Partner Support Service Portal User Guide

May 10, 2019

Overview

Partner Support Service (PSS) provides capabilities to discover, collect, analyze network device details and provide network aware information. PSS provides inventory reporting and analysis on network devices, which gives you information about contracts, expiring coverages, various product alerts, and different types of network summary reports.

With the web-based portal and associated reports, you can obtain all of the information that you need in order to manage your customer's Cisco inventory. The integrated smart capabilities provide current information about the installed base, contracts, and security alerts in order to enhance the efficiency of your support workflows.

This user guide provides information that you can use in order to:

- register and assign roles in the portal
- get started with the portal
- setup and customize the portal
- generate and use reports with the portal library

Important Registration Information

Please Read before Registering Users to the PSS Portal

You can launch the Partner Support Service portal from your web browser at https://services.cisco.com. For registering new users, Partner Administrators can use the Manage Users action to add, edit, or delete users to their Partner Definition (company access).

Note Do not be confused by the Cisco Services Connection label you see on the screen. When you see the Cisco Service Connection name at the top of the left navigation pane you are viewing the Partner Support Service (PSS) portal.

Please contact the Cisco Technical Support and open a support case if you have any issue with the registration process. E-mail: tac@cisco.com

Terminology

The following key terms are used in the user registration process:

Partner – Purchases PSS for their end-customers and can be assigned a user role in the Partner Support Service portal so they can access their end-customer's network data.

Cisco Services Connection – This is the user interface that provides access to Partner Support Service portal and all data associated to PSS contracts, as entitled by the respective user role. Administrators and users can access the data and reports of all customers to which their user roles have been associated. The portal allows users to customize reports generated by this service and to perform additional actions. The portal is accessed from your web browser at https://services.cisco.com.

Contracts – A partner must have a supported Partner Support Service (PSS) type contract in their user's Cisco.com profile (CCO ID). The partner company must have purchased a PSS contract for at least one end-customer in order for users in the partner company to be registered and get access to the data for end customer(s).

Entitled Company - Entitled Company in the PSS portal is the end-customer company for which you have purchased PSS. Or, in case you are trying out the capabilities on your own network/lab environment, the Entitled Company is your company. The Entitled Company displayed in the PSS portal may not be exactly the same as the Installed-At Site(s) on the contract(s) you have purchased or the company name you use to refer to your end-customer’s company. This is because the PSS portal does not use individual Installed-At Sites of a customer as Entitled Company but rolls these up to a company based on the D&B company information.

PSS Roles:

Partner Super Administrator (SA) – Cisco Support Agent On-Boards the Partner Administrator to Cisco Services Connection (PSS portal) as a Super Administrator, who registers employees to access capabilities using the PSS portal.

Partner Administrator (PA) – A Partner Administrator (PA) role can register users. The Partner Administrator privileges allow the administrator to perform the following tasks:

- Register a collector.
- Download a license file.
- Maintain collector registrations. [Add, Edit and Delete]
- View all reports.
- View, manage, and update PSS user access to end customer company information.

Partner User (PU) – A Super Administrator or Partner Administrator assigns a Partner User (PU) role to a registered user. A Partner User cannot manage other company users, user roles, or company associations. A partner company may or may not have a Partner User.

A Partner User can perform the following tasks:

- Access only those end-customers that they were associated to by PA or SA.
- Access one, multiple, or all end-customers of the partner company, which gives them visibility to all the data and reports for these end-customers (inventory, contracts, alerts, and so on).
- Register a collector
- Download a license file
- Maintain Collector Registrations

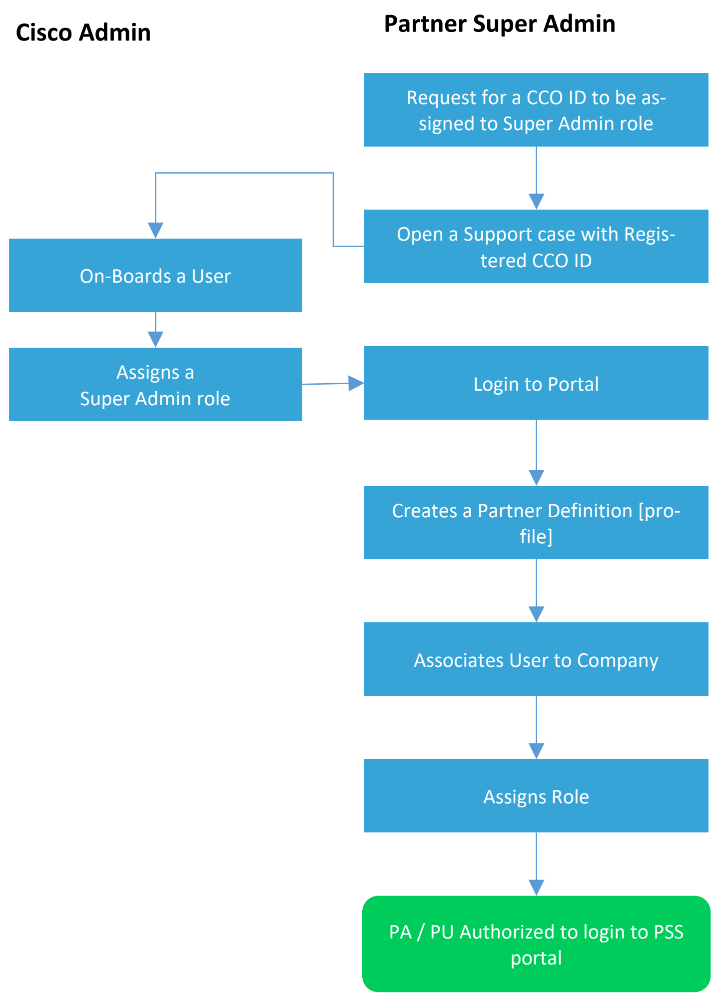
- End-Customer Company – The company for which the partner purchased PSS contracts for.

Partner Registration and Role-Assignment Process Flows

The Partner Super Administrator maintains the Partner Definition of customer PSS contracts being managed by the partner company. Contracts managed by PSS are defined in the Partner Definition, not in each partner company employee's Cisco.com profile. One Super Administrator is assigned for each Partner Definition.

Cisco Support Administrator on-boards the PSS partner, once he receives a request for a Partner Super Administrator. This Super Administrator would then have the ability to register partner employees using the PSS portal.

Note A user can be assigned the Super Administrator role for only one Partner Definition (company) and can also be assigned Partner Administrator or Partner User roles for Partner Definitions (company). As a Super Administrator, he has full access and is primarily responsible for managing the Partner Definition, managing collectors and assigning roles to the partner users using the PSS portal.



Getting Started with the Partner Support Service Portal

Follow the below steps to gain access to the Partner Support Service (PSS) portal, where the full value of PSS is realized for you and your customers.

In order for a Partner Super Administrator to be assigned, you must meet these requirements:

- You must have a valid Cisco account profile. A Cisco ID allows us to identify you and deliver the right information and capabilities to which you're entitled. To create a Cisco ID, please visit the Cisco.com Registration page.
- Your account must have one or more valid PSS contracts associated with it for the end-customer company (ies) to whom you need access. The following section discussed linking contracts/Bill-to Ids to your Cisco ID.

1. Link Contracts/Bill-to IDs to your Cisco ID

Associating the services your partner company has purchased with your Cisco ID unlocks access to the additional capabilities and resources to which you're entitled. To obtain technical support, request hardware replacement, or download software related to service contracts, you must associate all of your service contracts with your Cisco.com profile. Individual users may use Profile Manager to associate contracts with their profile.

2. Register for PSS Portal Access

First select a person at your organization who will administer the portal for your company. This person will register for portal access first, becoming the Super Administrator. Ideally, the Super Admin should be someone who already manages the user access and accounts within the organization. Network administrators are a good choice for this role.

Request Super Administrator Role

The person who will be registered as Super Administrator will perform the following steps:

1. Open a Support case using the registered Cisco.com ID that is to be given the Super Administrator role, include the Partner Company name and the Cisco.com ID of the person being nominated.
2. Cisco Support personnel receive the Support case request for a Partner Super Administrator, and on-boards the Partner Administrator to the PSS portal as a Super Administrator who then has the ability to:
   - Administer the Partner Definition
   - Administer partner user access to the PSS portal
   - Administer collectors
   - Run Reports
3. Bill-To IDs are pulled from the Super Administrator's Cisco.com ID profile (associated Service Contracts) to define the Bill-To IDs in the Partner Definition in the portal.
4. An email is sent to the Super Administrator when on-boarding is complete.
   - Contact the Cisco TAC and open a support case if you have any issue with the registration process: tac@cisco.com
   - View User Training for Managing the Portal Partner Definition (10:25) and Managing the Portal User Registrations for Partner Administrators (9:30)

Change Super Administrator to a Different Cisco.com ID

Should the Super Administrator leave the company, you will need to nominate a new one. Perform the following steps:

1. Open a Support case with the registered Cisco.com ID that is to be given the Super Administrator role.
2. Include the Partner Company name and the Cisco.com ID of the person being nominated.

Once the Super Administrator has been on-boarded to the portal, the next step in the process is to define the Partner Definition within the PSS portal.

3. Define the Partner Definition

Partner Support Service portal uses "partner definition(s)" to define the PSS customer contracts being managed. When approved as a Cisco Partner, the partner company is issued an ID. Partners have the option of having one ID for the entire company, or they can register regional offices with unique IDs.

Each partner company (ID) will provide a Super Administrator, who has a registered CCO ID Profile with customer contracts for PSS. The contracts associated to the Super Administrator serve as the basis for the PSS portal Partner Definition. Partner definitions could be based on different scenarios where association is with one location or with multiple Bill-To Addresses / locations.

Note: The Partner Definition consists of one or more of the partner Bill-To IDs used to purchase PSS contracts for their customers. Both the Partner ID and the Bill-To IDs are issued by Cisco to newly approved partners.

Super Administrators manage the Partner Definition in the PSS portal. Refer to the Manage Partner Definition section in this User Guide.

4. User Registration

With the Partner Definition defined, the Super Administrator can then add additional company users, allowing them to access the portal and perform tasks as assigned.

Add Bill-to IDs to Company Employees Cisco.com Accounts

Once assigned as Partner Super Administrators or Partner Administrator, use the Service Access Management Tool (SAMT) to add service contracts to your company employees Cisco.com profiles. Using this tool and a bill-to ID, all service contracts purchased under that bill-to ID, new and existing, are added to the user's profile.

Service contracts can also be added by individual contract number, but each service contract purchased must be added manually. See the Service Access Management Tool (SAMT) Training for more information.

Note: User Registrations for accessing the PSS portal, are done using SAMT. Registrations for the API Console are done using CSAM.

Assign Users in the Portal

Partner Super Administrator or **Partner Administrators** use the **Manage Users** report under **Actions** to view and edit the list of users, respective roles and what customers each user has access to. See the Manage Users section in this User Guide for details on adding, editing or deleting users.

Portal User Roles

Each company employee is assigned a role for accessing customer data on the PSS portal.

- **Super Administrator** - maintains the Partner Definition of the customer contracts that will be managed with PSS service and is also automatically registered as a Partner Administrator. There can be only one Super Administrator.
- **Partner Administrator** - has access to all functions in the PSS portal for all customers included in the Customer Definition from registering users on the portal, to running reports and collector management. The only task a Partner Administrator cannot perform is manage the Partner Definition. Any number of Partner Administrators can be assigned.
- **Partner User** - has access to all PSS portal functions except Manage Users for all customers, or a subset of the customers, as set up by the Partner Administrator.

The following illustration provides the different PSS roles and indicates what end-customer data each user role has access to:

Table 1 - List of user roles and the group of tasks that can be performed

Name	Assignment	Actions	Scope
Partner Super Admin	By Cisco Support	• Partner Definition Administration • User Administration • CSPC Collector Administration • All Reports	All Customers
Partner Admin	By Super Admin, or Partner Admin	• User Administration • CSPC Collector Administration • All Reports	All Customers
Partner User	By Super Admin, or Partner Admin	• CSPC Collector Administration • All Reports	Sets of Customers

5. Collector Registration Process

Both **Super Administrator** and **Partner Administrators,** can manage the collectors for all customers while a **Partner User** can manage the collectors for the customers that they are entitled to.

You can register a new collector for a customer site, edit or delete the collector registrations, regenerate a new collector security certificate, and view collectors needing revalidation upload. Refer to Manage Collectors in the Actions section in this User Guide.

Working with the PSS Portal

The Partner Support Service portal leverages the Cisco Services Connection platform that provides intuitive and easy-to-use reports. These reports can be filtered, viewed in different formats, and customized in order to define the manner in which the data is viewed.

Note As part of the Cisco policy to safeguard access to customer data, a pop-up message is displayed on the Partner Support Service portal screen after an hour of portal inactivity.

The below images illustrate the portal as it typically appears when you access it, provided it has been populated at least once with the device data for your organization:

Portal Components

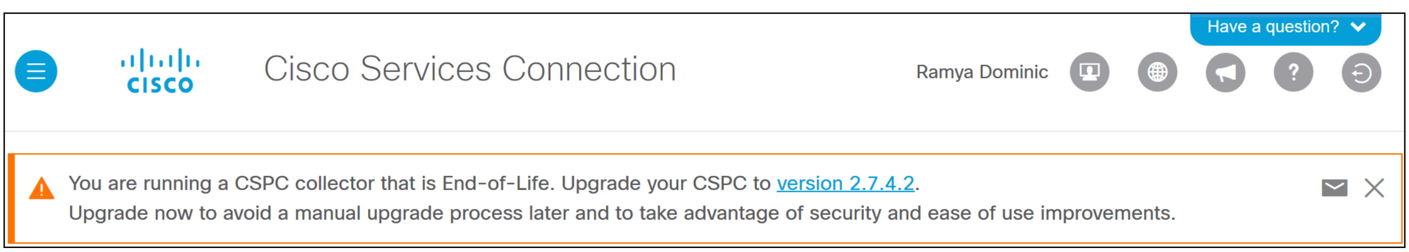
The portal is comprised of these components:

- Top panel – this section contains the following:
    - **Logged-in User** – The name of the user who is currently logged-in appears in this area.
    - **Time zone preference** – Set your time zone preference here.
    - **Feedback** – provide feedback regarding the platform.
    - **Have a question** – Click this icon in order to view how-to videos, download a copy of this guide, and search for information about Partner Support Service.
    - **Log Out** – Click this icon in order to log out of the portal.
- **Left Navigation Pane** – This portion of the page contains links to reports, dashboards, and portal settings. Further details on this below.
- **Content Area** – This portion of the page displays the dashboard or report selected in the Navigation Pane. Refer to **Content Area Components** for details on working with reports.

Note For more details about PSS portal navigation and components, refer to the Navigation Basics video.

Title Bar and Portal Banner

The Title bar and the banner are the top two layers of the Cisco Services Connection user interface. These two layers are described below in further detail.



The Title bar provides the following information:

- Icon to close the left navigation pane so more of the report can be seen online.
- The name of the active application (in example, Cisco Services Connection).
- User name
- Country and language settings option
- Options to provide feedback and find more information
- Log Out option

The lower pane displays the following:

- CSPC Version Reporting alerts regarding collector versions deployed by the logged in user. The banner displays when a collector on the network has an upgrade available to bring it current. Depending on the current collector version, the severity of the banner will change and appropriate alert message is displayed. Click the **Email** icon, to receive the list of collector details.
- The name of the active screen (in example, Manage Users).
- The Help icon to view the respective help file.
- Refresh icon to refresh the data grid.

Left Navigation Pane

Use the Data Filters at the top of the left navigation pane in order to set up and customize the data that displays in the reports. You can customize, or select, based on customers, and inventories.

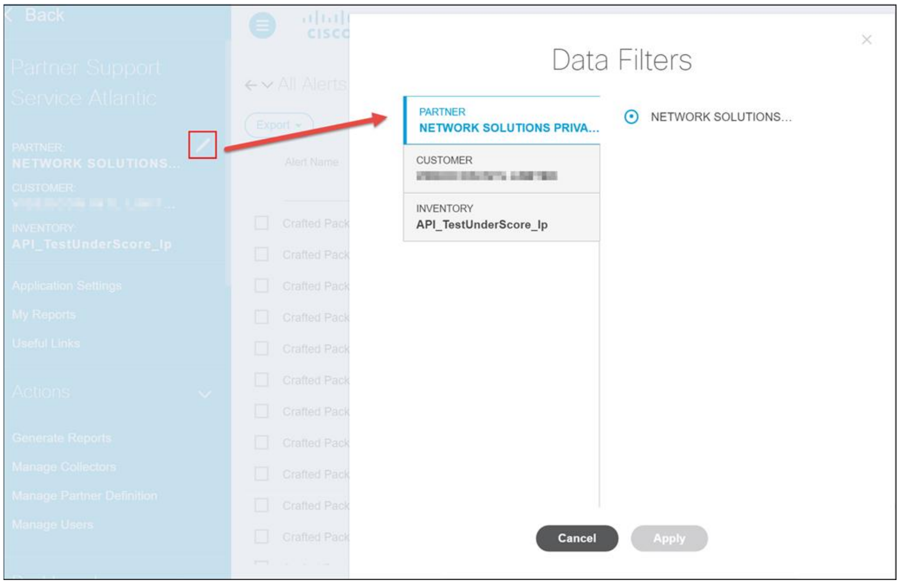
Note At the top of the left navigation pane, the name of the Cisco service that is currently in use is displayed. In this case, Partner Support Service. If entitled, you are able to switch to view other Cisco Service portals by using the Back arrow.

This section describes how to set up and customize the portal and related components:

- Data Filters
- Application Settings
- My Reports
- Useful Links
- Actions
- Dashboards
- Library

Data Filters

The partner, selected customer(s), and inventory (ies), are displayed beneath the service name. The Data Filters provide a way to change the amount of data you see at a very high-level. Click the pencil icon in the Left Navigation Pane (LNP) as highlighted in the snapshot.



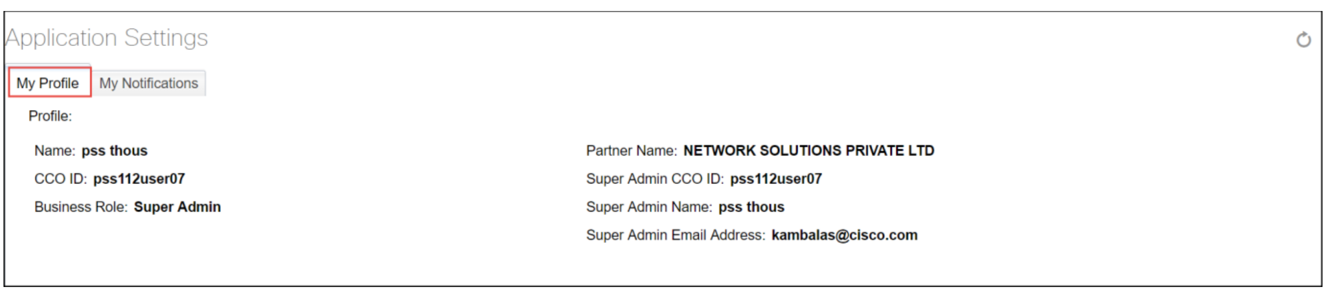
The Data Filter has several left pane tabs, which filters the data in the following ways:

- The first tab identifies the partner company, whose data you are entitled to use.
- The second tab lets you select one or more customers for whom you wish to view in the reports.
- The third tab lets you select one or more inventories for the selected customer(s).

Application Settings

Each logged in user can view their profile and also set the alert notification settings. It consists of two tabs:

- **My Profile** – This tab provides the details of your profile and include: the business role assigned to you, the customers to which you have access, and the role you have for each customer. Plus, the contact information of the Super Administrator – Name, Cisco.com ID, and email address.



Note My Profile tab only displays information for the logged in user after an inventory collection has been uploaded and processed for a customer to which that user has been associated.

- **My Notifications** - Use this tab to set to receive alerts and system messages from the portal system. You will receive notification of all the alerts that are newly uploaded and provides a cumulative count of all alerts and devices.

  By default, you will receive a notifications on the email address associated with your CCO ID.

Mon 07-03-2016 14:40

se-notify(mailer list)

Platform Notification

To <customeremailid>

Hello <Customer Name>

Alerts have been discovered for Entitled Company **<Company Name>** and Inventory **<Inventory Name>**

Table below displays number of Product Alerts with uploaded inventory:

Total Number of Hardware EOX : 5516256
Total Number of Software EOX : 8340096
Total Number of Field Notices : 4796384
Total Number of PSIRTS : 179799872
Total Number of Intellishield Alerts : 149645760

Total Number of devices(Chassis and Card) having Product Alerts with uploaded inventory:

Total Number of devices having Hardware EOX : 4659
Total Number of devices having Software EOX : 7034
Total Number of devices having Field Notice Alerts : 4050
Total Number of devices having PSIRTS Alerts : 5628
Total Number of devices having Intellishield Alerts : 5628

Please visit https://tools.cisco.com/csp for viewing alerts information.
This message was generated automatically. Please do not reply. For information or assistance, please visit one of the web locations shown in the email body or http://www.cisco.com.

Regards,
Cisco.
For corporate legal information please click here:

http://www.cisco.com/web/about/doing_business/legal/cri/index.html

If you do not wish to receive alert notifications, select **No** from the drop-down and click **Save**.

My Reports

The My Reports page shows a list of reports you recently requested from the Generate Reports page.

- Click the report type hyperlink (XLS or PDF) to download and view the associated report.
- If a report you requested is not visible in My Reports, click the refresh icon.
- When the report type appears in black, the report is currently being processed or there is no data available to view.
- Please access your generated reports as soon as possible. Cisco may retain an offline report for up to 8 days. You can request to have a report

Useful Links

The Useful Links page contains links to resources for:

- Training (such as how-to videos, links to this guide and PSS Release Notes)
- Partners
- Support (including tools, Partner Community and PSS Support Community)
- Quote, order and contract management
- CSPC Collector Center
- Account management
- Partner Support Service community

Actions

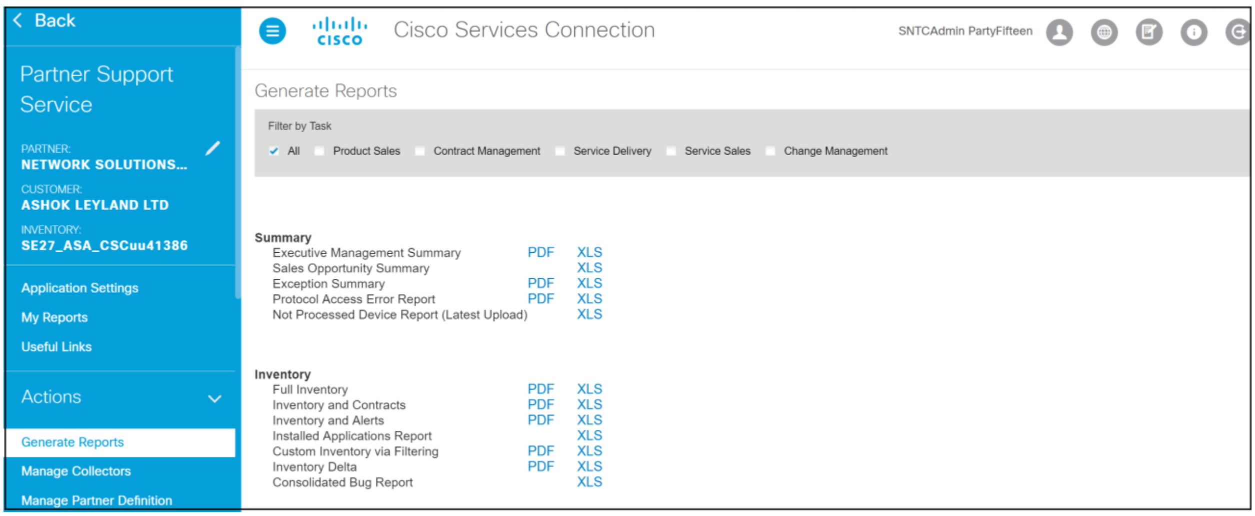
Each user is assigned a role for accessing customer data on the PSS portal:

- A **Super Administrator** maintains the Partner Definition of the customer contracts that will be managed with PSS Cisco services and is automatically registered as a Partner Administrator; enabling immediate user registrations and appears in the Manage Users list as a Partner Administrator.
- A **Partner Administrator** has access to all the functions in the PSS portal for all customers included in the Partner Definition from registering users on the portal, to running reports and managing Collectors.
- A **Partner User** has access to all PSS portal functions except Manage Users for all customers or a subset of the customers as set up by the Partner Administrator.

Generate Reports

Provides a list of all downloadable reports that can be generated and lets you select the format (PDF, XLS) to generate the report. The list of reports can be filtered by Task. When you select a task, only the reports most commonly used for those tasks will be highlighted. Although the remaining reports are greyed out, you can still generate the report.

When you click the XLS or PDF link to generate the report you will be prompted to select a single customer inventory.



Each report is filtered by task – Product Sales, Contract Management, Service Delivery, Service Sales, and Change Management.

Task	Reports
All	All reports in each category – Summary, Inventory, Contracts, Alerts and Assessment
Product Sales	Executive Management Summary
	Not Processed Device Report
	Uncovered Device Report
Contract Management	Inventory and Contracts
	Uncovered Device Report
Service Delivery	Full Inventory

	Alerts
Service Sales	Sales Opportunity Summary
	Uncovered Device Report
Change Management	Not Processed Device Report
	Uncovered Device Report

Types of Category Reports:

- **Summary** – Lists the various device reports for sales and management. If items were not processed, then the Not Processed Device Report can be generated to see a listing of Chassis and Cards that were not processed.
- **Inventory** – Lists the various reports to support customer base and services. The inventory, contracts, alerts, and installed applications.
- **Consolidated Bug Report** – This report provides a consolidated view of the bugs that Cisco has correlated for each and every item in the selected customer inventory.
- **Contracts** – Lists the devices that do have coverage contract in the Uncovered Device Report.
- **Alerts** – Lists all the latest product alerts for given partner/customer/inventory or all by default in Alerts report.
- **Assessment**: Lists the current state of your devices and help you plan for technology upgrades in various reports. For more information on the Assessment reports, view the Network Assessment Report video.

Once the reports are generated, go to My Reports in left navigation pane and see the status.

Note Access your generated reports as soon as possible. Cisco may retain an offline report for up to 8 days. You can request to have a report re-generated at any time.

Note For reports that are listed in the following tables, the Contract Status, Contract Start Date and Contract End Date heading refer to Coverage Status, Coverage Start Date and Coverage End Date.

Report Name	XLS/PDF File Name of the Report	Current Column Name	Actual Reference
Custom Inventory via Filtering	Custom Inventory	Contract Status	Coverage Status
		Contract Start Date	Coverage Start Date
		Contract End Date	Coverage End Date
Full Inventory	Custom Inventory	Contract Status	Coverage Status
		Contract Start Date	Coverage Start Date
		Contract End Date	Coverage End Date
Inventory and Contract	Custom Inventory	Contract Status	Coverage Status
		Contract Start Date	Coverage Start Date
		Contract End Date	Coverage End Date

Content Area Components

The Content Area displays the report currently selected in the Navigation Pane. When the view options menu is visible in a report, use it to toggle between table view, chart view, and billboard view, respectively. The next several sections identify the components of each view:

- Table Data View and Components
- Chart View and Components
- Billboard View and Components

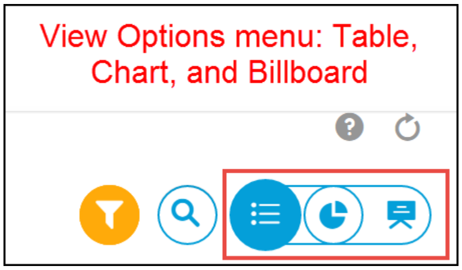
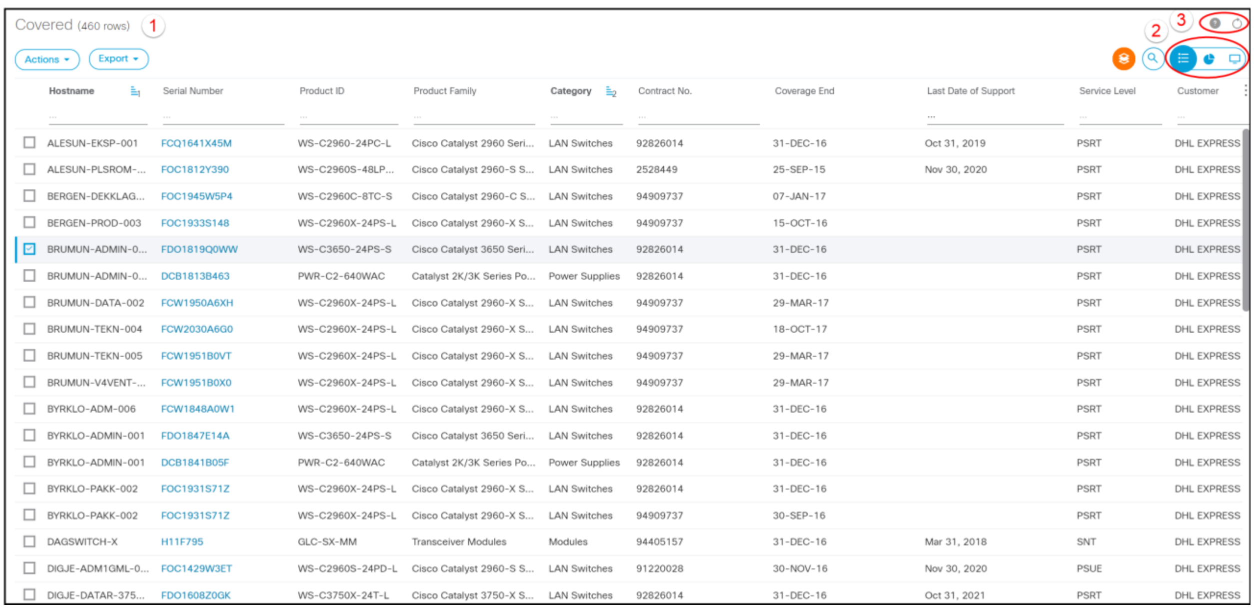


Table Data View and Components

This section identifies and describes the key components of the Table data view, the most common view when reviewing reports.



Hostname	Serial Number	Product ID	Product Family	Category	Contract No.	Coverage End	Last Date of Support	Service Level	Customer
ALESUN-EKSP-001	FCQ1641X45M	WS-C2960-24PC-L	Cisco Catalyst 2960 Seri...	LAN Switches	92826014	31-DEC-16	Oct 31, 2019	PSRT	DHL EXPRESS
ALESUN-PLSROM-...	FOC1812Y390	WS-C2960S-48LP...	Cisco Catalyst 2960-S S...	LAN Switches	2528449	25-SEP-15	Nov 30, 2020	PSRT	DHL EXPRESS
BERGEN-DEKKLAG...	FOC1945W5P4	WS-C2960C-8TC-S	Cisco Catalyst 2960-C S...	LAN Switches	94909737	07-JAN-17		PSRT	DHL EXPRESS
BERGEN-PROD-003	FOC1933S148	WS-C2960X-24PS-L	Cisco Catalyst 2960-X S...	LAN Switches	94909737	15-OCT-16		PSRT	DHL EXPRESS
BRUMUN-ADMIN-0...	FDO1819Q0WW	WS-C3650-24PS-S	Cisco Catalyst 3650 Seri...	LAN Switches	92826014	31-DEC-16		PSRT	DHL EXPRESS
BRUMUN-ADMIN-0...	DCB1813B463	PWR-C2-640WAC	Catalyst 2K/3K Series Po...	Power Supplies	92826014	31-DEC-16		PSRT	DHL EXPRESS
BRUMUN-DATA-002	FCW1950A6XH	WS-C2960X-24PS-L	Cisco Catalyst 2960-X S...	LAN Switches	94909737	29-MAR-17		PSRT	DHL EXPRESS
BRUMUN-TEKN-004	FCW2030A6G0	WS-C2960X-24PS-L	Cisco Catalyst 2960-X S...	LAN Switches	94909737	18-OCT-17		PSRT	DHL EXPRESS
BRUMUN-TEKN-005	FCW1951B0VT	WS-C2960X-24PS-L	Cisco Catalyst 2960-X S...	LAN Switches	94909737	29-MAR-17		PSRT	DHL EXPRESS
BRUMUN-V4VENT-...	FCW1951B0X0	WS-C2960X-24PS-L	Cisco Catalyst 2960-X S...	LAN Switches	94909737	29-MAR-17		PSRT	DHL EXPRESS
BYRKLO-ADM-006	FCW1848A0W1	WS-C2960X-24PS-L	Cisco Catalyst 2960-X S...	LAN Switches	92826014	31-DEC-16		PSRT	DHL EXPRESS
BYRKLO-ADMIN-001	FDO1847E14A	WS-C3650-24PS-S	Cisco Catalyst 3650 Seri...	LAN Switches	92826014	31-DEC-16		PSRT	DHL EXPRESS
BYRKLO-ADMIN-001	DCB1841B05F	PWR-C2-640WAC	Catalyst 2K/3K Series Po...	Power Supplies	92826014	31-DEC-16		PSRT	DHL EXPRESS
BYRKLO-PAKK-002	FOC1931S71Z	WS-C2960X-24PS-L	Cisco Catalyst 2960-X S...	LAN Switches	92826014	31-DEC-16		PSRT	DHL EXPRESS
BYRKLO-PAKK-002	FOC1931S71Z	WS-C2960X-24PS-L	Cisco Catalyst 2960-X S...	LAN Switches	94909737	30-SEP-16		PSRT	DHL EXPRESS
DAGSWITCH-X	H11F795	GLC-SX-MM	Transceiver Modules	Modules	94405157	31-DEC-16	Mar 31, 2018	SNT	DHL EXPRESS
DIGJE-ADM1GML-0...	FOC1429W3ET	WS-C2960S-24PD-L	Cisco Catalyst 2960-S S...	LAN Switches	91220028	30-NOV-16	Nov 30, 2020	PSUE	DHL EXPRESS
DIGJE-DATAR-375...	FDO1608Z0GK	WS-C3750X-24T-L	Cisco Catalyst 3750-X S...	LAN Switches	92826014	31-DEC-16	Oct 31, 2021	PSRT	DHL EXPRESS

The top of the table 1 has the report name and in parenthesis indicates the number of items listed in the current view.

Column filters are displayed below each column name. When you enter search criteria text you want to filter on, the filtering is performed only on the content in that specific column. To clear a filter, hover over the search criteria and click the 'x' in the right side of the filter box.

Note The search criteria text is not case sensitive and does not require a wildcard '*'.

The Action icon appears when you hover the mouse pointer on the left of each row, Click the action icon to view a list of actions available in the report. In the above snapshot, it shows a CSCC link that directs to the Cisco Service Contract

Center (CSCC) to view the contract details for one or more contracts by clicking the check-box to the left side of each device whose contract you want to review.

A column that is sorted has a triangle to the right of the column name [for example: Contract Number column as in snapshot]. An upward pointing triangle ▲ indicates the column content is sorted in an ascending order. A downward pointing triangle ▼ indicates the column content is sorted in a descending order.

Some table columns may not be visible in the current table if the table columns are hidden.

The content area components 2 (for example, table toolbar), which varies according to the type content pane. 3 displays the help icon and refresh icon while you hover the mouse over the report.

Chart View and Components

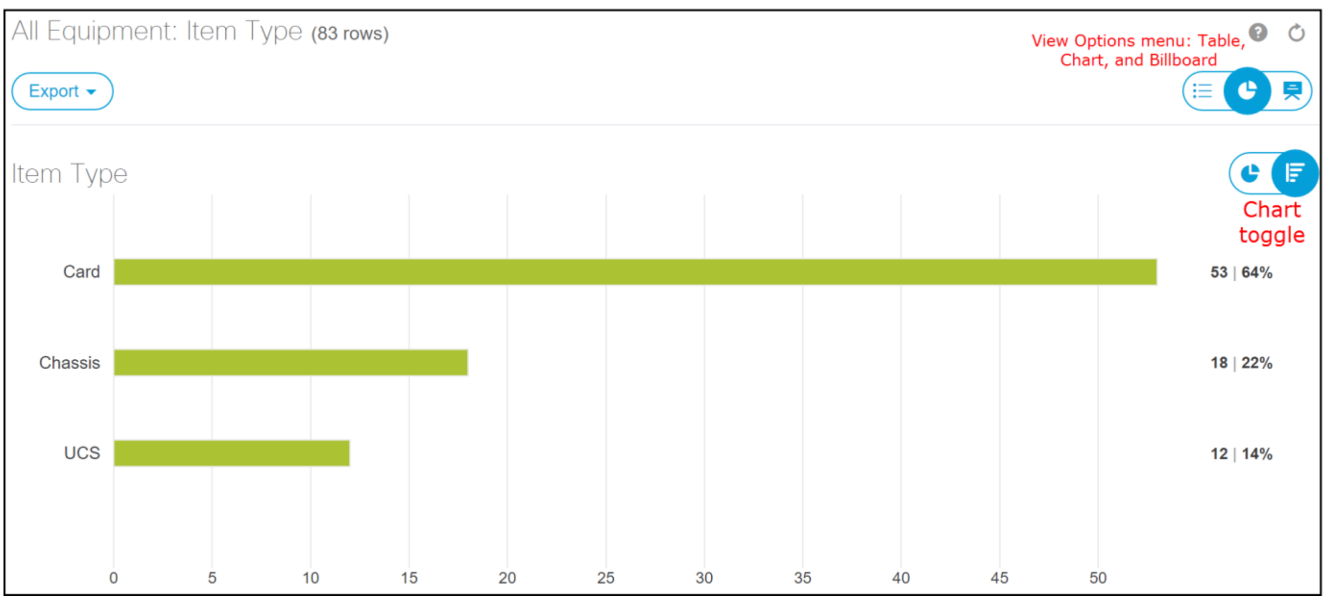
This section identifies the two types of charts, and describes the components in each one. To see a chart view of the data, perform the following steps:

- Click the View as Chart icon as highlighted in the snapshot.
- Select an option from the drop-down list (for example, Item Type). The chart data for the selected item appears.

Note The data in the drop-down list represents data from a specific column header in the table data (for example, Equipment Type). " View Chart By" options will be different for each library report.

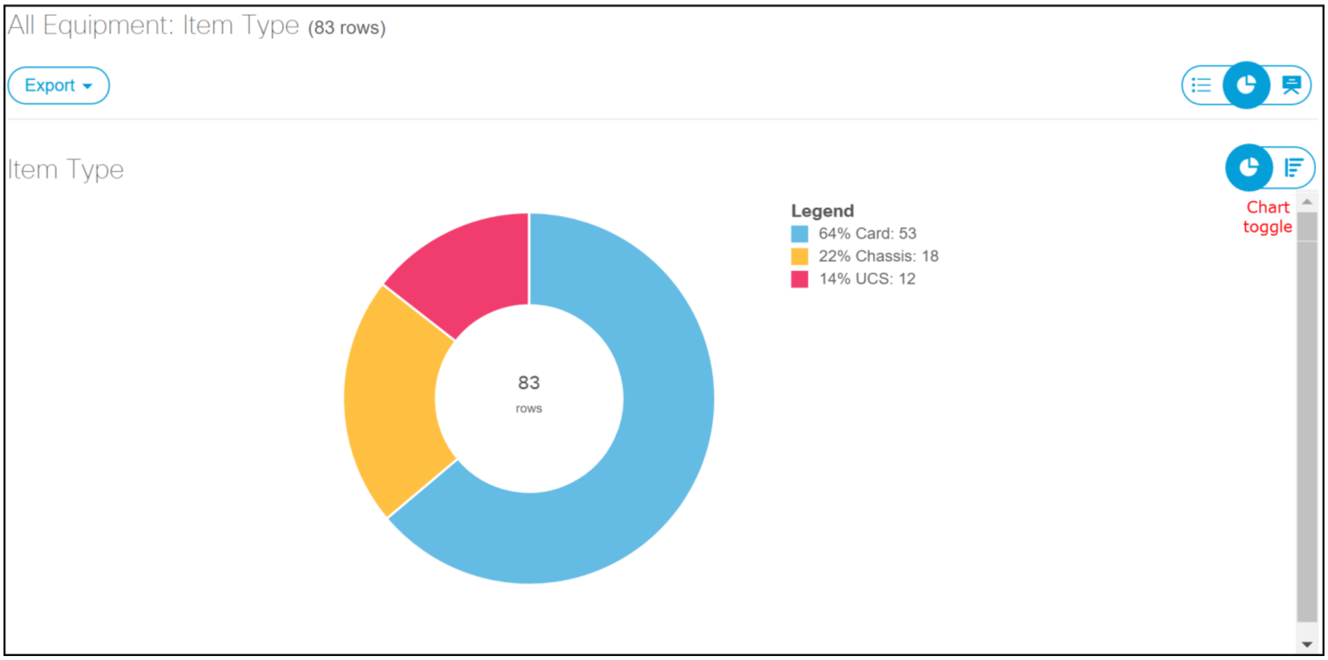
There are two types of charts and their related components are covered in the following areas:

Bar Chart Components: The bar chart reflects the data from the item previously selected in the chart drop-down list (in example, Item Type). The items in that drop-down list represent the names of column headings in the table.



The chart toggle lets you toggle between the pie chart and bar chart by clicking the respective icon in top-right corner of the Content Area. The pie chart icon is on the left, and the bar chart icon is on the right.

Pie Chart Components: The pie chart reflects the data from the item previously selected in the chart drop-down list. The items in that drop-down list represent the names of column headings in the table.

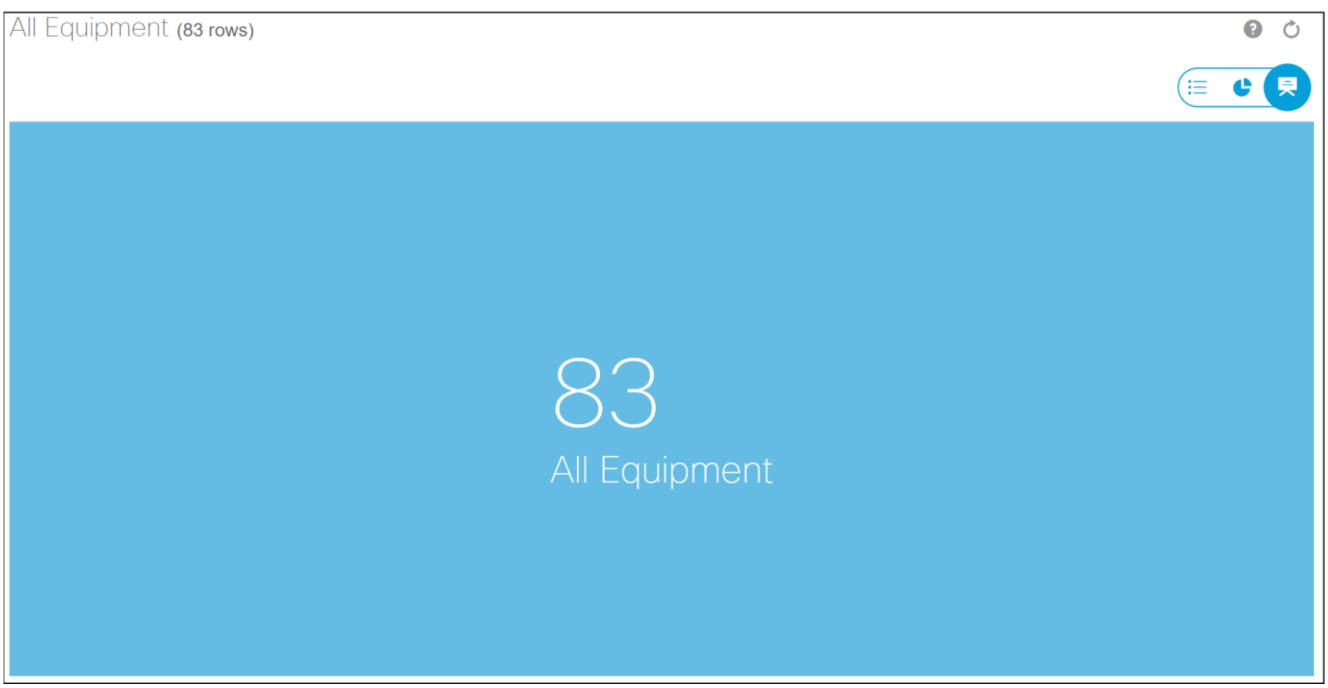


The chart toggle lets you switch between the pie chart and bar chart by clicking the respective icon  in top-right corner of the Content Area. The pie chart icon is on the left and the bar chart icon is on the right. The color legend correlates the list data with each specific section of the pie.

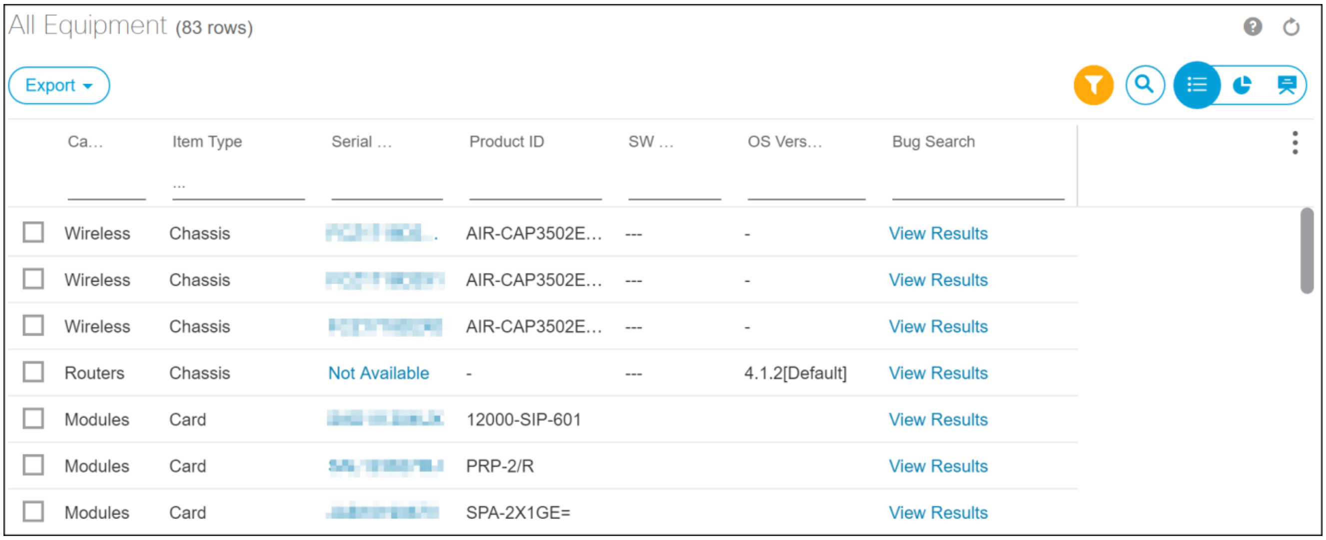
When you hover over a specific section of the pie chart, the corresponding list information is highlighted (for example, switch). Click to display a filtered view displaying only the selected information.

Billboard View and Components

The information in billboard view provides a high-level summary of the report and indicates the report name and the *number of items* in the report (in example, All Equipment (83)). 



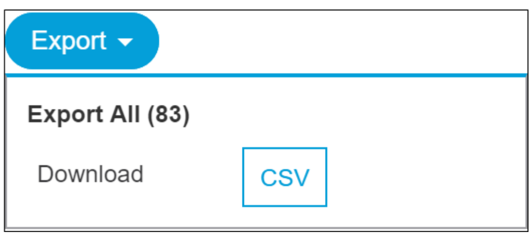
- When you move your mouse over the Billboard Content Area, the background turns blue; indicating a toggle to the table data view is active. Click to go to table data view.



- To return to Billboard view, click the Billboard icon in the table view.

Content Pane Toolbar

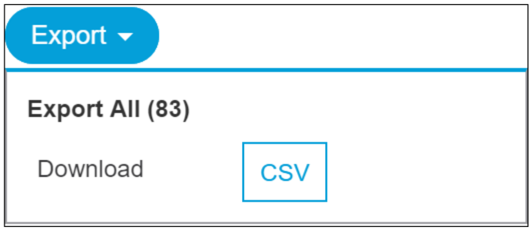
The content pane toolbar is present in all the three content area components (table, chart, and billboard). This toolbar is located in the top right corner of the respective content area component and will have some or all of the following functions:



- Help Icon provides context sensitive usage instructions and links to short training videos and documentation specific to the report currently in view.
- Refresh the report .

Export Menu

Exporting data from Cisco Services Connection gives you the ability to include the report data in presentations and reports for your customers and other stakeholders. In table view, the Export option will export the report to a CSV format. In chart view, the Export option will export the chart to a PNG format graphic. To export the report, perform the following steps:



- Click the **Export** menu drop-down list, the available download option appears.
- Select **Download** to generate of the associated file.

Note The **Export** feature is limited to 65,532 records per export for CSV files. If an inventory contains more records, consider filtering the report by Item Type and then exporting a report for each Item Type.

Working with Reports

This section covers the following areas related to reports:

- Viewing Reports
- Working with Columns
- Saving and Exporting a Smart Report
- Drilling into Report Data
- Filtering

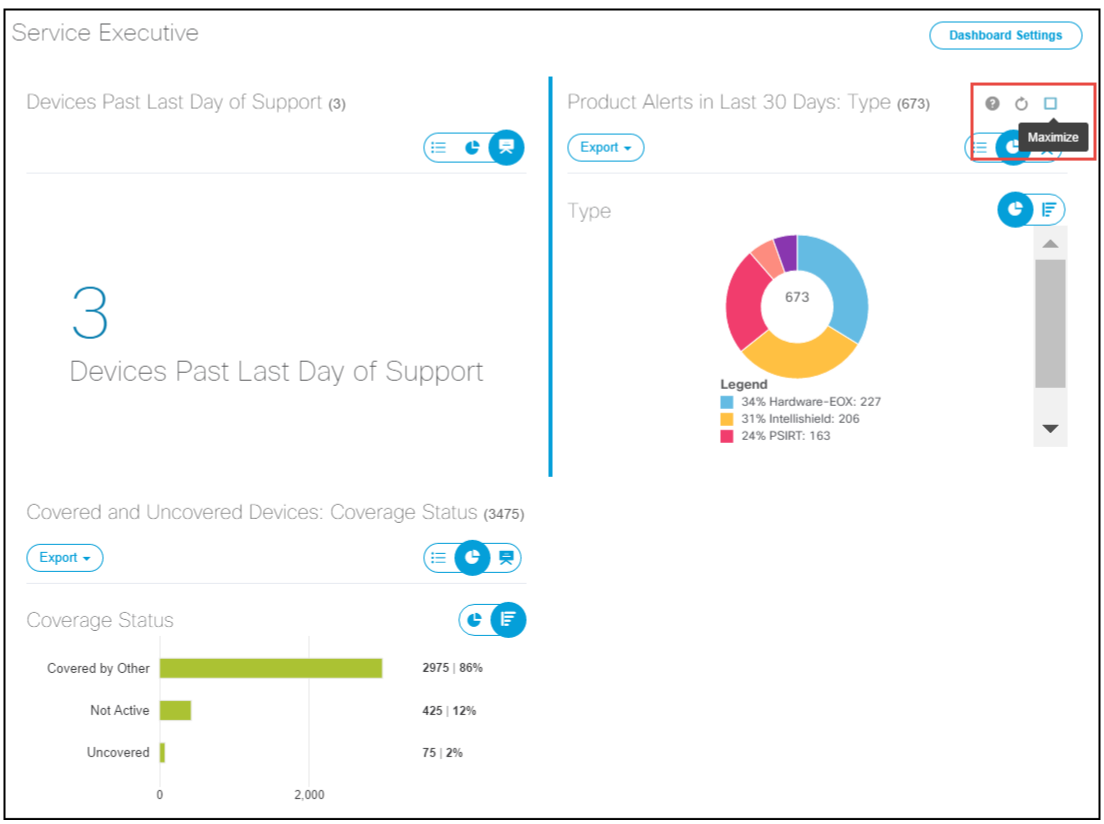
Viewing Reports

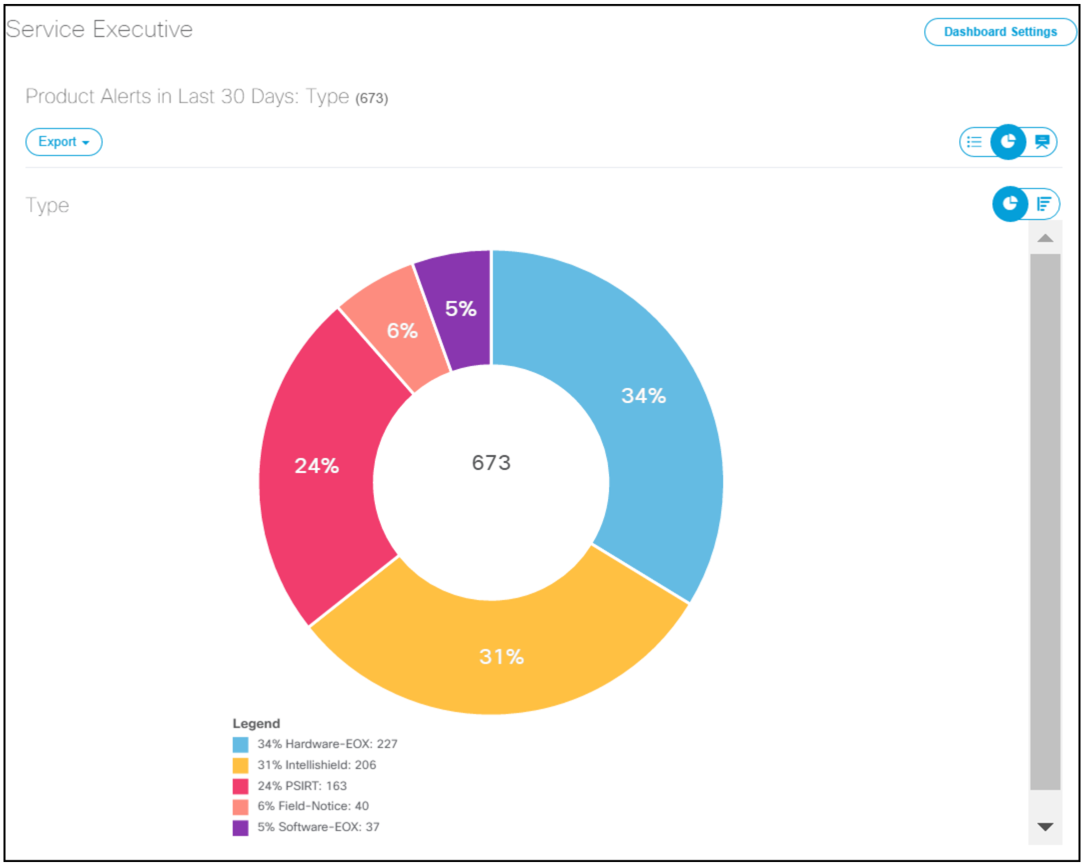
When you are viewing reports you can use the following viewing functions:

Note Maximizing and Restoring Reports options are available for dashlets in the dashboards.

Maximize and Restore Dashboard Views

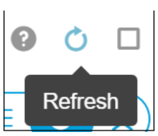
When you are viewing a report in a dashboard, you can maximize (icon) and minimize (icon) the report for better viewing:

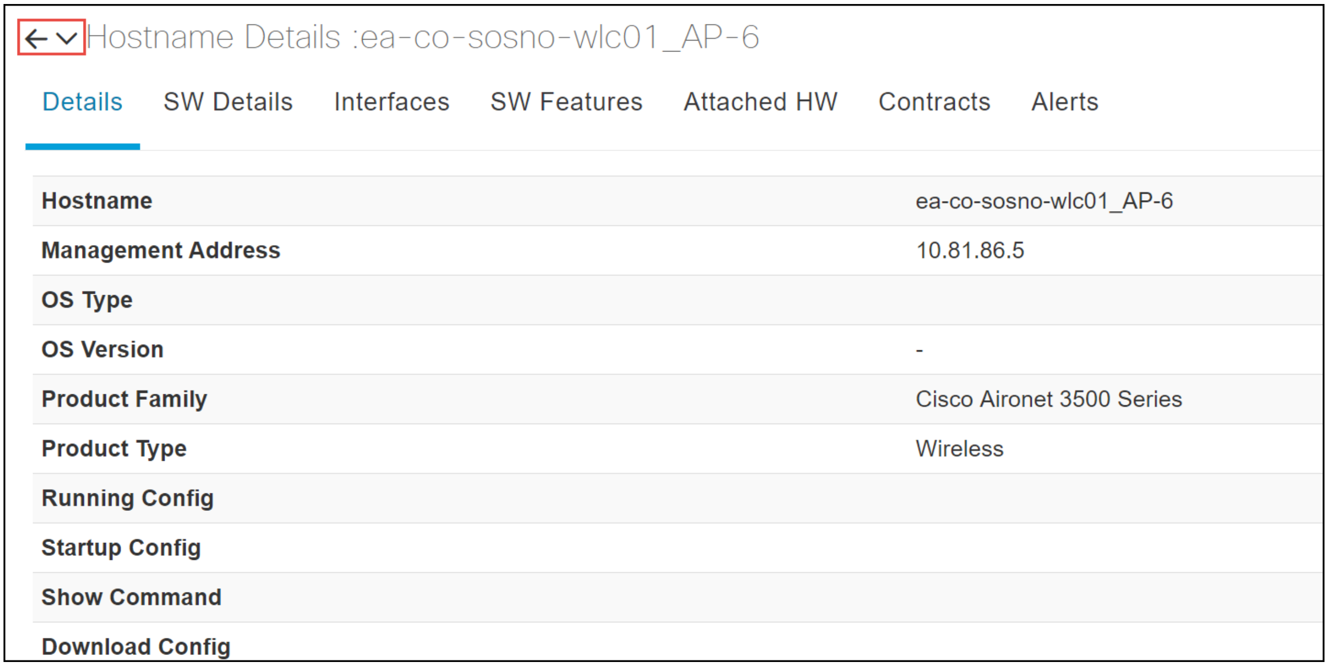




Refreshing Reports

Refresh an opened report to update the status of all the items in the report, by clicking the **Refresh** button.





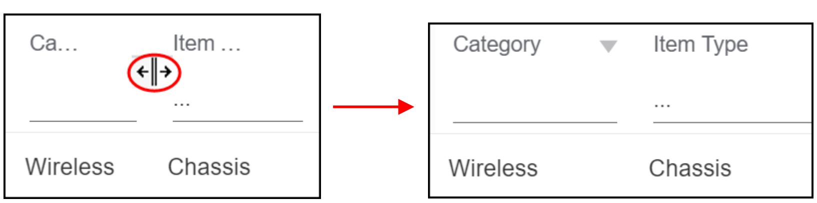
Working with Columns

When adjusting report columns, your report preferences are retained automatically in your profile. Modifications such as selected columns, order of column placements, and column size are retained across sessions until you change them. Filters and sort sequences, however, are retained only while the current session is open. This section covers how to perform the following column tasks:

- Sizing Columns
- Moving Columns
- Displaying and Hiding Columns

Sizing Columns

Columns can be sized (stretched or shrunken) by dragging a selected column edge to the left or to the right. To resize a column header perform the following steps:

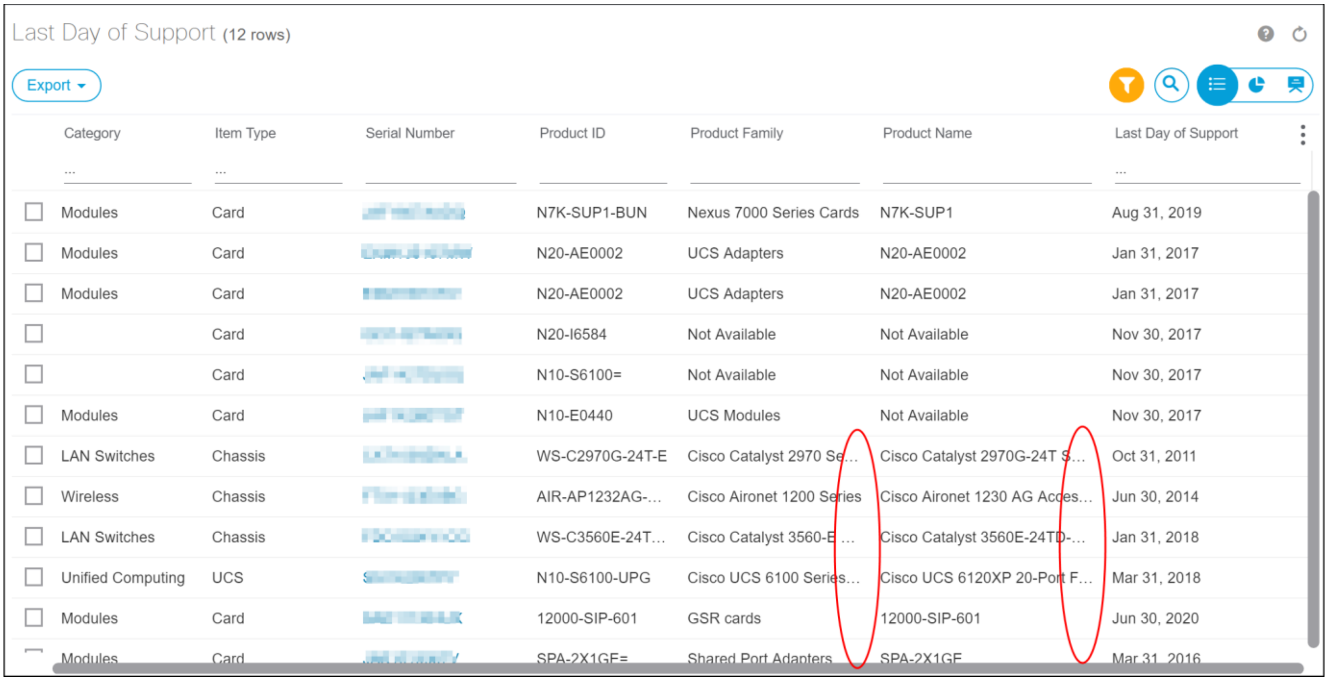


- Move your mouse to the column edge until the sizing cursor appears; press and hold the left-mouse button.
- While holding down the left-mouse button, drag the mouse to the left or right to stretch or shrink the column accordingly.
- When the column size is correct, release the left-mouse button.

Notes about column sizing:

- Dragging only resizes the column immediately to the left of the cursor.

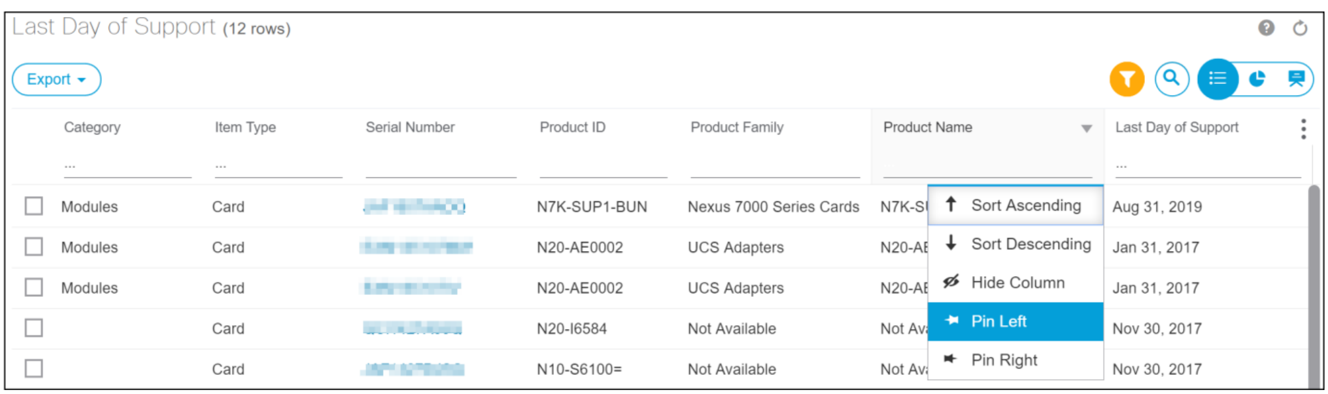
- All columns to the right are moved to the right or left (as the resized column is stretched or shrunken) to accommodate the resized column.
- If the column is stretched and causes the columns to the right to extend beyond the boundaries of the table, a horizontal scroll bar appears.
- If the column is shrunken, extra width is allocated to the last column.



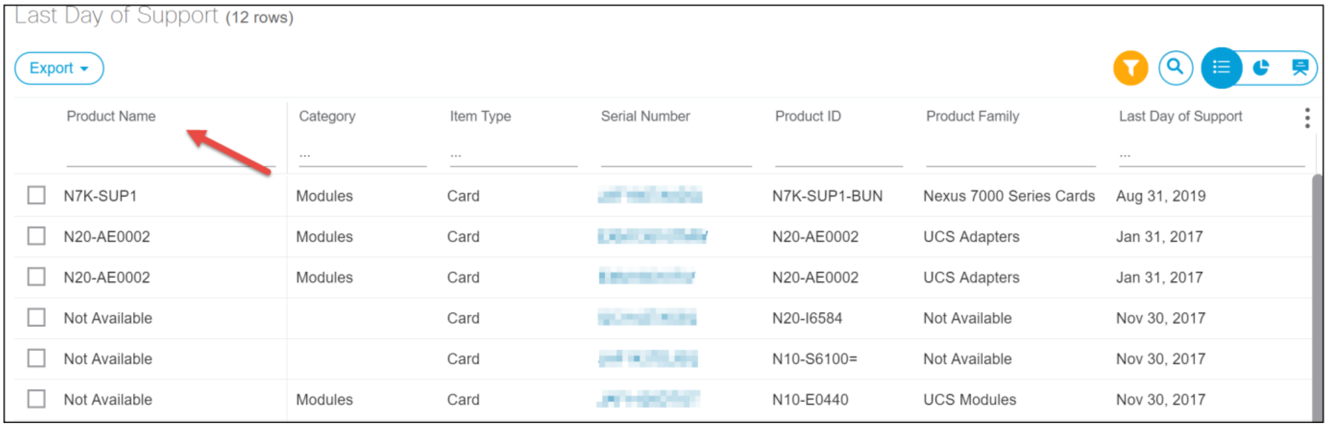
Note When you resize a column too small for the existing content, ellipses (...) are displayed to indicate that there is more information available than is currently being displayed.

Moving Columns

You can drag-and-drop the columns to your preferred position. Additionally, you can choose *Pin Left* or *Pin Right* in order to move the column to the extreme left or right.



- Select either one of the following options:
  - Pin Left: Moves the column to the left side of the table view.
  - Pin Right: Moves the column to the right side of the table view.



Last Day of Support (12 rows)

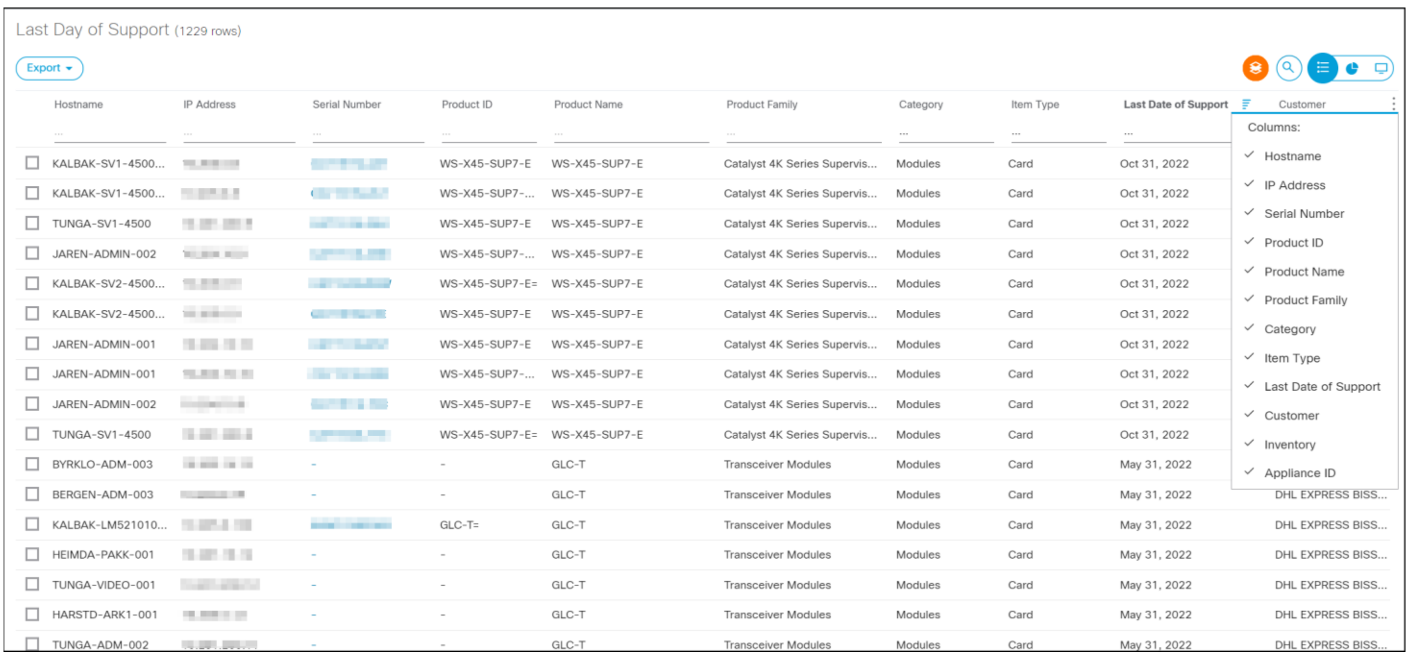
Export

	Product Name	Category	Item Type	Serial Number	Product ID	Product Family	Last Day of Support
☐	N7K-SUP1	Modules	Card	[illegible]	N7K-SUP1-BUN	Nexus 7000 Series Cards	Aug 31, 2019
☐	N20-AE0002	Modules	Card	[illegible]	N20-AE0002	UCS Adapters	Jan 31, 2017
☐	N20-AE0002	Modules	Card	[illegible]	N20-AE0002	UCS Adapters	Jan 31, 2017
☐	Not Available		Card	[illegible]	N20-I6584	Not Available	Nov 30, 2017
☐	Not Available		Card	[illegible]	N10-S6100=	Not Available	Nov 30, 2017
☐	Not Available	Modules	Card	[illegible]	N10-E0440	UCS Modules	Nov 30, 2017

- The Product Name column is moved to the left as shown in the image above.

Displaying and Hiding Columns

Columns can be added or hidden in the current table view. To add or hide a column from the table view, perform the following steps:



Last Day of Support (1229 rows)

Export

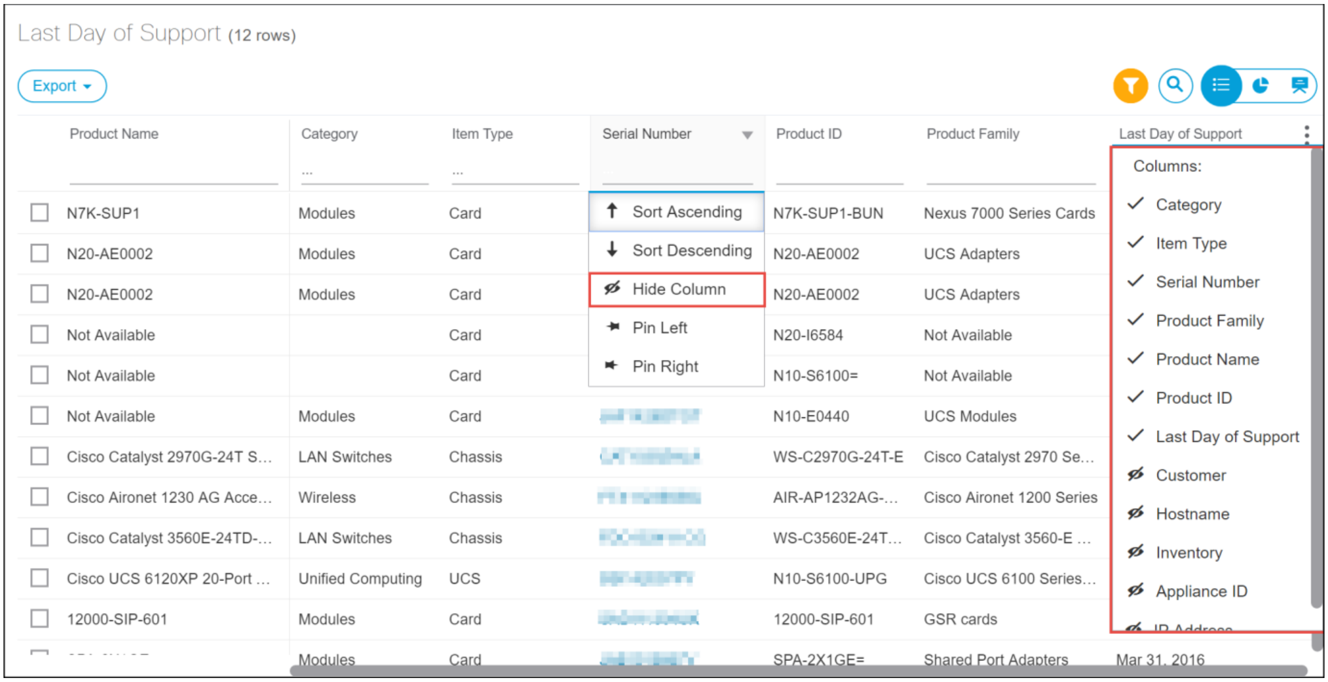
	Hostname	IP Address	Serial Number	Product ID	Product Name	Product Family	Category	Item Type	Last Date of Support	Customer
☐	KALBAK-SV1-4500...	[illegible]	[illegible]	WS-X45-SUP7-E	WS-X45-SUP7-E	Catalyst 4K Series Supervis...	Modules	Card	Oct 31, 2022	
☐	KALBAK-SV1-4500...	[illegible]	[illegible]	WS-X45-SUP7-...	WS-X45-SUP7-E	Catalyst 4K Series Supervis...	Modules	Card	Oct 31, 2022	
☐	TUNGA-SV1-4500	[illegible]	[illegible]	WS-X45-SUP7-E	WS-X45-SUP7-E	Catalyst 4K Series Supervis...	Modules	Card	Oct 31, 2022	
☐	JAREN-ADMIN-002	[illegible]	[illegible]	WS-X45-SUP7-...	WS-X45-SUP7-E	Catalyst 4K Series Supervis...	Modules	Card	Oct 31, 2022	
☐	KALBAK-SV2-4500...	[illegible]	[illegible]	WS-X45-SUP7-E=	WS-X45-SUP7-E	Catalyst 4K Series Supervis...	Modules	Card	Oct 31, 2022	
☐	KALBAK-SV2-4500...	[illegible]	[illegible]	WS-X45-SUP7-E	WS-X45-SUP7-E	Catalyst 4K Series Supervis...	Modules	Card	Oct 31, 2022	
☐	JAREN-ADMIN-001	[illegible]	[illegible]	WS-X45-SUP7-E	WS-X45-SUP7-E	Catalyst 4K Series Supervis...	Modules	Card	Oct 31, 2022	
☐	JAREN-ADMIN-001	[illegible]	[illegible]	WS-X45-SUP7-...	WS-X45-SUP7-E	Catalyst 4K Series Supervis...	Modules	Card	Oct 31, 2022	
☐	JAREN-ADMIN-002	[illegible]	[illegible]	WS-X45-SUP7-E	WS-X45-SUP7-E	Catalyst 4K Series Supervis...	Modules	Card	Oct 31, 2022	
☐	TUNGA-SV1-4500	[illegible]	[illegible]	WS-X45-SUP7-E=	WS-X45-SUP7-E	Catalyst 4K Series Supervis...	Modules	Card	Oct 31, 2022	
☐	BYRKLO-ADM-003	[illegible]	-	-	GLC-T	Transceiver Modules	Modules	Card	May 31, 2022	
☐	BERGEN-ADM-003	[illegible]	-	-	GLC-T	Transceiver Modules	Modules	Card	May 31, 2022	DHL EXPRESS BISS...
☐	KALBAK-LM521010...	[illegible]	[illegible]	GLC-T=	GLC-T	Transceiver Modules	Modules	Card	May 31, 2022	DHL EXPRESS BISS...
☐	HEIMDA-PAKK-001	[illegible]	-	-	GLC-T	Transceiver Modules	Modules	Card	May 31, 2022	DHL EXPRESS BISS...
☐	TUNGA-VIDEO-001	[illegible]	-	-	GLC-T	Transceiver Modules	Modules	Card	May 31, 2022	DHL EXPRESS BISS...
☐	HARSTD-ARK1-001	[illegible]	-	-	GLC-T	Transceiver Modules	Modules	Card	May 31, 2022	DHL EXPRESS BISS...
☐	TUNGA-ADM-002	[illegible]	-	-	GLC-T	Transceiver Modules	Modules	Card	May 31, 2022	DHL EXPRESS BISS...

Columns:
✓ Hostname
✓ IP Address
✓ Serial Number
✓ Product ID
✓ Product Name
✓ Product Family
✓ Category
✓ Item Type
✓ Last Date of Support
✓ Customer
✓ Inventory
✓ Appliance ID

1. Click the Select Columns icon (indicated by three vertical dots) to display or hide the list of available columns
2. Check the required columns to display in the table view. Column names that are not checked are currently not displayed in the table.

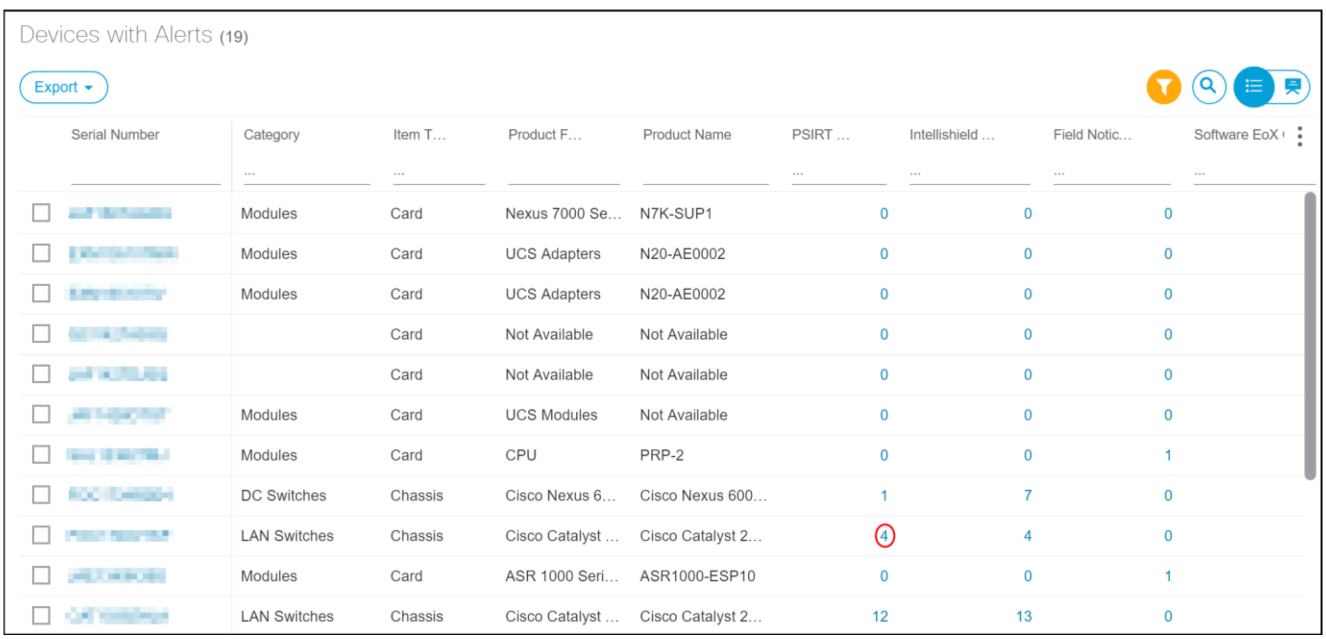
Note To hide a column from being viewed in the table, uncheck the elements of the column you want to hide.

- To remove the column from the view either uncheck from the list of columns or click the down arrow for the column that you want to remove and select **Hide Column**

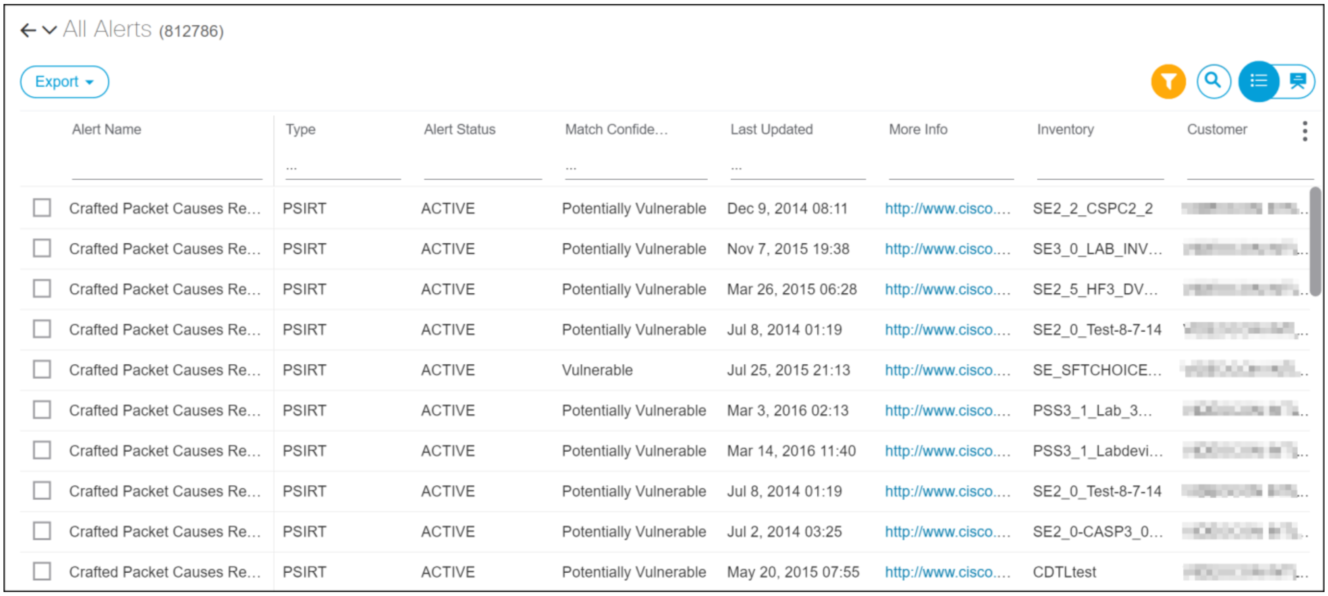


Drilling into Report Data

When data is displayed in the Content Area, quite often you are able to ‘drill down’ to get additional information. The term “drilling down” means to use the user interface to obtain more information about a specific item. Any item in a report that appears in blue will display more information when you click it. For example, on the Devices with Alerts report, there are several columns that list various types of alert counts. Perform the following steps to get additional information about a specific alert. Items that appear in blue are available to drill down.

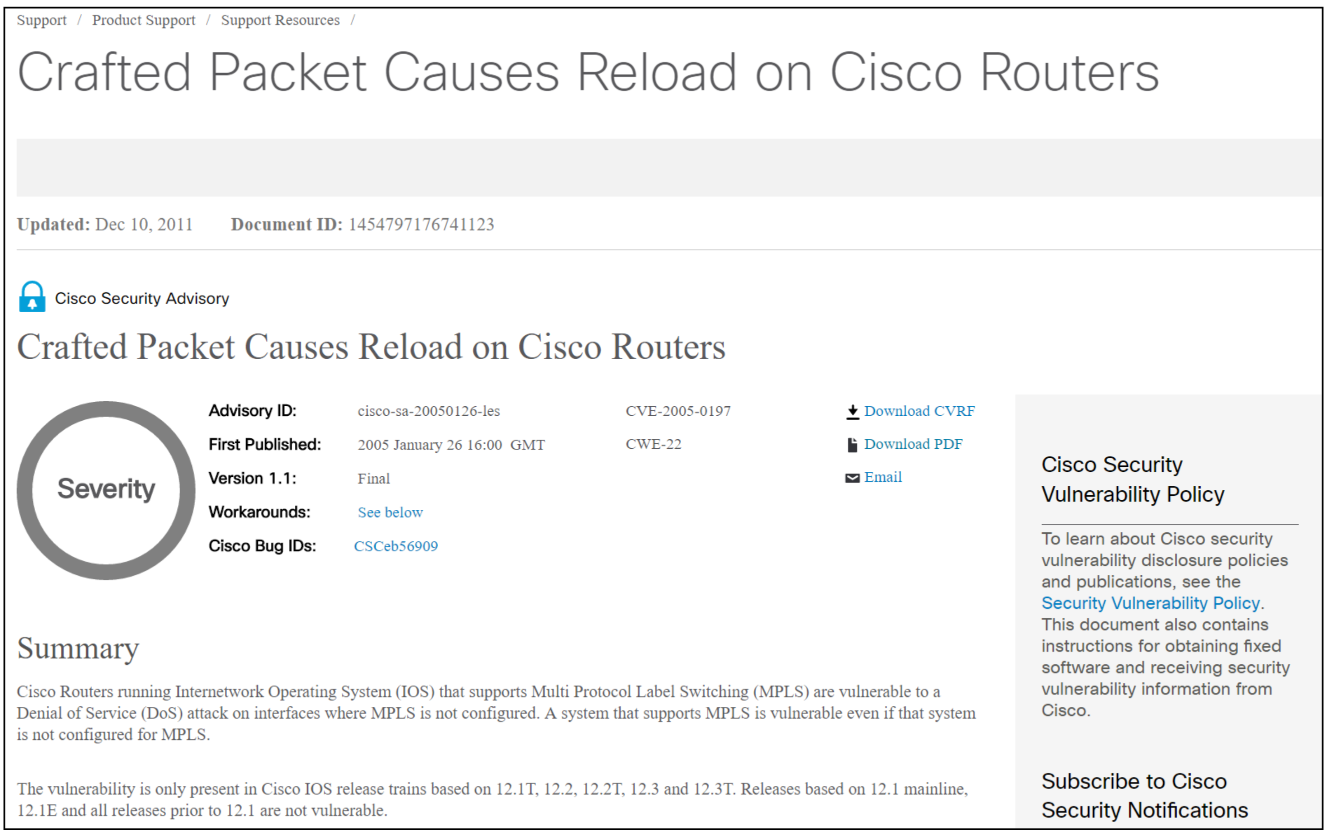


- If you want additional information about PSIRTs you can click the number 4 to see a list of the PSIRTs.



Alert Name	Type	Alert Status	Match Confide...	Last Updated	More Info	Inventory	Customer
Crafted Packet Causes Re...	PSIRT	ACTIVE	Potentially Vulnerable	Dec 9, 2014 08:11	http://www.cisco....	SE2_2_CSPC2_2	[illegible]
Crafted Packet Causes Re...	PSIRT	ACTIVE	Potentially Vulnerable	Nov 7, 2015 19:38	http://www.cisco....	SE3_0_LAB_INV...	[illegible]
Crafted Packet Causes Re...	PSIRT	ACTIVE	Potentially Vulnerable	Mar 26, 2015 06:28	http://www.cisco....	SE2_5_HF3_DV...	[illegible]
Crafted Packet Causes Re...	PSIRT	ACTIVE	Potentially Vulnerable	Jul 8, 2014 01:19	http://www.cisco....	SE2_0_Test-8-7-14	[illegible]
Crafted Packet Causes Re...	PSIRT	ACTIVE	Vulnerable	Jul 25, 2015 21:13	http://www.cisco....	SE_SFTCHOICE...	[illegible]
Crafted Packet Causes Re...	PSIRT	ACTIVE	Potentially Vulnerable	Mar 3, 2016 02:13	http://www.cisco....	PSS3_1_Lab_3...	[illegible]
Crafted Packet Causes Re...	PSIRT	ACTIVE	Potentially Vulnerable	Mar 14, 2016 11:40	http://www.cisco....	PSS3_1_Labdevi...	[illegible]
Crafted Packet Causes Re...	PSIRT	ACTIVE	Potentially Vulnerable	Jul 8, 2014 01:19	http://www.cisco....	SE2_0_Test-8-7-14	[illegible]
Crafted Packet Causes Re...	PSIRT	ACTIVE	Potentially Vulnerable	Jul 2, 2014 03:25	http://www.cisco....	SE2_0-CASP3_0...	[illegible]
Crafted Packet Causes Re...	PSIRT	ACTIVE	Potentially Vulnerable	May 20, 2015 07:55	http://www.cisco....	CDTLtest	[illegible]

- Click a URL in the **More Info** column to see additional data.



Support / Product Support / Support Resources /

Crafted Packet Causes Reload on Cisco Routers

Updated: Dec 10, 2011 **Document ID:** 1454797176741123

Cisco Security Advisory

Crafted Packet Causes Reload on Cisco Routers

Severity

Advisory ID: cisco-sa-20050126-les CVE-2005-0197 Download CVRF
First Published: 2005 January 26 16:00 GMT CWE-22 Download PDF
Version 1.1: Final Email
Workarounds: See below
Cisco Bug IDs: CSCeb56909

Summary

Cisco Routers running Internetwork Operating System (IOS) that supports Multi Protocol Label Switching (MPLS) are vulnerable to a Denial of Service (DoS) attack on interfaces where MPLS is not configured. A system that supports MPLS is vulnerable even if that system is not configured for MPLS.

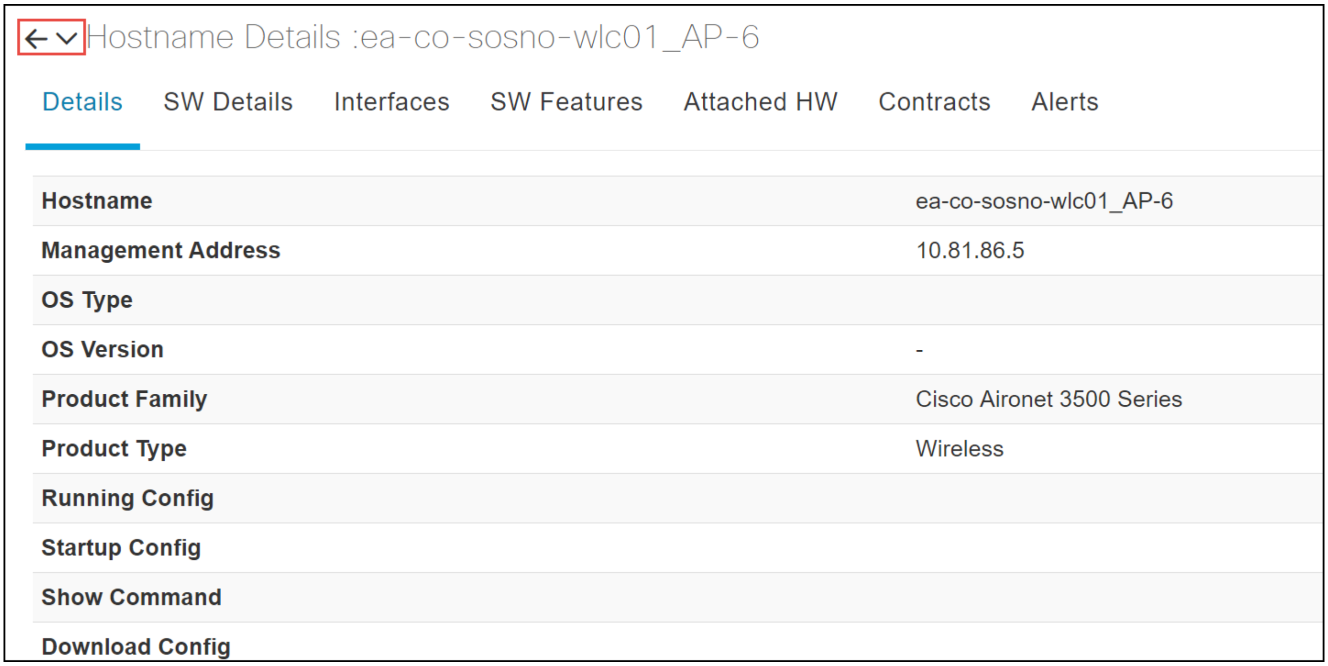
The vulnerability is only present in Cisco IOS release trains based on 12.1T, 12.2, 12.2T, 12.3 and 12.3T. Releases based on 12.1 mainline, 12.1E and all releases prior to 12.1 are not vulnerable.

Cisco Security Vulnerability Policy

To learn about Cisco security vulnerability disclosure policies and publications, see the Security Vulnerability Policy. This document also contains instructions for obtaining fixed software and receiving security vulnerability information from Cisco.

Subscribe to Cisco Security Notifications

- Data related to the selected PSIRT is displayed in a new window.
- In the grid, depending where you are in your navigation, you can navigate backwards using the previous-arrow or select specific previous screens using the down-arrow.



Filtering

Filters allow you to refine a report and reduce the amount of information displayed in the Content Area. There are many types of filters used in the reports. Some filters are used in many reports; some filters are used in only one or two reports.

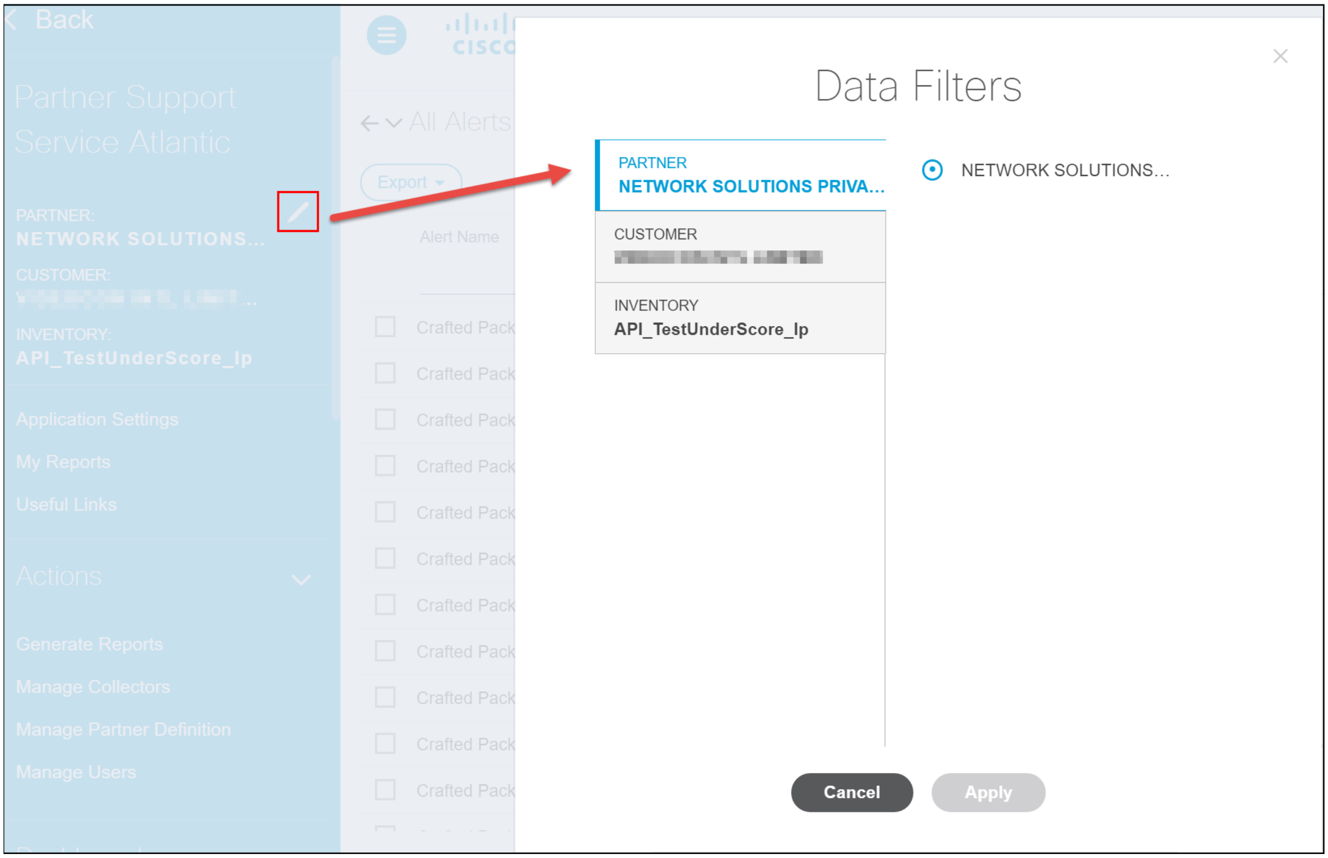
Note For those filters that are used by only one or two reports, the name of those report(s) that use that filter will be noted under the filter graphic and highlighted in blue.

There are several different ways to filter the data being displayed in the Content Area. This section describes the various functions that are available in the different filters.

- Data Filters
- Table Column Search Filters
- Chart Filters

Data Filters

Data Filters provide a way to change the amount of data you see at a very high-level. Click the pencil icon in the Left Navigation Pane (LNP) as highlighted in the snapshot. This Filter has several left pane tabs, which filters the data in the following ways:



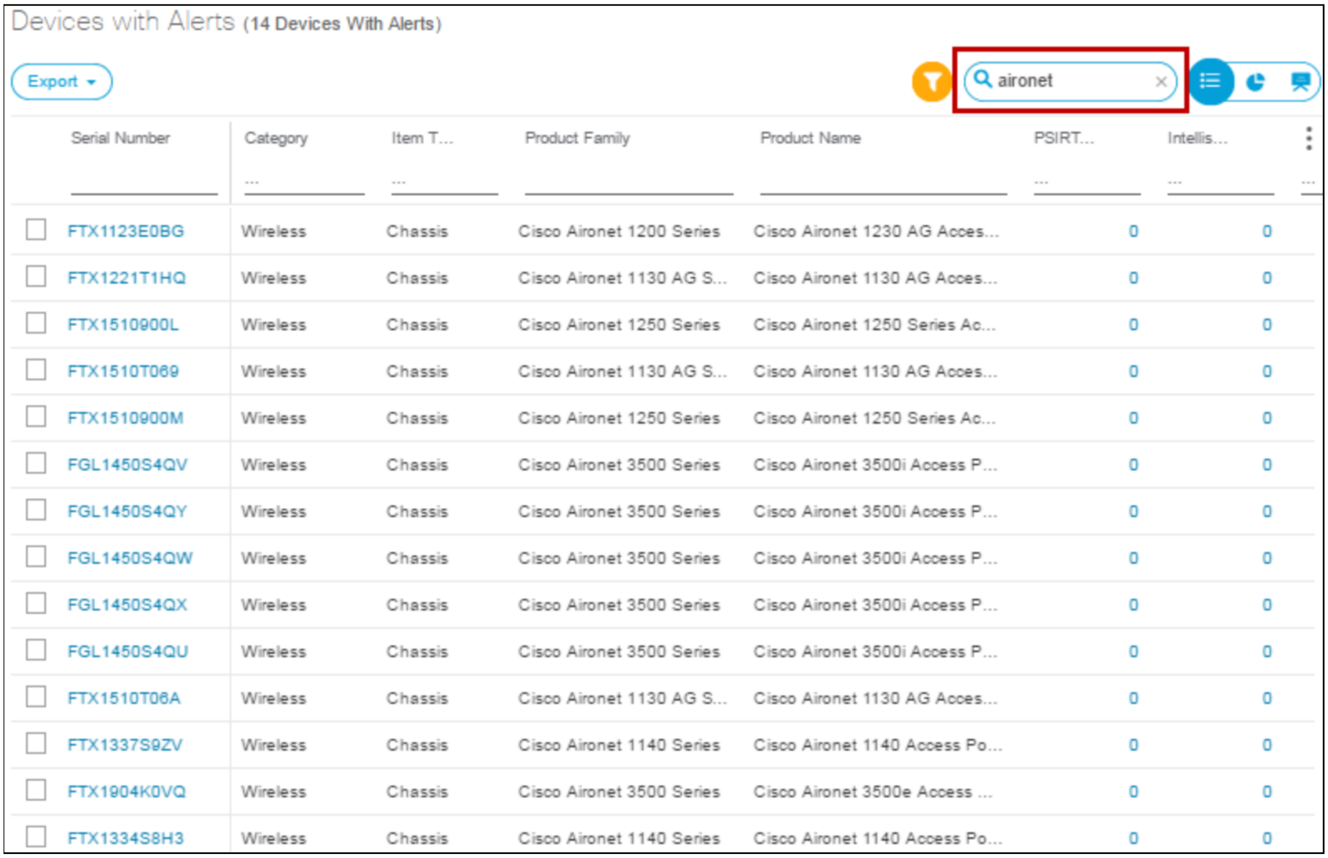
- The first tab identifies which partner company, whose data you are entitled to use.
- The second tab lets you select one or more customers for whom you wish to see the data / reports.
- The third tab lets you select one or more inventories for the selected customer(s).

Table Column Filters

In the table data view there is a search field under each column name. The search field is context sensitive, meaning the filter options are different depending on what column data is being displayed in that column. The next section describes the different types of table column search filters.

Search Filter

This type of filter lets you view all the data records (default), or display those records that match the search parameters.



Devices with Alerts (14 Devices With Alerts)

Export ▾ | aironet

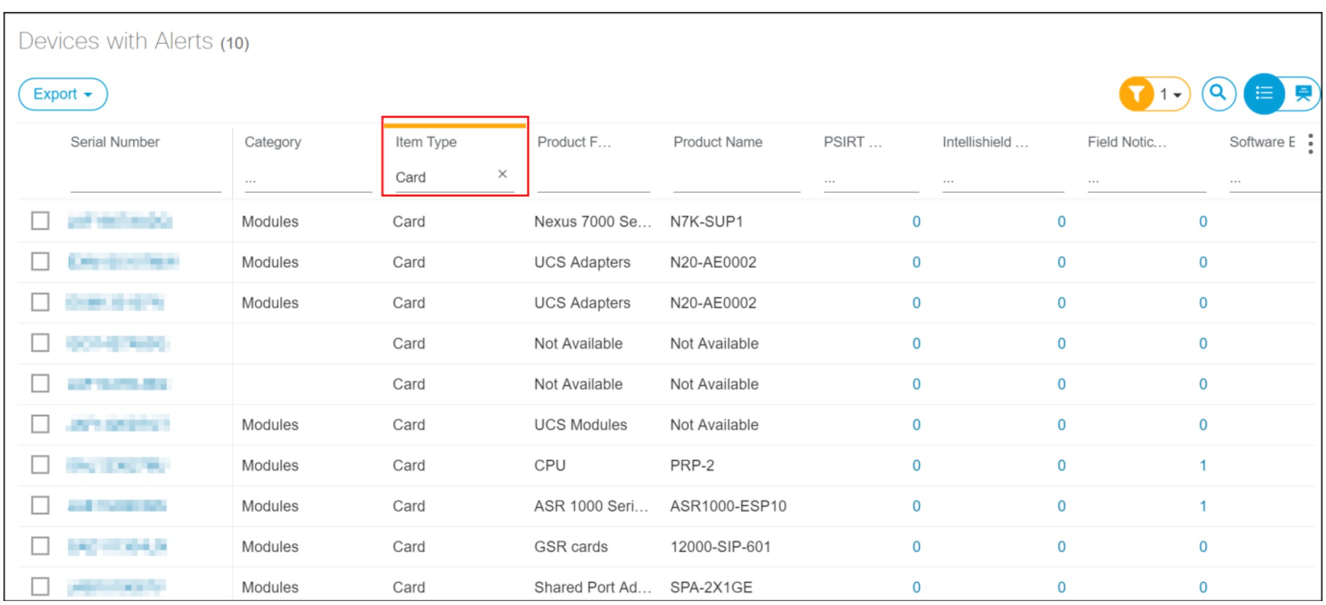
Serial Number	Category	Item T...	Product Family	Product Name	PSIRT...	Intellis...
FTX1123E0BG	Wireless	Chassis	Cisco Aironet 1200 Series	Cisco Aironet 1230 AG Acces...	0	0
FTX1221T1HQ	Wireless	Chassis	Cisco Aironet 1130 AG S...	Cisco Aironet 1130 AG Acces...	0	0
FTX1510900L	Wireless	Chassis	Cisco Aironet 1250 Series	Cisco Aironet 1250 Series Ac...	0	0
FTX1510T069	Wireless	Chassis	Cisco Aironet 1130 AG S...	Cisco Aironet 1130 AG Acces...	0	0
FTX1510900M	Wireless	Chassis	Cisco Aironet 1250 Series	Cisco Aironet 1250 Series Ac...	0	0
FGL1450S4QV	Wireless	Chassis	Cisco Aironet 3500 Series	Cisco Aironet 3500i Access P...	0	0
FGL1450S4QY	Wireless	Chassis	Cisco Aironet 3500 Series	Cisco Aironet 3500i Access P...	0	0
FGL1450S4QW	Wireless	Chassis	Cisco Aironet 3500 Series	Cisco Aironet 3500i Access P...	0	0
FGL1450S4QX	Wireless	Chassis	Cisco Aironet 3500 Series	Cisco Aironet 3500i Access P...	0	0
FGL1450S4QU	Wireless	Chassis	Cisco Aironet 3500 Series	Cisco Aironet 3500i Access P...	0	0
FTX1510T06A	Wireless	Chassis	Cisco Aironet 1130 AG S...	Cisco Aironet 1130 AG Acces...	0	0
FTX1337S9ZV	Wireless	Chassis	Cisco Aironet 1140 Series	Cisco Aironet 1140 Access Po...	0	0
FTX1904K0VQ	Wireless	Chassis	Cisco Aironet 3500 Series	Cisco Aironet 3500e Access ...	0	0
FTX1334S8H3	Wireless	Chassis	Cisco Aironet 1140 Series	Cisco Aironet 1140 Access Po...	0	0

The Search filter looks for the word or phrase in every column. In the example, " aironet" appeared in both the Product Family and the Product Name fields. Click the x to close the search filter.

Text Filter

This type of filter lets you view all the data records (default), or display those records that match the search parameters.

- In the example below see only those data records that have a description that contains the parameters noted in the search field.



Devices with Alerts (10)

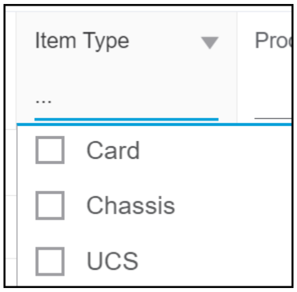
Export ▾

Serial Number	Category	Item Type (Card)	Product F...	Product Name	PSIRT ...	Intellishield ...	Field Notic...	Software E
[illegible]	Modules	Card	Nexus 7000 Se...	N7K-SUP1	0	0	0	
[illegible]	Modules	Card	UCS Adapters	N20-AE0002	0	0	0	
[illegible]	Modules	Card	UCS Adapters	N20-AE0002	0	0	0	
[illegible]		Card	Not Available	Not Available	0	0	0	
[illegible]		Card	Not Available	Not Available	0	0	0	
[illegible]	Modules	Card	UCS Modules	Not Available	0	0	0	
[illegible]	Modules	Card	CPU	PRP-2	0	0	1	
[illegible]	Modules	Card	ASR 1000 Seri...	ASR1000-ESP10	0	0	1	
[illegible]	Modules	Card	GSR cards	12000-SIP-601	0	0	0	
[illegible]	Modules	Card	Shared Port Ad...	SPA-2X1GE	0	0	0	

- This filter lets you view all the data records (default), or see only those data records that have an Item Type that contains the parameters noted in the search field (in example, “**card**”). Click the x to close the search filter.

Category Filter

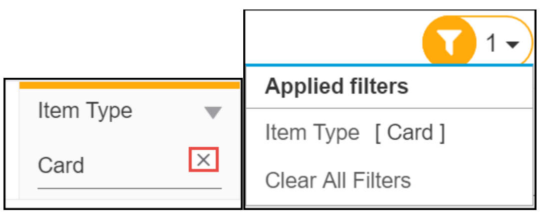
The category filter lists all the categories in a column and lets you see data in another selected category.



- Click the mouse button on the search filter field; a list of all the categories is displayed.
- Check the check box for the category data you want to display.

Note The user can select multiple categories.

- To change the filtering to another category do one of the following tasks:

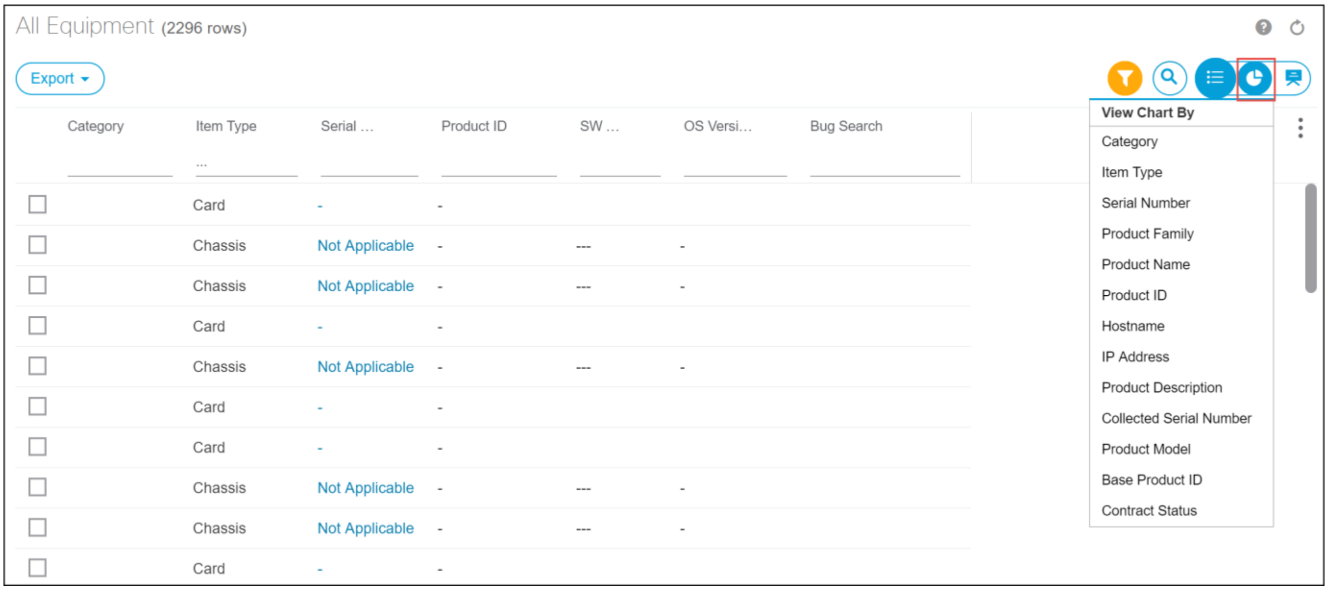


- To go back to the **All** view quickly, click the x to the right of the current category item, which resets the filter back to all items displayed.
- Click the  icon and **Clear All Filters** to view all the category data again.

Note The category filter is not available for each column that has different items listed. This filter is normally available only in those columns that have a limited number of category items in the associated column.

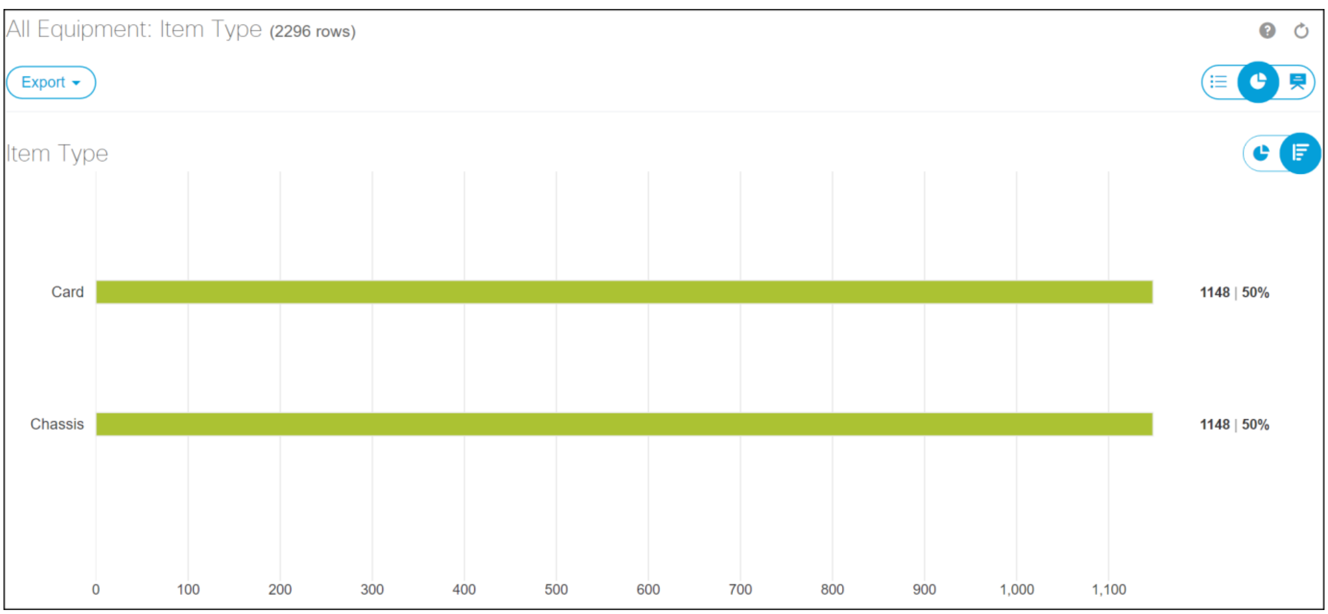
Chart Filters

Those reports that have the *view as chart* option provide filtering that allows you to see the chart data from a variety of category views. When selecting a chart view, one of the chart category view options must be selected. To see the chart data, perform the following steps:



- Click the chart drop-down list and select a chart view category from the list.

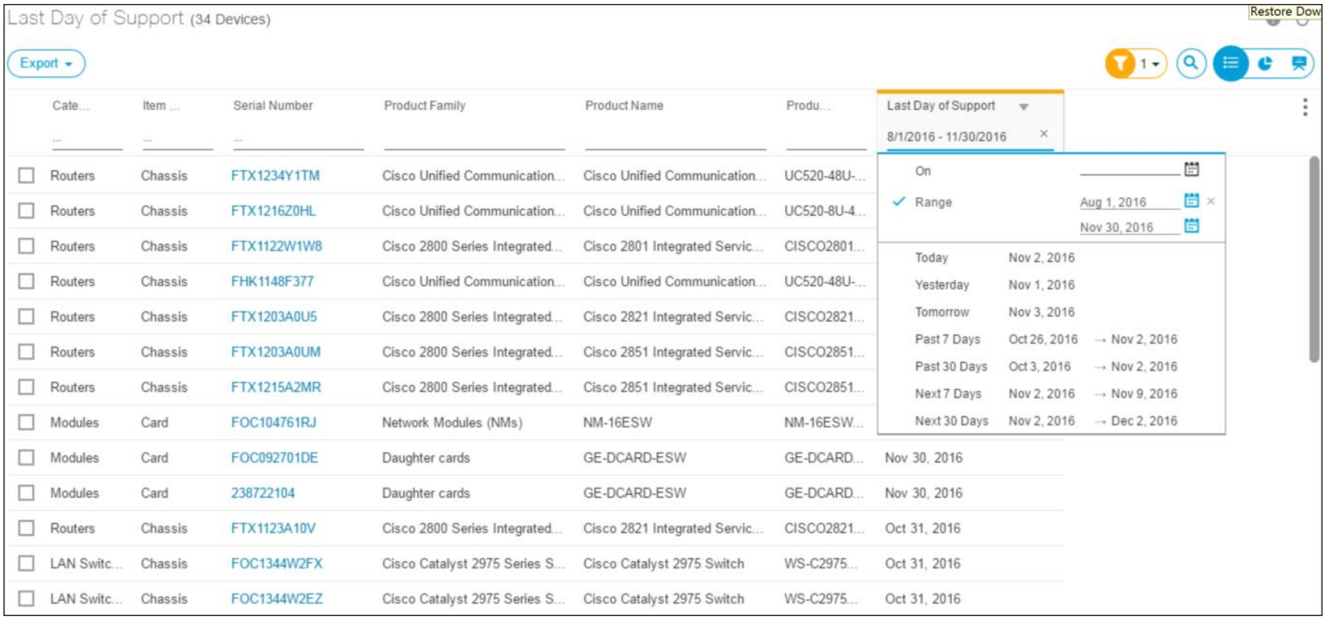
Note The category items provided in the chart list are columns that are available for viewing in the table view, but not necessarily displayed in the current table view; see Displaying and Hiding Columns for more info about displaying hidden table columns.



- At the top of the chart view of the report is the filter option you selected (in example, by Item Type).
- When the content area is displayed as a chart, the chart data view can be changed to another category view by clicking the chart drop-down list and selecting another chart category (in example, Item Type).

Date Filter

The date filter lists all the data for the selected date range. After specifying the date, the table shows only those records that match the specified date.



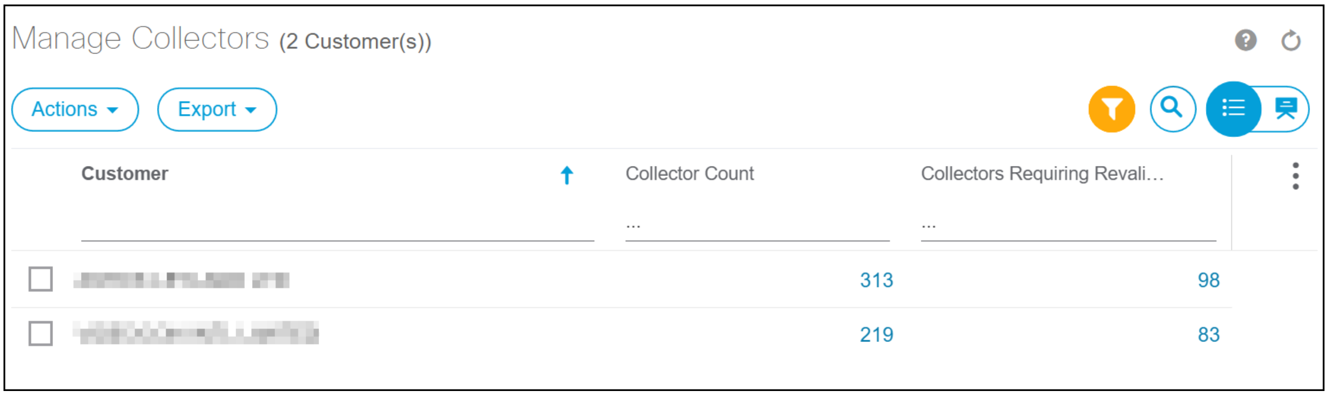
- Use the On option to select the date on the specific date.
- Use the Range to select the date range from the calendar icon.

Managing Collectors

The **Super Administrator** and **Partner Administrators**, can manage the collectors to maintain installed collectors for one or more customers while a **Partner User** can only manage the collectors for the customers to which they are entitled. It is assumed that the collector has been installed; or you are now ready to obtain then apply the security certificate required to activate the collector. You can register a new collector for a customer site, edit or delete the collector registrations, regenerate a new collector security certificate, and revalidate a blocked inventory upload.

To open the **Manage Collectors** report:

1. Open the list of **Actions** in the navigation pane.
2. Select **Manage Collectors**.



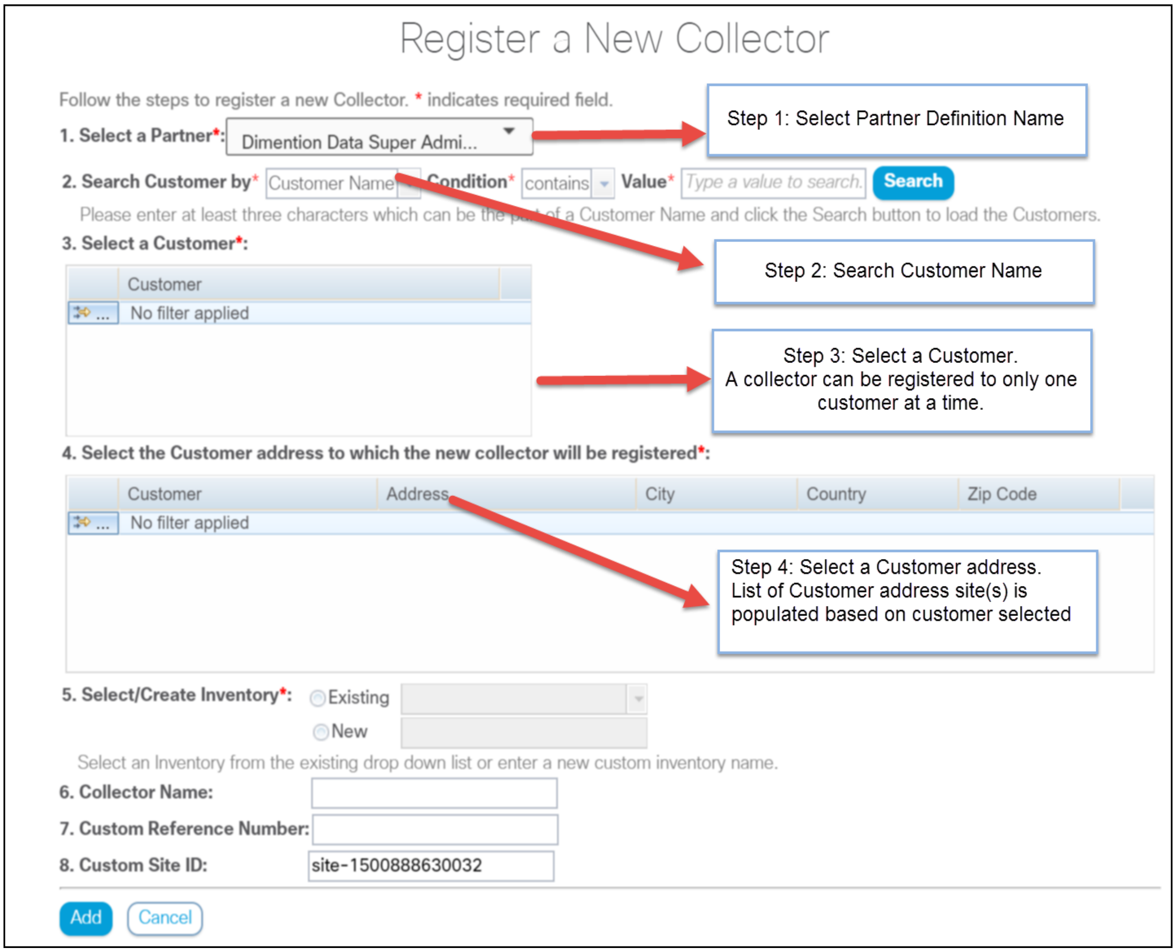
The Manage Collectors report appears in the content area displaying a list of all customers you are entitled to see along with each Customer name, Collector Count and count of the Collectors Requiring Revalidation.

Registering a New Collector

Before a collector can upload information to the Cisco Data Center to be processed and made available in the PSS portal, it must be registered to a customer site. To facilitate this, a security certificate must be issued through the portal, then must be downloaded and applied to the collector.

A successful collector registration allows validation to occur that creates a connection between the collector and the Cisco data center.

1. From the **Manage Collectors** report, click the **Actions** drop-down list and select **Register a New Collector**. The **Register a New Collector** window appears.



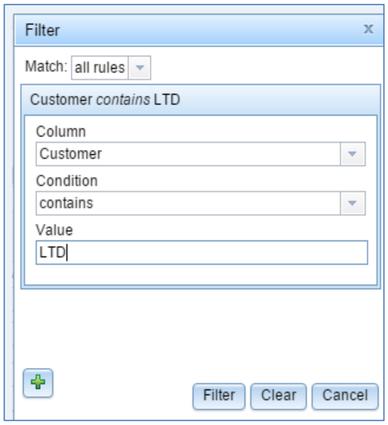
Note

- As a Partner User, you can manage collectors only for the customers you are entitled / associated to. Otherwise a message indicating you are not authorized to create / register a new collector for that customer will be displayed.
- If the Contract Number provided is not included in the Partner Definition or does not belong to the partner, no customer information will be displayed. Customer information will only be displayed if the contract is in the current Partner Definition.

2. Enter all the required information, which is designated by an asterisk (*).

- Select your Partner company name from the drop-down list.
- Select the **Customer** or **Contract Number** from the available list.
  - **Search Customer by**: Use this option to filter either by Customer Name or Contract Number
  - **Condition**: Use this option to set the condition. The value of the condition is based on the selected option of the Search Customer by column. The options are: is, contains, starts with and ends with.
  - **Value:** Enter the relevant value to filter the records. For example, the values can be part of the contract number or part of the text of the relevant column.
  - Click **Search** to display the Customer Name or Contract Number in the grid.

3. Click the radio button to select the **Customer** from the table.
    - (Optional) For a long list of companies, add a filter to show only the company where the collector will be registered.
    - Click the filter icon 



    - Set the **Column** to Customer.
    - Choose a **Condition** such as “contains”
    - In the **Value** field, enter the company name.
    - Click the **Filter** button
4. Click the radio button to select the **Customer** with the address to which the new collector will be registered.
5. Select the Inventory from the drop-down list of Existing Inventories or select **New** and enter a name for the new inventory. When you choose an existing inventory name, the manual import of the CSV file appends its device data to the previous inventory data.
6. Enter a **Collector Name** and **Custom Reference Number**.
7. The Custom Site ID is an auto-populated field. You may change it to more clearly to describe the location of the collector you are registering. The allowed characters include alphanumeric, #, &, _ and - characters.
8. Click the **Add** button; a message appears indicating that the submission was successful and instructs you to download a certificate. An email, which includes the details related to the Collector and a link to download the registration zip file, is sent to the end user.

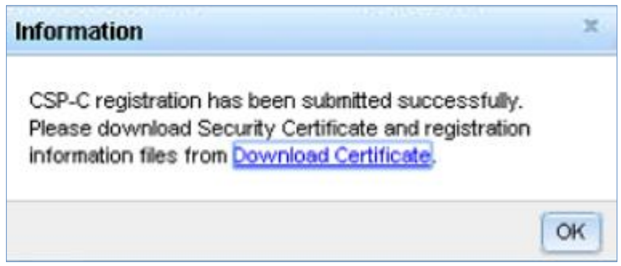
Note Only the individual who registers a collector will receive email notifications for Collector Registration, Uploads, and Re-validations.

Downloading a Registration Certificate

Downloading a collector registration certificate provides you entitlement files, a security certificate and other registration related files that are used when installing the Collector entitlement file.

To download a certificate:

1. Click the **Download Certificate** link in the registration success message dialog box or the email notification.

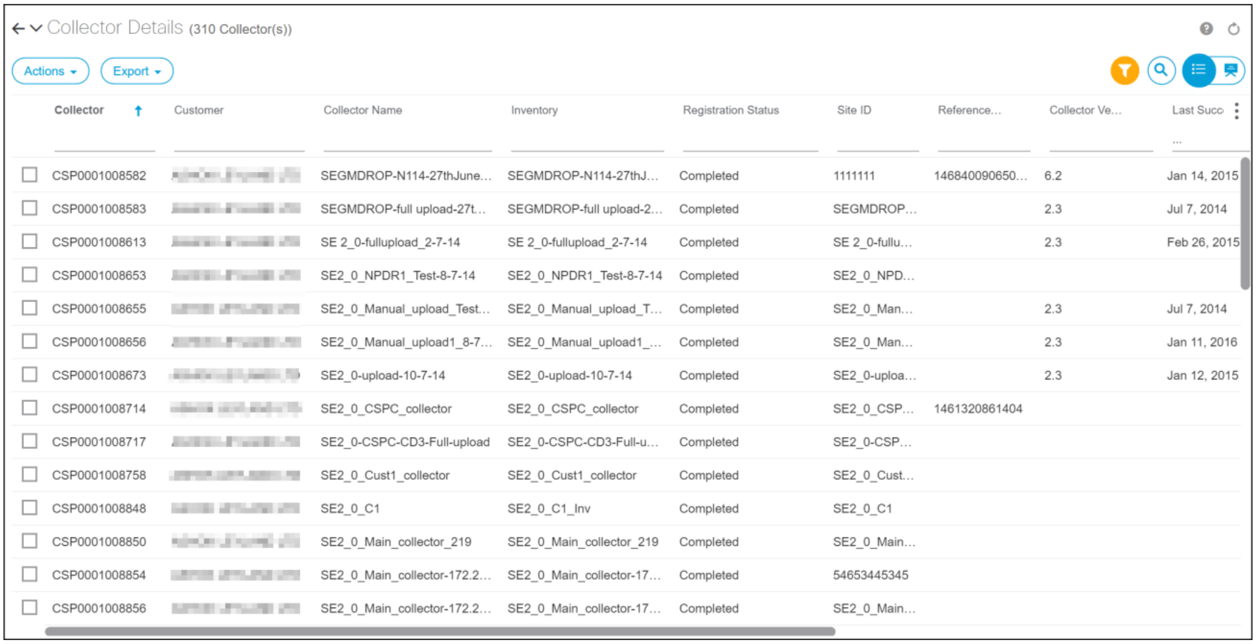


2. A zip file window appears requesting you to either save or open the entitlement file, which contains the certificate (license file) and other registration files.
3. Save the zip file in your local system. Do not unzip the file.
4. Load the registration certificate to the CSPC collector as part of the installation process. Documentation is available on our Common Services Platform Collector (CSPC) support page.

Note If the Download Certificate fails with the message " An error occurred while downloading the CSP-C certificate. Please try again later or contact Cisco Technical Support at tac@cisco.com if the problem persists" then wait for few minutes and try to download the certificate again. Refer to Generating a New Collector Certificate section.

Viewing Collector Details

- In the portal Library, select **Manage Collectors**. The **Manage Collectors** window appears including the **Customer Name**, **Collector Count**, and **Collectors Requiring Revalidation** details.
- Click the number link in the **Collector Count** column of a selected customer. The **Collector Details** window appears displaying the **Collector ID**, **Customer name**, **Inventory Name**, **Collector Name**, and **Upload Information**.



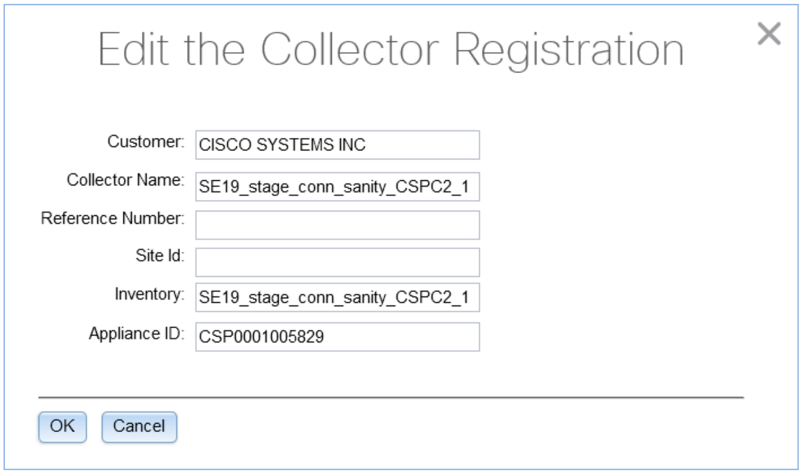
Collector	Customer	Collector Name	Inventory	Registration Status	Site ID	Reference...	Collector Ve...	Last Succ
CSP0001008582		SEGMDROP-N114-27thJune...	SEGMDROP-N114-27thJ...	Completed	1111111	146840090650...	6.2	Jan 14, 2015
CSP0001008583		SEGMDROP-full upload-27t...	SEGMDROP-full upload-2...	Completed	SEGMDROP...		2.3	Jul 7, 2014
CSP0001008613		SE 2_0-fullupload_2-7-14	SE 2_0-fullupload_2-7-14	Completed	SE 2_0-fullu...		2.3	Feb 26, 2015
CSP0001008653		SE2_0_NPDR1_Test-8-7-14	SE2_0_NPDR1_Test-8-7-14	Completed	SE2_0_NPD...			
CSP0001008655		SE2_0_Manual_upload_Test...	SE2_0_Manual_upload_T...	Completed	SE2_0_Man...		2.3	Jul 7, 2014
CSP0001008656		SE2_0_Manual_upload1_8-7...	SE2_0_Manual_upload1_...	Completed	SE2_0_Man...		2.3	Jan 11, 2016
CSP0001008673		SE2_0-upload-10-7-14	SE2_0-upload-10-7-14	Completed	SE2_0-uploa...		2.3	Jan 12, 2015
CSP0001008714		SE2_0_CSPC_collector	SE2_0_CSPC_collector	Completed	SE2_0_CSP...	1461320861404		
CSP0001008717		SE2_0-CSPC-CD3-Full-upload	SE2_0-CSPC-CD3-Full-u...	Completed	SE2_0-CSP...			
CSP0001008758		SE2_0_Cust1_collector	SE2_0_Cust1_collector	Completed	SE2_0_Cust...			
CSP0001008848		SE2_0_C1	SE2_0_C1_Inv	Completed	SE2_0_C1			
CSP0001008850		SE2_0_Main_collector_219	SE2_0_Main_collector_219	Completed	SE2_0_Main...			
CSP0001008854		SE2_0_Main_collector-172.2...	SE2_0_Main_collector-17...	Completed	54653445345			
CSP0001008856		SE2_0_Main_collector-172.2...	SE2_0_Main_collector-17...	Completed	SE2_0_Main...			

- Click a check-box to select a collector and from the **Actions** menu, select any one of the following tasks:
  - Access CSPC
  - Edit Collector registrations
  - Delete Collector registrations
  - Generate a new collector security certificate
  - Editing Collector Registrations

As an Administrator, you can edit the Collector registrations only on those registrations that have a registration status of **Completed**. Registrations that are in an unregistered state cannot be edited.

To edit the Collector registration, perform the following:

1. Select **Manage Collectors** from the Cisco Services Connection Library.
2. Click the **Collector Count**.
3. Select any Collector that needs to be edited.
4. Mouse hover on the left of the selected Collector, click the **Action** icon or right-click the Collector and click **Edit Collector Registration**. The **Edit Collector Registration** window appears.



5. Modify the collector name and serial number of the collector.

6. Click **OK**. The Collector information is edited.

7. An email notification is sent to the user who updated of the collector registration.

Deleting Collector Registrations

Active collector registrations can be deleted. When one collector is to be re-assigned to a new customer or site, the active registration is deleted and a new registration completed.

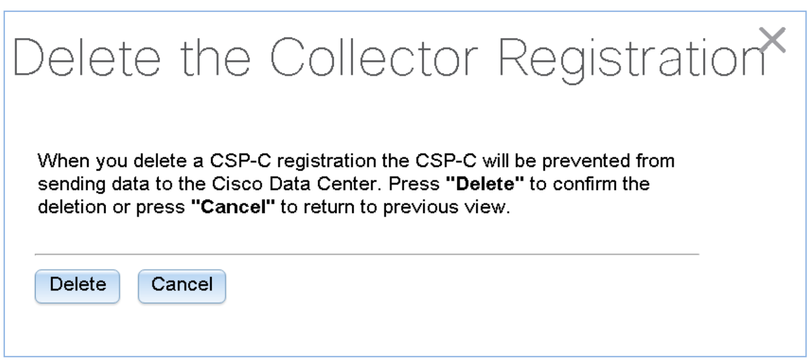
To delete a collector registration, perform the following:

1. Select **Manage Collectors** from the Cisco Services Connection Library.

2. Click **Collector Count**.

3. Select any Collector that must be deleted.

4. Click the check box on the left of the selected collector, click the **Action** menu and select **Delete** the Collector Registration. The **Delete Registration** confirmation message box appears.



5. A confirmation window appears to verify that you want to delete the registration and indicates that doing so will stop the Collector communication to the Cisco data center.

6. Click **Delete**; A status message appears on the previous view indicating the success of the registration deletion.

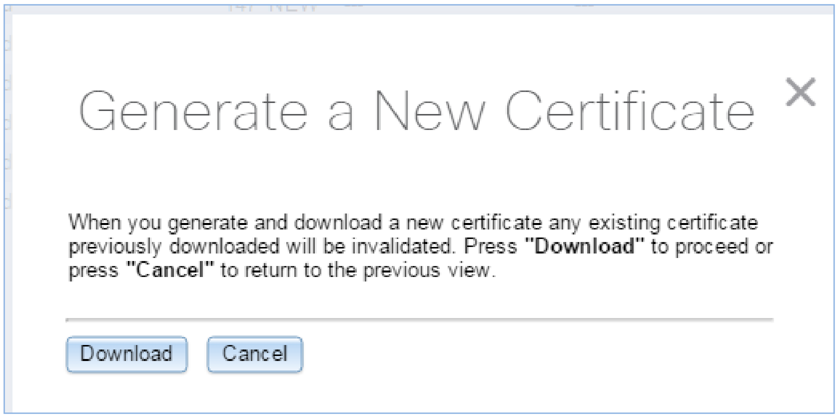
7. An email notification is sent to the user who deleted the collector registration.

When a registration is deleted, the collector is prevented from uploading inventory collections to the Cisco data center.

Generating a New Collector Certificate

To access new features for your collector, you will first download a new image(s), and then generate, and apply, a new security certificate. To generate a new collector, perform the following:

1. Select **Manage Collectors** from the Cisco Services Connection Actions panel.
2. Select any Collector for which a new security certificate must be generated.
3. Click the check box to select a collector, click the **Action** menu and select the option to **Generate a New Certificate**. The **Generate a New Certificate** confirmation window appears.



4. A confirmation window appears to verify that you want to **Generate a New certificate** and invalidate any existing certificate previously downloaded.
5. Click **Download**.
6. An email notification is sent to the user regarding the generation of a new certificate.

Manual Device Import

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

- A customer does not want a collector to be deployed on the network.
- A customer does not want the partner to collect information of all the devices from their network.
- A customer does not want the automated transfer of collected device data to Cisco.
- A customer has spares, not connected to the network, and wants a complete inventory.

In either of the cases, the partner can import the collector file that provides the details of the devices on the network.

- For CSP-C upload, you will need to download a “transport file” from the Collector application, then import that file into the PSS portal. For more information refer to Generating a transport file for CSP-C upload.
- For the CSV upload, you can download a sample file, enter the details of the devices and upload the .csv file.

Prerequisites

The prerequisites for using the manual import feature are:

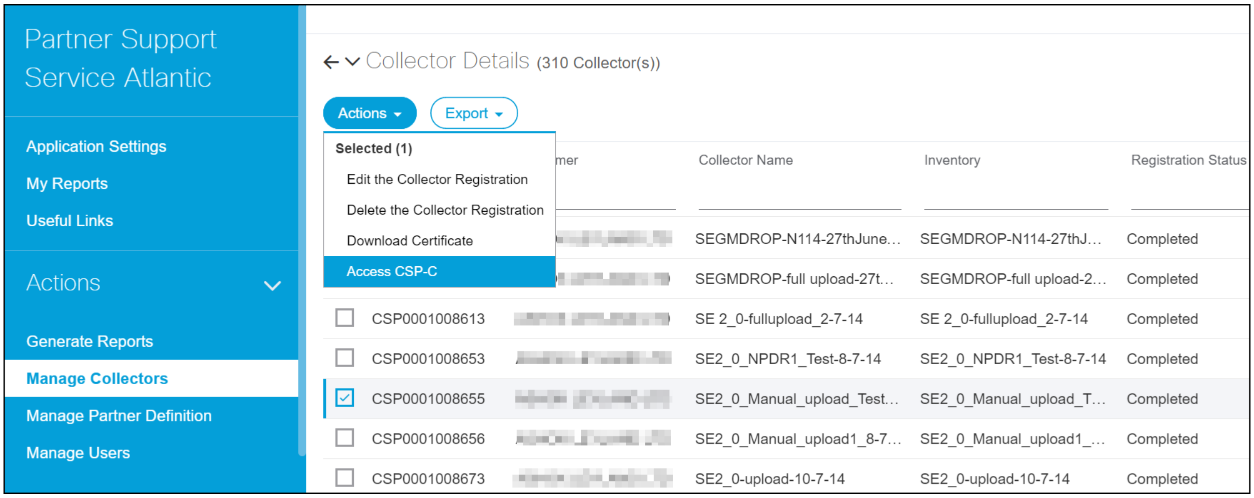
- At least one Bill-to ID must be enabled in the Partner Definition in order to manage collectors or manually import the device information on the network.

- There must be a registered company.
- The partner performing the manual import must be a registered Partner Administrator or Partner User in the portal.
- The user must select the specific customer company and its inventory for the import.

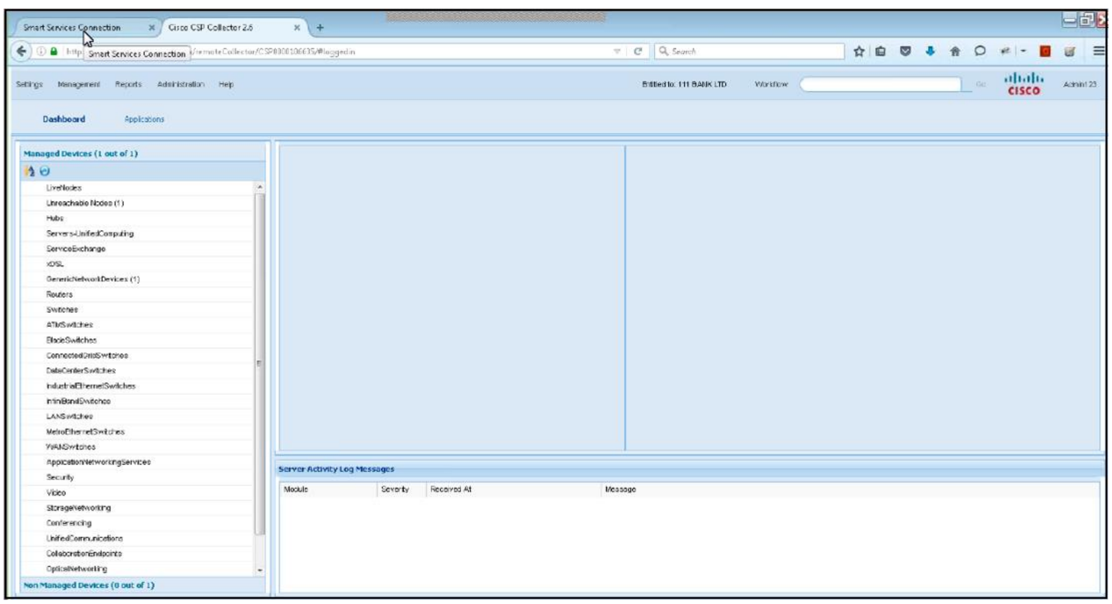
Generating a Transport File for CSP-C Upload

To login to remote Cisco CSPC Collector Application and to generate a transport file perform the following steps:

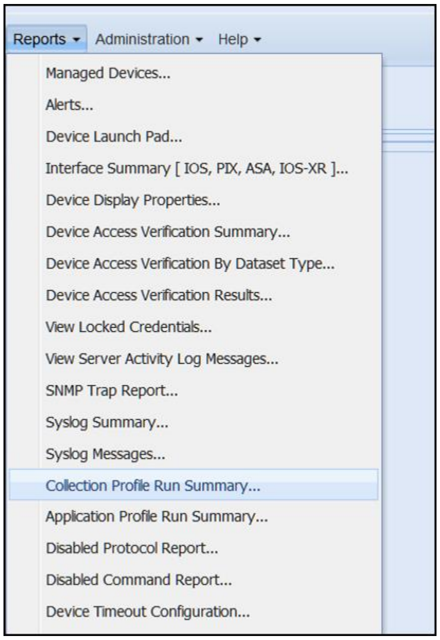
1. From the **Manage Collectors** > **Collector Details**, select a row and from **Actions** menu select **Access CSP-C**.



2. Directs to Cisco CSPC Collector Application, login and follow the process to generate the file.

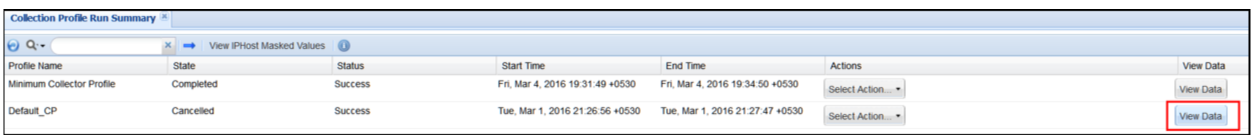


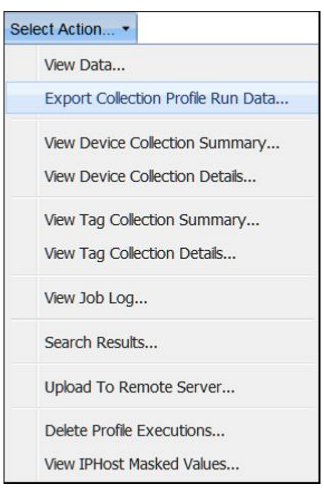
3. From the **Reports** menu, select **Collection Profile Run Summary** as shown in the snapshot.



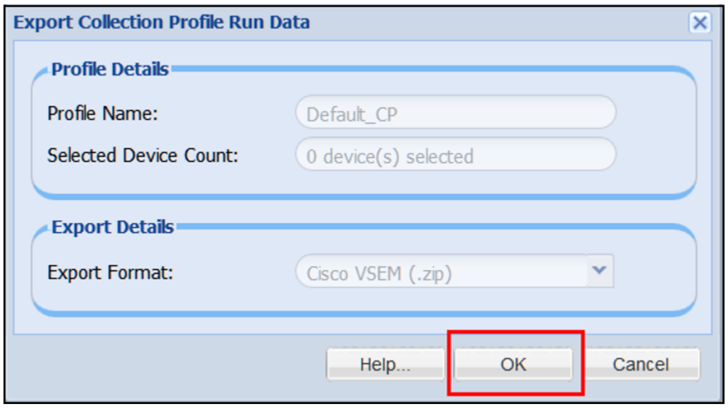
Ensure that the Profile is created and all the configuration of the device is setup. The summary provides the status and details of the collection.

4. Select the profile name and click **View Data** from the Collection Profile Run Summary window to view the raw data captured manually.



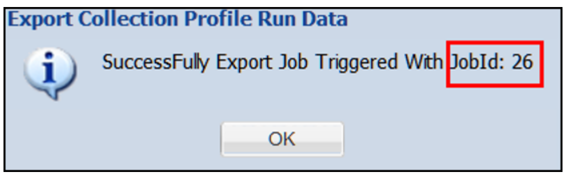


5. Click **Select Action** to perform the required action. Select **Export Collection Profile Run Data** from the drop-down. The window opens and provides the profile details to be exported.

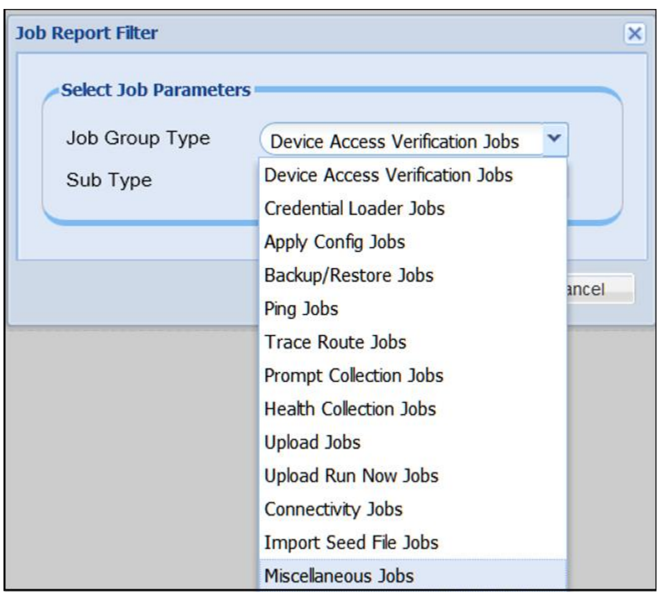


As shown in above snapshot, all the fields are preset and you do not need to change. The file is exported in standard export format that is a compressed zip file containing folders and xml files that details the network, customer info and devices on the network.

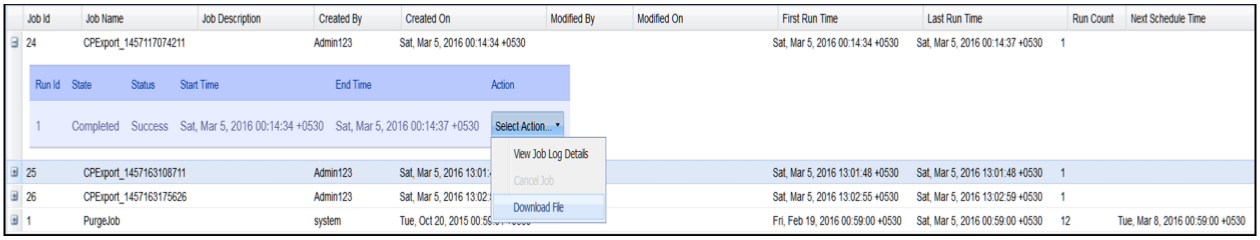
6. Verify the details and click **OK.** The application prompts with an information message on the status. Note the Job Id and click **OK.**



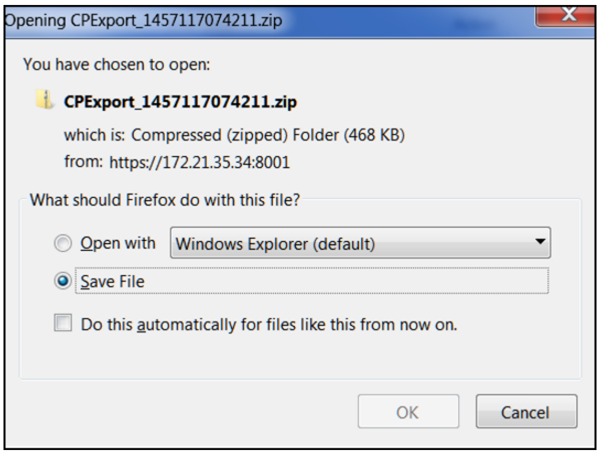
7. Go to **Reports** menu, select **Job Management Reports**. The **Job Report Filter** pops up to select the job parameters.



8. Select the **Job Group Type** as *Miscellaneous Jobs* and **Sub Type** as default – *CP Export Jobs.* You can view **all the jobs based on the parameters and also** click on the **+** symbol next to the Job Id to view the description of each job. It provides details on the Run Id, State (Successful/Aborted), Status (Completed/Not Completed), Start Time, End Time, and Job Log Details for the particular job.



9. Click **Select Action** in the report and select **Download File**. The application prompts you to save the file.



10. Select the option to save the file and click **OK.** The saved compressed file is in CSP-C VSEM format that you should use to manually import. Follow the [Manual CSP-C Upload](#) process to proceed.

Creating a CSV File for CSV Import

Use the sample CSV file to create your import file.

- To download the sample CSV file, click **Download Sample CSV File** in the **Manual Import** window. An excel sheet is downloaded.
- Enter the data for the parameters contained in the sample CSV. The device parameters must be mentioned in the identical order as specified in the sample file.

Note Ensure you follow the below mentioned points:

- The size limit of the import file is up to 50,000 serial numbers/rows.
- Devices listed in the CSV manual import file must remain in the file for subsequent file-import transactions. Any omitted or removed devices will be removed from the inventory on the next manual import of the file.
- If a parameter value contains a comma (,) insert a forward slash (/) before the comma. For example, within the OS version field, if the parameter value is 12.2(33)SX15,fc2 enter the parameter as 12.2(33)SX15/,fc2
- The CSV file name should be meaningful to assist the partner with tracking and versioning of the imported information.

- The Serial Number and the Product ID must be recognized by Cisco as legitimate. They must correspond to data in the Cisco database associated with your customer's company.
- Save the information as a CSV file.

The parameters contained in the sample CSV file and the maximum character limit for each parameter is listed in the following table.

CSV Parameter	Max Character Limit	Mandatory/Optional	Purpose
Host Name	255 Char (including spaces)	Mandatory	Used for chassis and card association.
IP Address	64 Char (including spaces) IPv4 only	Mandatory	Used for chassis and card association. Used by Delta report to identify IP changes.
Serial Number	50 Char (including spaces)	Mandatory	Used for contract validation.
Product ID	255 Char (including spaces)	Optional	Used for contract validation.
MAC Address	50 Char (including spaces)	Optional	Used to obtain serial number for IP phones.
SNMP Location	4000 Char (including spaces)	Optional	Used for inventory report to populate "SNMP Location" field.
OS Type	50 Char (including spaces)	Optional	Used for PSIRT alert and software alert report.
OS Version	50 Char (including spaces)	Optional	Used for software alert report.

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

CSV Import Limitations

- Manual Import is limited to 50K devices.
- All the headers are mandatory and must follow the identical order as specified in the sample CSV file.
- Users cannot import the CSV file if there is any pending request for that particular Entitled Company and Inventory combination.
- HOST_NAME, IP_ADDRESS, and SERIAL_NUMBER field values are mandatory for each device entry, otherwise import will fail.

- IP_ADDRESS must be in the valid format (IPv4 only) for each device entry, otherwise import will fail.
- The duplicate entries must be removed before importing the file.
- A manually imported CSV inventory is limited to Chassis only. (see note above)
- Alerts – Only Hardware Alerts and Field Notice alerts are processed for CSV Import Inventories.
- No data will appear for CSV Import Inventories in the following reports:
  - Exceptions Summary Report – No data.
  - Protocol Access Error Report – No data.
  - Installed Application Reports – No data.
- Discrepancies in NPDR reports.
- Ensure the most recent file from the collector has to be imported because the file overwrites the last imported CSV inventory.
- A device cannot be included in the CSV import file, if there is also ongoing processing of the device from the collector file. Only the collected device information will display.

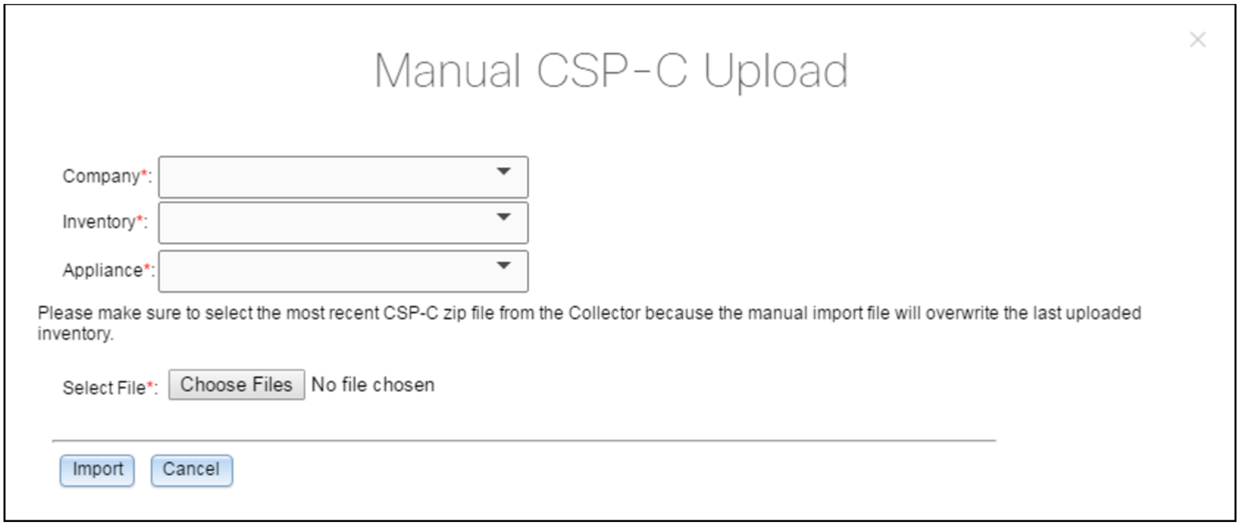
Leading Practices

- When you choose an existing inventory name, the manual import of the CSV file appends its device data to the CSP collected inventory data.
- When you create a new inventory name, the data is kept in a separate inventory.
- For the first manual CSV import, you may want to generate a new Appliance ID. The Appliance ID will begin with CSV rather than CSP so you can easily distinguish between the two collection methods.
- Mutual relationships are not established between the device information that is uploaded using the CSV file. For instance, if you upload the information for a router chassis and the cards installed within that chassis, PSS will not be able to discern that those cards are installed in the chassis. In addition, knowledge about the chassis support contract that actually covers the installed cards is not known. (For example, a card that is covered under a chassis contract will be reported as uncovered in the PSS reports).
- Concurrent CSV Manual Imports for the same customer company and inventory are not allowed. You cannot perform multiple imports from different browsers at the same time for the same customer company and inventory. Only the first import will be accepted and for the other import attempts, the portal displays an error message. Concurrent file imports will work for the same customer company but a different inventory name.
- If a device imported through Manual CSV Import is already part of an inventory collection for the same customer company and inventory, the PSS reports will show the collected device information only. Manually imported information for that device will not be displayed.

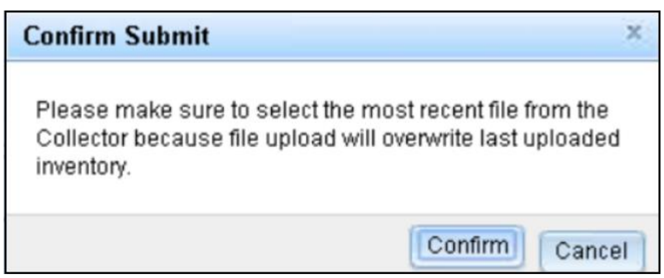
CSP-C Upload

To import a collection upload through a CSP-Collector, perform the following steps:

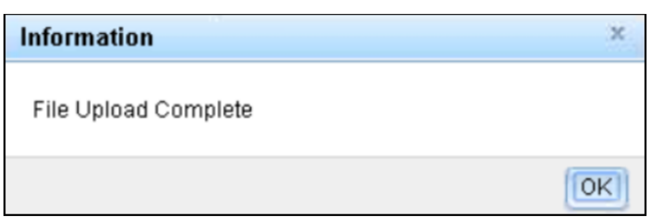
1. From the **Manage Collectors** LNP, under **Actions** drop-down menu, select the **Manual CSP-C Upload** option. The Manual CSP-C Upload dialog box appears.



2. Choose a company from the **Company** drop-down list.
3. Choose an existing **Inventory** from the drop-down list.
4. Choose an **Appliance** for an existing inventory from the drop-down list.
5. Click **Choose Files** and select the valid file that needs to be uploaded into the PSS portal from your local system. It is a .zip file that contains xml files.
6. Click **Import**.



7. Click **Confirm** to import the inventory information manually.



8. Click **OK** to complete the process and return to **Manage Collectors** window.

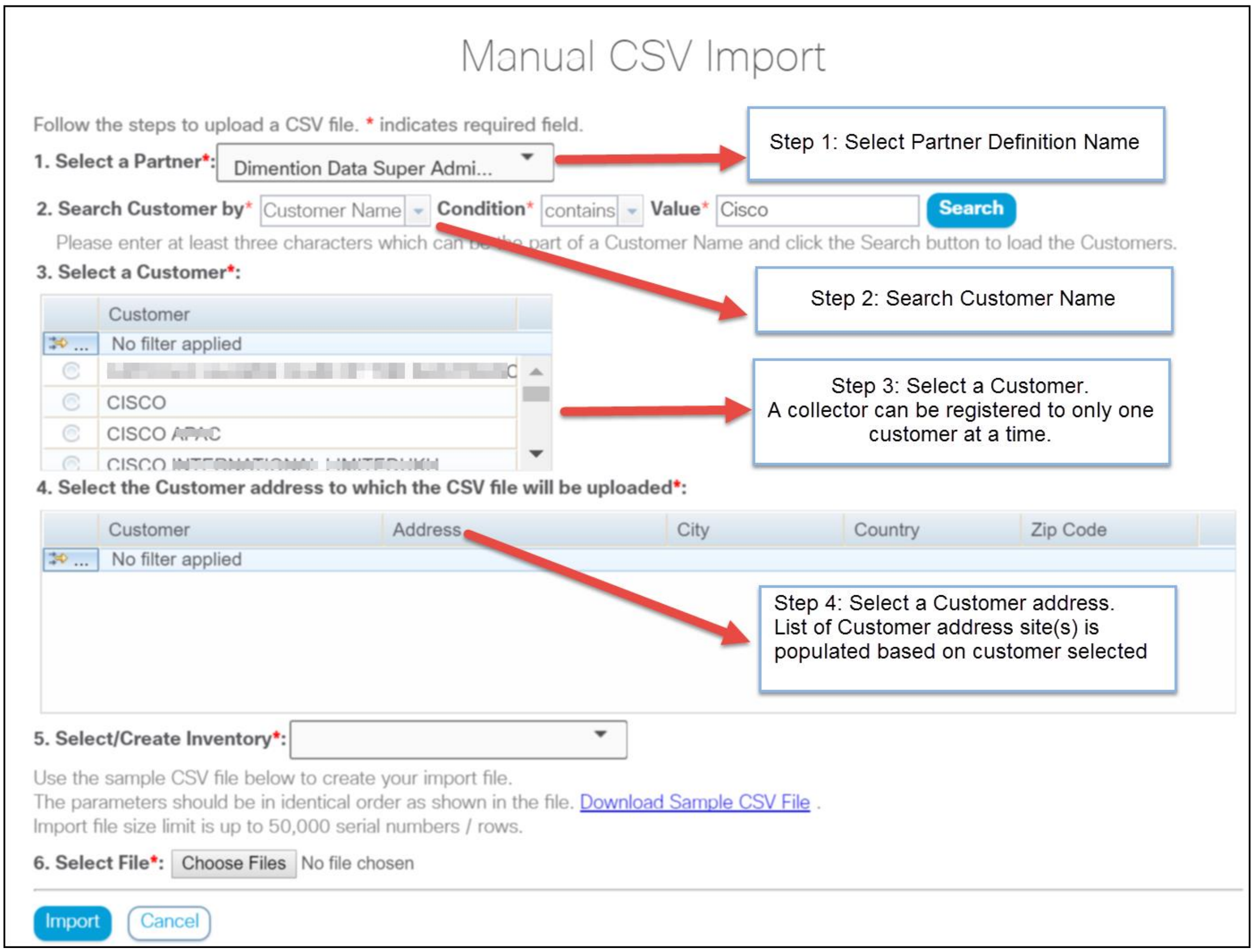
Note To view the collection upload details, verify correct inventory and customer is selected in the portal data filters, select **Inventory Collection** from left navigation pane and view the status of the upload. It may take some time for the data center to process the upload.

Note Due to security issues in older TLS protocols used for transporting data to Cisco, there is a change in the Cisco processing that will result in all CSPC collectors running 2.6 or earlier no longer being able to upload files. To avoid this, you should update your CSPC software to the latest version (CSCP 2.8.2) as soon as possible.

CSV Import

To import a collection upload through a CSV Import, perform the following steps:

1. From the **Manage Collectors** LNP, under **Actions** drop-down menu, select the **Manual CSV Import** option. The Manual CSV Import dialog box appears.



Note As a Partner User, you can manage collectors only for the customers you are entitled / associated to. Otherwise a message indicating you are not authorized to create / register a new collector for that customer will be displayed.

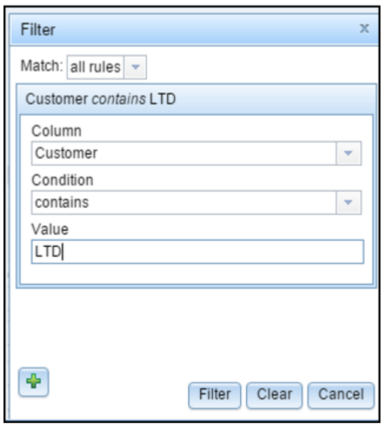
2. Enter all the required information, which is designated by an asterisk (*).

   - Select the **Partner** company name from the drop-down list.
   - Select the **Customer** from the available list.

- **Search Customer by**: Use this option to filter either by Customer Name or Contract Number
- **Condition**: Use this option to set the filter. The value of the condition is based on the selected option of the Search Customer by column. The options are: is, contains, starts with and ends with.
- **Value**: Enter the relevant value to filter the records. For example, the values can be part of the contract number or part of the text of the relevant column.
- Click **Search** to display the Customer Name or Contract Number in the grid.

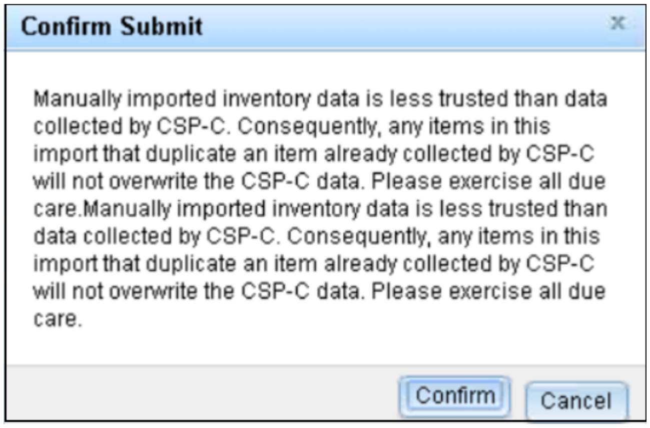
3. Click the radio button to select the **Customer** from the table.

- (*Optional)* For a long list of companies, you may want to add a filter to show only the company where the collector will be registered.
- Click the filter icon 

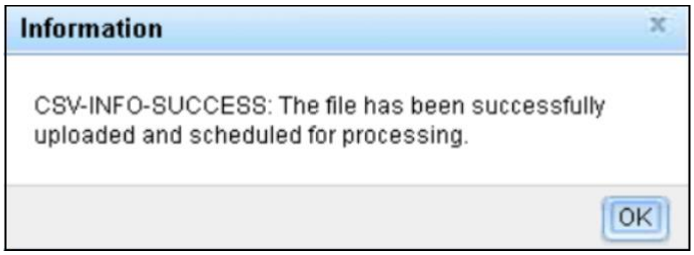


- Set the **Column** to Customer.
- Choose a **Condition** such as “contains”
- In the **Value** field, enter the company name.
- Click the **Filter** button

4. Click the radio button to select the **Customer** with the address to which the new collector will be registered.
5. Select the Inventory from the drop-down list of **Existing** Inventories or select **New** and enter a name for the new inventory.
6. Click **Choose Files** and select the valid file that needs to be uploaded into the portal from your local system. You can download a sample CSV file, enter the details and upload. Refer to Creating a CSV file.
7. Click **Import**.



8. Click **Confirm** to import the inventory information manually.



The portal displays the success message if the manual inventory is imported successfully. Once the inventory is successfully imported, it will start processing. Data will not be available in the portal until the processing has completed and the user receives an email notification on the file uploaded.

Note To view the file upload details, verify that the correct inventory and customer is selected in data filters, select **Inventory Collection** from left navigation pane and view the status.

Removing Manually Imported Devices

When a Partner Administrator imports another file for the same customer company and inventory, the new import will overwrite all device information previously manually imported. Any device that appeared in the previous CSV manual import file that is not in the most recent manual import is removed from the inventory reported in the PSS portal.

All Partner Support Service reports will display the most recent CSV import data.

Note Consider carefully before manually importing devices, it may be complicated to remove the information later because a blank CSV file cannot be imported.

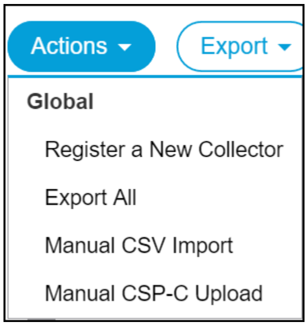
To remove all the manually imported data for an inventory you will need to complete the following steps:

1. Create a CSV file using the downloadable template.
2. Under the headings, add the mandatory information for a single device that is also in the CSP-Collected inventory.
3. Import the CSV file containing a single device.

Export All

An administrator can view the details of all the registered collectors to entitled customers. To download the Collector Inventory Upload Report, perform the following steps:

1. Click **Export All** from the **Actions** drop-down list in the **Manage Collectors** window. The new tab opens and saves a zip file.



2. A CSV file is downloaded with columns: Partner Name, Customer Name, Appliance Id, Registration Status, Serial Number, Version, Site ID, Last Successful Upload Date, First Successful Upload Date, Upload Received by Backend, Inventory Name, Appliance Name, Certificate Create Date, Created By, Last Updated On, Last Updated By.

3. Open the CSV file.

Providing PSS Service Coverage

Before an inventory collection can be uploaded, there needs to be at least one device in the collection covered by a PSS supported contract. The Cisco data center rejects any inventory collection that does not have an active PSS supported contract. This may be caused due to the following conditions:

- The PSS support contract has expired, or the contract is not a valid PSS contract.
- The contract Bill to IDs have not been managed within your Partner Definition.

Note PSS sends email before all contracts will expire, and again, when an inventory upload is blocked due to an expired contract.

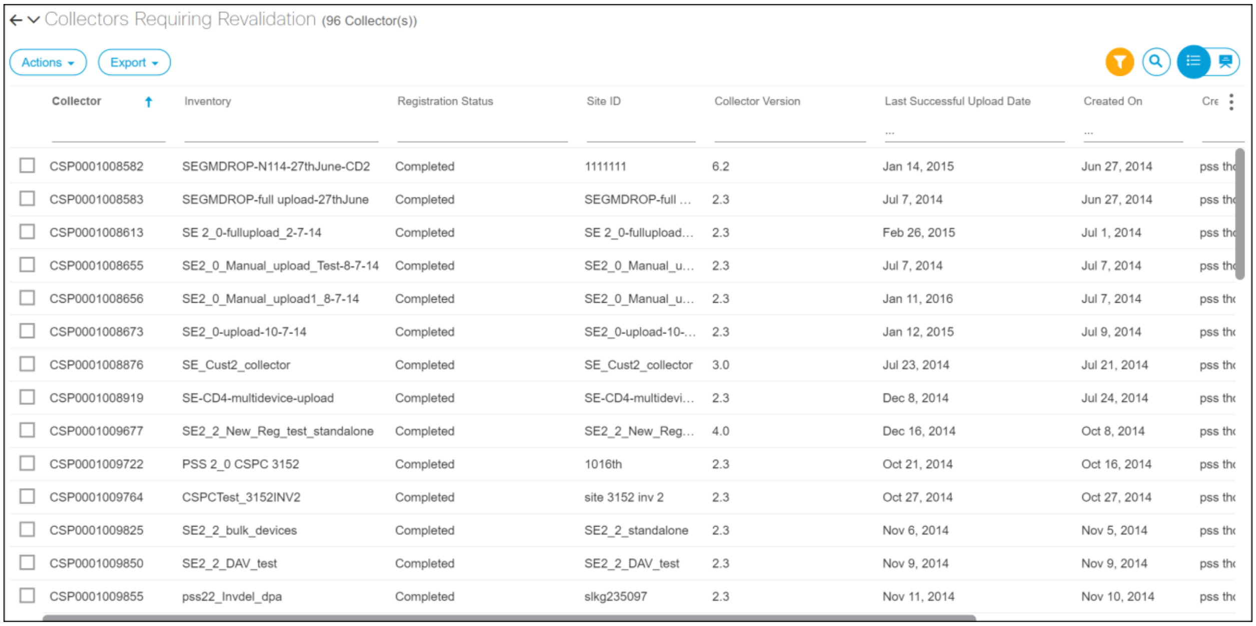
To allow validation, choose one of the following options:

- Renew a device contract for your customer's site under your Bill-to ID.
- Your Super Admin should make sure the Bill-to ID is enabled for your companies Partner Definition.

Note Revalidation of a blocked inventory upload is automated. You are not able to manually revalidate a blocked inventory, a valid contract association is required.

To view the blocked inventory upload, an Administrator performs the following steps:

- From the LNP, select **Manage Collectors**. The **Manage Collectors** window appears including the Customer Name, Collector Count, and count of Collectors Requiring Revalidation.
- Click the number link in the **Collectors Requiring Revalidation** column to display the **Collectors Requiring Revalidation** window.



Collector	Inventory	Registration Status	Site ID	Collector Version	Last Successful Upload Date	Created On	Cre
CSP0001008582	SEGMDROP-N114-27thJune-CD2	Completed	1111111	6.2	Jan 14, 2015	Jun 27, 2014	pss th
CSP0001008583	SEGMDROP-full upload-27thJune	Completed	SEGMDROP-full ...	2.3	Jul 7, 2014	Jun 27, 2014	pss th
CSP0001008613	SE 2_0-fullupload_2-7-14	Completed	SE 2_0-fullupload...	2.3	Feb 26, 2015	Jul 1, 2014	pss th
CSP0001008655	SE2_0_Manual_upload_Test-8-7-14	Completed	SE2_0_Manual_u...	2.3	Jul 7, 2014	Jul 7, 2014	pss th
CSP0001008656	SE2_0_Manual_upload1_8-7-14	Completed	SE2_0_Manual_u...	2.3	Jan 11, 2016	Jul 7, 2014	pss th
CSP0001008673	SE2_0-upload-10-7-14	Completed	SE2_0-upload-10-...	2.3	Jan 12, 2015	Jul 9, 2014	pss th
CSP0001008876	SE_Cust2_collector	Completed	SE_Cust2_collector	3.0	Jul 23, 2014	Jul 21, 2014	pss th
CSP0001008919	SE-CD4-multidevice-upload	Completed	SE-CD4-multidevi...	2.3	Dec 8, 2014	Jul 24, 2014	pss th
CSP0001009677	SE2_2_New_Reg_test_standalone	Completed	SE2_2_New_Reg...	4.0	Dec 16, 2014	Oct 8, 2014	pss th
CSP0001009722	PSS 2_0 CSPC 3152	Completed	1016th	2.3	Oct 21, 2014	Oct 16, 2014	pss th
CSP0001009764	CSPCTest_3152INV2	Completed	site 3152 inv 2	2.3	Oct 27, 2014	Oct 27, 2014	pss th
CSP0001009825	SE2_2_bulk_devices	Completed	SE2_2_standalone	2.3	Nov 6, 2014	Nov 5, 2014	pss th
CSP0001009850	SE2_2_DAV_test	Completed	SE2_2_DAV_test	2.3	Nov 9, 2014	Nov 9, 2014	pss th
CSP0001009855	pss22_Invdel_dpa	Completed	slkg235097	2.3	Nov 11, 2014	Nov 10, 2014	pss th

Contract Import

Contract importing is available to you for your customers who are already included in your Partner Definition. The contract import feature uses the covered device data available in the contract to add to a “Contract Imported” inventory as an alternative import capability. Only information from the contract is processed and used in the portal for reporting, so not all fields in the data grids will be populated as it would be from a CSPC collection.

When launching the contract import and selecting the customer, the portal lists the valid contract numbers of the customer that belong to the partner definition. The logged-in partner can choose one or more contract numbers available in the portal and perform a contract import. The imported files and the devices appear in the portal under a special inventory name “Contract Imported” under the customer and partner in the global filter.

This feature allows multiple customer association with single contract number. The logged in user selects the customer first and chooses the list of contract numbers that belongs to the customer for import.

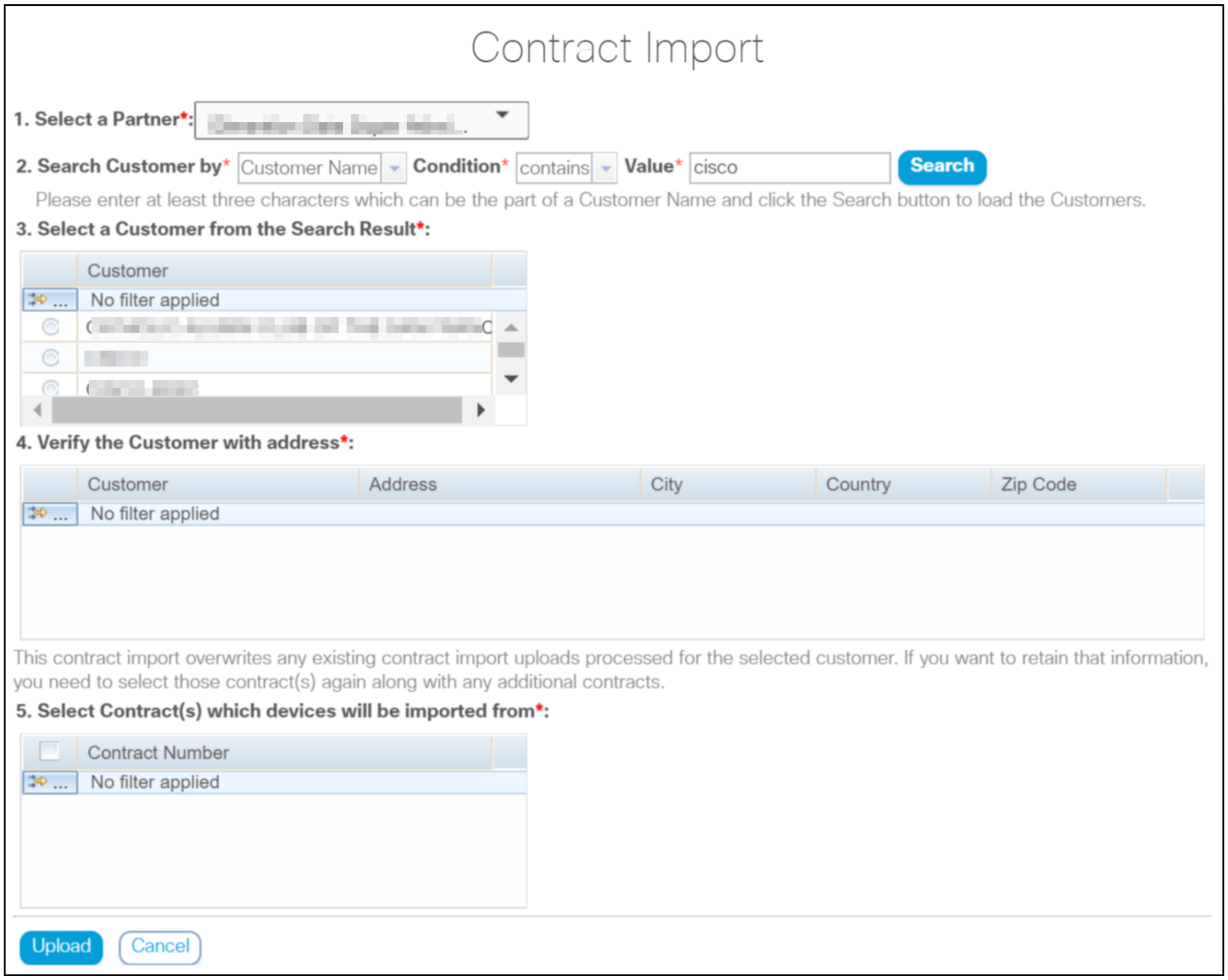
Pre-requisites

- The usage of special inventory name “Contract Imported” is restricted while registering a new CSP-C collector and importing manual CSV upload file. This restriction avoids the inventory being pointed to by multiple sources of data collection and will be used exclusively for contract import.
- If one or more devices associated with a contract number which is currently selected for contract import are already collected for the customer by different collection method (CSP-C or manual CSV import) with any inventory name, those pre-existing devices for the same customer will not be reported again as part of contract import.

If the contract import is performed again for the same customer, the recent one under the same inventory name “Contract Imported” will override the devices collected by last contract import.

To import a contract, perform the following:

1. From the **Manage Collectors** data grid, click **Actions** > **Contract Import**. The Contract Import page appears.



2. Select the **Partner** company name from the drop-down list. The drop-down lists the Partner Definition of the logged in user.

3. Select the Customer from the available list.

   - **Search Customer by**: Use this option to filter either by Customer Name or Contract Number
   - **Condition**: Use this option to set the condition. The value of the condition is based on the selected option of the Search Customer by column. The options are: is, contains, starts with and ends with.
   - **Value**: Enter the relevant value to filter the records. For example, the values can be part of the contract number or part of the text of the relevant column.
   - Click **Search** to display the Customer Name or Contract Number in the grid.

4. Click the radio button to select the **Customer** from the table.

5. Click the radio button to select the **Customer** with the address to which the new contract is imported. On selecting the customer, the associated contract number for the customer is listed.

Note You can select only one customer at a time.

6. Select the desired contract number from the list.

Note You can select multiple contracts at a time. If an imported contract is already selected, then the same will be overwritten.

7. Click **Upload** to extract all the devices that are associated to the contract. The extracted devices will be drawn together to a single payload file and will be sent to Cisco data center.

Once the contract import is processed for a customer, a collection titled "Contract Import" will be available in that customers Inventory for selection.

Note **Inventory overwrite rules**:

Similar to CSV Import, common devices in contract-imported inventory are overwritten by subsequent CSP-C upload for the same customer. However, these changes will be not be affected by subsequent CSV upload for the same customer. Both the CSV inventory and contract import inventory are categorized at the same level.

Note **Inventory import rules:**

Before importing devices associated with selected contract numbers, each device is verified to ensure that the device is not already collected as part of both the CSP-C uploaded inventory and CSV imported inventory (if available) for the same customer. If a device is already available for the customer other than contract imported inventory (that is, via CSP-C/CSV inventory), then the device will not be selected for contract imported inventory upload.

Limitations

Following are the limitation for Contract Import feature:

1. Hostname and IP address of the devices will not be drawn for Contract Imported inventory due to its unavailability in the source. In these fields, the dummy value will be shown as 'Host' and '0.0.0.0' for Hostname and IP address columns respectively.

2. The following off-line reports will not be generated (data will not be available) for contract imported inventory. This is similar to the manual CSV imported inventory.

    - Exception Summary
    - Protocol Access Error Report
    - EnergyWise Assessment Report
    - Medianet Assessment Report
    - TrustSec Assessment Report
    - Cloud Intelligent Network (CIN) Assessment Report

3. Columns listed below will not be populated for contract imported inventory across the online/offline reports in portal. This is similar to the manual CSV imported inventory.

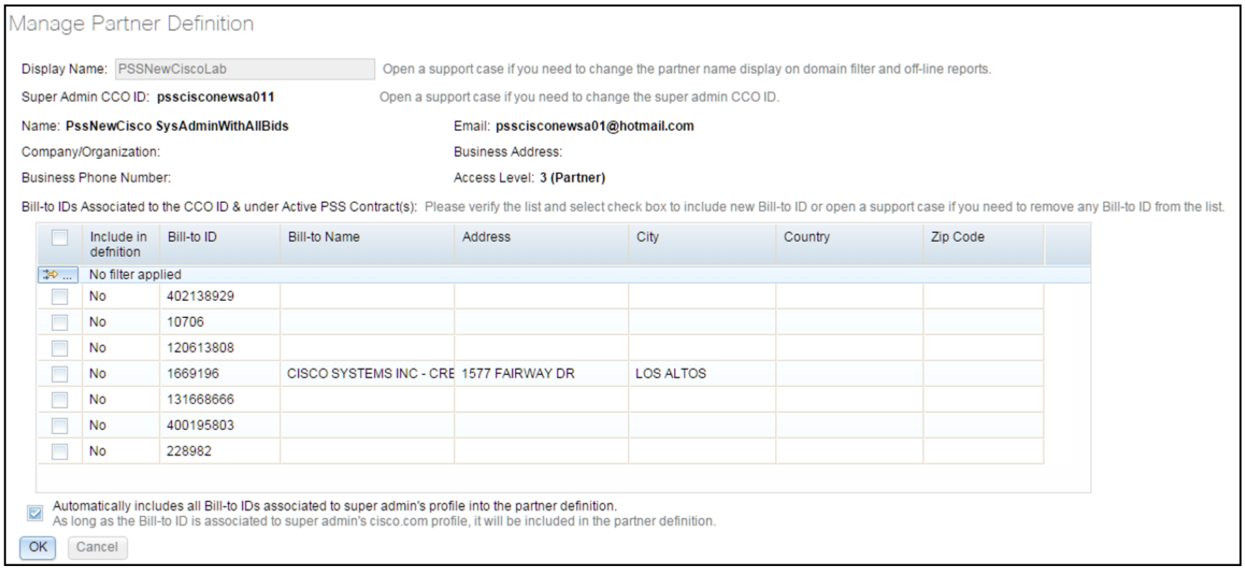
    - Running Config
    - Startup Config
    - Show Command
    - Download Config

- Flash Memory
- Installed RAM
- Manufacturer

The Collection – Inventory Details, which shows the processing detail breakup will not be accurate for this non-standard imports.

Manage Partner Definition

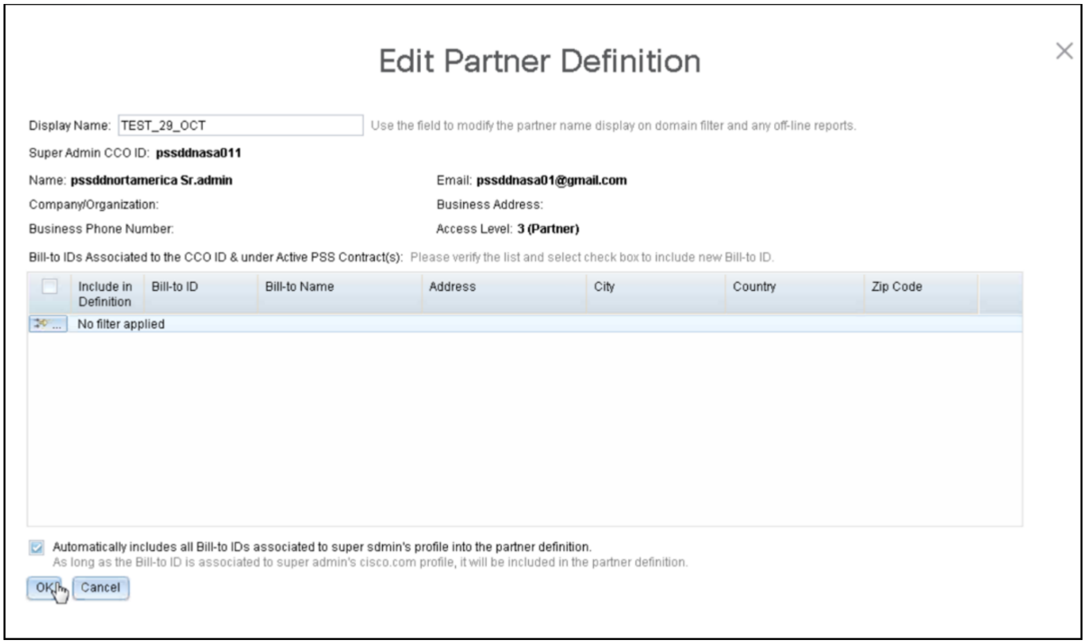
New Partner Definitions are created by Cisco Support personnel, then the Partner Super Administrator then manages the Partner Definition in the PSS portal under Actions.



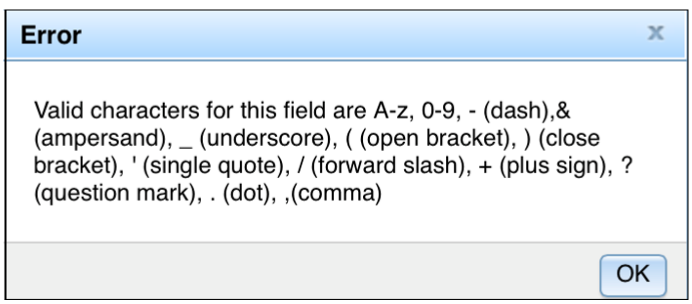
The Super Administrator modifies the Partner Definition by associating new Bill-to IDs to the CCO ID.

Editing Partner Definition

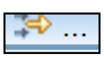
Edit Partner Definition dialog box popup opens to display the partner profile data.

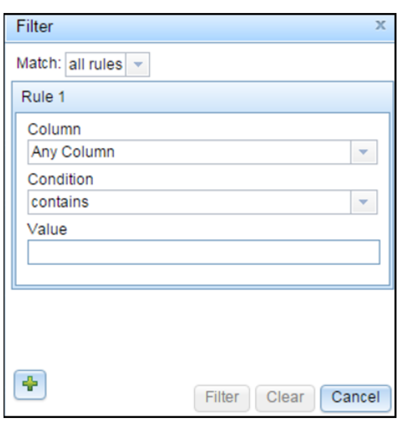


Here you can edit the Display Name (this will be shown in the portal and on any off-line reports) and select the Bill-to IDs to be associated to the Partner Super Admin's CCO ID. The supported characters for Partner Definition naming should follow the below criteria for a valid name:



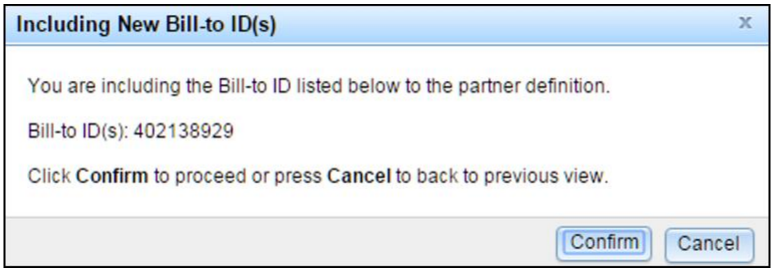
Editing Bill-to IDs in the Partner Definition

1. Use the filter icon  to filter the data in the grid based on criteria and value.



2. This filter is different from the Data Filters, which has a widespread effect on all the data views. You can set a rules that matches the criteria: select any or a specific column, set the condition and enter the search string as value. Additional rules can be added to the criteria. Once set, click **Filter** to segregate based on the rule set in the filter.

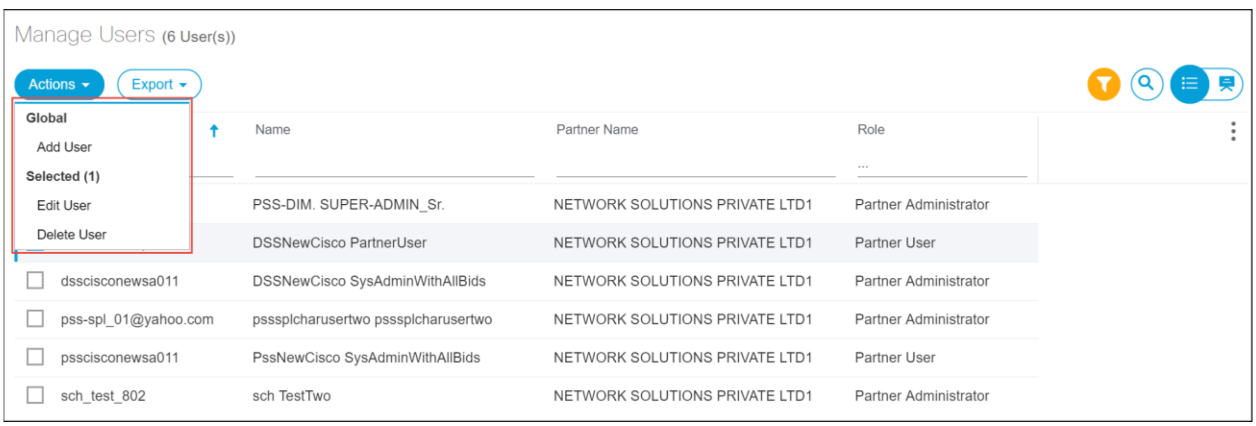
3. If desired you can select the check box to automatically include all the Bill-to IDs associated to the Super Administrator's cisco.com profile. Or select the Bill-to IDs to associate to the displayed CCO / PSS contract and click **OK**.



4. Verify the Bills-to IDs and click **Confirm** to proceed. The IDs are added and the Partner Definition is updated successfully.

Manage Users

The Manage Users data grid provides the Partner Super Admin and Partner Administrators with a list of all the Partner Users and Partner Administrators registered to use the PSS portal for their partner company. The Partner Super Administrator and Partner Administrator can add, edit or delete portal users using the Manage Users grid, available under **Actions**, and assign either the Partner Administrator or Partner User role to their employee.



Column Headings and Definitions:

CCO ID: The unique Cisco.com ID of a portal user assigned either a Partner Administrator or Partner User role.

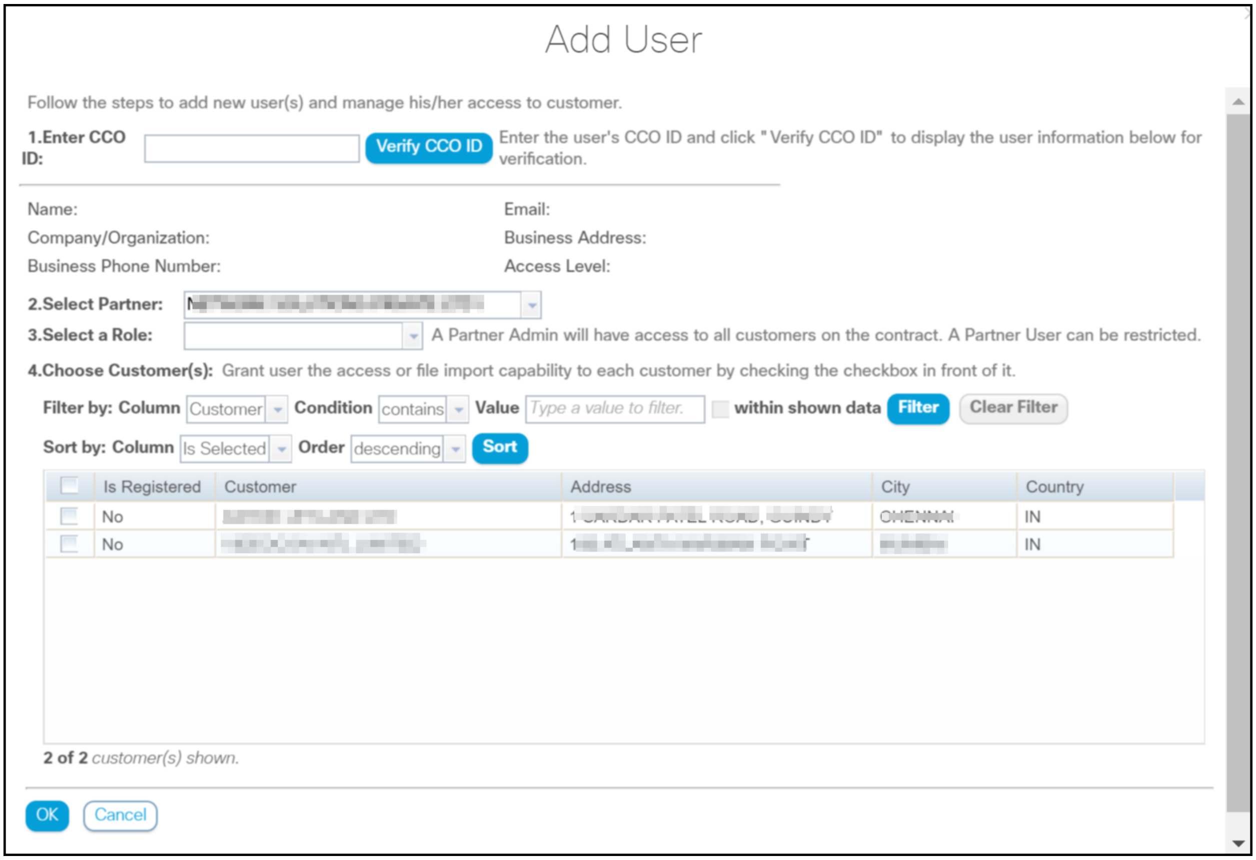
Name: Name of the user who is granted access.

Partner Name: Name of the partner company that this user belongs to.

Role: The user role assigned to this user's CCO-ID on the PSS portal, either Partner Administrator or Partner User.

Add User

Only the Super Administrator and Partner Administrators can add users and assign roles. In the **Actions** > **Manage Users** grid, click **Actions**, then select **Add User**. In the **Add User** form, follow the below steps:



1. Enter CCO ID and click the Verify CCO ID button. If a valid CCO ID is entered then the profile data of the user is populated and displayed.

Note

   a. Ensure that the correct CCO ID of the user is entered one with Partner Access level 3.

   b. Clicking Verify CCO ID ensures a valid CCO ID was entered and also allows you to review the user is the one you wish to assign to your company's Partner Definition.

   c. Incorrect CCO IDs will provide portal access to wrong users.

   d. Incorrectly added user can be deleted by any Partner Administrator or the Super Administrator.

2. Select a Partner from the drop-down list.

3. Select a **Role** to be assigned from the drop-down list; either **Partner Administrator** or **Partner User**.

Note By default, if Partner Administrator is selected, all customers are selected for registration. The Partner Administrator role cannot be granted for individual customers, only all customers.

4. Select the customers from the available list (for Partner User role only).

   - For accounts with multiple customers you can apply filters to focus the list.

For example:

1. To list customers that begin with the name of *Bank*, perform the following:

   - Select **Customer** from Filter by: Column drop-down list.

- Select **Contains** from **Condition** drop-down list.
- Type **bank** in the **Value** text box and click **Filter**. Customer names that contains bank are displayed.

  To sort columns in either ascending or descending order, perform the following:

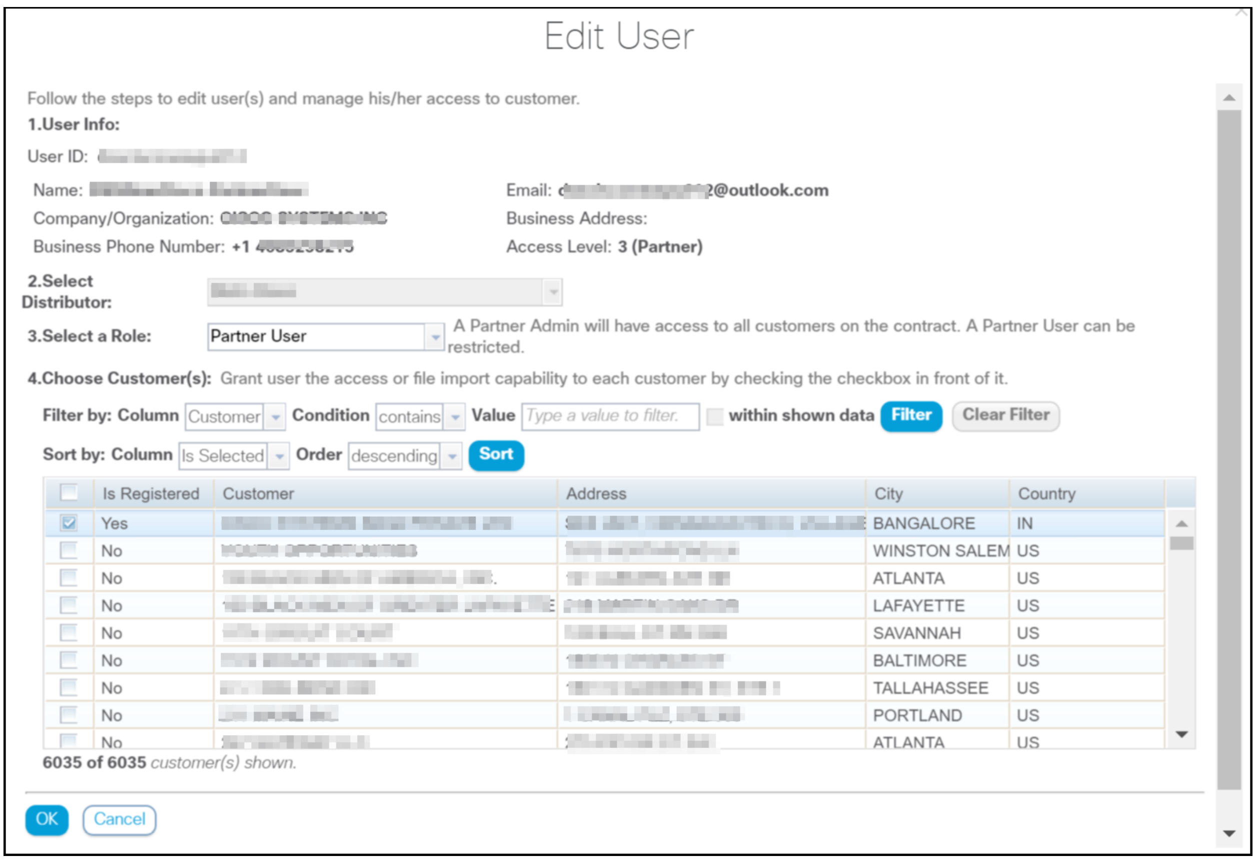
2. Select the desired value from the **Sort by: Column** drop-down list.
3. Select the either **Ascending** or **Descending** from the **Order** drop-down list and click **Sort**.
4. Click **OK**. A message indicating the user has been successfully registered for the selected customers is displayed.

With access granted Partner Administrators can register collectors for the partner's customers. Refer to Manage Collectors.

Edit User

A Partner Administrator can modify the details of a user.

1. Click the checkbox to the left of a row on the **Manage Users** report
2. Click on the **Action** menu icon and then select **Edit User** from the menu.

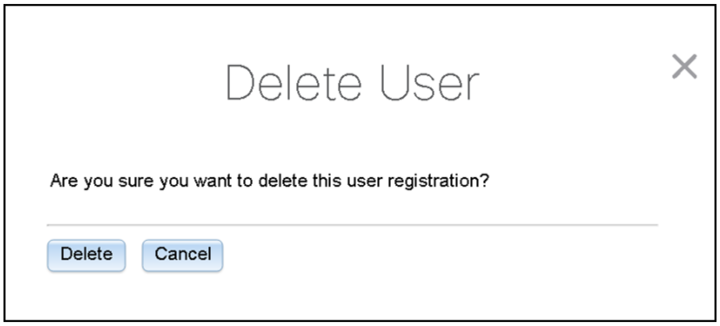


3. As a Partner Administrator, you can change the role of the selected Partner User and select the customers whose data the user is entitled to see.

Delete User

A Partner Administrator can delete a user's access to the PSS portal.

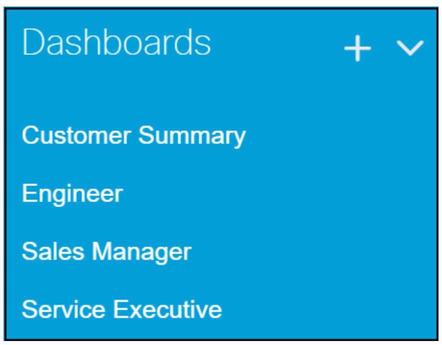
1. Click the checkbox to the left of a row on the Manage Users report
2. Then select **Delete User** from the **Actions** menu. The Delete User window appears to confirm to delete the selected user.



3. Click **Delete** to delete the user's access.

Dashboards

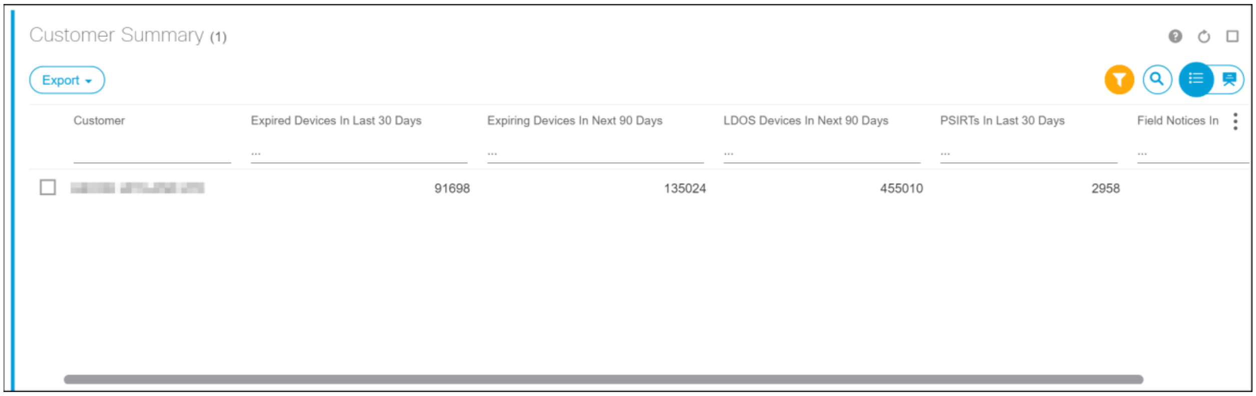
There are four default dashboards in the Dashboard category. Click **+** to add a new dashboard. You cannot delete the default dashboards. If you want to make changes to a default dashboard, first save it with a different name and later make the changes.



Customer Summary

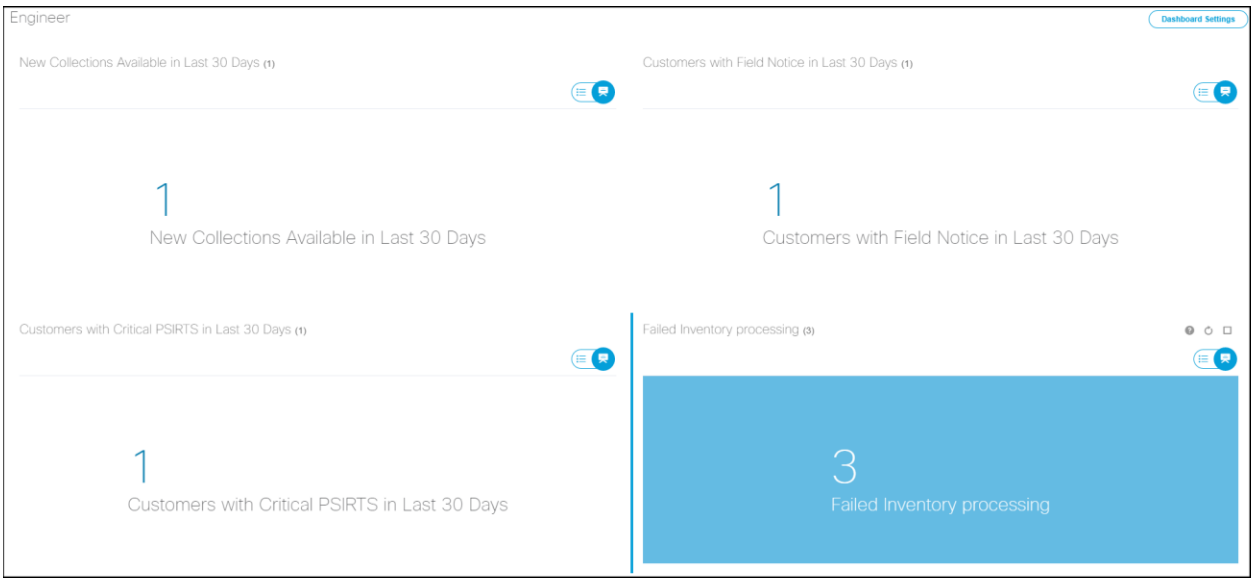
The **Customer Summary** report appears the first time you log in to PSS portal. This default high-level view of the health of your customers' network presents you with a list the customers' inventories you have selected in the Data Filters along with a count of devices with recent or upcoming changes that may require your attention.

Note The count of devices in the Customer Summary includes devices that are "Covered by Other", indicating the contract is held by a different partner. When you run the report from the **Library > Expiring Contracts**, devices "Covered by Other" will not be included therefore the count of items may not match the Customer Summary.



Engineer

The **Engineer** dashboard presents four billboard summary reports showing status for your customer's inventory collection uploads and customers selected in the [Data Filters](#) who have devices affected by recent Field Notices and Critical PSIRTs.

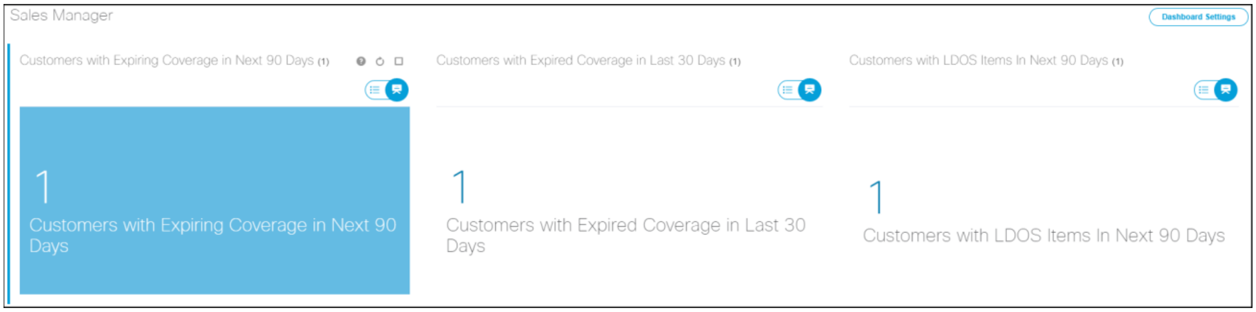


- The **New Collections Available in Last 30 Days** billboard report displays all inventory uploads that were processed in last 30 days, and their associated status.
  - Network and deployment engineers use this report to determine if all of their customers' inventories are successfully uploading on the expected schedule.
  - Click the status for an individual upload to see details about the inventory collected. If items were not processed, choose **Generate Reports > Not Processed Device Report** to see a listing of chassis and cards that were not processed. Items may not have been processed because there are not yet processing rules in the PSS data center or because there was a data discrepancy in one of the Cisco databases.
- The **Customers with Field Notices in Last 30 Days** billboard displays the count of customers who have devices in their inventory with Field Notice alerts reported within 30 days of their most recent inventory upload.
- The **Customers with Critical PSIRTs in last 30 Days** billboard displays a count of customers having devices in their inventory with critical PSIRT alerts reported within 30 days of their most recent inventory upload.

- The **Failed Inventory Processing** billboard report notifies you if any of your customer's inventory uploads were not successful. The collected inventory may need to be uploaded again.

Sales Manager

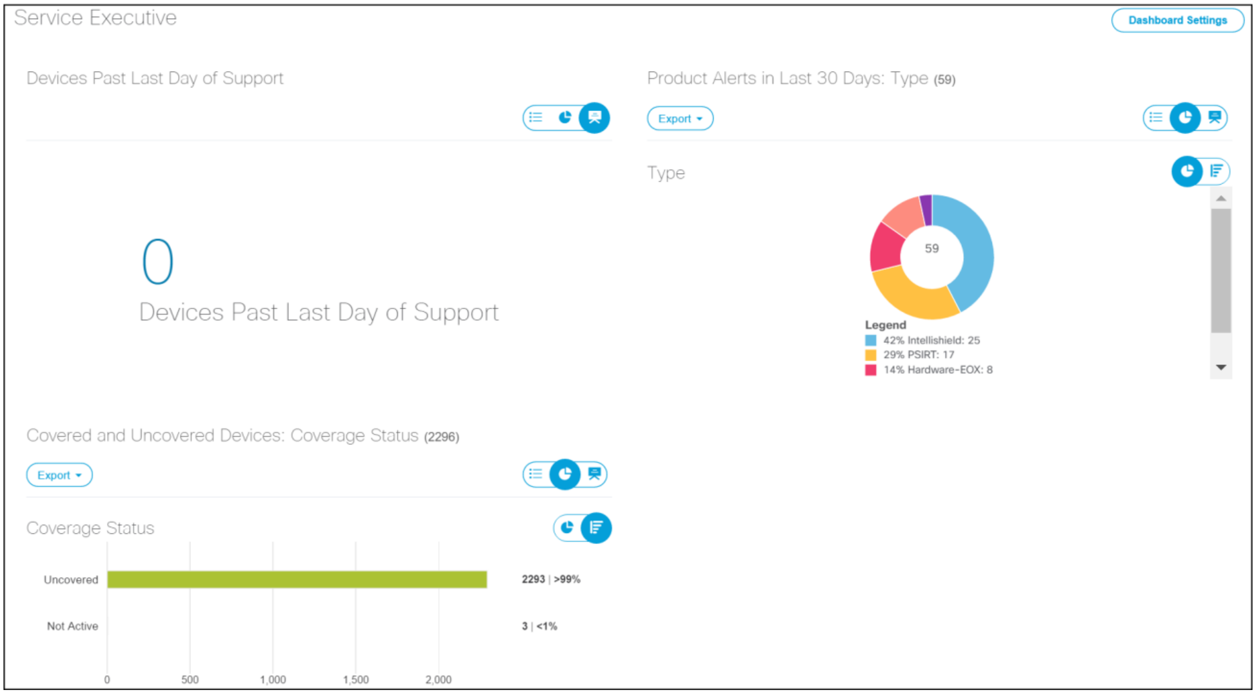
- The **Sales Manager** view presents three billboards that summarize how many customers have been affected by recent or upcoming changes to devices in their collected inventory.



- The billboards are based on the customers and inventories selected in the Data Filters.
- The **Customers with Expiring Coverage in Next 90 Days** billboard shows how many of your customers have device(s) with service contract coverages that will expire within 90 days of the most recent inventory upload.
- The **Customers with Expired Coverage in Last 30 Days** billboard shows how many of your customers have device(s) with expired contract coverage in the 30 days before the most recent inventory upload.
- The **Customers with LDOS Items in Next 90 Days** billboard displays the count of customers who have devices that will reach their last day of support within 90 days. When you click the billboard you will see the list of customers and a count of how many devices each customer has with a last 90 days of support. This high level view can be used to determine the potential opportunities.

Service Executive

The **Services Executive** presents two interactive chart summaries and one billboard view that are based on the customers and inventories selected in the Data Filters.



- The **Devices Past Last Day of Support** report counts devices that are no longer supported by Cisco and therefore have no support contract. These devices need to be replaced by newer versions. Click the billboard to see a table that lists each device past last day of support.
- The **Product Alerts in Last 30 Days** billboard shows both the count and the percent of devices affected by the five different types of product alerts reported within 30 days of the most recent inventory upload. Click the alert type in the pie chart to see a table of all alerts of that type. Double-click a line item to see details about the alert including information about the devices in the customer's inventory affected by the alert.
- The **Covered and Uncovered Devices: Coverage Status** billboard shows the count and percent of devices covered by an active support contract, covered by another partner, not active and not covered.

Working with Dashboards

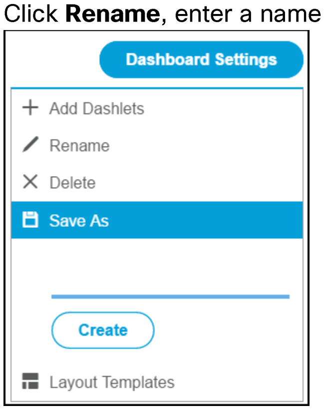
This section provides information to create and manage you own custom dashboard views:

Creating Custom Dashboard

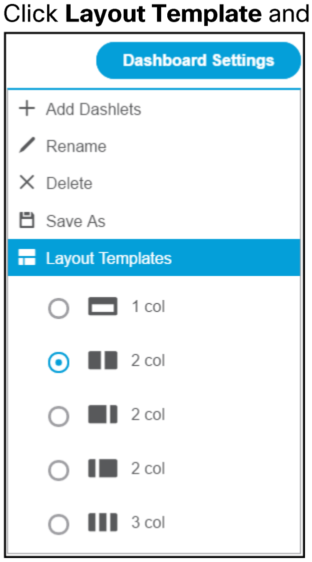
The purpose of a dashboard is to view multiple reports in one content area. In this section, you are going to see how to create a dashboard that contains all the contract report information in one dashboard view. Since the Customer Summary and three default dashboards cannot be deleted from the Dashboard, you must either save as a different name then make the changes.

To create a dashboard, perform the following steps:

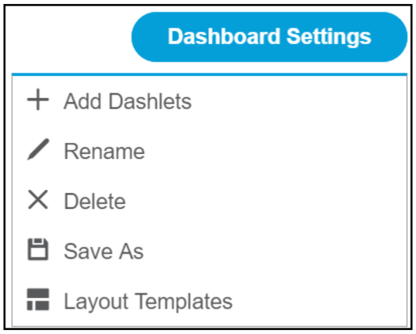
- Click **+** in navigation pane next to the Dashboard category.
- The **New Dashboard** is created and highlighted in the navigation panel.
- Click the **Dashboard settings** button as shown below.
- Click **Rename**, enter a name for the new dashboard and click the **Apply** button.



- Click the **Dashboard settings** button.
- Click **Layout Template** and select a 1, 2, or 3 column layout.



- Select **+ Add Dashlets** from the Dashboard settings menu and select the required report(s) to be saved in the new dashboard. Each dashlet you select will be listed as an element in the Dashboard drawer to be accessed when needed.

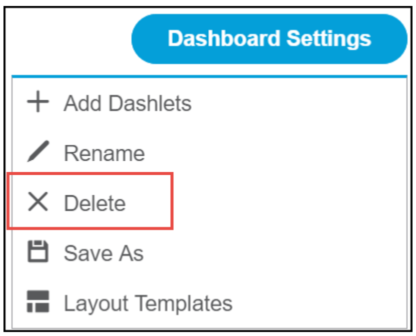


- The dashboard automatically saves and is now displayed in the Dashboards.

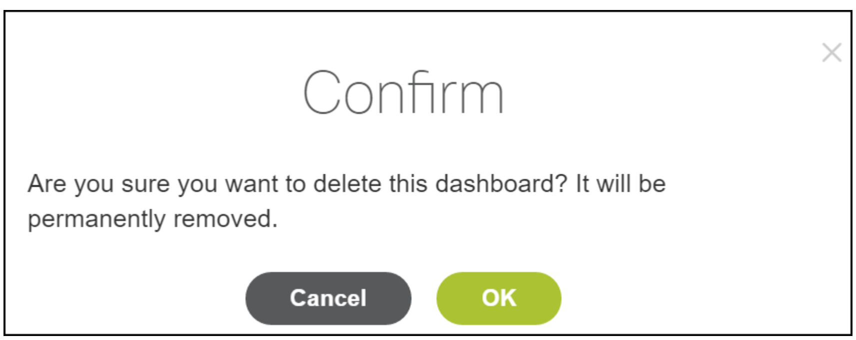
Deleting Custom Dashboard

To delete a custom dashboard view, perform the following steps:

1. In the navigation pane, select the dashboard you want to delete.
2. Click the **Dashboard Settings** button.



3. Select **Delete** from the menu.



4. Click **OK** to confirm the deletion.

Note This does not delete the actual report(s) that were saved in the dashboard.

Editing Dashboard

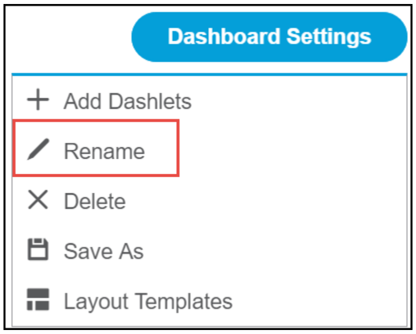
Changes that you make to a saved custom dashboard such as adding or deleting reports are saved automatically.

1. Select the custom dashboard you want to modify in the navigation pane.

2. From the **Dashboard Settings** menu, select **Save As** and enter a name.
3. To move a dashlet report to a different dashboard pane, click and drag the report, releasing the mouse when a dotted line appears in the content pane.

Renaming Dashboard

To rename a custom dashboard, perform the following steps:



1. Select the dashboard you want to rename in the navigation pane.
2. From the **Dashboard Settings** button, select the **Rename** option, enter a new name and click **Apply**.

Note The four default dashboards cannot be renamed. To create a new, duplicate copy of a default dashboard, select **Save As** from the Dashboard Settings menu. Then you can modify the dashboard by adding or removing dashlets.

Exporting Reports

For information on how to export a report see Export.

Library

The Library pane of the PSS portal contains report categories with their associated report(s).

Expand or collapse the respective report category to view/hide the reports that are associated with each report category.

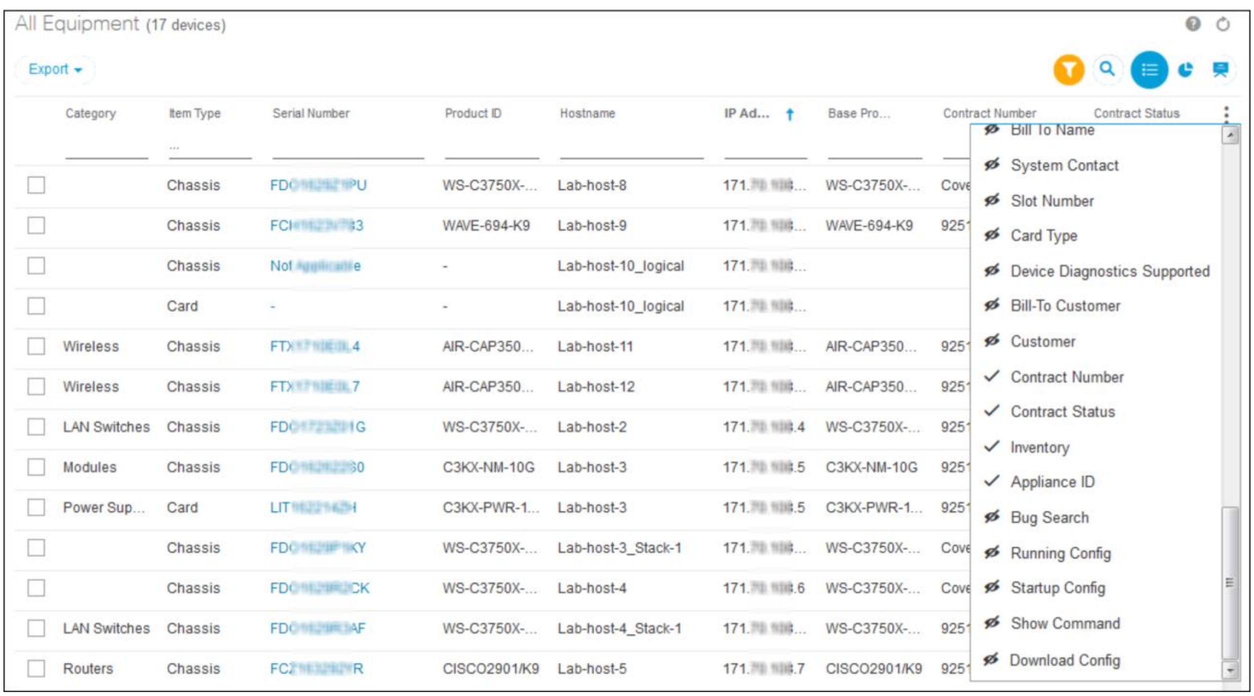
Inventory

This section contains the following types of Inventory reports to support management of your customer's installed base:

- All Equipment
- Covered Items
- Devices with Alerts
- Inventory Collection
- Inventory Delta
- Last Date of Support
- Uncovered Items

All Equipment

The **All Equipment** report provides you with a list of all devices for the customer(s)/partner(s) selected in the Data Filters. Both processed and non-processed devices will be displayed. The report also provides the device warranty information (if required) to help you determine whether service coverage is needed for the specified product IDs.



Note The Contract status available in the All Equipment report combines Covered Items, Uncovered Items, and those items with overdue and terminated contracts. You can drill down by clicking the items that appear in blue to get the list of equipment.

Column Headings and Definitions:

Category: The Category of the item displayed.

Item Type: Is the classification of an item as a CCM, Card, Chassis, IPPHONE, TP, or UCS.

Serial Number: The serial number of discovered device that was validated against the Cisco records.

Product Family: Grouping of similar Cisco Product Models.

Product Name: The name of the product.

Product ID: The product id of a discovered device that was validated against Cisco records.

Hostname: The name of the host where this device was discovered.

IP Address: IP Address of the physical entity. The address is a unique string of numbers separated by periods that identifies each computer using the Internet Protocol to communicate over a network.

Product Description: The detailed description of the device or card found in the inventory.

Collected Serial Number: The actual Serial Number of the item collected from the network. In some cases, this serial number may be different from what is found in Cisco's contract databases.

Product Model: The model of product (for example, modules, routers, power supplies).

Equipment ID: A unique Identification number of the equipment.

Orig. Inv. Date: Is the date when the first inventory was collected.

Last Inv. Date: Is the date the last inventory collection ended.

Base Product ID: The product ID of a discovered device that was validated against Cisco records.

Installed Ram: The information related to the RAM installed.

HW Version: The version of the hardware installed on the item.

SW Version: OS Version of the software installed on the item.

SW Type: OS Type of the software.

Flash Memory: The information related to the memory on the item.

Manufacturer: The name of the manufacturer of the item.

C3 Instance ID: A unique identification number that is issued by Cisco to refer to a specific piece of equipment within Cisco's IB records.

Ship Date: The date the item was initially shipped from Cisco.

OS Version: The version of the OS installed on the item.

Boot Version: The version of the bootable OS installed on the item.

Feature Set: The set of the features installed on the item.

Category Long Name: The detailed name of the category of an item.

SNMP Location: The SNMP location of the installed item.

Ship-to Address: The Address noted for the shipment in the Cisco Site record.

Installed-at Address: The first Address line noted in the Cisco Install Site record.

Installed-at City: The City noted in the Cisco Install Site record.

Installed-at Country: The Country noted in the Cisco Install Site record.

Bill-to Name: The name to be billed for the items.

System Contact: The contact details for the system.

Slot Number: The slot number of the item.

Card Type: The type of card used for the item.

Device Diagnostics Supported: Indicates whether the device meets all of the criteria for support of the Device Diagnostics / Smart Call Home capability.

Bill-To Customer: The name of the customer to be billed for the items.

Customer: The Customer that was selected in the Cisco Services Connection Data Filters customer drop-down.

Contract Number: Is the contract identifier of the Cisco Service Contract coverage for the specified product id and serial number.

Contract Status: Status of the contract - Active, Expired, Overdue, Terminated.

Inventory: The name assigned to the inventory.

Appliance ID: A unique identifier of an appliance.

Bug Search: Directs to the Bug search tool. Click View Results for one line item, parameters are passed to the tool based on the item type selected. Refer the Bug Search Tool for more information.

Running Config: Provides a link to the running configuration details.

Startup Config: Displays a link that directs to the startup configuration details page of the respective device.

Show Command: Displays a link that directs to the details page of the respective device.

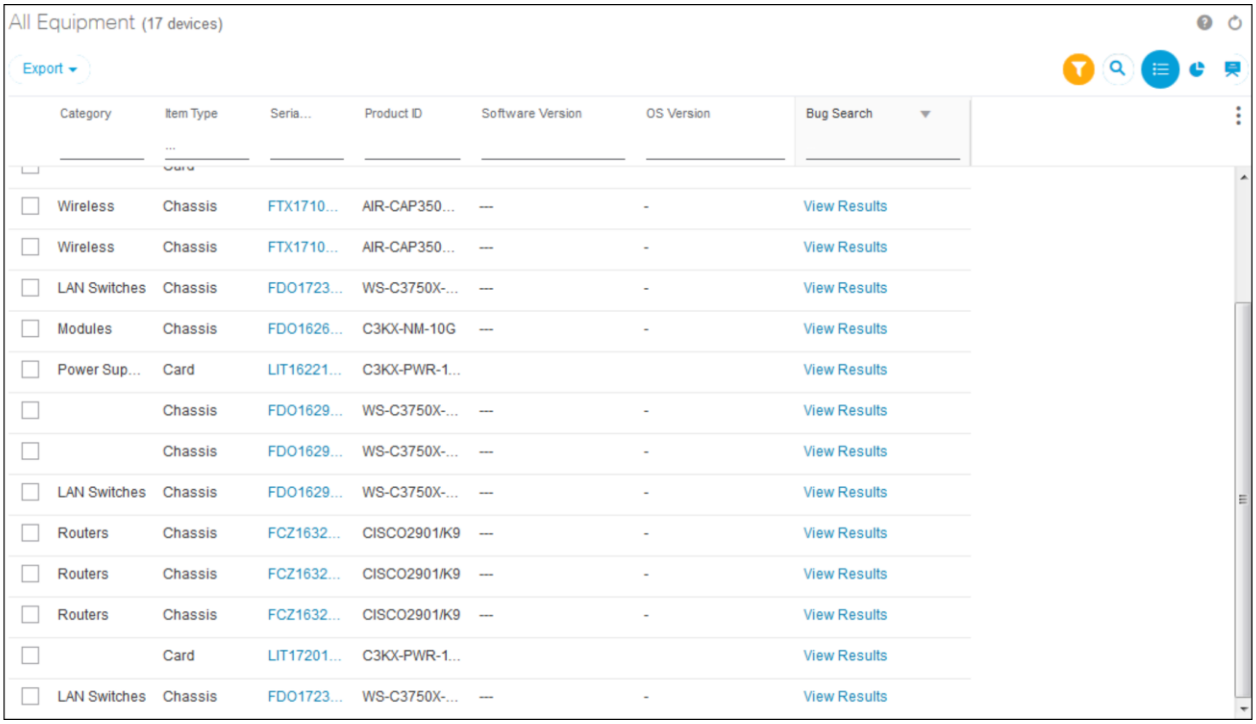
Download Config: A link to download the configuration details.

Bug Search Tool

From the PSS portal, you can launch the **Bug Search Tool** to find defects that are open for selected hardware. Perform the following steps to launch and pass the parameters and search the relevant bugs:

1. Select one or more CUSTOMERS and one or more INVENTORIES in the Data Filters.

2. From the **Library**, select **Inventory > All Equipment**.



All Equipment (17 devices)

Export

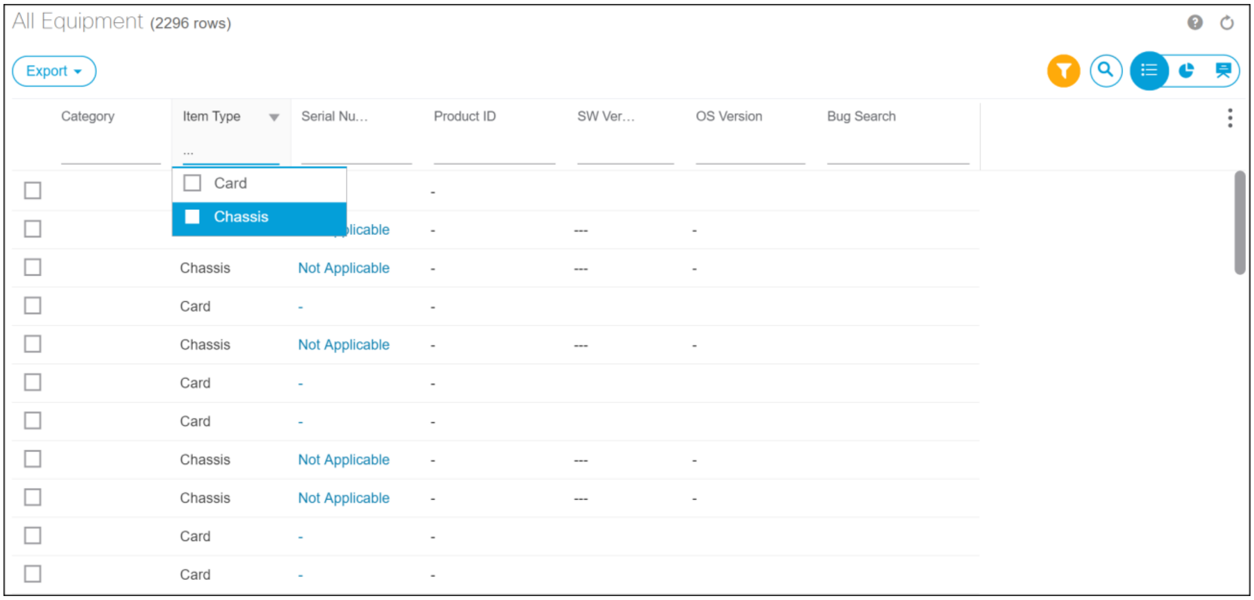
	Category	Item Type	Seria...	Product ID	Software Version	OS Version	Bug Search
	Wireless	Chassis	FTX1710...	AIR-CAP350...	---	-	View Results
	Wireless	Chassis	FTX1710...	AIR-CAP350...	---	-	View Results
	LAN Switches	Chassis	FDO1723...	WS-C3750X-...	---	-	View Results
	Modules	Chassis	FDO1626...	C3KX-NM-10G	---	-	View Results
	Power Sup...	Card	LIT16221...	C3KX-PWR-1...			View Results
		Chassis	FDO1629...	WS-C3750X-...	---	-	View Results
		Chassis	FDO1629...	WS-C3750X-...	---	-	View Results
	LAN Switches	Chassis	FDO1629...	WS-C3750X-...	---	-	View Results
	Routers	Chassis	FCZ1632...	CISCO2901/K9	---	-	View Results
	Routers	Chassis	FCZ1632...	CISCO2901/K9	---	-	View Results
	Routers	Chassis	FCZ1632...	CISCO2901/K9	---	-	View Results
		Card	LIT17201...	C3KX-PWR-1...			View Results
	LAN Switches	Chassis	FDO1723...	WS-C3750X-...	---	-	View Results

3. Simplify the report to display only those required columns to find defects such as show below

Show Columns	**Hide Columns**
Category	Product Family
Item Type	Product Name
Serial Number	Hostname
Product ID	IP Address
SW Version	
OS Version	
Bug Search	

4. It is also recommended to filter the **All Equipment** report to display one Item Type at a time. The possible options include:

- CCM
- Card
- Chassis
- IPPHONE
- TP
- UCS

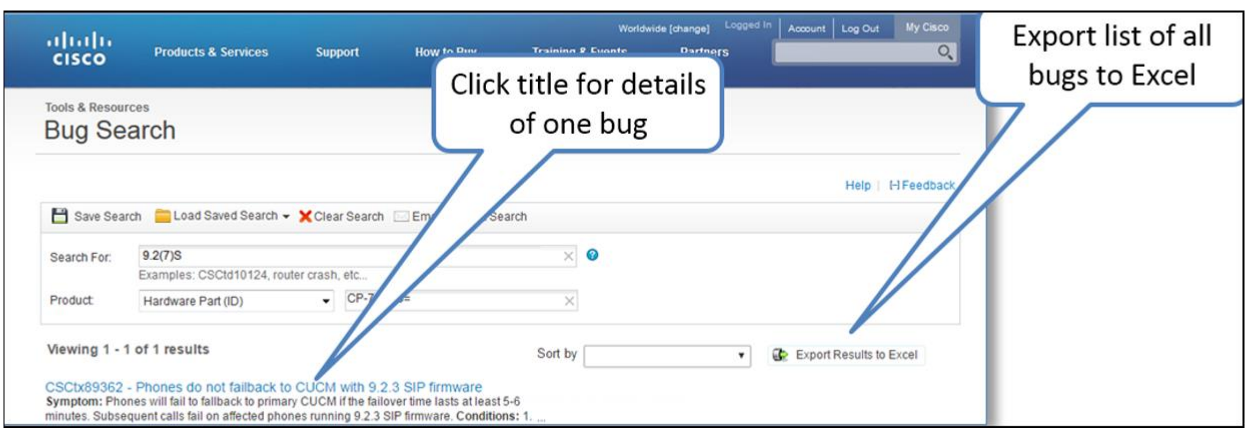


Note Dashes [---] in the Bug Search column indicate that the tool is not available because item is a 3rd party device or a device without enough information collected.

5. Click **View Results** for one-line item. Parameters passed to the Bug Search tool are based on the Item Type selected.

   - CCM, Chassis, TP and UCS pass the OS Version and Product ID
   - Cards pass Product ID
   - IP Phones pass SW Version and Product ID.

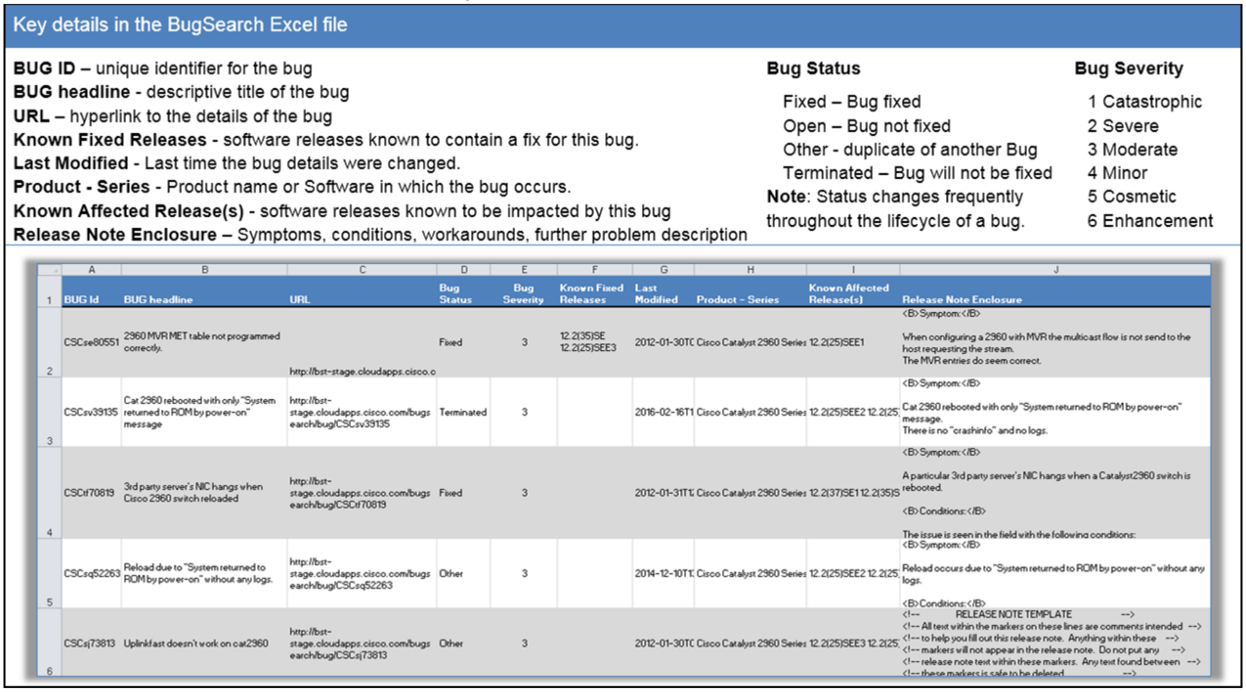
6. The Bug Search Tool is opened and a search is made using the parameters passed to the tool.



The Product ID and other parameters passed to the tool from the PSS portal are used in the search for bugs affecting the Product ID.

- Export results to Excel or
- Click the Bug title for more details.

A sample excel file exported from the Bug search tool.



Key details in the BugSearch Excel file

BUG ID – unique identifier for the bug
BUG headline - descriptive title of the bug
URL – hyperlink to the details of the bug
Known Fixed Releases - software releases known to contain a fix for this bug.
Last Modified - Last time the bug details were changed.
Product - Series - Product name or Software in which the bug occurs.
Known Affected Release(s) - software releases known to be impacted by this bug
Release Note Enclosure – Symptoms, conditions, workarounds, further problem description

Bug Status

Fixed – Bug fixed
Open – Bug not fixed
Other - duplicate of another Bug
Terminated – Bug will not be fixed

Note: Status changes frequently throughout the lifecycle of a bug.

Bug Severity

1 Catastrophic
2 Severe
3 Moderate
4 Minor
5 Cosmetic
6 Enhancement

	A	B	C	D	E	F	G	H	I	J
1	BUG Id	BUG headline	URL	Bug Status	Bug Severity	Known Fixed Releases	Last Modified	Product - Series	Known Affected Release(s)	Release Note Enclosure
2	CSCse80551	2960 MVR MET table not programmed correctly.	http://bst-stage.cloudapps.cisco.c	Fixed	3	12.2(35)SE 12.2(25)SEE3	2012-01-30T(	Cisco Catalyst 2960 Series	12.2(25)SEE1	<B>Symptom:</B> When configuring a 2960 with MVR the multicast flow is not send to the host requesting the stream. The MVR entries do seem correct.
3	CSCsv39135	Cat 2960 rebooted with only "System returned to ROM by power-on" message	http://bst-stage.cloudapps.cisco.com/bugsearch/bug/CSCsv39135	Terminated	3		2016-02-16T1	Cisco Catalyst 2960 Series	12.2(25)SEE2 12.2(25)	<B>Symptom:</B> Cat 2960 rebooted with only "System returned to ROM by power-on" message. There is no "crashinfo" and no logs.
4	CSCtf70819	3rd party server's NIC hangs when Cisco 2960 switch reloaded	http://bst-stage.cloudapps.cisco.com/bugsearch/bug/CSCtf70819	Fixed	3		2012-01-31T1	Cisco Catalyst 2960 Series	12.2(37)SE1 12.2(35)S	<B>Symptom:</B> A particular 3rd party server's NIC hangs when a Catalyst2960 switch is rebooted. <B>Conditions:</B> The issue is seen in the field with the following conditions:
5	CSCsq52263	Reload due to "System returned to ROM by power-on" without any logs.	http://bst-stage.cloudapps.cisco.com/bugsearch/bug/CSCsq52263	Other	3		2014-12-10T1	Cisco Catalyst 2960 Series	12.2(25)SEE2 12.2(25)	<B>Symptom:</B> Reload occurs due to "System returned to ROM by power-on" without any logs. <B>Conditions:</B>
6	CSCsj73813	Uplinkfast doesn't work on cat2960	http://bst-stage.cloudapps.cisco.com/bugsearch/bug/CSCsj73813	Other	3		2012-01-30T(	Cisco Catalyst 2960 Series	12.2(25)SEE3 12.2(25)	<!-- RELEASE NOTE TEMPLATE --> <!-- All text within the markers on these lines are comments intended --> <!-- to help you fill out this release note. Anything within these --> <!-- markers will not appear in the release note. Do not put any --> <!-- release note text within these markers. Any text found between --> <!-- these markers is safe to be deleted -->

Covered Items

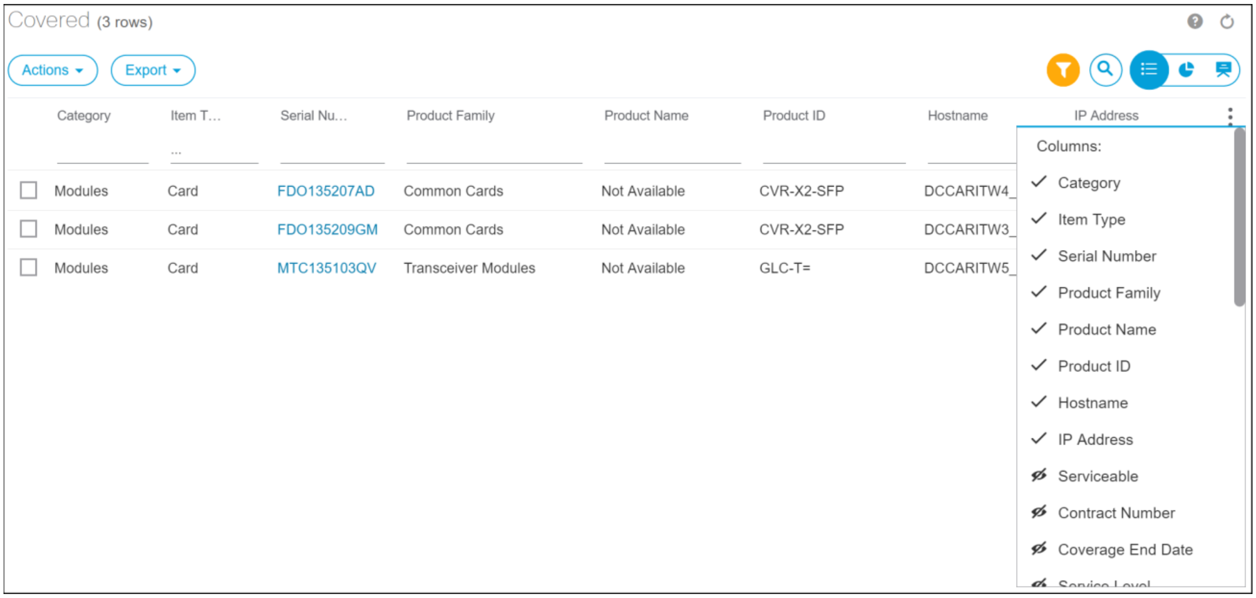
The Covered Items report displays a list of validated items such as chassis, Call Manager (CCM), IP Phone, cards, Unified Computing System (UCS), Telepresence (TP) and Identity Services Engine (ISE) that were discovered for the customer(s)/partner(s) selected in the Data Filters.

The data in this report displays only devices covered by valid contract coverage. The Covered Items report also provides the device warranty information (if required) to determine whether service coverage is needed for the specified PIDs.

Contract managers would typically filter this report to review the contract and support status of their customer's network devices when planning for pending renewals. To do this they would show the " Contract Number" , " Service Level" , " Coverage End Date" and " Last Day of Support" columns.

Support Engineers use this report to confirm service entitlement by searching for a device’s " Product ID" and " Serial Number" ; and then identifying the " Contract Number" and " Installed-At Site Name." These details will be used for PSS foundational services such as partner access to the TAC.

Mouse hover on the left of row, click on **Actions** icon and then select the **CSCC** action to quickly open the Cisco Service Contract Center



Column Headings and Definitions:

Category: The category of the item displayed.

Item Type: Is the classification of an item as a CCM, Card, Chassis, IPPHONE, TP, or UCS.

Serial Number: The serial number of discovered device that was validated against Cisco installed base records.

Product Family: Grouping of similar Cisco Product Models.

Product Name: The name of the product.

Product ID: The product id of a discovered device that was validated against Cisco records.

Hostname: The name of the host where this device was discovered.

IP Address: IP Address of the physical entity. The address is a unique string of numbers separated by periods that identifies each computer using the Internet Protocol to communicate over a network.

Serviceable: Indicates whether the item is serviceable or not. The value is 'N' for not serviceable, and 'Y' if a services price is associated to the item.

Contract Number: The contract identifier of the Cisco Service Contract coverage for the identified Product ID and Serial Number.

Coverage End Date: Date of the service ending.

Service Level: Abbreviated form for the type of service that is active on a Service Contract. (For example, PSUP, PSRT).

Warranty End Date: The End Date of the device warranty.

Warranty Type: The type of the device warranty.

Coverage Start Date: Date of the starting the service.

Customer: The Customer that was selected in the Cisco Services Connection Data Filters customer drop-down.

Installed-At City: The City noted in the Cisco Install Site record.

Installed-At Country: The Country noted in the Cisco Install Site record.

Installed-At Postal Code: The Postal Code noted in the Cisco Install Site record.

Installed-At Province: The Province noted in the Cisco Install Site record.

Installed-At State: The State noted in the Cisco Install Site record.

Instance ID: A unique identification number that is issued by Cisco to refer to a specific piece of equipment within Cisco's IB records.

Inventory: The name assigned to an inventory.

Appliance ID: The unique identifier of an appliance.

Last Day of Support: Day that Cisco will no longer offer the opportunity to purchase service coverage on a particular product.

P/C/S: An indicator that shows whether an item is a Parent, Child, or Stand Alone within a configuration.

Parent Instance ID: Instance ID within a network configuration of the parent item, under which a child item resides, according to Cisco's Installed Base records.

Ship Date: The date the item was initially shipped from Cisco.

SN Entry Type: The type of device (chassis/card).

SNMP SysName: Is the name assigned to a SNMP MIB or the Hostname from CLI data.

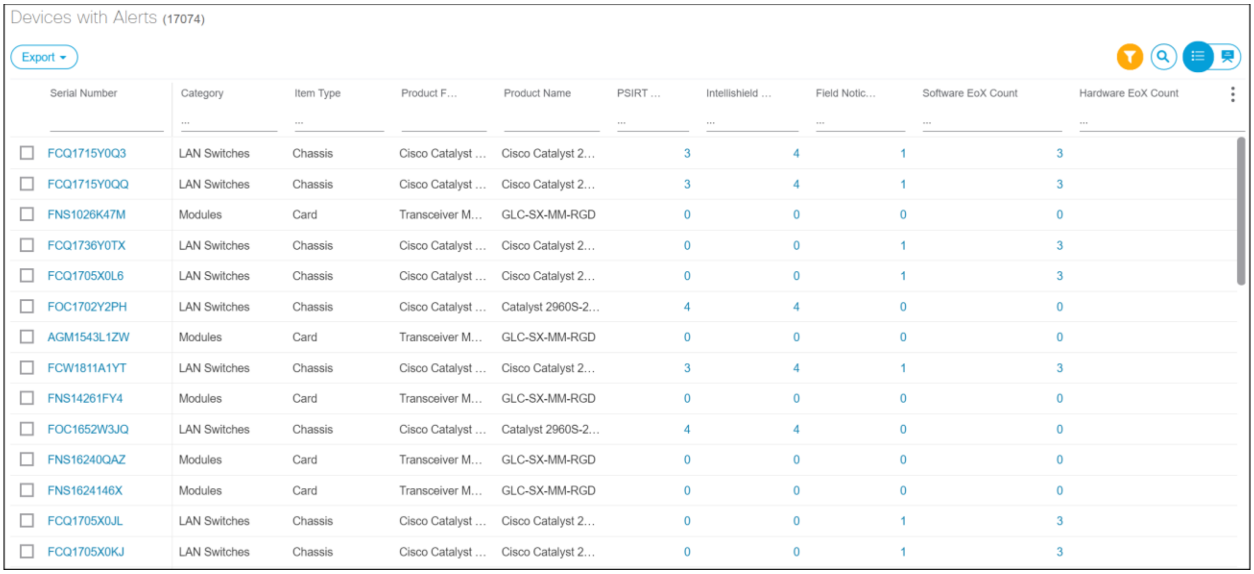
Warranty Start Date: The Start Date of the device warranty.

Devices with Alerts

The Devices with Alerts report provides you with view of devices found to be associated with alerts, for each alert type per device for the customer(s)/partner(s) selected in the **Data Filters**. Support Engineers can refer to this report to evaluate and maintain network health by remediating devices affected by alert issues.

From this report you can access the running Config Details column to link directly to the configuration details for the device impacted by alerts. Similarly the Startup Config Details and Show Command Details columns display links that directs to the details page of the respective device.

Note Config and command details must be enabled for collection on the CSPC collector in order for them to be available in the PSS portal reporting.



Devices with Alerts (17074)

Export

Serial Number	Category	Item Type	Product F...	Product Name	PSIRT ...	Intellishield ...	Field Notic...	Software EoX Count	Hardware EoX Count
FCQ1715Y0Q3	LAN Switches	Chassis	Cisco Catalyst ...	Cisco Catalyst 2...	3	4	1	3	
FCQ1715Y0QQ	LAN Switches	Chassis	Cisco Catalyst ...	Cisco Catalyst 2...	3	4	1	3	
FNS1026K47M	Modules	Card	Transceiver M...	GLC-SX-MM-RGD	0	0	0	0	
FCQ1736Y0TX	LAN Switches	Chassis	Cisco Catalyst ...	Cisco Catalyst 2...	0	0	1	3	
FCQ1705X0L6	LAN Switches	Chassis	Cisco Catalyst ...	Cisco Catalyst 2...	0	0	1	3	
FOC1702Y2PH	LAN Switches	Chassis	Cisco Catalyst ...	Catalyst 2960S-2...	4	4	0	0	
AGM1543L1ZW	Modules	Card	Transceiver M...	GLC-SX-MM-RGD	0	0	0	0	
FCW1811A1YT	LAN Switches	Chassis	Cisco Catalyst ...	Cisco Catalyst 2...	3	4	1	3	
FNS14261FY4	Modules	Card	Transceiver M...	GLC-SX-MM-RGD	0	0	0	0	
FOC1652W3JQ	LAN Switches	Chassis	Cisco Catalyst ...	Catalyst 2960S-2...	4	4	0	0	
FNS16240QAZ	Modules	Card	Transceiver M...	GLC-SX-MM-RGD	0	0	0	0	
FNS1624146X	Modules	Card	Transceiver M...	GLC-SX-MM-RGD	0	0	0	0	
FCQ1705X0JL	LAN Switches	Chassis	Cisco Catalyst ...	Cisco Catalyst 2...	0	0	1	3	
FCQ1705X0KJ	LAN Switches	Chassis	Cisco Catalyst ...	Cisco Catalyst 2...	0	0	1	3	

Column Headings and Definitions:

Category: The category of the item displayed.

Item Type: The classification of an item as a CCM, Card, Chassis, IPPHONE, TP, or UCS.

Serial Number: The serial number of discovered device that was validated against the Cisco records.

Product Family: The Cisco product family to which the product belongs.

Product Name: Displays the name of the product.

PSIRT Count: Total number of active PSIRT alerts for the device.

Field Notices Count: Total number of field notices count for the device.

Software EoX Count: Total number of software EoX count for the device.

Hardware EoX Count: Total number of hardware EoX count for the device.

OS Type: The specific type of the software that is installed on the host/system.

OS Version: The specific version of the software (Software Type) that is installed on the network element.

Running Config Details: A link that directs to the Running configuration details for the device [displayed for the device that have alerts].

Startup Config Details: A link that directs to the Startup Configuration details for the device [displayed for the device that have alerts].

Show Command Details: A link that directs to the Show Command details for Device. [Displayed for the device that have alerts].

Product Description: The description of the product.

Product ID: A unique identification number of the product.

Hostname: Displays the name of the host.

IP Address: IP Address of the physical entity. The address is a unique string of numbers separated by periods that identifies each computer using the Internet Protocol to communicate over a network.

Customer: The customer that was selected in the Cisco Services Connection Data Filters customer drop- down.

Equipment ID: A unique Identification number of the equipment.

Inventory: The name of the inventory given by customers.

Inventory ID: A unique identification of the Inventory.

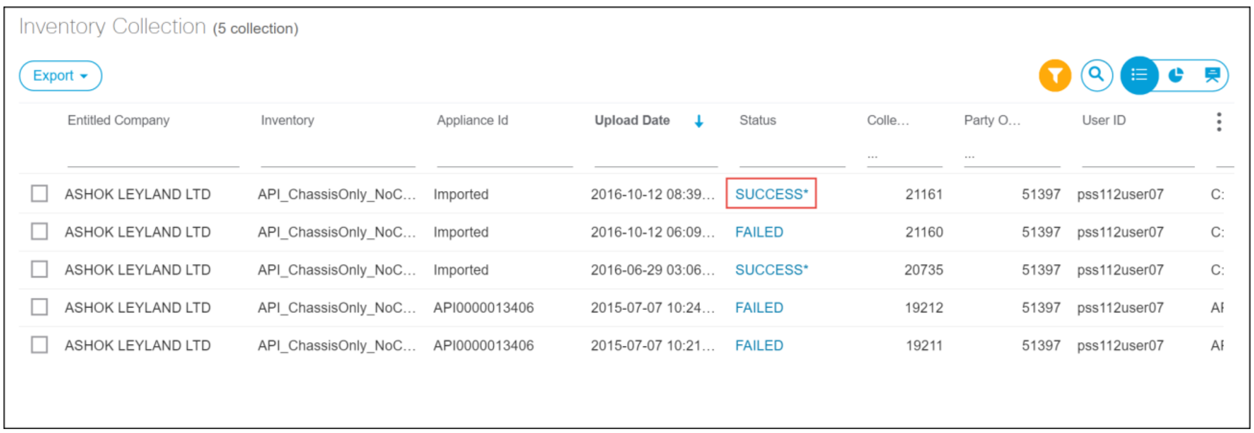
Appliance ID: A unique identifier of an appliance.

Partner Name: Displays the name of the partner.

Customer ID: A unique identification of the Customer.

Inventory Collection

The Inventory Collection report provides you with a list of all the inventories for the customers for this partner. The inventory collection details are used to see if collections and uploads are taking place on the expected schedule. To view the inventory details, click on the status **Success**.



Column Headings and Definitions:

Entitled Company: The name of the customer company that had an inventory collection performed on their network.

Inventory: The name that was given to this inventory that was processed.

Appliance ID: The ID of the appliance that performed the inventory processing.

Upload Date: The date the inventory was uploaded for processing.

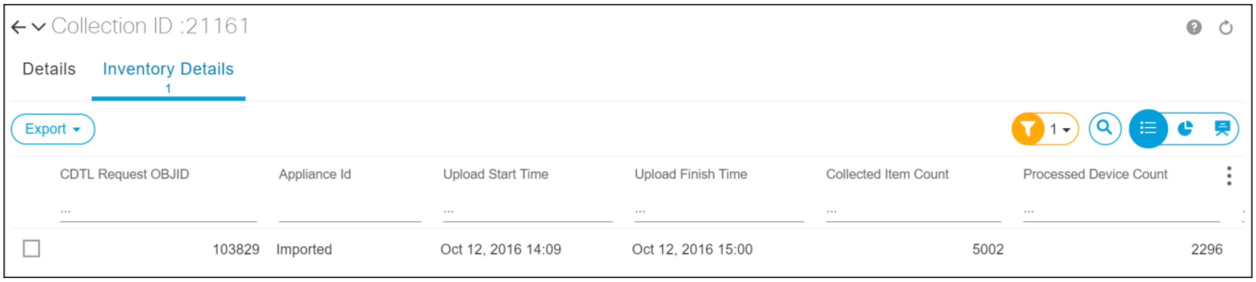
Status: The result of the inventory processing action. [SUCCESS *, PROCESSING, FAILED]

Collection OBJID: The objid has information that is for internal use only.

Party Objid: The objid has information that is for internal use only.

User ID: Is the user ID of the person who requested the inventory collection

The Inventory Details tab provides details on the successful upload of inventory for the customers of this partner. On Failed or Processing status, it does not display any details.



Column Headings and Definitions:

CDTL Request OBJID: Unique Identifier of Collection Detail Trace Log of the inventory.

Appliance ID: Unique Identifier of the appliance that performed the inventory collection.

Upload Start Time: The date and time the inventory upload was started.

Upload Finish Time: The date and time the inventory upload was finished.

Collected Item Count: The number of items collected during collection.

Number of Items Reported: The number of items displayed in the inventory report.

Not Collected Count: The number of items not collected during collection but available in the seed file.

Managed Device Count: The count of the managed devices in an inventory.

Number of Items not Reported: The number of items available in the collection but not displayed in the report because of various fallouts.

Collector Type: The type of collector used for this inventory collection.

Collection OBJID: Unique identifier for this collection.

Inventory Delta

The Inventory Delta report provides you with a list of deltas for the following items with respect to inventory between two specific dates.

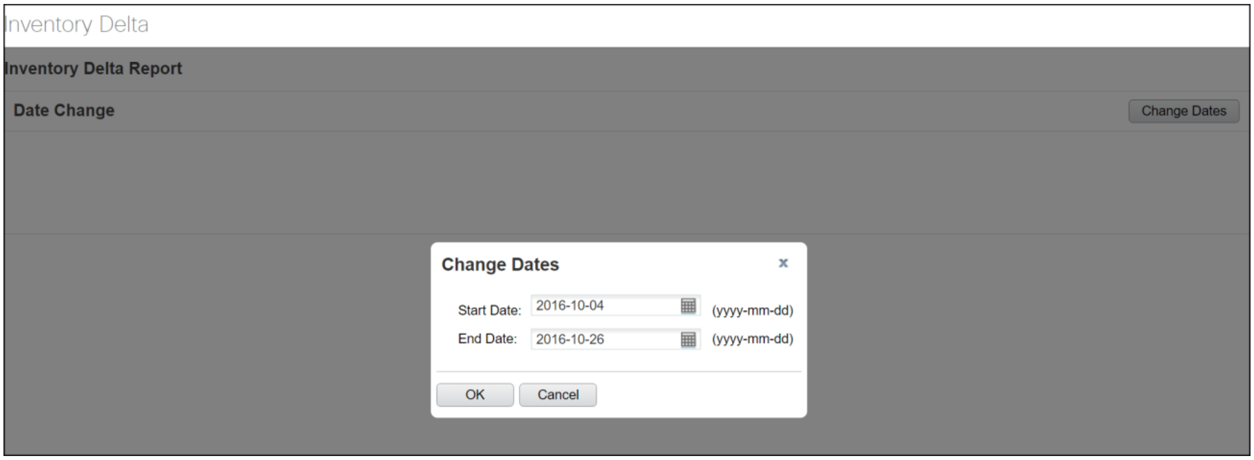
- Changes to the number of items collected based on the contract status of two specific dates.
- Changes to software release versions.
- Each change links to the All Equipment inventory view for items changed between two dates.

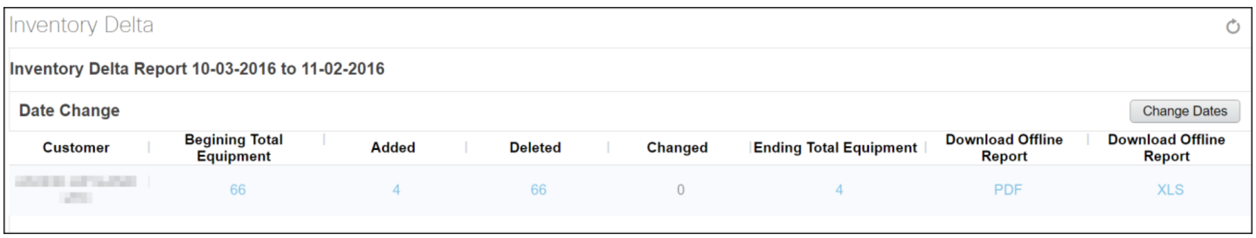
The Inventory Delta report provides information on only one customer inventory. Be sure to select a single inventory from the Data Filters prior to selecting this report from the Library.

1. Make a note of the **Start Date** and **End Date** to be used when you run the Inventory Delta Report. This is found in **Inventory** > **Inventory Collection**.
   - **Start Date** is a previous/older upload date
   - **End Date** is the more recent upload date.
2. Under **Inventory**, select **Inventory Delta**.
3. To set the start and end dates, click **Change Dates**. The Delta Range Setting dialog box appears. You can choose the dates from the calendar and click **Generate**. The Inventory Delta report appears for the selected two specific dates.

4. Click **OK**.

5. Click a blue hyperlink below a field to show a list of devices that have been added, deleted, or changed, or to download an offline PDF or Excel report.





Column Headings and Definitions:

Customer: The name of the customer.

Beginning Total Equipment: Total number of devices that were collected on the start date. The number in this column links to All Items report.

Added: Number of devices added in the collections between the two dates. The number in this column links to the Device Grid.

Note There might be some discrepancies in **Inventory Delta Report** > **Added Equipment Count**. The discrepancy in the Added Equipment LNP is due to the replication of device details with Alerts, Contract details and so on.

Deleted: Number of devices deleted in the collections between two dates. The number in this column links to Device Grid.

Changed: Number of attributes changed in the devices.

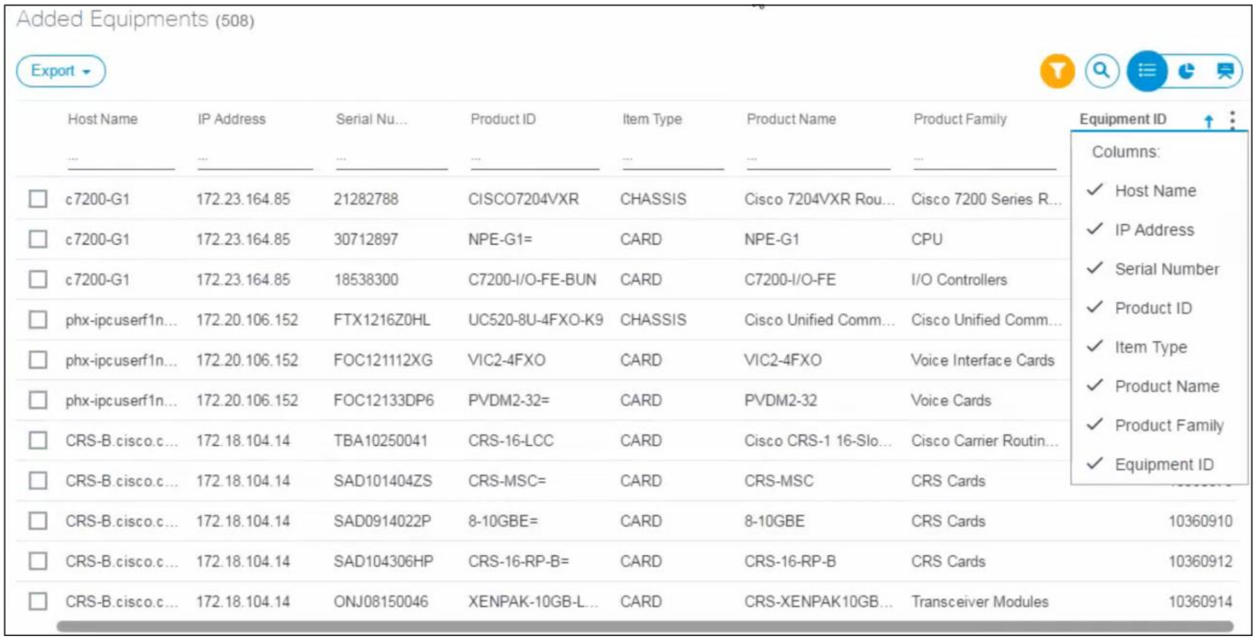
Ending Total Equipment: Total number of devices that were collected on the end date. The number in this column links to Device Grid.

Download Offline Report: The offline report is downloadable in the following required formats – XLS or PDF for the selected two dates. When you click the required format link in the report, the request is submitted for generating the offline inventory delta report. You can then view the delta report under My Reports in the left navigation pane.

Note You cannot traverse back to the Inventory Delta report, after you launch All Items report. You need to click the Inventory Delta again, choose the start/end dates, and then generate the delta report.

Added Drill-Down Report

The Added Equipment report provides information on the device added.



Added Equipments (508)

Export

Host Name	IP Address	Serial Nu...	Product ID	Item Type	Product Name	Product Family	Equipment ID
c7200-G1	172.23.164.85	21282788	CISCO7204VXR	CHASSIS	Cisco 7204VXR Rou...	Cisco 7200 Series R...	
c7200-G1	172.23.164.85	30712897	NPE-G1=	CARD	NPE-G1	CPU	
c7200-G1	172.23.164.85	18538300	C7200-I/O-FE-BUN	CARD	C7200-I/O-FE	I/O Controllers	
phx-ipcuserf1n...	172.20.106.152	FTX1216Z0HL	UC520-8U-4FXO-K9	CHASSIS	Cisco Unified Comm...	Cisco Unified Comm...	
phx-ipcuserf1n...	172.20.106.152	FOC121112XG	VIC2-4FXO	CARD	VIC2-4FXO	Voice Interface Cards	
phx-ipcuserf1n...	172.20.106.152	FOC12133DP6	PVDM2-32=	CARD	PVDM2-32	Voice Cards	
CRS-B.cisco.c...	172.18.104.14	TBA10250041	CRS-16-LCC	CARD	Cisco CRS-1 16-Slo...	Cisco Carrier Routin...	
CRS-B.cisco.c...	172.18.104.14	SAD101404ZS	CRS-MSC=	CARD	CRS-MSC	CRS Cards	
CRS-B.cisco.c...	172.18.104.14	SAD0914022P	8-10GBE=	CARD	8-10GBE	CRS Cards	10360910
CRS-B.cisco.c...	172.18.104.14	SAD104306HP	CRS-16-RP-B=	CARD	CRS-16-RP-B	CRS Cards	10360912
CRS-B.cisco.c...	172.18.104.14	ONJ08150046	XENPAK-10GB-L...	CARD	CRS-XENPAK10GB...	Transceiver Modules	10360914

Column Headings and Definitions:

Hostname: The name of the host where this device was discovered.

IP Address: IP Address of the physical entity. The address is a unique string of numbers separated by periods that identifies each computer using the Internet Protocol to communicate over a network.

Serial Number: The serial number of discovered device that was validated against the Cisco records.

Product ID: The product id of a discovered device that was validated against Cisco records.

Item Type: The classification of an item as a CCM, Card, Chassis, IPPHONE, TP, or UCS.

Product Name: The name of the product.

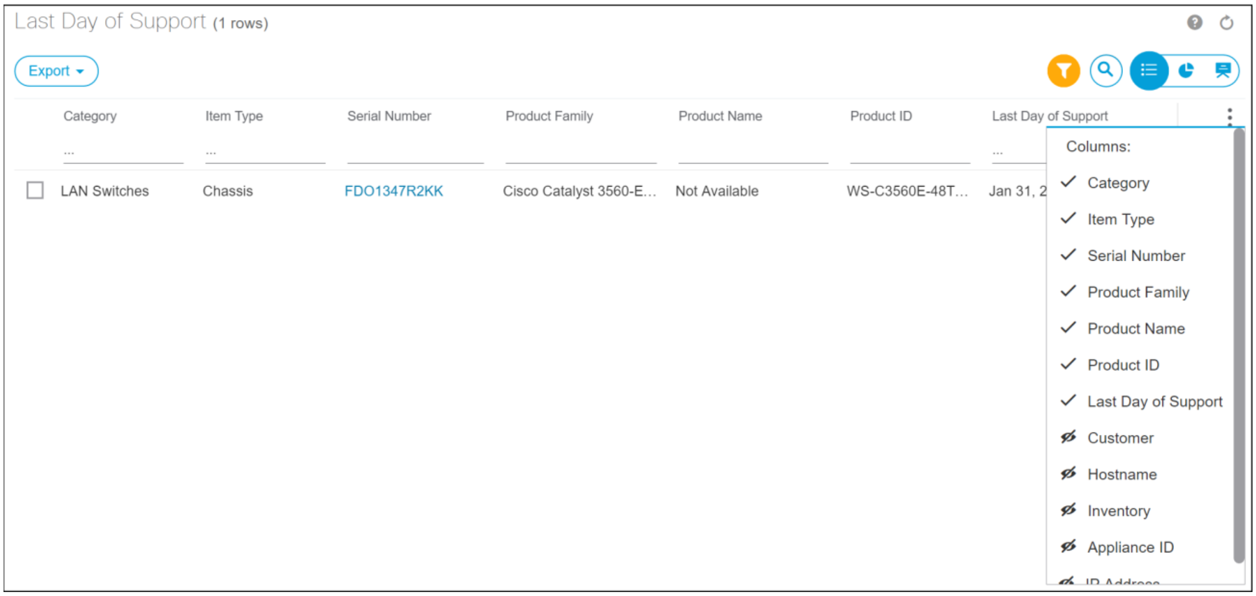
Product Family: Grouping of similar Cisco Product Models.

Equipment Type: A unique Identification number of the equipment.

Last Day of Support

The Last Day of Support report provides a list of covered and validated uncovered items where the LDoS has past or the published date is within the next two years. Sales Managers refer to the Last Day of Support report to see which devices should be replaced because of LDoS. Another report Sales Managers should consider using **Generate Reports** > **Uncovered Device Report** because it includes information on suggested replacement PIDs including price and one possible service level.

Service Executives refer to this report for a count of only those items that are past LDoS to develop a plan for product refresh.



Column Headings and Definitions:

Category: The category of the item displayed.

Item Type: Is the classification of an item as a CCM, Card, Chassis, IPPHONE, TP, or UCS.

Serial Number: The serial number of discovered device that was validated against Cisco installed base records.

Uncovered Items

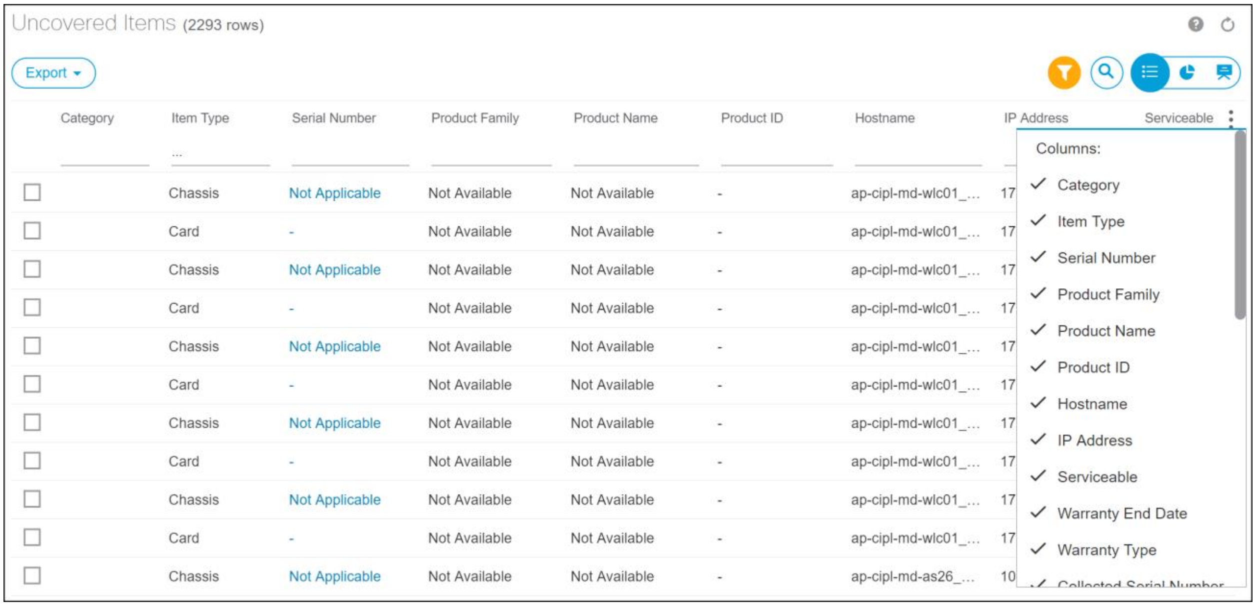
The Uncovered Devices report lists those items found during network discovery that are not presently covered under a service contract, such as chassis, Call Manager (CCM), IP Phones, cards, Unified Computing System (UCS), TelePresence (TP) and Identity Services Engine (ISE) devices. Both processed and non-processed devices will be displayed.

The Uncovered Items report also provides the device warranty information (if required) to determine whether the service coverage is needed for the specified PIDs.

Contract Managers check which devices are serviceable and eligible for contract coverage.

Sales Managers review warranty details of uncovered devices, for one or more customers to determine which uncovered devices should be covered under a service contract. Using the device details in the report, the Sales manager can develop contract proposals.

Support Engineers use this report to confirm service entitlement by searching for a device's " Product ID" and " Serial Number" ; and then identifying the " Contract Number" and " Installed-At Site Name." These details will be used for PSS foundational services such as partner access to the TAC.



Column Headings and Definitions:

Category: The category of the item displayed.

Item Type: The classification of an item as a CCM, Card, Chassis, IPPHONE, TP, or UCS.

Serial Number: The serial number of discovered device that was validated against Cisco installed base records.

Product Family: Grouping of similar Cisco Product Models.

Product ID: The product id of a discovered device that was validated against Cisco records.

Product Name: The name of the product.

Hostname: The name of the host where this device was discovered.

IP Address: IP Address of the physical entity. The address is a unique string of numbers separated by periods that identifies each computer using the Internet Protocol to communicate over a network.

Serviceable: Indicates whether the item is serviceable or not. The value is 'N' for not serviceable, and 'Y' if a services price is associated to the item.

Note Devices are defined to be Serviceable at the PID level. Should you see devices with the same PID that have both “Yes” and “No” serviceable identifiers, check the Serial Numbers for the Devices that are identified as Serviceable “No” to see if the serial numbers are valid.

Warranty End Date: The End Date of the device warranty.

Warranty Type: The type of the device warranty.

Collected Serial Number: The actual Serial Number of the item collected from the network. In some cases, this serial number may be different from what is found in Cisco’s contract databases.

Collected Product ID: The actual PID of the item collected from the network. In some cases, this PID may be different from what is found in Cisco’s contract databases.

Customer: The Customer that was selected in the Cisco Services Connection Data Filters customer drop-down.

Installed-At City: The City noted in the Cisco Install Site record.

Installed-At Country: The Country noted in the Cisco Install Site record.

Installed-At Postal Code: The Postal Code noted in the Cisco Install Site record.

Installed-At Province: The Province noted in the Cisco Install Site record.

Installed-At State: The State noted in the Cisco Install Site record.

Instance ID: A unique identification number that is issued by Cisco to refer to a specific piece of equipment within Cisco's IB records.

Inventory: The name assigned to an inventory.

Appliance ID: A unique identification of an appliance.

Last Day of Support: Day that Cisco will no longer offer the opportunity to purchase service coverage on a particular product.

P/C/S: An indicator that shows whether an item is a Parent, Child, or Stand Alone within a configuration.

Parent Instance ID: Instance ID within a network configuration of the parent item, under which a child item resides, according to Cisco's Installed Base records.

Ship Date: The date the item was initially shipped from Cisco.

SN Entry Type: The type of device (chassis/card).

SNMP SysName: Is the name assigned to a SNMP MIB or the Hostname from CLI data.

Warranty Start Date: The Start Date of the device warranty.

Contracts

The following items are a list of the various types of contract reports:

- All Contracts
- Expiring Contracts
- Product

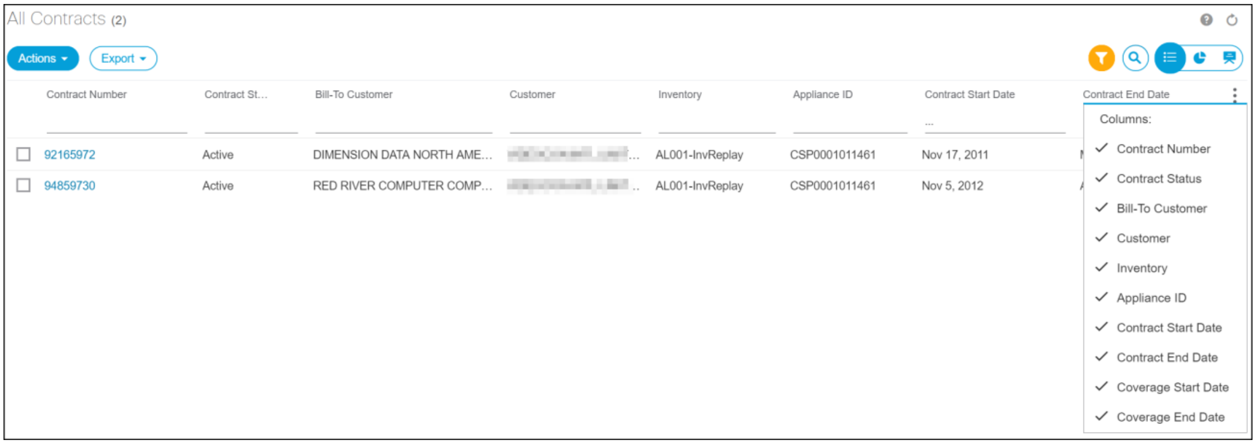
Contract information is privileged information that can only be seen by the partner who owns the service contract. The ownership of the service contract is determined by the Bill to ID listed on a service contract in the Cisco service contract database. The portal will display most of the information about all collected devices in the customer's network, regardless of who owns the contract. However, contract details will only be available for contracts you own. Product Alerts can be viewed by all partners who can collect from a device and upload to PSS portal.

All Contracts

The All Contracts report provides a comprehensive list of all contracts in relation to the items that were both found and validated by the network discovery.

The data in this report is based on the customers and inventories you have selected in the Data Filter. It displays only valid contracts that your CCO ID has been enabled to view for your company. Multiple contract numbers will be displayed when the coverage Start and Coverage Stop dates for devices coverage varies.

You can drill-down by clicking the **Contract Number** that appears in blue to view the contract details and the list of covered items.



Column Headings and Definitions:

Contract Number: The contract identifier of the Cisco Service Contract coverage for the specified Product ID and Serial Number.

Contract Status: Status of the contract. Active, Expired, Overdue, Terminated.

Bill-To Customer: The name of customer that is attached to items covered on the contract.

Customer: The customer that was selected in the Cisco Services Connection Data Filters customer drop-down.

Inventory: The name assigned to an inventory.

Appliance ID: A unique identification of an appliance.

Contract Start Date: Is the date of the contract started.

Contract End Date: Is the date of the contract ends.

Coverage Start Date: Is the date the contract starts providing coverage for the associated device.

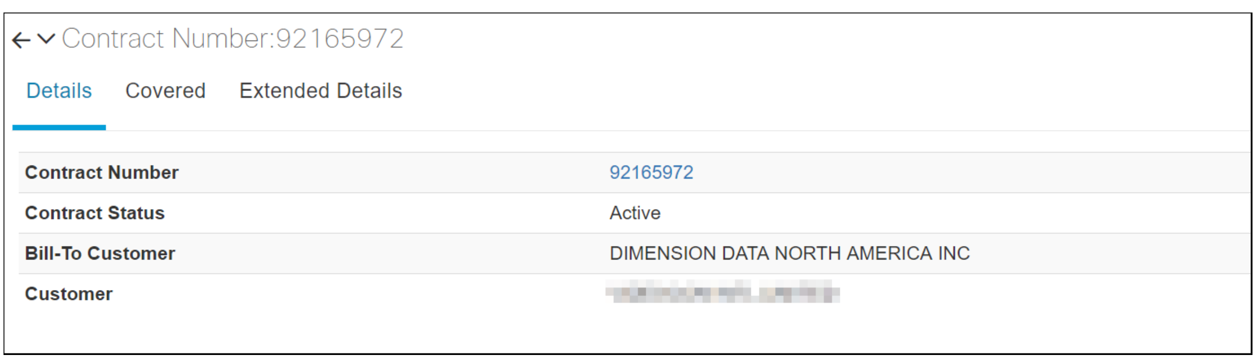
Coverage End Date: Is the date the contract no longer provides coverage for the associated device.

Contract Number Drill-Down Report

The Contract Number drill-down report provides three tabs of contract information including, Details, Covered, and Extended Details. These tabs provide comprehensive contract details and a list of all devices covered by the contract.

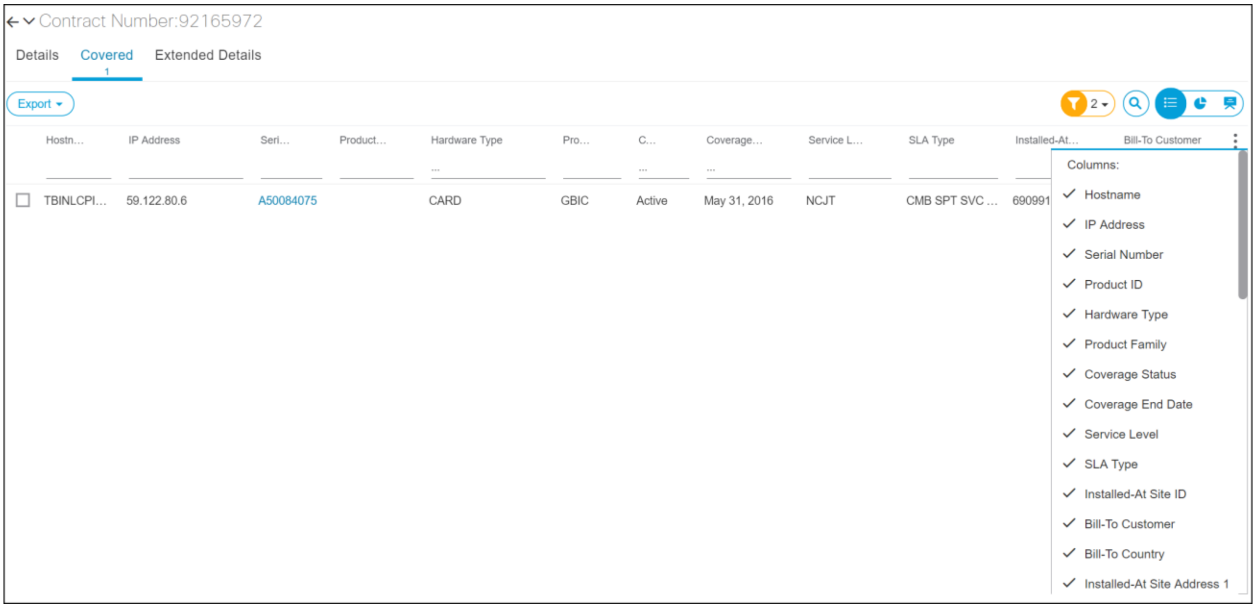
Details Tab:

This tab shows the contract number, status, Bill-To Customer and Customer.



Covered Tab:

The Covered tab provides a list of all devices that are covered under the selected Contract number.



Column Headings and Definitions:

Hostname: Is the assigned name for a particular device that is part of a computer network.

IP Address: IP Address of the physical entity. The address is a unique string of numbers separated by periods that identifies each computer using the Internet Protocol to communicate over a network.

Serial Number: The serial number of discovered device that was validated against Cisco installed base records.

Product ID: The product id of a discovered device that was validated against Cisco records.

Hardware Type: The type of Hardware.

Product Family: Grouping of similar Cisco Product Models.

Coverage Status: The status [Active/Not Active] of the coverage contract.

Coverage End Date: Is the date the contract no longer provides coverage for the associated device.

Service Level: Abbreviated form for the type of service that is active on a Service Contract. (Examples, NCJT).

SLA Type: The type of Service-Level Agreement.

Installed-At Site ID: The ID of the install site in the contract, which is created and synched up with Cisco contracts database.

Bill-To Customer: Name to which the billing is sent.

Bill-To Country: Name of the country of the customer that is attached to the device's contract.

Installed-At Site Address1: The first Address noted in the Cisco Install Site record.

Installed-At City: The City noted in the Cisco Install Site record.

Installed-At Province: The Province noted in the Cisco Install Site record.

Installed-At Country: The Country noted in the Cisco Install Site record.

Installed-At Postal Code: The Postal code noted in the Cisco Install Site record.

Ship-To Address1: The first address where shipments are sent.

Ship-To City: The City where the shipment is sent.

Ship-To Province: The Province noted for the shipment.

Ship-To Country: The Country noted for the shipment.

Ship-To Postal Code: The Postal Code for the shipment.

Customer: The customer that was selected in the Cisco Services Connection Data Filters customer drop-down.

Inventory: The name assigned to the inventory of the customer.

Appliance ID: A unique identification of an appliance.

Installed-At Site Address 2: The second Address noted in the Cisco Install Site record.

Ship-To Address 2: The second Address noted for the shipment in the Cisco Site record.

Warranty Start Date: The Start Date of the device warranty.

Warranty End Date: The End Date of the device warranty.

Warranty Type: The type of device warranty.

Equipment ID: A unique Identification number of the equipment.

Serviceable: Indicates whether the item is serviceable or not. The value is 'No' for not serviceable, and 'Yes' if a services price is associated to the item.

Hardline: The type of hardline network to be set.

Partner: The name of the partner.

Inventory_ID: A unique identifier of the inventory.

Contract Number: Is the contract identifier of the Cisco Service Contract coverage for the specified product id and serial number.

P/C/S: An indicator that shows whether an item is a Parent, Child, or Stand Alone within a configuration.

Coverage Start Date: Is the date the contract starts providing coverage for the associated device.

Last Date of Support: The last date of the devices support.

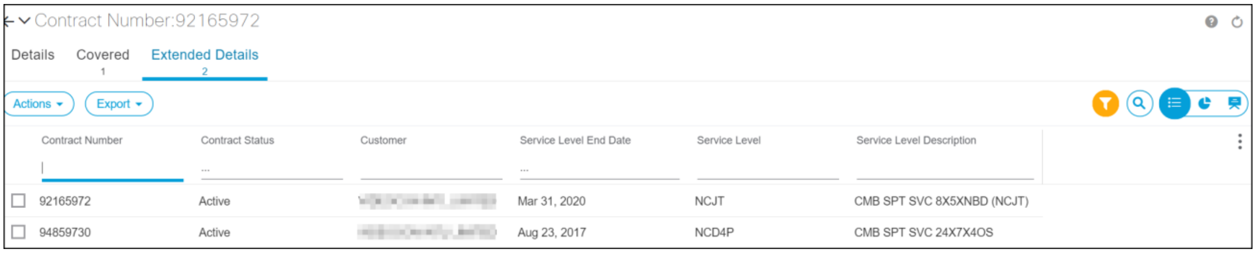
Parent Instance ID: Instance ID within a network configuration of the parent item, under which a child item resides, according to Cisco's Installed Base records.

Instance ID: A unique identification number that is issued by Cisco to refer to a specific piece of equipment within Cisco's IB records.

Customer ID: A unique Identification number of the customer.

Extended Details Tab:

The Extended Details tab provides a comprehensive list of all the details for the selected contract.



Column Headings and Definitions*:*

Contract Number: The contract identifier of the Cisco Service Contract coverage for the specified Product ID and Serial Number.

Contract Status: Status of the contract. Active, Expired, Overdue, Terminated.

Customer: The customer that was selected in the Cisco Services Connection Data Filters customer drop-down.

Service Level End Date: The end date of a contract.

Service Level: Abbreviated form for the type of service that is active on a Service Contract. (Examples, NCJT, NCD4P).

Service Level Description: Description of the service level (examples CMB SPT SVC 8X5XNBD (NCJT) or CMB SPT SVC 24X7X4OS).

Bill-To Customer: The name of the customer that is attached to items covered on the contract.

Service Level Start Date: The start date of a contract.

Bill-To Country: Name of the country of the customer that is attached to the device's contract.

Installed-At Site ID: The ID of the install site in the contract, which is created and synched up with Cisco contracts database.

Installed-At Site Name: The name of the install site in the contract, which is created and synched up with Cisco contracts database.

Installed-At Site Address: The Installed-At Address noted in the Cisco Install Site record.

Installed-At City: The City noted in the Cisco Install Site record.

Installed-At Province: The Province noted in the Cisco Install Site record.

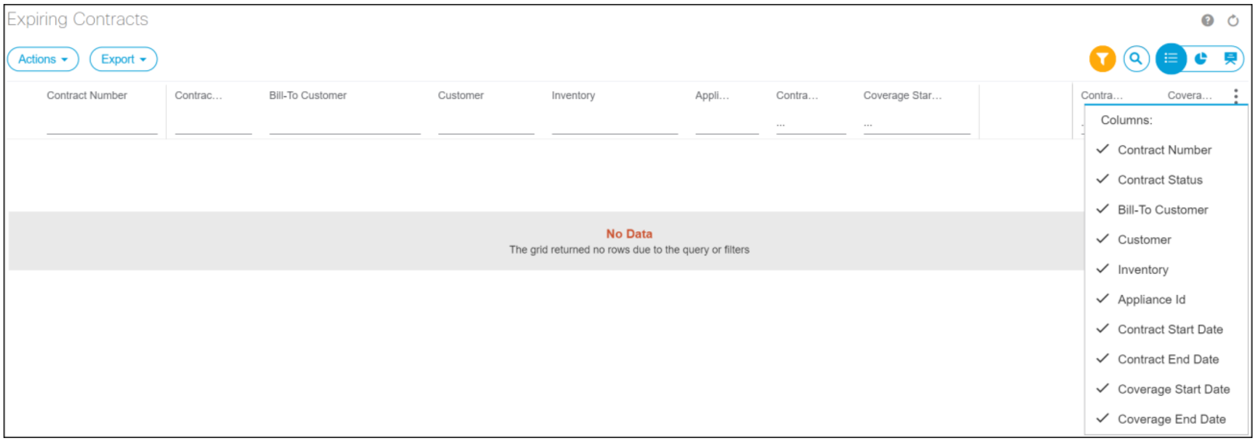
Installed-At State: The State noted in the Cisco Install Site record.

Installed-At Country: The Country noted in the Cisco Install Site record.

Installed-At Postal Code: The Postal Code noted in the Cisco Install Site record.

Expiring Contracts

The Expiring Contracts report lists contracts that are going to expire in the next month. Click on the contract number to get the list of covered items and extended details of the contract.



Column Headings and Definitions:

Contract Number: The contract identifier of the Cisco Service Contract coverage for the specified Product ID and Serial Number.

Contract Status: Status of the contract. Active, Expired, Overdue, Terminated.

Bill-to Customer: The name of the customer that is attached to items covered on the contract.

Customer: The customer that was selected in the Cisco Services Connection Data Filters customer drop- down.

Inventory: The name assigned to an inventory.

Appliance ID: A unique identifier of an appliance.

Contract Start Date: Is the date of the contract started.

Contract End Date: Is the date of the contract ends.

Coverage Start Date: Is the date the contract starts providing coverage for the associated device.

Coverage End Date: Is the date the contract no longer provides coverage for the associated device.

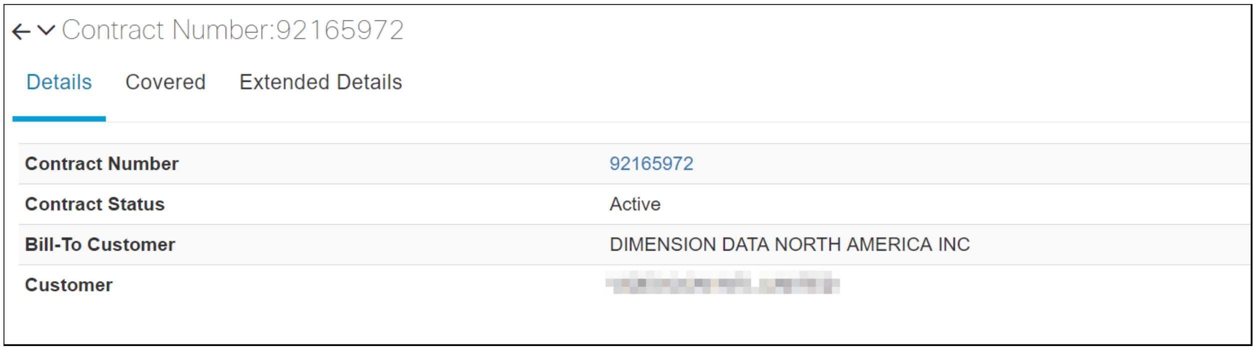
Contract Number Drill-down Report for Expiring Contracts

The Contract Number drill-down report for expiring contracts provides three tabs of contract information including:

Details, Covered, and Extended Details. These tabs provide comprehensive contract details and a list of all devices whose coverage will soon expire.

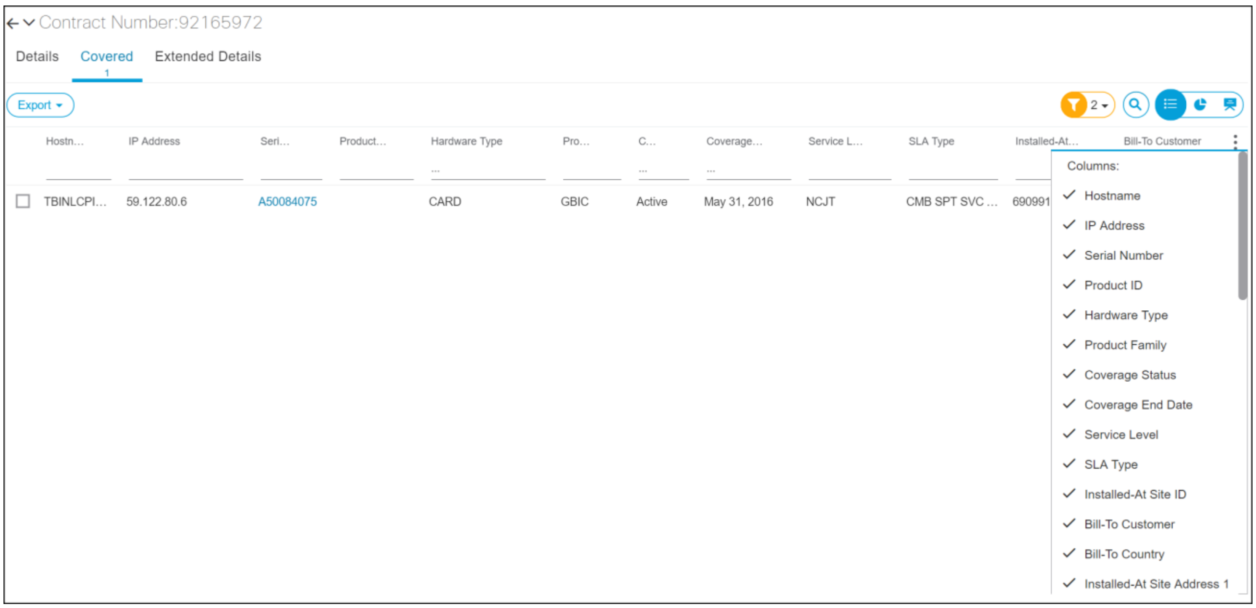
Details Tab:

This tab shows the contract number, status, Bill-To Customer and Customer.



Covered Tab:

The Covered tab provides a list of all devices that are covered under the selected Contract number.



Column Headings and Definitions:

Hostname: Is the assigned name for a particular device that is part of a computer network.

IP Address: IP Address of the physical entity. The address is a unique string of numbers separated by periods that identifies each computer using the Internet Protocol to communicate over a network.

Serial Number: The serial number of discovered device that was validated against Cisco installed base records.

Product ID: The product id of a discovered device that was validated against Cisco records.

Hardware Type: The type of Hardware.

Product Family: Grouping of similar Cisco Product Models.

Coverage Status: The status [Active/Not Active] of the coverage contract.

Coverage End Date: Is the date the contract no longer provides coverage for the associated device.

Service Level: Abbreviated form for the type of service that is active on a Service Contract. (Examples, NCJT, NCD4P).

SLA Type: The type of Service-Level Agreement.

Installed-At Site ID: The ID of the install site in the contract, which is created and synched up with Cisco contracts database.

Bill-To Customer: Name to which the billing is sent.

Bill-To Country: Name of the country of the customer that is attached to the device's contract.

Installed-At Site Address1: The first Address noted in the Cisco Install Site record.

Installed-At City: The City noted in the Cisco Install Site record.

Installed-At Province: The Province noted in the Cisco Install Site record.

Installed-At Country: The Country noted in the Cisco Install Site record.

Installed-At Postal Code: The Postal code noted in the Cisco Install Site record.

Ship-To Address1: The first address where shipments are sent.

Ship-To City: The City where the shipment is sent.

Ship-To Province: The Province noted for the shipment.

Ship-To Country: The Country noted for the shipment.

Ship-To Country: The Country noted for the shipment.

Ship-To Postal Code: The Postal Code for the shipment.

Customer: The customer that was selected in the Cisco Services Connection Data Filters customer drop-down.

Inventory: The name assigned to the inventory of the customer.

Appliance ID: A unique identification number of an appliance.

Installed-At Site Address 2: The second Address noted in the Cisco Install Site record.

Ship-To Address 2: The second Address noted for the shipment in the Cisco Site record.

Warranty Start Date: The Start Date of the device warranty.

Warranty End Date: The End Date of the device warranty.

Warranty Type: The type of device warranty.

Equipment ID: A unique Identification number of the equipment.

P/C/S: An indicator that shows whether an item is a Parent, Child, or Stand Alone within a configuration.

Coverage Start Date: Is the date the contract starts providing coverage for the associated device.

Contract Number: Is the contract identifier of the Cisco Service Contract coverage for the specified product id and serial number.

Partner: The name of the partner.

Serviceable: Indicates whether the item is serviceable or not. The value is 'N' for not serviceable, and 'Y' if a services price is associated to the item.

Inventory_ID: A unique identifier of the inventory.

Parent Instance ID: Instance ID within a network configuration of the parent item, under which a child item resides, according to Cisco's Installed Base records.

Instance ID: A unique identification number that is issued by Cisco to refer to a specific piece of equipment within Cisco's IB records.

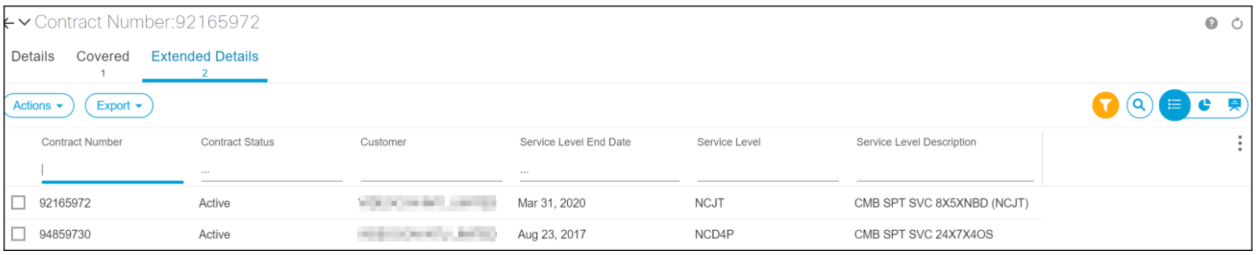
Last Date of Support: The last date of the devices support.

Hardline: The type of hardline network to be set.

Customer: A unique Identification number of the customer.

Extended Details Tab:

The Extended Details tab provides a comprehensive list of all the details for the selected contract that will soon expire.



Column Headings and Definitions:

Contract Number: The contract identifier of the Cisco Service Contract coverage for the specified Product ID and Serial Number.

Contract Status: Status of the contract. Active, Expired, Overdue, Terminated.

Customer: The customer that was selected in the Cisco Services Connection Data Filters customer drop-down.

Service Level End Date: The end date of a contract.

Service Level: Abbreviated form for the type of service that is active on a Service Contract. (Examples, NCJT, NCD4P).

Service Level Description: Description of the service level (examples CMB SPT SVC 8X5XNBD (NCJT) or CMB SPT SVC 24X7X4OS).

Bill-To Country: Name of the country of the customer that is attached to the device's contract.

Installed-At Site ID: The ID of the install site in the contract, which is created and synched up with Cisco contracts database.

Installed-At Site Name: The name of the install site in the contract, which is created and synched up with Cisco contracts database.

Installed-At Address: The Installed-At Address noted in the Cisco Install Site record.

Installed-At City: The City noted in the Cisco Install Site record.

Installed-At Province: The Province noted in the Cisco Install Site record.

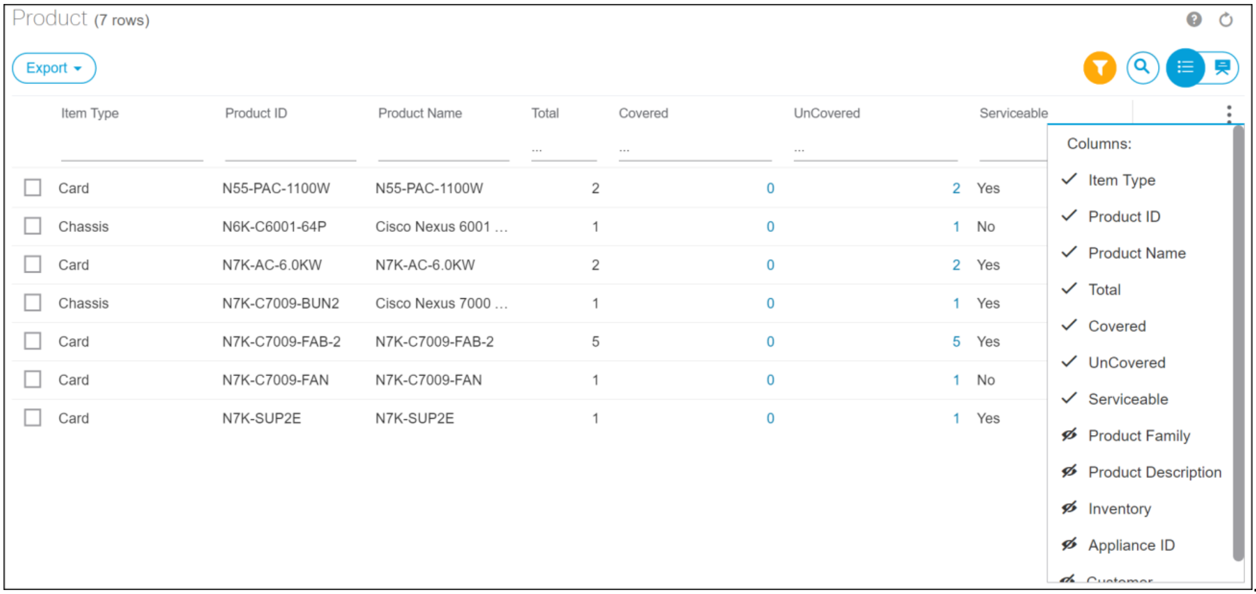
Installed-At State: The State noted in the Cisco Install Site record.

Installed-At Country: The Country noted in the Cisco Install Site record.

Installed-At Postal Code: The Postal Code noted in the Cisco Install Site record.

Product

The Product report provides a comprehensive list of all product types for the customers and inventories you have selected in the Data Filters.



Column Headings and Definitions:

Item Type: The classification of an item as a CCM, Card, Chassis, IPPHONE, TP, or UCS.

Product ID: Alpha-numeric reference to a specific Cisco Product Model.

Product Name: The name of the product.

Total: Count of identical PID's.

Covered: Count of items that are covered out of the " Total Count" .

Uncovered: Count of items that are not covered out of the “Total Count”.

Serviceable: Indicates whether the item is serviceable or not. The value is 'No' for not serviceable, and 'Yes' if a services price is associated to the item.

Product Family: Grouping of similar Cisco Product Models.

Product Description: The detailed description of the device or card found in the inventory.

Customer: The customer that is selected in the Cisco Services Connection Data Filters customer drop-down.

Inventory: The name of the inventory given by customers.

Appliance ID: A unique identification number of an appliance.

Alerts

This report category has the following associated report:

All Alerts

Product Alerts can be viewed by all partners who can collect from a device and upload to PSS portal, regardless of who owns the contract.

Alerts provided by PSS are intended to increase network security, improve network uptime because you can notify customers when a device is no longer supported by Cisco or there is a field notice about a defect that may impact the customer network operation and improve customer satisfaction. PSS Product Alerts are classified as:

- Field-Notices
- Hardware-EOX (Hardware End of Life)
- Software-EOX (Software End of Life)
- PSIRT (Cisco Product Security Incident Response)

Field Notices are published for significant issues that directly involve Cisco products and typically require an upgrade, workaround, or other action on the device in your customer's network.

Hardware and Software end of life alerts apply to devices at the end stage of their product life cycle. PSS alert reports include links to more details including in the dates for the End of Engineering, End of Sale, End of Service, End of SW Maintenance, Last Date of Support as well as appropriate replacements.

PSIRT alerts deliver security vulnerability information which is based on the Common Vulnerability Scoring System (CVSS). This industry-standard rating system, evaluates reported potential vulnerabilities in software on Cisco products, and determines which vulnerabilities warrant a Cisco Security Advisory or other type of publication. CVSS also conveys whether the alert severity is Vulnerable or Potentially Vulnerable.

All Alerts

The All Alerts report displays latest product alerts for the customers and inventories you have selected in the [Data Filters](#).

Click in the Type column filter in the heading and click to filter the report by Alert type. Click on **Alert Description** to display a list of devices affected by the alert.

Type	Description	Status	Match Co...	Alert La...	Al...	C...	More I...	CV...	I...	I...	IS...	IS ...	IS...
Field-Noti...	*Expired* FN - 28...	ACTIVE	Vulnerable	May 23, 2015	28655	0	http://www....	0		0			
Field-Noti...	*Expired* FN - 28...	ACTIVE	Vulnerable	May 23, 2015	28655	0	http://www....	0		0			
Field-Noti...	A Serial EEPROM ...	ACTIVE	Potentially Vul...	Apr 27, 2015	61240	0	http://www....	0		0			
Hardware...	Cisco 2800 Series ...	ACTIVE	Vulnerable	Apr 27, 2015	240097	0	http://www....	0		0			
Hardware...	Cisco 2800 Series ...	ACTIVE	Vulnerable	May 23, 2015	240097	0	http://www....	0		0			
Hardware...	Cisco 2800 Series ...	ACTIVE	Vulnerable	May 23, 2015	240097	0	http://www....	0		0			
Hardware...	Cisco 2800 Series ...	ACTIVE	Vulnerable	May 23, 2015	240116	0	http://www....	0		0			
Hardware...	Cisco 2800 Series ...	ACTIVE	Vulnerable	May 23, 2015	240116	0	http://www....	0		0			
Hardware...	Cisco 2800 Series ...	ACTIVE	Vulnerable	May 23, 2015	240116	0	http://www....	0		0			
Hardware...	Cisco 3800 Series ...	ACTIVE	Vulnerable	May 23, 2015	240159	0	http://www....	0		0			
Hardware...	Cisco 3800 Series ...	ACTIVE	Vulnerable	Apr 27, 2015	240159	0	http://www....	0		0			
Hardware...	Cisco 3800 Series ...	ACTIVE	Vulnerable	May 23, 2015	240159	0	http://www....	0		0			
Hardware...	Cisco Catalyst 296...	ACTIVE	Vulnerable	Apr 24, 2015	286007	0	http://www....	0		0			
Hardware...	Cisco Catalyst 296...	ACTIVE	Vulnerable	May 23, 2015	286012	0	http://www....	0		0		0	
Hardware...	Cisco Catalyst 296...	ACTIVE	Vulnerable	May 23, 2015	258190	0	http://www....	0		0		0	
Hardware...	Cisco Catalyst 296...	ACTIVE	Vulnerable	May 23, 2015	258190	0	http://www....	0		0		0	
Hardware...	Cisco Catalyst 356...	ACTIVE	Vulnerable	May 23, 2015	286483	0	http://www....	0		0		0	
Hardware...	Cisco Catalyst 356...	ACTIVE	Vulnerable	May 23, 2015	286483	0	http://www....	0		0		0	

Column Headings and Definitions:

Type: The type of alert, (for example, Hardware or Software EOX alert, PSIRT, Field Notice).

Alert Description: The description of the Product Alert.

Alert Status: Indicates whether the alert is still an active alert or not.

Match Confidence: Displays the confidence level [Vulnerable / Potential Vulnerable] of the alerts based on the alert types: PSIRT, Product Security, and Field Notice.

Alert Last Updated: The last date an inventory was collected.

More Info: The URL address for Product Alert Definition.

Software Type: Displays the type of Software.

Customer: The customer that was selected in the Cisco Services Connection Data Filters customer drop- down.

Alert ID: The unique identifier for each alert.

Customer ID: A unique identification of the customer.

CVSS Base Score: The base score of CVSS.

CVSS Temp Score: The temp score of CVSS.

Inventory: The name of the inventory given by customers.

Partner: The name of the partner.

Inventory ID: A unique identification of the Inventory.

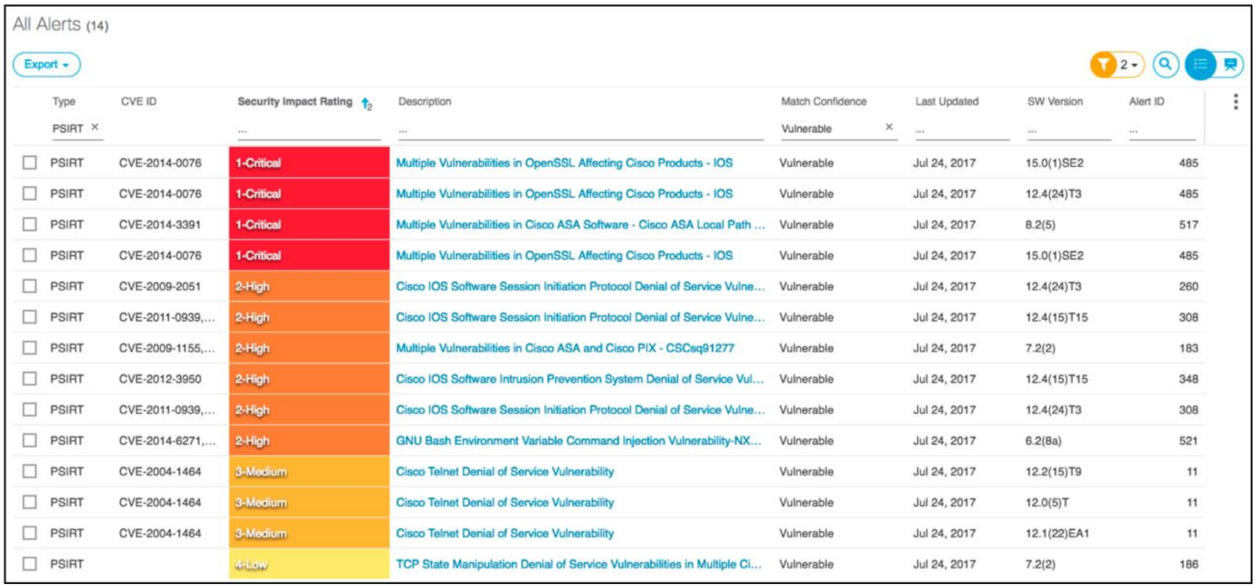
Appliance ID: A unique identification of an appliance.

Security Impact Rating: Severity of the PSIRT's affecting the devices in the portal. Cisco uses the Security Impact Rating (SIR) as a way to categorize vulnerability severity in a simpler manner. The SIR is based on the CVSS Qualitative Severity Rating Scale of the base score, may be adjusted by PSIRT to account for Cisco-specific variables, and is included in every Cisco Security Advisory.

Note Some PSIRT's like Network Address Translation (NAT) will not show Security Impact Rating.

CVE ID: A unique identification of the Common Vulnerability and Exposures for the PSIRT alert ids.

You can select PSIRTS, CVE ID, Security Impact Rating, Description, Match Confidence, Last updated, and other selection to create/export a report like this:


All Alerts (14)

Type	CVE ID	Security Impact Rating	Description	Match Confidence	Last Updated	SW Version	Alert ID
PSIRT	CVE-2014-0076	1-Critical	Multiple Vulnerabilities in OpenSSL Affecting Cisco Products - IOS	Vulnerable	Jul 24, 2017	15.0(1)SE2	485
PSIRT	CVE-2014-0076	1-Critical	Multiple Vulnerabilities in OpenSSL Affecting Cisco Products - IOS	Vulnerable	Jul 24, 2017	12.4(24)T3	485
PSIRT	CVE-2014-3391	1-Critical	Multiple Vulnerabilities in Cisco ASA Software - Cisco ASA Local Path ...	Vulnerable	Jul 24, 2017	8.2(5)	517
PSIRT	CVE-2014-0076	1-Critical	Multiple Vulnerabilities in OpenSSL Affecting Cisco Products - IOS	Vulnerable	Jul 24, 2017	15.0(1)SE2	485
PSIRT	CVE-2009-2051	2-High	Cisco IOS Software Session Initiation Protocol Denial of Service Vulne...	Vulnerable	Jul 24, 2017	12.4(24)T3	260
PSIRT	CVE-2011-0939,...	2-High	Cisco IOS Software Session Initiation Protocol Denial of Service Vulne...	Vulnerable	Jul 24, 2017	12.4(15)T15	308
PSIRT	CVE-2009-1155,...	2-High	Multiple Vulnerabilities in Cisco ASA and Cisco PIX - CSCsq91277	Vulnerable	Jul 24, 2017	7.2(2)	183
PSIRT	CVE-2012-3950	2-High	Cisco IOS Software Intrusion Prevention System Denial of Service Vul...	Vulnerable	Jul 24, 2017	12.4(15)T15	348
PSIRT	CVE-2011-0939,...	2-High	Cisco IOS Software Session Initiation Protocol Denial of Service Vulne...	Vulnerable	Jul 24, 2017	12.4(24)T3	308
PSIRT	CVE-2014-6271,...	2-High	GNU Bash Environment Variable Command Injection Vulnerability-NX...	Vulnerable	Jul 24, 2017	6.2(8a)	521
PSIRT	CVE-2004-1464	3-Medium	Cisco Telnet Denial of Service Vulnerability	Vulnerable	Jul 24, 2017	12.2(15)T9	11
PSIRT	CVE-2004-1464	3-Medium	Cisco Telnet Denial of Service Vulnerability	Vulnerable	Jul 24, 2017	12.0(5)T	11
PSIRT	CVE-2004-1464	3-Medium	Cisco Telnet Denial of Service Vulnerability	Vulnerable	Jul 24, 2017	12.1(22)EA1	11
PSIRT		4-Low	TCP State Manipulation Denial of Service Vulnerabilities in Multiple Ci...	Vulnerable	Jul 24, 2017	7.2(2)	186

First Publish Date: The date when the alert was first published.

Last Publish Date: The date when the alert was last published.

All Alerts Drill-Down Report

The Alerts drill-down report provides details on the affected devices. Select the hyperlink on Alert Description to navigate to All Alerts Drill-Down report.

Details tab:

This tab shows the Alert ID, description, type, Cisco.com info, collection date and last updated.

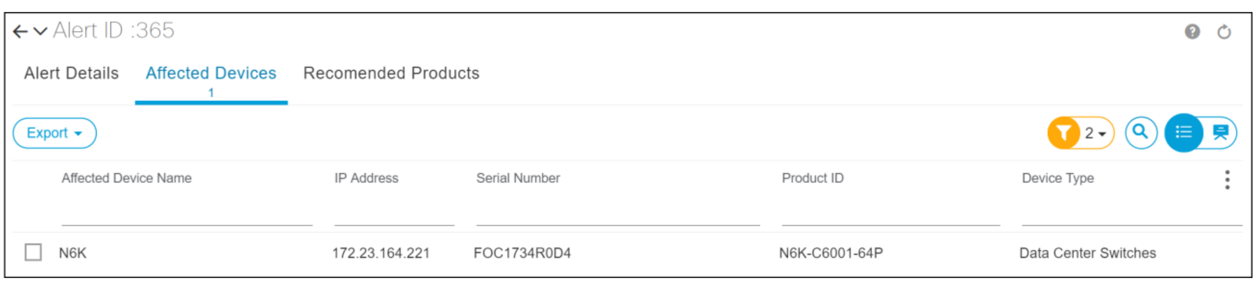

Alert ID :365

Alert Details | Affected Devices | Recomended Products

Alert ID	365
Description	Cisco Nexus 7000 Series NX-OS Software Release 6.0
Type	Software-EOX
More Info	http://www.cisco.com/en/US/prod/collateral/switches/ps9441/ps9402/eol__C51-726666.html
Collection Date	Mar 3, 2016 08:16
Last Updated	Mar 3, 2016 08:16

Affected Devices tab:

The Affected Devices tab provides a comprehensive list of all the affected devices for the selected device that is vulnerable/potentially vulnerable.


Alert ID :365

Alert Details | Affected Devices 1 | Recomended Products

Affected Device Name	IP Address	Serial Number	Product ID	Device Type
N6K	172.23.164.221	FOC1734R0D4	N6K-C6001-64P	Data Center Switches

Column Headings and Definitions:

Affected Device Name: The name of the affected device.

IP Address: IP Address of the physical entity. The address is a unique string of numbers separated by periods that identifies each computer using the Internet Protocol to communicate over a network.

Serial Number: The serial number of discovered device that was validated against Cisco installed base records.

Product ID: A unique identification of the product.

Device Type: The type of affected device.

Alert ID: A unique identification the alert.

Match Confidence: Displays the confidence level [Vulnerable / Potential Vulnerable] of the alerts based on the alert types: PSIRT, Product Security, and Field Notice.

All Alerts - Delta View

1. Use the All Alerts report to generate an Alerts Delta Report, a list of alerts affecting devices in a customer inventory that were last updated between two dates. The top level alerts report shows the following alert details by default: Alert Type, Alert Description, Alert Status, Match Confidence, Last Updated, More info, and Customer name. You can add or remove fields from the online report. Make a note of the **Start Date** and **End Date** to be used when you run the Inventory Delta Report. This is found in **Inventory** > **Inventory Collection**.
    - **Start Date** is a previous/older upload date
    - **End Date** is the more recent upload date.
2. Under **Alerts**, select **All Alerts**.
3. To set the start and end dates, filter the **Alert Last Updated** column to see the alerts updated between two dates.
    - Select **Range**.
    - Enter the **Start Date** which is a previous older date.
    - Choose an **End Date** which is the more recent date.

Note Select the dates using the calendar.

The Alerts report now displays only alerts affecting devices in the selected customer's inventory that were last updated between the selected dates. The report can be further filtered to focus on a specific **Alert Type**.

Cisco Trademark

Cisco Copyright