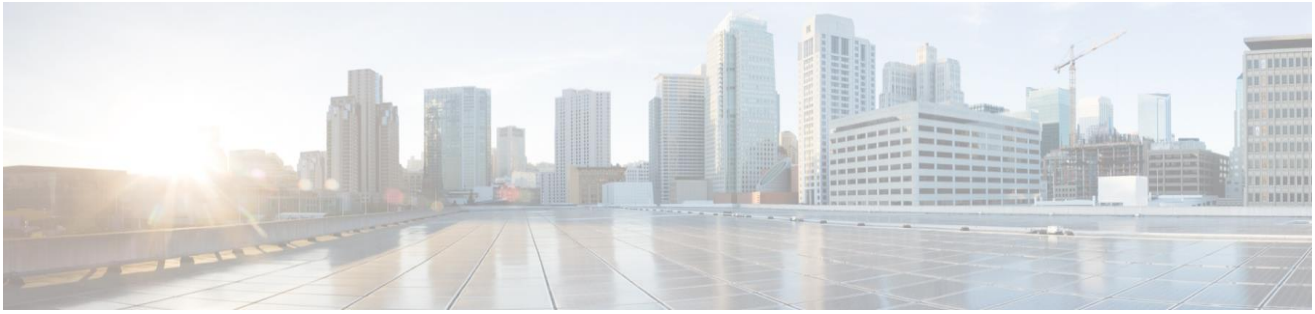




Common Services Platform Collector 2.5 Quick Start Guide

September 18, 2015

Corporate Headquarters

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

Introduction

The Cisco Partner Support Service (PSS) 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 data center stores the data uploaded from the associated Smart Collectors and uses that data to evaluate and report on the network's 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).

For PSS, there are two image options for a CSP-C:

- Use an ISO Image on a hardware device.
- Server Image (OVF 10) for OVF Compatible Hypervisors

The steps included in this Quick Start Guide provide the methods for completing the following tasks:

- Access and download images (download versus add-to-cart)
- Using the ISO image, which includes the following items:
 - How to get the Image
 - Install the ISO Image onto the CSP-C Collector
 - Configure the CSP-C Collector IP Address on the hardware device.
- Register the CSP-C on the PSS Smart Portal
- Configure the CSP-C and Device Credentials
- Discover and Manage Devices
- Manage the collector
- Upload an Inventory
- Basic Troubleshooting and Best Practices

Available PSS Image Options

There are two types of images that are available in the PSS release:

- Disk Image (ISO) for Physical Hardware
- Virtual Image (OVF 10) for OVF Compatible Hypervisors

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.

Type	Number of Managed Devices	CPU	RAM	Hard Drive
Virtual Image	10K or less	4 vCPUs	4 GB	200 GB
Disk Image	10K or less	1 x86 CPU	4 GB	200 GB

How to Access the Images

Go to the Smart Portal homepage (<https://tools.cisco.com/csp>)

In the Download Section, click **Smart Collector – Common Services Platform Software**

Support
Smart Portal

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

PSS will undergo weekly maintenance from 7 PM Saturday till 2 AM Sunday Pacific Time. You may notice interruptions in service during this window of time

Smart Portal Overview
Delivering capabilities to discover, collect and analyze network device details and provide network aware information.

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 psscommunity2external@cisco.com.

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

Inventory Collection
[Register CSP-C](#)
[Manage Collectors](#)
[Revalidate Inventory Uploads](#)
[Manual Import \(Sample CSV Format\)](#)

Installed Base Management, Alerts and Diagnostics
[Reports](#)
[Reports 2.0](#)

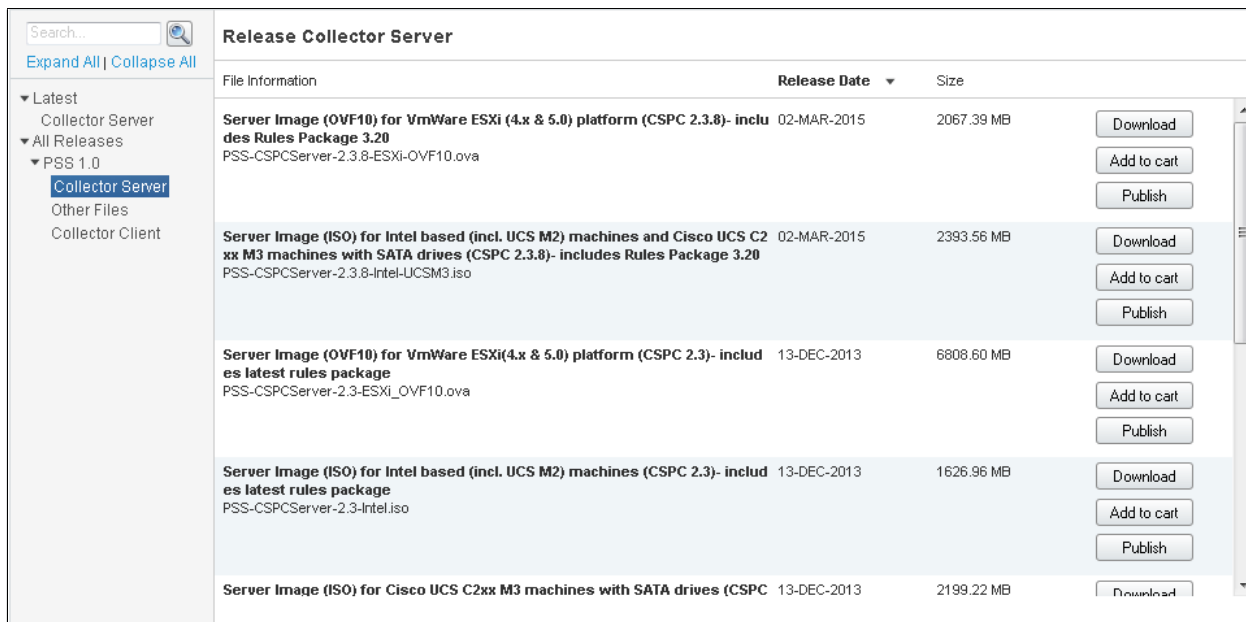
Toolkit: Roll over tools below

Related Tools
[Related Tools](#)
[TAC Case Query](#)
[TAC Case Create](#)
[Dynamic Configuration Tool](#)

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

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

Show Me How.



Release Collector Server

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

▼ Latest
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 2.3.8)- includes Rules Package 3.20 PSS-CSPCServer-2.3.8-ESXi-OVF10.ova	02-MAR-2015	2067.39 MB	Download Add to cart Publish
Server Image (ISO) for Intel based (incl. UCS M2) machines and Cisco UCS C2xx M3 machines with SATA drives (CSPC 2.3.8)- includes Rules Package 3.20 PSS-CSPCServer-2.3.8-Intel-UCSM3.iso	02-MAR-2015	2393.56 MB	Download Add to cart Publish
Server Image (OVF10) for VmWare ESXi(4.x & 5.0) platform (CSPC 2.3)- includes latest rules package PSS-CSPCServer-2.3-ESXi_OVF10.ova	13-DEC-2013	6808.60 MB	Download Add to cart Publish
Server Image (ISO) for Intel based (incl. UCS M2) machines (CSPC 2.3)- includes latest rules package PSS-CSPCServer-2.3-Intel.iso	13-DEC-2013	1626.96 MB	Download Add to cart Publish
Server Image (ISO) for Cisco UCS C2xx M3 machines with SATA drives (CSPC 2.3.8)- includes Rules Package 3.20 PSS-CSPCServer-2.3.8-UCS-C2xx-M3-ISO.iso	13-DEC-2013	2199.22 MB	Download

On Collector Server page, select the image (version) to be used and click **Download** to download the file.



Note You need a Cisco.com user name/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.

Default Login User IDs

By default, the following user accounts are created:

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

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

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

Deploying Images

- ISO – Mount the Image, then follow the installation instructions.
- OVA – Deploy into existing virtual environment.
- Once installation is complete, configure the CSP-C Collector's IP Address using the following command:

```
conf ip eth0 <ipaddr> <netmask> <gateway>Requirements for Upload
```

CSP-C Registration

A CSP-C registration needs to be performed before the collector can be utilized. The registration process requires you to obtain an entitlement file. The entitlement file is used to complete the CSP-C installation.

To register a CSP-C, and obtain the entitlement files, perform the following tasks.

Pre-deployment Preparation

- Associate valid PSS contract in your user profile.

To add contracts to profile, send the following email.

email: web-help@cisco.com

Subject: PSS Partner - <Partner Name> - Add contract to user profile

Body:

Please associate the following contract to CCOID profile:

CCO ID:

Name:

Contract ID:

Once completed, proceed to the next step.

- Log into the Smart Portal (<https://tools.cisco.com/csp/>)
- Register the Entitled Company
 - Log into the portal with your CCO ID <https://tools.cisco.com/csp/>
 - Select **Self Registration Or Register Users**
 - Type in your CCO ID and select **Get Contract Number**
 - Select contract you just added to profile and **Continue**
 - You will then select the customer name that will be set as the Entitled Company name.
 - If there are multiple instances of the customer name, select ONLY ONE, select the first valid name.



Note The Entitled Company name should be the end-customer's name and the Bill-To name equals to the Partner's legal entity name.

- Select **Complete** to finish this step.

Register the CSP-C

- Go to the Cisco Smart Portal (<https://tools.cisco.com/csp/>). On the Smart Portal Overview page, click on **Register CSP-C**. Complete the User Registration process from [Chapter 2 of the Smart Portal – Partner User Registration](#).

Default Login User IDs

By default, the following user accounts are created:

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

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

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

Access the Appliance

To access the CSP-C Web UI, perform the following steps:

- Use the following URL format to access our appliance:

https://your_appliance_ip_address:8001/



Note The recommended browsers are Microsoft Internet Explorer 8.0, 9.0 and Mozilla Firefox 18.x and above.

- Go to your appliance and enter your login credentials. The default user id/password is noted in the [Default Login User IDs](#) section.

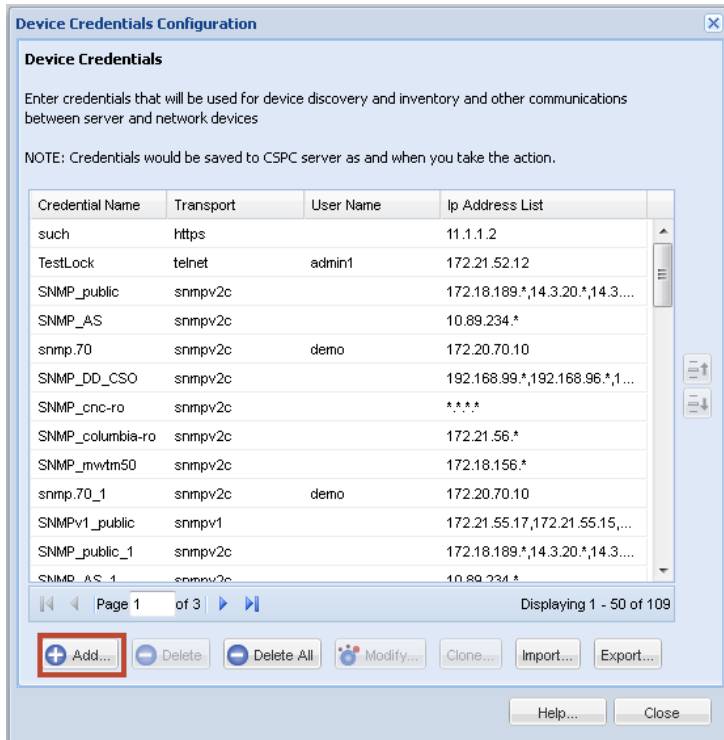
- Enter your login credentials. [Default Admin123 / Admin#123]

CSP-C Configuration and Device Credentials

In order to discover network devices and collect device data you must first enter the device credentials. SNMP credentials are required, SSH/Telnet credentials are recommended for collecting the show commands needed for classifying alerts in advanced collection.

To set the device credentials, perform the following:

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

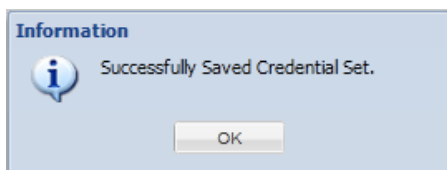


- Click **Add** to create a credential.

- Enter **Name** for Credential Identification.
- Select the **Protocol** to be used for this profile.
- Enter **IP addresses** to be used for this profile.

The **Include IP Address** Range option allows you to enter either a set of IP Addresses or a wildcard IP Addresses like 10.*.*, notifying any IP Address starting with 10. The **Exclude IP** Address Range works only for data collection. You can enter IP addresses by clicking IP Address List Editor, and give multiple IP addresses with comma separated in IP Address List field.

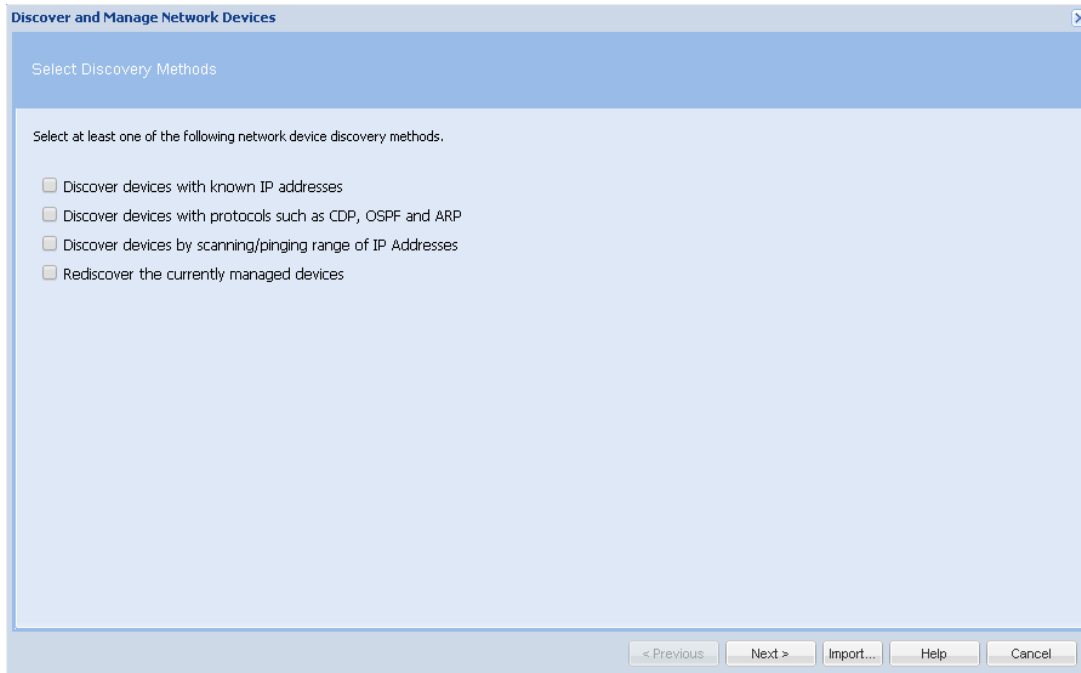
- Enter the required authentication fields for the protocol selected.
- Click **OK**: the **Edit Credential** window appears with a successful saved message.



Discover and Manage Devices

This section describes the process for discovering managed devices, after performing the collector upgrade:

- In the CSP-C navigation pane, click the **Applications** tab and choose **Device Management > Device Discovery and Management > Discover and Manage Devices**.
- The **Discover and Manage Network Devices** window appears displaying the Select Discovery Methods pane.



There are three discovery methods that CSP-C can use to manage devices:

- **Discover devices with Known IP Addresses**

You can enter the IP addresses manually or import the device list from either a CiscoWorks DCR file or a Pari Discovery Options XML file.

- **Protocols based Discovery (CDP, OSPF, ARP and more)**

For protocol based discovery, you need the following information:

- Protocol (CDP, Routing Table, ARP, OSPF Neighbors, BGP, HSRP, LLDP, etc.)
- Hop count (number of hops the discovery process should traverse)
- Seed IP Address(s) (Initial seed device or devices)

- **Range Based discovery (Start/End IP Address or CIDR)**

For IP Range Scanning based discovery, provide the Start IP address and the End IP address. You can also provide the Start IP in CIDR format as show here IP Address/subnet mask (x.x.x.x/x) and the End IP will be auto populated. You have select CIDR Address before providing Start IP Address.

Inventory Upload

To ensure a successful upload from a CSP-C Collector to the Cisco Data Center the following ports and specific IP addresses need to allow outbound access to the internet. ACL's on customers firewall might need to be configured to allow the CSP-C to upload successfully.

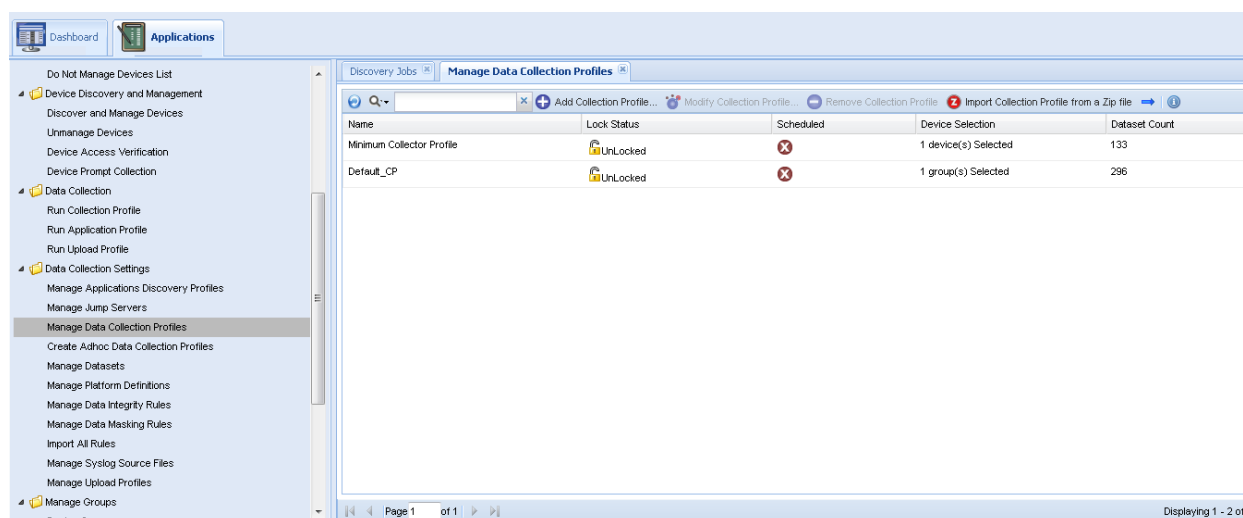
Protocol: HTTPS / SSL

Source IP Address	Source Port	Destination IP Address	Destination Hostname	Destination Port	Protocol	Direction
CSP-C Server IP	any	72.163.7.113	concsoweb-prd.cisco.com	443	TCP	Outgoing

Manage Data Collection Profiles

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

- Click the **Applications** tab and choose **Data Collection Settings > Manage Data Collection Profiles**. The Data Collection Profiles pane appears.



The Data Collection Profiles pane contains a Minimum Collector Profile. You can modify the Minimum Collector Profile by selecting the Minimum Collector Profile entry, and then clicking **Modify Collection Profile**.

Modify Collection Profile

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

Collection Profile Details

* Profile Title: Minimum Collector Profile

* Identifier: _mincp Generate

Description:

Profile Priority: Medium

Preserve Run Count: 1

Service Name: partner_support_service

Service Version:

Rule Package Version: 3.20

Use Fallback Credentials: ☐

Run Discovery Before Collection: ☒

Run Prompt Discovery Before Collection: ☐

Run DAV Before Collection: ☒

Disable Collection Interval: ☐

Mask IP Address: ☐

Mask Domain Name: ☐

Export Seed File: ☐

Advanced Options...

Collection Profile Schedule

☐ Schedule Periodic Collection

No schedule configured

Configure Schedule...

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

Export Options

☒ Export upon successful execution of collection profile

* Export Format: Cisco VSEM (.zip)

* File Name Prefix: Min_VSEM

Upload To Remote Server: ☒

Help... OK Cancel

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 Data Center, the data repository will not recognize the different service name and the data will not get routed correctly.

Manual Import

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

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

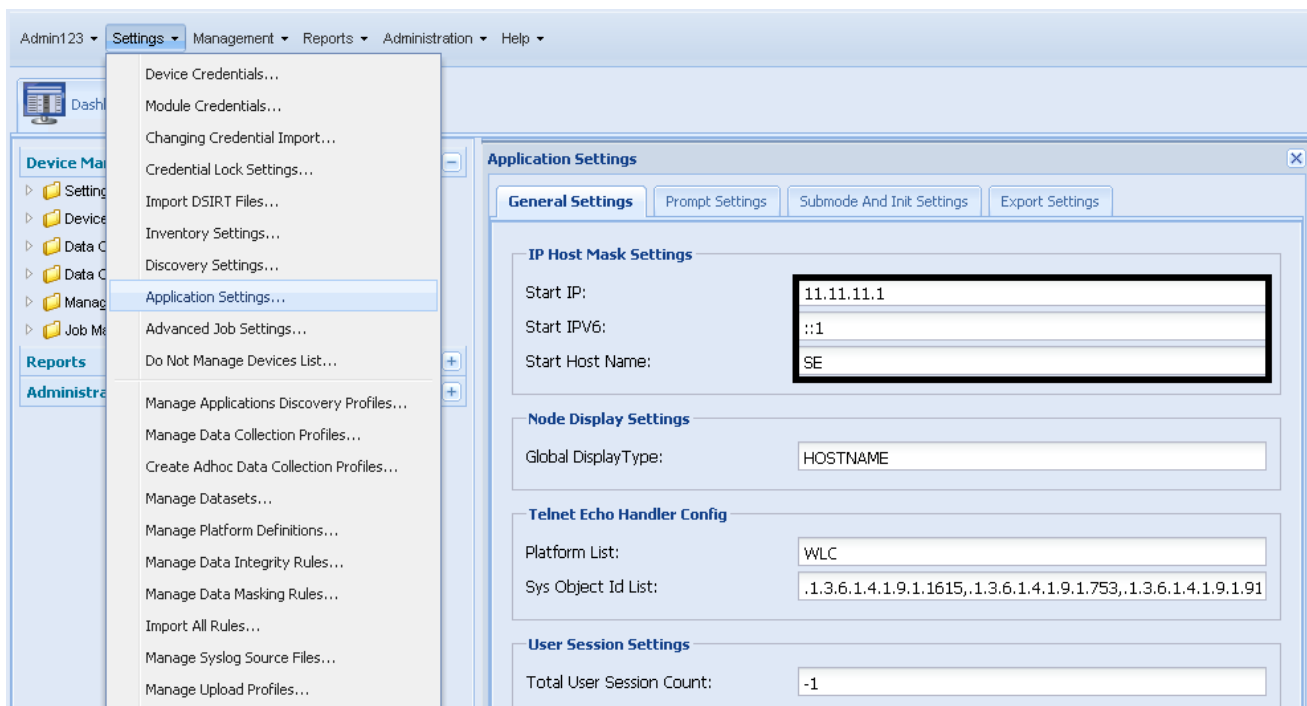
You can download the sample CSV format file from the [Smart Portal Overview page](#), add the required device information, and import the inventory manually.

For more information on importing the inventory manually into the Smart Portal, see [Smart Portal Partner Smart Collectors chapter](#) of the [Smart Portal User Guide for Partners](#).

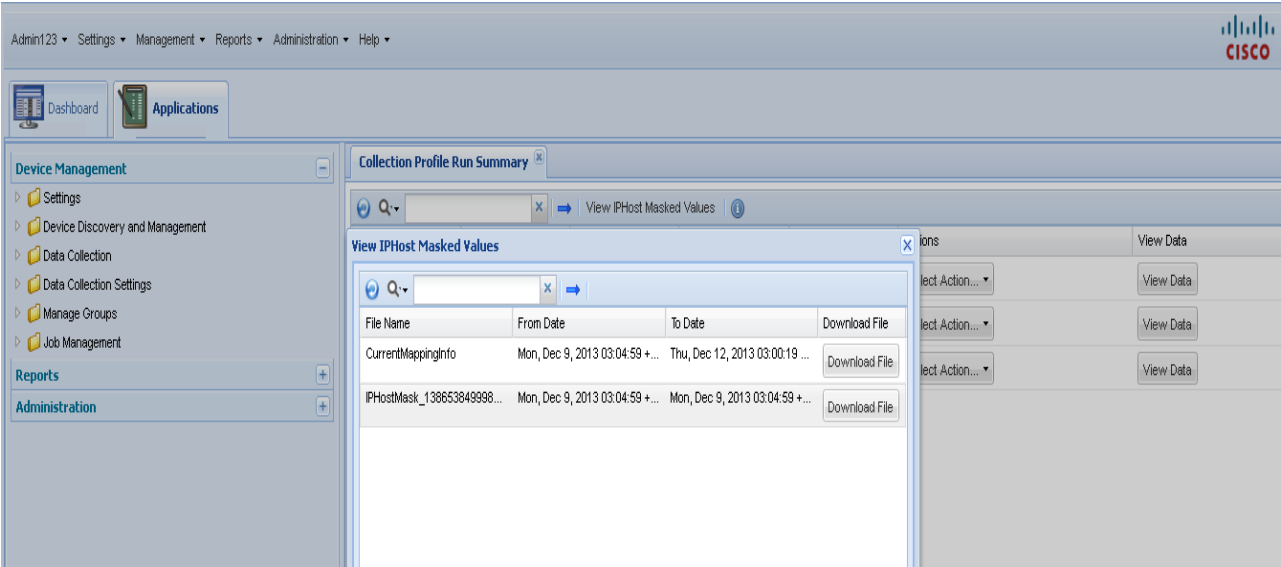
**Note**

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

DPA Masking for CSP-C 2.5



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



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
conf proxy *	conf proxy <ipaddr> [<port>][<user> <passwd>] The Conf proxy command allows the user to set the proxy server, which enables intranet/internet traffic to be routed from the configured proxy server originating from the Smart Services Appliance. The Conf Proxy command supports only HTTP traffic. This means if the appliance needs to access the internet via a NON-HTTP protocol like – XMPP, then the traffic will not be routed via the proxy servers. Smart services appliances use outbound traffic to communicate with Cisco. The specific ports for outbound communication are noted in section.	cisco, admin, user
connectivity direct-mode <options>	Options are enable or disable. Enables or disables connectivity direct mode (P2P gateway - IPsec tunnel).	cisco, admin, user
dmidecode *	Displays the hardware status provided by Boot Firmware.	cisco, admin, viewer
firewall <options>	Enable/disable firewall rules (this refers to the OS firewall and is meant for special circumstances only). In normal situations, firewall rules should be preconfigured in the appliance.	cisco
hostname <hostname>	Specifies the hostname of the device.	cisco, admin, user
log download *	This command places the selected log file into the 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 password to default	Can reset passwords for lower levels only (See default user accounts)

reload	Reboot the system	cisco, admin, user
route [-ad] *	Configures a static route on an interface. Options are: <intf> <network/mask> <gateway>	cisco, admin, user
show connectivity direct-mode	Indicates if Connectivity direct mode (the P2P gateway - IPsec tunnel connection) is enabled or disabled.	cisco, admin, user
show date	Show the current date	All (cisco, admin, user, viewer)
show firewall	Displays the firewall rules	cisco
show history *	Accesses the command history files stored on the appliance. Displays the command history for current user, if invoked without user id; displays a command history for specified user if specified with user id.	*'cisco' can view histories for all user ids. * 'admin' can view histories for 'admin', 'viewer' and 'user' * 'viewer' and 'user' can view their own histories
show hostname	Displays the hostname	All (cisco, admin, user, viewer)
show ipconfig	Shows the following information: - DHCP enabled (yes/no) - IP address - Subnet mask - Physical (MAC) address - Default gateway (proxy) - DNS server(s)	All (cisco, admin, user, viewer)

show logs *	Display logs based on selected file in each category. The options are: <logtype> (include exclude begin <pattern>) logtype = 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: (1) network utilization (%) for ethernet port (2) CPU and memory utilization	All (cisco, admin, user, viewer)
show route	Displays the routing table of the appliance.	cisco, admin, user
show timezone	Shows which time zone is set	All (cisco, admin, user, viewer)
show version	Display version	All (cisco, admin, user, viewer)
ssh <options>	Enables or disables ssh access 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	cisco, admin, user

	zone; enter (yes no)	
traceroute <host>	Lets you enable trace routing for a network device specified by the IP address and alternatively specify a file name for the results.	cisco, admin,
usb <options>	Options are: mount unmount list status copy from USB drive	cisco
User Help: User help for listing commands and for describing individual commands.	(1) Typing a command name without parameters shall list help for that command e.g. typing "show log". The command has to be available to the user id (privilege); otherwise, it is shown as not available. (2) Typing '?' after a command name shall be equivalent to typing the command without parameters. (3) General keywords such as "show" or "conf" shall list the show or conf commands available to the user, but no help for the commands. (4) Typing '?' will list all the CLI commands that are available to the user.	Each user ID has access to help for the commands that are relevant to its privilege level.