·IIIII CISCO



User Guide for CSPC Collection Platform Software

March 2024 Updated: Sept 16, 2024 CSPC 2.11.0.1 / 2.11.0.2

Cisco Systems, Inc. www.cisco.com

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices. THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

User Guide for CSPC Collection Platform Software © 2024 Cisco Systems, Inc. All rights reserved.



CH APT E R 1 CSPC Flow Chart 1-1

CH APT ER 2	Introduction 2-1				
	Introduction to CSPC Collection Platform Software 2-1				
	Who Should Use This Guide? 2-1				
	About this Guide 2-1				
	CSPC EOL Versions 2-1				
	Accessing the CSPC Collector 2-3				
	Recommendations on Password Usage 2-4				
	Password Creation 2-4				
	Password Change 2-4				
	Password Protection 2-5				
	Password Retrieval 2-5				
	Default Password 2-5				
	Not Permitted Characters 2-5				
	Not Permitted Password or Passphrase 2-6				
	Forgot Password 2-15				
	Server And Package Versions 2-17				
CH APT E R 3	CSPC Dashboard 3-1				
	Dashboard 3-1				
	Managed Devices 3-4				
	View Device Properties 3-7				
	View Latest Collection Details 3-7				
	Export 3-8				
	Non Managed Devices 3-8				
CH APT ER 4	CSPC Workflow 4-1				
CH APT ER 5	Quick Access Applications - Device Management 5-1				
	Common Application 5-1				
CH APT ER 6	Applications - Device Management 6-1				
	Device Management 6-1				

CHAPTER 7

Credential Management 6-2 Add/Import Credentials 6-2 Manage Sub Module Credentials 6-8 Manage Seed File 6-10 Imported Seed file 6-11 Do Not Manage Device List 6-13 **Device Grouping** 6-14 **Device Groups** 6-14 **General Settings** 6-18 **Application Settings** 6-19 **Discovery Settings** 6-24 **Access Verification Settings** 6-27 **Inventory Settings** 6-28 Advanced Job Settings 6-36 **Collection Rules** 6-38 Manage Data Collection Profiles 6-38 Manage MulitService Collection Profiles 6-44 Manage Upload Profiles 6-46 Manage Datasets 6-49 Manage Platform Definitions 6-69 Manage Data Integrity Rules 6-73 Manage Data Masking Rules 6-75 Manage Syslog Source Files 6-77 **Miscellaneous Rules** 6-80 **Export All Rules** 6-80 Import All Rules 6-80 Import DSIRT Files 6-80 Manage Application Discovery Profiles 6-81 Manage SNMP Trap Profiles 6-83 Manage Jump Server 6-85 Credential Lock Settings 6-87 Manage WorkFlow 6-88 **Applications - Management Tasks** 7-1 Management Tasks

7-1 **Device Tasks** 7-1 **Discover Devices** 7-1 Unmanage Devices 7-12 Verify Device Access 7-13 **Device Prompt Collection** 7-17

Common Tasks 7-20 Collect Data 7-20 **Upload Data** 7-22 Adhoc Data Collection 7-24 **Collect Application Data** 7-27 Job Run Status 7-28 Job Run Status 7-28 Job Management 7-29 Manage Discovery Jobs 7-29 Manage Device Access Verification Jobs 7-30 Manage Workflow Jobs 7-32 Manage Configuration Jobs 7-33 Manage Device Prompt Collection Jobs 7-34 Manage Health Monitor Jobs 7-35

Applications - Reports 8-1

Reports 8-1 **Device Reports** 8-1 View Managed Devices 8-2 View Unreachable Devices 8-3 View Duplicate Devices 8-3 Discovery Report 8-4 **Device Display Properties** 8-4 Non SNMP Devices 8-5 Interface Summary (IOS, PIX, ASA, IOS-XR) 8-5 **Device Access Verification Reports** 8-6 **Device Access Verification Summary** 8-6 Device Access Verification By Dataset Type 8-7 **View Access Verification Results** 8-8 **Data Collection Reports** 8-9 View Collected Data 8-9 View Collection Run Summary 8-15 Config Collected Devices 8-17 Config Data Per Device 8-19 **Export Detailed Device Data** 8-20 Services Reports 8-21 Alerts 8-21 **SNMP** Trap Report 8-21 Syslog Summary 8-23 Syslog Messages 8-24

CHAPTER 8

I

Job Reports 8-25
Discovery Jobs 8-26
Inventory Jobs 8-28
Device Access Verification Jobs 8-30
Job Management Reports 8-31
View Job Metrics 8-44
Audit Trails 8-46
Device Management Audit Trails 8-46
Data Collection Audit Trail Report 8-47
Server Audit Trail Report 8-47
Miscellaneous 8-48
Device Launch Pad 8-48
View Locked Credentials 8-50
Disabled Protocol Report 8-51
Disable Command Report 8-51
Device Timeout Configuration 8-52
Device Jump Server Mapping 8-52
Application Profile Run Summary 8-52
Application Discovery Report 8-53
Applications - Administration 9-1
Applications - Administration9-1Administration9-1
Applications - Administration9-1Administration9-1User Management9-1
Applications - Administration9-1Administration9-1User Management9-1Manage Users9-1
Applications - Administration9-1Administration9-1User Management9-1Manage Users9-1Manage Remote Authentication Servers9-3
Applications - Administration9-1Administration9-1User Management9-1Manage Users9-1Manage Remote Authentication Servers9-3Login Settings9-4
Applications - Administration9-1Administration9-1User Management9-1Manage Users9-1Manage Remote Authentication Servers9-3Login Settings9-4User Session Report9-6
Applications - Administration 9-1 Administration 9-1 User Management 9-1 Manage Users 9-1 Manage Remote Authentication Servers 9-3 Login Settings 9-4 User Session Report 9-6 User Preferences 9-6
Applications - Administration 9-1 Administration 9-1 User Management 9-1 Manage Users 9-1 Manage Remote Authentication Servers 9-3 Login Settings 9-4 User Session Report 9-6 User Preferences 9-6 Modify Data/Time Preference 9-6
Applications - Administration 9-1 Administration 9-1 User Management 9-1 Manage Users 9-1 Manage Remote Authentication Servers 9-3 Login Settings 9-4 User Session Report 9-6 User Preferences 9-6 Modify Data/Time Preference 9-6 Configure Default Device Display Property 9-7
Applications - Administration 9-1 Administration 9-1 User Management 9-1 Manage Users 9-1 Manage Remote Authentication Servers 9-3 Login Settings 9-4 User Session Report 9-6 User Preferences 9-6 Modify Data/Time Preference 9-6 Configure Default Device Display Property 9-7 Alert Management 9-7
Applications - Administration 9-1 Administration 9-1 User Management 9-1 Manage Users 9-1 Manage Remote Authentication Servers 9-3 Login Settings 9-4 User Session Report 9-6 User Preferences 9-6 Modify Data/Time Preference 9-6 Configure Default Device Display Property 9-7 Alert Management 9-7 Email Settings 9-7
Applications - Administration 9-1 Administration 9-1 User Management 9-1 Manage Users 9-1 Manage Remote Authentication Servers 9-3 Login Settings 9-4 User Session Report 9-6 User Preferences 9-6 Modify Data/Time Preference 9-6 Configure Default Device Display Property 9-7 Alert Management 9-7 Email Settings 9-7 Manage Subscribers 9-8
Applications - Administration 9-1 Administration 9-1 User Management 9-1 Manage Users 9-1 Manage Remote Authentication Servers 9-3 Login Settings 9-4 User Session Report 9-6 User Preferences 9-6 Modify Data/Time Preference 9-6 Configure Default Device Display Property 9-7 Alert Management 9-7 Email Settings 9-7 Manage Subscribers 9-8 Alert Configuration 9-9
Applications - Administration 9-1 Administration 9-1 User Management 9-1 Manage Users 9-1 Manage Remote Authentication Servers 9-3 Login Settings 9-4 User Session Report 9-6 User Preferences 9-6 Modify Data/Time Preference 9-6 Configure Default Device Display Property 9-7 Alert Management 9-7 Email Settings 9-7 Manage Subscribers 9-8 Alert Configuration 9-9 Backup and Restore 9-10
Applications - Administration 9-1 Administration 9-1 User Management 9-1 Manage Users 9-1 Manage Remote Authentication Servers 9-3 Login Settings 9-4 User Session Report 9-6 User Preferences 9-6 Modify Data/Time Preference 9-6 Configure Default Device Display Property 9-7 Alert Management 9-7 Email Settings 9-7 Manage Subscribers 9-8 Alert Configuration 9-9 Backup and Restore 9-10 Backup 9-11
Applications - Administration 9-1 Administration 9-1 User Management 9-1 Manage Users 9-1 Manage Remote Authentication Servers 9-3 Login Settings 9-4 User Session Report 9-6 User Preferences 9-6 Modify Data/Time Preference 9-6 Configure Default Device Display Property 9-7 Alert Management 9-7 Email Settings 9-7 Manage Subscribers 9-8 Alert Configuration 9-9 Backup and Restore 9-10 Backup 9-11 Restore Backup 9-14
Applications - Administration 9-1 Administration 9-1 User Management 9-1 Manage Users 9-1 Manage Remote Authentication Servers 9-3 Login Settings 9-4 User Session Report 9-6 User Preferences 9-6 Modify Data/Time Preference 9-6 Configure Default Device Display Property 9-7 Alert Management 9-7 Email Settings 9-7 Manage Subscribers 9-8 Alert Configuration 9-9 Backup and Restore 9-10 Backup 9-11 Restore Backup 9-14 Log Preferences 9-16
Applications - Administration 9-1 Administration 9-1 User Management 9-1 Manage Users 9-1 Manage Remote Authentication Servers 9-3 Login Settings 9-4 User Session Report 9-6 User Preferences 9-6 Modify Data/Time Preference 9-6 Configure Default Device Display Property 9-7 Alert Management 9-7 Email Settings 9-7 Manage Subscribers 9-8 Alert Configuration 9-9 Backup and Restore 9-10 Backup 9-11 Restore Backup 9-14 Log Preferences 9-16 Log Preferences 9-16

CSPC Collection Platform Software User Guide

CH APT ER 9

Miscellaneous Applications 9-18 Manage Add-on Process 9-18 Manage UI Add-Ons 9-18 Server Properties 9-19 Diagnostic Tools 9-21 XML API Console 9-22

I

Γ

си арт б.р. 10	Menu Ontions 10-1
CHAILER IV	Menus 10-1
	User Name 10-1
	Settings 10-2
	Management 10-3
	Reports 10-4
	Administration 10-5
	Help 10-6
	Quick Menus 10-6
APPENDIX 11	Adding Devices to CSPC 11-1
	Overview 11-1
	Examples 11-2
APPENDIX 12	Seed File Formats 12-1
	Header Information 12-2
	CNC Seed File Format 12-2
	Cisco Works Seed File Format 12-4
	Simplified Seed File Format 12-6
	Export File Format 12-7
APPENDIX 13	Optional Parameter for NATed Appliances 13-1
APPENDIX 14	Conditional Collection 14-1
	Conditional Collection Description 14-1
	What is Supported 14-1
	Audit Use Case 14-1
	nfidentiall Manager Use Case 14-1
	SNMP/CLI Configuration Fallback Collection 14-2
	Collected Value Based Follow-on Collections 14-2
	Commands Requiring Re-login 14-2
	Condition Collection in Detail 14-2

APPENDIX 15

Statement 14-2 **Condition Statement** 14-3 Loop Statement 14-4 Examples 14-5 **CLI** Complex Collection 14-5 **SNMP** Complex Collection 14-6 **XML APIs** 15-1 Seedfile job for runnow 15-1 Scheduled seedfile job 15-1 Add Notification 15-2 **Delete All Notifications** 15-2 Delete Single Notification 15-3 Get All Notification Types 15-3 Modify Notification 15-3 Add SNMP Trap Profile 15-4 Delete All SNMP Trap Profiles 15-4 Delete Single SNMP Trap profile 15-5 Get All SNMP Trap Profiles 15-5 Get Single SNMP Trap Profile 15-5 Modify SNMP Trap profile 15-6 SNMP Trap Report 15-6 Modify SNMP trap port and Purge Settings 15-7 CSPC DB backup and restore XML API 15-8 Backup Job XML API 15-8 Restore Job XML API 15-9 CLI Channel XML API 15-9 New Device Input XML 15-9 Modify Channel XML 15-12 CLI Channel Get Report XML 15-14 **Channel Delete Channel XML** 15-14 Get CLI Channel List Report XML15-15 Get Imported Devices Status Report 15-15 CSPC Backup (PSS) 15-15 CSPC Backup (PSS) - Schedule 15-16 Collection of Loopback Interface IP address (NOS) 15-17 Add Optional Metadata Label to OIDs in Custom Datasets (PSS) 15-17 Export and Import Collection Profiles (PSS) 15-18 Upload Signature for Custom Profiles (PSS) 15-19 **Discovery Classification 15-19**

	Enabling/Disabling the WebSocket Connection 15-20
	Enabling 15-20
	Disabling 15-21
	GET WebSocket Status 15-21
	Add External Platform Components Credentials 15-21
	Upload Health Information 15-23
	Error Message for Smart DAV based on SSH/Telnet 15-23
	Region Based Collection via User Groups 15-24
	Service Name for Service Prioritize 15-24
	Add Credentials 15-25
	Add SQL Datasets 15-25
	Schedule the Job with Service Name 15-26
	Add File Dataset 15-27
	API to Export and Get File name 15-27
	API to Download the Collection Profile Run Data 15-28
	Additional Device Properties 15-28
	Add Family OS type and Technology Properties 15-28
	Modify Additional Device Properties 15-29
	Delete Additional Device Properties 15-30
	Get Additional Device Properties 15-30
	Adding WMI Datasets 15-31
	Adding LDAP Datasets 15-32
APPENDIX 16	Uploading Valid SSL Certificate 16-1
APPENDIX 17	RSA SHA 256 Fingerprint 17-1
APPENDIX 18	CSPC - Automated Fault Management (AFM) Tool Integration 18-1
APPENDIX 19	Reset Root Password and Deployment of ESXi 7.0 19-1
	Recovering Root Password 19-1
	Deploying CSPC 2.11 OVA on ESXi 7.0 19-2
	I i g an
APPENDIX 20	Setting hostname as PrimaryDeviceName 20-1
APPENDIX 21	Frequently Asked Questions 21-1

Γ

Contents



CSPC Flow Chart

Γ







Introduction

Note: RADKit is now supported on the CSPC VM

Cisco RADKit is a network-wide orchestrator. Experience a radical new way of addressing your equipment, boost your Cisco Services, and expand your capabilities. It is now supported to run on the same VM as your CSPC collector. For more information visit: <u>https://radkit.cisco.com</u>

Introduction to CSPC Collection Platform Software

The Cisco Common Service Platform Collector (CSPC) is an SNMP-based tool that discovers and collects information from the Cisco devices installed on your network. The CSPC software provides an extensive collection mechanism to gather various aspects of customer device data. Information gathered by the collector is used by several Cisco Service offers, such as Smart Net Total Care, Partner Support Service, and Business Critical Services. The data is used to provide inventory reports, product alerts, configuration best practices, technical service coverage, lifecycle information, and many other detailed reports and analytics for both the hardware and operating system (OS) software.

This User Guide explains how to use CSPC software version 2.11. Refer to CSPC Release Notes for program updates, important notes, image location and other information.

CSPC 2.10 and earlier releases are no longer supported. If you experience problems with an earlier release you are recommended to update the collector software version to latest available.

Who Should Use This Guide?

This guide is written for Network and Security Administrators and Cisco Network Engineers who want to collect information on heterogeneous networks comprised of network devices such as routers, switches, firewalls, wireless devices, intrusion prevention systems, and so forth.

You should be familiar with network fundamentals, connectivity, network device configuration and administrative tasks you want to perform over your network.

About this Guide

The CSPC User Guide covers all available functionality in CSPC user interface.

CSPC EOL Versions

ALL CSPC < 2.11 have reached EDoS. Upgrade your collectors!

For continued effective delivery of services, customers are required to be on the supported versions of the collectors. You are running into issues; you may be required to update the collector software version before TAC helps in diagnosing the problem.

Figure 2-1 CSPC EOL Info

EOL Date	EOL Version	EoSWM Date	LDoS Date
Dec, 2012	CSPC 2.0.3	Jan, 2013	Apr, 2013
July, 2013	CSPC 2.1	Aug, 2013	Nov, 2013
April, 2014	CSPC 2.2	May, 2014	Aug, 2014
June, 2015	CSPC 2.3	July, 2015	Oct, 2015
March 3, 2016	CSPC 2.4	April 3, 2016	July 3, 2016
March 20, 2017	CSPC 2.5	April 20, 2017	July 20, 2017
May 9, 2018	CSPC 2.6	June 9, 2018	Oct 10, 2018
September 25, 2020	CSPC 2.7	October 25,2020	January 25, 2021
September 30, 2021	CSPC 2.8	Oct 30, 2021	January 30, 2022
March 31, 2023	CSPC 2.9	March 31, 2023	March 31, 2023
June 30, 2024	CSPC 2.10	July 30, 2024	Oct 30, 2024

Accessing the CSPC Collector

CSPC 2.11 is a web based application and can be accessed by using a URL.

Note

Supported browsers are Microsoft Internet Explorer 11, Chrome 85, and Mozilla Firefox 80. It is recommended to use Mozilla Firefox.

Follow the steps given below to access the CSPC application:

Step 1 In a web browser, open the URL:

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



CSPC-server-ip in the above URL is the IP address of the machine on which CSPC is installed.

- Certificate Error showing the website's security certificate message is displayed when you access the above URL. Click **Continue** to this website link or Upload the SSL Certificate to proceed for login. Refer Uploading Valid SSL Certificate
- You can use the default username and default username is **admin**. You have set the password for the first login.
- User account password will expire in 3 to 12 months and default is 6 months. Maximum password reset time is 12 months.
- · All the failed logins are detected and audited
- Number of failed user password entries that can be tried before that user account or IP address is locked and default values is 5 times
- Number of minutes that a user's account or IP address remains inaccessible after being locked in response to several invalid login attempts within the amount of time specified by the Lockout Reset Duration attribute and default values is 60 minutes.
- Time frame within which invalid login attempts must occur in order to lock the user account and default value is 5 minutes.
- Step 2 Setup the password for admin user and enter characters in the image, this is only for first login and screen appears as shown below.

Figure 2-2	Setup Password
	սիսիս
	CISCO.
Common	Service Platform Collector
2.10	
* Establish a	admin password to be used on the Collector Web Portal
Username:	admin
Password:	
Confirm Password:	
Enter the charac	ters you see in the below image.
w5	e3a º
* These characters a	are case sensitive.
	Login

Recommendations on Password Usage

Password Creation

- All passwords, passphrases, and PINs ("passwords") must comply with the Password Construction Standard.
- Users must not use the same password for Cisco accounts and for other non-Cisco access (for example, users must not use the same password (CEC) for Cisco accounts as for other non-Cisco access (for example, personal accounts, option trading, banking). Users must not store Cisco account passwords in external locations such as cloud service providers (for example, personal banking, email, and social media).
- Accounts used for administration with system-level privileges granted through group memberships
 or programs such as "Sudo", must have a unique password from all other accounts held by that user
 to access system-level privileges.

Password Change

- All user-level passwords (CSPC UI, SSH and CLI) must be changed at minimum every six months.
- All system-level passwords (privileged administration accounts or user-level accounts with privileged administration access) must be changed at minimum every 90 days.
- All production system-level passwords must be part of the Corporate Information Security administered global password management database
- If a password is guessed or cracked during period or random scans, the password must be changed to comply with this policy.

Password Protection

- Passwords must not be shared with anyone, including administrative assistants, managers, coworkers, and family members. All passwords must be classified Cisco Restricted data and handled according to the Data Protection Standard.
- Systems, applications, devices, and services must not store or transmit passwords in clear text or in any easily reversible form.
- Passwords must not be inserted into email messages, support cases, or other forms of electronic communication.
- Do not write passwords down and store them anywhere in your office. Do not store passwords in an unencrypted file on a computing device, mobile phone, or tablet.
- Do not use the "Remember Password" feature of applications (for example, web browsers) on non-trusted devices.
- · Users must report any suspected password compromise and reset all passwords immediately.

Password Retrieval

- · Password retrieval questions must be entered at the time of first log-in
- At least three security questions to be answered out of 20
- · Lost passwords cannot be retrieved without answering the security questions

Default Password

- Number of default user/Password shall be limited to bare minimum, depending on the application need.
- All default password if/when needed shall be dynamic. In other words, attempt shall be made to make the default passwords installation specific so that it cannot be used to compromise more than one system
- · Default user ID and password shall also follow Cisco InfoSec policy as defined above
- Strong passwords and passphrases must meet the following requirements:
- Contain at least eight alphanumeric characters.
- Contain both upper and lower case letters.
- Contain at least one number (for example, 0-9).
- In CLI Prefix all these characters (! $\& () | \langle ; ' \rangle$) with escape character (for example: \!).
- In CLI these characters (" < '?) are not accepted.

Not Permitted Characters

The following characters are not permitted because they may conflict with some Cisco applications:

- Special 8-bit characters (for example, £, Á ë, ô, Ñ, ¿, β)
- Spaces

Not Permitted Password or Passphrase

The following password or passphrase characteristics are not permitted:

- Match previous ten password or passphrases.
- Contain less than eight characters.
- Can be found in a dictionary, including foreign language, or exist in a language slang, dialect, or jargon
- Contain personal information such as birth dates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters
- Contain work-related information such as building names, system commands, sites, companies, hardware, or software
- · Contain the words cisco, sanjose, sanfran or a derivation
- Contain number patterns such as aaabbb, qwerty, zyxwvuts, or 123321
- Contain common words spelled backward, or preceded or followed by a number (for example, terces, secret1 or 1secret).
- Step 3 Enter the credential and characters in the image, click Login.

Figure 2-3	CSPC Collector		
Comm	iliii CISCO. ton Service Platform Collector 2.10 (CSPC)		
	* Enter your CSPC credentials		
Username:	admin		
Password:	•••••		
Enter the characters you see in the below image.			
þe			
" These chara	ters are case sensitive. Forgot Password?		
	Reset Login		

Step 4 Answer the questions and click **OK** button to save the password reset questions.

igure 2-4	Password Reset Questions	
sword Reset Ques	tions	×
First login requi	res user to answer the questioner Questions	
* Question 1:	Car I wished I owned?	
* Answer 1:	•••	
* Question 2:	Favorite game or sport to play?	
* Answer 2:	•••••	
* Question 3:	First vehicle I drove?	
* Answer 3:	•••••	
	OK	

Figure 2-5 End User License Agreement

Cisco Systems TERMS OF USE
Legal Agreement
Thank you for using the Cisco Systems Product CSP Collector (the "Product"). These Terms of Use apply to all users of the Product ("Users"), and constitute a binding, legal agreement ("Agreement") between User and Cisco Systems, Inc. ("Cisco Systems").
License
This License sets forth User's rights to use the software provided through the Appliance (the "Software"), related content (the "Content"), and all associated documentation (the "Documentation"), all of which are the proprietary and copyrighted material of Cisco Systems. Collectively, the Software, Content, and Documentation are referred to in this Agreement as the "Licensed Product." Upon receipt of the applicable license fee, Cisco Systems grants to User the non-exclusive, non-transferable right to use the Licensed Product solely for Users benefit.
Proprietary Rights

Step 5 Click Accept button to accept the terms of use.

Step 6 Enter the required fields to configure CSPC to collect devices. Click Next.

Parameter	Description
DNS Server	IP Address of DNS Server
NTP Server	IP Address of NTP Server
Time zone	Time zone of the collector
Set Time	Sets the appliance time, and time should match the actual time of the selected time zone
Host Name	Name of the host

Table 2-1Wizard Parameters

Parameter	Description
IP Address/Host Name	IP Address or Host Name of Proxy Server
Port	Port number of Proxy Server
Username	Credentials of Proxy Server
Password	

Note	

Proxy server is optional. It takes 30 second to configure.

hases	The second se	and to be all CCD Count on Francischer Justice all'action
install	This wizard walks you through the	steps to install CSr-C and configure it for device collection.
Register	DNS Server/Hostname:	Enter DNS server name
👍 Add Devices		
Access Credentials		
Collect	* Timezone:	Select timezone 👻 🕕
	Set Time (24 Hour Format):	HH MM V
	NTP Server:	Enter NTP server IP
	Hostname:	(Enter hostname)
	Proxy Server	
	* Ip Address/Hostname:	Enter IP Address
	* Port:	Enter port
	Username:	Enter Username
	Password:	
	Denotes Mandatory Fields	

- Step 7 You can register using one of following:
 - Browser to upload the Service Certificate File.

Figure 2	2-7 Service	Certificate File
cisco	Common Ser	rvice Platform Collector 2.10
Phases	Install Register Add Devices Access Credentials Collect	Now you need to register this collector to the respective service. Below options are available Prode Service Certificate from the service portal you plan to use this collector with. This registers CSPC with the service. Certificate File: Postret the collector without registering with any service (trial) Certificate file: Postret the collector without registering with any service (trial) Certificate file: Postret the registration and the data from backed up file:
		Next

OR

• Enter COO Credentials to get trail license. Select Send Usage Data to Cisco only if required and click Next



- You can download the CSPC and install using trail license, but CSPC needs to register with Cisco • before start using it. You can configure CSPC using the wizard as the first option.
- ٠ If you like to login to Cisco pages and get benefits, then you have create Cisco.com ID (CCO ID) this is the user ID

de de la co		
cisco	imon Service Platform Collector 2.10	
Phases Install Register Add Devic Access Cr Collect	Now you need to register this collector to the respective service. Below options are available I collector without registering with any service (trial) I collector without registering without registering without registering without registering without registering without registering without registeri	
OD	Next	

Figure 2-8 COO Credential

OR

• To restore the backup select Restore the registration and the data from backed up file.

co Common S	ervice Platform Collector 2.10
Phases	Now you need to register this collector to the respective service. Below options are available
install	Percented Counties Contribute forest the country workships to use this callectors with This expirators CEDC with the counter
🜻 Register	Provide Service Certificate from the service portat you plan to use this conector whith this registers CSFC with the service
Add Devices	Register the collector without registering with any service (trial)?
Access Credentials	
Collect	Restore the registration and the data from backed up file
	Next

Figure 2-9 Restore Backup

Chapter 2

Introduction



• Enter IP Address and use > to select the IP Address or range of IP Address.

>	Service Frational Concettor 2:10	
ses	Discover by IP Addresses Discover By Protocol	
Register	Define discovery settings for CSPC by adding a individual IP or range of	IP Addresses, Any or all methods of adding devices can be used.
Add Devices	IP Address Range/Subnet	Selected IP Address Range (1)
Access Credentials	From: 5011	📝 Start IP End IP
Collect	To: 5011d	5.0.1.1 5.0.1.10
		Delete
	IP Address ?	Selected IP Address (0)
		V IP Address
		>
	k. e	Delete

• Select the required **Protocol(s)**, **HOP Count**, and **Seed IP Address**. Use > to select seed IP Address.

5	Discover by IP Addresses Discover By Protocol	
Add Devices Add Devices Access Credentials Collect	Discover by IP Address Discover By Protocol Add devices by providing seed devices and protocols to discover other connected devices Select Protocols Cisco Discovery Protocol(CDP) OSPF Neighbours Border Gateway Protocol(BGP) Link Layer Discovery Protocol(LDP) Hop Count Hop Count: 1 V Selected Seed IP Address/Hostname (0) Input Seed Devices P Address	

Figure 2-11 Discovery By Protocol

Step 9 You can add credential using one of following and click Add Credential:

• If you select **SNMPV1/V2** enter **Credential Name**, **Read**, and **Write Community String**. Use > to select credential.

Register Add Devices Access Credentials Callect

If you select SNMPV3 enter Credential Name, User Name, Engine ID, Auth Algorithm, Password, Privacy Algorithm, Password. Use > to select credential.



565	SNMP Telnet/SSH					
Install	Provide SNMP V1/V2 or SNMP	V3 credentials for verifying the devices				
🛉 Register	SNMP V1/V2 SNMP V	73		Selected Credentials		
Add Devices				IVI Protocol	Credential Name	
P Access Credentials	Credential Name:					
Collect	* User Name:	(
	Engine Id:					
	Auth Algorithm:		~ >	j.		
	Auth Password:					
	Confirm Auth Password:					
	Privacy Algorithm:		~			
	Privacy Password:					
	Confirm Privacy Password:					

- If you select **Telnet** enter **Credential Name**, **User Name**, **Password**, **Enable User Name**, **Enable Password**, and **Pass Phase**. Use > to select credential
- If you select SSH enter Telnet enter Credential Name, User Name, Password, Enable User Name, Enable Password, and Pass Phase. Use > to select credential

Figure 2-14 Telnet and SSH

	i tovide relievor 5511 autoendoa	mon for verifying the devices			
Register	Telnet O SSH		Selected Credentials	The second	
Add Devices			Protocol	Credential Name	
Access Credentials	Credential Name:	(
Collect	Authentication				
	User Name:	<u></u>			
	Password:	C	>		
	Confirm Password:	C			
	Enable User Name:	Ç			
	Enable Password:				
	Confirm Enable Password:				
	Pass Phrase:				Deleti

Step 10 Select Start Collection now and click Collect Now to start collection instantly or click Schedule Periodic Collection and click Schedule to collect at a later time. You can schedule Start and End Date/Time or select the Recurrence pattern as Minutely, Daily, Weekly, Monthly, or Yearly as shown in Figure 2-16.

	Select option to collect immediately or schedule collection for later. Scheduling periodic collection is recommended
Register	Note: All newly added devices and existing managed devices will be considered for collection
Add Devices	Ander Full he way added de rices and existing managed derives will be considered for concention
Access Credentials	● Start collection now ○ Schedule periodic collection
Collect	
	Range of Recurrence
	Schedule Start Date/Time September 24,2021
	No end data
	Schedule End Date/Time
	UNITY
	Recurrence Pattern
	Minutely Every minutes.
	∪ Daily
	O Weekly
	O Monthly
	© Yearly

Figure 2-15 Collect Now



After logging in to the CSPC Collector, Dashboard screen is displayed



If the session is idle for 15 minutes or more, the user is logged out of the application.

Go back to CSPC Flow Chart

I

Forgot Password

If you forget password, click **Forgot Password?** link on the login screen. A dialog box as shown below is displayed.

If you select security question option. Answer the set of questions and enter a new password in the **New Password** text box. Enter the characters in the image.

Click OK button and the password is reset.

Reset By:	Security Questions One Time Passcode	
Security Questio	ns	_
* Question 1:	Car I wished I owned?	~
* Answer 1:		
* Question 2:	Favorite radio station (number on the dial - NN	~
* Answer 2:		
* Question 3:	Favorite game or sport to play?	~
* Answer 3:		
Please specify ne	w password	
* New Password	:	
Enter the charac	ters you see in the below image.	

 Figure 2-17
 Password Reset

If you select One Time Passcode option. Click **Generate OTP** and click **I have OTP** and enter the OTP that was sent to the registered mail ID set in Email Settings and enter a new password in the **New Password** text box. Enter the characters in the image.

Click OK button and the password is reset.

Reset Option	
Reset By:	Security Questions One Time Passcode
One Time Pass	code
Note: Mail se	ettings must be configured inorder to use this
feature	
OTP Status:	Generate OIP
Generate One	Time Passcode
Please specify	new password
ANT D	
* New Passwo	ra:
Enter the char	acters you see in the below image.
764	an a
1 1 1 1	
-	
* These character	s are case sensitive.

Figure 2-18 OTP Generation



	the second se
Reset By:	Security Questions One Time Passcode
One Time Passo	ode
Note: Mail set	ttings must be configured inorder to use this
feature	
OTP Status:	O Generate OTP
Entor OTP	
Litter OII.	
Please specify n	ew password
* New Passwor	d:
Enter the chara	cters you see in the below image.
ZEAH	
1 1 1 1	

I

Server And Package Versions

You can view the version of CSPC base collector, add-ons and other optional packages installed on CSPC on View Server Versions screen.

Once you are logged into CSPC, click Help menu > About > View Versions.

A screen showing the version information as shown in Figure 2-20 is displayed.

Figure 2-20 View Server Version

View Server Versions	w Server Versions		
Title	Version	Description	
CSPC Base Collector	2.10	Common Services Platform Collect	
Rules Package	4.14	Collection Rule Package for NO5, 5	
Agent	1.0	Addon Process: Intermediary betw	
Audit	1.5	Addon Process: Audit	
Update	1.9.3	Addon Process: Update	
NOS Full	NO5	Locked Collection Profile	
NOS Minimum	NOS	Locked Collection Profile	
DSIRT1.4	1.4	Installed Patch: DSIRT Package. DS	
LCM_GUI_Addon	1.9.4	Installed Patch: This LCM Add-on	
PoP_4.14	4.14	Installed Patch: Collection Profile P	
RP4.14	4.14	Installed Patch: Collection Rules Pa	
Audit_addon_1.7_CSPC2.9	1.7	Installed Patch: This patch will inst If you like to install this patch pleas	
NO5_RP4.14	4.14	Installed Patch: NOS Collection Pro	



For NOS Audit Addon details will be displayed on the above screen.



CSPC Dashboard

Dashboard

The dashboard is the primary screen of the CSP Collector. This screen is completely customizable for each user. After the layout is specified, it can be saved, and the next time you log in, you can see the customized layout.

Use the Dashboard to access menu options, Device Explorer Tree, Server Activity Log Messages, and the graphs. The dashboard consists of a menu bar (*User, Settings, Management, Reports, Administration,* and *Help*), Quick menu bar helps to get easy access to important features, and the two tabs (Dashboard and Applications). A search option is provided for easy navigation to CSPC Application. CSPC Notification communicator on the right corner detects various types of events such as, Job Completion that includes discovery, collection, DAV, upload, and so on. Customer name with certificate name is shown. Once the event is detected CSPC sends an event completion notification to UI and one or more email recipients as configured. Each event can have its own set of recipients. History of events is not maintained. Also, you can view the Server Activity Log Messages. **Disable Secure Browsing for CSPC** disable the Encryption of Communication between browser and server only if require as this might make the application vulnerable to security issues.

The node explorer on the left side of the screen displays all the managed devices by CSPC. Right clicking on any device opens a popup menu displaying selected device properties. Server Activity Log Messages window displays the status messages on both discovery and data collection.

ſ



CSPC Dashboard (NOS/ CSPT) Figure 3-1





Appliance configuration tab helps you in modifying and configure OS related configurations that was done during installation wizard also see Figure 2-6.

Γ

ppliance OS related configurations		
Use the below options to configure y	our Appliance.	
DNS Server/Hostname:	Enter DNS server name (i)	
Timezone:	Select timezone 🔻 🚺	
Set Time (24 Hour Format):	HH V mm V	
NTP Server:	Enter NIP server IP	
Hostname:	Enter hostname 1	
Proxy Server		
* Denotes Mandatory Fields		
		OK Cancel

To Change the password click **Change Password/setting** form drop down on top right of dashboard. Change all the required fields and click **OK**.

Account Settings			
11 11 10 1			
User Identification			
* Login Id:	admin		
* Auth Type:	Local User 💌		
Password:	••••••••		
Full Name:	Super Administrator		
Group Membersh	ip-		
* Group Name:	Administrator		
rassword Keset Qu	lesuons		
Question 1:	Favorite radio station (number on the 💌		
Answer 1:			
Question 2:	Favorite game or sport to play?		
Answer 2:	••••••		
Question 3:	Car I wished I owned?		
Answer 3:	•••••••••••••••••••••••••••••••••••••••		
Contact Informatio	n		
Email Address:			
Phone Number:			
Pager:			

Figure 3-4 Change Password

Managed Devices

The *Managed Devices* displays the list of the managed network devices, for which data collection is being performed by CSPC. Click on the arrow key next to the device name to expand the list. In the Managed Device Tree at a given time, only up to 50 devices are shown under each network device in the list. Click next button icon in the pagination bar to see more devices.
Γ

Managed Devices (60 out of 60)	L
20	
🕑 🥰 LiveNodes (58)	-
🖗 🥰 Unreachable Nodes (2)	
🥰 Hubs	
Servers-UnifiedComputing (3)	211
ServiceExchange (1)	
🦓 xDSL	
GenericNetworkDevices (3)	
Routers (12)	
🖓 Switches	
ATMSwitches	
💏 BladeSwitches	
ConnectedGridSwitches	
Alto Alto Alto Alto Alto Alto Alto Alto	
Real IndustrialEthernetSwitches	
Non Managed Devices (0 out of 60)	(+

Figure 3-5 Managed Device Tree

Figure 3-6 Managed Devices Menu Managed Devices (60 out of 60) -20 LiveNodes (58) . IN Page 1 of 2 > > Solution Page 1 - 50 of 58 🔮 Device View Device Properties... Device View Latest Device Collection Details... Device Cevice Managed Devices... Device Device Display Properties... 🔮 Device Device Access Verification Summary... Device Device Access Verification Results... 🔮 Device Disabled Protocol Report... C Device Device Timeout Configuration... 😂 Device 🔮 Device Unmanage Devices... Pevice 😵 Device Access Verification... Device Device Prompt Collection... Device Export Cevice Pevice_5_0_1_18

If you right click on any device, a menu as shown in Figure 3-6 is displayed.

Menu option shows the following options:

- View Device Properties
- View Latest Collection Details
- View Managed Devices
- Device Access Verification Summary
- Device Access Verification Summary
- View Access Verification Results
- Disabled Protocol Report
- Device Timeout Configuration
- Unmanage Devices
- Verify Device Access
- Device Prompt Collection
- Export

3-6

View Device Properties

To view the Device Properties, double-click any device or right click and select View Device Properties option. Device Properties screen as shown in Figure 3-7 is displayed.

igure 3-7	Device Properties
evice Properties - 17	/2.18.140.131 (nsite-ts-k01)
Device Properties	
lp Address	172.18.140.131
Host Name	nsite-ts-k01
Display Name	nsite-ts-k01
Display Type	Host Name
Device Type	Physical
B Hardware Propert	es
Device Family	Routers
Product Model	cisco2610XM
Vendor Name	Cisco Systems Inc.
Serial Number	2196525941
E Last Updated	
Discovery	1354533009000
SNMP Properties	
Sys Object Id	.1.3.6.1.4.1.9.1.466
Sys Description	Cisco Internetwork Operating System Software IOS (tm) C2600.
∃ Software Properti	25
OS Name	IOS
OS Version	12.3(6e)

View Latest Collection Details

I

To view the Latest Collection details right click any collection and select Latest Collection Details option. Latest Collection Details screen as shown in Figure 3-8 is displayed. You have select Dataset name from the drop down to view the details such as Command, Dataset Type, Command Status, Collection Profile, Last Collected, and Error Message. UI Commands have both UI and XML tabs and CLI commands have only CLI tab at the bottom of the page. You can also use search to open the dataset details.

iew Latest Collection Details(172.26.158.	118) 🗵			
20	Q.+	×		
🖌 🦓 LiveNodes (1)	Dataset Details			
∢ ∢ Page(1 of 1 ▶ ▶ 🖓 + Disp	Select Dataset	12. ciscoImageString		*
🔮 rtp9-spwifi-n7k	Command	ciscolmageString		
🚓 Unreachable Nodes	Dataset Type	SNMP	Command Stat	
📸 Video	Collection Drofile		Lest Oellested	
📸 StorageNetworking	Collection Profile	NOS_Detault_CP	Last Collected	Fri Oct 31 01:03:30 PD1 2014
📸 Conferencing	Error Message			
Real UnifiedCommunications				
CollaborationEndpoints	Instance Id		ciscolmageString	
Contract SuccessfulDevGrp	.3		CW_KICKSTART_IMAG	E\$n7000-s2-kickstart.6.1.1.bin\$
er OpticalNetworking	.2		CW_IMAGE\$n7000-s2-	dk9.6.1.1.bin\$
Real CloudandSystemsManagement	.1		CW_BEGIN\$\$	
Control Wireless	.9		CW_END\$\$	
🦓 Hubs	.8		CW_HOTSWITCHABILIT	YStrueS
Real DataCenterSwitches (1)	.7		CW_MEDIA\$RAM\$	
and ustrialEthernetSwitches	.6		CW_INTERIM_VERSION	\$6.1(1)\$
Revers-UnifiedComputing		f1 🕨 🕅		Displaying 1 -
💏 InfiniBandSwitches				
CanulasEvahanan	UI XML			

Figure 3-8 Latest Collection Details

Export

To download the Managed Devices DAV Results file, right click on the folder or the device as shown in Figure 3-6 and select Export option. ManagedDevicesCredentials.csv file is downloaded to your system. You can view this file in Microsoft Excel or any similar application.

Non Managed Devices

The Non *Managed Devices* displays the list of the non managed network devices, for which data collection is being performed by CSPC. Click on the arrow key next to the device name to expand the list.

igure 3-9	Non Manage	d Devices
Managed Devices (69	out of 69)	+
Non Managed Device	es (0 out of 69)	-
1 0		
🏘 SNMP Incompl	lete	
🥀 ICMP Pingable		
📸 Non Cisco		



CSPC Workflow

This is a powerful feature that helps you to discovery, add credentials, and collect device in one go. There are two types to add devices such as, Discovery by IP Address or Discovery by Protocol. You canaccess credential using SNMP V1/V2, V3, Telnet, or SSH and collect now or schedule it later.

To start the workflow, follow the steps below:

Click Workflow from menu bar. Step 1

I

-			
4	Wor	kf	IOU

- Step 2 You can add device using one of following and click Next:
 - Enter IP Address and use > to select the IP Address. You can also give range of IP Address.

es	Discover by IP Addresses Discover By Protocol			
Add Devices	Define discovery settings for CSPC by addi	ng a individual IP or range of IP Addresse	s. Any or all methods of add	ling devices can be used.
Access Credentials	IP Address Range/Subnet		Selected IP Address	Range (0)
Conect	From: To:		Start IP	End IP
				Delete
	IP Address	7	Selected IP Address	(0)
				Delete

Figure 4-2 Discovery By IP Address

Select the required **Protocol(s)**, **HOP Count**, and **Seed IP Address**. Use > to select seed IP Address.

	Discover by IP Addresses Discover By Protocol
Add Devices Access Credentials Collect	Add devices by providing seed devices and protocols to discover other connected devices. Select Protocol Cisco Discovery Protocol(CDP) OSPF Neighbours Border Gateway Protocol(BGP) Link Layer Discovery Protocol(LDP) Hop Count Imput Seed Devices Imput Seed Devices

- Step 3 You can add credential using one of following and click Add Credential:
 - If you select **SNMPV1/V2** enter **Credential Name**, **Read**, and **Write Community String**. Use > to select credential.

Figure 4-4	SNMPV1/V2	
Common Se	rvice Platform Collector 2.10	
Phases	SNMP Telnet/SSH	
Add Devices	Provide SNMP V1/V2 or SNMP V3 credentials for verifying the devices	
Access Credentials		Selected Credentials
📩 Collect	SNMP VI/V2 U SNMP V3	V Protocol Credential Name
	*Credential Name: One	
	Community Strings	
	Read:	
	Confirm Read:	
	Write:	
	Confirm Write:	
		Delete
	Cancel < Previous	Next

• If you select SNMPV3 enter Credential Name, User Name, Engine ID, Auth Algorithm, Password, Privacy Algorithm, Password. Use > to select credential.

I

Figure 4-5	SNMPV3					
cisco Common Se	rvice Platform Collector 2.10					
Phases	SNMP Telnet/55H					
👍 Add Devices	Provide SNMP V1/V2 or SNMP V3	credentials for verifying the devices				
Access Credentials				Selected Credentials		
📩 Collect	⊖ SINME V1/V2 @ SINME VS			Protocol	Credential Name	
	* Credential Name:	One	\supset			
	* User Name:		\supset			
	Engine Id:					
	Auth Algorithm:		* >			
	Auth Password:					
	Confirm Auth Password:					
	Privacy Algorithm:		*			
	Privacy Password:		\supset			
	Confirm Privacy Password:					
						Delete
		Cancel	< Previous	Next		

- If you select **Telnet** enter **Credential Name**, **User Name**, **Password**, **Enable User Name**, **Enable Password**, and **Pass Phase**.Use > to select credential
- If you select SSH enter Credential Name, User Name, Password, Enable User Name, Enable Password, and Pass Phase.Use > to select credential

Figure 4-6 Telnet and SSH

cisco Common Se	rvice Platform Collector 2.10				
Phases	SNMP Telnet/SSH				
Add Devices	Provide Telnet or 55H authentication for verifying the devices				
Access Credentials			Selected Credentials		
Collect	• Teinet U SSH		Protocol	Credential Name	
	Credential Name:				
	Authentication				
	User Name:				
	Password:				
	Confirm Password:				
	Enable User Name:				
	Enable Password:				
	Confirm Enable Password:				
	Pass Phrase:				
					Delete
	Cancel	< Previous	Next		

Step 4 Select Start Collection now and click Collect Now to start collection instantly or click Schedule Periodic Collection and click Schedule to collect at a later time. You can schedule Start and End Date/Time or select the Recurrence pattern as Minutely, Daily, Weekly, Monthly, or Yearly as shown in Figure 4-8.

	Select option to collect immediately or schedule collection for later. Scheduling periodic collection is recommended
Add Devices	Note: All newly added devices and existing managed devices will be considered for collection
Collect	Start collection now Schedule periodic collection
	Range of Recurrence Schedule Start Date/Time (September 24,2001 (05 :1000): Repeat whethele
	Schedule End Date/Time = End by September 20111 (2) 05 5 221
	Recurrence Pattern
	Minately Every minutes. Daily
	Weekly Secondary
	O Yeardy

Figure 4-7 Collect Now

Figure 4-8 Schedule Collection

cisco Common Se	ervice Platform Collector 2.10
Prases Add Devices Access Credentials Image: Collect	Select option to collect immediately or schedule collection for later. Scheduling periodic collection is recommended. Note: All newly added devices and existing managed devices will be considered for collection Start collection now Schedule periodic collection Fange of Recurrence Schedule Start Date/Time September 24.2021 OS:49: Repeat schedule Schedule End Date/Time September 24.2021 OS:52: Keurrence Pattern Schedule periodic collection Start option of the schedule periodic collection of the schedule schedule to the schedule schedule to the schedule schedule to the schedule to the schedule of the schedule schedule to the schedule of the schedule schedule schedule to the schedule to the schedule schedule to the schedule schedule to the schedule schedule schedule schedule to the schedule schedule schedule schedule to the schedule schedu
	Cancel < Previous Schedule



Quick Access Applications - Device Management

Common Application

You can use the Common Application tab to access tools with which you can specify, collect, and store software and hardware information about the network devices.

Figure 5-1 Device Managemen	ut –
Quick Access Applications	
4 💋 Common Applications	
Add/Import Credentials	
Discover Devices	
View Discovered Devices	
Verify Device Access	
View Access Verification Results	
Collect Data	
View Collected Data	
Upload Data	
Device Management	+
Management Tasks	+
Reports	+
Administration	+

This section describes the Common Application tools in the following topics:

- Add/Import Credentials
- Discover Devices
- View Managed Devices
- Verify Device Access
- Collect Data
- View Collected Data
- Upload Data

Use the links for navigation ..

Common Application

I



Applications - Device Management

Device Management

You can use the Device Management tab to access tools with which you can specify, collect, and store software and hardware information about the network devices.

Figure 6-1	Device Management	
Quick Acc	ess Applications	(
Device Ma	nagement	Ξ
🖻 💋 Cred	ential Management	
🖻 💋 Devi	ce Grouping	
🖻 💋 Gene	ral Settings	
🖻 💋 Colle	ection Rules	
🖻 💋 Miso	ellaneous Rules	
Manageme	ent Tasks	+
Reports		+
Administra	ation	+

This section describes the Device Management tools in the following topics:

- Credential Management
- Device Grouping
- General Settings
- Collection Rules

Miscellaneous Rules

I

Credential Management

Use the Credential Management sub tab of the Device Management tab to set up device or module credentials and manage seed file.

This section describes the Credential Management options in the following topics:

- Add/Import Credentials
- Manage Sub Module Credentials
- Manage Seed File
- Imported Seed file
- Do Not Manage Device List

Add/Import Credentials

In order to discover network devices and collect the data from the devices, you need to enter the credentials first. Device credentials set up in the CSPC is used for two purposes. The SNMP credentials are used only for initial discovery of the devices.

The remaining credentials like Telnet, SSH, HTTP, HTTPS, WMI, TL1, IIOP and SNMP are used for data collection from the discovered devices.

Use the Device Credentials Configuration wizard to add the credentials. Follow the wizard to choose your parameters for the credentials.

Figure 6-2 Device Credentials Configuration

	0		10	,		
I	Device Credentials (Configuration				×
	Device Credentials Enter credentials that between server and n NOTE: Credentials wo	will be used for device etwork devices uld be saved to CSPC	e discovery and inven server as and when y	tory and other communications you take the action.		
	Credential Name	Transport	User Name	lp Address List		
	such	https		11.1.1.2		
	TestLock	teinet	admin1	172.21.52.12	_	
	SNMP_public	snmpv2c		172.18.189.*,14.3.20.*,14.3	-	
	SNMP_AS	snmpv2c		10.89.234.*		
	snmp.70	snmpv2c	demo	172.20.70.10		
	SNMP_DD_CSO	snmpv2c		192.168.99.*,192.168.96.*,1		Et
	SNMP_cnc-ro	snmpv2c		*.*.*.*		ēŧ
	SNMP_columbia-ro	snmpv2c		172.21.56.*		
	SNMP_mwtm50	snmpv2c		172.18.156.*		
	snmp.70_1	snmpv2c	demo	172.20.70.10		
	SNMPv1_public	snmp∨1		172.21.55.17,172.21.55.15,		
	SNMP_public_1	snmpv2c		172.18.189.*,14.3.20.*,14.3		
	CNIMD AC 1	enmnu?e		10.80.03/ *	Ŧ	
	🚺 🖣 Page 1	of 3 🕨 🔰		Displaying 1 - 50 of	109	
	Add	Delete Delete /	All 😽 Modify	Clone Import Export.		
				Help	Clos	e

You can add, modify, delete, or clone an existing credential. To remove all the credentials from CSPC server, click **Delete All** button.

You can import credentials from applications like:

- Cisco Works DCR XML File (.xml)
- Pari Networks Credential Repository (.xml)
- Cisco Works DCR CSV File (.csv)
- CNC CSV File (.csv)
- Simplified CSV File (.csv)

Importing a Seed File

I

Seed file can be imported as a job. Any error or information messages for each device entry from the seed file being imported are captured as part of job log details. You can view the job log to check these messages.

When importing a seed file, save the original seed file by providing it a name. This helps users to get these files from database when required.

Create a new device group or select an existing device group to get the discovered devices added to them, as part of import seed file discovery process. Discovery and DAV are optional and are only applicable for DCR CSV and CNC CSV formats. DAV can be triggered only when Discovery option is checked. You can map the devices to default entitlement or to the entitlements in the drop down, using Map Devices option. Trigger DAV is enabled only for NOS and CSPT services. Create a group device during Discovery.

nport Options	
nport:	CNC CSV File (.csv)
ile/Directory:	Browne
Joh Name:	Dionaction
b Description	
Description:	
eed File Description:	
	Ingger Discovery Ingger DAV
	Default Mapping Map Devices to
	NOS C5P0001028436
Group Devices During D	iscovery
Create Groups By L	Jserfields
Add devices to use	r defined groups
New Device Gro	up Name
New Device Gro Select Existing Device Compared to the select Existing Device Compared t	evice Group
New Device Groo Select Existing D	up Name vice Group v
New Device Groo Select Existing D Job Scheduling Options	up Name vice Group v
New Device Groo Select Existing D Job Scheduling Options	up Name
New Device Groups Select Existing D Job Scheduling Options Start discovery now	up Name
New Device Groo Select Existing D Job Scheduling Options Start discovery now Schedule discovery	up Name
New Device Gro Select Existing D Job Scheduling Options Start discovery now Schedule discovery No schedule confi	up Name
New Device Groo Select Existing D Job Scheduling Options Start discovery now Schedule discovery No schedule confi	up Name evice Group
New Device Groo Select Existing D Job Scheduling Options Start discovery now Schedule discovery No schedule confi	up Name evice Group
New Device Groo Select Existing D Job Scheduling Options Start discovery now Schedule discovery No schedule confi	up Name
New Device Gro Select Existing D Job Scheduling Options Start discovery now Schedule discovery No schedule confi	up Name
New Device Groo Select Existing D Job Scheduling Options Start discovery now Schedule discovery No schedule confi	up Name evice Group
New Device Groo Select Existing D Select Existing D Start discovery now Schedule discovery No schedule confi Configure Schedule	up Name evice Group
New Device Groo Select Existing D Select Existing D Start discovery now Schedule discovery No schedule confi	up Name evice Group v gured
New Device Groo Select Existing D Job Scheduling Options Start discovery now Schedule discovery No schedule confi Configure Schedule	up Name evice Group

F	blow the steps given below to import a seed file:
In	the Device Credentials Configuration window, click Import button
F	om the Import drop down box, select any of the following files:
•	Cisco Works DCR XML File (.xml)
•	Pari Networks Credential Repository (.xml)
•	Cisco Works DCR CSV File (.csv)
•	CNC CSV File (.csv)
•	Simplified CSV File (.csv)
С	lick Browse button and select the seed file that you want to import
E	nter the job name, job description and seed file description in the respective fields
S	tep 5 and 6 are applicable only if you select CNC or CSV file format.
C fr	hoose Default Mapping or Map Devices To . If Map Devices To is selected, then select the entitlem om drop down
C ar	hoose Create Groups By User Fields or/and Add device Add devices to user defined groups. Selend enter New Device Group Name or Select Existing Device Group from the drop down.
Jo	b Name is a mandatory field.

Export

Export option is provided to export the existing credentials.

Figure 6-4	Export Options		
Export Options			×
Export Form	nat Pari Device	e Credentials Repository (.xm	I) ~
		ОК	Cancel

Follow the steps given below to export the contents:

- Step 1 In the Device Credentials Configuration window, click Export button
- Step 2 You are prompted to verify the password.

- Step 3 Enter the password that you used to login to CSPC
- Step 4 From the Export Format drop down box, select any of the following formats:
 - Pari Networks Credential Repository (.xml)
 - CNC CSV File (.csv)
- Step 5 Press OK button
- **Step 6** Save the file on your system

Note

- All devices in seed file imported by you are considered as managed devices even if the devices are unreachable at the time of CSPC discovery.
 - You can export seed file with Unreachable devices and the status of unreachable devices is shown as *Valid_Unreachable:Status* in this seed file *ManageDevicesCredentials.cvs*

Trigger Discovery And DAV Jobs

While importing the seed file you can also trigger the Discovery and DAV jobs. To do so, follow the steps given below:

- Step 1 Enter the details for importing seed file as given above
- Step 2 From the Import drop down box, select any of the following two options:
 - Cisco Works DCR CSV File (.csv)
 - CNC CSV File (.csv)
- Step 3 Check Trigger Discovery and/or Trigger DAV check boxes
- Step 4 You can start Discovery now or to Schedule Discovery at a later time, select Schedule Discovery option and then click Configure Schedule button.
- Step 5 You can schedule Start and End Date/Time or select the Recurrence pattern as Minutely, Daily, Weekly, Monthly, or Yearly as shown in Figure 6-5.

	Figure 6-5	Configure Schedule
Configure	e Schedule	×
Rang	ge of Recurrence	
Sch	nedule Start Date	Time April 21,2021 I T: 35 C Repeat schedule
Sch	edule End Date/	No end date End by April 21,2021 17:38
Recu	rrence Pattern	
	Minutely Every	
	Weekly	
01	Monthly	
	Voorly	
	rearry	
		OK Cancel
Step 6	Enter the devi	e group name in Device Group Name field
Step 7	Or click Selec box	Device Group Name radio button and select the device group name from the drop down
Step 8	Click OK but	on la constante de la constante

Go back to CSPC Flow Chart

Adding Credentials

To add credentials, click Add from the Device Credentials screen.

ŀ

rice Credentials			
Credential Identification		Include Ip Address Ranges/List (For Disco Collection) IP Address	very and Data
- Transport			
Protocol	telnet		
Port	23		
User Name Password		Exclude Ip Address Ranges/List (For Data	Collection only)
Password	<u></u>)	Exclude Ip List	2
Enable User Name			
Ellable Fassword	(!:		

Follow the steps given below to add the credentials:

- **Step 1** Enter the following information for creating a new Credential:
 - Name of the credential (user selected name to identify the credential)



The best practice is to set the credential name to "SNMP_Profile_1" or a generic name that you prefer.

- Transport protocol (CSPC supports various protocols for data collection that includes Telnet, SSHv1,SSHv2, HTTP, HTTPS, SNMPv1, SNMPv2c, SNMPv3, WMI, TL1, LDAP, LDAPS, SQL and IIOP)
- Specify the port number for SSH, Telnet, SQL, LDAP, LDAPs. Default port number for SSH is 22, Telnet is 23, LDAP is 389, LDAPS is 636, and SQL is 1433. This port number is considered during DAV, collection, apply IPS request, and connecting via jump server
- Authentication (depending on the protocol selected use the following authentication mechanisms:
 - Provide User Name, Password, Enable User Name and Enable Password for Telnet, SSH, HTTP, HTTPS, and TLI protocols
 - Provide User Name and Certificate (With/Without Pass Phrase) for SSH protocol certificate based authentication
 - Provide User Name, Password for WMI, LDAP, LDAPs, IIOP protocol
 - Provide User Name, Password for SQL protocol along with the Database details.
 - For SNMP V1 and V2, provide the READ and WRITE community strings
 - For SNMP V3 provide information on User Name, Engine ID, Authentication Algorithm to use and Authentication Password along with Privacy Algorithm and Privacy Password

• Include IP Address Range and Exclude IP Address Range.

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.

Step 2 Click OK.

You can also edit an existing credential by clicking **Modify**. Click **Delete** to delete a selected credential. Click **Clone** to create a copy of the selected credential for modification.

Go back to CSPC Flow Chart

Manage Sub Module Credentials

In order to collect the data from the modules you need to enter the credentials first. Module credentials are used to collect data from modules or sub modules that require additional authentication.

Use the Module Credentials wizard to add credentials. Follow the wizard to choose your parameters for credentials.

Modul	e Credentials Con	figuration		×
Modu Enter	ile module credentials t	hat will be used for modu	iles and other sub modules that require authentication	ı.
Cre	dential Name	User Name	IP Address List	
mod	11		10.1.1.1	
<			11	
			Add Delete 😽 Modify	
			Help OK Cance	1

Figure 6-7 Module Credentials Main Window

You can add, modify, or delete an existing credential. Vertical scroll bars are provided to move to either the previous or the next credential set in the table.

To add credentials, click Add from the Module Credentials screen as shown in Figure 6-8.

Credential Identification Include Ip Address Ranges/List (For Discovery a Collection) * Name cue Ip Address List *.*.*.*	and Data
Ip Address List ****	
	1
Module/Sub Mode Matching Expression	
* Expression targeted-service-engine 0/0 ses	
Authentication Exclude lp Address Ranges/List (For Data Colle	ection only)
User Name admin Exclude lp List	2
Password ••••	
Enable User Name	
Enable Password	

Follow the steps given below to add the module credentials:

Enter the following information for creating a new Credential: Step 1

- Name of the credential (user selected name to identify the credential)
- Module/Sub Mode Matching expression (expression used to match whether to use this credential on ٠ the module or not)
 - Authentication (depending on the protocol selected use the following authentication mechanisms: ٠
 - Provide User Name, Password, Enable User Name and Enable Password to access the module
- Include IP Address Range and Exclude IP Address Range.

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.

Step 2 Click OK.

You can also edit an existing credential by clicking Modify. Click Delete to delete a credential.

Go back to CSPC Flow Chart

Manage Seed File

You can import the seed file with the latest credentials and devices by placing the seed file manually in the default path. It determines what devices will be removed, updated, or added then perform the necessary actions. Devices not present in the seed file that is in CSPC will be deleted.

Note

In case of Multiple entitlement collector, to map devices to specific entitlement use file name format as <entitlement>.csv example: CSP0001027528.csv

8		
eed File Configuration		
Note : Supports import of seed file in V3	format only.	
Seed File Path		
Seed File Path:/data/SeedFileMgmt		
Note: In case of multiple entitlement of file name format as <entitlement>.csv</entitlement>	Collector, to map devices to specific entitlement, use for example:CSP0001027528.csv	
/ Job Scheduling Options		
Start seed file import now		
 Schedule seed file import 		
No schedule configured		
Configure Schedule		
Configure Schedule		
Configure Schedule		
Configure Schedule Perform Operations Delete device credentials not in seed file:		
Configure Schedule Perform Operations Delete device credentials not in seed file: Use existing credentials if not in seed file:		
Configure Schedule Perform Operations Delete device credentials not in seed file: Use existing credentials if not in seed file: Unmanage devices not in seed file:		
Configure Schedule Perform Operations Delete device credentials not in seed file: Use existing credentials if not in seed file: Unmanage devices not in seed file: Trigger Discovery:		
Configure Schedule Perform Operations Delete device credentials not in seed file: Use existing credentials if not in seed file: Unmanage devices not in seed file: Trigger Discovery: Trigger DaV:		
Configure Schedule Perform Operations Delete device credentials not in seed file: Use existing credentials if not in seed file: Unmanage devices not in seed file: Trigger Discovery: Trigger DAV:		
Configure Schedule Perform Operations Delete device credentials not in seed file: Use existing credentials if not in seed file: Unmanage devices not in seed file: Trigger Discovery: Trigger DAV:		

To import the seed file, perform these steps:

- **Step 1** Place the CNC V3 format seed file in the default location as shown on the screen. It is mandatory to place the seed file in the location as shown on the screen and read permission should be allowed to the file for CSPC users.
- Step 2 You can start Seed File Import now or to Schedule Seed File Import at a later time, select Schedule Seed File Import option and then click Configure Schedule button.
- Step 3 You can schedule Start and End Date/Time or select the Recurrence pattern as Minutely, Daily, Weekly, Monthly, or Yearly as shown in Figure 6-10.

Figure	6-10	Configure Schedule
onfigure Schedule		2
Range of Recur	rence	
Schedule St	art Date/Tir	Me April 21,2021 17:35 C Repeat schedule
Schedule En	d Date/Tim	e End by April 21,2021 I 17:38 \$
Recurrence Patt	ern	
Minutely	Every	
O Daily		
🔘 Weekly		
O Monthly		
🔘 Yearly		
		OK Cancel

Step 4 Check the required operation. click OK

Operations

Figure 6-11

Options	Description
Delete device credentials not in seed file	This removes only the device credentials which are not in seed file
Use existing credentials if not in seed file	If credentials are not present in the seed file, then CSPC uses the existing ones.
Unmanage devices not in seed file	This Unmanages the devices not in the seed file
Trigger Discovery	This Triggers Device Discover. By default, Trigger Discovery is selected.
Trigger DAV	This Triggers Device Access Verification

Imported Seed file

I

When you import a seed file, the information is captured in the imported seed file screen. Each row on the screen corresponds to one Import.

Seed file name field acts as a hyperlink as shown in Figure 6-12, on clicking this link you can download (or export) original seed file saved in the system. Screen captures all the details related to that import, like the file format, user info, file size and so on, along with the job log details of that import run.

You can also delete single or multiple rows from the screen.

Q Q	× → C	Delete Seed File	6					
Seed File Name	Seed File Description	Seed File Format	Group Name	File Size(KB)	User Name	Job Start Time	Job End Time	Job Log Details
<u>cnc.csv</u>		CISCO_CNC_C	NewGrp	7.93	cspcuser	Thu, Mar 14, 2	Thu, Mar 14, 2	View Job Log Details
rmeseedTest1.csv	CW Import	CISCO_WORK		0.94	cspcuser	Thu, Mar 14, 2	Thu, Mar 14, 2	View Job Log Details
CNC 20.csv		CISCO_CNC_C		0.04	cspcuser	Thu, Mar 14, 2	Thu, Mar 14, 2	View Job Log Details
40k sheer v1.csv		CISCO_CNC_C		2592.56	cspcuser	Thu, Mar 14, 2	Thu, Mar 14, 2	View Job Log Details
ManagedDevicesDAVR	CNC Import	CISCO_CNC_C	TestGrp	2.2	cspcuser	Thu, Mar 14, 2	Thu, Mar 14, 2	View Job Log Details

Figure 6-12 Imported Seed file

F

6-

Do Not Manage Device List

ſ

This provides you with an option to select a set of devices that should not be managed by the collector. If a device is added to Do Not Manage Device List then that device will not be discovered and will not be added to CSPC.

Figure 6-13 Do Not Manage Devices List

×	
► ≥i	Displaying 1 - 2 o

Click Add to add the device IP address.

As specified in the above screen, these three devices with IP Addresses 10.*.*.*, 1.1.1.1, and 10.1.2.43 are not inventoried even though they are all discovered devices.

Device Grouping

Use the Device Groups sub tab of the Device Management tab to create and manage device groups.

Device Groups

Device Groups option is used for Adding, Modifying or Deleting device groups. There are certain default system generated groups in CSPC. In addition, if you want to create device groups, then you can use these settings. Device groups can be Static or Dynamic. In static device groups you have to manually select the devices that are part of a given group. In dynamic group you will define a criterion and all devices that match the criterion (either currently managed or not) will automatically appear in this group.

Figure 6-14 Device Groups Main Window

Device Group	s 🗵				
0 Q	× €	🕽 Add Device Group 💣	Modify Device Group 😋 Removi	e Device Group 🔿 🔘	
Group Name	Category	Туре	Membership	Member Count	Description
Device Group2	Device Group	User Defined	Dynamic	0	Device Group2
Group Device	Device Group	User Defined	Dynamic	0	Group Device
TestGrp	Device Group	User Defined	Static	0	Static Device Group

When you select Add Device Group you choose whether to create a static group or dynamic group.

Figure 6-15 Add Device Group

Add Device Group	×
Create a static device group. The member devices of the devices that belong to this group.	f ths group are defined manually by selecting
Oreate static device group.	
Create a dynamic device group. The member devices evaluating a set of heuristics defined by the user.	s of ths group are defined automatically by
\bigcirc Create dynamic device group.	
	Help OK Cancel

Creation of static group is defined below.

Γ

Group Details * Group Name: Description: Select Group Members Select Devices Managed Devices:					
* Group Name: Description: Select Group Members Select Devices Managed Devices:					
Select Group Members Select Devices Managed Devices:					
Select Group Members Select Devices Managed Devices:					
Select Group Members Select Devices Managed Devices:					
Select Devices Managed Devices:					
Managed Devices:					
		5	elected Devices	/Groups:	
12 0			Q.+	×	
EtveNodes (64)	^		Device		
Unreachable Nodes (3815)					
💏 Hubs					
Servers-UnifiedComputing (3)					
ServiceExchange (1)					
* xDSL					
GenericNetworkDevices		->>			
Routers (13)					(
Switches					
ATMSwitches (1)					
ReadeSwitches					
ConnectedGridSwitches					
DataCenterSwitches (2)					
and IndustrialEthernetSwitches					
InfiniBandSwitches (1)					
LANSwitches (8)	~				
<			14 4 Page 1	of 1 👂 🕅 No data	to display
Upload Nodes From File(.txt):			Bros	wse.	
· · ·			(
		_			
	-				

Enter the group name and description, and select group members by moving the devices/groups to the selected list. Once the devices/groups are selected or click browse to upload .txt file containing the devices/groups, click **OK** to create the static device group.

Similarly, when you select the *Dynamic Group* option while creating new device groups you can define the heuristics used to identify which devices belong to that specific group. This is shown in Figure 6-17.

Group Details Grou	ip Rules	
Group Details		
* Group Name:	Dynamic	
Description:		^

Once you define the group name and description you are ready to define the Group Rules, as shown below.

oup Details Group R	ules					
Select Rule Match Type	e					
ule Match Type:	All of the Rules must be n	All of the Rules must be matched				
Define Group Rules			-			
Attribute	Operator	Value				
Device Host Name	equals	console				
			et			
			<u>=</u> +			
			n - n			
		an an anna an Anna an An An				
	+	Add × Delete 2 Modify Test R	tules			

Define the conditions or rules that must be matched or not matched based on the attributes and values. Add these conditions by clicking **Add**.

Γ

Figure 6-19 Gro	oup Rule Details
-----------------	------------------

Group Rule Details		×			
Group Rule Details					
* Attribute Name:	Device Host Name	•			
* Operator:	equals	v			
* Value:	console				
L					
ок	Test Regular Expression	Cancel			

Select any of the Attributes like Device Host Name, Device IP Address, Device OS Name, Device OS Version, Device Vendor Name, Device Product Module, Device Family, Device OS Type, Device Technology, UserField1, UserField1, or UserField1 and use one of the Operator like equals, contains in the list and so on, and provide a Value. You can create any number of rules.

Newly discovered devices are matched for these conditions automatically and are added to the dynamic groups.

Special Cases	Figures			
If you select Device OS Name as Attribute				
Name, then you need to select the value form the	Group Rule Details	×		
drop down	Group Rule Details			
	* Attribute Name:	Device OS Name		
	* Operator:	equals		
	* Value:	ACNS		
		ACNS		
		ACSW E		
		AlticaOS		
		ASA		
		CatOS		
		CBOS		
		CDS-IS		
		CDS-IV CMTC Firminare		
		Cisco IOS-700		
		Cisco ME1100		
		CSM		
		CTS		
If you select Device Ip Address as Attribute				
Name and Operator as does not belong to the	Group Rule Details	×		
range, then you need to enter Start Ip Address	Group Rule Details			
and End Ip Address	* Attribute Name:	Device In Address		
	* Operator:	deer not belong to the range		
	* Start To Address			
	* Cad Ta Address.			
	End Ip Address:			
	L			
		OK Test Regular Expression Cancel		

Table 6-1Special Cases in Group Rule

Special Cases	Figures
For any of the Attribute Name if you select does not exist in the list as Operator , then you need to add the Value manually using the edit icon on the screen.	Group Rule Details
If you select Inventory Status or Config Status as Attribute Name and Operator as contains or does not contain . Select the required status on the screen and Select the Available Services from the drop down. Only for Inventory Status NOS lists all the dataset name and you can select for the list. Inventory status provides you granular information. It is recommended to create the rule based on inventory status if you want to create a group based on dataset specific.	Group Rule Details * Attribute Name: Operator: Contains * Not Applicable Successful Integrity Check Failed Failed Skipped * Available Services: NOS * Available Services: NOS * Available Services: NOS * Available Services: NOS * Collection Type Collection Type Collection Type Collection Type Clisco-UNIFIED-COMPUT Clisco-UNIFIED-COMPUT State CHASSISMGREXT-MIB CHASSISMGREXT-MIB CHASSISMGREXT-MIB Clisco-UNIFIED-COMPUT Clisco-UNIFIED-COMPUT Clisco-UNIFIED-COMPUT Clisco-UNIFIED-COMPUT Clisco-UNIFIED-COMPUT Clisco-UNIFIED-COMPUT Clisco-UNIFIED-COMPUT Skibude

General Settings

Use the General Settings sub tab of the Device Management tab to set Application, Discovery, Inventory, and Advance Job.

This section describes the General Settings options in the following topics:

- Application Settings
- Discovery Settings
- Access Verification Settings
- Inventory Settings
- Advanced Job Settings

I

Application Settings

Application settings is used to set device inventory data collection preferences like Device prompt, Submode and Data export settings.

General Settings:

IP Host Mask Settings: If device IP Address and Hostname data privacy is enabled, customer device IP address and Hostname that is sent back to Cisco will be replaced by a set of user defined IP address and Hostname.

In *IP Address Mask* field, you can define the IP address range that is used to replace the real IP address of the customer, and define a prefix in *Hostname Mask* field that is used to replace the real customer hostname.

Figure 6-20 General Settings

Prompt & SNMP Trap Settings	Submode & Init Settings Export Settings Device Settings
ings	
0.0.0	1
::1	
MASK	ŝ
ngs	
Ност	NAME
er Config	
WLC	
.1.3.6	.1.4.1.9.1.1615,.1.3.6.1.4.1.9.1.753,.1.3.6.1.4.1.9.1.913
ngs	
Count: -1	
4	
	Prompt & SNMP Trap Settings ings 0.0.0. ::1 MASK ngs HOST er Config WLC .1.3.6 ngs Count: -1

Table 6-2General Settings

Field Name	Description
Start IP	IP to be used as start value while masking IPv4 data. IP will be incremented from this value for each of the IP's to be masked
Start IPv6	IP to be used as start value while masking IPv6 data. IP will be incremented from this value for each of the IP's to be masked
Start Hostname	Prefix used for masking hostnames
Global Display Type	Device attribute to be shown for distinct devices
Platform List	List of platforms for Telnet echo is enabled.
SysObject ID List	SystemObject ID for the Telnet echo enabled devices
Total User Session Count	Maximum number of unique CSPC user sessions

Prompt Settings:

ication Settings	
eneral Settings Prompt & SNM	P Trap Settings Submode & Init Settings Export Settings Device Settings
Prompts	
Login Prompts:	username, username:, user, user:, login, login:, enter user id:
Password Prompts:	password,password:,password :,pwd,passwd,passwd:
Other Prompts:	#,>,%,error
CLI Error Prompts:	invalid input detected at,% this command is not authorized, error: %, type
SNMP Error Prompts:	error
SOAP Error Prompts:	soap-env:fault
SNMP Trap Settings	
Retain Traps for:	14 Days
Port Number:	162

	Table 6-3	Prompt Settings	
Field Name		Description	
Prompts			
Login Prompts		Used for extra Login prompts that needs to be handled by CSPC	
Password Prompts		Used for extra Password prompts that needs to be handled by CSPC	
Other Prompts		Used for other prompts that needs to be handled by CSPC	
CLI Error Prompts		Used for extra CLI error prompts that needs to be handled by CSPC	
SNMP Error Prompts	\$	Used for extra SNMP error prompts that needs to be handled by CSPC	
SOAP Error Prompts		Used for extra SOPA error prompts that needs to be handled by CSPC	
SNMP Trap Settings			
Retain Traps for		Mention the number of days to retain traps.	
Port Number		Configure the port to receive the SNMP trap messages. Default port is 162.	
		Note If you configure a new in-bound port to listen the SNMP Trap messages, then you need to manually update the corresponding IP table rules and NAT router settings.	

Γ

Submode and Init Settings:

Figure 6-22 Submode And	Init Settings	
Application Settings		×
General Settings Prompt & SNMP Trap Set	ttings Submode & Init Settings Export Settings Device Settings	
Submode And Init Prompt Validation	15	_
OS Types:	nx-os,fwsm-os,pixos,fwsm,acsw,nxos,asa,	
IP Address List:		
SH Version Command:	show version	
SH Version Lines:	5,12	
SH Version Ignore Strings:	hours,seconds,minutes,uptime,	
Execute New Line For Submode		
Login Prompt:		
		_
	Help OK Ca	ncel

Table 6-4Submode and Init Settings

Field Name	Description
OS Type	Type of OS
IP Address List	List of IP addresses
SH Version Command	If show version needs to be executed while in submode
SH Version Lines	Number of lines in show version that need to be taken
SH Version Ignore Strings	Whether to consider or ignore show version settings
Execute New Line for Submode Login Prompt	Whether new line has to be executed at the end of submode login prompt

Export Settings:

10			T 15 ml		
eneral Settings Prompt & SNMP Irap	Settings	Submode & Init Settings	Export Settings	Device Settings	
Export And Upload Settings					_
Collection Profile Export Boundary:	1000				
Job Log Export Boundary:	2003				
Tailend Response Counter (secs):	90				
Tailend SendFile Counter (secs):	7200				
Upload Via:	Conne	ctivity			~
Connectivity Certificate:	CSP0001028437			~	
	Т	est upload to HEG using CSP	0001028437		
CSPC Identity Settings					
CSPC Identity:	CSP00	01027629			~
					_

Table 6-5Export Settings

Field Name	Description	
Collection Profile Export Boundary	Number of devices processed in batch during VSEM export.	
	Default values are as follows:	
	• Large - 100 devices	
	Medium - 50 devices	
	• Small or ultra-small - 25 devices	
Job Log Export boundary	Job log export boundary	
TailEnd Response Counter	Response counter for TailEnd is maximum wait time for entitlement registration and limit is 90 seconds	
TailEnd SeedFile Counter	Seed file counter for TailEnd is maximum wait time for connectivity file upload.	
Connectivity Certificate	Certificate used for connection	
Upload Via	Set the Upload via option to either of these:	
	• Transport Gateway (Only for NOS services)	
	• Connectivity upload supports AES 256 encryption with strong RSA key length of 2048bits.	
	• Disabled	

Field Name	Description
CSPC Identity	Select the valid CSPC certificate
Test Upload button	Check the connectivity using a certificate



I

- If Connectivity certificate changes, the new certificate is applied to connectivity. This takes 5-7 minutes to restart connectivity and apply the new certificate.
- Connectivity certificate gets modified based on the preference of the applied certificates. For Example, NOS uses connectivity for upload. All other services use Websocket. Since Web socket has higher preference, though you add NOS as connectivity certificate, it changes to the one that has higher preference like PSS, SNTC or SC.

Device Settings:

This enables or disables the key on the device during SSH communication. If it is disabled, then same key is being used repeatedly or else it generates new key.

Figure 6-24	Device Settings
-------------	-----------------

Application Setting	IS				x
General Settings	Prompt & SNMP Trap Settings	Submode & Init Settings	Export Settings	Device Settings	
Host Key					_
Device Host K	ey Validation: enab	le			~
			Help	ок	Cancel

Discovery Settings

In Discovery Settings you can set preferences of device discovery. You can set values for Discovery timeout, Include platform, and Exclude platform.

In Preference tab, enter the values as shown in Table 6-6.

Figure 6-25 Discovery Settings

Settings		
SNMP Timeout (in sec):	3	
SNMP Retry:	1	
Max Thread Count:	100	
Max Credential Sets For Protocol:	10	
Max Discovery Time (in sec):	600	
Max Device Discovery:	180	
P Phone Discovery:	No	
Serial Number Duplicate Check:	No	
Aac Address Duplicate Check:	No	
Exclude Non-Cisco Device:	No	
NMAP Timeout (in sec):	30	
Ping ICMP before Discovery:	No	
inable Fallback:	Yes	
Enable SNMP Config Push:	Yes	
CLI Timeout (in sec):	3	
HTTP Timeout (in sec):	4	

Table 6-6

Discovery Timeout

Field Name	Description	
SNMP Timeout (in sec)	SNMP connection timeout value in seconds. Default value is 3 seconds	
SNMP Retry	SNMP connection retry count. Default value is 1	
Max Thread Count	Thread pool size for each discovery job. Default value is 100.	
Max Credential Sets For Protocol	Maximum number of Credential Sets to use for each protocol. Default value is 10.	
Max Discovery Time (in sec)	Maximum discovery time in seconds per device. Default value is 600 seconds. Valid values 0 or \geq 60. Zero no window time will be enforced. If value is set between 0 and 60, default value 600 will be used.	
Max Device Discovery	Maximum discovery time in seconds for a single device. Default value is 180 seconds. Valid values: 5 seconds and above. If value is < 5, then 5 is enforced.	

Field Name	Description	
IP Phone Discovery	Option to enable/disable IP Phone discovery.	
Serial Number Duplicate Check	Checks for the duplicate's serial numbers. If not enabled, then serial number will not be polled for the device.	
Mac Address Duplicate Check	Checks for the duplicate MAC Address.	
Exclude Non-Cisco Device	If enabled excludes all the non-cisco devices from discovery	
Ping ICMP before Discovery	Option is to enable/disable. If enabled pings the device before Discovery.	
Enable Fallback	If discovery of selected protocols fails, and if fall back is selected discovery is tried for other protocols as per discovery properties file. \$CSPCHOME/resources/discovery/properties/disc overy-cso-startup.properties	
	For properties name: PRIMARY_COMM_PROTOCOL	
	This is applicable only for known discovery and rediscovery.	
Enable SNMP Config Push	If enable fallback option is selected and discovery happens using CLI protocols (telnet, SSHv1, and SSHv2), then SNMP Config push for RO string is applied.	
CLI Timeout	CLI connection timeout value in seconds. Default value is 3 seconds.	
HTTP Timeout	HTTP connection timeout value in seconds. Default value is 4 seconds	

Include Platform (optional):

Γ

As to any platform that is specified in *include platform* list, only those specific platform devices will be discovered, and all other devices will be discarded.

Preferences Include Platform	Exclude Platfo	orm	
Include Platform			
IO5_10000 IO5_12000 IO5_4000 IO5_7200 IO5_7300 IO5_7500	*	* * *	IOS_XR IOS_VSS IOS_Cat IOS_as5300
IOS_8500 IOS_as5300 IOS_Cat IOS_cat3700 IOS_LS1010 IOS_VSS IOS_XE	E		
IOS_XR IPS MIB_II NME_NAM NXOS	+		

Figure 6-26 Include Platform
Exclude Platform (optional):

Any platform is specified in exclude platform list, all devices belonging to that platform will be ignored.

Preferences	Include Platform	Exclude Platfo	orm		
Exclude Pla	atform				
ACNS		*	-	ADEOS	٦
ACSW			+	ACNS	
ADEOS		Ξ	+	ACSW	
AltigaOS			-		
ASA_CSCu	b30913				
CatOS					
CatO5_500	D				
CatO5_63g	e				
CCM					
CCM4x					
CCM5x					
CTS					
DISABLE_I	OS_XR_OID1				
DISABLE_I	OS_XR_OID2				
DISABLE_S	HOW_INVENTORY				
DISABLE_S	SH1				
DISABLE_S	SH10				
DISABLE_S	SH2	+			

Access Verification Settings

I

This setting is used to select and order protocols to use them in device access verification. This is global settings that is used in DAV.

Select the protocols order to be used for access verification using side arrows and reorder them using the up and down arrows. To avoid failure, you can use the option **Use All Selected Protocol Versions** and to override the failed protocol select the option **Override Enable Failed**. If Use all selected protocol version is selected, then all the selected protocol are used even if the first protocol passes. If Override enable failed is selected, then status is shown as enabled by default even if device do not enter enable mode. If **Run DAV for Unreachable** is selected, then DAV job is trigged for all the unmanaged devices.

cess verification	Settings		×
lease select and or	rder protocols below to use then	device access verification	^
Include SNMP	Protocols snmpv3 snmpv2c snmpv1	Include CLI Protocols sshv2 shv1 telnet	
Include HTTP	Protocols https http (*)	Include Other Protocols	
Use All Select	ted Protocol Versions ble Failed		~

Figure 6-28 Access Verification Setting

Inventory Settings

Inventory Settings allows you to set some advanced collection settings.

These include setting up inventory threads, device connectivity options, time out options, device prompts, disable protocol rules and disable collection rules.

Advanced Settings:

The Advanced Settings tab of Inventory Settings screen provides the following options:

- Inventory Threads: To set up the maximum number of inventory threads you would like the collector to use. By default, the value for Microsoft Windows is 40 and for Linux it varies from 40 100 based on the hardware configuration. Maximum value that can be set is for both Microsoft Windows and Linux is 200.
- Connection Settings: To set up the maximum number of connections a device can have, or the maximum number of connections per the whole collector. These settings apply only for Telnet or SSH credentials. In some networks, authentication servers provide a limit on the number of connections of either an application or a device, so this needs to be set. By default, there is only one connection per device, and no connection limit for the whole collector.

Advanced Settings	Global Timeouts	Device Prompts	Disable Protocol Rules	Disable Collection Rules
Maximum Number	of Threads			
* Inventory Thread	ls:	40		
Connection Setting	gs mum number of 1	Felnet/SSH connec	tions to be opened from	n the server to the
to the entire network	ome networks ma ork or to each of	ay restrict the maxi the network devic	mum number of simulta es.	neous connections
Maximum Connection	ons (System):			
Maximum Connection	ons (Device):			

Figure 6-29 Inventory Settings



I

Inventory Thread count vary based on system configurations. It is 100 for large OVA

Go back to CSPC Flow Chart

Global Timeouts:

The *Global Timeouts* tab allows you to select the time out options for a given IP address or a range of IP addresses. This is where you can specify a time out option for any given protocol like Telnet, SSH, SNMP or HTTP and so on.

Vertical scroll bars are provided to move to either the previous or the next timeout option on the window. Use up and down arrow to prioritize the custom timeouts set by user.

I Timeouts Protocols ptocol npv1 npv2c npv3 net	Device Prompts Timeout(ms) 5000 5000 5000 5000	Establish Timeout(s	Retry Count	llection Rul
Protocols ptocol npv1 npv2c npv3 net	Timeout(ms) \$ 5000 5000 5000	 Establish Timeout(s 	Retry Count 2 2	
otocol npv1 npv2c npv3 net	Timeout(ms) 5000 5000 5000	Establish Timeout(s	Retry Count 2 2	
npv1 npv2c npv3 net	5000 5000 5000		2 2	-
npv2e npv3 net	5000 5000		2	
npv3 net	5000			
net			2	
	10000	10		
w1	10000	10		(mark)
w2	10000	10		
	10000	10		
		C 8 554 4	elete 🧷 Modife	
		10000	10000 10 * Add * D	10000 10 Add × Delete & Modify

You can enter these timeouts by clicking **Add** button. On Timeout Details screen, you can enter the following details:

- Hostname / IP Address: You can select the IP Address Expression like 10.*.*.* (to represent all IP Addresses that start with a 10)
- Protocol: Select the protocol (Telnet, SSHv1 or SSHv2, HTTP, HTTPS, TL1, SNMPv1, SNMPv2 or SNMPv3 or WMI, IIOP)
- Timeout (ms): Type timeout in milliseconds (ranging from 1000 milliseconds (1 second) to 600000 milliseconds (10 minutes))
- Establish Timeout (sec): Time taken to establish a connection for a device. By default, it is 10seconds.
- Retry Count: You can select the "retry" count as well

Figure	6-31 Global Time	eout			
Timeou	t Details				×
Pr	otocol Timeout Details —				
*1	Hostname / Ip Address:	*.*.*.*			
*1	Protocol:	snmpv1		~	
*	Timeout(ms):	5000			
Es	tablish Timeout(sec):	10			
Re	try Count:				
			ок	Cancel	

Use the *Modify* button to modify the global time out value. Use the *Delete* button to delete a time out value.

Go back to CSPC Flow Chart

I

Device Prompts:

The *Device Prompts* tab allows you to select specific prompt options for any given device or device group. Device prompts are used when the data collection is done on a device or device group where the prompts are changed (through an authentication server for security reasons). When the device prompts change, the collector must be able to process those prompts in order to perform data collection successfully.

There are two ways of setting up these options; the first one is based on matching prompts by order and the second one on matching a specific string/regular expression.

Figure 6-32 Device Prompts

dvanced Settings	Global Time	eouts Device	Prompts	Disable Protocol Rules	Disable Collection	n Rules
Define Device Pro	ompts					
Ip Address Expres	sion	Match Type		Prompts		
						[≣‡]
						=4
				🕈 Add 🦻	Celete 🖉 Modify	

Both Order and Regular Expression are explained below.

Device D	mont Dataile					
Device Fi	iompe Decaus					
* Ip Addr	ess Expression:	*.*.*				
* Prompt	Match Type:	Match Pr	rompts By Order	~		
Define De	evice Prompts in	n the orde	r they appear			
Device P	rompt					
	Prompt				×	
	Device Pro	ompt:	User Name		~	
	2		User Name			E#
			Enable User Name Password			E+

In the first method the device or a device group is expecting the collector to send the credential information in a particular order. For example, if the device expects to see the Password and Enable User Name and Enable Password in that order, you can change those as shown in Figure 6-33.

Similarly, if the prompts are to be matched by prompting a string, you can select that as shown in Figure 6-34.

ompt Details			
ss Expression:	*.*.*.*		
latch Type:	Match Pro	ompts By String 🗸 🗸	
vice Prompts in	the order	they appear	
pression		Device Prompt	
Prompt		×	
Prompt Ex	pression:		
Device Pro	mpt:	User Name	Et
-		User Name	-1
		Password	
2		Enable Password).
		Enable Password	
		🕈 Add 🗙 Delete 🖉 Mod	lify
	rice Prompts in pression Prompt Prompt Ex Device Pro	recently period of the order of	Add X Delete & Mac

In this example for the device with IP Address 1.1.1.1 the User Name must have an expression of *user*: as the device prompt.

Use the *Modify* button to modify any prompts value. Use the *Delete* button to delete any prompts.

I

Go back to CSPC Flow Chart

Disable Protocol Rules:

The *Disable Protocol Rules* tab allows you to configure the protocols that need to be disabled for a specific platform. Inventory and Device Access Verification will not run for the disabled protocol for the specified platform. This helps in enabling/disabling protocols without modifying the datasets. All DSIRT protocols rules are locked.

Figure 6-35	Device Protocol Rules
	Derice I rorocor Itares

Advanced Settings	Global Timeouts	Device Prompts	Disable Protocol Rules	Disable Co	llection Rules
Disable Protocols fo	or Data Collection				
Platform		Protocol		Lock Status	1
DSIRT_ASA_DISA	BLE_SSHV2	sshv2		Unlocked	
DSIRT_CATOS_CA	AT6K_SSHV2	sshv2		Unlocked	
DSIRT_ASA_SNM	P	snmpv1, snmpv3	, snmpv2c	Unlocked	
DSIRT_PIX_SSH		sshv1, sshv2		Unlocked	
DSIRT_7206VXR_9	SH	sshv1, sshv2		Unlocked	(=-)
			de Add X Delet	a 🥒 Madifr	
			- Aut - Delet	e 🖉 wouny	

You can add, modify, or delete an existing disable protocol rule. Vertical scroll bars are provided to move to either the previous or the next rule in the table. To add disable protocol rule, click **Add** in the Disable Protocol Rules screen.

Constitution for	disabling a Destagal	
Specify criteria for	uisabiling a Protocol	
* Select Platform:	ACNS	*
* Select Protocol:	V telnet	_
	Sshv1	
	sshv2	
	Snmpv1	E
	snmpv2c	
	snmpv3	
	🔽 http	
	Mttps	-
	Select All Unselec	t All

Figure 6-36Disable Protocol Rule Details

Follow the steps given below to create a new disable protocol rule:

- Step 1 Enter the following information:
 - Select Platform: Select a platform for which protocol needs to be disabled from the combo list. All the configured platforms, both system and custom defined are displayed here
 - Select Protocols: Select the protocol that has to be disabled for the above selected platform. All the supported protocols (Telnet, SSHv1,SSHv2, HTTP, HTTPS, SNMPv1, SNMPv2c, SNMPv3, WMI, TL1, LDAP, LDAPS, SQL and IIOP) will be displayed here
- Step 2 You can also select or unselect all the protocols using Select All/Unselect All buttons
- Step 3 Click OK to add the configured rule to CSPC

I

Disable Collection Rules:

The *Disable Collection Rules* tab will allow you to disable specific commands/OIDs on a specific platform. Inventory will not run for the disabled command/OIDs.

If in a given dataset, there are multiple OIDs then inventory will run for dataset and results will be displayed for OIDs which are not disabled, but collection will not happen for disabled OID.

All DSIRT collection rules are locked.

nory settings						
dvanced Settings	Global Timeo	uts Device Prompts I	Disable Protocol Rule	Disable C	Collec	tion Rule
Disable Data Colle	ction					
Platform	Dataset Type	Operator	Value	Lock Status		
DSIRT_NXOS	CLI	matches regular expression	show env sho	Unlocked	•	
DSIRT_NXOS	CLI	matches regular expression	show run	Unlocked		
DSIRT_ASA_c	SNMP	matches regular expression	\.1\.3\.6\.1\.4	Unlocked		
DSIRT_NXOS	CLI	equals	show vpc consi	Unlocked		
DSIRT_NXOS	CLI	equals	show vlan	Unlocked	Ξ	-
DSIRT_CRS_S	CLI	equals	show diag pow	Unlocked		
DSIRT_CRS_S	CLI	matches regular expression	show diag	Unlocked		=+
DSIRT_7206VX	SNMP	matches regular expression	\.1\.3\.6\.1\.4	Unlocked		
DSIRT_CAT6K	CLI	equals	show memory	Unlocked		
DSIRT_CAT6K	SNMP	matches regular expression	\.1\.3\.6\.1\.4	Unlocked		
DSIRT_CAT6K	SNMP	matches regular expression	\.1\.3\.6\.1\.4	Unlocked		
DSIRT_CAT6K	SNMP	matches regular expression	\.1\.3\.6\.1\.4	Unlocked	_	
DOIDT CATCH	~					
			T Add A	Delete 🖉 Moi		

You can add, modify, or delete an existing disable collection rule. Vertical scroll bars are provided to move to either the previous or the next rule in the table.

To add disable collection rule, click Add on the Disable Collection Rules screen.

Vigure 6-38 Disable Collection Rule Details							
Disable Collec	tion Rule De	etails					×
Specify	criteria for d	lisabling a C	ollection				1
* Select	Platform:	ACNS				~	
* Datase	t Type:	CLI				~	
* Operat	tor:	equals				~	
* Value:		sh run					
Annotati	ion:						
				ОК	0	ancel	

Follow the steps given below to create a new disable collection rule:

Step 1 Enter the following information:

- **Select Platform**: Select a platform for which protocol needs to be disabled from the combo list. All the configured platforms, both system and custom defined will be displayed here
- Select Dataset Type: Supported Dataset types are CLI or SNMP
- **Operator**: Operator can be any of equals, does not equals, matches regular expression, does not match regular expression
- Value: The exact CLI command or OID to be disabled
- Annotation: You can add a note here
- Step 2 Click OK to add the configured rule to CSPC

Go back to CSPC Flow Chart

Advanced Job Settings

This setting provides with an option to configure various jobs. You can define preferences for triggering a job, as well as define what jobs can be skipped and what jobs needs to wait based on a trigger preference. You can add new job trigger preferences by selecting *Add* button in the Advanced Job Settings window.

ab Trigger Proferences	Contrion Drighter Cottings		
ob mgger merences	Service I nority Settings		
ob Type Name	Skip Job List	Wait Job List	
Jpload Jobs		Inventory Jobs, Device Access	
nventory Jobs		Upload Jobs	
Device Access Verification Job	DS	Upload Jobs	
mport Seed File Jobs		Discovery Jobs, Device Acces	
			-+
		💠 Add 🗙 Delete 🧷 Modify	

You can add jobs to Wait Job List and Skip Job List:

Wait Job List: Any job specified in Job Type Name will start only after the job specified in Wait Job list completes.

Skip Job List: Any job specified in Job Type Name will not start if any job specified in Skip Job is running.

Figure 6-40 Add a Job Trigger Preferences

Skip Job List			, h, h	
Inventory Jobs Backup/Restore Jobs Diag Jobs Device Access Verification Jobs Credential Loader Jobs Workflow Jobs	• •	$\mathbf{\hat{*}} \mathbf{+} \mathbf{\hat{*}}$	Inventory Jobs Backup/Restore Jobs Diag Jobs Device Access Verification Jobs Credential Loader Jobs	, m
	- 7			18
Inventory Jobs		-	1	
Backup/Restore Jobs	-	*		
Diag Jobs		+		
Device Access Verification Jobs Credential Loader Jobs		*		
Workflow Jobs	-			

To set the service priority list click **Service Priority Settings** and **use** arrows to add the services to the services priority list and set the priority using up and down arrows.

gure 0-41	Service Priority Set	ings	
vanced Job Settings			
ob Trigger Preferences	Service Priority Settings		
Service Priority			
OPTIMIZATION ASCNA	● ● ● ●		=== ===
		Help	OK Cancel

Figure 6-41 Service Priority Setting

ſ

Collection Rules

You can use the Collection Rules sub tab of the Device Management tab to set up data collection profiles, create new datasets, manage data integrity and masking rules.

This section describes the Collection Rules options in the following topics:

- Manage Data Collection Profiles
- Manage MulitService Collection Profiles
- Manage Upload Profiles
- Manage Datasets
- Manage Platform Definitions
- Manage Data Integrity Rules
- Manage Data Masking Rules
- Manage Syslog Source Files

Manage Data Collection Profiles

Collection profile defines what data to collect, from what devices that data needs to be collected and how often the data needs to be collected.

Figure 6-42 Collection Profile Main Window

e q	×	Add Collection Profile	Wodify Collection Profile	Remove Collection Profile	2 Import Collection Profile from a Zip file	📰 »
Name		Lock Status	Scheduled	Device Select	ion Dataset Count	
config		UnLocked	8	Selected	1	
test1		UnLocked	8	Selected	1	
dsirt		UnLocked	8	Selected	4	
rr		GUnLocked	8	Selected	1	
oom		UnLocked	8	1 device(s) S	elected 1	
context		GUnLocked	3	Selected	4	
Default_CP		GUnLocked	8	All Devices S	elected 260	
cml		UnLocked	0	Selected	2	
test			8	1 group(s) Se	lected 2	

Note

Based on service entitlement(s) CP are added.

If there are no collection profiles created, CSPC does not collect any data from any device.

New data collection profiles can be created by clicking *Add Collection Profile* from Manage Data Collection Profiles window.

You can also import collection profiles from a zip file stored locally on your system. To do so, click *Import Collection Profile from Zip File* button and select the zip file with collection profiles.

To add a new data collection profile, follow the steps given below:

- Step 1 Select the Devices
- Step 2 Select Datasets
- Step 3 Select Profile details
- Step 4 Click OK

I

 All managed devices Only the following selected devices 				
Managed Devices:		Selected D	evices/Groups:	
12 10				
🖓 Video	-			
KarageNetworking				
Carl Telepresence	H.			
🖏 OpticalNetworking		*		
🏘 CloudandSystemsManagement		→		
Wireless (1)		+		
Real VoiceandUnifiedCommunications				
💏 Hubs				
ataCenterSwitches				
Revers-UnifiedComputing				
Reference Switches				
ReviceExchange	+			
Upload Nodes From File(.txt):		Browse		

Figure 6-43 Select Devices for a Collection Profile

To start the collection, select a device or a set of devices or import the .txt file which has IP address of devices and each IP should be enter in the consecutive line, from which the data is to be collected as shown in the above figure. Once you select the devices, the second step in creating a profile is to select some datasets. A dataset in CSPC is an output of a command (CLI), a SNMP request, a SOAP/XML request, or a File. *Datasets* are explained in the *Manage Datasets* chapter.

Select Datasets				Folosted Deteorter		
Available Datasets:						
20	0.11 × . T			Dataset	Tune	
A III T Lawrence (0)	Collection 1	Da		Dataset	rype	
- i telepresence (8)		^				
A Page of 1 P P To Displaying						
DL_TP Codecs DYN_CI5CO-ENTITY-A	SNMP					
DL_TP Codecs DYN_CISCO-TELEPRES	SNMP					
DL_TP Codecs DYN_CI5CO_CDP_MIB_	SNMP		-			1
DL_TP Codecs DYN_ENTITY_MIB_entF	SNMP		•			+
DL_TP Codecs DYN_IF_MIB_if	SNMP		< *			
DL_TP Codecs DYN_RFC1213_MIB_if	SNMP					
DL_TP Codecs DYN_RFC1213_MIB_ipA	SNMP					
DL_TP Codecs DYN_SNMPV2_MIB	SNMP					
DO NOT SELECT - Dynamic Dataset Input (
Configuration (22)						
CLI-Security (14)						
CLI-Operational (24)						
b III ct t t /50)		~		<	>	
				M A Profession N	No data ta disata	1

Use arrows to add the datasets to the Selected datasets list and to move the selected datasets use up and down arrows, click **OK**. Once the required Datasets are selected, select the profile options that define how often you want to collect the data, as shown below.

ſ

collection Profile		
ect Devices Select Datasets		
Collection Profile Details		
* Profile Title:		
* Identifier:	Generate	
Description:		:
Tag:		
Profile Priority:	Medium	
Preserve Run Count:	1	
Service Name:		
Service Version:		
Rule Package Version:		
Aging Mode:	Default Aging	
Collection Interval(ms):		
Use Fallback Credentials:		
Run Discovery Before Collection:		
Include Non Managed devices for discovery:		
Run Prompt Discovery Before		
Collection: Run DAV Before Collection:		
Disable Mask Rule:		
Disable Collection From Device:		
Mask IP Address:		
Mask Domain Name:		
Export Seed File:		
	Advanced Options	
		_
Collection Profile Schedule		
Schedule Periodic Collection		
No schedule configured		
Configure Schedule		1
Resume this job automatically	if its interrupted due to a CSPC server restart	
		_
Export Options		
Export upon successful exect	ution of collection profile	:
* Export Format:	Cisco VSEM (.zip)	
* File Name Prefix:		
Upload To Remote Server:		

This provides an option to select the priority of the profile itself, and how many versions of this profile run data need to be preserved and finally how often the profile is executed to collect data. You need to provide a title that identifies this profile as well as an identifier (which is used by the XML APIs to uniquely identify this profile). If no identifier is provided, the system generates an automatic identifier for this profile.

Tag is an information that get appends to VSEM file, select the option from drop-down or enter the tag manually to tag the profile.

Each profile is set up with a specific priority. Higher priority profiles always take precedence when there is a contention for resources.

You can specify the *Service Name* and *Service Version* for the profile created. Service version is for the specific service program that collects and uploads the data. Service name is mandatory to creating collections profiles. Without service name collection profiles can be created, but it will get upload as it is necessary to be mapped to any of services that you have uploaded.

Specify the Rule package version.

Select the data Aging Mode from drop-down:

If you select *Default Aging*, then it takes time interval that is already available. This option is enabled by default and uses the aging interval specified in the dataset.

If you select *Disable Aging*, then data aging is disabled. This option disables data aging, and the collection happens directly from the device.

If you select *Custom Aging*, then you have to define the Collection Interval in milliseconds. This option refers to CP level data aging (milliseconds) and this will override the aging defined in the dataset, also enables *Disable Collection From Device* option to use.

Use *Disable Collection From Device* option to disable collection from devices. If enabled, it does not collect missing/aging expired dataset data directly from the devices. The data for those datasets will be shown as 'Skipped' in the CP summary report. If disabled, it collects missing/aging expired dataset data from the device.

The Use Fallback Credentials option is provided in case the credential that is being used for data collection fails (typically if you are using the Discovery Credentials for the data collection as well, it might not work on all the devices). CSPC picks up the next credential that passed Device Access Verification as a fall back credential to collect the data.

Use the *Run Discovery before Collection* option to rediscover the devices before running the inventory.

Use Include Non Managed devices for discovery option to discovery the non managed devices.

The *Run Prompt Discovery before Collection* option is used to collect the prompts before running the inventory.

Use the *Run DAV before Collection* option to verify the credentials before running the inventory.

Use Disable Mask Rule option not to mask the data collection as per the rules set.

Use the *Mask IP Address* option to mask the IP addresses collected from the customer before uploading them to Cisco.

Use the *Mask Domain Name* option to mask the domain names collected from the customer before uploading them to Cisco.

Mask IP Address and *Mask Domain Name* options are for data privacy and their usage depends on customer needs. You can specify the mask settings in *Advanced Settings* option under *Settings* menu.

Use the *Export Seed File* option, if you want to upload all the original seed files saved in the system along with the Collection profile. You can also export Unreachable devices. This option is disabled if masking/DPA is enabled.

Use *Export Options* if you would like to export the collection profile data after the successful execution of the collection profile. You can export the data to the following format:

• Cisco VSEM(.zip)

Check the Upload to Remote Server checkbox, if you would like to upload the collection profile details to the remote server. If the Upload to Remote Server box is left unchecked the collection profile data is not uploaded to remote server.

Once these steps are finished, click **OK** and the Data Collection Profile is created and ready for use.

I

When a Collection Profile is scheduled to run at later time, 'Resume this job automatically if it's interrupted due to a CSPC Server restart' option will be available. If the CSPC restarts for any reason while Collection Profile is running, CSPC will resume the job upon restart.

When you click Advanced Options in Profile Details window, following windows is displayed.



anced Collection Profil	e Options			
Advanced Settings	Inventory Change Rules			
Select Data Masking Apply masking Masking Rule	Rule Options rule defined in the dataset fi	irst	~	
Select Filtered Collec	tion Profile Options			
Collection Profile	file only if the following Col	llection Profile dat	a changes	
Select SNMP Protoco	ls			
LocalStorage snmpv1 snmpv2c snmpv3	***			
Select CLI Protocols				
LocalStorage telnet sshv1 sshv2	+**			
Select H111P Protocol	5			
LocalStorage http https	••			
	*			

Advanced Collection Profile Options window shows the available, SNMP, CLI and HTTP protocols. You can select the desired protocol from the list and add it by clicking arrow the double arrow .

You can move the protocol up or down by using the arrow keys next to the selected box. The protocol on top in the selected box takes precedence and is run first as compared to the ones below it.

If you select *LocalStorage*, then whenever you execute for a particular device or dataset it will first check if it exists in the local database, if it is not found then based on the protocol order selected it will go to the next one.

You can also set a filter to execute the profile only if a certain collection profile changes. To set the filter, select the check box next to *Execute this profile only if the following collection profile data changes*, click **Browse** button and select the collection profile.

To apply mask rule select *Apply masking rule defined in the dataset first* and select the Masking rule from drop-down.

Click Inventory Change Rules to add of modify the Rule. Select Dataset and enter Ignore Regular Expression and click OK

igure 6-47	Inventory Chang	ze Rule Details
dvanced Collection P	rofile Options	
Advanced Settings	Inventory Change Rules	
Inventory Chang	e Detection Rules	
Q	×	
Dataset 🔺		Ignore Expression
Inventory Chan	ge Rule Details	×
Ignore Reg	ular Expression:	OK Cancel
		Add Delete 😽 Modify
		OK Cancel

Click **OK** button to save the selection.

Go back to CSPC Flow Chart

Manage MulitService Collection Profiles

Manage Multi Service Collection Profiles is used to define, and configure the Multi Service Collection Profile. Collection profiles that are executed together and you can Add, Modify, or Delete a collection profile. It combines devices and datasets from all the selected collection profiles and collects data in one single inventory job. If any of collection profile has run Discovery, DAV, Prompt before collection, and if any other settings are enabled then those settings are considered for multi service collection profile.

Γ

Manage MultiService Co	ollection Profiles 🗵			
0 Q-	× O Add MultiServ	ice Collection Profile 🐮 Modify Multificentice Collection Profile	O Remote MultiService Collection Profile	→ 0
Name		Title	Lock Status	Scheduled
Name Test, 1_NOS Minimum_d	emo_NO5 Full	Title Test_L_NOS Minimum_demo_NOS Full	Edd Satus	Scheduled
H 4 Page(1 of 1	× H			Displaying 1 - 1 o

Figure 6-48 MulitService Collection Profiles

In collection profile dialog box, select the collection profile using arrows.

igure 0-4)	Aud Maniservice Concentral Tojine	
	Add MultiService Collection Profile	×
	Select Collection Profiles Profile Details	~
	Collection Protiles NOS Full NOS Minimum SNTC	
		~
	Help OK Cance	1

Figure 6-49 Add MultiService Collection Profile

In Profile details dialog box, enter the Profile name and generate the identifier. You can schedule the collections periodically or run the collections now. To run collection, refer Collect Data.

Figure 6-50	Profile Details	
	Add MultiService Collection Profile	×
	Select Collection Profiles Profile Details	
	Application Profile Details Profile Title: Identifier: Description: Collection Profile Schedule Schedule Periodic Collection No schedule configured Configure Schedule Resume this job automatically if its interrupted due to a CSPC server restart	
	Help OK Cancel	

Manage Upload Profiles

In Manage Upload Profiles, you can specify the type of data which includes syslogs, inventory, and DAV that needs to be uploaded locally or to the backend.



Default upload profiles are created for NOS service when a nos configurer gets installed. Below screen is only for NOS.

Γ

Manage Upload Profiles	×		
o Q	× OAdd Upload Profile	💣 Modify Upload Profile 🔵 Remove Upl	pad Profile 👩 Import Upload Profile from a Zip file 🔿 🍈
Name		Lock Status	Scheduled
NOS Full Upload			0
NOS Incremental Upload		G UnLocked	8
NOS Default Upload			0

Figure 6-51 Manage Upload Profile

You can import an upload profile from zip file stored on your system. To do so, click **Upload Profile from** a Zip file icon on Manage Upload Profiles screen. In Upload File dialog box, browse to the fileand click **Submit** button to start uploading the file.

I

pload Profile Details		
Profile Title	Cart	
Identifier	test	
Deservice	tl	Generate
Description	sample	Q
elect Collection Protile(5) a	nd Devices	
 All Collection Profiles 	For Service	Single Collection Profile
Limit upload to devices	mapped to registration certificate	
Default Upload	Upload Only Devices Mapped to	<u> </u>
Export Options		
Export To Remote S	erver	
O Export To Local Ser	ver File Name Prefix:	
Devices Selection for Up	oload	
Managed Reachable	and Unreachable devices	
O Managed Reachable	devices	
O Managed and all No	onManaged devices	
elect Module For Upload =		
elect Module For Upload Upload Inventory Select Devices Upload All Device I Upload Inventory Up From Last Success	Data dated Device Data	✓ Upload Syslogs Select Syslog Options □ Include Parsed Syslogs Only □ Collector Received Time ○ From Last Successful Upload ○ Time Interval minutes.
elect Module For Upload Upload Inventory Select Devices Upload All Device I Upload Inventory Upc From Last Success Time Interval	Data dated Device Data sful Upload minutes.	 ✓ Upload Syslogs Select Syslog Options □ Include Parsed Syslogs Only □ Collector Received Time ○ From Last Successful Upload ○ Time Interval ○ Date/Time Range
Upload Inventory Select Devices Upload All Device I Upload Inventory Uploa	Data dated Device Data sful Upload minutes.	✓ Upload Syslogs Select Syslog Options □ Include Parsed Syslogs Only □ Collector Received Time ○ From Last Successful Upload ○ Time Interval ○ Date/Time Range Start Date/Time January 07,2019 □ 14 : 37 :
elect Module For Upload Upload Inventory Select Devices Upload All Device I Upload Inventory Up From Last Success Time Interval	Data dated Device Data sful Upload minutes.	✓ Upload Syslogs Select Syslog Options □ Include Parsed Syslogs Only □ Collector Received Time ○ From Last Successful Upload ○ Time Interval minutes. ○ Date/Time Range Start Date/Time January 07,2019 □ 14 : 37 End Date/Time January 07,2019 □ 14 : 42 ○
elect Module For Upload Upload Inventory Select Devices Upload All Device I Upload Inventory Upload DAV Data Upload DAV Data	Data dated Device Data sful Upload minutes.	✓ Upload Syslogs Select Syslog Options □ Include Parsed Syslogs Only □ Collector Received Time ○ From Last Successful Upload ○ Time Interval minutes. ○ Date/Time January 07,2019 □ 14 : 37 End Date/Time January 07,2019 □ 14 : 42 ○
elect Module For Upload Upload Inventory Select Devices Upload All Device I Upload All Device I Upload Inventory Up From Last Success Time Interval Upload DAV Data Upload Profile Schedule	Data dated Device Data sful Upload minutes.	✓ Upload Syslogs Select Syslog Options □ Include Parsed Syslogs Only □ Collector Received Time ○ From Last Successful Upload ○ Time Interval minutes. ○ Date/Time Range Start Date/Time January 07,2019 □ 14 : 37 End Date/Time January 07,2019 □ 14 : 42 ○
elect Module For Upload Upload Inventory Select Devices Upload All Device I Upload Inventory Upload DAV Data Upload Profile Schedule Schedule Periodic Upl	Data dated Device Data sful Upload minutes.	✓ Upload Syslogs Select Syslog Options □ Include Parsed Syslogs Only □ Collector Received Time ○ From Last Successful Upload ○ Time Interval ○ Date/Time Range Start Date/Time January 07,2019 □ 14 : 37 End Date/Time January 07,2019 □ 14 : 42 ○
elect Module For Upload Upload Inventory Select Devices Upload All Device I Upload Inventory Upload DAV Data Upload Profile Schedule Schedule Periodic Upl No schedule config	Data dated Device Data sful Upload minutes.	✓ Upload Syslogs Select Syslog Options □ Include Parsed Syslogs Only □ Collector Received Time ○ From Last Successful Upload Time Interval minutes. ○ Date/Time Range Start Date/Time January 07,2019 □ 14 : 37 End Date/Time January 07,2019 □ 14 : 42 14 : 42 15 : 42 16 : 42 17 : 42 17 : 42 18 : 42 : 42 18 : 42 : 42 18 : 42 : 42 : 42 : 42 : 42
elect Module For Upload Upload Inventory Select Devices Upload All Device I Upload Inventory Upload DAV Data Upload Profile Schedule Schedule Periodic Upload Config	Data dated Device Data sful Upload minutes.	✓ Upload Syslogs Select Syslog Options □ Include Parsed Syslogs Only □ Collector Received Time ○ From Last Successful Upload ○ Time Interval
elect Module For Upload Upload Inventory Select Devices Upload All Device I Upload All Device I Upload Inventory Up From Last Success Time Interval Upload DAV Data Upload Profile Schedule Schedule Periodic Upl No schedule config Configure Schedule	Data dated Device Data sful Upload minutes.	✓ Upload Syslogs Select Syslog Options Include Parsed Syslogs Only From Last Successful Upload Time Interval minutes. Date/Time Range Start Date Time January 07,2019 Id : 37 : End Date/Time January 07,2019 Id : 42 :
elect Module For Upload Upload Inventory Select Devices Upload All Device I Upload All Device I Upload Inventory Upload From Last Success Time Interval Upload DAV Data Upload Profile Schedule Schedule Periodic Upl No schedule config Configure Schedule NOTE: Frequent repeat up	Data dated Device Data sful Upload minutes.	✓ Upload Syslogs Select Syslog Options □ Include Parsed Syslogs Only □ Collector Received Time ○ From Last Successful Upload □ minutes. ○ Date/Time Range Start Date/Time Start Date/Time January 07,2019 ③ End Date/Time January 07,2019 ③ 14 : 42 : start Date/Time January 07,2019 ④ 14 : 42 :

You can choose **All Collection Profiles For Service** or **Single Collection Profile** and select corresponding registration certificate from drop down.

You can upload devices to the default registration certificate using **Default Upload** or to a registration certificate from drop down using **Upload only devices mapped to**.

Select the required type of devices to upload such as

- Managed Reachable and Unreachable devices (Default)
- Managed Reachable devices
- Managed and all Non Managed devices (this option uploads all the devices in CSPC).

If **Upload Inventory** is selected, then you can **Upload All Device Data** (Full Inventory upload) or collected data with in specified time interval by specifying the **Time Interval** in minutes or choosing an option **From Last Successful Upload**. (Incremental Inventory upload).

If **Upload Syslogs** is selected, then you can upload Syslogs by choosing an option **From Last Successful Upload** or by providing **Date/Time Range** or specifying **Time Interval** in minutes.

Selecting **Include Parsed Syslogs Only** if this option not selected, then by default all the syslogs are considered and If **Collector Received Time** is selected, then the time selected is form collector else it is default system time

To upload DAV data, select the Upload DAV Data.

You can also schedule periodic uploads of the data using Configure Schedule option. This data can be exported to remote server or to a server locally.

igure 6-53	Upload Warning Message
nformation	
Lowering uploaded	the upload frequency (not recommended) may result in performance degradation and high bandwidth consumption.Data will be only if data is changed from the last successfull upload

Note Frequent repeated uploads will be suppressed if there is no change in data. If no change in the collected data from the previous successful upload, then upload data will be suppressed by bundling only limited requiredfiles.

Manage Datasets

I

Manage Datasets is used for creating a new data collection point. Datasets are the building blocks of CSPC Collection Profile. Datasets contain the platform definitions, data/masking rules. You can either Add, Modify or Delete a dataset.

A Data Set in CSPC is an output of a command (CLI), SNMP request (SNMP) or XML output (SOAP/XML).

e q	× G	Add Dataset 👹 Modify	Dataset 🔘 Remo	ve Dataset 🔞 Import Data	aset from a Zip file 🔛	0	
Dataset Name	Туре	Collection Type	Lock Status	Applicable Platforms	Category	Created By	
PhysicalPortID_ContainedIn	Dynamic	SNMP	G UnLocked		PhysicalPort	admin	
PhysicalPortID_Descr	Dynamic	SNMP	GUnLocked		PhysicalPort	system	
PhysicalPortID_HardwareRev	Dynamic	SNMP	G UnLocked		PhysicalPort	system	
PhysicalPortID_Index	Dynamic	SNMP	G UnLocked		PhysicalPort	admin	
PhysicalPortID_Name	Dynamic	SNMP	GUnLocked		PhysicalPort	admin	
PhysicalPortID_ParentRelPos	Dynamic	SNMP	C UnLocked		PhysicalPort	system	
show_context_asa	Static	CLI	GUnLocked	[Custom]	SubModule	system	
show_context_asa_run	Static	CLI		[Custom]	SubModule	system	
show_context_asa_run_dyn	Dynamic	CLI	GUnLocked		Subvdc	system	
show_context_asa_start	Static	CLI	GUnLocked	[Custom]	SubModule	system	
show_context_asa_start_dyn	Dynamic	CLI	UnLocked		Subvdc	system	
show_context_run	Static	CLI	GUnLocked	[Custom]	SubModule	system	
show context run Dynamic	Dynamic	CLI	GUnLocked		Subcontext	admin	
show_context_start	Static	CLI	GUnLocked	[Custom]	SubModule	system	
show context start Dynamic	Dynamic	CLI			Subcontext	admin	
show_vdc	Static	CLI	GUnLocked	[Custom]	SubModule	system	
show_vdc_run	Static	CLI	G UnLocked	[Custom]	SubModule	system	
show vdc run Dynamic	Dynamic	CLI	GUnLocked		Subvdc	admin	
show_vdc_start	Static	CLI		[Custom]	SubModule	system	

Figure 6-54 Manage Datasets

Select *Add* Dataset option when you are ready to create a new data set. You can create Static and Dynamic datasets.

You can also import datasets from a zip file. To do so, click "Import Dataset from a zip file" button on the Manage Datasets window and select to the zip file to import.

Static Dataset

Collection mechanism specified in the static dataset is defined as a command or SNMP request Follow the steps given below to add a new static data set:

- Step 1 Provide data set details
- Step 2 Provide data set platforms
- Step 3 Click OK

Select **Create static dataset** option and then click **OK** button to create a static dataset as shown in the figure below.

Figure 6-55	Add Datase
-------------	------------

Add Dataset	×
Create a static dataset. The collection mechanism speict command or SNMP request.	fied in the static dataset is defined as a
Create a static dataset	
Create a dynamic dataset. The dynamic datasets allow or another command or set of commands.	collection of data based on the output
C Create a dynamic dataset	
	Help OK Cancel

Add/Modify Dataset is used for creating/modifying a Dataset. Dataset can be added either as locked or unlocked.

The following are the steps to add a dataset.

Step 1 Provide the following dataset details:

Title: Name of the Dataset. This is a mandatory field

Identifier: This can be user defined. If this is not defined by user, this will be generated by System

Category: This is a mandatory field. This is custom defined by user. If you enter a category that does not exist, a new category is created

Collection Interval: You can specify the collection intervals in milliseconds

Tag: Select the tag from the drop down list

Description: Description for the Dataset

taset Details Dataset	Platforms	
Dataset Details		
* Title:	datasetdetails	
* Identifier:	_datasetdetails	Generate
* Category:	CISCO-MEMORY-POOL-MIB	
Tag:	Config	
Collection Interval(ms):	100000	
Description:		د.

Step 2 Once this information is provided, you can now select the applicable platforms for this dataset and the collection method using the following options:

Dataset Type:

- CLI
- SNMP
- SOAP XML Requests
- Config Retrieval using SNMP
- FILE
- XML
- WMI
- HTTP
- TL1
- IIOP
- SQL

Γ

• LDAP

CLI:

CLI is selected in this example. CLIs are the datasets which contains commands to execute on the device.

Add Dataset Dataset Details Dataset Platforms Select Data Collection Type Dataset Type: CLI × CLI Select Platform an SNMP SOAP XML Requests Platform Config Retrieval using SNMP FILE XML WMI нттр -1÷ 🕈 Add 🗙 Delete 🖉 Modify Help. ОК Cancel

Figure 6-57 Dataset Platform Options (select CLI)

Select a specific platform for which this dataset is applicable. The list of platforms is pretty extensive, and you can select a platform based on a matching operating system, matching device group or any other format. You can also create your own platform definitions as explained in the *Manage Platform Definitions* chapter.

Figure 6-58 Dataset Entry Details (CLI)

Select Platform:	ACNS	~
Command String:		
Add/Modify Sub Mode	Add/Modify SubMode Commands	
Maximum Lines:	(
ntegrity Rule:		~
Masking Rule:		~
Dataset Timeout(ms):	(

Once the platform is selected, enter a command string (as you are creating a dataset based on CLI) for NATed Appliances you need to use this format as explained in Optional Parameter for NATed Appliances, page C-1, and enter other details such as:

- Sub mode is list of commands to enter and exit sub mode context
- Sub mode command is used to include all the commands that are required to executed in the sub mode context
- Maximum Lines (some command outputs might run in to thousands of lines, using this option provides a way to curtail that information to the selected number of lines)
- Integrity Rule (helps to determine if the command output returned from the device is a proper output on successful execution of the command or the output returned is an error message. You can define your own integrity rules. Integrity Rules are discussed further in *Applications->Device Management-*>*Data Collection Settings* tab),
- Masking Rule (what specific fields in the command output needs to be masked)
- Dataset time out (how much time collector should wait for the data output).

SNMP:

Select SNMP option from Dataset Type and click Add button.

taset Details	Dataset Platforms				
Select Data C	ollection Type				
Dataset Type:	SNMP				
Select Platfor	rm and Collection Para	imeters			
Platform		Request Type	No. Of OIDs	Timeout	
ACNS		Column	1	1000	
			4	• Add × Delete 🧷	Modify.

The following screen shots show adding an SNMP data set. Once you select *SNMP* in the Dataset Platform Options, add the MIB variables as shown in Figure 6-60. All the MIBs that are preloaded are shown, and you can pick which MIB and which variables you would like to add to your dataset.

ir object betails				
Known SNMP C	Object Id			
Object Id:				
ïtle:				
ag:		~		
Request Type:	Scalar	~		
Browco SNMP	MIRs to select Object Id(s)			
DIOWSE SHIFF I	ADS to select Object Id(s)			
Select a MIB:		~		
ame	OID Number	Data Type	OID Type Access Ty	pe OID Name

Once the selection is finished, click OK.

SNMP variables are added to your new data set as shown below.

Figure 6-61 Dataset Entry Details - SNMP

Dataset Entry Details			×
* Select Platform: Dataset Timeout: Max Retries: Select SNMP Object	ACNS 10000 2 ts	v	
Object Id	Title	Туре	
1212	Cisco Test	Scalar	
1231	CFlashDev	Column	
990011	CiscoFlashD2	Column	
		🕂 Add 🗙 Dele	te 🖉 Modify
			OK Cancel

ſ

SOAP XML Request:

Select SOAP XML Request option from Dataset Type and click Add button.

Figure 6-62 Dataset Platforms (select SOAP XML Requests) Add Dataset Dataset Details Dataset Platforms Select Data Collection Type Dataset Type: SOAP XML Requests * Select Platform and Collection Parameters Platform URL ACNS soap/astsvc.dll 三十 Ē4 🕈 Add 🛪 Delete 🖉 Modify Help... OK Cancel

Enter the details for *SOAP XML* as defined below. Once all the data is entered you are ready to add a new SOAP *XML* dataset.

Figure 6-63	Dataset Entry Details - SOAP XMI

Dataset Entry Details			×
* Select Platform	CCM5x		
* URL •	/realtimesenvice/cenvices/RecPort	-	
* Desweet Desku			
* Request Body:	1		
SOAR Action:		-	
Datasat Timoout:		-	
VSLT File Name		_	
ASET File Marrie:			
	OK Car	ncel	
	UN UN		

Config Retrieval using SNMP:

Once you select Config Retrieval option, and click **Add** button you can start collecting the configuration (either running or startup) using SNMP. Once you select the type of data set you would like to create based on the protocol selected, click **Add** button to enter the details for the data set.

Figure 6-64 Dataset Platforms (select Config Retrieval using SNMP)

	Provide the second seco			
taset Type:	Config Retrieval us	ing SNMP		
elect Platform	and Collection Paran	ieters		
Platform		Command	Timeout	
ACNS		Running Configuration	1000	
				
			Tr Add in Delete 22	mouny

Enter the details for SNMP *ConfigRetrieval*. Once all the data is entered you are ready to add a new *ConfigRetrieval* using SNMP.

Figure 6-65Config Retrieval using SNMP Details

* Select Platform:	IOS	*
* Config Type:	Running Configuration	~
Integrity Rule:	CNC Global Interity Rule	~
Masking Rule:	CNC Configuration Masking Rule	~
Dataset Timeout:	10000	

Γ

FILE:

When you select FILE option, and click **Add** button, you can start collecting the data based on either a *predefined file* or *user defined file*.

Figure 6-66	Dataset Platforms (Select FILE)	
Add Dataset			1
Dataset Details D	ataset Platforms		
Select Data Coll	ection Type		
Select Platform	and Collection Parameters		. Lost
Platform		File	
ACNS		VLAN	
			(iii) (iii)
			🕈 Add 🗙 Delete 🦧 Modify
			Help OK Cancel

Select the Platform and enter the details for File name, File location and Download Command. If required enter Generate Command and dataset timeout. Also, you can select Integrity Rule and MaskingRule. Once all the data is entered you are ready to add a new FILE dataset.

gure 6-67	Dataset Entry Details - FILE	
aset Entry Details		
* Select Platform:	Cisco Device	~
* File Name:	test.ucs	\supset
* File Location:	/var/local/ucs/	\supset
Generate Command:	tmsh save sys ucs <#SOURCEFILEPATH#>	
* Download	scp <#SOURCEFILEPATH#>	\prec
Command:	<#USERNAME#>@<#SERVERIP#>: <#DESTINATIONFILEPATH#>	
Integrity Rule:		•
		V
Masking Rule:		

XML:

Once you select XML Dataset option and click **Add** button, you can start collecting data in XML format for supported platforms. Once you select the type of data set you would like to create based on the protocol selected, click **Add** button to enter the details for the data set.

Figure 6-68Dataset Platforms (Select XML)

Dataset			
ataset Details	Dataset Platforms		
Select Data	Collection Type		
Dataset Typ	e: XML		~
Select Platf	orm and Collection Parameters		
Platform		XML	
Cisco IOS Devices Running >= 12.2		XML Test	
			Ēt
			(Ξ 4)
		÷	Add X Delete 2 Modify

Enter the details for XML selection. Once all the data is entered you are ready to add a new XML dataset.

Figure 6-69 Data Entry Details - XML

Select Platform:	Cisco Device				~
XML Request:	wml</td <td>version="1.0"</td> <td>encoding="UTF-8"</td> <td>standalone='</td> <td>'ye</td>	version="1.0"	encoding="UTF-8"	standalone='	'ye
	· ·		m		F
ataset Timeout:	10000				

ſ

WMI:

Once you select WMI Dataset option and click **Add** button, you can start collecting WMI data for supported platforms. Select the platform, enter Name space, select Query type, enter the Query. Select the masking rule and enter the Dataset Timeout (ms) Click **OK** button to add the data.



elect Platform and	Collection Parameters			
Platform	Namespace	Query	Query Type	
				-**
			🕈 Add 🗙 Delete 🧷 Mod	lify

Enter the details for WMI selection. Once all the data is entered you are ready to add a new WMI dataset.

Select Platform:	Cisco Device	Y
* Namespace:	cimv2	
* Select QueryType:	(PS	~
* Query:	Get-ItemProperty -Path 'HKLM:\\SYSTEM\\CurrentControlSet\\Service	s\\an
		~
Masking Rule:		

Figure 6-71	Dataset Entry Details - WMI

Select Platform:	Cisco Device	
Namespace:	cimv2	
Select QueryType:	WQL	
Query:	Select * from Win32_DiskDriveToDiskPartition	
Masking Rule:		
Dataset Timeout(ms):		

HTTP:

Once you select HTTP option and click **Add** button, Select the platform, and specify the URL. These are mandatory fields. Once done you can start collecting the data.

Γ

ataset Details Dataset Platforms		
Select Data Collection Type		
Dataset Type: HTTP		~
Select Platform and Collection Parame	eters	
Platform	URL	
TP_Conductor	/RPC2	
TP_Codian	/RPC2	
		View

TL1:

Once you select TL1 option and click **Add** button, Select the platform and the Command string. These are mandatory fields. You can also enter Maximum Lines, Integrity Rule, Masking Rule, Dataset Timeout. Click **OK** button to add the data.

Figure 6-73 Dataset Platforms (Select TL1)

the second second second second				
ataset Details	Dataset Platforms			
Select Data	Collection Type			
Dataset Type	2: TL1			~
Select Platf	orm and Collection Pa	irameters		
Platform		Command	Timeout	
Cisco Devi	De	show version	3000	
			I 🕈 Add 🛛 🗙 Delete 🖉 Modify	
			I 🏶 Add 🛛 X Delete 🖉 Modify	
			I 🗣 Add i 🗶 Delete 🖉 Modify	
			I 🗣 Add 🛛 X Delete 🖉 Modify	
IIOP:

Once you select IIOP option and click Add button, Select the platform. This is a mandatory field. You can also enter Dataset Timeout and choose APIs or All APIs. Click OK button to add the data.

Figure 6-74 Dataset Platforms (Select IIOP)

Add Dataset	×
Dataset Details Dataset Platforms	
Select Data Collection Type Dataset Type: IIOP	×
Select Platform and Collection Parameters	
Platform Timeout	
ASA_CSCub30913	
	ēt _
	-+
Add Y Dot	to d Modifi
	ie 🖉 moony
Help	OK Cancel

Figure 6-75 Dataset Entry Details

Γ

Select Platform.	ACNS	*	
imeout:			
All API's			
Only the following	API's		

SQL:

Once you select SQL option and click **Add** button, Select the platform enter the Query. Select the masking rule and enter the Dataset Timeout (ms) Click **OK** button to add the data.

Figure 6-76 Dataset Platforms (Select SQL)

dd Dataset	×
Dataset Details Dataset Platforms	
Select Data Collection Type Dataset Type: SQL	
Select Platform and Collection Parameters	
Platform	Query
Cisco IO5 Routers	12
	Add × Delete 2 Modify
	HelpOK Cancel

Figure 6-77 Dataset Entry Details

* Select Platform:	TMS		~
Query:	SELECT * FROM tmsng.d	ibo.IPZones1	
Masking Rule:	(I		~
Dataset Timeout(ms):			

Go back to CSPC Flow Chart

LDAP:

Once you select LDAP option and click **Add** button, Select Platform, enter Search base, Select Search scope, enter Search filter and if required enter Attributes To Return, select Masking Rule, and Dataset Timeout (ms). Click **OK** button to add the data.

Γ

aset Details	Dataset Platforms				
select Data Coll	ection Type				
Dataset Type:	LDAP				*
Select Platform a	and Collection Paramet	ers			
Platform	Searchbase	Searchfilter	Searchscope	Attributes To Ret	
					<u>-</u> +
					Et E4
			🗣 Add	× Delete 🙎 Modify	<u></u> +
			💠 Add	🗙 Delete 💋 Modify	<u>.</u>
			🌩 Add	🗙 Delete 🥒 Modify	<u><u><u></u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u></u>
			Add	🗙 Delete 🥒 Modify	

Figure 6-78 LDAP

Figure 6-79 Data Entry Details

~
~

Table 6-7LADP Parameters

Field	Description
Search Base	The base for the search. It must be a valid distinguished name and it is mandatory otherwise a validation error is thrown.
Search Filter	The filter to use for this search and it is mandatory filed. For an invalid search filter, a validation error is thrown.

I

Field	Description
Search Scope	The search scope is OBJECT, ONELEVEL, or SUBTREE and it is a mandatory field.
Attributes to Return	The attributes to use for this search and it is optional. If nothing is provided, then it fetches all available attributes.

p

Dynamic Dataset

Dynamic datasets allow the collection of data based on the output of another command or set of commands.

To create a dynamic dataset, follow the steps given below:

Step 1 In Collection Rules, click Manage Datasets

Step 2 Click Add Dataset button

ł	Figure 6-80 Add Dataset
	Add Dataset X
	Create a static dataset. The collection mechanism speicfied in the static dataset is defined as a command or SNMP request.
	C Create a static dataset
	Create a dynamic dataset. The dynamic datasets allow collection of data based on the output another command or set of commands.
	Create a dynamic dataset
	Help OK Cancel

Step 3 Select Create Dynamic Dataset and click OK

Step 4In Dataset Definition box, specify the dynamic datasetXML.XML file uses the Pari API XML Schema

Step 5 Click OK

ſ

Dynamic Dataset is created and added to Manage Datasets.

	amic Dataset Editor - Create a new Dataset	
Da	ataset Definition	
10	Oataset identifier="show_module_version">	
2	<type>Dynamic</type>	
3 -	<title>show modules version</title>	
4	<collectiontype>CLI</collectiontype>	
5	<categoryname>Hodule Version</categoryname>	
6	<statements></statements>	
7	<loop identifier="_show_module_1"></loop>	
8	<pre></pre>	
9	<block></block>	
0	<input/>	
1	(Dataset)	
2	<pre>datasetName Failure="error_nessage">_ahow_nodule</pre>	
3		
4		
5	(Parans)	
6	<start ignozecase="false">Mod\sPorts\sCard\sType\s+Model\s+Serial\sNo.</start>	
7	<end ignorecase="false">Hod\sPorts\sCard\sType\s+Hodel\s+Serial\sNo.</end>	
E	<idsconfigblocks>false</idsconfigblocks>	
9		
0		
1		
4	(Statements)	
3	<loop identifier=" show module 1 1"></loop>	
ess	ssages - Log	
		DV Devel Method V

Figure 6-81 Create Dynamic Datasets

Manage Platform Definitions

Chapter 6

I

Manage Platform Definitions lets you select a group of devices that match a specific condition. You can select what data is to be collected from this group of devices using *Manage Datasets*. When a new device is discovered that matches this specific condition, it automatically becomes part of this platform. Hence, the same data that is collected for other devices in this platform definition is collected from the new device.

Creating new platform definitions is shown below:

e q	× GAdd Plat	form Definition 👹 Modify P	Platform Definition 🥥 Rem	ove Platform Definition	2
Platform		LockStatus	NoOfConditi	CreatedBy	
ССМ		UnLocked	1	system	-
IOS_XR	Add Platform Definition			×	
IOS_LS1010	Platform Details Platfor	m Conditions			
IOS_as5300					3
IPVC	* T#los			-	
SanOS	* Identifier:		Gener	ata	
IOS_12000_1	Description:		Gener		
ADEOS					
WebNS_CSS115xx					
IOS_10000					
CatOS_1	Help.		nOK Ca	Incel	
CCM4x		G UnLocked	1	system	
CatOS_63ge_1			2	system	

Figure 6-82 Create Platform Definitions

- Step 1 Click Add Platform Definition button
- Step 2 As shown in Figure 6-82, enter the Title, Identifier and Description for the new platform definition
- Step 3 Once the base data is entered, enter the conditions that make up this platform definition as shown below

Figure 6-83 Add	Platform Conditions	
Add Platform Definition		1
Platform Details Plat	tform Conditions	
Select Condition M	atch Type	
Match Type:	All of the Columns must	: be matched
Define Platform Co	onditions	
Property	Operator	Values(s)
lp Address	equals	10.1.1.2
		🕂 Add 🗙 Delete 🖉 Modify
	Help	p Test Platform Definition OK Cancel

- **Step 4** Select whether all the conditions that you are defining need to match in order for a device to be part of this platform definition or some of the condition matching is sufficient.
- Step 5 Click Add to start adding the conditions.

Fig	ure 6-84 Platfor	n Conditions	
Pla	tform Condition		×
	Condition Details		
	* Device Property:	OS Name	~
	* Operator:	equals	*
	* Value:	SAN-OS	~
	Test Re	ular Expression	Cancel

- **Step 6** When entering the conditions, you have the following options:
 - You can select OS Name, OS Version, Product Model or SNMP Sys Object ID., and SNMP Sys
 Description
 - Depending on the Device Property the *Value* field is changed (either OS Name selected from the list, or values provided for version, model, or sys object id) an *Operator* can be used to match these two
 - The operator provides 6 different options: equals, does not equal, in the list, not in the list, does not match regular expression and matches regular expression.

Go back to CSPC Flow Chart

Γ

Step 7 Once the platform definition is created, use *Test Platform Definition* to check if any platforms match this definition, as shown below.

latform Details	Platform Conditions	
Platform Detai	ls	
* Title:	IOS2	
* Identifier:	_IOS2	Generate
Description:		~
		-

Figure 6-85 Test Platform Definitions





Platform Applicability Status		
Device	Platform Applicability	
🔮 rcdn-astp-cmpub02	Not Applicable	
Device_5_0_1_22	Not Applicable	
Device_5_0_1_51	Not Applicable	
Device_5_0_1_52	Not Applicable	E
Device_5_0_1_25	Not Applicable	
Device_5_0_1_26	Not Applicable	
Device_5_0_1_23	Not Applicable	
Device_5_0_1_24	Not Applicable	
WLCUCM86P	Not Applicable	
🔮 wsa061	Not Applicable	
Device_5_0_1_27	Not Applicable	
Device_5_0_1_46	Not Applicable	-

Figure 6-87 Platform Applicability Status

You can also import platform definition from a zip file stored locally on your system. To do so, right-click in the Manage Platform Definitions window and select "Import Platform Definition from Zip File" option, browse to the zip file with platform definition on your system as shown in Figure 6-88 and click Submit.



Import from Zip Platform Definition	×
Upload File	
C:\Users\shahians\Desl Browse_ Submit	
Done	

Manage Data Integrity Rules

Data Integrity Rules are defined to identify whether a command execution returned a correct response or an error message. You can create new data integrity rules as shown below:

× ⊕,	kdd Data Integrity Rule 👹 Modify Data Inte	egrity Rule 🔵 Remov	ve Data Integrity Rule	3
ule	Lock Status	No. of Condi	Created By	
NC Global Interity Rule	C UnLocked	27	system	
Add Data Integrity Rule		×		
Rule Details Rule Condition	15			
Integrity Rule Details				
* Title:	- 415			
* Identifier:	Gen	erate		
Description:		*		
	Help OK	Cancel		

Figure 6-89 Create a New Data Integrity Rule

Step 1 Click Add Data Integrity Rules.

Γ

- Step 2 Enter the Title, Identifier and Description for the new data integrity rule
- Step 3 Once the base data is entered, enter the rule conditions that make up this rule as shown below

Figure 6-90 Rule	Conditions for	Data Integr	ity Rules		
Add Data Integrity Rule					×
Rule Details Rule C	onditions				
Select Rule Match	Туре				
Rule Match Type:	All of the Rule	s must be r	natched		~
Define Integrity R	ule Conditions				
Operator	Exp	ression			
matches the expres	sion ciso	:0			
<	m				4
		🕈 Add	× Delete 🖉 I/	lodify	
		Help	ок	Can	cel

- **Step 4** Select whether all the conditions that you are defining need to match in order for a device to be part of this integrity rules or if some of the condition matching is sufficient.
- Step 5 Click Add to start adding the conditions.

Fig	ure 6-91 Rule C	onditions	
Dat	ta Integrity Rule Con	dition Details	×
Г			
	Data Integrity Rul	e Condition Details	
	* Operator:	matches the expression 👻	
	* Expression:	cisco	
	Error Message:	Invalid Command	
	ОК	Test Regular Expression Cancel	

Step 6 When entering the conditions, select the operator (*matches the expression* or *does not match the expression*), the regular expression value and what error message to display.

You can also import platform definition from a zip file stored locally on your system. To do so, right-click in the Manage Data Integrity Rules window and select "Import Data Integrity Rules from a Zip File" option, browse to the zip file with Integrity rules on your system and click **Submit**.

Go back to CSPC Flow Chart

Chapter 6	Applications - Device Managemer
-----------	---------------------------------

Manage Data Masking Rules

Masking options are provided to mask certain sensitive information such as User Names/Passwords in the configuration files before exporting them to higher level applications. You can create data masking rules that tell the collector what data to mask before exporting it.

Create a new masking rules as shown below:

Figure 6-92 Create New Data Masking Rule

	Lock Status	No. of Patte	CreatedBy
Configuration Masking Rule	UnLocked	156	system
Add Masking Rule Rule Details Rule Patterns		×	
* Title:		Generate	

Step 1 Click Add Masking Rules button

I

In the Add Masking Rules window, enter Title, Identifier and Description for the new masking rule Step 2

Once the base data is entered, enter the rule patterns that make up this rule as shown below Step 3

Replacement Value

Add × Delete

Figure 6-93 Rule Patterns for Data Masking Rules

- Step 4 Click Add to start adding the conditions.
 - Figure 6-94 Rule Pattern Conditions

Dat	ta Mask Pattern Deta	iils	×
	Data Mask Patterr	1 Details	
	* Expression:	^[]*username+\(\$	
	* Replacement:	######	
	ОК	Test Regular Expression Cano	cel

Step 5 As defined here whenever there is a Username followed by Password in the configuration files they are replaced by the string *xxxxxx*.

You can also import masking rules from a zip file stored locally on your system. To do so, right-click in the Manage Data Masking Rules window and select "Import Masking Rules from Zip File" option, browse to the zip file with masking rules on your system and click **Submit** button.

Go back to CSPC Flow Chart

No. of Filters

Device Management

Manage Syslog Source Files

ł

0 Q .-

Source File Name

Syslog Source Files options are provided to define the syslog collection from devices. You can add new settings for syslog sources.

I

This feature is only for NOS services

Manage Syslog Source Files

es
2S

× G Add Syslog Source Settings..

SyslogSource	10000	0	
Source Log	15000	0	
A A Page 1 of 1 P P			Displaying 1 - 2 o

💣 Modify Syslog Sour

Pooling Frequence(ms)

Create new syslog source file by selecting the Add button.

Add Syslog Source option is provided to add a new Syslog source. There are two tabs in adding the syslog sources.

First tab is **File Details** as shown in Figure 6-96. You need to provide the following information on this screen:

- Source File Path: The path where the Syslog source is located.
- Identifier: It can be either user defined, or system generated.
- **Roll Over File Name**: This is the name of the file that needs to be spooled in case the primary filed rolled over.
- **Polling Frequency**: This is the polling frequency to poll the Syslog messages. The value will be in between 5000 to 3600000 milliseconds.
- **Description**: Description of the file.

Note

Add S	yslog Source Settings			X
File	e Details Input Filters			
	Syslog Source File Details			1
	* Source File Path:	c:\syslog_modified.txt		
•	* Identifier:	_csyslog_modifiedtxt	Generate	
F	Rollover File Name:	syslogmode		
3	* Pooling Frequency(ms):	5000		
(Description:		*	
			-	
				1
		Help OK	Cancel	

Figure 6-96 Add Syslog Source

Second tab is **Input Filters**; when you select the Add button, Input Filter Details window will pop up. You need to provide the following information for this screen:

- Source Device: Device from which messages to be spooled.
- Minimum Severity: Minimum Severity that needs to be displayed.
- Maximum Severity: Maximum Severity that needs to be displayed.
- Component Name: Name of the component in the message.
- Mnemonic Text: Mnemonic text in the message.
- **Description**: Description in the message.
- Action to be taken: It can either be Accept or Drop the syslog.

Γ

Figure 6-97 Add Input Filter	
Modify Syslog Source Settings	×
File Details Input Filters	
Define Syslog Input Filters	
Conditions	Action
(Source matches 10.1.1.1) && (MinSeverity equals to 0) && (MaxSeverity equals to 3) && (Componen	Accept
	•
	🕈 Add 🛛 Delete 🖉 Modify
Нер.	OK Cancel

Click Add button, a screen as shown in Figure 7-23 is displayed. Enter the details as shown below.

Source Device:	10.1.1.1
Minimum Severity:	0 (emergency)
Maximum	3 (error)
Seventy:	
Component Name:	SYSLOG
Mnemonic Text:	CPUHOG
Description:	
Action to be taker	1
* Action:	Accept
* Action:	Ассерц

Figure 6-98 Add Input Filter Details

Miscellaneous Rules

Use the Miscellaneous Rule sub tab of the Device Management tab to set up rules, profiles and manage workflow.

This section describes the Miscellaneous Rules options in the following topics:

- Export All Rules
- Import All Rules
- Import DSIRT Files
- Manage Application Discovery Profiles
- Manage SNMP Trap Profiles
- Manage Jump Server
- Credential Lock Settings
- Manage WorkFlow

Export All Rules

Use Export All Rules option under Data Collection Settings to Export all rules. Click Yes to export all rules and zip file is downloaded.

Figure 6-99	Export All Rules				
Confirm	of the execute budgefult all the day	icor will be cole	eted for collec	ion profiles. Do you want to coninue?	
As part of	a the export, byteratic all the text	res will be sele	cted for collec	on promes: Do you want to connue?	
		Yes	No		

Import All Rules

Use Import All Rules option under Data Collection Settings to import all rules. In the dialog box that is displayed click Browse button, select the rules file in zip format and click OK to start importing all rules.

Figure 6-100	Import All Rules	
Import All Rules from	Zip File	×
Upload File		
	Browse Submit	
		Done

Import DSIRT Files

In Import DSIRT Files, you can select a DSIRT (Device Software Issues Reporting Tool) file and import it in the tool.

Figure 6-101	Import DSIRT Files	
Import DSIRT Files	2	<
Upload File		
	Browse Submit	
	Done	

Go back to CSPC Flow Chart

Manage Application Discovery Profiles

In Manage Application Discovery profiles you can add or edit an application discovery profile, define the devices that collect data and how often the data needs to be collected. Application discovery detects what applications are installed/running on devices (typically compute server) by collecting information from devices.

Figure 6-102 Manage Application Discovery Profiles

Manage Applications Discovery	Profiles 🗵		
0 Q-	🗙 🕒 Add Application Discovery Profile 💝 🛙	odify Application Discovery Profile 🔘 Re	emove Application Discovery Profile 🔿 🔘
Name	Title	Lock Status	Scheduled
profileNew	profileNew	GUnLocked	8
test	test	GUnLocked	8
Discoveryprofile	Discoveryprofile		0
4 4 Page 1 of 1 ▶ ▶			Displaying 1 - 3 of 3

New application discovery profiles can be created by clicking *Add Application Discovery Profile* icon from Manage Application Discovery Profiles window.

To add a new application discovery profile, follow the steps given below:

- Step 1 Select the Devices
- Step 2 Select Profile details
- Step 3 Click OK.

I



Figure 6-103Select Devices for an Application Discovery Profile

To start the collection, select a device or a set of devices from which the data is to be collected as shown in Figure 6-103. Once you select the devices, select the profile options that define how often you want to collect the data, as shown in Figure 6-104.

Application Profile Details			
* Profile Title:	DemoProfile		
* Identifier:	DemoProfile	Generate	
Description:			
Collection Profile Schedule			
Schedule Periodic Collectio	n		
No schedule configured	cally if its interrupted due to a CSPC	server restart	
No schedule configured	ally if its interrupted due to a CSPC	server restart	
No schedule configured	cally if its interrupted due to a CSPC	server restart	

If you schedule a job for periodic collection, the job can be resumed even if the CSPC server is restarted by selecting the option "Resume this job automatically if it is interrupted due to a CSPC server restart".

Manage SNMP Trap Profiles

This helps you to add the new SNMP Trap profiles and store them depending on the filter you configure. One trap can be applied to multiple filters. You get a notification when a trap is received.



I

This feature is only for NCCM services



To create new SNMP Trap Profile click *Add SNMP Trap Configuration* icon from Manage SNMP Trap Profiles window.

To add a new SNMP Trap Profile, follow the steps given below:

Step 1 Select Profile Details

- a. Enter the **Profile** and **Queue** name is JMF queue where add-on process should subscriber to the given JMF Queue
- *b.* Click arrows to select the **Notification Types.** By default ,there are only two notification types if required you can add as many as notifications through xml request. *Refer to "XML APIs"*

Step 2 Select the Devices

Step 3 Click OK.

	Calact Daviana	
Profile Details	Select Devices	
Profile Details		
Profile Name:	Enter Profile Name)
Queue Name:	Enter Queue Name	
Select Notificat	ion Types	
CISCO-CONF	IG-MAN-MIB	
CISCO-CONF	IG-COPY-MIB	
	-45	
	-	
	+	
	(*	
]

Select Devices tab as shown in Figure 6-110 allows you to map the devices to the specific Trap Profiles.

There are two options to map the devices to Taps Profiles:

- All managed devices It maps all the devices to the specified Taps Profile
- Only the following selected devices It maps only the selected devices to the specified Taps Profile.

No. Barbala	C-l-+ Di	1				
rofile Details	Select Devices					
Select Devic All manage Only the Managed Device	es ged devices following selected wices:	devices		54	elected Devices/Groups	52
12 €	lodes (5)					
Ø Unreal	achable Nodes (8)					
🦓 Video))		=			
🚓 Stora	geNetworking			->>		
🦓 Confe	erencing			->		+
🦓 Unifie	dCommunications	(*		+
🦓 Colla	borationEndpoints					
🕨 🦓 Succe	essfulDevGrp (1)					
en Optic	alNetworking					
Cloud	landSystemsMana	gement				
🦓 Wirele	855					
💏 Hubs			Ŧ			/

Manage Jump Server

The Jump server support allows CSPC to connect to any device CLI via a Jump Server where direct access to the device CLI is prevented. The Jump Server configuration allows you to configure the Jump Server feature. In Manage Jump Server you can add or edit a Jump server. It manages the device and the type of connection and test the connection.

Figure 6-108	Manage Jump Server	
Manage Jump Serve	/ers 🕷	
0 Q.+	× 🕞 Add Jump Server 👸 Modify Jump Server 🥥 Remove Jump Server 👄 🕕	
IP Address	Description	
10.1.1.10	New	

To create new Jump Server click Add Jump Server icon from Manage Jump Server window.

To add a new jump server, follow the steps given below:

- Step 1 Select Profile details
- Step 2 Select the Devices
- Step 3 Click OK.

Γ

I

		×
rofile Details Select Dev	lices	-
Jump Server Details	10.1.1.10	
* User Name:	Test	
* Password:	••••	
* Number of Connections:	2	
Protocol:	sshv2	
Description:	telnet	
	sshv1	1
lest Connection		

Table 6-8

Jump Server Parameters

Field Name	Description
Host name	Name defined to server
User Name	Login username
Password	Login Password
Number of Connections	No of connections to jump server.
Protocol	Select the protocol to be used
Description	Description of the server
Test Connection	To check the jump server credentials

Note: Device must be SNMP supported without jump server in order to be discovered in CSPC. If not, DAV will be skipped & Collection would fail.

Select Devices tab as shown in Figure 6-110 allows you to map the devices to the specific Jump Server.

There are two options to map the devices to Jump Server:

- · All managed devices It maps all the devices to the Jump Server
- Only the following selected devices It maps only the selected devices to the specified Jump Server.

If you select "**All managed devices**" option, it maps all the devices to the specified Jump Server. If you want to map all devices to specified jump server you have to make sure that no other devices are mapped to any other Jump Server.

If you select "**Only the following selected devices**" option, it maps only the selected devices to the specified Jump Server. If some of the devices which you are trying to map to the specified Jump Server are already mapped to any other Jump Server, then while creating the Jump Server these already mapped device will be excluded from the mapping and unique devices will be mapped.

Jump Server					
Profile Details	Select Devices				
Select Device All manage Only the f Managed De	is ad devices ollowing selected devices vices:			Selected Devices/Groups:	
Con Con IN	Communications	isplaying		ege rooters	
Router		ĥ			
D Canada Generic	NetworkDevices (8)				
Coptical		E	-10		
🚓 Storage			+		-
🦓 Video			+		*
🚓 Univer	salGatewaysAndAccessServers		-		
Applica	tionNetworking				
🦛 VoiceG	ateways				
🚓 Voice					
🚓 DataCe	enter	-			
•	III	•			-

Credential Lock Settings

Credential Lock Settings allows you to set the maximum number of failed attempts for any given credential. You can also specify a lock period for a credential. If a lock period is present that credential will be unlocked once the lock period expires.

There is also an option for the user to manually unlock the credential. This helps in continuation of the discovery/inventory processes even after a device fails to respond to a specific credential.

Configure Credential Lock Se	ettings	
* Maximum Failed Attempts:	2	
* Lock Period:	10000	(milli seconds)
	8	2

You can also remove the previously added lock settings by using Remove Settings button.

Manage WorkFlow

This Helps you to Modify, Start, Stop, Remove, Resume, and see Log. This Displays Name, Status, Created By, Created Time, and Service.

- Click Modify to modify the workflow
- Click **Start** to start the workflow which are in open and stop status.
- Click Stop to stop the workflow and click Resume to resume the workflow

Figure 6-112 Manage Workflow

Manage Workflows				
0 Q.+	× 🔿 🎯 Modify [Start 🚺 Stop 🖨 Remove 🚺	Resume 📄 Log	
Name	Status	Created By	Created Time	Service
3nov-1017	OPEN	admin	Tue, Nov 3, 2015 21:36:3	7 +0 NOS
test1016.3nov	OPEN	admin	Tue, Nov 3, 2015 21:35:3	7 +0 NOS
3nov-1026-1	OPEN	admin	Tue, Nov 3, 2015 21:45:3	2 +0 NOS
3Nov-1031	OPEN	admin	Tue, Nov 3, 2015 21:50:1	3 +0 NOS
3nov440	OPEN	admin	Tue, Nov 3, 2015 15:59:5	6 +0 NOS
3nov-1040	OPEN	admin	Tue, Nov 3, 2015 22:00:0	0 +0 NOS
3nov-1050	OPEN	admin	Tue, Nov 3, 2015 22:09:1	8 +0 NOS
Default_Work_Flow	OPEN	admin	Tue, Nov 3, 2015 12:14:4	8 +0 NOS
3nov1	OPEN	admin	Tue, Nov 3, 2015 16:00:5	9 +0 NOS
4nov1	OPEN	admin	Wed, Nov 4, 2015 09:52:	24 + NOS
3Nov447	OPEN	admin	Tue, Nov 3, 2015 16:06:3	2 +0 NOS



Applications - Management Tasks

Management Tasks

You can use the Management tasks to access tools with which you can discovery, collect profile, retrieve job status.

This section describes the Management Tasks options in the following topics:

- Device Tasks
- Common Tasks
- Job Run Status
- Job Management

Device Tasks

Use the Device Tasks sub tab of the Management tasks to set up device discovery and data collection process.

This section describes the Device Tasks options in the following topics:

- Discover Devices
- Unmanage Devices
- Verify Device Access
- Device Prompt Collection

Discover Devices

The Discover Devices feature allows you to discover devices and manage them. When you double-click **Discover Devices**, a new wizard called **Discover and Manage Network Devices** appear. It allows you to select the Discovery method and the devices to be discovered by entering either the IP address or host name of the device.



To overcome the exposure of the credentials to all hosts in the IP range:

- Use trusted networks for discovery based on IP ranges.
- It is recommended to add devices using individual IP address.

There are multiple ways to discover a device:

- Known Device List
- Protocol based discovery (CDP, OSPF, ARP, BGP, etc.). Not supported in UC Discovery.
- IP Address Range Scanning
- Rediscover the currently managed devices

Note

A message box "Please select at least one discovery method" is displayed when you click **Next** button without selecting any Discovery method.



Γ



CSPC Collection Platform Software User Guide



I



1	Figure 7-5 Discover and Manage Network Devices	
	Discover and Manage Network Devices	×
	Select Discovery Methods	
	Select at least one of the following network device discovery methods.	
	Discover devices with known IP addresses	
	Discover devices with protocols such as CDP, OSPF and ARP	
	Discover devices by scanning/pinging range of IP Addresses	
	Rediscover the currently managed and non-managed devices	
	Import < Previous Next > Help Canc	el
J		

Figure 7-5 Discover and Manage Network Devices

You could also import the device list from either a CiscoWorks DCR file or a Pari Discovery Options XML file.

For Known Device List discovery, enter the IP addresses or hostnames as shown in Figure 7-6.



If multiple discovery types are selected then first selected SNMP version protocol will be used for range and protocol based discovery

I

over and Manage Network Devices	
nter the list of IP addresses for the known devices.	
IP Address/Host Name	
♣ Add ¥ Delete 2 Modify	
10.1.1.10	

Figure 7-6 Discover Devices using Known IP Addresses

To include protocols, select the protocol and use the arrows to move back and forth. To change the priority of protocols, use the up and down arrows.

If you Select **Do not Manage Devices** option, then the devices are not be managed but discovered. These devices can be exported as a zip file which contains *.csv* files for Discovered Devices and Un-Reachable Devices. Discovered Devices *csv* file is of *CNC CSV* format. This export option is available under Discovery Jobs.

If you select **Enable Loopback** option, then discovery will prefer a loopback IP address and it will attempt to use other addresses if a loopback is not found. Loopback is tried if Mac Address Duplicate Check option is selected in Discovery Settings.

If required provide job specific SNMP timeout value in SNMP Timeout (in sec) field.

Enter the Job Description and select the Service Name from drop down.

over and Manage Netwo	ork Devices					
Management Protocol						
/ Include Protocols						
snmpv3 snmpv2c telnet http https	sshv2 snmpv1 sshv1 *					
Enable NMAP D	Discovery Mana	ige Devices				
Enable Loopback	k					
SNMP Timeout						5.
* SNMP Timeout (in :	sec): 3					
Iob Details						
Job Description:						
Service Name:			~			
Job Scheduling Optio	ns					
Start discovery	now					
Schedule discovery	very					
No schedule c	onfigured					
Configure Schedule						
(

Figure 7-7 Discovery Schedule Options

For protocol based discovery, enter 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)

Discover and Manage Network	Devices			×
Select list of seed devices and pr	otocols need to be used in discovery operation			
Select Protocols	Cisco Discovery Protocol (CDP) OSPF Neighbours Hot Standby Router Protocol (HSRP)	Routing Table Border Gateway Protocol (BGP)	Address Resolution Protocol (ARP) Link Layer Discovery Protocol (LLDP)	
Hop Count	2			
Seed IP Address/Name				
🕈 Add 🗙 Delete 🖉 Modi	fy			
10.20.1.2				
		< Prev	vious Next > Help Cance	

Figure 7-8 Protocol Based Discovery

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 also have "select CIDR Address" before providing Start IP Address.

Figure 7-9 IP Scanning

ſ

wer devices by scanning/pinging range of IP Addi the list of Ip Addresses ranges for scanning. The devices	resses at these addresses will t				
the list of Ip Addresses ranges for scanning. The devices	at these addresses will b				
the list of Ip Addresses ranges for scanning. The devices	at these addresses will b				
		be pinged using ICM	P Ping mechanism		
art IP Address	CIDR Address?]			
d IP Address	i				
Add 🗙 Delete 🧷 Modify					

You can select the option **Rediscovering Currently Managed and NON Managed Devices**. It will discover with all the previous discovered protocol and for unreachable devices, and non-managed devices it will try all SNMP protocol and discovery process will rediscover all the devices that are currently managed.

Select the management protocol used for the discovery process. The current options are SNMPv1, SNMPv2 or SNMPv3.

Enter the Job Description and select the Service Name from drop down.

Once the type of discovery is specified, you are ready to discover the devices. You can schedule the discovery process either right away or at a later time.

Figure 7-10 Discovery Schedule Options

Management Protocol snmpv3 snmpv2c telnet https			
Discovery Options Enable NMAP Discovery Manage Devices Do not Manage Devices Enable Loopback SNMP Timeout SNMP Timeout Job Details Job Details		 	
Job Scheduling Options Start discovery now Schedule discovery No schedule configured Configure Schedule			

To Schedule Discovery at a later time, select Schedule Discovery option and then click **Configure Schedule** button.

You can schedule Start and End Date/Time or select the Recurrence pattern as Minutely, Daily, Weekly, Monthly, or Yearly as shown in Figure 7-11.
Figure 7-11 Configure Schedule	Configure Schedule	×
Range of Recur Schedule St Schedule En	tart Date/Time April 21,2021 17:35 Repeat schedule O No end date Date/Time End by April 21,2021 17:38 C	
Recurrence Patt Minutely Daily Weekly Monthly Yearly 	tern	
		OK Cancel

After the *Discover and Manage* operation is finished, you see the results which include the IP Address (of the selected device), Host Name, Device Type, Status (which indicates whether or not the device is managed), and Message. Discovery operation can be closed and run in the background. You can check the *Job Log Reports->Discovery Jobs* to view the results of the background operation.

You can also Clone an older discovery job to use as a new discovery job to speed up discovery. Refer to *Job Log Reports ->Discovery Jobs* for more information on cloning a discovery operation.

In the discovery jobs report, you can create a new discovery job by right clicking on any discovered joband selecting 'Create new discovery by cloning this job'.

		Job Completer	4	
		oob completed		
	Ma	inaged Devices:128 🧶 F	ailed Devices:208	
Hos	it Name	Device Type	Status	Message
.1 L18	4	cisco7606	Discovered	Device is already managed using th
1 Dev	vice_5_0_1_51	AIR-CT5508-K9	Discovered	Device is already managed using th
Dev	rice_5_0_1_5	WS-C2948	Discovered	Device is already managed using th
2 Dev	rice_5_0_1_52	ciscoWLSE1030	Discovered	Device is already managed using th
Dev	rice_5_0_1_4	vpnClientRev1	Discovered	Device is already managed using th
			Failed	5.0.1.7: Device Unreachable or Inco
3			Failed	5.0.1.53: Device Unreachable or Inc
Dev	rice_5_0_1_6	wsc5505sysID	Discovered	Device is already managed using th
) Dev	rice_5_0_1_10	ciscoDPA7630	Discovered	Device is already managed using th
Dev	rice_5_0_1_9	ciscoTSPri	Discovered	Device is already managed using th
1 Dev	rice_5_0_1_11	ciscoMDE10XVB	Discovered	Device is already managed using th
Dev	rice_5_0_1_8	ISM	Discovered	Device is already managed using th
2 Dev	vice_5_0_1_12	ciscoWsSvcFwm1sc	Discovered	Device is already managed using th
	A Hos A Hos A L18 A Dev Dev Dev Dev Dev Dev A Dev Dev A Dev Dev Dev Dev Dev Dev Dev Dev	Host Name .1 L18 1 Device_5_0_1_51 Device_5_0_1_52 Device_5_0_1_52 Device_5_0_1_6 Device_5_0_1_6 0 Device_5_0_1_9 1 Device_5_0_1_10 Device_5_0_1_12 Device_5_0_1_14	Job Completed Managed Devices:128 F Host Name Device Type 1 L18 cisco7606 1 Device_5_0_1_51 AR-CTS508-K9 Device_5_0_1_51 AR-CTS508-K9 Device_5_0_1_52 cisco7006 1 Device_5_0_1_52 ciscoWLSE1030 Device_5_0_1_6 wsc5505sysD Device_5_0_1_6 wsc5505sysD Device_5_0_1_9 ciscoMDE10XVB Device_5_0_1_8 ISM 2 Device_5_0_1_12	Job Completed Image Devices:128 Failed Devices:208 Host Name Device Type Status 1 L18 cisco7606 Discovered 1 Device_5_0_1_51 AR-CT5508-K9 Discovered 1 Device_5_0_1_52 ciscoWLSE1030 Discovered 2 Device_5_0_1_52 ciscoWLSE1030 Discovered 0 Device_5_0_1_4 vpnClientRev1 Discovered 3 Envice_5_0_1_6 wsc5505sysID Discovered 0 Device_5_0_1_6 wsc5505sysID Discovered 0 Device_5_0_1_10 ciscoMDPA7630 Discovered 1 Device_5_0_1_11 ciscoMDE10XVB Discovered 0 Device_5_0_1_13 ISM Discovered 2 Device_5_0_1_14 ciscoWLSTPri Discovered

Figure 7-12 Discovery in Progress

I

You can export the Discovery Settings to an XML file, as well export the discovered devices report. Go back to CSPC Flow Chart

Unmanage Devices

Double-clicking **Unmanage Devices** opens a new window. It shows the list of devices that are already managed, and allows you to select the devices that you want to Unmanage. After selecting the devices or groups, the selected devices or groups appear on right side of the window. Then, click **Unmanage** to remove the selected devices or groups, as shown below. You can also browse to upload list of nodes from *.txt* file.



Select Devices				
Managed Devices:		Selected	Devices/Groups:	
12 0				
Real Universal Gateways And Access Servers				
R Voice				
Real VoiceGateways				
🚓 Video				
GenericNetworkDevices (87)		-		
Unreachable Nodes (65)	H	+		+
🚓 Storage		<u>*</u>		
🚓 Telepresence		*		
Coptical				
RetworkManagement				
🚓 DataCenter				
🕨 🥰 Wireless (1)				
Communications				
ServiceReadyPlatform	-			

Once this operation is completed, CSPC removes the unmanaged devices along with all the corresponding data (collection profile data and so on) from its database.

Verify Device Access

I

Use Device Access Verification when you want to check whether a given device is accessible through a specific credential, as shown below. All the settings are taken from Access Verification Settings. You can also make the changes to settings and is applicable only for the job you change the settings.

Follow the steps given below to perform device access verification:

- Step 1 Select the devices for which data access needs to be verified. You can also browse to upload list of nodes from *.txt* file.
- Step 2 Select the protocols order to be used for verification using side arrows and reorder them using the up and down arrows. To avoid the failure, you can use the option Use All Selected Protocol Versions and to override the failed protocol select the option Override Enable Failed. If all the protocol fails, then you have an option to use ICMP for reachability of device. If Use all selected protocol version is selected, then all the selected protocol are used even if the first protocol passes. If Override enable failed is selected, then status is shown as enabled by default, even if device do not enter enable mode.
- Step 3 Start the verification process now or schedule it at a later time

Select Devices			
All managed devices (Only Reachable Devices)	evices.)		
Only the following selected devices			
Managed Devices:		Selected Device	s/Groups:
M @			
LiveNodes (63)	*		
🕨 🦓 Unreachable Nodes (6)			
🖓 Hubs			
Servers-UnifiedComputing (3)			
ServiceExchange (1)		•	•
🥰 xDSL		•	*
GenericNetworkDevices (2)		(
Routers (13)			
🏟 Switches			
ATMSwitches (1)			
🏘 BladeSwitches			
ConnectedGridSwitches	*		

Figure 7-14Device Access Verification - Device Selection

	Device A	ccess Verification					
lease select and or	der proto	cols below to use t	them devic	e access verification			
Include SNMP	Protocols			Include CLI Pro	tocols		
	· •	snmpv3			sshv2	1	-t-
	+ +	snmpv2c	-		sshv1		
	.	sninpvi			(telnet		
The second second							
Include HITP	Protocols			Include Other P	rotocols		
	-#>	http	÷.		→ til		ēt.
		mp	±+.		wmi		±+
<u> </u>	(•			2		~	
Use All Select	ed Proto	col Versions		\$ 			
Override Enal	ble Failed	1					
Run DAV for	Unreacha	able					
Use ICMP if all	l the abov	ve protocols fail					
Optimize Devi	on timone	and the second					
	ce unieou	its on successful	verificatio	on			
dvanced Options		its on successful	verificatio	on			
dvanced Options		its on successful	verificatio	on			
advanced Options b Details ob Name:		its on successful	verificatio	on			
b Details ob Name:		ats on successful	verificatio	on			
b Details ob Name: b Description:		ats on successful	verificatio	on	3		
b Details ob Name: b Description: rvice Name:		its on successful	verificatio	90			
dvanced Options b Details ob Name: b Description: rvice Name: lscovery		ats on successful	verificatio	90			
dvanced Options b Details ob Name: b Description: rvice Name: lacovery in Discovery Befo	ore DAV:	ats on successful		on	×		
dvanced Options b Details ob Name: b Description: rvice Name: lscovery in Discovery Before b Schedule Optio	ore DAV:	its on successful		20	×		
dvanced Options b Details ob Name: b Description: rvice Name: liscovery un Discovery Befe b Schedule Optio) Start Device A	ore DAV:	its on successful		201	•		
dvanced Options b Details ob Name: b Description: rvice Name: iscovery in Discovery Bef b Schedule Optio Start Device A) Schedule Dev	ore DAV:	rification Now		201	V		
dvanced Options b Details ob Name: b Description: rvice Name: iscovery in Discovery Bef b Schedule Optio Start Device A Schedule Dev: No schedule Oet	ore DAV: ins Access Ve ice Acces configur	rification Now s Verification red		on 	×		
dvanced Options b Details ob Name: b Description: rvice Name: lscovery in Discovery Befor b Schedule Optio Start Device A Schedule Dev: No schedule of	ore DAV: ms Access Ver ice Acces configur	rification Now is Verification red		on 			
dvanced Options b Details ob Name: b Description: rvice Name: lacovery an Discovery Befor b Schedule Optio Start Device A) Schedule Dev: No schedule of	ore DAV: ms Access Ver ice Acces configur	rification Now Is Verification red		90 			
dvanced Options b Details ob Name: b Description: rvice Name: liacovery an Discovery Before b Schedule Optio Start Device A Schedule Dev No schedule of	ore DAV: ns Access Vei ice Acces	rification Now s Verification red		9N			
dvanced Options b Details ob Name: b Description: rvice Name: liacovery un Discovery Befor b Schedule Optio Start Device A Schedule Dev. No schedule of	ore DAV: ns Access Vei ice Acces	rification Now Is Verification red		201			

Figure 7-15 Device Access Verification - Protocol Selection

Enter the Job Name, Job Description, and select the Service Name from drop down.

Use the **Run Discovery before DAV** option to rediscover the unreachable device for a particular job before running DAV.

To Schedule Device Access Verification at a later time, select Schedule Device Access Verification option and then click Configure Schedule button. You can schedule Start and End Date/Time or select the Recurrence pattern as Minutely, Daily, Weekly, Monthly, or Yearly as shown in Figure 7-16.

<i>igure 7-16</i> onfigure Schedule	Configure	Schedule						\$
Schedule Sta	art Date/Time	April 21,2021		17:35	Repeat	schedule		
Schedule En	d Date/Time	No end date End by	ril 21,2021	•	17:38			
Recurrence Patte	2m							
Minutely Deily								
O Monthly								
O Yearly								
							OY	Grand
							OK	Cancel

You can click on **Advanced Options** button and select the credentials to run DAV on as shown in Figure 7-17.

Figure 7-17	DAV Advanced Options
-------------	----------------------

Credential Name	

Once the job is started you can view the successful and failed credentials/protocols for a given device as shown below.

There is also an option to Optimize device timeouts on successful verification. This is applicable only for SNMP. The option once enabled will automatically calculate the timeout for a specific device and add it to the Global Timeouts under the advanced settings.

When a device access verification job is scheduled to run at a later time, 'Resume this job automatically if it is interrupted due to a CSPC Server restart' option will be available. If the CSPC restarts for any reason while device access verification job is running, CSPC will resume the job upon restart.

By default, CSPC pings a device to check if it is responding Additional ping.

If all the selected protocols have failed for DAV, by default an Additional Ping feature is triggered to check if the devices are responding.

Device Access Verification × Job Completed Selected Devices:71
 Completed Devices:71 No Device Protocol Status Credential (172.20.106.75) telnet Skipped DAV as device is unreachable (172.20.108.12) telnet Skipped DAV as device is unreachable 2 Ξ Information 3 (172.20 Successfully completed the Device Access Verification Job. (72.20. OK 5 (172.20 Skipped DAV as device is unreachable 6 (172.20.106.36) telnet (172.20.106.171 telnet Skipped DAV as device is unreachable (172.20.108.17C telnet Skipped DAV as device is unreachable 8 Skipped DAV as device is unreachable 9 (172.20.106.135 telnet 10 (172.20.108.231 telnet Skipped DAV as device is unreachable 11 1172 18 179 12¢ telnet Skipped DAV as device is unreachable Page 1 of 2 🕨 🔰 Displaying 1 - 50 of 75 < Previous Finish Help Export Report.

Figure 7-18 Device Access Verification - Results

Go back to CSPC Flow Chart

Device Prompt Collection

I

You can use Device Prompt Collection option to collect the Device Prompt and DNS Names for the devices that are selected.

Follow the steps given below to perform device prompt collection:

- Step 1 Select the devices for, which device prompts needs to be collected
- Step 2 Enter the Job name, Job Description, and select the Service Name from drop down to create a job for collection.
- Step 3 Start the job now or schedule it at a later time



Figure 7-19 Select Devices for Prompt Collection

Device Prompt Collection		×
Device Prompt Collection Schedule Options		
Job Details * Job Name: Job Description:		
Service Name:	NOS OPTIMIZATION	
Start Device Prompt Collection Now Schedule Device Prompt Collection	ASCNA	
No schedule configured		
Configure Schedule		
	< Previous Finish Help Close	

Figure 7-20 Create a job for prompt collection

To Schedule Device Prompt Collection at a later time, select Schedule Device Prompt Collection option and then click Configure Schedule button. You can schedule Start and End Date/Time or select the Recurrence pattern as Minutely, Daily, Weekly, Monthly, or Yearly as shown in Figure 7-21.

Γ

<i>Figure 7-21</i> onfigure Schedule	Configure Schedule	×
Range of Recur	irrence	
Schedule St	itart Date/Time April 21,2021	
Schedule En	No end date nd Date/Time End by April 21,2021 17:38	
Recurrence Patt	ttern	
Minutely	Every minutes.	
O Monthly		
	OK	Cancel

Once the job is started you can view the successful and failed collection for a given device as shown in Figure 7-22.

		,	Job Completed	
No	Device	Terminal Port	DNS Name	Status
1	WLCUCM86P		WLCUCM86P	Failed to collect the prompt data. Successfully c.
2	😂 L15		L15	Failed to collect the prompt data. Successfully c.
3	🚱 D15		D15	Failed to collect the prompt data. Successfully c.
4	🚱 L16		L16	Failed to collect the prompt data. Successfully c.
	Informa	ation Successfully com Job.	pleted the Device	Prompt Collection
	Informa	ation Successfully com Job.	pleted the Device OK	Prompt Collection

Figure 7-22 Prompt Collection Job in Action

Common Tasks

You can use the Common Tasks sub tab of the Management Tasks tab to execute a selected collection profile. Collection Profiles are described in the Collection Rules and Miscellaneous Rules chapters.

This section describes the Data Collection options in the following topics:

- Collect Data
- Upload Data
- Adhoc Data Collection
- Collect Application Data

Collect Data

You can select any collection profile from the list of collection profiles defined and run it as needed. Select the profile and click **Finish** button to run the profile.

Figure 7-23 Select the Collection Profile

ollection Profile			
lect Collection Pr	ofile		
ame	Schedule	Device Selection	Dataset Collection
IOS Full	0	All Devices Selected	282
105 Minimum	8	All Devices Selected	180
NTC	8	All Devices Selected	8
est_1_NOS Minimu	m 🔞		

Once you start the job, the results are displayed including device name, IP address, and success or failure, as shown below.

Γ

Selected Devices:0 Completed Devices:3 Address Host Name Message 15.10.1.2 D15 Inventoried 15.10.1.2	
lp Address Host Name Message	
15 10 1 2 D15 Inventoried 15 10 1 2	
16.10.1.1 L16 Inventoried 16.10.1.1	
15.10.1.1 L15 Inventoried 15.10.1.1	

Figure 7-24 Executed Data Collection Profile Results

Upload Data

Run Upload Profile screen lists all the profiles created using Manage Upload Profiles. You can select a profile from Run Upload Profile screen and click **Finish** to start uploading the profile.

Note

This feature is only for NOS services

		×
Lock Status	Schedule	
G UnLocked	9	
G UnLocked	\otimes	
G UnLocked	\bigcirc	
	< Previous Fi	nish Close
	Lock Status	Lock Status Schedule CULLOCKED

Job Progress screen showing the status of the uploaded profile is displayed as shown in Figure 7-26.

	Job Comp	leted
Job Status: Success Export Location: _NOS/79 Other Details: CSP0007	9_1 1040009: SUCCESS	3
Phase Name	Phase Status	Message
Phase Name INITIALIZING	Phase Status	Message
Phase Name INITIALIZING SELECTING_DEVICES	Phase Status SUCCESSFUL SUCCESSFUL	Message 67 devices selected
Phase Name INITIALIZING SELECTING_DEVICES SEGMENTING	Phase Status SUCCESSFUL SUCCESSFUL SUCCESSFUL	Message 67 devices selected
Phase Name INITIALIZING SELECTING_DEVICES SEGMENTING EXPORTING (CSP0001040009)	Phase Status SUCCESSFUL SUCCESSFUL SUCCESSFUL SUCCESSFUL	Message 67 devices selected transport-inventory-CSP0001040009-15468446
Phase Name INITIALIZING SELECTING_DEVICES SEGMENTING EXPORTING (CSP0001040009) UPLOADING (CSP0001040009)	Phase Status SUCCESSFUL SUCCESSFUL SUCCESSFUL SUCCESSFUL SUCCESSFUL	Message 67 devices selected transport-inventory-CSP0001040009-15468446 SUCCESS

Figure 7-26 Job Results

The status is shown in orange color if the upload is running, in green if the upload is successful and in red color if the upload failed.

If any of the phase status is failure, you have to re-run the upload profile.

Go back to CSPC Flow Chart

Γ

Ad hoc Data Collection

You can create adhoc collection profile if you want some devices to be configured to collect data based on the datasets.

In general, a collection profile will be associated with a set of devices. This means when you run collection profile, collection will be performed on devices associated with this collection profile definition.

If you wants to run a collection profile for a different set of devices other than what is present in the profile definition, an ad hoc collection profile serves this purpose.

When you create ad hoc collection profile, select:

- A base collection profile
- · Device details
- · Scheduling information

Ad hoc collection profiles inherit collection details (like data sets) from a given base collection profile. It inherits all the details except device details and scheduling information.

On clicking "Create Ad hoc Data Collection Profiles", screen as shown in Figure 7-27 is displayed.

Figure 7-27 Ad hoc Collection Select Devices

All managed devices Only the following selected devices		
Managed Devices:	Selected Devices/Gr	oups:
20		
LiveNodes (b)		
Video		
StoreseNetworking	=	
UnifiedCommunications	(t)	•
CollaborationEndpoints	*	
0 📸 SuccessfulDevGrp (1)		
CpticalNetworking		
R CloudandSystemsManagement		
R Wireless		
R Hubs	•	
Upload Nodes From File(.txt):	Browse	
	HOROS HE HIL	

Enter the mandatory details under the following two sections:

- Select Devices
- Profile Details

In Select Devices you can select all managed devices or only few devices. You can also browse to upload list of nodes from .txt file. Profile Details you can add the mandatory details as shown in Figure 7-28.

Figure 7-28 Ad hoc Collection Profile Details

Select Devices Profile Details			
* Profile Title:	TestAdhoc		
* Identifier:	_TestAdhoc	Generate	
* Base Collection Profile:	NOS Full	v	
Schedule Start Date/Time	Wed, Apr 21, 2021 21:29:00		

Note

I

If configure schedule is not provided, then ad hoc collection profile will be scheduled as soon as it is created.

The drop down box beside "Base Collection Profile" lists all the collection profiles present in the CSPC. You need to select a collection profile as a base collection profile. It is mandatory to select a base collection profile.

Configure schedule can be used to schedule ad hoc collection at a specified time and can be repeated at certain intervals by giving the required details.

<i>igure 7-29</i> nfigure Schedule	Configure S	chedule					
Range of Recurrence	ence						
Schedule Sta	rt Date/Time Af	ril 21,2021		17 : 35 🗘	Repeat sche	edule	
Schedule End	I Date/Time	o end date	21,2021	1	7:38		
Recurrence Patte	m						
Minutely							
🔘 Daily							
O Weekly							
O Monthly							
🔘 Yearly							
						OK	Cancel

Click **OK** to save the Profile and device details to the ad hoc collection profile. On successful completion, you will receive a message as shown in Figure 7-30.

Figure 7-3	0 Confirmation Message
User Edit	or
(į)	The Adhoc collection profile(JobId = 19) was scheduled successfully.
	OK

The ad hoc collection profile created will appear in the Manage Data Collection Profiles tab.

Collect Application Data

ſ

Run Application Profile shows the list of application profiles. You can select any application profile from the list of application profiles defined and run it as needed. Select the profile and click **Finish** to run the profile.

Figure 7-31 Run Application Profile

 Run Application Profile

 Select Application Profile

 Name
 Title

 apd
 apd

 UnLocked
 Image: Close

Once you start the job, the results are displayed including IP address, Host Name and success or failure, as shown in Figure 7-32.

Job Progress Job Completed Selected Devices:1 Completed Devices:1 Inventoried 10.77.240.132 1 10.77.240.132 PE-M40e Inventoried 10.77.240.132									
Job Completed Selected Devices:1 Completed Devices:1 No Ip Address Host Name Message 1 10.77.240.132 PE-M40e Inventoried 10.77.240.132									
Job Completed Selected Devices:1 Completed Devices:1 No Ip Address Host Name Message 10.77.240.132 PE-M40e Inventoried 10.77.240.132 IV Page 1 of 1 IV Displaying 1-									
Selected Devices:1 No Ip Address Host Name Message 1 10.77.240.132 PE-M40e Inventoried 10.77.240.132									
No Ip Address Host Name Message 1 10.77.240.132 PE-M40e Inventoried 10.77.240.132									
No Ip Address Host Name Message 1 10.77.240.132 PE-M40e Inventoried 10.77.240.132									
1 10.77.240.132 PE-M40e Inventoried 10.77.240.132 Image: The state of the sta									
Image Of 1 Image Displaying 1 -									
4 4 Page 1 of 1 ▶ ▶ Displaying 1 -									

Figure 7-32 Executed Application Collection Profile Results

Job Run Status

Job Run Status

This helps you to know the status of all the jobs you run. In addition, you can see the description of each job by clicking the + symbol next to the *Job Id*. Clicking the + sign shows the *Run Id*, *State* (Successful/Aborted), *Status* (Completed/Not Completed), *Start Time*, *End Time*, and *Job Log Details* for this particular job, as shown in Figure 7-33.

ΊĮ	zure	e 7 - 33		Job run Si	tatus							
Job I	Run Statu	15 (X)										
9	₽ ‡ ₽ ;	Q		× → 0								
J	ob Id	Job Type		Job Name		Runs	State(Latest)	Status(Latest)	Start Time(Latest)	End Time(Latest)	Next Schedule Time	
1 8	1	Discovery		Discover Devices147685164787	8	1	Completed	Success	Wed, Oct 19, 2016 10:04:07 +0530	Wed, Oct 19, 2016 10:04:08 +0530		
	Run Id	State Stat	tus St	tart Time	End Time		Action					
	1	Completed Su	iccess V	Ved, Oct 19, 2016 10:04:07	7 +0530 Wed, Oct 19, 20	016 10:04:0	08 +0530 Select Act	ion •				
							View	Job Log Details				
7	8.	DAV		smartcare_minCP_1476809633	465_Dav_1476809661618	1	Comple	altab	Tue, Oct 18, 2016 22:24:21 +0530	Tue, Oct 18, 2016 22:25:13 +0530		
6	i.	Discovery		smartcare_minCP_1476809633	465_Discovery_1476809636575	1	Completera	Juccess	Tue, Oct 18, 2016 22:23:56 +0530	Tue, Oct 18, 2016 22:24:17 +0530		
5	Č.	Data Collection		smartcare_minCP_1476809633	465	1	Completed	Success	Tue, Oct 18, 2016 22:23:53 +0530	Tue, Oct 18, 2016 22:26:57 +0530		
4		DAV		seed_Dav_1476807006730		1	Completed	Success	Tue, Oct 18, 2016 21:40:06 +0530	Tue, Oct 18, 2016 21:40:58 +0530		
3		Discovery		seed_Discovery_147680698143	9	1	Completed	Success	Tue, Oct 18, 2016 21:39:41 +0530	Tue, Oct 18, 2016 21:40:05 +0530		
2	6	Seedfile Import		seed		1	Completed	Success	Tue, Oct 18, 2016 21:39:40 +0530	Tue, Oct 18, 2016 21:41:01 -0530		

Select the *Action* button in the report to view either the Job Log details for this particular job, or to cancel a job while it is still running.

Figure 7-34 shows the job log details.

Figure 7-34	Job Log Details	
Log Messages fo	r the Job 91/1	×
Message		
All Devices (1) s	elected.	
Protocols Selecte	ed: telnet	
5.0.1.38 (telnet)	: Successful with credential '5.0.1.38_telnet'	
Device Access	Verification Job completed with Status: Success	
Updating device	working credentials.	
Updating device	working credentials.	

Job Management

Use the Job Management sub tab of the Management tasks to retrieve Job information. The job information can also be exported to an output file. The currently supported file formats are PDF, HTML, DOC, CSV (Comma delimited), TXT (Tab delimited).

This section describes the Job Management options in the following topics:

- Manage Discovery Jobs
- Manage Device Access Verification Jobs
- Manage Workflow Jobs
- Manage Configuration Jobs
- Manage Device Prompt Collection Jobs
- Manage Health Monitor Jobs

Manage Discovery Jobs

I

Manage Discovery Jobs provides a list of all the discovery jobs previously run, and provides you with an option to either export the job information or delete job information from the database as shown below.

C Q	× CRemove Job	0		
Job Id	Job Name	Created By	Description	Created On
1	Discover Devices1348651452504	system		Wed, Sep 26, 201
2	Discover Devices1348651805031	sys C Refresh		Wed, Sep 26, 201
3	Discover Devices1348651855166	adır 🕦 Help		Wed, Sep 26, 201
4	Discover Devices1348652079990	adn		Wed, Sep 26, 201
5	Discover Devices1348652251311	adır 🗢 Remove	Job	Wed, Sep 26, 201
6	Discover Devices1348652403611	adm 💟 Export		Wed, Sep 26, 201
7	Discover Devices1348652611816	admin		Wed, Sep 26, 201
18	Discover Devices1348673234040	admin		Wed, Sep 26, 201
34	Discover Devices1348728871253	admin		Thu, Sep 27, 201
38	Discover Devices1348730047836	admin		Thu, Sep 27, 201
46	Discover Devices1348730680929	admin		Thu, Sep 27, 201
50	Discover Devices1348730997841	admin		Thu, Sep 27, 201
51	Discover Devices1348732076984	admin		Thu, Sep 27, 201
52	Discover Devices1348732615240	admin		Thu, Sep 27, 201
66	Discover Devices1348741516989	admin		Thu, Sep 27, 201
67	Discover Devices1348741574537	admin		Thu, Sep 27, 201
70	Discover Devices1348746566737	admin		Thu, Sep 27, 201
A A Page	1 of 3 🕨 🔰			Displaying 1 - 50 of 13

Manage Device Access Verification Jobs

Manage Device Access Verification Jobs provides a list of all the device verification jobs previously run, and provides you with an option to either export the job information or delete job information from the database as shown below.

Γ

C Q	× 🔾 Remove Jo	b 🖸 🚺			
Job Id	Job Name	Created	Ву	Description	Created On
8	telnrt	admin			Wed, Sep 26, 201
9	re	admin	a n	-feeb	Wed, Sep 26, 201
10	2	admin	GR	eiresn	Wed, Sep 26, 201
11	3	admin	Он	elp	Wed, Sep 26, 201
19	wer	admin		emove Joh	Wed, Sep 26, 201
20	ert	admin		chove soo	Wed, Sep 26, 201
35	12	admin	E E	xport	Thu, Sep 27, 201
39	123	admin			Thu, Sep 27, 201
47	4	admin			Thu, Sep 27, 201
48	5	admin			Thu, Sep 27, 201
53	566	admin			Thu, Sep 27, 201
54	45	admin			Thu, Sep 27, 201
71	456	admin			Thu, Sep 27, 201
86	dav1	cspcad	min		Fri, Sep 28, 2012
87	safg	cspcad	min		Fri, Sep 28, 2012
91	122	admin			Fri, Sep 28, 2012
96	13	admin			Fri, Sep 28, 2012

Figure 7-36 Manage Device Access Verification Jobs

Manage Workflow Jobs

Manage Workflow Jobs provides a list of workflow jobs that are previously run, and provide you with an option to either export the job information or delete the job information from the database as shown below.

Manage Work	flow Jobs 🖲			
0 Q	× 🕞 Remove Job	• 0		
Job Id	Job Name	Created By	Description	Created On
51	CollectionExportWorkFlowJob	system	 Refresh Help Remove Job ⇒ Export 	Fri, May 3, 2013 02





ſ

Manage Configuration Jobs provides a list of all the device configuration jobs previously run, and provides you with an option to either export the job information or delete job information from the database as shown below.

Figure 7-38 Manage Configuration Jobs 🗵 C Q .-× 🔾 Remove Job 💟 🛈 Job Id Description Created On Job Name Created By 74 Thu, Sep 27, 2012.. 1 admin 75 2 Thu, Sep 27, 2012... admin 76 3 Thu, Sep 27, 2012... admin C Refresh 77 4 Thu, Sep 27, 2012... admin 78 1 Help Thu, Sep 27, 2012... 5 admin 79 6 admin Thu, Sep 27, 2012 Remove Job 80 7 Thu, Sep 27, 2012... admin Export 81 8 Thu, Sep 27, 2012... admin 82 Thu, Sep 27, 2012... 9 admin 83 10 Thu, Sep 27, 2012... admin 84 11 Thu, Sep 27, 2012... admin 85 12 Thu, Sep 27, 2012... admin Displaying 1 - 12 of 12 14 4 Page 1 of 1 🕨 🕅



Manage Device Prompt Collection Jobs

Manage Device Prompt Collection Jobs provides a list of all the device prompt collection jobs previously run, and provides you with an option to either export the job information or delete job information from the database as shown in Figure 7-39.

The jobs info can also be exported to an output file. The currently supported file formats are PDF, HTML, DOC, CSV (Comma delimited), TXT (Tab delimited)

d d	× 📿 Rer	nove Job 🔛 🚺		
Job Id	Job Name	Created By	Description	Created On
192	test	admin		Mon, Oct 8, 2012.
		C rencon		
		Help Remove Job Export		

Manage Health Monitor Jobs

Health Monitor Jobs provides a list of all the monitor jobs previously run, and provides you with an option to either export the job information or delete job information from the database.

Health Monitor job which comes as part of NOS configure installation. This is a daily scheduled job. A user cannot alter or create a scheduled health monitor job from GUI/CLI. The screen shot of health monitor job after installation is shown in Figure 7-40. The jobs information can also be exported to an output file. The currently supported file formats are PDF, HTML, DOC, CSV (Comma delimited), TXT (Tab delimited)



I

This feature is only for NOS services



Job run details can also be viewed from **Reports** -> **Job Management Reports**. From the drop down select Health Collection jobs and click **OK** as shown in Figure 7-41.

Manage Heal	th Monitor Jobs 🛞			
0 Q	× 🕞 Remove Job 🔿	0		
Job Id	Job Name	Created By	Description	Created On
6	NOS_HealthMonitor_Job	nosadmin		Mon, Mar 25, 2013
	Select Job Parameters Job Group Type Health Collection J	ок с	ancel	
14 4 Page	of1 ▶ ₽∥			Displaying 1 - 1 of

Figure 7-42 Health Collection Jobs

2		Q		×	i)						
9	Job Id	Job Name	Job Descript	Created	Created On	Modifie	Modified On	First Run Time	Last Run Time	Run	Next Schedule T
3	6	NOS_Health		nosadmin	Mon, Mar 25, 20			Tue, Mar 26, 20	Tue, Mar 26, 20	1	Wed, Mar 27, 20

In Figure 7-42 you could see Job Id, Job Name, Created By, Created On, Modified By, Modified On, First Run Time, Last Run Time, Run Count, Next Scheduled Time. On the screen, there is no option from where the job could be triggered manually.

I

There are two CLI's using which this could be achieved. The CLIs are listed below:

- job_schedule_healthMonitor_runnow.sh
- show_settings_healthMonitor_jobparameters.sh

Using show_settings_healthMonitor_jobparameters.sh you could view any health monitor job parameters and the first CLI, job_schedule_healthMonitor_runnow.sh is used to create a run now job. It expects 4 parameters. Figure 7-43 shows the view health monitor job parameters from CLI.





A new health monitor runnow job can be scheduled from CLI as shown in Figure 7-43.

CLI Command		
B administrator@nosdev-229	/opt/CSPC/cli/components/2.2/cli/bin/linux	
now.sh ./ [root@nosdev-229 linu Details true IncludeC	x]# sh job_schedule_healthMonitor_runnow.sh jobname test_health_r ollectorLogs true IncludeAddOnHealth true UploadData true	unnow IncludeSystem
Schedule successfully	created:	
Column	Data	
JobName	test health runnow	
JobType	HealthMonitorJobGroup	
JobId.		
JobRunId		
[root8nosdev-229 linu	×1#	
[root@nosdev-229 linu	×] #	
[root@nosdev-229 linu	×]#	
[root@nosdev-229 linu	×]#	
[root@nosdev-229 linu	×]#	1.00
[root8nosdev-229 linu	×]#	
[root@nosdev-229 linu	×]# 🧧	-



Applications - Reports

Reports

Use the Reports tab to view the collected data and job log details for discovery, inventory, collection, and backup jobs.

This section describes the Reports options in the following topics:

- Device Reports
- Device Access Verification Reports
- Data Collection Reports
- Services Reports
- Job Reports
- Audit Trails
- Miscellaneous

All the reports can be exported to various formats such as HTML, Microsoft Word, PDF, CSV, and TXT formats, along with various graphing options. Each report is easy to navigate with filtering and report formatting options.

Device Reports

Use the Device Reports sub tab to view the collected data for the selected devices. This section describes the Reports options in the following topics:

- View Managed Devices
- View Unreachable Devices
- View Duplicate Devices
- Discovery Report
- Device Display Properties
- Non SNMP Devices
- Interface Summary (IOS, PIX, ASA, IOS-XR)

View Managed Devices

I

Discovered Devices report shows all the devices that have been discovered and managed, along with their respective details such as IP Address, Host Name, Sys Object Id, Device Family, Product Model, Serial Number, Vendor Name, OS Name, OS Version, Discovery date and time, Source, and Reachable. The report can be exported to various formats such as HTML, Microsoft Word, PDF, CSV, and TXT formats, along with various graphing options. The report is easy to navigate with filtering and report formatting options.

Figure 8-1	View Managed Devices
------------	----------------------

View Manage	ed Devices (*												
0 9.		× - 1. 0											
Ip Address	Host Name	Display Name	Sys Object Id	Device Family	Product Model	Serial Number	Vendor Name	O5 Name	OS Version	Discovery Date/Time	Source	Reachable	
5011	Device_5_0_1_1	Device_5_0_1_1	13614191	ApplicationN	cascoCe560		Cisco System	ACN5	5.5.5	Fri, Sep 2, 2016 08:35:36 +0	Collector	0	-
5.0.1.2	Device_5_0_1_2	Device_5_0_1_2	13614191	ApplicationN	ciscoACE4710K9	5012	Cisco System	ACSW		Fri, Sep 2, 2016 08:35:36 +0	Collector	0	
5.0.1.3	Device_5_0_1_3	Device_5_0_1_3	13614191	Security	ISE-3395-K9	Device_5_0_1_3	Cisco System	ADE-05	2.0	Fri, Sep 2, 2016 08:35:36 +0	Collector	0	
5.0.1.4	Device_5_0_1_4	Device_5_0_1_4	13.614130	Security	vpvClientRev1		Altiga Netwo	AltigaO5	41.3.Rel	Fri, Sep 2, 2016 08:35:36 +0	Collector	0	
5.0.3.5	Device_5_0_1_5	Device_5_0_1_5	13614195	LANSwitches	W5-C2948	5015	Cisco System	CatO5	8.4(11)GLX	Fri, Sep 2, 2016 08:35:36 +0	Collector	0	11
5.0.1.6	Device_5_0_1_6	Device_5_0_1_6	13614195	LAN5sritches	wsc5505sysID		Cisco System	CatO5	4.5(13a)	Fri, Sep 2, 2016 08:35:37 +0	Collector	0	
5.0.1.8	Device_5_0_1_8	Device_5_0_1_8	.136.14.19.1	Video	ISM	5018	Cisco System	CDS-IS	2.5.11	Fri, Sep 2, 2016 08:35:37 +0,	Collector	0	
5.0.3.10	Device_5_0_1_10	Device_5_0_1_10	13614191	UnifiedCom	daceDPA7630		Cisco System	DPA	1.2(1)	Fri, Sep 2, 2016-08:35:37 +0	Collector	0	
5.0.1.11	Device_5_0_1_11	Device_5_0_1_11	13614191	Video	direeMDE10XVB		Cisco System	ECD5	2.5.5	Fri, Sep 2, 2016 08:35:37 +0	Collector	0	
5.01.12	Device_5_0_1_12	Device_5_0_1_12	13614191	Security	ciscoWsSvcFwm1sc		Cisco System	FWSM-O5	4.1(8)1	Fri, Sep 2, 2016 08:35:35 +0	Collector	0	
5.0.1.13	Device_5_0_1_13	Device_5_0_1_13	13.61.41.9.5	LANSwitches	wac1900sysID		Cisco System	G105	9.00.07	Fri, Sep 2, 2016 08:35:35 -0	Collector	0	
5.01.14	Device_5_0_1_14	Device_5_0_1_14	13614191	ApplicationN	dacoG55		Cisco System	GS5		Fri, Sep 2, 2016 08:35:35 +0	Collector	0	
5.0.1.15	Device_5_0_1_15	Device_5_0_1_15	13614191	Routers	CI5C03845	50115	Claco System	105	12.4(20090203	Fri, Sep 2, 2016 08:35:35 +0	Collector	0	
5.0.1.16	Device_5_0_1_16	Device_5_0_1_16	13614191	Routers	cisco10005	Device_5_0_1_16	Cisco System	105	12.0(25)5X10	Fri, Sep 2, 2016 08:35:36 +0	Collector	0	
5.0.1.17	Device_5_0_1_17	Device_5_0_1_17	13614191	Routers	73-2587-1 rev 80 dev 0	Device_5_0_1_17	Cisco System	105	12.0(32)5Y2e	Fri, Sep 2, 2016 08:35:36 +0	Collector	0	
5.0.1.18	Device_5_0_1_18	Device_5_0_1_18	13614191	Routers	cisco4500	Device_5_0_1_18	Cisco System	105	11.3(11a)	Fri, Sep 2, 2016 08:35:36 +0	Collector	0	
5.0.1.19	Device_5_0_1_19	Device_5_0_1_19	13614191	Routers	CI5CO7206	Device_5_0_1_19	Casco System	105	12.4(25c)	Fri, Sep 2, 2016 08:35:36 +0	Collector	0	

All these reports also provide various graphing options along with a device product family graph as shown in Figure 8-2.



<u>II.</u> -	0
<u>lı.</u>	Network Summary by Device Family
¢	Network Summary by Product Model
¢	Network Summary by Vendor Name
¢	Network Summary by OS Name



Go back to CSPC Flow Chart

View Unreachable Devices

All the devices that are unreachable and are not detected while performing discovery are shown in this report. This report provides the details like host name, IP address, reason, Manage status and discovery time for each unreachable device.

To perform the rediscovery of the device, right click on any device and select Start Discovery Job option. You can also delete any unreachable device or all unreachable devices by clicking **Delete Unreachable Device** or **Delete All Unreachable Device** button respectively.

Figure 8-4	View Unro	eachable Devices			
View Unreachable	Devices ×				
0 Q.	×	👄 🔵 Delete Unreachable Devices 🥥 Delete All Unreachable De	evices 🛛 🔘		
Host Name	IP Address	Reason	Managed	Discovery Time	
Device_Unreach	172.21.54.143	172.21.54.143 : SNMP Unreachable or Incorrect SNMP Credentials.	9	Tue, Oct 18, 2016 22:24:16 +0530	
11.1.1.1	11.1.1.1	11.1.1.1 : SNMP Unreachable or Incorrect SNMP Credentials.	9	Tue, Oct 18, 2016 22:24:16 +0530	
1.2.2.4	1.2.2.4	1.2.2.4 : SNMP Credentials Not Set.	9	Wed, Oct 19, 2016 10:04:06 +0530	

View Duplicate Devices

I

All the devices that are duplicate are shown in this report as shown in Figure 8-83. This report provides the details such as device name, Managed by, and Details of the device.

View Duplicate	Devices 🗵		
0 Q+	×	→ (i)	
Device Name	Managed By	View Details	

Discovery Report

All the devices that are discovered are shown in this report. This report provides the details like host name, IP address, Credential name, Status and Protocol for each discovered device.

Figure 8-6 Discovery Report

Discovery Report					
0 Q.	× → 0				
IP Address	Host Name	Credential Name	Status	Protocol	
5.0.1.12	Device_5_0_1_12	5.0.1.12_snmpv3	Device already in managed state	SNMPv3	^
5.0.1.13	Device_5_0_1_13	5.0.1.13_snmpv3	Device already in managed state.	SNMPv3	
5.0.1.14	Device_5_0_1_14	5.0.1.14_snmpv3	Device already in managed state.	SNMPv3	
5.0.1.15	Device_5_0_1_15	5.0.1.15_snmpv3	Device already in managed state.	SNMPv3	
5.0.1.16	Device_5_0_1_16	5.0.1.16_snmpv3	Device already in managed state.	SNMPv3	
5.0.1.17	Device_5_0_1_17	5.0.1.17_snmpv3	Device already in managed state.	SNMPv3	
5.0.1.18	Device_5_0_1_18	5.0.1.18_snmpv3	Device already in managed state.	SNMPv3	
5.0.1.19	Device_5_0_1_19	5.0.1.19_snmpv3	Device already in managed state.	SNMPv3	

Device Display Properties

Device Display Properties report shows the display properties configured for all the devices. In addition, from this window you can configure display property for a specific device or a group of devices. You can assign a specific name for a device property such as Host Name, IP Address, DNS Name, Primary Device name and so on.

Figure 8-7	Device Display	Properties

Device Display	Properties (8)										
0 Q	×	+ 0									
Device	Display Type	Custom Name	Ip Address	Host Name	Terminal Prompt	DNS Name	Sys Name	Sys Object Id	Mac Address	Primary De	vice Name
Oevice_	_0_1_3!		5.0.1.35	Device_5_0_1_35			Device_5_0_1_35	13.6.1.4.1.9.12.3.1.3		5.0.1.35	
📢 Device_5	_0_1_3(5.0.1.36	Device_5_0_1_36			Device_5_0_1_36	.1.3.6.1.4.1.9.12.3.1.3		5.0.1.36	
Device_5	_0_1_3(Host Name		5.0.1.30	Device_5_0_1_30			Device_5_0_1_30	13.6.1.4.1.9.1.662		5.0.1.30	
Oevice_5	_0_1_3:		5.0.1.31	Device_5_0_1_31			Device_5_0_1_31	13.6.1.4.1.903.100.2		5.0.1.31	
🔮 Device_5	_0_1_3; Host Name		5.0.1.32	Device_5_0_1_32			Device_5_0_1_32	13614191404		5.0.1.32	Ξ
Device_5	0_1_3 Host Name		5.0.1.3	Device_5_0_1_3			Device_5_0_1_3	136141911424		5.0.1.3	
Oevice_5	_0_1_3; Host Name		5.0.1.37	Device_5_0_1_37			Device_5_0_1_37	1.3.6.1.4.1.3607.1.20		5.0.1.37	
Oevice_	_0_1_2 Host Name		5.0.1.2	Device_5_0_1_2			Device_5_0_1_2	.1.3.6.1.4.1.9.1.824		5.0.1.2	
Oevice_5	_0_1_4, Host Name		5.0.1.44	Device_5_0_1_44			Device_5_0_1_44	136141351110		5.0.1.44	
Oevice_5	_0_1_4! Host Name		5.0.1.45	Device_5_0_1_45			Device_5_0_1_45	1.3.6.1.4.1.9.1.458		5.0.1.45	
Oevice_5	_0_1_4(Host Name		5.0.1.40	Device_5_0_1_40			Device_5_0_1_40	13.6.1.4.1.5655.1.3		5.0.1.40	
🔮 Device_5	0_1_4		5.0.1.41	Device_5_0_1_41			Device_5_0_1_41	13.6.1.4.1.8164		5.0.1.41	

Right click on any listed device and select *Edit Properties* option to add a custom name to the display properties of the device. The settings configured locally will override the global settings.

Γ

Figure 8-8	Edit Device Display Properties	
	Edit Device Display Properties	×
	Select a display property for the selected device(s)	
	Display Property: User Defined Name	
	Enter a custom display name for the selected device	
	Custom Name: Juni	
	Help OK Cancel	

Interface Summary (IOS, PIX, ASA, IOS-XR)

Interface Summary report displays the list of all the interfaces available in CSPC.

: 🙌 타 만 🖓	C Q	×							
Calibration of the second seco	Node	Interface Name	MAC Address	Ip Address	Net M	MTU (Spee	Line	Proto.
etatic (19)	😵 sts-nat1760-1	Fa0/0	000c.ce05.b835	172.21.54.131		-1	-1	up	up
🥰 Voice	😵 sts-nat1760-1	Lo0		10.10.10.21		-1	-1	up	up
🖓 VoiceGateways (2)	🔗 sts-nat1760-1	Lo1		1.1.1.21		-1	-1	up	up
Video (1)	😵 sts-nat1760-1	Nu0				-1	-1	up	up
Storage (1)	🎯 ciscoasa	Ethernet0/0	0000.0000.0000			-1	-1	up	down
Telepresence (2)	🔮 ciscoasa	Ethernet0/3	0000.0000.0000			-1	-1	up	down
Coptical (1)	🌒 ciscoasa	inside	0013.c480.7a1f	192.168.100.1		-1	-1	up	up
The workManagement (1)	Ciscoasa	manage	0013.c480.7a20	10.78.177.39		-1	-1	up	up
WinfiedCommunications (2) ServiceReadyPlatform Routers (16) LiveNodes (67) ApplicationNetworking (4) Switches (13)									

Figure 8-10	Interface Summary
-------------	-------------------

Interface Summary data can be also seen in a graphical format, clicking on graphics icon following options:



- Interface Status Summary
- Interface IP Address Summary
- Interface Type Summary

Device Access Verification Reports

- Device Access Verification Summary
- Device Access Verification By Dataset Type
- View Access Verification Results

Device Access Verification Summary

The Device Access Verification Summary report provides summary of the access verification. This report provides high level overview of the types of protocols used, and number of devices either succeeded or not along with number of devices that are not verified. This is shown in Figure 8-11.

Verification Protocol	Number of Devices Passed	Number of Devices Failed	Number of Devices Unverified					
teinet	3873	1127	1					
sshv1	0	5000	1					
sshv2	0	5000	1					
snmpv1	3835	1165	1					
snmpv2c	3836	1165	0					
snmpv3	0	5000	1					
http	0	5000	1					
https	0	5000	1					
wmi	0	5000	1					
ti1	1	5000	0					

Figure 8-11 Device Access Verification Summary

In Device Access Verification Summary, you can export the failed devices in CNC format. The data related to the selected filter type (Device, Protocol, Status and so on) and only failed credentials are exported as part of a seed file. This export option is supported for both manually added devices and devices added through seed file import.

Device Access Verification By Dataset Type

I

The Device Access Verification by Dataset Type shows the devices and whether they are support CLI, SNMP, SNM Configuration, SOAP, XML, WMI, FILE type protocols and files.

& Q	×							
Device	CLI	SNMP	SNMP_CONFIG	SOAP	XML	WMI	FILE	
Oevice_5_0_1_50	•		0	8	•	8	8	
Oevice_5_0_1_49	8		0	8	8	8	8	
Device_5_0_1_48	8	0	9	8	8	8	8	
Device_5_0_1_45	0	0	9	8	0	8	8	
Pevice_5_0_1_44	8	0	9	8	8	8	8	
Device_5_0_1_41	8	0	0	8	8	8	0	-
Device_5_0_1_53	8	0	0	8	8	8	0	
Device_5_0_1_40	8	0	0	0	8	8	0	
Device_5_0_1_37	0	9	0	0	0	8	8	
Device_5_0_1_35	8	0	0	8	8	8	8	
🔮 dc3qa-ind10	8	9	0	0	0	8	8	
Bevice_5_0_1_32	0	0	0	0	0	8	0	
Oevice_5_0_1_30	8	9	0	0	0	8	8	
2 Device_5_0_1_29	0		0	0	0	0	0	

Figure 8-12 Device Access Verification By Dataset Type

View Access Verification Results

The View Access Verification Report shows the latest device access verification results. It provides details on verification time and source of the verification (either part of discovery or a separate verification job) and the successful/failed protocol, Status of each protocol, Messages and status of each device, device combinations, and User defined fields. This is shown in Figure 8-13.

Figure 8-13 View Access Verification Report

9		0 9.	× → 0							
😪 LiveNodes (64)	^	Device	IP Address	Verification Time	SNMPV1	SNMPV2C	SNMPV3	TELNET	SSHV1	SSH
📢 Unreachable Nodes (3815)		Oevice_5_0_1_35	5.0.1.35	Thu, Jun 21, 2018 05:13:18	Skipped	Skipped	Successful	Skipped	Skipped	Suc A
😪 Hubs		A Denter 5 A 1 26	50136	Thu, Jun 21, 2018 05-13-18	Skinned	Skinned	Successful	Skinned	Skinned	Surr
🕞 Servers-UnifiedComputing (3)		Device_5_0_1_56	And And		andless	seeklee			see from	
🖓 ServiceExchange (1)		Device_5_0_1_30	5.0.1.30	Thu, Jun 21, 2018 05:13:18	Skipped	Skipped	Successful	Successful	Connection Failed	Con
A xDSL		Denin E 0 1 11	50131	Thu Jun 21 2018/05/13/17	Skinned	Skinned	Successful	Successful	Connection Failed	Con
GenericNetworkDevices		Device_0_0_1_01								
Routers (13)		Device_5_0_1_32	5.0.1.32	Thu, Jun 21, 2018 05:13:18	Skipped	Skipped	Successful	Successful	Connection Failed	Con
🖓 Switches		Device 5.0.1.3	5013	Thu, Jun 21, 2018 05-13-18	Skipped	Skipped	Successful	Successful	Connection Failed	Con
ATMSwitches (1)		- 01100-00-00								
RadeSwitches		Device_5_0_1_37	5.0.1.37	Thu, Jun 21, 2015 05:13:18	Skipped	Skipped	Successful	Successful	Connection Failed	Con
ConnectedGridSwitches		Device 5.0.1.2	5.0.1.2	Thu, Jun 21, 2018 05:13:18	Skipped	Skipped	Successful	Skipped	Skipped	Succ
CataCenterSwitches (2)				SR 93	355	100			1920	_
industrialEthernetSwitches		Device_5_0_1_44	5.0.1.44	Thu, Jun 21, 2018 05:13:18	Skipped	Skipped	Successful	Successful	Connection Failed	Con
infiniBandSwitches (1)		Device 5.0.1.45	5.0.1.45	Thu, Jun 21, 2018 05:13:18	Skipped	Skipped	Successful	Successful	Connection Failed	Con
CANSwitches (8)							2			-
MetroEthernetSwitches		Device_5_0_1_40	5.0.1.40	Thu, Jun 21, 2018 05 13 18	Skipped	Skipped	Successful	Successful	Connection Failed	Con
WANSwitches (5)		O Device_5_0_1_41	5.0.1.41	Thu, Jun 21, 2018 05-13-18	Skipped	Skipped	Successful	Skipped	Skipped	Succ
ApplicationNetworkingServices (4)		0	501/2	Thus Ison 21, 2018 05-12-18	Shinead	Shinead	Successful	Successful	Connection Earled	
Security (5)		Device_5_0_1_43		1100, Jun 23, 2010 03-13-10	contribution	ompres	Juccession	Juccessia	Connection ranea	CON
Video (4)		Device_5_0_1_48	5.0.1.48	Thu, Jun 21, 2015 05:13:17	5ldpped	Skipped	Successful	Successful	Connection Failed	Con
StorageNetworking (1)		(An. 1010)	50149	Thu Jun 21 2018/05/13/18	Skinned	Skinned	Successful	Successful	Connection Failed	Con
Conferencing (2)		Device_5_0_1_49	5.0.1.45	1110, Juli 11, 2010 00 15.10	Sabbea	papped	Juccessium	Succession	Connection Faired	V
Communications (4)		<		11						>
CollaborationEndpoints (2)		II I Prest at 2	6-16F						- Paristan and a second	

The intelligent search options are shown in this report as well. When you start typing "tel" to list only the Telnet credentials, the report only shows those entries that match the "tel" string you entered. As shown in the above screen, the search options are quite extensive, and you can search based on any field/value in the report. You can also specify wild cards, regular expressions, matching patterns, etc. This helps to pinpoint the data you are looking for in a fast and easy way.

Figure 8-14	Device Message
-------------	----------------

Message		×
Device_5_0_1_35		
Protocol	Message	
wmi	No credentials found	
tl1	No credentials found	
telnet	Skipped because other version of the protocol is passed	
sshv2		
sshv1	Skipped because other version of the protocol is passed	
snmpv3		
snmpv2c	Skipped because other version of the protocol is passed	
snmpv1	Skipped because other version of the protocol is passed	
iiop	No credentials found	
https	No credentials found	
http	No credentials found	

Go back to CSPC Flow Chart
Data Collection Reports

- View Collected Data
- View Collection Run Summary
- Config Collected Devices
- Config Data Per Device
- Export Detailed Device Data

View Collected Data

This report provides a summary of the completed collection profiles and the data that is collected while completing those collection profiles. You can view a specific completed collection profile data, export data to a report, look at job log status and delete the collected data.

Figure 8-15 Collection Profile Run Summary Main Window

0 Q.	× 🔿 V	iew IPHost Masked Valu	es 🕕			
Profile Name	State	Status	Start Time	End Time	Actions	View Data
NO5 Full	Completed	Successful	Fri, Aug 4, 2017 14:55:56	Fri, Aug 4, 2017 15:07:30	Select Action *	View Data
					View Data Export And Upload Data	
					View Device Collection Summary View Device Collection Details	
					View Tag Collection Summary View Tag Collection Details	
					View Job Log	
					Search Results	
					Delete Profile Executions View IPHost Masked Values	

You can select any row in the report, right click on it to get all the options associated with that row:

- View Data
- Export and Upload Data
- View Device Collection Summary
- View Device Collection Details
- View Tag Collection Summary
- View Tag Collection Details
- View Job Log
- Search Results

I

- Delete Profile Executions
- View IP Host Masked Values

When you select *View Data*, you are provided with the data collection profile run data viewer, as shown in Figure 8-16.

A	Selected Data Set : _CISCO-ENTIT	TY-ASSET-MIE_ceAssetTable						
EliveNodes (65)	Q.	x						
+ Page1 of 2 ▶ № 🐨 Disp	Dataset	Type Status Context	Command Er	TOF				
Device 5.0 1.29	1 CISCOLENTITY ASSET	OVMP Grow	CISCO-ENTITY-ASSET AU					
Oevice 5 0 1 33	2 CISCO-CDP-MIR odpCarbs	SNMP Succ	CISCO CDP MIR eduCache		=			
Oevice_5_0_1_34	3 CISCO-ENHANCED-ME	SNMP Succ	CISCO ENHANCED ME					
Router I	4 CISCO-FLASH-MIR cisco 5	SNMP Suce	CISCO FLASH MIR dates					
Device_5_0_1_36	5. CISCO-MEMORY POOL	SNMP Suce View Row Data	CISCO MEMORY POOL					
Device_5_0_1_39	6 ENTITY-MIB entPhysical	SNMF Succ	ENTITY MIB entPhysical					
Oevice_5_0_1_46								
Oevice_5_0_1_47	IN Pagel of 6 > >1			Displ	aying 1 - 50 of 26	3		
Device_5_0_1_42								
Oevice_5_0_1_55	Instance Id ceAssetTag ceA	ssetIsFRU ceAssetCLEI ceAssetAlus	ceAssetOrd ceAssetSeri ceAssetSoft	ceAssetFir		ceAssetMig	ceAssetHar ceAssetSoft	ceAssetFir
Device_5_0_1_44	1	000000000			01	68-3237-01	3.7.2.151	
Device_5_0_1_45	3	IPUCARJB		Version 1.0	10	68-3160-05	3.7.2.151	
Device_5_0_1_37	70	IPU3AEW		Version 1.0	17	68-3152-04	3.7.2.151	
G Device_5_0_1_40	.\$1	Methode Ele				00-0000-00	3.7.2.151	
S	73	CI5CO-AV				00-0000-00	3.7.2.151	
Device_20_0_1_14	13						223241	
Device_5_0_1_41	30	000000000			02	68-3238-02	3.7.2.151	
Device_5.0_1_41 Device_5.0_1_38	.30 .97	00000000 Methode Ele			02	68-3238-02	3.7.2.151	
Device_5_0_1_41 Oevice_5_0_1_41 Oevice_5_0_1_38 Oevice_5_0_1_43	30 97 89	00000000 Methode Ele Methode Ele			02	68-3238-02 00-0000-00 00-0000-00	3.7.2.151 3.7.2.151 3.7.2.151	
 Orrac, 20, 9, 1, 41 Orrac, 5, 0, 1, 41 Orrac, 5, 0, 1, 58 Orrac, 5, 0, 1, 58 Orrac, 5, 0, 1, 51 	30 97 89 113	00000000 Methode Ele Methode Ele CISCO-FINIS			02	68-3238-02 00-0000-00 00-0000-00 00-0000-00	3.7.2.151 3.7.2.151 3.7.2.151 3.7.2.151	
Device, 30,0,1,34 Device, 5,0,1,41 Device, 5,0,1,43 Device, 5,0,1,43 Device, 5,0,1,51 Device, 5,0,1,51	30 97 89 113 47	00000000 Methode Ele Methode Ele CISCO-FINIS 00000000			02 02	68-3238-02 00-0000-00 00-0000-00 00-0000-00 68-3238-02	3.72.151 3.72.151 3.72.151 3.72.151 3.72.151 3.72.151	
Derice, 5, 0, 1, 3	30 30 37 59 113 47 34	00000000 Methode Ele CISCO-FINIS 00000000 IPUCARIB			02 02 06	68-3238-02 00-0000-00 00-0000-00 00-0000-00 68-3238-02 68-3160-04	3.72.151 3.72.151 3.72.151 3.72.151 3.72.151 3.72.151	
Ories 2,0,0,1,4 Ories 2,0,1,4 Ories 2,0,1,4 Ories 2,0,1,4 Ories 2,0,1,4 Ories 3,0,1,4 Ories 3,0,1,4 Ories 3,0,1,4	30 30 37 59 113 47 244 137	00000000 Methode Ele CISCO-FINIS 00000000 IPUCARIB CISCO-FINIS			02 02 06	68-3238-02 00-0000-00 00-0000-00 00-0000-00 68-3238-02 68-3160-04 00-0000-00	3.7.2.151 3.7.2.151 3.7.2.151 3.7.2.151 3.7.2.151 3.7.2.151 3.7.2.151	
Devis 2,0,0,1,4 Devis 2,0,1,4 Devis 2,0,1,4	30 30 37 39 47 244 .137 244 .137	00000000 Methode Ele CISCO-ENIS 00000000 IPUCARIB CISCO-ENIS CISCO-ENIS			02 02 06	68-3238-02 00-0000-00 00-0000-00 68-3238-02 68-3160-04 00-0000-00 00-0000-00	372181 372191 372191 372191 372191 372191 372191 372191 372191	
Oreins, 20,0,1,14 Oreins, 20,0,1,14 Oreins, 5,0,1,55 Oreins, 5,0,1,55 Oreins, 5,0,1,45 Oreins, 5,0,1,45 Oreins, 5,0,1,45 Oreins, 5,0,1,45 Oreins, 5,0,1,15	30 30 37 59 113 47 244 137 121 105	0000000 Methode Ele CISCO-FINIS 0000000 IPUCARIS CISCO-FINIS CISCO-FINIS CISCO-FINIS			02 02 06	68-3238-02 00-0000-00 00-0000-00 68-3238-02 68-3160-04 00-0000-00 00-0000-00 00-0000-00	37218 37219 37219 37219 37219 37219 37219 37219 37219 37219	

Figure 8-16 Collection Profile Run Data Viewer

Once you select a specific dataset the output of the dataset along with, if the data collection is successful or not appears (command status). The Command Status is shown as one of these states:

- Successful
- Failed
- Not Applicable

To see the dataset properties right click on a dataset and click View Row Data.

Figure 8-17	View Row Data
-------------	---------------

Dataset Properties		×
∃ 3. CISCO-STACKWISE-MI	B_cswSwitchInfoTable	
Context		
Status	Successful	
Type	SNMP	
Command	_CISCO-STACKWISE-MIB_cswSwitchInfoTable	
Error		

Export and Upload data provide options to use collection profile settings, export and upload the data, as shown in Figure 8-18

Γ

Profile Name:	NOS Full	
elected Device Count:	(63 device(s) selected	
xport Format:	Cisco VSEM (.zip)	~
Jpload Options	 Use Collection Profile Settings Export Only 	
	• Export and Upload	

Figure 8-18 Export and Upload Data

You can select the required options on the screen

- Use Collection Profile Settings: Uses the collection profile settings.
- Export Only: Only exports the data.
- Export and Upload: Exports and uploads the data.

View Collection Summary and View Collection Details provide collection summary and details for the selected collection profile. This is shown in Figure 8-19.

Figure 8-19	Collection Profile Device	Run Summarv
0		

å Q	×					
levice	Dataset Count	Success Count	Integrity Failed Count	Failed Count	Not Applicable Count	
Oevice_5_0_1_17	248	40	14	4	190	
Oevice_5_0_1_18	248	37	17	4	190	
2 Device_5_0_1_15	272	72	12	4	184	
2 Device_5_0_1_16	248	40	14	4	190	
(5.0.1.21)	248	39	15	4	190	
Device_5_0_1_22	248	40	17	4	187	
2 Device_5_0_1_19	248	39	15	4	190	
(5.0.1.20)	248	45	9	4	190	
Device_5_0_1_25	248	42	7	4	195	
Device_5_0_1_26	248	39	17	4	188	
Oevice_5_0_1_23	248	40	13	4	191	
Device_5_0_1_24	248	41	23	4	180	
Oevice_5_0_1_29	248	31	6	4	207	
G Device 5 0 1 30	248	11	1	4	232	

2 C	C Q	×					
💐 UniversalGatewaysAndAcce	Device	Dataset Name	Collection Type	Status	Resu	Collection Time	Message
er eft test (1)	10.91.81.1	40 ActivelPPhone	SOAP	Failed	0	Fri, Oct 19, 201	No working HT
Koice	10 91 81 1	40 ConfiguredIPPh	SOAP	Failed	0	Fri, Oct 19, 201	No working HT
VoiceGateways			and control			54.0.440.004	and control and a second
🥰 Video	Device_5_	0_1_2 device_query	нир	NOT Applicable	0	Fn, Oct 19, 201	
GenericNetworkDevices	10.91.81.1	40 device_query	HTTP	Not Applicable	0	Fri, Oct 19, 201	
🥰 Storage	Device 5	0 1 ; ActivelPPhone	SOAP	Failed	0	Fri, Oct 19, 201	No working HT
Relepresence	A	ConfiguredIPPh	SOAR	Failed	0	Eri Oct 19, 201	No working HT
🖓 Optical	Device_5_	0_1_2 ConfigurediPPh	SUAP	raieu	U	FII, OCI 19, 201	NO WORKING HT
RetworkManagement	10.91.81.1	40 show boot	CLI	Not Applicable	0	Fri, Oct 19, 201	
Reference (2)	10.91.81.1	40 show environm	CLI	Not Applicable	0	Fri, Oct 19, 201	
Wireless (1)		e ehow fileevete	CLL	Not Applicable	0	Eri Oct 19, 201	
With the second seco	10.91.81.1	40 anow meayate	CEI	Not Applicable	Ŭ	11, 00, 13, 201	
ServiceReadyPlatform	10.91.81.1	40 show process	CLI	Not Applicable	0	Fri, Oct 19, 201	
Routers (4)	10.91.81.1	40 show time	CLI	Not Applicable	0	Fri, Oct 19, 201	
LiveNodes (12)	AD 01 81 1	40 show top brief	CLI	Not Applicable	0	Fri Oct 19 201	
ApplicationNetworking (1)	10.91.81.1	40 Sherr top brief.r.				,	
🖓 Switches (1)		an show frame-rel	CU	Not Applicable	0	Fri Oct 19 201	

Figure 8-20Collection Profile Run Details

You can view the log messages for specific job runs, along with the status of the collection for each data set for the selected devices as shown below.

Figure 8-21	Collection	Profile Run	Summary I	Log M	lessages
-------------	------------	-------------	-----------	-------	----------

Log Messages for the Job 88/1	×
Log Messages	
Selected datasets ->	
show_context_asa_run_dyn	
show_context_asa_start_dyn	
show context run Dynamic	
show context start Dynamic	
Execution of Collection Profile start for 172.21.31.159 (Fri Sep 28 07:33:09 IST 2012)	
172.21.31.159: Successfully collected show context output.	
Time taken to execute dataset (show_context_asa):67490	
172.21.31.159: Successfully collected show running-config output.	
Time taken to execute dataset (show_context_asa_run):56125	
172.21.31.159: Successfully collected show running-config output.	
Time taken to execute dataset (show_context_asa_run):70307	
172.21.31.159: Successfully collected show startup-config output.	
Time taken to execute dataset (show_context_asa_start):56138	
172.21.31.159: Successfully collected show context output.	
Time taken to execute dataset (_show context):2537	
Time taken to run the collection profile on (172.21.31.159) :265 sec	
Execution of Collection Profile end for - 172.21.31.159 (Fri Sep 28 07:37:35 IST 2012)	

You can also delete a specific instance of the collection profile execution by selecting *Delete Profile Executions*.

To check the differences between two selected runs, select *Show Differences between selected Runs* option as shown below.

Use the *View Tag Collection Summary* option to list the summary of the commands that have been tagged earlier. Collection tag summary screen shows the device count of the tag along with the count of success, failed and not applicable devices, as shown in Figure 8-22.

I

Collection Profile Run Su	mmary 🗵 Collection Profile Run Tag	Summary(1/8) 🗵		
Q	×			
ag Name	Selected Device Count	Success Count	Failed Count	Not Applicable Count
lonfig	46	30	6	10

Figure 8-22 View Tag Collection Summary

Use the *View Tag Collection Details* option to show the details of the commands that have been tagged. The screen shows the Device name, Tag name, Dataset name, Dataset type, Status and Message.

Collection Profile Run Summary (8) Collection Profile Run Tag Details(13/1) 11 🔥 타 만 🖓 C Q .-× Call UniversalGatewaysAndAcces Device Tag Name Dataset Name Dataset Type Status Message static dc3qa-ind10 ActivelPPhone SOAP Successful View Data Real Voice ConfiguredIPPhone SOAP Successful 🔮 dc3qa-ind10 View Data Real Dynamic Real VoiceGateways 🔮 dc3qa-ind10 test HTTP Successful View Data Kideo test1 HTTP Successful 🔮 dc3qa-ind10 View Data CenericNetworkDevices R Storage Relepresence Coptical RetworkManagement DataCenter (1) References wireless Real UnifiedCommunications ReadyPlatform Routers LiveNodes (1) ReplicationNetworking Real Switches Recurity ÷

Figure 8-23 View Tag Collection Details

Use the Search Results option to search for the results. Specify the search string and select the tags to search the results, as shown in Figure 8-24.

lection Profile Run S	ummary	×
 Specify the Search * Search String: Select Tags: 	h String	
	Ok	Cancel

Figure 8-24Collection Profile Run Summary

To remove the profile executions select Delete Profile Executions

Select the View IP Host Masked Values option to view the IP hosted masked values. You can also download the file in txt format by clicking on Download button.

Figure 8-25 View IP Host Masked Values

0 Q-	× →		
File Name	From Date	To Date	Download File
CurrentMappingInfo	Fri, May 31, 2013 13:57:29 +	Fri, May 31, 2013 13:57:29 +	Download File

To view the difference between the selected runs chose the option Show Difference Between Selected Runs as shown in Figure 8-26.

C Q			× 🖸 🛈					
Profile Name	State		Status	Start Time	End Time	Actions	View Data	
Default_CP	Complet	ed	Success	Fri, Sep 28, 201	Fri, Sep 28, 201	Select Action •	View Data	
Default_CP	Cance (C	Refresh		Wed, Oct 3, 201	Select Action •	View Data	
Default_CP	Compl	0	Help		Wed, Oct 3, 201	Select Action •	View Data	
Default_CP	Compl		View Data		Wed, Oct 10, 20	Select Action •	View Data	
Default_CP	Compl		Export Collection Profile	Kun Data	Wed, Oct 10, 20	Select Action •	View Data	
context	Compl		View Device Collection Summary		Thu, Sep 27, 20	Select Action •	View Data	
context	Compl		View Tag Collection Sum	mary	Fri, Sep 28, 201	Select Action •	View Data	
context	Abort		View Tag Collection Deta	ails	-1	Select Action •	View Data	
context	Compl		View Job Log		Fri, Sep 28, 201	Select Action •	View Data	
context	Compl		Search Results		⁻ ri, Sep 28, 201	Select Action •	View Data	
cml	Compl		Upload to Remote Serve	er	Thu, Sep 27, 20	Select Action •	View Data	
kml	Compl		Delete Profile Execution	s	Thu, Sep 27, 20	Select Action •	View Data	
kml	Compl		Chau Differences Robus	and the stand Provention	Thu Sep 27 20	[[]	

Figure 8-26 Show Differences between Selected Runs

When you select two different runs, you can see what has changed between those runs in a Diff report where color codes (green-additions, red-deletions, and blue-changes) identify exactly what has changed.

Figure 8-27 Differences Between Two Collection Profile Runs

Name Profile Default_CP excuted at Sep 28, 2012 Profile hy executed at Oct 14, 2012 Result Size Device Name Type Status Result Size Status Image: Colspan=Ind10 Active/PPhone SOAP Not Executed Successful 1180 Image: Colspan=Ind10 test HTTP Not Executed Successful 48
Dataset details Profile Default_CP executed at Sep 28, 2012 Profile hy executed at Oc 14, 2012 Result Size Device Name Type Status Result Size Status Image: dc3qa-ind10 ActivePPhone SOAP Not Executed Successful 1180 Image: dc3qa-ind10 test HTTP Not Executed Successful 48
Device Name Type Status Result Size Status Image: dc3qa-ind10 ActiveIPPhone SOAP Not Executed Successful 1180 Image: dc3qa-ind10 test1 HTTP Not Executed Successful 48 Image: dc3qa-ind10 test HTTP Not Executed Successful 48
Image: Widc3qa-ind10 Active/PPhone SOAP Not Executed Successful 1180 Image: Widc3qa-ind10 test1 HTTP Not Executed Successful 48 Image: Widc3qa-ind10 test HTTP Not Executed Successful 48
@ dc3qa-ind10 test1 HTTP Not Executed Successful 48 @ dc3qa-ind10 test HTTP Not Executed Successful 48
Carlos-ind10 test HTTP Not Executed Successful 48
🚯 dc3qa-ind10 ConfiguredIPPhone SOAP Not Executed Successful 0

Go back to CSPC Flow Chart

Γ

View Collection Run Summary

Collection Run Summary report provides the summary of inventory. You can view the All Collection Profiles for Service or Single Collection Profile. To view collection profile and devices, select the option. In Available Services and Collection Profile drop down box, select the available service and click **OK** as shown in Figure 8-28.



Inventory Summary Filter	>
Select Collection Profile(s) and Devices	
All Collection Profiles For Service	
Available Services:	~
Single Collection Profile	
Available Collection Profile:	~
Help OK C	Cancel
	· · · · · · · · · · · · · · · · · · ·

View Collection Run Summary Input screen is displayed. It shows the list of Device Type and Device Count as shown in Figure 8-29.

Figure 8-29 View Collection Run Summary

View Collection Run Summary 🕷	
❷ Q• X → 😌 🕚	
Device Type	Device Count
Managed Devices(Selected for collection)	<u>69</u>
Active/Collected Devices	<u>63</u>
Unreachable/Collection Skipped Devices	6
Unmanaged Devices	1
Config Collected Devices	<u>0</u>
Config Failed Devices	<u>0</u>
Config Not Applicable Devices	<u>0</u>

By clicking on the Device Count, View Managed Devices for that Device is displayed as shown in Figure 8-30.

) Q-	×	-											
p Address	Host Name	Display Name	5ys Object Id	Device Family	Product Model	Serial Number	Vendor Name	O5 Name	O5 Version	Discovery Date/Time	Source	Reachable	
1.0.8.125	Device_11_0_8_125	Device_11_0_8_125	1361419	Routers	cisco7206		Cisco System	105	12.2(24)	Sat, Jul 29, 2017 00:15:40 +	Collector	9	
1.0.28.132	Device_11_0_28_132	Device_11_0_28_132	1361419	Routers	discoASR1002F		Cisco System	105-XE	12.2(33)XND	Sat, Jul 29, 2017 00:15:40 +	Collector	9	
1.0.8.126	Device_11_0_8_126	Device_11_0_8_136	.1.3.6.1.4.1.9	Routers	disco7206		Cisco System	105	12.2(24)	5at, Jul 29, 2017 00:15:40 +	Collector	9	
1.0.28.133	Device_11_0_28_133	Device_11_0_28_133	1361419	Routers	ciscoASR9006		Cisco System	IOS XR	3.7.2.151	Sat, Jul 29, 2017 00 15 40 +	Collector	9	
1.0.8.123	Device_11_0_8_123	Device_11_0_6_123	1361419	Routers.	disco7206		Cisco System	105	12.2(24)	Sat, Jul 29, 2017 00:15:40 +	Collector	0	
1.0.28.134	Device_11_0_28_134	Device_11_0_28_134	.1361419	Routers	discoASR9006		Cisco System	105 XR	3.7.2.151	Sat, Jul 29, 2017 00:15:41 +	Collector	9	
1.0.8.124	Device_11_0_8_124	Device_11_0_8_124	1361419	Routers	cisco7206		Cisco System	105	12.2(24)	Sat, Jul 29, 2017 00:15:41 +	Collector	0	
1.0.28.135	Device_11_0_28_135	Device_11_0_28_135	.1361419	Routers	cascoASR9006		Cisco System	105 XR	3.7.2.151	Sat, Jul 29, 2017 00:15:41 +	Collector	0	
1.0.8.129	Device_11_0_8_129	Device_11_0_8_129	1361419	Routers	cisco7206		Cisco System	105	12.2(24)	5at, Jul 29, 2017 00:15:41 +	Collector	9	
1.0.15.92	Device_11_0_15_92	Device_11_0_15_92	.1.3.6.1.4.1.9	LANSwitches	catalyst37xx9tack		Cisco System	105	12.2(25)FZ	Sat, Jul 29, 2017 00:15:41 +	Collector	9	
1.0.15.91	Device_11_0_15_91	Device_11_0_15_91	1361419	LANSwitches	catalyst37xx5tack		Cisco System	105	12.2(25)FZ	Sat, Jul 29, 2017 00:15:41 +	Collector	9	
1.0.8.127	Device_11_0_6_127	Device_11_0_8_127	1361419	Routers	cisco7206		Cisco System.	105	12.2(24)	5at, Jul 29, 2017 00:15:41 +	Collector	9	
1.0.15.90	Device_11_0_15_90	Device_11_0_15_90	.1.3.6.1.4.1.9	LANSwitches	catalyst37xx5tack		Cisco System	105	12.2(25)#Z	5at, Jul 29, 2017 00:15:41 +	Collector	0	
1.0.28.130	Device_11_0_28_130	Device_11_0_28_130	1361419	Routers	etiscoASR1002F		Cisco System	IOS-XE	12.2(33)XND	Sat, Jul 29, 2017 00 15:41 +	Collector	9	
1.0.39.61	Device_11_0_39_61	Device_11_0_39_61	.1361419	LANSwitches	cat6506		Cisco System	105	12.1(26)E5	Sat, Jul 29, 2017 00:15:41 +	Collector	9	
1.0.8.128	Device_11_0_8_128	Device_11_0_8_128	.13614.19	Routers	disco7206		Cisco System	105	12.2(24)	5at, Jul 29, 2017 00:15:41 +	Collector	0	
1.0.28.131	Device_11_0_28_131	Device_11_0_28_131	1361419	Routers	ciscoASR1002F		Cisco System	105-XE	12.2(33)XND	Sat, Jul 29, 2017 00:15:41 +	Collector	0	
1.0.39.60	Device_11_0_39_60	Device_11_0_39_60	1361419	LANSwitches	cat6506		Cisco System	105	12.1(36)E5	Sat, Jul 29, 2017 00:15:41 +	Collector	9	
1.0.15.96	Device_11_0_15_96	Device_11_0_15_96	.136.14.19	LANSwitches	catalyst37xx5tack		Cisco System	105	12.2(25)#Z	5at, Jul 29, 2017 00:15:41 +	Collector	0	
1.0.37.177	Device_11_0_37_177	Device_11_0_37_177	1361419	LANSwitches	cat6506		Cisco System.	105	12.1(26)E5	Sat, Jul 29, 2017 00:15:41 +	Collector	0	
1 / 20 42	Director 11 (1 20 62	Denne 11 0 29 62	1261119	T SNGLIMBER	wethe		Cure Guten	106	in these	CH 1.3 10 1017-0015-01-	Calleran	-	

Figure 8-30 Inventory Input Data Report

Config Collected Devices

Γ

You can filter and view the Collection Profile and devices. You can also enter the filter value in the Search String to view the config collected devices.

Search String:		
Select Collection Profile(s)	and Devices	
All Collection Profiles All Collection Profiles All Collection Profiles All Collection Profiles Section Profile Section Profiles Section Profiles Section Profiles Section Profiles Section Profile Sec	For Service	
Available Services:	\subset	~
Single Collection Profi	le	
Available Collection Profil	le:	~

Config Collected Devices screen is displayed. It shows the list of Device IP and Device Primary Name as shown in Figure 8-32.

In addition, you can see the description of each device by clicking the + symbol next to the Device Ip Clicking the + sign shows the Collection Time, Context, Dataset Type, Error Message, and Config Command for this particular device.

0	₩\$ ₩\$ Q.•	$\times \Rightarrow $	70		
	Device IP	Dev	rice Primary Nan	ne	
9	5.0.1.1	5.0.1	.1		
	Collection Time	Context	Dataset Type	Error Message	Config Command
	Tue, Oct 18, 2016 22:25:28 +0530		CLI		show running-config View Data
	Tue, Oct 18, 2016 22:25:28 +0530		CLI		show startup-config View Data
ŧ	5.0.1.2	5.0.1	2		
Ð	5.0.1.3	5.0.1	.3		
Ð	5.0.1.8	5.0.1	.8		
Ð	5.0.1.11	5.0.1	.11		
Ð	5.0.1.12	5.0.1	.12		
Ð	50113	501	13		

Figure 8-32 Config Collected Devices

Click View Data in the report to view config command for this particular device Figure 7-49 shows the Config command details.

Figure 8-33 Config Command

Config	Command	×
1	interface ethernet 0	~
2	ip address 10.86.178.181 255.255.255.0	
3	gss-communications	
4	gss-tcp-keepalives	
5		
6	hostname Device_5_0_1_14.gss.com	
7	ip default-gateway 10.86.178.1	
8	ip name-server 161.44.124.122	
9		-
10	ssh enable	=
11	no ssh keys	
12	no ssh protocol version 1	
13	telnet enable	
14	ftp enable	
15		
16	terminal length 0	
17	exec-timeout 20	
18		
19	logging disk enable	
20	logging disk priority Notifications(5)	
21	no logging host enable	
22	logging host priority Warnings(4)	
23	logging facility local5	
24	logging diet enheuetem dreserver priority Frrore (3)	
	OK	

Config Data Per Device

I

Config Data Per Devices report shows the configs collected by CSP Collector. You can select configs based on Collection Profile. Config data per device filter can be configured by providing required inputs as shown below.

Figure 8-34 Config Data Per Device Filter Config Data Per Device Filter × * Select Devices All managed devices Only the following selected devices Managed Devices: Selected Devices/Groups: 10 * LiveNodes (64) Unreachable Nodes (3) 💐 Hubs * + * Servers-UnifiedComputing (3) ServiceExchange (1) + xDSL 🔍 🟘 GenericNetworkDevices (5) Routers (13) 💏 Switches ATMSwitches (1) 🖓 BladeSwitches ConnectedGridSwitches Select Collection Profile(s) and Devices All Collection Profiles For Service Available Services: v Single Collection Profile Available Collection Profile: × Help. OK Cancel

The config data will be processed for the mentioned devices as shown in Figure 8-35. On clicking View Data, collected config data is displayed for the specified device.

8-



Export Detailed Device Data

You can export the detailed device data such as, device, access verification config time and collection time and so on. You can select devices based on Collection Profile for service. Devices can be downloaded in csv format by providing required inputs as shown below.

Only the following selected devices				
Managed Devices:		Selecte	d Devices/Groups:	
12 0				
LiveNodes (1)	*			
🥰 Unreachable Nodes				
real Hubs				
💏 Servers-UnifiedComputing		-		
🖓 ServiceExchange		•		•
xDSL		E		*
GenericNetworkDevices				
📸 Routers				
🖓 Switches				
ATMSwitches				
🖓 BladeSwitches				
ConnectedGridSwitches	~			
Select Collection Profile(s) and Devices				
All Collection Profiles For Service				
Available Services:		*		
Single Collection Profile				

Figure 8-36 Export Detailed Device Data

Services Reports

- Alerts
- SNMP Trap Report
- Syslog Summary
- Syslog Messages

Alerts

This report provides a list of all Alerts. The report contains Event ID, Module, Time of event, severity, message, and View Details. Alerts that are older than 14 days in CSPC system are purged.

There two types of alerts UI Notification and Email alerts.

- UI Notification alerts appears on the UI when a notification is received.
- · Email alerts are the alerts sent via mail to the subscribed email address

Figure 8-37	Alerts				
Alerts X					
0 Q.+	× 🔿 Oelete Aler	Delete All Alerts			
Event Id	Module	Time Of Event	Severity	Message	View Details

SNMP Trap Report

I

This report shows a list of traps sorted by Device, Notification types, Trap Data, and Received At. To generate the SNMP Trap Report, do the following steps:

 Step 1
 Select the Trap Received Time from drop down

 • If custom is selected, then enter the Start Date/Time and End Date/Time

 Step 2
 Browse to select the Source Device

 Step 3
 Select Notification Types

 Step 4
 Click OK

NMP Trap Filter		×
Note : Maximum number	of records to be retrieved is limited to 1000.	
Select Time Period		
Trap Recieved Time	Custom	
Start Date/Time	Custom 15 : 01 🛊	
End Date/Time	Last 1 Hour 15 : 01 :	
	Last 2 Hours	
Select SNMP Trap Para	Last 6 Hours	51
Source Device	Last 12 Hours	
Source Device	Last 1 Day Browse	
Coloct Natification Type	Last 1 Week	_
Select Notification Type	Last 2 weeks	ר ו
CISCO-CONFIG-MAN	MIB	
CISCO-CONFIG-COP	(-MIB	
	•	
	<u>(*</u>	
	Help OK Cance	2

Figure 8-38 SNMP Trap Filte

To view the Trap Data click View Trap Data.

NMP Trap Report									
10	© Q.+	× I → I 字 (0)							
🥰 LiveNodes (3)	A Device	Notification Type	Trap Data	Received At					
🚓 Unreachable Nodes (3)	Myrouter	CISCO-CONFIG-MAN-MIB	View Trap Data	Wed, Nov 19, 201	4 15:48:45 +0530				
🥰 Video	Myrouter	CISCO-CONFIG-MAN-MIB	View Trap Data	Wed, Nov 19, 201	4 15:48:40 +0530				
Reg StorageNetworking				W. ()) (0.000					
Conferencing	Myrouter	SNMD Trap Data	View Trap Data	wed, Nov 19, 201	4 10:48:20 +0030				
Real UnifiedCommunications	Myrouter								
CollaborationEndpoints	@ SR520-1	1 1.3.6.1.2.1.1.3.0 = 29 a	1 1.3.6.1.2.1.1.3.0 = 29 days						
CloudandSystemsManagement	😵 SR520-1	4	3 U11617.28						
🚓 Wireless	SR520-1	5 1.3.6.1.6.3.1.1.4.1.0 =	5 1.3.6.1.4.1.9.9.43.1.1.6.1.3.757 = 1 8 1.3.6.1.4.1.9.9.43.1.1.6.1.4.757 = 3						
CataCenterSwitches	E 🔗 SR520-1	7 1.3.6.1.4.1.9.9.43.1.1.6							
Real IndustrialEthernetSwitches	8R520-1	9 1.3.6.1.4.1.9.9.43.1.1.6 10							
R Servers-UnifiedComputing	SR520-1	11 1.3.6.1.4.1.9.9.43.1.1.6	.1.5.757 = 2		i9:00 +0530				
R InfiniBandSwitches	😵 SR520-1	12 13	12						
R LANSwitches	SR520-1	15			38:40 +0530				
R xDSL	(D) I wanted	16			5-10 +0530				
RetroEthernetSwitches	myrouter	18							
CenericNetworkDevices (3)	Myrouter	19			15:05 +0530				
Real WANSwitches	Myrouter	20			4:50 +0530				
ApplicationNetworkingServices	Myrouter			ОК	4:45 +0530				
Security	CO Married	CISCO.CONFIG.MAN.MIR	View Tran Data	Wed Nov 19 201	4 13-18-04 +0530				
Routers (3)	* Myrouter	CIGGO-CONFIG-MAN-MIB	Tiew Hap Uala	**Ed, NOV 13, 201	4 13.10.04 40000				

Syslog Summary

Γ

Syslog Summary report provides the summary of the all the syslogs collected by CSPC. You need to provide the filtering information such as when was the log(s) received, and do you want to see the summary based on severity and so on as shown in Figure 8-40.

elect 11me Period			
.og Recieved Time	Custom		
Start Date/Time	April 21,2021 18:20	•	
End Date/Time	April 21,2021 22:20	•	
la d Caula a Rama			
elect Syslog Parameters			
Source Device	10.197.174.195		Browse
Component Name	Asr1		
Inemonic <mark>T</mark> ext			
/linimum Severity	5 (notification)	~	
Aaximum Severity	2 (critical)	~	
elect Syslog Summary I	Keport Type		
Report Type	Syslog Count By Severity	~	

Once the filter is selected, the summary report matching that filter is provided.



Figure 8-41 Syslog Summary

Syslog Messages 🗷 Syslog Count By Severity 🗵	
⊘ Q x ⇒ <u>11</u> \ ()	
Severity	Message Count
0 (emergency)	0
1 (alert)	0
2 (critical)	0
3 (error)	303
4 (warning)	27
5 (notification)	0
6 (informational)	0
7 (debugging)	60

Syslog Messages

Γ

Syslog messages report provides all the syslogs that are collected by CSPC. Just like the Syslog Summary report, you need to provide the filter that needs to be applied before providing the detailed syslog message report.

elect Time Period —					
Log Recieved Time	Custom	~			
Start Date/Time	November 05,2014	1	10 : 52	:	
End Date/Time	C	•	10 : 52	•	
elect Syslog Paramet	ers				
Source Device	<u> </u>			\supset	Browse
Component Name	<u> </u>				
Mnemonic Text	C				
Minimum Severity	C			~	
Maximum Severity	<u> </u>			~	
elect Syslog Count ar	nd Order				
Number of Syslogs	C				
Syslogs to be shown	Sort messages by asce	ending o	rder]~	

Figure 8-43 Syslog Messages

20	0 Q	× =	• 🕈 🛈					
🔍 🦓 LiveNodes (65)	Device	Source	Seq	Component	Mnemonic	Severity	Message	Received At
😪 Unreachable Nodes (1)			0			6 (informational)	icwecwevcwefcewwdwdwef	Fri, Jul 21, 2017 17:07:1
🦓 Hubs			0			6 (informational)	qwdhwegf3gefyg2gfhedwehh	Fri, Jul 21, 2017 17:07:1
😤 Servers-UnifiedComputing (3)			0			6 (informational)	wdwhfd3hefyh2eyhfycehfychye	Fri. Jul 21, 2017 17:07:1
😪 static		0001	1	MCAST	CURTINOWN	2 (mitianly	Reih ICh III anne stier fer fedde	Ti, jul 21, 2017 17:00.4
🥰 dynamic (1)		8.0.0.1	1	MCASI	SHUIDOWN	2 (critical)	built iCMP connection for faddr	Fri, Jul 21, 2017 17:09:4
RerviceExchange (1)		8.0.0.1	2	COMMON_FIB	FIB_RECURSION	6 (informational)	Line protocol on Interface Loop	Fri, Jul 21, 2017 17:09:4
💏 xDSL		8.0.0.1	3	CDP	NVLANMISMATCH	4 (warning)	New double space Format 3	Fri, Jul 21, 2017 17:09:4
GenericNetworkDevices (2)	Device_5_0_1_60	5.0.1.60	4	CDP	SENDFAIL	3 (error)	New double space Format 4	Fri, Jul 21, 2017 17:09:4
🥞 Routers (14)	Davies 5 0 1 60	50160	5	OSPE	ADICHG	5 (notification)	New single space Format 5	Fri. Jul 21, 2017 17:09:4
🥰 Switches	Device_5_0_1_60	0.011100		0011	insjerio	o (noundation)	rich single space romato	
RTMSwitches (1)								
💏 BladeSwitches								
Real Connected GridSwitches								
Real DataCenterSwitches (2)								
Regional Endustrial Ethernet Switches								
🦂 InfiniBandSwitches (1)								
🥰 LANSwitches (8)								
RetroEthernetSwitches								
🖓 WANSwitches (5)								
ReplicationNetworkingServices (5)								
🥰 Security (5)								
🖓 Video (4)								
StorageNetworking (1)								

Job Reports

Use the Job Log Reports sub tab to view the collected logs for various operations that are performed through the CSP collector.

This section describes the Reports options in the following topics:

- Discovery Jobs
- Job Management Reports
- Inventory Jobs
- Device Access Verification Jobs
- View Job Metrics

Discovery Jobs

I

The discovery jobs report includes information on all the network device discovery jobs performed.

In addition, you can see the description of each job by clicking the + symbol next to the *Job Id*. Clicking the + sign shows the *Run Id*, *State* (Successful/Aborted), *Status* (Completed/Not Completed), *Start Time*, *End Time*, and *Job Log Details* for this particular job.

You can cancel any job by clicking the *View Job Details -> Cancel Job* button.

These details are common to all Job Reports.



Select the *Action* button in the report to view either the Job Log details for this particular job, look at the Job itself (what options are provided for the discovery, etc.) or you can create a new job by cloning this discovery job. Figure 8-45 shows the job log details. You can also **Export Seed File** and **Export Imported Device Status**. To know the status of imported devices you can generate/export the report based on Discovery JobId and JobRunId and to export the status of imported devices into .csv file, with the name ImportedDeviceStatus_jobid_jobrunid.cvs click **Export Imported Devices Status**.

Pause and resume jobs using the **Pause Job** and **Resume Job** menu options. Pause is activated when job starts running and resume is activated once the job is paused.

L

g Messages for the Job 1/1	
Message	
Starting Known Devices Discovery	-
Entered IP addresses->	
10.88.145.18,5.0.1.1,5.0.1.3,5.0.1.4,5.0.1.5,5.0.1.6,5.0.1.7,5.0.1.8,5.0.1.9,5.0.1.10,5.0.1.11,5.0.1.12,5.0.1.1	-
10.88.145.18: Device Unreachable or SNMP Credentials Not Set.	
5.0.1.1: Device Unreachable or SNMP Credentials Not Set.	
5.0.1.3: Device Unreachable or SNMP Credentials Not Set.	
5.0.1.4: Device Unreachable or SNMP Credentials Not Set.	
5.0.1.5: Device Unreachable or SNMP Credentials Not Set.	
5.0.1.6: Device Unreachable or SNMP Credentials Not Set.	
5.0.1.7: Device Unreachable or SNMP Credentials Not Set.	
5.0.1.8: Device Unreachable or SNMP Credentials Not Set.	
5.0.1.9: Device Unreachable or SNMP Credentials Not Set.	
5.0.1.10: Device Unreachable or SNMP Credentials Not Set.	
5.0.1.11: Device Unreachable or SNMP Credentials Not Set.	
5.0.1.12: Device Unreachable or SNMP Credentials Not Set.	
5.0.1.13: Device Unreachable or SNMP Credentials Not Set.	
5.0.1.14: Device Unreachable or SNMP Credentials Not Set.	
5.0.1.15: Device Unreachable or SNMP Credentials Not Set.	
5.0.1.16: Device Unreachable or SNMP Credentials Not Set.	
5.0.1.17: Device Unreachable or SNMP Credentials Not Set.	
5.0.1.18: Device Unreachable or SNMP Credentials Not Set.	

When you select the **Cloning** or **Modify Discovery Job** option, you see the exact job that was completed earlier, and can modify it to create another job as shown below.

Figure 8-46 Clone This Discovery Job

Discover and Manage Network Devices	×
Select at least one of the following network device discovery methods.	
Jiscover devices with known IP addresses	
Discover devices with protocols such as CDP, OSPF and ARP	
Discover devices by scanning/pinging range of IP Addresses	
Rediscover the currently managed and non-managed devices	
Import. <- Previous Next>	Help Cancel

To IP Address/Host Name , click Next button.

Enter the list of IP addresses for the known de	evices.		
IP Address/Host Name			
🕈 Add 🗙 Delete 🖉 Modify			
10.1.1.10			

Figure 8-47 Discover Devices using Known IP Addresses

To schedule discovery options, click $\ensuremath{\textit{Next}}$ button.

Figure 8-48 Discovery Schedule Options

Inventory Jobs

Γ

This report includes all the network device inventory jobs performed.

I

In addition, you can see the description of each job by clicking the + symbol next to the *Job Id*. Clicking the + sign shows the *Run Id*, *State* (Successful/Aborted), *Status* (Completed/Not Completed), *Start Time*, *End Time*, and *Job Log Details* for this particular job, as shown in the figure below.



Figure 8-49 Inventory Jobs Main Window

Select the *Action* button in the report to view either the Job Log details for this particular job, or to cancel a job while it is still running. You can pause any running job and later resume it by using the Pause Job and Resume Job options.

By selecting *Recollect Failed Datasets* option, the data from only those devices is collected that showed an error earlier, once the data is collected it is merged with the other data before it is sent to Cisco.

Use view collection profile device status is to see the progress of device collection and it is enabled only if collection is in running state.

Figure 8-50 shows the job log details.

. 9.		
Log	g Messages for the Job 272/1	>
h	Message	
s	Selected datasets ->	
s	show_context_asa_run_dyn	
E	Execution of Collection Profile start for 10.78.177.39 (Wed Oct 10 10:03:15 IST 2012)	
1	10.78.177.39: Successfully collected show context output.	
T	Time taken to execute dataset (show_context_asa):66728	
1	10.78.177.39: Successfully collected show running-config output.	
T	Time taken to execute dataset (show_context_asa_run):66659	
1	10.78.177.39: Successfully collected show running-config output.	
T	Time taken to execute dataset (show_context_asa_run):67090	
T	Time taken to run the collection profile on (10.78.177.39) :214 sec	
E	Execution of Collection Profile end for - 10.78.177.39 (Wed Oct 10 10:06:49 IST 2012)	

Figure 8-50 Job Log Details

Device Access Verification Jobs

I

The Device Access Verification Jobs report includes all the network device verification jobs performed. In

addition, you can see the description of each job by clicking the + symbol next to the *Job Id*. Clicking the + sign shows the *Run Id*, *State* (Successful/Aborted), *Status* (Completed/Not Completed), *Start Time*, *End Time*, and *Job Log Details* for this particular job, as shown in Figure 8-51.

De	vice Ac	ess Verification]	obs 🗵											
0	₩‡ Ę	1 Q		×	0									
	Job Id	Job Name	Description	Created By	Created On	Modified	Modified On	Run	First Run Time	Last Ru	n Time	Next Schedule Time	Service Name	
8	5	NO5_Defaul	Collection Pr	admin	Fri, Mar 2, 2018 0			1 F	ri, Mar 2, 2018 0	Fri, Mar 2,	2018 0			^
	Run	Id State	Status	Start Time		End Tim	e/Last Paused Time		Action					
	1	Completed	Success	Fri, Mar 2, 2	2018 00:40:20 +0530) Fri, Mar	2, 2018 00:40:22	+0530	Select Action		_			
Ð	14	real	real	admin	Tue, Aug 14, 2018			1 1	View Job Lo	g Details	2018			
	19	NO5 Defau	Collection Pr	admin	Tue, Aug 14, 2018			1 1	Cancel Job		2018	N	05	
Ð	22	_NO5_Defau	Collection Pr	admin	Tue, Aug 14, 2018			1 1	Tu View Job De	etails	2018	N	D5	
Ð	27	_NO5_Defau	Collection Pr	admin	Tue, Aug 14, 2018			1 1	fu Modify DA	V Job	2018	N	D5	
Ð	38	import_Dav	Seed file imp	admin	Tue, Aug 14, 2018			1 1	fu Pause Job		2018			
ŧ	55	NO5_Defaul	Collection Pr	admin	Thu, Aug 16, 201			1 1	Resume Job		. 201	N	D5	
Ð	59	xfvdsfs	xfvdsfs	admin	Thu, Aug 16, 201			1 1	Thu, Aug 16, 201	Thu, Aug	6, 201			

Figure 8-51 Device Access Verification Jobs Main Window

Select the *Action* button in the report to view either the Job Log details for this particular job, or to cancel a job while it is still running. You can also view and modify the job details. Pause and resume jobs using the **Pause Job** and **Resume Job** menu options. Pause is activated when job starts running and resume is activated once the job is paused.

Figure 8-53 shows the job log details.

Figure 8-52	Job Log Details
Log Messages	for the Job 91/1
Message	
All Devices (1)) selected.
Protocols Sele	cted: telnet
5.0.1.38 (telne	t) : Successful with credential '5.0.1.38_telnet'
Device Acces	s Verification Job completed with Status: Success
Updating device	ce working credentials.

Job Management Reports

Job Management Reports option is a container from where you can select any of the supported jobs, except for discovery jobs and inventory jobs.

Job Management Reports allows to select any of the supported Job reports. You can select any job from the Job Group Type drop down list to go to the specified Job report. In addition, for all the jobs you can see the description of each job by clicking the + symbol next to the Job Id. Clicking the + sign shows the Run Id, State (Successful/Aborted), Status (Completed/Not Completed), Start Time, End Time, and Job Log Details for the particular job.

Select the Action button in the report to view either the Job Log details for this particular job, or to cancel a job while it is still running.

The currently supported jobs are:

- Credential Loader Jobs
- Apply Config Jobs
- Backup and Restore Jobs
- Ping Jobs
- Trace Route Jobs
- Prompt Collection Jobs
- Health Collection Jobs
- Upload Jobs
- Upload Run Now Jobs
- Connectivity Jobs
- Import Seed File Jobs
- Miscellaneous Jobs
- Key Rotation Job

After opening the Job Management Reports window, select the Job which you want to display and click **OK** button. More details on the Jobs are given below. Jobs can be either Unscheduled or Scheduled. Jobs can be edited by right clicking on the Job and selecting Edit Job Schedule option.

Job Group Type	Audit	~
Sub Type	Credential Loader Jobs Apply Config Jobs	^
	Backup/Restore Jobs	
	Ping Jobs Trace Route Jobs Prompt Collection Jobs Health Collection Jobs Upload Jobs	
	Upload Run Now Jobs	
	Connectivity Jobs Import Seed File Jobs	
	Miscellaneous Jobs	
	Key Rotation Job	~

Figure 8-53Job Management Reports

Credential Loader Jobs

Γ

Credential Loader Jobs allows you to view all the jobs runs/created using Changing Credential Import.

Cr	edentia	l Loader Jobs 🕱									
0		<u>t</u> Q	2								
	Job Id	Job Name	Job Descript	Created	Created On	Modifie	Modified On	First Run Time	Last Run Time	Run	Next Schedu
ŧ	36	FreqChangingCred		admin	Wed, Dec 12, 20					0	Wed, Dec 12
						m					
M	V Pa	age 1 of 1 🕨 🖡	1							Displ	aying 1 - 1 of

Figure 8-54 Credential Loader Jobs

Jobs can also be Unscheduled, or Schedules can be edited by right clicking on the Job name.

In addition, you can see the description of each job by clicking the + symbol next to the *Job Id*. Clicking the + sign shows the *Run Id*, *State* (Successful/Aborted), *Status* (Completed/Not Completed), *Start Time*, *End Time* for this particular job.

Apply Config Jobs

The Apply Config Jobs report allows you to view the configuration jobs that were applied from the CSP collector. You can view all the jobs, job creator, etc.

In addition, you can see the description of each job by clicking the + symbol next to the *Job Id*. Clicking the + sign shows the *Run Id*, *State* (Successful/Aborted), *Status* (Completed/Not Completed), *Start Time*, *End Time*, and *Job Log Details* for this particular job, as shown in Figure 8-55.

	•		712 500		a	142.102	1.12 102/02	14			
1	obld	JobName	JobDescription	Created	CreatedOn	Modifie	ModifiedOn	Run	FirstRunTime	LastRunTime	NextScheduleTim
7	4	1		admin	Thu, Sep 27, 20			1	Thu, Sep 27, 20	Thu, Sep 27, 20	
8	13	10		admin	Thu, Sep 27, 20			1	Thu, Sep 27, 20	Thu, Sep 27, 20	
8	34	11		admin	Thu, Sep 27, 20			1	Thu, Sep 27, 20	Thu, Sep 27, 20	
8	5	12		admin	Thu, Sep 27, 20			1	Thu, Sep 27, 20	Thu, Sep 27, 20	
7	'5	2		admin	Thu, Sep 27, 20			1	Thu, Sep 27, 20	Thu, Sep 27, 20	
7	6	3		admin	Thu, Sep 27, 20			1	Thu, Sep 27, 20		
7	7	4		admin	Thu, Sep 27, 20			1	Thu, Sep 27, 20		
7	8	5		admin	Thu, Sep 27, 20			1	Thu, Sep 27, 20	Thu, Sep 27, 20	
7	'9	6		admin	Thu, Sep 27, 20			1	Thu, Sep 27, 20	Thu, Sep 27, 20	
8	0	7		admin	Thu, Sep 27, 20			1	Thu, Sep 27, 20	Thu, Sep 27, 20	
8	1	8		admin	Thu, Sep 27, 20			1	Thu, Sep 27, 20	Thu, Sep 27, 20	
8	2	9		admin	Thu, Sep 27, 20			1	Thu, Sep 27, 20	Thu, Sep 27, 20	

Figure 8-55 Apply Config Jobs

Backup and Restore Jobs

I

The Backup and Restore Jobs report allows you to view the backup and restore jobs that were applied on the CSP collector. You can view all the jobs, job creator, etc.

In addition, you can see the description of each job by clicking the + symbol next to the *Job Id*. Clicking the + sign shows the *Run Id*, *State* (Successful/Aborted), *Status* (Completed/Not Completed), *Start Time*, *End Time*, and *Job Log Details* for this particular job, as shown in the figure below.

9	· · · ·	Q			×	⇒ _								
1	Job Id .	Job Name	1	Job Descript.	Created.	. Crea	ted On	Modifie	Modified On	First Run Time	Las	t Run Time	Run	Next Schedule T.
) (9 1	Periodic Ba	IC	Backup/Rest	cspcuse	Wed	, May 29, 2	•••		Wed, May 29, 2	Wee	i, May 29, 2	1	
	Run Io	I State		Status	Start Tin	е			End Time			Action		
	1	Comp	leted	Succes	Wed, N	lay 29,	2013 06:	29:00 +0530	Wed, May 29	, 2013 06:29:44	+0530	Select Action		

Figure 8-56 Backup/Restore Jobs

I

Ping Jobs

Ping Jobs allows you to view the ping jobs that were applied on the CSP collector from XML API interface.

In addition, you can see the description of each job by clicking the + symbol next to the *Job Id*. Clicking the + sign shows the *Run Id*, *State* (Successful/Aborted), *Status* (Completed/Not Completed), *Start Time*, *End Time*, and *Job Log Details* for this particular job, as shown in the figure below.

7ig	ure 8	8-57	Pir	ıg Jol	bs							
Pi	ng Jobs	8										
0	•	1 Q -			× →							
-	Job ld	Job Name	Job De	scription	Created	Created On	Modified	Modified On	First Run Time	Last Run Time	Run	Next Schedule Time
9	1	TestPing2	This pi	ng job	cspcuser	Fri, May 31, 2013			Fri, May 31, 2013		1	
	Run	ld State	Status	Start Ti	ime		End Time	Action				
	1	Aborted	Failed	Fri, M	ay 31, 201	3 09:40:15 +0530		Select Action •				

Trace Route Jobs

Γ

In Trace Route Jobs you can view all the trace route jobs that were performed on a CSP collector.

Tr	ace Rout	e Jobs 😤										
0	P. 2	Q.	3	× 🖚								
	Job Id	Job Name	Job Description	Created By	Creat	ted On	Modified By	Modified On	First Run Time	Last Run Time	Run	Next Schedule Time
	56	my_traceroute	This is tracero	admin	Fri, Ju	un 28, 2013 11:			Fri, Jun 28, 2013 11:	Fri, Jun 28, 2013 11:	1	
	Prole	Cinto	Platus Ptor	+ Time		Log Message	s for the Job	56/1			×	
	Ronito	, omn	ousus our	1 TIME		Q.		× →				
	3	Completed	Success Fri,	Jun 28, 2013	11:22	Message		ISSI IN MAL				
						Timeout Val	ue:5					
						No of device	is:1					
						1 172.21.31	1 0.309 ms 0.3	07 ms 0.168 ms				
						2 172.25.10	3.5 0.506 ms 0.	206 ms 0.193 ms				
						3 172.23.82	37 0.266 ms 0.	230 ms 0.227 ms				
						4 172.23.1.1	0.539 ms 0.28	9 ms 0.269 ms				
						5 172.23.1.2	2 0.369 ms 0.2	92 ms 0.278 ms				
						6 172.24.11	3.154 0.550 ms	0.461 ms 0.323 ms				
						7 172.21.54	131 [closed] 1.	082 ms 0.869 ms 0.	846 ms			
						Selected de	vice eth0, addre	ess 172.21.31.28, p	ort 56673 for outgoing packe	ts		
						Tracing the	path to 172.21.5	54.131 on TCP port	80 (http), 30 hops max		- 1	
						TraceRoute	Job Completed	r.				
14	Pag	e 1 of 1	- 21			10					_	Displaying 1 - 1

You can see the description of each job by clicking the + symbol next to the *Job Id*. Clicking the + sign shows the *Run Id*, *State* (Successful/Aborted), *Status* (Completed/Not Completed), *Start Time*, *End Time*, and *Job Log Details* for this particular job.

Prompt Collection Jobs

The Prompt Collection Jobs report includes all the Prompt Collection jobs performed.

In addition, you can see the description of each job by clicking the + symbol next to the *Job Id*. Clicking the + sign shows the *Run Id*, *State* (Successful/Aborted), *Status* (Completed/Not Completed), *Start Time*, *End Time*, and *Job Log Details* for this particular job, as shown in the figure below.

	e‡	Q		×C	3							
Jobid	Job	Name .	lobDescription	Created	CreatedOn	Modifie	ModifiedOn	Run	FirstRunTim	e	LastRunTime	NextScheduleTim
192	test			admin	Mon, Oct 8, 201			1	Mon, Oct 8,	201	Mon, Oct 8, 20	1
Run	ld	State	Status	Start Time			End Time			Action		
1		Completed	Success	Mon, Oct	t 8, 2012 13:48:37	7 +0530	Mon, Oct 8, 20	12 13:48:	39 +0530	Selec	at Action •	
											View Job Log De	tails

Figure 8-59 Prompt Collection Jobs

Health Collection Jobs

Γ

The Health Collection Jobs report includes all the Health Monitor jobs performed on CSPC

In addition, you can see the description of each job by clicking the + symbol next to the *Job Id*. Clicking the + sign shows the *Run Id*, *State* (Successful/Aborted), *Status* (Completed/Not Completed), *Start Time*, *End Time*, and *Job Log Details* for this particular job, as shown in Figure 8-60.



He	alth Colle	ction Jobs									
9	■‡ ₽ !	Q		×	•)						
	Job ld J	b Name	Job Descript	Created	Created On	Modifie	Modified On	First Run Time	Last Run Time	Run	Next Schedule T.
Ð	6 N	OS_Health		cspcuser	Wed, May 29, 2			Thu, May 30, 20	Tue, Jun 4, 2013	6	Wed, Jun 5, 201.
9	11 h	ealth_mfoni		cspcuser	Wed, May 29, 2			Wed, May 29, 2	Wed, May 29, 2.	. 1	
	Run Id	State	Status	Start Time			End Time		Action		
	1	Completed	d Success	Wed, Ma	y 29, 2013 06:3	8:34 +0530	Wed, May 29), 2013 06:39:14 +05	30 Select Act	ion 👻	

Upload Jobs

In the Upload Jobs report you can view all the scheduled jobs with Upload Profile, view the upload jobs that are user defined and created by the system. You can unschedule a job or edit an existing job schedule. You can also check the status of uploaded jobs, view job log details or cancel any running job.

) ■‡ 5	<u>I</u> Q		× =	• 1						
Job Id	Job Name	Job Descript	Created	Created On	Modifie	Modified On	First Run Time	Last Run Time	Run	Next Schedule T.
2	Full_Upload		admin	Sat, Dec 1, 2012			Mon, Dec 3, 201	Mon, Dec 3, 201	1	Mon, Dec 10, 20.
3	Incremental		admin	Sat, Dec 1, 2012			Sun, Dec 2, 201	Thu, Dec 6, 201	4	Fri, Dec 7, 2012
Run	ld State	Status	Start Time			End Time		Action		
1	Complete	d Success	Sun, De	c 2, 2012 23:00:0	00 +0530	Sun, Dec 2, 201	12 23:00:05 +0530	Select Action		
2	Complete	d Success	Tue, De	c 4, 2012 23:00:0	0 +0530	Tue, Dec 4, 201	2 23:07:06 +0530	Select Action		
3	Complete	d Success	Wed, De	c 5, 2012 23:00:0	00 +0530	Wed, Dec 5, 20	12 23:01:32 +0530	Select Action		
4	Complete	d Success	Thu, De	c 6, 2012 23:00:0	0 +0530	Thu, Dec 6, 201	2 23:00:06 +0530	Select Action		
4	Complete	a Success	Thu, De	, 2012 23.00.0	0 +0030	Thu, Dec 6, 201	2 23.00.06 +0530	Select Action		

To check the status of the Uploaded jobs, click the '+' button next to Job Id. Job status along with data and time is displayed as shown in the above figure. To view the log details of a job as shown in Figure 8-62, click Select Action button and then View Job Log Details.

Figure 8-62 View Job Log Details

Q	
Message	
Upload Phase :INITI	ALIZE_FILES Upload Phase Status :RUNNING JobStatus :RUNNING
Upload Phase :INITI	ALIZE_FILES Upload Phase Status :SUCCESSFUL JobStatus :RUNNING
Upload Phase :DUN	IPING_UPLOAD_DATA Upload Phase Status :RUNNING JobStatus :RUNNING
Upload Phase :DUM	IPING_UPLOAD_DATA Upload Phase Status :SUCCESSFUL JobStatus :RUNNING
Upload Phase :ZIP_	FILE_CREATION Upload Phase Status :RUNNING JobStatus :RUNNING
Upload Phase :ZIP_	FILE_CREATION Upload Phase Status :SUCCESSFUL JobStatus :RUNNING
Upload Phase :UPL	OAD_TO_BACKEND Upload Phase Status :RUNNING JobStatus :RUNNING
Upload Phase :UPL	OAD_TO_BACKEND Upload Phase Status :SUCCESSFUL JobStatus :RUNNING
Upload Phase :UPL	OAD_TO_BACKEND Upload Phase Status :SUCCESSFUL JobStatus :SUCESS
Upload job complet	ed successfully. Upload File Location :/opt/CSPC/uploaddata/Incremental_Upload/31/transport-invento
TransactionId/Conr	resp =4833680201860723340

If you do not want to run a scheduled upload, right click on the job, and then click Unschedule Job button.

ſ

0	• • •	Q -		× =	()						
	Job Id	Job Name	Job Descript	Created	Created On	Modifie	Modified On	First Run Time	Last Run Time	Run	Next Schedule T.
ŧ	2	Full_Upload		admin	Sat, Dec 1, 2012			Mon, Dec 3, 201	Mon, Dec 3, 201	1	Mon, Dec 10, 20
H	3	Incremental	Unsch Edit Jo	edule Job bb Schedule	Dec 1, 2012	4		Sun, Dec 2, 201	Thu, Dec 6, 201	4	Fri, Dec 7, 2012

Figure 8-63 Unschedule Job / Edit Job Schedule

A confirmation box as shown in Figure 8-64 is displayed.

Figure 8-64	Unschedule Job
Confirm	
?	Are you sure you want to unschedule the job with id 6 ?
4	
	Yes No

Click Yes button to unschedule the job.

If you want to edit an existing upload job schedule, right click on the job, and click Edit Job Schedule button. Modify Job Schedule screen as shown below is displayed.

Figure 8-65 Modify Job Schedule

Modify Job Schedule - Incr	emental_Upload		×
Schedule Details			
* Job Name:	Incremental_Upload		
Job Description:			
Schedule Start Date/Tim Repeat Every 1 Weeks on Sunday Tuesday Wede No End date	e Sat, Dec 1, 2012 23:00:37 nesday Thursday Friday Saturday		
		ок	Cancel
	Modify Job Schedule - Incr Schedule Details * Job Name: lob Description: Schedule Start Date/Time Repeat Every 1 Weeks on Sunday Tuesday Wedr No End date Configure Schedule	Modify Job Schedule - Incremental_Upload Schedule Details * Job Name: Incremental_Upload lob Description: Schedule Start Date/Time Sat, Dec 1, 2012 23:00:37 Repeat Every 1 Weeks on Sunday Tuesday Wednesday Thursday Friday Saturday No End date	Modify Job Schedule - Incremental_Upload Schedule Details * Job Name: Incremental_Upload lob Description:

You can reconfigure the schedule by clicking the Configure Schedule button. Except the Job Name all details can be modified.

I

Upload Run Now Jobs

In Upload Run Now Jobs you can view all the run now jobs performed with upload Profile. Upload Run Now Jobs are System upload jobs created by system with the system generated job schedule.

-	oload R	un Now Jobs 🗵									
0	₽ ‡ 8	21 Q		× =							
	Job Id	Job Name	Job Descript	Created	Created On	Modifie	Modified On	First Run Time	Last Run Time	Run	Next Schedule T
Ð	10	Full_Upload		admin	Mon, Dec 3, 201			Mon, Dec 3, 201	Mon, Dec 3, 201	1	
Ð	11	Full_Upload		admin	Mon, Dec 3, 201			Mon, Dec 3, 201	Mon, Dec 3, 201	1	
3	12	Full_Upload		admin	Mon, Dec 3, 201			Mon, Dec 3, 201	Mon, Dec 3, 201	1	
	Run	Id State	Status	Start Time			End Time		Action		
	1	Completer	d Success	Mon, De	c 3, 2012 15:28:	26 +0530	Mon, Dec 3, 2012	15:29:51 +0530	Select Action •		
Ð	13	Full_Upload		admin	Mon, Dec 3, 201			Mon, Dec 3, 201	Mon, Dec 3, 201	1	
B	14	Full_Upload		admin	Mon, Dec 3, 201			Mon, Dec 3, 201	Mon, Dec 3, 201	1	
Ð	15	Full_Upload		admin	Mon, Dec 3, 201			Mon, Dec 3, 201	Mon, Dec 3, 201	1	
Đ	16	Full_Upload		admin	Mon, Dec 3, 201			Mon, Dec 3, 201	Mon, Dec 3, 201	1	
Ð	24	Full_Upload		admin	Wed, Dec 5, 201			Wed, Dec 5, 201	Wed, Dec 5, 201	1	
Đ	25	Full_Upload		admin	Wed, Dec 5, 201			Wed, Dec 5, 201	Wed, Dec 5, 201	1	
	32	Incremental		admin	Thu, Dec 6, 201			Thu, Dec 6, 201	Thu, Dec 6, 201	1	

For user jobs which are already completed without repeat schedule, you can only edit the job schedule. This will change the future runs of the system uploads.

Fij	g <i>ure</i> bload R	8-67 tun Now Jobs 🕷	Edit Job Sche	edule								
0	8	₹ ! Q	×	-								
	Job Id	Job Name		Job Description	Created By	Created On		Modified By	Mod	First Run Time	Last Run Time	Run
Ŧ	11	Incremental_Up	load_1354499025024	1	nduninintenti	Man. Dan 2. 30	20			Mon, Dec 3, 2012 0	Mon, Dec 3, 2012 0	1
Ð	12	Incremental_Up	load_1354500043338	ad_1354500043338			20			Mon, Dec 3, 2012 0	Mon, Dec 3, 2012 0	1
£	13	Full_Upload_13	54501218230		Edit Jo	b Schedule	20			Mon, Dec 3, 2012 0	Mon, Dec 3, 2012 0	1
÷	14	Incremental Up	load 1354501984593		administrat	Mon, Dec 3, 20	120			Mon, Dec 3, 2012 0	Mon, Dec 3, 2012 0	1

The change in schedule will be reflected in the Next Schedule Time of Upload Run Now Jobs.

Connectivity Jobs

Γ

Connectivity Jobs report shows the connectivity related information, along with run count, first and last run time.

Super Administrator • Settings • Management •	Reports • Administra	ation 🔻 He	elp •									cisco
Dashboard Applications												
Device Access verification by balaset rype	• 0	onnectivi	ity Jobs 🗵									
View Locked Credentials	e) = t e	Q -		×	*						
View Server Activity Log Messages		Job Id	Job Name	Job Descript	Created	Created On	Modifie	Modified On	First Run Time	Last Run Time	Run Count	Next Schedu
Syslog Summary												
Syslog Messages												
Collection Profile Run Summary												
Disabled Protocol Report												
Disabled Command Report												
Device Timeout Configuration												
Unreachable Devices												
Inventory Summary												
Config Collected Devices												
Config Data Per Device												
a 🤣 Job Reports	E											
Discovery Jobs												
Inventory Jobs												
Job Management Reports												
4 💋 Server Audit Trails												
Device Management Audit Trails												
Data Collection Audit Trail Report												
Server Audit Trail Report	×						III					+
Administration	+ + H	A Pag	ge 1 of	1 1 11							N	o data to display

For user jobs which are already completed without repeat schedule, you can only edit the job schedule. This will change the future runs of the system uploads.

Figure 8-69 Edit Job Schedule

_											
0	18) B	21 Q	×	-							
	Job Id	Job Name		Job Description	Created By	Created On	1	Modified By Mod	First Run Time	Last Run Time	Run (
Ð	11	Incremental_Upload_1354499025024	1		ndulalatent	Man. Dan. 2. 001	20		Mon, Dec 3, 2012 0	Mon, Dec 3, 2012 0	1
Ð	12	Incremental_Upload_1354500043338	3				20		Mon, Dec 3, 2012 0	Mon, Dec 3, 2012 0	1
ŧ	13	Full_Upload_1354501218230			Edit Jo	b Schedule	20		Mon, Dec 3, 2012.0	Mon, Dec 3, 2012 0	1
	14	Incremental_Upload_1354501984593	3		administrat	Mon, Dec 3, 201	20		Mon, Dec 3, 2012 0	Mon, Dec 3, 2012 0	1

The Change in schedule will be reflected in the Next Schedule Time of Connectivity Run Now Jobs.

I

Import Seed File Jobs

Import seed file jobs report shows the list of imported seed file jobs. You can see the description of each job by clicking the + symbol next to the Job Id. It shows the Run Id, State (Completed/Not Completed), Status (Successful/Aborted), Start Time, End Time.Select the Action button in the report to view either the Job Log details for this particular job, or to cancel a job while it is still running.

Figure 8-70 Import Seed File Jobs

Im	port See	d File Jobs 🛞									
0	■‡ ₽Ì	Q:-		× 🔿							
	Job Id	Job Name	Job Description	Created By	Created On	Modified By	Modified On	First Run Time	Last Run Time	Run	Next Schedule
•	6 2	280thJan	Import SeedF	cspcuser V	Ved, May 15, 201		We	d, May 15, 201 Wed	, May 15, 201	1	
	Run Id	State	Status S	Start Time		End Tin	ne	Action			
	1	Completed	Success V	Ved, May 15,	, 2013 06:11:07 +053	0 Wed, I	May 15, 2013 06:11	:52 +0530 Select	Action 🔻		
Ð	8 i	import13	Import SeedF	cspcuser V	Ved, May 15, 201		We	d, May 15, 201 Wed	, May 15, 201	1	

Miscellaneous Jobs

Miscellaneous Jobs shows a list of all the relatively small one time asynchronous jobs. Example of one such job is Collection Profile export job.
Mi	<i>tre</i> 8- scellane	Jobs 🕷	Misceiia	ineo	us Jobs								
Θ	• † •	Q:-		×									
	Job Id	Job Name		-	Job Description	Created By	Created On	Modified	Modified On	First Run Time	Last Run Time	Run	
9	25	CPExport_13713	12005710			cspcuser	Sat, Jun 15, 2013			Sat, Jun 15, 2013	Sat, Jun 15, 2013	. 1	
	Run Id	State	Status	Start 7	īme		End Time		A	ction			
	1	Completed	Success	Sat,	Jun 15, 2013 2	1:30:05 +06	530 Sat, Jun 16,	2013 21:31	08 +0530	Select Action •			

Key Rotation Job

Key Rotation jobs report shows the list of key rotated jobs. You can see the description of each job by clicking the + symbol next to the Job Id. It shows the Run Id, State (Completed/Not Completed), Status (Successful/Aborted), Start Time, End Time.Select the Action button in the report to view either the Job Log details for this particular job, or to cancel a job while it is still running.

Figure 8-7	72	Key Ro	otation .	Iobs							
Key Rotation Job	(8)										
0 =: e: Q	• (×	•								
Job Id Job I	Name J	ob Description	Created By	Created On	Modified By	Modified On	First Run Time	Last Run Time	Run C	Next Schedule Time	Service Name

View Job Metrics

You can see metrics for job specific details, in Discovery job what type of job was triggered, in inventory and upload what were the service or collection profile name, and in DAV what were the protocols used. Each job metrics displays the average time taken for 100 devices

ew Job Au	etrics *					
0						
Discovery	Job Metrics					
Job Id	Discovery Types	Devices Attempted	Devices Successful	Devices Failed	Devices Skipped	Duration
31	IP based discovery	69	65	3	0	10 Second(s)
28	IP based discovery	69	63	6	0	23 Second(s)
24	IP based discovery	69	63	6	0	21 Second(s)
22	IP based discovery	69	-63	6	0	23 Second(s)
19	IP based discovery	69	63	6	0	23 Second(s)
	Average time taken for 100 devices :					
	Known IP based discovery → 29 Second(s) IP Scan based → Seed IP based →					
DAV Job N	detrics					
Job Id	Protocols Selected		Devices Attempted		Duration	
32	Protocol selected snmpv2c, sshv1, snmpv3, sshv2, https, http, snmpv1, telnet		65		1 Mirute(s)	6 Second(s)
29	Protocol selected srunpv2c, sshv1, srunpv3, sshv2, https, https, srunpv1, telnet		63		1 Minute(s)	6 Second(s)
36	Protocol selected telnet		1		26 Second(s)	
20				63		
25	Protocol selected snmpv2c, sshv1, snmpv3, sshv2, https, https, snmpv1, teinet Protocol selected somm2s, latter takent solution and a chu2 somm4, latter		63		1 Minute(s)	S Second(s)
25 20	Protocol selected srumpv2c, sahv2, srumpv3, sahv2, https, http, srumpv1, teinet Protocol selected srumpv2c, http, teinet, sahv1, srumpv3, sahv2, srumpv1, https		63 63		1 Minute(s) 1 Minute(s)	8 Second(s) 6 Second(s)
25 20 nventory J	Protocol selected srumpv2c, sshv1, srumpv3, sshv2, https, http, srumpv1, teinet Protocol selected srumpv2c, http, teinet, sshv1, srumpv3, sshv2, srumpv1, https ob Metzlcs		63 63		1 Minute(s) 1 Minute(s)	8 Second(s) 6 Second(s)
25 20 Iventory J	Protocol selected srmgv2c, sshv2, srmpv3, sshv2, https, http, srmpv1, teinet Protocol selected srmpv2c, http, teinet, sshv1, srmpv3, sshv2, armpv1, https ob Metrics CP Name/Service Name		63 63 Devices Attempted	Config Col	1 Minute(s) 1 Minute(s) lected Durat	8 Second(s) 6 Second(s) tion
25 20 nventory J Job Id 30	Protocol selected srumpv2c, sshv2, srumpv3, sshv2, https, http, srumpv1, teinet Protocol selected srumpv2c, http, teinet, sshv1, srumpv3, sshv2, srumpv1, https ob Metrics CP Name/Service Name NO5		63 63 Devices Attempted 65	Config Coll 45	1 Minute(s) 1 Minute(s) lected Durat 7 Minu	8 Second(s) 6 Second(s) tion tte(s) 49 Second(s)
25 20 Job Id 30 27	Protocol selected srumpv2c, sshv2, srumpv3, sshv2, https, http, srumpv1, teinet Protocol selected srumpv2c, http, teinet, sshv1, srumpv3, sshv2, srumpv1, https ob Metrics CP Name/Service Name NO5 NO5		63 63 Devices Attempted 65 63	Config Coll 45 45	1 Minute(s) 1 Minute(s) lected Durat 7 Minu 5 Minu	8 Second(s) 6 Second(s) tion te(s) 49 Second(s) te(s) 9 Second(s)
25 20 Job Id 30 27 23	Protocol selected srumpv2c, sshv2, srumpv3, sshv2, https, http, srumpv1, teinet Protocol selected srumpv2c, http, teinet, sshv1, srumpv3, sshv2, arumpv1, https ob Metrics CP Name/Service Name NO5 NO5 NO5		63 63 Devices Attempted 65 63 63	Config Coll 45 45 38	1 Minute(s) 1 Minute(s) lected Durat 7 Minu 8 Minu 8 Minu	s Second(s) 6 Second(s) tion tte(s) 49 Second(s) tte(s) 7 Second(s) tte(s) 7 Second(s)
25 20 noventory J Job Id 30 27 23	Protocol selected srumpv2c, sshv2, srumpv3, sshv2, https, http, srumpv1, teinet Protocol selected srumpv2c, http, teinet, sshv1, srumpv3, sshv2, arumpv1, https ob Mettrics CP Name/Service Name NO5 NO5 NO5 NO5		63 63 Devices Attempted 65 63 63	Contig Col 45 45 38	1 Minute(s) 1 Minute(s) lected Durat 7 Minu 8 Minu 8 Minu	8 Second(s) 6 Second(s) tion tto(s) 49 Second(s) tto(s) 9 Second(s) tte(s) 7 Second(s)
25 20 noventory J Job Id 30 27 23	Protocol selected srungv2c, sshv2, srungv3, sshv2, https, http, srungv1, teinet Protocol selected srungv2c, http, teinet, sshv1, srungv3, sshv2, arungv1, https ob Metrics CP Name/Service Name NOS NOS NOS NOS NOS		63 63 Devices Attempted 65 63 63	Config Col 45 45 38	1 Minute(s) 1 Minute(s) lected Durat 7 Minu 8 Minu 8 Minu	8 Second(s) 6 Second(s) tion te(s) 49 Second(s) te(s) 9 Second(s) te(s) 7 Second(s)
25 20 Job Id 30 27 23	Protocol selected armyv2c, salv2, srmpv3, salv2, https, http, snmpv1, teinet Protocol selected armyv2c, http, teinet, salv1, armpv3, salv2, armpv1, https ob Metzics CP Name/Service Name NO5		63 63 65 63 63	Contig Col 45 45 38	1 Minute(s) 1 Minute(s) lected Durat 7 Minu 8 Minu 8 Minu	8 Second(s) 6 Second(s) lion tre(s) 49 Second(s) tre(s) 9 Second(s) tre(s) 7 Second(s)
25 20 Job Id 30 27 23	Protocol selected armyv2c, sahv2, armyv3, sahv2, https, http, srampv1, teinet Protocol selected armyv2c, http, teinet, sahv1, armpv3, sahv2, armpv1, https ob Metrics CP Name/Service Name NO5 NO5 NO5 NO5 NO5 NO5 CF Name/Service Name CF Name/Service Name		63 63 65 63 63 63 • Device Attempted	Config Col 45 45 38 s Attempted	1 Minute(s) 1 Minute(s) lected Durat 7 Minu 8 Minu 8 Minu 8 Minu	8 Second(s) 6 Second(s) tion tet(s) 49 Second(s) tet(s) 9 Second(s) tet(s) 7 Second(s)

8-73 Job Metric

Audit Trails

Audit Trail report includes all the server related logs. Use the Server Audit Trails Reports sub tab to view the audit trails of the server, data collection and device management aspects. The columns displayed are username, module, sub module, message, log time, job log details.

The sub module includes changes made to session management, patch management, user management, groups. It will also show any unauthorized connection attempts made from other hosts. This report can be exported to PDF, HTML, DOC, CSV (Comma delimited), TXT (Tab delimited) formats.

This section describes the Reports in the following topics:

- Device Management Audit Trails
- Data Collection Audit Trail Report
- Server Audit Trail Report

Device Management Audit Trails

Device Management Audit Trails report includes all device management logs. It also displays the Job Log Details for various jobs. The columns displayed include usern ame, module, sub module, message, log time, job log details. For some jobs, Job Log Details button is displayed. When you click on it, it displays the appropriate job log.

The sub module includes changes made to device credential, discovery subsystem, device access verification, device state change, inventory subsystem, server preferences. The contents of this report can be exported to PDF, HTML, DOC, CSV (Comma delimited), TXT (Tab delimited) formats.

C Q	× 🖸 🛈					
User Name	Module	Sub Module	Message	Log Time	Job Log Details	
admin	Device Management	DeviceCredentials	System Credential(s) hav	Wed, Sep 26, 2012 11:55		
admin	Device Management	DeviceCredentials	System Credential(s) hav	Wed, Sep 26, 2012 14:53		
admin	Device Management	DeviceCredentials	System Credential Set, 10	Wed, Sep 26, 2012 14:53		
admin	Device Management	DeviceCredentials	System Credential Set, 10	Wed, Sep 26, 2012 14:53		
admin	Device Management	DeviceCredentials	System Credential Set, 10	Wed, Sep 26, 2012 14:53		
admin	Device Management	DeviceCredentials	System Credential Set, 10	Wed, Sep 26, 2012 14:53		
admin	Device Management	DeviceCredentials	System Credential Set, 5	Wed, Sep 26, 2012 14:53		
admin	Device Management	DeviceCredentials	System Credential Set, 5	Wed, Sep 26, 2012 14:53		
admin	Device Management	DeviceCredentials	System Credential Set, 5	Wed, Sep 26, 2012 14:53		
admin	Device Management	DeviceCredentials	System Credential Set, 5	Wed, Sep 26, 2012 14:53		
admin	Device Management	DeviceCredentials	System Credential Set, 5	Wed, Sep 26, 2012 14:53		
admin	Device Management	DeviceCredentials	System Credential Set, 5	Wed, Sep 26, 2012 14:53		
admin	Device Management	DeviceCredentials	System Credential Set, 5	Wed, Sep 26, 2012 14:53		
admin	Device Management	DeviceCredentials	System Credential Set, 5	Wed, Sep 26, 2012 14:53		
admin	Device Management	DeviceCredentials	System Credential Set, 5	Wed, Sep 26, 2012 14:53		
admin	Device Management	DeviceCredentials	System Credential Set, 5	Wed, Sep 26, 2012 14:53		
admin	Device Management	DeviceCredentials	System Credential Set, 5	Wed, Sep 26, 2012 14:53		

Figure 8-74 Device Management Audit Trails

Data Collection Audit Trail Report

Data Collection Audit Trail report provides all the data collection profiles audit trails. The columns displayed are username, module, sub module, message, log time, job log details.

This report includes all the changes made to data collection settings which includes collection profile, datasets, platforms, integrity rule and masking rule.

This report can be exported to PDF, HTML, DOC, CSV (Comma delimited), TXT (Tab delimited) formats.

G d	× 🖬 O					
User Name	Module	Sub Module	Message	Log Time	Job Log Details	
system	Data Collection	Mask Rules	Mask rule 'CNC Configura	Wed, Sep 26, 2012 11:00		
system	Data Collection	Integrity Rules	Integrity rule 'CNC Global I	Wed, Sep 26, 2012 11:00		
system	Data Collection	Custom Platforms	User defined platform '_E	Wed, Sep 26, 2012 11:00		
system	Data Collection	Custom Platforms	User defined platform '_IP	Wed, Sep 26, 2012 11:00		
system	Data Collection	Custom Platforms	User defined platform '	Wed, Sep 26, 2012 11:00		
system	Data Collection	Custom Platforms	User defined platform '_A	Wed, Sep 26, 2012 11:00		
system	Data Collection	Custom Platforms	User defined platform '_T	Wed, Sep 26, 2012 11:00		
system	Data Collection	Custom Platforms	User defined platform '	Wed, Sep 26, 2012 11:00		
system	Data Collection	Custom Platforms	User defined platform '_C	Wed, Sep 26, 2012 11:00		
system	Data Collection	Custom Platforms	User defined platform '_Cl	Wed, Sep 26, 2012 11:00		
system	Data Collection	Custom Platforms	User defined platform '_L	Wed, Sep 26, 2012 11:00		
system	Data Collection	Custom Platforms	User defined platform '_C	Wed, Sep 26, 2012 11:00		
system	Data Collection	Custom Platforms	User defined platform '_I	Wed, Sep 26, 2012 11:00		
system	Data Collection	Custom Platforms	User defined platform '	Wed, Sep 26, 2012 11:00		
system	Data Collection	Custom Platforms	User defined platform '_I	Wed, Sep 26, 2012 11:00		
system	Data Collection	Custom Platforms	User defined platform '_G	Wed, Sep 26, 2012 11:00		
system	Data Collection	Custom Platforms	User defined platform ' I	Wed, Sep 26, 2012 11:00		

Figure 8-75 Data Collection Audit Trail Report

Server Audit Trail Report

Server Audit Trail report includes all the server related logs. The columns displayed are usern ame, module, sub module, message, log time, job log details.

The sub module includes changes made to session management, patch management, user management, groups. It will also show any unauthorized connection attempts made from other hosts.

This report can be exported to PDF, HTML, DOC, CSV (Comma delimited), TXT (Tab delimited) formats.

C Q	× 🖬 🛈					
User Name	Module	Sub Module	Message	Log Time	Job Log Details	
gwtserver	Server Administration	SessionManagement	gwtserver logged in from	Wed, Sep 26, 2012 11:01		
cspcadmin	Server Administration	SessionManagement	cspcadmin logged in from	Wed, Sep 26, 2012 11:06		
cspcadmin	Server Administration	SessionManagement	Unauthorized connection	Wed, Sep 26, 2012 11:52		
cspcadmin	Server Administration	SessionManagement	cspcadmin logged in from	Wed, Sep 26, 2012 11:52		
admin	Server Administration	SessionManagement	admin logged in from 10.1	Wed, Sep 26, 2012 11:54		
admin	Server Administration	SessionManagement	admin logged in from 127	Wed, Sep 26, 2012 14:40		
admin	Server Administration	UserManagement	New entitlement/license fi	Wed, Sep 26, 2012 14:40		
gwtserver	Server Administration	SessionManagement	gwtserver logged in from	Wed, Sep 26, 2012 14:51		
admin	Server Administration	SessionManagement	admin logged in from 10.1	Wed, Sep 26, 2012 14:52		
admin	Server Administration	SessionManagement	admin logged in from 127	Wed, Sep 26, 2012 15:32		
admin	Server Administration	UserManagement	User preferences changed.	Wed, Sep 26, 2012 15:32		
admin	Server Administration	SessionManagement	admin logged in from 10.1	Wed, Sep 26, 2012 15:48		
admin	Server Administration	SessionManagement	admin logged in from 10.1	Wed, Sep 26, 2012 17:30		
admin	Server Administration	SessionManagement	admin logged in from 10.6	Wed, Sep 26, 2012 20:56		
admin	Server Administration	SessionManagement	admin logged in from 10.6	Wed, Sep 26, 2012 22:15		
gwtserver	Server Administration	SessionManagement	gwtserver logged in from	Wed, Sep 26, 2012 23:00		
admin	Server Administration	SessionManagement	admin logged in from 10.6	Wed, Sep 26, 2012 23:00		

Figure 8-76 Server Audit Trail Report

Miscellaneous

- Device Launch Pad
- View Locked Credentials
- Disabled Protocol Report
- Disable Command Report
- Device Timeout Configuration
- Device Jump Server Mapping
- Application Profile Run Summary
- Application Discovery Report

Device Launch Pad

I

The Device Launch Pad report provides a list of all devices. You can choose what applications to launch for those devices.

Generating report is a two-step process. First you select the devices, and then you select the applications. Specific application report selected will be launched against the devices selected.

Select Devices				
Managed Devices:			Selected Devices/Groups:	
V2 C ▷ 🦓 VoiceGateways (2) ▷ ▷ 🦓 Video (1) C	*		Storage (1) Wireless (3) LiveNodes (67)	
		*	WLCUCM86P	+
Device_5_0_1_23 WLCUCM86P		+		•
• wsa061 • 🚓 Storage (1) • 🚓 Telepresence (2)				
 ▷ 🤫 Optical (1) ▷ 式 NetworkManagement (1) 				

Figure 8-78 Select application to Launch

Device Launch Pad



Once the selection is done, the specific application will be launched for the given devices.

View Locked Credentials

Γ

This report provides a list of all the locked credentials. The report contains Credential name, Protocol, Username, Locked time, and Will be Unlocked At (based on the configured Lock Period)

View Locked Credential	((8)			
0 Q -	× → ()			
Credential Name	Protocol	User Name	Locked Time	Will be unlocked at
locked	teinet	locked	Tue, Jun 25, 2013 08:43:16 +0530	Tue, Jun 25, 2013 08:43:26 +0530

To unlock a credential, right click on the Credential you want to unlock and select *Unlock the Credential...* option.

L

Disabled Protocol Report

Disabled Protocol Report shows all the protocols that are disabled for a given device/group. The report contents can be exported in one of the supported formats. The supported formats are HTML, PDF, Microsoft Word, CSV, and TXT.

transis I				
10	0 Q.	+ 0		
Ref UniversalGatewaysAndAccessServers	Device	Protocol	Status	Message
R Voice	Oevice_5_0_1_1	snmpv2c	Disabled	The protocol 'snmpv2c' is disabled by for the platform: ACN
🥰 NP (54)	Device 5.0.1.1	ti1	Disabled	The protocol 'ti1' is disabled by for the platform: ACNS
Reference (2)			District	The sector distribution distribution for the school of the sector
video (3)	Oevice_5_0_1_1	teinet	Disabled	The protocol teiner is disabled by for the platform; ACNS
GenericNetworkDevices (1)	Device_5_0_1_1	https	Disabled	The protocol 'https' is disabled by for the platform: ACNS
Ref Storage (1)	Device 5 0 1 1	wmi	Disabled	The protocol 'wmi' is disabled by for the platform: ACNS
R Telepresence (1)			Disabled	The ended line of the desired by the students again
Coptical (1)	Oevice_5_0_1_1	SSRV2	Disabled	The protocol ssrv2 is disabled by for the platform: ACNS
RetworkManagement (1)	Device_5_0_1_1	sshv1	Disabled	The protocol 'sshv1' is disabled by for the platform: ACNS
Ref DataCenter (4)	Device 5 0 1 1	http	Disabled	The protocol 'http' is disabled by for the platform: ACNS
🐳 Wireless (3)		commut.	Disabled	The protocol 'some of is disabled by for the elettern: ACMS
Communications (3)	U Device_5_0_1_1	bringer	Disablog	The protocul simply his disabled by for the platform. Notes
ReviceReadyPlatform	Device_5_0_1_1	snmpv3	Disabled	The protocol 'snmpv3' is disabled by for the platform: ACNS
Routers (10)				
Revenues (55)				
ReplicationNetworking (5)				
Ref Switches (14)				
Recurity (6)				

Figure 8-80 Disabled Protocol Report

Disable Command Report

Disabled Command Report shows the details of commands that are disabled for a given device.

isabled Command Report					
20	0 Q.	× → ()			
🙀 UniversalGatewaysAndAccessServers	Device	DatasetType	Command	Status	Message
Voice	2 Device 5_0_1_29	SNMP	matches regular e	Disabled	
💏 NP (1)					
VoiceGateways					
📸 Video					
CenericNetworkDevices					
🚓 Storage					
Relepresence					
Coptical					
RetworkManagement					
🙀 DataCenter					
📸 Wreless					
🙀 UnifiedCommunications					
ServiceReadyPlatform					
Routers (1)					
LiveNodes (1)					
ApplicationNetworking					
💏 Switches					
Security					

Figure 8-81Disable Command Report

Device Timeout Configuration

Device Timeout Configuration report provides all the timeout configurations specified for different devices, along with retry counts. These values are populated from the timeouts configured in the Global Timeouts under Advanced Settings. This report can be exported into PDF, HTML, DOC, CSV (Comma delimited), TXT (Tab delimited) formats.

Figure 8-82	Device Timeout Configuration
1 151110 0 01	Derice Timeour Configuration

20	0 Q.+	× → 0		
🖏 UniversalGatewaysAndAccessServers	Device	Protocol	Timeout	Retry Count
Voice	172.21.31.13	snmpv1	5000	2
NoiceGateways	172.21.31.13	snmpv2o	5000	2
GenericNetworkDevices (2)	172.21.31.13	snmpv3	5000	2
Storage	0 172.21.31.13	teinet	10000	
Telepresence	Ø 172.21.31.13	sahut	10000	
RetworkManagement	() 172.21.31.13	sshv2	10000	
🖏 DataCenter	172.21 137.172	snmpv1	5000	2
📸 Wreless	Ø 172.21.137.172	snmpv2c	5000	2
ServiceReadyPlatform	Q 172.21.137.172	snmpv3	5000	2
Routers	C 172.21.137.172	teinet	10000	
ApplicationNetworking	Ø 172.21.137.172	sehvi	10000	
Switches	172.21.137.172	sshv2	10000	
re Security	The doctriner bacture			
	Page 1 of 1	2 2i		Displaying 1 -

Device Jump Server Mapping

All the devices or groups that are mapped to the jump server are shown in this report as shown in Figure 8-83. This report provides the details such as device/group name or IP address of the device and the Jump server IP which it is mapped to.

Figure 8-83	Jump server	Mapping	
Device JumpSo	erver Mapping 🗵		
0 Q		× 🔿 🔘	
Device		Jump Server IP Ad	ldress/ Host Name
Routers		10.126.77.90	
172.20.106.53		10.126.77.90	

Application Profile Run Summary

I

Application profile run summary report provides a summary of the completed application profiles as shown in Figure 8-84.

Application Profile Ru	In Summary 🗵			
0 Q-	× → 0			
Profile Name	State	Status	Start Time	End Time
test	Completed	Success	Wed, May 15, 2013 02:57:27 +0530	Wed, May 15, 2013 02:57:37 +053

Figure 8-84 Application Profile Run Summary

Application Discovery Report

Application Discovery Report shows the list of discovery applications installed on the server (see list below). For each installed application it shows the system level information like, OS type, OS version, CPU type, Total memory installed and so on as shown in Figure 8-85.

Appl	ication Disc	overy Report																
0	e; e: Q	-	× ⇒	0														
8	P Address	Mac Address	Subnet Address	OS Name	OS Version	OS Vendor	OS Type	CPU	CPU Type	CPU Speed	Total Memory	Free Memory	Hardware Vendor	Hardware Product	Hardware Version	Hardware Serial	Hardware UUID	Is Virtual N
Ð 1	72.21.31.13	00:50:56:99:5E:84	255.255.255.0	Linux	5.8		CentOS	GenuineIntel	Intel(R) Xeo	2666.761	4119040 kB	2077344 kB	VMware, Inc.	VMware Virtual	None	VMware-42 19	42199D27-C1E	YES
± 1	72.21.137	00:50:56:99:5F:4F	255.255.255.0	MicrosoftWindo	6.1.7601	MicrosoftCo		Intel64Family6	Intel(R)Xeo	2133	8385852	6912716	VMware,inc.	VMwareVirtualP	None	VMware-42190		

Expanding each row shows a list of installed application and its details like Name of the application, Version, Vendor, Path where the application is installed, Installed date and its running state as shown in Figure 8-86.

Installed Discovery Applications

Here is the list of applications that can be discovered on Microsoft Windows and Linux platforms.

Microsoft Window:

Tomact, MySQL, ArgoSoft, DB2, SQL Server, OpenLDAP, NetBIOS Session Service, EmailArchitect Super Service, JBOSS, DNS Server, MSMQ, VMWare Workstation, WebSphere, Oracle, RPC, IIS Admin, SANSurfer.

Γ

Linux:

Tomcat, MySQL, httpd, OpenLDAP, FTP Server, SendMail, Telnet, DNS Server.

Figure 8-86 Application Discovery Report Expanded

6)	et et q		x	- 0														
	IP Address	Mac Address	Subnet Addre	iss OS Name	OS Version	OS Vendor	OS Type	CPU	CPU Type	CPU Speed	Total Memory	Free Memory	Hardware Vendor	Hardware Product	Hardware Version	Hardware Serial	Hardware UUID	ls Virtu
3	172.21.31.13	00:50:56:99:5E:84	255.255.255	0 Linux	5.8		CentOS	GenuineIntel	Intel(R) Xeo	2666.761	4119040 kB	2077344 kB	VMware, Inc.	VMware Virtual	None	VMware-42 19	42199D27-C1E	YES
	Name		Version	Vendor	Path Status	Install Date												
	EmailArch	itect Super Service	e 8.13.8	CentOS	is runni	ng Fri, Mar 1	6, 2012 06:	55:24 +0530										
	httpd		2.2.3	CentOS	stoppe	Fri, Mar 1	5, 2012 06:	55:18 +0530										
	Telnet		0.17	CentOS	is runni	ng Fri, Mar 1	8, 2012 06:	54:32 +0530										
	SMB Serv	er	3.0.33	CentOS	stoppe	Fri, Mar 1	5, 2012 06:	55:21 +0530										
	openidap		2.3.43	CentOS		Fri, Mar 1	5, 2012 06:	54:38 +0530										
	FTP Serve	ər	2.0.5	CentOS	stoppe	Fri, Mar 1	6, 2012 06:	55:39 +0530										
	DNS Serv	er	9.3.6	Oracle America	stopper	Mon, Nov	19, 2012 0	2:31:28 +0530										
	Mysql		5.0.77	CentOS		Fri, Mar 1	5, 2012 06:	54:43 +0530										
9	172.21.137	00:50:56:99:5F:4F	255.255.255	0 MicrosoftWind	io 6.1.7601	MicrosoftCo.		Intel64Family6	. Intel(R)Xeo	2133	8385852	6912716	VMware,Inc.	VMwareVirtualP	None	VMware-42190		
	Name		Version	Vendor	Pa									Status In	stall Date			
	Remote P	rocedure Call			C:	Windows/\syst	em32\\local	tor.exe						Stopped				
	EmailArch	itect Super Service	8		C:1	ProgramFiles()	(86)\\Email	Architect(\Email/	ArchitectSvc.ex	9				Running				
	JBoss We	b			\C	\ProgramFiles(x86)\\JBos	s.org\\JBossWel	b2.1\\bin\\jbossv	veb.exe\				Stopped				
	Message	Queuing			C:	Windows\\syst	em32\\mqs	vc.exe						Running				
	SQL Servi	er	9.4.5000	.00 MicrosoftCo	rporation \c:	ProgramFiles(:	(86)\\Micro	softSQLServer/\	MSSQL.111MSS	QL\\Binn\\sqt	servr.exel-sSQ	LEXPRESS		Running				
	IIS Admin				C:	Windows\\syst	em32\\inets	rv/\inetinfo.exe						Running				



Applications - Administration

Administration

Use the Administration tab to create users for the CSPC server, take backups of the collected data, look at the server patches, etc.

This section describes the Reports in the following topics:

- User Management
- User Preferences
- Alert Management
- Backup and Restore
- Log Preferences
- Miscellaneous Applications

User Management

The User Management sub tab is used to create users and modify user preferences for a given CSPC server.

This section describes the options in the following topics:

- Manage Users
- Manage Remote Authentication Servers
- Login Settings
- User Session Report

Manage Users

When you double-click *Manage Users*, a new Manage Users window appears which allows you to create and manage the collector users, as shown in the following screen.

Γ

Manage Users 🕱				
e q	× 🔂 Add User 谢	lodify User. 🛛 Remove User 🔛 🚺		
Login	Full Name	Authentication Type	User Group	
cspcadmin		Local User	Administrator	
admin	Super Administrator	Local User	Administrator	

Figure 9-1 Manage Users



	ew User	
User Identification Login Id: Auth Type: Password: Full Name:	Local User	
Group Membersh * Group Name:	ip Administrator	~
Contact Informati	on	
Contact Informati Email Address:	on	5
Contact Informati Email Address: Phone Number:	on	

To add a new user, click *Add User*. This window shows the following information for each defined user on the system:

- Login ID
- Authentication Type (Local, Remote User Authentication)
- Password (masked)
- Full Name
- · Group Name is the group of users belonging to
 - Administrator: Administrator will have full access on the entire CSPC server.
 - External Client User: External Client User is used for the purpose of external client authentication on collector. Login access for this user through GUI and CLI interface is disabled. Security features such as password expire, user account lock, session time out are not applicable for this type of user group.
 - Network Operator: Network Operator will have full access on managed network, and he/she can configure all the settings related to management. But he can't make any changes that effect theserver.
 - Report user: Report User can only be able to view reports.
 - SFTP User: Users can be of two types:
 - Local User: User configured in the local database.
 - Remote User: User configured on some remote authentication server. For remote users, password field is not needed.
- Email Address
- Phone Number
- Pager

Click **Modify User** to modify the details of existing user. Click **Remove User** to delete an existing user. Click **OK** a prompt appears to verify the password. Enter the password and click **OK**.

Fig	ure 9-3 Verij	fy User Password	
	Verify User Passwo	rd	×
	* User Name	admin	
	* Password		
		OK Cancel	

Manage Remote Authentication Servers

I

If the user authentication type is remote authentication, CSPC gets the user credentials from a remote authentication server. The remote authentication servers need to be set up for the server to contact for credentials as defined below.

	Authentication Type	Details	
neth1	LDAP Server	Idap://serv1:389/	
Add R	mote Authentication Server	>	2
с с	ightweight Directory Access Protocol (LE emote Authentication Dial In User Servic Ferminal Access Controller Access-Control	OAP) Server e (RADIUS) Server System Plus (TACACS+) Serve	(
		Add Cancel	

Figure 9-4 Setup Remote Authentication Servers

Login Settings

You can select and de-select the security options as per your requirements. Key rotation helps you to change the encryption key once in 3,6,12, or 24 months as per your requirements.

Security Settings	
Disable Captcha Prompt:	
Password Settings	
Expire Passwords (days):	Never After 90
Session Settings	
Logout (mins):	O Never O After 20
Encryption Settings	
Key Rotation Interval (months):	Never O After
Key Encryption Key (KEK):	
Data Encryption Key (DEK):	
Remote KMS Type:	none
Access Key Id:	
Secret Key:	
Region:	×

Figure 9-5 Login settings

Γ

To configure the login settings, perform the following:

- Step 1 Select the Disable Captcha Prompt to remove the captcha prompt appearing on login screen
- Step 2 Enter the number of days after the password should expires
- Step 3 Set the session Logout time in minutes
- Step 4 Select the Key Rotation Interval as Never or to occur After months
- Step 5 Select Key Encryption Key (KEK) or/and Data Encryption Key (DEK)
- Step 6 Select Remote KMS Type to store the data as none or AWS
- Step 7 If AWS selected a prompt appears read it and click OK.
 - a. Enter Access Key Id and Secret Key.
 - **b.** Select the required **Region**.

User Session Report

The User Session Report window displays the list of users who are currently connected to the server.

Figure 9-6	User Session K	Report				
User Session Repo	rt 🗵					
C Q	× 🖬 🛈					
Login	User Type	Remote Server	User Role	Logged In From	Login Time	
admin	Local User		Administrator	10.65.78.187	Tue, Oct 16, 2012 15:18:	
admin	Local User		Administrator	173.39.68.162	Mon, Oct 15, 2012 14:46:	
cspcadmin	Local User		Administrator	10.142.32.202	Wed, Oct 10, 2012 12:21:	
admin	Local User		Administrator	173.39.69.22	Mon, Oct 8, 2012 11:59:1	-
admin	Local User		Administrator	173.39.68.162	Mon, Oct 15, 2012 15:39:	
admin	Local User		Administrator	173.39.69.22	Thu, Oct 11, 2012 16:00:	
admin	Local User		Administrator	64.103.237.48	Tue, Oct 16, 2012 15:09:	
admin	Local User		Administrator	173.39.68.162	Mon, Oct 15, 2012 11:12:	
admin	Local User		Administrator	10.35.90.161	Wed, Oct 10, 2012 15:33:	
admin	Local User		Administrator	173.39.69.22	Thu, Oct 11, 2012 13:37:	
admin	Local User		Administrator	173.39.68.183	Tue, Oct 16, 2012 13:41:	
admin	Local User		Administrator	10.142.32.184	Thu, Oct 11, 2012 12:44:	
admin	Local User		Administrator	10.142.32.156	Tue, Oct 9, 2012 14:47:4	
admin	Local User		Administrator	173.39.69.22	Thu, Oct 11, 2012 15:01:	
admin	Local User		Administrator	10.65.83.64	Fri, Oct 5, 2012 14:58:46	
admin	Local User		Administrator	10.142.32.156	Mon, Oct 8, 2012 11:20:3	
admin	Local User		Administrator	10.35.90.161	Wed, Oct 10, 2012 18:34:	-

User Preferences

The User Preferences sub tab is used to modify user preferences for a given CSPC server.

This section describes the options in the following topics:

- Modify Data/Time Preference
- Configure Default Device Display Property

Modify Data/Time Preference

Modify Data/Time Preferences allows you to setup the data and time preferences. You can choose to display date and time in client time zone or in the server time zone as shown in Figure 9-7.

After the changes are done, the preferences are stored for the specific user account.

et Date/Time Preference		
Date/Time Display Propertie Date/Time Display Type:	s Display Date/Time in Client Tin	e Zone 👻
	Display Date/Time in Server Tim	Zone
	Display Date/Time in Client Time	Zone
	a contraction of the second statement of the second statem	

Configure Default Device Display Property

Configure Default Device Display Property allows you to select the device property that will be the default for all managed devices.

Select default dis	play property for all the managed devices
Display Property:	Host Name 🗸
	Management Ip Address
	Host Name
	Terminal Prompt
	DNS Name
	SNMP Sys Name
	SNMP Sys Object Id
	User Defined Name
	Mac Address
	Drimony Davica Nama

Figure 9-8 Configure Default Device Display Property

Alert Management

The Alert Management sub tab is used to define Email settings and other alert for a given CSPC server. This section describes the options in the following topics:

- Email Settings
- Manage Subscribers ٠
- ٠ Alert Configuration

Email Settings

I

This setting provides you with an option to configure a SMTP server for mail exchange.

	_
C	
Please enter port number.	
Please enter recipients email address.	
Please enter senders email address.	5
	\leq
Please enter sender's user name	
1	
Please enter sender's user name	

Enter all the Mandatory fields and click OK

Field Name	Descriptions
SMTP Server	Server name or identity of the server
SMTP Port	Port number used for the server
Email To	Receiver mail address
Sender's Mail ID	Sender mail address
Username	Login name
Password	Login password

To reset the SMTP Settings to default value click Default Settings.

Only **Admin** user can configure/modify the email settings, however the network user can update "Email To" option if the settings are configured. Incase if the login settings are not defined, an error will be thrown for **Network** user.

Manage Subscribers

This option enables you to manage all the subscribers.

Figure 9-10	Manage Subscribers			
Manage Subscribers 🛞				
0 Q.	X 🖸 Add Subscribers 谢 Modify Subscribers .	🔵 Remove Subscribers 👄 🔘		
Module	Notification Enabled	Notification Type	Emails Configured	
DISCOVERY	у	DB		

Step 1 To add a Subscribers, click Add Subscribers the below screen appears shown in Figure 9-11

Server Information		
* Module Name:	ALL	*
Notification Enabled:		
Notification Type:	Display on GUI only	~
Email To:	Email + Display on GUI	
	Display on GUI only	

Step 2 Enter *Module Name*, select *Notification Enabled*, and if required enter *Notification Type* and *Email To* and then click *OK*.

Alert Configuration

Γ

Alert a workflow CSPC service and pushes the notifications to the user. You do not need to login every time to see what the status of the job.

Figure 9-12	Alert Configurations	
Alert Configuration		
0 Q.+	🛪 🚯 Add Alert Configurations 💣 Modify Alert Configurations 🛢	Remove Alert Configurations 👄 🔘
Module	Protocols	Percentage
Discovery		3
Inventory	HTTP, Telnet, SNMP, WMI, TL1, SSH, LDAP	6,6,6,6,6,6

Step 1 To add an alert, click Add Alert Configurations the screen appears as shown in Figure 9-13

Alert Configuration Edito	or - Create a new Configuration	×
Alert Configuration		
Alert Configuration	1	
* Module Name:	Inventory	Y
All:	All Success Percentage:	0
SNMP:	SNMP Success Percentage:	0
TELNET:	TELNET Success Percentage:	0
HTTP:	HTTP Success Percentage:	0
WMI:	WMI Success Percentage:	0
TL1:	TL1 Success Percentage:	0
SSH:	SSH Success Percentage:	0
LDAP:	LDAP Success Percentage:	0
IIOP:	IIOP Success Percentage:	0
	Help	OK Cancel

Figure 9-13 Add Alert Configurations

Step 2 Select the Module Name from the drop down,

- If Discovery is selected, then enter the Discovery success Percentage value
- If *Inventory* or *DAV* is selected, then select the protocol(s) and the enter the success percentage value for protocol(s)

```
Step 3 Click OK
```



You can select ALL or any protocol of your choice

Backup and Restore

The Backup and Restore sub tab is used to take backups of the collector data, as well as to restore the backed up data in case of a failure.



To make the file transfer more secure:

• It is recommended to use the secure protocols SFTP and SCP against insecure one's such as FTP and TFTP. If SFTP server is selected, then refer to RSA SHA 256 Fingerprint to generate the corresponding host key.

This section describes the options in the following topics:

- Backup
- Restore Backup

Backup

The Backup option allows you to select the database backup at a given instant, or to specify options for periodic database backup.

To perform the backup job, follow the below steps:

Step 1 Select FTP Server, SFTP Server, or Local Server

- If FTP Server selected enter the following
 - Server Name: IP Address/Host Name of the FTP server
 - User Name: FTP server username
 - Password: FTP server password
- If SFTP Server selected enter the following
 - Server Name: IP Address/Host Name of the SFTP server
 - User Name: SFTP server username
 - Password: SFTP server password
 - Fingerprint: Authentication received from server
- If Local Server is selected continue



It is recommended to use the secure protocol SFTP against insecure FTP.

- Step 2 Select required options Incremental Backup or/and Full Backup or/and Ignore Inventory Data and enter the following:
 - Target Directory: The directory where the backup file needs to be stored
 - · Backup File prefix: The tag that will be appended to the backed up file
 - To start backup instantly select **Run Backup Now** or to schedule the job later select **Schedule Periodic Backup.** For Periodic backup, you can configure schedule to specify the range of recurrences, Schedule start date/time, Schedule end date/time and recurrences pattern for the data backup. This is shown in Figure 9-15.
 - Job Name: Enter the job name
 - Job Description: Enter the description of the job



To remove inventory data from backup select Ignore Inventory Data.

ıp			
FTP Server Details			
Backup To:	FTP Server SFTP Server Local Server		
Server Name:	a		
User Name:	xyz		
Password:	••••		
Fingerprint:	qwer		
Incremental Backup	🗸 Full Backup 📝 Ignore Inventory Data		
incremental Backup		Full Backup	
larget Directory:		Target Directory:	
3ackup File Prefix:		Backup File Prefix:	
		Run Backup Now	
		Schedule Periodic B	ackup
Job Name:		* Job Name:	Periodic BackupRestore
ob Description:		Job Description:	
		No schedule configu	ured
		Configure Schedule	
able Incremental Bac	kup		Exclude Backup Files
			Remove Settings HelpOK Ca

۵, Note

To disable incremental backup click Disable Incremental Backup and this will prompt for the restart of the CSPC. Similarly, to enable click Enable Incremental Backup and it also requires restart.

Figure 9-15 Con	nfigure	Schedule
-----------------	---------	----------

Kange of Kecurance		
Schedule Start Date/Ti	me May 27,2013 3 04 : 21 :	Repeat schedule
	C No end date	
Schedule End Date/ I in	e End by May 27,2013 3 04	24 🗘
Recurance Dattern		
in annual in the		
C Dade		
C Weekby		
C Monthly		
C Vearly		
The second se		

Step 3 To exclude the files from **Backup** unselect the files as shown in Figure 9-16.

Γ

To see the files here you have enter the file path in properties file.

Fig	ure 9-16	Exclude Backup Files		
Exc	ude Backup Files		×)
✓	File Path			1
V	/opt/CSPC/logs/csp	ocwebui.log		
				1
		Please unselect to exclude	de backup. OK Cancel	

Restore Backup

The Restore Backup option lets you restore a previously stored data backup. You need to provide the server information, such as where the backup file resides, and CSPC loads that backup to the system. This is shown in Figure 9-17.

To restore the backup file, follow the below steps:

- Step 1 Select FTP Server or Local Server
 - If FTP Server selected enter the following
 - Server Name: IP Address/Host Name of the FTP server
 - User Name: FTP server username
 - Password: FTP Server Password
 - If SFTP Server selected enter the following
 - Server Name: IP Address/Host Name of the SFTP server
 - User Name: SFTP server username
 - Password: SFTP server password
 - Fingerprint: Authentication received from server
 - If Local Server is selected continue



It is recommended to use the secure protocol SFTP against insecure FTP.

Step 2 Select Incremental Restore or/and Full Restore and enter the following:

- Directory Name: The directory where the backup file needs to be restored
- Backup File: The backup file name
- To start restore instantly, select **Run Restore Now** or to schedule the job later select **Schedule Periodic Restore.** For Periodic restore, you can configure schedule to specify the range of recurrences, Schedule start date/time, Schedule end date/time and recurrences pattern for the data backup. This is shown in Figure 9-18.
- Job Name: Enter the job name
- Job Description: Enter the description of the job

Restore From.	FTP Server SFTP Server Control Local Server		
* Server Name:	a		
User Name:	xyz		
* Password:	(••••		
* Fingerprint:	abc		
Incremental Restore	V Full Restore		
Incremental Backup		Full Backup	
Directory Name:	Get Backup Files	Directory Name:	Get Backup File
Backup File:	× (*)	* Backup File:	
Run Restore Now		Run Restore Now	
🔘 Schedule Periodic	Restore	💿 Schedule Periodic	Restore
* Job Name:	Periodic BackupRestore	* Job Name:	Periodic BackupRestore
Job Description:		Job Description:	
No schedule confi	gured	No schedule config	gured
		Configure Schedule	

Figure 9-17 Restore Server Backup

Γ

Note To enable slave mode click Enable Slave Mode and it requires CSPC to restart. This disables all other jobs expect Backup and Restore jobs on CSPC. Similarly, to disable click Disable Slave Mode and it also requires restart.

Figure 9-18 Configure Schedule

Range of Recurance						
Schedule Start Date/Tim	e May 27,2013	3	04 : 21 :	📄 Repeat s	chedule	
Schedule End Date/Time	No end date End by May	27,2013	0	4 : 24 🛟		
Recurance Pattern						
Minutely Every						
C Daily						
C Weekdy						
C Monthly						
C Yearly						

Log Preferences

The Server Log Preference sub tab is used to manage the server logs that are helpful in identifying and fixing any support issues.

This section describes the options in the following topics:

- Log Preferences
- Export Log Files

Log Preferences

Using Log Preferences, you can select detailed logging level for each module of CSPC. Log preferences of the server as well as UI component can be changed.

Logging levels could be any one of the following:

- Fatal
- Error
- Warning
- Information
- Debug
- Trace

Log levels can be changed by clicking on the logging level and selecting the appropriate level. You can also select *none* and ignore the log for a specific module. This setting will be used for displaying the log messages in CSPC logs. Click **Reset to Default** to change all the log levels to default values.

Figure 9-19 Log Preferences

Module Name	Logging Level
Cli	Warning
Discovery	Warning
HelperServers	Warning
Common	Warning
WebUI	Warning
Der	Warning
Dav	Warning
Collection	Warning
Export	Warning
Transport	Warning
Core	Warning
XmlApi	Warning

Export Log Files

Γ

The Export Log Files feature allows you to export all the server log files to the Cisco CSP support staff in case there is an error, and the support staff needs to access the server logs. Log Files can be exported both based on file name or time stamp. This is shown in the following screen.

Figure 9-20 E	Export Log Files by File	
Export Log Files		×
Select Server Log	files	
Log Search Type:	Get the selected files	
Select All	Get the selected files	
discovery_cso/	Get the logs for the selected dat ascovery_cso.iog	*
/.t.swp		
cspcwebui/csp	cwebui.log.2012-10-04	=
cspcwebui/csp	cwebui.log.2012-10-12	
cspcwebui/csp	cwebui.log.2012-09-29	
cspcwebui/csp	cwebui.log.2012-09-27	
cspcwebui/csp	cwebui.log.2012-09-26	
cspcwebui/csp	cwebui.log	
cspcwebui/csp	cwebui.log.2012-10-13	
cspcwebui/csp	cwebui.log.2012-09-30	
cspcwebui/csp	cwebui.log.2012-10-05	-
	Help OK Cano	el

F	igure 9-21 Ex	port Log Files by	Tim	estan	np		
Е	xport Log Files						×
F	Select Server Log fil	es					
L	Log Search Type: G	et the logs for the	e seleo	cted	da 🗸		
L	Select Time Period						
L	Start Date/Time	October 17,2012	•	20	25	\$	
	End Date/Time		•	20	25	\$	
L	Select All						
L	discovery_cso					-	
L						Ξ	
L	cspcwebui						
L	Jobid_385_Runid_	1					
L	Jobid_141_Runid_	1					
	postout					-	
L							-
		Help	ж		Can	cel	

Miscellaneous Applications

The Miscellaneous Applications sub tab shows server information, resynchronizes the client to server and provides some diagnostic tools.

This section describes the options in the following topics:

- Manage Add-on Process
- Manage UI Add-Ons
- Server Properties
- Diagnostic Tools
- XML API Console

Manage Add-on Process

Manage Add-on Process provides details on all the Server Processes including add-on processes for CSPC. This report includes Process Name, Process Type, Process State, and a Message associated withthat process as shown in Figure 9-22.



NOS service will have audit addon process and DCOS service will have dcos addon process

Figure 9-22 View Server Process Summary

0 Q	× → 0			
Process Name	Process Type	Process State	Message	
Agent	Java Process	STARTED	Process started	

Manage UI Add-Ons

Manage UI Add-Ons screen shows the list of Add-Ons, action taken on the Add-On, the user who initiated the action, time of action and next possible action.

Figure 9-23	Manage UI Add-Ons			
Manage UI Add-ons 🛪				
0 Q.	× 🔿			
Add-on +	Last Action Taken	Action Initiated By	Action Initiated At	Possible Next Action

Server Properties

The View CSPC Server Properties window shows information about the server itself. The data shown in this window includes *Server Properties and License Properties*. This gives information, such, the IP address of the server, server version, default gateway, sever time zone, etc., as shown in Figure 9-24.

■ Server Properties Server Host/Ip Address localhost.localdomain Server Version 2.9 CPU Model Intel(R) Xeon(R) CPU E5-2697 v4 @ 2.30GHz CPU cores 12 RAM Size 15867M Hard disk size 975G Hardware Type VMware Virtual Platform	
Server Host/Ip Address localhost localdomain Server Version 2.9 CPU Model Intel(R) Xeon(R) CPU E5-2697 v4 @ 2.30GHz CPU cores 12 RAM Size 15867M Hard disk size 975G Hardware Type VMware Virtual Platform	
Server Version 2.9 CPU Model Intel(R) Xeon(R) CPU E5-2697 v4 @ 2.30GHz CPU cores 12 RAM Size 15867M Hard disk size 975G Hardware Type VMware Virtual Platform	
CPU Model Intel(R) Xeon(R) CPU E5-2697 v4 @ 2.30GHz CPU cores 12 RAM Size 15867M Hard disk size 975G Hardware Type VMware Virtual Platform	
CPU cores 12 RAM Size 15867M Hard disk size 975G Hardware Type VMware Virtual Platform	
RAM Size 15867M Hard disk size 975G Hardware Type VMware Virtual Platform	
Hard disk size 975G Hardware Type VMware Virtual Platform	
Hardware Type VMware Virtual Platform	
S Network Properties	
Default Gateway 10.126.77.1	
Ip Address (eth0) 10.126.77.199/255.255.255.0	

Figure 9-24 Server Properties

- CSPC Registration Properties: provides details of the certificate stored in CSPC that identifies the appliance and should be constant as long as the collector has not been decommissioned (with the exception of transition from evaluation to a service certificate).
- Connectivity Registration Properties: provides details of the certificate stored in CSPC, that after application to connectivity enables connectivity to communicate with Cisco. Any service certificate may be selected for connectivity certificate. Certificates supporting web-sockets have precedence over those that do not support.

You can also find the Certificate information of the server by clicking *Registration Certificate Properties.* You can expand each registration certificate to see the properties and click **Add** and browse to add new certificate file and click **Replace** to upgrade or change the certificate. Click **Delete** to remove the certificate as shown in Figure 9-25.

CC00000000144				
CSP0001028141			~	
Certificate ID	1			
Customer ID	CSPC_NC	95		
Certificate Service Name	NOS			
erial Number	675432113	34red		
nventory Name	CSPC_NC	9S		
'rovisional Certificate Service N	Jame			
Appliance ID	CSP00010	28141		
xpiration Date	2099-01-0			
CSP0001028140				
Certificate ID	2		~	
Customer ID	CSPC NO	95		
1: CSP0001028141	NOS	Add Replace Delete Replace Delete	-	

iouro	9_25	Liconso	Pronortio
ie ui c	1-45	Lucinsc	ITODUNC

Note

CSPC supports multiple service on single collector and more than 10 k devices are uploaded. You can install the certificate at any point of time. The first certificate is applied during the installation. If you add multiple registration certificates for a service, then company name should be same for all the certificate or if it is different service on the same collector then company name can differ. You can upload multiple registration certificates for different servicer on the same collector and configures based the certificate. Name of the service should be in accordance with the registration certificate. Old certificate created before 2.8 will not work in fresh installation, but upgrade can be done. Service specific Registration Certificate is used to upload data to backend of the specific service.

Note Maximum allowed certificates for NOS/CSPT service is four and rest can have one.

Diagnostic Tools

Γ

This option provides simple diagnostic tools like *ping* and *traceroute* to check if the device is availableor connectivity is to the device is established. Pick the command you want to use and select the deviceon which you want the diagnostics to run, and click *Run Command*. The results appear in the *Command Result* section of the window.

Figure 9-26	Diagnostic Tools - ping utility	,	
Diagnostic Tools			×
* Command	ping 👻		
* Target Host	google.com	Browse	
Timeout (in secs)	10		
Run Command			
1			
2			
3 PING maa03s1	6-in-f8.1e100.net [google	e.com] with 56(84) bytes of data	ι.
4			
5 6 Avg Response	Time:0.0 ms Total Pkts	Sent:5 Pkts Received:0	
7			
8			
9			
10			
12			
13			
14			
15			
16			
17			
10			
			Help Close

Figure 9-27 Diagnostic Tools - Trace Route Utility

<pre>* Command trace route v * Target Host google.com Browse Timeout (in secs) 10 1 traceroute to google.com (74.125.236.164), 30 hops max, 40 byte packets 2 1 10.105.134.1 (10.105.134.1) 1.025 ms 0.605 ms 0.493 ms 3 2 14.160.83.97 (14.160.83.97) 0.401 ms 0.512 ms 0.643 ms 4 3 10.104.146.37 (10.104.146.37) 0.423 ms 0.548 ms 0.510 ms 5 4 10.104.146.9 (10.104.146.9) 0.596 ms 0.846 ms 0.799 ms 6 5 bgl11-sbb-gwl-gig3-10.cisco.com (72.163.187.65) 0.639 ms 0.343 ms 0.504 ms 7 6 bgl11-rbb-gwl-tenl-1.cisco.com (72.163.171.138) 0.299 ms 0.290 ms 0.279 ms 9 8 bgl11-dmzbb-gwl-gig2-43.cisco.com (72.163.216.230) 1.472 ms 1.505 ms 1.250 ms 10 9 maa03s16-in-f4.1e100.net (74.125.236.164) 0.847 ms 0.730 ms 0.639 ms 112 13</pre>
<pre>* Target Host google.com Browse Timeout (in secs) 10 * Target Host google.com (74.125.236.164), 30 hops max, 40 byte packets 1 traceroute to google.com (74.125.236.164), 30 hops max, 40 byte packets 1 10.105.134.1 (10.105.134.1) 1.025 ms 0.605 ms 0.493 ms 2 14.160.83.97 (14.160.83.97) 0.401 ms 0.512 ms 0.643 ms 4 3 10.104.146.37 (10.104.146.37) 0.423 ms 0.548 ms 0.510 ms 5 4 10.104.146.9 (10.104.146.9) 0.596 ms 0.846 ms 0.799 ms 6 5 bgll1-sbb-gwl-gig3-10.cisco.com (72.163.187.65) 0.639 ms 0.343 ms 0.504 ms 7 6 bgll1-rbb-gwl-tenl-1.cisco.com (72.163.171.138) 0.299 ms 0.290 ms 0.279 ms 9 8 bgll1-dmzbb-gwl-gig2-43.cisco.com (72.163.216.230) 1.472 ms 1.505 ms 1.250 ms 10 9 maa03s16-in-f4.1e100.net (74.125.236.164) 0.847 ms 0.730 ms 0.639 ms 11 12 13</pre>
Target Host google.com Browse Timeout (in secs) 10 Run Command 10 1 traceroute to google.com (74.125.236.164), 30 hops max, 40 byte packets 2 1 10.105.134.1 (10.105.134.1) 3 2 14.160.83.97 (14.160.83.97) 0.401 ms 0.512 ms 0.643 ms 4 3 10.104.146.37 (10.104.146.37) 0.423 ms 0.548 ms 0.510 ms 5 4 10.104.146.9 (10.104.146.9) 0.596 ms 0.846 ms 0.799 ms 6 5 bgl11-sbb-gwl-gig3-10.cisco.com (72.163.187.65) 0.639 ms 0.343 ms 0.504 ms 7 6 bgl11-rbb-gwl-tenl-1.cisco.com (72.163.171.138) 0.299 ms 0.290 ms 0.279 ms 9 8 bgl11-dmzbb-gwl-gig2-43.cisco.com (72.163.216.230) 1.472 ms 1.505 ms 1.250 ms 10 9 maa03s16-in-f4.1e100.net (74.125.236.164) 0.847 ms 0.730 ms 0.639 ms
Timeout (in secs) 10 Run Command 1 traceroute to google.com (74.125.236.164), 30 hops max, 40 byte packets 2 1 10.105.134.1 (10.105.134.1) 3 2 14.160.83.97 (14.160.83.97) 0.401 ms 0.512 ms 0.643 ms 4 3 10.104.146.37 (10.104.146.37) 0.423 ms 0.548 ms 5 4 10.104.146.9 (10.104.146.9) 0.596 ms 0.846 ms 0.799 ms 6 5 bgl11-sbb-gwl-gig3-10.cisco.com (72.163.177.65) 0.639 ms 0.343 ms 0.504 ms 7 6 bgl11-sbb-gwl-gig0-2.cisco.com (72.163.171.138) 0.299 ms 0.297 ms 9 8 bgl11-dmzbb-gwl-gig2-43.cisco.com (72.163.216.230) 1.472 ms 1.505 ms 1.250 ms 10 9 maa03s16-in-f4.1e100.net (74.125.236.164) 0.847 ms 0.730 ms 0.639 ms 11 12 13 13 14 14 14
Run Command 1 traceroute to google.com (74.125.236.164), 30 hops max, 40 byte packets 2 1 10.105.134.1 (10.105.134.1) 1.025 ms 0.605 ms 0.493 ms 3 2 14.160.83.97 (14.160.83.97) 0.401 ms 0.512 ms 0.643 ms 4 3 10.104.146.37 (10.104.146.37) 0.423 ms 0.548 ms 0.510 ms 5 4 10.104.146.9 (10.104.146.9) 0.596 ms 0.846 ms 0.799 ms 6 5 bgl11-sbb-gwl-gig3-10.cisco.com (72.163.177.65) 0.639 ms 0.343 ms 0.504 ms 7 6 bgl11-rbb-gwl-ten1-1.cisco.com (72.163.171.138) 0.299 ms 0.290 ms 0.279 ms 8 bgl11-dmzbb-gwl-gig0-2.cisco.com (72.163.171.138) 0.299 ms 0.290 ms 0.279 ms 9 maa03s16-in-f4.1e100.net (74.125.236.164) 0.847 ms 0.730 ms 0.639 ms 11 12 13
<pre>1 traceroute to google.com (74.125.236.164), 30 hops max, 40 byte packets 2 1 10.105.134.1 (10.105.134.1) 1.025 ms 0.605 ms 0.493 ms 3 2 14.160.83.97 (14.160.83.97) 0.401 ms 0.512 ms 0.643 ms 4 3 10.104.146.37 (10.104.146.37) 0.423 ms 0.548 ms 0.510 ms 5 4 10.104.146.9 (10.104.146.9) 0.596 ms 0.846 ms 0.799 ms 6 5 bgll1-sbb-gwl-gig3-10.cisco.com (72.163.171.21) 0.533 ms 0.541 ms 0.387 ms 7 6 bgll1-rbb-gwl-en1-1.cisco.com (72.163.171.138) 0.299 ms 0.290 ms 0.279 ms 9 8 bgll1-dmzbb-gwl-gig2-43.cisco.com (72.163.216.230) 1.472 ms 1.505 ms 1.250 ms 10 9 maa03s16-in-f4.1e100.net (74.125.236.164) 0.847 ms 0.730 ms 0.639 ms 11 12</pre>
<pre>1 traceroute to google.com (74.125.236.164), 30 hops max, 40 byte packets 2 1 10.105.134.1 (10.105.134.1) 1.025 ms 0.605 ms 0.493 ms 3 2 14.160.83.97 (14.160.83.97) 0.401 ms 0.512 ms 0.643 ms 4 3 10.104.146.37 (10.104.146.37) 0.423 ms 0.548 ms 0.510 ms 5 4 10.104.146.9 (10.104.146.9) 0.596 ms 0.846 ms 0.799 ms 6 5 bgll1-sbb-gwl-gig3-10.cisco.com (72.163.171.21) 0.533 ms 0.541 ms 0.387 ms 7 6 bgll1-rbb-gwl-ten1-1.cisco.com (72.163.171.138) 0.299 ms 0.290 ms 0.279 ms 9 8 bgll1-dmzbb-gwl-gig2-43.cisco.com (72.163.216.230) 1.472 ms 1.505 ms 1.250 ms 11 12 13</pre>
<pre>1 traceroute to google.com (74.125.236.164), 30 hops max, 40 byte packets 2 1 10.105.134.1 (10.105.134.1) 1.025 ms 0.605 ms 0.493 ms 3 2 14.160.83.97 (14.160.83.97) 0.401 ms 0.512 ms 0.643 ms 4 3 10.104.146.37 (10.104.146.37) 0.423 ms 0.548 ms 0.510 ms 5 4 10.104.146.9 (10.104.146.9) 0.596 ms 0.846 ms 0.799 ms 6 5 bgll1-sbb-gwl-gig3-10.cisco.com (72.163.187.65) 0.639 ms 0.343 ms 0.504 ms 7 6 bgll1-rbb-gwl-ten1-1.cisco.com (72.163.171.21) 0.533 ms 0.541 ms 0.387 ms 8 7 bgll2-corp-gwl-gig0-2.cisco.com (72.163.171.138) 0.299 ms 0.290 ms 0.279 ms 9 8 bgll1-dmzbb-gwl-gig2-43.cisco.com (72.163.216.230) 1.472 ms 1.505 ms 1.250 ms 11 12 13</pre>
<pre>2 1 10.105.134.1 (10.105.134.1) 1.025 ms 0.605 ms 0.493 ms 3 2 14.160.83.97 (14.160.83.97) 0.401 ms 0.512 ms 0.643 ms 4 3 10.104.146.37 (10.104.146.37) 0.423 ms 0.548 ms 0.510 ms 5 4 10.104.146.9 (10.104.146.9) 0.596 ms 0.846 ms 0.799 ms 6 5 bgll1-sbb-gwl-gig3-10.cisco.com (72.163.187.65) 0.639 ms 0.343 ms 0.504 ms 7 6 bgll1-rbb-gwl-ten1-1.cisco.com (72.163.171.138) 0.299 ms 0.343 ms 0.387 ms 8 7 bgll2-corp-gwl-gig0-2.cisco.com (72.163.171.138) 0.299 ms 0.290 ms 0.279 ms 9 8 bgll1-dmzbb-gwl-gig2-43.cisco.com (72.163.216.230) 1.472 ms 1.505 ms 1.250 ms 10 9 maa03s16-in-f4.1e100.net (74.125.236.164) 0.847 ms 0.730 ms 0.639 ms 11 12 13</pre>
3 2 14.160.83.97 (14.160.83.97) 0.401 ms 0.512 ms 0.643 ms 3 10.104.146.37 (10.104.146.37) 0.423 ms 0.548 ms 0.510 ms 4 10.104.146.9 (10.104.146.9) 0.596 ms 0.846 ms 0.799 ms 5 bgll1-sbb-gwl-gig3-10.cisco.com (72.163.187.65) 0.639 ms 0.343 ms 0.504 ms 6 bgll1-rbb-gwl-tenl-1.cisco.com (72.163.171.121) 0.533 ms 0.541 ms 0.387 ms 8 7 bgll2-corp-gwl-gig0-2.cisco.com (72.163.171.138) 0.299 ms 0.290 ms 0.279 ms 9 8 bgll1-dmzbb-gwl-gig2-43.cisco.com (72.163.216.230) 1.472 ms 1.505 ms 1.250 ms 10 9 maa03s16-in-f4.1e100.net (74.125.236.164) 0.847 ms 0.730 ms 0.639 ms 11 12 13
 4 3 10.104.146.37 (10.104.146.37) 0.423 ms 0.548 ms 0.510 ms 4 10.104.146.9 (10.104.146.9) 0.596 ms 0.846 ms 0.799 ms 5 bgll1-sbb-gwl-gig3-10.cisco.com (72.163.187.65) 0.639 ms 0.343 ms 0.504 ms 6 bgll1-rbb-gwl-ten1-1.cisco.com (72.163.171.21) 0.533 ms 0.541 ms 0.387 ms 7 bgl12-corp-gwl-gig0-2.cisco.com (72.163.171.138) 0.299 ms 0.290 ms 0.279 ms 9 bgl11-dmzbb-gwl-gig2-43.cisco.com (72.163.216.230) 1.472 ms 1.505 ms 1.250 ms 10 maa03s16-in-f4.1e100.net (74.125.236.164) 0.847 ms 0.730 ms 0.639 ms
 5 4 10.104.146.9 (10.104.146.9) 0.596 ms 0.846 ms 0.799 ms 5 bgl11-sbb-gw1-gig3-10.cisco.com (72.163.187.65) 0.639 ms 0.343 ms 0.504 ms 6 bgl11-rbb-gw1-ten1-1.cisco.com (72.163.171.21) 0.533 ms 0.541 ms 0.387 ms 8 bgl12-corp-gw1-gig0-2.cisco.com (72.163.171.138) 0.299 ms 0.290 ms 0.279 ms 9 bgl11-dmzbb-gw1-gig2-43.cisco.com (72.163.216.230) 1.472 ms 1.505 ms 1.250 ms 9 maa03s16-in-f4.1e100.net (74.125.236.164) 0.847 ms 0.730 ms 0.639 ms
<pre>6 5 bgll1-sbb-gwl-gig3-10.cisco.com (72.163.187.65) 0.639 ms 0.343 ms 0.504 ms 7 6 bgll1-rbb-gwl-ten1-1.cisco.com (72.163.171.21) 0.533 ms 0.541 ms 0.387 ms 8 7 bgll2-corp-gwl-gig0-2.cisco.com (72.163.171.138) 0.299 ms 0.290 ms 0.279 ms 9 8 bgll1-dmzbb-gwl-gig2-43.cisco.com (72.163.216.230) 1.472 ms 1.505 ms 1.250 ms 10 9 maa03s16-in-f4.1e100.net (74.125.236.164) 0.847 ms 0.730 ms 0.639 ms 11 12 13</pre>
<pre>7 6 bgll1-rbb-gwl-ten1-1.cisco.com (72.163.171.21) 0.533 ms 0.541 ms 0.387 ms 8 7 bgll2-corp-gwl-gig0-2.cisco.com (72.163.171.138) 0.299 ms 0.290 ms 0.279 ms 9 8 bgll1-dmzbb-gwl-gig2-43.cisco.com (72.163.216.230) 1.472 ms 1.505 ms 1.250 ms 10 9 maa03s16-in-f4.1e100.net (74.125.236.164) 0.847 ms 0.730 ms 0.639 ms 11 12 13</pre>
<pre>8 7 bgll2-corp-gwl-gig0-2.cisco.com (72.163.171.138) 0.299 ms 0.290 ms 0.279 ms 9 8 bgll1-dmzbb-gwl-gig2-43.cisco.com (72.163.216.230) 1.472 ms 1.505 ms 1.250 ms 10 9 maa03s16-in-f4.1e100.net (74.125.236.164) 0.847 ms 0.730 ms 0.639 ms 11 12 13</pre>
9 8 bgll1-dmzbb-gwl-gig2-43.cisco.com (72.163.216.230) 1.472 ms 1.505 ms 1.250 ms 9 maa03s16-in-f4.1e100.net (74.125.236.164) 0.847 ms 0.730 ms 0.639 ms 11 12 13
10 9 maa03s16-in-f4.1e100.net (74.125.236.164) 0.847 ms 0.730 ms 0.639 ms 11 12 13
11 12 13
12 13
13
14
15
16
17
18
Help Close

XML API Console

XML API Console option is provided to execute XML APIs on the CSPC server. This option is provided for third party application integration with CSPC. This is shown in Figure 9-28.

Figı	ure 9-28 XML API Console
XM	IL API Console 🛞
	Run XML API
1 2 3 4 4 5 6 7 7 8 9 9 10 11 12 13 14 15 16 17 7 18 19 20 21 22 3 24 24 24	<request xmlns="http://www.parinetworks.com/api/schemas/1.1" requestId="DisplaySettings"> <kanage> <kdodify operationid="1"> <pre> <pre> <pr< th=""></pr<></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></kdodify></kanage></request
Mos	<response requestid="DisplaySettings"> <status code="SUCCESSFUL"></status> <modify operationid="1"> <status code="SUCCESSFUL"></status> <modify> <modify> <response> Response></response></modify></modify></modify></response>
Mes	<response requestid="DisplaySettings"> <status code="SUCCESSFUL"></status> <kanage> <kodify operationid="1"> <status code="SUCCESSFUL"></status> </kodify></kanage></response>



Menu Options

Menus

Menu options are provided as a quick way to access the applications.

Figure 10-1		Menu Option		
	Settings • Management •	Reports • Administration • Help • Cust	tomer: NBC UNIVERSAL INC	Super Administrator 🔹
	Workflow 🧃 Credentials	🖏 Discovery 😺 Managed Devices 💭 Collect 🗿 Collected Data 🍙 Upload 📗 Job Run Status	Search CSPC Application	To Launch 💌 🗙

The menu options provided in CSPC are:

- User Name
- Settings
- Management
- Reports
- Administration
- Help
- Quick Menus

User Name

Γ

Shows the Name/Username of the user logged into CSPC application. In the illustration shown in Figure 10-1, the Super Administrator is logged in.

It has the following option:

- · Logout: Logs out and closes the CSPC client application
- Change Password/settings: Resets the password

Settings

Settings in the menu bar provides various options for setting up device credentials and collection profiles for collecting device specific information, as displayed in the following figure. These options are described in the *Applications->Device Management Tab*.

Figure 10-2

9

Menu	Option -	Settings
------	-----------------	----------

Add/Import Credentials Manage Sub Module Credentials Manage Seed File	
Imported Seed Files Do Not Manage Devices List	
Device Groups Application Settings Discovery Settings Inventory Settings Advanced Job Settings	
Manage Data Collection Profiles Manage Upload Profiles Manage Datasets Manage Platform Definitions Manage Data Integrity Rules Manage Data Masking Rules Manage Syslog Source Files	Export All Rules Import All Rules Import DSIRT Files Manage Applications Discovery Profiles Manage SNMP Trap Profiles Manage Iump Servers
Miscellaneous	Credential Lock Settings
Chapter 10 Menu Options

Management

Γ

Management in the menu bar provides various options for discovering and managing devices and running collection profiles, as shown in the following figure. These options are described in the *Applications->Device Management Tab*.

igure 10-3	Menu Option - Managemen
Management 🔹	
Discover D	evices
Unmanage	Devices
Verify Devi	ice Access
Device Pro	mpt Collection
Collect Dat	a
Upload Da	ta
Adhoc Dat	a Collection
Collect App	plication Data
Job Run Sta	atras

Reports

Reports in the menu bar provide various reporting options for viewing collected data as shown in the following figure. These options are described in the *Applications->Reports Tab*.

Figure 10-4 Menu Option - Reports

Re	ports •	
	Device/Discovery Reports	
	Device Access Verification Reports	1
	Inventory Collection Reports	1
	Discovery Jobs	
	Inventory Jobs	
	Job Management Reports	
	Alerts	
	SNMP Trap Report	
	Syslog Summary	
	Syslog Messages	
	Audit Reports	1
	Miscellaneous	1

Administration

I

Administration in menu the bar provides various options for administrating server, device, and collection profiles, as shown in the following figure. These options are described in the *Applications->Administration Tab*.

```
Figure 10-5
                  Menu Option - Administration
Administration -
     Manage Users...
     Manage Remote Authentication Servers...
     User Session Report...
     Modify Date/Time Preference...
     Configure Default Device Display Property...
     Email Settings...
     Manage Subscribers...
     Alert Configuration ...
     Backup...
     Restore Backup...
     Log Preferences...
     Export Log Files...
     Manage Add-on Process...
     Manage UI Add-ons...
     Server Properties...
     Configure CSPC Appliance...
     Diagnostic Tools...
     XML API Console ...
```

Help

Under Help menu, following option is shown:

- About
- Help Contents
- View/Upgrade Registration

Figure 10-6	Menu Option - Help
Help 🔹	
About	
Help Con	tents
View/Upg	rade Registration

Quick Menus

This Menu helps for the fast and easy access for the vital features on CSPC.

Menu Options	Description
🛃 Credentials	This takes you to Device Credentials page for more info refer to: Add/Import Credentials.
5 Discovery	This takes you to Select Discovery Methods page for more info refer to: Discover Devices.
Janaged Devices	This takes you to View Discovery Devices page for more info refer to: View Managed Devices.
Collect	This takes you to Select Collection Profile page for more info refer to: Collect Data.
Ollected Data	This takes you to View Collected Data page for more info refer to: View Collected Data.
🙆 Upload	This takes you to Select Upload Profile page for more info refer to: Upload Data.
11 Job Run Status	This takes you to Job Run Status page for more info refer to: Job Run Status.

Table 10-1Quick Menu



Adding Devices to CSPC

Overview

Adding devices to CSPC is a sequential, two-step process. First one adds credentials for the devices. Adding credentials for a device does not add the device, however. After the credentials have been added, the additional step of managing the device is necessary. Managing the device uses the credentials to contact the device via SNMP and collect device classification data from it.

There are two ways to add credentials. Credentials can be added individually, or through an import. You can import credentials from applications like:

- Cisco Works DCR XML File (.xml)
- Pari Networks Credential Repository (.xml)
- Cisco Works DCR CSV File (.csv)
- CNC CSV File (.csv)
- Simplified CSV File (.csv)

All the methods of adding credentials are performed on the credentials screen.

In CSPC there is a one-to-many relationship between credentials and devices. Multiple devices are stored against a single credential. The multiple devices can be specified by wildcards matching IP addresses or by IP address enumeration. Wildcards matching IP addresses is the preferred approach.

On the first collection, if the first wildcard matching the device does not succeed, the second wildcard matching the device will be tried. On subsequent collections the last successful credential will be tried first.

In addition, the protocol for the dataset type will be determined by the credentials order. For example, the choice between SSH and Telnet is controlled by the order of the SSH and Telnet credentials.

Thus, the order of credentials is important, and can be manipulated.

Credentials may be exported, but only in the Pari Credentials File Format.

After the credentials have been added, the devices can be managed. While credentials must be entered by wildcards matching IP addresses or the IP addresses themselves, the devices can be managed by either IP address or DNS name.

Examples

ice Credentials			
Credential Identifica	tion	Include Ip Address Ranges/List (For Di Collection) * IP Address List	scovery and Data
Protocol Port	(telnet 23		
Authentication User Name		Exclude Ip Address Ranges/List (For Da	ata Collection only)
Password Enable User Nan Enable Password	ne	Exclude lp List	2

Here an SSH credential is added against a wildcard:

Result is shown in Figure A-2:

Figure A-2Device Credential Configuration

Device Credentials C	Configuration				×
Device Credentials Enter credentials that will be used for device discovery and inventory and other communications between server and network devices					
NOTE: Credentials wo	uld be saved to CSPC	server as and when y	ou take the action.		
Credential Name	Transport	User Name	lp Address List		
such	https		11.1.1.2	*	
TestLock	telnet	admin1	172.21.52.12	=	
SNMP_public	snmpv2c		172.18.189.*,14.3.20.*,14.3		
SNMP_AS	snmpv2c		10.89.234.*		
snmp.70	snmpv2c	demo	172.20.70.10		
SNMP_DD_CSO	snmpv2c		192.168.99.*,192.168.96.*,1		
SNMP_cnc-ro	snmpv2c		*.*.*		Ē₽
SNMP_columbia-ro	snmpv2c		172.21.56.*		
SNMP_mwtm50	snmpv2c		172.18.156.*		
snmp.70_1	snmpv2c	demo	172.20.70.10		
SNMPv1_public	snmpv1		172.21.55.17,172.21.55.15,		
SNMP_public_1	snmpv2c		172.18.189.*,14.3.20.*,14.3		
CNIMD AC 1	epmpy?c		10.89.03/ *	Ŧ	
🚺 🖣 Page 1	of 3 🕨 🔰		Displaying 1 - 50 of	109	
Add	Delete Delete A	Modify	Clone Import Export.		
			Help	Close	

Now the devices can be managed. Devices are managed by discovery of known devices. This is a special kind of discovery that does not discover anything.

Гідиге А	5 Discover unu manage metwork Devices	
Discover and I	nage Network Devices	×
Select at lea	one of the following network device discovery methods.	
Discov	devices with known IP addresses	
Discov	r devices with protocols such as CDP, OSPF and ARP	
Discov	devices by scanning/pinging range of IP Addresses	
📃 Redisc	ver the currently managed and non-managed devices	
	Import < Previous Next> Help	Cancel
	import Criterous inext iterp	Galicer

Figure A-3 Discover and Manage Network Devices

Either the IP Address or the DNS Name.

Figure A-4	Discover and Manage	Network Devices

ver and Manage Network Devices	
ter the list of IP addresses for the known devices.	
P Address/Host Name	
🕈 Add 🛪 Delete 🥒 Modify	
10.1.1.10	
	< Previous Next > Help Cance



Seed File Formats

CSPC supports following seed file formats:

- 1. CNC Seed File Format
- 2. Cisco Works Seed File Format
- 3. Simplified Seed File Format

CNC seed file format has following three formats:

- 1. CNC 20-field format
- 2. CNC 30-field format
- 3. CNC 36-field format

And Cisco Works has following two formats:

- 1. Cisco Works 30-field format
- 2. Cisco Works 34-field format



All the above seed file formats are of .csv type.

Simplified seed file format allows users to easily specify credentials for all devices or set of devices using wild cards.

The basic difference between Simplified Format and rest of the formats is that for the same device there are multiple entries, each entry corresponds to one protocol. In other formats same entry carries for all devices.

Header Information

CNC Seed File Format

Header in CNC 20-field format contains the fields listed below:

- ; Col# = 1: Name (including domain or simply an IP),
- ; Col# = 2: RO community string,
- ; Col# = 3: RW community string,
- ; Col# = 4: Serial Number,
- ; Col# = 5: User Field 1,
- ; Col# = 6: User Field 2,
- ; Col# = 7: User Field 3,
- ; Col# = 8: User Field 4,
- ; Col# = 9; Name = Telnet password,
- ; Col# = 10; Name = Enable password,
- ; Col# = 11; Name = Enable secret,
- ; Col# = 12; Name = Tacacs user,
- ; Col# = 13; Name = Tacacs password,
- ; Col# = 14; Name = Tacacs enable user,
- ; Col# = 15; Name = Tacacs enable password,
- ; Col# = 16; Name = Local user,
- ; Col# = 17; Name = Local password,
- ; Col# = 18; Name = Rcp user,
- ; Col# = 19; Name = Rcp password,
- ; Col# = 20; Name = Enable User,

Header in CNC 30-field format contains the fields listed below:

; Col# = 1: IP Address (including domain or simply an IP),

- ; Col# = 2: Host Name,
- ; Col# = 3: Domain Name,
- ; Col# = 4: Device Identity,
- ; Col# = 5: Display Name,
- ; Col# = 6: SysObjectID ,
- ; Col# = 7: DCR Device Type,
- ; Col# = 8: MDF Type,
- ; Col# = 9; Snmp RO
- ; Col# = 10; Snmp RW
- ; Col# = 11; SnmpV3 User Name

- ; Col# = 12; Snmp V3 Auth Pass
- ; Col# = 13; Snmp V3 Engine ID
- ; Col# = 14; Snmp V3 Auth Algorithm
- ; Col# = 15; RX Boot Mode User
- ; Col# = 16; RX Boot Mode Pass
- ; Col# = 17; Primary User (Tacacs User)
- ; Col# = 18; Primary Pass (Tacacs Pass)
- ; Col# = 19; Primary Enable Pass
- ; Col# = 20; Http User
- ; Col# = 21; Http Pass
- ; Col# = 22; Http Mode
- ; Col# = 23; Http Port
- ; Col# = 24; Https Port
- ; Col# = 25; Cert Common Name,
- ; Col# = 26; Secondary User,
- ; Col# = 27; Secondary Pass,
- ; Col# = 28; Secondary Enable Pass,
- ; Col# = 29; Secondary Http User,
- ; Col# = 30; Secondary Http Pass,

Header in CNC 36-field format contains the fields listed below:

- ; Col# = 1: IP Address (including domain or simply an IP),
- ; Col# = 2: Host Name,
- ; Col# = 3: Domain Name,
- ; Col# = 4: Device Identity,
- ; Col# = 5: Display Name,
- ; Col# = 6: SysObjectID,
- ; Col# = 7: DCR Device Type,
- ; Col# = 8: MDF Type,
- ; Col# = 9; Snmp RO
- ; Col# = 10; Snmp RW

I

- ; Col# = 11; SnmpV3 User Name
- ; Col# = 12; Snmp V3 Auth Pass
- ; Col# = 13; Snmp V3 Engine ID
- ; Col# = 14; Snmp V3 Auth Algorithm
- ; Col# = 15; RX Boot Mode User
- ; Col# = 16; RX Boot Mode Pass

- ; Col# = 17; Primary User (Tacacs User)
- ; Col# = 18; Primary Pass (Tacacs Pass)
- ; Col# = 19; Primary Enable Pass
- ; Col# = 20; Http User
- ; Col# = 21; Http Pass
- ; Col# = 22; Http Mode
- ; Col# = 23; Http Port
- ; Col# = 24; Https Port
- ; Col# = 25; Cert Common Name,
- ; Col# = 26; Secondary User,
- ; Col# = 27; Secondary Pass,
- ; Col# = 28; Secondary Enable Pass,
- ; Col# = 29; Secondary Http User,
- ; Col# = 30; Secondary Http Pass,
- ; Col# = 31; Snmp V3 Priv Algorithm,
- ; Col# = 32; Snmp V3 Priv Pass,
- ; Col# = 33; User Field 1,
- ; Col# = 34; User Field 2,
- ; Col# = 35; User Field 3,
- ; Col# = 36; User Field 4,

A new feature is implemented to decide the primary device name using column1, column2, and column3 of 30 and 36 column CNC seedfile. This eliminates the need of manual updating of /etc/hosts.

Hostname and Domain name is decided based on below scenarios:

- If seed file has defined hostname in Column 2 and domain name in Column 3, then CSPC combines both the (Hostname in Column2 + Domain name Column3) and use this as a primary device name
- If seed file has defined hostname in Column 2 and no domain name in Column 3, then CSPC uses hostname in Column2 as a primary device name
- If seed file has defined hostname in Column 1, no data in Column2, and domain name in Column3, then CSPC combines both of them (Hostname in Column1 + Domain name in Column3) and uses this as a primary device name
- If no value present in Column2 and Column3 then CSPC uses Column1 value (Ipaddress or hostname) as a primary device name

Cisco Works Seed File Format

Header in Cisco Works 30 seed file contains these fields:

- management_ip_address
- host_name

- domain_name
- device_identity
- display_name
- sysObjectID
- dcr_device_typemdf_typesnmp_v2_ro_comm_string
- snmp_v2_rw_comm_string
- snmp_v3_user_idsnmp_v3_passwordsnmp_v3_engine_id
- snmp_v3_auth_algorithm
- rxboot_mode_username
- rxboot_mode_password
- primary_username
- primary_password
- primary_enable_password
- http_username
- http_password
- http_mode
- http_port
- https_port
- cert_common_name
- secondary_username
- secondary_password
- secondary_enable_password
- secondary_http_username
- secondary_http_password

Header in Cisco Works 34 seed file contains these fields:

- management_ip_address
- host_name
- domain_name
- device_identity
- display_name
- sysObjectID
- dcr_device_type
- mdf_type
- sysContact
- sysLocation

- snmp_v2_ro_comm_string
- snmp_v2_rw_comm_string

- snmp_v3_user_id
- snmp_v3_password
- snmp_v3_engine_id
- snmp_v3_auth_algorithm
- snmp_v3_priv_password
- snmp_v3_priv_algorithm
- rxboot_mode_username
- rxboot_mode_password
- primary_username
- primary_password
- primary_enable_password
- http_username
- http_password
- http_mode
- http_port
- https_port
- cert_common_name
- secondary_username
- secondary_password
- secondary_enable_password
- secondary_http_username
- secondary_http_password

Simplified Seed File Format

Header in Simplified Seed file contains these fields:

- IPAddress
- protocol
- port
- username
- password
- enableusername
- enablepassword
- SnmpRO
- SnmpRW
- SnmpV3Id
- SnmpV3Password
- SnmpV3EngineId

- Snmpv3AuthAlogorithm
- SnmpV3PrivAlgorithm
- SnmpVPrivPassword

Export File Format

I

These are the contents of the file generated by the export utility of Service Appliance 1.0:

- ; Col# = 1: IP Address (including domain or simply an IP)
- ; Col# = 2: Host Name
- ; Col# = 3: Domain Name
- ; Col# = 4: Device Identity
- ; Col# = 5: Display Name
- ; Col# = 6: SysObjectID
- ; Col# = 7: DCR Device Type
- ; Col# = 8: MDF Type
- ; Col# = 9; Snmp RO
- ; Col# = 10; Snmp RW
- ; Col# = 11; SnmpV3 User Name
- ; Col# = 12; Snmp V3 Auth Pass
- ; Col# = 13; Snmp V3 Engine ID
- ; Col# = 14; Snmp V3 Auth Algorithm
- ; Col# = 15; RX Boot Mode User
- ; Col# = 16; RX Boot Mode Pass
- ; Col# = 17; Primary User(Tacacs User)
- ; Col# = 18; Primary Pass(Tacacs Pass)
- ; Col# = 19; Primary Enable Pass
- ; Col# = 20; Http User
- ; Col# = 21; Http Pass
- ; Col# = 22; Http Mode
- ; Col# = 23; Http Port
- ; Col# = 24; Https Port
- ; Col# = 25; Cert Common Name
- ; Col# = 26; Secondary User
- ; Col# = 27; Secondary Pass
- ; Col# = 28; Secondary Enable Pass
- ; Col# = 29; Secondary Http User
- ; Col# = 30; Secondary Http Pass
- ; Col# = 31; Snmp V3 Priv Algorithm

- ; Col# = 32; Snmp V3 Priv Pass
- ; Col# = 33; User Field 1
- ; Col# = 34; User Field 2
- ; Col# = 35; User Field 3
- ; Col# = 36; User Field 4
- ; Col# = 37; Status_Msg



Optional Parameter for NATed Appliances

This feature allows TFTP dataset/CLI datasets/ ApplyIPSsignature/ApplyConfig to create/execute with commands having CSPC server IP, which needs to be added dynamically while executing the TFTP dataset/CLI datasets/ApplyIPSsignature/ApplyConfig. To use this feature for CLI datasets/ ApplyIPSsignature/ApplyConfig ,a unique tag called <#SERVERIP#> has to be added to the command where CSPC server IP needs to be replaced. Updating TFTP dataset is not needed. By default, CSPC will replace it with its own IP but, in case the externally visible IP is not the same as the internal CSPC IP, then use the following XML to added/modify the IP to be used for replacing the <#SERVERIP#> tag

To add/modify a CSPC Server IP, use below xml API

<Request requestId="" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://www.parinetworks.com/api/schemas/1.1 pari_api.xsd" xmlns="http://www.parinetworks.com/api/schemas/1.1"> <Manage> <Add operationId="1"> <ServerDetails> <IPAddress>x.x.x.</IPAddress>

</ServerDetails>

</Add>

I

</Manage>

</Request>

..



Conditional Collection

Conditional Collection Description

The phrase "Conditional Collection" generally refers to any collection decision (whether to collect/what to collect/how many times to collect) that is made based on the result of bunch of conditions or the results of another data collection. Other terms used for this are "Complex Collection", "Dynamic Collection", "Follow-on Collection".

What is Supported

Audit Use Case

I

- Execute a dataset (SNMP or CLI)
- Parse the output and capture a bunch of values
- · Execute another command for each of the values captured above

Cisco Call Manager Use Case

In Cisco Call Manager detection, if the SysOID is one of a configurable set of OIDs, and an additional OID returns a value, the device is considered a Cisco Call Manager, and the CCM call manager platform applies.

Support Details:

This will be supported in Conditional collection. However, "platform definitions" in CSPC depend only on the results of discovery operation and cannot depend on the inventory collection results.

This means that you need to implement it in the following way:

- 1. Define a platform "Possible Call Manager" by providing the set of SysOIDs
- 2. Define a Conditional collection that is applicable only for the "Possible Call Manager" platforms
- **3.** In this Conditional collection, execute the additional OIDs and based on their return value, collect the final dataset you wish to collect

SNMP/CLI Configuration Fallback Collection

There are four configurations controlling config collection from the device. CLI only and SNMP only do not require follow on collections. However, CLI fallback to SNMP and SNMP fallback to CLI configurations will issue a follow on collection if the first attempted collection protocol fails.

Support Details:

This will be supported in Conditional Collection. However, while this makes sense for collecting configuration, it may not be very useful for other collections.

For example: Interface statistics would result in completely different output based on whether you collected it using SNMP or CLI.

Collected Value Based Follow-on Collections

There are more examples of these in Audits than in Inventory. These are the cases of follow on collection controlled by the "Condition" block in the RBML, and so could be considered the "true" conditional collections.

Support Details:

These use cases are supported as part of Audit Use Cases above.

Commands Requiring Re-login

Commands Requiring Re-login to the Same Device multiple times with mutated community strings to access card in different slots

This is the case where the same OID is issued against the same device multiple times, each time after logging in to a different card in a different slot. Here it is not the command that is mutating but the community string. Log in with the password *public@SM_1* to access the card in slot module 1. These are issued against WAN switches.

Support Details:

This will be supported in Conditional Collection. However, the support will be limited to changing the community string dynamically. (We do not support changing the other credentials like username/password or device IP address etc. dynamically. That needs to be handled by the add-on module if there is such a requirement).

Condition Collection in Detail

Conditional Collection in CSPC is based on recursive algorithm were in the output from each processing units will be fed as input to the next processing unit, until the last processing is complete.

Statement

Statement is the fundamental processing units in Conditional Collection. Statements mark the starting point of each processing units. Each statement is identified with an "identifier" and can optionally have a title and Input. Statement is represented by <Statement> tag

Statements are classified into two types:

- 1. Condition
- 2. Loop

The input of each statement will depend on the type of the statement. Input will be a scalar input for condition statement and vector input for loop statements.

Condition Statement

Condition Statement is represented by <Condition> tag and is identified by the statement identifier. Each condition statements input is a scalar input. In order to process the output of input the <Operation> tag is used where the user choose what to do with the output. Based on the operation performed the <Match> and <NonMatch> tags can be used to decide whether to continue with the single unit of processing or to go to the next processing.

Under the <Match> and <NonMatch> tag, user can choose to store the values in a variable which can be used for further processing. To store the values, <Assignment> tags are used under <Match> tag. Basedon the operation performed the engine can be used to:

- a. Execute the next statement (Use <Goto>)
- **b.** Use the next value from the processing (Use <Continue>)
- **c.** Exit the process (Use <Exit>)
- d. On a certain Matching situation break the recursion (Use <Break>)

Use the <Output> tag if a condition statement is the last program of execution where the output of condition collection is done. Two types of output processing are currently supported in CSPC:

1. **Dataset**: Execute another dataset with the variables populated in previous steps. Make sure the datasets uses the same variable string (case sensitive) that was used for assigning.

Example: If the variable name is "name" and if the output dataset is to login to each slot then the command will be: **session slot <name> processor 1**

2. AddOutput: This type of output can be used to display the processed output in the format that is desired by the user.

Scalar Input

Scalar Inputs are the integral part of condition statement and can be only used with condition statements. There are five type of scalar inputs that can be used for processing in condition statements namely:

- 1. Device Property: Used for validating the device properties
- 2. Variable: Used in initializations
- 3. **Datasets**: Dataset names which needs to be provided if any commands needs to use issued in the device
- 4. Loop Context: Input Datatype which communicates to the engine if the input needs to be taken from the current loop
- 5. SNMPIndex / SNMPOid/SNMPValue: Used for processing SNMP data

Operation

In order to process the output of the scalar input the <Operation> tag is used. There are two types of operations:

- 1. String Operation: Used with java regular expression. Each of the matching patterns are then compared with the java string for matches, doesnotmatch, contains, doesnotcontain, isEmpty, equals and notEquals checks
- 2. Vector Operation: Used as a normal java vector where in the output can be added to a variable and later used for processing

Assignment

The condition statement assignment is the important place where the resultant variable are populated at the end of each operation. In order to assign values to a variable, a variable is created under <Variable>tag under assignment. The variable is populated with the results based on the following important tags:

- a. append: Denotes if the matching result needs to be appended to the resulting variable
- b. onlyIfNotNull: Add the result to variable only if the result is not null
- c. trim: Trims the resulting string and add to the variable
- **d. vectorType**: List/Set/OrderedList are the vector types in which the result will be added in the resultant list. By default, the results will be added to a list. But if the order of insertion is needs to be maintained then OrderedList needs to be used. Use Set, if only unique result string are required in the variable
- e. **Operation**: add/remove. Add, adds the result to the resulting list and Remove, removes the string if present from the resulting list

Loop Statement

Loop statements are like while loop where each statement is executed recursively till the exit criteria is met. Loop Statement is represented by <Loop> tag and is identified by the statement identifier. Loop statement will be the first statement in any conditional collection dataset.

Each loop statements input is a vector input. Each loop-statement must terminate with a condition statement. Data collected from the vector input will be subjected to further processing using specific matching conditions and condition statement(s).

Vector Input

There are four type of vector-inputs used in conditional collection. Each of these vector inputs have discrete significance in achieving the needs of the complex collection. Four type of vector inputs are:

- 1. Block Vector Input: Block Vector Input is used whenever a block of response from the device response needs to be processed. Each of the block input has a mandatory <Input> and <Params> fields. The input used in block can be any of the scalar inputs except SNMP. The params filed has a start and end string which marks the starting and the ending of the block. Also, the start and end strings are java pattern matched. The result of matched pattern is further processed in a condition statement or in a loop statement.
- 2. Line Vector Input: Line Vector Input is used whenever the response from device needs to be processed line by line. Each of the line input has a mandatory <Input> and <Params> fields. The input used in line can be any of the scalar inputs except SNMP. The params filed has a match <Match> tag criteria which is string and is java pattern matched against the result. The result of matched pattern is further processed in a condition statement or in a loop statement.

- 3. SNMP Table: It is used for processing SNMP response from SNMP Table. Each of the SNMP input has a mandatory <Input> and <Rows> fields. The input used in SNMP must be any of the SNMP scalar inputs.
- 4. Variable Vector Input: It is used like java array-list. The input list is populated and is fed for subsequent processing units for further processing.

Actions

Actions are used in conditional collection when a specific action needs to be done before, while or after processing a request. In most cases actions do assignment to variables which will be used in further processing

Examples

CLI Complex Collection

Collection of Show interfaces from device followed by interface status of those interface which contain the string "FastEthernet".

<Dataset identifier="ios_show_int_accounting_dynamic">

<Type>Dynamic</Type>

<Title>ios_show_int_accounting_dynamic</Title>

<CollectionType>CLI</CollectionType>

<CategoryName> show_int_accounting</CategoryName>

<Statements>

<Loop identifier="_show_interface_1">

<VectorInput>

<Line>

<Input>

- <Dataset>
- <DatasetName Failure="error_message">_show interface</DatasetName>

</Dataset>

</Input>

<Params>

<Match ignoreCase="false">FastEthernet[^A-Za-z_]*</Match>

</Params>

</Line>

</VectorInput>

<Statements>

<Condition identifier="output_cond">

<Input>

I

<LoopContext></LoopContext>

</Input>

<Operation>

<NotEquals ignoreCase="true"></NotEquals>

</Operation>

<Match>

<Assignment>

<Variable append="false" onlyIfNotNull="true" trim="true" vectorType ="List" operation="add">interface</Variable>

<Value></Value>

</Assignment>

<Output>

<Dataset>

<DatasetName>ios_show_interface accounting</DatasetName>

<Variables>

<Variable>interface</Variable>

</Variables>

</Dataset>

</Output>

<Continue></Continue>

</Match>

<NonMatch>

<Continue></Continue>

</NonMatch>

</Condition>

</Statements>

</Loop>

</Statements>

</Dataset>

SNMP Complex Collection

<Dataset identifier="ifHCOutOctets_all_interfaces_9089">

<Type>Dynamic</Type>

<Title>ifHCOutOctets_all_interfaces For AIF: 9089 Created at Dec 20, 2011 9:48:06 PM</Title>

<CollectionType>SNMP</CollectionType>

<CategoryName>AIF_9089</CategoryName>

<Statements>

<Loop identifier="loop1">

<Title>Get SNMP Interface Types</Title>

<VectorInput>

<SNMPTable>

<Input>

<Dataset>

<DatasetName>ifType_9089_internal</DatasetName>

</Dataset>

</Input>

<Rows>

</Rows>

</SNMPTable>

</VectorInput>

<Actions>

<Assignment>

<Variable append="false" onlyIfNotNull="false" trim="false" vectorType="Set" Operation="add">ifTypes</Variable>

<Values>

< Value > 6 < /Value > Value > 62 < /Value > Value > 5 < /Value > Value > 6 < /Value > Value > 9 < /Value > Value > 15 < /Value > Value > 17 < /Value > Value > 18 < /Value > Value > 19 < /Value > Value > 22 < /Value > Value > 30 < /Value > Value > 32 < /Value > Value > 37 < /Value > Value > 39 < /Value > Value > 49 < </Value > Value > 63 < /Value > Value > 73 < /Value > Value > 76 < /Value > Value > 77 < /Value > Value > 81 < /Value > Value > 100 < /Value > Value > 101 < /Value > Value > 102 < /Value > Value > 103 < /Value > Value > 103 < /Value > Value > 101 < /Value > Value > 103 < /Value > Value > 103 < /Value > Value > 101 < /Value > Value > 103 < /Value > Value > 101 < /Value > Value > 103 < /Value > Value > 101 < /Value > Value > 103 < /Value > Value > 101 < /Value > Value > 103 < /Value > Value > 103 < /Value > Value > 101 < /Value > Value > 103 < /Value > Value > Value > 103 < /Value > 103 < /Value > Value > 103 < /Value > 103 <

</Assignment>

</Actions>

<Statements>

<Condition identifier="loop1_cond1">

<Title>Check to see if Interface is required type</Title>

<Input>

<SNMPValue>

<LoopContext></LoopContext>

</SNMPValue>

</Input>

<Operation>

<IsMemberOf><VariableName>ifTypes</VariableName>

</IsMemberOf>

</Operation>

<Match>

I

<Goto></Goto>

</Match>

<NonMatch>

<Continue></Continue>

</NonMatch>

</Condition>

<Condition identifier="loop1_cond_last">

<Title>Save the ifIndex</Title>

<Input>

<SNMPIndex>

<LoopContext></LoopContext>

</SNMPIndex>

</Input>

<Operation>

<Matches ignoreCase="false">^.*\.([0-9]+)\$</Matches>

</Operation>

<Match>

<Assignment>

<Variable append="true" onlyIfNotNull="true" trim="true" vectorType="Set" Operation="add">interfaceList</Variable>

<Value><loop1_cond_last.1></Value></Assignment>

<Goto></Goto>

</Match>

<NonMatch>

<Continue></Continue>

</NonMatch>

</Condition>

</Statements>

</Loop>

<Loop identifier="loop2">

<Title>Get SNMP Interface Oper Status</Title>

<VectorInput>

<SNMPTable>

<Input>

<Dataset>

<DatasetName>ifOperStatus_9089_internal</DatasetName>

</Dataset>

</Input>

<Rows>

</Rows>

</SNMPTable>

</VectorInput>

<Statements>

<Condition identifier="loop2_cond1">

<Input>

<SNMPValue>

<LoopContext></LoopContext>

</SNMPValue>

</Input>

<Operation>

<Equals ignoreCase="false">1</Equals>

</Operation>

<Match>

<Continue></Continue>

</Match>

<NonMatch>

<Goto></Goto>

</NonMatch>

</Condition>

<Condition identifier="loop2_cond2">

<Title>Remove If Interface is not up</Title>

<Input>

<SNMPIndex>

<LoopContext></LoopContext>

</SNMPIndex>

</Input>

<Operation>

<Matches ignoreCase="false">^.*\.([0-9]+)\$</Matches>

</Operation>

<Match>

<Assignment>

<Variable append="false" onlyIfNotNull="false" trim="false" vectorType="List" Operation="add">interfaceList</Variable>

<Value><loop2_cond2.1></Value></Assignment>

<Goto></Goto>

</Match>

I

<NonMatch>

- <Continue></Continue>
- </NonMatch>
- </Condition>
- </Statements>
- </Loop>
- <Loop identifier="last">
- <Title>Collect the output</Title>
- <VectorInput>
- <SNMPTable>
- <Input>
- <Dataset>

<DatasetName>ifHCOutOctets_all_interfaces_9089_ifHCOutOctets</DatasetName>

- </Dataset>
- </Input>
- <Rows>
- </Rows>
- </SNMPTable>
- </VectorInput>
- <Statements>
- <Condition identifier="last_cond1">
- <Input>
- <SNMPIndex>
- <LoopContext></LoopContext>
- </SNMPIndex>
- </Input>
- <Operation>
- <Matches ignoreCase="false">^.*\.([0-9]+)\$</Matches>
- </Operation>
- <Match>
- <Assignment>
- <Variable append="false" onlyIfNotNull="true" trim="true" vectorType="List" Operation="add">oid</Variable>
- <Value></Value></Assignment>
- <Goto></Goto>
- </Match>
- <NonMatch>
- <Continue></Continue>

</NonMatch>

</Condition>

<Condition identifier="last_cond2">

<Title>Check to see if this is in the final List</Title>

<Input>

<Variable>last_cond1.1</Variable>

</Input>

<Operation>

<IsMemberOf><VariableName>interfaceList</VariableName>

</IsMemberOf>

</Operation>

<Match>

<Goto></Goto>

</Match>

<NonMatch>

<Continue></Continue>

</NonMatch>

</Condition>

<Condition identifier="last_cond3">

<Title>Add the value to the final output</Title>

<Input>

<SNMPValue>

<LoopContext></LoopContext>

</SNMPValue>

</Input>

<Operation>

<Matches ignoreCase="false">^(.*)\$</Matches>

</Operation>

<Match>

<Assignment>

<Variable append="false" onlyIfNotNull="true" trim="true" vectorType="List" Operation="add">interface</Variable>

<Value><last_cond1.1></Value></Assignment>

<Output>

I

<AddOutput>

<Value><SnmpDatasetResponse><SNMPRequest><RequestType>Column</RequestType><ObjectLis t><Object><oid></ObjectList></SNMPRequest><SnmpResponse><Row><InstanceId><las t_cond1.1></InstanceId><Columns><Column><last_cond3.1></Column></Row></Snm pResponse></SnmpDatasetResponse></Value>

<Variables>

<Variable>interface</Variable>

</Variables>

</AddOutput>

</Output>

<Goto></Goto>

</Match>

<NonMatch>

<Continue></Continue>

</NonMatch>

</Condition>

</Statements>

</Loop>

</Statements>

</Dataset>



XML APIs

Seedfile job for runnow

<Request requestId="" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"

xsi:schemaLocation="http://www.parinetworks.com/api/schemas/1.1 ../../../CSPC2.3Dev/pari/dash/resources/server/schema/pari_api.xsd"

xmlns="http://www.parinetworks.com/api/schemas/1.1">

<Job>

<Schedule operationId="1">

<JobSchedule runnow="true">

</JobSchedule>

<RegressiveSeedFileJob>

<TriggerDav>true</TriggerDav>

<DeleteCreds>true</DeleteCreds>

 $<\!\!DeleteDevices\!\!>\!\!true\!<\!\!/DeleteDevices\!\!>$

</RegressiveSeedFileJob>

</Schedule>

</Job>

</Request>

Scheduled seedfile job

I

<Request requestId="" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"

xsi:schemaLocation="http://www.parinetworks.com/api/schemas/1.1 ../../../CSPC2.3Dev/pari/dash/resources/server/schema/pari_api.xsd"

xmlns="http://www.parinetworks.com/api/schemas/1.1">

<Job>

<Schedule operationId="1">

<JobSchedule runnow="false">

<Start>1409607000000</Start>

<Repeat>

<IntervalMilliSeconds>600000</IntervalMilliSeconds>

<!- <End>1254316663640</End>->

</Repeat>

</JobSchedule>

<RegressiveSeedFileJob>

<TriggerDav>true</TriggerDav>

<DeleteCreds>true</DeleteCreds>

<DeleteDevices>true</DeleteDevices>

</RegressiveSeedFileJob>

</Schedule>

</Job>

</Request>

Add Notification

<Request xmlns="http://www.parinetworks.com/api/schemas/1.1" requestId="4444">

<Manage>

<Add operationId="1">

<NotificationList>

<Notification>

<TrapOID></TrapOID>

<NotificationType></NotificationType>

</Notification>

</NotificationList>

</Add>

</Manage>

</Request>

Delete All Notifications

<Request xmlns="http://www.parinetworks.com/api/schemas/1.1" requestId="4444">

<Manage>

<Delete operationId="1">

<NotificationList all="true">

</NotificationList>

</Delete>

</Manage>

</Request>

Delete Single Notification

<Request xmlns="http://www.parinetworks.com/api/schemas/1.1" requestId="4444">

<Manage>

<Delete operationId="1">

<NotificationList>

<Notification>

<TrapOID></TrapOID>

</Notification>

</NotificationList>

</Delete>

</Manage>

</Request>

Get All Notification Types

<Request xmlns="http://www.parinetworks.com/api/schemas/1.1" requestId="4444">

<Manage>

<Get operationId="1">

<NotificationList all="true">

</NotificationList>

</Get>

</Manage>

</Request>

Modify Notification

I

<Request xmlns="http://www.parinetworks.com/api/schemas/1.1" requestId="4444">

<Manage>

<Modify operationId="1">

<NotificationList>

<Notification>

<TrapOID></TrapOID>

<NotificationType></NotificationType>

</Notification>

</NotificationList>

</Modify>

</Manage>

</Request>

Add SNMP Trap Profile

<Request xmlns="http://www.parinetworks.com/api/schemas/1.1" requestId="44444">

<Manage>

<Add operationId="1">

<SNMPTrapProfileList>

<SNMPTrapProfile>

<ProfileName>profile1</ProfileName>

<QueueName>queue1</QueueName>

<NotificationList>

<Notification>

<NotificationType>config</NotificationType>

</Notification>

</NotificationList>

<DeviceSelection all="true">

</DeviceSelection>

</SNMPTrapProfile>

</SNMPTrapProfileList>

</Add>

</Manage>

</Request>

Delete All SNMP Trap Profiles

<Request xmlns="http://www.parinetworks.com/api/schemas/1.1" requestId="4444">

<Manage>

<Delete operationId="1">

<SNMPTrapProfileList all="true" />

</Delete>

</Manage>

</Request>

Delete Single SNMP Trap profile

<Request xmlns="http://www.parinetworks.com/api/schemas/1.1" requestId="4444">

- <Manage>
- <Delete operationId="1">

<SNMPTrapProfileList>

<SNMPTrapProfile>

<ProfileName>profile</ProfileName>

</SNMPTrapProfile>

</SNMPTrapProfileList>

- </Delete>
- </Manage>
- </Request>

Get All SNMP Trap Profiles

<Request xmlns="http://www.parinetworks.com/api/schemas/1.1" requestId="4444">

- <Manage>
 - <Get operationId="1">

<SNMPTrapProfileList all="true" />

</Get>

</Manage>

</Request>

Get Single SNMP Trap Profile

<Request requestId="4444" xmlns="http://www.parinetworks.com/api/schemas/1.1">

<Manage>

<Get operationId="1">

<SNMPTrapProfileList>

<SNMPTrapProfile> <ProfileName>profile</ProfileName>

</SNMPTrapProfile>

</SNMPTrapProfileList>

</Get>

</Manage>

</Request>

I

Modify SNMP Trap profile

<Request xmlns="http://www.parinetworks.com/api/schemas/1.1" requestId="44444">

<Manage>

<Modify operationId="1">

<SNMPTrapProfileList>

<SNMPTrapProfile>

<ProfileName>profile1</ProfileName>

<QueueName>queue1</QueueName>

<NotificationList>

<Notification>

<NotificationType>config</NotificationType>

</Notification>

</NotificationList>

<DeviceSelection all="false">

<DeviceList>

<Device>

<IPAddress>x.x.x.x</IPAddress>

</Device>

</DeviceList>

</DeviceSelection>

</SNMPTrapProfile>

</SNMPTrapProfileList>

</Modify>

</Manage>

</Request>

SNMP Trap Report

Custom Report XML

<Request xmlns="http://www.parinetworks.com/api/schemas/1.1 "requestId="44444">

<Report>

<Get operationId="1">

<SnmpTrapReport>

<TimePeriod>

<Custom>

<FromTime></FromTime>

<ToTime></ToTime>
</Custom> </TimePeriod> <Source> </Source> <NotificationList> <Notification></Notification> </NotificationList> </SnmpTrapReport> </Get> </Report>

</Request>

Report based on Time Interval

<Request xmlns="http://www.parinetworks.com/api/schemas/1.1 "requestId="44444">

<Report>

<Get operationId="1">

- <SnmpTrapReport>
- <TimePeriod>
- <SinceTime>
- </SinceTime>
- </TimePeriod>
- <Source>
- </Source>
- <NotificationList>
- <NotificationType></NotificationType>
- </NotificationList>
- </SnmpTrapReport>

</Get>

</Report>

</Request>

<SinceTime><!-- /* Style Definitions */ table.MsoNormalTable

Unknown macro: {mso-style-name}

Modify SNMP trap port and Purge Settings

<Request requestId="4444" xmlns="http://www.parinetworks.com/api/schemas/1.1">

<Manage>

I

<Modify operationId="1">

- <ApplicationPreferencesSettings>
- <SnmpTrapSettings>
- <PurgeSettings>15</PurgeSettings>
- <SnmpTrapPort>162</SnmpTrapPort>
- </SnmpTrapSettings>
- </ApplicationPreferencesSettings>
- </Modify>
- </Manage>
- </Request>

After these changes user has to restart CSPC to get this affect visible

CSPC DB backup and restore XML API

Backup Job XML API

<Request xmlns="http://www.parinetworks.com/api/schemas/1.1" requestId="3333">

<Job>

- <Schedule operationId="123">
- <JobSchedule runnow="true">
- </JobSchedule>
- <BackupJob jobName="Backup_Scheduled1">
- <IgnoreRunningJobs>false</IgnoreRunningJobs>
- <FTPServerOptions>
- <ServerHost>x.x.x.x</ServerHost>
- <UserName>root</UserName>
- <Password>XXXXX</Password>
- <Directory>resources</Directory>
- <FileName>file_temp_1</FileName>
- </FTPServerOptions>
- <PropertiesConfigFile>resources/server/backup_resource_config.properties</PropertiesConfigFile>
- </BackupJob>
- </Schedule>
- </Job>
- </Request>

Restore Job XML API

```
<Request xmlns="http://www.parinetworks.com/api/schemas/1.1" requestId="3333">
<Job>
```

- <Schedule operationId="123">
- <JobSchedule runnow="true" />
- <RestoreJob jobName="Backup">
- <FTPServerOptions>
- <ServerHost>x.x.x.</ServerHost>
- <UserName>user</UserName>
- $<\!\!Password\!\!>\!\!xxxx<\!\!/\!Password\!\!>$
- <Directory>resources</Directory>
- <FileName>_1391384366427.pbx</FileName>
- </FTPServerOptions>
- </RestoreJob>
- </Schedule>

</Job>

</Request>

CLI Channel XML API

CSPC CLI Channel dynamically supports the devices and accepts the required inputs using xml and stores these inputs in DB for future use.

New Device Input XML

I

```
<?xml version="1.0"?>
```

<Request xmlns="http://www.parinetworks.com/api/schemas/1.1" requestId="12">

<Manage>

<Add operationId="1" replace="true">

<ChannelType channelId = "StarOS"> <!-- Provide unique name for new channel -->

<ChannelTypeRules>

<Rules>

<MatchType>ANY</MatchType> <!-- MatchType is based on rules provided, ANY or ALL --> <Rule>

<Attribute><![CDATA[OSTYPE]]></Attribute> <!-- Provide the attribute which needs to be matched with device OSTYPE, SYSOBJID, VERSIONTYPE -->

<Operator>EQUALS</Operator> <!-- Provide operator used to match with attribute EQUALS, INDEXOF, STARTSWITH, ENDSWITH, CONTAINS, GREATERTHAN, LESSTHAN -->

<Operands>

<Operand><![CDATA[Star OS]]></Operand> <!-- Operand depend on attribute and operator values -->

</Operands>

</Rule>

</Rules>

</ChannelTypeRules>

<CLIRules>

<MorePromptRules>

<Rules>

<MatchType>ANY</MatchType> <!-- MatchType is based on rules provided, ANY or ALL -->

<Rule>

<Attribute><![CDATA[OUTPUT]]></Attribute>

<Operator>INDEXOF</Operator> <!-- Provide operator used to match with attribute EQUALS, INDEXOF, STARTSWITH, ENDSWITH, CONTAINS -->

<Operands>

<Operand><![CDATA[--More--]]></Operand> <!-- Provide more prompts available for the device -->

</Operands>

</Rule>

</Rules>

<ContinueChar><![CDATA[32]]></ContinueChar> <!-- Provide character needs to be entered if more prompt available -->

</MorePromptRules>

<OtherPromptRules>

<Rules><!-- This OtherPromptRules are used when the device is having prompts other than more prompts -->

<MatchType>ANY</MatchType>

<Rule>

<Attribute><![CDATA[OSTYPE]]></Attribute>

<Operator>EQUALS</Operator>

<Operands>

<Operand><![CDATA[AsyncOS]]></Operand>

</Operands>

</Rule>

<Rule>

<Attribute><![CDATA[OUTPUT]]></Attribute>

<Operator>INDEXOF</Operator>

<Operands>

<Operand><![CDATA[Do you want to mask the password]]></Operand> <!-- The prompt appears on the device -->

</Operands>

</Rule>

</Rules>

</OtherPromptRules>

<EnableRules>

<EnableCommand>enable</EnableCommand> <!-- Provide command used to enter into enable mode -->

<EnableUserPrompts><![CDATA[Username:&login:&user:]]></EnableUserPrompts><!-- Provide user prompts -->

<EnablePwdPrompts><![CDATA[Password:]]></EnablePwdPrompts> <!-- Provide password prompts -->

</EnableRules>

<ClearTerminalLengthDefinition>

 $<\!\! \rm Command\!\!>\! \rm terminal \ length 0<\!\!/ \rm Command\!\!>\!<\!\! \rm !--$ Provide commands used to set terminal length for the device -->

<Command>terminal width 0</Command>

</ClearTerminalLengthDefinition>

<AfterLoginCommand>

<Command>clish</Command> <!-- some devices required commands after login to the device and before entering into the enable mode, provide those commands here -->

</AfterLoginCommand>

<ReplaceEscChar>[j</ReplaceEscChar> <!-- Provide escape characters to be replaced -->

<ClearLineDef>3</ClearLineDef> <!-- This will clear the buffer before executing the command while collecting the data from the device -->

<ControlChar>\n</ControlChar>

<Priority>100</Priority>

<UsePariPatentEndOfCommand>true</UsePariPatentEndOfCommand>

</CLIRules>

</ChannelType>

</Add>

</Manage>

</Request>

Modify Channel XML

<?xml version="1.0"?>

<Request xmlns="http://www.parinetworks.com/api/schemas/1.1" requestId="12">

<Manage>

<Modify operationId="1">

<ChannelType channelId = "ACNS"> <!-- Provide unique name for new channel -->

<ChannleTypeRules>

<Rules>

<MatchType>ANY</MatchType> <!-- MatchType is based on rules provided, ANY or ALL -->

<Rule>

<Attribute><![CDATA[OSTYPE]]></Attribute> <!-- Provide the attribute which needs to be matched with device OSTYPE, SYSOBJID, VERSIONTYPE -->

<Operator>EQUALS</Operator> <!-- Provide operator used to match with attribute EQUALS, INDEXOF, STARTSWITH, ENDSWITH, CONTAINS, GREATERTHAN, LESSTHAN -->

<Operands>

<Operand><![CDATA[Star OS]]></Operand> <!-- Operand depend on attribute and operator values -->

</Operands>

</Rule>

</Rules>

</ChannleTypeRules>

<CLIRules>

<MorePromptRules>

<Rules>

<MatchType>ANY</MatchType> <!-- MatchType is based on rules provided, ANY or ALL -->

<Rule>

<Attribute><![CDATA[OUTPUT]]></Attribute>

<Operator>INDEXOF</Operator> <!-- Provide operator used to match with attribute EQUALS, INDEXOF, STARTSWITH, ENDSWITH, CONTAINS, GREATERTHAN, LESSTHAN -->

<Operands>

<Operand><![CDATA[--More--]]></Operand> <!-- Provide more prompts available for the device -->

<Operand><![CDATA[<--- More --->]]></Operand>

</Operands>

</Rule>

</Rules>

```
<ContinueChar><![CDATA[32]]></ContinueChar> <!-- Provide character needs to be entered if more prompt available -->
```

</MorePromptRules>

<OtherPromptRules>

<Rules><!-- This OtherPromptRules are used when the device is having prompts other than more prompts -->

<MatchType>ANY</MatchType>

<Rule>

<Attribute><![CDATA[OSTYPE]]></Attribute>

<Operator>EQUALS</Operator>

<Operands>

<Operand><![CDATA[AsyncOS]]></Operand>

</Operands>

</Rule>

<Rule>

<Attribute><![CDATA[OUTPUT]]></Attribute>

<Operator>INDEXOF</Operator>

<Operands>

 $<\!\!Operand\!\!><\!\!![CDATA[Do you want to mask the password]]\!\!><\!\!/Operand\!\!><\!\!!-- The prompt appears on the device --\!\!>$

</Operands>

</Rule>

</Rules>

<ContinueChar><![CDATA[Y]]></ContinueChar> <!-- ContinueChar is used if we need to input any data/character to continue further from the prompt -->

</OtherPromptRules>

<EnableRules>

<EnableCommand>enable</EnableCommand> <!-- Provide command used to enter into enable mode -->

<EnableUserPrompts><![CDATA[Username:&Password:&login:&user:]]></EnableUserPrompts><!-- Provide user prompts -->

<EnablePwdPrompts><![CDATA[Password:]]></EnablePwdPrompts> <!-- Provide password prompts

</EnableRules>

I

<ClearTerminalLengthDefinition>

 $<\!\! \rm Command\!\!>\! \rm terminal \ length 0<\!\!/ \rm Command\!\!>\!<\!\! \rm !--$ Provide commands used to set terminal length for the device -->

<Command>terminal width 0</Command>

</ClearTerminalLengthDefinition>

<AfterLoginCommand>

<Command>Clish</Command> <!-- some devices required commands after login to the device and before entering into the enable mode, provide those commands here -->

</AfterLoginCommand>

<ReplaceEscChar>[j</ReplaceEscChar> <!-- Provide escape characters to be replaced -->

<ClearLineDef>3</ClearLineDef> <!-- This will clear the buffer before executing the command while collecting the data from the device -->

<ControlChar>\n</ControlChar>

<Priority>100</Priority>

<UsePariPatentEndOfCommand>true</UsePariPatentEndOfCommand>

</CLIRules>

</ChannelType>

</Modify>

</Manage>

</Request>

CLI Channel Get Report XML

<Request xmlns="http://www.parinetworks.com/api/schemas/1.1" requestId="CLIChannelReport">

<Manage>

<Get operationId="1">

<CLIChannelReport all = "false"> <!-- all equals true will get the all channels Channel Type rules only not CLI rules -->

<ChannelId>IOS</ChannelId> <!-- if all equals false we need to provide channel id to get that particular channel channel type rulas and cli rules -->

</CLIChannelReport>

</Get>

</Manage>

</Request> ?

Channel Delete Channel XML

- <Request xmlns="http://www.parinetworks.com/api/schemas/1.1" requestId="ChannelList">

- <Manage>
- <Delete operationId="1">
- <ChannelType channelId="Acsw" />
- <!-- This Xml deletes channel definitions which is provided here as channelId
- -->
- </Delete>
- </Manage>
- </Request>

Get CLI Channel List Report XML

Request xmlns="http://www.parinetworks.com/api/schemas/1.1" requestId="ChannelList">

<Manage>

<Get operationId="1">

<ChannelList all = "true"/> <!-- This report lists all the existing channel ids list --> </Get>

</Manage>

</Request>?

Get Imported Devices Status Report

<Request xmlns="http://www.parinetworks.com/api/schemas/1.1" requestId="44444">

<Manage>

<Get operationId="1">

<ImportedDeviceStatusReport>

<DiscoveryJobId>32</DiscoveryJobId>

<DiscoveryJobRunId>1</DiscoveryJobRunId>

</ImportedDeviceStatusReport>

</Get>

</Manage>

</Request>

CSPC Backup (PSS)

I

<Request xmlns="http://www.parinetworks.com/api/schemas/1.1" requestId="3333">

<Job>

<Schedule operationId="123">

<JobSchedule runnow="true">

</JobSchedule>

<BackupJob jobName="Backup_RunNow">

<BackupJobType>Full_Backup</BackupJobType>

<IgnoreRunningJobs>true</IgnoreRunningJobs>

<FTPServerOptions>

<ServerHost>x.x.x.x</ServerHost>

<UserName>root</UserName>

<Password>cXXXXX</Password>

<Directory>CSPC_Backup</Directory>

<FileName>backup</FileName>

</FTPServerOptions>

<IgnoreInventoryData>true</IgnoreInventoryData>

</BackupJob>

</Schedule>

</Job>

</Request>

CSPC Backup (PSS) - Schedule

<Request xmlns="http://www.parinetworks.com/api/schemas/1.1" requestId="3333"> <Job>

<Schedule operationId="123">

<JobSchedule runnow="false">

<Start>1450692900000</Start>

</JobSchedule>

<BackupJob jobName="Backup_RunNow">

<BackupJobType>Full_Backup</BackupJobType>

<IgnoreRunningJobs>true</IgnoreRunningJobs>

<FTPServerOptions>

<ServerHost>10.127.152.54</ServerHost>

<UserName>admin</UserName>

<Password>XXXXX</Password>

<FileName>xml</FileName>

</FTPServerOptions>

<IgnoreInventoryData>true</IgnoreInventoryData>

</BackupJob>

</Schedule>

</Job>

</Request>

Collection of Loopback Interface IP address (NOS)

<Request xmlns="http://www.parinetworks.com/api/schemas/1.1" requestId="3333"> <Job>

<Schedule operationId="1">

<JobSchedule runnow="true" />

<DiscoveryJob identifier="my_discovery123">

<DiscoveryOptionsList>

<DiscoveryOptions>

<IPAddressList>

<IPAddress>x.x.x.x</IPAddress>

</IPAddressList>

<useLoopBackIp>true</useLoopBackIp>

</DiscoveryOptions>

</DiscoveryOptionsList>

</DiscoveryJob>

</Schedule>

</Job>

</Request>

Add Optional Metadata Label to OIDs in Custom Datasets (PSS)

<Request xmlns="http://www.parinetworks.com/api/schemas/1.1" requestId="44444"> <Manage> <Add operationId="1"> <DatasetList> <Dataset identifier="_snmp_XML_SNTest2"> <Title>_snmp_XML_SNTest2</Title> <Description /> <CategoryName>1</CategoryName> <CreatedUser>XML</CreatedUser> <Locked>false</Locked> <CollectionType>SNMP</CollectionType> <VersionedDatasetList> <VersionedDataset identifier="cisco"> <SNMP>

<SNMPRequest>

I

<RequestType>Scalar</RequestType>

<ObjectList> <Object> <Id>.1.3.6.1.4.1.9.2.1.3</Id> <Title>hostName</Title> <Tag>!@#\$%^&*()":.,</Tag> <Type>Scalar</Type> </Object> </ObjectList> </SNMPRequest> </SNMP> </VersionedDataset> </VersionedDatasetList> </Dataset> </DatasetList> </Add> </Manage>

</Request>

Export and Import Collection Profiles (PSS)

- Api for Export All Rules <Request> <Export> <ExportAllRules> <ExportLocation></ExportLocation> </ExportAllRules> </Request> API for Import All Rules <Request>
- <Execute>
- <ImportAllRulesFromZipFile>

<AllRuleZipFileLocation>/opt/CSPC/data/ruleExport/CSPCRules_1450433792272.Zip</AllRuleZipFileLocation>

</ImportAllRulesFromZipFile>
</Execute>

</Request>

Upload Signature for Custom Profiles (PSS)

<CollectionProfile identifier="_ASA_Test">

<Title>ASA Test</Title>

- <CreatedUser>admin</CreatedUser>
- <CreationTime>1439385708000</CreationTime>
- <Locked>false</Locked>
- <Tag>DONOTPROCESS</Tag>
- <ExportSeedFile>false</ExportSeedFile>
- <ApplicationDiscoveryProfile>false</ApplicationDiscoveryProfile>
- <DisableCollectionInterval>false</DisableCollectionInterval>
- <Priority>Medium</Priority>
- <PreserveRunCount>1</PreserveRunCount>
- <CredentialFallback>false</CredentialFallback>
- <RunDiscoveryBeforeExecution>false</RunDiscoveryBeforeExecution>
- <RunDAVBeforeExecution>false</RunDAVBeforeExecution>
- <RunPromptCollectionBeforeExecution>false</RunPromptCollectionBeforeExecution>
- <DeviceSelection all="true" />
- <DatasetList>
- <Dataset>_show running_config</Dataset>
- </DatasetList>
- <DataPrivacy>
 - <IsIPPrivacyEnabled>false</IsIPPrivacyEnabled>
- <IsHostPrivacyEnabled>false</IsHostPrivacyEnabled>
- </DataPrivacy>
- </CollectionProfile>

Discovery Classification

I

- <Request requestId="123">
- <Manage>
- <Modify operationId="11">
- <ApplicationPreferencesSettings>
 - <Discovery>

<SnmpTimeout>3</SnmpTimeout>

<SnmpRetry>1</SnmpRetry>

<MaxThreadCount>100</MaxThreadCount>

<MaxCredentialSets>10</MaxCredentialSets>

<MaxDiscoveryTime>600</MaxDiscoveryTime>

<MaxDeviceDiscoveryTime>180</MaxDeviceDiscoveryTime>

<IpPhoneDiscovery>false</IpPhoneDiscovery>

<NmapTimeout>30</NmapTimeout>

<SerialNumDuplicateCheckEnabled>false</SerialNumDuplicateCheckEnabled>

<IncludePlatformList>[]</IncludePlatformList>

<TryPingFirst>true</TryPingFirst>

<ExcludePlatformList>[_EXCLUDE_CSCus90617]</ExcludePlatformList>

<EnableCLIdiscovery>false</EnableCLIdiscovery>

<CLIDiscoveryTimeOut>3</CLIDiscoveryTimeOut>

<EnableSnmpConfigPush>false</EnableSnmpConfigPush>

</Discovery>

</ApplicationPreferencesSettings>

</Modify>

</Manage>

</Request>

Enabling/Disabling the WebSocket Connection

Now, with this XML API, you can control (enabling/disabling) WebSocket Connection from CSPC.

Enabling

<Request requestId="4444" xmlns="http://www.parinetworks.com/api/schemas/1.1">

<Manage>

<Modify operationId="1">

<WebSocketSettings>

<Enable>Yes</Enable>

</WebSocketSettings>

</Modify>

</Manage>

</Request>

Disabling

<Request requestId="4444" xmlns="http://www.parinetworks.com/api/schemas/1.1">

<Manage>

<Modify operationId="1">

<WebSocketSettings>

<Enable>No</Enable>

</WebSocketSettings>

</Modify>

</Manage>

</Request>

Note: If you get any error while closing the connection, try to execute same XML one more time.

GET WebSocket Status

<Request requestId="4444" xmlns="http://www.parinetworks.com/api/schemas/1.1">

<Manage>

<Get operationId="1">

<WebSocketSettings>

</WebSocketSettings>

</Get>

</Manage>

</Request>

Add External Platform Components Credentials

<Request requestId="63" xmlns="http://www.parinetworks.com/api/schemas/1.1">

<Manage>

I

<Add operationId="1">

<AddExternalComponents>

<DeviceCredential identifier="CIMC_snmpv3"> ---- Provide credential name

<Type>CIMC</Type> — Provide valid Type ex: CIMC, PFSENSE, ESXI

<IpExpressionList>

<IpExpression>x.x.x.</IpExpression> — Give valid IP address

</IpExpressionList>

<SNMPV3UserName>ucsSNMPV3user</SNMPV3UserName> --- Provide SNMPV3 credentials details if SNMPV3 enabled

- <SNMPV3AuthProtocol>SHA</SNMPV3AuthProtocol>
- <SNMPV3AuthPassPhrase>xxxxx</SNMPV3AuthPassPhrase>
- <SNMPV3PrivProtocol>AES-128</SNMPV3PrivProtocol>
- <SNMPV3PrivPassPhrase>xxxxx</SNMPV3PrivPassPhrase>
- <SNMPV3EngineId>authpriv</SNMPV3EngineId>
- <Protocol>snmpv3</Protocol>
- </DeviceCredential>

<DeviceCredential identifier="ESXI_snmpv3">

- <Type>ESXI</Type>
- <IpExpressionList>
 - <IpExpression>x.x.x.</IpExpression>
- </IpExpressionList>
- <SNMPV3UserName>xxxx</SNMPV3UserName>
- <SNMPV3AuthProtocol>SHA</SNMPV3AuthProtocol>
- <SNMPV3AuthPassPhrase>XXXXX</SNMPV3AuthPassPhrase>
- <SNMPV3PrivProtocol>AES-128</SNMPV3PrivProtocol>
- <SNMPV3PrivPassPhrase>XXXXX</SNMPV3PrivPassPhrase>
- <SNMPV3EngineId>authpriv</SNMPV3EngineId>
- <Protocol>snmpv3</Protocol>
- </DeviceCredential>
- <DeviceCredential identifier="pfsense_snmpv2">
 - <Type>PFSENSE</Type>
 - <IpExpressionList>
- <IpExpression>x.x.x.x</IpExpression> Provide SNMPV2 credentials details if SNMPV2 enabled
 - </IpExpressionList>
 - <ReadCommunity>public</ReadCommunity>
 - <Protocol>snmpv2c</Protocol>
 - </DeviceCredential>
 - </AddExternalComponents>
 - </Add>
- </Manage>
- </Request>

Upload Health Information

<Request xmlns="http://www.parinetworks.com/api/schemas/1.1" requestId="63"> <Job>

<Schedule operationId="1">

<JobSchedule runnow="true" />

<HealthMonitorJob jobName="HMJ1">

<IncludeSystemDetails>true</IncludeSystemDetails>

<IncludeCollectorLogs>true</IncludeCollectorLogs>

<IncludeAddOnHealth>true</IncludeAddOnHealth>

<IncludeExternalDeviceData>true</IncludeExternalDeviceData> —— Set IncludeExternalDeviceData to true to include 3rd external components data

<UploadData>true</UploadData>

</HealthMonitorJob>

</Schedule>

</Job>

</Request>

Error Message for Smart DAV based on SSH/Telnet

<Request xmlns="http://www.parinetworks.com/api/schemas/1.1" requestId="cp_schedule"> <Job>

<Schedule operationId="1">

<JobSchedule runnow="true">

</JobSchedule>

<DAVJob jobName="SBTestDavJobXML">

<DeviceSelection all="true"/>

<OverrideEnableFailed>true</OverrideEnableFailed>

<RunDAVForUnreachable>true</RunDAVForUnreachable>

<RunDiscoveryBeforeExecution>false</RunDiscoveryBeforeExecution>

<Pingable>true</Pingable>

</DAVJob>

</Schedule>

</Job>

I

</Request>

Region Based Collection via User Groups

For creating static device group based on the user fields during import seedfile:

```
<?xml version="1.0" encoding="UTF-8"?>
<Request xmlns="http://www.parinetworks.com/api/schemas/1.1" requestId="seedfile">
 <Job>
   <Schedule operationId="1">
     <JobSchedule runnow="true" />
     <ImportSeedFileJob jobName="q20">
       <Description>a1</Description>
       <DeviceGroup></DeviceGroup>
       <SeedFileDescr />
       <GroupByUserField>true</GroupByUserField>
       <SeedFileFormat>CISCO_CNC_CSV</SeedFileFormat>
       <FileDetails>
         <SeedFileName>Seed11.csv</SeedFileName>
       </FileDetails>
       <TriggerDiscovery>true</TriggerDiscovery>
       <TriggerDav>false</TriggerDav>
       <EntitlementId>CSP0001040260</EntitlementId>
     </ImportSeedFileJob>
   </Schedule>
  </Job>
</Request>
```

Service Name for Service Prioritize

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<Request xmlns="http://www.parinetworks.com/api/schemas/1.1" requestId="1111">
<Manage>
<Add>
<ServiceRegistration>
<Application type="add-on" name = "ADDONNAME"> </Application>
</ServiceRegistration>
</Add>
```

</Request>

Add Credentials

_____ <Request xmlns="http://www.parinetworks.com/api/schemas/1.1" requestId=""> <Manage> <Add operationId="1" replace="true"> <DeviceCredentialList> <DeviceCredential identifier="My_sql"> <Protocol>sql</Protocol>-----Protocol <Port>1433</Port>-----Port number <DBServer>Microsoft SQL</DBServer>----- Database server <DBIpaddress>*.*.*</DBIpaddress>----- IP address Database <DBName>***</DBName>-----Database name <UserName>***</UserName>----- database user name <Password>****</Password>------database password <IpExpressionList> <IpExpression>*.*.*</IpExpression> ------IP address </IpExpressionList> </DeviceCredential> </DeviceCredentialList> </Add> </Manage> </Request>

Add SQL Datasets

I

<Request xmlns="http://www.parinetworks.com/api/schemas/1.1" requestId="44444">

<Manage>

<Add operationId="1">

<DatasetList>

<Dataset identifier="Name">

<Title>Title</Title>

<CategoryName>Sql</CategoryName> <CreatedUser>xyz</CreatedUser> <Locked>false</Locked> <CollectionType>SQL</CollectionType> <VersionedDatasetList> <VersionedDataset identifier="cisco"> <SQL> <Command>command</Command>----- Provide sql query/command </SQL> </VersionedDataset> </VersionedDatasetList> </Dataset> </DatasetList> </Add> </Manage> </Request>

Schedule the Job with Service Name

<Request xmlns="http://www.parinetworks.com/api/schemas/1.1" requestId="3333">

```
<Job service_name="NOS">
```

<Description />

- <Schedule operationId="1">
- <JobSchedule runnow="true"/>

<DiscoveryJob identifier="ipList">

<DiscoveryOptionsList>

<DiscoveryOptions>

<IPAddressList>

- <IPAddress>5.0.1.2</IPAddress>
- </IPAddressList>
- </DiscoveryOptions>
- </DiscoveryOptionsList>
- </DiscoveryJob>
- </Schedule>
- </Job>
- </Request>

Add File Dataset

<Request requestId="44444" xmlns="http://www.parinetworks.com/api/schemas/1.1">

<Manage>

<Add operationId="1"><DatasetList>

<Dataset identifier="file">

<Title>file</Title>

<CategoryName>File</CategoryName>

<CreatedUser>admin</CreatedUser>

<CreationTime>1522161616000</CreationTime>

<Locked>false</Locked>

<CollectionType>FILE</CollectionType>

<CollectionInterval>0</CollectionInterval>

<ApplicablePlatforms>[CISCO]</ApplicablePlatforms>

<VersionedDatasetList>

<VersionedDataset identifier="cisco">

<File>

<Name><![CDATA[File Name]]></Name>

<Location><![CDATA[File path]]></Location>

<GenerateFileCommand><![CDATA[Command to generate file]]GenerateFileCommand>

<DownloadFileCommand><![CDATA[Command to download the

file]]></DownloadFileCommand>

<IntegrityRule> INTEG_RULE</IntegrityRule>

</File>

</VersionedDataset>

</VersionedDatasetList>

</Dataset>

</DatasetList>

</Add>

</Manage>

</Request>

API to Export and Get File name

I

REST API call to export and get the filename https://localhost:8001/cspc/xml/

@POST @Consumes({MediaType.APPLICATION_XML}) Input: XML Request : <Request xmlns="http://www.parinetworks.com/api/schemas/1.1" requestId="44444"> <Export> <CollectionList> <Collection> <CollectionProfile identifier="_cpname"/> <ExportFromRestAPI>true</ExportFromRestAPI> </Collection> </CollectionList> </Export> </Request> Response/output : <Response requestId="44444"> <Status code="SUCCESSFUL" /> <Export> <CollectionList> <JobId>32</JobId> <FileName>CPExport_1534231458802_export.zip</FileName> </CollectionList> </Export> </Response>

API to Download the Collection Profile Run Data

REST API GET call to download the collection profile run data https://localhost:8001/cspc/file/filename.zip?fileStoreType=export&jobid=32

Additional Device Properties

Add Family OS type and Technology Properties

<Request xmlns="http://www.parinetworks.com/api/schemas/1.1" requestId="44444">

<Manage>

<Add operationId="1">

- <DevicePropertiesList>
- <AdditionalDeviceProperties>
- <IpAddress>10.10.10.10</IpAddress>
- <Family>family1</Family>
- <OSType>abcd</OSType>
- <TechnologyList>
- <Technology>tech1</Technology>
- <Technology>tech2</Technology>
- </TechnologyList>
- </AdditionalDeviceProperties>
- </DevicePropertiesList>

</Add>

</Manage>

</Request>

Modify Additional Device Properties

<Request xmlns="http://www.parinetworks.com/api/schemas/1.1" requestId="44444">

<Manage>

<Modify operationId="1">

<DevicePropertiesList>

<AdditionalDeviceProperties>

<IpAddress>10.10.10.10</IpAddress>

```
<Family>family2</Family>
```

<OSType>abcde</OSType>

<TechnologyList>

- <Technology>tech3</Technology>
- <Technology>tech4</Technology>
- </TechnologyList>
- </AdditionalDeviceProperties>
- </DevicePropertiesList>

</Modify>

</Manage>

I

</Request>

Delete Additional Device Properties

```
<Request xmlns="http://www.parinetworks.com/api/schemas/1.1" requestId="44444">
<Manage>
<Get operationId="1">
<DevicePropertiesList>
<AdditionalDeviceProperties>
<IpAddressList>
<IpAddress>10.10.10.10</IpAddress>
<IpAddress>10.10.10.11</IpAddress>
</IpAddressList>
</AdditionalDeviceProperties>
</DevicePropertiesList>
</Get>
</Request>
```

Get Additional Device Properties

```
<Request xmlns="http://www.parinetworks.com/api/schemas/1.1" requestId="44444">
```

<Manage>

<Delete operationId="1">

<DevicePropertiesList>

<AdditionalDeviceProperties>

<IpAddressList>

<IpAddress>5.0.1.1</IpAddress>

- <IpAddress>5.0.1.2</IpAddress>
- </IpAddressList>

</AdditionalDeviceProperties>

- </DevicePropertiesList>
- </Delete>
- </Manage>

</Request>

Adding WMI Datasets

<Request xmlns="http://www.parinetworks.com/api/schemas/1.1" requestId="44444">

<Manage>

<Add operationId="1">

<DatasetList>

<Dataset identifier="_netstat_wmi">

<Title>netstat_wmi</Title>

<CategoryName>wmi</CategoryName>

<TagName />

<CreatedUser>admin</CreatedUser>

<Locked>false</Locked>

<CollectionType>WMI</CollectionType>

<CollectionInterval >0</CollectionInterval>

<ApplicablePlatforms>[CISCO]</ApplicablePlatforms>

<VersionedDatasetList>

<VersionedDataset identifier="cisco">

<WMI>

<Namespace>CIMV2</Namespace>

<Query type="PS/WMI">Command to be added</Query>

</WMI>

</VersionedDataset>

</VersionedDatasetList>

```
</Dataset>
```

</DatasetList>

</Add>

</Manage>

</Request>

I

Adding LDAP Datasets

<Request xmlns="http://www.parinetworks.com/api/schemas/1.1" requestId="44444"> <Manage> <Add operationId="1"> <DatasetList> <Dataset identifier="_ldap_dataset"> <Title>ldap_dataset</Title> <CategoryName>ldap</CategoryName> <TagName /> <CreatedUser>admin</CreatedUser> <Locked>false</Locked> <CollectionType>LDAP</CollectionType> <CollectionInterval>0</CollectionInterval> <ApplicablePlatforms>[Custom]</ApplicablePlatforms> <VersionedDatasetList> <VersionedDataset identifier="_ACNS"> <LDAP> <SearchBase></SearchBase> <SearchFilter></SearchFilter> <SearchScope></SearchScope> <AttributesToReturn></AttributesToReturn> <MaskRule> </MaskRule> <Timeout></Timeout> </LDAP> </VersionedDataset> </VersionedDatasetList> </Dataset> </DatasetList> </Add> </Manage> </Request>



Uploading Valid SSL Certificate

To upload SSL certificate to CSPC Keystore, Perform the following :

- Step 1 Choose any one the following:
 - Customer who wants to upload SSL certificate of their choice may provide SSL certificate purchased from a trusted certificate authority

OR

• Customers can provide their own self signed certificate

For the above two scenario's you can directly start from Step 4.



I

All the Self signed certificates provides a warning message on the browser.

Figure F-1 Warning Message

The owner of stolen, Firefox has not co	has configured their website improperly. To protect onnected to this website.	your information from being	
Learn more			
Go Back		Advanced	
Report errors like th	is to help Mozilla identify and block malicious sites		
Report errors like th	is to help Mozilla identify and block malicious sites s an invalid security certificate.		
Report errors like th use The certificate is not trust The certificate is not valid	is to help Mozilla identify and block malicious sites s an invalid security certificate. ted because it is self-signed. I for the name		
Report errors like th use The certificate is not trust The certificate is not valid Error code: SEC_ERROR_	is to help Mozilla identify and block malicious sites s an invalid security certificate. ted because it is self-signed. for the name UNKNOWN_ISSUER		

You will not get this waring if we use the SSL certificate provided by the trusted signing authority like Symantec (Verisign) or Digicert.

Generating a Self-signed certificate

Self-signed certificate needs Private key and Certificate signing request (CSR)

Step 2 Generate the Private key and Certificate Signing Request (CSR) using the below Command in CSPC CLI. Customer must provide the input field details

```
#openssl req -new -newkey rsa:2048 -nodes -keyout localhost.key -out
localhost.csr
Generating a 2048 bit RSA private key
. . . . . . . . . . . . . . . . +++
. . . . . . . . . . . . . . . . +++
writing new private key to 'localhost.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or
a DN.
There are quite a few fields, but you can leave some
blank.For some fields there will be a default value,
If you enter '.', the field will be left blank.
Country Name (2 letter code) [XX]:IN
State or Province Name (full name) []:TN
Locality Name (eg, city) [Default City]:Trichy
Organization Name (eg, company) [Default Company Ltd]:KSKTech
Organizational Unit Name (eg, section) []:IT
Common Name (eg, your name or your server's hostname) []:cspc
```

Email Address []:ksk@wxyz.com

Please enter the following 'extra' attributes to be sent with your certificate request A challenge password []:password An optional company name []:AEY

Above command generates two files localhost.key (Key file) and localhost.csr (CSR file)

- Scenario 1: Some customer may request us to generate only the key & CSR file and they will create the certificate using the generated key /CSR files. Provide the above files (localhost.csr & localhost.key) to the customer, they will generate and provide the certificate. The certificate file will be either .crt or .cer. (.cer file generally belongs to Microsoft Platform) and proceed to Step 4.
- Scenario 2: Customer may request us to create the certificate from the generated key and CSR file (localhost.csr & localhost.key), continue with Step 3

```
Step 3 Create certificate using below command
```

```
# openssl x509 -req -days 500 -in localhost.csr -signkey localhost.key
-out localhost.crt
Signature ok
```

subject=/C=IN/ST=TN/L=Trichy/O=KSKTech/OU=IT/CN=cspc/emailAddress= ksk@wxyz.com

Getting Private key

Above command generates the self-signed certificate file, localhost.crt

This step is optional:

Use the following command to check the certificate provided by the customer before creating the keystore

```
/opt/cisco/ss/adminshell/applications/CSPC/jreinstall/bin/keytool
-printcert -v -file localhost.crt
```

Step 4 Creating the keystore use the following command

#openssl pkcs12 -export -in localhost.crt -inkey localhost.key >
localhost.p12

Enter ExportPassword:cspcgxt

Verifying - Enter Export Password:cspcgxt

Above command generates.p12 file

Note

Use "cspcgxt" as password (if some other password is used then you need to create a separate keystore and need to edit the server.xml file entries "keystoreFile" and "keystorePass".

Step 5 Importing the created keystore into CSPC's keystore using command

```
/opt/cisco/ss/adminshell/applications/CSPC/jreinstall/bin/keytool
-importkeystore -srckeystore localhost.pl2 -srcstoretype pkcsl2
-destkeystore $CSPCHOME/webui/tomcat/conf/cspcgxt -deststoretype jks
```

Enter destination keystore password:cspcgxt

Enter source keystore password:cspcgxt

Entry for alias 1 successfully imported.

Import command completed: 1 entries successfully imported, 0 entries failed or canceled

Step 6 Deleting the existing alias from the CSPC keystore

*checking the CSPC keystore for details using command

/opt/cisco/ss/adminshell/applications/CSPC/jreinstall/bin/keytool
-list -v -keystore \$CSPCHOME/webui/tomcat/conf/cspcgxt

Your keystore contains 2 entries

Alias name: tomcat

Alias name: 1

You have to delete the tomcat Alias since it contains the CSPC self-signed certificate using below command

```
/opt/cisco/ss/adminshell/applications/CSPC/jreinstall/bin/keytool
-delete -alias tomcat -keystore $CSPCHOME/webui/tomcat/conf/cspcgxt
Enter keystore password:cspcgxt
```

/opt/cisco/ss/adminshell/applications/CSPC/jreinstall/bin/keytool -list -v -keystore \$CSPCHOME/webui/tomcat/conf/cspcgxt Enter keystore password:cspcgxt Now the CSPC keystore has only 1 Alias, Keystore type: JKS Keystore provider: SUN Your keystore contains 1 entry Alias name: 1

Changing Alias name to tomcat (this step is optional) using the command below.

/opt/cisco/ss/adminshell/applications/CSPC/jreinstall/bin/keytool
-changealias -alias 1 -destalias tomcat -keystore
\$CSPCHOME/webui/tomcat/conf/cspcgxt

Enter keystore password: cspcgxt

Step 7 Verifying the Alias name change,

/opt/cisco/ss/adminshell/applications/CSPC/jreinstall/bin/keytool
-list -v -keystore \$CSPCHOME/webui/tomcat/conf/cspcgxt

Enter keystore password: cspcgxt

Keystore type: JKS

Keystore provider: SUN. Your keystore contains 1 entry

Alias name: tomcat

Step 8 Restart the CSPC service using below command

service cspc restart

Step 9 Verify the uploaded SSL certificate in a browser below screen appears

ſ



Figure F-2 Certificate Information



RSA SHA 256 Fingerprint

To generate the RSA SHA 256 fingerprint for the corresponding host key, perform the following:

Step 1 Login to the host box where you want to perform backup or restore and execute the below command ssh-keygen -l -f /etc/ssh/ssh host rsa key

Sample Output

I

db:db:97:37:b9:af:df:fc:c5:af:b6:b4:1a:85:02:7f (MD5 checksum)

zU7R1r/JZaWFLmF1jKVm5Zrtu0aGvTyQzVU60RI73n0 (base64-encoded SHA256 checksum)

Note

In OpenSSH 7.0 and earlier versions this fingerprint was a hexadecimal MD5 checksum. Now it is base64- encoded SHA256 checksum.



CSPC - Automated Fault Management (AFM) Tool Integration

CloudRay deployment with CSPC, NCE should follow the steps to establish the secured SSL based communication channel between CSPC and CloudRay.

- Step 1 Create a new user with group type "External Client User", on CSPC.
- Step 2 Configure the above created user's username and password, on CloudRay JMS client.
- Step 3 Replace the existing pariTrustStore with the latest one available in \$CSPCHOME/bin. on CloudRay JMS client. This step is mandatory only if the pariTrustStore is modified on CSPC.
- **Step 4** Add the below firewall rule just before the loopback interface rules that would allow to accept the connections from CloudRay on port 61617, on CSPC.
- Step 5 This should be a permanent entry and finally restart the iptables.

Γ

iptables -A INPUT -p tcp -m tcp --dport 61617 -j ACCEPT


Reset Root Password and Deployment of ESXi 7.0

Recovering Root Password

Step 2 Step 3 Step 4 Step 5 Step 6 Step 7

Γ

To recover the root password, perform the following:

Step 1 Reboot the server from console and as the boot process starts, press e to edit the first boot option.

Figure I-1	Console	
CSPC29_	-	🖬 🖬 🛄 🋱 Actions 🕲
CentOS	S Linux (4.18.0-193.14.2.e18_2.x86_64) 8 (Core)	
CentO	S Linux (4.18.0-147.018.x86_64) 8 (Lore) S Linux (0-rescue-96a7ab34b04c49d18b1c12ed0a41993a)	8 (Core)
	and and to have described and the second law	
Press	he ⊤ and ↓ keys to change the selection. 'e' to edit the selected item, or 'c' for a command	prompt.
The selec	cted entry will be started automatically in 3s.	I · I
Enter grub Use	rname (root) and Password.	
Search the kern	el for the line that starts with linux, change ro to rw init=/	'sysroot/bin/sh
$Press \; \texttt{CTRL}{+}x$	or F10 to boot single user mode	
Access the syst	em using command chroot /sysroot	
Execute comma	nd passwd to change the root password	
Execute the foll	lowing commands to force the system file to relabel and reboot.	

touch /.autorelabel exit logout reboot

Deploying CSPC 2.11 OVA on ESXi 7.0

To deploy CSPC 2.11 OVA on ESXi 7.0 and modify the configurations post deployment

- Step 1 Log in to the VMware vSphere Web Client and navigate to the VMs tab.
- Step 2 Add the Deploy OVF Template action button via the Actions drop-down list.
- Step 3 Click the newly added Deploy OVF Template button.
- Step 4 Click on Browse to upload CSPC ova from local path.
- Step 5 Accept end user license and select Deployment Type as Ultrasmall.
- Step 6 Click Finish, once CSPC OVA is deployed.
- Step 7 Power off VM to change ultrasmall to small, medium, or large deployment types.
- Step 8 Right click and then click Edit settings.

irtual Hardware VM Optio	ns		
📃 Add hard disk 🛛 🛤 Add ne	etwork adapter 🛛 📒 Ad	dd other device	
🕨 🖬 CPU <u>A</u>	2 ~	0	
Momonu A	2048	MB	~
	2040	200200	

You can reconfigure Vcpus, Memory, and Storage for small, medium, and large as below:

Deployment Type	Vcpus	Memory	Storage		
Small	4 Vcpus	4GB	250GB		
Medium	8 Vcpus	8GB	500GB		
Large	12 Vcpus	16GB	1TB		

Step 9 Click Save and Power on the VM.



Setting hostname as PrimaryDeviceName

- Step 1 Login into CSPC VM as collectorlogin then switch to root user
- Step 2 Change directory to /opt/cisco/ss/adminshell/applications/CSPC/resources/server/mainserver
- Step 3 Update hostNameInPrimaryDevice=true in mainserver.properties file (by default hostNameInPrimaryDevice=false)
- Step 4 Restart the CSPC service

Note: If the device is already in managed state in this case if you set the hostNameInPrimaryDevice to true in mainserver.properties file it will not set the PrimaryDeviceName as the host name. We have to unmanaged the existing managed device first to reflect PrimaryDeviceName as the host name.



Frequently Asked Questions

Q. Does adding credentials manage a device? **A.** No.

Q. Can credentials be added by DNS Name?A. No.

Q. Can CNC seed files be imported? **A.** Yes.

Q. Can Ciscoworks DCR files be imported?

A. Yes, but only the XML Version and only if the IP Addresses were exported from Ciscoworks, not the DNS Names.

Q. Does importing a credentials file ever manage a device?

A. No.

Q. Can credentials be exported?

A. Yes, in Pari credentials and CNC CSV formats.

Q. Is it better to enumerate IP address or to use wild cards?

A. It is better to use wild cards.

Q. Is the order of credentials important?

A. Yes, the order of credentials is used to choose the preferred protocol for a dataset type and also to choose between multiple matching wildcards.

Q. Does Discovery of Known Devices discover anything?

- A. No, but it will filter out any devices it cannot collect device properties from using the SNMP credentials.
- **Q.** How come all my devices weren't added?
- **A.** Because Discovery of Known Devices filters out any devices it cannot collect device properties from using the SNMP credentials.
- Q. Are SNMP credentials necessary to manage a device?
- A. Yes.
- Q. Can I select Cisco or third party vendor products where the data is collected?
- A. Yes, by default CSPC discovery engine collects all devices that are SNMP/CLI enabled, If you want a set of devices not to be collected, then add those to ignore list. Refer to Exclude Platform
- Q. Can I disable remote access for SW uploads to CSPC?
- A. Yes, you can uncheck the uploads to remote server. Refer to Export Options in Profile Details
- **Q.** I have legacy products that may be LDoS or past SW Maintenance and are sweating assets. Will CSPC still collect the data from these legacy products?
- A. Yes
- Q. I have procured third part products, will CSPC collect data from those?
- A. Yes, CSPC collects the data and those will be considered as Cisco products.

Q. Will data be collected and processed for analytics from third party products that now are Cisco?

A. Yes, below is list of PID supported for collection by CSPC. You can see the supported third party PIDs.

Physical Type	Product Family	•	PID	OS Type	¥	Name	٠
Chassis	Cisco SD-WAN		vBond	Viptela		vBond Orchestrator	
Chassis	Cisco SD-WAN		vManage	Viptela		vManage NMS	
Chassis	Cisco SD-WAN		vSmart	Viptela		vSmart Controller	
Chassis	Cisco vEdge Router		VEDGE-100-AC	Viptela		Cisco vEdge Router Model	1
Chassis	Cisco vEdge Router		VEDGE-1000-AC-K9	Viptela		Cisco vEdge Router Model	1
Chassis	Cisco vEdge Router		VEDGE-1008-AC-K9	Viptela		Cisco vEdge Router Model	1
Chassis	Cisco vEdge Router		VEDGE-100M-AT-K9	Viptela		Cisco vEdge Router Model	1
Chassis	Cisco vEdge Router		VEDGE-100M-GB-K9	Viptela		Cisco vEdge Router Model	1
Chassis	Cisco vEdge Router		VEDGE-100M-NA-K9	Viptela		Cisco vEdge Router Model	1
Chassis	Cisco vEdge Router		VEDGE-100M-NT-K9	Viptela		Cisco vEdge Router Model	1
Chassis	Cisco vEdge Router		VEDGE-100M-SP-K9	Viptela		Cisco vEdge Router Model	1
Chassis	Cisco vEdge Router		VEDGE-100M-VZ-K9	Viptela		Cisco vEdge Router Model	1
Chassis	Cisco vEdge Router		VEDGE-100WM-AT-K9	Viptela		Cisco vEdge Router Model	1
Chassis	Cisco vEdge Router		VEDGE-100WM-GB-K9	Viptela		Cisco vEdge Router Model	1
Chassis	Cisco vEdge Router		VEDGE-100WM-NA-K9	Viptela		Cisco vEdge Router Model	1
Chassis	Cisco vEdge Router		VEDGE-100WM-NT-K9	Viptela		Cisco vEdge Router Model	1
Chassis	Cisco vEdge Router		VEDGE-100WM-SP-K9	Viptela		Cisco vEdge Router Model	1
Chassis	Cisco vEdge Router		VEDGE-100WM-VZ-K9	Viptela		Cisco vEdge Router Model	1
Chassis	Cisco vEdge Router		VEDGE-2000-AC-K9	Viptela		Cisco vEdge Router Model	1
Chassis	Cisco vEdge Router		VEDGE-CLOUD	Viptela		VEDGE-CLOUD	

Figure J-1 Third Party PIDs