication are noted in section.	cisco, admin, user
connectivity direct-mode <options>	Options are enable or disable. Enables or disables connectivity direct mode (P2P gateway - IPsec tunnel).	cisco, admin, user
dmidecode *	Displays the hardware status provided by Boot Firmware.	cisco, admin, viewer
firewall <options>	Enable/disable firewall rules (this refers to the OS firewall and is meant for special circumstances only). In normal situations, firewall rules should be preconfigured in the appliance.	cisco
hostname <hostname>	Specifies the hostname of the device.	cisco, admin, user
log download *	This command places the selected log file into the CSPC/logs directory when enabled. The selected log file	cisco, admin, user

	can then be downloaded into the desktop using the CSPC browser. Options are: <logtype> (enable | disable) logtype = CSPC | addon | UNIX | adminshell	
logout	Logout from this session	All (cisco, admin, user, viewer)
passwd	Change cisco/admin passwd	Each user changes their own password
ping *	View ping details	cisco, admin,
poweroff	Shutdown and power off the system	cisco, admin, user
proxy <options>	Turns on/off the proxy configuration for an appliance. Options are: (enable | disable)	cisco, admin, user
pwdreset <user>	Reset cisco/admin user password to default	Can reset passwords for lower levels only (See default user accounts)
reload	Reboot the system	cisco, admin, user
route [-ad] *	Configures a static route on an interface. Options are: <intf> <network/mask> <gateway>	cisco, admin, user
show connectivity direct-mode	Indicates if Connectivity direct mode (the P2P gateway - IPsec tunnel connection) is enabled or disabled.	cisco, admin, user
show date	Show the current date	All (cisco, admin, user, viewer)
show firewall	Displays the firewall rules	cisco
show history *	Accesses the command history files stored on the appliance. Displays the command history for current user, if invoked without user id; displays a command history for specified user if specified with user id.	*'cisco' can view histories for all user ids. * 'admin' can view histories for 'admin', 'viewer' and 'user' * 'viewer' and 'user' can view their own histories
show hostname	Displays the hostname	All (cisco, admin, user, viewer)

show ipconfig	Shows the following information: - DHCP enabled (yes/no) - IP address - Subnet mask - Physical (MAC) address - Default gateway (proxy) - DNS server(s)	All (cisco, admin, user, viewer)
show logs *	Display logs based on selected file in each category. The options are: <logtype> (include | exclude | begin <pattern>) logtype = ADMINSHELL | ADDON | LINUX | CSPC The include | exclude | begin options allow users to specify various search criteria based on the specified pattern on the selected log file. Usage: admin# show logs (logtype) include|exclude|begin (pattern) E.g.: admin# show logs ADMINSHELL admin# show logs ADDON admin# show logs LINUX admin# show logs CSPC	cisco, admin, viewer
show monitor	Shows the following information: (1) network utilization (%) for ethernet port (2) CPU and memory utilization	All (cisco, admin, user, viewer)
show route	Displays the routing table of the appliance.	cisco, admin, user
show timezone	Shows which time zone is set	All (cisco, admin, user, viewer)
show version	Display version	All (cisco, admin, user, viewer)
ssh <options>	Enables or disables ssh access	cisco, admin, user

	Options are: (enable | disable)	
Sudo <command>	Launch Linux shell from admin shell using the 'sudo' command to prefix Linux shell command. Example use cases: - Can also be used to view logs accessible via the Linux shell only. - View the appliances directory structure - Mount and unmount an external drive (e.g. USB flash), view directory structure of external drive, copy files between external drive and appliance's hard drive.	cisco
telnet <options>	Enable or disable telnet access. Options are: (enable | disable)	cisco, admin, user
timezone	After pressing enter the system displays all the time zones and then asks if you want to change the time zone; enter (yes | no)	cisco, admin, user
traceroute <host>	Lets you enable trace routing for a network device specified by the IP address and alternatively specify a file name for the results.	cisco, admin,
usb <options>	Options are: mount | unmount | list | status | copy from USB drive	cisco
User Help: User help for listing commands and for describing individual commands.	(1) Typing a command name without parameters shall list help for that command e.g. typing "show log". The command has to be available to the user id (privilege); otherwise, it is shown as not available. (2) Typing '?' after a command name shall be equivalent to typing the command without parameters. (3) General keywords such as "show" or "conf" shall list the show or conf commands available to the user, but no help for the commands. (4) Typing '?' will list all the CLI commands that are available to the user.	Each user ID has access to help for the commands that are relevant to its privilege level.

Legal Disclaimer

The information, documents, tools, and other materials that are included or referenced in this document (collectively, "Information") may be used by a Cisco Authorized Channel solely in connection with such Authorized Channel's activities to promote and sell Cisco services. Authorized Channel's use of such Information is subject to the systems integrator agreement or indirect channel partner agreement (ICPA), between Authorized Channel and Cisco.

Cisco owns and shall continue to own all right, title, and interest in and to the Information. Cisco assumes no responsibility for the accuracy of the Information or of any modifications made by Authorized Channel to such Information. Cisco reserves the right to change the programs or products covered by the Information at any time without notice. Mention of non-Cisco products or services is for information purposes only and constitutes neither an endorsement nor a recommendation.

ALL INFORMATION, DOCUMENTS, TOOLS, AND OTHER MATERIALS ARE PROVIDED "AS IS" WITH ALL FAULTS AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO'S LIABILITY WITH RESPECT TO THE INFORMATION, DOCUMENTS, TOOLS, AND OTHER MATERIALS INCLUDED OR REFERENCED IN THIS DOCUMENT EXCEED THE AMOUNTS PAID FOR THEM BY YOU. CISCO AND ITS SUPPLIERS SHALL NOT BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR REVENUES, WHETHER ARISING IN CONTRACT, TORT (INCLUDING NEGLIGENCE), OR OTHERWISE, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0910R)

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA 08/23/16