User Guide for CSPC Collection Platform Software

Version 2.8.1
January, 2019

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.
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

CHAPTER  7 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

Chapter 8 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
Contents

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
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
    Export Log Files  9-17
## Contents

Statement 14-2  
Condition Statement 14-3  
Loop Statement 14-4  

Examples 14-5  
CLI Complex Collection 14-5  
SNMP Complex Collection 14-6  

### APPENDIX 15  
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 XML 15-15  
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 Frequently Asked Questions 19-1
CSPC Flow Chart

1. Start
   2. Login to CSPC
   3. Add Device Credentials
   4. Discover Devices
   5. Import Seed File
   6. Run DAV
   7. Import Rules
   8. View Managed Devices

   - Is Seed File Imported: Yes
   - CNC V1/V2 & RME Seed File Format
   - Auto Discovery Devices
   - Is ICMP Ping Enabled: Yes
   - Device Discarded
   - Add SNMP RO credential to device
   - Repot as SMNP Unreachable: No
   - Is CLI discovery Enabled: Yes
   - Is SMNP config push Enabled: Yes
   - CLI Access Only
Introduction

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 2.8. Refer to CSPC Release Notes for program updates, important notes, image location and other information.

CSPC 2.6.x 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 the 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 < 2.6 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

<table>
<thead>
<tr>
<th>EOL Date</th>
<th>EOL Version</th>
<th>EoSWM Date</th>
<th>LDoS Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dec, 2012</td>
<td>CSPC 2.0.3</td>
<td>Jan, 2013</td>
<td>Apr, 2013</td>
</tr>
<tr>
<td>April, 2014</td>
<td>CSPC 2.2</td>
<td>May, 2014</td>
<td>Aug, 2014</td>
</tr>
<tr>
<td>March 20, 2017</td>
<td>CSPC 2.5</td>
<td>April 20, 2017</td>
<td>July 20, 2017</td>
</tr>
<tr>
<td>May 9, 2018</td>
<td>CSPC 2.6</td>
<td>June 9, 2018</td>
<td>Oct 10, 2018</td>
</tr>
</tbody>
</table>
Accessing the CSPC Collector

CSPC 2.8 is a web based application and can be accessed by using a URL.

Note

The recommended browsers are Microsoft Internet Explorer 9.0 to 11.0 and Mozilla Firefox 27 to 49.

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

Note

- <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.
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).
  • Contain at least one special character (for example: !$%^&*()_+-="{}\|;:'<>?,/).
  • In CLI Prefix all these characters (! $ & ( ) | \ ; ' ? ) 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, £, Å, ë, Æ, Ñ, ć, ß)

• 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

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS Server</td>
<td>IP Address of DNS Server</td>
</tr>
<tr>
<td>NTP Server</td>
<td>IP Address of NTP Server</td>
</tr>
<tr>
<td>Timezone</td>
<td>Time zone of the collector</td>
</tr>
<tr>
<td>Set Time</td>
<td>Sets the appliance time, and time should match the actual time of the selected time zone</td>
</tr>
<tr>
<td>Host Name</td>
<td>Name of the host</td>
</tr>
</tbody>
</table>
### 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.

**Figure 2-6 Install CSPC**

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

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

**Note**
- 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.
- 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

OR

- To restore the backup select **Restore the registration and the data from backed up file.**
Step 8  You can add device using one of following and click Add Device:

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

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

- If you select SNMPV3 enter Credential Name, User Name, Engine ID, Auth Algorithm, Password, Privacy Algorithm, Password. Use > to select credential.
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.
After logging in to the CSPC Collector, Dashboard screen is displayed.
Note  If the session is idle for 15 minutes or more, the user is logged out of the application.

Go back to CSPC Flow Chart
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.

*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.
Figure 2-18  OTP Generation

Verify either security answers or One Time Password and set new password

Reset Option

Reset By:  
- Security Questions  
- One Time Passcode

One Time Passcode

Note: Mail settings must be configured inorder to use this feature

OTP Status:  
- Generate  
- I have OTP

Generate One Time Passcode

Please specify new password

* New Password:

Enter the characters you see in the below image.

* These characters are case sensitive.

OK  Cancel

Figure 2-19  OTP Input

Verify either security answers or One Time Password and set new password

Reset Option

Reset By:  
- Security Questions  
- One Time Passcode

One Time Passcode

Note: Mail settings must be configured inorder to use this feature

OTP Status:  
- Generate  
- I have OTP

* Enter OTP:

Please specify new password

* New Password:

Enter the characters you see in the below image.

* These characters are case sensitive.

OK  Cancel
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.

![View Server Version Table]

*Note*

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 provide 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.
Appliance configuration tab helps you in modifying and configure OS related configurations that was done during installation wizard also see Figure 2-6.
To Change the password click **Change Password/setting** form drop down on top right of dashboard. Change all the required fields and click **OK**.

*Figure 3-3   Appliance configuration*

[Diagram of Appliance configuration settings]

Use the below options to configure your Appliance.

- **DNS Server/Hostname:** Enter DNS server name
- **Timezone:** Select timezone
- **Set Time (24 Hour Format):** Enter NTP server IP
- **Hostname:** Enter hostname

* Proxy Server

* Denotes Mandatory Fields
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.
Figure 3-5  Managed Device Tree

Managed Devices (60 out of 60)
- LiveNodes (56)
- Unreachable Nodes (2)
- Hubs
- Servers-UnifiedComputing (3)
- ServiceExchange (1)
- xDSL
- GenericNetworkDevices (3)
- Routers (12)
- Switches
- ATMSwitches
- BladeSwitches
- ConnectedGridSwitches
- DataCenterSwitches (2)
- IndustrialEthernetSwitches

Non Managed Devices (0 out of 60)
If you right click on any device, a menu as shown in Figure 3-6 is displayed.

![Managed Devices Menu](image)

Menu option shows the following options:

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

Figure 3-7  Device Properties

View Latest Collection Details

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.
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.
CSPC Workflow

This is a powerful features 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 can access credential using SNMP V1/V2, V3, Telnet, or SSH and collect now or schedule it later.

To start the workflow follow the steps below:

**Step 1**  
Click Workflow from menu bar.

![Workflow Menu](Image)

**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.

![Discovery By IP Address](Image)

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

- If you select SNMPV3 enter Credential Name, User Name, Engine ID, Auth Algorithm, Password, Privacy Algorithm, Password. Use > to select credential.
Figure 4-5    SNMPV3

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

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.
**Figure 4-7  Collect Now**

The figure shows the interface for collecting data immediately or scheduling a collection. The interface includes options for specifying the collection time and recurrence pattern. The user can select whether to start the collection now or schedule it for a later date.

**Figure 4-8  Schedule Collection**

The figure displays the interface for scheduling a collection. Similar to Figure 4-7, this interface allows the user to select a start date and time, as well as a recurrence pattern for the collection.
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.

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.
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.

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

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

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 devices during Discovery.

**Figure 6-3 Import Option**
Note

Default mapping and Map Devices to options is available to NOS services

Follow the steps given below to import a seed file:

**Step 1** In the Device Credentials Configuration window, click **Import** button

**Step 2** From 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)

**Step 3** Click Browse button and select the seed file that you want to import

**Step 4** Enter the job name, job description and seed file description in the respective fields

**Note** Step 5 and 6 are applicable only if you select CNC or CSV file format.

**Step 5** Choose **Default Mapping** or **Map Devices To**. If **Map Devices To** is selected, then select the entitlement from drop down

**Step 6** Choose **Create Groups By User Fields** or/and **Add device Add devices to user defined groups**. Select and enter **New Device Group Name** or **Select Existing Device Group** from the drop down.

**Note** Job Name is a mandatory field.

**Step 7** Click **OK** button. Seed file is imported.

**Export**

Export option is provided to export the existing credentials.

**Figure 6-4 Export Options**

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 device in seed file imported by the you are consider 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.csv

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 Minutley, Daily, Weekly, Monthly, or Yearly as shown in Figure 6-5.
Step 6 Enter the device group name in Device Group Name field

Step 7 Or click Select Device Group Name radio button and select the device group name from the drop down box

Step 8 Click **OK** button

Go back to CSPC Flow Chart

Adding Credentials

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

**Note** 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 TL1 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.

**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**.
Figure 6-8  Module Credentials

Follow the steps given below to add the module credentials:

**Step 1** Enter the following information for creating a new Credential:
- 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 the module or not)
- Authentication (depending on the protocol selected use the following authentication mechanisms:
  - 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 and are 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

Figure 6-9  Seed File Configuration

To import the seed file perform the 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.
Chapter 6      Applications - Device Management

Device Management

Figure 6-10   Configure Schedule

Step 4  Check the required operation. click **OK**

Figure 6-11   Operations

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

**Imported Seed file**

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.
**Figure 6-12** Imported Seed file

<table>
<thead>
<tr>
<th>Seed File Name</th>
<th>Seed File Description</th>
<th>Seed File Format</th>
<th>Group Name</th>
<th>File Size (KB)</th>
<th>User Name</th>
<th>Job Start Time</th>
<th>Job End Time</th>
<th>Job Log Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>dsc.csv</td>
<td></td>
<td>Cisco</td>
<td>NewGrp</td>
<td>7.93</td>
<td>csuser</td>
<td>Thu, Mar 14, 2...</td>
<td>Thu, Mar 14, 2...</td>
<td>View Job Log Details</td>
</tr>
<tr>
<td>nresedTest1.csv</td>
<td>CW Import</td>
<td>Cisco</td>
<td></td>
<td>6.94</td>
<td>csuser</td>
<td>Thu, Mar 14, 2...</td>
<td>Thu, Mar 14, 2...</td>
<td>View Job Log Details</td>
</tr>
<tr>
<td>C1C_26.csv</td>
<td></td>
<td>Cisco</td>
<td></td>
<td>6.04</td>
<td>csuser</td>
<td>Thu, Mar 14, 2...</td>
<td>Thu, Mar 14, 2...</td>
<td>View Job Log Details</td>
</tr>
<tr>
<td>a2k_sheer_v1.1</td>
<td></td>
<td>Cisco</td>
<td></td>
<td>2690.58</td>
<td>csuser</td>
<td>Thu, Mar 14, 2...</td>
<td>Thu, Mar 14, 2...</td>
<td>View Job Log Details</td>
</tr>
<tr>
<td>_e9008_8024_</td>
<td></td>
<td>Cisco</td>
<td>TestGrp</td>
<td>2.2</td>
<td>csuser</td>
<td>Thu, Mar 14, 2...</td>
<td>Thu, Mar 14, 2...</td>
<td>View Job Log Details</td>
</tr>
</tbody>
</table>
**Do Not Manage Device List**

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**

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 criteria and all devices that match the criteria (either currently managed or not) will automatically appear in this group.

![Figure 6-14 Device Groups Main Window](image)

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

![Figure 6-15 Add Device Group](image)

Creation of static group is defined below.
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.
Once you define the group name and description you are ready to define the Group Rules, as shown below.

Define the conditions or rules that must be matched or not matched based on the attributes and values. Add these conditions by clicking Add.
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, UserField2, or UserField3 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.

Table 6-1 Special Cases in Group Rule

<table>
<thead>
<tr>
<th>Special Cases</th>
<th>Figures</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you select <strong>Device OS Name</strong> as <strong>AttributeName</strong>, then you need to select the value from the drop down</td>
<td><img src="image1.png" alt="Group Rule Details" /></td>
</tr>
<tr>
<td>If you select <strong>Device Ip Address</strong> as <strong>AttributeName</strong> and <strong>Operator</strong> as does not belong to the range, then you need to enter <strong>Start Ip Address</strong> and <strong>End Ip Address</strong></td>
<td><img src="image2.png" alt="Group Rule Details" /></td>
</tr>
</tbody>
</table>
Special Cases

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.

If you select **Inventory Status or Config Status** as Attribute Name and **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.

---

### 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
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.

![General Settings](image)

**Table 6-2 General Settings**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start IP</td>
<td>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</td>
</tr>
<tr>
<td>Start IPv6</td>
<td>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</td>
</tr>
<tr>
<td>Start Hostname</td>
<td>Prefix used for masking hostnames</td>
</tr>
<tr>
<td>Global Display Type</td>
<td>Device attribute to be shown for distinct devices</td>
</tr>
<tr>
<td>Platform List</td>
<td>List of platforms for Telnet echo is enabled.</td>
</tr>
<tr>
<td>SysObject ID List</td>
<td>SystemObject ID for the Telnet echo enabled devices</td>
</tr>
<tr>
<td>Total User Session Count</td>
<td>Maximum number of unique CSPC user sessions</td>
</tr>
</tbody>
</table>
## Prompt Settings:

*Figure 6-21* Prompt Settings

![Prompt Settings Diagram](image)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prompts</td>
<td></td>
</tr>
<tr>
<td>Login Prompts</td>
<td>Used for extra Login prompts that needs to be handled by CSPC</td>
</tr>
<tr>
<td>Password Prompts</td>
<td>Used for extra Password prompts that needs to be handled by CSPC</td>
</tr>
<tr>
<td>Other Prompts</td>
<td>Used for other prompts that needs to be handled by CSPC</td>
</tr>
<tr>
<td>CLI Error Prompts</td>
<td>Used for extra CLI error prompts that needs to be handled by CSPC</td>
</tr>
<tr>
<td>SNMP Error Prompts</td>
<td>Used for extra SNMP error prompts that needs to be handled by CSPC</td>
</tr>
<tr>
<td>SOAP Error Prompts</td>
<td>Used for extra SOAP error prompts that needs to be handled by CSPC</td>
</tr>
<tr>
<td>SNMP Trap Settings</td>
<td></td>
</tr>
<tr>
<td>Retain Traps for</td>
<td>Mention the number of days to retain traps.</td>
</tr>
<tr>
<td>Port Number</td>
<td>Configure the port to receive the SNMP trap messages. Default port is 162.</td>
</tr>
</tbody>
</table>

**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.
Submode and Init Settings:

### Table 6-4 Submode and Init Settings

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS Type</td>
<td>Type of OS</td>
</tr>
<tr>
<td>IP Address List</td>
<td>List of IP addresses</td>
</tr>
<tr>
<td>SH Version Command</td>
<td>If show version needs to be executed while in submode</td>
</tr>
<tr>
<td>SH Version Lines</td>
<td>Number of lines in show version that needs to be taken</td>
</tr>
<tr>
<td>SH Version Ignore Strings</td>
<td>Whether to consider or ignore show version settings</td>
</tr>
<tr>
<td>Execute New Line for Submode Login Prompt</td>
<td>Whether new line has to be executed at the end of submode login prompt</td>
</tr>
</tbody>
</table>
### Export Settings:

**Figure 6-23 Export Settings**

![Export Settings](image)

**Table 6-5 Export Settings**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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 (secs) | Response counter for TailEnd is maximum wait time for entitlement registration and limit is 90 seconds  
| TailEnd SeedFile Counter (secs) | 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 |
Device Management

Note

- 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

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSPC Identity</td>
<td>Select the valid CSPC certificate</td>
</tr>
<tr>
<td>Test Upload button</td>
<td>Check the connectivity using a certificate</td>
</tr>
</tbody>
</table>
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

Table 6-6  Discovery Timeout

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMP Timeout (in sec)</td>
<td>SNMP connection timeout value in seconds. Default value is 3 seconds</td>
</tr>
<tr>
<td>SNMP Retry</td>
<td>SNMP connection retry count. Default value is 1</td>
</tr>
<tr>
<td>Max Thread Count</td>
<td>Thread pool size for each discovery job. Default value is 100.</td>
</tr>
<tr>
<td>Max Credential Sets For Protocol</td>
<td>Maximum number of Credential Sets to use for each protocol. Default value is 10.</td>
</tr>
<tr>
<td>Max Discovery Time (in sec)</td>
<td>Maximum discovery time in seconds per device. Default value is 600 seconds. Valid values 0 or &gt;= 60. Zero no window time will be enforced. If value is set between 0 and 60, default value 600 will be used.</td>
</tr>
<tr>
<td>Max Device Discovery</td>
<td>Maximum discovery time in seconds for a single device. Default value is 180 seconds. Valid values: 5 seconds and above. If value is &lt; 5, then 5 is enforced.</td>
</tr>
</tbody>
</table>
Include Platform (optional):
Any platform that is specified in include platform list, only those specific platform devices will be discovered and all other devices will be discarded.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Phone Discovery</td>
<td>Option to enable/disable IP Phone discovery.</td>
</tr>
<tr>
<td>Serial Number Duplicate Check</td>
<td>Checks for the duplicate serials numbers. If not enabled, then serial number will not be polled for the device.</td>
</tr>
<tr>
<td>Mac Address Duplicate Check</td>
<td>Checks for the duplicate MAC Address.</td>
</tr>
<tr>
<td>Exclude Non-Cisco Device</td>
<td>If enabled excludes all the non-cisco devices from discovery.</td>
</tr>
<tr>
<td>NMAP Timeout (in sec)</td>
<td>Timeout value in seconds to discovery device using Nmap application. Default value is 30 seconds. Valid values &gt; 0. If value is &lt; 0, then default is enforced.</td>
</tr>
<tr>
<td>Ping ICMP before Discovery</td>
<td>Option is to enable/disable. If enabled pings the device before Discovery.</td>
</tr>
<tr>
<td>Enable Fallback</td>
<td>If discovery of selected protocols fails, and if fall back is selected discovery is tried for other protocols as per discovery properties file.</td>
</tr>
<tr>
<td></td>
<td>$CSPCHOME/resources/discovery/properties/discovery-cso-startup.properties</td>
</tr>
<tr>
<td></td>
<td>For properties name: PRIMARY_COMM_PROTOCOL</td>
</tr>
<tr>
<td></td>
<td>This is applicable only for known discovery and rediscovery.</td>
</tr>
<tr>
<td>Enable SNMP Config Push</td>
<td>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.</td>
</tr>
<tr>
<td>CLI Timeout</td>
<td>CLI connection timeout value in seconds. Default value is 3 seconds.</td>
</tr>
<tr>
<td>HTTP Timeout</td>
<td>HTTP connection timeout value in seconds. Default value is 4 seconds.</td>
</tr>
</tbody>
</table>
Figure 6-26  Include Platform

![Include Platform Image]

- IOS_10000
- IOS_12000
- IOS_4000
- IOS_7200
- IOS_7300
- IOS_7500
- IOS_8500
- IOS_asc5300
- IOS_Cat
- IOS_cata3700
- IOS_LS1010
- IOS_VSS
- IOS_XE
- IOS_XR
- IDS
- MIB_IT
- NME_NAM
- NXOS

[Include Platform Options]
Exclude Platform (optional):
Any platform is specified in exclude platform list, all devices belonging to that platform will be ignored.

Figure 6-27   Exclude Platform

Access Verification Settings

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 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 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 unmanged devices.
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.
**Figure 6-29  Inventory Settings**

![Inventory Settings](image)

**Note**

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.
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 10 seconds.
- **Retry Count:** You can select the “retry” count as well

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
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**

![Device Prompts Tab](image)

Both *Order* and *Regular Expression* are explained below.
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.

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.
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.

![Device Protocol Rules](image)

Figure 6-35 **Device Protocol Rules**

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.
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.
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.

**Figure 6-37 Disable Collection Rules**

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.

**Figure 6-38 Disable Collection Rule Details**
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 a new job trigger preferences by selecting **Add** button in the Advanced Job Settings window.

*Figure 6-39 Advanced Job Settings*
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.

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.
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 MultiService 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.

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**

*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.
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.
This provides an options 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 the *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.
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.

*Figure 6-46 Advanced Collection Profile Options*

*Advanced Collection Profile Options* window shows the available, SNMP, CLI and HTTP protocols. You can selected the desired protocol from the list and add it by clicking arrow or select all by clicking on 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.
Click **OK** button to save the selection.

Go back to **CSPC Flow Chart**

**Manage MultiService 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.
In collection profile dialog box, select the collection profile using arrows.

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.
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.

**Note**
Default upload profiles are created for NOS service when a nos configurer gets installed. Below screen is only for NOS.
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 file and click **Submit** button to start uploading the file.
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 an 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 NonManaged 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 from 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.

**Figure 6-53  Upload Warning Message**

<table>
<thead>
<tr>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lowering the upload frequency (not recommended) may result in performance degradation and high bandwidth consumption. Data will be uploaded only if data is changed from the last successful upload.</td>
</tr>
</tbody>
</table>

**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 required files.

**Manage Datasets**

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).

**Figure 6-54  Manage Datasets**

<table>
<thead>
<tr>
<th>Dataset Name</th>
<th>Type</th>
<th>Collection Type</th>
<th>Lock Status</th>
<th>Applicable Platforms</th>
<th>Category</th>
<th>Created By</th>
</tr>
</thead>
<tbody>
<tr>
<td>PhysicalPort_Configured</td>
<td>Dynamic</td>
<td>SNMP</td>
<td>Unlocked</td>
<td>PhysicalPort</td>
<td>admin</td>
<td></td>
</tr>
<tr>
<td>PhysicalPort_Access</td>
<td>Dynamic</td>
<td>SNMP</td>
<td>Unlocked</td>
<td>PhysicalPort</td>
<td>system</td>
<td></td>
</tr>
<tr>
<td>PhysicalPort_Interfaces</td>
<td>Dynamic</td>
<td>SNMP</td>
<td>Unlocked</td>
<td>PhysicalPort</td>
<td>admin</td>
<td></td>
</tr>
<tr>
<td>PhysicalPort_Index</td>
<td>Dynamic</td>
<td>SNMP</td>
<td>Unlocked</td>
<td>PhysicalPort</td>
<td>admin</td>
<td></td>
</tr>
<tr>
<td>PhysicalPort_Name</td>
<td>Dynamic</td>
<td>SNMP</td>
<td>Unlocked</td>
<td>PhysicalPort</td>
<td>admin</td>
<td></td>
</tr>
<tr>
<td>PhysicalPort_Devices</td>
<td>Dynamic</td>
<td>SNMP</td>
<td>Unlocked</td>
<td>PhysicalPort</td>
<td>admin</td>
<td></td>
</tr>
<tr>
<td>show_coredump</td>
<td>Static</td>
<td>CLI</td>
<td>Unlocked</td>
<td>[ Custom ]</td>
<td>Submodule</td>
<td>system</td>
</tr>
<tr>
<td>show_coredump_run</td>
<td>Static</td>
<td>CLI</td>
<td>Unlocked</td>
<td>[ Custom ]</td>
<td>Submodule</td>
<td>system</td>
</tr>
<tr>
<td>show_coredump_run_dyn</td>
<td>Dynamic</td>
<td>CLI</td>
<td>Unlocked</td>
<td>Submodule</td>
<td>system</td>
<td></td>
</tr>
<tr>
<td>show_coredump_start</td>
<td>Static</td>
<td>CLI</td>
<td>Unlocked</td>
<td>Submodule</td>
<td>system</td>
<td></td>
</tr>
<tr>
<td>show_coredump_start_dyn</td>
<td>Dynamic</td>
<td>CLI</td>
<td>Unlocked</td>
<td>Submodule</td>
<td>system</td>
<td></td>
</tr>
<tr>
<td>show_dev_entry</td>
<td>Static</td>
<td>CLI</td>
<td>Unlocked</td>
<td>[ Custom ]</td>
<td>Submodule</td>
<td>system</td>
</tr>
<tr>
<td>show_dev_entry_run</td>
<td>Static</td>
<td>CLI</td>
<td>Unlocked</td>
<td>[ Custom ]</td>
<td>Submodule</td>
<td>system</td>
</tr>
<tr>
<td>show_dev_entry_run_dyn</td>
<td>Dynamic</td>
<td>CLI</td>
<td>Unlocked</td>
<td>Submodule</td>
<td>system</td>
<td></td>
</tr>
<tr>
<td>show_dev_start</td>
<td>Static</td>
<td>CLI</td>
<td>Unlocked</td>
<td>Submodule</td>
<td>admin</td>
<td></td>
</tr>
<tr>
<td>show_dev_start_dyn</td>
<td>Dynamic</td>
<td>CLI</td>
<td>Unlocked</td>
<td>Submodule</td>
<td>admin</td>
<td></td>
</tr>
<tr>
<td>show_dev_port</td>
<td>Static</td>
<td>CLI</td>
<td>Unlocked</td>
<td>Submodule</td>
<td>admin</td>
<td></td>
</tr>
<tr>
<td>show_dev_port_run</td>
<td>Static</td>
<td>CLI</td>
<td>Unlocked</td>
<td>Submodule</td>
<td>admin</td>
<td></td>
</tr>
<tr>
<td>show_dev_port_run_dyn</td>
<td>Dynamic</td>
<td>CLI</td>
<td>Unlocked</td>
<td>Submodule</td>
<td>admin</td>
<td></td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Provide data set details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Provide data set platforms</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click <strong>OK</strong></td>
</tr>
</tbody>
</table>

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

![Add Dataset Figure](image)

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:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Provide the following dataset details:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Title</strong>: Name of the Dataset. This is a mandatory field</td>
<td></td>
</tr>
<tr>
<td><strong>Identifier</strong>: This can be user defined. If this is not defined by user, this will be generated by System</td>
<td></td>
</tr>
<tr>
<td><strong>Category</strong>: 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</td>
<td></td>
</tr>
<tr>
<td><strong>Collection Interval</strong>: You can specify the collection intervals in milliseconds</td>
<td></td>
</tr>
<tr>
<td><strong>Tag</strong>: Select the tag from the drop down list</td>
<td></td>
</tr>
<tr>
<td><strong>Description</strong>: Description for the Dataset</td>
<td></td>
</tr>
</tbody>
</table>
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
- LDAP
CLI:

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

**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)**
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.

**Figure 6-59  Dataset Platforms Options (select SNMP)**

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.
Once the selection is finished, click **OK**.
SNMP variables are added to your new data set as shown below.
SOAP XML Request:
Select SOAP XML Request option from Dataset Type and click Add button.

Figure 6-62  Dataset Platforms (select SOAP XML Requests)

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 XML
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)

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

Figure 6-65 Config Retrieval using SNMP Details
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)

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 Masking Rule. Once all the data is entered you are ready to add a new FILE dataset.

Figure 6-67 Dataset Entry Details - FILE
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 6-68**  Dataset Platforms (Select XML)

![Dataset Platforms (Select XML)](image)

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

![Data Entry Details - XML](image)
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.

*Figure 6-70  Dataset Platforms (Select WMI)*

Enter the details for WMI selection. Once all the data is entered you are ready to add a new WMI dataset.
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.
Figure 6-72  Dataset Platforms (Select HTTP)
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)*
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)

**Figure 6-75**  
Dataset Entry Details
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)

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.

Go back to CSPC Flow Chart
Chapter 6  Applications - Device Management

Device Management

Figure 6-78  LDAP

Figure 6-79  Data Entry Details

Table 6-7  LDAP Parameters

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search Base</td>
<td>The base for the search. It must be a valid distinguished name and it is mandatory otherwise a validation error is thrown.</td>
</tr>
<tr>
<td>Search Filter</td>
<td>The filter to use for this search and it is mandatory filed. For an invalid search filter an validation error is thrown.</td>
</tr>
</tbody>
</table>
### Device Management

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search Scope</td>
<td>The search scope is OBJECT, ONELEVEL, or SUBTREE and it is a mandatory field.</td>
</tr>
<tr>
<td>Attributes to Return</td>
<td>The attributes to use for this search and it is optional. If nothing is provided, then it fetches all available attributes.</td>
</tr>
</tbody>
</table>
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

**Figure 6-80 Add Dataset**

**Step 3** Select Create Dynamic Dataset and click OK

**Step 4** In Dataset Definition box, specify the dynamic dataset XML

XML file uses the Pari API XML Schema

**Step 5** Click OK

Dynamic Dataset is created and added to Manage Datasets.
Figure 6-81  Create Dynamic Datasets

![Dynamic Dataset Editor - Create a new Dataset](image)

```xml
<Dataset identifier="show_module_version">
  <Type>
    <Title>show module version</Title>
    <CollectionType>CSPC</CollectionType>
    <Category>Device</Category>
  </Type>
  <Statement>
    <Loop identifier="show_module_1">"
    <Values>
      <Value>
        <DeviceStatus Failure="error_message">show module</DeviceStatus>
      </Value>
    </Values>
  </Statement>
</Dataset>
```

**Messages - Log**

```
```

[Help | OK | Cancel | Validate XML]
Manage Platform Definitions

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:

**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
Device Management

Figure 6-83  Add Platform Conditions

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.

Figure 6-84  Platform Conditions

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

**Figure 6-85  Test Platform Definitions**

![Test Platform Definitions](image1)

**Figure 6-86  Test Customer Platform Definition**

![Test Customer Platform Definition](image2)
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**.
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:

**Figure 6-89  Create a New Data Integrity Rule**

- **Step 1** Click **Add Data Integrity Rules**.
- **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.
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.

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
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**

![Create New Data Masking Rule](image)

**Step 1**  Click Add Masking Rules button

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

**Step 3**  Once the base data is entered, enter the rule patterns that make up this rule as shown below
Step 4  Click **Add** to start adding the conditions.

**Figure 6-94  Rule Pattern Conditions**

- **Expression:** `^[]*username+[)$`
- **Replacement:** `######`

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**
Chapter 6      Applications - Device Management

Device Management

Manage Syslog Source Files

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

Note

This feature is only for NOS services

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

**Figure 6-98 Add Input Filter Details**

- **Source Device:** 10.1.1.1
- **Minimum Severity:** 0 (emergency)
- **Maximum Severity:** 3 (error)
- **Component Name:** SYSLOG
- **Mnemonic Text:** CPUHOG
- **Description:**

  **Action to be taken**
  - **Action:** Accept
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

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 DSIRT Files

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

In Manage Application Discovery profiles you can add or edit a 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.

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.
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.
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.

**Note**

This feature is only for NCCM services

---

**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.

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.
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.

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.
Figure 6-109 Profile Details

Table 6-8 Jump Server Parameters

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host name</td>
<td>Name defined to server</td>
</tr>
<tr>
<td>User Name</td>
<td>Login username</td>
</tr>
<tr>
<td>Password</td>
<td>Login Password</td>
</tr>
<tr>
<td>Number of Connections</td>
<td>No of connections to jump server.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Select the protocol to be used</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the server</td>
</tr>
<tr>
<td>Test Connection</td>
<td>To check the jump server credentials</td>
</tr>
</tbody>
</table>

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.
CSPC Collection Platform Software User Guide

Chapter 6    Applications - Device Management

Device Management

Figure 6-110    Select Devices

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.

Figure 6-111    Credential Lock Settings

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**

<table>
<thead>
<tr>
<th>Name</th>
<th>Status</th>
<th>Created By</th>
<th>Created Time</th>
<th>Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>3nov-1017</td>
<td>OPEN</td>
<td>admin</td>
<td>2015 11 02 21:30:27</td>
<td>NOS</td>
</tr>
<tr>
<td>test1016:3nov</td>
<td>OPEN</td>
<td>admin</td>
<td>2015 11 03 21:35:37</td>
<td>NOS</td>
</tr>
<tr>
<td>3nov-1026-1</td>
<td>OPEN</td>
<td>admin</td>
<td>2015 11 03 21:45:32</td>
<td>NOS</td>
</tr>
<tr>
<td>5Nov-1031</td>
<td>OPEN</td>
<td>admin</td>
<td>2015 11 03 21:50:13</td>
<td>NOS</td>
</tr>
<tr>
<td>3nov-1004</td>
<td>OPEN</td>
<td>admin</td>
<td>2015 11 03 21:59:58</td>
<td>NOS</td>
</tr>
<tr>
<td>3nov-1040</td>
<td>OPEN</td>
<td>admin</td>
<td>2015 11 03 22:09:40</td>
<td>NOS</td>
</tr>
<tr>
<td>3nov-1059</td>
<td>OPEN</td>
<td>admin</td>
<td>2015 11 03 22:10:18</td>
<td>NOS</td>
</tr>
<tr>
<td>Default_WorkFlow</td>
<td>OPEN</td>
<td>admin</td>
<td>2015 11 03 22:14:40</td>
<td>NOS</td>
</tr>
<tr>
<td>2nov1</td>
<td>OPEN</td>
<td>admin</td>
<td>2015 11 02 16:00:59</td>
<td>NOS</td>
</tr>
<tr>
<td>4nov1</td>
<td>OPEN</td>
<td>admin</td>
<td>2015 11 04 09:52:24</td>
<td>NOS</td>
</tr>
<tr>
<td>5Nov447</td>
<td>OPEN</td>
<td>admin</td>
<td>2015 11 03 16:08:32</td>
<td>NOS</td>
</tr>
</tbody>
</table>
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.

Note

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.

Figure 7-1 Rediscovery
Figure 7-2  Known IP

Known IP/Seed File Discovery

For Seed file Protocol are SNMPv3, SNMPv2c, and SNMPv1

Protocol Selection

List of known IP address

Discover Devices using each or next selected protocol

Is Discovery Successful

Yes

No

Is Last Management Protocol

Yes

No

Select the next fallback Protocol

Yes

No

Add to Managed reachable group

Is SNMP

Yes

No

Is CLI

Yes

No

Is HTTP

Yes

No

CLI Access Only

Is SNMP Configuration enabled in Discovery Settings

Add SNMP RO credential to device

Report as Managed Unreachable incomplete (user can fix credentials/ increase the timeout and try discovery again)
Figure 7-3 Range Discovery

Range Discovery

Range of IP addresses

Is Ping Enabled in Discovery Settings

Yes

Try ICMP Ping on every device in the range before SNMP Discovery

No

Add to SNMP Reachable - Managed

Discovery Successful

SNMP Discovery (MIBz, Entity, Interface & additional MIBs)

No response to SNMP

SNMP Incomplete - Non Managed

Report as ICMP Pingable - Non Managed

(User can fix SNMP credentials/Increase SNMP timeout and Try discovery again)

SNMP Reachable - Managed

ICMP Pingable - Non Managed

SNMP Incomplete - Non Managed

Device discarded & User will not see this device in CSCP

Incomplete Discovery (All mandatory MIBs not collected in the stipulated period)

Report as SNMP Incomplete - Non Managed

(User can increase the SNMP Timeout and Try discovery again)
Figure 7-4  Seed IP and Protocol Based Discovery

Seed IP & Protocol based Discovery

Seed IP address/Host Name along with protocols such as CDP, ARP, RT, OSPF, BGP, LLDP & HSRP

Is Ping Enabled in Discovery Settings

Try ICMP Ping on Seed IP/Host Name/Neighbor device

Device discarded & User will not see this device in CSPC

Is Ping Successful

Add to SNMP Reachable - Managed

SNMP Discovery (MIBs, Entity, Interface & additional MIBs)

No response to SNMP

Gets the neighboring devices based on the selected protocol (CDP, ARP, RT, OSPF, BGP, LLDP & HSRP), Then for each neighbor device, do ping & discovery.

SNMP Reachable - Managed

ICMP Pingable - Non Managed

SNMP Incomplete - Non Managed

Report as SNMP Incomplete - Non Managed (User can increase the SNMP Timeout and Try discovery again)

Incomplete Discovery (All mandatory MIBs not collected in the stipulated period)

Discovery Successful

C

Report as ICMP Pingable - Non Managed (User can fix SNMP credentials/Increase SNMP timeout and Try discovery again)
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.

**Note**

If multiple discovery types are selected then first selected SNMP version protocol will be used for range and protocol based discovery.
Figure 7-6  Discover Devices using Known IP Addresses

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

CSPC uses Nmap (Network Mapper) based discovery when device is not reachable through SNMP protocol because of incorrect SNMP credentials or device does not support SNMP protocol. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services those hosts are offering, what operating systems (and OS versions) they are running and many other characteristics.

Nmap Discovery can be enabled when you are scheduling discovery to discover devices using one of the discovery options like CDP, OSPF, ARP or using IP address range(s). When you select Nmap check box in Discovery Schedule Options screen, NMAP discovery is performed on each of the IP address discovered using the specified discovery protocol or on each of the IP address within the specified address range.

Select Enable NMAP discovery option, in case you want to discover any Non-SNMP devices (devices on which SNMP agent is not running). Any Non-SNMP devices discovered can be viewed under “Non-SNMP devices” report. Enabling NMAP Discovery in turn activates Manage Devices checkbox. If you require to manage non SNMP devices, then choose Manage Devices.

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.
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)
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 \textit{IP Address/subnet mask (x.x.x.x/x)} and the End IP will be auto populated. You have select CIDR Address before providing Start IP Address.

Figure 7-8 \textit{Protocol Based Discovery}

Figure 7-9 \textit{IP Scanning}
Management Tasks

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.

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**.
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 job and selecting 'Create new discovery by cloning this job'.

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.

**Figure 7-13 Unmanage Devices**

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

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

*Figure 7-14    Device Access Verification - Device 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**.
You can click on Advanced Options button and select the credentials to run DAV on as shown in Figure 7-17.

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.

**Figure 7-18  Device Access Verification - Results**

Go back to CSPC Flow Chart
Device Prompt Collection

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*
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 Minute, Daily, Weekly, Monthly, or Yearly as shown in Figure 7-21.
Once the job is started you can view the successful and failed collection for a given device as shown in Figure 7-22.

Figure 7-21 Configure Schedule

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

Once you start the job, the results are displayed including device name, IP address, and success or failure, as shown below.
Figure 7-24  Executed Data Collection Profile Results

<table>
<thead>
<tr>
<th>No</th>
<th>IP Address</th>
<th>Host Name</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>15.10.1.2</td>
<td>D15</td>
<td>Invented 15.10.1.2</td>
</tr>
<tr>
<td>2</td>
<td>16.10.1.1</td>
<td>L16</td>
<td>Invented 16.10.1.1</td>
</tr>
<tr>
<td>3</td>
<td>15.10.1.1</td>
<td>L15</td>
<td>Invented 15.10.1.1</td>
</tr>
</tbody>
</table>
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

*Figure 7-25  Run Upload Profile*

Job Progress screen showing the status of the uploaded profile is displayed as shown in *Figure 7-26.*
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
Adhoc 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 Adhoc collection profile serves this purpose.

When you create adhoc collection profile, select:

- A base collection profile
- Device details
- Scheduling information

Adhoc 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 Adhoc Data Collection Profiles”, screen as shown in Figure 7-27 is displayed.

Figure 7-27 Adhoc Collection Select Devices

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  Adhoc Collection Profile Details**

![Add Adhoc Collection Profile](image)

**Note**
If configure schedule is not provided, then adhoc 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 needs 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 adhoc collection at a specified time and can be repeated at certain intervals by giving the required details.
Click **OK** to save the Profile and device details to the adhoc collection profile. On successful completion, you will receive a message as shown in Figure 7-30.

**Figure 7-30**  **Confirmation Message**

![Confirmation Message](image)

The adhoc collection profile created will appear in the Manage Data Collection Profiles tab.
Collect Application Data

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*

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

---

**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**

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.
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.
Figure 7-36  Manage Device Access Verification Jobs

The figure shows a table titled "Manage Device Access Verification Jobs." The table contains columns for "Job ID," "Job Name," "Created By," "Description," and "Created On." Each row represents a different job with details such as the job ID, name, creator, description, and date created. The interface appears to be part of a software platform, possibly for managing device access verification tasks. The interface includes options like "Refresh," "Help," and "Remove Job."
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.

Figure 7-37  Manage Workflow Jobs
Manage Configuration Jobs

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
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)

Figure 7-39  Device Prompt Collection Jobs
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)

Note
This feature is only for NOS services

Figure 7-40 Health Monitor Jobs

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.
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.
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.

Figure 7-43   CLI Command

![CLI Command Figure]

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

CLI Command

![CLI Command Figure]

![CLI Command Figure]
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

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

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

Figure 8-2 Graphing Options
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.

View Duplicate Devices

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.
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 devices.

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.

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.
Non SNMP Devices

Non SNMP Devices report list devices that are discovered through "Nmap" mechanism and on these devices SNMP agent is not running. These devices can be moved to managed state. To do so, select the device and right click on it, select Manage Devices.

If device OS detected by Nmap is not accurate, then you can select the appropriate OS name from drop down list.

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

Interface Summary report displays the list of all the interfaces available in CSPC.
Interface Summary data can be also seen in a graphical format, clicking on graphics icon shows the 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.
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**

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.

**Figure 8-11  Device Access Verification Summary**

<table>
<thead>
<tr>
<th>Verification Protocol</th>
<th>Number of Devices Passed</th>
<th>Number of Devices Failed</th>
<th>Number of Devices Unverified</th>
</tr>
</thead>
<tbody>
<tr>
<td>tcp</td>
<td>3873</td>
<td>1127</td>
<td>1</td>
</tr>
<tr>
<td>sshv1</td>
<td>0</td>
<td>5000</td>
<td>1</td>
</tr>
<tr>
<td>sshv2</td>
<td>0</td>
<td>5000</td>
<td>1</td>
</tr>
<tr>
<td>snmpv1</td>
<td>3836</td>
<td>1165</td>
<td>1</td>
</tr>
<tr>
<td>snmpv2</td>
<td>3836</td>
<td>1165</td>
<td>0</td>
</tr>
<tr>
<td>http</td>
<td>0</td>
<td>5000</td>
<td>1</td>
</tr>
<tr>
<td>https</td>
<td>0</td>
<td>5000</td>
<td>1</td>
</tr>
<tr>
<td>wmi</td>
<td>0</td>
<td>5000</td>
<td>1</td>
</tr>
<tr>
<td>if</td>
<td>1</td>
<td>5000</td>
<td>0</td>
</tr>
</tbody>
</table>

**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

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

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

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
- Delete Profile Executions
- View IP Host Masked Values
When you select to View Data you are provided with the data collection profile run data viewer, as shown in Figure 8-16.

![Collection Profile Run Data Viewer](image)

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.

![View Row Data](image)

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

**Figure 8-19 Collection Profile Device Run Summary**
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.

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.
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.

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.
Chapter 8      Applications - Reports

Reports

Figure 8-24   Collection 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

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

Reports

**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

Go back to CSPC Flow Chart
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.

Figure 8-28  View Inventory Summary Filter

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

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

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.

**Figure 8-31** View Config Collected Devices Filter

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.
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

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

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

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.
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.
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 are two types of alerts: UI Notification and Email alerts.

- UI Notification alerts appear 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](image)

SNMP Trap Report

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
Figure 8-38  **SNMP Trap Filter**

To view the Trap Data click **View Trap Data**.

Figure 8-39  **SNMP Report**
Syslog Summary

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

Figure 8-40  Syslog Summary Filter

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

Figure 8-41  Syslog Summary

<table>
<thead>
<tr>
<th>Severity</th>
<th>Message Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 (emergency)</td>
<td>0</td>
</tr>
<tr>
<td>1 (alert)</td>
<td>0</td>
</tr>
<tr>
<td>2 (critical)</td>
<td>0</td>
</tr>
<tr>
<td>3 (error)</td>
<td>303</td>
</tr>
<tr>
<td>4 (warning)</td>
<td>27</td>
</tr>
<tr>
<td>5 (notification)</td>
<td>0</td>
</tr>
<tr>
<td>6 (informational)</td>
<td>0</td>
</tr>
<tr>
<td>7 (debugging)</td>
<td>60</td>
</tr>
</tbody>
</table>
Syslog Messages

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.
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**

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**.

*Figure 8-44 Discovery Jobs*

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_jobunid.csv** click on **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.
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.

To IP Address/Host Name, click Next button.
To schedule discovery options, click **Next** button.

### Inventory Jobs

This report includes all the network device inventory 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.

**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.
Device Access Verification Jobs

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.

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.
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.
Credential Loader Jobs

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

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.

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

Figure 8-55  Apply Config Jobs
Backup and Restore Jobs

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.

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

Figure 8-56 Backup/Restore Jobs

![Backup/Restore Jobs](image)
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.

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

Figure 8-57  Ping Jobs
Trace Route Jobs

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

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.

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

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

Figure 8-59  Prompt Collection Jobs
Health Collection Jobs

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.

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

Figure 8-60 Health Collection Jobs
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.

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.

If you do not want to run a scheduled upload, right click on the job and then click Unschedule Job button.
A confirmation box as shown in Figure 8-64 is displayed.

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.

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

**Figure 8-66  Upload Run Now Jobs**

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 8-67  Edit Job Schedule**

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

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

Figure 8-68 Connectivity Jobs

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

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

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.
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.

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.
### Figure 8-73  Job Metrics

#### Discovery Job Metrics

<table>
<thead>
<tr>
<th>Job Id</th>
<th>Discovery Type</th>
<th>Devices Attempted</th>
<th>Devices Successful</th>
<th>Devices Failed</th>
<th>Devices Skipped</th>
<th>Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>34</td>
<td>IP based discovery</td>
<td>40</td>
<td>05</td>
<td>3</td>
<td>0</td>
<td>20 Second(s)</td>
</tr>
<tr>
<td>25</td>
<td>IP based discovery</td>
<td>60</td>
<td>03</td>
<td>6</td>
<td>0</td>
<td>22 Second(s)</td>
</tr>
<tr>
<td>32</td>
<td>IP based discovery</td>
<td>60</td>
<td>03</td>
<td>3</td>
<td>0</td>
<td>23 Second(s)</td>
</tr>
<tr>
<td>29</td>
<td>IP based discovery</td>
<td>60</td>
<td>03</td>
<td>6</td>
<td>0</td>
<td>23 Second(s)</td>
</tr>
</tbody>
</table>

**Average time taken for 100 devices:**

*Ethernet IP based discovery — 20 Second(s)*

*Seed IP based —

#### DAV Job Metrics

<table>
<thead>
<tr>
<th>Job Id</th>
<th>Protocol Selected</th>
<th>Devices Attempted</th>
<th>Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>32</td>
<td>esrp, ssl, ssh, http</td>
<td>60</td>
<td>1 Minute 6 Second(s)</td>
</tr>
<tr>
<td>29</td>
<td>esrp, ssl, ssh, http</td>
<td>60</td>
<td>1 Minute 4 Second(s)</td>
</tr>
<tr>
<td>29</td>
<td>esrp, ssl, ssh, http</td>
<td>60</td>
<td>1 Minute 4 Second(s)</td>
</tr>
<tr>
<td>29</td>
<td>esrp, ssl, ssh, http</td>
<td>60</td>
<td>1 Minute 4 Second(s)</td>
</tr>
</tbody>
</table>

#### Inventory Job Metrics

<table>
<thead>
<tr>
<th>Job Id</th>
<th>CP Name/Service Name</th>
<th>Devices Attempted</th>
<th>Devices Collected</th>
<th>Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>30</td>
<td>NIC9</td>
<td>60</td>
<td>60</td>
<td>7 Minute 49 Second(s)</td>
</tr>
<tr>
<td>37</td>
<td>NIC9</td>
<td>60</td>
<td>60</td>
<td>5 Minute 9 Second(s)</td>
</tr>
<tr>
<td>40</td>
<td>NIC9</td>
<td>60</td>
<td>98</td>
<td>8 Minute 7 Second(s)</td>
</tr>
</tbody>
</table>

**Average time taken for 100 devices:**

*Ethernet — 12 Minute(s) 27 Second(s)*

#### Updated Job Metrics

<table>
<thead>
<tr>
<th>Job Id</th>
<th>CP Name/Service Name</th>
<th>Devices Attempted</th>
<th>Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>24</td>
<td>NIC9</td>
<td>60</td>
<td>20 Second(s)</td>
</tr>
</tbody>
</table>

**Average time taken for 100 devices:**

*Upload — 10 Second(s)*
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 user name, 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 user name, 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.

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 user name, 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.

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 user name, 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.
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

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.
Once the selection is done, the specific application will be launched for the given devices.
View Locked Credentials

This report provides a list of all the locked credentials. The report contains Credential name, Protocol, User Name, Locked time and Will be Unlocked At (based on the configured Lock Period).

**Figure 8-79  View Locked Credentials**

To unlock a credential, right click on the Credential you want to unlock and select *Unlock the Credential...* option.
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.

Figure 8-80  Disabled Protocol Report

Disable Command Report

Disabled Command Report shows the details of commands that are disabled for a given device.

Figure 8-81  Disable 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

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

Application Profile Run Summary

Application profile run summary report provides a summary of the completed application profiles as shown in Figure 8-84.
Figure 8-84  Application Profile Run Summary

Figure 8-85  Application Discovery Report

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.

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:
Tomcat, MySQL, ArgoSoft, DB2, SQL Server, OpenLDAP, NetBIOS Session Service, EmailArchitect Super Service, JBOSS, DNS Server, MSMQ, VMWare Workstation, WebSphere, Oracle, RPC, IIS Admin, SANSurfer.
Linux:
Tomcat, MySQL, httpd, OpenLDAP, FTP Server, SendMail, Telnet, DNS Server.

Figure 8-86   Application Discovery Report Expanded
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.
Figure 9-1  Manage Users

![Manage Users](image1)

<table>
<thead>
<tr>
<th>Login</th>
<th>Full Name</th>
<th>Authentication Type</th>
<th>User Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>cpadmin</td>
<td></td>
<td>Local User</td>
<td>Administrator</td>
</tr>
<tr>
<td>admin</td>
<td>Super Administrator</td>
<td>Local User</td>
<td>Administrator</td>
</tr>
</tbody>
</table>

Figure 9-2  Manage Collector Users

![Manage Collector Users](image2)
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 can configure all the settings related to management. But he can't make any changes that effect the server.
  - 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.

Manage Remote Authentication Servers

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.
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.

Figure 9-5  Login settings
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.

![User Session Report](image)

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.
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.

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
- Alert Configuration

Email Settings

This setting provides you with an option to configure a SMTP server for mail exchange.
Enter all the Mandatory fields and click OK

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMTP Server</td>
<td>Server name or identity of the server</td>
</tr>
<tr>
<td>SMTP Port</td>
<td>Port number used for the server</td>
</tr>
<tr>
<td>Email To</td>
<td>Receiver mail address</td>
</tr>
<tr>
<td>Sender's Mail ID</td>
<td>Sender mail address</td>
</tr>
<tr>
<td>User Name</td>
<td>Login name</td>
</tr>
<tr>
<td>Password</td>
<td>Login password</td>
</tr>
</tbody>
</table>

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.

Step 1: To add a Subscribers, click Add Subscribers the below screen appears shown in Figure 9-11
Step 2 Enter Module Name, select Notification Enabled, and if required enter Notification Type and Email To and then click OK.

Alert Configuration

Alert an 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.

Step 1 To add an alert, click Add Alert Configurations the screen appears as shown in Figure 9-13
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 enter the success percentage value for protocol(s)

Step 3  Click **OK**

Note  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.

Note  To make the file transfer more secure:

- It is recommended to use the secure protocols SFTP and SCP against insecure ones 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 user name
  - **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 user name
  - **Password**: SFTP server password
  - **Fingerprint**: Authentication received from server

- If Local Server is selected continue

**Note**

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

**Note**

To remove inventory data from backup select Ignore Inventory Data.
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.

Step 3  To exclude the files from **Backup** unselect the files as shown in Figure 9-16.
To see the files here you have to enter the file path in properties file.

**Figure 9-16 Exclude Backup Files**

![Exclude Backup Files](image)

Please unselect to exclude 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 user name
  - **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 user name
  - **Password**: SFTP server password
  - **Fingerprint**: Authentication received from server

- **If Local Server** is selected continue

---

**Note**

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
Figure 9-17  Restore Server Backup

Note  To enable slave mode click **Enable Slave Mode** and it requires CSPC to restart. This disables all other jobs except **Backup and Restore** jobs on CSPC. Similarly to disable click **Disable Slave Mode** and it also requires restart.

Figure 9-18  Configure Schedule
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*
Export Log Files

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 Export Log Files by File

Figure 9-21 Export Log Files by Timestamp
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 with that process as shown in Figure 9-22.

Note

NOS service will have audit addon process and DCOS service will have dcos addon process

Figure 9-22 View Server Process Summary

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
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, server time zone, etc, as shown in Figure 9-24.

**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.
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 service 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

This option provides simple diagnostic tools like ping and traceroute to check if the device is available or connectivity is to the device is established. Pick the command you want to use and select the device on 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

Figure 9-27  Diagnostic Tools - Trace Route Utility
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.

Figure 9-28 XML API Console
Menu Options

Menus

Menu options are provided as a quick way to access the applications.

The menu options provided in CSPC are:

- User Name
- Settings
- Management
- Reports
- Administration
- Help
- Quick Menus

User Name

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*.

![Menu Option - Settings](image)
Management

*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*.

<table>
<thead>
<tr>
<th>Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discover Devices...</td>
</tr>
<tr>
<td>Unmanage Devices...</td>
</tr>
<tr>
<td>Verify Device Access</td>
</tr>
<tr>
<td>Device Prompt Collection...</td>
</tr>
<tr>
<td>Collect Data...</td>
</tr>
<tr>
<td>Upload Data...</td>
</tr>
<tr>
<td>Adhoc Data Collection...</td>
</tr>
<tr>
<td>Collect Application Data...</td>
</tr>
<tr>
<td>Job Run Status...</td>
</tr>
</tbody>
</table>
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
Administration

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

<table>
<thead>
<tr>
<th>Administration</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Manage Users...</td>
<td>Manage Remote Authentication Servers...</td>
</tr>
<tr>
<td>User Session Report...</td>
<td>Modify Date/Time Preference...</td>
</tr>
<tr>
<td>Configure Default Device Display Property...</td>
<td>Email Settings...</td>
</tr>
<tr>
<td>Manage Subscribers...</td>
<td>Alert Configuration...</td>
</tr>
<tr>
<td>Backup...</td>
<td>Restore Backup...</td>
</tr>
<tr>
<td>Log Preferences...</td>
<td>Export Log Files...</td>
</tr>
<tr>
<td>Manage Add-on Process...</td>
<td>Manage UI Add-ons...</td>
</tr>
<tr>
<td>Server Properties...</td>
<td>Configure CSPC Appliance...</td>
</tr>
<tr>
<td>Diagnostic Tools...</td>
<td>XML API Console...</td>
</tr>
</tbody>
</table>
Help

Under Help menu, following option is shown:

- About
- Help Contents
- View/Upgrade Registration

Figure 10-6 Menu Option - Help

Quick Menus

This Menu helps for the fast and easy access for the vital features on CSPC.

Table 10-1 Quick Menu

<table>
<thead>
<tr>
<th>Menu Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Credentials]</td>
<td>This takes you to Device Credentials page for more info refer to: Add/Import Credentials.</td>
</tr>
<tr>
<td>![Discovery]</td>
<td>This takes you to Select Discovery Methods page for more info refer to: Discover Devices.</td>
</tr>
<tr>
<td>![Managed Devices]</td>
<td>This takes you to View Discovery Devices page for more info refer to: View Managed Devices.</td>
</tr>
<tr>
<td>![Collect]</td>
<td>This takes you to Select Collection Profile page for more info refer to: Collect Data.</td>
</tr>
<tr>
<td>![Collected Data]</td>
<td>This takes you to View Collected Data page for more info refer to: View Collected Data.</td>
</tr>
<tr>
<td>![Upload]</td>
<td>This takes you to Select Upload Profile page for more info refer to: Upload Data.</td>
</tr>
<tr>
<td>![Job Run Status]</td>
<td>This takes you to Job Run Status page for more info refer to: Job Run Status.</td>
</tr>
</tbody>
</table>
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

Here an SSH credential is added against a wildcard:

Figure A-1  Device Credentials
Result is shown in Figure A-2:

Figure A-2  Device Credential Configuration

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.
Figure A-3  Discover and Manage Network Devices

Either the IP Address or the DNS Name.

Figure A-4  Discover and Manage Network Devices
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

Note: 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
; 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
A new feature is implemented to decide the primary device name using column 1, column 2, and column 3 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_type
• mdf_type
• 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
• 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
• Snmpv3AuthAlgorithm
• SnmpV3PrivAlgorithm
• SnmpVPrivPassword

Export File Format

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 add/modify the IP to be used for replacing the <#SERVERIP#> tag.

To add/modify a CSPC Server IP, use below xml API

```xml
<Request requestId="" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.parinetworks.com/api/schemas/1.1 pari_api.xsd"
xmns="http://www.parinetworks.com/api/schemas/1.1">
  <Manage>
    <Add operationId="1">
      <ServerDetails>
        <IPAddress>x.x.x.x</IPAddress>
      </ServerDetails>
    </Add>
  </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

- 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 can not 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. Based on 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 slots then the command will be: `session slot <name> processor 1`

2. **AddOutput**: This type of output can be use 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 / SNMPObjectId/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 were in the output can be added to a variable and latter 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".

```xml
<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>

```

```xml```
<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>
        <Rows>
          </Rows>
        </SNMPTable>
      </VectorInput>
      <Actions>
        <Assignment>
          <Variable append="false" onlyIfNotNull="false" trim="false" vectorType="Set"
            Operation="add">ifTypes</Variable>
          <Values>
            </Values>
          </Assignment>
        </Actions>
        <Statements>
          <Condition identifier="loop1_cond1">
            <Title>Check to see if Interface is require type</Title>
            <Input>
              <SNMPValue>
                </LoopContext>
              </SNMPValue>
            </Input>
            <Operation>
              <IsMemberOf><VariableName>ifTypes</VariableName>
              <IsMemberOf><VariableName>ifTypes</VariableName>
            </Operation>
            <Match>
<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>
</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>
<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>
</Statements>
</Loop>
<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>
      <AddOutput>
        <Value><SnmpDatasetResponse><SNMPRequest><RequestType>Column</RequestType><ObjectList><Object><oid></Object></ObjectList></SNMPRequest><SnmpResponse><Row><InstanceId><last_cond1.1></InstanceId><Columns><Column><last_cond3.1></Column></Columns></Row></SnmpResponse></SnmpDatasetResponse></Value>
      </AddOutput>
    </Output>
  </Match>
</Condition>
<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

```xml
<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"
xmns="http://www.parinetworks.com/api/schemas/1.1">
  <Job>
    <Schedule operationId="1">
      <JobSchedule runnow="true">
        <RegressiveSeedFileJob>
          <TriggerDav>true</TriggerDav>
          <DeleteCreds>true</DeleteCreds>
          <DeleteDevices>true</DeleteDevices>
        </RegressiveSeedFileJob>
      </JobSchedule>
    </Schedule>
  </Job>
</Request>
```

Scheduled seedfile job

```xml
<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"
xmns="http://www.parinetworks.com/api/schemas/1.1">
  <Job>
    <Schedule operationId="1">
      <JobSchedule runnow="false">
        <Start>1409607000000</Start>
      </JobSchedule>
    </Schedule>
  </Job>
</Request>
```
Add Notification

```
<Request xmlns="http://www.parinetworks.com/api/schemas/1.1" requestId="4444">
  <Manage>
    <Add operationId="1">
      <NotificationList>
        <Notification>
          <TrapOID/>
          <NotificationType/>
        </Notification>
        <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"/>
    </Delete>
  </Manage>
</Request>
```
Appendix E  XML APIs

Delete Single Notification

```xml
<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

```xml
<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

```xml
<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

```xml
<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"/>
        </SNMPTrapProfile>
      </SNMPTrapProfileList>
    </Add>
  </Manage>
</Request>
```

Delete All SNMP Trap Profiles

```xml
<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

```xml
<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

```xml
<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

```xml
<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>
```
Modify SNMP Trap profile

```xml
<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>
            <FromDate></FromDate>
            <ToDate></ToDate>
          </Custom>
        </TimePeriod>
      </SnmpTrapReport>
    </Get>
  </Report>
</Request>
```
Report based on Time Interval

```xml
<Request xmlns="http://www.parinetworks.com/api/schemas/1.1" requestId="44444">
  <Report>
    <Get operationId="1">
      <SnmpTrapReport>
        <TimePeriod>
          <SinceTime>
            ...
          </SinceTime>
        </TimePeriod>
        <Source>
          ...
        </Source>
        <NotificationList>
          ...
        </NotificationList>
        <NotificationType>
          ...
        </NotificationType>
        <NotificationList>
          ...
        </NotificationList>
        <SnmpTrapReport>
          ...
        </SnmpTrapReport>
      </Get>
    </Report>
  </Request>
</Request>
```

Modify SNMP trap port and Purge Settings

```xml
<Request requestId="4444" xmlns="http://www.parinetworks.com/api/schemas/1.1">
  <Manage>
    <Modify operationId="1">
      ...
    </Modify>
  </Manage>
</Request>
```
<ApplicationPreferencesSettings>
  <SnmpTrapSettings>
    <PurgeSettings>15</PurgeSettings>
    <SnmpTrapPort>162</SnmpTrapPort>
  </SnmpTrapSettings>
</ApplicationPreferencesSettings>

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>
      </Schedule>
    </Job>
    <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>
  </Request>

Appendix E      XML APIs

Restore Job XML API

```xml
<Request xmlns="http://www.parinetworks.com/api/schemas/1.1" requestId="3333">
  <Job>
    <Schedule operationId="123">
      <JobSchedule runnow="true" />
    </Schedule>
    <RestoreJob jobName="Backup">
      <FTPServerOptions>
        <ServerHost>x.x.x.x</ServerHost>
        <UserName>user</UserName>
        <Password>xxxx</Password>
        <Directory>resources</Directory>
        <FileName>_1391384366427.pbx</FileName>
      </FTPServerOptions>
    </RestoreJob>
  </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

```xml
<?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 -->
            </Rule>
          </Rules>
        </ChannelTypeRules>
      </ChannelType>
    </Add>
  </Manage>
</Request>
```
<Operands>
<Operand><![CDATA[Star OS]]></Operand> <!-- Operand depend on attribute and operator values -->
</Operands>
</Rule>
</Rules>
</ChannelTypeRules>

<CILIRules>
<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>
</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>
<Operator>INDEXOF</Operator>
</Rule>
</Rules>
</OtherPromptRules>
<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:&login:&user:]]></EnableUserPrompts> <!-- Provide user prompts -->
 <EnablePwdPrompts>![CDATA[Password:]]></EnablePwdPrompts> <!-- Provide password prompts -->
</EnableRules>

<ClearTerminalLengthDefinition>
 <Command>terminal length 0</Command> <!-- Provide commands used to set terminal length for the device -->
 <Command>terminal width 0</Command>
</ClearTerminalLengthDefinition>

<AfterLoginCommand>
 <Command>cli</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
<?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 -->
        <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>
          <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>
            </MorePromptRules>
          </CLIRules>
        </ChannelTypeRules>
      </Modify>
    </Manage>
  </Request>
```
</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:&Password:&login:&user:]]></EnableUserPrompts> <!-- Provide user prompts -->
<EnablePwdPrompts><![CDATA[Password:]]></EnablePwdPrompts> <!-- Provide password prompts -->
</EnableRules>

<ClearTerminalLengthDefinition>
<Command>terminal length 0</Command> <!-- Provide commands used to set terminal length for the device -->
<Command>terminal width 0</Command>
</ClearTerminalLengthDefinition>

<AFTERLOGINCOMMAND>
    <Command>Clis</Command> <!-- some devices required commands after login to the device and before entering into the enable mode, provide those commands here -->
    </AFTERLOGINCOMMAND>

<ReplaceEscChar>\[</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**

```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 rules and cli rules -->
        </CLIChannelReport>
        </Get>
    </Manage>
    </Request> ?
```

**Channel Delete Channel XML**

```xml
- <Request xmlns="http://www.parinetworks.com/api/schemas/1.1" requestId="ChannelList">
```
- <Manage>
- <Delete operationId="1">
  <ChannelType channelId="Acsw" />
- <!-- This XML deletes channel definition 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)

<Request xmlns="http://www.parinetworks.com/api/schemas/1.1" requestId="3333">
  <Job>
    <Schedule operationId="123">
      <JobSchedule runnow="true"/>
    </JobSchedule>
  </Job>
</Request>
CSPC Backup (PSS) - Schedule

```xml
<Request xmlns="http://www.parinetworks.com/api/schemas/1.1" requestId="3333">
  <Job>
    <Schedule operationId="123">
      <JobSchedule runnow="false">
        <Start>1450692900000</Start>
      </JobSchedule>
    </Schedule>
    <BackupJob jobName="Backup_RunNow">
      <BackupJobType>Full_Backup</BackupJobType>
      <IgnoreRunningJobs>true</IgnoreRunningJobs>
      <FTPServerOptions>
        <ServerHost>10.127.152.54</ServerHost>
        <UserName>admin</UserName>
        <Password>XXXXX</Password>
        <Directory>xml</Directory>
      </FTPServerOptions>
      <IgnoreInventoryData>true</IgnoreInventoryData>
    </BackupJob>
  </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>
          <VersionedList>
            <VersionedDataset identifier="cisco">
              <SNMP>
                <SNMPRequest>
                  <RequestType>Scalar</RequestType>
                </SNMPRequest>
              </SNMP>
            </VersionedDataset>
          </VersionedList>
        </Dataset>
      </DatasetList>
    </Add>
  </Manage>
</Request>
```
<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
<Request>
  <Export>
    <ExportAllRules>
      <ExportLocation></ExportLocation>
    </ExportAllRules>
  </Export>
</Request>

API for Import All Rules
REQUEST
<Request>
  <Execute>
    <ImportAllRulesFromZipFile>
      <AllRuleZipFileLocation>/opt/CSPC/data/ruleExport/CSPCRules_1450433792272.Zip</AllRuleZipFileLocation>
    </ImportAllRulesFromZipFile>
  </Execute>
</Request>
Appendix E      XML APIs

Upload Signature for Custom Profiles (PSS)

Listing 25: XML for uploading a signature for custom profiles

```xml
<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

```xml
<Request requestId="123">
    <Manage>
        <Modify operationId="11">
            <ApplicationPreferencesSettings>
                <Discovery>
                </Discovery>
            </ApplicationPreferencesSettings>
        </Modify>
    </Manage>
</Request>
```
<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>
</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>
    <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.x</IpExpression> —— Give valid IP address
          </IpExpressionList>
      </AddExternalComponents>
    </Add>
  </Manage>
</Request>
```
<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.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="pfense_snmpv2">
  <Type>PFSENSE</Type>
  <IpExpressionList>
    <IpExpression>x.x.x.x</IpExpression>
  </IpExpressionList>
  <ReadCommunity>public</ReadCommunity>
  <Protocol>snmpv2c</Protocol>
</DeviceCredential>
</AddExternalComponents>
</Add>
</Manage>
</Request>
Upload Health Information

```xml
<Request xmlns="http://www.parinetworks.com/api/schemas/1.1" requestI d="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

```xml
<Request xmlns="http://www.parinetworks.com/api/schemas/1.1" requestI d="cp_schedule">
  <Job>
    <Schedule operationId="1">
      <JobSchedule runnow="true" />
      <DAVJob jobName="SBTestDavJobXML">
        <DeviceSelection all="true"/>
        <OverrideEnableFailed>true</OverrideEnableFailed>
        <RunDAVForUnreachable>true</RunDAVForUnreachable>
        <RunDiscoveryBeforeExecution>false</RunDiscoveryBeforeExecution>
        <Pingable>true</Pingable>
      </DAVJob>
    </Schedule>
  </Job>
</Request>
```
Region Based Collection via User Groups

For creating static device group based on the user fields during import seedfile:

```xml
<?xml version="1.0" encoding="UTF-8"?>
<Request xmlns="http://www.parinetworks.com/api/schemas/1.1" requestId="seedfile">
  <Job>
    <Schedule operationId="1">
      <ImportSeedFileJob jobName="q20">
        <Description>a1</Description>
        <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
<?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>
  </Manage>
</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>
      </DeviceCredentialList>
    </Manage>
  </Request>

Add SQL Datasets

<Request xmlns="http://www.parinetworks.com/api/schemas/1.1" requestId="44444">
  <Manage>
    <Add operationId="1">
      <DatasetList>
        <Dataset identifier="Name">
          <Title>Title</Title>
        </Dataset>
        <DatasetList>
      </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">
    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

```xml
<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

REST API call to export and get the filename
https://localhost:8001/cspc/xml/
Additional Device Properties

API to Download the Collection Profile Run Data

REST API GET call to download the collection profile run data


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>
</Request>
Delete Additional Device Properties

```xml
<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>
  </Manage>
</Request>
```

Get Additional Device Properties

```xml
<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>
              </Dataset>
            </VersionedDatasetList>
          </VersionedDatasetList>
          </Dataset>
        </DatasetList>
      </Add>
    </Manage>
  </Request>
Adding LDAP Datasets

```xml
<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>
        </Dataset>
        <VersionedDatasetList>
          <VersionedDataset identifier="_ACNS">
            <LDAP>
              <SearchBase/>
              <SearchFilter/>
              <SearchScope/>
              <AttributesToReturn/>
              <MaskRule/>
              <Timeout/>
            </LDAP>
          </VersionedDataset>
        </VersionedDatasetList>
      </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**.

**Note**
All the Self signed certificates provides a warning message on the browser.

**Figure F-1 Warning Message**

You will not get this warning 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

```bash
# openssl x509 -req -days 500 -in localhost.csr -signkey localhost.key -out localhost.crt
```

Signature ok
Appendix F  Uploading Valid SSL Certificate

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.p12 -srcstoretype pkcs12
-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
Figure F-2 Certificate Information

Certificate Information

This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: sbre

Issued by: sbre


Learn more about certificates
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**

```
zU7R1r/JZaWFLmFljKVm5Zrtu0aGvTyQzVU60RI73n0 (base64-encoded SHA256 checksum)
```

**Note**
In OpenSSH 6.7 and earlier versions this fingerprint was an 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.

```
iptables -A INPUT -p tcp -m tcp --dport 61617 -j ACCEPT
```
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?
Appendix I  Frequently Asked Questions

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.

Figure I-1  Third Party PIDs