

Common Services Platform Collector 2.2 Quick Start Guide

September 27, 2013

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>

INTRODUCTION	4
ACCESSING PSS 1.X IMAGES	5
HOW TO GET THE IMAGES.....	5
ACCESSING RELEASE PSS 1.0.....	7
IMAGE DOWNLOAD METHODS (DOWNLOAD VS. ADD TO CART).....	8
<i>Download</i>	9
<i>Add to Cart</i>	10
END USER LICENSE AGREEMENT.....	12
DEFAULT LOGIN USER IDS AND PRIORITIES.....	13
CHANGING THE ROOT PASSWORD.....	13
CONFIGURE PROXY SERVER	16
USING AN ISO IMAGE	20
CHECK CSP-C PREREQUISITES.....	20
<i>Preparation Checklist for CSP-C Collector Install</i>	20
<i>CSP-C Collector System Requirements</i>	21
<i>Available Mode Requirements for Upload</i>	22
<i>Browser Requirements</i>	22
BURN THE DOWNLOADED ISO IMAGE ON TO A DVD.....	23
INSTALL THE ISO IMAGE ONTO THE CSP-C COLLECTOR.....	24
PERFORM ISO POST-INSTALLATION TASKS.....	28
CONFIGURE THE CSP-C COLLECTOR IP ADDRESS ON TO THE TARGET HARDWARE.....	29
VMWARE VIRTUALIZATION PLATFORMS	31
VMWARE VIRTUALIZATION ESXi PLATFORMS.....	31
<i>ESXi 4.1</i>	31
<i>ESXi 5.0</i>	34
<i>Install the CSP-C ESXi image</i>	38
CONFIGURE VMWARE SMART COLLECTOR IP ADDRESS.....	52
CSP-C REGISTRATION	55
REGISTER THE CSP-C.....	55
DOWNLOAD THE CERTIFICATE.....	57
ACCESS THE APPLIANCE.....	58
UPLOAD NEW LICENSE.....	61
CSP-C CONFIGURATION AND DEVICE CREDENTIALS	64
RULES PACKAGE	68
RULES PACKAGE COMPONENTS.....	68
INSTALLING RULES PACKAGE IN THE CSPC.....	68
<i>Prerequisites</i>	68
<i>Importing All Rules</i>	69
<i>Importing Rules Package One by One:</i>	70
<i>Manage Data Masking Rules</i>	70
<i>Manage Data Integrity Rules</i>	72
<i>Manage Platform Definitions</i>	73
<i>Manage Datasets</i>	75
<i>Manage Data Collection Profiles</i>	76
UPGRADING OR DELETING THE EXISTING RULES FROM CSPC.....	77
<i>Manage Data Collection Profiles</i>	78
<i>Manage Datasets</i>	79
<i>Manage Platform Definitions:</i>	80
<i>Manage Data Integrity Rules:</i>	81
<i>Manage Data Masking Rules</i>	82

CSPC COLLECTOR UPGRADE	84
WHAT TO EXPORT	84
<i>Device Credentials</i>	84
<i>Managed Devices</i>	87
<i>Discovery Jobs</i>	89
WHAT TO IMPORT	91
<i>Import of Device Credentials</i>	91
<i>Discover and Manage Devices</i>	94
<i>Import Discovery Jobs</i>	97
SOFTWARE IMAGE UPGRADES.....	100
LCM AGENT MANAGER	100
APPLIANCE INTERFACE	100
SOFTWARE IMAGE BUILD SETUP	101
PERFORM A PATCH UPGRADE	102
<i>On-Demand Option</i>	102
<i>Auto-Update Option</i>	105
ACCESSING THE IDA SOFTWARE IMAGE SERVER	106
INVENTORY UPLOAD	109
DISCOVER THE DEVICES	109
CREATE AND MANAGE DATASETS	112
DATA COLLECTION PROFILES.....	116
<i>Add Collection Profile</i>	116
<i>Manage Data Collection Profiles</i>	123
RUN COLLECTION PROFILE AND UPLOAD DATA	125
DATA ACCESS VERIFICATION	127
MINIMUM COLLECTION PROFILE	131
MULTI-SERVICE COLLECTION	132
CSP-C CLI COMMANDS.....	134
CSP-C BASIC TROUBLESHOOTING.....	139
NETWORK CONFIGURATION ERRORS	139
COLLECTOR REGISTRATION ERRORS.....	140
VMWARE BASIC TROUBLESHOOTING.....	141
NETWORK CONFIGURATION ERRORS	141
COLLECTOR REGISTRATION ERRORS.....	142
VMWARE IMAGE CONFIGURATION ERRORS.....	142
BEST PRACTICES	143
ADDING MULTIPLE DEVICES IN IP ADDRESS HOST NAME FIELD	143
FILE NAME PREFIX SUGGESTION	145
REUSING THE SAME CERTIFICATE FOR ANOTHER COLLECTOR	146

Introduction

This document provides information about the CSPC 2.2 release. If you want information about the previous CSPC 2.1 T1 release, then go to the following URL:

http://www.cisco.com/en/US/docs/net_mgmt/smart_portal/Common_Services_Platform_Collector_Quick_Start_Guide_2.1T1.pdf

The Cisco smart portal provides data collection and serviceability that works in conjunction with one or more instances of Smart Collector(s) to provide centralized data collection and reporting across multiple customer sites. The Cisco IT backend stores the data received from the associated Smart Collectors and uses that data to summarize the networks health. The Smart Collector also provides the capability to get and display various serviceability log files ensuring that the administrators are notified of issues or status as quickly as possible.

Smart Collector is a generic reference to the Common Services Platform Collector (CSP-C). There are two image options for CSP-C:

- [Accessing PSS 1.x Images](#)
- [Using a CSP-C ISO Image](#) on Target Hardware.
- Using VMware to run a CSP-C image virtually on one of the following VMware platforms:
 - VMware vSphere Hypervisor [ESXi 4.x](#) virtual platform
 - VMware vSphere Hypervisor [ESXi 5.x](#) virtual platform.

This Quick Start Guide is a compilation of steps that provides a method for performing the following tasks:

- How to access the download images ([download](#) versus [add-to-cart](#))
- Explains the processes for using the ISO image option, which includes the following items:
 - [How to Get the Images](#)
 - [Install the ISO Image onto the CSP-C Collector](#)
 - [Configure the CSP-C Collector IP Address on to the Target Hardware](#)
- Covers the steps for using one of the VMware virtualization platforms, which includes:
 - **[Error! Reference source not found.](#)**
 - [VMware](#)
- [CSP-C Registration](#)
- [CSP-C configuration and Device Credentials](#)
- Working with the [Rules Package](#) (Installing / Updating / Deleting)
- [CSPC Collector Upgrade](#)
- [Software Image Upgrades](#)
- [Inventory Upload](#)
- [Minimum Collection Profile](#)
- [Multi-Service Collection](#)

This Quick Start Guide also provides information about the following items:

- [CLI Commands](#) (Configure IP address, Start/stop data collection, View logs)
- [Basic Troubleshooting](#)
- [Best Practices](#)

Accessing PSS 1.x Images

There are several types of images that are available in the PSS 1.x release:

- CSP-C Intel ISO Image for PSS for UCS C200 M2.
- CSP-C Rules for PSS (the CSP-C Rules are automatically installed; they are part of the CSP-C software image).
- VMware Images for VMware vSphere Hypervisor releases.
- DPA CLI's of Windows for PSS (optional).

The next section describes the different ways to go to the location of the images.

How to Get the Images

There are two different ways to access the various images. Both ways get you to the [PSS 1.0 image download page](#).

To download a single image file, perform the following steps:

Go to URL

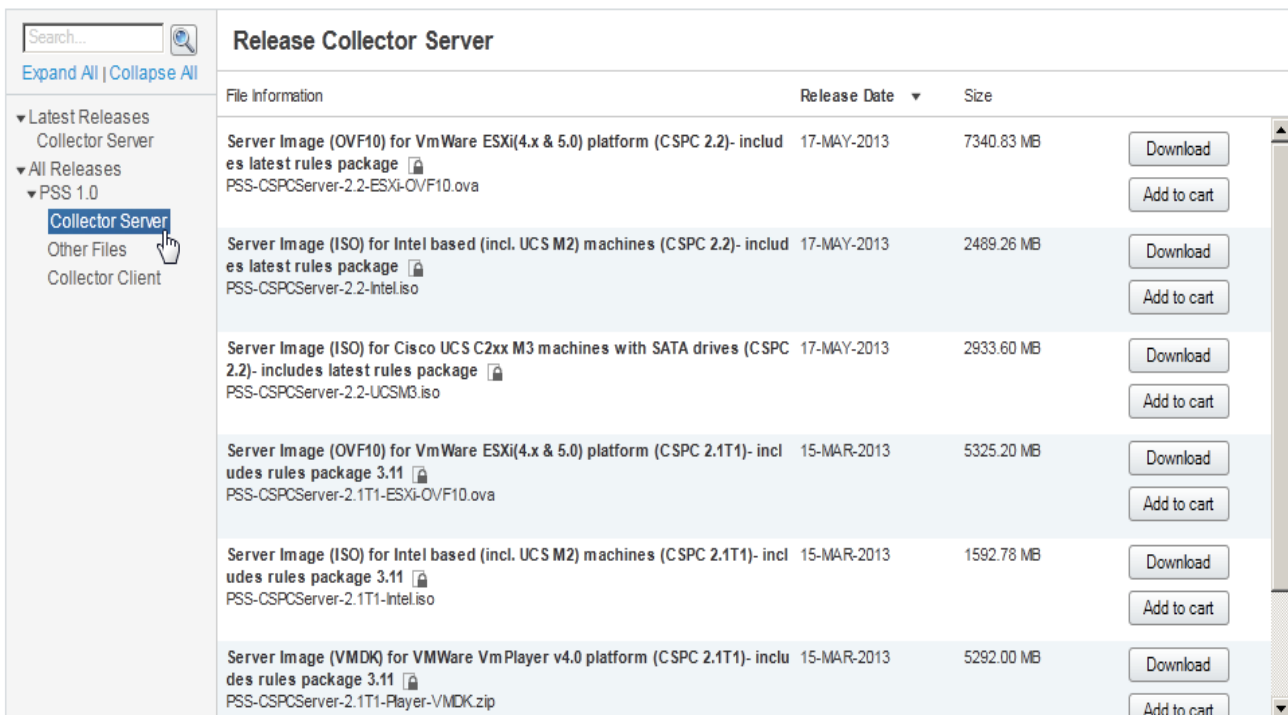
<http://www.cisco.com/cisco/software/release.html?mdfid=283114009&catid=268439477&softwareid=283308676&release=Collector%20Server&rellifecycle=&relind=AVAILABLE&reltype=all;>

Download Software

 Download Cart (0 items) [\[-\]Feedback](#) [Help](#)

[Downloads Home](#) > [Products](#) > [Cloud and Systems Management](#) > [Cisco Services](#) > [Cisco Smart Collector](#) > [Smart collector](#) >
Smart Collector Software-Collector Server

Smart collector









Release Collector Server

Expand All | Collapse All

Search...

▼ Latest Releases
Collector Server

▼ All Releases
▼ PSS 1.0
Collector Server
Other Files
Collector Client


File Information	Release Date	Size	
Server Image (OVF10) for VmWare ESXi(4.x & 5.0) platform (CSPC 2.2)- includes latest rules package  PSS-CSPCServer-2.2-ESXi-OVF10.ova	17-MAY-2013	7340.83 MB	Download Add to cart
Server Image (ISO) for Intel based (incl. UCS M2) machines (CSPC 2.2)- includes latest rules package  PSS-CSPCServer-2.2-Intel.iso	17-MAY-2013	2489.26 MB	Download Add to cart
Server Image (ISO) for Cisco UCS C2xx M3 machines with SATA drives (CSPC 2.2)- includes latest rules package  PSS-CSPCServer-2.2-UCSM3.iso	17-MAY-2013	2933.60 MB	Download Add to cart
Server Image (OVF10) for VmWare ESXi(4.x & 5.0) platform (CSPC 2.1T1)- includes rules package 3.11  PSS-CSPCServer-2.1T1-ESXi-OVF10.ova	15-MAR-2013	5325.20 MB	Download Add to cart
Server Image (ISO) for Intel based (incl. UCS M2) machines (CSPC 2.1T1)- includes rules package 3.11  PSS-CSPCServer-2.1T1-Intel.iso	15-MAR-2013	1592.78 MB	Download Add to cart
Server Image (VMDK) for VMWare VmPlayer v4.0 platform (CSPC 2.1T1)- includes rules package 3.11  PSS-CSPCServer-2.1T1-Player-VMDK.zip	15-MAR-2013	5292.00 MB	Download Add to cart

Click **PSS 1.0**, and then click **Collector Server**; the Release Collector Server pane appears.



Note You need a Cisco.com user/password and an associated contract in order to download the images. Some of the file names noted above may change as newer releases are created for the files noted above.

- Go to the images using the download link on the smart portal web interface, described next.
 - The link to the download location of the Smart Collector – CSP-C ISO image, and other related images can be found on the [Smart Portal Overview page](#).

Overview	User Registration	Smart Collector - Common Services Platform
<p>Smart Portal Overview Delivering capabilities to discover, collect and analyze network device details and provide network aware information. Learn More - Partner Support Service</p> <p>PSS Support Community For more up-to-date information and other resources, please visit PSS Support Community. For information about how to get access to this private community, please send e-mail to psscommunity@external.cisco.com.</p>		 <p>Resources</p> <p>PSS Smart Portal Training PSS API Console</p> <p>Download</p> <p>User Guide Smart Collector - Common Services Platform Software 1</p>
<p>User Registration Self Registration Or Register Users Maintain User Registrations</p> <p>Common Services Platform Collector (CSP-C) Register CSP-C Manage Collectors</p> <p>Installed Base Management, Alerts and Diagnostics Reports</p>		

- On the [smart portal Overview page](#), in the Download section, click **Smart Collector – Common Services Platform Software**; 1 the [Release PSS 1.0 page](#) appears.

Accessing Release PSS 1.0

There are several different images that are associated to the PSS 1.0 release and displayed on the Smart collector download page. To download the images perform the following steps:

Download Software Download Cart (0 items) Feedback Help

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

Smart collector

Search...

Expand All | Collapse All

- ▼ Latest Releases
 - Collector Server
- ▼ All Releases
 - ▼ PSS 1.0
 - Collector Server**
 - Other Files
 - Collector Client

Release Collector Server

File Information	Release Date	Size	
Server Image (OVF10) for VmWare ESXi(4.x & 5.0) platform (CSPC 2.2)- includes latest rules package	17-MAY-2013	7340.83 MB	Download Add to cart
Server Image (ISO) for Intel based (incl. UCS M2) machines (CSPC 2.2)- includes latest rules package	17-MAY-2013	2469.26 MB	Download Add to cart
Server Image (ISO) for Cisco UCS C2xx M3 machines with SATA drives (CSPC 2.2)- includes latest rules package	17-MAY-2013	2933.60 MB	Download Add to cart
Server Image (OVF10) for VmWare ESXi(4.x & 5.0) platform (CSPC 2.1T1)- includes rules package 3.11	15-MAR-2013	5325.20 MB	Download Add to cart
Server Image (ISO) for Intel based (incl. UCS M2) machines (CSPC 2.1T1)- includes rules package 3.11	15-MAR-2013	1592.78 MB	Download Add to cart
Server Image (VMDK) for VMWare VmPlayer v4.0 platform (CSPC 2.1T1)- includes rules package 3.11	15-MAR-2013	5292.00 MB	Download Add to cart

- Click **PSS 1.0**, then click **Collector Server**; the Release Collector Server pane appears.



Note You need a Cisco.com user/password and an associated contract in order to download the images. Some of the file names noted above may change as newer releases are created for the files noted above.

The above image downloads are large, and could take quite a while to download.

Download Software Download Cart (0 items) Feedback Help

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

Smart collector

Search...

Expand All | Collapse All

- ▼ Latest Releases
 - Collector Server
 - SNTC 1.6
- ▼ All Releases
 - ▼ PSS 1.0
 - Collector Server
 - Other Files
 - Collector Client**

Release Collector Client

File Information	Release Date	Size	
Client Image for Windows 32 bit platforms (CSPC 2.1T1)	16-NOV-2012	77.30 MB	Download Add to cart
Client Image for Windows 32 bit platforms	23-APR-2012	75.45 MB	Download Add to cart

- To download the CSP-C Client, click **Collector Client**; the client image appears in the download area on the right (login & valid contract are required).







Note The Collector client is valid only CSPC 2.1T1 and earlier releases.

Download Software

 Download Cart (0 items) [Feedback](#) [Help](#)
[Downloads Home](#) > [Products](#) > [Cloud and Systems Management](#) > [Cisco Services](#) > [Cisco Smart Collector](#) > [Smart collector](#) > [Smart Collector Software-Other Files](#)

Smart collector

Release Other Files		Release Date	Size	
File Information				
Smart Collector Rules (3.11) for CSPC-2.1 T1 PSS-CSPCRules-2.1T1.zip	 5	15-FEB-2013	0.16 MB	Download Add to cart
Smart Collector Rules PSS-CSPCRules-2.0.3.zip		23-APR-2012	0.11 MB	Download Add to cart
Smart Collector DPA CLIs for Linux PSS-dpaCisLinux.zip	 6	23-APR-2012	40.28 MB	Download Add to cart
Smart Collector DPA CLIs for Windows PSS-dpaCisWin.zip	 7	23-APR-2012	30.68 MB	Download Add to cart

- To download the Smart Collector DPA files, click **Other Files**; **C** the following images appear in the download area on the right:
 - Smart Collector Rules (login & valid contract are required) **5**



Note For the CSP-C 2.1T1 release there are no Rules files to download or install. The CSP-C Rules are automatically installed; they are part of the CSP-C software image.

- Smart Collector DPA CLI's for Linux (login & valid contract are required) **6**
- Smart Collector DPA CLI's for Windows (login & valid contract are required) **7**

Image Download Methods (Download vs. Add to Cart)

There are two different ways that you can download a file on the Release PSS 1.0 page:

- Download** – this method is used for downloading a single image file.
- Add to cart** – this method is used for downloading multiple image files.

Download

To download a single image file, perform the following steps:

- Go to URL
<http://www.cisco.com/cisco/software/release.html?mdfid=283114009&catid=268439477&softwareid=283308676&release=Collector%20Server&relicycle=&reind=AVAILABLE&reltype=all>

Download Software Download Cart (0 items) Feedback Help

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

Smart collector

Search:

Expand All | Collapse All

Latest Releases
 Collector Server
 All Releases
 PSS 1.0
 Collector Server
 Other Files
 Collector Client

Release Collector Server

File Information	Release Date	Size	
Server Image (OVF10) for VmWare ESXi(4.x & 5.0) platform (CSPC 2.2)- includes latest rules package PSS-CSPCServer-2.2-ESXi-OVF10.ova	17-MAY-2013	7340.83 MB	<input type="button" value="Download"/> <input type="button" value="Add to cart"/>
Server Image (ISO) for Intel based (incl. UCS M2) machines (CSPC 2.2)- includes latest rules package PSS-CSPCServer-2.2-Intel.iso	17-MAY-2013	2489.26 MB	<input type="button" value="Download"/> <input type="button" value="Add to cart"/>
Server Image (ISO) for Cisco UCS C2xx M3 machines with SATA drives (CSPC 2.2)- includes latest rules package PSS-CSPCServer-2.2-UCSM3.iso	17-MAY-2013	2933.60 MB	<input type="button" value="Download"/> <input type="button" value="Add to cart"/>
Server Image (OVF10) for VmWare ESXi(4.x & 5.0) platform (CSPC 2.1T1)- includes rules package 3.11 PSS-CSPCServer-2.1T1-ESXi-OVF10.ova	15-MAR-2013	5325.20 MB	<input type="button" value="Download"/> <input type="button" value="Add to cart"/>
Server Image (ISO) for Intel based (incl. UCS M2) machines (CSPC 2.1T1)- includes rules package 3.11 PSS-CSPCServer-2.1T1-Intel.iso	15-MAR-2013	1592.78 MB	<input type="button" value="Download"/> <input type="button" value="Add to cart"/>
Server Image (VMDK) for VmWare VmPlayer v4.0 platform (CSPC 2.1T1)- includes rules package 3.11 PSS-CSPCServer-2.1T1-Player-VMDK.zip	15-MAR-2013	5292.00 MB	<input type="button" value="Download"/> <input type="button" value="Add to cart"/>

- Click PSS 1.0, then click Collector Server; the Release Collector Server pane appears.
- Find the image you want to download (i.e., PSS-CSPCServer-2.2-Intel.iso image), then click the respective **Download** button; the [End User License Agreement \(EULA\)](#) window appears.

End User License Agreement X

By downloading this file you acknowledge that you have read and agree to be bound by the terms and conditions of the [Cisco End User License Agreement](#)



Note To download the software images, you must have a CCO Log In and have a valid service contract associated to your Cisco.com profile. If not you will receive an error window indicating this condition.

- To continue this download process click **Agree** for the End User License Agreement.

Add to Cart

Use the Add to cart option to download multiple image files. To use the Add to cart option, perform the following steps:

- Go to URL
<http://www.cisco.com/cisco/software/release.html?mdfid=283114009&catid=268439477&softwareid=283308676&release=Collector%20Server&relicycle=&relind=AVAILABLE&reltype=all;>

Download Software

Download Cart (0 items) [\[-\]Feedback](#) [Help](#)

[Downloads Home](#) > [Products](#) > [Cloud and Systems Management](#) > [Cisco Services](#) > [Cisco Smart Collector](#) > [Smart collector](#) > [Smart Collector Software-Collector Server](#)


Smart collector

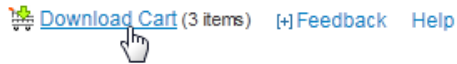
File Information	Release Date	Size	
Server Image (OVF10) for VmWare ESXi(4.x & 5.0) platform (CSPC 2.2)- includes latest rules package PSS-CSPCServer-2.2-ESXi-OVF10.ova	17-MAY-2013	7340.83 MB	Download Add to cart
Server Image (ISO) for Intel based (incl. UCS M2) machines (CSPC 2.2)- includes latest rules package PSS-CSPCServer-2.2-Intel.iso	17-MAY-2013	2489.26 MB	Download Add to cart
Server Image (ISO) for Cisco UCS C2xx M3 machines with SATA drives (CSPC 2.2)- includes latest rules package PSS-CSPCServer-2.2-UCSM3.iso	17-MAY-2013	2933.60 MB	Download Add to cart
Server Image (OVF10) for VmWare ESXi(4.x & 5.0) platform (CSPC 2.1T1)- includes rules package 3.11 PSS-CSPCServer-2.1T1-ESXi-OVF10.ova	15-MAR-2013	5325.20 MB	Download Add to cart
Server Image (ISO) for Intel based (incl. UCS M2) machines (CSPC 2.1T1)- includes rules package 3.11 PSS-CSPCServer-2.1T1-Intel.iso	15-MAR-2013	1592.78 MB	Download Add to cart
Server Image (VMDK) for VMWare VmPlayer v4.0 platform (CSPC 2.1T1)- includes rules package 3.11 PSS-CSPCServer-2.1T1-Player-VMDK.zip	15-MAR-2013	5292.00 MB	Download Add to cart

- Click **PSS 1.0**, then click **Collector Server**; the Release Collector Server pane appears.






File Information	Release Date	Size	
Server Image (OVF10) for VmWare ESXi(4.x & 5.0) platform (CSPC 2.2)- includes latest rules package PSS-CSPCServer-2.2-ESXi-OVF10.ova	17-MAY-2013	7340.83 MB	In Cart
Server Image (ISO) for Intel based (incl. UCS M2) machines (CSPC 2.2)- includes latest rules package PSS-CSPCServer-2.2-Intel.iso	17-MAY-2013	2489.26 MB	In Cart
Server Image (ISO) for Cisco UCS C2xx M3 machines with SATA drives (CSPC 2.2)- includes latest rules package PSS-CSPCServer-2.2-UCSM3.iso	17-MAY-2013	2933.60 MB	In Cart
Server Image (OVF10) for VmWare ESXi(4.x & 5.0) platform (CSPC 2.1T1)- includes rules package 3.11 PSS-CSPCServer-2.1T1-ESXi-OVF10.ova	15-MAR-2013	5325.20 MB	Download Add to cart

- Find the images you want to download.

- Press the respective **Add to cart** button for the image you want.
- As you click the Add to cart buttons, two things happen”
 - The button changes to an  **In Cart** icon.



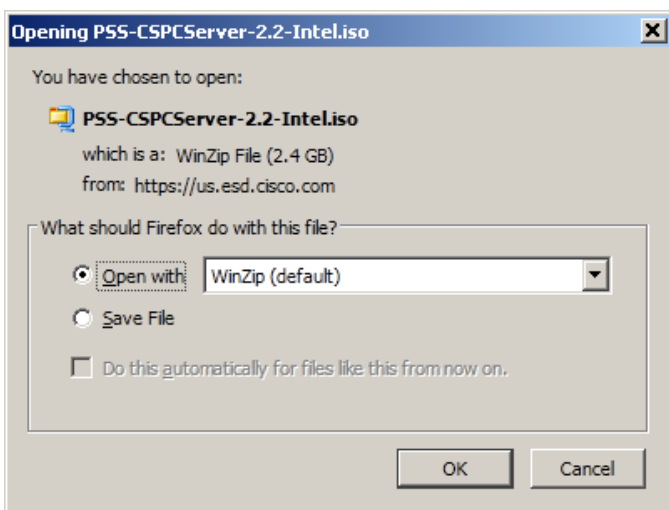
- The Download Cart number increments to the number of items selected.
- Click Download Cart, the Cart window appears.

- You have several options on this page:
 - Download all the listed images at the same time, by clicking **Download All**. 
 - Download each image separately by clicking the respective **Download** button. 
 - Add the selected product by clicking the **Add Device icon** 
 - The **Set Cisco Notification Alert icon**  lets you set the notification alert for a product.
 - The Remove from the Download Cart,  removes the associated image from the Download Cart.
- After selecting one of the download options, then continue this download process at the [End User License Agreement](#) section.

End User License Agreement



- Perform one of the following tasks:
 - Click **Cisco End User License Agreement**; ⁶ the End User License Agreement document appears in another window or tab. After reading the EULA, return to the previous window or tab and perform the next step.
 - Click the **Agree** button ⁷ the Opening PSS-CSPCServer-2.1T1-Intel.iso window appears.



- Choose one of the above radio button options (i.e., **Open With** or **Save File**) then click **OK**; the download starts.
- The next step depends on the type image downloaded:

Default Login User Ids and Priorities

By default, six default user accounts are created by each supported Collector image (ISO, Virtual VMware Appliances (ESXi/Player)). The higher the priority number, the more privileges the user id has.

S. No.	User-ID	Password	Shell
1	root	<Disabled by default>	Linux (Bash)
2	nsalogin	<Disabled by default>	Linux (Bash)
3	admin	Admin!23	Admin Shell
4	cisco	<Disabled by default>	Admin Shell
5	user	<Disabled by default>	Admin Shell
6	viewer	<Disabled by default>	Admin Shell
7	Admin123	Admin123	CSPC GUI



Note For the root:user id, direct SSH login is not allowed; see Changing the Root Password for more details on how to change the root password.

Changing the Root Password

There is a special process used when changing the Root password, since a direct SSH login is not allowed. To change the Root password, perform the following steps:

```

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

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

Changing password for user admin.
Old password:
New password:
Retype new password:

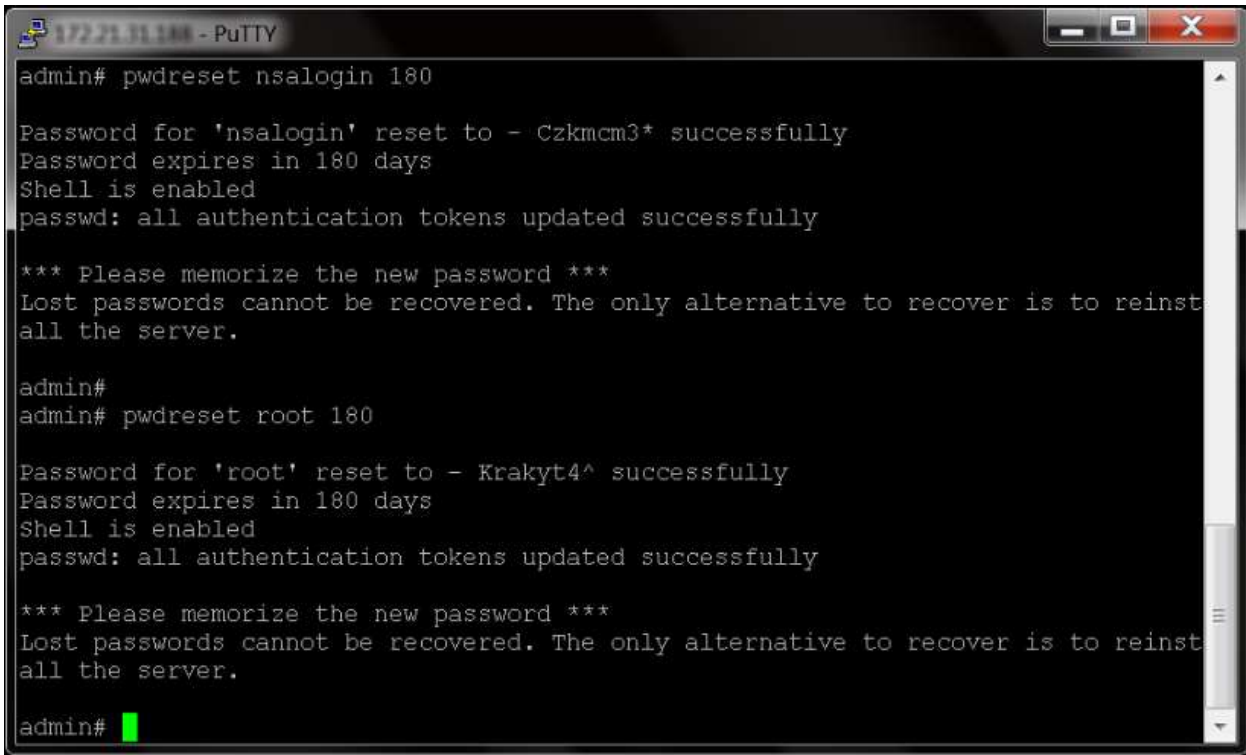
passwd: all authentication tokens updated successfully

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

admin# █

```

- In brand new appliance state (never logged into before), only the Admin account is enabled. Login to the appliance and enter **admin** as the login id.
- Enter the password **Admin!23**; the next step is to login to nsalogin.



```

172.21.31.188 - PuTTY
admin# pwdreset nsalogin 180

Password for 'nsalogin' reset to - Czkmcm3* 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 reinst
all the server.

admin#
admin# pwdreset root 180

Password for 'root' reset to - Krakyt4^ 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 reinst
all the server.

admin# █

```

Need

- Enter **pwdreset nsalogin 180**; this creates a new password (in example, Czkmcm3*). that is good for 180 days.
- Enter **pwdreset root 180**; this creates a new password (in example, Krakyt4^). that is good for 180 days.
- To change the root password you must first login as nsalogin, using the newly generated password.

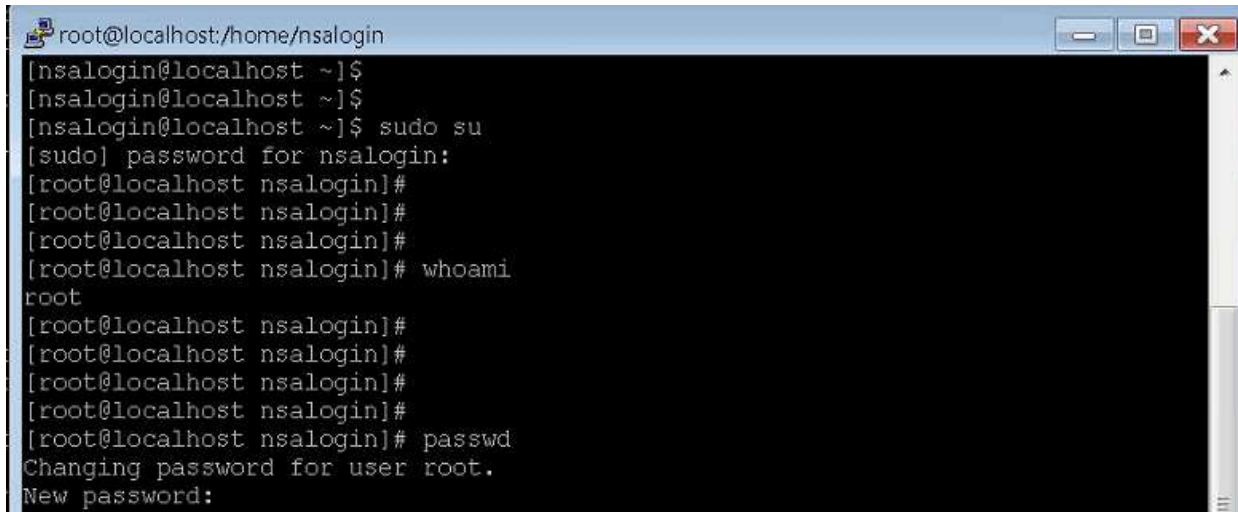


```

nsalogin@localhost:~
login as: nsalogin
Warning private system unauthorized users will be prosecuted.
Server refused our key
nsalogin@172.21.31.188's password:
Last login: Sat May  4 00:30:02 2013 from 10.154.113.120
[nsalogin@localhost ~]$ █
[nsalogin@localhost ~]$ █
[nsalogin@localhost ~]$ █
[nsalogin@localhost ~]$ █
[nsalogin@localhost ~]$ █
[nsalogin@localhost ~]$ █
[nsalogin@localhost ~]$ whoami
nsalogin
[nsalogin@localhost ~]$ █
[nsalogin@localhost ~]$ █
[nsalogin@localhost ~]$ sudo su
[sudo] password for nsalogin: █

```

- Login as **nsalogin**, then enter the previously generated password (in example, **Czkmcm3***).



```
root@localhost:/home/nsalogin
[nsalogin@localhost ~]$
[nsalogin@localhost ~]$
[nsalogin@localhost ~]$ sudo su
[sudo] password for nsalogin:
[root@localhost nsalogin]#
[root@localhost nsalogin]#
[root@localhost nsalogin]#
[root@localhost nsalogin]# whoami
root
[root@localhost nsalogin]#
[root@localhost nsalogin]#
[root@localhost nsalogin]#
[root@localhost nsalogin]#
[root@localhost nsalogin]# passwd
Changing password for user root.
New password:
```

- Enter **sudo su**, which changes the user to root.
- Enter **passwd**, then enter a new password; the password is now changed for root.

Configure Proxy Server

To configure a proxy server you must use the following process:

- Disable Connectivity direct mode if enabled
- Configure Proxy Server Settings
- Apply XML API Code through CSPC Client
- Execute CLI based commands listed below

Important For CSPC with Proxy there is an additional work around that is required and you should contact SSB for assistance at http://www.cisco.com/assets/services/ts/smartnet/sch/smart_service_bureau.html.

To configure a Proxy Server, perform the following steps:

```
admin#
admin# sh ip

Interface eth0 is up
DHCP is disabled
  Device      : eth0
  IP          : 172.26.26.100
  MAC        : 98:9C:29:09:09:11

Subnet Mask      : 255.255.255.0

DNS Servers :
  Nameserver1 : 172.26.26.100

Gateway :
  Interface   : eth0
  Gateway    : 172.26.26.1

Proxy is not configured
admin#
```

- Enter **show ip**; the bottom of the response indicates the proxy is not configured
- Enter **show connectivity direct-mode**; response indicates the connectivity direct-mode settings.
- If connectivity direct-mode is enabled, then you must enter “connectivity direct-mode disable”.

```
admin# conf proxy
-----
Usage:
conf proxy <ipaddr/host> <port> <user> <passwd>
      user,port(default is 8080),password are optional.
Eg:
admin# conf proxy 192.168.1.1 8080 cisco cisco
-----
admin# conf proxy 172.26.26.26 8080

Proxy settings saved successfully...please reboot
admin# █
```

- Enter **conf proxy** to see the command format, then enter the required command parameters.


```
Proxy settings saved successfully...please reboot
admin#
admin# sh ip

Interface eth0 is up
DHCP is disabled
    Device       : eth0
    IP           : 172.21.31.100
    MAC          : 08:00:C8:29:09:3F:11

Subnet Mask      : 255.255.255.0

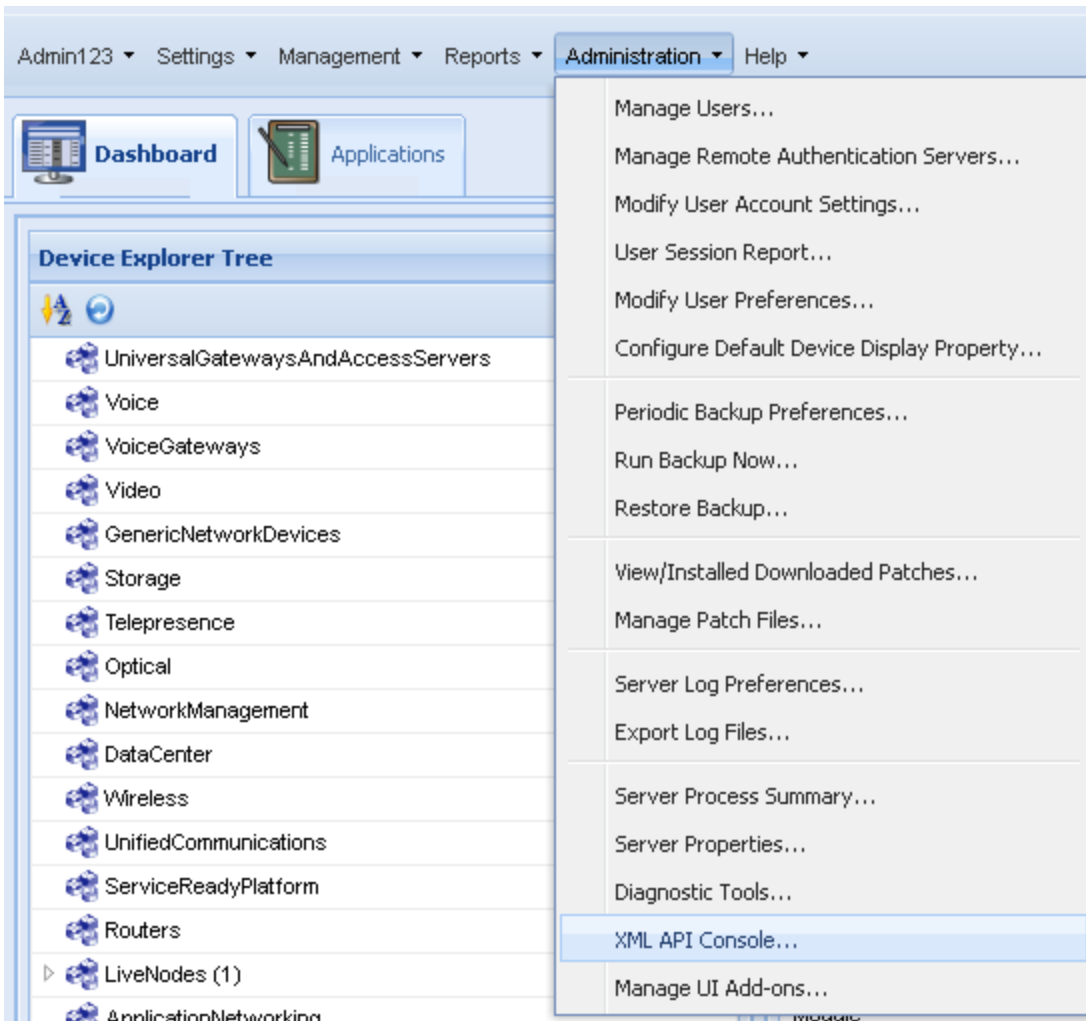
DNS Servers :
    Nameserver1 : 171.70.169.169

Gateway :
    Interface   : eth0
    Gateway     : 172.21.31.1

Proxy details :
    proxyname   : 173.76.136.35
    proxyport   : 8080
    status      : enabled

admin# █
```

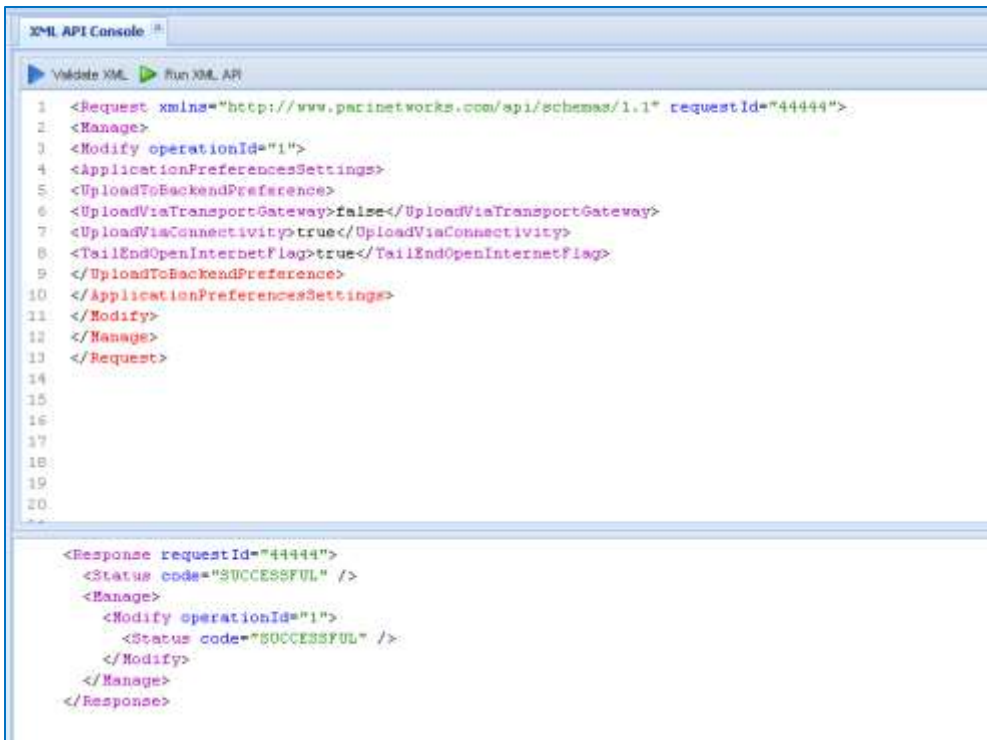
- Enter the **show ip** command to view the proxy settings.
- On the CSPC browser, go to **Administration -> XML API Console feature** to execute the following API command that changes the "connectivity_service_feature_mapping.properties" file through the XML API Console.



Use the API request code that is shown below:

```
<Request xmlns="http://www.parinetworks.com/api/schemas/1.1" requestId="44444">
<Manage>
<Modify operationId="1">
<ApplicationPreferencesSettings>
<UploadToBackendPreference>
<UploadViaTransportGateway>>false</UploadViaTransportGateway>
<UploadViaConnectivity>>true</UploadViaConnectivity>
<TailEndOpenInternetFlag>>true</TailEndOpenInternetFlag>
</UploadToBackendPreference>
</ApplicationPreferencesSettings>
</Modify>
</Manage>
</Request>
```

- Copy the XML code into the Console and click **Run XML API** and verify the results for success.

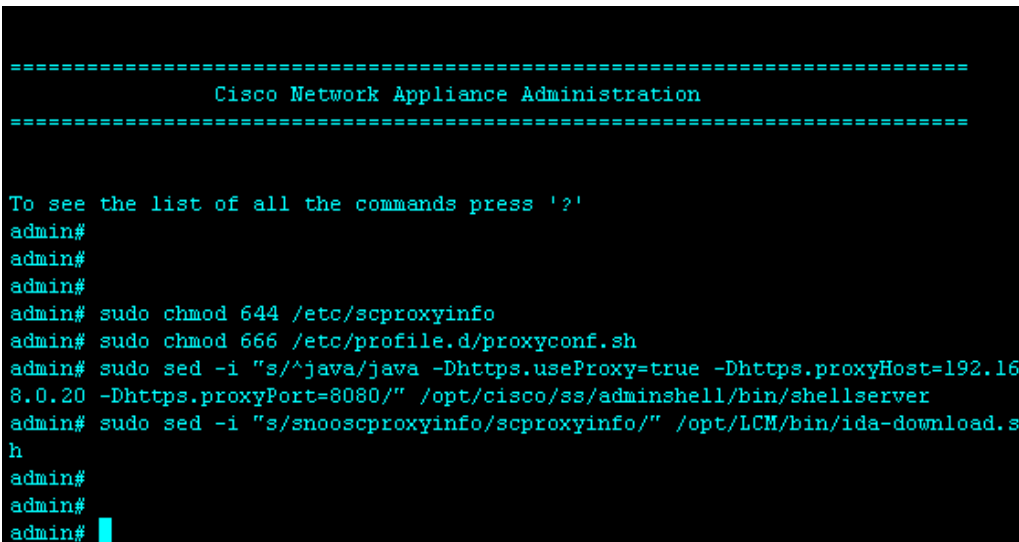


```

XML API Console
Validate XML Run XML API
1 <Request xmlns="http://www.pacinetworks.com/api/schemas/1.1" requestId="44444">
2 <Manage>
3 <Modify operationId="1">
4 <ApplicationPreferencesSettings>
5 <UploadToBackendPreference>
6 <UploadViaTransportGateway>false</UploadViaTransportGateway>
7 <UploadViaConnectivity>true</UploadViaConnectivity>
8 <TailEndOpenInternetFlag>true</TailEndOpenInternetFlag>
9 </UploadToBackendPreference>
10 </ApplicationPreferencesSettings>
11 </Modify>
12 </Manage>
13 </Request>
14
15
16
17
18
19
20
...
<Response requestId="44444">
  <Status code="SUCCESSFUL" />
  <Manage>
    <Modify operationId="1">
      <Status code="SUCCESSFUL" />
    </Modify>
  </Manage>
</Response>

```

- From the admin user, run the following commands:



```

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

To see the list of all the commands press '?'
admin#
admin#
admin#
admin# sudo chmod 644 /etc/scproxyinfo
admin# sudo chmod 666 /etc/profile.d/proxyconf.sh
admin# sudo sed -i "s/^java/java -Dhttps.useProxy=true -Dhttps.proxyHost=192.16
8.0.20 -Dhttps.proxyPort=8080/" /opt/cisco/ss/adminshell/bin/shellserver
admin# sudo sed -i "s/snooscpoxyinfo/scproxyinfo/" /opt/LCM/bin/ida-download.s
h
admin#
admin#
admin#

```

- sudo chmod 644 /etc/scproxyinfo
- sudo chmod 666 /etc/profile.d/proxyconf.sh
- sudo sed -i "s/^java/java -Dhttps.useProxy=true -Dhttps.proxyHost=**192.168.0.20** -Dhttps.proxyPort=**8080**" /opt/cisco/ss/adminshell/bin/shellserver



Note The two items listed above in red will be unique for your Proxy IP address and port number.

- sudo sed -i "s/snooscpoxyinfo/scproxyinfo/" /opt/LCM/bin/ida-download.sh
- Reboot the collector for proxy settings to take effect.

Using an ISO Image

This section covers the following areas of using an ISO image or the UCS image:

- [Check CSP-C Prerequisites](#)
- [Burn the Downloaded ISO Image on to a DVD](#)
- [Install the ISO Image onto the CSP-C Collector](#)
- [Perform ISO Post-Installation Tasks](#)
- [Configure the CSP-C Collector IP Address on to the Target Hardware](#)

Check CSP-C Prerequisites

There are CSP-C pre-requisites for the following areas:

- [Preparation Checklist for CSP-C Collector Install](#)
- [CSP-C Collector System requirements](#)
- [Available Mode Requirements for Upload](#)
- [Browser Requirements](#)

Preparation Checklist for CSP-C Collector Install

To prepare for the installation of the CSP-C collector, perform the following steps:

- Procure the recommended hardware (noted in the [CSP-C Collector System Requirements](#) section) at the customer site.
- Make sure you have the Windows environment, with [DVD burning tool\(s\)](#), to burn the DVD, and a DVD R/W drive.
- Procure a couple of empty writable DVD –R's to burn the ISO image.

CSP-C Collector System Requirements

To ensure the proper installation and operation of the CSP-C environment on your CSP-C collector, verify that the requirements listed in the following table are met before proceeding any further. The below requirements must be met for any component that you are using as the collector.

Component	Processor Type	Hard Drive Requirement	DRAM Memory Requirement
Intel based 32-bit platform	Intel Xeon, Celeron, Pentium type processor (Min. 2.0 GHz)	500 GB	4 GB
UCS C200 M2	Up to 2 Intel® Xeon® 5500 series multicore processors	500 GB	3 GB
UCS C22 M3	Intel® Xeon® Processor E5-2403 (10M Cache, 1.80 GHz, 6.40 GT/s Intel® QPI)	500 GB SATA drive	8 GB
UCS C220 M3	Intel® Xeon® Processor E5-2609 (10M Cache, 2.40 GHz, 6.40 GT/s Intel® QPI)	500 GB SATA drive	8 GB

Available Mode Requirements for Upload

To ensure a successful upload from a CSP-C Collector to the Cisco backend the following ports and specific IP addresses need to allow outbound access to the internet. The CSPC has several available modes that will allow for a successful upload to Cisco. ACL's on customers firewall might need to be configured to allow the CSP-C to upload successfully.



Note Only one of the below mode requirements is needed

IPSEC

Source IP Address	Source Port	Destination IP Address	Destination Port	Protocol	Direction
CSPC Server IP	any	72.163.7.138	5222	TCP	Outgoing
CSPC Server IP	any	72.163.7.138	7337	TCP	Outgoing
CSPC Server IP	any	72.163.7.88	3478	UDP	Outgoing
CSPC Server IP	any	72.163.7.96/27	4500	UDP	Outgoing

SSL

Source IP Address	Source Port	Destination IP Address	Destination Port	Protocol	Direction
CSPC Server IP	any	72.163.7.113	443	TCP	Outgoing

XMPP

Source IP Address	Source Port	Destination IP Address	Destination Port	Protocol	Direction
CSPC Server IP	any	72.163.7.138	5222	TCP	Outgoing
CSPC Server IP	any	72.163.7.138	7337	TCP	Outgoing

Browser Requirements

The CSPC Web UI was tested with the browsers mentioned in the following table.

Type	Version
Internet Explorer	8.0.x
Firefox	16.0.x

Burn the Downloaded ISO Image on to a DVD

After the [download of the CSP-C ISO image](#) is complete, then the next step is to burn the downloaded ISO image on to an empty DVD using any of the standard DVD burning tools installed on the Windows environment.



Fig 1.0



Note Figure 1.0 depicts one such tool (Sonic DVD burning tools in the Windows XP environment), or you can use Windows DVD Maker tool in the Windows 7 environment.

To burn the downloaded ISO image onto a DVD, perform the following steps:

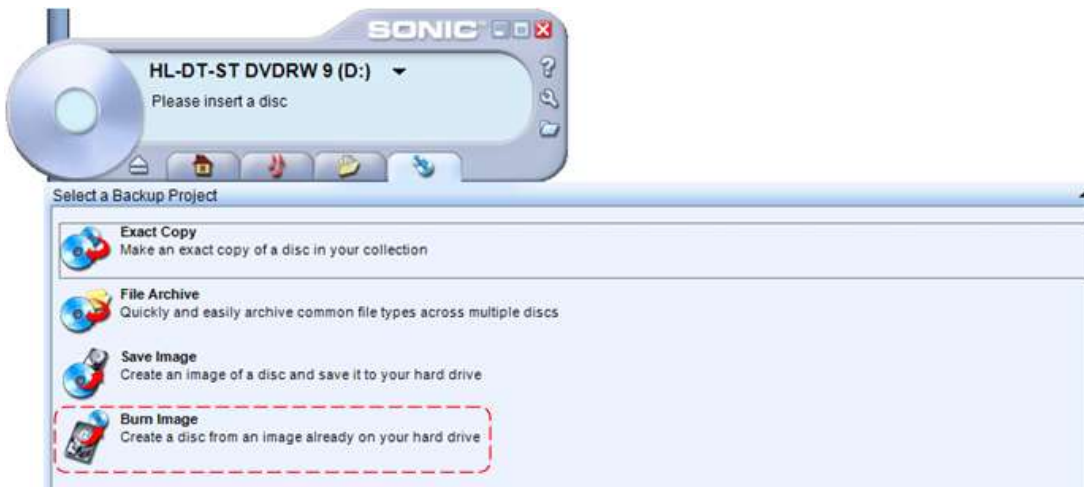



Fig 1.1

- Click **Burn Image**; the Burn Image pane appears.



Fig 1.2

- Click **Browse** to specify the location of the image.
- Place an empty DVD into the DVD R/W drive.
- Select the image that was stored on the local machine (e.g. PSS-CSPCServer-2.1T1-Intel.iso).
- Click the **Burn** button. 
- Once the image is successfully burned/written onto the DVD, a pop-up window appears indicating that the DVD burn option is completed.



Note The above graphics depict only the Sonic DVD tool, directions may vary for other DVD burning tools.

Install the ISO Image onto the CSP-C Collector

To install the burned DVD ISO image onto the CSP-C collector, perform the following steps:

- Make sure that the CSP-C collector is properly connected (display, keyboard, network, etc.) and ensure that the collector is powered on.
- Make sure the CSP-C collector has a DVD ROM, or that the collector is connected to an external DVD ROM.



Note Configuring an external DVD ROM to the CSP-C collector is out-of-scope of this document.

- Place the DVD that has the burned collector ISO image, [from the previous steps](#), into the CSP-C collector DVD ROM.
- Reboot the CSP-C collector, to ensure that DVD ROM reads the ISO Image from the DVD ROM; the machine boots up with the CloneZilla interface, shown in the following graphic.



Note Image name in the following graphics might be different depending on what version you downloaded.

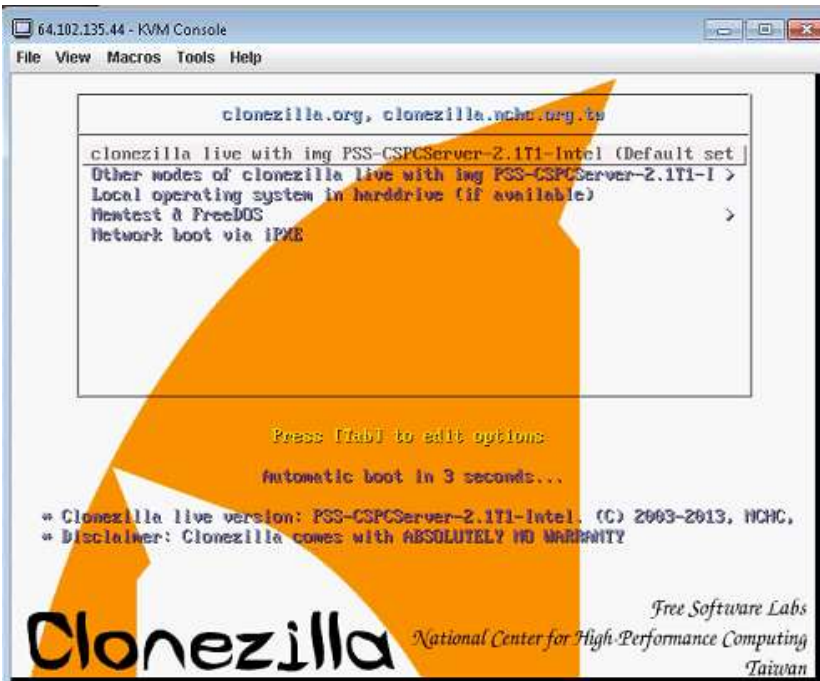


Fig 2.1

- Select the default (first option on the screen); if the user does not select the first option, the system will pick the first option by default, after a couple of seconds.
- Allow the system to boot the image until it selects all the disks and then prompts the user to enter 'Y' as shown in Fig 2.2.

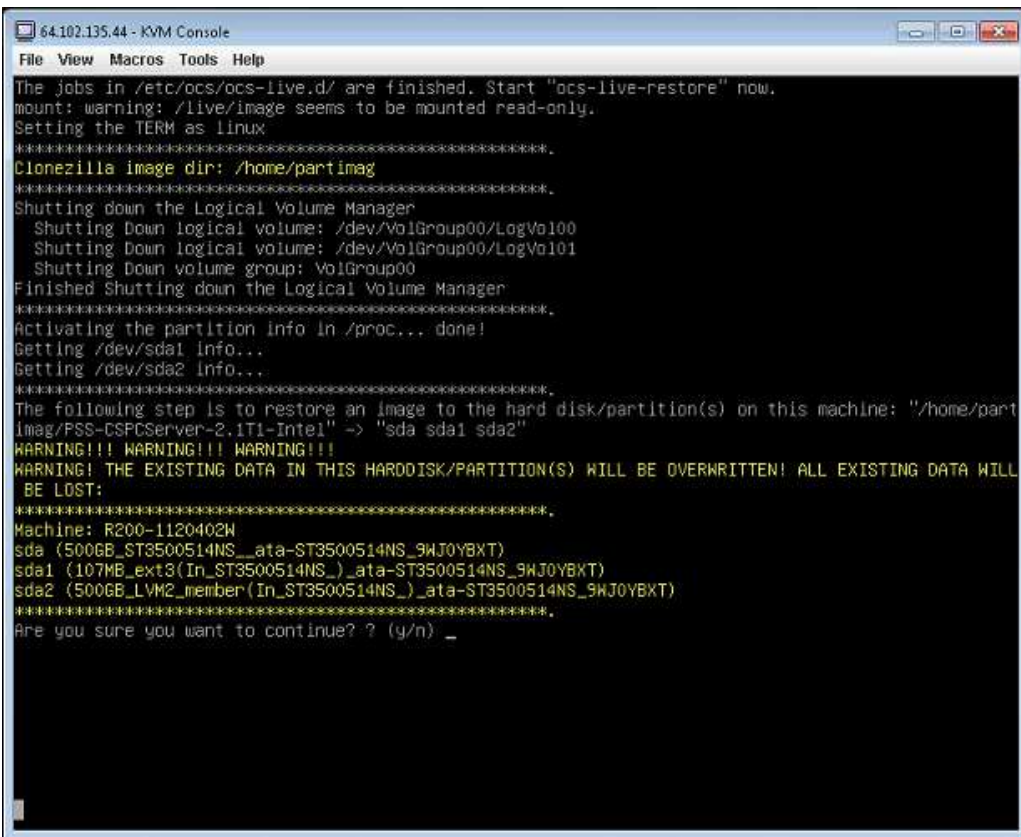
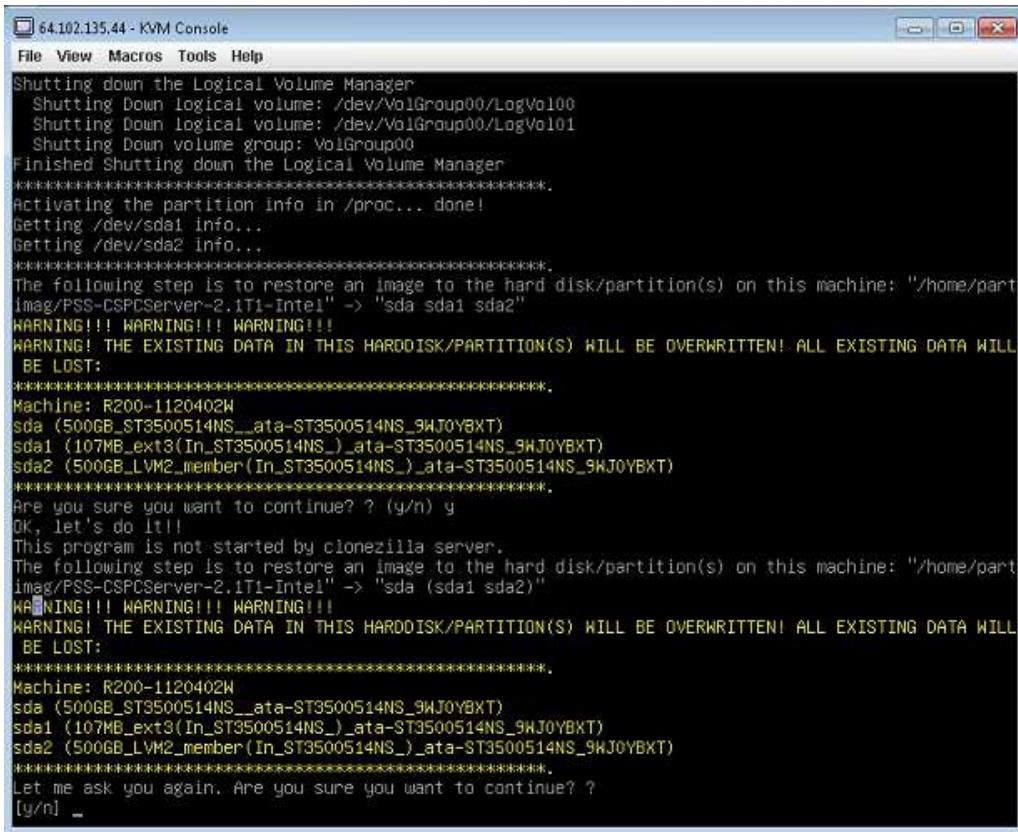


Fig 2.2

- Enter Y via the console keyboard.

Important Allow the system to continue to boot the image, until it clears all the data on the existing disk and then writes the new image onto the disk, as shown in Fig 2.3.



```

64.102.135.44 - KVM Console
File View Macros Tools Help
Shutting down the Logical Volume Manager
  Shutting Down logical volume: /dev/VolGroup00/LogVol100
  Shutting Down logical volume: /dev/VolGroup00/LogVol101
  Shutting Down volume group: VolGroup00
Finished Shutting down the Logical Volume Manager
*****
Activating the partition info in /proc... done!
Getting /dev/sda1 info...
Getting /dev/sda2 info...
*****
The following step is to restore an image to the hard disk/partition(s) on this machine: "/home/part
imag/PSS-CSPCServer-2.1T1-Intel" -> "sda sda1 sda2"
WARNING!!! WARNING!!! WARNING!!!
WARNING! THE EXISTING DATA IN THIS HARDDISK/PARTITION(S) WILL BE OVERWRITTEN! ALL EXISTING DATA WILL
BE LOST:
*****
Machine: R200-1120402W
sda (500GB_ST3500514NS_ata-ST3500514NS_9WJ0YBXT)
sda1 (107MB_ext3(In_ST3500514NS_)_ata-ST3500514NS_9WJ0YBXT)
sda2 (500GB_LVM2_member(In_ST3500514NS_)_ata-ST3500514NS_9WJ0YBXT)
*****
Are you sure you want to continue? ? (y/n) y
OK, let's do it!!
This program is not started by clonezilla server.
The following step is to restore an image to the hard disk/partition(s) on this machine: "/home/part
imag/PSS-CSPCServer-2.1T1-Intel" -> "sda (sda1 sda2)"
WARNING!!! WARNING!!! WARNING!!!
WARNING! THE EXISTING DATA IN THIS HARDDISK/PARTITION(S) WILL BE OVERWRITTEN! ALL EXISTING DATA WILL
BE LOST:
*****
Machine: R200-1120402W
sda (500GB_ST3500514NS_ata-ST3500514NS_9WJ0YBXT)
sda1 (107MB_ext3(In_ST3500514NS_)_ata-ST3500514NS_9WJ0YBXT)
sda2 (500GB_LVM2_member(In_ST3500514NS_)_ata-ST3500514NS_9WJ0YBXT)
*****
Let me ask you again. Are you sure you want to continue? ?
[y/n] _

```

Fig 2.3

- Enter Y via console keyboard.
- Allow the system to continue to boot the image.



Note Installation flow is captured in the following screen shots, as shown in Figure 2.4 to Figure 2.7


```

64.102.135.44 - KVM Console
File View Macros Tools Help
localepurge: Disk space freed in /usr/share/man: 0 KiB

Total disk space freed by localepurge: 0 KiB

Installing grub 1 on Clonozilla live/SE now..
(Reading database ... 21920 files and directories currently installed.)
Preparing to replace grub-common 1.99-18 (using ../grub-common_1.99-18_i386.deb) ...
Unpacking replacement grub-common ...
Selecting previously unselected package grub-legacy.
(Reading database ... 21920 files and directories currently installed.)
Unpacking grub-legacy (from ../grub-legacy_0.97-66_i386.deb) ...
Checking grub-install version...
Running: grub-install --no-floppy --root-directory=/tmp/hd_img.TMW9qb /dev/sda
Installation finished. No error reported.
This is the contents of the device map /tmp/hd_img.TMW9qb/boot/grub/device.map.
Check if this is correct or not. If any of the lines is incorrect,
fix it and re-run the script 'grub-install'.

(hd0) /dev/disk/by-id/ata-ST3500514NS_9WJ0YBXT
done!
.....
The NTFS boot partition was not found or not among the restored partition(s). Skip running partclone
.ntfsfixboot.
.....
.....
This program is not started by Clonozilla server, so skip notifying it the job is done.
Finished!
Now syncing - flush filesystem buffers...

"ocs-live-restore" is finished.
Now you can choose to:
(0) Poweroff
(1) Reboot
(2) Enter command line prompt
(3) Start over (image repository /home/partimag, if mounted, will be unmounted)
[2] _

```

Fig 2.6

- Once the image is properly written to disk, the system will prompt the user to eject the DVD disk placed in the DVD ROM.
- Remove the DISK and reboot the CSP-C collector, using the Reboot option as shown in Figure 2.6.
- Once the machine is rebooted, the CSP-C collector will boot with the newly created image.

Perform ISO Post-Installation Tasks

There are several tasks that need to be performed after the CSP-C collector install, please perform the following steps:

- Remove the DVD that was placed in DVD ROM. This will ensure that the CSP-C collector will not read the ISO image again when you reboot the machine.
- Reboot the CSP-C collector, to make sure that it boots up the ISO image that was previously installed from the DVD.
- The machine should boot with the default Hardened OS; once the Hardened OS is loaded, the machine will prompt the user as show in the Fig 3.1 (requesting user to login).

```

171.69.37.17 - PuTTY
login as: █

```

Fig 3.1

- You can verify the installation by logging into the CSP-C collector, using one of the [default user accounts](#) created by the collector server image.

Configure the CSP-C Collector IP Address on to the Target Hardware

An IP address needs to be configured on the hardware running the CSP-C collector. To configure the IP address on the hardware, after installing the ISO image, perform the following steps:

- Login to the CSP-C collector hardware via the connected console using admin/admin account/password; you will see the following screen.

```

?                - print the list of available commands
about            - about appliance
apply *         - install updates for Appliance components
check update *  - check availability of updates for Appliance components
clear history * - purge command history for user/s
clrscr*         - clear current screen/s
collector <start/stop/status/restart - collector start/stop/status/restart
conf autoupdate * - configure auto-update policy
conf date *     - configure date and/or time
conf dhcp <intf> - configure dhcp
conf dns [-ad] * - configure DNS server(s)
conf ip *       - configure static IP
conf proxy *    - configure proxy server
conf server-connection * - configure connection with server used for updates
connectivity direct-mode <enable/disable> - enable or disable connectivity direct-mode
delete autoupdate * - delete configured auto-update policy
dmidecode *     - view SMBIOS table
download *      - download updates for Appliance components
exit            - exits from this session
firewall <enable/disable> - enable/disable firewall rules
history-size <number> * - sets the maxsize for history file
hostname <hostname> - change hostname
logout         - logout from this session
passwd         - change user passwd
ping *        - view ping details
poweroff      - shutdown and power off the system
proxy <enable/disable/clear> - enable/disable or clear proxy
pwdreset <user> <expiry_interval> - reset cisco/admin user passwd to random string for a specified no of days
reboot        - reboot the system
reload        - reboot the system
route [-ad] <intf> <network/mask> < - add static route to a network
show apply *  - display status of apply operation
show autoupdate * - display details of configured auto-update policy
show connectivity direct-mode - display status of connectivity direct-mode
show date    - display date and time information
show download * - display status of download operation
show firewall - display the firewall rules
show history * - display command history for user/s and size of the history file
show hostname - display hostname
show ipconfig - display network configuration
show logs *  - display logs
show monitor - display appliance status(cpu, memory, disk)
show route  - display configured routes
show server-connection - display details of connection with server used for updates
show timesync - display current NTP sync interval and last update time
show timezone - display current timezone
show version * - display version for servicepack/Jeos
ssh <enable/disable> - enable or disable ssh access
sudo <command> - run linux command with sudo
telnet <enable/disable> - enable or disable telnet access
timesync *    - synchronize system time with NTP server and configure NTP synchronization interval
timezone     - set timezone information
traceroute <host> - traceroute host
admin#

```

Fig 4.1 Supported CLI commands



Note Cisco recommends that you change the default password.

- By default the appliance uses DHCP which configures a dynamic IP address. To configure a dynamic IP address, go to the command prompt admin# and enter conf dhcp eth0

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



Note As noted in the example, it is recommended to use eth0 interface for DHCP IP address configuration.

Also, make sure that DHCP server is running in your network so the server can provide a DHCP IP address to the CSP-C collector.

If you change the IP address settings for the CSP-C collector, reboot using the reload command. When the operating system on the CSP-C collector restarts with its new IP profile, continue with the rest of the configuration.

If you do not use the DHCP option then configure a static IP address. At the command prompt admin# enter conf ip and assign an IP address (static IP Address) for this device.

```
admin# conf ip help
-----
Usage:
admin# conf ip <intf> <ipaddr> <netmask> <gateway>
Eg:
admin# conf ip eth0 xxx.xxx.xxx.xxx 255.255.0 192.xxx.xxx.xxx
admin# conf ip eth0 xxx.xxx.xxx.xxx 255.255.0 192.xxx.xxx.xxx
```

Fig 4.3 IP Address configuration

- **Once** the configuration is successful, reboot the CSP-C collector in order to use the newly configured IP address.



Note As noted in the above example, it is recommended to use eth0 interface on your hardware to configure the static IP Address.

Also if you change the IP address settings for the CSP-C collector, reboot using the reload command. When the operating system on the CSP-C collector restarts with its new IP profile, continue with rest of the configuration.

VMware Virtualization Platforms

There VMware platform that is supported in this release is VMware vSphere Hypervisor > VMware vSphere Hypervisor ESXi 4.0 and ESXi 5.x



This section of the guide explains how to install a CSP-C Collector image on to an “already installed” VMware platform. This guide does not provide directions on how to install the different VMware platforms; links are provided in each respective VMware group on where to find the download image and directions on how to install the downloaded VMware platform image.

VMware Virtualization ESXi Platforms

There are two VMware Virtualization ESXi Platforms that are supported in this release:

- [ESXi 4.1](#)
- [ESXi 5.0](#)

ESXi 4.1

This section provides information on the following areas:

- [System Requirements](#)
- [Download the VMware vSphere Hypervisor ESXi 4.x Smart Collector Image](#)
- [Install VMware vSphere Hypervisor ESXi 4.x](#)
- [Additional Resources](#)

System Requirements

To ensure the proper installation and operation of VMware based smart collector environment on your machine, verify that all of the following requirements are met before proceeding.

64-bit Processor

These are the requirements for a 64-bit Processor:

- VMware ESX/ESXi 4.x only installs and run on servers with 64-bit x86 CPUs.
- Known 64-bit processors:
 - All AMD Opterons support 64 bit.
 - All Intel Xeon 3000/3200, 3100/3300, 5100/5300, 5200/5400, 7100/7300, and 7200/7400 support 64-bit.
 - All Intel Nehalem support 64-bit.

RAM

The RAM requirements are 2 GB RAM minimum.

Network Adapters

The supported network adapters include the following items:

- Broadcom NetXtreme 570x gigabit controllers
- Intel PRO 1000 adapters

SCSI Adapter, Fibre Channel Adapter, or Internal RAID Controller

One or more of these controllers (any combination) can be used:

- Basic SCSI controllers are Adaptec Ultra-160 and Ultra-320, LSI Logic Fusion-MPT, and most NCR/Symbios SCSI controllers.
- Fibre Channel, see the [Hardware Compatibility Guide](#).
- RAID adapters supported are HP Smart Array, Dell Perc (Adaptec RAID and LSI MegaRAID), and IBM (Adaptec) ServeRAID controllers.

Installation and Storage

The Installation and Storage requirements are:

- SCSI disk, Fibre Channel LUN, or RAID LUN with unpartitioned space. In a minimum configuration, this disk or RAID is shared between the service console and the virtual machines.
- For hardware iSCSI, a disk attached to an iSCSI controller, such as the QLogic qla405x. Software iSCSI is not supported for booting or installing ESX.
- Serial attached SCSI (SAS).
- For Serial ATA (SATA), a disk connected through supported SAS controllers or supported on-board SATA controllers. SATA disk drives connected behind supported SAS controllers or supported on-board SATA controllers.
- Supported SAS controllers include:
 - LSI1068E (LSISAS3442E)
 - LSI1068 (SAS 5)
 - IBM ServeRAID 8K SAS controller
 - Smart Array P400/256 controller
 - Dell PERC 5.0.1 controller
- Supported on-board SATA controllers include:
 - Intel ICH9
 - Nvidia MCP55
 - ServerWorks HT1000

When installing ESX on SATA drives, consider these points:

- Ensure that your SATA drives are connected through supported SAS controllers or supported onboard SATA controllers.
- Do not use SATA disks to create VMFS datastores shared across multiple ESX hosts.

ATA and IDE disk drives – ESX supports installing and booting on either an ATA drive or ATA RAID is supported, but ensure that your specific drive controller is included in the supported hardware. IDE drives are supported for ESX installation and VMFS creation.

Download the VMware vSphere Hypervisor ESXi 4.x Smart Collector Image

To Install the VMware vSphere Hypervisor ESXi 4.x smart collector onto a Windows Host Machine, go to the following URL:

<http://www.cisco.com/cisco/software/release.html?mdfid=283114009&catid=268439477&softwareid=283308676&release=Collector%20Server&rellifecycle=&relind=AVAILABLE&reltype=all>; the Release Collector Server images appear.

Download Software

Download Cart (0 items) [\[-\] Feedback](#) [Help](#)

[Downloads Home](#) > [Products](#) > [Cloud and Systems Management](#) > [Cisco Services](#) > [Cisco Smart Collector](#) > [Smart collector](#) > [Smart Collector Software-Collector Server](#)

Smart collector

Expand All | Collapse All

- ▼ Latest Releases
- Collector Server
- ▼ All Releases
- ▼ PSS 1.0
- Collector Server
- Other Files
- Collector Client

Release Collector Server

File Information	4.x & 5.0) platform	Release Date	Size	
Server Image (OVF10) for VmWare ESXi(4.x & 5.0) platform (CSPC 2.2)- include latest rules package	PSS-CSPCServer-2.2-ESXi-OVF10.ova	17-MAY-2013	7340.83 MB	<input type="button" value="Download"/> <input type="button" value="Add to cart"/>
Server Image (ISO) for Intel based (incl. UCS M2) machines (CSPC 2.2)- include latest rules package	PSS-CSPCServer-2.2-Intel.iso	17-MAY-2013	2489.26 MB	<input type="button" value="Download"/> <input type="button" value="Add to cart"/>
Server Image (ISO) for Cisco UCS C2xx M3 machines with SATA drives (CSPC 2.2)- includes latest rules package	PSS-CSPCServer-2.2-UCSM3.iso	17-MAY-2013	2933.60 MB	<input type="button" value="Download"/> <input type="button" value="Add to cart"/>
Server Image (OVF10) for VmWare ESXi(4.x & 5.0) platform (CSPC 2.1T1)- include rules package 3.11	PSS-CSPCServer-2.1T1-ESXi-OVF10.ova	15-MAR-2013	5325.20 MB	<input type="button" value="Download"/> <input type="button" value="Add to cart"/>
Server Image (ISO) for Intel based (incl. UCS M2) machines (CSPC 2.1T1)- include rules package 3.11	PSS-CSPCServer-2.1T1-Intel.iso	15-MAR-2013	1592.78 MB	<input type="button" value="Download"/> <input type="button" value="Add to cart"/>
Server Image (VMDK) for VMWare VmPlayer v4.0 platform (CSPC 2.1T1)- include rules package 3.11	PSS-CSPCServer-2.1T1-Player-VMDK.zip	15-MAR-2013	5292.00 MB	<input type="button" value="Download"/> <input type="button" value="Add to cart"/>

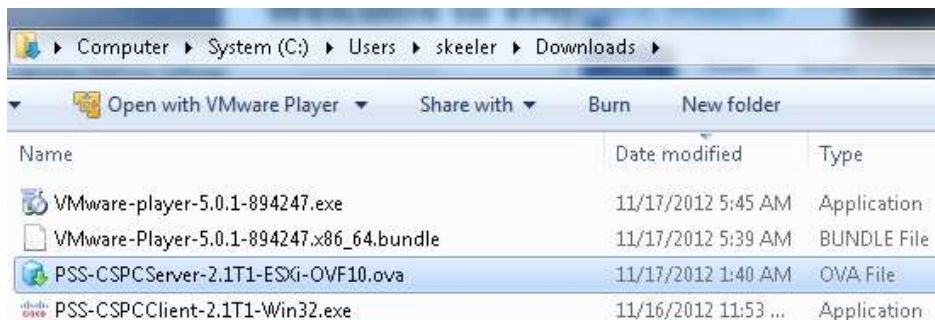
- Find the PSS-CSPCServer-2.1T1-ESXi-OVF10.ova file and click the corresponding Download button.



Note For more information on the download processes go to [Accessing Release PSS 1.0](#).

Install VMware vSphere Hypervisor ESXi 4.x

To install the VMware vSphere Hypervisor ESXi 4.x, perform the following steps:



- Note the folder where you downloaded the **PSS-CSPCServer-2.1T1-ESXi-OVF10.ova** file, that location will be needed when deploying the OVF Template, during the image install process.
- Go to the [Install the CSP-C ESXi image](#) for directions on how to install the ESXi image.

Additional Resources

This section contains a list of additional resources:

- Make sure your hardware is compliant by referring to the [Hardware Compatibility Guide](#).
- [Installing ESXi/ESX 4.1 and vCenter Server 4.1 best practices \(1022101\)](#).
- For disk space see [Recommended disk or LUN sizes for VMware ESX/ESXi installations \(1026500\)](#) .

ESXi 5.0

This section provides information on the following areas:

- [System Requirements](#)
- [Download the VMware vSphere Hypervisor ESXi 5.x Smart Collector Image](#)
- [Install the VMware vSphere Hypervisor ESXi 5.x](#)
- [Additional Resources](#)

System Requirements

To ensure the proper installation and operation of VMware based smart collector environment on your machine, verify that all of the following requirements are met before proceeding.

64-bit Processor

These are the requirements for a 64-bit Processor:

- ESXi 5.0 installs and run only on servers with 64-bit x86 CPUs.
- ESXi 5.0 requires a host machine with at least two cores.
- ESXi 5.0 supports only LAHF and SAHF CPU instructions.
- Known 64-bit processors:
 - All AMD Opteron processors
 - All Intel Xeon 3000/3200, 3100/3300, 5100/5300, 5200/5400, 5500/5600, 7100/7300, 7200/7400, and 7500 processors

RAM

The RAM requirements are 2 GB RAM minimum.

Network Adapters

There can be one or more Gigabit or 10 GB Ethernet controllers. For a list of supported network adapter models, see the [VMware Compatibility Guide](#).

SCSI Adapter, Fibre Channel Adapter or Internal RAID Controller

The supported network adapters include any combination of one or more of the following controllers:

- Basic SCSI controllers. Adaptec Ultra-160 or Ultra-320, LSI Logic Fusion-MPT, or most NCR/Symbios SCSI.
- RAID controllers. Dell PERC (Adaptec RAID or LSI MegaRAID), HP Smart Array RAID, or IBM (Adaptec) ServeRAID controllers.

Installation and Storage

The Installation and Storage requirements are:

- SCSI disk or a local, non-network, RAID LUN with unpartitioned space for the virtual machines.
- For Serial ATA (SATA), a disk connected through supported SAS controllers or supported on-board SATA controllers. SATA disks will be considered remote, not local. These disks will not be used as a scratch partition by default because they are seen as remote.

ESXi 5.0 supports installing on and booting from the following storage systems:

- SATA disk drives. SATA disk drives connected behind supported SAS controllers or supported on-board
- SATA controllers. Supported SAS controllers include:
 - LSI1068E (LSISAS3442E)
 - LSI1068 (SAS 5)
 - IBM ServeRAID 8K SAS controller
 - Smart Array P400/256 controller
 - Dell PERC 5.0.1 controller
- Supported on-board SATA include:
 - Intel ICH9
 - NVIDIA MCP55
 - ServerWorks HT1000
- Serial Attached SCSI (SAS) disk drives. Supported for installing ESXi 5.0 and for storing virtual machines on VMFS partitions.
- Dedicated SAN disk on Fibre Channel or iSCSI
- USB devices. Supported for installing ESXi 5.0. For a list of supported USB devices, see the [VMware Compatibility Guide](#).

Download the VMware vSphere Hypervisor ESXi 5.x Smart Collector Image

To Install the VMware vSphere Hypervisor ESXi 5.x smart collector onto a Windows Host Machine, go to the following URL:

<http://www.cisco.com/cisco/software/release.html?mdfid=283114009&catid=268439477&softwareid=283308676&release=Collector%20Server&rellifecycle=&relind=AVAILABLE&reltype=all>; the Release Collector Server images appear.

Download Software

 Download Cart (0 items) [\[-\]Feedback](#) [Help](#)







[Downloads Home](#) > [Products](#) > [Cloud and Systems Management](#) > [Cisco Services](#) > [Cisco Smart Collector](#) > [Smart collector](#) > [Smart Collector Software-Collector Server](#)

Smart collector

Release Collector Server

[Expand All](#) | [Collapse All](#)

- ▼ Latest Releases
 - Collector Server
- ▼ All Releases
 - ▼ PSS 1.0
 - Collector Server
 - Other Files
 - Collector Client

File Information	4.x & 5.0) platform	Release Date	Size	
Server Image (OVF10) for VmWare ESXi(4.x & 5.0) platform (CSPC 2.2)- includes latest rules package 	PSS-CSPCServer-2.2-ESXi-OVF10.ova	17-MAY-2013	7340.83 MB	<input type="button" value="Download"/> <input type="button" value="Add to cart"/>
Server Image (ISO) for Intel based (incl. UCS M2) machines (CSPC 2.2)- includes latest rules package 	PSS-CSPCServer-2.2-Intel.iso	17-MAY-2013	2489.26 MB	<input type="button" value="Download"/> <input type="button" value="Add to cart"/>
Server Image (ISO) for Cisco UCS C2xx M3 machines with SATA drives (CSPC 2.2)- includes latest rules package 	PSS-CSPCServer-2.2-UCSM3.iso	17-MAY-2013	2933.60 MB	<input type="button" value="Download"/> <input type="button" value="Add to cart"/>
Server Image (OVF10) for VmWare ESXi(4.x & 5.0) platform (CSPC 2.1T1)- includes rules package 3.11 	PSS-CSPCServer-2.1T1-ESXi-OVF10.ova	15-MAR-2013	5325.20 MB	<input type="button" value="Download"/> <input type="button" value="Add to cart"/>
Server Image (ISO) for Intel based (incl. UCS M2) machines (CSPC 2.1T1)- includes rules package 3.11 	PSS-CSPCServer-2.1T1-Intel.iso	15-MAR-2013	1592.78 MB	<input type="button" value="Download"/> <input type="button" value="Add to cart"/>
Server Image (VMDK) for VMWare VmPlayer v4.0 platform (CSPC 2.1T1)- includes rules package 3.11 	PSS-CSPCServer-2.1T1-Player-VMDK.zip	15-MAR-2013	5292.00 MB	<input type="button" value="Download"/> <input type="button" value="Add to cart"/>

- Find the PSS-CSPCServer-2.1T1-ESXi-OVF10.ova file and click the corresponding Download button.



For more information on the download processes go to [Accessing Release PSS 1.0](#).

Install the VMware vSphere Hypervisor ESXi 5.x

To install the VMware vSphere Hypervisor ESXi 5.x, perform the following steps:



- Note the folder where you downloaded the **PSS-CSPCServer-2.1T1-ESXi-OVF10.ova** file, that location will be needed when deploying the OVF Template, during the image install process.
- Go to the [Install the CSP-C ESXi image](#) for directions on how to install the ESXi image.

Additional Resources

This section contains a list of additional resources:

- Make sure your hardware is compliant by referring to the [Hardware Compatibility Guide](#).
- [vSphere Installation and Setup 5.0](#).
- For disk space requirements, see [Recommended disk or LUN sizes for VMware ESX/ESXi installations \(1026500\)](#).

Install the CSP-C ESXi image

To install the downloaded VMware vSphere Hypervisor ESXi x.x Smart Collector Image, perform the following steps:



The install process for ESXi 4.x and 5.x files are the same.

The screenshot displays the vSphere Client interface for a VMware ESXi host. The main content area is divided into several sections:

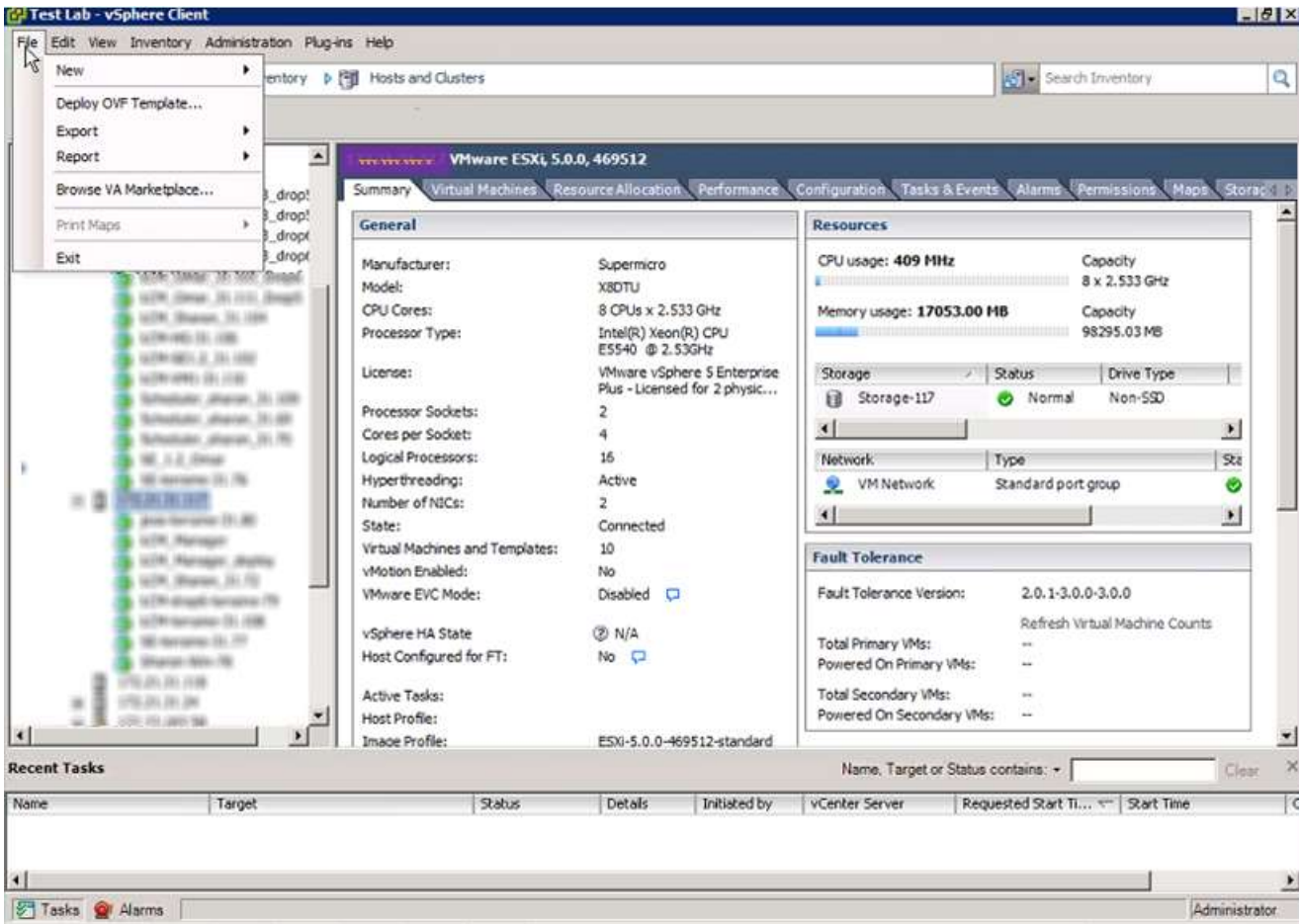
- General:**
 - Manufacturer: Supermicro
 - Model: X8DTU
 - CPU Cores: 8 CPUs x 2.533 GHz
 - Processor Type: Intel(R) Xeon(R) CPU E5540 @ 2.53GHz
 - License: VMware vSphere 5 Enterprise Plus - Licensed for 2 physic...
 - Processor Sockets: 2
 - Cores per Socket: 4
 - Logical Processors: 16
 - Hyperthreading: Active
 - Number of NICs: 2
 - State: Connected
 - Virtual Machines and Templates: 10
 - vMotion Enabled: No
 - VMware EVC Mode: Disabled
 - vSphere HA State: N/A
 - Host Configured for FT: No
 - Active Tasks:
 - Host Profile: ESXi-5.0.0-469512-standard
- Resources:**
 - CPU usage: 409 MHz (Capacity: 8 x 2.533 GHz)
 - Memory usage: 17053.00 MB (Capacity: 98295.03 MB)
 - Storage: Storage-117 (Status: Normal, Drive Type: Non-SSD)
 - Network: VM Network (Type: Standard port group)
- Fault Tolerance:**
 - Fault Tolerance Version: 2.0,1-3.0,0-3.0,0
 - Total Primary VMs: --
 - Powered On Primary VMs: --
 - Total Secondary VMs: --
 - Powered On Secondary VMs: --

At the bottom of the interface, there is a 'Recent Tasks' section with a search bar and a table with columns: Name, Target, Status, Details, Initiated by, vCenter Server, Requested Start Time, and Start Time.

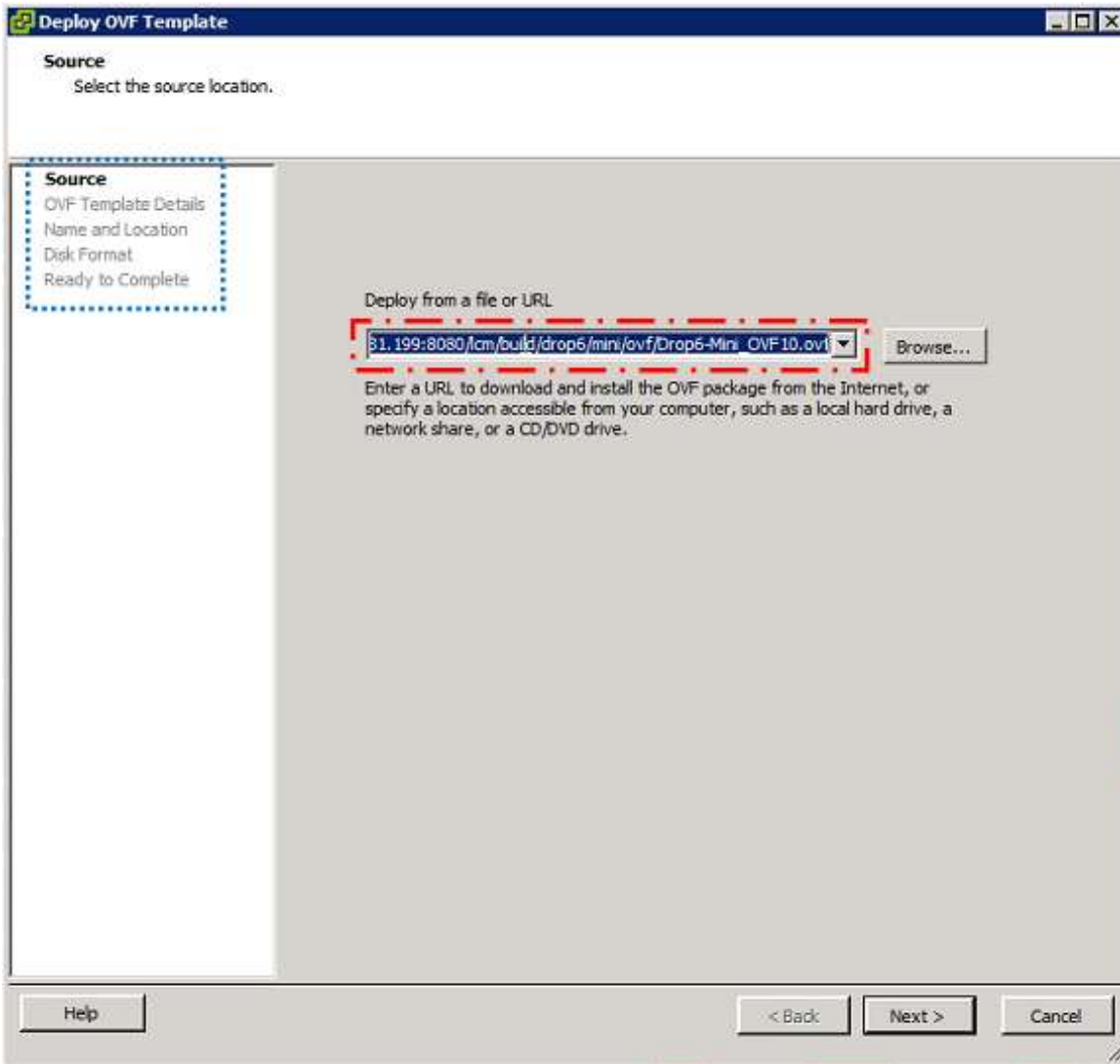
- Open the vSphere client and select which device to use.



The XXXXXXXXXX is being used to blank out the network IP addresses.



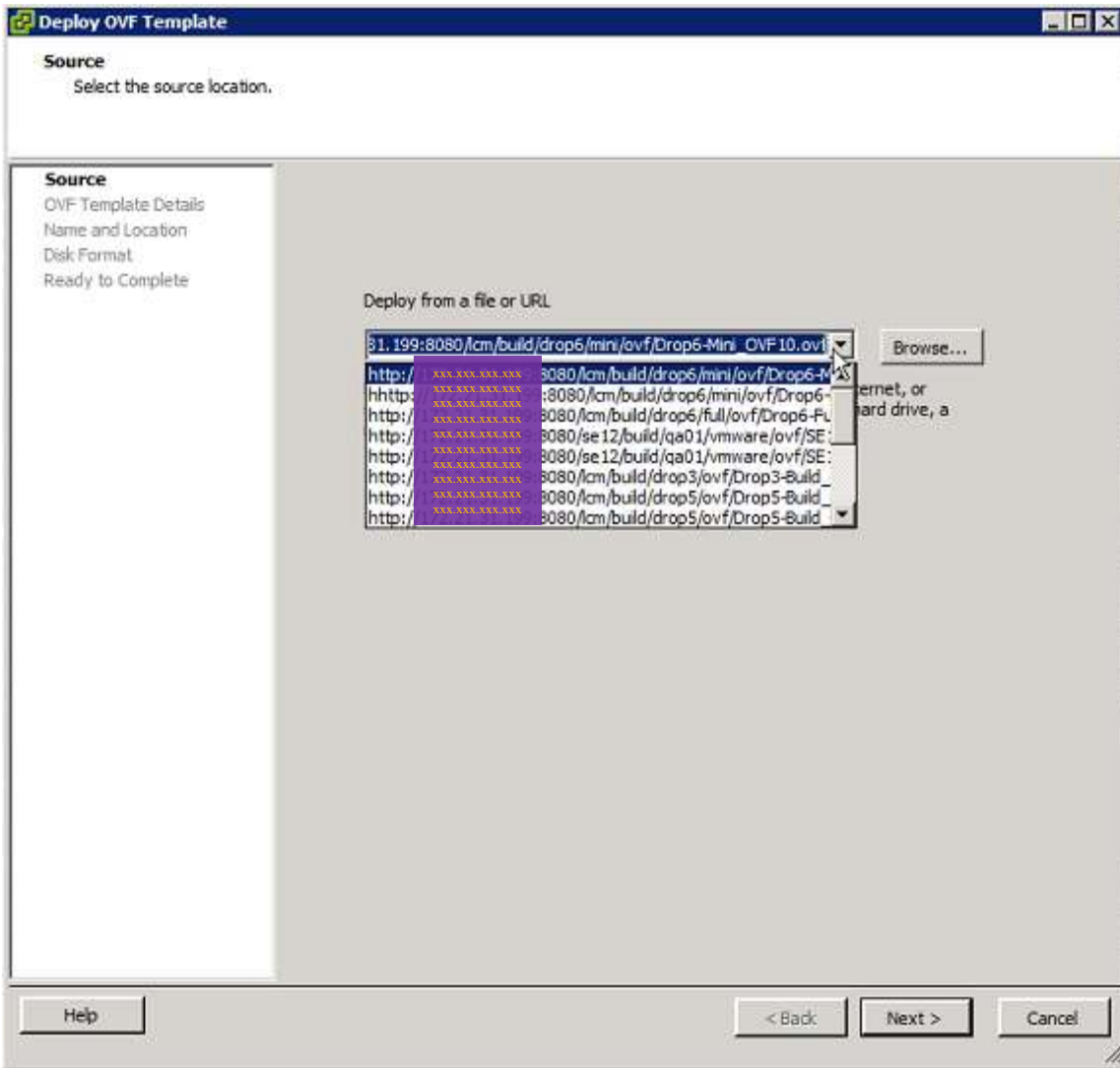
- On the menu choose **File > Deploy OVF Template...**; the Deploy OVF Template window appears with the source information.



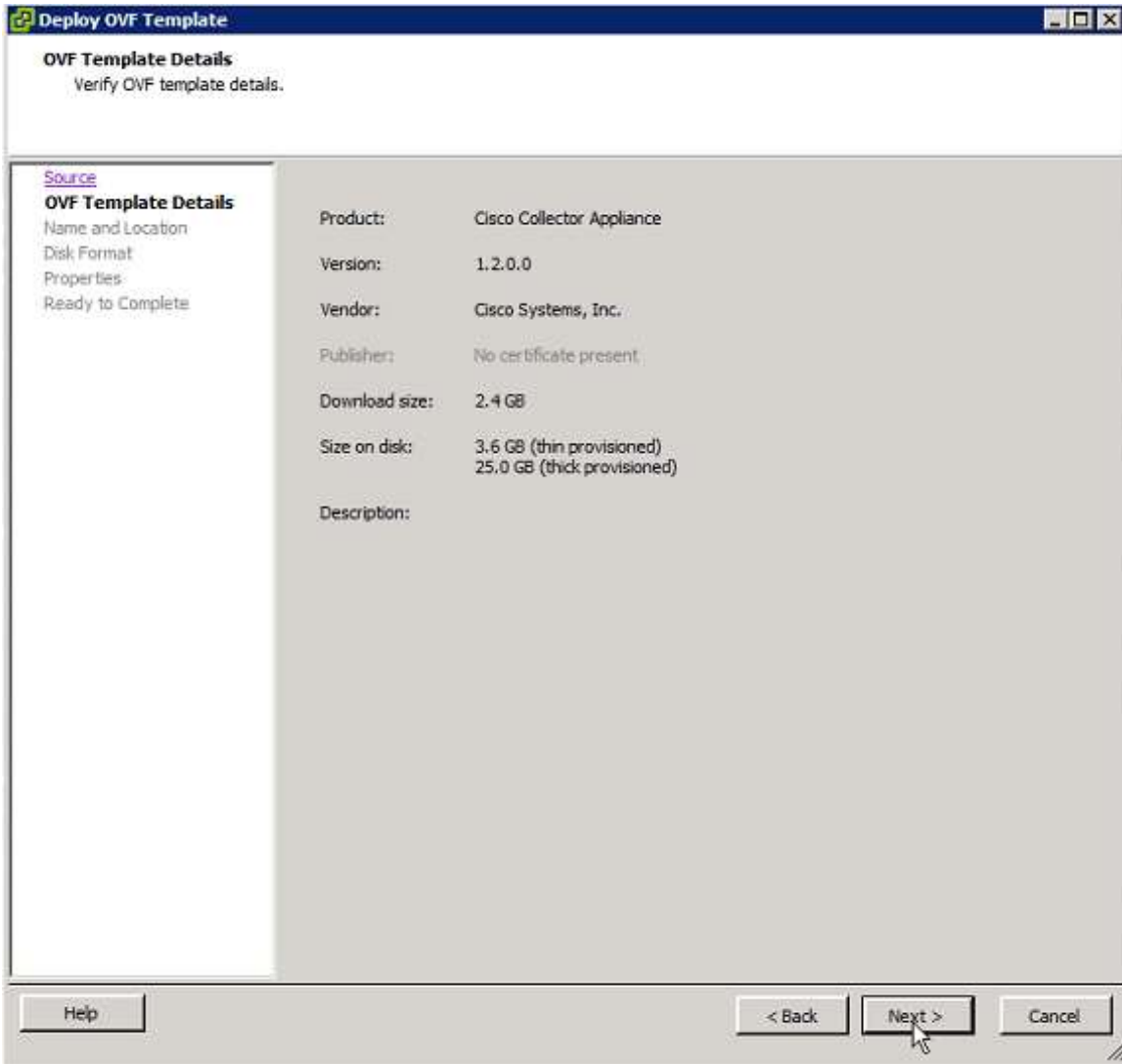
- The drop-down list shows the location where the image is.



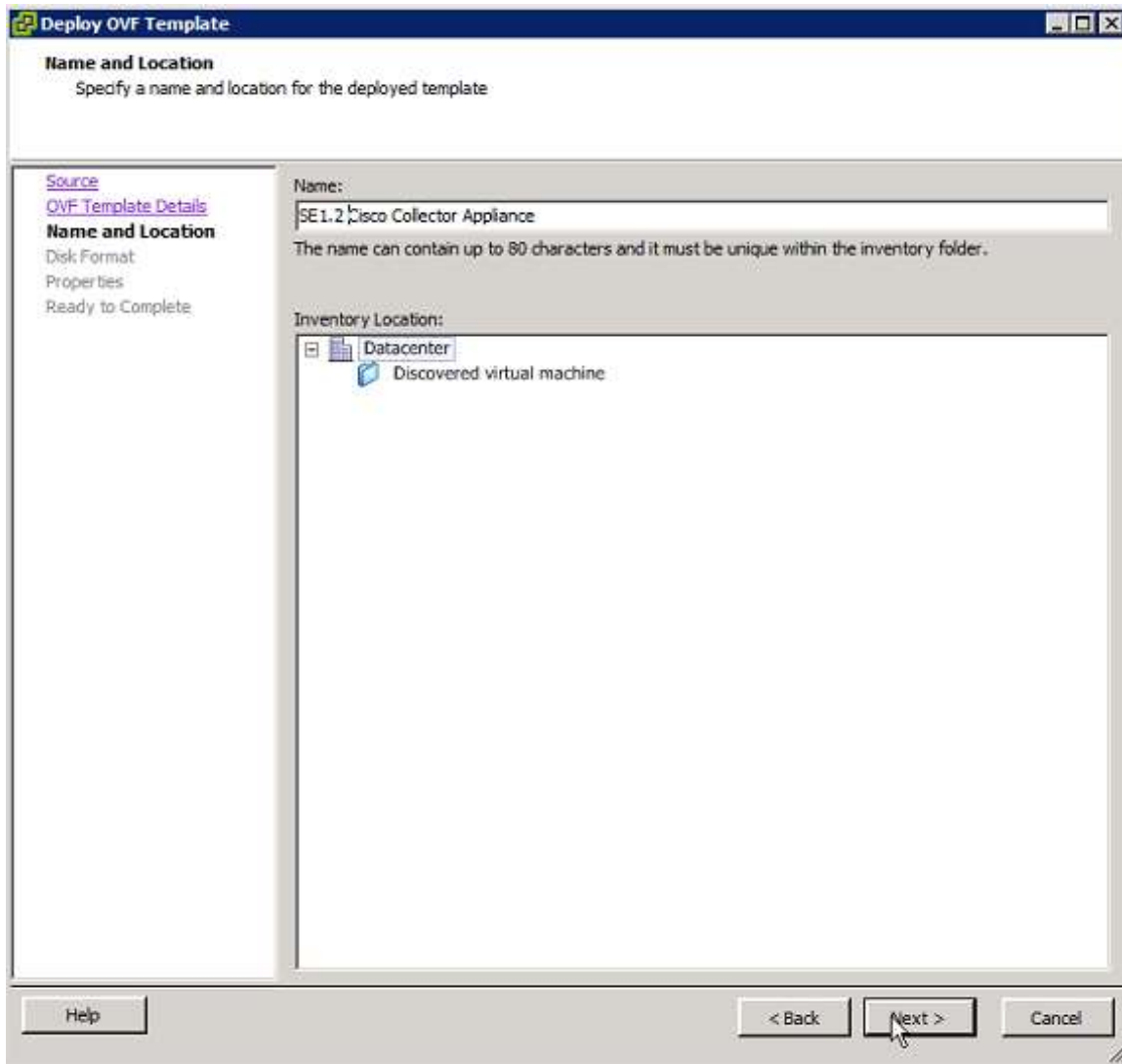
Note The navigation menu on the left indicates where you are in the Deploy OVT Template process, for example, this part is the **Source** process, which appears in bold.



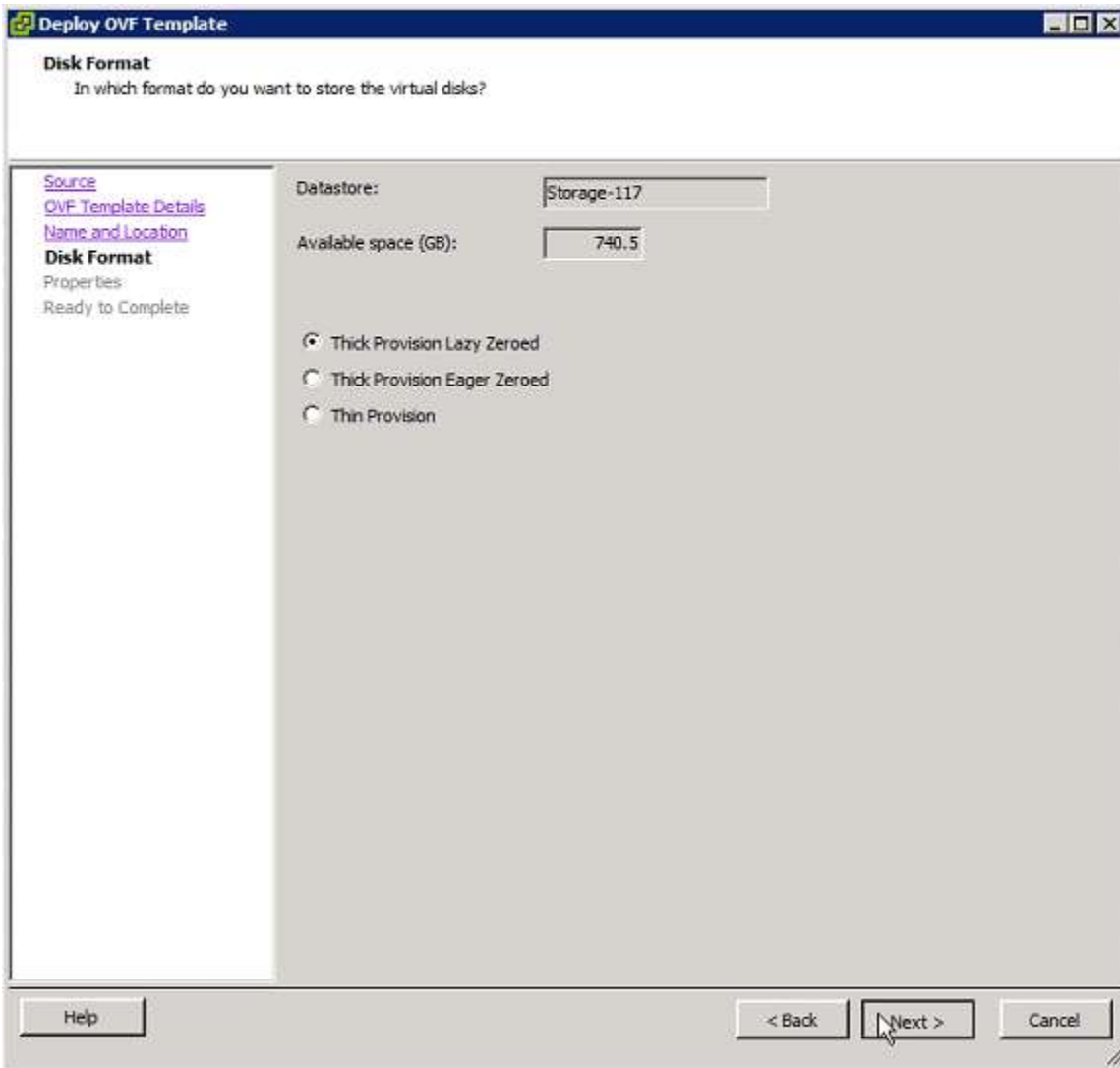
- If this is not the correct location, then perform one of the following tasks:
 - Click the drop-down list button and select one of the other locations.
 - Click the adjacent **Browse** button and specify the correct location.
- After specifying the correct file location, then click **Next**; the OVT Template Details section appears.



- The OVT Template Details section provides information about the previously selected image. Click **Next**; the Name and Location section appears.



- In the name field, specify the name you want associated to this image.
- Click **Next**; the Disk Format section appears.



- This section provides information about the Disk Format and lets you change the type provisioning for the selected disk.
- Click **Next**; the Properties section appears.

Deploy OVF Template

Properties
Customize the software solution for this deployment.

[Source](#)
[OVF Template Details](#)
[Name and Location](#)
[Disk Format](#)
Properties
Ready to Complete

Networking Properties

Default Gateway
The default gateway address for this VM. Leave blank if DHCP is desired.

DNS
The domain name servers for this VM (comma separated). Leave blank if DHCP is desired.

Network 1 IP Address
The IP address for this interface. Leave blank if DHCP is desired.

Network 1 Netmask
The netmask or prefix for this interface. Leave blank if DHCP is desired.

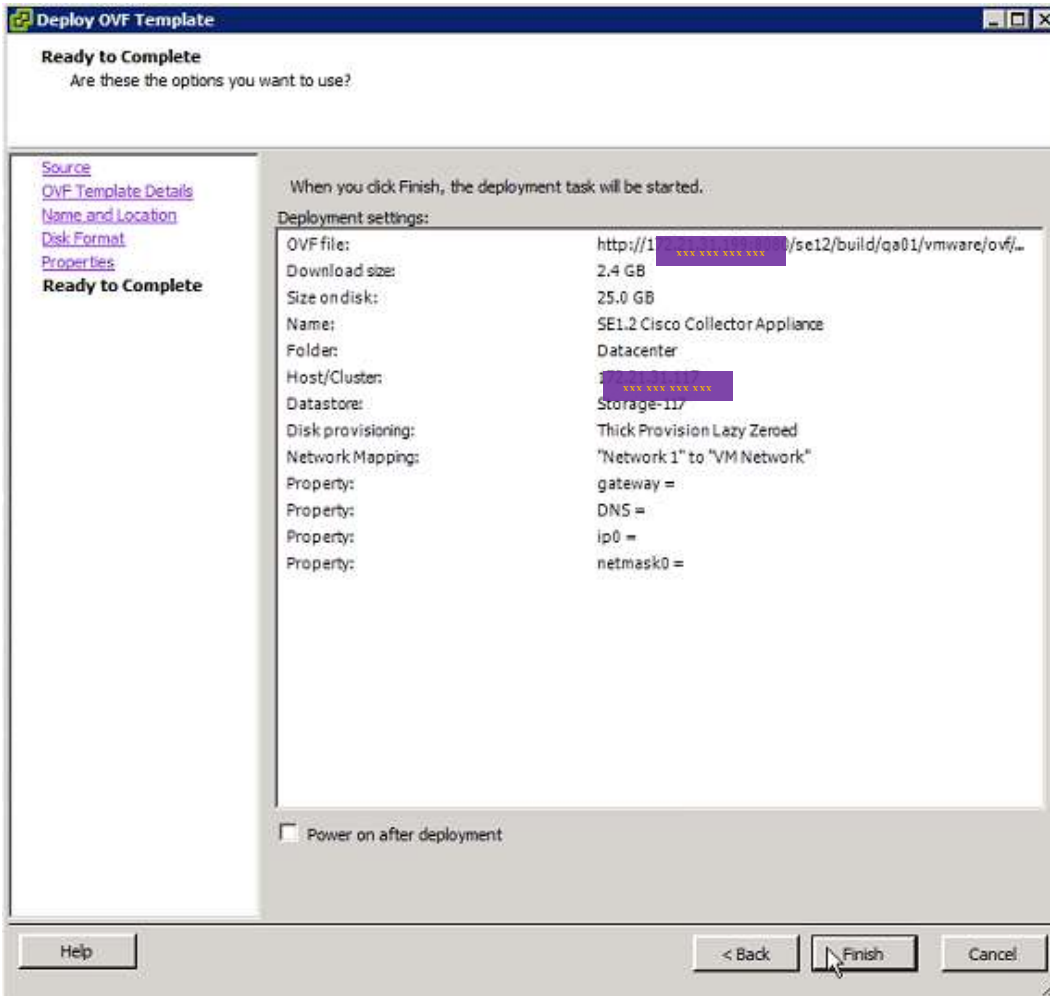
Help < Back Next > Cancel

- The Networking Properties section has fields for specifying different networking properties; however, no information specified here will be configured.

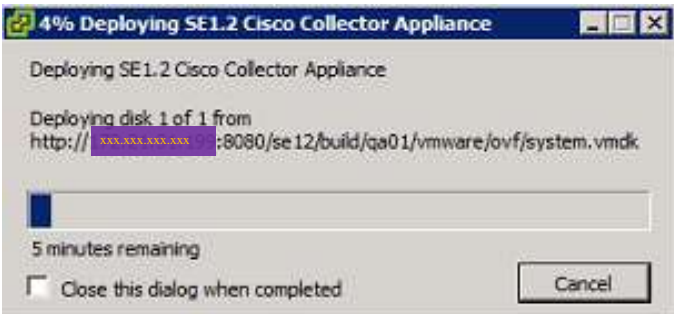


Note Please leave the entries blank for Network Properties. The appliance network configuration will be done via the Admin shell once the appliance is booted. Any information specified here will NOT be used.

- Click **Next**; the Ready to Complete section appears.



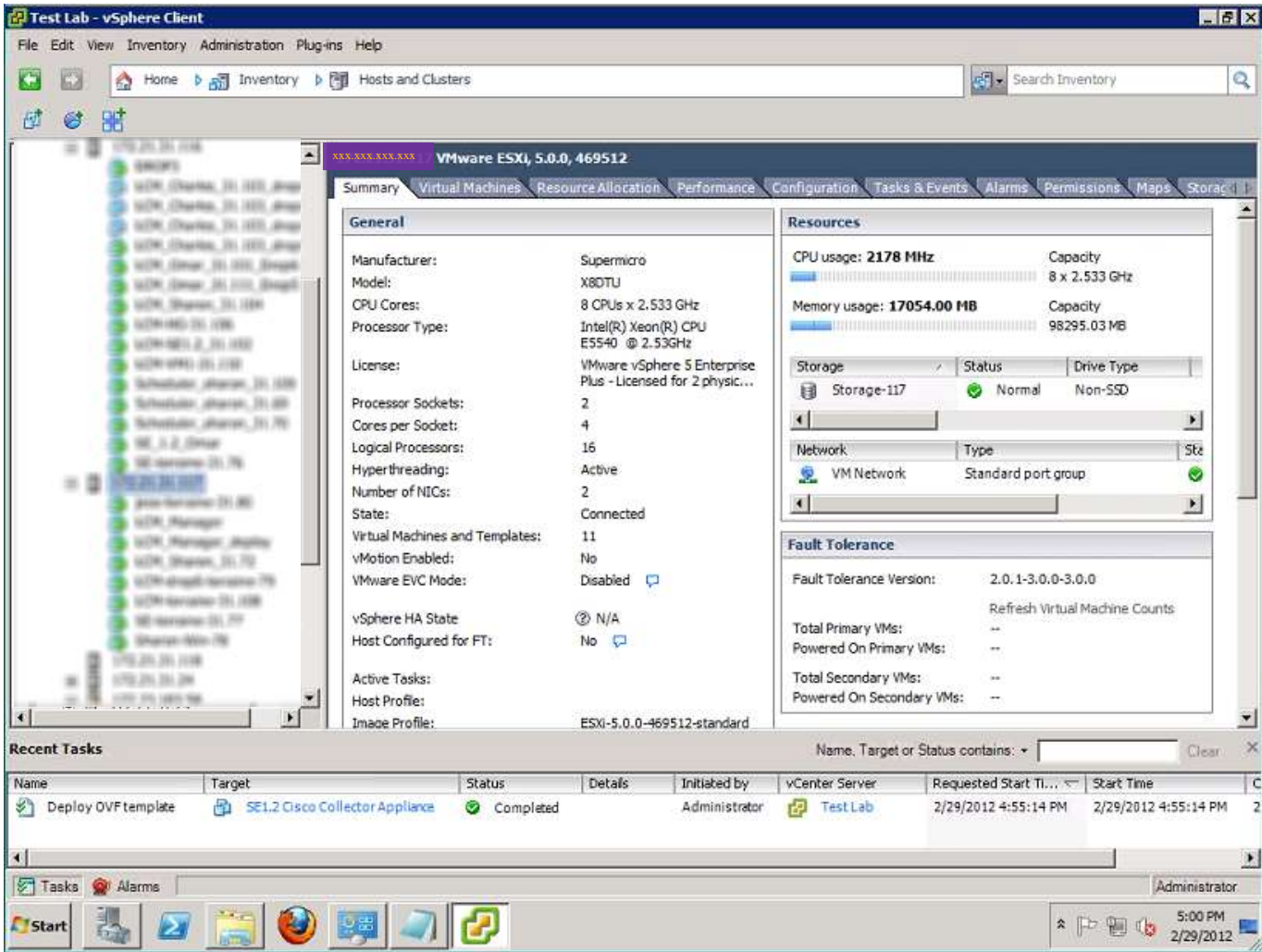
- This section provides a summary of all the previously accepted information.
- Review the list and go back to the respective section if something needs to be changed, otherwise, click **Finish**; a status window appears indicating the progress of the deployment.





Note The deployment could take several minutes, depending on the size of the file.

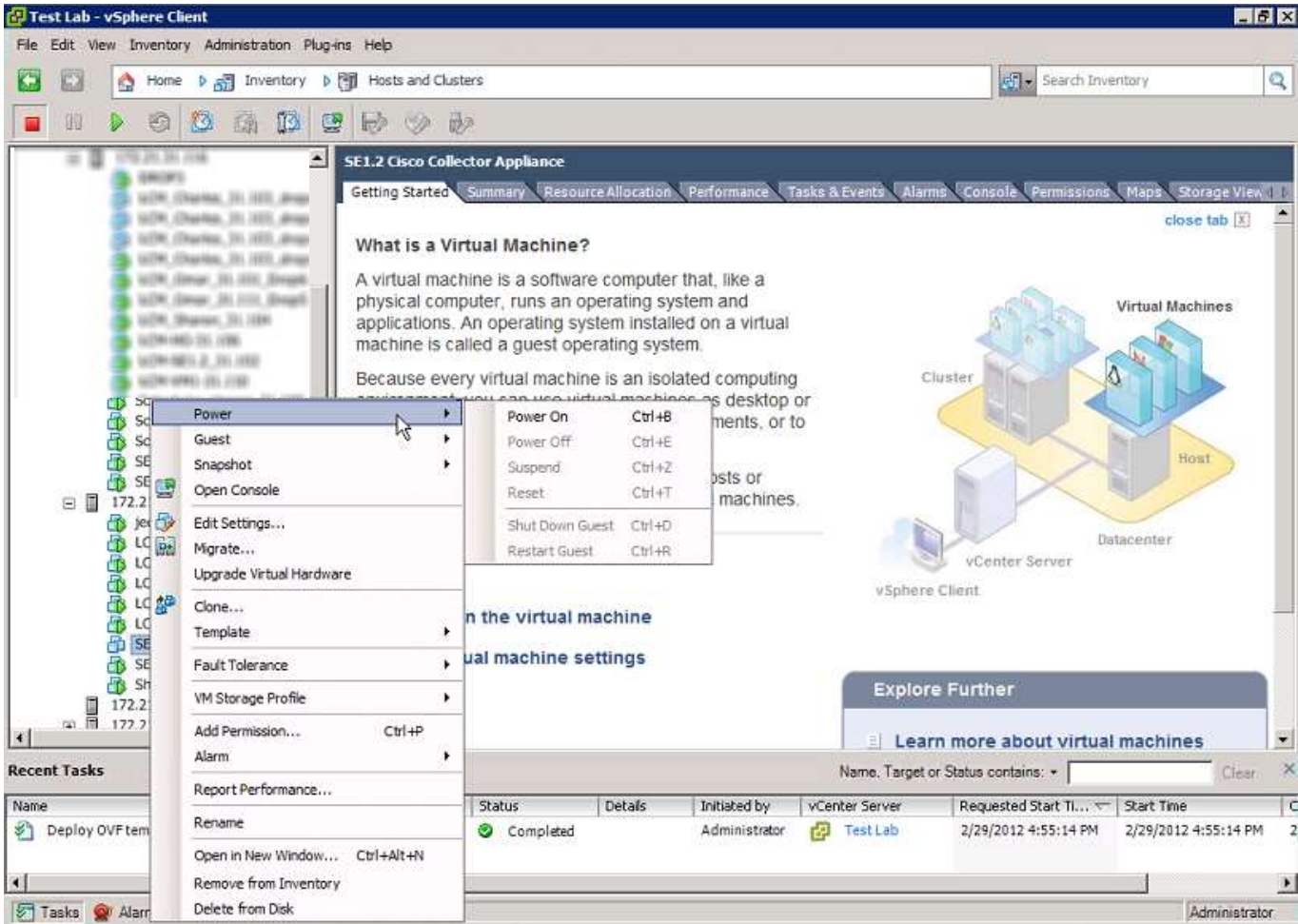


- After the deployment is finished, a Deployment Completed Successfully information window appears.
- Click the **Close** button.

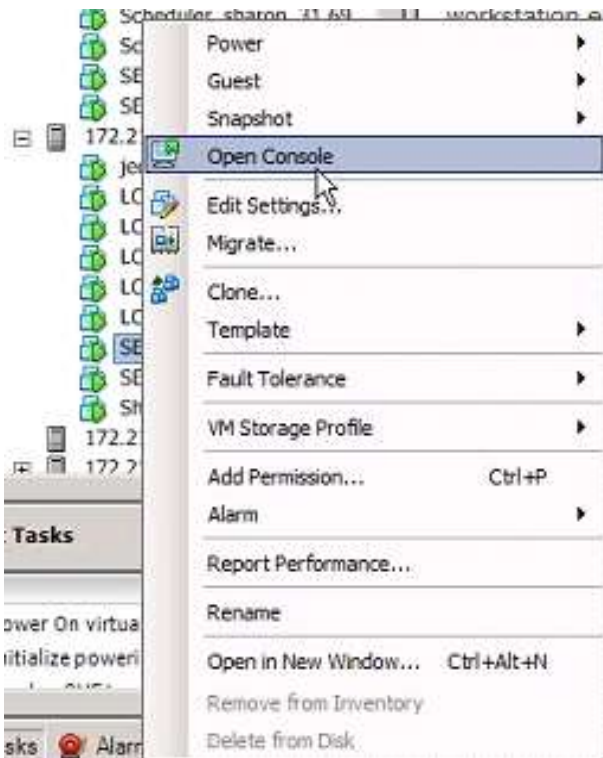


Several new items can be seen as a result of the deployment:

- The Recent tasks section displays the Deploy OVT Template task and associated information.
- The name appears in the list under the corresponding device
- The color of the icon indicates if the device is powered on:
 - If the icon is blue,  then the device is powered off.
 - If the icon is green,  then the device is powered on.



- To power on the device, right-click the appliance name, in the pop-up menu choose **Power > Power On** or press keys **Ctrl+B**.



- After powering on the device, click **Open Console**; the console window appears.


```

SE1.2 Cisco Collector Appliance on xxx.xxx.xxx.xxx
File View VM
Number of active connections has changed. There are now 2 active connections to this console
Your authentication has been saved in /root/.ssh/id_rsa.pub.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
07:67:b7:0c:2b:f8:b5:45:a7:1d:10:3c:50:66:6e:02 root@localhost.localdom
[ OK ]
Starting system logger: [ OK ]
Starting kernel logger: [ OK ]
iscsid (pid 1343) is running...
Setting up iSCSI targets: iscsiadm: No records found! [ OK ]
Starting acpi daemon: [ OK ]
[IPTABLES DROP] : IN=eth0 OUT= MAC=00:50:56:b1:20:03:00:00:00:00:00:00:00:00:00 SRC
=10.0.0.0 DST=224.0.0.1 LEN=36 TOS=0x00 PREC=0x00 TTL=1 ID=0 OPT (94040000) PROT
D=2
Starting cups: [ OK ]
Starting xinetd: [ OK ]
Starting Common Services Platform Collector:
Starting MySQL. [ OK ]
Starting CSPC Helper Servers (tftp & syslog):
Starting Base Collector and add-ons Starting cron: [ OK ]
Starting atd: [ OK ]
Starting yum-updatesd: [ OK ]
Starting Avahi daemon... _


```

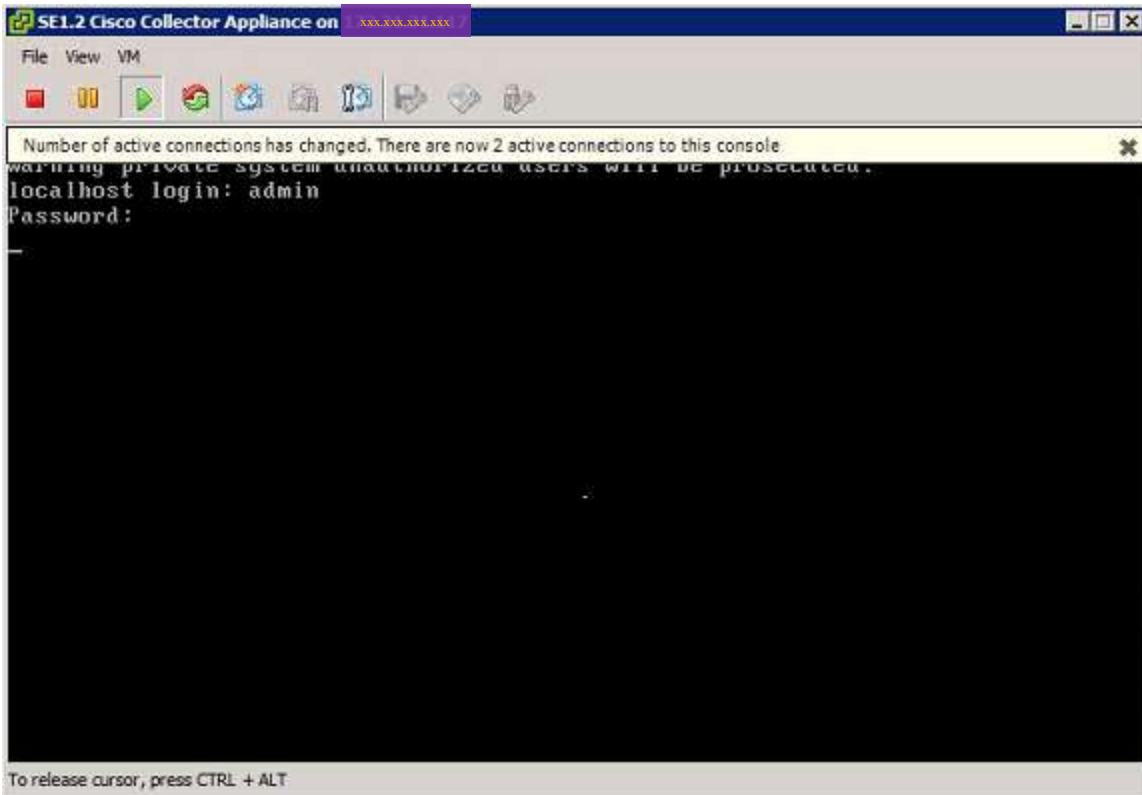


Note

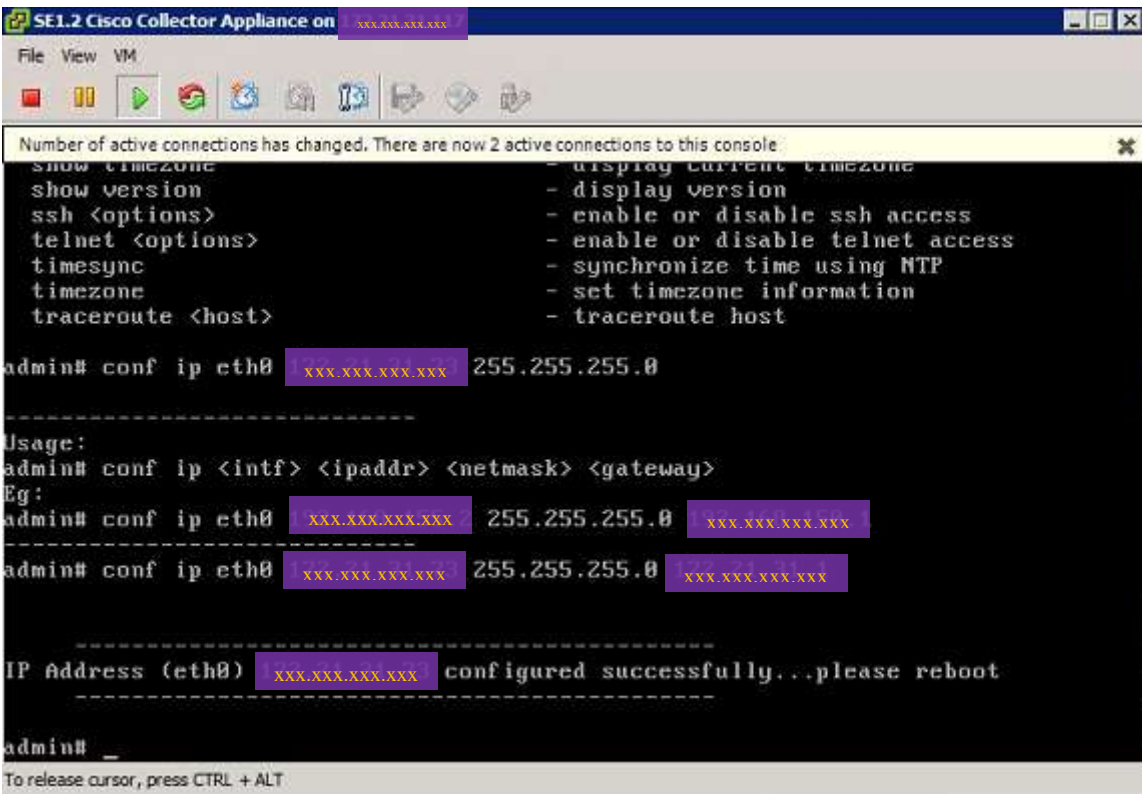
Some versions of vSphere client have a problem under the console. The console shows only the bottom portion of the display. For example if on a vSphere client you enter a “?” to see list of all the CLI commands, the list of commands scrolls by and you see only bottom portion of command list, you have no scroll bar to scroll up to see top part of command list.

To currently get around this problem use an SSH client and connect to the CSP-C server and enlarge the window or use the scroll bar on the right to scroll upward.

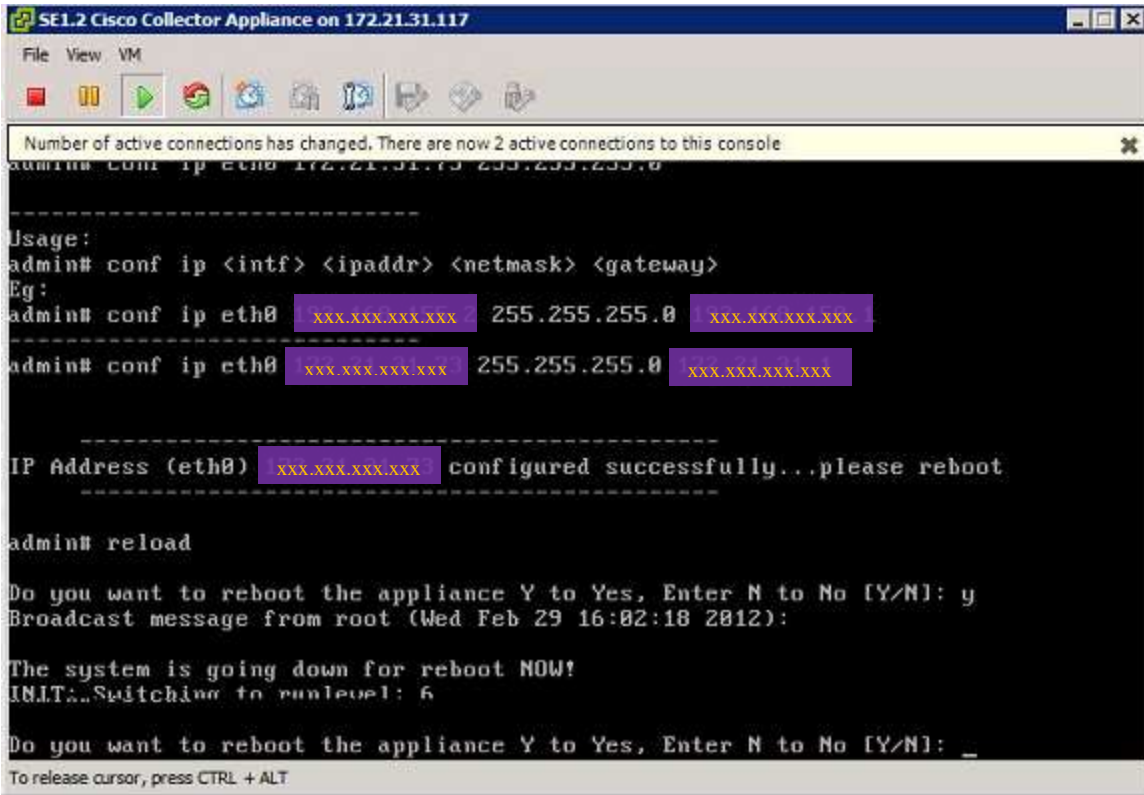
- The initialization process is displayed in the console window; also the numbers of active connections to the console are identified. 



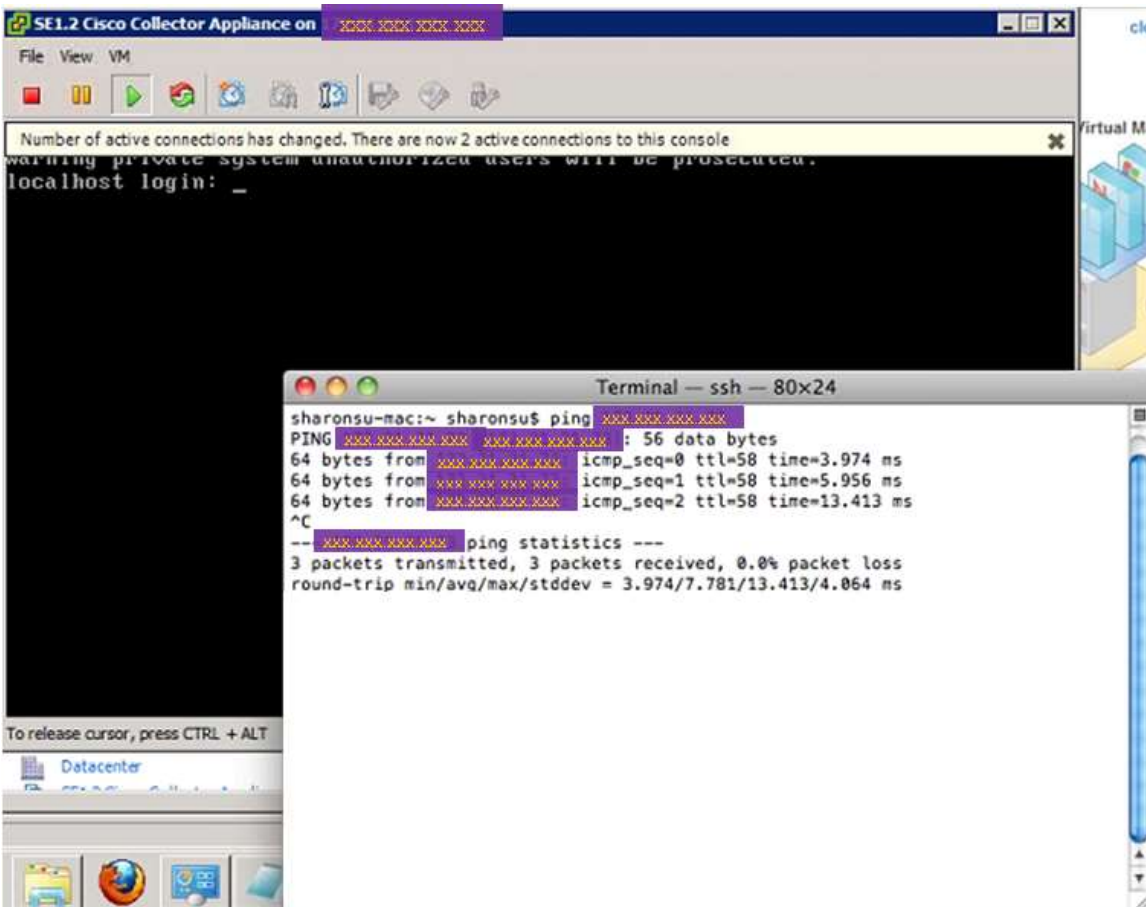
- After the initialization completes, login with your credentials.



- Configure the IP address using the **conf ip** command.



- After the configuration is complete, then reboot the device using the **reload** command. After the reload, log back in and the interface and associated IP address will be active.



- Ping the new added IP address, from another device, to verify that the new interface and IP address are active.

Configure VMware Smart Collector IP Address

To configure the IP address of the VMware smart collector, perform the following steps:

- Login to the VMware smart collector via connected console using cisco/cisco account/password.



Note Cisco recommends that you change the default password, after your initial log in.

- When you login to the VMware smart collector using cisco/cisco, you will see the following screen that lists the supported CLI commands.

```

?                - print the list of available commands
about            - about appliance
apply *          - install updates for Appliance components
check update *  - check availability of updates for Appliance components
clear history * - purge command history for user/s
clrscr*         - clear current screen/s
collector <start/stop/status/restart - collector start/stop/status/restart
conf autoupdate * - configure auto-update policy
conf date *     - configure date and/or time
conf dhcp <intf> - configure dhcp
conf dns [-ad] * - configure DNS server(s)
conf ip *       - configure static IP
conf proxy *    - configure proxy server
conf server-connection * - configure connection with server used for updates
connectivity direct-mode <enable/disable> - enable or disable connectivity direct-mode
delete autoupdate * - delete configured auto-update policy
dmidecode *    - view SMBIOS table
download *     - download updates for Appliance components
exit           - exits from this session
firewall <enable/disable> - enable/disable firewall rules
history-size <number> * - sets the maxsize for history file
hostname <hostname> - change hostname
logout        - logout from this session
passwd       - change user passwd
ping *       - view ping details
poweroff    - shutdown and power off the system
proxy <enable/disable/clear> - enable/disable or clear proxy
pwdreset <user> <expiry_interval> - reset cisco/admin user passwd to random string for a specified no of days
reboot     - reboot the system
reload    - reboot the system
route [-ad] <intf> <network/mask> < - add static route to a network
show apply * - display status of apply operation
show autoupdate * - display details of configured auto-update policy
show connectivity direct-mode - display status of connectivity direct-mode
show date - display date and time information
show download * - display status of download operation
show firewall - display the firewall rules
show history * - display command history for user/s and size of the history file
show hostname - display hostname
show ipconfig - display network configuration
show logs * - display logs
show monitor - display appliance status(cpu, memory, disk)
show route - display configured routes
show server-connection - display details of connection with server used for updates
show timesync - display current NTP sync interval and last update time
show timezone - display current timezone
show version * - display version for servicepack/Jeos
ssh <enable/disable> - enable or disable ssh access
sudo <command> - run linux command with sudo
telnet <enable/disable> - enable or disable telnet access
timesync * - synchronize system time with NTP server and configure NTP synchronization interval
timezone - set timezone information
traceroute <host> - traceroute host

admin#

```



Note Some vSphere consoles have a problem letting you see previously displayed console information. For more details on how to work around this issue see [vSphere client console problem](#).

- To assign the IP address for the VMware smart collector, at the command prompt (cisco>) enter: **passwd** to change the password.
- Enter the enable password, which is **admin**; the Administration screen appears.


```

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

?                - print this help
about            - about appliance
collector <options> - collector start/stop/restart
conf dhcp <intf> - dhcp configuration
conf dns *       - configure DNS server(s)
conf ip *        - static IP configuration
date            - show time information
exit            - exit current session
hostname <hostname> - change hostname
logout          - logout from this session
passwd <user>    - change cisco/admin passwd
ping *          - view ping details
poweroff        - shutdown and power off the system
pwdreset <user> - reset cisco/admin user passwd to default
reload          - reboot the system
show addonlog   - display add-on log contents
show adminlog   - display adminshell CLI logs
show collectorlog - display collector log contents
show hostname   - display hostname
show net        - display network configuration
show version    - display version
ssh <options>   - enable or disable ssh access
timesync        - synchronize time using NTP

admin# █

```

- At the command prompt admin#, enter **conf ip** and assign an appropriate IP address for this device.

```

admin# conf ip help
-----
Usage:
admin# conf ip <intf> <ipaddr> <netmask> <gateway>
Eg:
admin# conf ip eth0  xxx.xxx.xxx.xxx 255.255.255.0 xxx.xxx.xxx.xxx
-----
admin# conf ip eth0  xxx.xxx.xxx.xxx 255.255.255.0 xxx.xxx.xxx.xxx

```

- Once the configuration is successful, reboot the device in order to use the newly configured IP address.



Note As noted in the above example, it is recommended that you use the eth0 interface on your hardware to configure the static IP address. If you change the IP address settings for the VMware smart collector, reboot the device using the reload command. When the operating system on the VMware smart collector restarts with its new IP profile, continue with the rest of the configuration.

- Users can also configure the IP address using the DHCP command (which is enabled by default). At the command prompt admin# enter **conf dhcp eth0** (e.g. **admin# conf dhcp eth0**)



Note As noted in the above example, it is recommended that you use the eth0 interface for DHCP IP address configuration. Also, the user should make sure that the DHCP server is running in your network so that it can provide a DHCP IP address to the target hardware.

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

Fig 7.4 DHCP Address configuration



Note If you change the IP address settings for the VMware smart collector, reboot the system using the reload command. When the operating system on the VMware smart collector restarts with its new IP profile, continue with the rest of the configuration.

Important From this point you can continue with the next step in the CSP-C Registration directions by going to the next section, [CSP-C Registration](#).

CSP-C Registration

A CSP-C registration needs to be performed before the collector can be utilized by the Cisco smart portal. The registration allows a validation to occur that creates a connection between the CSP-C collector and the Cisco Backend. The registration process also requires you to obtain the [entitlement files](#) (a security certificate and other registration files). The entitlement files are used later to complete the CSP-C installation.

There are two parts to the CSP-C registration on the Cisco smart portal:

- [Register the CSP-C](#)
- [Download the Certificate](#)

To register a CSP-C, and obtain the entitlement files, perform the following steps:

Register the CSP-C

- Go to the Cisco smart portal application at URL: <https://tools.cisco.com/csp/>; the Cisco smart portal Log In window opens.

Log In

Existing User	New User
<p>User Name:</p> <input type="text"/>	<p>There are various levels of access depending on your relationship with Cisco. Review the user benefits and find the level that is most appropriate for you.</p> <p>Registered Guest</p> <p>Partner & Reseller</p> <p>Registered Customer</p>
<p>Password:</p> <input type="password"/> <input type="button" value="Log In"/>	
<p>Forgot your password?</p>	<p><input type="button" value="Register Now"/></p>

- Enter your Cisco.com ID user name and password.
- Click **Log In**; the Cisco smart portal Overview window opens and displays the Overview page.

Overview [User Registration](#) **2** [Smart Collector - Common Services Platform](#)

Smart Portal Overview
Delivering capabilities to discover, collect and analyze network device details and provide network aware information.
[Learn More - Partner Support Service](#)

PSS Support Community
For more up-to-date information and other resources, please visit [PSS Support Community](#). For information about how to get access to this private community, please send e-mail to psscommunity@external.cisco.com.

User Registration
[Self Registration Or Register Users](#)
[Maintain User Registrations](#)

Common Services Platform Collector (CSP-C)
[Register CSP-C](#) **1**
[Manage Collectors](#)

Installed Base Management, Alerts and Diagnostics
[Reports](#)

Resources
[PSS Smart Portal Training](#)
[PSS API Console](#)

Download
[User Guide](#)
[Smart Collector - Common Services Platform Software](#)

- On the Smart Portal Overview page, click one of the following items:
 - [Register CSP-C](#) ①
 - [Smart Collector- Common Services Platform tab](#) ②
- Clicking either of the above options displays the Smart Collector- Common Services Platform page; by default this page displays all the registered CSP-C's, if any have been registered.

- On the Smart Collector - Common Services Platform page, click **New Request**; ③ the CSP-C Registration view appears.

- Enter all the required information, which is designated by a red asterisk *.



Note Enter information that is relevant to the device/site, which will make finding/working with the device easier in the future. For the Site ID you can either manually enter the id or select one from the drop-down list. ①

For actual physical collectors, the serial number information ② can be obtained from the invoice or from the paperwork that came with the device; however, the best source for the serial number is from the actual device.

The serial number for the collector can use only the following characters: 1... 0, a... Z. Specifically, no special characters are to be used.

For virtual collectors (those using VMware) a good serial number ② could use the date and time, for example, *PartnernameYYMMDDHHMMSS*.



Note The serial number is used to help the partner identify a particular collector. Quite often part of the serial number is related to a location or customer. Basically the serial number can be anything you want it to be to assist you with collector identification and management.

- Click **Submit**; a message appears indicating that the submission was successful and instructs you to download a certificate. An email, which includes the details related to CSP-C and a link to download the [registration zip file](#), is sent to the end user.

Overview User Registration Smart Collector - Common Services Platform Smart Collector - Embedded

13/AUG/2010: REG-INFO-83001: Your CSP-C registration has been submitted successfully. To complete the CSP-C installation you will need a Security Certificate & Registration information files, which you can download from [Download Certificate](#)

[New Request](#) Register a new CSP-C

Common Services Platform Collector (CSP-C) Registrations										
	CSP-C NAME	APPLIANCE ID	ENTITLED COMPANY	REGISTRATION STATUS	SITE ID	INVENTORY NAME	CREATED ON	CREATED BY	UPDATED BY	LAST UPDATE
<input type="radio"/>	CSP-C doctest	CSP0000000461	CISCO SYSTEMS	Completed	RTP-Bldg 10	cisco devices	13/Aug/2010	Sch Test		
<input type="radio"/>	JUNKED_schellaTest	CSP0000000142	CISCO SYSTEMS	Completed	N/A	schellaTest	22/Jun/2010	Sch Test		

[Download Certificate](#) [Update](#) [Delete](#)

Download the Certificate

Downloading a certificate provides you entitlement files, a security certificate and other registration related files that are used when [installing the CSP-C entitlement file](#). To download a certificate, perform the following steps:

Overview User Registration Smart Collector - Common Services Platform Smart Collector - Embedded

13/AUG/2010: REG-INFO-83001: Your CSP-C registration has been submitted successfully. To complete the CSP-C installation you will need a Security Certificate & Registration information files, which you can download from [Download Certificate](#) **1**


[New Request](#) Register a new CSP-C

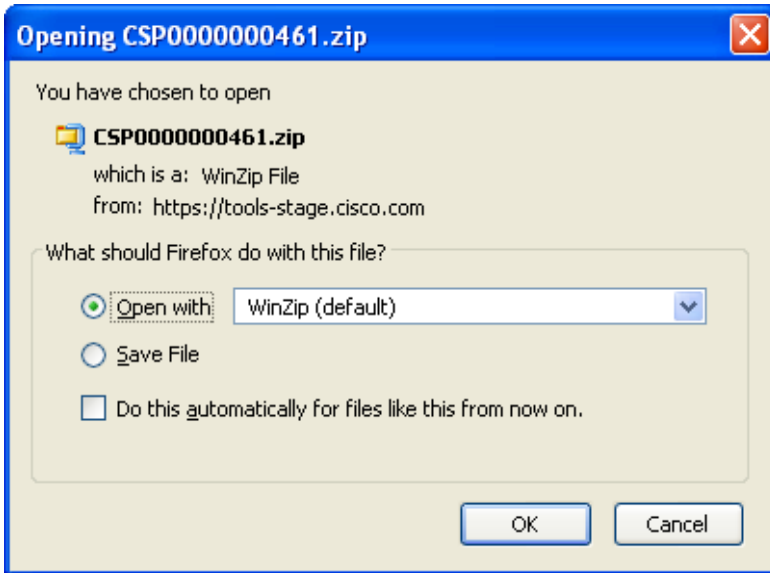
Common Services Platform Collector (CSP-C) Registrations										
	CSP-C NAME	APPLIANCE ID	ENTITLED COMPANY	REGISTRATION STATUS	SITE ID	INVENTORY NAME	CREATED ON	CREATED BY	UPDATED BY	LAST UPDATE
<input checked="" type="radio"/>	CSP-C doctest	CSP0000000461	CISCO SYSTEMS	Completed	RTP-Bldg 10	cisco devices	13/Aug/2010	Sch Test		
<input type="radio"/>	JUNKED_schellaTest	CSP0000000142	CISCO SYSTEMS	Completed	N/A	schellaTest	22/Jun/2010	Sch Test		

[Download Certificate](#) **2** [Update](#) [Delete](#)

There are several ways to download the certificate:

- Certificate can be downloaded directly by clicking [Download Certificate](#) **1** in the confirmation message box.
- It can be downloaded using the CSP-C registration link specified in the confirmation email.

- Click the Download Certificate button,  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.



- Click the **Save File** radio button.



Note Do not open the zip file, instead save it; opening the zip file could cause problems when the files are used later in the process. Store the zip file in a safe place that will be easy to find later, when configuring the CSP-C.

This section describes the process of accessing the appliance and how to upload the [previously obtained certificate](#).

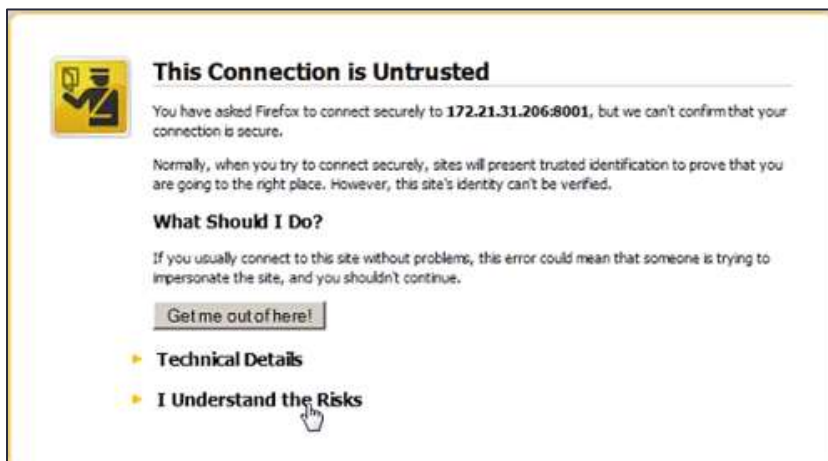
Access the Appliance

The appliance has a built-in web browser, also known as a 'thin-client'. The thin-client interface is what you use to access the appliance GUI. To access the appliance, perform the following steps:

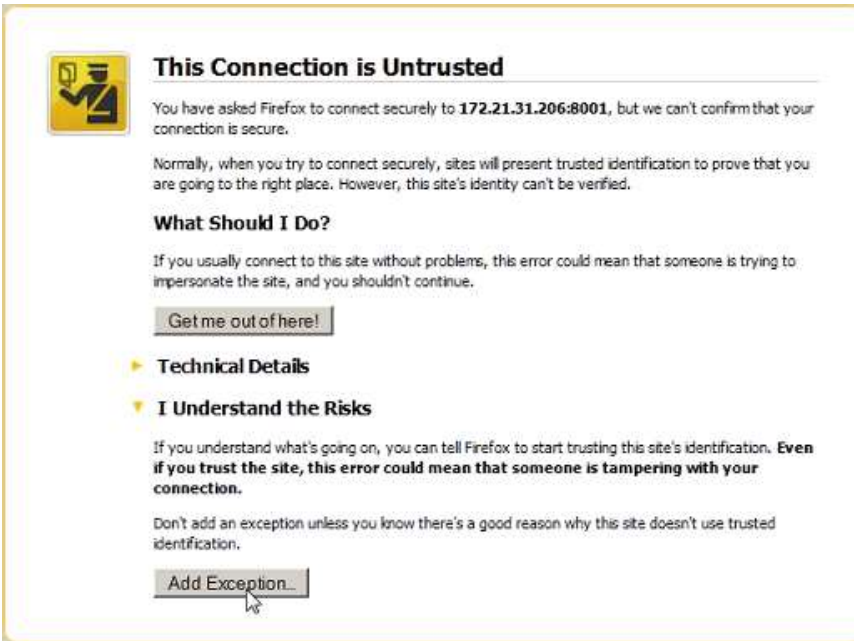
- Use the following URL format to access our appliance:
https://your_appliance_ip_address:8001/cspcgxt/
- Go to your appliance and enter your login credentials. The default user id/password is noted in the [Default Login User Ids and Priorities](#) section.
- After entering your login credentials you will see some type of security certificate warning on your browser. The warning will be different depending upon the type browser you have. Some examples are noted below.



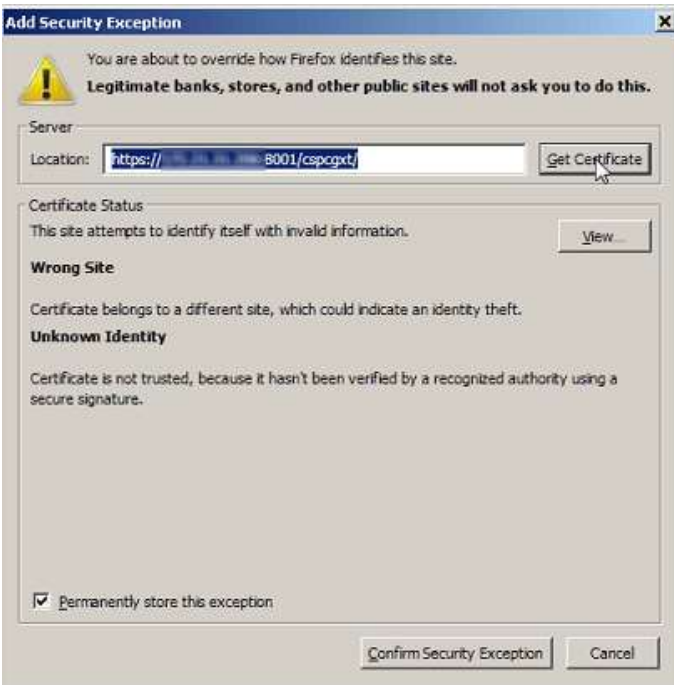
- Will see the above security warning on Internet Explorer



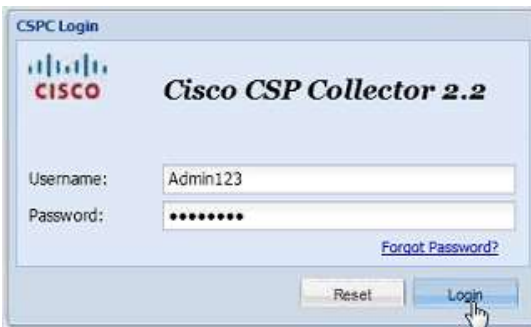
- Will see the above security warning on Firefox.
- Click **I Understand the Risks**, which expands additional info for you to read and select.



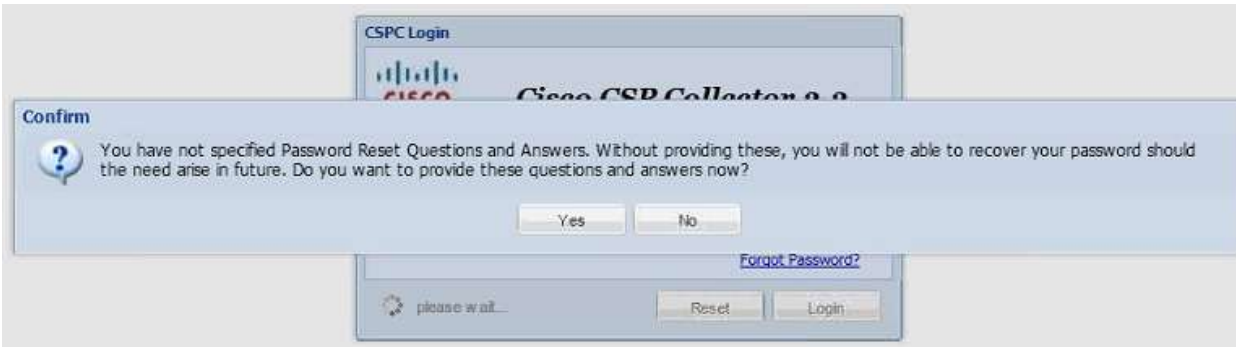
- Click **Add Exception** to continue access to the collector appliance.



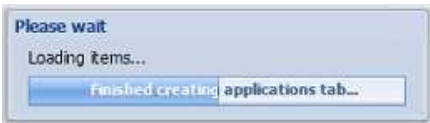
- Click **Confirm Security Exception**, which allows you to continue the login process.



- Enter your login credentials



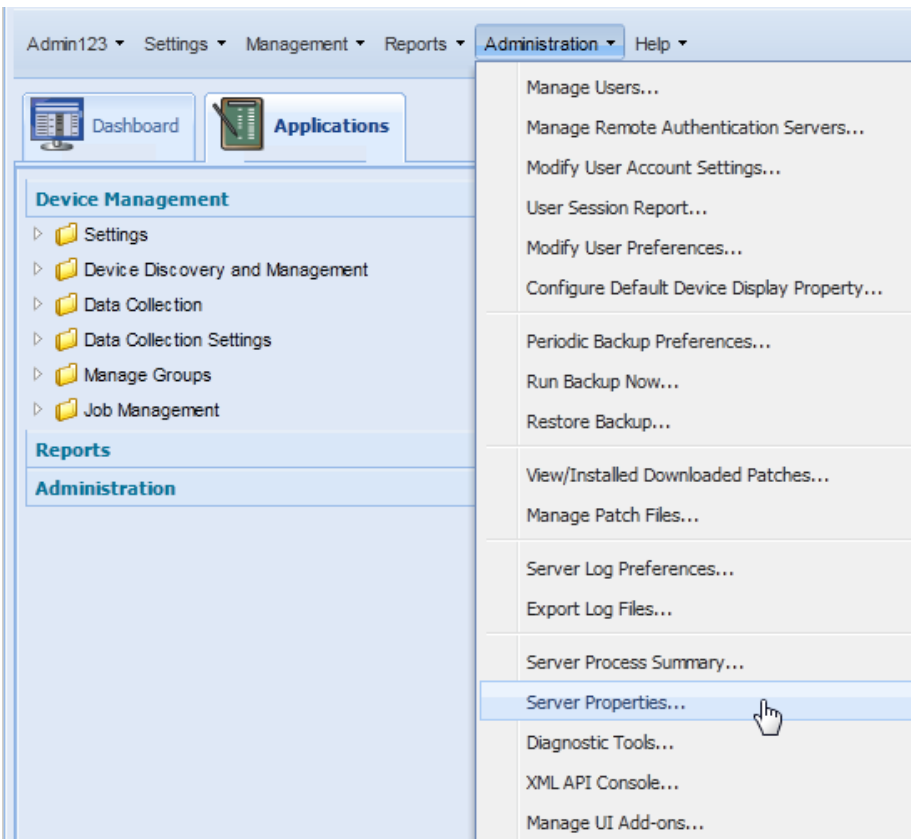
- You will be prompted for Password Reset Questions if you have not provided them yet. Click **Yes** to provide them now or Click **No** to provide this information at some later time.



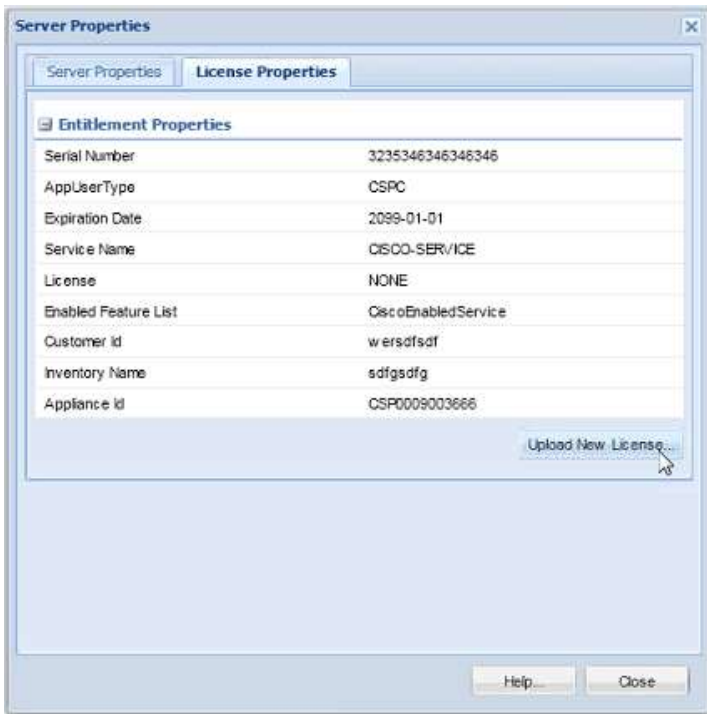
- After you have provided your Password Reset Questions, or clicked **No**, then the appliance loads its software items for operation.
- After all the software is loaded, the browser thin-client GUI appears.

Upload New License

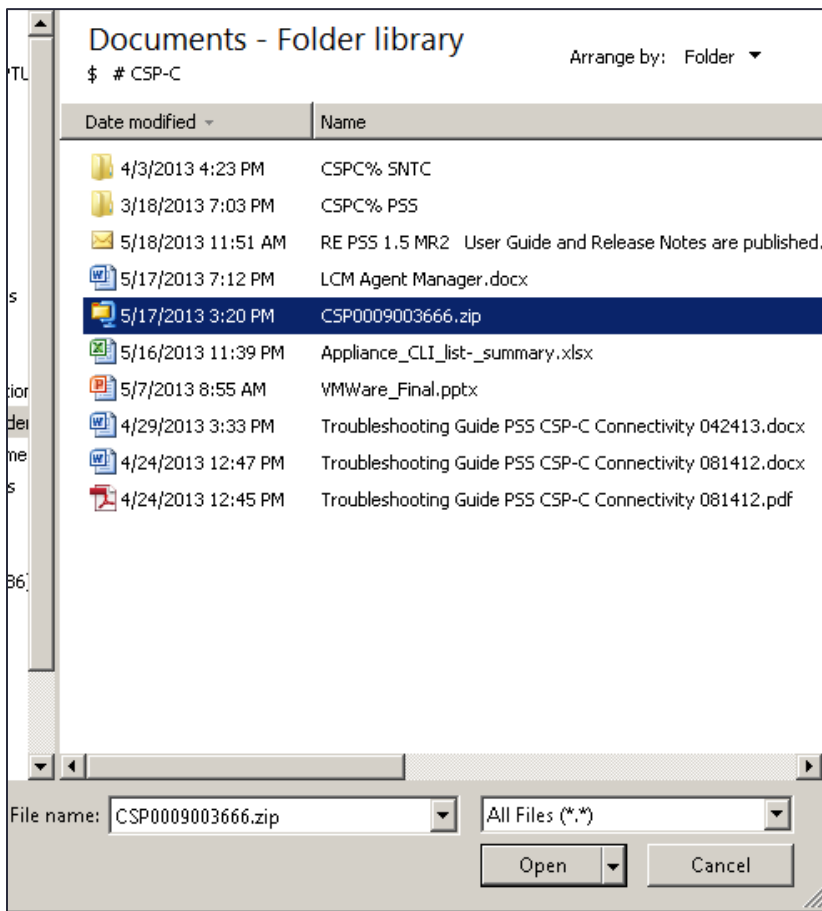
To upload the new license file, perform the following steps:



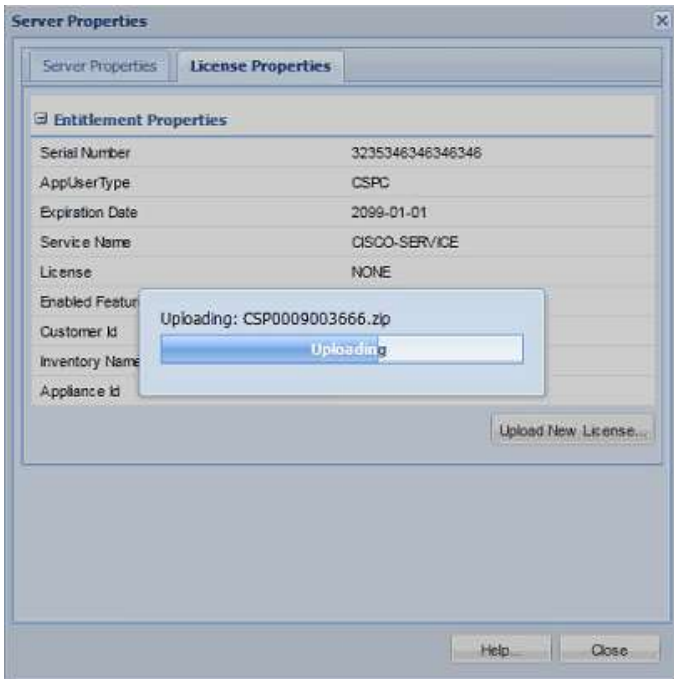
- On the menu choose **Administration > Server Properties**; the Server Properties window appears.



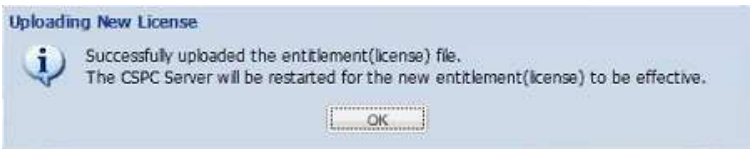
- Click the **License Properties** tab, then click **Upload New License**; the Documents – Folder Library window appears.



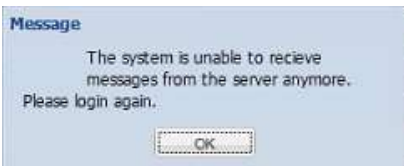
- Select the license file, then click **Open**.



- The license file gets uploaded to the appliance.



- After the license file gets uploaded to the appliance, a message appears indicating that the license file was successfully uploaded.
- Click **OK**, which restarts the CSPC server appliance.



- The CSPC server gets restarted and a message appears indicating the CSPC server appliance is unable to receive any messages and that a login is required.
- Click **OK** to start the login process.

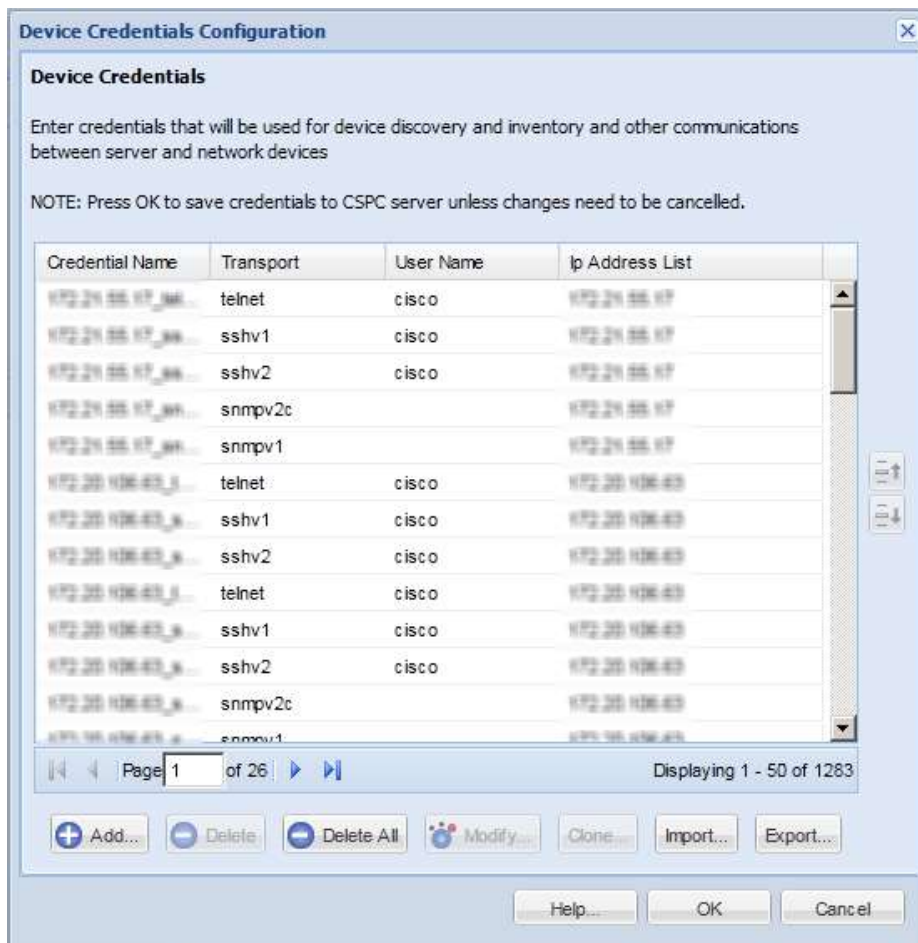
CSP-C Configuration and Device Credentials

There is a special process related to configuring the CSP-C server, that process is specifying 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 the CSP-C are used for two purposes:

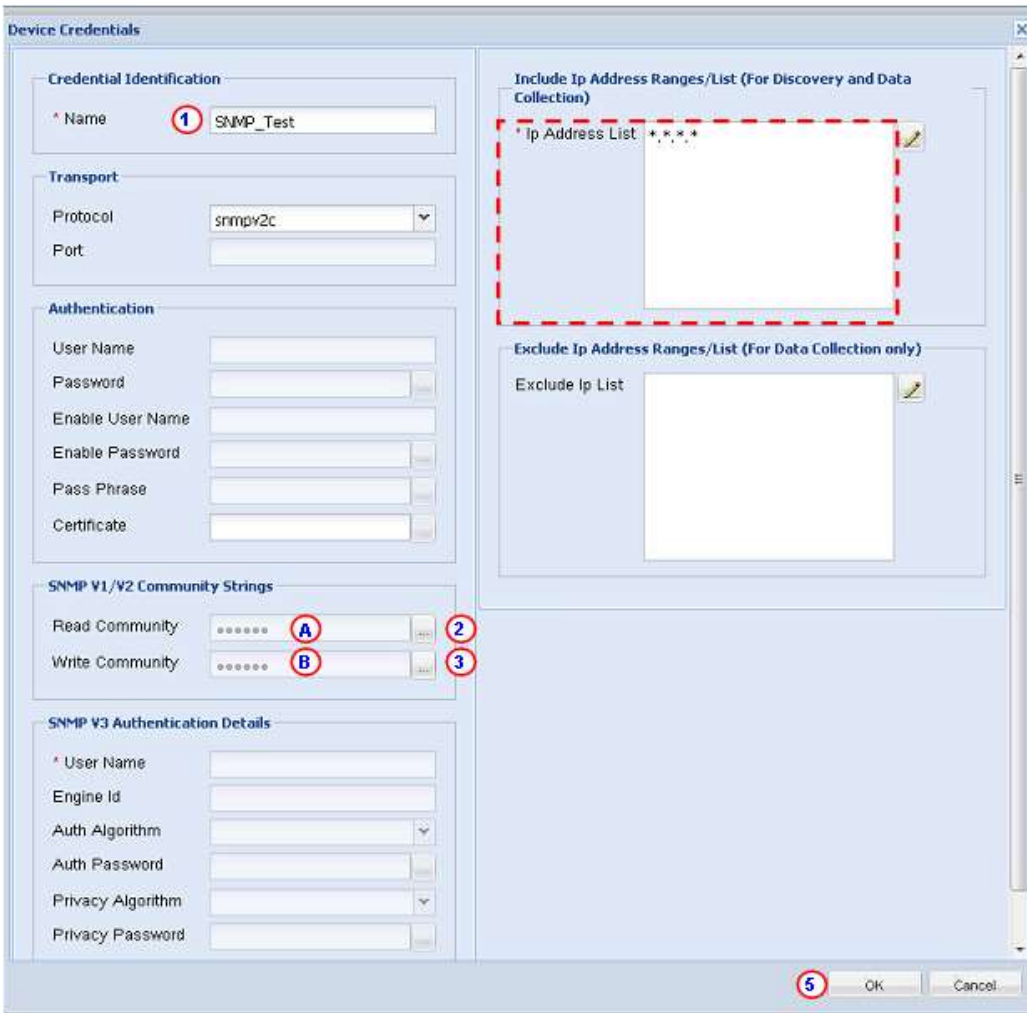
- **SNMP credentials** are used only for the initial discovery of the devices.
- In addition to SNMP, the remaining credentials (that is, telnet, SSH, HTTP, HTTPS) are used for data collection from the discovered devices.

To set the device credentials perform the following steps:

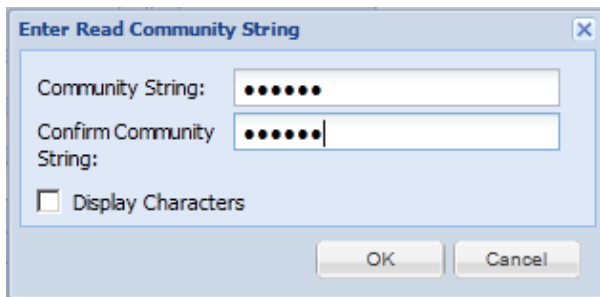
- On the browser menu choose **Settings > Device Credentials...**; the Device Credential Configuration window appears.



- Click **Add** to create a credential, the device credentials window appears, which contains credential identification, authentication information, and SNMP Read community **R** and Write community **W** string details (see next graphic).



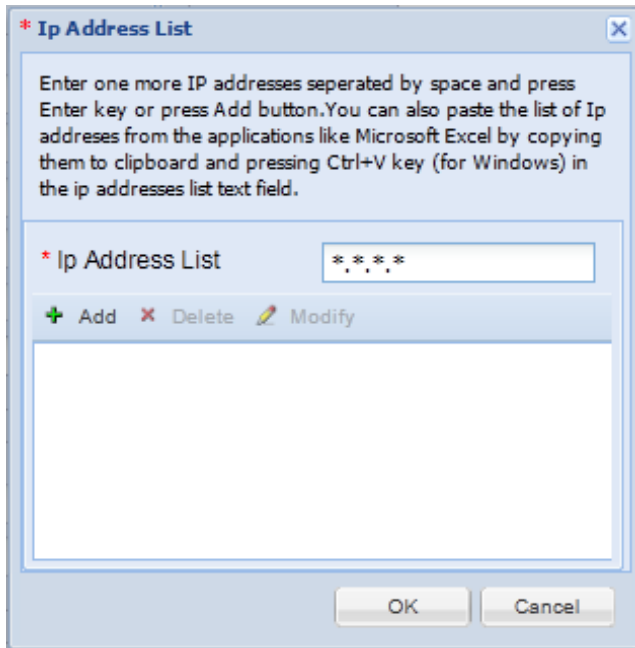
- Fill out the required data:
 - [Enter a credential name \(that is, UAT-Test\).](#) ①
 - [For SNMP V1/V2 Community Strings section, enter the respective Read community string by clicking the ... icon; ② the Enter Read Community String window appears.](#)



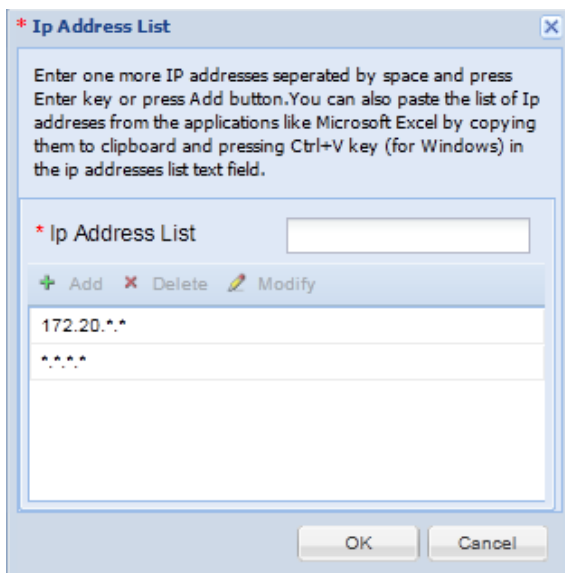
- [In the Enter Read Community String window enter the read community string \(for devices the default is public\) then click **OK**; the community string is added to the Read Community field.](#) ④
- [Enter the Write community string by clicking the ... icon; ③ the Enter Write Community String window appears.](#)



- [In the Enter Write Community String window enter the write community string \(for devices the default is private\) then click **OK**; the community string is added to the Write Community field.](#)
- [Enter an IP Address list by clicking the pencil icon **4** to the right of the IpAddress list field in the device credentials window, then enter the IP Address list.](#)

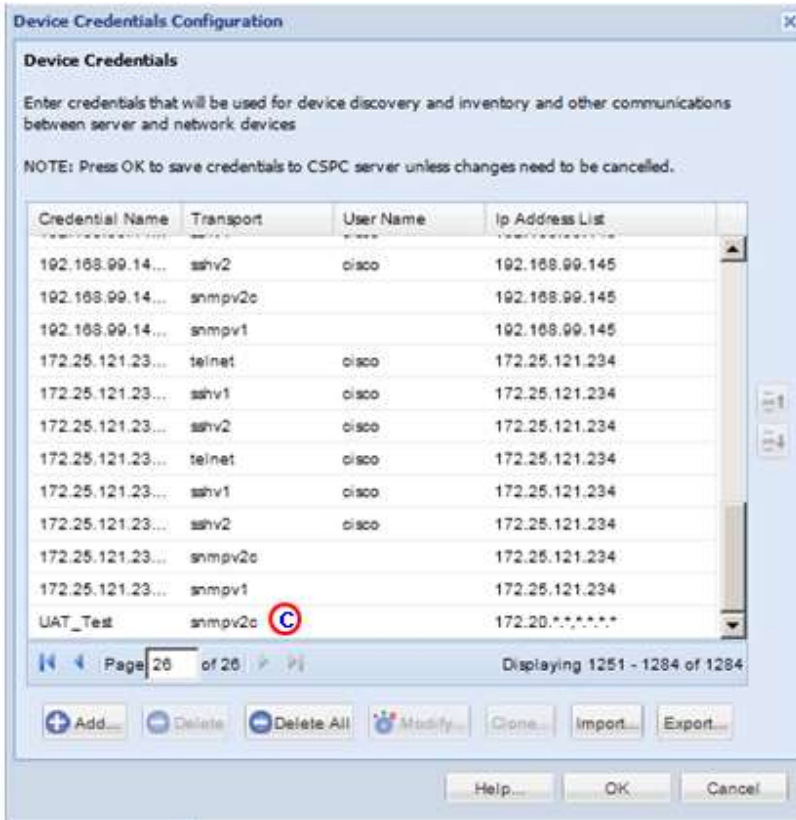


- [After entering the IP Address list details click **Add**; the entered data is added to the IpAddress List.](#)

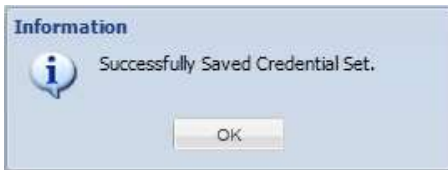


Note Entering *.*.*.* looks for all the network devices, entering 172.20.*.* look for those devices in the 172.20 subnet.

- After entering the above data click **OK**; the new credential appears in the Device Credentials list.



- Click **OK**; the Edit Credentials window appears with a successful saved message.



- Click **OK**, the window closes; the next step is performing the steps for an inventory upload.

Rules Package

This section covers the following Rules package areas:

- [Rules Package Components](#)
- [Installing Rules Package in the CSPC](#)
- [Upgrading or Deleting the Existing Rules from CSPC](#)

Rules Package Components

The following list identifies the different components that make up the rules package and states what their purpose is:

- **Manage Data Collection Profiles** – defines, and configures the Collection Profile, which contains datasets and lets you identify the devices for which the data sets needs to be fetched. You can Add, Modify, or Delete a collection profile.
- **Manage Data Sets** – is used for creating a new data collection point. Datasets are the building blocks of CSPC Collection Profile. Datasets contains the platform definitions, data masking rules. You can Add, Modify or Delete datasets.
- **Platform Definitions option** –defines custom existing platforms which are not already defined in CSPC. You can add a new platform definition, and modify or delete an existing platform definition.
- **Manage Data Integrity Rules option** – is used to Add, Modify, or Delete a data integrity rule. Data Integrity Rules are used to generate custom error messages whenever it encounters a pre-defined expression.
- **Manage Data Masking Rules option** – is provided to add a new Data Masking Rule. Masking Rules are used to mask some of the sensitive data in the command output. You can Add, Modify, or Delete a masking rule.

Installing Rules Package in the CSPC

The installation of the rules package is performed in two different scenarios:

- Installing the rules package on a collector for the first time
- Performing a rules package upgrade (upgrading the rules package from a previous release).



Note In the rules package upgrade process the existing rules are first removed (see [Upgrading or Deleting the Existing Rules from CSPC](#) for more details) then this section (Installing Rules) is performed next.

This section describes the process for installing a new rules package:

Prerequisites

This section describes the rules package installation pre-requisites:

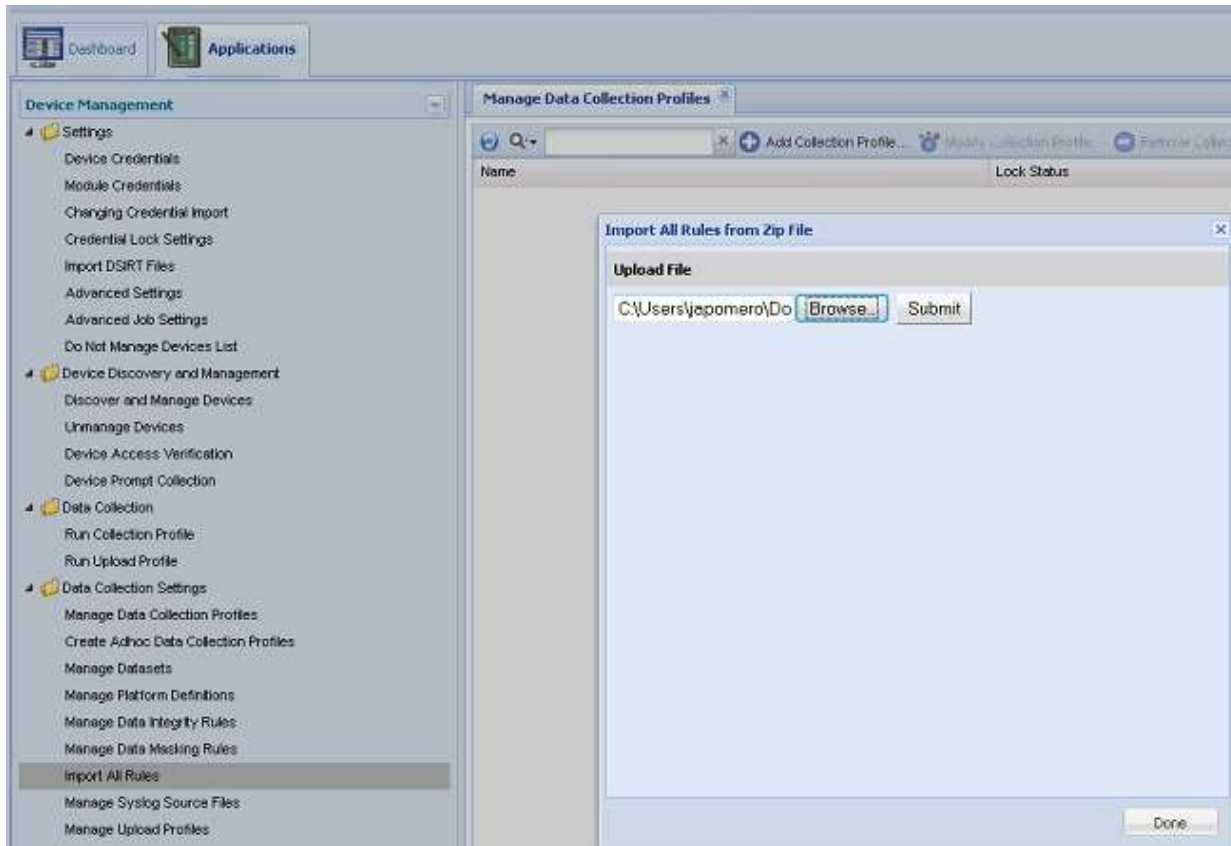
- Download the rules from the CCO location or get the latest rules from rules team.
- Unzip the rule package in your local desktop.

User can load the rules by the following two methods,

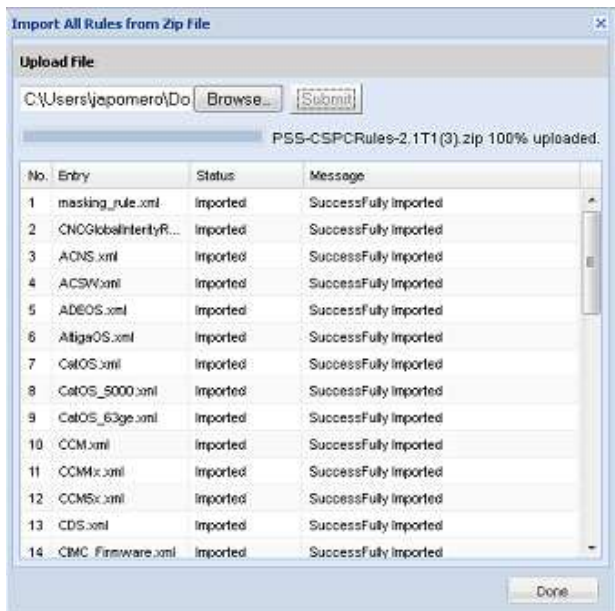
- Loading all rules in one download
- Loading rules one by one.

Importing All Rules

This section describes the process for importing all the rules at one time:



- On the CSPC navigation pane choose **Categories > Data Collection Settings > Import All Rules** ; an All Rules window appears.
- In the All Rules window click **Browse**.
- Navigate to the location where you downloaded your rules package and select **CSPC2-DD-RP1.42.0.zip** (or whatever rules package may be applicable).
- Click **OK**; this starts the rules package installation process.



- Wait for the processing to complete.

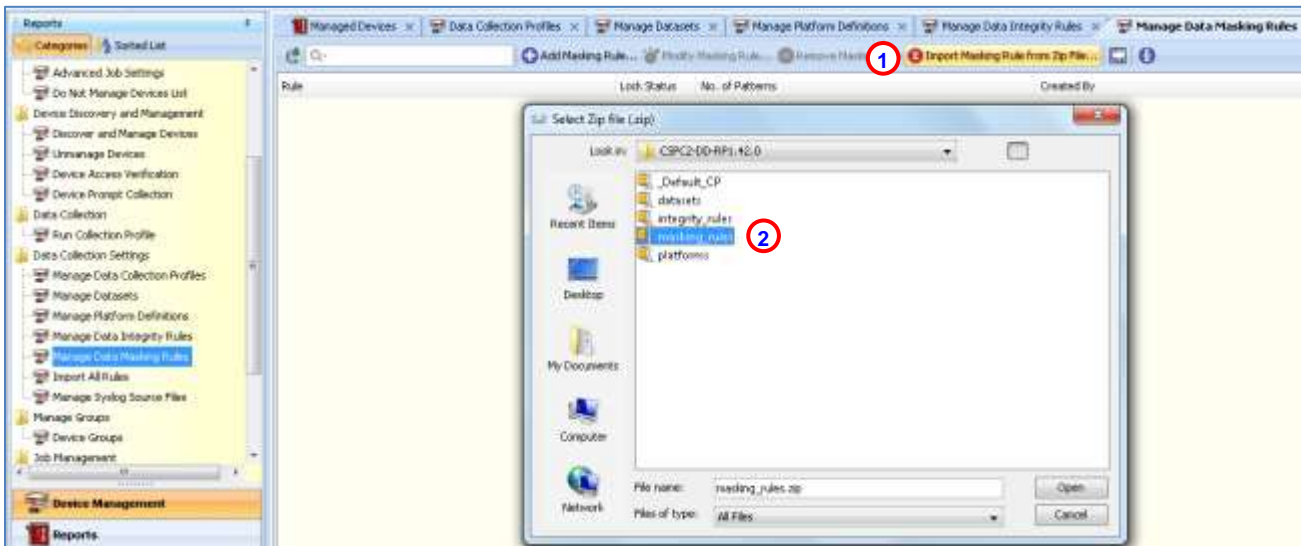
Importing Rules Package One by One:

This section describes the process for loading the rules package one at a time. The install process uses the following sequence when loading the rules package:

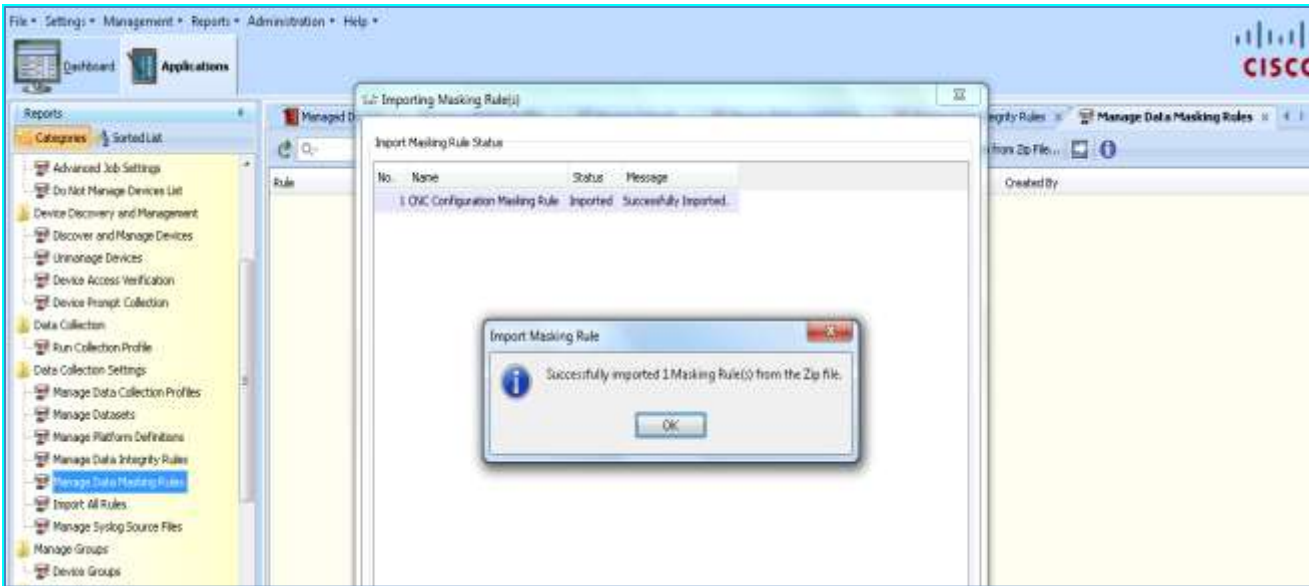
- [Manage Data Masking Rules](#)
- [Manage Data Integrity Rules](#)
- [Manage Platform Definitions](#)
- [Manage Datasets](#)
- [Manage Data Collection Profiles](#)

Manage Data Masking Rules

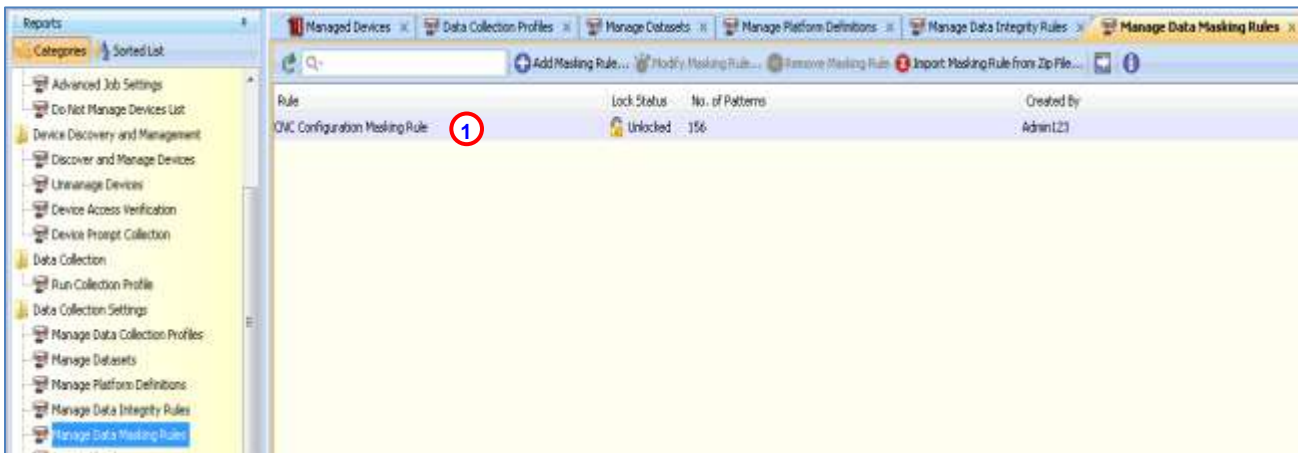
This section describes the process for loading the data masking rules:



- On the CSPC navigation pane choose Categories > Data Collection Settings > Manage Data Masking Rules
- Select Import Masking Rule from Zip File. ①
- Select the **masking_rules.zip** ② from the local desktop, which the user already downloaded.
- Unzip the latest rule package.
- Click **Open** to install.



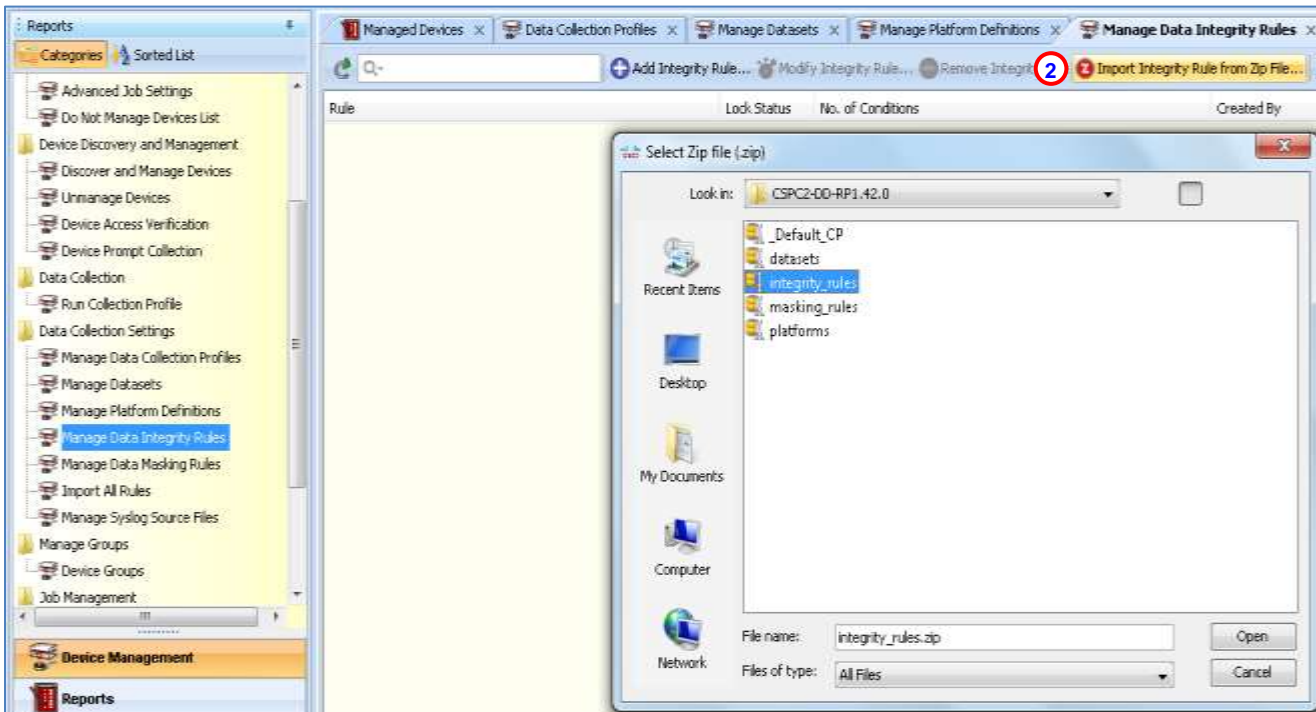
- You will see a message indicating a successful import of the Masking Rules.



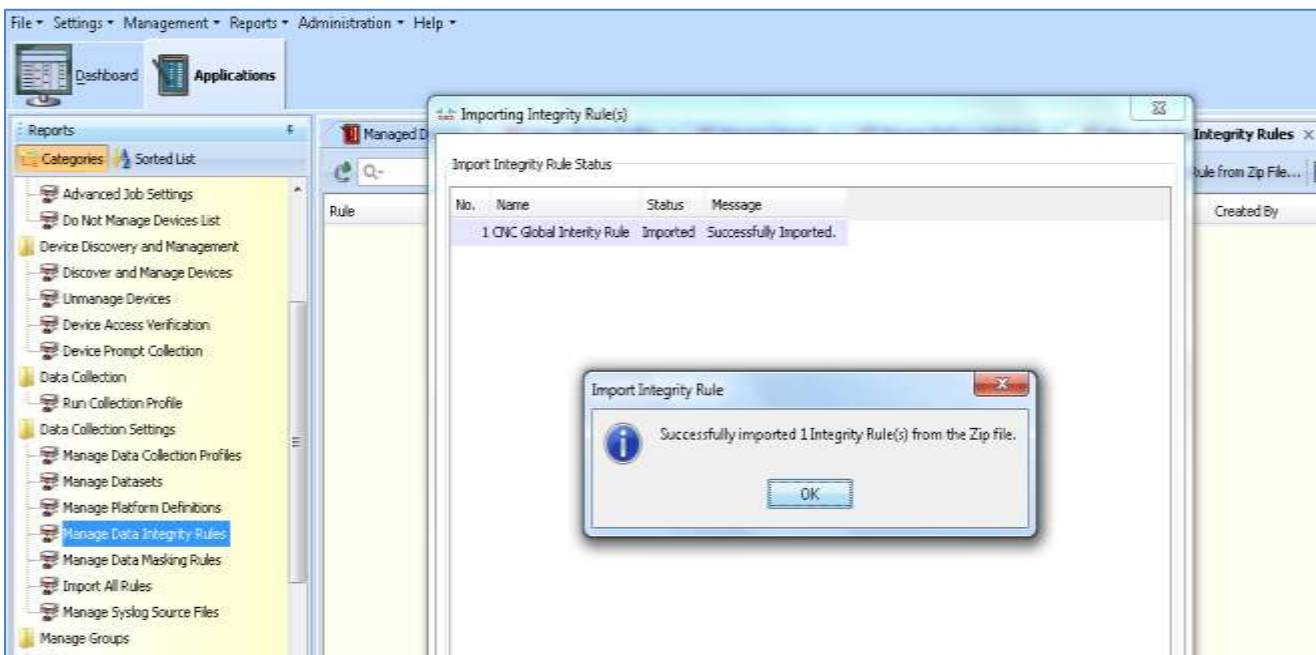
- Make sure that the masking rule installed properly by ensuring that the update appears in the CSPC application window. ①

Manage Data Integrity Rules

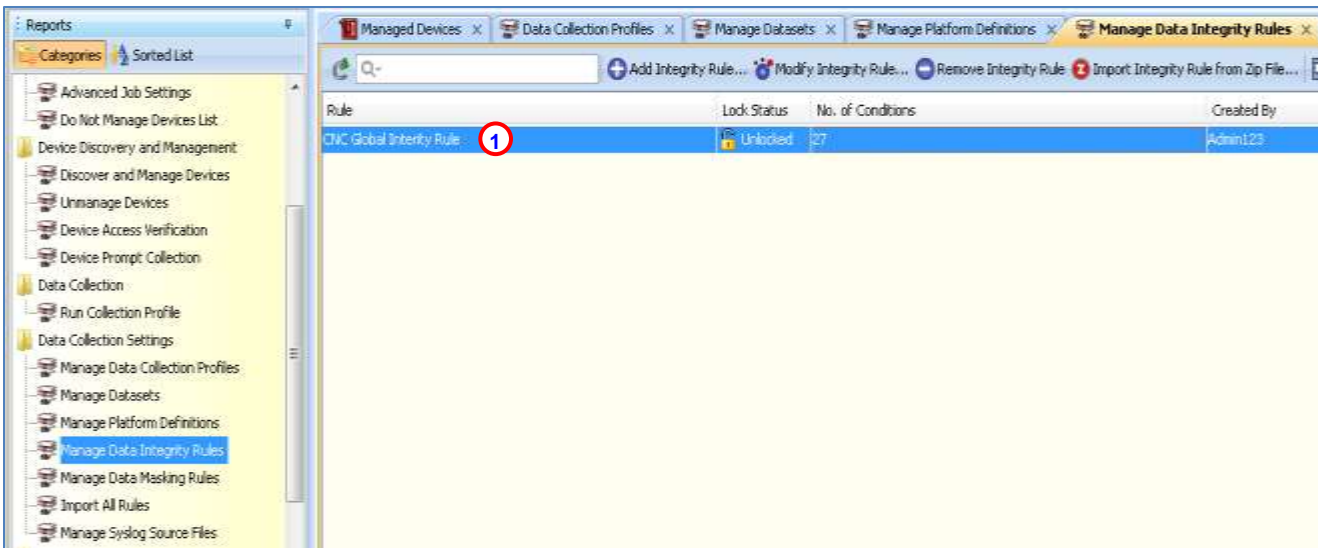
This section describes the process for loading the data integrity rules:



- On the CSPC navigation pane choose Categories > Data Collection Settings > Manage Data Integrity Rules
- Select **Import Integrity Rule from Zip File**; ② the Select Zip file window appears.
- Select the **integrity_rules.zip** from the local desktop, which the user already downloaded.
- Unzip the latest rule package.
- Click **Open** to install.



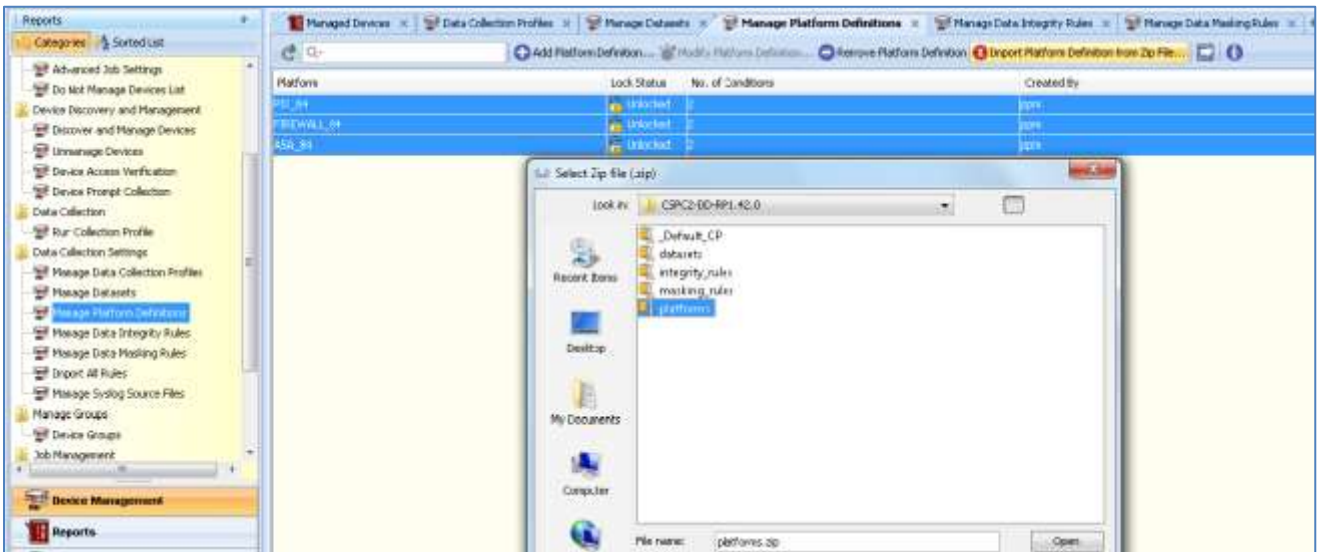
- You will see a message indicating a successful import of the Masking Rules.



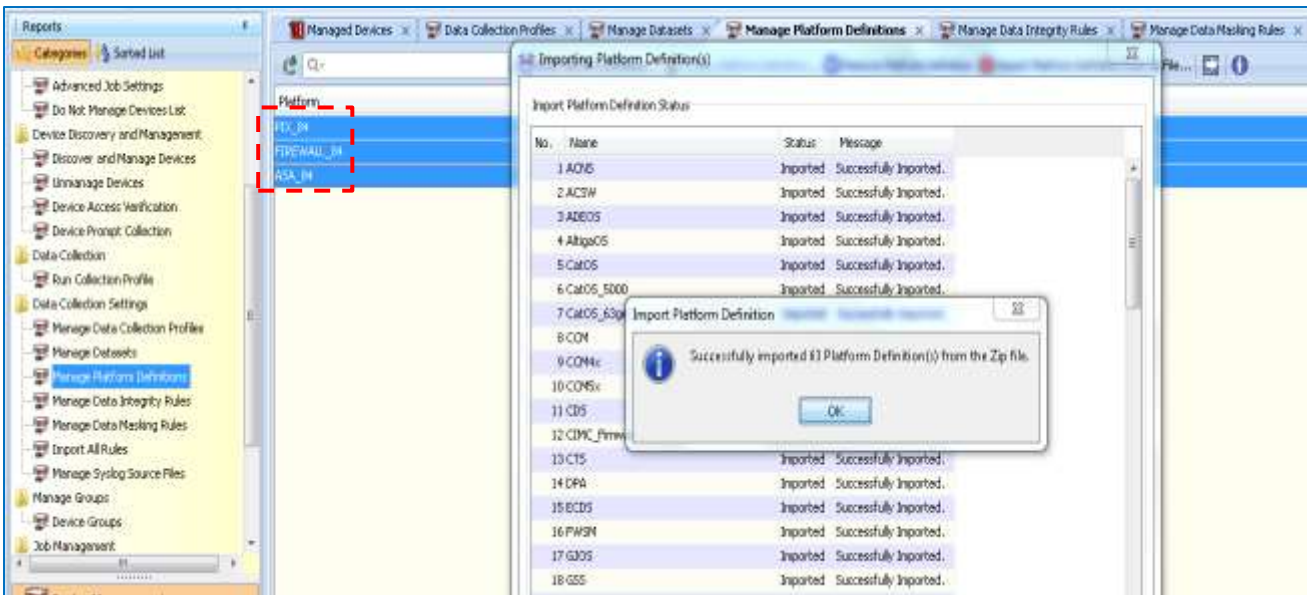
- Make sure that the integrity rule installed by ensuring that the update appears in the CSPC application window. 1


Manage Platform Definitions

This section describes the process for loading the data integrity rules:



- On the CSPC navigation pane choose Categories > Data Collection Settings > Manage Platform Definitions.

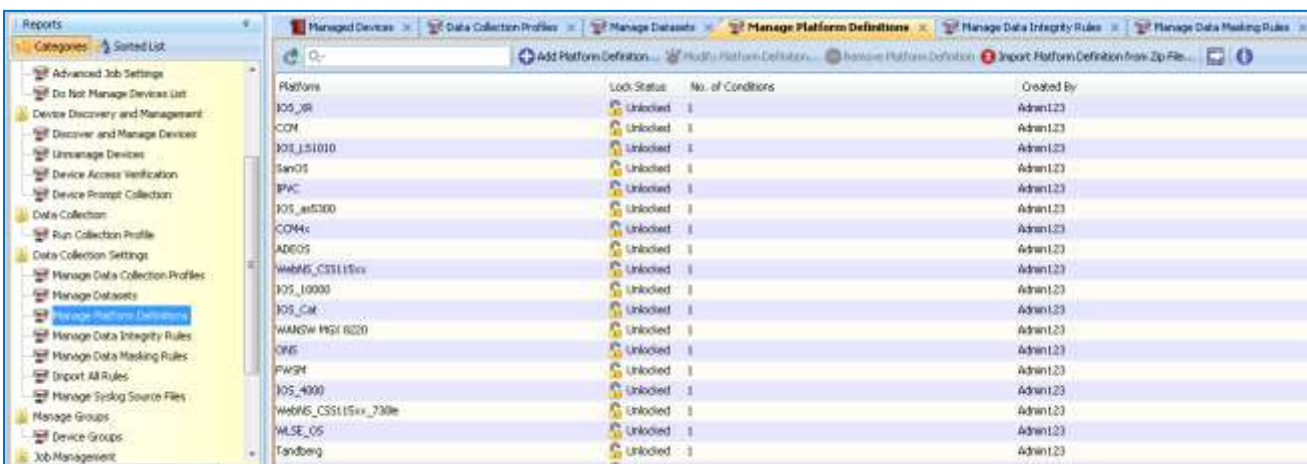


Note If this is not a new install, but is instead an upgrade, then the following rules  should already be present before importing the platform rule::

- PIX_84
- FIREWALL_84
- ASA_84

The user can upgrade the latest rules on top of these three pre-existing rules without any issues.

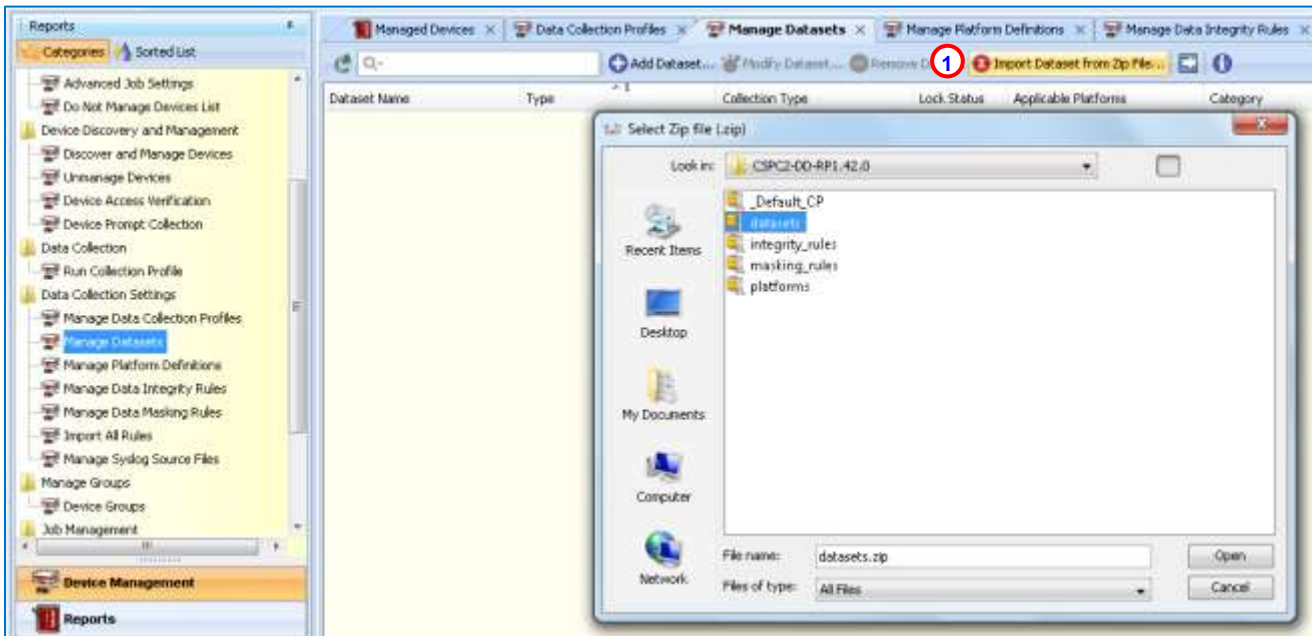
- Click Import Platform Definition from Zip File.
- Select the **platforms.zip** from the local desktop, which user already downloaded.
- Unzip the latest rule package.
- Click **Open** to install.




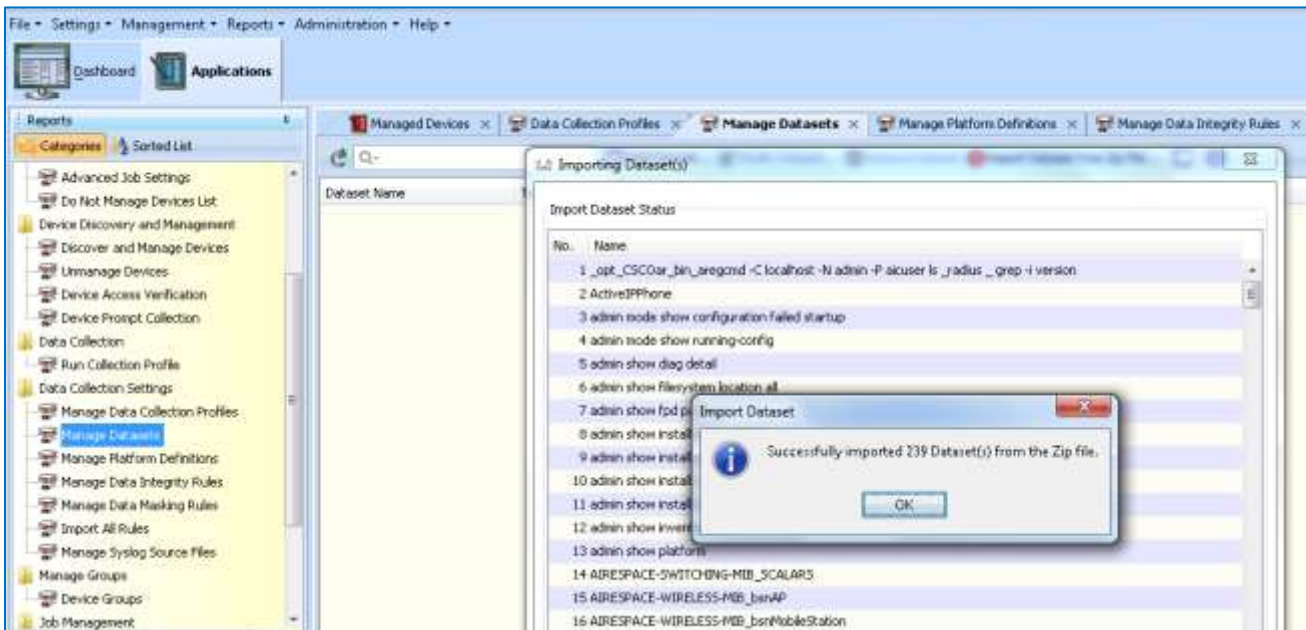
- Make sure that the platform definition rules installed properly by ensuring that the update appears in the CSPC application window.

Manage Datasets

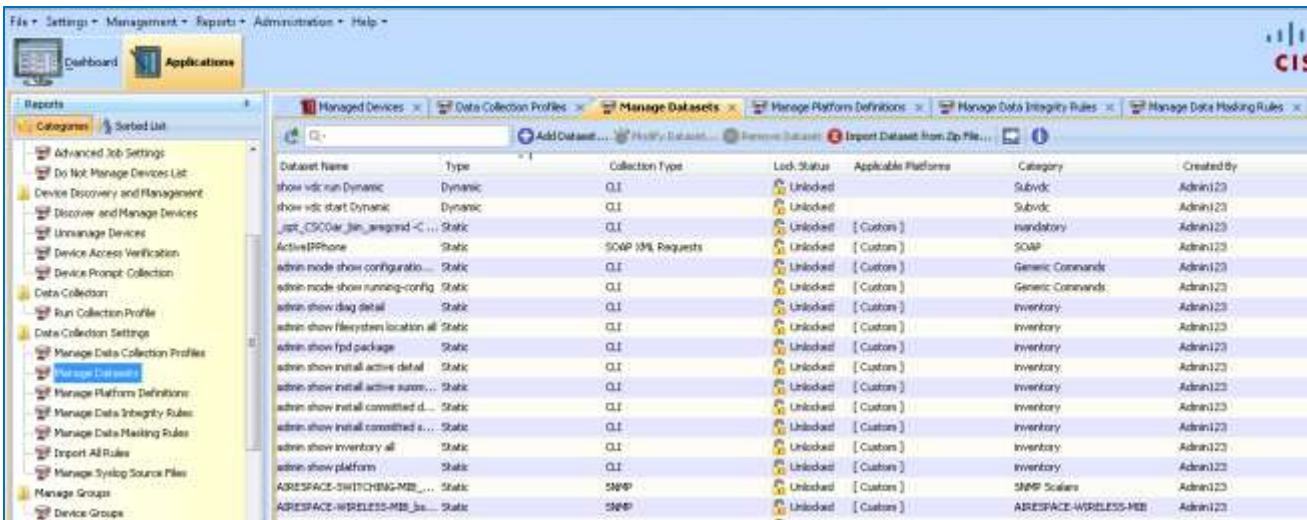
This section describes the process for loading the data integrity rules:



- On the CSPC navigation pane choose Categories > Data Collection Settings > Manage datasets,
- Click Import Dataset from Zip File. 
- Select the **datasets.zip** from the local desktop, which the user already downloaded.
- Unzip the latest rule package.
- Click **Open** to install.



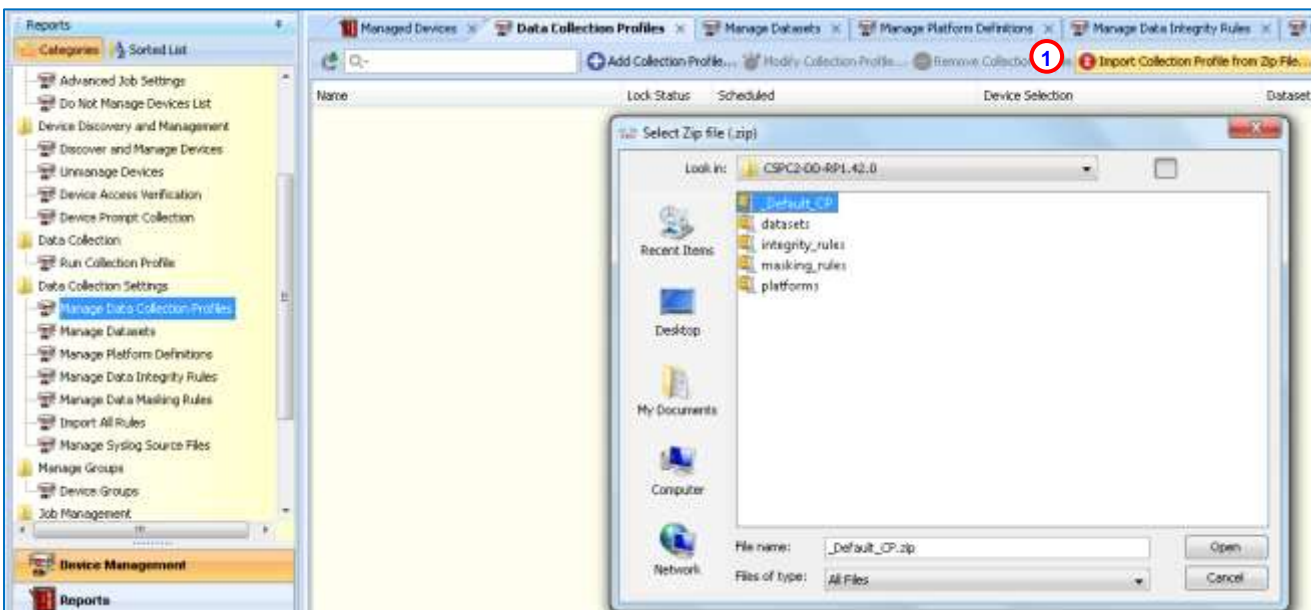
- You will see a message indicating a successful import of the datasets from the zip file.



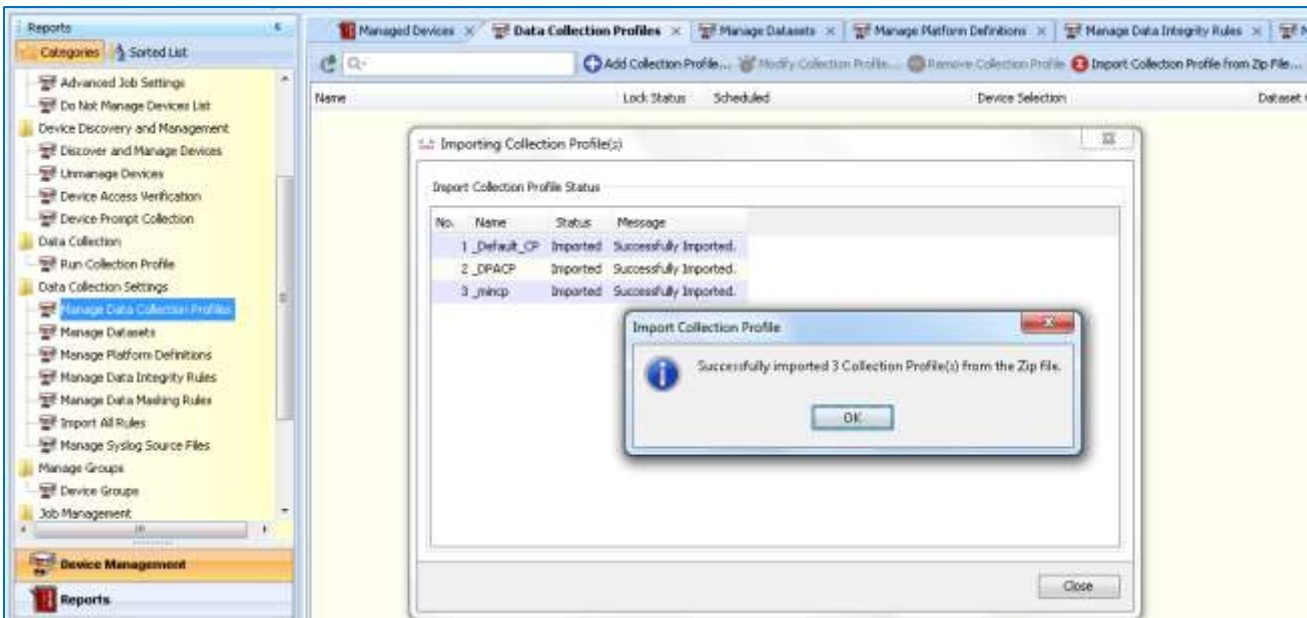
- Make sure that the Dataset rules installed properly by ensuring that the update appears in the CISCSP application window.

Manage Data Collection Profiles

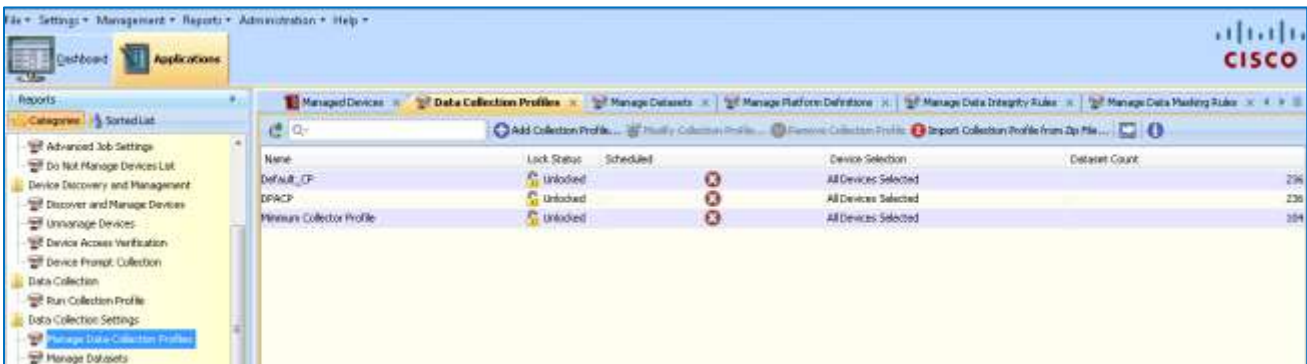
This section describes the process for loading the data collection profiles:



- On the CISCSP navigation pane choose Categories > Data Collection Settings > Manage Data Collection Profiles.
- Click Import Collection Profile from Zip File. ①
- Select **_Default_CP.zip** from the local desktop, which the user already downloaded.
- Unzip the latest rule package.
- Click **Open** to install.



- You will see a message indicating a successful import of the Collection Profile.



Upgrading or Deleting the Existing Rules from CSPC

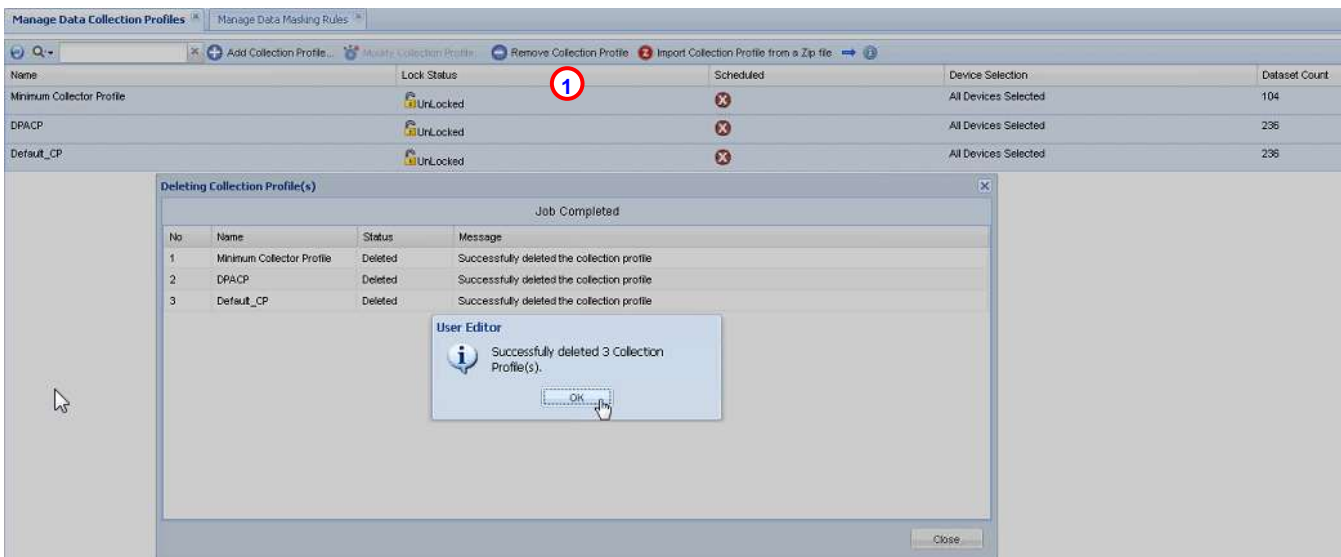
The process for upgrading the rules package from one release to another requires the deletion of the current rules package and then the installation on the new rules package. This section describes the process for deleting the current rules package.


Important There is a very specific order for deleting the existing rules from the CSPC server, follow the deletion order noted below:

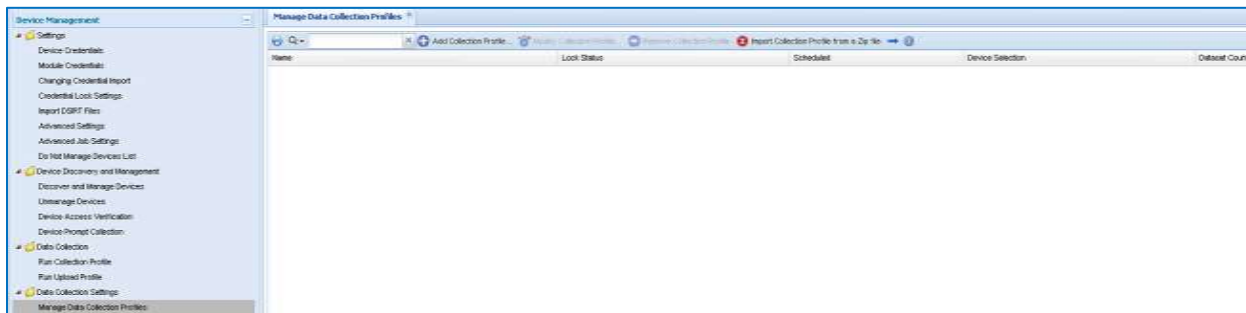
- Data Collection Profiles
- Datasets
 - Delete Dynamic Rules first
 - Delete Static Rules last
- Platform Definitions
- Data Integrity Rules
- Data Masking Rules

Manage Data Collection Profiles

This section describes the process for removing the data collection profiles



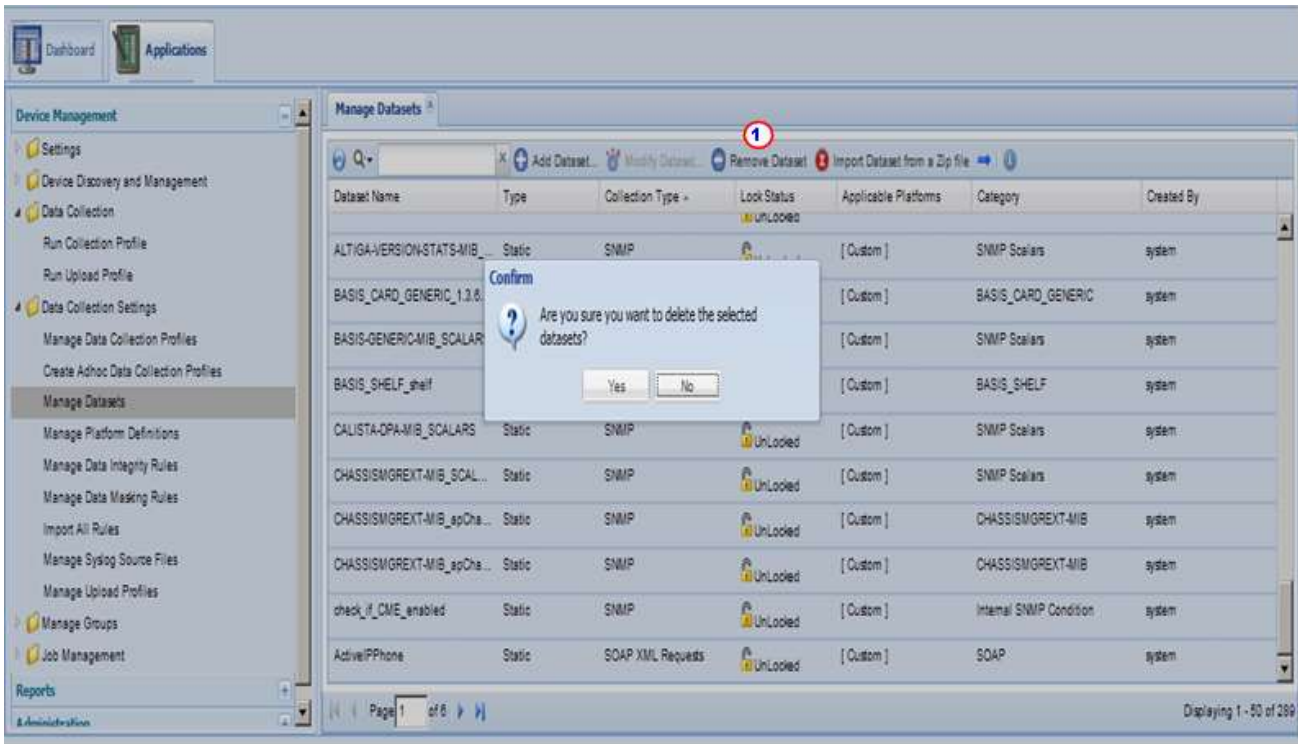
- On the CSPC navigation pane choose Categories > Data Collection Settings > Manage Data Collection Profiles
- Select all 3 collection profiles:
 - Minimum Collection Profile
 - DPACP
 - Default_CP
- Click Remove Collection Profile 



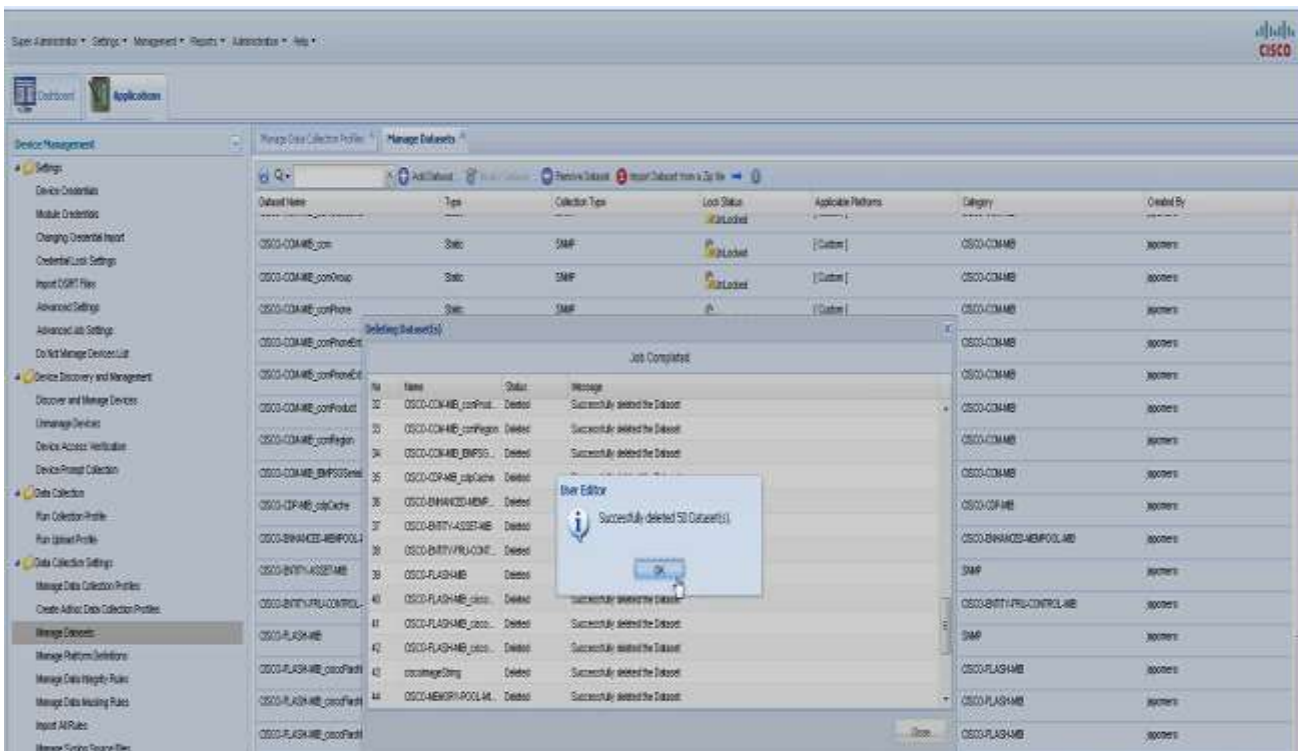
- Make sure that all 3 collection profiles were deleted successfully from the collector.

Manage Datasets

This section describes the process for removing the datasets:



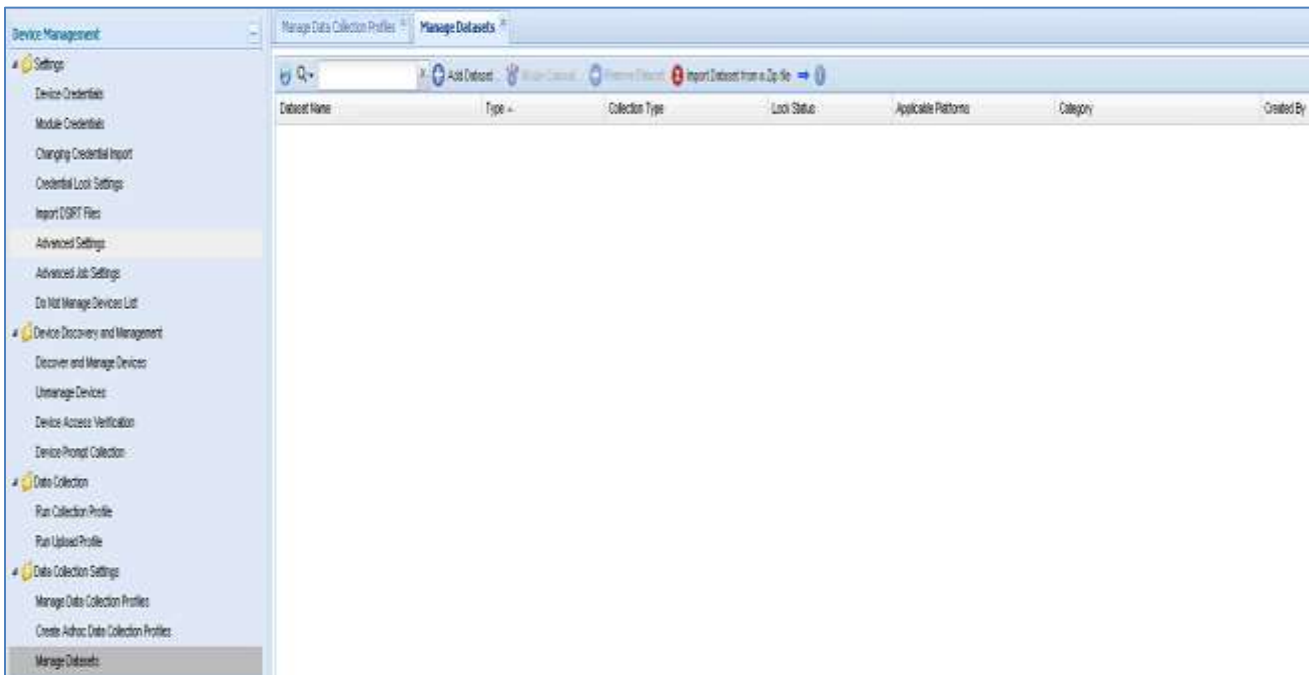
- On the CSPC navigation pane choose Applications > Data Collection Settings > Manage Datasets
- Click **Remove Dataset**; a confirmation window appears, click **OK**.



- A message appears indicating that the first set of datasets have been successfully deleted; click **OK**.



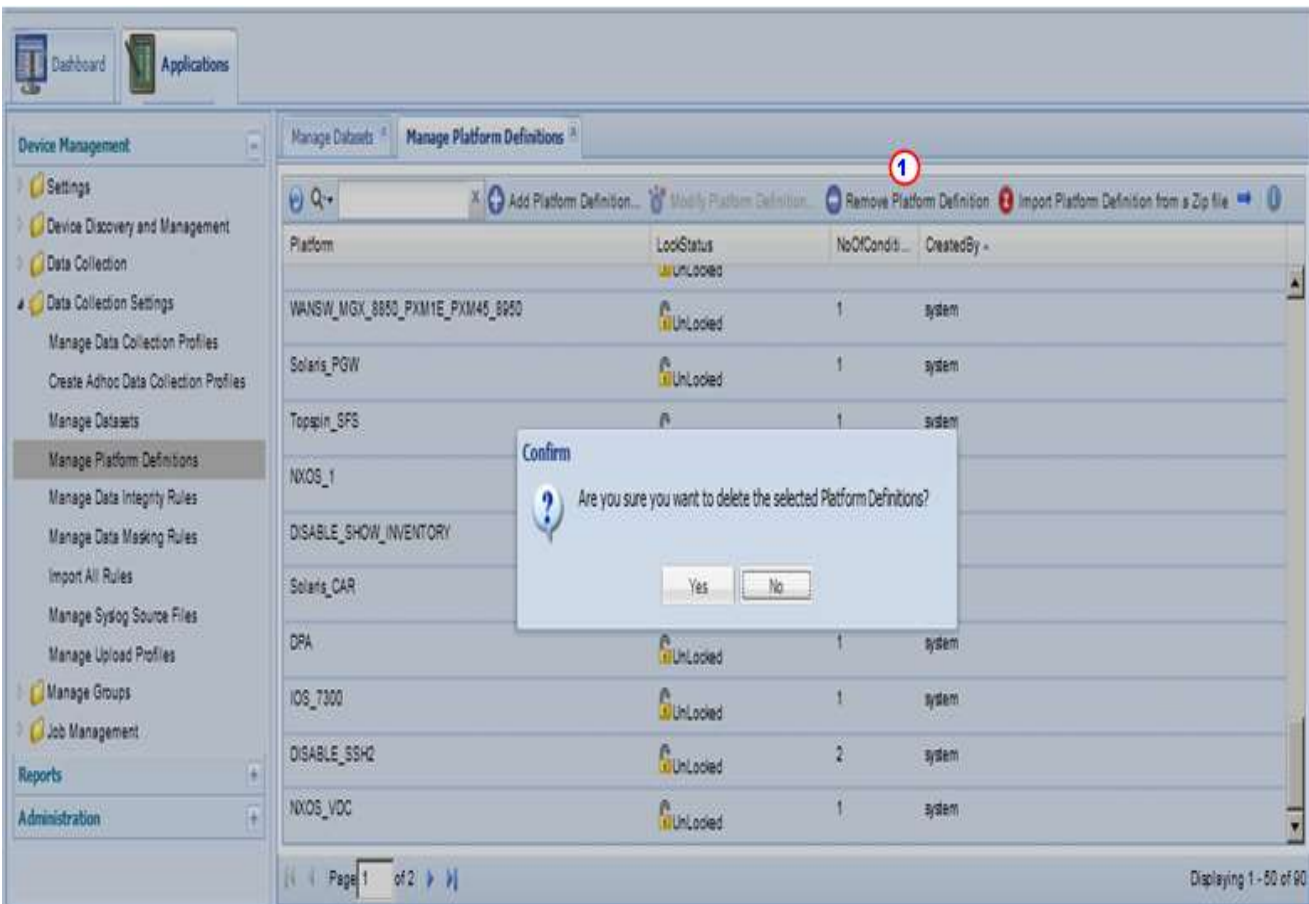
Note The web-client allows you to view and delete only 50 datasets at a time.




- Make sure that all the datasets are deleted from the server.

Manage Platform Definitions:

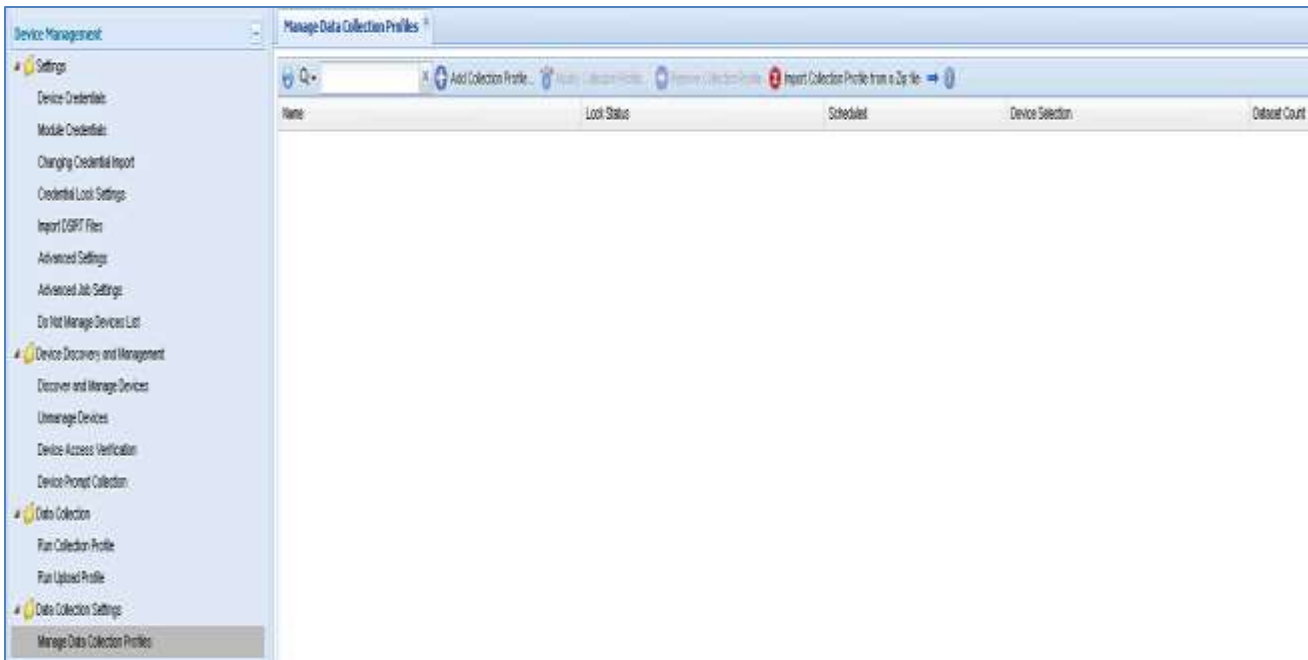
This section describes the process for removing the platform definition



- On the CSPC navigation pane choose Applications > Data Collection Settings > Manage Platform Definitions.
- Select all the platform rules.
- Click Remove Platform Definition. 
- A message appears indicating that the first set of datasets have been successfully deleted; **click OK.**

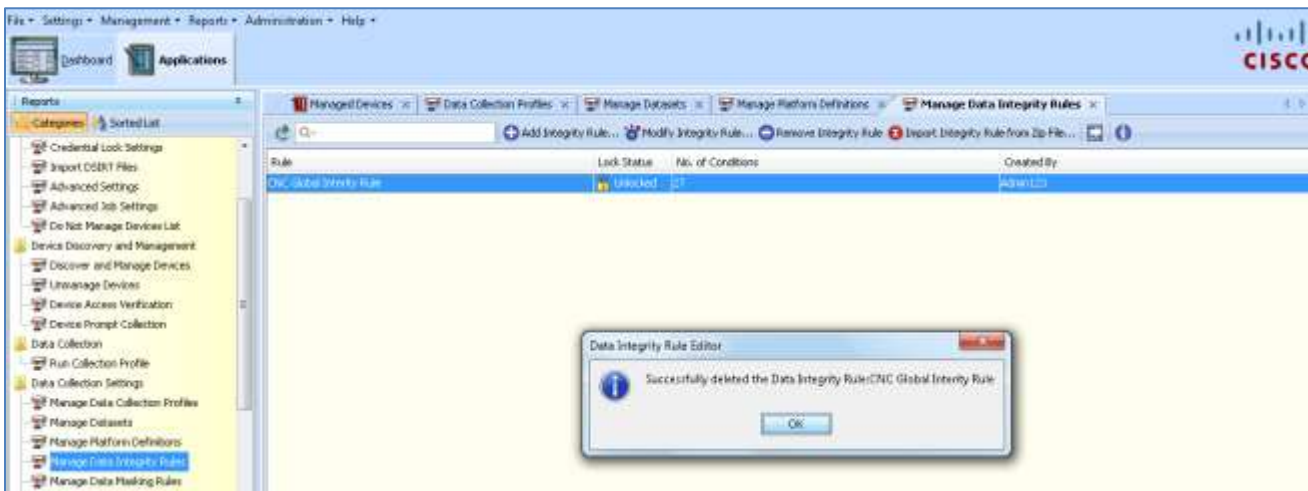


Note The web-client allows you to view and delete only 50 datasets at a time.

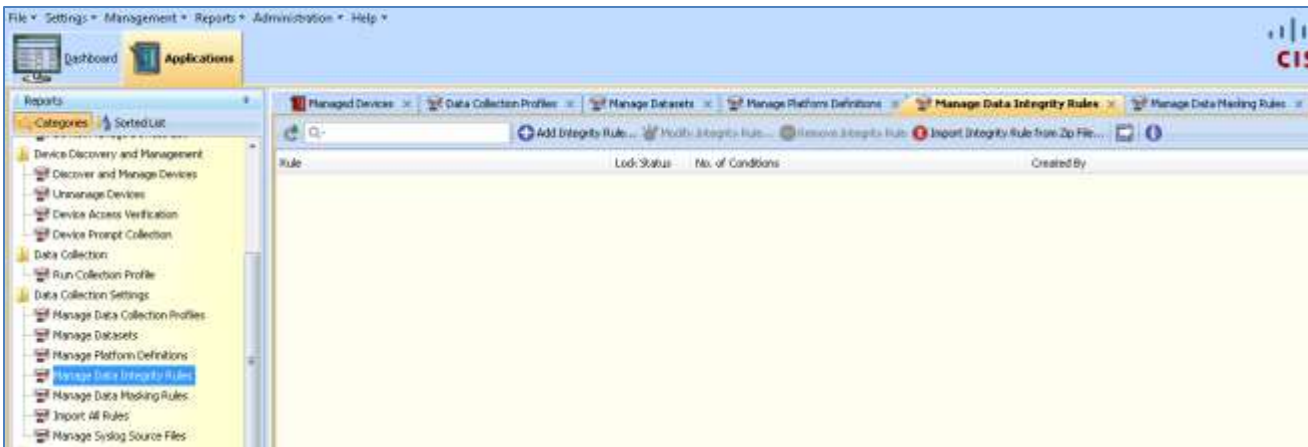


Manage Data Integrity Rules:

This section describes the process for removing the Data Integrity rules:



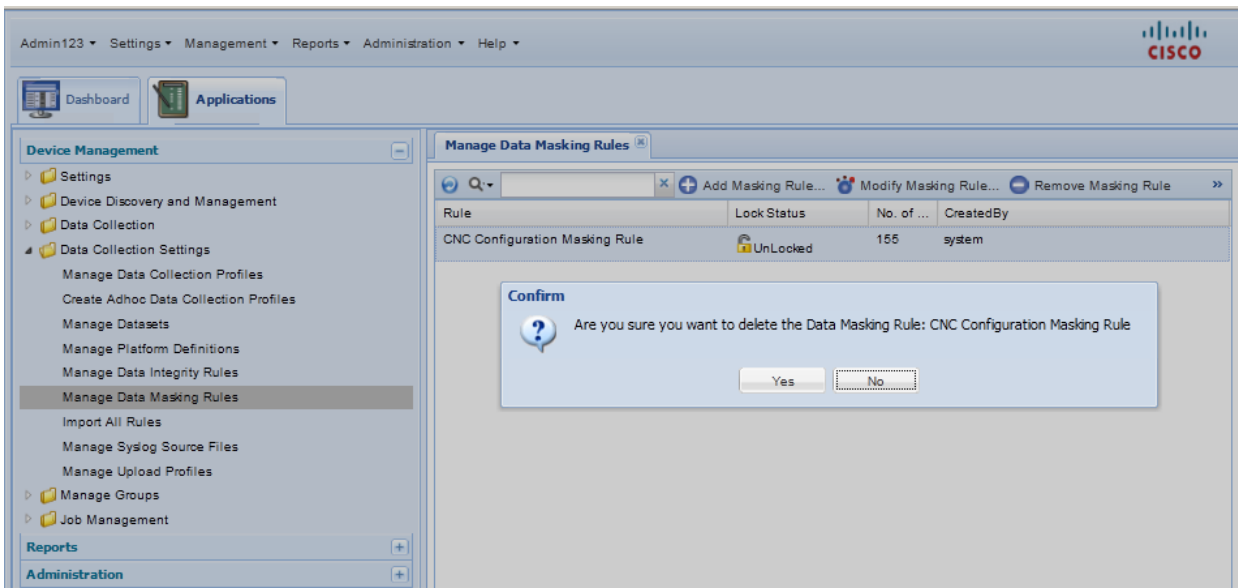
- On the CSPC navigation pane choose Categories > Data Collection Settings > Manage Data Integrity Rules.
- Select CNC Global Integrity Rule.
- Click Remove Integrity Rule.



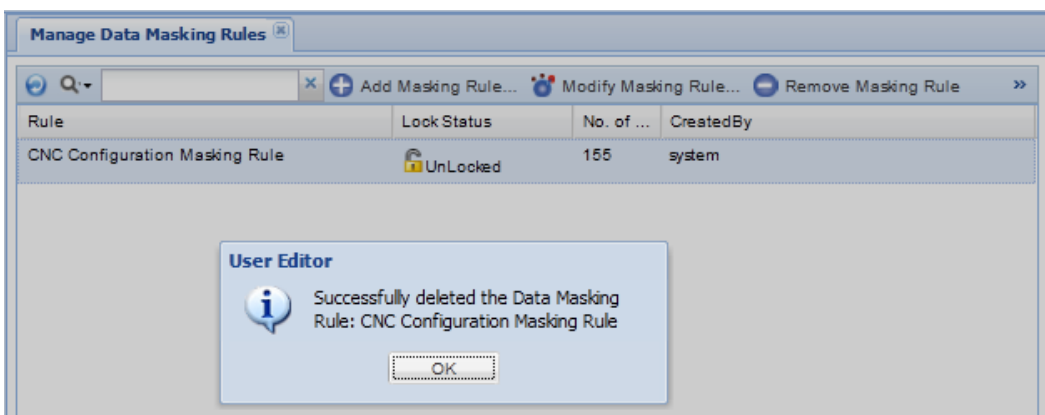
- Make sure that the rule was deleted.

Manage Data Masking Rules

This section describes the process for removing the data collection profiles:



- On the CSCP navigation pane choose Categories > Data Collection Settings > Manage Data Masking Rules.
- Select CNC Configuration Masking Rule.
- Click Remove Masking Rule.



- Make sure that the rule is deleted.



Note

ISO image: Initially the rule appears to be properly removed from the collector (as seen from CSPC – Browser), but it was not. The DPACP, Datasets and few more platform definition rules popped up after restarting the server.

Workaround: To avoid DPACP, datasets resurfacing in the ISO image when the collector needs to have rules upgraded, you need not restart server. But instead import w/ new rules, over the collector

ZIP & OVA Images: No issues if user follows the above mentioned order while deleting the rules.

The required work for deleting the existing rules from the collector has been completed. The next step in the rules upgrade process is installing the new rules package. Go to [Installing Rules Package in the CSPC](#) for details on performing the next part of the upgrade process

CSPC Collector Upgrade

This section describes the process of how to preserve, and then re-use some of the important data used by the collector when upgrading your collector to another release. Collector information that this section covers are the following areas:

- [What to Export](#)
- [What to Import](#)

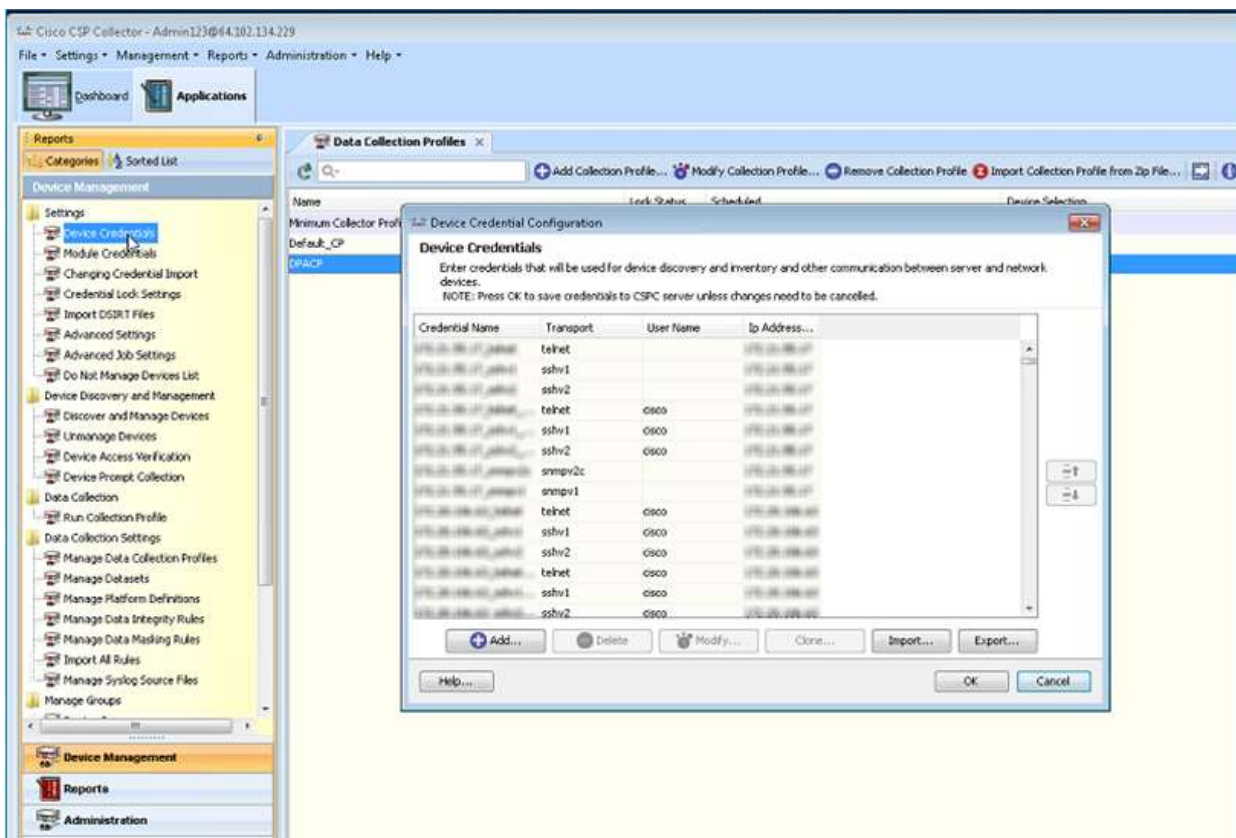
What to Export

The following sections identify the areas of data that can be exported before the performing the collector upgrade:

- [Device Credentials](#)
- [Managed Devices](#)
- [Discovery Jobs](#)

Device Credentials

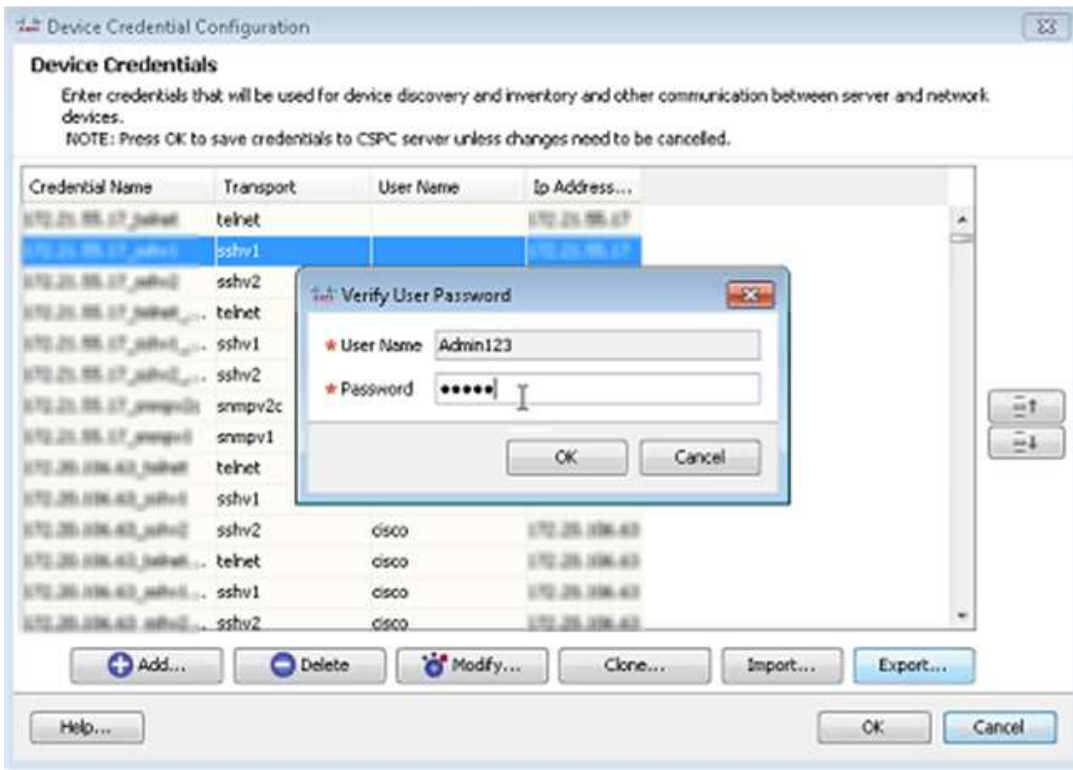
This section describes the process for exporting the device credentials:



- On the CSPC navigation pane choose **Categories > Device Management > Settings > Device Credentials**; the Device Credentials window appears.
- Select all the entries in the list.



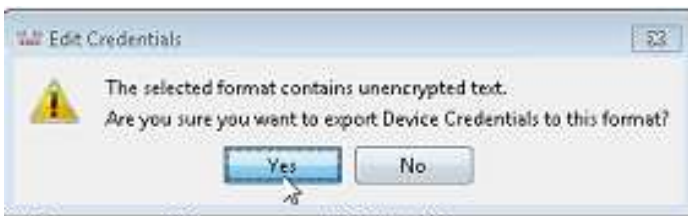
Note When you select none OR all entries, both of those options select ALL the devices in the list. If you select one or more entries then you will export only the devices you selected.



- Click **Export**, the Verify User Password window appears.
- Enter the user name and password, then click **OK**.



- Select the **Pari Device** option.
- Click **Browse** to designate what folder you want the exported file saved.
- Click **OK**, an Edit Credentials warning appears.



- The Edit Credentials warning provides a warning about unencrypted data being available in the chosen export format; click **Yes**.



- An informational message indicates the export was successful.



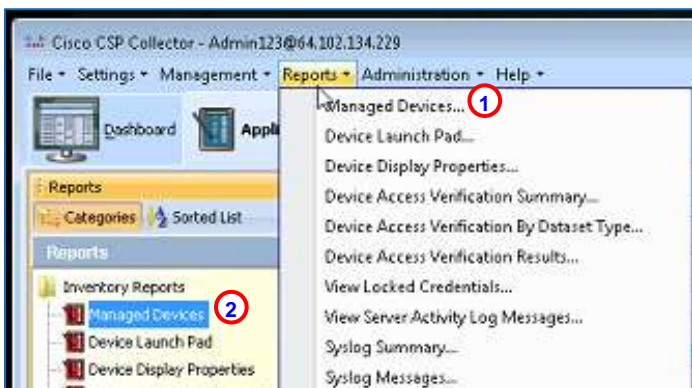
There is an entry id and entry name **1** for each device credential that was exported.



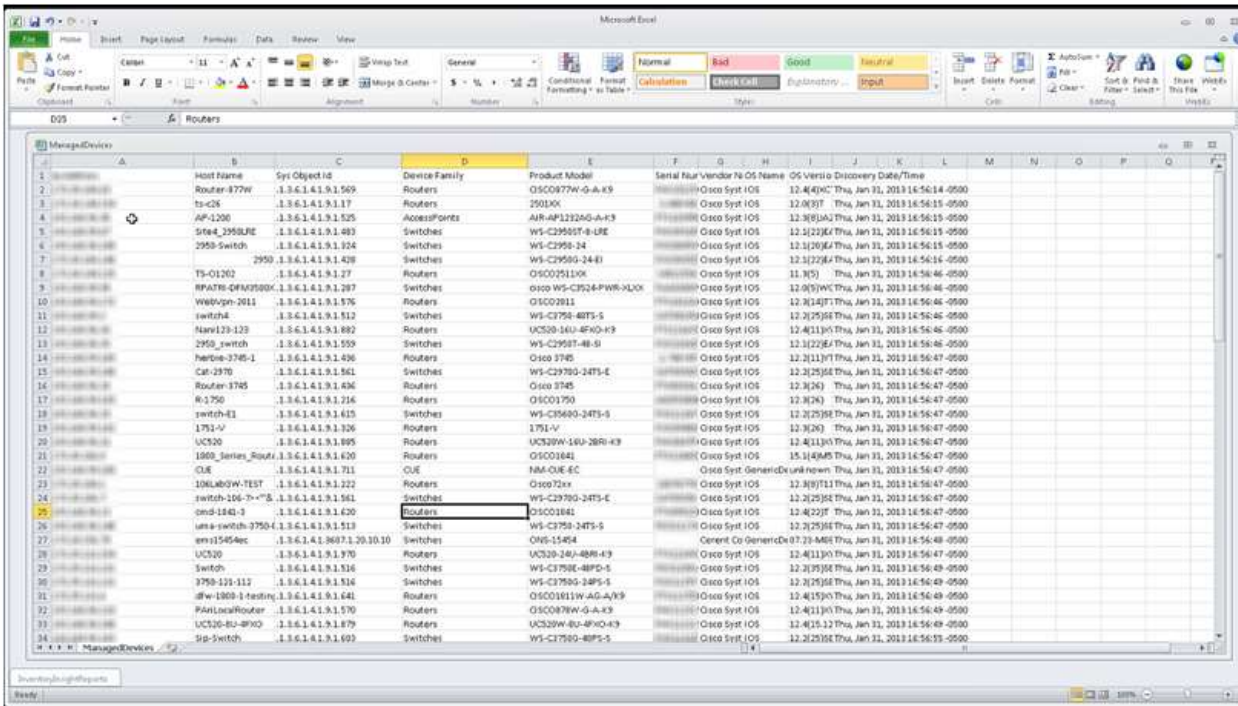
Note IP Address related info in the above graphic has been blurred out.

Managed Devices

This section describes the process for exporting the Managed Devices information:



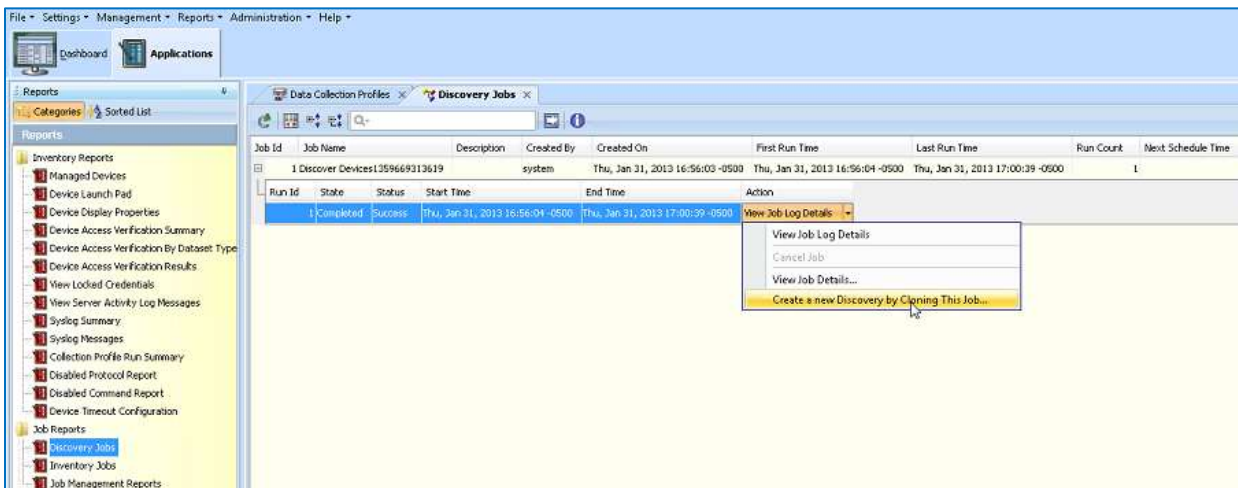
- There are two ways to access the Managed Devices data, from the menu **1** or navigation pane. **2**




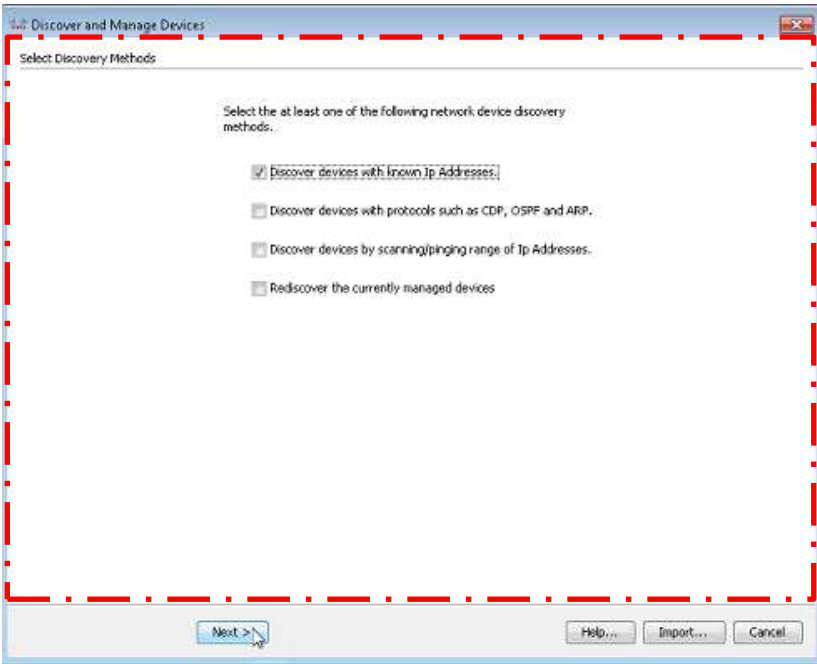
- Since the exported Managed Devices data is CSV (Comma Separated Value) data, the Info can be viewed in an Excel spread sheet.

Discovery Jobs

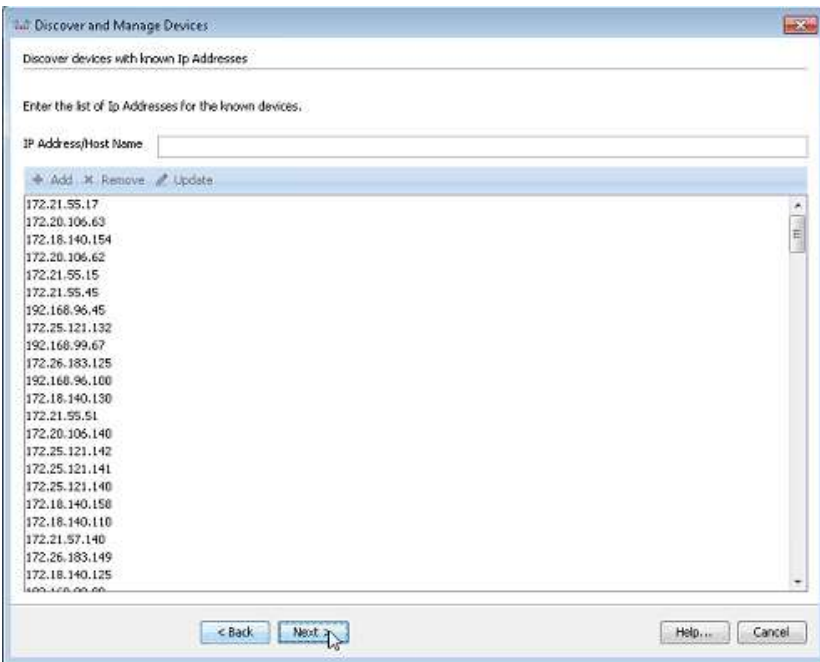
This section describes the process for exporting the Discovery Jobs information:



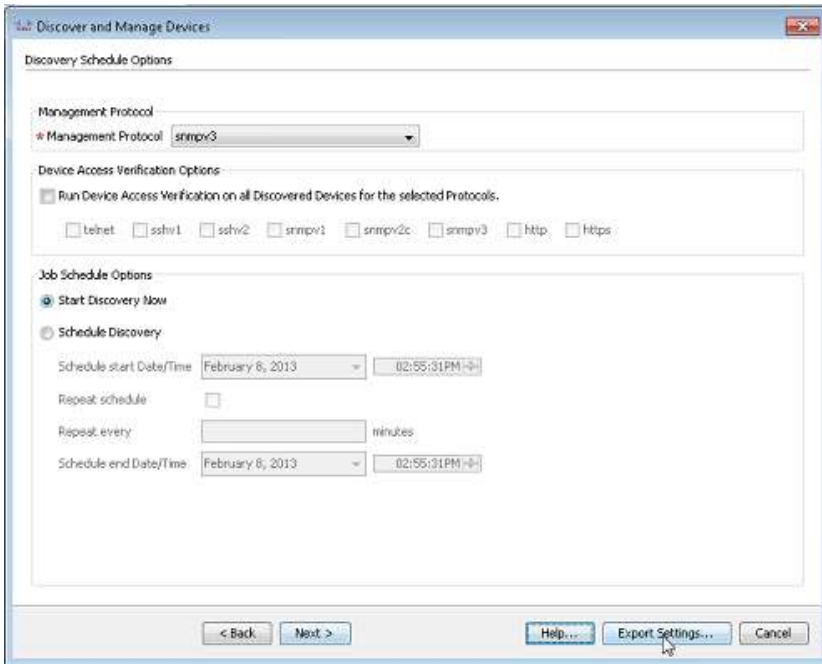
- On the CSPC navigation pane choose **Categories > Job Reports > Discovery Jobs**; the Discovery Jobs window appears.
- Click the **View Job Log Details** drop-down list, then click **Create a new Discovery by Cloning This Job ...** option. The Discover and Manage Devices window appears, displaying the Select Discovery Methods pane. 



- Check the Discover devices with known IP Addresses check box.
- Click **Next**; the Discover devices with known IP Addresses pane appears.



- The Discover devices with known IP Addresses pane lists all the IP Addresses known by the collector. Click **Next**; the Discovery Schedule Options pane appears.



- On the Discovery Schedule Options pane click **Export Settings**.
- For Firefox goes directly to the download section

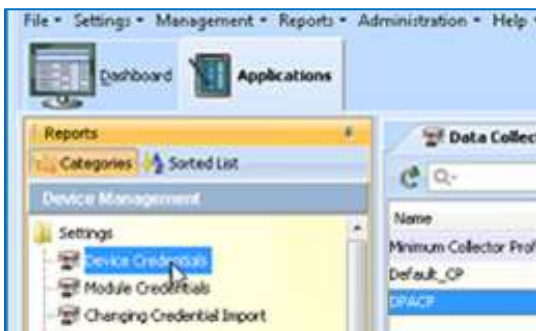
What to Import

This section identifies the areas of data that can be imported after performing the collector upgrade, and the [data was previously exported](#) before the upgrade. The following sections identify the areas of data that can be exported before the performing the collector upgrade:

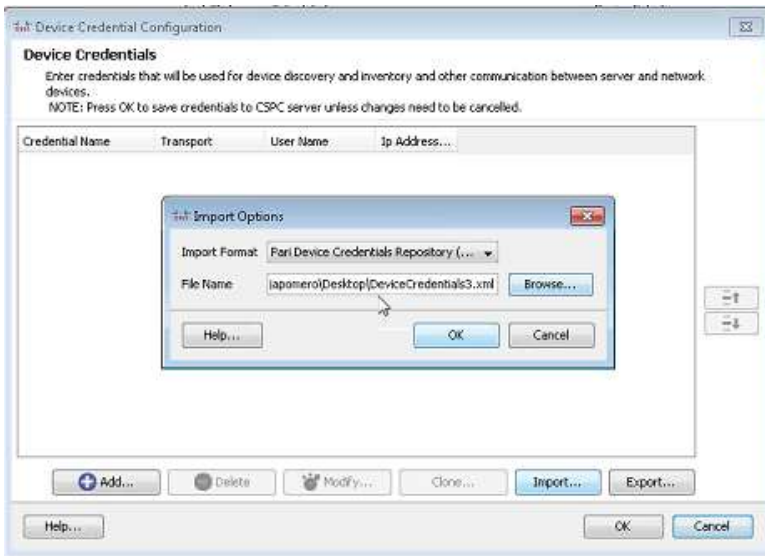
- [Import of Device Credentials](#)
- [Discover and Manage Devices](#)
- [Import Discovery Jobs](#)

Import of Device Credentials

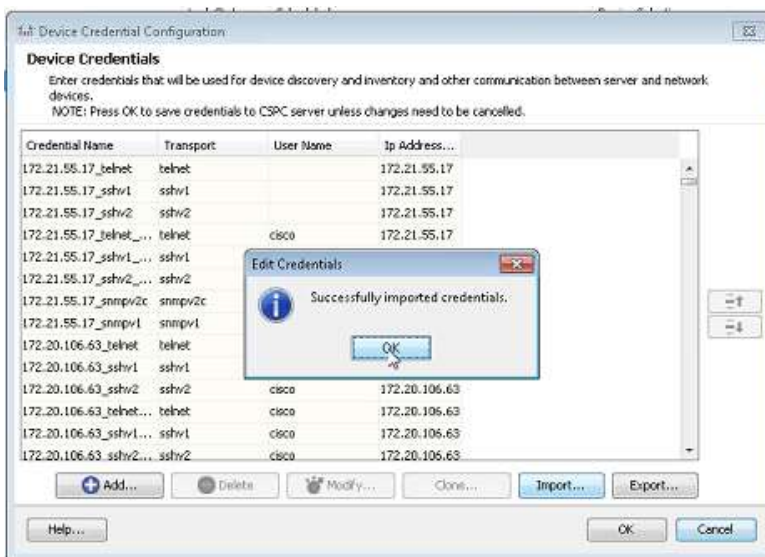
This section describes the process for importing the device credentials, after performing the collector upgrade:



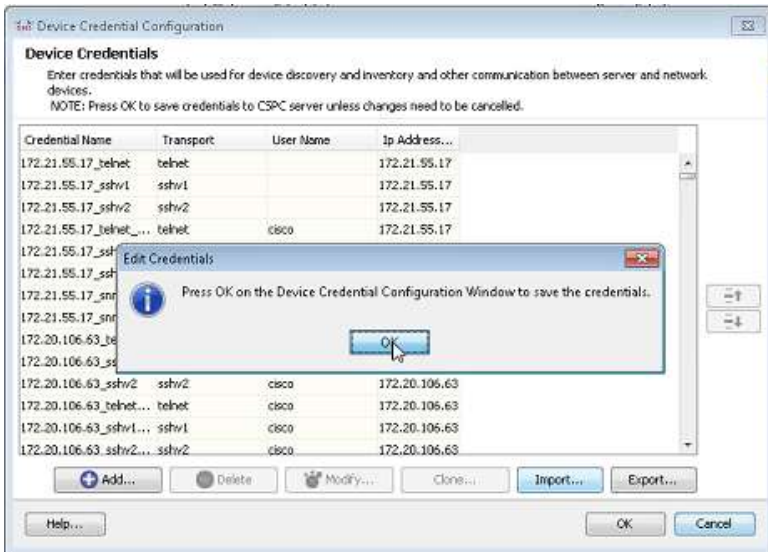
- On the CSPC navigation pane choose **Categories > Device Management > Settings > Device Credentials**; the Device Credentials window appears.



- Click **Import**; the Import Options window appears.
- In the Import Format field specify **Pari device ...**
- Click **Browse**, then indicate the name and location of the previously exported device credentials file.
- In the Import Options window click **OK**, the previously exported device credentials are loaded into the Device Credentials window.



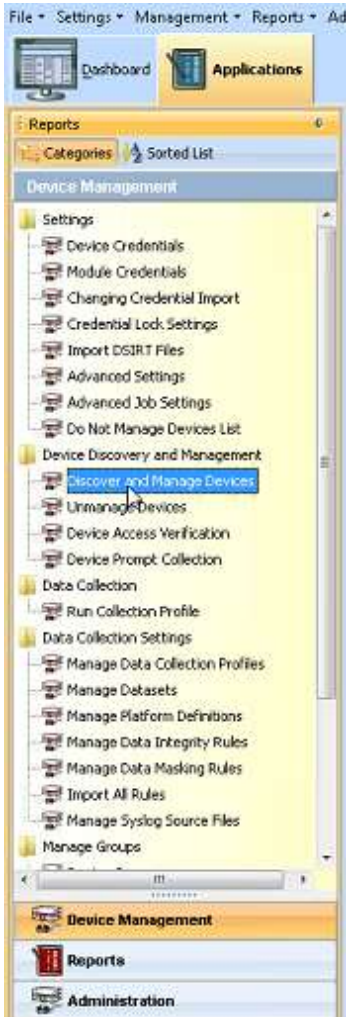
- An informational window indicates a successful import, click **OK**; an Edit Credentials window appears.




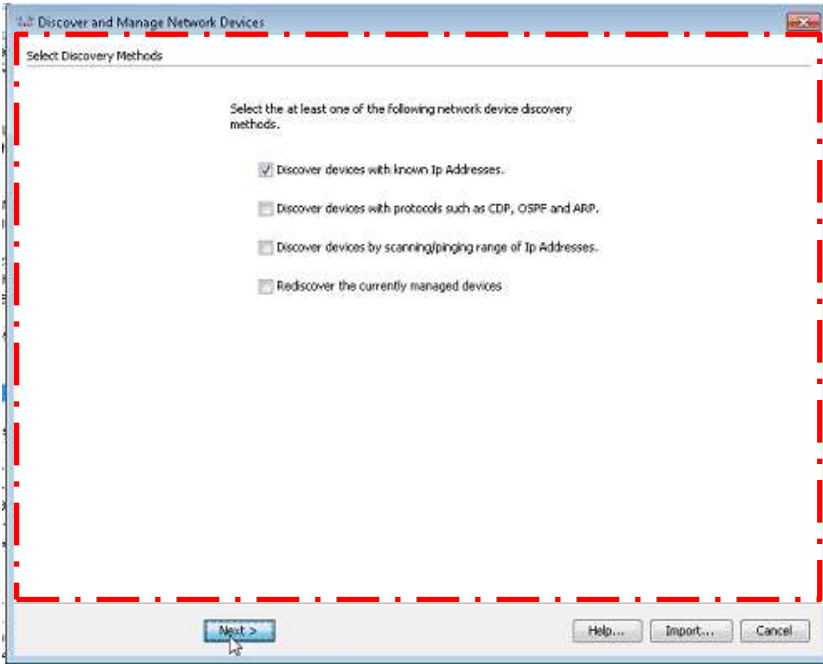
- In the Edit Credentials window click OK, this saves the credentials

Discover and Manage Devices

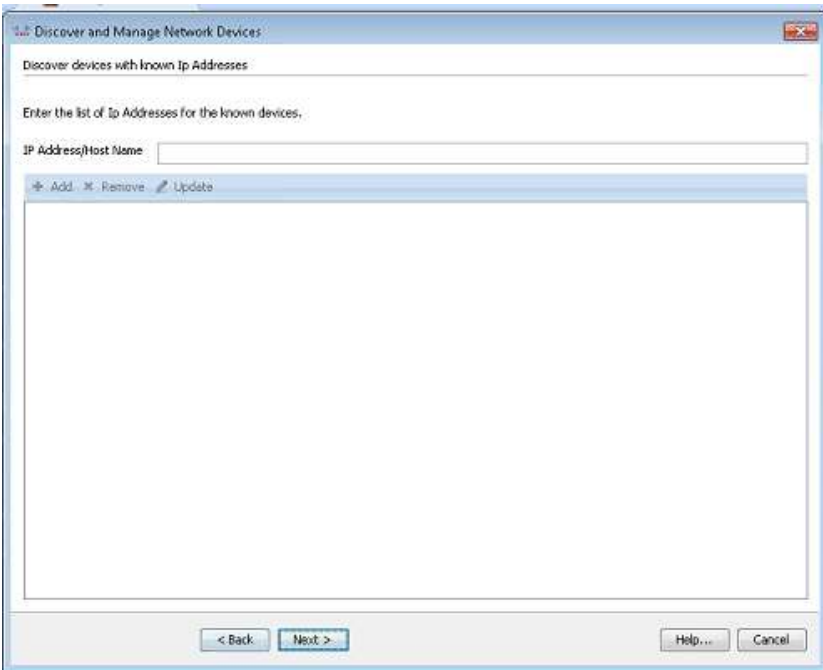
This section describes the process for importing the Managed Devices data, after performing the collector upgrade:



- On the CSPC navigation menu choose **Categories > Device Management > Settings > Discover and Manage Devices**; the Discover and Manage Network Devices window appears, displaying the Select Discovery Methods pane. 



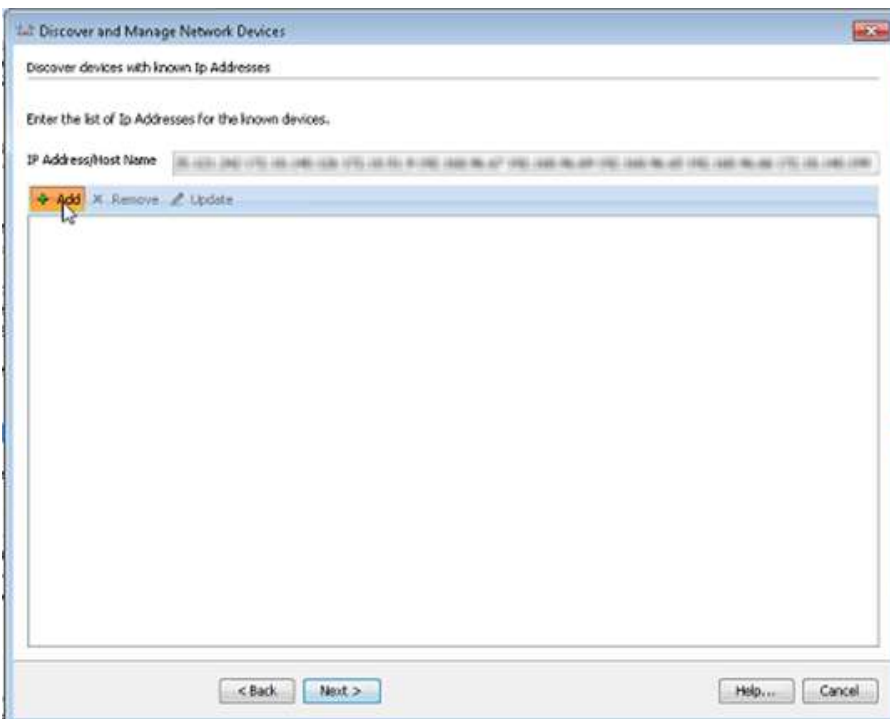
- Check the Discover devices with known IP Addresses check box.
- Click **Next**; the Discover devices with known IP Addresses pane appears.



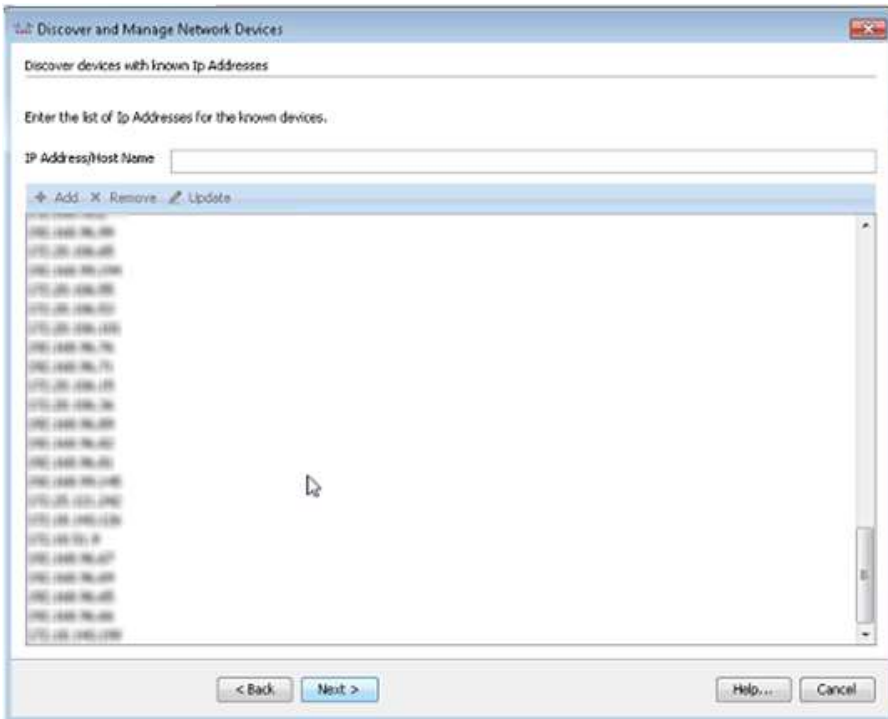
- The next step is to enter the IP Addresses into the IP Address/Host Name field.
- Open the exported Managed Devices data file, which was saved as CSV data in the [Managed Devices export option section](#).

	A	B
1	Ip Address	Host Name
2	172.20.106.43	Router-877W
3	172.20.106.1204	ts-c26
4	172.20.106.45	AP-1200
5	172.20.106.47	site4_2950LRE
6	172.20.106.100	2950-Switch
7	172.20.106.100	2950
8	172.20.106.1205	TS-O1202
9	172.20.106.96	RPATRI-DFM3500X
10	172.20.106.170	WebVpn-2611
11	172.20.106.2	switch4
12	172.20.106.96	Nani123-123
13	172.20.106.96	2950_switch
14	172.20.106.100	herbie-3745-1
15	172.20.106.100	Cat-2970
16	172.20.106.26	Router-3745
17	172.20.106.100	R-1750
18	172.20.106.26	switch-E1
19	172.20.106.100	1751-V
20	172.20.106.26	UC520
21	172.20.106.9	1800_Series_Route
22	172.20.106.100	CUE
23	172.20.106.1	106LabGW-TEST
24	172.20.106.7	switch-106-7-4"
25	172.20.106.13	cmd-1841-3
26	172.20.106.100	uma-switch-3750-t
27	172.20.106.76	ems15454ec
28	172.20.106.100	UC520
29	172.20.106.100	Switch
30	172.20.106.100	3750-121-112
31	172.20.106.4	dfw-1800-1-testing

- In the Excel spread sheet that contains all the exported managed devices data, copy all the IP Addresses that are located in the first column.



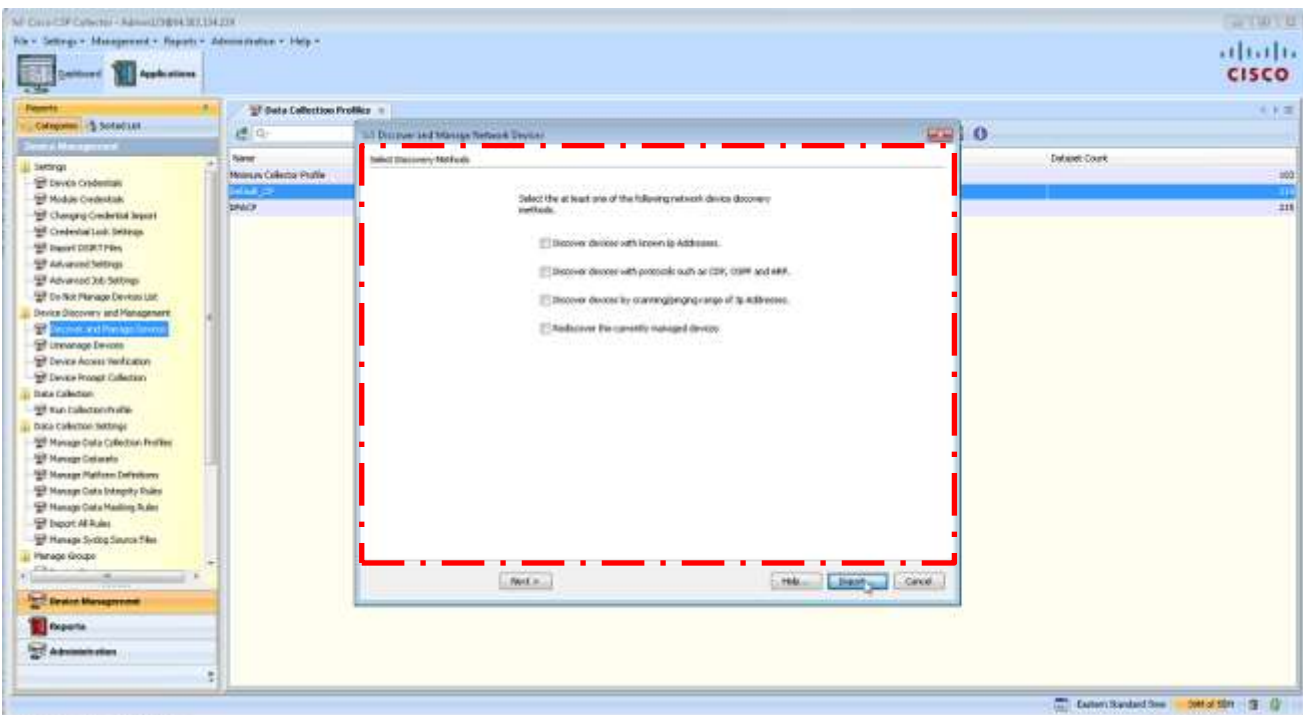
- Paste the spread sheet IP Addresses into the IP Address/Host Name field, then click **Add**.



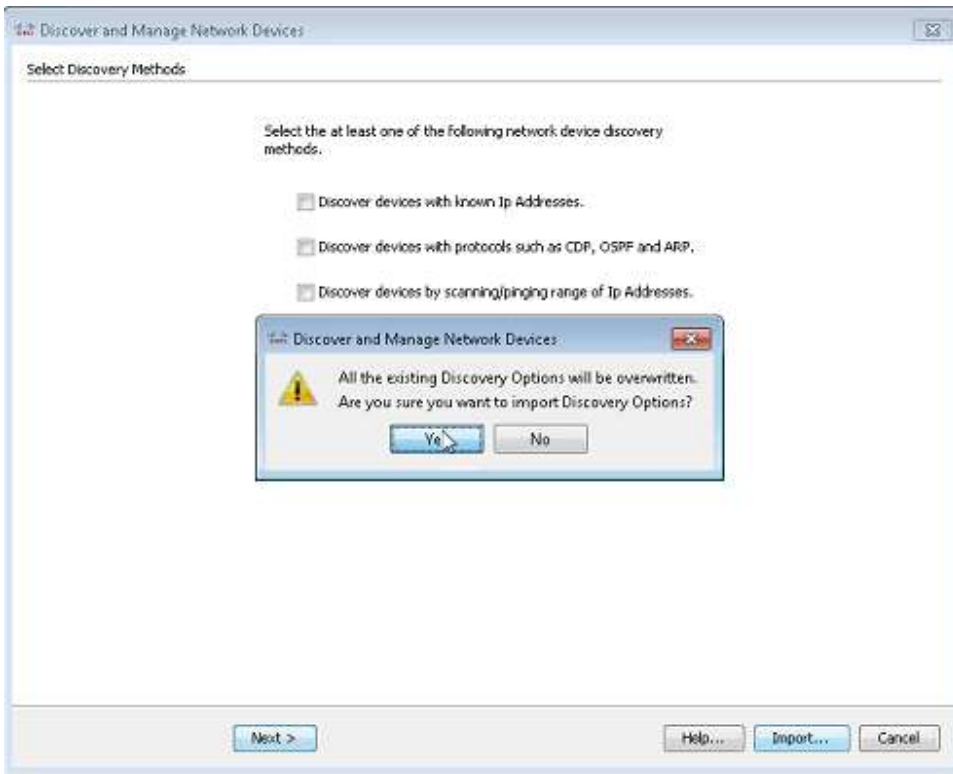
- The IP Addresses are added into the section below. From now on when you open the Discovery and Manage Devices window all the devices from the previous release will be identified and ready for use.

Import Discovery Jobs

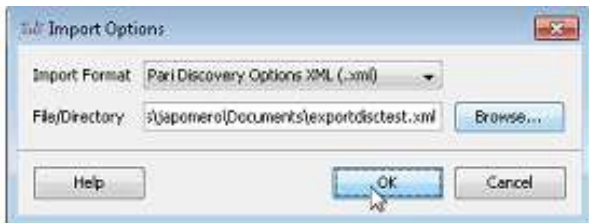
This section describes the process for importing Discovery Jobs, after performing the collector upgrade. The importing of Discovery Jobs is performed by using the Discovery and Manage Devices function.



- On the CSCP navigation menu choose **Categories > Device Management > Settings > Discover and Manage Devices**; the Discover and Manage Network Devices window appears, displaying the Select Discovery Methods pane. 



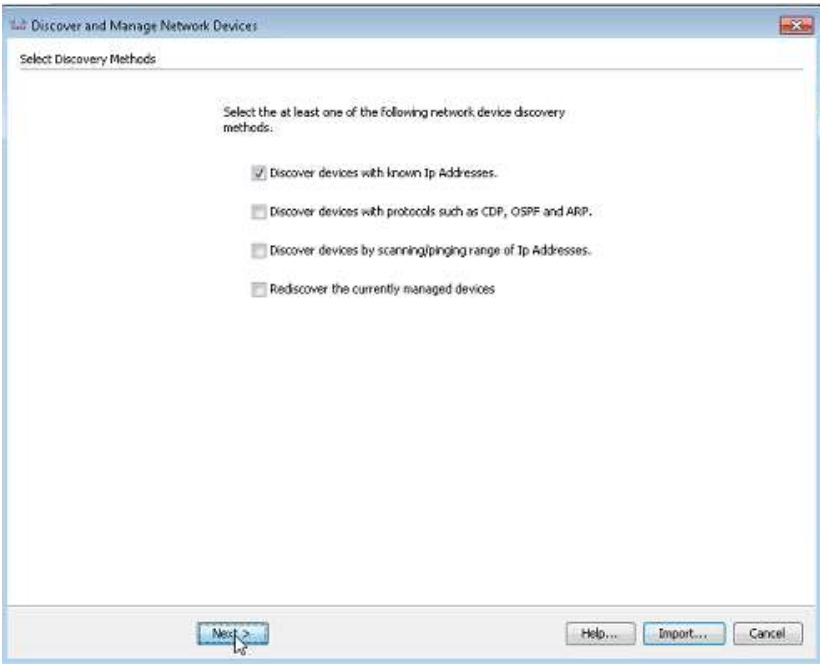
- A warning message appears about overwriting all the existing Discovery Options ..., click Yes.



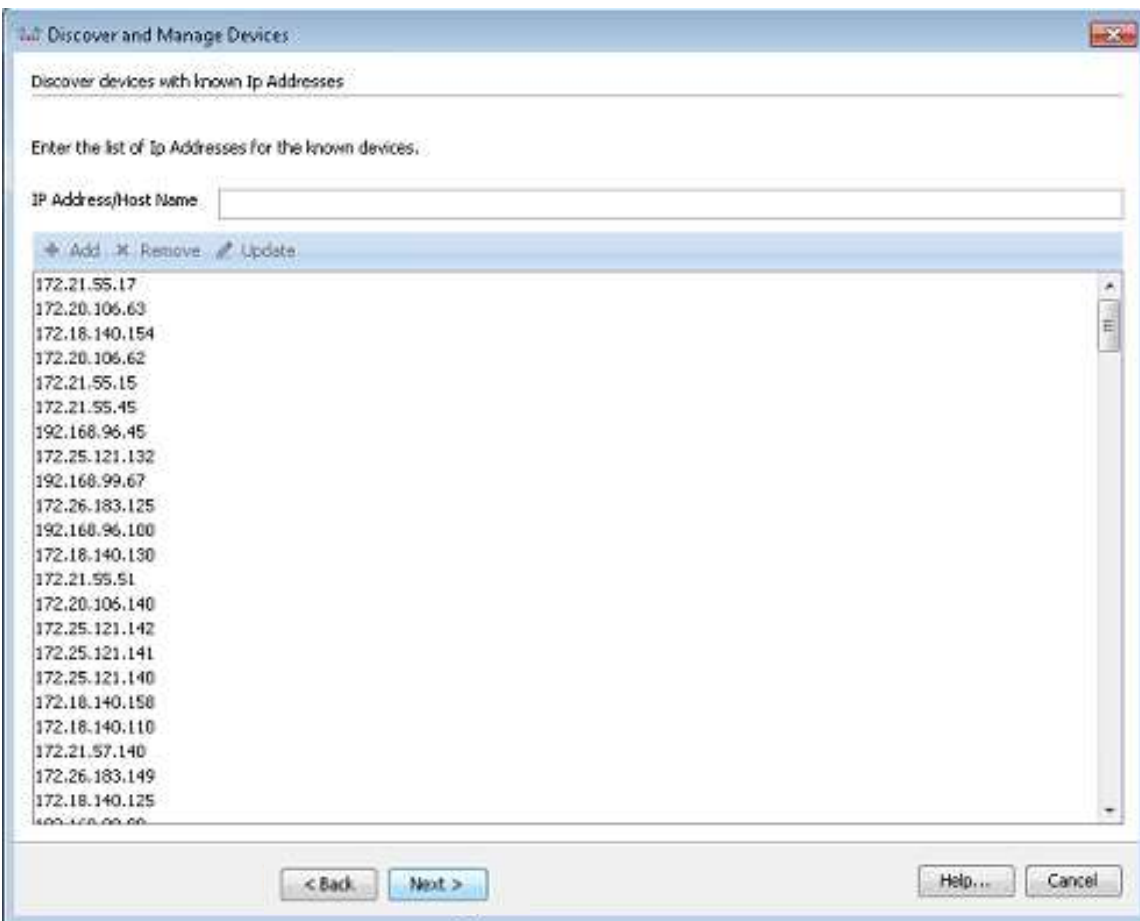
- Specify **Pari Discovery ...** for the export format.
- Click **Browse** and specify the location to save the export file.
- Click **OK** to perform the import.



- An informational message appears indicating that the import of the discovery settings was successful.



- In the Select Discovery Methods pane check the **Discover devices with known IP Addresses** check box.
- Click **Next**; the Discover devices with known IP Addresses pane appears.



- The IP Addresses that were exported in the [Discovery Jobs export process](#) appear in the pane.

Software Image Upgrades

Software image upgrades allows small code updates to be applied without having to redeploy a whole image on an appliance. This section covers the following areas that are related to software image upgrades:

- [LCM Agent Manager](#)
- [Appliance Interface](#)
- [Software Image Build Setup](#)
- [Perform a Patch Upgrade](#)

LCM Agent Manager

The Life Cycle Management (LCM) Agent Manager is located in the Cisco backend and supports different types of services (SNTC, PSS, Smart Call Home, and RMS). The interaction with the LCM Agent Manager is done through a CLI. The LCM Agent Manager manages the versioning of the software components that are going to be added to the appliance. So instead of having to redeploy a whole image when a fix for a problem is available, the LCM Agent Manager provides support for service pack updates, which is a small code update that fixes a specific problem. The LCM Agent Manager also provides support for release and rules packages, and data profiles.

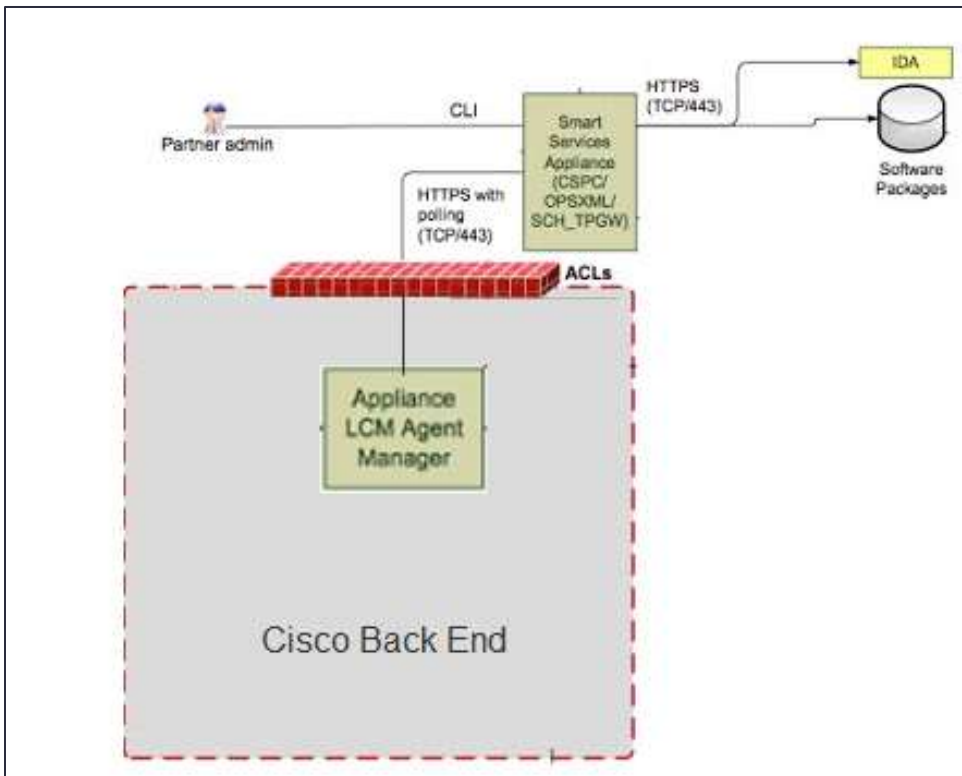
The software packages are loaded into a production data repository called Intelligent Download Application (IDA), which allows any Cisco device to be enabled for patch support. IDA also provides an infrastructure that supports automatic updates. IDA also maintains a list of 'notorious IP addresses'. If an appliance was trying to download software from a device that had a 'notorious IP address', then that download would be blocked by IDA.

Appliance Interface

There are different appliance interfaces that are used in the software image upgrade process. There is a CLI that the partner admin can use, that is used for various show and configure commands that enable on-demand and auto-update image upgrades.

There is also a browser based graphical user interface (GUI), which is also referred to as a 'thin-client'. The browser thin-client replaces the previous CSPC client interface, which also referred to as a 'thick-client'. The browser GUI provides access to the CSPC administrator console that includes a tab for user registration. The browser user interface uses a secure HTTPS connection that utilizes TCP port 443.

The appliance also has an IDA interface that connects the appliance to the IDA software image server. This interface is where the appliance gets access to all the different software images that are used to update key areas of the deployment image.



Software Image Build Setup

The software image build is made of several software components that provide different functions for the appliance:

- Package-type indicates the type of package (for example, service pack, rules, data profile).
- Version represents the version the package is supporting (in example, service pack sp-2.0.0-0-0 for a 64 bit Linux OS).
- Component identifies what functional component is being supported (in example, DPA and its version 1.1 and the CSCP base level 2.2.0.1 that it runs on).
- The components listed below are combined into the JEOS (Just Enough Operating System) package:
 - Serviceability function and its version.
 - ConscoTgw is the tail end gateway that provides the connectivity connection.
 - Jetty is the webserver component that provides the thin-client web-browser interface.
 - Adminshell component represents the LCM Agent function.
 - Hardened CentOS is the 64 bit operating system.

```

Package-type : ServicePack
Version      : sp-2.0.0-0-0-lnx64

Component   : CSPC DPA Add-on
Version     : 1.1
Component   : CSPC Base
Version     : 2.2.0.1
Package-type : JeOS
Version     : jeos-2.0.0-0-lnx64
Component   : Serviceability
Version     : 1.0.9
Component   : ConcsoTgw
Version     : 1.4.2
Component   : Jetty
Version     : 7.1.0
Component   : AdminShell
Version     : 0.7
Component   : Hardened CentOS
Version     : 6.3 patch #0

```

Perform a Patch Upgrade

There are two ways to download a software image and perform a patch upgrade:

- [On-Demand Option](#) – user indicates that they want to download the software image now.
- [Auto-Update Option](#) – user configures a policy that specifies a certain time frame when they want the updates checked, downloaded and possibly applied.

On-Demand Option

The On-demand option uses the following commands in the software image download process:

- **show server-connection** – indicates whether there is a connection to the software image server.
- **conf server-connection enable | disable** – enables or disables the connection to the software image server.
- **check update** – shows what software images are available for download
- **download *version_number*** – downloads the selected collector software image.
- **show download** – shows what software images have been downloaded.
- **apply *version_number*** – installs the specified downloaded software image.
- **show apply** – shows which downloaded software images have been installed and what their status is.

Verify the Server Connection

Before downloading a software image you must first verify that you have a connection to the server that provides the software images. To verify the connection to the image server, perform the following steps:

```
admin# sh server-connection
Connection with server for Software Updates is currently disabled.
admin#
admin#
admin# conf server-connection enable
This operation will enable connection with server for Software Updates.

  CCO Id   : alele
  Password :

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

Operation succeeded.
admin#
admin# sh server-connection
Connection with server for Software Updates is currently enabled.

  CCO Id       : alele
  Appliance ID : CSP0001004320
  Enabled date  : 09 May 2013 19:52:22 UTC
admin#
```

- Enter the **show server-connection** command; the response indicates whether your server connection is enabled or not.
- If your server connection is not enabled, then enter **conf server-connection enable**.
- You will be prompted to enter your CCO Id username and password.



Note The CCO id and password prompt is to comply with export regulations. The CCO Id /password is the best way to ensure that restricted countries do not get access to the software images. The IDA server uses the CCO Id authentication to block attempted image downloads from any restricted country.

- Answer the 'Would you like to continue' prompt with a 'y' to continue.

Check Updates

Once the server connection is determined to be available, then you can check to see if there are any updates available. Enter the **check update** command to see if any updates are currently available. If there are then a list of the available updates will be displayed.

Download the Software Image

When there are available software images to be downloaded then perform the following steps:

```
admin# download sp-3.0.1-0-0-lnx64
Requested package has been downloaded.

Do you want to download it again [y|n]? y

Connecting to Software Download Server using User Id 'alele' ...

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
```

- Enter the download `version_number` command, where `version_number` represents the software image version number.
- You will be prompted with a EULA; enter 'y' to continue the download.



Note See [Accessing the IDA Software Image Server](#) for more details EULA and software image access.

```
admin#
admin# show download
      Version           : sp-3.0.1-0-0-lnx64
      Downloaded File   : sp-3.0.1-0-0-lnx64-package.zip
      Status            : Downloaded
      Start Time        : May/02/2013 20:58:27
      End Time          : May/02/2013 20:58:34
      Completed %      : 100.0
admin#
```

- Enter the `show download` command to see what software images have been downloaded and what their associated status is.

Apply the Software Image

After the software image has been downloaded, then apply the image to the appliance, by performing the following steps:

```
admin#
admin# apply sp-3.0.1-0-0-lnx64
Requested package has been applied.

Do you want to apply it again [y|n]? y

After installation of package, affected services will be restarted.

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

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

- Enter **apply** `version_number` to install the specified software image.

```
admin#
admin# sh apply
      Version Number    : sp-3.0.1-0-0-lnx64
      Status            : Apply-failed
      Start Time        : May/09/2013 19:56:16
      End Time          : May/09/2013 19:56:17
      Reason            : Installation of package "sp-3.0.1-0-0-lnx64.zip" failed
admin#
```

- Enter **show apply** to find out the status of a previous apply.


```

admin# sh ver -d
  Build-name      : SE 1.6 Maintenance Build 1

  Package-type   : ServicePack
  Version        : sp-3.0.1-0-0-lnx64
    Component    : CSPC DPA Add-on
    Version      : 1.2
    Component    : CSPC SE Add-on
    Version      : 1.1
    Component    : CSPC Base
    Version      : 2.2.0.4
  Package-type   : JeOS
  Version        : jeos-3.0.1-0-lnx64
    Component    : Serviceability
    Version      : 1.0.9
    Component    : ConcsoTgw
    Version      : 1.4.2
    Component    : Jetty
    Version      : 7.1.0
    Component    : AdminShell
    Version      : 0.7.1
    Component    : Hardened CentOS
    Version      : 6.4 patch #0

admin# █

```



Note Use **show version -d** to see details of the current build and verify info from the show apply command.

Auto-Update Option

This option lets the user configure a policy that specifies certain parameters that identify when they want the updates checked and downloaded and for what types of software images.

The conf auto command has several parameters that can be used in the configuration of the auto-update.

The parameters can be any of the following items:

- A specific day / time (by itself)
- Minor update, with/without a specified time
- Maintenance with/without a specified time
- Patch with/without a specified time

An example of some of these autoupdate options are shown below:

```

admin#
admin# conf auto
Invalid Option specified
-----
Usage:
admin# conf autoupdate [<level>] <schedule> [-W]
Eg:
admin# conf auto Sat 8:30 PM
admin# conf auto minor Tuesday 11:00 PM -W
admin# conf autoupdate maintenance Thursday 1:00 AM
admin# conf autoupdate patch Daily 2:00 AM
-----
admin#

```



Note The `-W` option will perform a download, but not apply the software image to the appliance.

```

admin#
admin# sh auto
Current:
    maintenance Friday 6:46 PM
    minor Saturday 8:30 PM
    data Daily 12:00 AM
admin#

```

- The `show auto` command displays the current auto-update settings.

Accessing the IDA Software Image Server

On the appliance, when you enter the [download request command](#), you are requesting a specific software image from the IDA Software Image Server.

This IDA server provides the CSPC server appliance access to different software images that are used to update key areas of the deployment image. The IDA server provides Cisco devices the ability to perform patch upgrades, instead of having to redeploy the whole image in order to obtain a software update.

When you access the IDA server the first time you are required to provide your CCO Id login credentials and sign an End User License Agreement (EULA). The CCO Id login and EULA is an export verification requirement that validates the user and ensures that software images are not being downloaded to countries listed in the restricted list.

When you access the IDA Software Image Server the first time, you will see the following message and link:

CCO Id is not authorized to download encrypted software. Please register for this service using below URL and try again.

<http://tools.cisco.com/legal/k9/controller/do/k9Check.x?eind=Y>

Click the above URL; the CCO Id window appears

Log In

Choose language of Login: English

Log into an Existing Account

User Name

Password

[Forgot your user ID and/or password?](#)

- Enter your CCO login credentials; the EULA window appears.

CISCO

Click Accept - Cisco Systems

Instructions

To apply for eligibility to download strong encryption software images:

1. Ensure the address listed in your [Cisco.com User Profile](#) is correct and complete.
2. **Read each of the conditions below carefully prior to selecting your answer.**
3. Type your full name in the field provided.
4. Submit this form.

Conditions

1. Cisco software images are subject to United States (U.S.) national security, foreign policy, anti-terrorism laws, export regulations and other national local laws.

I agree to secure Cisco software images in a manner that prevents unauthorized access or transfer. Certain persons, countries or entities may require a U.S. export license in order to obtain restricted Cisco images. Detailed information regarding compliance with U.S. use, export, re-exports, and transfer laws may be found at: http://www.cisco.com/ww/espoticompliance_provisions.html. The lists of restricted entities is available at: <http://www.bis.doc.gov/ComplianceAndEnforcement/ListsToCheck.htm>

I shall not electronically or physically transfer Cisco software images to any unauthorized persons, countries or entities, identified at the aforementioned web pages, without first obtaining required export authorizations or licenses from the U.S. and any local governments.

2. I am not on any of the following U.S. denied persons lists:
 - [Table of Denial Orders](#) (U.S. Department of Commerce)
 - [Specially Designated Nationals List](#) (U.S. Department of Treasury, Office of Foreign Assets Controls (OFAC))
 - [Debarred List](#) (U.S. Department of State)
3. I agree to abide by all [export, import, use](#), and development and/or re-export laws in the country in which I reside. I understand and agree that Cisco Systems, Inc. is not responsible for the recipient's failure to abide by any such law.
4. I agree to [contact Cisco's Export Compliance and Regulatory Affairs group](#) if I know or have reason to believe that another party has or intends to violate U.S. export laws or local country export laws.
5. I will not knowingly transfer (physically or electronically) [strong encryption](#) images to [denied persons, sanctioned entities, territories, or uses](#) without ensuring compliance with U.S. and local laws and regulations.
6. I will not knowingly transfer (physically or electronically) [strong encryption](#) images to, or for, [government organizations/enterprises](#) other than those of, or in: Austria, Australia, Belgium, Canada, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Italy, Japan, Latvia, Lithuania, Luxembourg, Malta, Netherlands, New Zealand, Norway, Poland, Portugal, Slovakia, Slovenia,

- Read each EULA condition, then scroll to the bottom of the EULA.

Common Services Platform Collector Quick Start Guide

Austria, Australia, Belgium, Canada, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Japan, Latvia, Lithuania, Luxembourg, Malta, Netherlands, New Zealand, Norway, Poland, Portugal, Slovakia, Slovenia, Spain, Sweden, Switzerland, United Kingdom, United States.

without written authorization from Cisco Systems, Inc. and/or the governments of the United States, United Kingdom, and The Netherlands.

7. I will not supply network services (e.g., routing a virtual private network) to, or for [government organizations/businesses](#) other than those of, or in:

Austria, Australia, Belgium, Canada, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Japan, Latvia, Lithuania, Luxembourg, Malta, Netherlands, New Zealand, Norway, Poland, Portugal, Slovakia, Slovenia, Spain, Sweden, Switzerland, United Kingdom, United States.

without written authorization from Cisco Systems, Inc. and/or the governments of the U.S., United Kingdom, and The Netherlands.

8. I agree to notify, consignee and end-user of conditions **4, 5, 6 & 7** above.

If you are unable to comply with each and every condition as set forth above, please [contact Regulatory Affairs](#).

By clicking the Accept button below, I hereby verify that I, as a duly authorized representative of the organization identified by the [Cisco.com User Profile](#), understand and agree to abide by the conditions set forth above regarding the usage of Cisco Systems, Inc. hardware and/or software.

USER DETAILS	
First Name	EMA
Last Name	Demo
E-Mail	emademo1@gmail.com
COO User ID	emademo1
Business division's function *	<input checked="" type="radio"/> Commercial/Chilian entity <input type="radio"/> Government entity, a Military entity or Defense Contractor If Government entity, a Military entity or Defense Contractor, see also in: Austria, Australia, Belgium, Canada, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Japan, Latvia, Lithuania, Luxembourg, Malta, Netherlands, New Zealand, Norway, Poland, Portugal, Slovakia, Slovenia, Spain, Sweden, Switzerland, United Kingdom or the United States. <input type="radio"/> Yes <input checked="" type="radio"/> No
Confirmation *	<input checked="" type="checkbox"/> By checking this field, I hereby verify that I, as a duly authorized representative of the organization, understand and agree to abide by the conditions set forth above regarding the usage of Cisco Systems, Inc. hardware and/or software.

Accept **Decline**

Document ID: #02_200802_02154033

© 1992-2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

- Verify the user details information, then click **Accept**; you are provided access to the requested download software image.

Inventory Upload

There are several different processes that are required to perform an inventory upload, those processes are:

- [Discover the Devices](#)
- [Create and Manage Datasets](#)
- [Manage Data Collection Profiles](#)
- [Run Collection Profile and Upload Data](#)

Discover the Devices

This process helps us find what devices are available in the customers managed network and then manage them. There are several ways to find those devices:

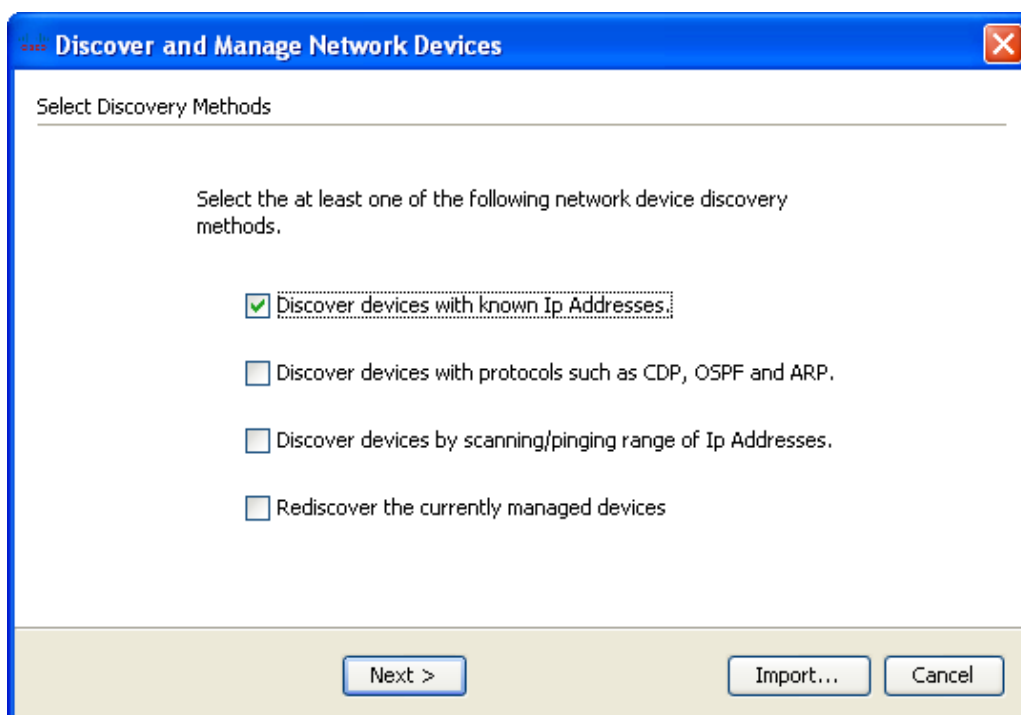
- Add devices manually.
- Use a seed file.
- Use the discovery process.

To use a seed file refer to the information contained in the following documents:

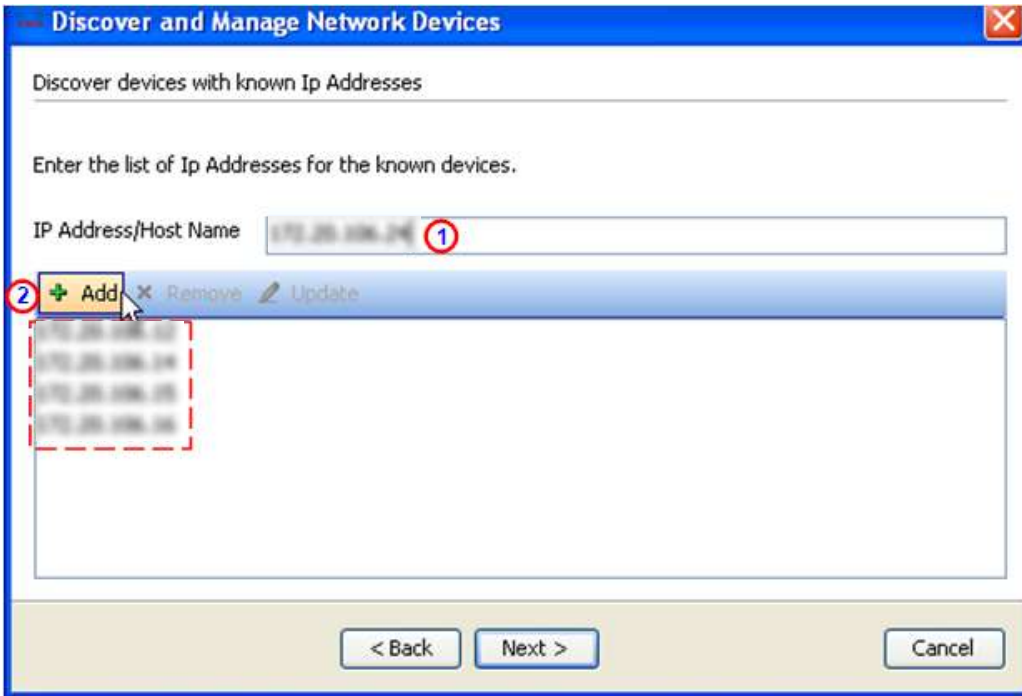
- Seedfile Maintenance Guide
http://www.cisco.com/web/partners/services/programs/collaborative/downloads/services_seedfile_maintanance_user_guide.pdf
- Installed Base Management & Alert Deployment Guide
http://www.cisco.com/web/partners/services/programs/collaborative/downloads/services_pss_install_base_management_and_alerts_deployment_guide.pdf


To discover the devices perform the following steps:

- On the browser menu choose **Management > Discover and Manage Devices**; the Discover and Manage Network Devices window appears.

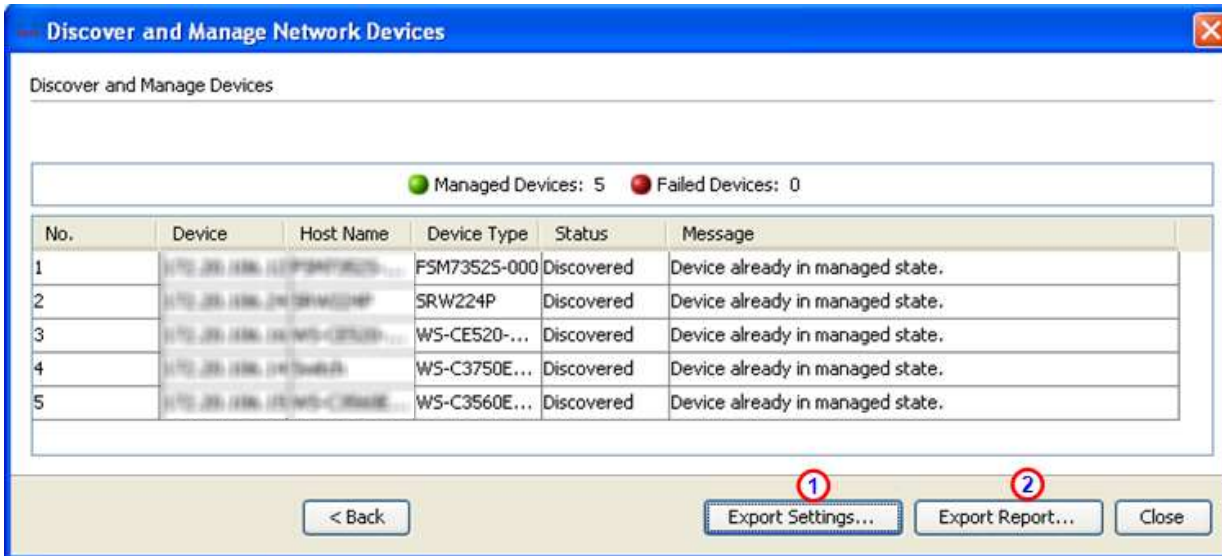


- Check the check box for the method you want to use for discovery, then click **Next**; the pane associated to the method you selected appears.



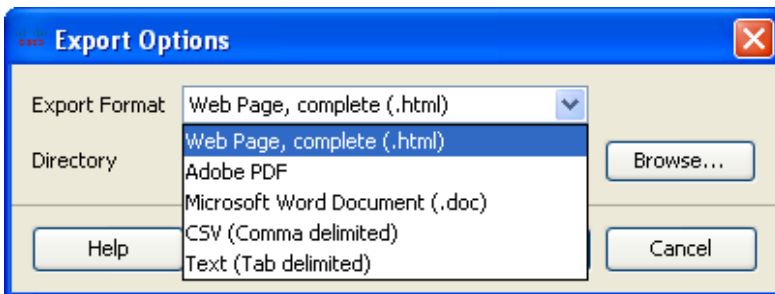
- Enter the IP Addresses that you want discovered in your network. Place the IP Address in the IP Address/Host Name field ① then click **Add**, ② or press the enter key; the IP Address is added to the IP Address list. 
- Click **Next**; the Discovery Schedule Options pane appears.

- Specify the type Management Protocol 1 you want to use (for example snmpv2c) for the discovery process; this is a required field as noted by the red asterisk *.
- If you want to verify if the discovered devices have specific protocols enabled, then perform the following steps:
 - In the Device Access Verifications Options area, check the **Run Device Access Verifications ...** check box. 2
 - Select the associated check box for each protocol you want verified (for example telnet, sshv1, sshv2, etc.) on the discovered devices.
- You have two options for scheduling a discovery in the Job Schedule Options area: 3
 - Click the **Start Discovery Now** radio button. 3
 - Click the **Schedule Discovery** radio button, 4 and then specify the time frame parameters you want in the Schedule Discovery area. 4
- Click **Next**; there are different responses to this depending on the previous option that was selected:
- If a Start Discovery Now option was selected then the discovery process starts immediately and presents the results of the discovery.



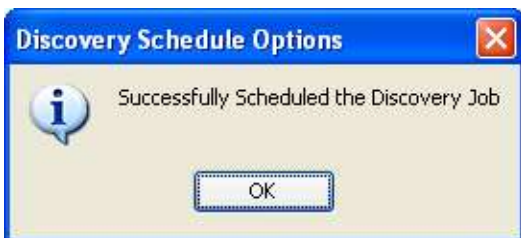
Note The discovery options can be saved and used later by clicking the **Export Settings...** button. ①

The above report can be exported by clicking the **Export Report...** button. ② The report can be saved in a variety of formats that are noted in the Export Options drop-down list.



Specify what export format and browse to the folder you want the report exported. You can view the results at a later time at the saved folder location.

- If a scheduled discovery was requested then a status message appears and the discovery is run later at the specified time.



Create and Manage Datasets


A dataset is the output of a particular command or set of commands issued by the CSP-C server. The commands issued by the CSP-C server are sent to a specific device and the device output from those commands is referred to as a dataset.

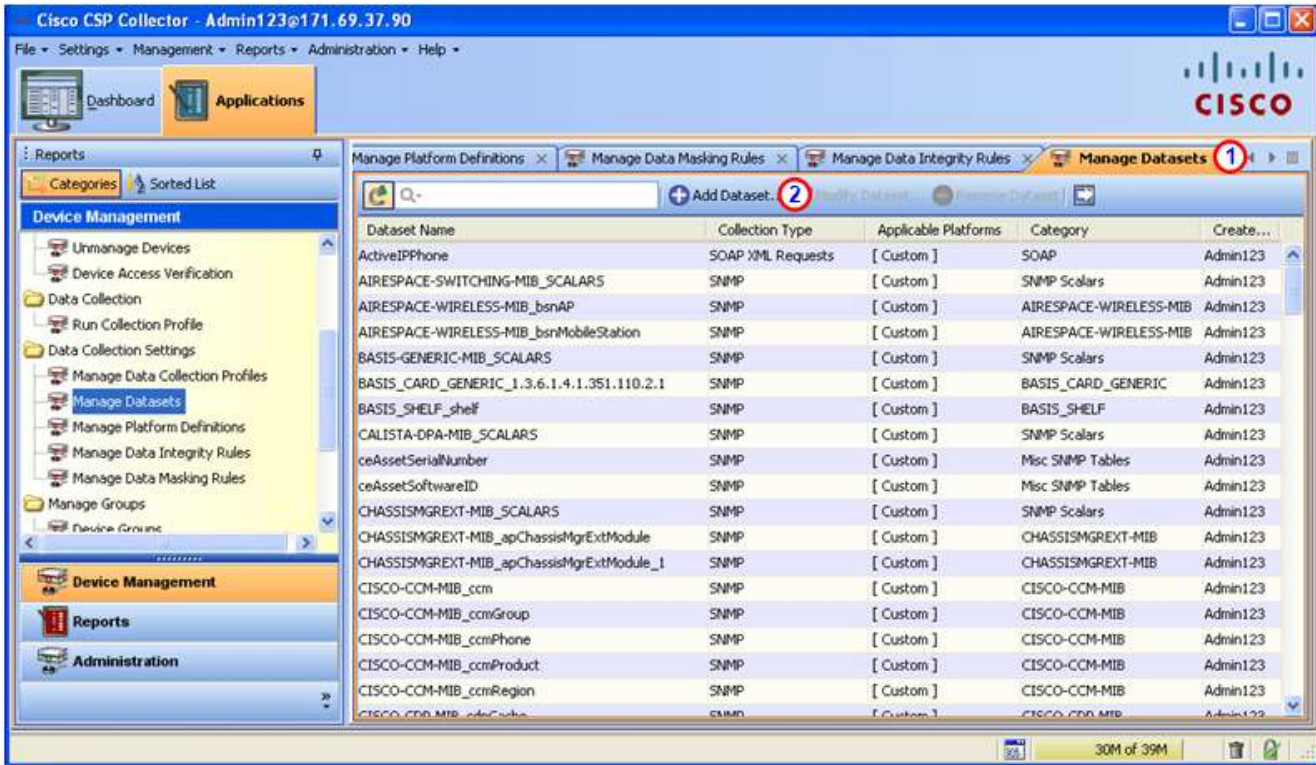
The creation of the dataset involves specifying what type mechanism to use to collect the dataset. Some of the mechanisms that can be used are:


- Output of a command (CLI)
- SNMP request (SNMP)
- XML output (SOAP/XML)

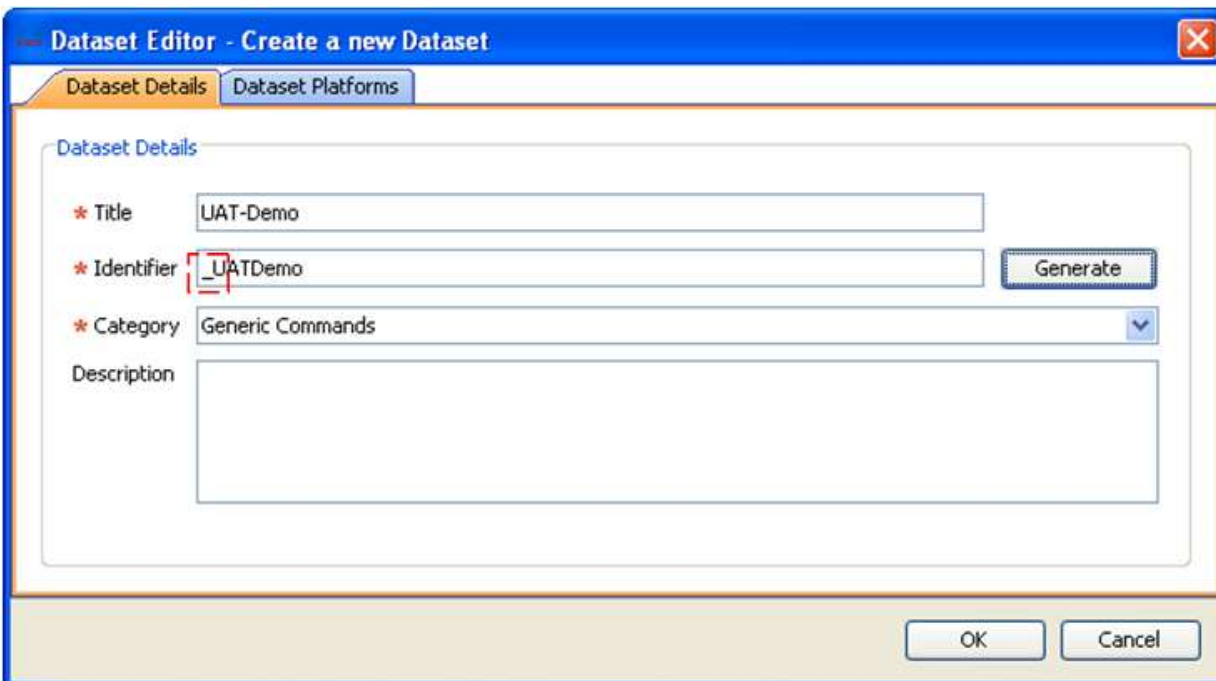
Along with specifying one of the above mechanisms a platform must also be selected. A platform (that is a router or switch platform) must be specified for the selected mechanism to run on. The platform identifies what type router or switch they have and indicates what commands can be run on those devices.

To create a dataset perform the following steps:

- On the browser menu choose **Applications tab > Device Management > Data Collection Settings > Manage Datasets**; the CSP-C browser displays the Manage Datasets pane. 



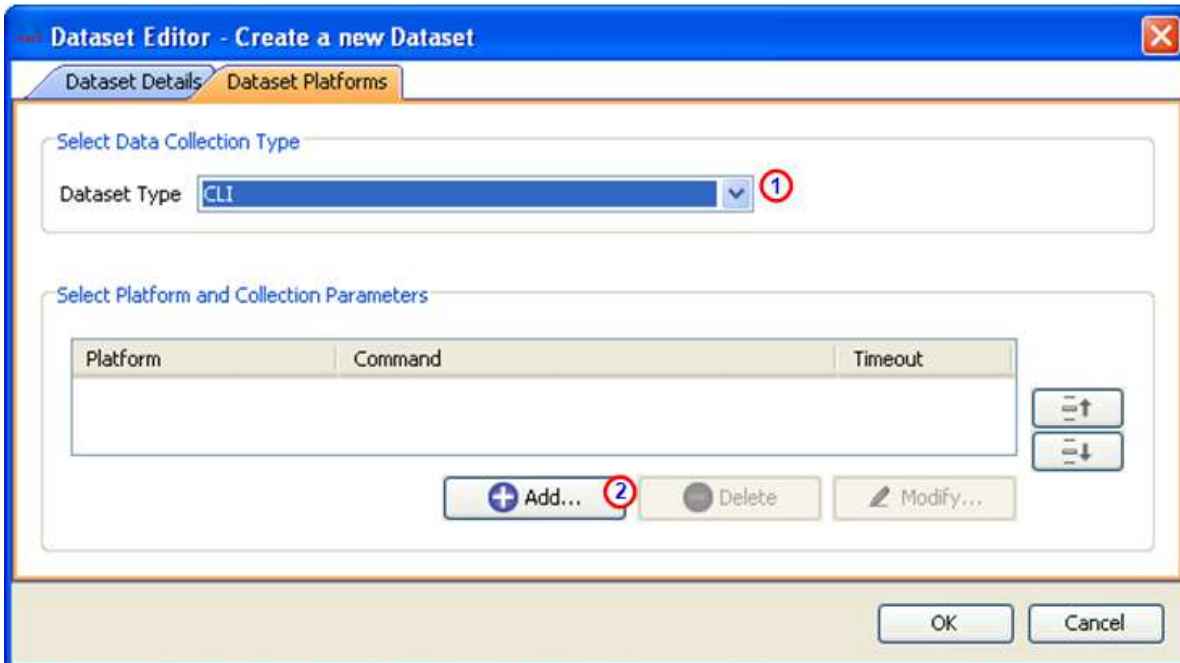
- To create a new dataset, click **Add Dataset**;  the Dataset Editor – Create a new Dataset window appears.



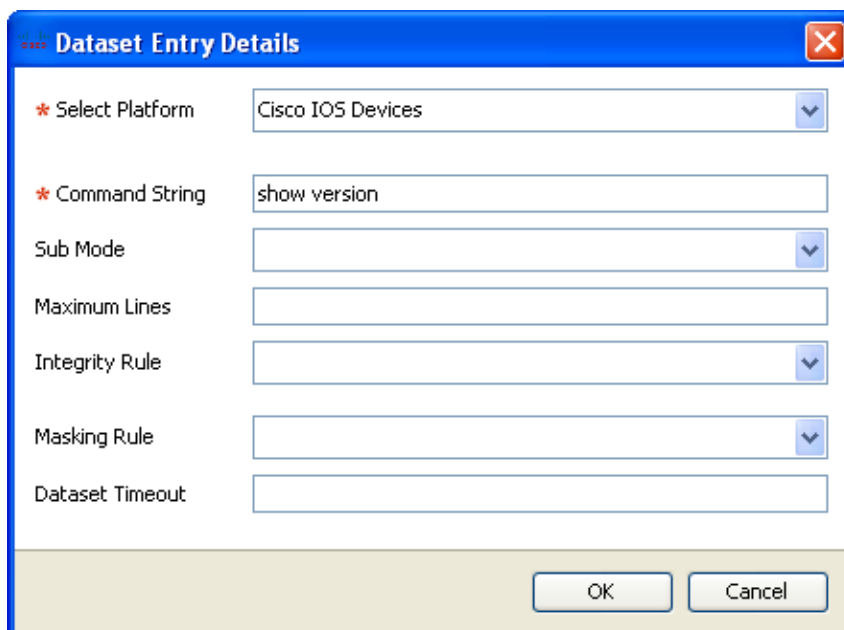
- Fill in the required information, then click the **Dataset Platforms** tab; the Dataset Platforms pane appears.



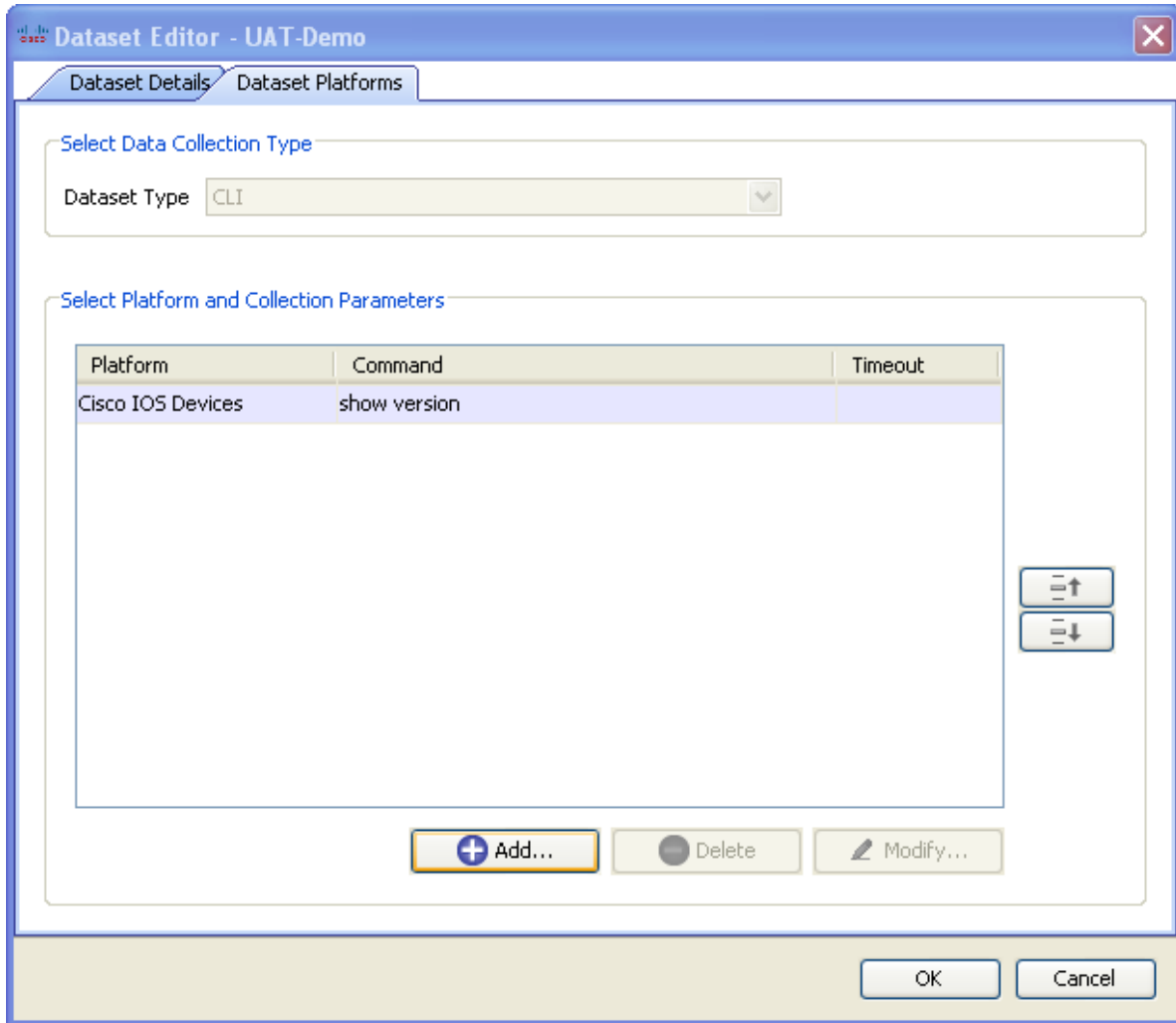
Note The Identifier must start with an underscore **_** at the beginning of the identifier name. Use the Generate button to automatically generate a valid identifier name from the name in the Title field (that is, UAT-Demo).



- Need to specify the following items:
 - [Dataset type](#)
 - Click the **Dataset Type** drop-down list **1** and select a dataset (that is, CLI).
 - Click the **Add** button **2** Dataset Entry Details window appears for specifying the platform.
 - [Platform and collection parameters -](#)



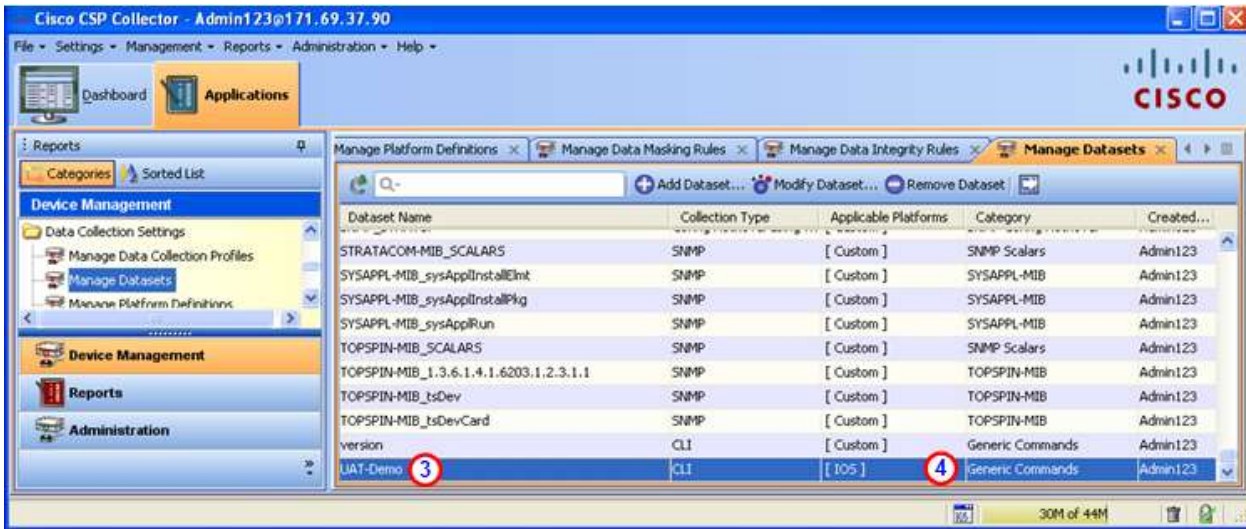
- Enter the required info.
- Click **OK**; the platform is added to the platform list



- Click **OK**; a success message window appears.



- Click **OK**; the UAT_Demo dataset name 3 is added to the list



- Click **OK**; the dataset is added to the list and is noted having the Generic Commands category. ④



Note Remember both the dataset name and the category type. This info will be needed later during the [Add Collection Profile process](#).

The next step in the inventory process is to manage the data collection profiles.

Data Collection Profiles

A collection profile defines what data to collect from the devices, from what type devices the data needs to be collected, and how often the data needs to be collected. There are two different profile categories covered:

- [Add Collection Profile](#)
- [Manage Data Collection Profiles](#)

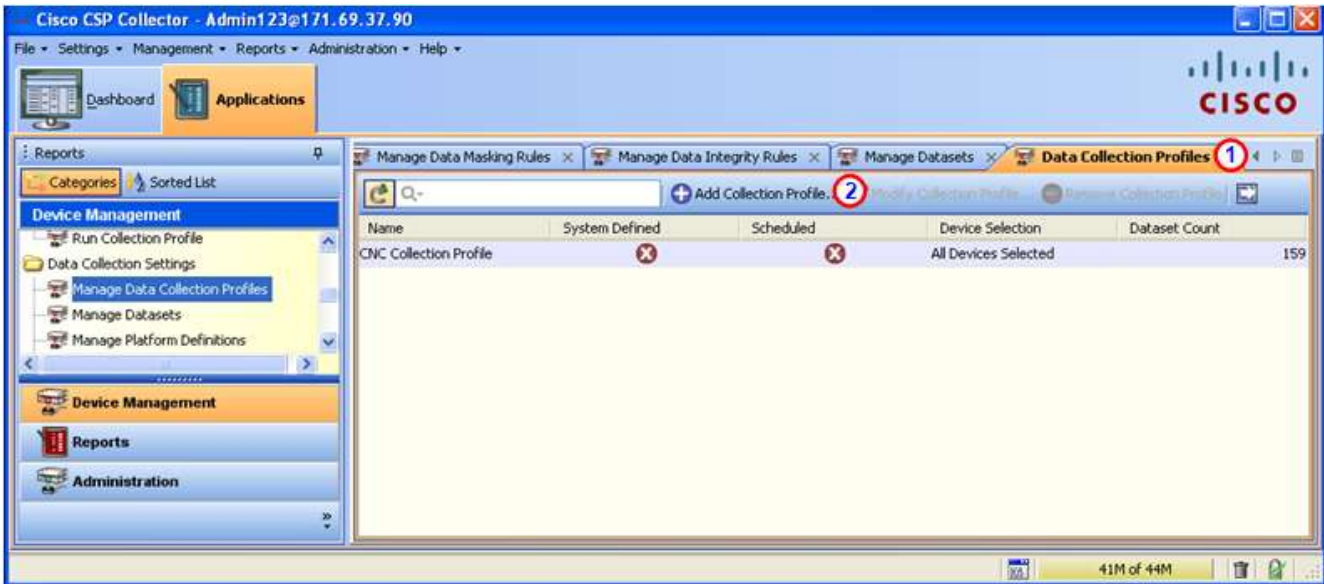
Add Collection Profile

To add a data collection profile perform the following steps:

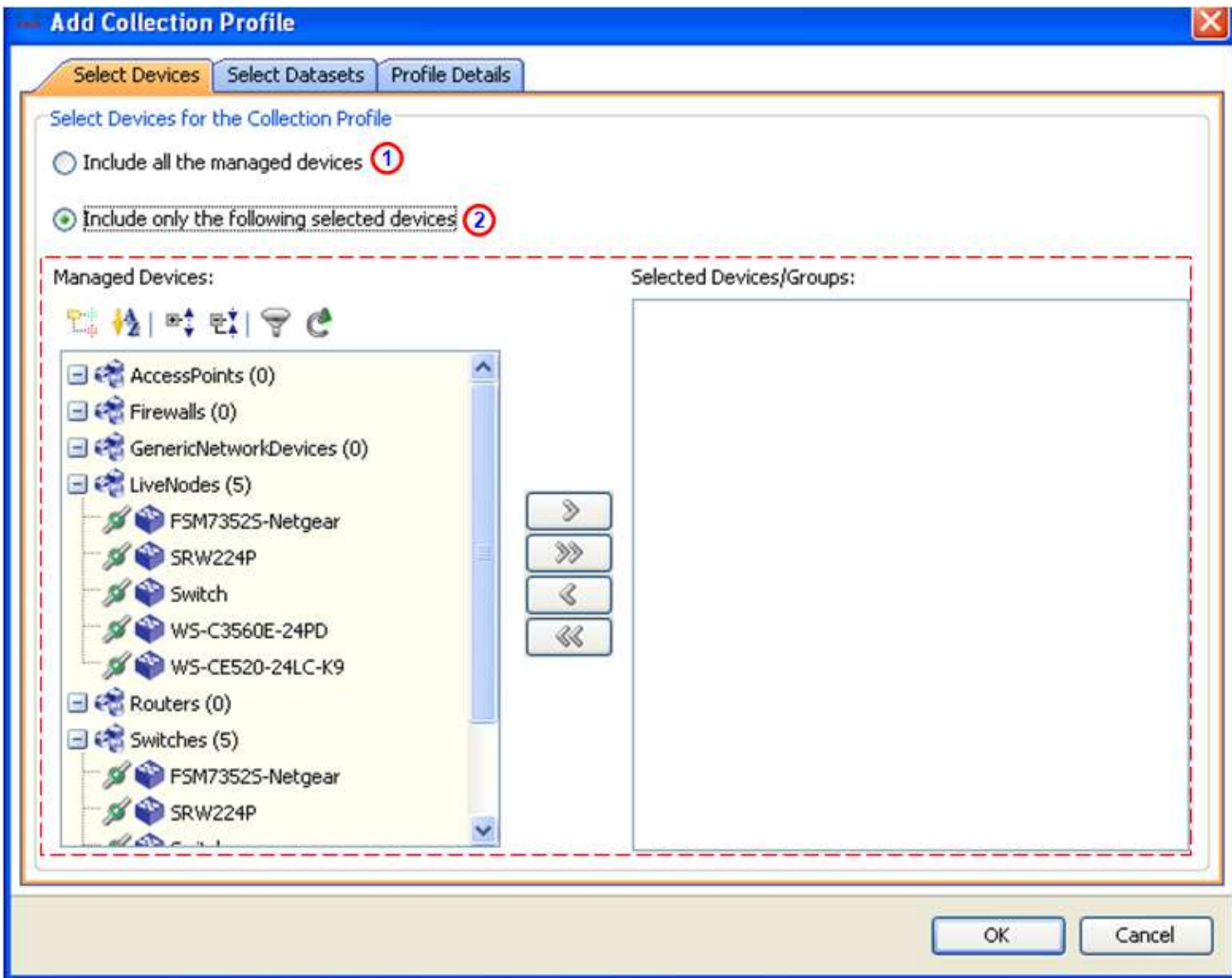
- On the menu choose **Applications tab > Manage Data Collection Profiles > Add Collection Profiles**, the CSP-C browser displays the Data Collection Profiles pane. ①




Note This is where existing devices get associated to the commands that are noted in the various datasets.

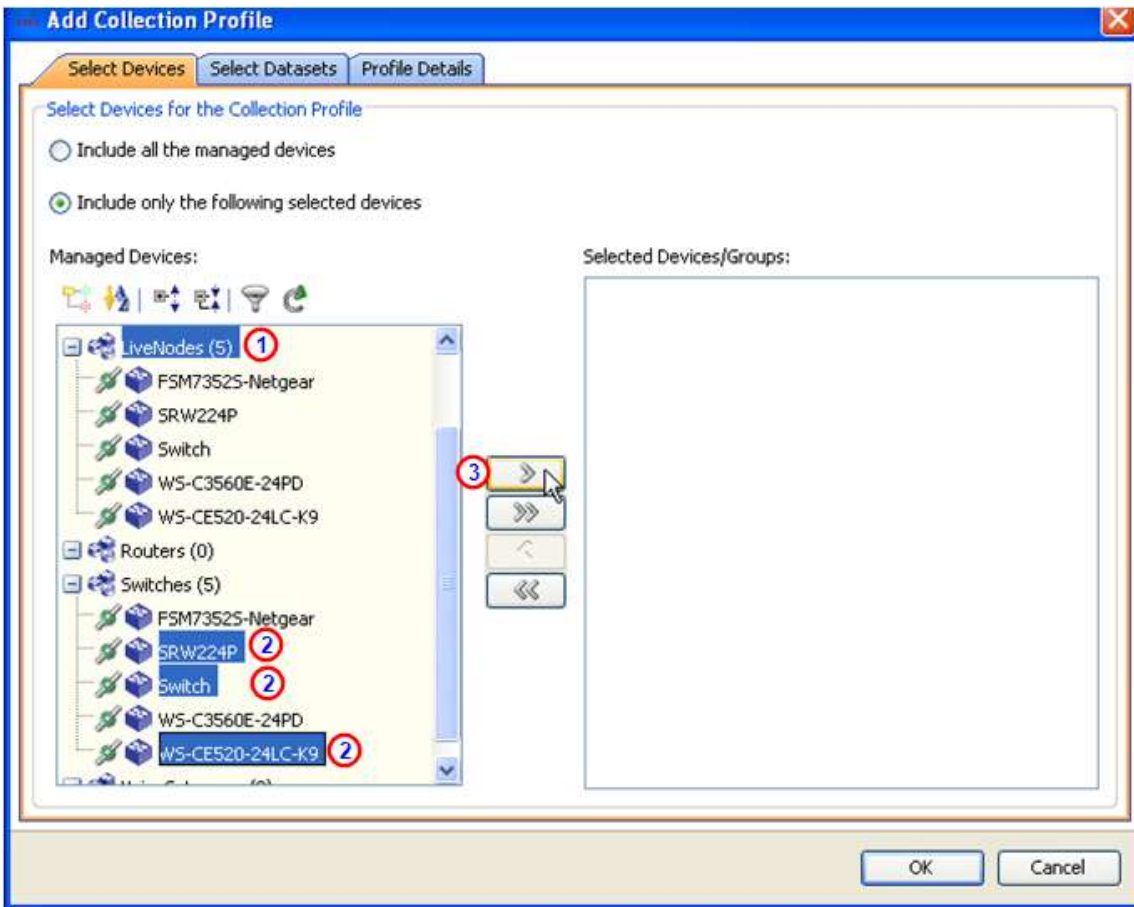


- To create a new Collection Profile, click **Add Collection Profile...**; ² the Add Collection Profile window appears, displaying the Select Devices tab.



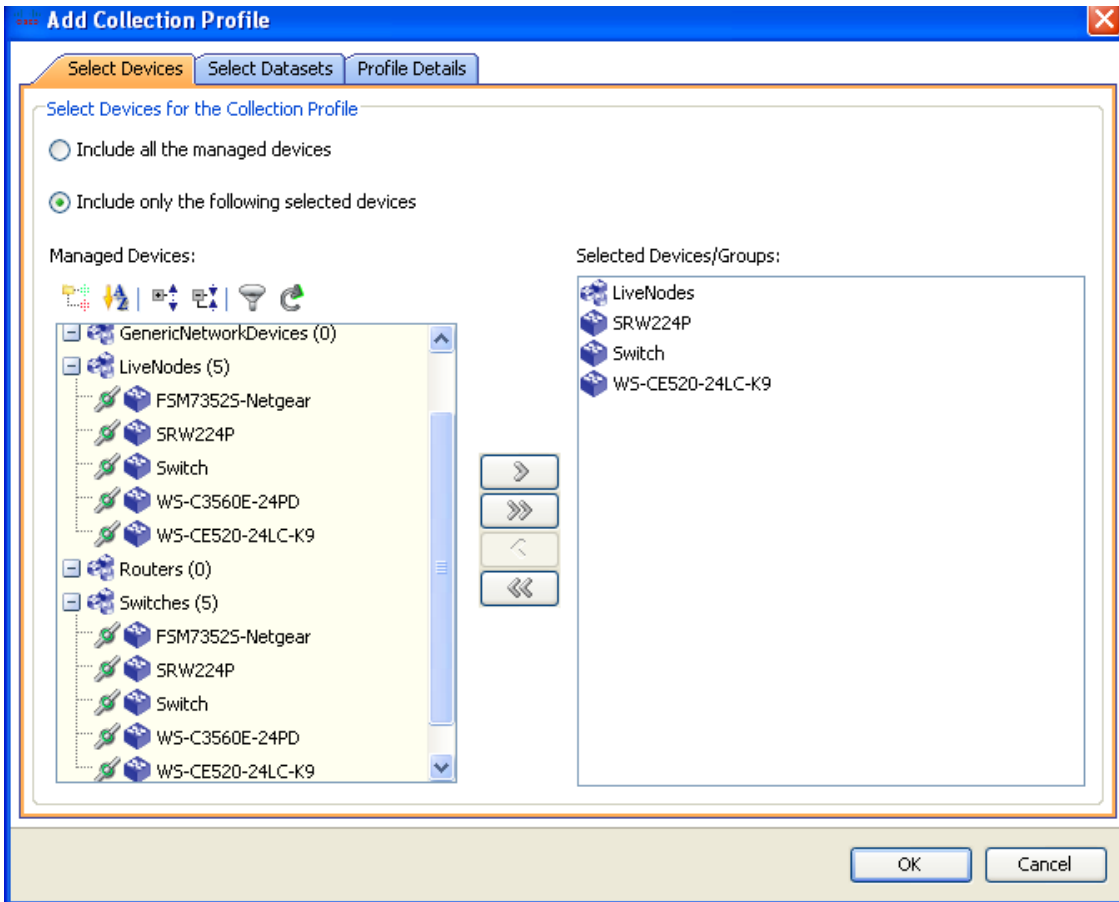
- There are two options for selecting devices for a collection profile:
 - Include all the managed devices. ¹
 - Include only those devices that you select; ² this option enables the selections area. 

- The second option **2** that lets you select what devices will be associated to a dataset, and works in the following manner:
 - [Select the devices you want in the Selected Devices/Groups pane.](#)

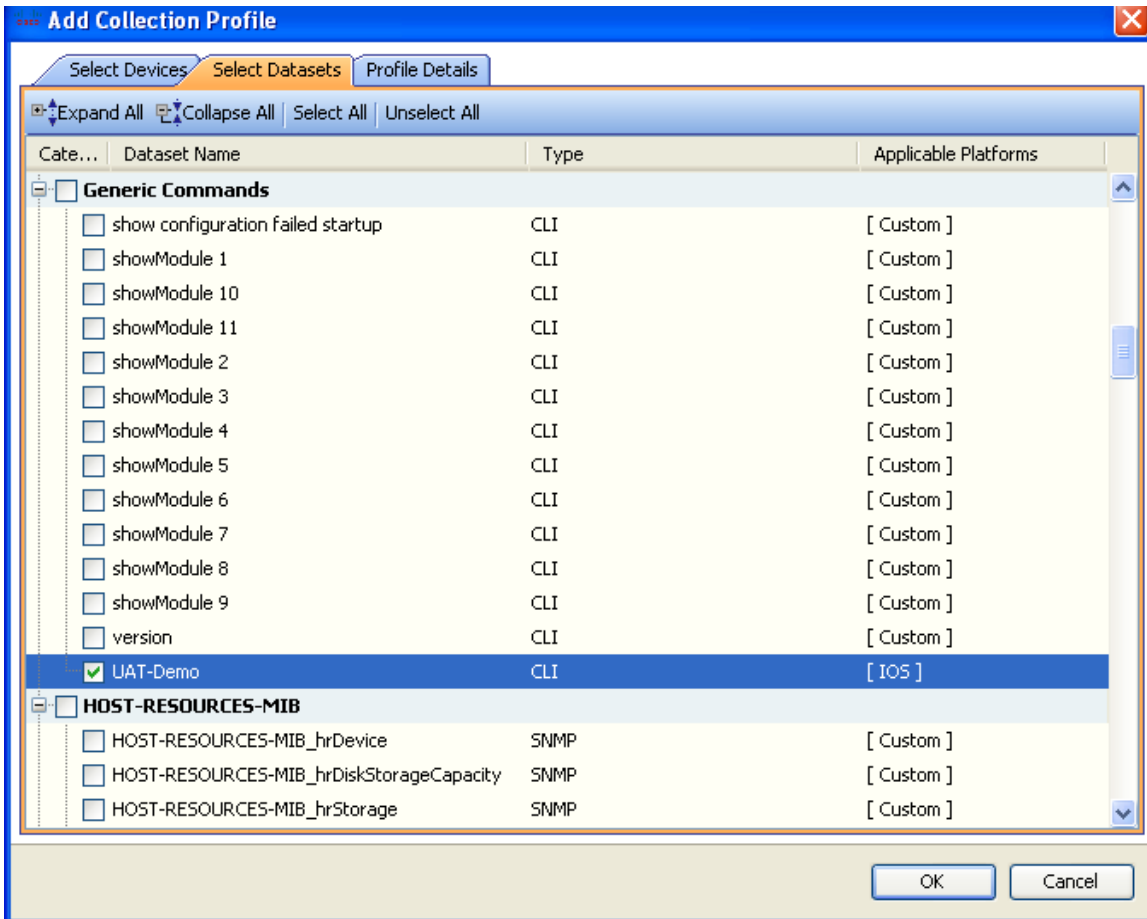


Note You can select multiple items and the items can be a group of devices **1** or individual devices. **2**

- After selecting the devices or groups, click the right pointing arrow; **3** the selected devices and groups get moved to the Selected Devices/Groups pane.



- The selected devices are now also in the Selected Devices/Groups pane; these devices represent the devices that are going to be associated to a set of commands in the next tab.
- Click the **Select Datasets** tab.



- Select the dataset names you want to associate to the devices. For this example look for the category name Generic Commands, which is where the UAT-Demo dataset name we created earlier is located.
- Check the **UAT-Demo** check box.



Note The combination of Generic Commands category name with UAT-Demo dataset was performed during the [add dataset section](#).

- Click the **Profile Details** tab, the Profile Details tab appears.

Modify Collection Profile

Select Devices | Select Datasets | **Profile Details**

Collection Profile Details

* Profile Title: UAT-Demo

* Identifier: UATDemo Generate 1

Description: [Empty text area]

Profile Priority: Medium

Preserve Run Count: 5

Use Fallback Credentials:

Collection Profile Schedule

Schedule Periodic Collection

Schedule start Date/Time: October 15, 2010 07:27:26PM Now

Repeat schedule:

Repeat every: [Empty] minutes

Schedule end Date/Time: [Empty] 07:27:26PM

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

Export Options

2 Export upon successful execution of the Collection Profile

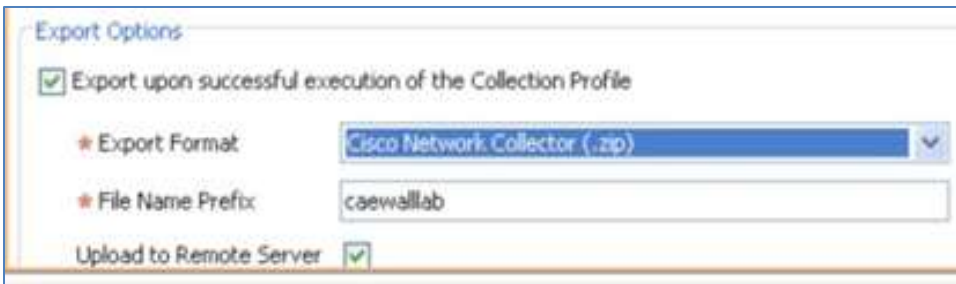
* Export Format: Cisco VSEM (.zip) 3

* File Name Prefix: UAT-Demo

Upload to Remote Server:

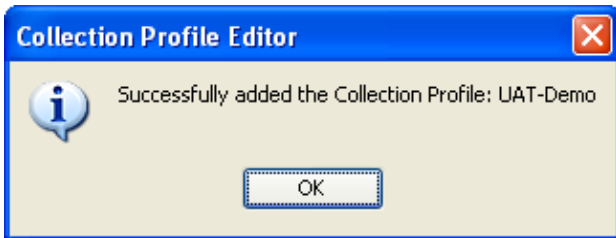
OK Cancel

- Enter the title in the Profile Title field, and then click the **Generate** button; 1 the browser creates the Identifier name i automatically.
- To send the inventory data to the Cisco backend perform the following steps:
 - [In the Export Options area \(at the bottom\), check the Export upon successful execution... check box.](#) 2
 - [Select a format from the Export Format drop-down list.](#) 3

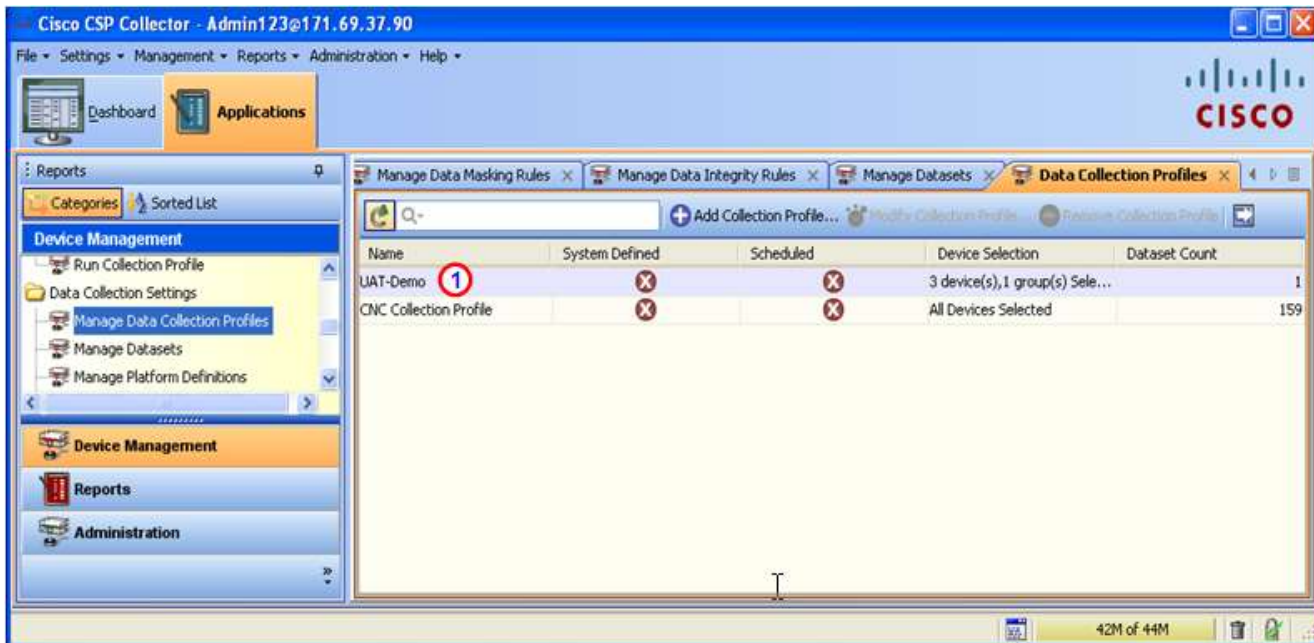


Important The default that comes up for the export options (Cisco VSEM (.zip)) should be changed to **Cisco Network Collector (.zip)** when uploading to the Cisco backend.

- [Enter a name in the File Name Prefix field \(that is, UAT-Demo\).](#)
- [Check the Upload to Remote Server check box.](#)
- Click **OK**; a Collection Profile Editor window appears with a success message.



- Click **OK**; the Data Collection Profiles pane appears with the new data collection profile **1** added to the list.

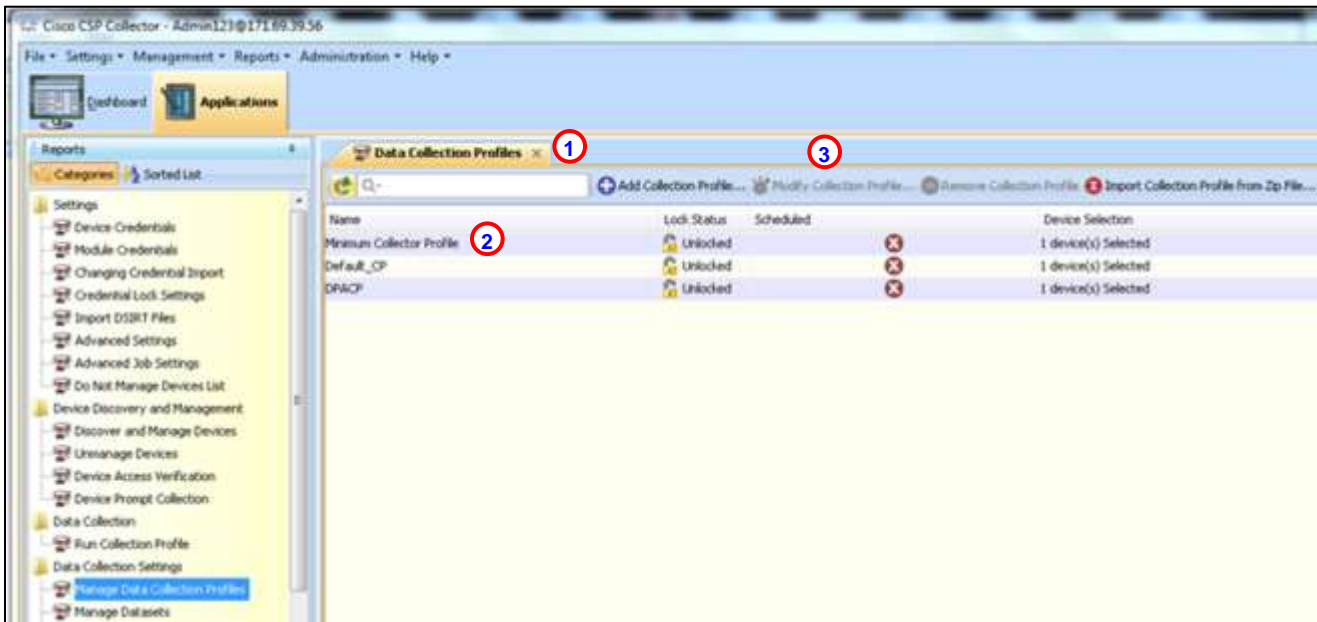


The next step in the process is to run an inventory collection to collect the data from the specified commands.

Manage Data Collection Profiles

To manage the data collection profiles that have already been added, perform the following steps:

- On the menu choose **Applications tab > Manage Data Collection Profiles** the CSP-C browser displays the Data Collection Profiles pane. ①



The Data Collection Profiles tab ① contains a Minimum Collector Profile. You can modify the Minimum Collector Profile by selecting the Minimum Collector Profile entry, ② and then clicking Modify Collection Profile. ③

The screenshot shows the 'Modify Collection Profile' dialog box with the 'Profile Details' tab selected. The 'Service Name' field, containing 'partner_support_service', is highlighted with a red dashed box. Other fields include Profile Title (Default_CP), Identifier (_Default_CP), Description (PSS Default Collection Profile...), Profile Priority (Medium), and Preserve Run Count (5). There are also several checkboxes for advanced options like 'Use Fallback Credentials' and 'Run Discovery Before Collection'.

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.

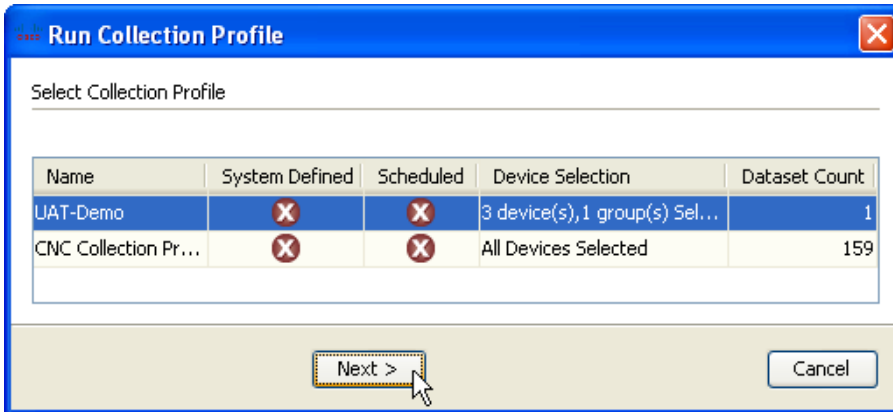
Important Do NOT change the service name (in example, partner_support_service) that is in the service name field. The field is allowed to be modified; however, if you change the name to something else, when inventory data gets sent to the Cisco backend the data repository will not recognize the different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

Run Collection Profile and Upload Data

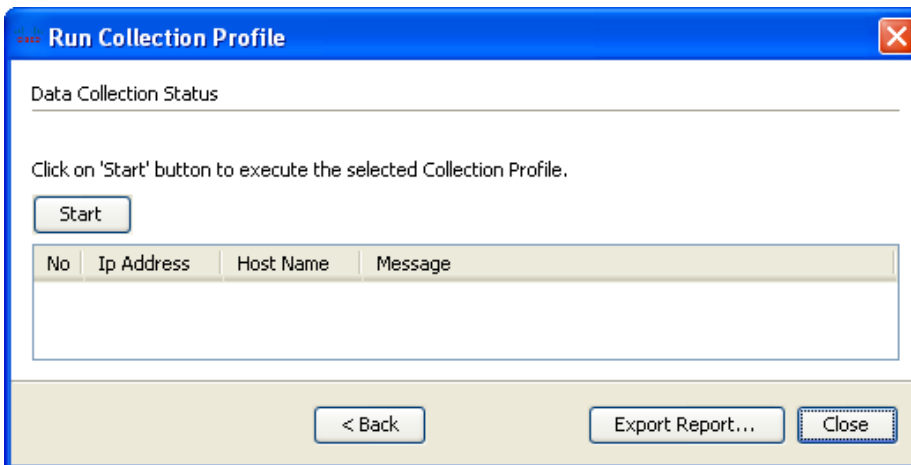
This part of the process collects the data from the devices in the customer network.

To create a dataset perform the following steps:

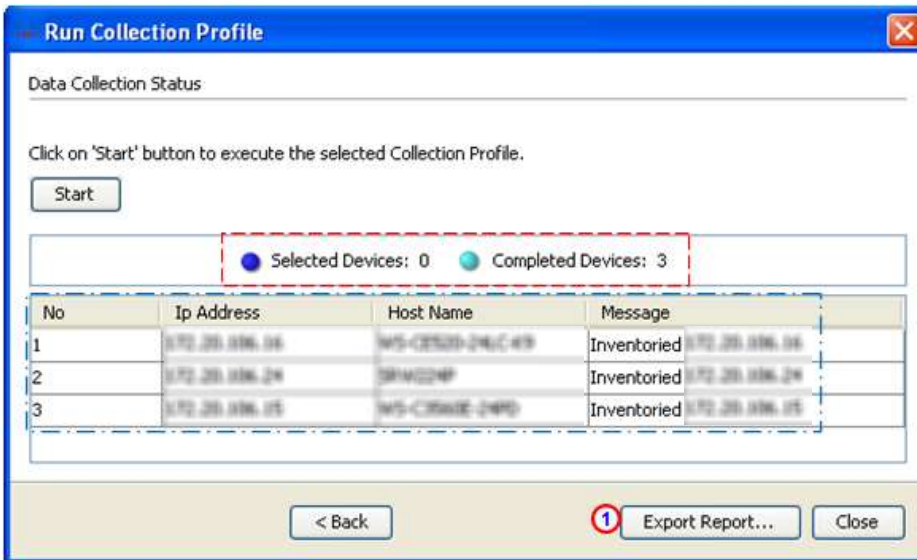
- On the browser menu choose **Applications tab > Data collection > Run Collection Profile**; the Run Collection Profile window appears.

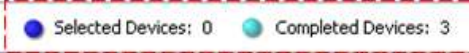




- Select the collection profile you want to run (that is, UAT-Demo).
- Click **Next**, the Data Collection Status area appears.



- Click **Start**; the data collection process is started.

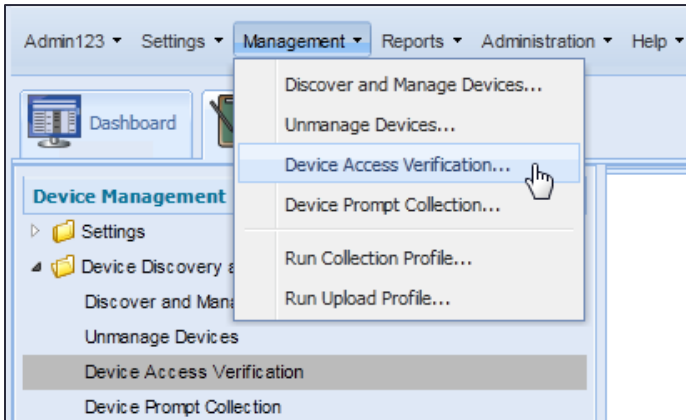


- The details of the data collection are filled in. A summary is above  and the details are below. 
- The above report can be exported by clicking the **Export Report...** button.  See the [Export Report section](#) for more details.
- Click **Close**.

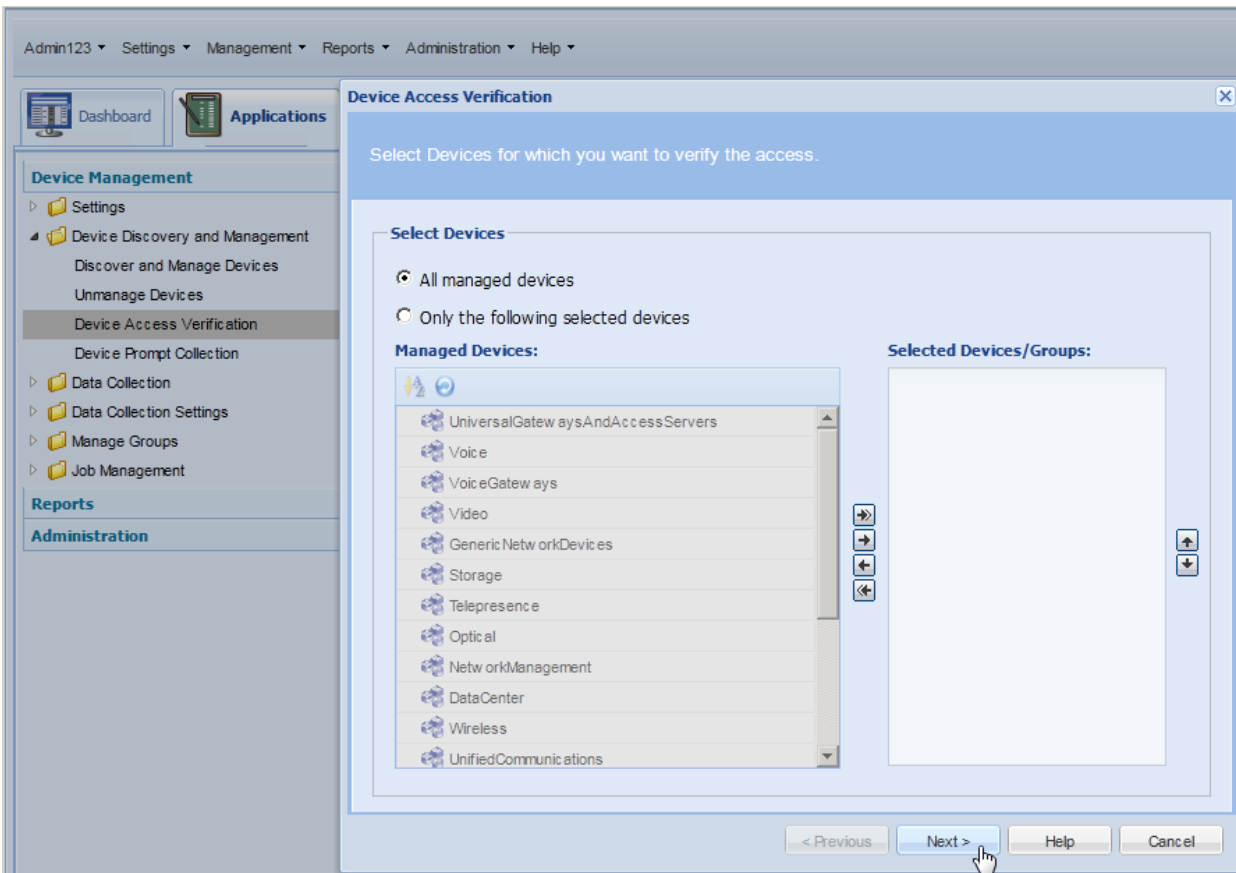
With the collection of the data, it is sent to the Cisco backend, if the [Upload to Remote Server check box](#) was previously selected.


Data Access Verification

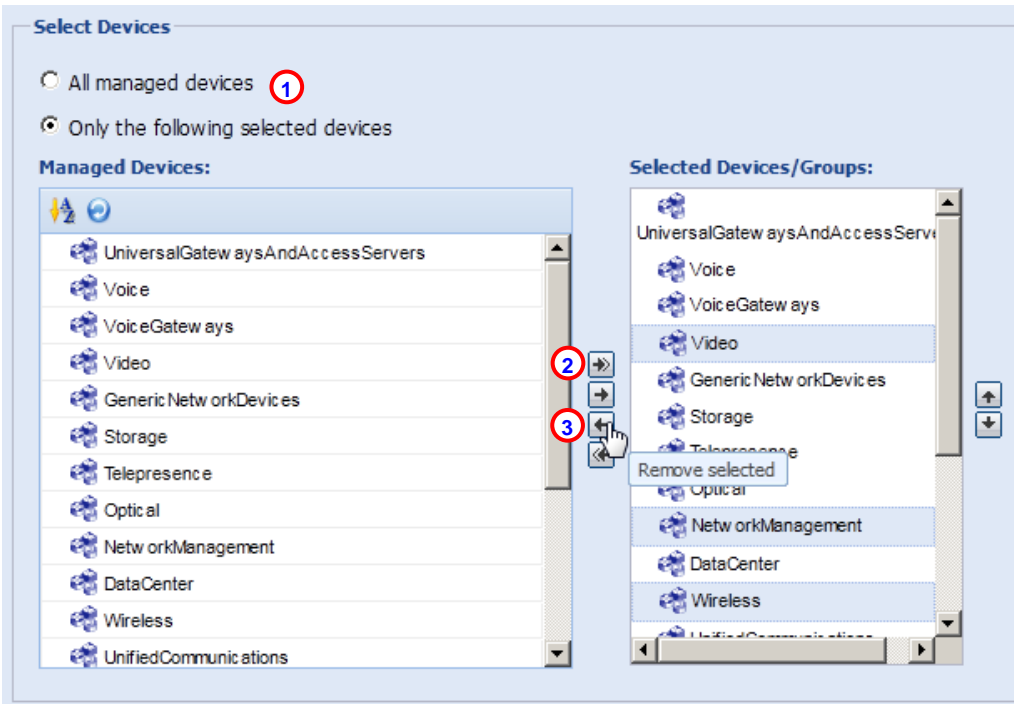
User needs to run Data Access Verification (DAV) once after [uploading the certificate / license file](#) in to the CSPC server appliance. It is good to run DAV before running collection profiles. To run DAV, perform the following steps:



- On the CSPC server appliance menu choose **Management > Data Access Verification**.



- Or on the navigation pane select **Applications > Device Discovery and Management > Data Access Verification**; the Data Access Verification pane appears.
- In the Select Devices section select one of the following options:
 - Select **All managed devices** radio button, which verifies all the devices known to the appliance.
 - Select Only the following selected devices radio button.
 - In the Managed Devices pane, select which specific devices you want verified and click the arrow buttons  to move the selected devices to the Selected Devices/Groups pane.



Note Selecting the **All managed devices** ¹ radio button or the **Add All** button, ² performs the same initial function; all the devices are selected for verification. One key difference for the Add all button is that the Add All function copies all the devices over to the Selected Devices/Groups pane, where you have the ability to further refine the list by selecting those few devices that you may not want in the list.

The scenario where the Add All button is very helpful is when you want most of, but not all, the managed devices verified. Simply click the **Add All** button, ² then once all the devices are copied over to the Selected Devices/Groups pane, select those few devices you don't want in the list and click the **Remove Selected** button; ³ those devices are removed from the Selected Devices/Groups pane and you can now proceed with the Data Access Verification.

Tip You can select non-contiguous devices (items not in contiguous sequence with each other) by selecting the first item with your mouse, then pressing the **Ctrl** key and select the remaining items you want in the list (see above graphic). To select contiguous items in a list, with your mouse select the first item in the list, press the shift key, then select the last item in the list. All the items between and including the first and last selected items are now selected in the list.

- After the devices have been selected, click **Next**; the Data Access Verification Schedule Options pane appears.

Device Access Verification

Device Access Verification Schedule Options

Select Protocols For Device Access Verification

telnet sshv1 sshv2
 snmpv1 snmpv2c snmpv3
 http https wmi

Optimize Device timeouts on successful verification

Advanced Options

Job Details

* Job Name:

Job Description:

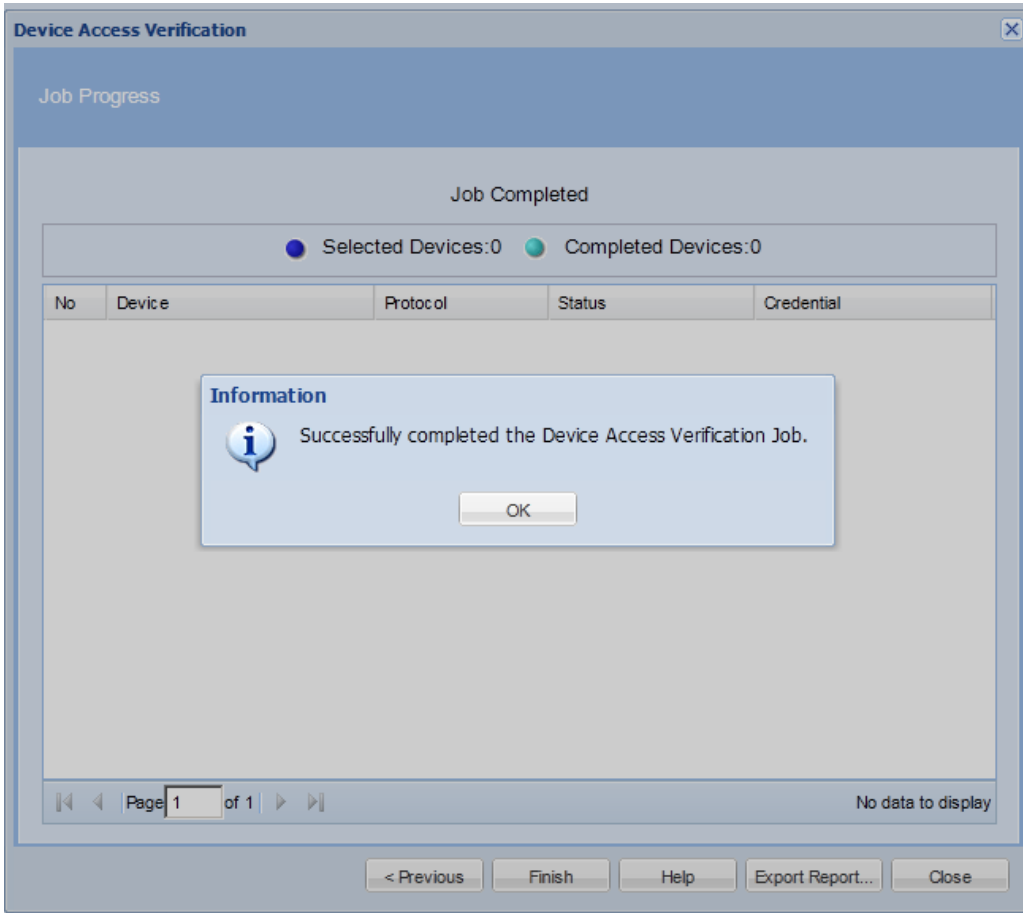
Job Schedule Options

Start Device Access Verification Now
 Schedule Device Access Verification

No schedule configured

< Previous Finish Help Close

- Fill in the respective fields as needed; there are only two required fields:
 - Select at least one protocol for Data Access Verification section.
 - Provide a name in the Job Name: field, which is preceded with the * red asterisk.
- After all the fields are filled in, then click **Finish**.



- If any devices are found, they are listed in the Job Completed area, also a successful information message appears.

Minimum Collection Profile

The Minimum Collection Profile and the Default Collection Profile are bundled with the CSP-C appliance. The Minimum Collection Profile contains a minimum set of mandatory collection commands that are required to be processed for each inventory collection/upload. The inventory from the Minimum Collection Profile contains information related to the processing of the following commands that are the minimum set of mandatory collection commands that need to be processed during the inventory collection:

- CLI commands:
 - show_c7200
 - show_diag
 - show_hardware
 - show_idprom_all
 - show_inventory
 - show_module
 - show_rsp_chassis-info
 - show_version
- Configurations commands:
 - show startup-config
 - show running-config

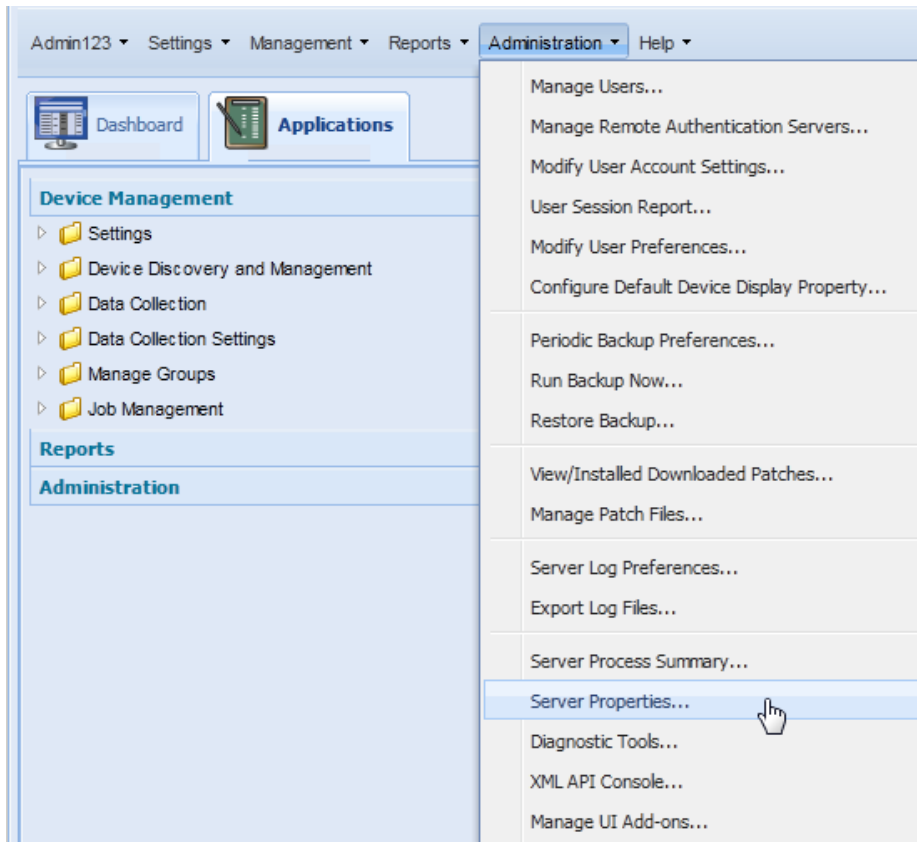


Note

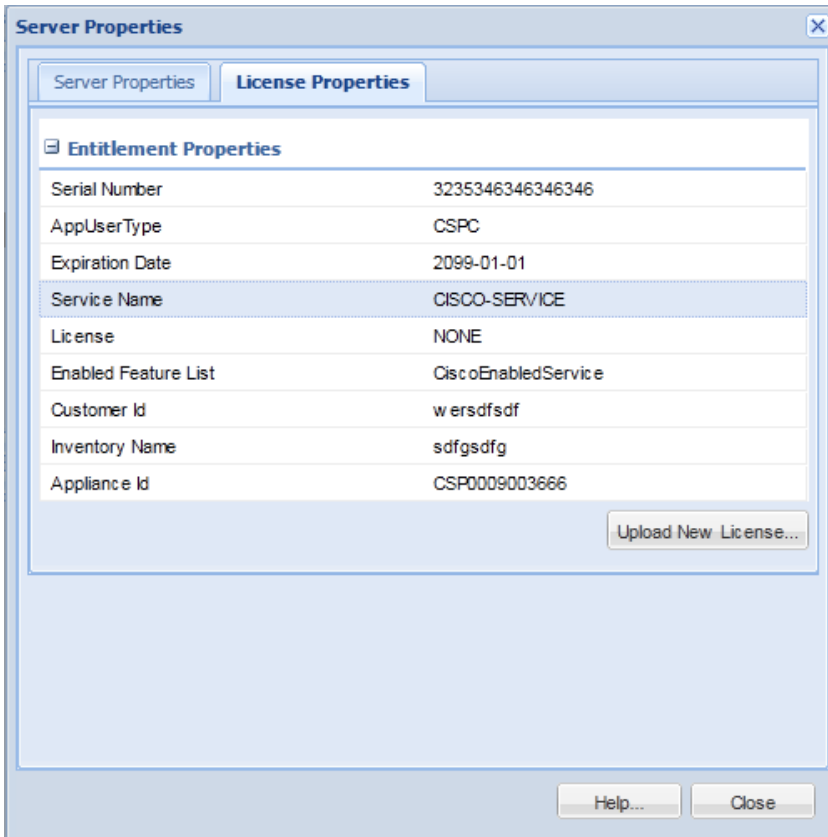
The Minimum Collection Profile has only a subset of the datasets that are present in the Default Collection profile.

Multi-Service Collection

This feature allows a single CSP-C collector to collect data for multiple Cisco services on a customer network, eliminating the need for partners to install multiple collectors. To see the current Service Name, perform the following steps:



- On the menu choose **Administration > Server Properties**; the Server Properties window appears.



- Click the **License Properties** tab, the Service Name field displays the name of the current service (in example, CISCO-SERVICE).


CSP-C 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/CSP-C image, using the standard ssh client, and can then configure the CSP-C.

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 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	cisco, admin, user
conf ip *	Static IP Configuration, lets you configure: <intf> <ipaddr> <netmask> <gateway>	cisco, admin, user

<p>conf proxy *</p>	<p>conf proxy <ipaddr> [<port>][<user> <passwd>]</p> <ul style="list-style-type: none"> • 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 • Available Mode Requirements for Upload <p>To ensure a successful upload from a CSP-C Collector to the Cisco backend the following ports and specific IP addresses need to allow outbound access to the internet. The CSPC has several available modes that will allow for a successful upload to Cisco. ACL's on customers firewall might need to be configured to allow the CSP-C to upload successfully.</p> <p> Note Only one of the below mode requirements is needed</p> <p><u>IPSEC</u></p> <table border="1"> <thead> <tr> <th>Source IP Address</th> <th>Source Port</th> <th>Destination IP Address</th> </tr> </thead> <tbody> <tr> <td>CSPC Server IP</td> <td>any</td> <td>72.163.7.138</td> </tr> <tr> <td>CSPC Server IP</td> <td>any</td> <td>72.163.7.138</td> </tr> <tr> <td>CSPC Server IP</td> <td>any</td> <td>72.163.7.88</td> </tr> <tr> <td>CSPC Server IP</td> <td>any</td> <td>72.163.7.9627</td> </tr> </tbody> </table> <p><u>SSL</u></p> <table border="1"> <thead> <tr> <th>Source IP Address</th> <th>Source Port</th> <th>Destination IP Address</th> </tr> </thead> <tbody> <tr> <td>CSPC Server IP</td> <td>any</td> <td>72.163.7.113</td> </tr> </tbody> </table>	Source IP Address	Source Port	Destination IP Address	CSPC Server IP	any	72.163.7.138	CSPC Server IP	any	72.163.7.138	CSPC Server IP	any	72.163.7.88	CSPC Server IP	any	72.163.7.9627	Source IP Address	Source Port	Destination IP Address	CSPC Server IP	any	72.163.7.113	<p>cisco, admin, user</p>
Source IP Address	Source Port	Destination IP Address																					
CSPC Server IP	any	72.163.7.138																					
CSPC Server IP	any	72.163.7.138																					
CSPC Server IP	any	72.163.7.88																					
CSPC Server IP	any	72.163.7.9627																					
Source IP Address	Source Port	Destination IP Address																					
CSPC Server IP	any	72.163.7.113																					

	<p>XMPP</p> <table border="1"> <thead> <tr> <th>Source IP Address</th> <th>Source Port</th> <th>Destination IP Address</th> </tr> </thead> <tbody> <tr> <td>CSPC Server IP</td> <td>any</td> <td>72.163.7.138</td> </tr> <tr> <td>CSPC Server IP</td> <td>any</td> <td>72.163.7.138</td> </tr> </tbody> </table> <ul style="list-style-type: none"> • 	Source IP Address	Source Port	Destination IP Address	CSPC Server IP	any	72.163.7.138	CSPC Server IP	any	72.163.7.138	
Source IP Address	Source Port	Destination IP Address									
CSPC Server IP	any	72.163.7.138									
CSPC Server IP	any	72.163.7.138									
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 CSP-C/logs directory when enabled. The selected log file can then be downloaded into the desktop using the CSP-C browser. Options are: <logtype> (enable disable) logtype = CSP-C addon UNIX adminshell	cisco, admin, user									
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 passwd 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 = ADMIN SHELL ADDON LINUX CSP-C 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 ADMIN SHELL admin# show logs ADDON admin# show logs LINUX admin# show logs CSP-C	cisco, admin, viewer
show monitor	Shows the following information:	All (cisco, admin,

	(1) network utilization (%) for ethernet port (2) CPU and memory utilization	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 Options are: (enable disable)	cisco, admin, user
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 a ? 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 a ? shall list all CLI commands available to the user.	Each user ID has access to help for the commands that are relevant to its privilege level.

CSP-C Basic Troubleshooting

This section includes basic troubleshooting suggestions for some problems that you may encounter.

Network Configuration Errors

The following errors are related to network configuration:

- **Basic network connection** - Make sure the network cable is properly connected to the CSP-C collector box.
- **Showing Network Configuration** – From the command prompt, enter **show ipconfig**; a sample screen shot is shown in Fig 9.1.

```
cisco# show ipconfig

Interface eth0 is up
DHCP is disabled
Device       : eth0
IP           : xxx.xxx.xxx.xxx
MAC         : xx:xx:xx:xx:xx:xx

Subnet Mask  : 255.255.255.0

DNS Servers :
  Nameserver1 : xxx.xxx.xxx.xxx

Gateway :
  Interface   : eth0
  Gateway     : xxx.xxx.xxx.xxx

Proxy is not configured
```

Fig 9.1

- **Trying to Ping** - From the CSP-C collector, try to ping another device in the same network from the command prompt. Enter **ping 171.69.37.63** ; A sample screen shot is shown in Fig 9.2

```
admin# ping xxx.xxx.xxx.xxx
PING xxx.xxx.xxx.xxx (xxx.xxx.xxx.xxx) 56(84) bytes of data.
64 bytes from xxx.xxx.xxx.xxx : icmp_seq=1 ttl=64 time=1.65 ms
64 bytes from xxx.xxx.xxx.xxx : icmp_seq=2 ttl=64 time=0.518 ms
64 bytes from xxx.xxx.xxx.xxx : icmp_seq=3 ttl=64 time=0.523 ms
64 bytes from xxx.xxx.xxx.xxx : icmp_seq=4 ttl=64 time=0.531 ms
64 bytes from xxx.xxx.xxx.xxx : icmp_seq=5 ttl=64 time=0.525 ms

--- xxx.xxx.xxx.xxx ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.518/0.750/1.653/0.451 ms
```

Fig 9.2



Note Make sure the CSP-C collector is reachable over the network, via a ping command.

- **Show ipconfig (errors)** – show ipconfig does not properly display the IP address, mode or device details. Make sure that you know which interface is the network interface (**eth0**). In addition, make sure that a known working network cable is properly connected to your network at one end and to the **eth0** end on the hardware.

- **Timesync (errors)** – Even though the user provided a correct NTP server IP address, issuing timesync command obtains an error. Make sure that your hardware is properly connected to the network, using the **eth0** interface. Also, make sure that your hardware is configured with the proper IP address, and that it is able to reach the network.



Note If you initially configured the ip address to ethernet interface eth0, then subsequently reconfigured the collector to another ethernet interface (e.g. eth1), you must re-install the CentOS image and reconfigure the ip address to eth1. However, the reverse direction from ip-configuring with eth1 then switching to eth0, would not require re-installation of the CentOS image

Collector Registration Errors

The following errors are related to collector registration:

- **Collector Status** - From the command prompt enter **collector status**. A sample screen shot is show in Fig 9.3

```
admin# collector status

Checking status...please wait
Collector is up and running

Collector is running

admin#
```

Fig 9.3

- **Registration Status** – Make sure that the registration file uploads to the CSP-C collector without any errors on the browser.

VMware Basic Troubleshooting

This Section includes some of the basic troubleshooting suggestions for some problems you may encounter.

Network Configuration Errors

Basic network connection - Make sure network cable is properly connect to target hardware box

Showing the network configuration – From the command prompt enter **show ipconfig**. A sample graphic is shown in the following graphic.

```
cisco# show ipconfig

Interface eth0 is up
DHCP is disabled
    Device       : eth0
    IP           : xxx.xxx.xxx.xxx
    MAC          : xx:xx:xx:xx:xx:xx

Subnet Mask     : 255.255.255.0

DNS Servers :
    Nameserver1 : xxx.xxx.xxx.xxx

Gateway :
    Interface   : eth0
    Gateway     : xxx.xxx.xxx.xxx

Proxy is not configured
```

Trying to Ping - From the target hardware, try to ping another device in the same network from the command prompt. Enter ping **171.69.37.63**. A sample graphic is shown in the following graphic.

```
admin# ping xxx.xxx.xxx.xxx
PING xxx.xxx.xxx.xxx (xxx.xxx.xxx.xxx) 56(84) bytes of data.
64 bytes from xxx.xxx.xxx.xxx : icmp_seq=1 ttl=64 time=1.65 ms
64 bytes from xxx.xxx.xxx.xxx : icmp_seq=2 ttl=64 time=0.518 ms
64 bytes from xxx.xxx.xxx.xxx : icmp_seq=3 ttl=64 time=0.523 ms
64 bytes from xxx.xxx.xxx.xxx : icmp_seq=4 ttl=64 time=0.531 ms
64 bytes from xxx.xxx.xxx.xxx : icmp_seq=5 ttl=64 time=0.525 ms

--- xxx.xxx.xxx.xxx ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.518/0.750/1.653/0.451 ms
```

Also, make sure the target hardware is reachable over the network, via a ping command.

Show ipconfig (errors) – Issuing the **show ipconfig** command does not display the IP Address, mode, or device details. Ensure that your hardware network interface is using interface (**eth0**). In addition, make sure that working network cable is properly connected to your network at one end and to the **eth0** on the hardware.

Timesync (errors) – Even though a user provided the proper NTP server IP address, issuing the **timesync** command obtains an error. Ensure that your hardware is connected to network using the **eth0** interface. Also, make sure that your hardware is configured with proper IP Address and is able to reach network.

Collector Registration Errors

Collector Status - From the command prompt enter **collector status**. A sample graphic is show in the following graphic.

```
cisco# collector status

Checking status...please wait
Collector is up and running

Collector is running
```

Registration Status – Make sure that registration file is uploaded into target hardware without any errors on the browser.

VMware Image Configuration Errors

Cisco recommends that the Linux (Host) machine has a NIC card, which is properly configured and network reachable. It is recommended that Linux (Host) machine is running over DHCP so that the VMware smart collector running on the Linux (Host) machine can get a proper DHCP address.

In order for the VMware smart collector to function normally, make sure that it gets proper IPAddress via DHCP or configured with reachable static IPAddress (based on your network configuration).

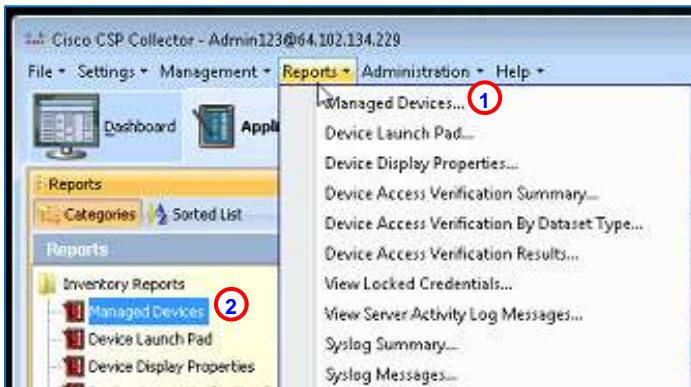
Best Practices

This section provides suggestions and tips that allow you to update information more efficiently on the collector and configure data that will make collector data identification easier. This section covers the following areas:

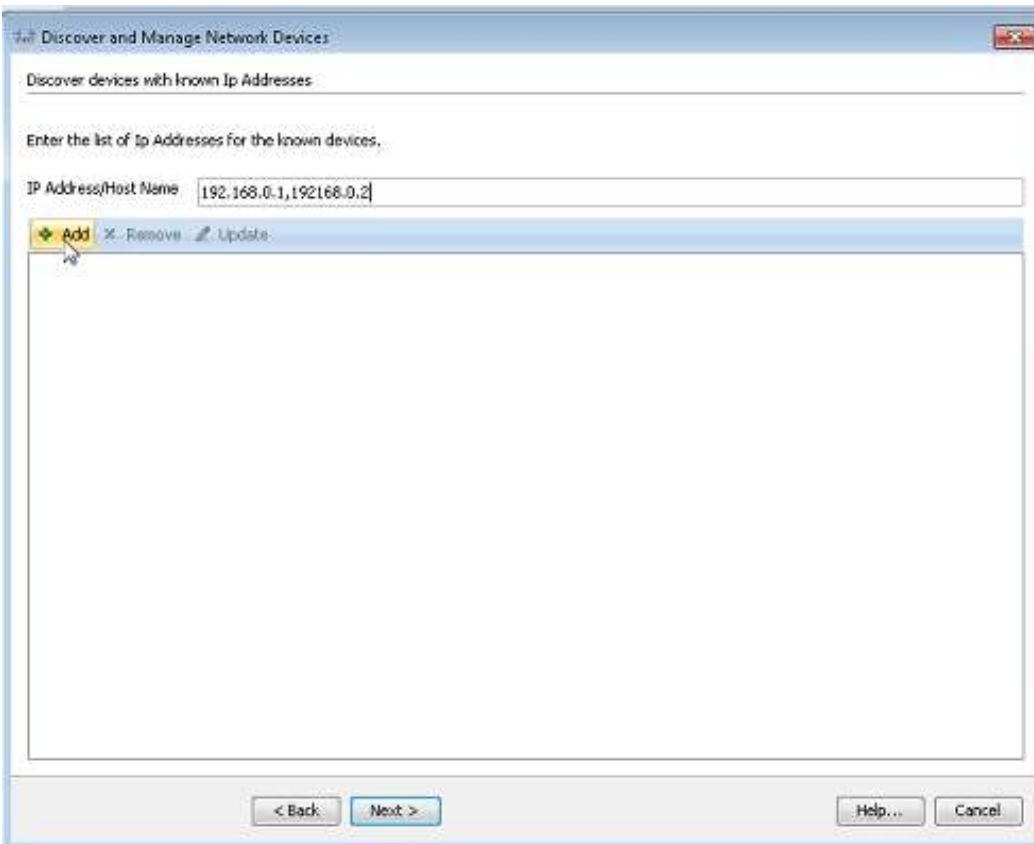
- [Adding Multiple Devices in IP Address Host Name Field](#)
- [File Name Prefix Suggestion](#)
- [Reusing the Same Certificate for another Collector](#)

Adding Multiple Devices in IP Address Host Name Field

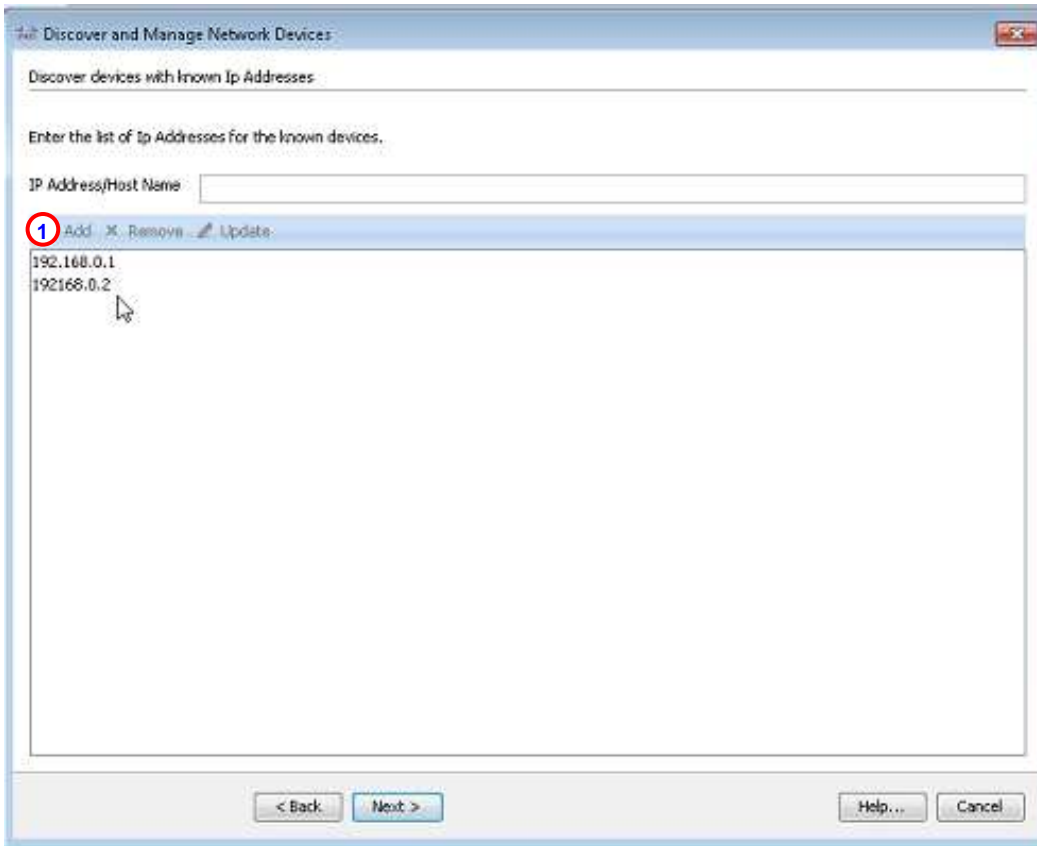
This section describes how to add multiple devices to the IP Address Host Name Field.



- There are two ways to access the Managed Devices data, from the menu 1 or navigation pane. 2



- In the IP Address/Host Name field enter the IP Addresses separated by a comma or space delimiter to add multiple addresses.



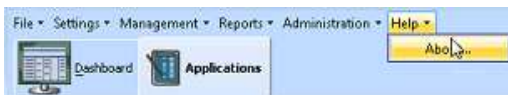
- Click **Add**, 1 this adds the addresses that you entered in the IP Address/Host Name field.

File Name Prefix Suggestion

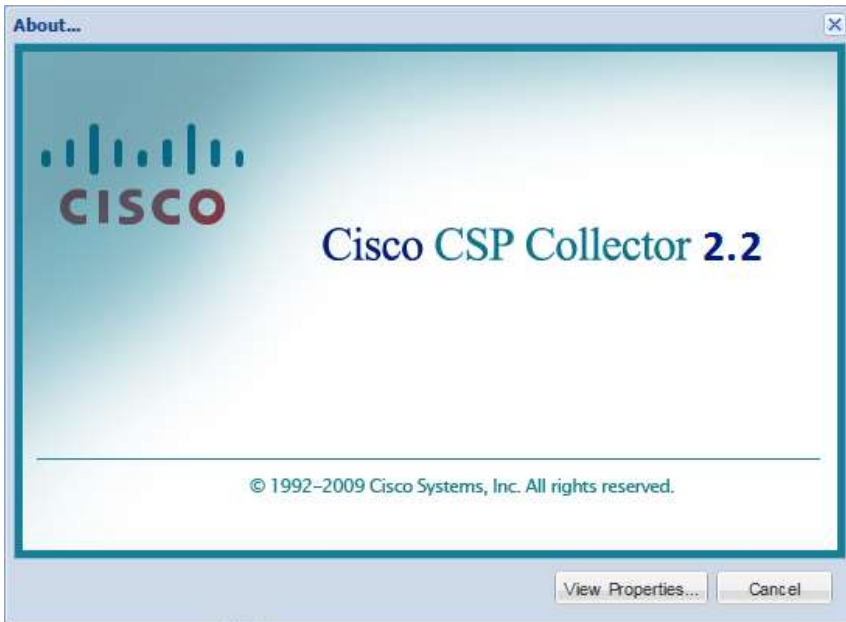
This section describes the process and benefits of changing the default file name prefix.

If the default file name prefix is used on every collector that you have, then it will be very difficult to determine which export file is associated to which collector. Instead of using default file name prefix, use something different like the appliance id for each file name prefix.

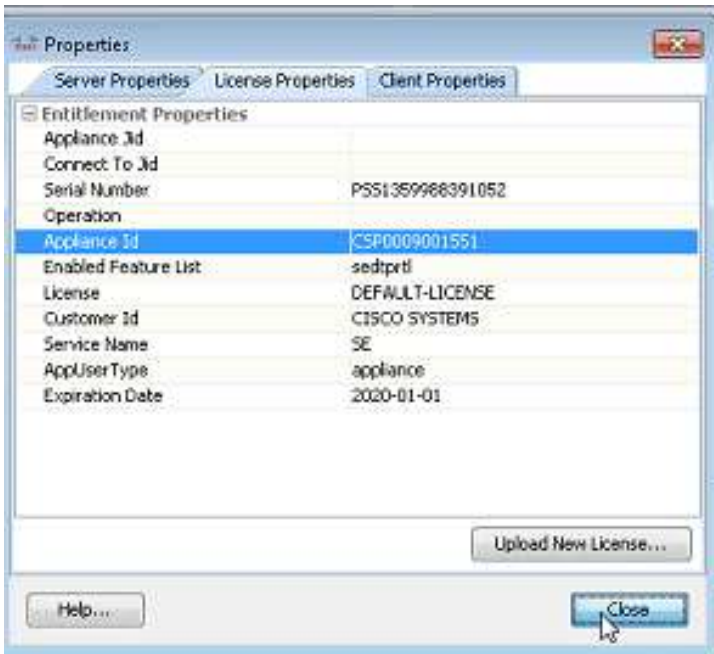
The appliance id can be found by perform the following steps:



- On the CSPC menu choose Help > About ; the Cisco CSP Collector – About window appears.



- Click **View Properties**; the Properties window appears.



- The appliance id is located halfway down the list. Use the appliance id (CSP...) as the file name prefix, the finding of the export file for each collector will be much easier.

Reusing the Same Certificate for another Collector

To re-use the same certificate on another collector perform the following steps:

- Find the collector certificate information (go to [finding appliance id](#)).
- Shutdown the first collector.
- Start the new collector.
- Use the same certificate number (obtained in the first step of this section) in the new collector.

Important Make sure that you do not use the same appliance id/certificate on two active collectors, since this would cause issues during uploads (not knowing which collector sent the upload).