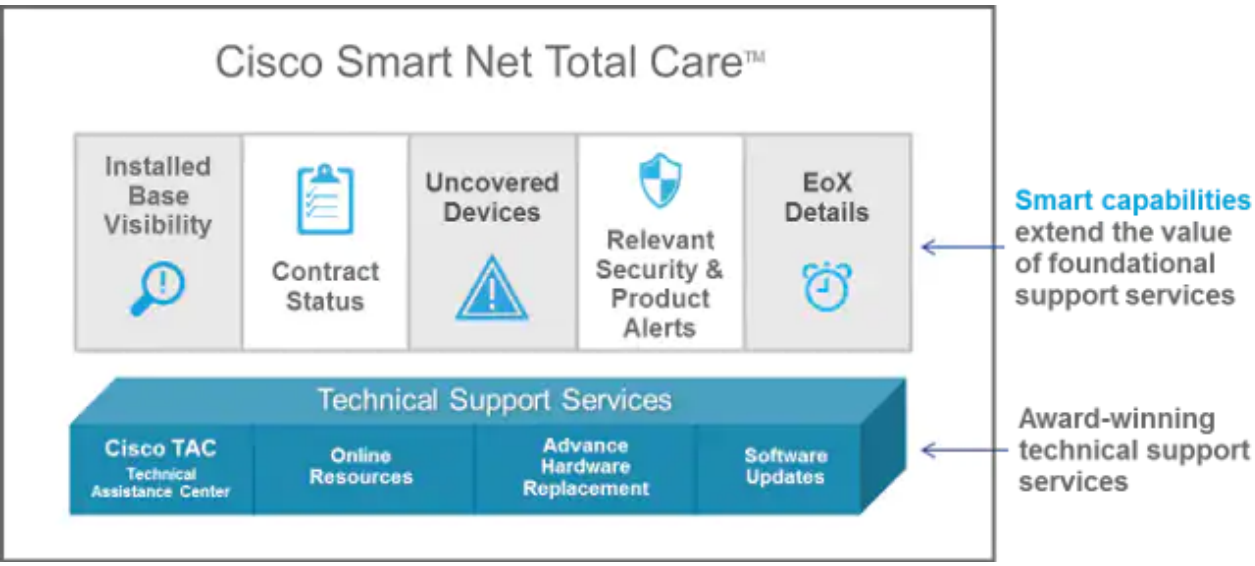
Smart Net Total Care Portal User Guide

Updated: April 15, 2019 **Document ID:** 1493687820423221

The Cisco Smart Net Total Care™ service is a part of Cisco's technical services portfolio. This service combines Cisco's industry-leading and award-winning, foundational technical services with an extra level of actionable business intelligence that is delivered to you through the smart capabilities in the Smart Net Total Care portal.

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

- **Faster problem resolution** – Identify issues quickly and streamline your incident management processes in order to improve IT service levels and resolve problems more quickly. Smart capabilities, which includes proactive alerts, automated diagnostics, up-to-date contract coverage data, and product information, helps minimize downtime and promote business continuity.
- **Risk mitigation** – Reduce risk with access to the Cisco technical experts (Cisco Technical Assistance Center) and smart tools that improve visibility into the state of your IT infrastructure 24 hours a day, 365 days a year. Installed-base visibility in the portal helps ensure that your critical Cisco products are covered by the proper service contracts. The portal also makes it easy to proactively plan and budget for refreshes of the Cisco products that are expected to reach End-of-Life (EoL) or Last Date of Support (LDoS).
- **Operational efficiency** – Increase your operational efficiency through proactive management tools and automated processes that make the network administrators and managers more productive. The automated inventory and contract management highlights changes and provides budget and planning foresight in order to minimize the effort that is required in order to maintain an up-to-date view of your network.



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

- Get started with the portal.
- Setup and customize the portal.
- Generate and use reports with the portal library.

Get Started

The Smart Net Total Care portal uses device information and analyzes it against security and support data from the Cisco knowledge base. This provides you with actionable information so that you can resolve problems more quickly, improve operational efficiency, and better manage support risks.

This section directs you to information on the various portal roles and access levels and the self-service onboarding process, plus provides an overview of the portal and its components:

- Logging into Smart Net Total Care

- Roles and Access
- Self-Service Onboarding
- Initial Inventory Creation
- Basic Portal Navigation

Logging into Smart Net Total Care

You can launch the Smart Net Total Care from your web browser at https://services.cisco.com

---

> **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 Smart Net Total Care portal.

Roles and Access

Refer to the *Portal Roles and Access* section of the Cisco Smart Net Total Care Portal Administration and Management page for information about roles and access levels.

Self-Service Onboarding

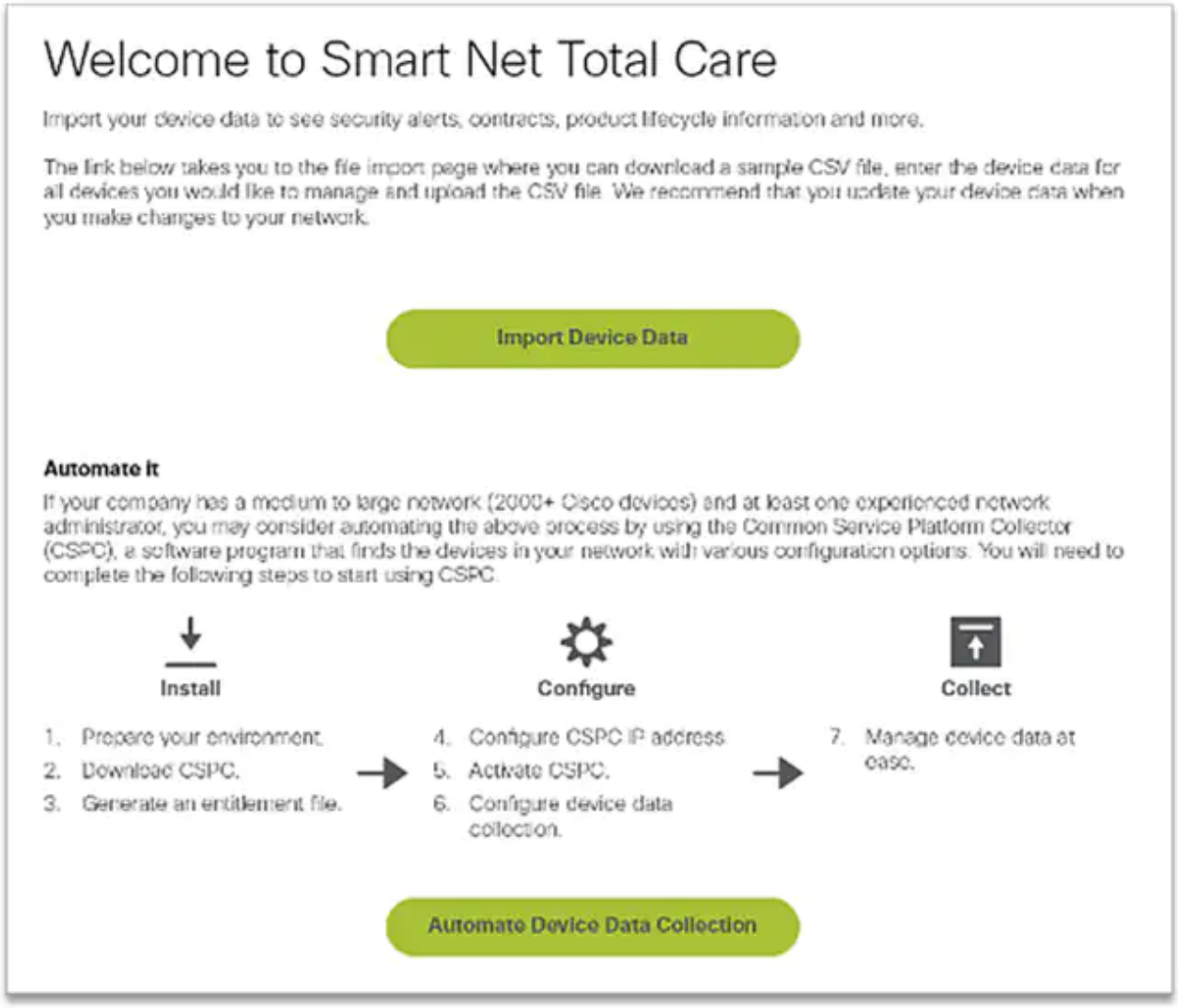
Refer to the Cisco Smart Net Total Care Portal Onboarding Guide for information about the self-service onboarding process.

Initial Inventory Creation

An *inventory* is a set of devices that are uploaded into the Smart Net Total Care system through one or all of the supported methods. You can use these methods in order to upload your Cisco-installed base information into the portal:

- The Cisco Common Service Platform Collector (CSPC)
- A third-party collector
- A comma-separated value (CSV) file import

If you are a new customer administrator and no inventory has been created, you are directed to the *Get Started* page upon login. This page contains step-by-step guidance in order to help you import your inventory through a CSV file import, or automate device collection through a collector.



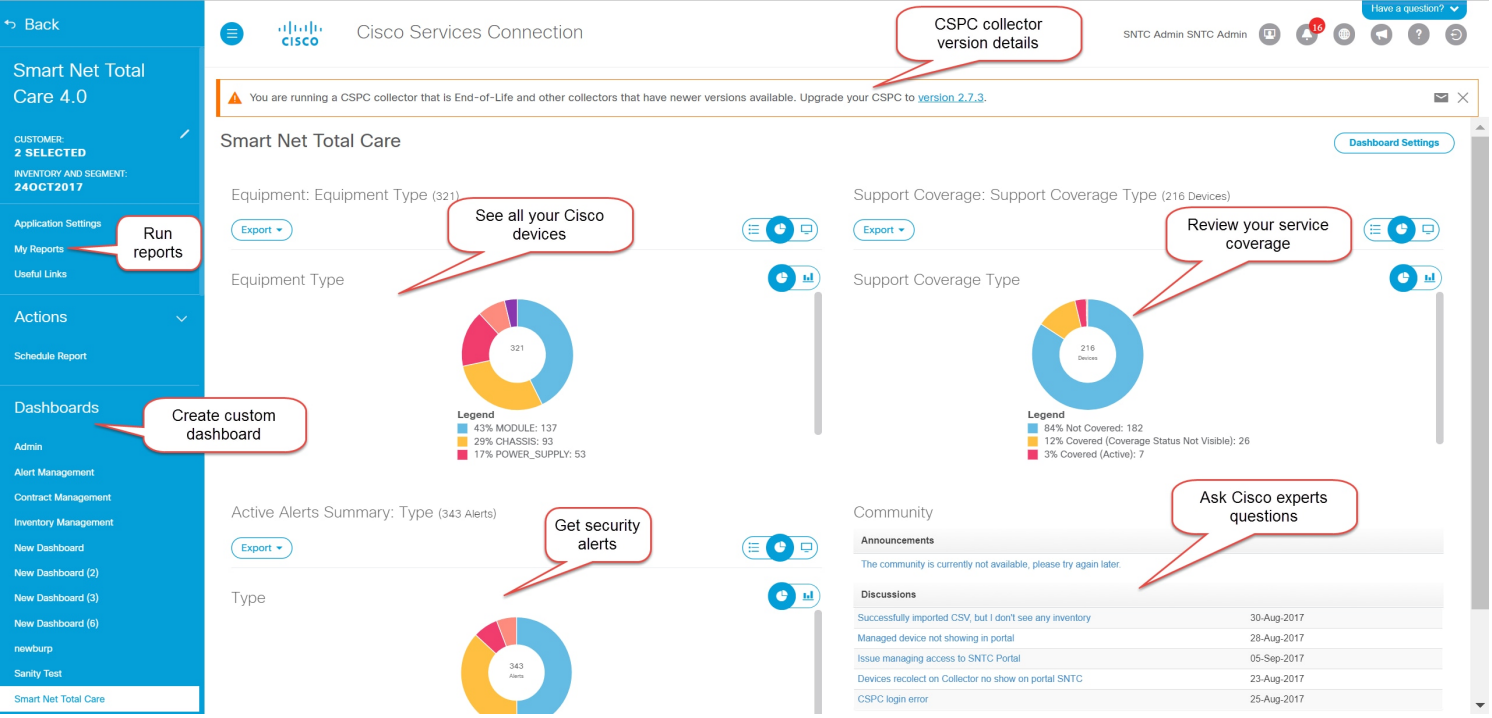
If you are a new user and a *No Records Found* message appears when you log in, then contact your customer administrator and ask them to create the initial inventory.

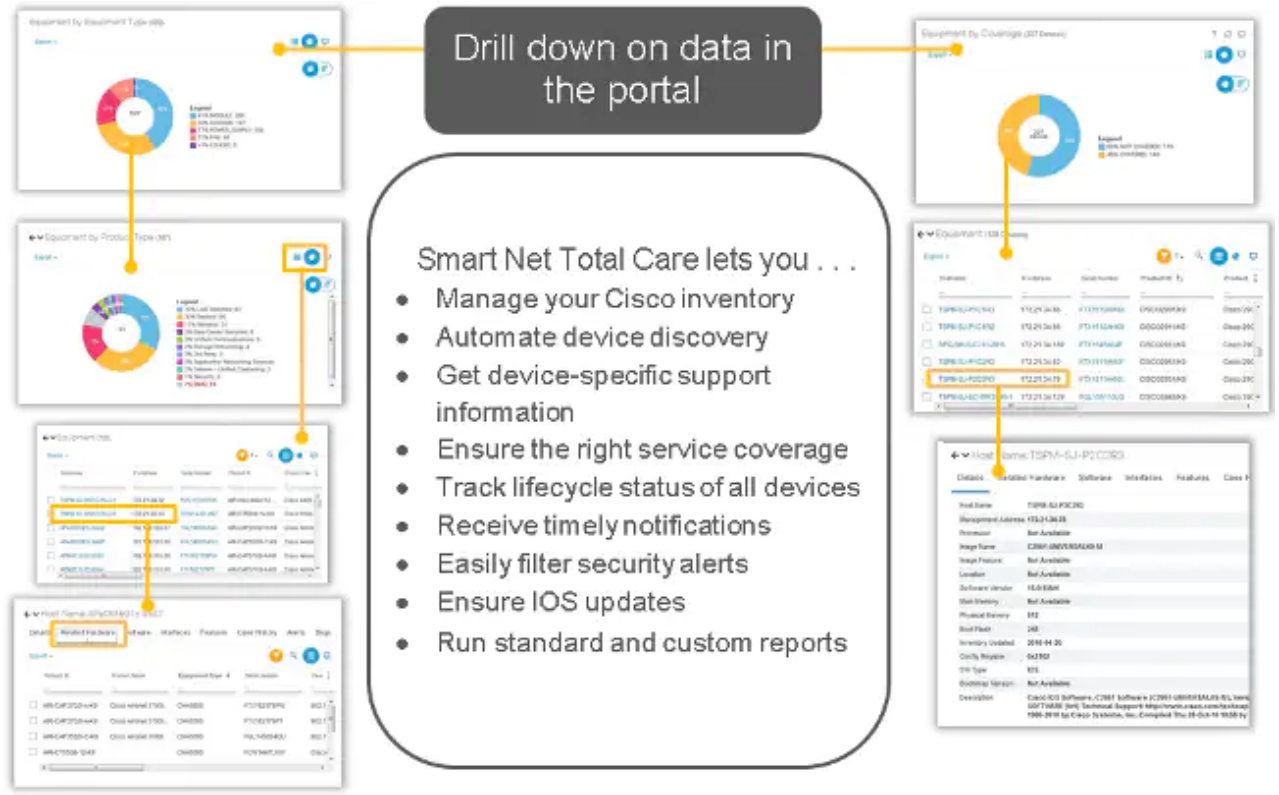
If you are associated with accounts for multiple customers (multi-role user) in the portal and the reports show *No Records Found* when you log in, then it is likely that the device data for the organization has not been uploaded. Contact the customer administrator(s) for that customer and request that inventory be uploaded.

Basic Portal Navigation

The Smart Net Total Care portal leverages the 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.

These 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:

- **Left Navigation Pane** – This portion of the page contains links to the reports, dashboards, and portal settings.
- **Logged-in User** – The name of the user who is currently logged-in appears in this area.
- **Select Language** – Click this icon in order to select the language for localized reports and the portal. Currently, the portal screens are localized in French, Spanish, Japanese, and Simplified Chinese. You can also set your timezone preference here.

Note: Some reports or help for the reports might not be available in the selected language.

- **Information** – Click this icon in order to view how-to videos, download a copy of this guide, and to receive more information about Smart Net Total Care.
- **Log Out** – Click this icon in order to log out of the portal.

Note: As part of the Cisco policy to safeguard access to customer data, a pop-up message is displayed on the Smart Net Total Care portal screen after an hour of portal inactivity.

- **Personalize Views** – Click the drop-down arrow next to the column name in order to set/sort the data in that column.

Tip: 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.

- **CSPC Version Reporting** – This portion of the page alerts the collector version being used by the logged in user. The banner alerts the collector prior to the current version of the collector that is used and an upgrade is required. Depending on the older 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.
- **Filter Text** – You can type a value into this field and press **Enter** in order to filter the data in the column so that it shows the results that match the specified criteria. You can add filter values to one or more columns.
- **Applied Filters** – Click this icon in order to view the filters that are applied to the columns (if any) in the report.
- **Select Column** – Click this icon in order to view the whole list of columns that are available for the report. Click the column name in order to hide or show it in the report.

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.

Tip: For more details about Smart Net Total Care portal navigation and components, refer to the Navigation and Dashboards video.

Setup and Customize

You can use the Smart Net Total Care selector panel 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, inventories, and segments.

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, Smart Net Total Care.

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

Customer

The customer name, along with the inventory and segment, is displayed beneath the service name. This is the name of the entitled customer whose device data is visible in the reports.

Most customers see only one choice on the Customer page – the name of their organization. Customers that are associated with more than one business organization see multiple choices for each organization that they are entitled to access. Partners or multi-role users, authorized to view their customer data, might also see multiple customers listed here.

Inventory and Segment

The inventories and segments that are available for the selected customers appear under the Inventory and Segment page. The content depends on the user access settings that are assigned to you.

An *inventory* is the device data that is uploaded from one collection source. An inventory can be further partitioned into *segments*.

Complete these steps in order to select which inventories and segments are shown in the portal reports:

1. Click the pencil icon, and the Global Filters window opens.
2. Click **Customer**, if it is not already selected.
3. Choose a customer name in order to set a filter so that only the data for the selected customer(s) appears in the reports.
4. Click **Inventory and Segment**.
5. Choose the desired inventories and segments so that only the data from the selected inventories and segments appears in the reports.

> **Note**: The portal supports only 50 or less segments to be selected at a time.

6. Click **Apply** in order to have your selection take affect.

> **Note**: If you choose more than one inventory or segment, the reports include the data from each. Some reports allow only a single customer and inventory/segment to be selected.

General

The *General* tab provides the list of business services and customers that you can access, along with your role for each customer.

Company Notifications

If you have an administrator role, use this tab in order to manage the distribution lists for the messages that you want to send to the users.

My Notifications

Use this tab in order to manage the desired frequency for which alerts and system messages are received from the portal.

Custom Display Name

This tab allows the administrator to modify or customize the display name of the organization. Complete these steps in order to customize the display name of the organization:

1. Click **Edit** in the Display Name column. The cursor appears in the name field.
2. Enter the name into the name field.
3. Click **Save**.
4. Click **View** in **Display Name Change History** in order to view the history of the change in display name.

Company Display Name

This tab shows your company's name as registered with Cisco, a display name, if your customer administrator has specified one, your user role, and a way to view the history of any display name changes that have been made.

My Reports

The My Reports page contains this information:

- All of the reports that you recently generated through the Export function. The report names are the same as those listed in the left navigation pane. In order to generate these reports, click **Export** in the reports.
- The scheduled reports are generated by the system via the Schedule Report function. By default, these report names include the username and a unique numeric identifier. You can change the report name when you schedule the reports.

The reports allows you to:

- Download a report on local device for analyzing further or sharing with colleagues.
- See the status of all requested reports.
- See the date on which the report was created. This helps in determining the age of the data in the report.

The saved reports can be in PDF, XLSX, or CSV format, as specified when you generate the report. The reports are usually retained for 72 hours from the time that they are generated.

In order to download the reports to your local device, click the format link (such as XLSX or PDF) in the *Download* column.

> **Note**: Dependent upon the amount of data that must be processed, report generations might take several minutes or hours before they are available for download.

Useful Links

The *Useful Links* page contains links to resources for:

- Training (such as how-to videos, and links to this guide and the CSPC Installation and User Guide)
- Smart Net Total Care community access
- Support
- Contract management
- CSPC software download and release notes
- Smart Net Total Care troubleshooting procedures
- Account management
- Return Material Authorization (RMA) process

Actions

Schedule Report

The Schedule Report feature is available under Actions in the left navigation pane. This allows you to automate generation of the following reports for the selected customer and inventory/segment:

- **Consolidated Bug Report** – This report provide a consolidated view of the bugs that Cisco has correlated for each and every item in the selected customer inventory.
- **Contracts Management Report** – This report provides details about the contract status of all serviceable items that were collected and processed by Smart Net Total Care. This report provides contract information, along with related device information, and helps you manage your Cisco technical support contracts. The report includes only items that are successfully processed and recognized as a Cisco device. The report is presented in twelve main tabs in an Excel file.
- **Custom Inventory Report** – This report provides details about the collected devices in your selected inventory that have been processed by Smart Net Total Care. This report provides contract information, along with related device information, and helps you manage your Cisco technical support contracts. The report includes only items that are successfully processed and recognized as a Cisco device.
- **Inventory Collection Delta** – The Inventory Collection Delta report displays the changes that have occurred in your network devices for a set time duration. This information is useful when you set your report preference to Comprehensive view in the portal application settings. If your network is constantly changing, having a centralized

view of those changes is critical to maintain a highly reliable network. With the inventory collection delta report, you can easily confirm moves, adds, and changes that are made to your network.

- **Inventory Insight Report** – The Inventory Insight Report provides information on all items in all collections for the Entitled Company. The tabs include items that were successfully processed and those that were not. The tabs are classified as 'Actionable', indicating the customer can perform the remedial steps suggested, or 'Informational', indicating that there is no specific customer action required.
- **Upload Processing Report** – The Upload Processing Report provides information on all devices that were part of the Managed Device List and collection but are not reported in Inventory, Contract and Alert reports for various reasons. This report provides visibility for all collections in the Entitled company, provides actionable or informational details. The tabs are classified clearly as 'Actionable', indicating that the customers can perform remedial steps suggested or 'Informational', indicating that there is no specific customer action required. The data is presented to account for every IP address presented for analysis.

To access the scheduler, perform the following:

1. Click the **Schedule Task** link.
2. Select the desired report from the drop-down list.

By default, these report names include the username and a unique numeric identifier. You can change the report name before running reports. You can also add a detailed description for the report. This step is optional.

To run the report on-demand, click **Run Now**. To schedule the report, click **Next**.

1. Set up Recurrence and when to start, then click **Next**.
2. Enter Notification by selecting checkboxes for additional users to be notified by email that the completed report is available, then click **Next**.
3. Review the parameters set in the previous steps, then click **Next**.

Once the report is generated, the report is sent to the registered e-mail address and the report is available under My Reports.

Dashboards

The dashboards provide a consolidated view of the most important data. You can use these dashboards in order to obtain the contract status overview, inventories, devices, and alerts within the installed base of the chosen customer.

The portal includes these dashboards:

- Admin
- Alert Management
- Contract Management
- Inventory Management
- Smart Net Total Care

In order to view the reports and alerts that are most relevant to you, you can create personalized dashboards and save them. These dashboards are retained over subsequent sessions.

Admin

The Admin dashboard is used by the administrators in order to manage the users and device data collections.

The data and reports that the users see within the portal are determined by their roles. Administrators can apply *role-based access control* in order to limit users' access based on what they need to know. For example, one group of users can be given access to data for a specific network segment, while access to another group of users can be limited to only specific reports.

The Admin dashboard contains four *dashlets*:

- Segment Management
- Uploads
- Users

Segment Management

Note: This dashlet is only available to Customer and Partner administrators.

The Segment Management dashlet displays the segments within an inventory and related information. The segments are used for security, for access control, and in order to divide the data that is presented in the portal based on hostname, IP address, or SysName. The segmentation is completed by the administrators, who later grant users access to the individual segments.

You can use the segments in order to direct the users to the information that they use most often, such as by *cost center* or *location*. The users might have access to all of the segments, dependent upon the administrator definitions. If multiple segments contain the same device, and a user selects multiple segments to view, then duplication in the reports occurs.

You can complete these actions through the Segment Management dashlet:

- Create data segments based on multiple criteria, to include Boolean conditions.
- View a list of devices that are included in a created segment.
- Grant users access to data for a segment.
- View, modify, copy, or delete current segments.

Complete these steps in order to create a new segment:

1. Click **Actions**, and then click **Create a New Segment**. The Create a New Segment window appears.
2. Enter a unique segment name into the Name field. Special characters or spaces are not allowed, but you can use numbers.
3. Choose a condition value, such as Hostname or IP Address.
4. Choose a Boolean operator, such as contains or begins with.
5. Enter a matching condition. You can use wildcards.
6. If you must set another condition, click the plus (+) icon.
7. Repeat the previous steps.
8. Review the device list and assign user access, if needed.

Tip: If you want to assign user to segments after you create the segments, alternate methods are provided in the sections that follow.

---

9. Click **Create**. A new segment is created.

Complete these steps in order to view a list of devices in a segment:

1. Right-click a segment name.
2. In the Actions button, choose **View/Modify**.
3. Click **See Device List**.

Complete these steps in order to grant users access to data in a segment:

1. Right-click a segment name
2. In the Actions button, choose **View/Modify**.
3. Click **Select User**. You can select all users or individual users.
4. Click **Add** in order to grant access to the selected users. Users and other customer administrators receive an email notification when they are granted access to a segment or when their access is revoked.
5. Click **Apply** in order to save your changes.

Complete these steps in order to view or modify a segment:

1. Right-click a segment name.
2. In the Actions button, choose **View/Modify**.
3. Modify the settings, as necessary.
4. Click **Apply** in order to save your changes.

Complete these steps in order to make a copy of a segment:

1. Right-click a segment.
2. In the Actions button, choose **Copy to a New Segment**.
3. Enter a new, unique name for this segment.
4. Modify the settings, as necessary.
5. Click **Create**.

The segments that are created by Cisco Branded Reseller (CBR) administrators are visible to the customer administrator in the Segment Management dashlet only. From this dashlet, customer administrators can assign CBR users to a segment that is created by a CBR administrator. However, customer administrators cannot assign customer users to segments that are created by a CBR administrator.

> **Note**: The segments that are created and managed in this dashlet only impact the manner in which data is presented and accessed in the portal reports. This segmentation does not impact the networks themselves at the customer site.

> **Tip**: For more details about segment management, refer to the Network Segment Management video.

Uploads

The Uploads dashlet displays a record of the last collections that were made for an entitled company through one of these methods:

- CSPC upload
- CSV file imports
- Collector file uploads from supported third-party collectors

You can use this dashlet in order to monitor the frequency at which you refresh your network data in the portal.

> **Note**: As a leading practice, customers set their collections to upload once a week or month. Cisco allows a maximum of 5 uploads a day per customer inventory from all methods.

Users

The Users dashlet lists the users who can access data for a given account. As a customer administrator, you can use this dashlet in order to:

- Grant or revoke user access to particular features of the portal.
- View a log of changes that were made to a user account.
- Revalidate the Letter of Authorization (LoA) for CBR users and CBR administrators.

> **Note**: The changes that are made to user access settings become active the next time that the user logs into the system.

In order to view the users that you can manage as a customer administrator, click the icon with three vertically-aligned dots and un-hide the *Manageable* column (if it was previously hidden). If the *Manageable* value for a user is set to *Yes*, then you can manage the user.

If you are a customer administrator, then you can complete these steps in order to manage the access levels for a user:

1. Click the radio button for a user row.
2. From the Actions button, choose **Manage Access**.
3. Grant the user access to Information and Capabilities and Inventory and Segments, as provided in the dialog box. Information and Capabilities refers to features that the user can see or functions that they can perform. Inventory and Segments determine whether the user can perform actions within a given set of collected data.
4. Click **OK** in order to save your changes.

Complete these steps in order to update the LoA for a CBR user:

1. Click the radio button in order to select the user.
2. Click **Actions**, and then click **Revalidate Letter of Authorization (LoA) Access**. A table appears that lists the users whose LoA privilege expires within the next 30 days.
3. Click **Revalidate** in order to continue the LoA privilege for the user.

Note: Customer administrators can perform this action for CBR users and CBR administrators.

Complete these steps in order to view the profile update history:

1. Click the radio button in order to select a user.
2. Click **Actions**, and then click **Profile Update History**.

After these steps are complete, a log appears that lists the actions that were taken by administrators for the selected user. You can use this log in order to review the actions that were completed by other customer administrators.

Note: As an alternative method, you can also view this log via **Actions > Profile Update History > Manage Access**.

Tip: For more details about user access management, refer to the Access Management video.

Alert Management

The Smart Net Total Care system provides information about the customer devices that are impacted by Cisco-published product alerts and security advisories.

Alert management workflows enable you to assign status messages to received alerts. These three status options are available for active alerts, which you can use in order to filter alerts so that you only view those that are most relevant:

- Ignore
- Action Taken
- Action Required

The Alert Management dashboard contains two dashlets: *Active Alerts Summary* and *Last Date of Support*.

Tip: In order to view the alerts in table format, click the link next to the *Alert Type* category legend or the section for the pie in the chart display.

Active Alerts Summary

Note: In default *chart* view, the name of this dashlet is *Active Alerts Summary by Type*.

The Active Alerts Summary dashlet shows the total alert count for each alert type, for the selected inventories. Active alerts are the alerts that you have not acknowledged.

You can use this report in order to:

- View an overall summary of the outstanding alerts by category.
- Export the report data for reference purposes.
- View the devices that are impacted by an alert category (click the appropriate section in the pie chart).

This dashlet helps network administrators and technicians to quickly focus on the most relevant alerts, which increases operational efficiency and improves risk management.

Tip: For more details about alert management, refer to the Alert Prioritization or Alert Administration video.

Last Date of Support

The Last Date of Support dashlet lists the number and details of devices (in the selected inventories) for which the published LDoS for the device hardware:

- Is within 12 months
- Is over 12 months but within 24 months
- Has passed

Tip: For more details about this topic, refer to the Coverage Gaps video.

Contract Management

The Contract Management dashboard shows the status of the Cisco service contracts and the associated devices. This dashboard gives you full visibility into your Cisco network devices, so you can simplify renewals, verify entitlement, and identify coverage gaps and opportunities to consolidate contracts with ease. This dashboard contains these four dashlets:

- All Contracts
- Support Coverage
- Equipment with Expiring Coverage in 30 Days
- Equipment with Overdue Coverage

All Contracts

The All Contracts dashlet provides comprehensive details of the service contracts for the devices that are discovered and validated by the network discovery.

Tip: You can also navigate to **Library > Contracts** in order to view this information, which displays in the table format by default.

Support Coverage

The Support Coverage dashlet displays the number of devices, grouped by their contract status. The pie chart provides consolidated information that is extracted from the more detailed reports in the Contracts library.

For covered devices, these statuses appear:

- **Covered (Signed)** – This status indicates the number of devices for which the coverage is set to begin on a future date.
- **Covered (Active)** – This status indicates the number of devices that are currently covered under a service contract and all of the unique devices with at least one active contract.
- **Covered (Overdue)** – This status indicates the number of devices for which the contract has expired. The contract for these devices can be renewed within 30 days of the expiry date.
- **Covered (Expiring in 90 days)** – This status indicates the number of devices for which the contract will expire within 90 days.
- **Covered (Coverage status not visible)** – This status indicates the number of devices of which you are not authorized to view the contract status. This scenario occurs if the devices are covered by partner contracts.

For non-covered devices, these statuses appear:

- **Not Covered** – This status indicates the number of devices that are not covered by Cisco contracts.
- **Not Covered (Acknowledged)** – This status indicates the number of devices that are not covered by Cisco contracts, but the reason for non-coverage is provided.

If a device is covered by multiple contracts that have different statuses, the device appears under both statuses. For example, if a device has a contract that is active and another that is overdue, the device is counted under both *Covered (Active)* and *Covered (Overdue)* statuses.

If a certain type of contract status is not available in the inventory, it does not appear in the pie chart. For example, if there are no devices with signed contracts, the *Covered (Signed)* status does not appear.

This dashlet provides network administrators and contract administrators a high-level view of the contract coverage for their inventory. This helps them manage contracts more efficiently, which increases the operational efficiency and improves risk management.

> **Note**: The number of covered devices in this dashlet might be different to the number displayed in the Contracts library report and the Inventory Summary report. This is because the covered count in this dashlet represents the number of devices per inventory that are covered by at least one valid Cisco contract. The Contracts library reports and Inventory Summary reports, however, list the number of valid contracts per device. A device might be covered under multiple contracts and can appear multiple times in the report. The number that appears beside the report name represents the row count of the report.

Equipment with Expiring Coverage in 30 Days

The Equipment with Expiring Coverage in 30 Days dashlet lists the devices for which the Cisco service contract expires within 30 days. You can click the *Hostname URL* for more information.

Equipment with Overdue Coverage

The Equipment with Overdue Coverage dashlet lists the devices for which coverage is overdue.

Inventory Management

This dashboard is comprised of data that is collected from your devices and is matched with the Cisco manufacturing and commerce records. It contains two dashlets: *Equipment Type* and *Inventory Source*.

> **Note**: The dashlets in this dashboard provide network administrators and technicians a greater visibility of the devices in their network, which increases operational efficiency and improves risk management.

Equipment Type

The Equipment Type dashlet provides a summary of all devices in your network and is segregated into categories such as power supplies and chassis. Click each category in order to navigate through the various levels of categorization and reach the individual device details.

Inventory Source

The Inventory Source dashlet indicates the source from which each device is uploaded (in the selected inventories), which can be one of these methods:

- Collectors (CSPC and third-party)
- CSV file import
- Collector file upload

Smart Net Total Care

This is the default dashboard that opens when you visit the portal for the first time. This dashboard contains four dashlets:

- Equipment Type
- Support Coverage
- Active Alerts
- Community

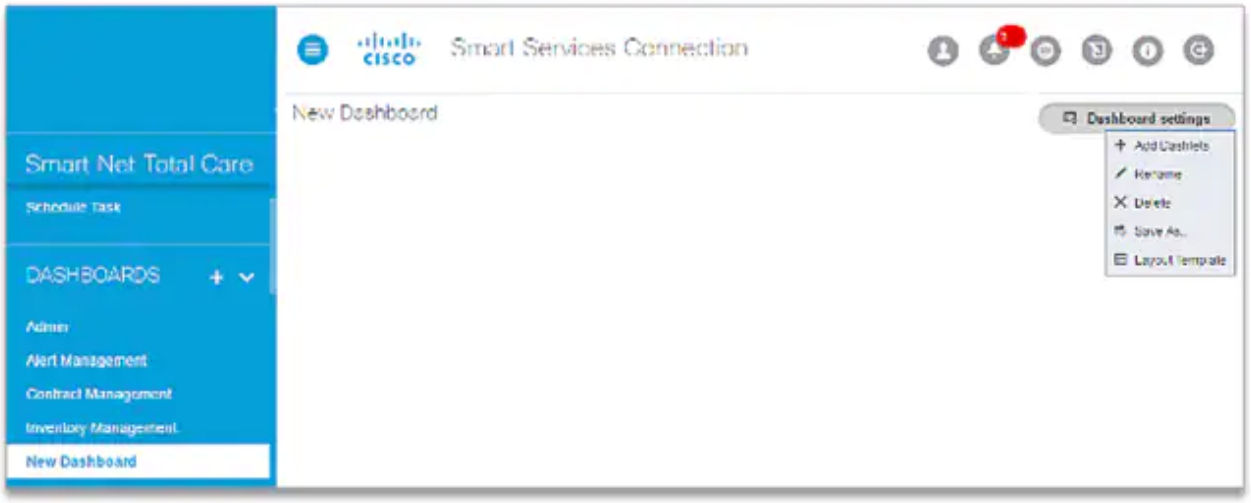
> **Note**: The Community dashlet displays the recent announcements from the Smart Net Total Care team and links to popular discussion topics in the online forum.

Customized Dashboard Creation

In order to view the reports that are most important to you, you can create customized dashboards. These dashboards are saved in the portal and can be accessed from the left navigation pane.

Complete these steps in order to create your own dashboard:

1. Click the plus symbol (**+**) next to the DASHBOARDS heading in the left navigation pane. A blank New Dashboard pane opens.
2. Click **Dashboard Settings** in the New Dashboard pane, and then click **Layout Template**. All of the available layouts for the dashboard appear.
3. Click the radio button next to a layout in order to select it.
4. Click **Add Dashlets**. A list that contains all of the Library reports appears:



5. Choose the report that you want to include in the dashboard. Continue until you add all of the reports that you want to view.
6. Click **Save As** in order to save the dashboard. You can enter a new name for the dashboard, and then click **Create** in order to save it.
7. Click **Rename** in order to rename the dashboard.
8. Click **Delete** in order to delete the dashboard.

Generate and Use Reports

All of the Smart Net Total Care reports are grouped under these categories in the *Library*:

- Administration
- Alerts
- Contracts
- Incidents
- Inventory
- Inventory Insight

This section describes how to use the reports that are grouped under these categories.

Administration

If you are an administrator, the reports in this catalog allow you to track service contract coverage, identify and monitor new devices, and filter for the most relevant alerts. Reliable and regular reports help you proactively access concerns and minimize risks. These reports also help you plan resources and allocate budgets.

Upload Processing

The Upload Processing report provides the status of the completed inventories, or the inventories for which the data analysis is in progress. Sources of inventory upload include:

- Collectors (CSPC and third-party)
- CSV file import

- Collector file upload

When there are more than 20 uploads from the same collector in a 24-hour window, the Customer Administrator is notified by email that duplicate uploads are deleted. This ensure that the uploads are processed

Active Alerts

> **Note**: This report is only visible to the administrators and authorized users.

The Active Alerts report enables administrators to view the alerts that apply to the devices in your inventory and provide/manage alert access to users. SNTC alert reporting takes into account the hardware and software versions, IOS and running config of devices, when that information is available, to determine level of vulnerability (Vulnerable, Potentially Vulnerable, etc.). These alerts can consist of hardware alerts, software alerts, Field Notices (FNs), and Product Security Incident Response Team (PSIRT) alerts. Administrators can use this report in order to:

- Set the alert status to Ignore and explain the reason with comments or notes for all of the affected devices.
- Access the Affected Devices report and set the alert status to Ignore, Action Taken, or Action Required for one particular device.
- Enter a note in order to bring attention to an alert.
- View the alert details.
- View the status and notes for each alert.

This report allows network administrators and technicians to acknowledge the alerts and document actions that you take in response to them, so you are not presented with the same alerts repeatedly. This allows you to check-off alerts to which you have responded, but keep a record of your actions. This also improves operational efficiency and risk management.

Complete these steps in order to change the alert status for all of the devices that are impacted by a particular alert:

1. Click the appropriate checkboxes for each row that you want to modify.
2. Click **Actions**, and then click **Change Alert Status**. A new window opens.
3. Select **Ignore** in order to change the status of an alert from Active to Ignore. Afterwards, the alert no longer appears in the Active Alerts report. In order to revert to Active status, use the All Alerts report.
4. Enter a note into the Notes field. (This step is optional.)
5. Enter a comment into the Comment field. (This step is optional.)
6. Click **OK** in order to confirm.

> **Note**: When you change the status for an Alert, it affects all of your inventories.

Affected Devices

The Affected Devices report lists the devices that are affected by the same alert in the selected inventories. In order to view a list of the devices that are affected by an alert type, click the number link in the *Affected Devices* column.

You can use this report in order to:

- Respond to alerts for individual devices.
- Add additional appliances in an inventory that already exists.

Complete these steps in order to set a response to an alert for individual devices that are impacted by a particular alert:

1. Select the checkboxes for the desired devices.
2. Click **Actions** > **Response to the Alert**.
3. Select one of these options:

- Ignore
- Action taken
- Action Required

4. Enter a comment into the Comments box (this is optional).

5. Click **OK** in order to confirm. Click the **X** in the upper right corner of the dialog box in order to cancel.

Note: Your responses appear in both online and offline alert reports.

In order to view the details of a device, click the link for the desired device in the *Hostname* column.

In order to view the alert status and notes, un-hide the *Response* and *Comments* columns (if not visible by default).

Tip: For more details about alert management, refer to the Identify Relevant Alerts or Alert Administration video.

All Collectors

The All Collectors report lists collectors that are registered for the selected company. The All Collectors grid displays a blue dot icon in front of those collectors with an older CSPC version installed. This highlights CSPC collectors with supported versions and a new version is available.

Review the listed collectors and noted versions. If the version is not available, review further to determine if the collector is online or is no longer active and the registration can be removed.

Data that is gathered from these collectors is included in the data that is reported by the portal.

Note: The additional methods of data upload include CSV file import and collector file upload.

File Import

Note: Only administrators and authorized users can complete a file import.

If you maintain your device data manually in spreadsheets, you can upload the formatted data into the portal. The data is then analyzed and enriched with Cisco support information. This feature enables you to upload device inventory data from a file rather than from an onsite collector.

You can use the File Import feature as a stand-alone method in order to upload data (if you do not want to install a collector) or in conjunction with the collector.

You can use either of these two methods in order to generate the device data file:

- Use the template file that is provided and enter the device information into the file.
- Use a collector in order to generate the device file, and then use the File Import feature in order to upload the device data. In this case, you use the collector in order to gather the device data, but then upload the data manually.

When you upload a file manually along with a collector, you supplement the collector inventory. This enables you to add the devices that are in your network and cannot be collected by the collector. For example, some of the devices might be located behind a Firewall, and some spare devices might not be currently powered-on or connected to the network.

Complete these steps in order to prepare a CSV file for upload with the use of a template:

1. Select **CSV File Import** as the import type.
2. Click the link in order to download the sample CSV file.
3. Enter the information for the parameters.

Note: Remember to delete row 2 and column I.

4. Save the file in .csv format.

Note: You can only have one inventory selected while you access the file import capability.

Complete these steps in order to prepare a collector file for upload:

1. Retrieve the inventory file from the collector. Do not modify this file.
2. Save the file to your local hard drive.

Complete the steps that follow in order to upload the CSV or collector file.

> **Note**: If you intend to replace an inventory that already exists, then select that inventory in the data filter before you proceed.

1. Select the appropriate import type (CSV file import or collector file import).
2. Select the listed inventory that already exists or click **Create a New Inventory**.
3. If you chose to create a new inventory, enter a name into the appropriate field.
4. Choose the type of file that you desire to upload (collector-generated file or CSV file with the use of the template).
5. Click **Choose File** in order to locate the file on your local desktop.
6. Click **Import** in order to upload the file.

The Serial Number (SN) and the Product ID must be recognized as valid by Cisco and must correspond to the data in the Cisco database that is associated with your *entitled* company. If the values are not recognized as valid values, then the item is displayed as such in the Inventory Insight report.

> **Note**: You can add devices to the CSV file for subsequent uploads and they are added to those that you previously uploaded. In order to check the status of an imported file, click **Upload Processing** in the Administration Library.

> **Tip**: For detailed information about the file upload process, refer to the File Import Capability video.

Inventory Deletion

This report allows a Customer/CBR admin to remove an inventory from the customer selection. Administrators can use this report to:

- Remove irrelevant inventories
- Reduce the size of the inventory by deleting old inventories

> **Note** Inventory Deletion can be done only by Customer Admins and CBR Admins. The Customer administrators can provide CBR Admins through the Manage Users option. The inventory deletion will only be from the Customer selection and not a data base deletion. If the collector remains active (registered and uploading) it will re-enable the customers inventory to the portal.

To delete an inventory, perform the following:

1. Click the desired inventory.
2. Click **Actions** > **Inventory Deletion**. A confirmation screen appears.
3. Click **Confirm** to delete the inventory.
4. Click **Refresh** to view the updated list of inventory in this report.

> **Note** To view the changes in the portal, refresh your browser.

To view the Inventory Deletion History, perform the following:

1. Click **Actions** > **Inventory Deletion History**.
2. The Inventory Deletion History page appears with the list of deleted inventories.
3. Click **Close** to close the Inventory Deletion page.

To view the Inventories Restored During Collection, perform the following:

1. Click **Actions**, > **Inventory Restored with New Collection**.

2. The Inventory Restored with New Collection page appears with the list of restored inventory when CSPC is configured during automatic collection.

3. Click ,**Close** to close the Inventory Restored with New Collection page.

Tip: For more detailed information about the inventory deletion, refer to the Inventory Deletion video.

Segment Exclusions

The Segment Exclusions report lists all of the devices in an inventory that are not grouped into a segment. This is especially helpful if you use segments in order to group your devices.

Administrators can use the *Actions* menu in the Segment Management dashlet of the Administration Dashboard in order to create/edit segments, set-up access rules, and place the un-segmented devices into specific segments.

This report helps administrators determine the devices that are not grouped into a segment and take action.

Alerts

The reports in this catalog are related to the alerts that are provided by the portal. In order to preempt network disruption and minimize vulnerabilities, you can identify and proactively act on the alerts that impact the devices in your network.

With an active alerts report you can:

- Quickly learn which devices are vulnerable to threats
- Identify which devices require software updates
- Review your alert remediation activities

Here are the different types of alerts that might impact the devices in your network:

- Hardware alerts inform you about End-of-Life (EoL) issues with the devices in your network.
- Software alerts inform you about EoL issues with the software versions you use in your network.
- Security alerts inform you about the security vulnerabilities that are associated with specific devices in your network.
- Hardware Field Notices (FNs) inform you about other significant issues (apart from security vulnerability issues) with a hardware device. A hardware FN often requires customer action, such as a Return Material Authorization (RMA).
- Software FNs inform you of other significant issues (apart from security vulnerability issues) with a software version you use in your network. A software FN often requires customer action as well.

SNTC alert reporting takes into account the hardware and software versions, IOS and running config of devices, when that information is available, to determine level of vulnerability (Vulnerable, Potentially Vulnerable, etc.). These reports help network administrators and technicians focus on the alerts and FNs that are most important, which improves operational efficiency and risk management.

Tip: For more details about alerts, refer to the Alert Prioritization or Alert Administration video.

All Alerts

The All Alerts report lists the product alerts for the selected inventories, categorized by type. You can use this report in order to:

- Change the status of an alert from Ignore to Active.
- Review the alerts based on the number of affected devices or sort by status.

In order to view the alerts that affect the maximum number of devices, click the **Affected Devices** column heading so that the arrow-head points down. This sorts the information in descending order.

In order to view the alert description, as published by Cisco, click the URL for the desired alert row in the *More Info* column.

In order to view the alert status, notes, and have the ability to sort by status, un-hide the *Status* and *Notes* columns (if not visible by default).

Complete these steps in order to change the alert status from *Ignore* to *Active*:

1. Click the appropriate checkbox for each alert that you want to change.
2. Click **Actions**, and then click **Change Alert Status**. The Active status is selected by default.

3. Enter a note in the Notes field. (This step is optional.)

Note: Only administrators and users with alert management permissions can complete this task.

The Actions menu in this report cannot be used in order to change the status from Active to Ignore. If you have access to the Administrator reports, navigate to **Library > Administration > Active Alerts** and change the status from Active to Ignore. Otherwise, contact the customer administrator in your organization.

Note: After you take action on all of the affected devices for a given alert, the status becomes *Acknowledge*.

All Field Notices

The All Field Notices report lists the hardware and software FNs, categorized by type, for the selected inventories. You can use this report in order to:

- Change the status of an FN from Ignore to Active.
- Review FNs based on:
  - The number of affected devices
  - The vulnerability assessment of FNs

In order to view the FNs that affect the maximum number of devices, click the **Affected Devices** column heading so that the arrow-head points down. This sorts the information in descending order.

In order to view the FN description, as published by Cisco, click the URL for the desired row in the *More Info* column.

In order to view the FN status and notes, un-hide the *Status* and *Notes* columns (if not visible by default).

Complete these steps in order to change the FN status from *Ignore* to *Active*:

1. Click the appropriate checkboxes for each of the FNs that you want to change.
2. Click **Actions**, and then click **Change Alert Status**. The Active status is selected by default.
3. Enter a note into the Notes field. (This step is optional.)

Note: This task can only be performed by administrators and users that have alert management permissions.

Note: After you take action on all of the affected devices for a given FN, the status becomes *Acknowledge*.

The Actions menu in this report cannot be used in order to change the status from Active to Ignore. If you have access to the Administrator reports, navigate to **Library > Administration> Active Alerts**, and then change the status from Active to Ignore. Otherwise, contact the Smart Net Total Care administrator in your organization.

All Hardware Alerts

The All Hardware Alerts report lists the hardware alerts, categorized by type, for the selected inventories. You can use this report in order to:

- Change the status of an alert from Ignore to Active.
- Review the alerts based on:
  - The number of affected devices
  - The LDoS for the device hardware (if published)

In order to view the alerts that affect the maximum number of devices, click the **Affected Devices** column heading so that the arrow-head points down. This sorts the information in descending order.

In order to view the alert description, as published by Cisco, click the URL for the desired row in the *More Info* column.

In order to view the alerts status and notes, un-hide the *Status* and *Notes* columns (if not visible by default).

Complete these steps in order to change the alert status from *Ignore* to *Active*:

1. Click the appropriate checkboxes for each alert that you want to change.

2. Click **Actions**, and then click **Change Alert Status**. The Active status is selected by default.
3. Enter a note into the Notes field. (This step is optional.)

Note: After you take action on all of the affected devices for a given alert, the status becomes *Acknowledge*.

Note: This task can only be performed by administrators and users that have alert management permissions.

The Actions menu in this report cannot be used in order to change the status from Active to Ignore. If you have access to the Administrator reports, navigate to **Library > Administration > Active Alerts**, and then change status from *Active* to *Ignore*. Otherwise, contact the Smart Net Total Care administrator in your organization.

All Security Advisories (PSIRTs)

Note: Only the High and Critical Product Security Incident Response Team (PSIRT) advisories are displayed in this report.

The All Security Advisories (PSIRTs) report lists the PSIRT advisories, categorized by type, for the selected inventories. The PSIRTs are available only for the devices that run these Operating Systems (OSs):

- IOS
- IOS XE
- ASA
- IOS XR
- NX-OS

You can use this report in order to:

- Change the status of a PSIRT from Ignore to Active.
- Review alerts based on:
  - The number of affected devices
  - The vulnerability assessment of PSIRTs
- View the Security Impact Rating (SIR) based on the Common Vulnerability Scoring System (CVSS) score. 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.

In order to view the PSIRTs that affect the maximum number of devices, click the **Affected Devices** column heading so that the arrow-head points down. This sorts the information in descending order.

In order to view the PSIRT description, as published by Cisco, click the URL for the desired row in the *More Info* column.

In order to view the PSIRT status and notes, un-hide the *Status* and *Notes* columns (if not visible by default).

Complete these steps in order to change the PSIRT status from *Ignore* to *Active*:

1. Click the appropriate checkboxes for each of the PSIRTs you want to change.
2. Click **Actions**, and then click **Change Alert Status**. The Active status is selected by default.
3. Enter a note into the Notes field. (This step is optional.)

Note: This task can only be performed by administrators and users that have alert management permissions.

Note: After you take action on all of the affected devices for a given alert, the status becomes *Acknowledge*.

The Actions menu in this report cannot be used in order to change the status from Active to Ignore. If you have access to the Administrator reports, navigate to **Library > Administration > Active Alerts**, and then change status from *Active* to *Ignore*. Otherwise, contact the Smart Net Total Care administrator in your organization.

All Software Alerts

The All Software Alerts report lists software alerts, categorized by type, for the selected inventories. You can use this report in order to:

- Change the status of an alert from Ignore to Active.
- Review alerts based on:
  - The number of affected devices
  - The LDoS for the device software (if published)

In order to view the alerts that affect the maximum number of devices, click the **Affected Devices** column heading so that the arrow-head points down. This sorts the information in descending order.

In order to view the alert description, as published by Cisco, click the URL for the desired row in the *More Info* column.

In order to view the alert status and notes, un-hide the *Status* and *Notes* columns (if not visible by default).

Complete these steps in order to change the alert status from *Ignore* to *Active*:

1. Click the appropriate checkboxes for each alert that you want to change.
2. Click **Actions**, and then click **Change Alert Status**. The Active status is selected by default.
3. Enter a note into the Notes field. (This step is optional.)

Note: This task can only be performed by administrators and users that have alert management permissions.

Note: After you take action on all of the affected devices for a given alert, the status becomes *Acknowledge*.

The Actions menu in this report cannot be used in order to change the status from Active to Ignore. If you have access to the Administrator reports, navigate to **Library > Administration > Active Alerts**, and then change the status from *Active* to *Ignore*. Otherwise, contact the Smart Net Total Care administrator in your organization.

Devices with Alerts

The Devices with Alerts report provides an alert count for each alert type, for every device in the selected inventories.

In order to view the unique alerts for a device, click the number link under each alert type column.

Last Day of Support

The Last Day of Support report lists all of the devices (in the selected inventories) for which the published LDoS for the device hardware is within the next two years or past the current date.

This report enables the network administrators and contract administrators to plan proactively for current or future changes in device availability, which increases operational efficiency and improves risk management.

In order to change the date range in the Last Date of Support column, click the search field under the *Last Date of Support* column heading and use the date search function in order to enter a date range.

Complete these steps in order to view the LDoS record for a specific device:

1. Click the search field under the Serial Number column heading and enter the device SN.
2. Press **Enter**.

If no records appear, the LDoS of the device hardware is not within the next two years.

In order to view the LDoS alert, click the link that corresponds to the device in the *Alert URL* column.

Complete these steps in order to view the contract details for a device:

1. Scroll horizontally in the report until the Contract No. column becomes visible.

2. Click the URL that corresponds to the desired device. If the Contract No. value is Other or Partner Branded Contracts, then you are not authorized to access the details.

Complete these steps in order to update notes:

1. Select the checkboxes for the desired devices.

2. Click **Actions** > **Specify LDOS Notes**. The Specify LDOS Notes page appears.
3. Enter the relevant notes in the text box.
4. Click **OK** to save the notes.

Note: To view the changes in the portal, refresh your browser.

You can also select multiple devices and specify LDOS notes. Alternatively, you can filter the required columns and specify LDOS notes. For example, filter the Equipment Type with CHASSIS to list the corresponding devices. From the **Actions** menu, select **Specify LDOS Notes**.

Tip: For more details about LDoS, refer to the Coverage Gaps video.

Product Alerts Delta

The Product Alerts Delta report displays the new or modified alerts (of each type) for a particular inventory over a specific time period. Here are the types of alerts that appear in this report:

- **New Alerts** – This area of the report indicates the number of alerts that were added between the start and end date.
- **Modified Alerts** – This area of the report indicates the number of alerts that were changed between the start and end date.

  Note: If the same alert is modified in the consequent upload, then the new alert is marked as zero and added to the modified alert count.

- **Total Alerts as on <End_Date>** – This area of the report indicates the total number of alerts (of each type) that are available in the database on the selected end date. This includes the new alerts, the modified alerts, and the unmodified old alerts.

Complete these steps in order to change the date range:

1. Choose a start date for the desired time period from the Start Date pop-up calendar.
2. Choose the end date for the desired time period from the End Date pop-up calendar. This date must be later than the start date.
3. Click **OK** in order to confirm.

In order to view a list of devices for each category, click the numbers under the *New Alerts* or *Modified Alerts* column.

The default time period for this report is 90 days. Complete these steps in order to change this default time period:

1. Click the gear icon.
2. Choose **Set Timeframe**.
3. Change the timeframe as appropriate.

Contracts

The reports in this library provide information about the service contracts that your company has with Cisco.

All Contracts

The All Contracts report provides comprehensive details for all of the service contracts, devices under the contracts, and also the status of the contracts. You can complete these tasks with this report:

- Identify the coverage gaps and the associated risks in the network.
- View any future expirations.
- View the contract details.
- View the devices that are associated with each contract.

The contract administrators can use this report in order to receive a comprehensive view of their network from a support perspective, which helps to improve operational efficiency and risk management.

For more details about the All Contracts report, refer to these videos:

- Contract Details
- Access Service Coverage Information
- Coverage Gaps
- Expiring Coverage
- Access Service Contracts

Covered

The Covered report lists the devices (in the selected inventories) that are covered by one or more valid Cisco service contracts. You can complete these tasks with this report:

- View the devices and their associated contracts.
- View the LDoS for a device (if published).
- View the contract details.
- Set coverage actions, including additional comments
- Ability to request Installed-at-Site information changes from within the portal by customer administrator and any user granted access.

The contract administrators can use this report in order to view the contracts that are associated with the various devices in their network and set coverage actions with comments, which improves operational efficiency and risk management.

To specify the coverage action history, perform the following:

1. Select the checkbox for each contract row you want to specify the coverage action.
2. Click **Actions** > **Specify Coverage Action**. The Specify Coverage Action screen appears.
3. Select the relevant reason from the list.
4. Enter a note in the **Notes** field. (This step is optional.)
5. Click **OK**.

To view the Coverage Action History, perform the following:

1. Select the checkbox for each contract row you want to review the coverage action.
2. Click **Actions** > **View Coverage Action History**. The Coverage Action History screen appears.

To view request the Update Installed-at-Site, perform the following:

1. Select the checkbox for each contract row you want to review the coverage action.
2. Click **Actions** > **Update Installed-at-Site**. The Update Installed-at-Site screen appears.
3. Select the relevant option:

- To add/update to an Installed-at-Site, Select Installed-at-Site. Search the required details in the text box.
- To create a new Installed-at-Site, Select New Installed-at-Site. Enter the required new site information.

4. Click Update to update the Installed-at-Site information.

Note: Updates may take up to 72 hours, Cisco will make the changes through the standard case process.

To verify the pending request for the selected devices, perform the following:

1. Select the checkbox for each contract row you want to review the coverage action.
2. Click **Actions** > **View Site Info History**. The View Site Info History page appears.

To view bulk action status, perform the following:

1. Select the checkbox for each contract row you want to view the coverage action status.
2. Click **Actions** > **Bulk Action Status**. The Bulk Action Status screen appears.

For more details about this report, refer to these videos:

- Contract Details
- Access Service Coverage Information
- Coverage Gaps
- Expiring Coverage
- Access Service Contracts

Not Covered

The Not Covered report lists the devices in the selected inventories that are not presently covered under a service contract. You can use the Actions menu to annotate any needed coverage action, thereby cleaning up the report.

The contract administrators can use this report in order to view the devices in their network that might need service coverage, which improves operational efficiency and risk management.

To specify the needed coverage action, perform the following:

1. Select the checkbox for each device row you want to specify the coverage action.
2. Click **Actions** > **Specify Coverage Action**. The Specify Coverage Action screen appears.
3. Select the relevant reason from the list.

- Review Needed
- Still Under Warranty
- To Cover
- Renew Coverage
- Spare, Not to Cover
- Replacement Planned
- Decommissioned
- No Coverage Required

4. [Optional] Enter a note in the **Comments** field.
5. Click **OK**

Once processed, you can then filter the report to focus on specific actions needed or reasons not covered.

For more details about this report, refer to these videos:

- Access Service Coverage Information
- Coverage Gaps
- Access Service Contracts

Expiring Device Coverages

The Expiring Device Coverage report lists the devices whose coverage end date is close. By default, the devices are sorted by coverage end date. You can complete these tasks with this report:

- Obtain a list of devices for which the service contract is about to end.
- View the contract details.

This report helps contract administrators to renew device coverage in a timely manner, which improves operational efficiency and risk management.

Tip: In order to sort the devices by equipment type, coverage status, or other categories, click the chart icon.

For more details about this report, refer to these videos:

- Contract Details
- Access Service Coverage Information
- Coverage Gaps
- Expiring Coverage

- Access Service Contracts

Devices with Multiple Contracts

The Devices with Multiple Contracts report lists the devices (in the selected inventories) that are covered by more than one service contract.

> **Tip**: In order sort the devices by equipment type, coverage status, or other categories, click the chart icon.

> **Note**: If the Contract No. value is *Other* or *Partner Branded Contracts*, you are not authorized to access the details.

For more details about this report, refer to these videos:

- Contract Details
- Access Service Coverage Information
- Coverage Gaps
- Expiring Coverage
- Access Service Contracts

Incidents

Your interactions with the Cisco Technical Assistance Center (TAC) are available in the Incidents report.

All Support Cases for Past 90 Days

The All Support Cases report lists the service requests that you (the logged in user) have raised with the Cisco TAC within the last 90 days (for the selected inventories and customer).

This report provides visibility to all of the open TAC cases in one report. This helps network administrators and network technicians manage risks more efficiently.

> **Note**: SNTC portal will list cases created only from SNTC portal. It will not display cases created from other portals like Support Case Manager etc.

Inventory

The reports that are included in this library provide a comprehensive view of your Cisco installed base and include the device and configuration details such as SNs, Product IDs (PIDs), OS versions, installed memory and firmware, IP addresses, and hostnames. This information enables you to complete these tasks:

- Identify the Cisco products that will soon reach EoL, End-of-Sale (EoS), or LDoS.
- View the data about that which has been moved, added, or changed within your network.
- Verify whether your Cisco hardware runs the most current and supported software versions.
- Plan upgrades for the devices that are no longer supported.

These reports enable network administrators and technicians to view the details for all of the equipment within their network and the product coverage status, which helps improve operational efficiency and risk management.

For more details about the Inventory reports, refer to these videos:

- See Inventory Devices
- Inventory Collection Delta

Summary

The Summary report lists the total number of chassis, modules, power supplies, fans, and other devices in the inventory, based on different categories such as contract coverage and LDoS records. Keep your inventories current and accurate, so you have a comprehensive view of the devices on your network.

With the summary report, you can easily:

1. See a summary of devices in your network
2. Identify devices covered and not covered
3. Review last day of support data

This information is available in the Summary report:

- **Devices in Inventory (all sources)** – This section lists all of the equipment within the inventory system.
- **Devices Collected** – This section of the report lists the services that were obtained through a collector, such as CSPC, in the inventory system.
- **Devices Imported** – This section lists the devices that were manually entered in the inventory system through CSV upload.
- **Devices Recognized** – This section lists the services that are recognized by the system because their SN is present in the Cisco manufacturing databases.
- **Devices Covered** – This section lists the recognized devices that are covered by a valid service contract.
- **Devices Not Covered** – This section lists the recognized devices that are not covered by a valid service contract.
- **Past LDoS** – This section lists the devices for which the LDoS has been reached.
- **LDoS within 12 Months** – This section lists the devices for which the LDoS is within the next 12 months.
- **LDoS over 12 months and within 24 Months** – This section lists the devices for which the LDoS is between 13 to 24 months from the current day.

Tip: In order to view the equipment details, click the number link under the desired category and equipment type.

All Equipment

The All Equipment report lists all of the equipment with the equipment type (such as chassis, modules, power supply, and fan) for the selected inventories. You can complete these tasks with this report:

- View a summary of the devices that are discovered by collection or file import.
- Create customized inventory reports from specified data.

Note: If no IP address is received for a device during the inventory upload, its *IP Address* field is "--".

You can click the desired link under Hostname in order to view the device details.

Complete these steps in order to create a support case:

1. Click the checkbox next to the device for which you want to create a support case.
2. Click **Actions**, and then click **Create Support Cases**.

Inventory Duplicates

The Inventory Duplicates report provides the details for devices that are included in more than one inventory.

In order to view the device details, click the desired link under *Hostname*.

Note: If no IP address is received for a device during the inventory upload, its *IP Address* field is "--".

Inventory by Product

The Inventory by Product report provides an inventory report that is sorted and grouped by Product ID (PID). You can complete these tasks with this report:

- View a summary of the deployed devices that is sorted by PID.
- Identify the number of products and their coverage statuses, based on their PID.
- View the LDoS for the devices. The LDoS is displayed only if the LDoS is past the current (system) date.

In order to view the device details, click the number link under *Covered and Not Covered*.

In order to view the Cisco-specified alert notices, click the desired URL under *Alert URL*.

Inventory Collection Delta

The Inventory Collection Delta report displays the changes that have occurred in your network devices for a set time duration. This information is useful when you set your report preference to *Comprehensive view* in the portal application settings. You can complete these tasks with this report:

- View the number of devices that were added, deleted, or changed for any two uploads.
- Categorize the changes based on the equipment type.
- View the details of the selected devices.

Note: You must select a single inventory in order to use this report.

The report profile identifies the date and time of the upload for each snapshot, the collector from which the inventory was uploaded, and the total number of devices that where uploaded and imported in each inventory.

In order to view the details of the changed devices, click the numbered link for any of the device totals.

Tip: For more details about the Inventory Collection Delta report, refer to the Inventory Collection Delta video.

Inventory by Sites

The Inventory by Sites report shows the installation location details for the devices in the inventory. This report provides the unique installed-at-site ID, the address, and the customer for each of the identified sites.

You can use this report in order to view the number of devices at each site that are covered or not covered by a Cisco service contract.

Note: If no IP address is received for a device during the inventory upload, its *IP Address* field is "--".

All Hosts

The All Hosts report lists all of the hosts in the inventory. You can use this report in order to accomplish these tasks:

- View all of the chassis within the inventory.
- View the chassis or cards that have independent host names.
- Identify the OS type and versions on the devices.

Note: A master chassis might refer to a slave chassis, each with their own identity.

In order to view the device details or the device configuration for the host, click the desired link under *Hostname*, and the details page opens.

In order to view the configuration details, click **Running Configuration** or **Startup Configuration**, and the configuration details appear in a new window.

Custom Inventory

The Custom Inventory report lists all of the equipment and their details for the selected inventories. This report also provides the contract information, and the LDoS (if published) for the devices in the inventory.

In order to view the device details, click the desired link under *Hostname*.

Note: If no IP address is received for a device during the inventory upload, its *IP Address* field is "--".

Inventory Insight

The reports that are included in the Inventory Insight library provide additional information about the devices that are identified by the service.

These reports provide network administrators and technicians an up-to-date view of their network, which helps them maintain business continuity, increase operational efficiency, and improve risk management.

Summary

The Summary report lists the information about the collector through which the selected inventory was uploaded. It displays the Appliance ID, the most recent upload time, and an overview of the collection.

The Summary report provides this information:

- **IP addresses in the Managed Device List** – This section of the report provides the total IP addresses in the managed device list.
- **IP addresses Not Collected** – This section of the report shows the total IP addresses in the managed device list that the collector could not reach. These are the potential reasons that the collector could not reach the devices:
  - The device had bad credentials.
  - The device was offline.
  - The device did not respond.
- **Reported** – This section of the report lists the equipment in the collection that is included in the Smart Net Total Care Installed Base Management and Contract Management reports. The equipment in this section is presented via these categories:
  - **Chassis** – This category shows the chassis that are successfully identified and processed.
  - **Module** – This category shows the modules that are successfully identified and processed.
  - **Power Supply** – This category shows the power supplies that are successfully identified and processed.
  - **Fan** – This category shows the fans that are successfully identified and processed.
  - **Other** – This category is used for all other types of equipment that are successfully identified and processed.
  - **Not Field Replaceable** – The equipment that cannot be replaced without assistance from Cisco are included in this category. In order to view the device details, click the number link.
  - **Not Recognized** – The equipment that is not found in the Cisco records is included in this category and is, therefore, not recognized as Cisco equipment. In order to view the device details, click the number link.
- **Not Reported** – This section of the report provides the equipment in the collection that is not rendered in the Smart Net Total Care Installed Base Management and Contract Management reports due to processing errors or data discrepancies in one of the Cisco databases. For equipment that is included in this section, follow the remedial action that is provided (if any). The equipment in this section is presented via these categories:
  - **3rd Party** – This category shows the equipment that was identified as non-Cisco, third-party equipment. In order to view the device details, click the number link.
  - **Duplicate** – This category presents any duplicate equipment information that is identified in the inventory. In order to view the device details, click the number link.
  - **Others** – This category lists the equipment that could not be fully categorized by the current Smart Net Total Care software system based on the collected information. In order to view the device details, click the number link.

Not Collected

The Not Collected report lists all of the devices that were included in the managed device list, but did not respond to the collector. You can use this report in order to view the Cisco devices that are processed (enriched with Cisco data), but not a part of the current collection. This report also provides this information:

- The reason that the device was not collected. The most common reason is incorrect credentials in the Managed Device list. Check the Managed Device list for errors.
- The suggested actions that you can complete in order to rectify the errors.

Note: If no IP address is received for a device during the inventory upload, its *IP Address* field is "--".

Tip: For more details about this report, refer to the Update Managed Device List video.

Third Party

The Third Party report lists all of the collected devices that are identified as non-Cisco devices. This report gives you a complete picture of your installed base because it includes third-party devices, even though they cannot be enriched by the Cisco support information.

> **Note**: If no IP address is received for a device during the inventory upload, its *IP Address* field is "--".

Duplicates

The Duplicates report lists the devices that appear more than once in the collected data. This report also provides the possible reasons for the duplicate entries.

Not Recognized

The Not Recognized report lists the Cisco devices (in the selected inventories) that could not be validated as Cisco devices, or the system could not determine the device type. This report helps you identify the Cisco devices that can potentially be processed by the collection and enriched with Cisco data.

The report also provides the reason that certain devices are not identified.

> **Note**: If no IP address is received for a device during the inventory upload, its *IP Address* field is "--".

Not Field Replaceable

The Not Field Replaceable report lists the components within the devices (in the selected inventories) that are no longer serviced or replaced by the Cisco Field team.

> **Note**: The non-field replaceable devices are not covered by a service contract, so spare parts cannot be procured for them.

> **Note**: If no IP address is received for a device during the inventory upload, its *IP Address* field is "--".

Others

The Others report lists the devices that appear due to a problem with the data analysis. These devices are not accounted for by the other Inventory reports. This report provides the possible reasons for the problems.

You can use this report in order to identify the devices that can potentially be enriched with the Cisco support information in the portal.