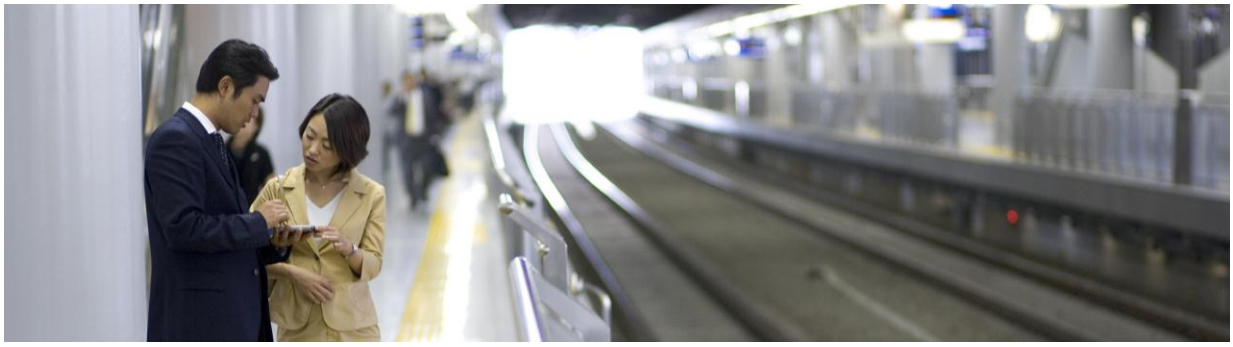
White Paper

Smart Net Total Care: Increasing Operational Efficiency and Reducing Risk to Your Network



As networks become more critical for business applications and communications, the ability to understand your Cisco installed base and maintain business continuity becomes crucial.

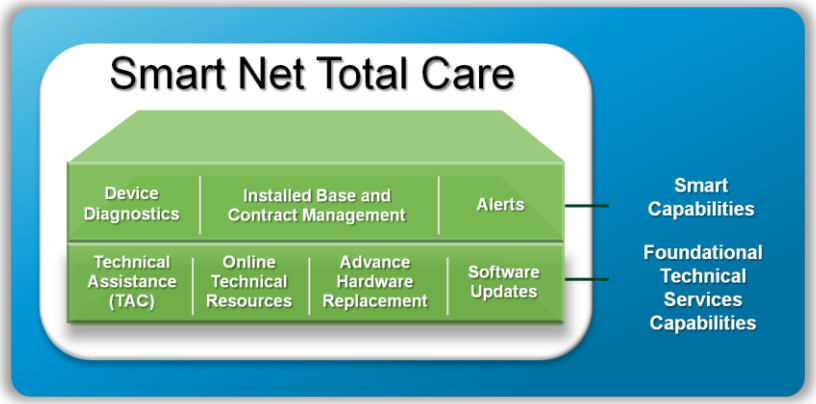
Cisco® Smart Net Total Care service meets these needs by providing extensive installed base and contract management, along with foundational technical services, device diagnostics, and alerts for your Cisco products. This proactive maintenance package improves risk management, helps resolve problems quickly, and reduces operating expenses. Using information from a secure discovery of Cisco products and correlating it with Cisco's intellectual capital and product expertise, Smart Net Total Care delivers actionable intelligence, relevant recommendations and information, and proactive support capabilities that reduce operating costs and minimize downtime.

Contents

Introduction

Smart Net Total Care identifies your Cisco inventory and securely communicates this to Cisco's data center, where it is validated and analyzed against unique Cisco manufacturing, security, shipping and contract data. The result is a comprehensive view of your installed base and service contracts, helping you to make informed decisions about your network. Detailed inventory information, life cycle status, contract coverage, and targeted alerts are available through a secure web portal. Proactive device diagnostics and foundational technical service capabilities all work together to help you maintain your Cisco network.

Figure 1. Smart Net Total Care packaging



Core Capabilities

Installed Base and Contract Management

Regular collection and flexible reporting capabilities help you manage your Cisco inventory and contracts by identifying and tracking what's new, what's changed, what's covered, and what's not. In this way service coverage and issue resolution are delivered using world-class Cisco expertise. Smart Net Total Care delivers

- Insight into your Cisco installed base and contract coverage for supported Cisco network, data center, and collaboration products
- Secure, ongoing Cisco product visibility, validated and correlated with Cisco intellectual capital (including contract and manufacturing databases)
- Lifecycle management assistance with reporting on end-of-life, end-of-sale, or end-of-support (EoX) in the next 12 months
- Contract consolidation to minimize and simplify the number of contracts
- Regular network discovery to manage network changes over time
- Powerful, flexible reporting capabilities

Alerts and Notifications

Network disruption is minimized by proactively identifying and notifying administrators of installed devices affected by Cisco product-specific alerts and security advisories. Smart Net Total Care provides targeted hardware,

software, field, and Product Security Incident Response Team (PSIRT) alerts and notifications, which are targeted to your collected Cisco installed base.

Device Diagnostics

Smart Net Total Care accelerates early diagnosis and remediation of faults through proactive, rules-based problem resolution. Devices enabled with Smart Call Home technology can continuously monitor their own health and notify you of potential issues using a secure, personalized web portal that contains messages, detailed diagnostics, and recommendations. With these diagnostics, you have

- Real-time troubleshooting, alerts, and remediation advice
- Automatic generation of Cisco service requests to Cisco technical engineers, if needed
- Secure, reliable data transport
- Personalized web-based portal to review Call Home messages, detailed diagnostics, recommendations, and inventory

Foundational Technical Services

Critical network issues must be resolved rapidly. Smart Net Total Care combines expert technical support, flexible hardware coverage, and smart, personalized capabilities to facilitate issue resolution and improve operational efficiency. This coverage gives you

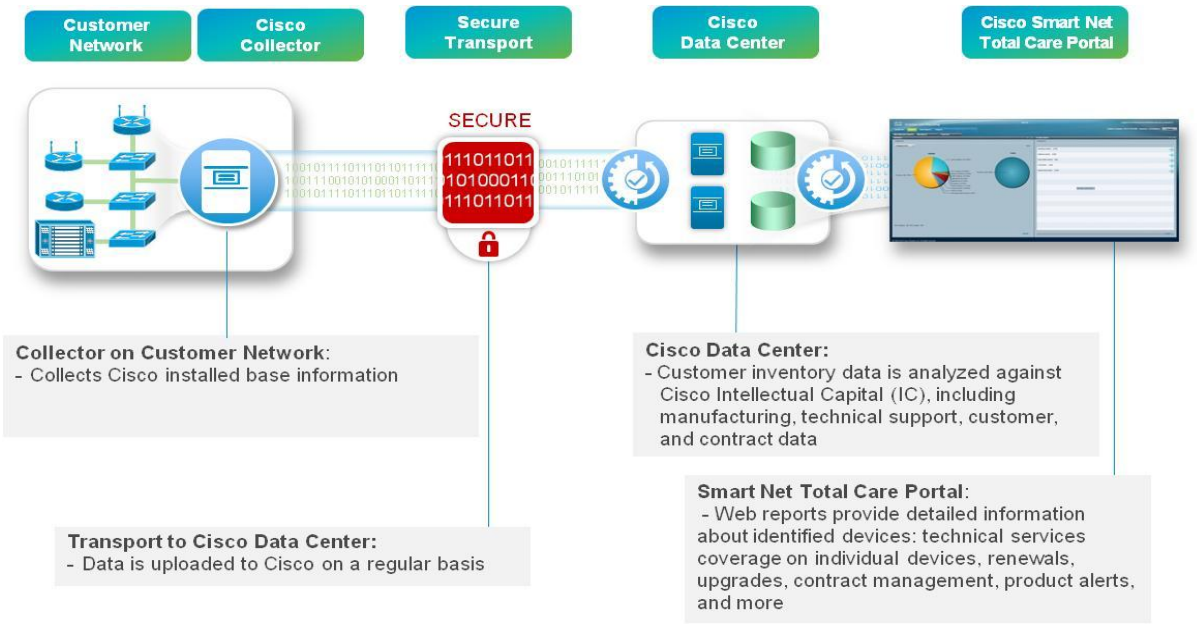
- Direct access 24 hours a day, 365 days a year to specialized engineers in the Cisco Technical Assistance Center (TAC)
- Online resources provide fast self-service support
- Advance hardware replacement is available to fit your needs, with rapid access to critical replacement parts in as little as 2 hours
- Anytime access to eligible software updates
- Standard or optional onsite replacement by Cisco field engineers

An End-to-End View

There are three major components in the Smart Net Total Care solution

- Cisco collector
- Cisco data center
- Reports via Smart Net Total Care portal

Figure 2. Major components of Smart Net Total Care



Cisco Collector

A key component in the collection process is the Cisco collector, which gathers inventory data from devices in the customer's network. Except where noted, the term *collector* applies to either the Common Services Platform Collector (sometimes referred to as CSPC) or the Cisco Network Collector (also known as CNC), a specially configured Solaris based appliance.

The collector automates data collection from the installed Cisco devices. This collection is accomplished by either automatic discovery of Cisco devices or using a customer-provided seed file for data collection.

- A seed file consists of the IP addresses and access credentials for the devices that are to be inventoried.
- The collector also allows automatic discovery of Cisco devices using various protocols such as CDP, Routing Table, ARP, OSPF, BGP and ping sweep.

The collector uses several protocols to collect inventory information from the Cisco devices in the customer network. The customer provides appropriate access between the collector and the Cisco devices to support the use of these protocols. The supported protocols are as follows:

SNMP

SNMP access between the collector and each device is necessary for the collector to function properly. The collector uses the SNMP read-only string to manage devices and collect inventory data.

Telnet

The collector can be configured to use telnet to collect data. The collector software requires privileged mode access for devices to collect configuration data. Cisco recommends the use of a TACACS+ server to store user names and passwords to authenticate access to network devices. With appropriate configuration of the TACACS+ server, the customer can further limit the types of commands that the collector can execute on their devices.

SSH

The collector supports SSH-based CLI access to network devices. Cisco recommends using this method for CLI access instead of the less secure telnet-based sessions. SSH provides a secure form of remote access to network devices by encrypting all traffic—including passwords—between the collector and the network device. The collector supports both SSH versions 1.5 and 2.0 for inventory collection.

ICMP

The collector uses ICMP ping messages as a method of discovering Cisco devices and as a way to monitor device and network availability.

Secure Transport

After the customer's worldwide installed base data is collected, data is transported from the collector to the Cisco data center on a regular basis via a secure connection. The frequency of data uploads is mutually agreed upon by the customer and Cisco. Cisco strongly recommends inventory collection processing at least once every quarter so that an up-to-date set of information is available to produce reports.

To successfully and securely upload the data to the Cisco data center, the collector requires access via SSL to the Cisco upload servers. Prior to transmission, customer raw data is packaged and encrypted using the AES-128 encryption algorithm. The encrypted data is also signed using Public Key Infrastructure (PKI).

The encrypted and signed package is then transported via the secured HTTPS or SSL protocols to the Cisco data center. By using HTTPS or SSL, the customer data is again encrypted before it reaches the upload server in the Cisco data center. All sensitive device passwords/credentials, such as SNMP strings and encoded enable passwords, are masked with x's from the associated device configurations.

Security is further enhanced in the Smart Net Total Care 1.6 release with the data privacy feature. This feature allows customers to keep IP addresses and/or hostnames private. Customers have the option to map the IP address and/or hostname fields in the data collected by CSPC before the data is sent to the Cisco data center. As a result, only the mapped values are sent to Cisco data center; the actual hostname and/or IP address never leaves the customer's network. Customers also have the option to translate the mapped values with actual values on their network through Excel offline reports. Data privacy is applicable only for CSPC with Smart Net Total Care v1.6.

Cisco Data Center

After the information is securely packaged and encrypted, it is transported to the Cisco data center. The data is processed and analyzed against Cisco intellectual capital, which includes manufacturing, contract, technical support, and security data. The data is then made available to the customer through a secure web-based portal.

Smart Net Total Care Portal

Valuable information related to the collected Cisco devices is made available through the Smart Net Total Care portal in a secure portal, accessible only by CCO IDs with the appropriate entitlements. These reports highlight portions of the network that need attention.The next section discusses how the reports available in the secure web portal can assist in solving the following support challenges:

- Installed base management
- Contract management

- Proactive product alerts
- Network changes

Installed Base Management

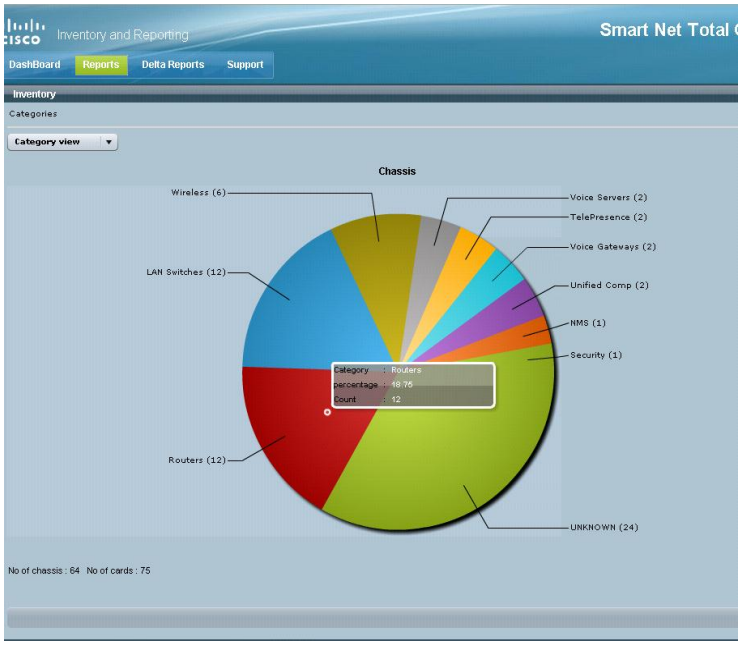
One of the largest challenges with network support is having current inventory information for all the devices that are installed within the network. Having an up-to-date list of network devices, and associated lifecycle data, code version, serial number, and related alerts is a daunting task for all network support professionals. Smart Net Total Care solves this problem by providing a detailed customizable inventory report as well as an Executive Summary report.

Inventory Reports

Inventory reports simplify the task of inventory management by providing a comprehensive list of the devices within the Cisco installed base, along with details for each of those devices.

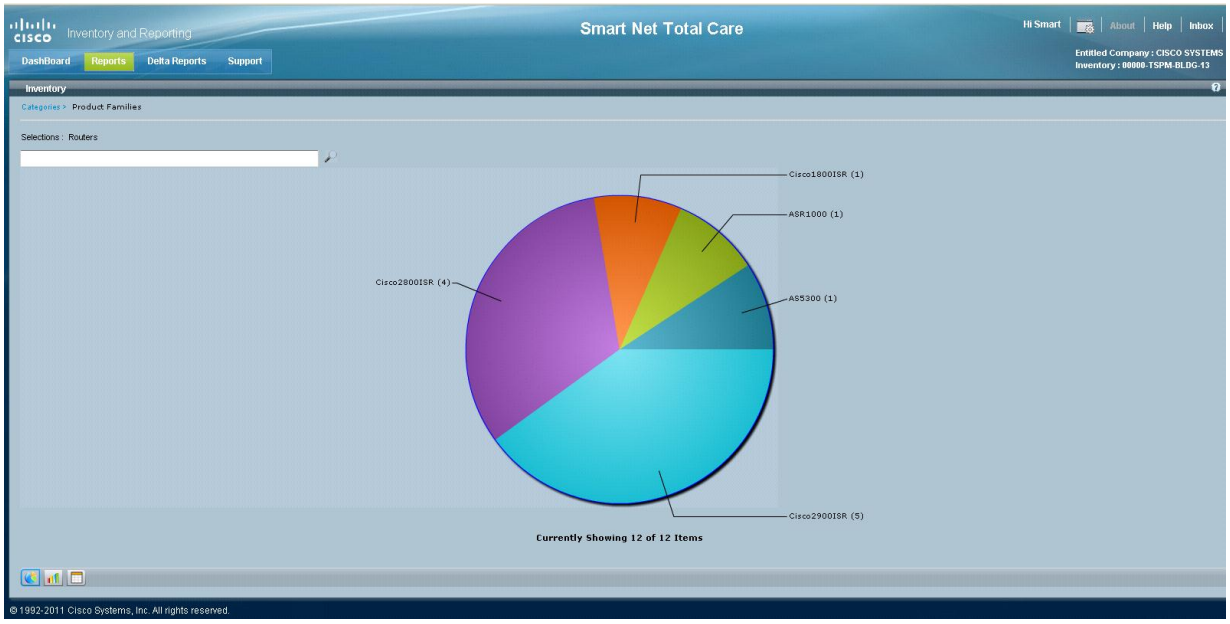
For example, a network administrator is planning to implement VOIP over IPV6. As part of the implementation, he needs to perform an IOS upgrade for all 2800 routers installed in the network. He'll need to know how many 2800 routers are installed within the network and what version of code are they running. He can access this information by logging in to the Smart Net Total Care portal and selecting the *Inventory* tab under the *Reports* tab. This displays an overall view of the devices installed within the network (Figure 3).

Figure 3. Inventory category view



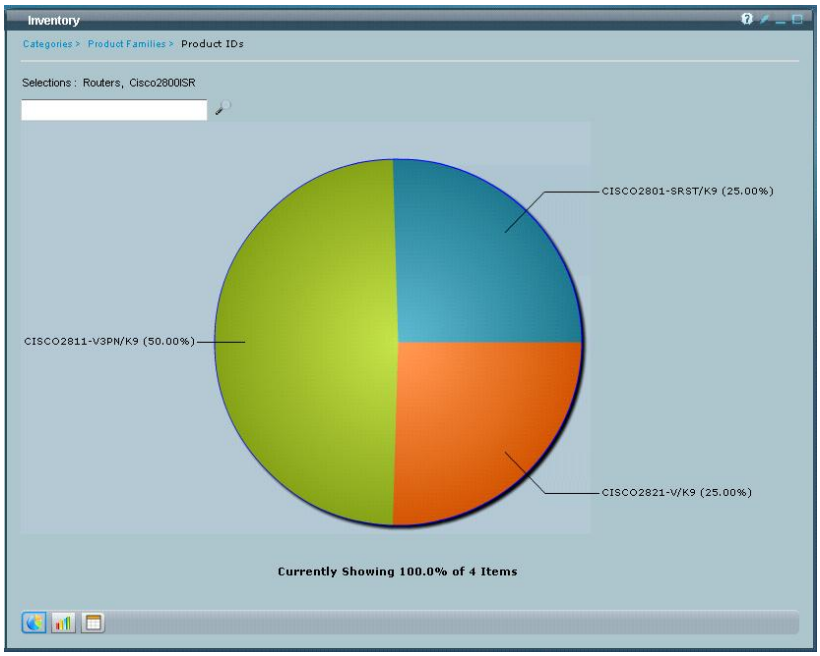
He can drill down into the specifics of a category by clicking directly in the chart. For example, clicking on the **Routers** segment of the pie chart displays the router types that are installed in the network (Figure 4).

Figure 4. Routers installed in the network



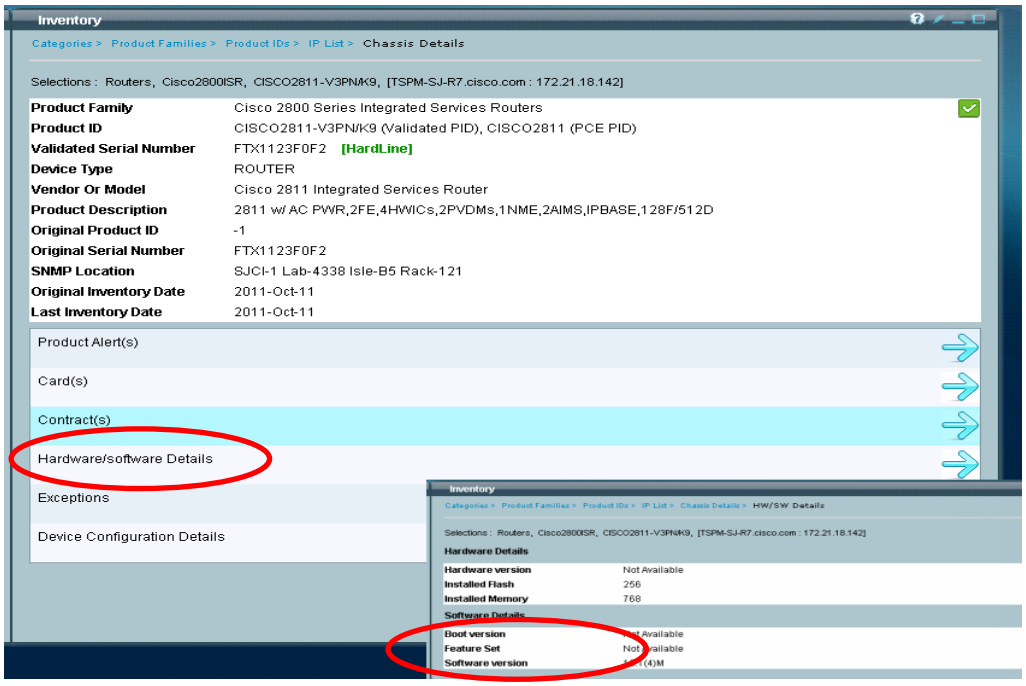
He can select the Cisco 2800 portion of the pie chart in Figure 4 to display the different model numbers of the Cisco 2800 series router. He can see that there are four Cisco 2800 series routers within the network and three model types (Figure 5).

Figure 5. Cisco 2800 series in the network



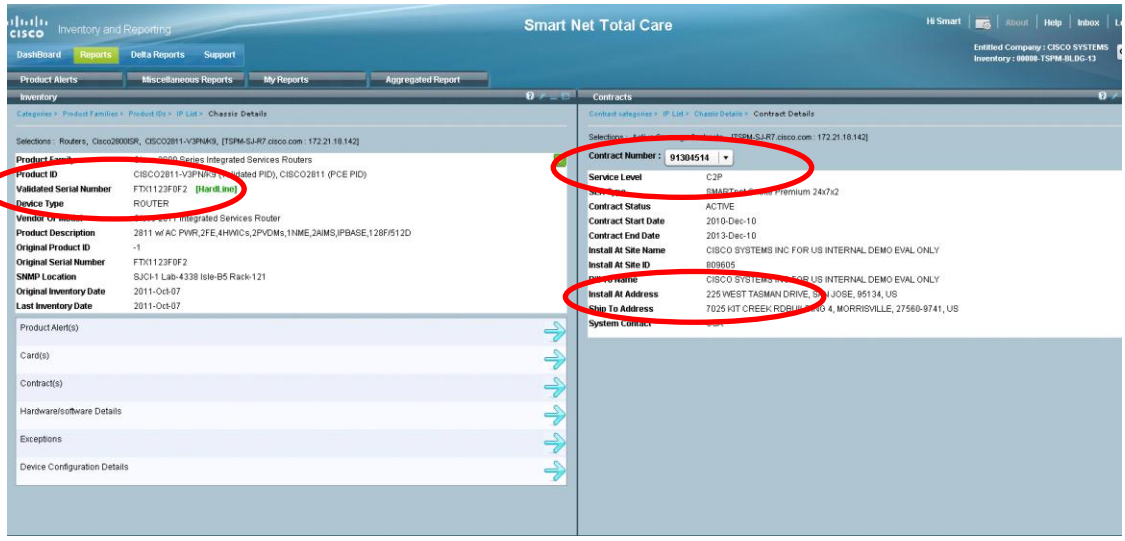
Choosing any portion of the pie chart displays the individual entries for each of the routers in the Cisco 2800 series, which allows him to access the detailed inventory information. By selecting **Hardware/Software Details**, he can see the version of code that the router is running (Figure 6).

Figure 6. Hardware/software details



During the upgrade, he notices a router hardware failure, so he has to replace the router via the Return Material Authorization (RMA) process. The validated serial number, contract information, and installed-at address provided by the *Chassis Details View* allow him to streamline the RMA process (Figure 7).

Figure 7. Chassis details view



Custom inventory reports are also available in Microsoft Excel or PDF format, and are stored on the portal for easy retrieval. In Figure 8, a custom report is created by selecting the **Export** button at the lower right of the screen and choosing **router** for *Device Type* field (Figure 9). Once generated, custom reports appear in *My Reports* where they are they are stored for up to three days.

Figure 8. Custom inventory report

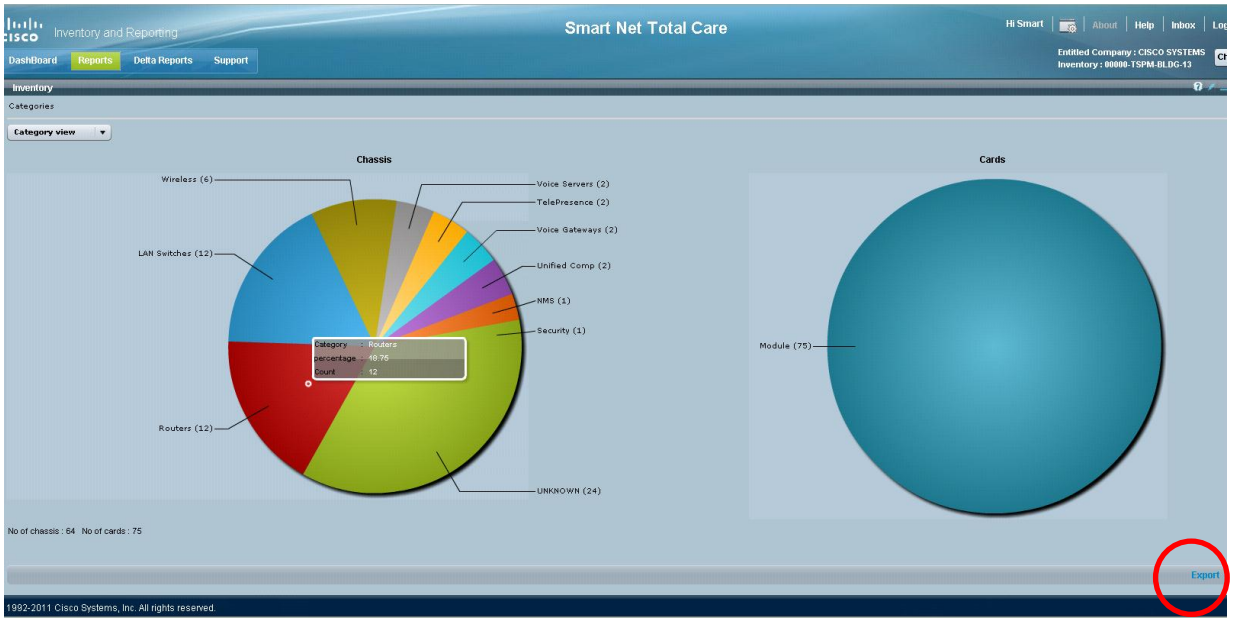
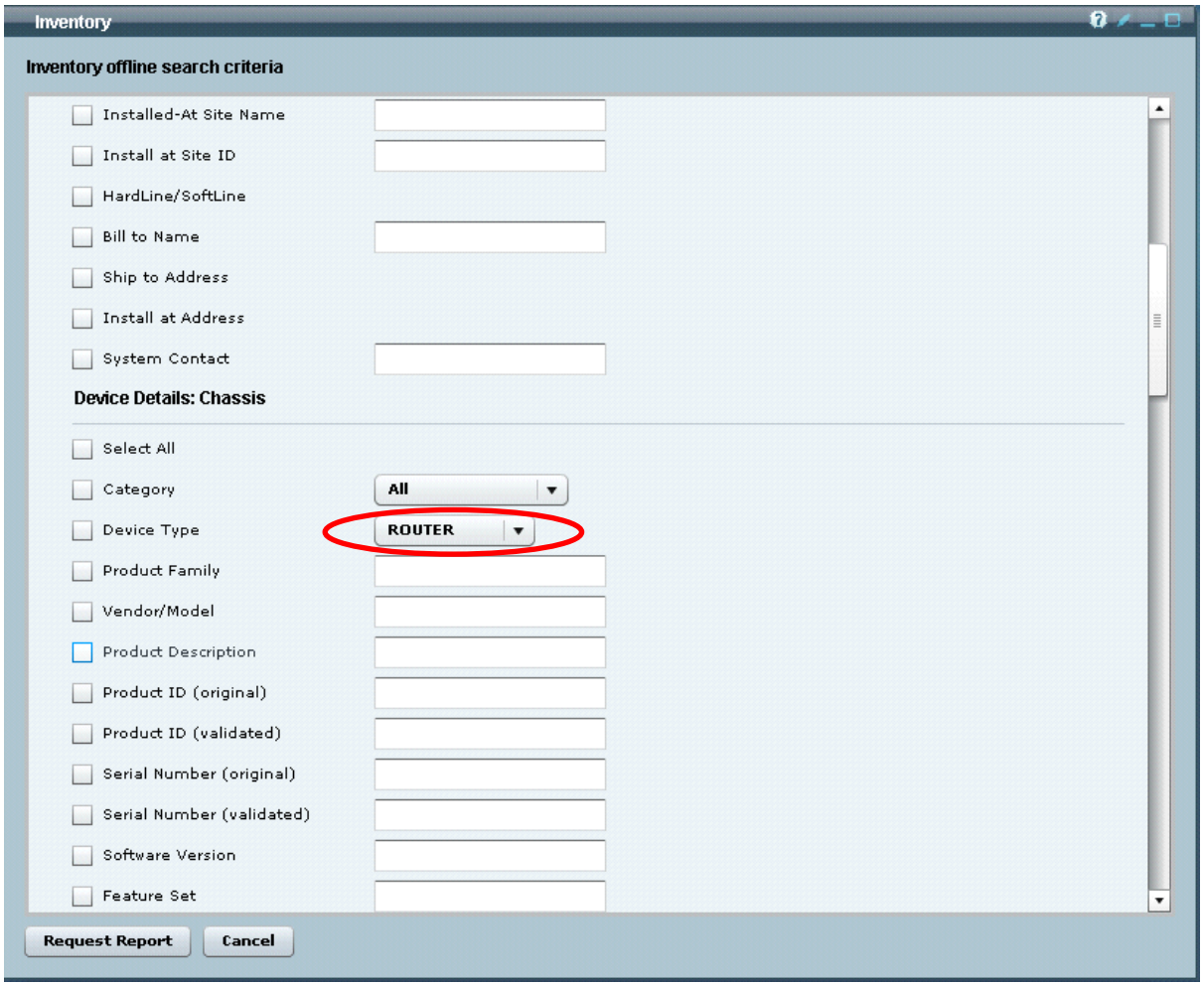


Figure 9. Custom inventory report filter criteria

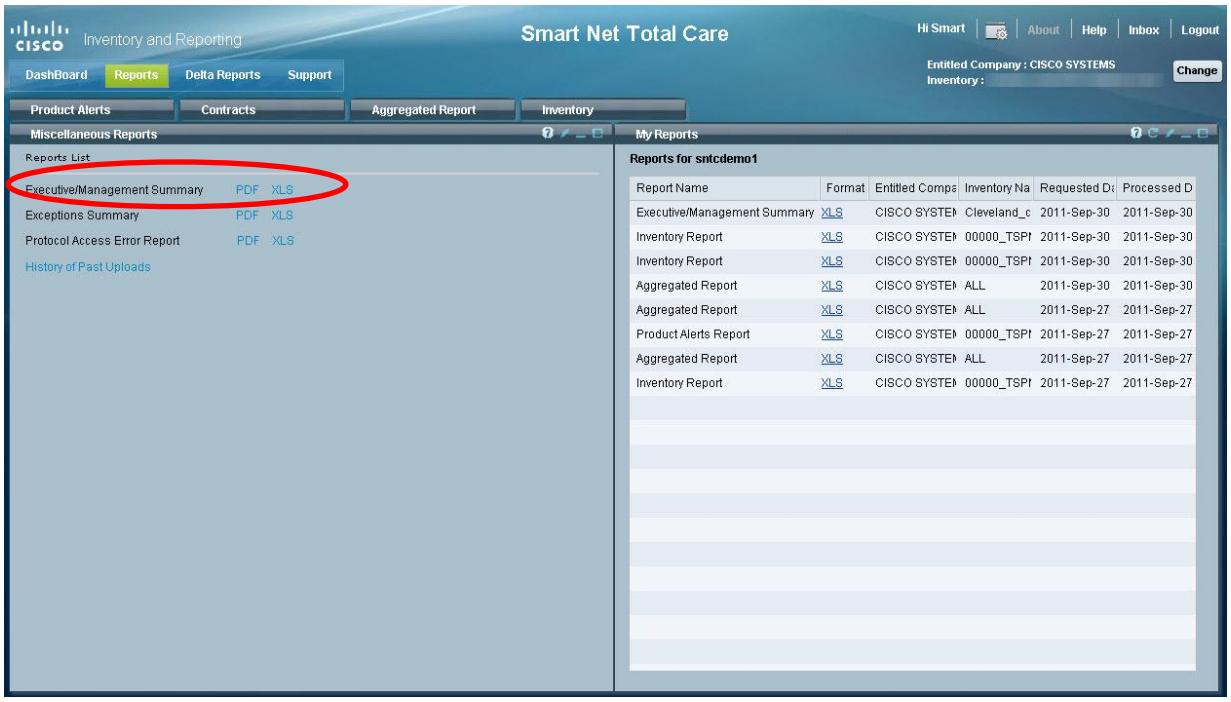


Executive Summary Reports

Executive Summary reports display both the number and types of devices installed in the network. This information can help you standardize the hardware and software versions on your network, reducing the overall combinations of configurations, thereby simplifying management and increasing device predictability.

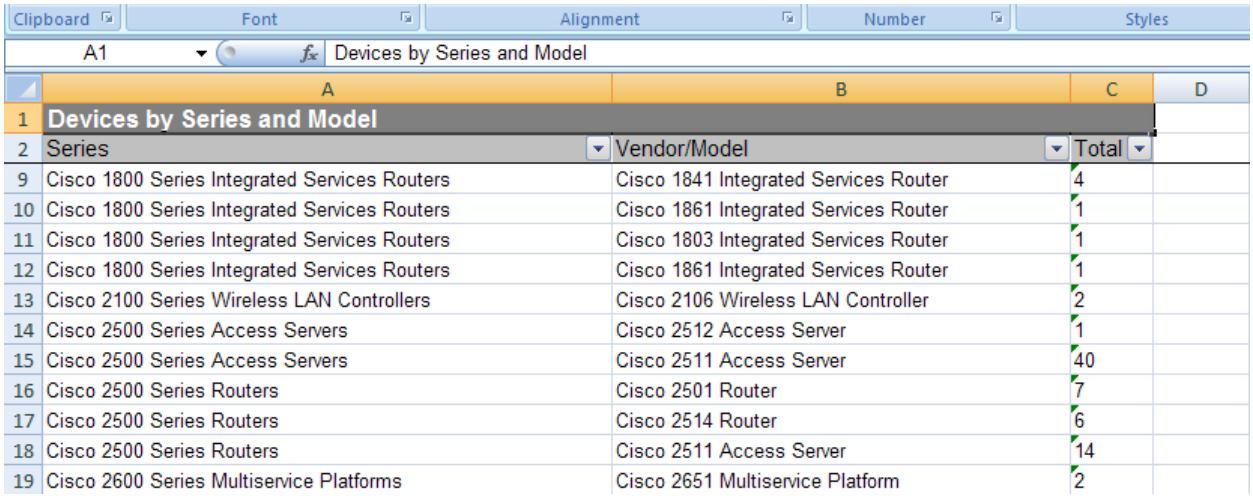
Consider an IT manager who is planning a hardware and software refresh. In preparation, he wants to determine the number and types of hardware and software versions discovered in the network. In this case, all he needs to do is to click the format link—PDF or XLS—to the right of the *Executive/Management Summary* (Figure 10).

Figure 10. Executive Summary reports



Clicking on the *Executive/Manager Summary* report under *My Reports* tab will download the report. The report lists the device type by series and model and the total number deployed within the network (Figure 11).

Figure 11. Device type by series and model



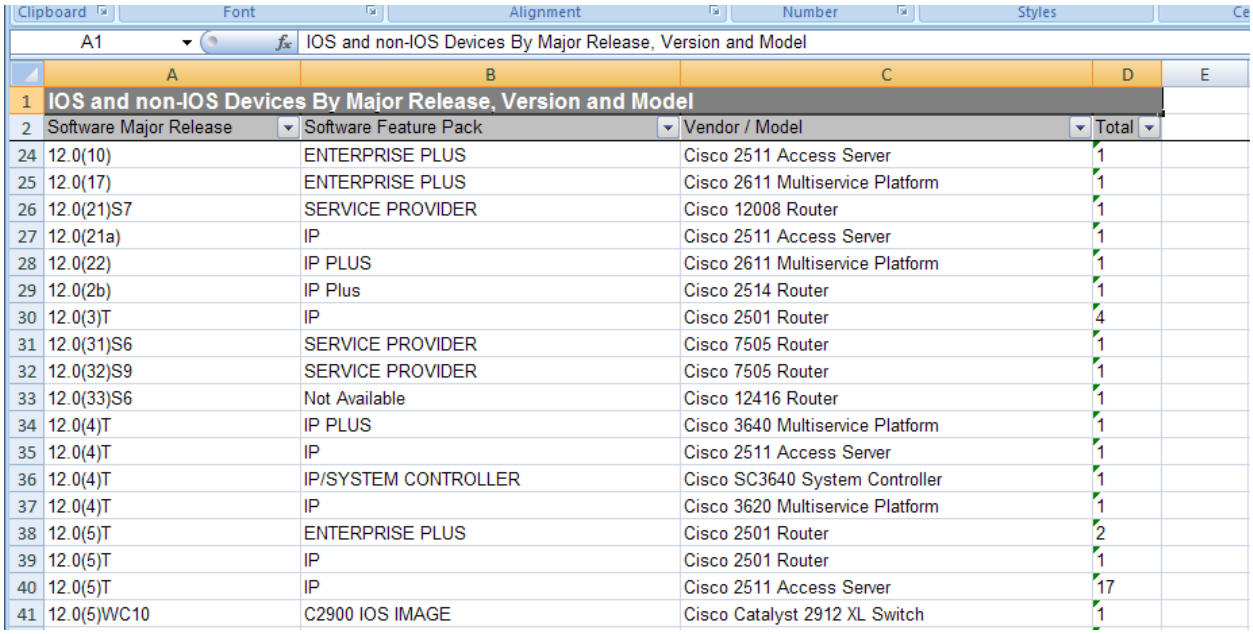
Clipboard | Font | Alignment | Number | Styles

A1 | Devices by Series and Model

	A	B	C	D
1	**Devices by Series and Model**			
2	Series	Vendor/Model	Total	
9	Cisco 1800 Series Integrated Services Routers	Cisco 1841 Integrated Services Router	4	
10	Cisco 1800 Series Integrated Services Routers	Cisco 1861 Integrated Services Router	1	
11	Cisco 1800 Series Integrated Services Routers	Cisco 1803 Integrated Services Router	1	
12	Cisco 1800 Series Integrated Services Routers	Cisco 1861 Integrated Services Router	1	
13	Cisco 2100 Series Wireless LAN Controllers	Cisco 2106 Wireless LAN Controller	2	
14	Cisco 2500 Series Access Servers	Cisco 2512 Access Server	1	
15	Cisco 2500 Series Access Servers	Cisco 2511 Access Server	40	
16	Cisco 2500 Series Routers	Cisco 2501 Router	7	
17	Cisco 2500 Series Routers	Cisco 2514 Router	6	
18	Cisco 2500 Series Routers	Cisco 2511 Access Server	14	
19	Cisco 2600 Series Multiservice Platforms	Cisco 2651 Multiservice Platform	2	

Included in the same spreadsheet output is a list of software versions and feature sets as well as the number of times the device was discovered within the network (Figure 12).

Figure 12. List detailing software versions and feature sets



Clipboard | Font | Alignment | Number | Styles

A1 | IOS and non-IOS Devices By Major Release, Version and Model

	A	B	C	D	E
1	IOS and non-IOS Devices By Major Release, Version and Model				
2	Software Major Release	Software Feature Pack	Vendor / Model	Total	
24	12.0(10)	ENTERPRISE PLUS	Cisco 2511 Access Server	1	
25	12.0(17)	ENTERPRISE PLUS	Cisco 2611 Multiservice Platform	1	
26	12.0(21)S7	SERVICE PROVIDER	Cisco 12008 Router	1	
27	12.0(21a)	IP	Cisco 2511 Access Server	1	
28	12.0(22)	IP PLUS	Cisco 2611 Multiservice Platform	1	
29	12.0(2b)	IP Plus	Cisco 2514 Router	1	
30	12.0(3)T	IP	Cisco 2501 Router	4	
31	12.0(31)S6	SERVICE PROVIDER	Cisco 7505 Router	1	
32	12.0(32)S9	SERVICE PROVIDER	Cisco 7505 Router	1	
33	12.0(33)S6	Not Available	Cisco 12416 Router	1	
34	12.0(4)T	IP PLUS	Cisco 3640 Multiservice Platform	1	
35	12.0(4)T	IP	Cisco 2511 Access Server	1	
36	12.0(4)T	IP/SYSTEM CONTROLLER	Cisco SC3640 System Controller	1	
37	12.0(4)T	IP	Cisco 3620 Multiservice Platform	1	
38	12.0(5)T	ENTERPRISE PLUS	Cisco 2501 Router	2	
39	12.0(5)T	IP	Cisco 2501 Router	1	
40	12.0(5)T	IP	Cisco 2511 Access Server	17	
41	12.0(5)WC10	C2900 IOS IMAGE	Cisco Catalyst 2912 XL Switch	1	

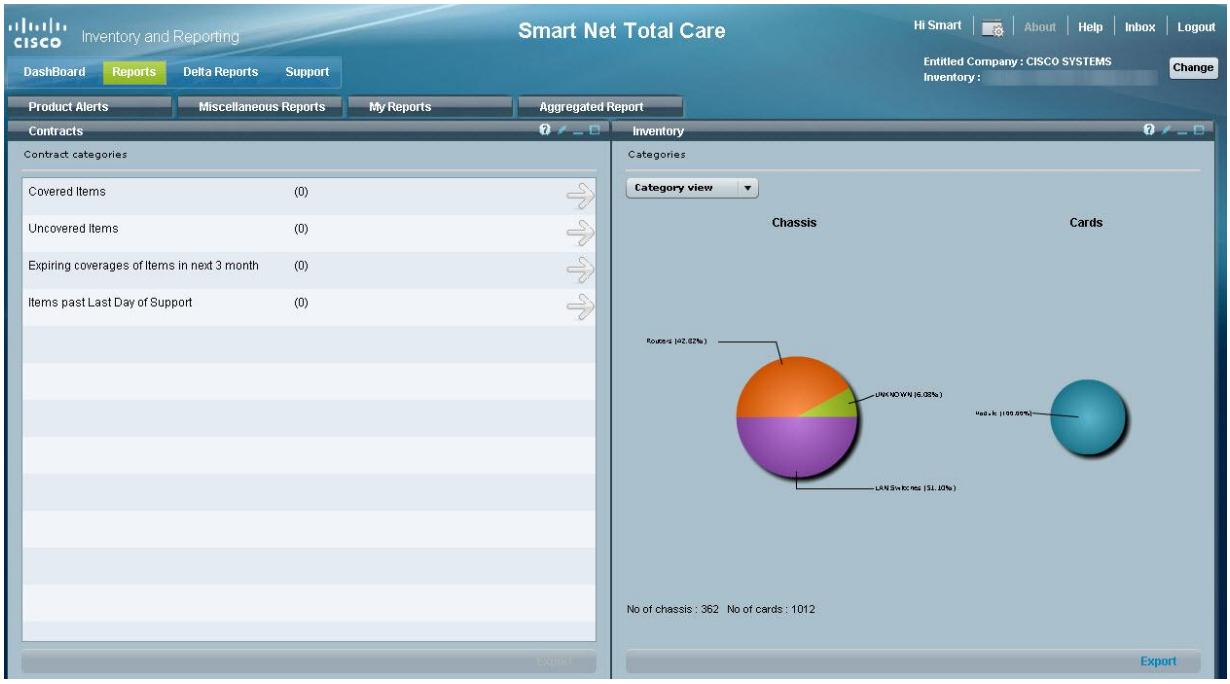
Contract Management

A clear understanding of current service coverage on critical systems and devices helps you minimize risk and quickly resolve issues. Several reports offered through Smart Net Total Care help determine whether critical Cisco products are covered with the right service agreements and where those devices are in their product and contract life cycle. This information is found in the Contracts report and the Aggregated report.

Contracts Report

The Contracts report shows what Cisco products are covered under which contract service level, helping ensure that the proper coverage is in place (Figure 13).

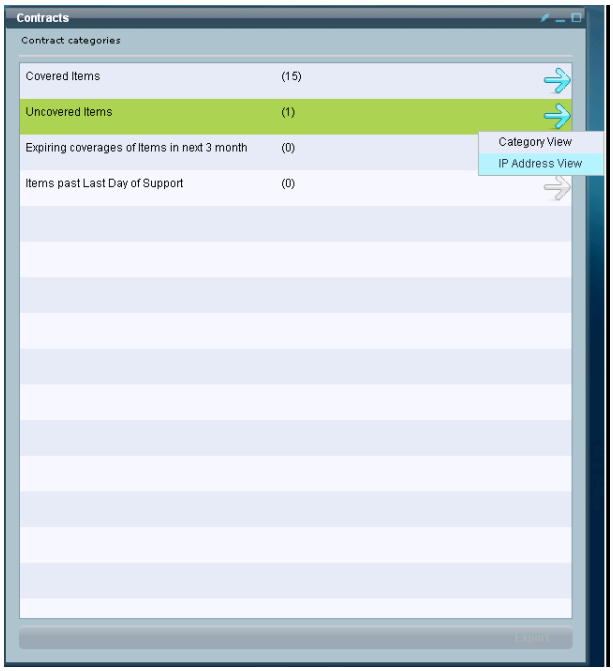
Figure 13. Contracts report



Cisco products without proper service coverage can reduce service availability. For example, a CIO recently experienced downtime in the company data center, and one of the contributing factors was lack of contract coverage for a Cisco Nexus switch. To reduce risk factors such as these, the CIO wants to know what devices in the network are near the end of their contract coverage, or not covered at all.

To view a list of devices that are not covered by a contract, he can click the **arrow icon** for *Uncovered Items* in the *Contract Categories* list (Figure 14).

Figure 14. Uncovered items



Clicking the **blue arrow** next to the device provides information on any device that is not covered by a contract (Figures 15 and 16).

Figure 15. Uncovered devices

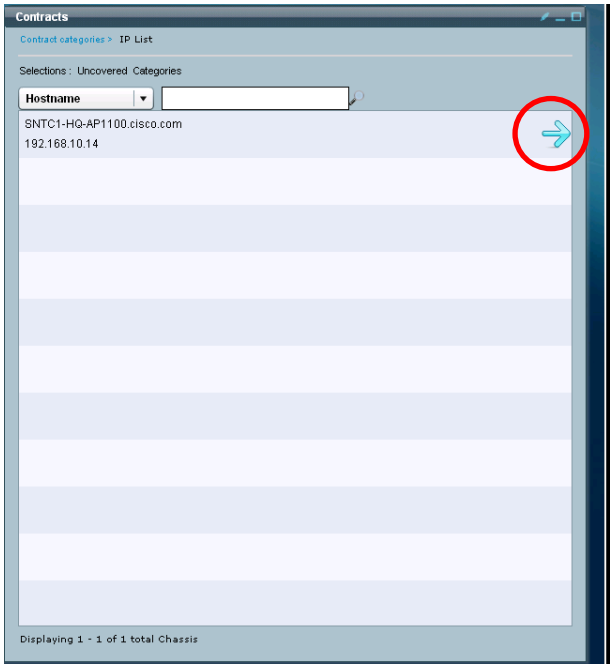
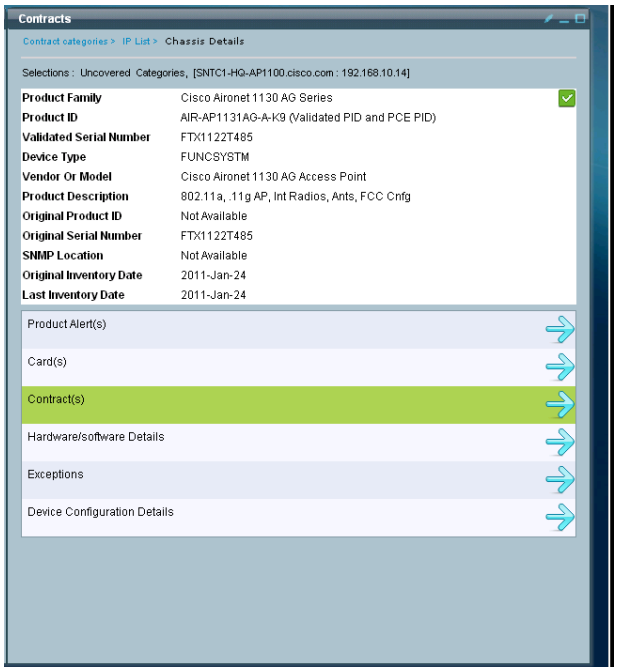
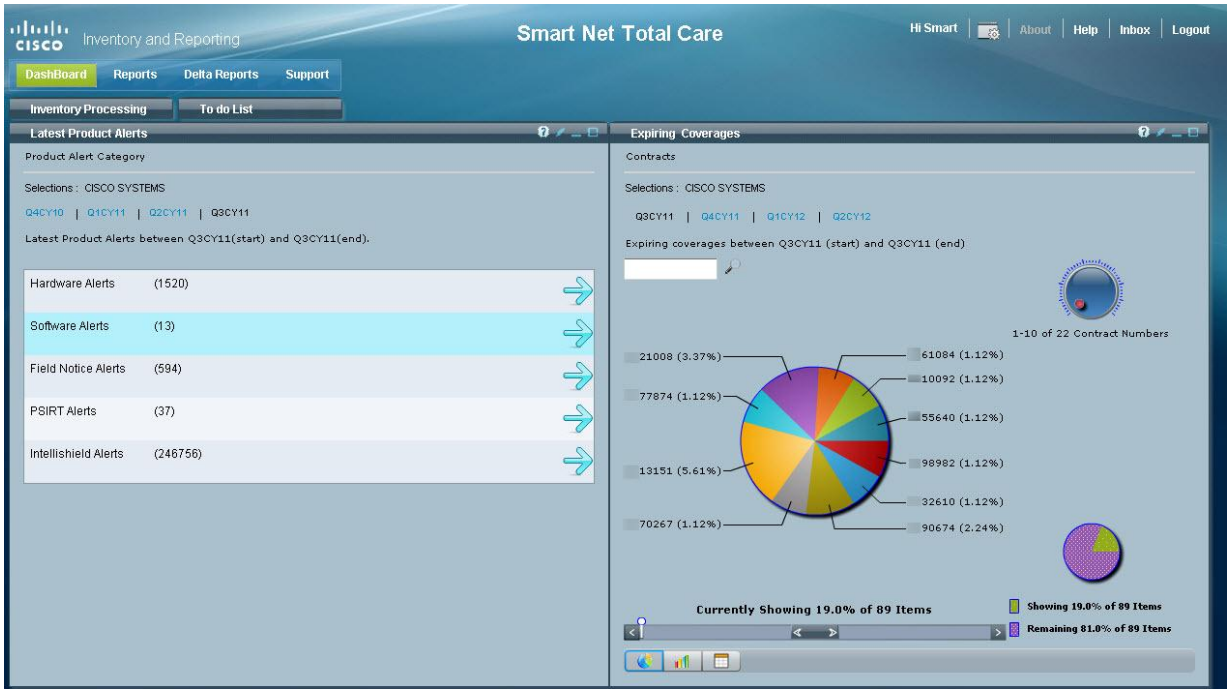


Figure 16. Uncovered device details



To view the list contracts nearing end of coverage, he can choose the *Expiring Coverages* tab from the portal dashboard. This shows which contracts will expire in the next 12 months. They are grouped by quarter, which helps him budget for upcoming support contract renewals (Figure 17).

Figure 17. Expiring Coverages report



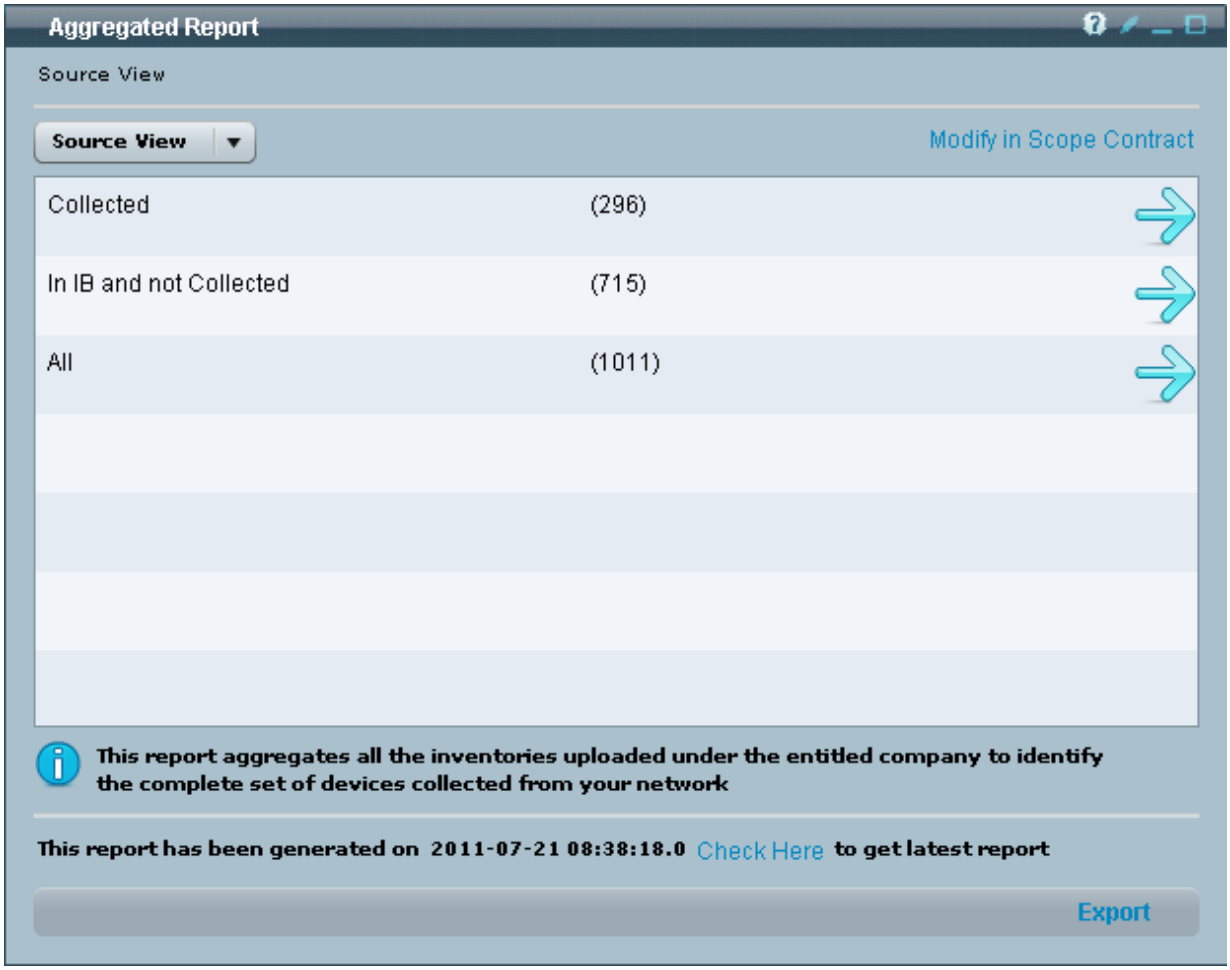
Clicking on a contract number (or pie segment) displays the devices under that contract that are about to expire. Additional information about each device is available using the arrows to the right.

Aggregated Report

Although the Contracts report lists the devices that are found in a collection, users can gain a more comprehensive view of their installed base when service contract information is included. Using information from the customer's service contract can help manage devices regardless of whether the device was actually included in the collection. The Aggregated report provides a comprehensive list of the customer's collected installed base and associated contracts. This "collected contract" view will include all devices on a contract as long as at least one device from that contract is found in a collection. This means that not every device on contract has to be collected for it to display as part of the report.

For example, a network administrator wants to view all items in a particular contract, including some switches that are offline. Selecting the *Aggregated* report tab under the *Report* tab displays the *Source View*, which allows the user to browse through both collected and uncollected device details. By choosing the option *In IB and Not Collected*, he can display details of all the devices that are in Cisco's databases and on one of the in-scope contracts, but not collected by collector (Figure 18). He can apply filter to view all items on a particular contract.

Figure 18. Aggregated report source view



Note: In situations where a contract has multiple end-users (MEUs), such as when the entitled resale partner keeps devices from many individual companies on a single Cisco contract, Smart Net Total Care will maintain customer confidentiality by withholding that data. If a collection results in finding contracts with MEUs, the Aggregated report will not include additional devices from such contracts. Customers who wish to see their devices that happen to be on these shared contracts should contact their Cisco Services resale partner to have the situation rectified.

Proactive Product Alerts

Network managers often deal with the challenge of having little to no visibility of the alerts that can affect the management of their network operation. In addition, they may find that they have no way to see into the potential vulnerabilities of their network equipment.

Product Alerts Report

The Smart Net Total Care portal can proactively inform users of alerts that affect management of their network operation. Not only do these alerts deliver relevant hardware, software, and security information, but the customer is able to see which alerts apply to their Cisco devices.

Customers can see alerts for

- Hardware End of Life milestones
- Software End of Life milestones
- PSIRTs
- IntelliShield
- Hardware and software field notices

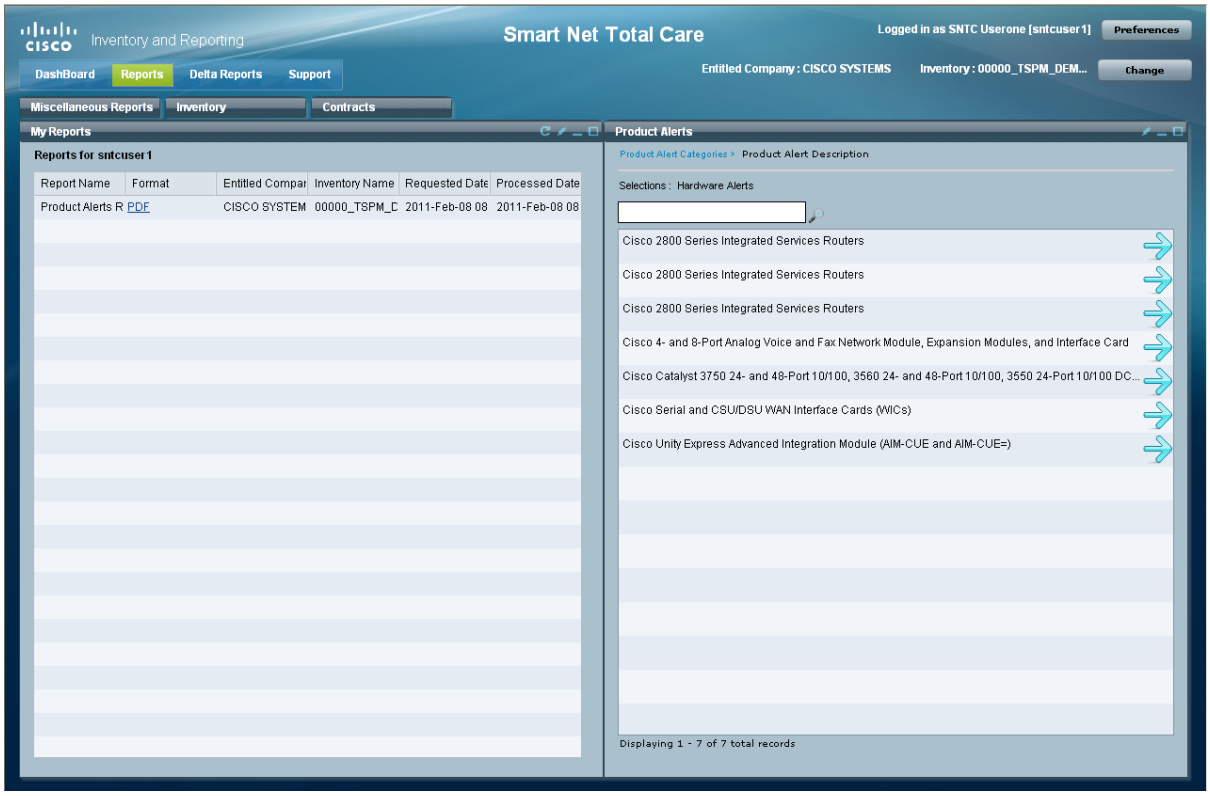
For each device that is affected by an alert, the Smart Net Total Care portal also provides a link to the product bulletin on Cisco.com, which includes additional details about the alert.

The following scenario can help illustate how the Product Alerts report can help mitigate risks. For annual budgeting and operational planning, an IT manager wants to know which Cisco products are End of Life and may need to be upgraded or replaced. He selects the *Products Alerts* tab under the *Reports* tab. This displays an overall view of the product alerts applied to their network (Figure 19)

Figure 19. Product Alerts View

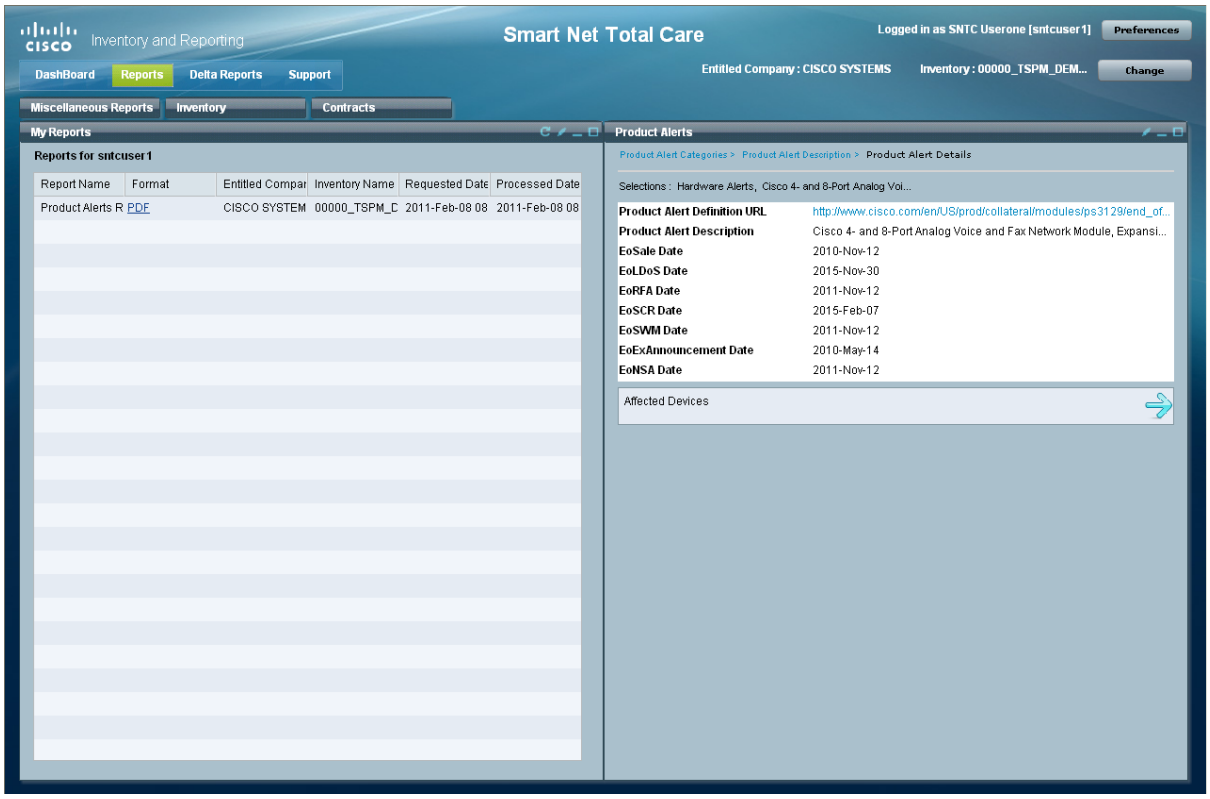
By choosing hardware alerts, he can view a list of the specific hardware alerts that were found during the backend processing of the information gathered from the network (Figure 20).

Figure 20. Hardware alerts



Choosing a specific alert lists the affected devices as well as specific information pertaining to that alert (Figure 21).

Figure 21. Specific alert details



By choosing *Affected Devices*, he can pinpoint the device and card that are affected (Figures 22 and 23).

Figure 22. Correlating alerts with device

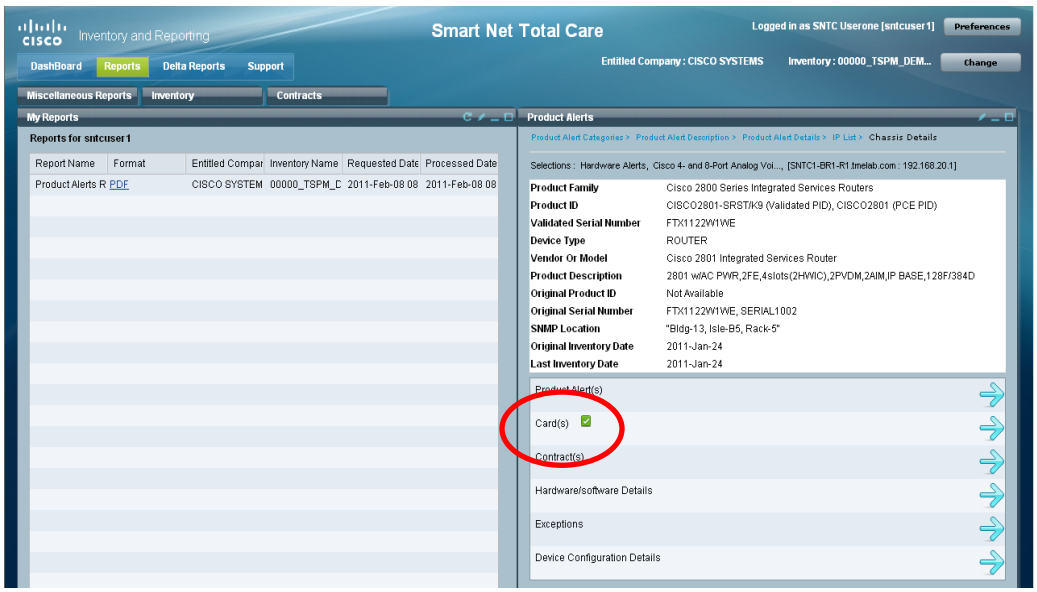
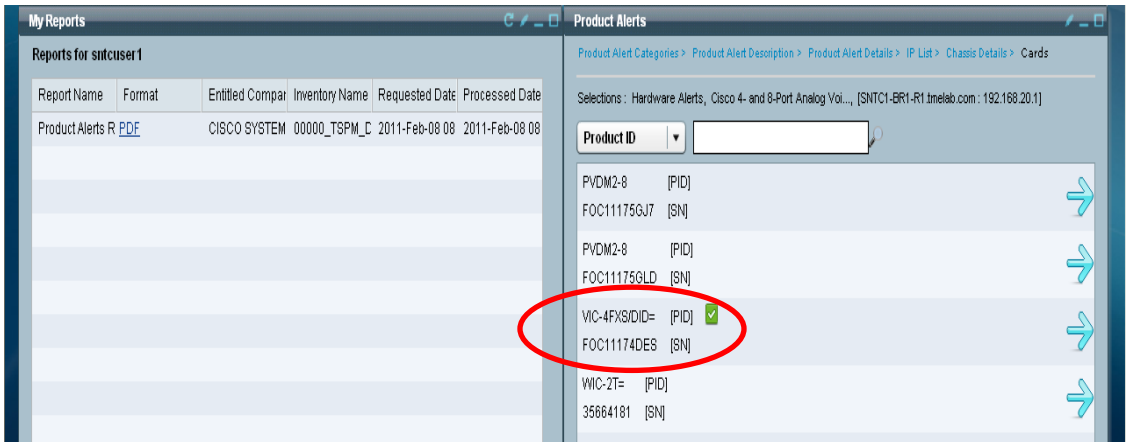
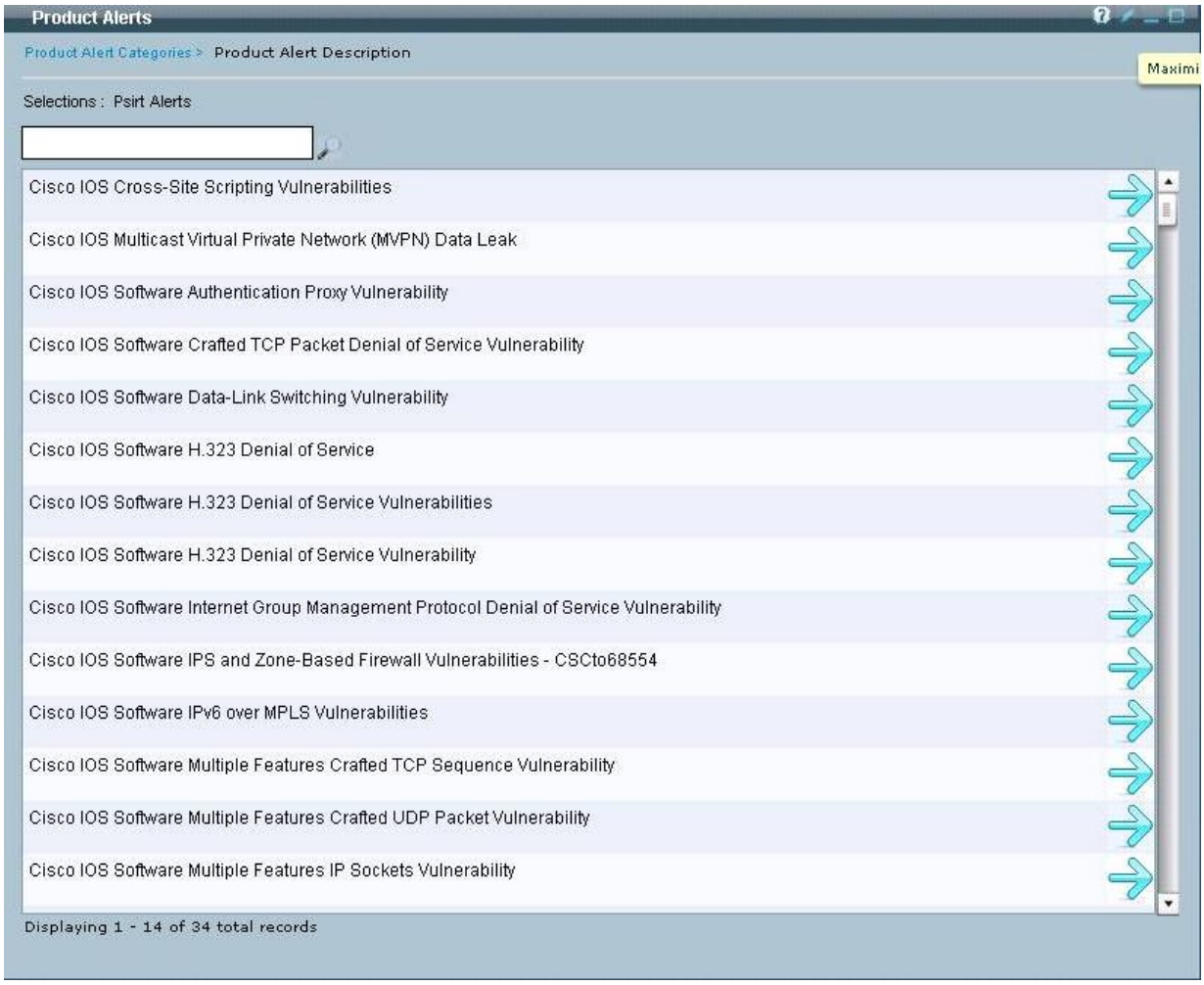


Figure 23. Correlating devices with card



With the importance of today's converged networks, security is paramount. Identifying the vulnerabilities in network equipment is essential to providing a secure environment. Once information is gathered from network devices, Smart Net Total Care will search for all devices that have active PSIRT vulnerabilities. This information is then made available to the customer through a report on the secure portal. This report identifies the affected device and the open vulnerability for that device (Figure 24).

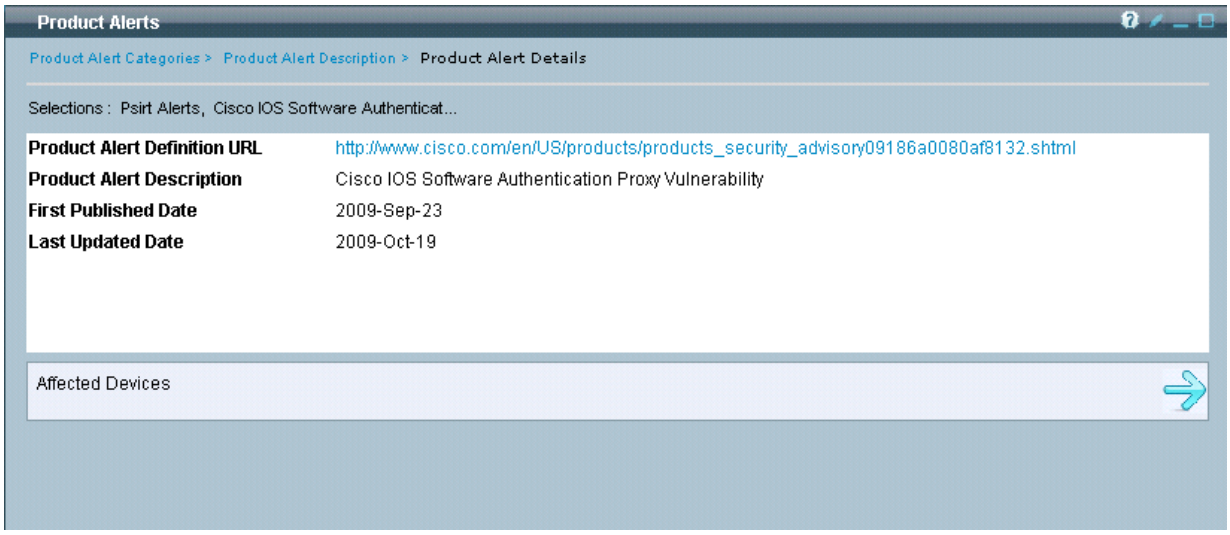
Figure 24. Devices with PSIRT vulnerabilities



Although all security vulnerability information is available through Cisco.com, Smart Net Total Care simplifies the process of locating this information and providing a comprehensive report of security exposures within the network. The time saved by automating this process allows network support staff to focus on correcting these vulnerabilities, thus securing the network.

Choosing a particular PSIRT allows the support staff to determine which devices are susceptible to that vulnerability, as well as the URL for the alert definition (Figure 25).

Figure 25. PSIRT details



Managing Network Changes

It can be difficult to manage changes to the installed base in large and complex networks. The Delta report identifies which Cisco products have been moved, added, or changed in your collected Cisco installed base over a period of time.

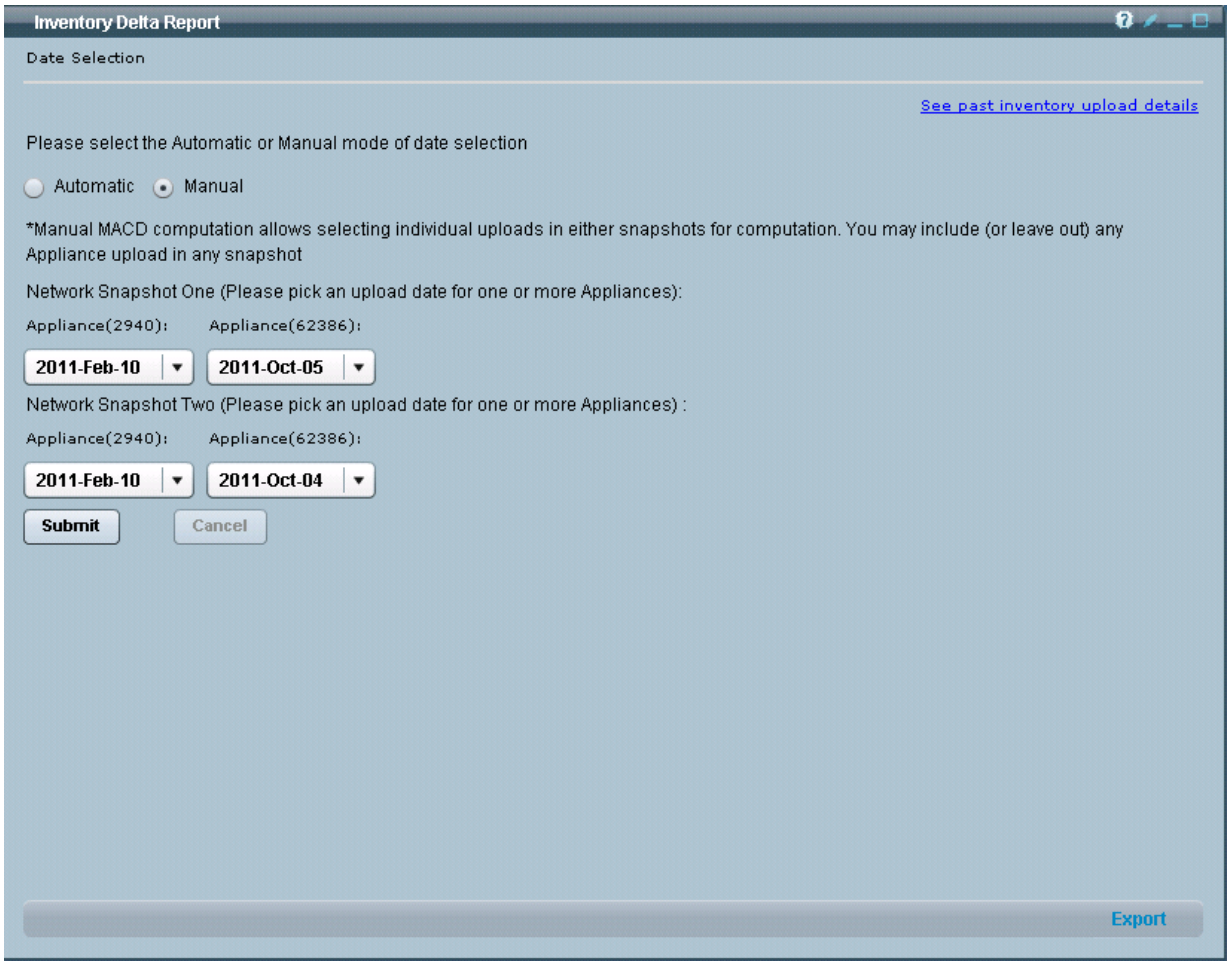
Delta Report

Every collection of network inventory gives you the ability to determine how many devices have been added, modified,or removed since the previous collection. This simplifies contract and installed base management. Product Alert Delta reports are also available to show alerts published over a period of time, helping further mitigate risk.

Consider a company undergoing a data center reconsolidation. The network administrator wants to ensure the devices added to the network have proper coverage. At the same time, in the interest of cost reduction, he wants to make sure any device no longer in the network has been removed. The inventory Delta report is used to determine the changes in the collected Cisco installed base between the two selected dates

In Figure 26, dates were selected for both Cisco collectors to show the overall network changes.

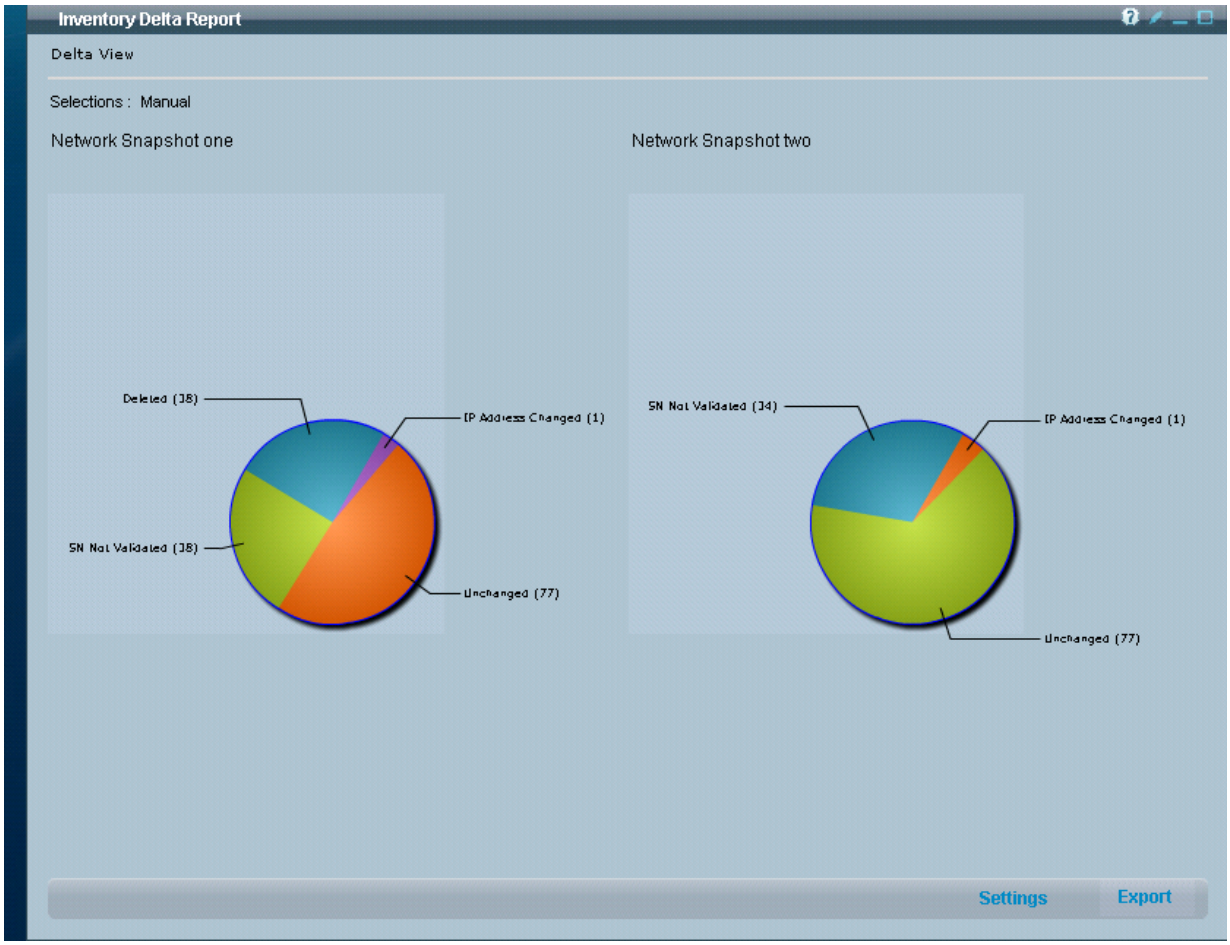
Figure 26. Delta reports



The Network Snapshot View (Figure 27) shows that 38 devices were removed between the two dates selected. This report not only lists the devices that were added to or removed from the network, but also the individual cards that may have been removed or replaced. For instance, if a chassis has a failed card that is replaced, it will appear on the Delta report as a deleted card, and the new one will appear as added. If cards are removed , this report will list those cards as deleted.

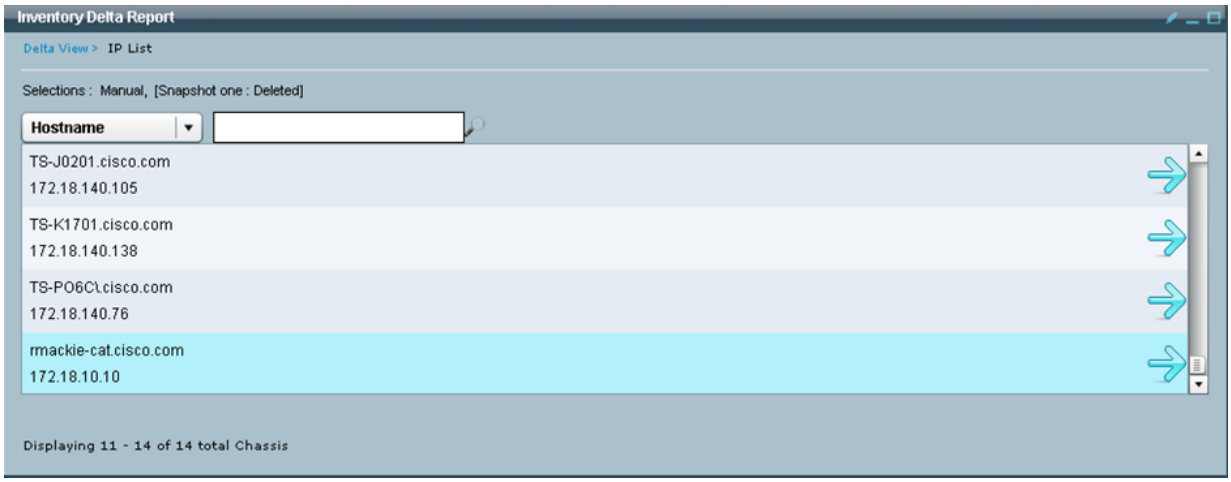
Choosing the *Deleted* section in Figure 27 shows these deleted cards (Figure 27).

Figure 27. Network Snapshot view



By choosing a specific chassis in Figure 28, in this case *rmackie-cat.cisco.com*, you can see that there has been a change in the card(s) section of the Chassis Details (Figure 28).

Figure 28. Deleted cards as represented in Delta reports



You can access further information by choosing the arrow at the right of the card(s) section in Figure 29. This displays specific information about that card (Figure 30).

Figure 29. Card(s) section change in Chassis Details

Figure 30. Specific information about deleted cards

Conclusion

Today, the network is a strategic platform in a world that delivers the demands better integration between people, information, and ideas. Technical service information and capabilities, aligned with your business goals, help you maximize business continuity. Smart Net Total Care provides these capabilities with faster problem resolution, which reduces operating expenses and improves risk management. With Smart Net Total Care, you benefit from

- **Improved risk management** through up-to-date visibility of Cisco device contracts, and life cycle management on the installed base to identify Cisco products that are end-of-life (EoL) or end-of-support (EoS).
- **Faster problem resolution** through quicker diagnosis and remediation. Once an issue has been identified, Smart Net Total Care provides comprehensive, best-in-class service processes and resources, and helps ensure that up-to-date information is in place to minimize downtime.
- **Reduced operating expenses** with comprehensive, flexible reporting and contract consolidation, helping you to manage large and complex networks, streamline renewals, and enable you to more easily manage your Cisco devices and associated service contracts. Less downtime and fewer administrative resource requirements means lower operating expenses.

For More Information

To learn more about Smart Net Total Care Service, visit http://www.cisco.com/go/total or contact your local account representative.

Cisco.com Technical Support Resources for Users of Smart Net Total Care

The Cisco website offers a full range of online resources to help you use Smart Net Total Care. Please be sure to visit the award-winning support website and support community.

Visit the Cisco Support Website for Smart Net Total Care Technical Resources

The Cisco Support Website is your comprehensive base of technical knowledge and tools to help you design, operate and troubleshoot your Smart Net Total Care products and technologies. The website offers robust features that enable you to:

Find technical content

Explore the library of 90,000+ documents and use troubleshooting tools to help diagnose and resolve technical issues quickly

Personalize your support

Customize the My Cisco web portal to be your central hub for viewing modular information on your products, notifications, Service Requests, and more

Download software

Find your software and the related product information from one location; save time by storing your software choices in the download cart

Use the Cisco Support Community for Technical Questions on Smart Net Total Care

Join the Cisco Support Community to learn more about Smart Net Total Care by interacting with networking peers and experts worldwide. The community offers a variety of resources that help you:

Connect with peers

Ask questions, get answers and share insights in the discussion forums (such as the Network Infrastructure forum)

Learn from Cisco experts

Learn about specific networking topics via online Ask the Expert discussions, interactive webinars and archived sessions; or explore expert blogs and videos

Share knowledge

Collaborate with peers to post wiki content, and share documents through social media outlets like Facebook or Twitter

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA 04/13