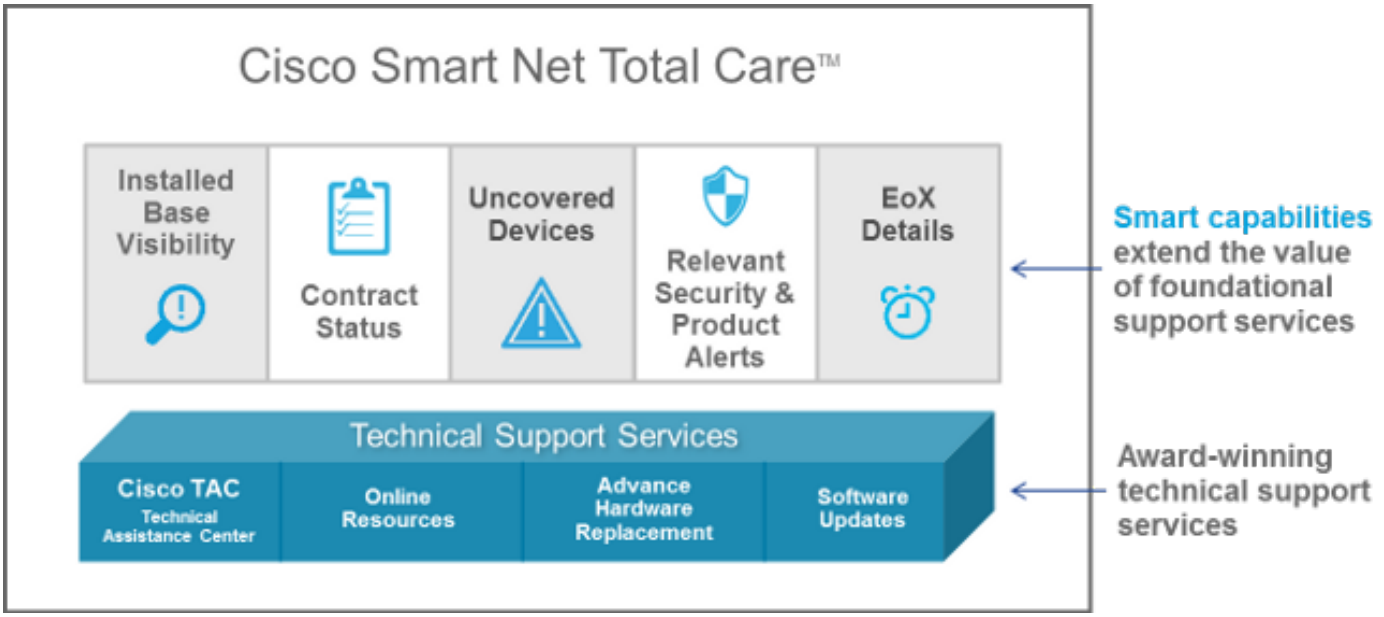
Benutzerhandbuch zum Smart Net Total Care Portal

Der Cisco Smart Net Total Care™-Service ist Teil des technischen Services-Portfolios von Cisco. Dieser Service kombiniert branchenführende und preisgekrönte grundlegende technische Services von Cisco mit einer zusätzlichen, umsetzbaren Business Intelligence, die Ihnen über die intelligenten Funktionen im Smart Net Total Care-Portal zur Verfügung gestellt wird.

Über das webbasierte Portal und die zugehörigen Berichte erhalten Sie alle Informationen, die Sie für die Verwaltung Ihres Cisco Inventars benötigen. Die integrierten intelligenten Funktionen bieten aktuelle Informationen zu vorhandenen Installationen, Verträgen und Sicherheitswarnungen, um die Effizienz Ihrer Support-Workflows zu steigern. Das Portal bietet:

- **Schnellere Problembehebung** - Erkennen Sie Probleme schnell und optimieren Sie Ihre Incident-Management-Prozesse, um die Servicelevel der IT zu verbessern und Probleme schneller zu lösen. Intelligente Funktionen, darunter proaktive Warnmeldungen, automatisierte Diagnosen, aktuelle Daten zur Vertragsabdeckung und Produktinformationen, tragen zur Minimierung von Ausfallzeiten bei und fördern die Geschäftskontinuität.
- **Risikominimierung** - Reduzieren Sie Risiken durch den Zugang zu technischen Experten von Cisco (Cisco Technical Assistance Center) und intelligenten Tools, die den Überblick über den Zustand Ihrer IT-Infrastruktur rund um die Uhr (365 Tage im Jahr) verbessern. Durch die Transparenz der vorhandenen Installationen im Portal wird sichergestellt, dass Ihre wichtigen Cisco Produkte durch die entsprechenden Serviceverträge abgedeckt sind. Das Portal erleichtert zudem die proaktive Planung und Budgetierung von Aktualisierungen für Cisco Produkte, deren End-of-Life (EoL)- oder Last Date of Support (LDoS)-Status erwartet wird.
- **Betriebseffizienz** - Steigern Sie Ihre Betriebseffizienz durch proaktive Management-Tools und automatisierte Prozesse, die die Produktivität von Netzwerkadministratoren und -managern steigern. Das automatisierte Bestands- und Vertragsmanagement hebt Änderungen hervor und ermöglicht Budget- und Planungsvorausschau, um den Aufwand zu minimieren, der für die Aufrechterhaltung einer aktuellen Netzwerkübersicht erforderlich ist.



Dieses Benutzerhandbuch enthält Informationen, die Sie verwenden können, um:

- Beginnen Sie mit dem Portal.
- Einrichtung und Anpassung des Portals
- Erstellen und Verwenden von Berichten mit der Portalbibliothek

Erste Schritte

Das Smart Net Total Care-Portal verwendet Geräteinformationen und analysiert diese mit Sicherheits- und Support-Daten aus der Cisco Knowledge Base. So erhalten Sie aussagekräftige Informationen, mit denen Sie Probleme schneller beheben, die Betriebseffizienz steigern und Support-Risiken besser kontrollieren können.

In diesem Abschnitt erhalten Sie Informationen zu den verschiedenen Portalrollen und Zugriffsebenen sowie zum Self-Service-Onboarding-Prozess. Außerdem erhalten Sie einen Überblick über das Portal und seine Komponenten:

- Anmeldung bei Smart Net Total Care
- Rollen und Zugriff
- Self-Service-Onboarding
- Erstellung des anfänglichen Bestands
- Grundlegende Portalnavigation

Anmeldung bei Smart Net Total Care

Sie können Smart Net Total Care über Ihren Webbrowser unter https://services.cisco.com starten.

> **Hinweis**: Verwechseln Sie nicht die auf dem Bildschirm angezeigte Cisco Services Connection-Bezeichnung. Wenn Sie den Namen Cisco Service Connection oben im linken Navigationsbereich sehen, wird das Smart Net Total Care-Portal angezeigt.

Rollen und Zugriff

Informationen zu Rollen und Zugriffsebenen finden Sie im Abschnitt *"Portalrollen und Zugriff"* auf der Cisco Smart Net Total Care Portal Administration and Management-Seite.

Self-Service-Onboarding

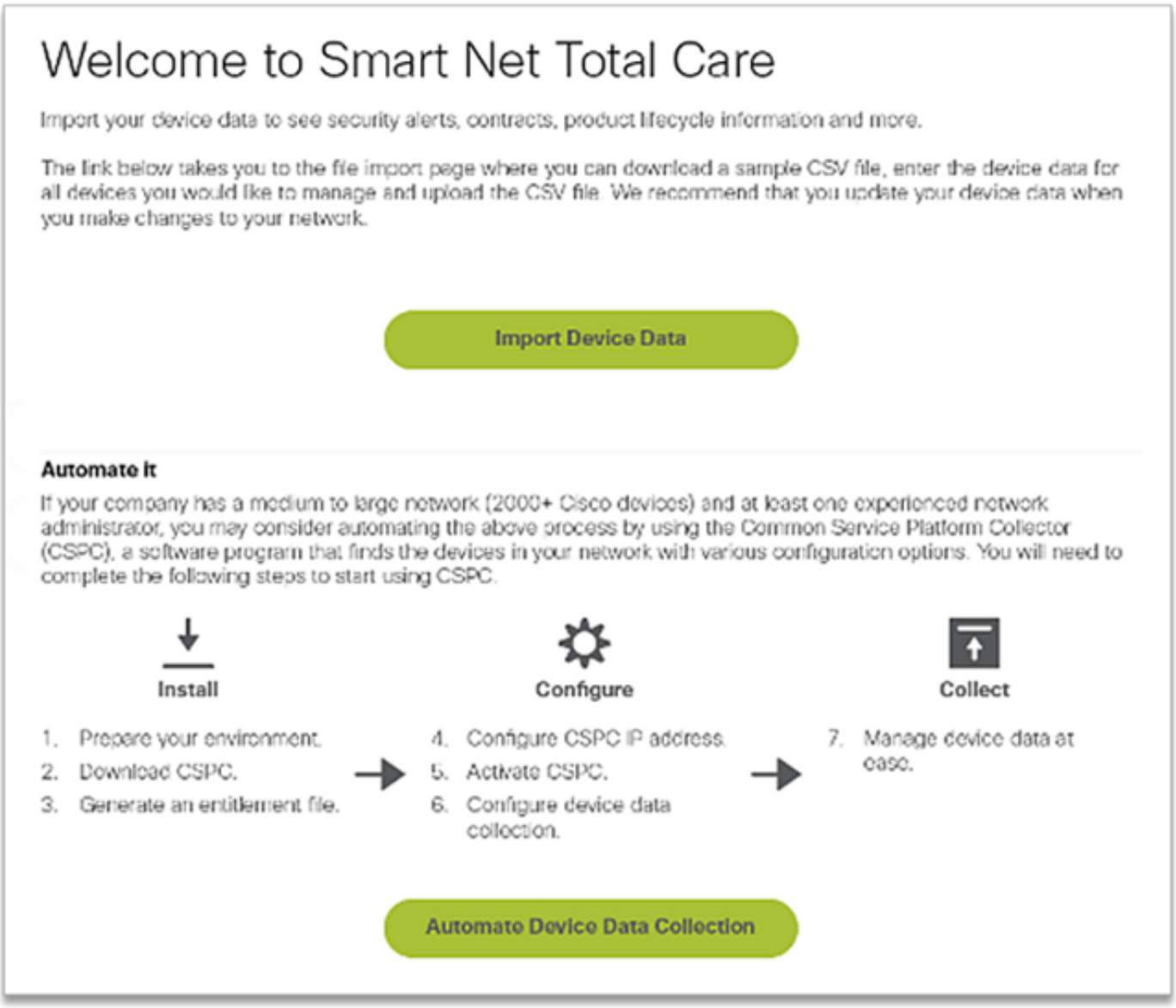
Weitere Informationen zum Self-Service-Onboarding-Prozess finden Sie im Cisco Smart Net Total Care Portal Onboarding Guide.

Erstellung des anfänglichen Bestands

Ein *Bestand* besteht aus einer Reihe von Geräten, die über eine oder alle unterstützten Methoden in das Smart Net Total Care-System hochgeladen werden. Sie können diese Methoden verwenden, um Informationen zu vorhandenen Cisco Installationen in das Portal hochzuladen:

- Cisco Common Service Platform Collector (CSPC)
- Collector eines Drittanbieters
- CSV-Dateiimport (Comma-Separated Value)

Wenn Sie ein neuer Kundenadministrator sind und kein Inventar erstellt wurde, werden Sie nach dem Anmelden zur *Startseite* weitergeleitet. Diese Seite enthält schrittweise Anleitungen, die Sie beim Importieren Ihres Bestands durch einen CSV-Dateiimport oder bei der automatisierten Erfassung von Geräten durch einen Collector unterstützen.



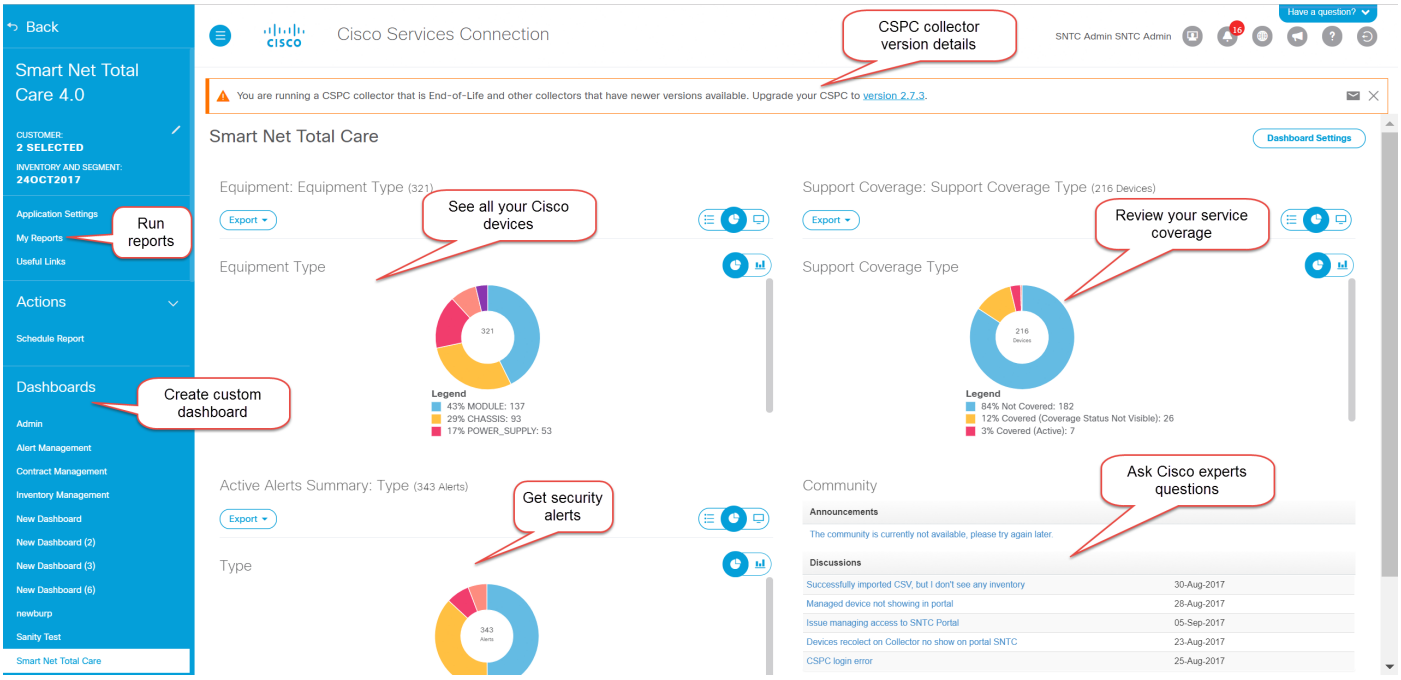
Wenn Sie ein neuer Benutzer sind und bei der Anmeldung eine Meldung *No Records Found* (Keine Datensätze gefunden) angezeigt wird, wenden Sie sich an den Kundenadministrator, und bitten Sie ihn, den ursprünglichen Bestand zu erstellen.

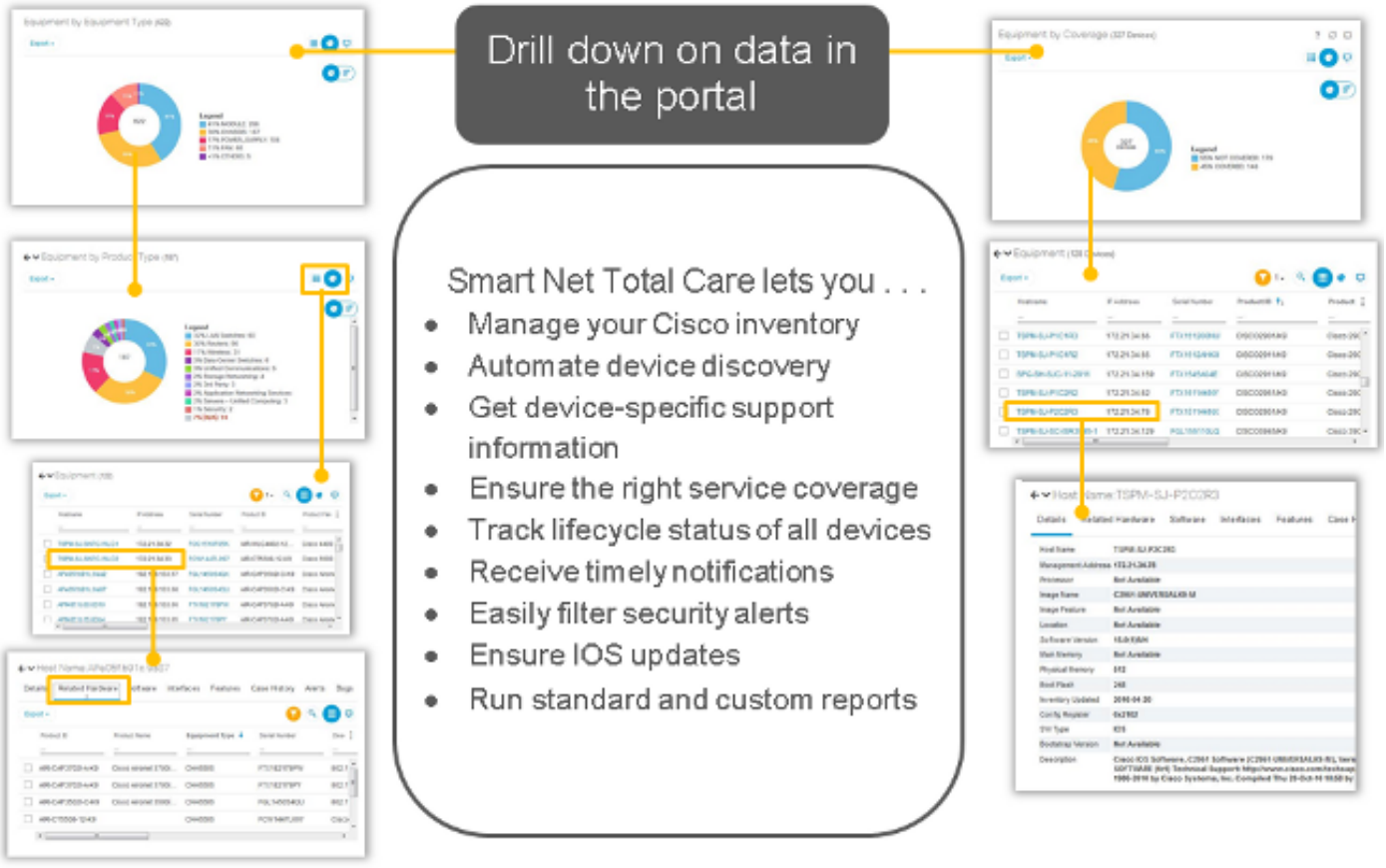
Wenn Sie Konten für mehrere Kunden (Multi-Role User) im Portal zugeordnet sind und die Berichte bei der Anmeldung *keine Datensätze gefunden* haben, ist es wahrscheinlich, dass die Gerätedaten für die Organisation nicht hochgeladen wurden. Wenden Sie sich an den/die Kundenadministrator(en) für diesen Kunden, und fordern Sie das Hochladen des Bestands an.

Grundlegende Portalnavigation

Das Smart Net Total Care-Portal nutzt die Services Connection-Plattform, die intuitive und benutzerfreundliche Berichte bereitstellt. Diese Berichte können gefiltert, in verschiedenen Formaten angezeigt und angepasst werden, um die Art und Weise zu definieren, in der die Daten angezeigt werden.

Diese Bilder veranschaulichen das Portal, wie es normalerweise beim Zugriff angezeigt wird, vorausgesetzt, es wurde mindestens einmal mit den Gerätedaten für Ihr Unternehmen ausgefüllt:





Portalkomponenten

Das Portal besteht aus den folgenden Komponenten:

- **Navigationsbereich links** - Dieser Teil der Seite enthält Links zu Berichten, Dashboards und Portaleinstellungen.
- **Logged-in User** (Benutzer angemeldet): In diesem Bereich wird der Name des Benutzers angezeigt, der derzeit angemeldet ist.

- **Wählen Sie Sprache** - Klicken Sie auf dieses Symbol, um die Sprache für lokalisierte Berichte und das Portal auszuwählen. Derzeit sind die Portalbildschirme in Französisch, Spanisch, Japanisch und Chinesisch (vereinfacht) lokalisiert. Hier können Sie auch Ihre Zeitzonenvoreinstellung festlegen.

  Hinweis: Einige Berichte oder Hilfen für die Berichte sind in der ausgewählten Sprache möglicherweise nicht verfügbar.

- **Informationen**: Klicken Sie auf dieses Symbol, um Anleitungsvideos anzuzeigen, eine Kopie dieses Leitfadens herunterzuladen und weitere Informationen zu Smart Net Total Care zu erhalten.
- **Abmelden** - Klicken Sie auf dieses Symbol, um sich vom Portal abzumelden.

  Hinweis: Im Rahmen der Cisco Richtlinie zum Schutz des Zugriffs auf Kundendaten wird nach einer Stunde Inaktivität des Portals eine Popup-Meldung auf dem Smart Net Total Care-Portalbildschirm angezeigt.

- **Ansichten anpassen**: Klicken Sie auf den Dropdown-Pfeil neben dem Spaltennamen, um die Daten in dieser Spalte festzulegen/zu sortieren.

  Tipp: Sie können die Spalten per Drag-and-Drop an die gewünschte Position verschieben. Zusätzlich können Sie *Pin Left* oder *Pin Right* auswählen, um die Spalte nach links oder rechts zu verschieben.

- **CSPC-Versionsberichte** - Dieser Teil der Seite benachrichtigt die Collector-Version, die vom angemeldeten Benutzer verwendet wird. Das Banner benachrichtigt den Collector vor der aktuellen Version des verwendeten Collectors, und es ist ein Upgrade erforderlich. Je nach der älteren Collector-Version ändert sich der Schweregrad des Banners, und es wird eine entsprechende Warnmeldung angezeigt. Klicken Sie auf das **E-Mail**-Symbol, um eine Liste der Collector-Details zu erhalten.
- **Text filtern**: Sie können einen Wert in dieses Feld eingeben und die **Eingabetaste** betätigen, um die Daten in der Spalte zu filtern, sodass die Ergebnisse angezeigt werden, die den angegebenen Kriterien entsprechen. Sie können einer oder mehreren Spalten Filterwerte hinzufügen.
- **Angewendete Filter**: Klicken Sie auf dieses Symbol, um die Filter anzuzeigen, die auf die Spalten (sofern vorhanden) im Bericht angewendet werden.
- **Wählen Sie Spalte** - Klicken Sie auf dieses Symbol, um die gesamte Liste der Spalten anzuzeigen, die für den Bericht verfügbar sind. Klicken Sie auf den Spaltennamen, um ihn im Bericht auszublenden oder anzuzeigen.

Ihre Berichtseinstellungen werden automatisch in Ihrem Profil übernommen. Änderungen wie die ausgewählten Spalten, die Reihenfolge der Spaltenplatzierungen und die Spaltengröße werden während der Sitzungen beibehalten, bis Sie sie ändern. Filter und Sortierfolgen werden jedoch nur bei geöffneter Sitzung beibehalten.

Tipp: Weitere Informationen zur Portalnavigation und zu Komponenten von Smart Net Total Care finden Sie im Video Navigation und Dashboards.

Einrichtung und Anpassung

Sie können das Auswahlfeld Smart Net Total Care oben im linken Navigationsbereich verwenden, um die in den Berichten angezeigten Daten einzurichten und anzupassen. Sie können die Auswahl nach Kunden, Beständen und Segmenten anpassen.

> **Hinweis**: Oben im linken Navigationsbereich wird der Name des aktuell verwendeten Cisco Service angezeigt. In diesem Fall Smart Net Total Care.

In diesem Abschnitt wird beschrieben, wie Sie das Portal und die zugehörigen Komponenten einrichten und anpassen:

- Kunde
- Bestand und Segment
- Meine Berichte
- Aktionen
- Nützliche Links
- Dashboards

Kunde

Der Kundenname sowie der Bestand und das Segment werden unter dem Servicenamen angezeigt. Dies ist der Name des berechtigten Kunden, dessen Gerätedaten in den Berichten angezeigt werden.

Die meisten Kunden sehen auf der Seite "Kunden" nur eine Option: den Namen ihres Unternehmens. Kunden, die mehr als einem Unternehmen zugeordnet sind, haben für jedes Unternehmen, auf das sie Zugriff haben, mehrere Auswahlmöglichkeiten. Partner oder Benutzer mit mehreren Rollen, die zum Anzeigen ihrer Kundendaten autorisiert sind, können hier auch mehrere Kunden auflisten.

Bestand und Segment

Die für die ausgewählten Kunden verfügbaren Bestände und Segmente werden auf der Seite "Bestand und Segment" angezeigt. Der Inhalt hängt von den Benutzerzugriffseinstellungen ab, die Ihnen zugewiesen sind.

Ein *Bestand* sind die Gerätedaten, die von einer Sammelquelle hochgeladen werden. Ein Bestand kann weiter in *Segmente* unterteilt werden.

Gehen Sie wie folgt vor, um auszuwählen, welche Inventare und Segmente in den Portalberichten angezeigt werden:

1. Klicken Sie auf das Bleistiftsymbol, und das Fenster *Globale Filter* wird geöffnet.
2. Klicken Sie auf **Kunde**, wenn dieser noch nicht ausgewählt ist.
3. Wählen Sie einen Kundennamen, um einen Filter festzulegen, sodass nur die Daten für die ausgewählten Kunden in den Berichten angezeigt werden.
4. Klicken Sie auf **Bestand und Segment**.
5. Wählen Sie die gewünschten Bestände und Segmente so aus, dass nur die Daten aus den ausgewählten Inventaren und Segmenten in den Berichten angezeigt werden.

   Hinweis: Das Portal unterstützt maximal 50 Segmente, die gleichzeitig ausgewählt werden können.

7. Klicken Sie auf **Apply**, um Ihre Auswahl beeinflussen zu lassen.

   Hinweis: Wenn Sie mehr als einen Bestand oder ein Segment auswählen, enthalten die Berichte die Daten jedes Bestands. Bei einigen Berichten kann nur ein einziger Kunde und ein Inventar/Segment ausgewählt werden.

Allgemeines

Die Registerkarte *Allgemein* enthält eine Liste der Business-Services und Kunden, auf die Sie zugreifen können, sowie Ihre Rolle für jeden Kunden.

Firmenbenachrichtigungen

Wenn Sie eine Administratorrolle haben, verwenden Sie diese Registerkarte, um die Verteilerlisten für die Nachrichten zu verwalten, die Sie an die Benutzer senden möchten.

Meine Benachrichtigungen

Verwenden Sie diese Registerkarte, um die gewünschte Häufigkeit zu verwalten, mit der Warnmeldungen und Systemmeldungen vom Portal empfangen werden.

Angepasster Anzeigename

Auf dieser Registerkarte kann der Administrator den Anzeigenamen der Organisation ändern oder anpassen. Gehen Sie wie folgt vor, um den Anzeigenamen der Organisation anzupassen:

1. Klicken Sie in der Spalte Anzeigename auf **Bearbeiten**. Der Cursor wird im Namensfeld angezeigt.
2. Geben Sie den Namen in das Namensfeld ein.
3. Klicken Sie auf **Speichern**.
4. Klicken Sie in **Anzeigename-Änderungsverlauf auf Anzeigen**, um den Verlauf der Änderung des Anzeigenamens anzuzeigen.

Anzeigename des Unternehmens

Auf dieser Registerkarte werden der Name Ihres Unternehmens als bei Cisco registriert angezeigt. Sie können einen Anzeigenamen, eine Benutzerrolle und den Verlauf aller vorgenommenen Änderungen an den Anzeigenamen anzeigen, wenn der Administrator einen Namen angegeben hat.

Meine Berichte

Die Seite Meine Berichte enthält folgende Informationen:

- Alle Berichte, die Sie kürzlich über die *Export*-Funktion erstellt haben. Die Berichtsnamen entsprechen den im linken Navigationsbereich aufgeführten Namen. Klicken Sie zum Erstellen dieser Berichte in den Berichten auf **Exportieren**.
- Die geplanten Berichte werden vom System über die Funktion *Schedule Report* generiert. Standardmäßig enthalten diese Berichtsnamen den Benutzernamen und einen eindeutigen numerischen Bezeichner. Sie können den Namen des Berichts ändern, wenn Sie die Berichte planen.

Die Berichte ermöglichen Ihnen Folgendes:

- Laden Sie einen Bericht über das lokale Gerät herunter, um weitere Analysen zu erstellen oder Kollegen darüber zu informieren.
- Den Status aller angeforderten Berichte anzeigen.
- Sehen Sie sich das Erstellungsdatum des Berichts an. Dies hilft bei der Bestimmung des Alters der Daten im Bericht.

Die gespeicherten Berichte können im PDF-, XLSX- oder CSV-Format vorliegen, wie beim Generieren des Berichts angegeben. Die Berichte werden in der Regel 72 Stunden nach ihrer Erstellung aufbewahrt.

Um die Berichte auf Ihr lokales Gerät herunterzuladen, klicken Sie in der Spalte *Download* auf den Link Format (z. B. XLSX oder PDF).

> **Hinweis**: Je nach Datenmenge, die verarbeitet werden muss, können Berichtsgenerationen mehrere Minuten oder Stunden dauern, bis sie zum Download verfügbar sind.

Nützliche Links

Die *Links*-Seite enthält Links zu Ressourcen für:

- Schulungen (wie Anleitungsvideos und Links zu diesem Leitfaden und dem CSPC-Installations- und -Benutzerhandbuch)
- Community-Zugriff auf Smart Net Total Care
- Support
- Vertragsmanagement
- Download- und Versionshinweise für CSPC-Software
- Fehlerbehebungsverfahren für Smart Net Total Care
- Kontoverwaltung
- Retourengenehmigung (Return Material Authorization, RMA)

Aktionen

Bericht planen

Die Funktion "Bericht planen" ist im linken Navigationsbereich unter Aktionen verfügbar. So können Sie die Erstellung der folgenden Berichte für den ausgewählten Kunden und Bestand/Segment automatisieren:

- **Konsolidierter Fehlerbericht** - Dieser Bericht bietet eine konsolidierte Ansicht der Fehler, die Cisco für jeden Posten im ausgewählten Kundenbestand korreliert hat.
- **Bericht zum Vertragsmanagement** - Dieser Bericht enthält Details zum Vertragsstatus aller wartbaren Artikel, die von Smart Net Total Care erfasst und verarbeitet wurden. Dieser Bericht enthält Vertragsinformationen sowie zugehörige Geräteinformationen und unterstützt Sie bei der Verwaltung Ihrer Cisco Verträge für technischen Support. Der Bericht enthält nur Elemente, die erfolgreich verarbeitet und als Cisco Gerät erkannt wurden. Der Bericht wird in zwölf Hauptregisterkarten in einer Excel-Datei angezeigt.
- **Benutzerdefinierter Bestandsbericht** - Dieser Bericht enthält Details zu den erfassten Geräten in Ihrem ausgewählten Bestand, die von Smart Net Total Care verarbeitet wurden. Dieser Bericht enthält Vertragsinformationen sowie zugehörige Geräteinformationen und unterstützt Sie bei der Verwaltung Ihrer Cisco Verträge für technischen Support. Der Bericht enthält nur Elemente, die erfolgreich verarbeitet und als Cisco Gerät erkannt wurden.
- **Inventory Collection Delta (Delta für Bestandserfassung)** - Der Delta-Bericht über die Bestandserfassung zeigt die Änderungen an, die in Ihren Netzwerkgeräten für einen festgelegten Zeitraum aufgetreten sind. Diese Informationen sind nützlich, wenn Sie die Berichtspräferenz in den Portalanwendungseinstellungen auf eine umfassende Ansicht festlegen. Wenn sich Ihr Netzwerk ständig ändert, ist eine zentrale Übersicht dieser Änderungen unerlässlich, um ein hochzuverlässiges Netzwerk zu gewährleisten. Mit dem Delta-Report zur Bestandserfassung können Sie problemlos Verschiebungen, Hinzufügungen und Änderungen in Ihrem Netzwerk bestätigen.
- **Inventory Insight Report** - Der Inventory Insight Report enthält Informationen zu allen Artikeln in allen Sammlungen für das berechtigte Unternehmen. Die Registerkarten enthalten Elemente, die erfolgreich verarbeitet wurden, sowie solche, die nicht verarbeitet wurden. Die Registerkarten werden als "aussagekräftig" klassifiziert, d. h. der Kunde kann die vorgeschlagenen Abhilfemaßnahmen durchführen, oder als "Information", was darauf hinweist, dass keine spezifischen Kundenmaßnahmen erforderlich sind.
- **Upload Processing Report** - Der Upload Processing Report enthält Informationen zu allen Geräten, die Teil der Liste und Sammlung verwalteter Geräte waren, aber aus verschiedenen Gründen nicht in den Berichts-Berichten zu Bestand, Verträgen und Warnungen aufgeführt

werden. Dieser Bericht bietet Transparenz für alle Sammlungen im gesamten Unternehmen und liefert aussagekräftige oder informative Details. Die Registerkarten werden eindeutig als "aussagekräftig" klassifiziert, d. h. sie geben an, dass die Kunden empfohlene Korrekturmaßnahmen durchführen können, oder als "Information", was darauf hinweist, dass keine spezifischen Kundenmaßnahmen erforderlich sind. Die Daten werden für jede zur Analyse vorgestellte IP-Adresse angegeben.

So greifen Sie auf den Scheduler zu:

1. Klicken Sie auf den Link **Aufgabe planen**.
2. Wählen Sie den gewünschten Bericht aus der Dropdown-Liste aus.

Standardmäßig enthalten diese Berichtsnamen den Benutzernamen und einen eindeutigen numerischen Bezeichner. Sie können den Namen des Berichts ändern, bevor Sie Berichte ausführen. Sie können dem Bericht auch eine detaillierte Beschreibung hinzufügen. Dieser Schritt ist optional.

Um den Bericht bei Bedarf auszuführen, klicken Sie auf **Jetzt ausführen**. Um den Bericht zu planen, klicken Sie auf **Weiter**.

1. Richten Sie die Zeitspanne für die Wiederholung ein, und klicken Sie dann auf **Weiter**.
2. Geben Sie Notification ein, indem Sie Kontrollkästchen aktivieren, um weitere Benutzer per E-Mail darüber zu benachrichtigen, dass der abgeschlossene Bericht verfügbar ist, und klicken Sie dann auf **Weiter**.
3. Überprüfen Sie die in den vorherigen Schritten festgelegten Parameter, und klicken Sie dann auf **Weiter**.

Nachdem der Bericht erstellt wurde, wird der Bericht an die registrierte E-Mail-Adresse gesendet, und der Bericht ist unter "Meine Berichte" verfügbar.

Dashboards

Die Dashboards bieten eine konsolidierte Ansicht der wichtigsten Daten. Sie können diese Dashboards verwenden, um einen Überblick über den Vertragsstatus, Inventare, Geräte und Warnungen innerhalb der vorhandenen Installationen des ausgewählten Kunden zu erhalten.

Das Portal umfasst folgende Dashboards:

- Administrator
- Alert-Management
- Vertragsmanagement
- Bestandsverwaltung
- Smart Net Total Care

Um die für Sie relevantesten Berichte und Warnungen anzuzeigen, können Sie personalisierte Dashboards erstellen und speichern. Diese Dashboards werden in späteren Sitzungen beibehalten.

Administrator

Das Admin-Dashboard wird von den Administratoren verwendet, um die Benutzer- und Gerätedatensammlungen zu verwalten.

Die Daten und Berichte, die die Benutzer im Portal sehen, werden durch ihre Rollen bestimmt. Administratoren können die *rollenbasierte Zugriffskontrolle* anwenden, um den Zugriff der Benutzer entsprechend ihrer Anforderungen zu beschränken. Beispielsweise kann eine Benutzergruppe Zugriff auf Daten für ein bestimmtes Netzwerksegment erhalten, während der Zugriff auf eine andere Benutzergruppe auf bestimmte Berichte beschränkt werden kann.

Das Admin-Dashboard enthält vier *Dashboards*:

- Segmentverwaltung
- Uploads
- Benutzer

Segmentverwaltung

> **Hinweis**: Dieses Dashboard steht nur Administratoren von Kunden und Partnern zur Verfügung.

Das Dashboard Segment Management zeigt die Segmente innerhalb eines Bestands und zugehörige Informationen an. Die Segmente werden für die Sicherheit, die Zugriffskontrolle und zur Aufteilung der im Portal angezeigten Daten auf Hostname, IP-Adresse oder SysName verwendet. Die Segmentierung wird von den Administratoren abgeschlossen, die den Benutzern später Zugriff auf die einzelnen Segmente gewähren.

Sie können die Segmente verwenden, um die Benutzer auf die Informationen zu verweisen, die sie am häufigsten verwenden, z. B. nach *Kostenstelle* oder *Standort*. Abhängig von den Administratordefinitionen können die Benutzer auf alle Segmente zugreifen. Wenn mehrere Segmente dasselbe Gerät enthalten und ein Benutzer mehrere Segmente zum Anzeigen auswählt, erfolgt die Duplizierung in den Berichten.

Sie können diese Aktionen über das Dashboard "Segmentverwaltung" ausführen:

- Erstellen Sie Datensegmente auf der Grundlage mehrerer Kriterien, um boolesche Bedingungen einzuschließen.
- Zeigen Sie eine Liste der Geräte an, die in einem erstellten Segment enthalten sind.
- Gewähren Sie Benutzern Zugriff auf Daten für ein Segment.
- Anzeigen, Ändern, Kopieren oder Löschen aktueller Segmente.

Gehen Sie wie folgt vor, um ein neues Segment zu erstellen:

1. Klicken Sie auf **Aktionen** und dann auf **Neues Segment erstellen**. Das Fenster *Neues Segment erstellen* wird angezeigt.
2. Geben Sie im Feld *Name* einen eindeutigen Segmentnamen ein. Sonderzeichen oder Leerzeichen sind nicht zulässig, aber Sie können Zahlen verwenden.
3. Wählen Sie einen Bedingungswert aus, z. B. *Hostname* oder *IP-Adresse*.
4. Wählen Sie einen booleschen Operator aus, z. B. *enthält* oder *beginnt mit*.
5. Geben Sie eine *übereinstimmende Bedingung ein*. Sie können Platzhalter verwenden.
6. Wenn Sie eine andere Bedingung festlegen müssen, klicken Sie auf das *Plus*- (+)-Symbol.
7. Wiederholen Sie die vorherigen Schritte.
8. Überprüfen Sie die Geräteliste, und weisen Sie ggf. Benutzerzugriff zu.

> **Tipp**: Wenn Sie nach dem Erstellen der Segmente den Segmenten Benutzer zuweisen

möchten, werden in den folgenden Abschnitten alternative Methoden bereitgestellt.

9. Klicken Sie auf **Erstellen**. Ein neues Segment wird erstellt.

Gehen Sie wie folgt vor, um eine Liste der Geräte in einem Segment anzuzeigen:

1. Klicken Sie mit der rechten Maustaste auf einen Segmentnamen.
2. Wählen Sie auf der Schaltfläche *Aktionen* die Option **Anzeigen/Ändern aus**.
3. Klicken Sie auf **Geräteliste anzeigen**.

Gehen Sie wie folgt vor, um Benutzern Zugriff auf Daten in einem Segment zu gewähren:

1. Klicken Sie mit der rechten Maustaste auf einen Segmentnamen.
2. Wählen Sie auf der Schaltfläche *Aktionen* die Option **Anzeigen/Ändern aus**.
3. Klicken Sie auf **Benutzer auswählen**. Sie können alle Benutzer oder einzelne Benutzer auswählen.
4. Klicken Sie auf **Hinzufügen**, um den ausgewählten Benutzern Zugriff zu gewähren. Benutzer und andere Administratoren von Kunden erhalten eine E-Mail-Benachrichtigung, wenn ihnen der Zugriff auf ein Segment gewährt oder ihr Zugriff entzogen wird.
5. Klicken Sie auf **Apply**, um die Änderungen zu speichern.

Gehen Sie wie folgt vor, um ein Segment anzuzeigen oder zu ändern:

1. Klicken Sie mit der rechten Maustaste auf einen Segmentnamen.
2. Wählen Sie auf der Schaltfläche *Aktionen* die Option **Anzeigen/Ändern aus**.
3. Ändern Sie die Einstellungen nach Bedarf.
4. Klicken Sie auf **Apply**, um die Änderungen zu speichern.

Gehen Sie wie folgt vor, um eine Kopie eines Segments zu erstellen:

1. Klicken Sie mit der rechten Maustaste auf ein Segment.
2. Wählen Sie in der Schaltfläche *Aktionen* die Option **In Neues Segment kopieren aus**.
3. Geben Sie einen neuen eindeutigen Namen für dieses Segment ein.
4. Ändern Sie die Einstellungen nach Bedarf.
5. Klicken Sie auf **Erstellen**.

Die Segmente, die von den Administratoren von Cisco Branded Reseller (CBR) erstellt werden, sind für den Kundenadministrator nur im Dashboard "Segment Management" sichtbar. In diesem Dashboard können Kundenadministratoren CBR-Benutzer einem Segment zuweisen, das von einem CBR-Administrator erstellt wurde. Kundenadministratoren können Kunden jedoch keine Segmente zuweisen, die von einem CBR-Administrator erstellt wurden.

> **Hinweis**: Die Segmente, die in diesem Dashboard erstellt und verwaltet werden, wirken sich nur auf die Art und Weise aus, wie Daten in den Portalberichten dargestellt und abgerufen werden. Diese Segmentierung hat keine Auswirkungen auf die Netzwerke am Kundenstandort.

> **Tipp**: Weitere Informationen zum Segmentmanagement finden Sie im Video zum Netzwerksegmentmanagement.

Uploads

Das Dashlet Uploads zeigt einen Datensatz der letzten Sammlungen an, die für ein berechtigtes Unternehmen mithilfe einer der folgenden Methoden erstellt wurden:

- CSPC-Upload
- Importe von CSV-Dateien
- Collector-Datei-Uploads von unterstützten Collectors von Drittanbietern

Sie können dieses Dashboard verwenden, um die Häufigkeit zu überwachen, mit der Sie Ihre Netzwerkdaten im Portal aktualisieren.

> **Hinweis**: Als bewährtes Verfahren legen Kunden ihre Sammlungen fest, um sie einmal pro Woche oder Monat hochzuladen. Cisco ermöglicht maximal 5 Uploads pro Tag pro Kundenbestand aus allen Methoden.

Benutzer

Das Benutzer-Dashlet listet die Benutzer auf, die für ein bestimmtes Konto auf Daten zugreifen können. Als Kundenadministrator können Sie dieses Dashboard verwenden, um:

- Gewähren oder Widerrufen des Benutzerzugriffs auf bestimmte Funktionen des Portals
- Zeigen Sie ein Protokoll der Änderungen an, die an einem Benutzerkonto vorgenommen wurden.
- Validieren Sie die LoA (Letter of Authorization) für CBR-Benutzer und CBR-Administratoren.

> **Hinweis**: Die Änderungen, die an den Benutzerzugriffseinstellungen vorgenommen werden, werden aktiv, wenn sich der Benutzer beim nächsten Mal beim System anmeldet.

Um die Benutzer anzuzeigen, die Sie als Kundenadministrator verwalten können, klicken Sie auf das Symbol mit drei vertikal ausgerichteten Punkten, und blenden Sie die Spalte *Verwaltbar* aus (wenn sie zuvor ausgeblendet wurde). Wenn der *verwaltbare* Wert für einen Benutzer auf *Ja* festgelegt ist, können Sie den Benutzer verwalten.

Wenn Sie ein Kundenadministrator sind, können Sie die folgenden Schritte ausführen, um die Zugriffsebenen für einen Benutzer zu verwalten:

1. Klicken Sie auf das Optionsfeld für eine Benutzerzeile.
2. Wählen Sie auf der Schaltfläche *Aktionen* die Option **Zugriff verwalten aus**.
3. Gewähren Sie dem Benutzer wie im Dialogfeld beschrieben Zugriff auf *Informationen und Funktionen* sowie auf *Bestands- und Segmente*. Informationen und Funktionen beziehen sich auf Features, die der Benutzer sehen kann, oder Funktionen, die er ausführen kann. Bestand und Segmente bestimmen, ob der Benutzer Aktionen innerhalb eines bestimmten Satzes von erfassten Daten ausführen kann.
4. Klicken Sie auf **OK**, um die Änderungen zu speichern.

Gehen Sie wie folgt vor, um das LoA für einen CBR-Benutzer zu aktualisieren:

1. Klicken Sie auf das Optionsfeld, um den Benutzer auszuwählen.
2. Klicken Sie auf **Aktionen** und dann auf **LoA-Zugriff (Letter of Authorization) erneut validieren**.

Es wird eine Tabelle mit den Benutzern angezeigt, deren LoA-Berechtigung innerhalb der nächsten 30 Tage abläuft.

3. Klicken Sie auf **Revalidieren**, um die LoA-Berechtigung für den Benutzer fortzusetzen.

Hinweis: Kundenadministratoren können diese Aktion für CBR-Benutzer und CBR-Administratoren durchführen.

Gehen Sie wie folgt vor, um den Verlauf der Profilaktualisierungen anzuzeigen:

1. Klicken Sie auf das Optionsfeld, um einen Benutzer auszuwählen.
2. Klicken Sie auf **Aktionen** und dann auf **Profilaktualisierungsverlauf**.

Nach Abschluss dieser Schritte wird ein Protokoll angezeigt, in dem die Aktionen aufgeführt sind, die von Administratoren für den ausgewählten Benutzer durchgeführt wurden. Sie können dieses Protokoll verwenden, um die Aktionen anderer Kundenadministratoren zu überprüfen.

Hinweis: Alternativ können Sie dieses Protokoll auch über **Aktionen > Verlauf der Profilaktualisierung > Zugriff verwalten** anzeigen.

Tipp: Weitere Informationen zur Verwaltung des Benutzerzugriffs finden Sie im Video für die Zugriffsverwaltung.

Alert-Management

Das Smart Net Total Care-System bietet Informationen zu den Kundengeräten, die von von Cisco veröffentlichten Produktwarnungen und Sicherheitsempfehlungen betroffen sind.

Warnungsverwaltungs-Workflows ermöglichen es Ihnen, empfangenen Warnmeldungen Statusmeldungen zuzuweisen. Diese drei Statusoptionen stehen für aktive Warnungen zur Verfügung, mit denen Sie Warnungen filtern können, sodass nur die relevantesten angezeigt werden:

- Ignorieren
- Maßnahmen
- Maßnahme erforderlich

Das Warnungs-Management-Dashboard umfasst zwei Dashboards: *Aktive Warnmeldungen Zusammenfassung* und *letztes Support-Datum*.

Tipp: Um die Warnungen im Tabellenformat anzuzeigen, klicken Sie auf den Link neben der Kategoriebeldung *Alert Type* oder auf den Abschnitt für den Kuchen in der Diagrammanzeige.

Zusammenfassung der aktiven Warnmeldungen

Hinweis: In der Standard-*Diagrammansicht* lautet der Name dieses Dashlet *Aktive Warnmeldungszusammenfassung nach Typ*.

Das Dashboard "Übersicht über aktive Warnmeldungen" zeigt die Gesamtzahl der Warnungen für jeden Warnungstyp für die ausgewählten Inventare an. Aktive Warnmeldungen sind die Warnungen, die Sie nicht bestätigt haben.

Sie können diesen Bericht verwenden, um:

- Zeigen Sie eine Gesamtübersicht der ausstehenden Warnungen nach Kategorie an.
- Exportieren Sie die Berichtsdaten zu Referenzzwecken.
- Zeigen Sie die Geräte an, die von einer Warnungskategorie betroffen sind (klicken Sie im Diagramm auf den entsprechenden Abschnitt).

Dieses Dashboard unterstützt Netzwerkadministratoren und -techniker dabei, sich schnell auf die relevantesten Warnungen zu konzentrieren, was die Betriebseffizienz erhöht und das Risikomanagement verbessert.

> **Tipp**: Weitere Informationen zur Verwaltung von Warnmeldungen finden Sie im Video Alert Prioritization oder Alert Administration.

Letztes Support-Datum

Im Dashlet "Last Date of Support" (Letztes Datum des Supports) werden Anzahl und Details der Geräte (in den ausgewählten Beständen) aufgeführt, für die das veröffentlichte LDoS für die Gerätehardware:

- innerhalb von 12 Monaten
- ist über 12 Monate, aber innerhalb von 24 Monaten
- Wurde bestanden

> **Tipp**: Weitere Informationen zu diesem Thema finden Sie im Video "Abdeckungslücken".

Vertragsmanagement

Das Dashboard für das Vertragsmanagement zeigt den Status der Cisco Serviceverträge und der zugehörigen Geräte an. Dieses Dashboard bietet vollständige Transparenz für Ihre Cisco Netzwerkgeräte. So können Sie Verlängerungen vereinfachen, Berechtigungen überprüfen und Abdeckungslücken und Möglichkeiten zur Vertragskonsolidierung einfach identifizieren. Dieses Dashboard enthält die folgenden vier Dashboards:

- Alle Verträge
- Support-Abdeckung
- Geräte mit auslaufender Abdeckung in 30 Tagen
- Geräte mit überfälliger Abdeckung

Alle Verträge

Das Dashboard "All Contracts" (Alle Verträge) enthält umfassende Details zu den Serviceverträgen für die Geräte, die durch die Netzwerkerkennung erkannt und validiert werden.

> **Tipp**: Sie können auch zu **Library > Contracts** navigieren, um diese Informationen anzuzeigen, die standardmäßig im Tabellenformat angezeigt werden.

Support-Abdeckung

Das Dashboard "Support Coverage" zeigt die Anzahl der Geräte an, gruppiert nach ihrem Vertragsstatus. Das Datendiagramm enthält konsolidierte Informationen, die aus den detaillierteren Berichten in der Contracts-Bibliothek extrahiert werden.

Für abgedeckte Geräte werden folgende Status angezeigt:

- **Abgedeckt (Signiert)** - Dieser Status gibt die Anzahl der Geräte an, für die die Abdeckung zu einem späteren Zeitpunkt beginnen soll.
- **Abgedeckt (Aktiv)** - Dieser Status gibt die Anzahl der Geräte an, die derzeit durch einen Servicevertrag abgedeckt sind, sowie alle eindeutigen Geräte mit mindestens einem aktiven Vertrag.
- **Abgedeckt (Überfällig)** - Dieser Status gibt die Anzahl der Geräte an, für die der Vertrag abgelaufen ist. Der Vertrag für diese Geräte kann innerhalb von 30 Tagen nach Ablaufdatum verlängert werden.
- **Abgedeckt (läuft in 90 Tagen ab)** - Dieser Status gibt die Anzahl der Geräte an, für die der Vertrag innerhalb von 90 Tagen abläuft.
- **Abgedeckt (Abdeckungsstatus nicht sichtbar)** - Dieser Status gibt die Anzahl der Geräte an, zu denen Sie nicht autorisiert sind, den Vertragsstatus anzuzeigen. Dieses Szenario tritt ein, wenn die Geräte durch Partnerverträge abgedeckt sind.

Für nicht abgedeckte Geräte werden folgende Status angezeigt:

- **Nicht abgedeckt** - Dieser Status gibt die Anzahl der Geräte an, die nicht durch Cisco Verträge abgedeckt sind.
- **Not Covered (Not Covered, nicht abgedeckt)** - Dieser Status gibt die Anzahl der Geräte an, die nicht von Cisco Verträgen abgedeckt sind. Der Grund für die Nichtabdeckung wird jedoch angegeben.

Wenn ein Gerät von mehreren Verträgen mit unterschiedlichen Status abgedeckt ist, wird das Gerät unter beiden Status angezeigt. Wenn beispielsweise ein Gerät einen Vertrag hat, der aktiv ist, und ein anderer Vertrag überfällig ist, wird das Gerät unter den Status *Covered (Active)* und Covered (*Overdue)* gezählt.

Wenn ein bestimmter Vertragsstatus im Inventar nicht verfügbar ist, wird er nicht im Tortendiagramm angezeigt. Wenn es z. B. keine Geräte mit signierten Verträgen gibt, wird der Status *Covered (Signed)* nicht angezeigt.

Dieses Dashboard bietet Netzwerkadministratoren und Vertragsadministratoren einen umfassenden Überblick über die Vertragsabdeckung für ihr Inventar. So können sie Verträge effizienter verwalten, was die Betriebseffizienz erhöht und das Risikomanagement verbessert.

> **Hinweis**: Die Anzahl der abgedeckten Geräte in diesem Dashboard kann sich von der Anzahl unterscheiden, die im Bericht über die Vertragsbibliothek und im Bericht über die Bestandsübersicht angezeigt wird. Der Grund hierfür ist, dass die Anzahl der in diesem Dashlet abgedeckten Geräte die Anzahl der Geräte pro Bestand darstellt, die durch mindestens einen gültigen Cisco Vertrag abgedeckt sind. Die Berichte der Vertragsbibliothek und die Bestandszusammenfassung enthalten jedoch eine Liste der gültigen Verträge pro Gerät. Ein Gerät kann unter mehreren Verträgen abgedeckt sein und mehrmals im Bericht angezeigt werden. Die Nummer, die neben dem Berichtsnamen angezeigt wird, stellt die Zeilenanzahl des Berichts dar.

Geräte mit auslaufender Abdeckung in 30 Tagen

Im Dashlet "Geräte mit auslaufender Abdeckung in 30 Tagen" werden die Geräte aufgeführt, für die der Cisco Servicevertrag innerhalb von 30 Tagen abläuft. Sie können auf die *Hostname-URL* klicken, um weitere Informationen zu erhalten.

Geräte mit überfälliger Abdeckung

Im Dashboard "Equipment with Overdue Coverage" (Geräte mit übermäßiger Abdeckung) werden die Geräte aufgelistet, für die eine Abdeckung überfällig ist.

Bestandsverwaltung

Dieses Dashboard besteht aus Daten, die von Ihren Geräten gesammelt werden und mit den Herstellungs- und E-Commerce-Datensätzen von Cisco abgeglichen werden. Es umfasst zwei Dashlets: *Gerätetyp* und *Bestandsquelle*.

> **Hinweis**: Die Dashboards in diesem Dashboard bieten Netzwerkadministratoren und -technikern eine bessere Übersicht über die Geräte im Netzwerk, was die Betriebseffizienz erhöht und das Risikomanagement verbessert.

Gerätetyp

Das Dashlet "Gerätetyp" bietet eine Zusammenfassung aller Geräte im Netzwerk und ist in Kategorien wie Netzteile und Chassis unterteilt. Klicken Sie auf jede Kategorie, um durch die verschiedenen Kategorisierungsstufen zu navigieren und die einzelnen Gerätedetails zu erreichen.

Bestands-Quelle

Das Dashlet "Inventory Source" (Bestandsquelle) gibt die Quelle an, von der jedes Gerät hochgeladen wird (in den ausgewählten Inventaren). Dabei kann es sich um eine der folgenden Methoden handeln:

- Collectors (CSPC und DrittesParty)
- CSV-Dateiimport
- Collector-Datei-Upload

Smart Net Total Care

Dies ist das Standard-Dashboard, das beim ersten Besuch des Portals geöffnet wird. Dieses Dashboard enthält vier Dashboards:

- Gerätetyp
- Support-Abdeckung
- Aktive Warnungen
- Gemeinschaft

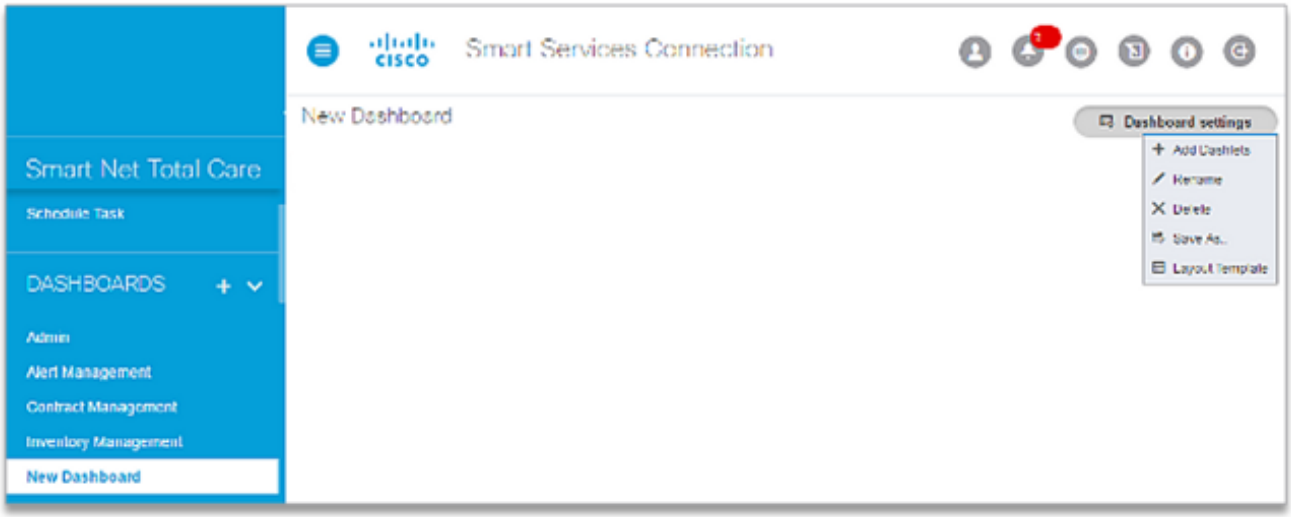
> **Hinweis**: Im Community-Dashlet werden die jüngsten Ankündigungen des Smart Net Total Care-Teams sowie Links zu beliebten Diskussionsthemen im Online-Forum angezeigt.

Benutzerdefinierte Dashboard-Erstellung

Um die für Sie wichtigsten Berichte anzuzeigen, können Sie benutzerdefinierte Dashboards erstellen. Diese Dashboards werden im Portal gespeichert und können über den linken Navigationsbereich aufgerufen werden.

Gehen Sie wie folgt vor, um ein eigenes Dashboard zu erstellen:

1. Klicken Sie im linken Navigationsbereich auf das Pluszeichen (**+**) neben der Überschrift *DASHBOARDS*. Ein leerer Bereich *Neues Dashboard* wird geöffnet.
2. Klicken Sie im Bereich Neues Dashboard auf **Dashboard-Einstellungen** und anschließend auf **Layoutvorlage**. Alle für das Dashboard verfügbaren Layouts werden angezeigt.
3. Klicken Sie auf das Optionsfeld neben einem Layout, um es auszuwählen.
4. Klicken Sie auf **Add Dashlets**. Eine Liste mit allen Bibliotheksberichten wird angezeigt:



5. Wählen Sie den Bericht aus, den Sie in das Dashboard einfügen möchten. Fahren Sie fort, bis Sie alle Berichte hinzufügen, die Sie anzeigen möchten.
6. Klicken Sie auf **Speichern unter**, um das Dashboard zu speichern. Sie können einen neuen Namen für das Dashboard eingeben und dann auf **Erstellen** klicken, um das Dashboard zu speichern.
7. Klicken Sie auf **Umbenennen**, um das Dashboard umzubenennen.
8. Klicken Sie auf **Löschen**, um das Dashboard zu löschen.

Erstellen und Verwenden von Berichten

Alle Smart Net Total Care-Berichte sind in der *Bibliothek* unter den folgenden Kategorien gruppiert:

- Administration
- Warnungen
- Verträge
- Vorfälle
- Bestand
- Bestandsaufnahme

In diesem Abschnitt wird beschrieben, wie die Berichte verwendet werden, die in diesen Kategorien gruppiert sind.

Administration

Wenn Sie ein Administrator sind, können Sie die Servicevertragsabdeckung mithilfe der Berichte in diesem Katalog verfolgen, neue Geräte identifizieren und überwachen und nach den relevantesten Warnmeldungen filtern. Zuverlässige und regelmäßige Berichte helfen Ihnen, proaktiv auf Bedenken zuzugreifen und Risiken zu minimieren. Mithilfe dieser Berichte können Sie auch Ressourcen planen und Budgets zuweisen.

Upload-Verarbeitung

Der Bericht Upload Processing (Upload-Verarbeitung) gibt den Status der kompletten Inventare oder der Inventare an, für die die Datenanalyse durchgeführt wird. Zu den Quellen für den Hochladen von Beständen gehören:

- Collectors (CSPC und Drittanbieter)
- CSV-Dateiimport
- Collector-Datei-Upload

Wenn in einem 24-Stunden-Fenster mehr als 20 Uploads vom gleichen Collector ausgeführt werden, erhält der Kundenadministrator per E-Mail eine Benachrichtigung, dass doppelte Uploads gelöscht werden. Dadurch wird sichergestellt, dass die Uploads verarbeitet werden.

Aktive Warnungen

Hinweis: Dieser Bericht ist nur für Administratoren und autorisierte Benutzer sichtbar.

Der Bericht über aktive Warnmeldungen ermöglicht es Administratoren, die Warnungen anzuzeigen, die auf die Geräte in Ihrem Inventar angewendet werden, und Warnmeldungen für Benutzer bereitzustellen/zu verwalten. Bei der SNTC-Warnmeldung werden Hardware- und Softwareversionen, IOS und die aktuelle Konfiguration von Geräten berücksichtigt, sobald diese Informationen verfügbar sind, um den Grad der Schwachstelle (Anfällig, Potenziell anfällig usw.) zu ermitteln. Diese Warnungen können Hardware-Warnungen, Software-Warnungen, Problemhinweise (Field Notices, FNs) und Warnungen des Product Security Incident Response Team (PSIRT) umfassen. Administratoren können diesen Bericht verwenden, um:

- Legen Sie den Warnstatus auf *Ignorieren fest* und erläutern Sie den Grund mit Kommentaren oder Notizen für alle betroffenen Geräte.
- Rufen Sie den Bericht Affected Devices (Betroffene Geräte) auf, und legen Sie den Warnstatus auf *Ignore (Ignorieren)*, *Action* (Abgegangene Aktion) oder *Action Required (Erforderlich)* für ein bestimmtes Gerät fest.
- Geben Sie einen Hinweis ein, um auf eine Warnung aufmerksam zu machen.
- Zeigen Sie die Alarmdetails an.
- Zeigen Sie den Status und die Notizen für jede Warnung an.

Dieser Bericht ermöglicht es Netzwerkadministratoren und -technikern, die Warnungen zu bestätigen und Aktionen zu dokumentieren, die Sie als Reaktion auf diese Warnungen durchführen. Sie erhalten also nicht wiederholt dieselben Warnmeldungen. So können Sie Warnungen abhören, auf die Sie geantwortet haben, aber Ihre Aktionen protokollieren. Dies verbessert auch die Betriebseffizienz und das Risikomanagement.

Gehen Sie wie folgt vor, um den Warnstatus für alle Geräte zu ändern, die von einer bestimmten

Warnmeldung betroffen sind:

1. Klicken Sie für jede Zeile, die Sie ändern möchten, auf die entsprechenden Kontrollkästchen.
2. Klicken Sie auf **Aktionen** und dann auf **Warnstatus ändern**. Ein neues Fenster wird geöffnet.
3. Wählen Sie **Ignorieren**, um den Status einer Warnung von *Aktiv* in *Ignorieren* zu ändern. Anschließend wird die Warnmeldung nicht mehr im Bericht über aktive Warnmeldungen angezeigt. Um zum *aktiven* Status zurückzukehren, verwenden Sie den Bericht Alle Warnungen.
4. Geben Sie einen Hinweis in das Feld *Notizen ein*. (Dieser Schritt ist optional.)
5. Geben Sie einen Kommentar in das Feld *Kommentar ein*. (Dieser Schritt ist optional.)
6. Klicken Sie zur Bestätigung auf **OK**.

Hinweis: Wenn Sie den Status für eine Warnung ändern, wirkt sich dies auf alle Ihre Inventare aus.

Betroffene Geräte

Im Bericht Affected Devices (Betroffene Geräte) sind die Geräte aufgeführt, die von derselben Warnung in den ausgewählten Inventaren betroffen sind. Um eine Liste der Geräte anzuzeigen, die von einem Warnungstyp betroffen sind, klicken Sie in der Spalte *Betroffene Geräte* auf den Link Nummer.

Sie können diesen Bericht verwenden, um:

- Reaktion auf Warnungen für einzelne Geräte
- Fügen Sie zusätzliche Appliances in einem bereits vorhandenen Bestand hinzu.

Gehen Sie wie folgt vor, um eine Warnmeldung für einzelne Geräte festzulegen, die von einer bestimmten Warnmeldung betroffen sind:

1. Aktivieren Sie die Kontrollkästchen für die gewünschten Geräte.
2. Klicken Sie auf **Aktionen > Antwort auf die Warnung**.
3. Wählen Sie eine der folgenden Optionen aus:
    - Ignorieren
    - Maßnahmen
    - Maßnahme erforderlich
4. Geben Sie einen Kommentar in das Feld *Kommentare ein* (dies ist optional).
5. Klicken Sie zur Bestätigung auf **OK**. Klicken Sie auf das **X** in der rechten oberen Ecke des Dialogfelds, um den Vorgang abzubrechen.

Hinweis: Ihre Antworten werden sowohl in Online- als auch in Offline-Warnberichten angezeigt.

Um die Details eines Geräts anzuzeigen, klicken Sie in der Spalte *Hostname* auf den Link für das gewünschte Gerät.

Um den Warnstatus und die Notizen anzuzeigen, deaktivieren Sie die Spalten *Antwort* und *Kommentare* (sofern diese standardmäßig nicht sichtbar sind).

Tipp: Weitere Informationen zur Verwaltung von Warnmeldungen finden Sie im Video

Identifizieren relevanter Warnmeldungen oder Alert Administration.

Alle Collectors

Im Bericht All Collectors werden die Collectors aufgelistet, die für das ausgewählte Unternehmen registriert sind. Das Raster All Collectors (Alle Collectors) zeigt ein blaues Punktsymbol vor den Collectors an, bei denen eine ältere CSPC-Version installiert ist. Hier werden CSPC-Collectors mit unterstützten Versionen vorgestellt, und es ist eine neue Version verfügbar.

Überprüfen Sie die aufgeführten Collectors und notifizierte Versionen. Wenn die Version nicht verfügbar ist, prüfen Sie weiter, ob der Collector online ist oder nicht mehr aktiv ist, und können Sie die Registrierung entfernen.

Daten, die von diesen Collectors erfasst werden, sind in den Daten enthalten, die vom Portal gemeldet werden.

> **Hinweis**: Zu den zusätzlichen Methoden für das Hochladen von Daten gehören der Import von CSV-Dateien und das Hochladen von Collector-Dateien.

Dateiimport

> **Hinweis**: Nur Administratoren und autorisierte Benutzer können einen Dateiimport durchführen.

Wenn Sie Ihre Gerätedaten manuell in Tabellen speichern, können Sie die formatierten Daten in das Portal hochladen. Die Daten werden anschließend analysiert und mit Support-Informationen von Cisco erweitert. Mit dieser Funktion können Sie Geräteinventarddaten aus einer Datei hochladen, nicht aus einem Collector vor Ort.

Sie können die Dateiimport-Funktion als eigenständige Methode verwenden, um Daten hochzuladen (wenn Sie keinen Collector installieren möchten) oder in Verbindung mit dem Collector.

Sie können eine der beiden folgenden Methoden verwenden, um die Gerätedatendatei zu generieren:

- Verwenden Sie die bereitgestellte Vorlagendatei, und geben Sie die Geräteinformationen in die Datei ein.
- Verwenden Sie einen Collector, um die Gerätedatei zu generieren, und laden Sie dann die Gerätedaten mithilfe der Dateiimport-Funktion hoch. In diesem Fall verwenden Sie den Collector, um die Gerätedaten zu erfassen, laden die Daten dann aber manuell hoch.

Wenn Sie eine Datei manuell zusammen mit einem Collector hochladen, ergänzen Sie die Collector-Sammlung. Dadurch können Sie die Geräte hinzufügen, die sich im Netzwerk befinden und vom Collector nicht erfasst werden können. Einige Geräte befinden sich beispielsweise möglicherweise hinter einer Firewall, und einige Ersatzgeräte sind derzeit nicht eingeschaltet oder mit dem Netzwerk verbunden.

Gehen Sie wie folgt vor, um eine CSV-Datei für den Upload mithilfe einer Vorlage vorzubereiten:

1. Wählen Sie **CSV-Dateiimport** als Importtyp aus.

2. Klicken Sie auf den Link, um die CSV-Beispieldatei herunterzuladen.
3. Geben Sie die Informationen für die Parameter ein.

   Hinweis: Denken Sie daran, Zeile 2 und Spalte I zu löschen.

4. Speichern Sie die Datei im Format *.csv*.

   Hinweis: Beim Zugriff auf die Dateiimport-Funktion kann nur ein Inventar ausgewählt werden.

Gehen Sie wie folgt vor, um eine Collector-Datei für den Upload vorzubereiten:

1. Abrufen der Bestandsdatei aus dem Collector Ändern Sie diese Datei nicht.
2. Speichern Sie die Datei auf Ihrer lokalen Festplatte.

Führen Sie die folgenden Schritte aus, um die CSV- oder Collector-Datei hochzuladen.

Hinweis: Wenn Sie einen bereits vorhandenen Bestand ersetzen möchten, wählen Sie diesen Bestand im Datenfilter aus, bevor Sie fortfahren.

1. Wählen Sie den entsprechenden Importtyp aus (CSV-Dateiimport oder Import einer Collector-Datei).
2. Wählen Sie den aufgelisteten Bestand aus, der bereits vorhanden ist, oder klicken Sie auf **Neuen Bestand erstellen**.
3. Wenn Sie ein neues Inventar erstellt haben, geben Sie einen Namen in das entsprechende Feld ein.
4. Wählen Sie den Dateityp aus, den Sie hochladen möchten (Collector-generierte Datei oder CSV-Datei unter Verwendung der Vorlage).
5. Klicken Sie auf **Datei auswählen**, um die Datei auf Ihrem lokalen Desktop zu suchen.
6. Klicken Sie auf **Importieren**, um die Datei hochzuladen.

Die Seriennummer (SN) und die Produkt-ID müssen von Cisco als gültig anerkannt werden und den Daten in der Cisco Datenbank entsprechen, die Ihrem *berechtigten* Unternehmen zugeordnet sind. Wenn die Werte nicht als gültige Werte erkannt werden, wird das Element als solcher im Bericht über die Bestandsaufnahme angezeigt.

Hinweis: Sie können der CSV-Datei Geräte für spätere Uploads hinzufügen. Diese werden den zuvor hochgeladenen Geräten hinzugefügt. Um den Status einer importierten Datei zu überprüfen, klicken Sie in der Verwaltungsbibliothek auf **Upload Processing (Verarbeitung hochladen)**.

Tipp: Ausführliche Informationen zum Datei-Upload finden Sie im Video File Import Capability (Dateiimport-Funktion).

Löschen des Bestands

Mit diesem Bericht kann ein Kunde/CBR-Administrator einen Bestand aus der Kundenauswahl entfernen. Administratoren können mit diesem Bericht:

- Entfernen irrelevanter Bestände
- Reduzierung der Bestandsgröße durch Löschen alter Bestände

Hinweis Die Bestandslöschung kann nur von Kundenadministratoren und CBR-Administratoren vorgenommen werden. Die Kundenadministratoren können CBR-Administratoren über die Option Benutzer verwalten zur Verfügung stellen. Der Löschen des Inventars erfolgt nur aus der Kundenauswahl und nicht aus der Löschung der Datenbank. Wenn der Collector aktiv bleibt (registriert und hochgeladen), aktiviert er den Kundenbestand wieder in das Portal.

So löschen Sie ein Inventar:

1. Klicken Sie auf den gewünschten Bestand.
2. Klicken Sie auf **Aktionen > Bestandslöschung**. Ein Bestätigungsbildschirm wird angezeigt.
3. Klicken Sie auf **Bestätigen**, um den Bestand zu löschen.
4. Klicken Sie auf **Aktualisieren**, um die aktualisierte Liste des Bestands in diesem Bericht anzuzeigen.

Hinweis Aktualisieren Sie Ihren Browser, um die Änderungen im Portal anzuzeigen.

So zeigen Sie den Verlauf der Bestandslöschung an:

1. Klicken Sie auf **Aktionen > Verlauf der Bestandslöschung**.
2. Die Seite "Inventory Deletion History" (Verlauf der Bestandslöschung) wird mit der Liste der gelöschten Inventare angezeigt.
3. Klicken Sie auf **Schließen**, um die Seite zum Löschen des Bestands zu schließen.

So zeigen Sie die während der Sammlung wiederhergestellten Bestände an:

1. Klicken Sie auf **Aktionen**, **> Bestand mit neuer Sammlung wiederhergestellt**.
2. Die Seite "Inventory Restore with New Collection" (Mit neuer Sammlung wiederhergestellter Bestand) wird mit der Liste der wiederhergestellten Bestände angezeigt, wenn der CSPC während der automatischen Erfassung konfiguriert wird.
3. Klicken Sie auf **Schließen**, um die Seite Bestand mit der neuen Sammlung wiederherzustellen zu schließen.

Tipp: Ausführlichere Informationen zum Löschen des Inventars finden Sie im Video zum Löschen des Inventars.

Segment-Ausschlüsse

Im Bericht Segmentausschlüsse sind alle Geräte in einem Bestand aufgeführt, die nicht in einem Segment gruppiert sind. Dies ist besonders hilfreich, wenn Sie Segmente zur Gruppierung Ihrer Geräte verwenden.

Administratoren können das *Aktionen*-Menü im Segmentmanagement-Dashboard des Verwaltungs-Dashboards verwenden, um Segmente zu erstellen/zu bearbeiten, Zugriffsregeln einzurichten und die nicht segmentierten Geräte in bestimmte Segmente zu unterteilen.

Mit diesem Bericht können Administratoren die Geräte ermitteln, die nicht in einem Segment

gruppiert sind, und entsprechende Maßnahmen ergreifen.

Warnungen

Die Berichte in diesem Katalog beziehen sich auf die vom Portal bereitgestellten Warnmeldungen. Um Netzwerkunterbrechungen vorzubeugen und Sicherheitslücken zu minimieren, können Sie Warnmeldungen identifizieren und proaktiv auf diese reagieren, die sich auf die Geräte in Ihrem Netzwerk auswirken.

Mit einem aktiven Warnbericht können Sie:

- Schnelle Ermittlung der Geräte, die für Bedrohungen anfällig sind
- Identifizierung der Geräte, für die Software-Updates erforderlich sind
- Überprüfung Ihrer Maßnahmen zur Behebung von Warnmeldungen

Im Folgenden werden die Warnungen aufgeführt, die sich auf die Geräte in Ihrem Netzwerk auswirken können:

- Hardware-Warnmeldungen informieren Sie über EoL-Probleme (End-of-Life) bei den Geräten in Ihrem Netzwerk.
- Software-Warnmeldungen informieren Sie über EoL-Probleme mit den Softwareversionen, die Sie in Ihrem Netzwerk verwenden.
- Sicherheitswarnungen informieren Sie über Sicherheitsschwachstellen, die mit bestimmten Geräten in Ihrem Netzwerk verbunden sind.
- Hardware Field Notices (FNs) informieren Sie über andere wichtige Probleme (abgesehen von Sicherheitslücken) mit einem Hardware-Gerät. Ein Hardware-FN erfordert häufig Kundenaktionen, wie z. B. eine Retourengenehmigung (Return Material Authorization, RMA).
- Software-FNs informieren Sie über andere wichtige Probleme (abgesehen von Sicherheitslücken) mit einer Softwareversion, die Sie in Ihrem Netzwerk verwenden. Ein Software-FN erfordert häufig auch Kundenaktionen.

Bei der SNTC-Warnmeldung werden Hardware- und Softwareversionen, IOS und die aktuelle Konfiguration von Geräten berücksichtigt, sobald diese Informationen verfügbar sind, um den Grad der Schwachstelle (Anfällig, Potenziell anfällig usw.) zu ermitteln. Diese Berichte helfen Netzwerkadministratoren und -technikern, sich auf die wichtigsten Warnmeldungen und FNs zu konzentrieren, wodurch die Betriebseffizienz und das Risikomanagement verbessert werden.

> **Tipp**: Weitere Informationen zu Warnmeldungen finden Sie im Video Alert Prioritization oder Alert Administration.

Alle Warnungen

Im Bericht "Alle Warnungen" werden die Produktwarnungen für die ausgewählten Aufstellungen nach Typ kategorisiert. Sie können diesen Bericht verwenden, um:

- Ändern Sie den Status einer Warnung von *Ignore* in *Active (Aktiv)*.
- Überprüfen Sie die Warnungen anhand der Anzahl der betroffenen Geräte, oder sortieren Sie sie nach Status.

Um Warnungen anzuzeigen, die sich auf die maximale Anzahl von Geräten auswirken, klicken Sie auf die Spaltenüberschrift **Affected Devices** (Betroffene Geräte), sodass der Pfeil nach unten zeigt.

Dadurch werden die Informationen in absteigender Reihenfolge sortiert.

Um die von Cisco veröffentlichte Warnmeldungsbeschreibung anzuzeigen, klicken Sie in der Spalte *Weitere Informationen* auf die URL für die gewünschte Alert-Zeile.

Um den Warnstatus, Notizen und die Möglichkeit zur Sortierung nach Status anzuzeigen, deaktivieren Sie die Spalten *Status* und *Hinweise* (sofern sie standardmäßig nicht sichtbar sind).

Gehen Sie wie folgt vor, um den Warnstatus von *Ignore* auf *Active* zu ändern:

1. Aktivieren Sie das entsprechende Kontrollkästchen für jede Warnung, die Sie ändern möchten.
2. Klicken Sie auf **Aktionen** und dann auf **Warnstatus ändern**. Der *aktive* Status ist standardmäßig ausgewählt.
3. Geben Sie im Feld *Hinweise* einen Hinweis ein. (Dieser Schritt ist optional.)

Hinweis: Diese Aufgabe kann nur von Administratoren und Benutzern mit Warnmeldungsverwaltungsberechtigungen ausgeführt werden.

Das Menü Aktionen in diesem Bericht kann nicht verwendet werden, um den Status von Aktiv in Ignorieren zu ändern. Wenn Sie Zugriff auf die Administratorberichte haben, navigieren Sie zu **Library > Administration > Active Alerts** und ändern Sie den Status von Active (Aktiv) in Ignorieren. Wenden Sie sich andernfalls an den Kundenadministrator in Ihrem Unternehmen.

Hinweis: Nachdem Sie für eine bestimmte Warnung Aktionen an allen betroffenen Geräten durchgeführt haben, wird der Status *Bestätigen*.

Alle Problemhinweise

Im Bericht "All Field Notices" werden die Hardware- und Software-FNs für die ausgewählten Bestände nach Typ kategorisiert. Sie können diesen Bericht verwenden, um:

- Ändern Sie den Status eines FN von *Ignore* in *Active (Aktiv)*.
- Überprüfung von FNs auf der Grundlage:
  - Die Anzahl der betroffenen Geräte
  - Schwachstellenbewertung von FNs

Um die FNs anzuzeigen, die sich auf die maximale Anzahl von Geräten auswirken, klicken Sie auf die Spaltenüberschrift **Affected Devices** (Betroffene Geräte), sodass der Pfeil nach unten zeigt. Dadurch werden die Informationen in absteigender Reihenfolge sortiert.

Um die von Cisco veröffentlichte FN-Beschreibung anzuzeigen, klicken Sie in der Spalte *Weitere Informationen* auf die URL für die gewünschte Zeile.

Um den FN-Status und die Notizen anzuzeigen, deaktivieren Sie die Spalten *Status* und *Notes* (sofern diese standardmäßig nicht sichtbar sind).

Gehen Sie wie folgt vor, um den FN-Status von *Ignore* auf *Active* zu ändern:

1. Klicken Sie auf die entsprechenden Kontrollkästchen für die FNs, die Sie ändern möchten.
2. Klicken Sie auf **Aktionen** und dann auf **Warnstatus ändern**. Der *aktive* Status ist standardmäßig ausgewählt.
3. Geben Sie einen Hinweis in das Feld *Notizen ein*. (Dieser Schritt ist optional.)

Hinweis: Diese Aufgabe kann nur von Administratoren und Benutzern ausgeführt werden, die über die Berechtigung für das Warnmanagement verfügen.

Hinweis: Nachdem Sie für ein bestimmtes FN Maßnahmen auf allen betroffenen Geräten ergriffen haben, wird der Status *Bestätigung*.

Das Menü Aktionen in diesem Bericht kann nicht verwendet werden, um den Status von Aktiv in Ignorieren zu ändern. Wenn Sie Zugriff auf die Administratorberichte haben, navigieren Sie zu **Library > Administration > Active Alerts**, und ändern Sie den Status von Active (Aktiv) in Ignorieren. Andernfalls wenden Sie sich an den Smart Net Total Care-Administrator in Ihrer Organisation.

Alle Hardwarewarnungen

Im Bericht "Alle Hardware-Warnungen" werden die Hardware-Warnungen für die ausgewählten Inventare nach Typ kategorisiert. Sie können diesen Bericht verwenden, um:

- Ändern Sie den Status einer Warnung von *Ignore* in *Active (Aktiv)*.
- Überprüfen Sie die Warnmeldungen anhand der folgenden Kriterien:
  - Die Anzahl der betroffenen Geräte
  - Der LDoS für die Gerätehardware (falls veröffentlicht)

Um Warnungen anzuzeigen, die sich auf die maximale Anzahl von Geräten auswirken, klicken Sie auf die Spaltenüberschrift **Affected Devices** (Betroffene Geräte), sodass der Pfeil nach unten zeigt. Dadurch werden die Informationen in absteigender Reihenfolge sortiert.

Um die von Cisco veröffentlichte Warnmeldungsbeschreibung anzuzeigen, klicken Sie in der Spalte *Weitere Informationen* auf die URL für die gewünschte Zeile.

Um den Status und die Notizen der Warnmeldungen anzuzeigen, deaktivieren Sie die Spalten *Status* und *Hinweise* (sofern diese standardmäßig nicht sichtbar sind).

Gehen Sie wie folgt vor, um den Warnstatus von *Ignore* auf *Active* zu ändern:

1. Klicken Sie für jede Warnung, die Sie ändern möchten, auf die entsprechenden Kontrollkästchen.
2. Klicken Sie auf **Aktionen** und dann auf **Warnstatus ändern**. Der *aktive* Status ist standardmäßig ausgewählt.
3. Geben Sie einen Hinweis in das Feld *Notizen ein*. (Dieser Schritt ist optional.)

Hinweis: Nachdem Sie für eine bestimmte Warnmeldung auf allen betroffenen Geräten Maßnahmen ergriffen haben, wird der Status *Bestätigung*.

Hinweis: Diese Aufgabe kann nur von Administratoren und Benutzern ausgeführt werden, die über die Berechtigung für das Warnmanagement verfügen.

Das Menü Aktionen in diesem Bericht kann nicht verwendet werden, um den Status von Aktiv in Ignorieren zu ändern. Wenn Sie Zugriff auf die Administratorberichte haben, navigieren Sie zu **Library > Administration > Active Alerts**, und ändern Sie dann den Status von *Active (Aktiv)* in *Ignorieren*. Andernfalls wenden Sie sich an den Smart Net Total Care-Administrator in Ihrer

Organisation.

Alle Sicherheitsempfehlungen (PSIRTs)

> **Hinweis**: In diesem Bericht werden nur die Ratgeber des High and Critical Product Security Incident Response Team (PSIRT) angezeigt.

Im Bericht All Security Advisories (PSIRTs) werden die PSIRT-Ratgeber aufgelistet, die nach Typ kategorisiert sind, für die ausgewählten Inventare. Die PSIRTs sind nur für Geräte verfügbar, auf denen diese Betriebssysteme ausgeführt werden:

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

Sie können diesen Bericht verwenden, um:

- Ändern Sie den Status eines PSIRT von *Ignore* in *Active (Aktiv)*.
- Überprüfung von Warnmeldungen auf der Grundlage von:
  - Die Anzahl der betroffenen Geräte
  - Die Schwachstellenbewertung von PSIRTs
- Zeigen Sie die Security Impact Rating (SIR) auf Basis des CVSS-Scores (Common Vulnerability Scoring System) an. Cisco setzt die Security Impact Rating (SIR) ein, um den Schweregrad von Sicherheitslücken einfacher zu kategorisieren. Die SIR basieren auf der CVSS Qualitative Severity Rating Scale des Basisscore, können vom PSIRT entsprechend der Cisco spezifischen Variablen angepasst werden und sind in jeder Cisco Security Advisory enthalten.

Um die PSIRTs anzuzeigen, die die maximale Anzahl von Geräten betreffen, klicken Sie auf die Spaltenüberschrift **Affected Devices** (Betroffene Geräte), sodass der Pfeil nach unten zeigt. Dadurch werden die Informationen in absteigender Reihenfolge sortiert.

Um die von Cisco veröffentlichte PSIRT-Beschreibung anzuzeigen, klicken Sie in der Spalte *Weitere Informationen* auf die URL für die gewünschte Zeile.

Um den PSIRT-Status und die Notizen anzuzeigen, deaktivieren Sie die Spalten *Status* und *Notizen* (sofern diese standardmäßig nicht sichtbar sind).

Gehen Sie wie folgt vor, um den PSIRT-Status von *Ignore* in *Active* zu ändern:

1. Klicken Sie auf die entsprechenden Kontrollkästchen für die einzelnen PSIRTs, die Sie ändern möchten.
2. Klicken Sie auf **Aktionen** und dann auf **Warnstatus ändern**. Der *aktive* Status ist standardmäßig ausgewählt.
3. Geben Sie einen Hinweis in das Feld *Notizen ein*. (Dieser Schritt ist optional.)

> **Hinweis**: Diese Aufgabe kann nur von Administratoren und Benutzern ausgeführt werden, die über die Berechtigung für das Warnmanagement verfügen.

Hinweis: Nachdem Sie für eine bestimmte Warnmeldung auf allen betroffenen Geräten Maßnahmen ergriffen haben, wird der Status *Bestätigung*.

Das Menü Aktionen in diesem Bericht kann nicht verwendet werden, um den Status von Aktiv in Ignorieren zu ändern. Wenn Sie Zugriff auf die Administratorberichte haben, navigieren Sie zu **Library > Administration > Active Alerts**, und ändern Sie dann den Status von *Active (Aktiv)* in *Ignorieren*. Andernfalls wenden Sie sich an den Smart Net Total Care-Administrator in Ihrer Organisation.

Alle Software-Warnungen

Im Bericht All Software Alerts (Alle Software-Alerts) werden Software-Alerts für die ausgewählten Inventare nach Typ kategorisiert. Sie können diesen Bericht verwenden, um:

- Ändern Sie den Status einer Warnung von *Ignore* in *Active (Aktiv)*.
- Überprüfung von Warnmeldungen auf der Grundlage von:
  - Die Anzahl der betroffenen Geräte
  - Der LDoS für die Gerätesoftware (falls veröffentlicht)

Um Warnungen anzuzeigen, die sich auf die maximale Anzahl von Geräten auswirken, klicken Sie auf die Spaltenüberschrift **Affected Devices** (Betroffene Geräte), sodass der Pfeil nach unten zeigt. Dadurch werden die Informationen in absteigender Reihenfolge sortiert.

Um die von Cisco veröffentlichte Warnmeldungsbeschreibung anzuzeigen, klicken Sie in der Spalte *Weitere Informationen* auf die URL für die gewünschte Zeile.

Um den Warnstatus und die Notizen anzuzeigen, deaktivieren Sie die Spalten *Status* und *Anmerkungen* (sofern diese standardmäßig nicht sichtbar sind).

Gehen Sie wie folgt vor, um den Warnstatus von *Ignore* auf *Active* zu ändern:

1. Klicken Sie für jede Warnung, die Sie ändern möchten, auf die entsprechenden Kontrollkästchen.
2. Klicken Sie auf **Aktionen** und dann auf **Warnstatus ändern**. Der *aktive* Status ist standardmäßig ausgewählt.
3. Geben Sie einen Hinweis in das Feld *Notizen ein*. (Dieser Schritt ist optional.)

Hinweis: Diese Aufgabe kann nur von Administratoren und Benutzern ausgeführt werden, die über die Berechtigung für das Warnmanagement verfügen.

Hinweis: Nachdem Sie für eine bestimmte Warnmeldung auf allen betroffenen Geräten Maßnahmen ergriffen haben, wird der Status *Bestätigung*.

Das Menü Aktionen in diesem Bericht kann nicht verwendet werden, um den Status von Aktiv in Ignorieren zu ändern. Wenn Sie Zugriff auf die Administratorberichte haben, navigieren Sie zu **Library > Administration > Active Alerts**, und ändern Sie dann den Status von *Active* to *Ignore*. Andernfalls wenden Sie sich an den Smart Net Total Care-Administrator in Ihrer Organisation.

Geräte mit Warnmeldungen

Der Bericht "Devices with Alerts" (Geräte mit Warnmeldungen) enthält eine Warnmeldung für

jeden Warnungstyp für jedes Gerät in den ausgewählten Inventaren.

Um die eindeutigen Warnmeldungen für ein Gerät anzuzeigen, klicken Sie unter jeder Spalte für den Warnungstyp auf den Link Nummer.

Letzter Support-Tag

Im Bericht "Last Day of Support" (Letzter Tag des Supports) werden alle Geräte (in den ausgewählten Beständen) aufgelistet, für die der veröffentlichte LDoS für die Gerätehardware innerhalb der nächsten zwei Jahre oder nach dem aktuellen Datum vorliegt.

Dieser Bericht ermöglicht Netzwerkadministratoren und Vertragsadministratoren die proaktive Planung für aktuelle oder zukünftige Änderungen der Geräteverfügbarkeit, wodurch die Betriebseffizienz erhöht und das Risikomanagement verbessert wird.

Um den Datumsbereich in der Spalte "Last Date of Support" (Letztes Datum der Unterstützung) zu ändern, klicken Sie unter der Überschrift "*Last Date of Support" (Letztes Datum der Unterstützung) auf das Suchfeld* und geben Sie mithilfe der Funktion zur Suche des Datums einen Datumsbereich ein.

Gehen Sie wie folgt vor, um den LDoS-Datensatz für ein bestimmtes Gerät anzuzeigen:

1. Klicken Sie unter der Spaltenüberschrift *Seriennummer* auf das Suchfeld und geben Sie die Geräte-SN ein.
2. Drücken Sie **die Eingabetaste**.

Wenn keine Datensätze angezeigt werden, befindet sich der LDoS der Gerätehardware nicht innerhalb der nächsten zwei Jahre.

Um die LDoS-Warnung anzuzeigen, klicken Sie auf den Link, der dem Gerät in der Spalte *Alert URL* entspricht.

Gehen Sie wie folgt vor, um die Vertragsdetails für ein Gerät anzuzeigen:

1. Blättern Sie im Bericht horizontal, bis die Spalte *Vertragsnummer* sichtbar wird.
2. Klicken Sie auf die URL, die dem gewünschten Gerät entspricht. Wenn der Wert für die Vertragsnummer *Andere* oder *Partner-Markenverträge* ist, sind Sie nicht berechtigt, auf die Details zuzugreifen.

Gehen Sie wie folgt vor, um Hinweise zu aktualisieren:

1. Aktivieren Sie die Kontrollkästchen für die gewünschten Geräte.
2. Klicken Sie auf **Aktionen > LDOS-Hinweise angeben**. Die Seite "LDOS Notes angeben" wird angezeigt.
3. Geben Sie die entsprechenden Anmerkungen in das Textfeld ein.
4. Klicken Sie auf **OK**, um die Notizen zu speichern.

Hinweis: Aktualisieren Sie Ihren Browser, um die Änderungen im Portal anzuzeigen.

Sie können auch mehrere Geräte auswählen und LDOS-Notizen angeben. Alternativ können Sie die erforderlichen Spalten filtern und LDOS-Anmerkungen angeben. Filtern Sie z. B. den Gerätetyp mit CHASSIS, um die entsprechenden Geräte aufzulisten. Wählen Sie im Menü **Aktionen** die Option **LDOS-Notizen angeben aus**.

Tipp: Weitere Informationen zu LDoS finden Sie im Video "Abdeckungslücken".

Produktbenachrichtigungen - Delta

Der Product Alerts Delta-Bericht zeigt die neuen oder geänderten Warnungen (jedes Typs) für einen bestimmten Bestand über einen bestimmten Zeitraum an. Die Warnmeldungen in diesem Bericht sind wie folgt:

- **Neue Warnmeldungen**: In diesem Bereich des Berichts wird die Anzahl der Warnmeldungen angezeigt, die zwischen dem Start- und dem Enddatum hinzugefügt wurden.
- **Geänderte Warnmeldungen** - In diesem Bereich des Berichts wird die Anzahl der Warnungen angegeben, die zwischen dem Start- und dem Enddatum geändert wurden.

  Hinweis: Wenn dieselbe Warnmeldung beim nachfolgenden Upload geändert wird, wird die neue Warnmeldung als 0 (null) markiert und der geänderten Warnungszahl hinzugefügt.

- **Gesamtwarnungen wie am <End_Date>** - Dieser Bereich des Berichts gibt die Gesamtanzahl der Warnungen (jedes Typs) an, die in der Datenbank für das ausgewählte Enddatum verfügbar sind. Dazu gehören die neuen Warnmeldungen, die geänderten Warnungen und die nicht geänderten alten Warnungen.

Gehen Sie wie folgt vor, um den Datumsbereich zu ändern:

1. Wählen Sie im Popup-Kalender für den gewünschten Zeitraum ein Startdatum aus.
2. Wählen Sie im Popup-Kalender *Enddatum* das Enddatum für den gewünschten Zeitraum aus. Dieses Datum muss nach dem Startdatum liegen.
3. Klicken Sie zur Bestätigung auf **OK**.

Um eine Liste der Geräte für jede Kategorie anzuzeigen, klicken Sie unter der Spalte *"Neue Warnungen*" oder "*Geänderte Warnungen" auf die* Nummern.

Der Standardzeitraum für diesen Bericht beträgt 90 Tage. Führen Sie die folgenden Schritte aus, um den Standardzeitraum zu ändern:

1. Klicken Sie auf das Zahnrad-Symbol.
2. Wählen Sie **Zeitrahmen festlegen aus**.
3. Ändern Sie den Zeitrahmen nach Bedarf.

Verträge

Die Berichte in dieser Bibliothek enthalten Informationen zu den Serviceverträgen Ihres Unternehmens mit Cisco.

Alle Verträge

Der Bericht All Contracts (Alle Verträge) enthält umfassende Details zu allen Serviceverträgen, Geräten im Rahmen der Verträge sowie zum Vertragsstatus. Dieser Bericht umfasst folgende Aufgaben:

- Identifizieren Sie Abdeckungslücken und die damit verbundenen Risiken im Netzwerk.
- Alle zukünftigen Ablaufdaten anzeigen.
- Zeigen Sie die Vertragsdetails an.
- Zeigen Sie die Geräte an, die den einzelnen Verträgen zugeordnet sind.

Die Vertragsadministratoren können diesen Bericht verwenden, um von der Support-Perspektive aus einen umfassenden Überblick über ihr Netzwerk zu erhalten, was zur Verbesserung der betrieblichen Effizienz und des Risikomanagements beiträgt.

Weitere Informationen zum Bericht Alle Verträge finden Sie in den folgenden Videos:

- Vertragsdetails
- Zugriff auf Informationen zur Serviceabdeckung
- Abdeckungslücken
- Abdeckung läuft aus
- Zugriff auf Serviceverträge

Abgedeckt

Im Bericht "Abgedeckt" werden die Geräte (in den ausgewählten Beständen) aufgeführt, die durch einen oder mehrere gültige Cisco Serviceverträge abgedeckt sind. Dieser Bericht umfasst folgende Aufgaben:

- Zeigen Sie die Geräte und die zugehörigen Verträge an.
- Zeigen Sie das LDoS für ein Gerät an (falls veröffentlicht).
- Zeigen Sie die Vertragsdetails an.
- Festlegen von Abdeckungsaktionen, einschließlich zusätzlicher Kommentare
- Möglichkeit zum Anfordern von Änderungen an Informationen zu installierten Standorten innerhalb des Portals durch den Kundenadministrator und einen beliebigen Benutzer mit Zugriffsberechtigung.

Die Vertragsadministratoren können diesen Bericht verwenden, um die Verträge anzuzeigen, die den verschiedenen Geräten in ihrem Netzwerk zugeordnet sind, und Abdeckungsaktionen mit Kommentaren festzulegen, wodurch die Betriebseffizienz und das Risikomanagement verbessert werden.

So geben Sie den Verlauf der Abdeckungsaktion an:

1. Aktivieren Sie das Kontrollkästchen für jede Vertragszeile, für die Sie die Abdeckungsaktion angeben möchten.
2. Klicken Sie auf **Aktionen > Abdeckungsaktion angeben**. Der Bildschirm Abdeckungsaktion angeben wird angezeigt.
3. Wählen Sie den entsprechenden Grund aus der Liste aus.
4. Geben Sie im Feld **Hinweise** einen Hinweis ein. (Dieser Schritt ist optional.)
5. Klicken Sie auf **OK**.

So zeigen Sie den Verlauf der Abdeckungsaktion an:

1. Aktivieren Sie das Kontrollkästchen für jede Vertragszeile, die Sie die Abdeckungsaktion überprüfen möchten.
2. Klicken Sie auf **Aktionen > Abdeckungsaktionsprotokoll anzeigen**. Der Bildschirm

Abdeckungsaktion wird angezeigt.

So zeigen Sie die Anforderung der Update Installed-at-Site an:

1. Aktivieren Sie das Kontrollkästchen für jede Vertragszeile, die Sie die Abdeckungsaktion überprüfen möchten.
2. Klicken Sie auf **Aktionen > Installationsstandort aktualisieren**. Der Bildschirm Update Installed-at-Site wird angezeigt.
3. Wählen Sie die entsprechende Option aus:
   - Wählen Sie Installed-at-Site aus, um eine Installation hinzuzufügen/zu aktualisieren. Durchsuchen Sie die erforderlichen Details im Textfeld.
   - Um eine neue Installation am Standort zu erstellen, wählen Sie Neu installiert am Standort aus. Geben Sie die erforderlichen Informationen zum neuen Standort ein.
4. Klicken Sie auf Aktualisieren, um die Informationen zum Installationsstandort zu aktualisieren.

Hinweis: Updates können bis zu 72 Stunden in Anspruch nehmen. Die Änderungen werden von Cisco im Rahmen des Standardverfahrens vorgenommen.

So überprüfen Sie die ausstehende Anforderung für die ausgewählten Geräte:

1. Aktivieren Sie das Kontrollkästchen für jede Vertragszeile, die Sie die Abdeckungsaktion überprüfen möchten.
2. Klicken Sie auf **Aktionen > Website-Info-Verlauf anzeigen**. Die Seite Website-Info-Verlauf anzeigen wird angezeigt.

So zeigen Sie den Status der Massenaktion an:

1. Aktivieren Sie das Kontrollkästchen für jede Vertragszeile, die Sie den Status der Abdeckungsaktion anzeigen möchten.
2. Klicken Sie auf **Aktionen > Status der Massenaktion**. Der Bildschirm "Bulk Action Status" wird angezeigt.

Weitere Informationen zu diesem Bericht finden Sie in den folgenden Videos:

- Vertragsdetails
- Zugriff auf Informationen zur Serviceabdeckung
- Abdeckungslücken
- Abdeckung läuft aus
- Zugriff auf Serviceverträge

Nicht abgedeckt

Der Bericht "Nicht abgedeckt" listet die Geräte in den ausgewählten Beständen auf, die derzeit nicht durch einen Servicevertrag abgedeckt sind. Sie können das Menü Aktionen verwenden, um alle erforderlichen Abdeckungsaktionen zu kommentieren und so den Bericht zu bereinigen.

Die Vertragsadministratoren können diesen Bericht verwenden, um die Geräte im Netzwerk anzuzeigen, für die eine Serviceabdeckung erforderlich sein könnte, was die Betriebseffizienz und das Risikomanagement verbessert.

So geben Sie die gewünschte Abdeckungsaktion an:

1. Aktivieren Sie das Kontrollkästchen für jede Gerätezeile, für die Sie die Abdeckungsaktion angeben möchten.
2. Klicken Sie auf **Aktionen > Abdeckungsaktion angeben**. Der Bildschirm Abdeckungsaktion angeben wird angezeigt.
3. Wählen Sie den entsprechenden Grund aus der Liste aus.
   - Erforderliche Überprüfung
   - Gesichert
   - Abdeckung
   - Verlängerungsabdeckung
   - Ersatzteil, nicht zur Abdeckung
   - Ersatz geplant
   - Stillgelegt
   - Keine Abdeckung erforderlich
4. [Optional] Geben Sie im Feld **Kommentare** einen Hinweis ein.
5. Klicken Sie auf **OK**

Nach der Verarbeitung können Sie den Bericht filtern, um sich auf bestimmte erforderliche oder nicht abgedeckte Aktionen zu konzentrieren.

Weitere Informationen zu diesem Bericht finden Sie in den folgenden Videos:

- Zugriff auf Informationen zur Serviceabdeckung
- Abdeckungslücken
- Zugriff auf Serviceverträge

Auslaufende Geräteabdeckung

Im Bericht über die auslaufende Geräteabdeckung werden die Geräte aufgelistet, deren Abdeckungsenddatum nahe ist. Standardmäßig werden die Geräte nach Enddatum der Abdeckung sortiert. Dieser Bericht umfasst folgende Aufgaben:

- Rufen Sie eine Liste der Geräte ab, für die der Servicevertrag demnächst abläuft.
- Zeigen Sie die Vertragsdetails an.

Dieser Bericht hilft Vertragsadministratoren, die Geräteabdeckung zeitnah zu verlängern, wodurch die Betriebseffizienz und das Risikomanagement verbessert werden.

> **Tipp**: Um die Geräte nach Gerätetyp, Abdeckungsstatus oder anderen Kategorien zu sortieren, klicken Sie auf das Diagrammsymbol.

Weitere Informationen zu diesem Bericht finden Sie in den folgenden Videos:

- Vertragsdetails
- Zugriff auf Informationen zur Serviceabdeckung
- Abdeckungslücken
- Abdeckung läuft aus
- Zugriff auf Serviceverträge

Geräte mit mehreren Verträgen

Im Bericht Geräte mit mehreren Verträgen werden die Geräte (in den ausgewählten Beständen) aufgeführt, die durch mehr als einen Servicevertrag abgedeckt sind.

> **Tipp**: Um die Geräte nach Gerätetyp, Abdeckungsstatus oder anderen Kategorien zu sortieren, klicken Sie auf das Diagrammsymbol.

> **Hinweis**: Wenn der Wert für die Vertragsnummer *Andere* oder *Partner-Markenverträge* ist, sind Sie nicht berechtigt, auf die Details zuzugreifen.

Weitere Informationen zu diesem Bericht finden Sie in den folgenden Videos:

- Vertragsdetails
- Zugriff auf Informationen zur Serviceabdeckung
- Abdeckungslücken
- Abdeckung läuft aus
- Zugriff auf Serviceverträge

Vorfälle

Ihre Interaktionen mit dem Cisco Technical Assistance Center (TAC) sind im Incidents Report enthalten.

Alle Support-Tickets für die letzten 90 Tage

Im Bericht All Support Cases (Alle Support-Fälle) sind die Serviceanfragen aufgeführt, die Sie (der angemeldete Benutzer) innerhalb der letzten 90 Tage beim Cisco TAC gemeldet haben (für die ausgewählten Bestände und Kunden).

Dieser Bericht bietet Einblick in alle offenen TAC-Fälle in einem Bericht. So können Netzwerkadministratoren und Netzwerktechniker Risiken effizienter verwalten.

> **Hinweis**: Im SNTC-Portal werden nur aus dem SNTC-Portal erstellte Fälle aufgelistet. Es werden keine Tickets angezeigt, die aus anderen Portalen wie Support Case Manager usw. erstellt wurden.

Bestand

Die in dieser Bibliothek enthaltenen Berichte bieten einen umfassenden Überblick über Ihre installierten Cisco Geräte und Konfigurationsdetails wie SNs, Produkt-IDs (PIDs), Betriebssystemversionen, installierten Speicher und Firmware, IP-Adressen und Hostnamen. Mithilfe dieser Informationen können Sie folgende Aufgaben durchführen:

- Identifizieren Sie die Cisco Produkte, die bald die EoL-, End-of-Sale- (EoS) oder LDoS-Zertifizierung erreichen werden.
- Zeigen Sie die Daten an, die in Ihrem Netzwerk verschoben, hinzugefügt oder geändert wurden.
- Überprüfen Sie, ob Ihre Cisco Hardware die aktuellsten und unterstützten Softwareversionen

ausführt.
- Planen Sie Upgrades für die Geräte, die nicht mehr unterstützt werden.

Mithilfe dieser Berichte können Netzwerkadministratoren und -techniker Details zu allen Geräten im Netzwerk und den Abdeckungsstatus anzeigen und so die betriebliche Effizienz und das Risikomanagement verbessern.

Weitere Informationen zu den Bestandsberichten finden Sie in den folgenden Videos:

- Siehe Bestandsgeräte
- Bestandserfassungs-Delta

Zusammenfassung

Der zusammenfassende Bericht listet die Gesamtzahl der Chassis, Module, Netzteile, Lüfter und anderen Geräte im Bestand auf, basierend auf verschiedenen Kategorien wie Vertragsabdeckung und LDoS-Aufzeichnungen. Halten Sie Ihre Bestände auf dem neuesten Stand und präzise, damit Sie einen umfassenden Überblick über die Geräte in Ihrem Netzwerk haben.

Der zusammenfassende Bericht bietet Ihnen folgende Vorteile:

1. Eine Zusammenfassung der Geräte in Ihrem Netzwerk
2. Identifizieren der abgedeckten und nicht abgedeckten Geräte
3. Überprüfen der Support-Daten am letzten Tag

Diese Informationen sind im zusammenfassenden Bericht verfügbar:

- **Geräte im Inventar (alle Quellen)** - In diesem Abschnitt werden alle Geräte im Bestandssystem aufgeführt.
- **Collected Devices** (Erfasste **Geräte**) - In diesem Abschnitt des Berichts werden die Services aufgelistet, die über einen Collector (z. B. CSPC) im Bestandssystem abgerufen wurden.
- **Importierte Geräte** - Dieser Abschnitt listet die Geräte auf, die manuell durch CSV-Upload in das Bestandssystem eingegeben wurden.
- **Erkannte Geräte** - In diesem Abschnitt werden die vom System erkannten Services aufgelistet, da ihre SN in den Cisco Fertigungsdatenbanken vorhanden sind.
- **Abgedeckte Geräte** - In diesem Abschnitt werden die erkannten Geräte aufgeführt, die durch einen gültigen Servicevertrag abgedeckt sind.
- **Nicht abgedeckte Geräte** - In diesem Abschnitt werden die erkannten Geräte aufgeführt, die nicht durch einen gültigen Servicevertrag abgedeckt sind.
- **Vergangene LDoS** - Dieser Abschnitt listet die Geräte auf, für die der LDoS erreicht wurde.
- **LDoS innerhalb von 12 Monaten** - In diesem Abschnitt werden die Geräte aufgelistet, für die das LDoS innerhalb der nächsten 12 Monate verfügbar ist.
- **LDoS über 12 Monate und innerhalb von 24 Monaten** - In diesem Abschnitt werden die Geräte aufgeführt, für die das LDoS zwischen 13 und 24 Monaten ab dem aktuellen Tag liegt.

> **Tipp**: Klicken Sie zum Anzeigen der Gerätedetails unter der gewünschten Kategorie und dem Gerätetyp auf den Link Nummer.

Alle Geräte

Im Bericht All Equipment (Alle Geräte) sind alle Geräte mit dem Gerätetyp (z. B. Chassis, Module, Netzteil und Lüfter) für die ausgewählten Bestände aufgeführt. Dieser Bericht umfasst folgende Aufgaben:

- Zeigen Sie eine Zusammenfassung der Geräte an, die durch Erfassung oder Dateiimport erkannt werden.
- Erstellen Sie angepasste Bestandsberichte aus angegebenen Daten.

> **Hinweis**: Wenn beim Hochladen des Bestands keine IP-Adresse für ein Gerät eingeht, lautet das Feld *IP-Adresse* "—".

Sie können auf den gewünschten Link unter Hostname klicken, um die Gerätedetails anzuzeigen.

Gehen Sie wie folgt vor, um ein Support-Ticket zu erstellen:

1. Aktivieren Sie das Kontrollkästchen neben dem Gerät, für das Sie ein Support-Ticket erstellen möchten.
2. Klicken Sie auf **Aktionen** und dann auf **Support-Fälle erstellen**.

Bestandsduplikate

Der Bericht "Inventory Duplicates" enthält Details zu Geräten, die in mehr als einem Bestand enthalten sind.

Um die Gerätedetails anzuzeigen, klicken Sie unter *Hostname* auf den gewünschten Link.

> **Hinweis**: Wenn beim Hochladen des Bestands keine IP-Adresse für ein Gerät eingeht, lautet das Feld *IP-Adresse* "—".

Bestand nach Produkt

Der Bericht Inventory by Product (Bestand nach Produkt) enthält einen Bestandsbericht, der sortiert und nach Produkt-ID (PID) gruppiert ist. Dieser Bericht umfasst folgende Aufgaben:

- Zeigen Sie eine Zusammenfassung der bereitgestellten Geräte an, die nach PID sortiert ist.
- Geben Sie anhand der PID die Anzahl der Produkte und deren Abdeckungsstatus an.
- Zeigen Sie das LDoS für die Geräte an. Der LDoS wird nur angezeigt, wenn der LDoS das aktuelle (System-)Datum überschreitet.

Um die Gerätedetails anzuzeigen, klicken Sie unter *"Abgedeckt und nicht abgedeckt"* auf den Link Nummer.

Um die von Cisco festgelegten Warnmeldungen anzuzeigen, klicken Sie unter *Alert URL* auf die gewünschte URL.

Bestandserfassungs-Delta

Der Delta-Bericht über die Bestandserfassung zeigt die Änderungen an, die in Ihren Netzwerkgeräten für einen festgelegten Zeitraum vorgenommen wurden. Diese Informationen sind nützlich, wenn Sie die Berichtspräferenz auf eine *umfassende Ansicht* in den Portalanwendungseinstellungen festlegen. Dieser Bericht umfasst folgende Aufgaben:

- Zeigen Sie die Anzahl der Geräte an, die für zwei Uploads hinzugefügt, gelöscht oder geändert wurden.
- Kategorisieren Sie die Änderungen je nach Gerätetyp.
- Zeigen Sie die Details der ausgewählten Geräte an.

> **Hinweis**: Sie müssen nur einen Bestand auswählen, um diesen Bericht verwenden zu können.

Im Berichtsprofil werden Datum und Uhrzeit des Uploads für jeden Snapshot, der Collector, von dem der Bestand hochgeladen wurde, und die Gesamtzahl der Geräte angegeben, die in jedem Bestand hochgeladen und importiert wurden.

Um die Details der geänderten Geräte anzuzeigen, klicken Sie auf den nummerierten Link für eines der Geräte.

> **Tipp**: Weitere Informationen zum Delta-Bericht über die Bestandserfassung finden Sie im Video Inventory Collection Delta.

Bestand nach Standorten

Der Bericht Inventory by Sites (Bestand nach Standorten) zeigt die Details des Installationsstandorts für die Geräte im Bestand an. Dieser Bericht enthält die eindeutige ID für den installierten Standort, die Adresse und den Kunden für die einzelnen identifizierten Standorte.

Sie können diesen Bericht verwenden, um die Anzahl der Geräte an jedem Standort anzuzeigen, die durch einen Cisco Servicevertrag abgedeckt sind oder nicht abgedeckt sind.

> **Hinweis**: Wenn beim Hochladen des Bestands keine IP-Adresse für ein Gerät eingeht, lautet das Feld *IP-Adresse* "—".

Alle Hosts

Im Bericht All Hosts werden alle Hosts im Bestand aufgelistet. Sie können diesen Bericht verwenden, um folgende Aufgaben auszuführen:

- Zeigen Sie alle Chassis im Bestand an.
- Zeigen Sie das Chassis bzw. die Karten an, die über unabhängige Hostnamen verfügen.
- Identifizieren des Betriebssystems und der Versionen auf den Geräten

> **Hinweis**: Ein Master-Chassis kann sich auf ein Slave-Chassis beziehen, jedes mit eigener Identität.

Um die Geräteinformationen oder die Gerätekonfiguration für den Host anzuzeigen, klicken Sie unter *Hostname* auf den gewünschten Link, und die Detailseite wird geöffnet.

Um die Konfigurationsdetails anzuzeigen, klicken Sie auf **Konfiguration ausführen** oder **Startkonfiguration**, und die Konfigurationsdetails werden in einem neuen Fenster angezeigt.

Benutzerdefinierter Bestand

Im benutzerdefinierten Bestandsbericht sind alle Geräte und ihre Details für die ausgewählten Bestände aufgeführt. Dieser Bericht enthält auch die Vertragsinformationen und (falls veröffentlicht) das LDoS für die Geräte im Bestand.

Um die Gerätedetails anzuzeigen, klicken Sie unter *Hostname* auf den gewünschten Link.

> **Hinweis**: Wenn beim Hochladen des Bestands keine IP-Adresse für ein Gerät eingeht, lautet das Feld *IP-Adresse* "—".

Bestandsaufnahme

Die Berichte, die in der Inventory Insight-Bibliothek enthalten sind, bieten zusätzliche Informationen zu den Geräten, die vom Service identifiziert werden.

Diese Berichte bieten Netzwerkadministratoren und -technikern einen aktuellen Überblick über ihr Netzwerk. So können sie die Geschäftskontinuität aufrechterhalten, die Betriebseffizienz steigern und das Risikomanagement verbessern.

Zusammenfassung

Im Bericht Zusammenfassung werden die Informationen zum Collector aufgelistet, über den die ausgewählte Bestandsaufnahme hochgeladen wurde. Es zeigt die Appliance-ID, die aktuellste Upload-Zeit und eine Übersicht der Sammlung an.

Der zusammenfassende Bericht enthält folgende Informationen:

- **IP-Adressen in der Liste verwalteter Geräte** - Dieser Abschnitt des Berichts enthält die gesamten IP-Adressen in der Liste der verwalteten Geräte.
- **Nicht erfasste IP-Adressen** - In diesem Abschnitt des Berichts werden die gesamten IP-Adressen in der Liste der verwalteten Geräte angezeigt, die der Collector nicht erreichen konnte. Dies sind die potenziellen Gründe dafür, dass der Collector die Geräte nicht erreichen konnte:
  - Das Gerät hatte schlechte Anmeldeinformationen.
  - Das Gerät war offline.
  - Das Gerät antwortete nicht.
- **Bericht** - In diesem Abschnitt des Berichts werden die Geräte in der Sammlung aufgeführt, die in den Berichten zu vorhandenen Smart Net Total Care-Installationen und Vertragsmanagement enthalten sind. Die Geräte in diesem Abschnitt werden in den folgenden Kategorien präsentiert:
  - **Chassis** - Diese Kategorie zeigt das Chassis, das erfolgreich identifiziert und verarbeitet wurde.
  - **Modul** - In dieser Kategorie werden die Module angezeigt, die erfolgreich identifiziert und verarbeitet wurden.
  - **Netzteil** - Diese Kategorie zeigt die Netzteile an, die erfolgreich identifiziert und verarbeitet wurden.
  - **Lüfter**: In dieser Kategorie werden die Lüfter angezeigt, die erfolgreich identifiziert und verarbeitet wurden.
  - **Sonstige** - Diese Kategorie wird für alle anderen Gerätetypen verwendet, die erfolgreich identifiziert und verarbeitet wurden.

    - **Nicht vor Ort austauschbar** - Geräte, die nicht ohne Unterstützung durch Cisco ausgetauscht werden können, gehören zu dieser Kategorie. Um die Gerätedetails anzuzeigen, klicken Sie auf den Link Nummer.
    - **Nicht erkannt** - Geräte, die nicht in den Cisco Datensätzen aufgeführt sind, gehören zu dieser Kategorie und werden daher nicht als Cisco Geräte anerkannt. Um die Gerätedetails anzuzeigen, klicken Sie auf den Link Nummer.
- **Not Reports (Nicht gemeldet)**: Dieser Abschnitt des Berichts enthält die Geräte in der Sammlung, die aufgrund von Verarbeitungsfehlern oder Datendiskrepanzen in einer der Cisco Datenbanken *nicht* in den Berichten zu vorhandenen Smart Net Total Care-Installationen und Vertragsmanagement aufgeführt werden. Befolgen Sie bei Geräten, die in diesem Abschnitt enthalten sind, die (ggf.) bereitgestellten Abhilfemaßnahmen. Die Geräte in diesem Abschnitt werden in den folgenden Kategorien präsentiert:
    - **3**Drittanbieter-Geräte: In dieser Kategorie sind Geräte aufgeführt, die nicht von Cisco stammen. Um die Gerätedetails anzuzeigen, klicken Sie auf den Link Nummer.
    - **Duplikat** - Diese Kategorie stellt doppelte Geräteinformationen dar, die im Inventar aufgeführt sind. Um die Gerätedetails anzuzeigen, klicken Sie auf den Link Nummer.
    - **Sonstige**: In dieser Kategorie sind Geräte aufgeführt, die aufgrund der gesammelten Informationen nicht vollständig vom aktuellen Smart Net Total Care-Softwaresystem kategorisiert werden konnten. Um die Gerätedetails anzuzeigen, klicken Sie auf den Link Nummer.

Nicht erfasst

Der Not Collected-Bericht listet alle Geräte auf, die in der Liste der verwalteten Geräte enthalten waren, aber nicht auf den Collector reagiert haben. Sie können diesen Bericht verwenden, um die verarbeiteten Cisco Geräte anzuzeigen (die mit Cisco Daten angereichert sind), jedoch nicht Teil der aktuellen Sammlung. Dieser Bericht enthält außerdem folgende Informationen:

- Der Grund, warum das Gerät nicht erfasst wurde. Der häufigste Grund sind falsche Anmeldeinformationen in der Liste für verwaltete Geräte. Überprüfen Sie die Liste Verwaltete Geräte auf Fehler.
- Die vorgeschlagenen Maßnahmen, die Sie durchführen können, um die Fehler zu beheben.

Hinweis: Wenn beim Hochladen des Bestands keine IP-Adresse für ein Gerät eingeht, lautet das Feld *IP-Adresse* "—".

Tipp: Weitere Informationen zu diesem Bericht finden Sie im Video Update Managed Device List (Liste verwalteter Geräte aktualisieren).

Drittanbieter

Der Drittanbieterbericht listet alle erfassten Geräte auf, die als Nicht-Cisco-Geräte identifiziert wurden. Dieser Bericht gibt Ihnen ein vollständiges Bild von Ihren vorhandenen Installationen, da er Geräte von Drittanbietern enthält, auch wenn diese nicht durch die Cisco Support-Informationen bereichert werden können.

Hinweis: Wenn beim Hochladen des Bestands keine IP-Adresse für ein Gerät eingeht, lautet das Feld *IP-Adresse* "—".

Duplikate

Der Bericht Duplicates listet die Geräte auf, die in den erfassten Daten mehrmals angezeigt werden. Dieser Bericht enthält auch die möglichen Gründe für die doppelten Einträge.

Nicht erkannt

Der Bericht "Nicht erkannt" listet die Cisco Geräte (in den ausgewählten Beständen) auf, die nicht als Cisco Geräte validiert werden konnten, oder das System konnte den Gerätetyp nicht bestimmen. Dieser Bericht hilft Ihnen dabei, die Cisco Geräte zu identifizieren, die durch die Erfassung verarbeitet und mit Cisco Daten bereichert werden können.

Der Bericht gibt auch den Grund dafür an, dass bestimmte Geräte nicht identifiziert werden.

> **Hinweis**: Wenn beim Hochladen des Bestands keine IP-Adresse für ein Gerät eingeht, lautet das Feld *IP-Adresse* "—".

Nicht vor Ort austauschbar

Im Bericht Not Field Replaceable (Nicht vor Ort austauschbar) werden die Komponenten der Geräte (in den ausgewählten Beständen) aufgeführt, die nicht mehr vom Cisco Field Team gewartet oder ersetzt werden.

> **Hinweis**: Die nicht vor Ort austauschbaren Geräte sind nicht durch einen Servicevertrag abgedeckt, sodass Ersatzteile nicht für sie beschafft werden können.

> **Hinweis**: Wenn beim Hochladen des Bestands keine IP-Adresse für ein Gerät eingeht, lautet das Feld *IP-Adresse* "—".

Andere

Im Bericht Andere werden die Geräte aufgeführt, die aufgrund eines Problems mit der Datenanalyse angezeigt werden. Diese Geräte werden in den anderen Bestandsberichten nicht berücksichtigt. Dieser Bericht liefert die möglichen Gründe für die Probleme.

Sie können diesen Bericht verwenden, um die Geräte zu identifizieren, die mit den Cisco Support-Informationen im Portal bereichert werden können.