Smart Call Home Portal Web Application

Revised: July 10, 2014, Smart Call Home 3.7

The Smart Call Home web application provides access to:

- An overview page with quick links to key Smart Call Home functions and documentation. Most of the quick links are available within the Registration management and Reports pages. However, tasks for managing device groups are available on the Overview page only and include:
  - Create Device Group
  - Edit Device Group
  - Set Maintenance Window for Individual Devices
  - Set Maintenance Window for Device Groups
  - Edit Group Preferences
- Registration Management functions, including:
  - Registered Devices
  - Devices Pending Registration
  - Transport Gateways
  - Registered Users
  - Bulk Registration
- Reports about Call Home enabled devices and the messages they send:
  - Device Report
  - Call Home History Report
  - Network Summary Report
  - Registration Summary Report

To begin using the Smart Call Home portal:

Step 1 Go to http://tools.cisco.com/sch and login with your Cisco.com ID.

Note If you do not have a Cisco.com ID, register at https://tools.cisco.com/RPF/register/register.do. Ensure that the service contracts for your company are included in your account profile. To verify or add a contract to your Cisco.com ID, go to the Profile Manager and click **Access** tab.

Overview Page

This is the portal home page and provides quick links to popular functions. It also provides helpful links to the Smart Call Home support community and related tools. Most of the quick links are available within the Registration Management and Reports pages. However, the Registered Devices link and the links under the Manage Device Groups heading are available on the Overview page only.

Manage Device Groups

In this area, a customer admin can create and edit device groups, customize preferences, and set maintenance windows.

To create a device group:

1. Go to Smart Call Home portal and login with your Cisco.com ID.

2. Click **Create Device Group**. The Create Device Group window appears.

3. Enter a group name (customer defined) in the space provided.

4. Search for devices by any or all of the search options and click **Search**. The serial numbers of the devices fitting the search criteria appear in the Devices Available for Group field.

5. Click the serial numbers of the devices you wish to add to the group and click **Add**.

6. Click **Save.**

Devices may be added or removed from the device group by clicking the **Edit Device Group** link from the home page of the Smart Call Home portal. Device group preferences can be modified by clicking the **Edit Group Preferences** link. Devices may not belong to more than one device group.
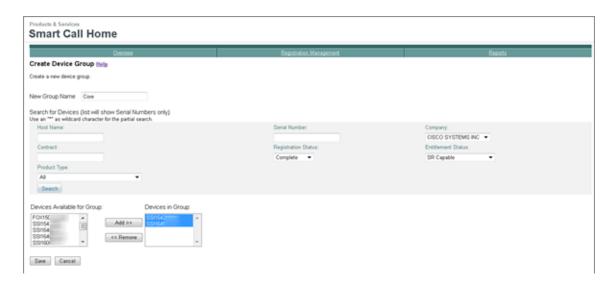

Figure 3-1   Create Device Group

To set a maintenance window:

Step 1   Go to Smart Call Home portal and login with your Cisco.com ID.

Step 2   Click **Set Maintenance Window for Individual Devices** or **Set Maintenance Window for Device Groups**.

Step 3   Search for individual devices or select a device group.

Step 4   Select a start and end time for the maintenance window by clicking the calendar icons and selecting dates. Options exist for applying the maintenance window to the device group or selected serial numbers within the device group.

Step 5   After making desired selections, click **Set Maintenance Window**.

To edit group preferences:

Step 1   Go to Smart Call Home portal and login with your Cisco.com ID.

Step 2   Click **Edit Group Preferences**.

Step 3   Select an existing group from the menu.

Note   For instructions on how to edit device preferences, see the Edit Device Preferences section.

Registration Management

All registration activities are consolidated within the Registration Management page. Here you can view information about:

- Registered Devices
- Devices Pending Registration
- Transport Gateways
- Registered Users
- Bulk Registration

Note   Users with the Customer Admin role can add, edit and delete users, whereas a Customer User can only view users.

Registered Devices

To view registered devices, go to the Smart Call Home portal and click **Registration Management > Registered Devices.** A list of registered devices appears. Search for specific devices using the search fields at the top of the page. When Smart Call Home receives the first message from the device, it places the device in a pending registration status. The customer then receives an email that contains instructions for confirming registration. Follow the instructions in the email to register devices.

Information about customer devices on the Registered Devices page includes:

Serial Number: device serial number. Devices using Virtual Switching System (VSS) (which allows for the merging of two physical Catalyst 6500 switches into a single logically-managed entity) will have several serial numbers listed per device host name.

The serial number column also contains an information callout for the device that lists device preferences. Users can change device preferences and contract information from this screen.

Note Smart Call Home validates the input serial numbers and product ids reported in the Call Home message against Cisco databases. If the validation is not successful the registration of the device could fail.

Host Name: the host name of the device. Devices using Virtual Device Context (VDC) (each configured VDC presents itself as a unique Nexus 7000 device to connected users within the framework of one physical switch; the VDC runs as a separate logical entity within the switch) will list multiple hostnames per device serial number.

Product ID: the product ID or PID for the device.

Contract: the contract number and type of contract under which the device is registered.

Company: the company to which the device is registered.

Registration Status Date Stamp: the registration status and date that status was activated. Possible registration statuses include:

   – **Pending -** Status occurs when a device sends its first Call Home message to Smart Call Home.

   – **Complete** - When a customer uses the web application to confirm the device registration for a device that is pending registration.

   – **Unregistered** - Devices that have had the registration deleted.

   – **Expired -** Indicates that the contract or trial period for the associated device has expired and is no longer valid.

Entitlement Status End Date: indicates if the device is entitled to full Smart Call Home functionality (SR Capable) or is registered under a 120-day trial period (SR Trial Capable). If the device is covered by a service contract, the system registers the device using this contract. When the device is not covered by a service contract or the device is under warranty, the system allows the user to register the device for a contract_required status. If the device is not under warranty and is not covered by a service contract, all such functionality is available for 120 days.

Devices Pending Registration

To view devices pending registration, go to the Smart Call Home portal and click **Registration Management > Devices Pending Registration**. Devices are in a pending registration status until the customer confirms registration. For step-by-step instructions on device registration, refer to the Smart Call Home Deployment Guide.

Transport Gateways

To view registered transport gateways, go to the Smart Call Home portal and click **Registration Management > Transport Gateways**. Transport gateways registered under your company appear. You can complete registration and delete transport gateway registrations from this page. For instructions on how to register a transport gateway, refer to the Smart Call Home Deployment Guide.

Note Available only to a user with Customer Admin role.

Registered Users

To view registered users for your company, go to the Smart Call Home portal and click **Registration Management > Registered Users**. This page lists those users for your company, their Cisco.com ID, and their function (administrator or user). Administrators can delete, add, and update users from this page. See Table1 for User roles and functions.

- Administrators can add a user by clicking **Add User** and following the prompts. You will need the new user's Cisco.com ID.

- Use the **Update User** option to change user's role

- Use the **Delete User** option to remove the user.

- Use the **Update Device Owner** option to change the owner of a device. Only administrators can be device owners.

Select the user and click **Update Device Owner.** Next, verify the details, select the new device owner from the menu and click **Submit.**

Table 3-1   Customer User Roles and Functions

Function	Customer Admin	Customer User
Edit Device Preferences	Yes	No
Delete Devices	Yes	No
Complete Device Registration	Yes	Yes
Add/Delete/Update Registered Users	Yes	No
Add/Delete/Update Registered End Customers	No	No
Manage Device Groups/Set Maintenance Window	Yes	No
Run/Download Device/Call Home History/Registration Summary Reports	Yes	Yes
Run/Download Network Summary Report	Yes	Yes

Bulk Registration

Use the bulk registration function to register multiple devices at once.

Step 1   Click on the sample CSV or XLS file to use as a template for filling out device information. The file requires the following information for each device:

(A) Cisco.com ID

(B) Serial Number

(C) Product ID

(D) Email Address

(E) Host Name (optional)

(F) Contract Number (optional)

Step 2   Once the CSV or XLS file is complete, click **Browse** and select the CSV or XLS file just created.

Step 3   Click **Upload File.**

Step 4   You will receive an email with an attached file that includes an appended column with the registration status for each device
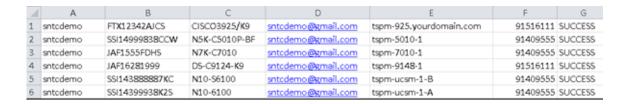

	A	B	C	D	E	F	G
1	sntcdemo	FTX12342AJCS	CISCO3925/K9	sntcdemo@gmail.com	tspm-925.yourdomain.com	91516111	SUCCESS
2	sntcdemo	SSI14999838CCW	N5K-C5010P-BF	sntcdemo@gmail.com	tspm-5010-1	91409555	SUCCESS
3	sntcdemo	JAF1555FDHS	N7K-C7010	sntcdemo@gmail.com	tspm-7010-1	91409555	SUCCESS
4	sntcdemo	JAF16281999	DS-C9124-K9	sntcdemo@gmail.com	tspm-9148-1	91516111	SUCCESS
5	sntcdemo	SSI143888887KC	N10-S6100	sntcdemo@gmail.com	tspm-ucsm-1-B	91409555	SUCCESS
6	sntcdemo	SSI14399938K2S	N10-6100	sntcdemo@gmail.com	tspm-ucsm-1-A	91409555	SUCCESS

Figure 3-2   Registration Status File

End Customer Access (Partners only)

To view which portal reports a customer has access to, go to the Smart Call Home portal and click **Registration Management > End Customer Access**.

To update customer access to reports:

Step 1   Click the checkbox next to the appropriate Cisco.com ID.

Step 2   Click the checkbox next to each report to which you want to grant access.

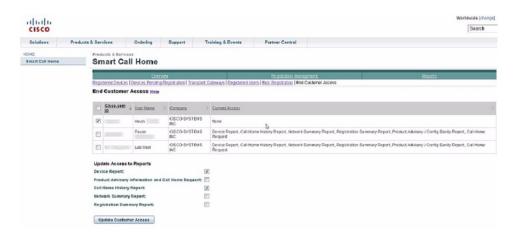**Step 3**   Click **Update Customer Access.**

Figure 3-3   End Customer Access

Reports

Smart Call Home reports are available on the Smart Call Home portal in the Reports tab. The following reports are available:

- **Device Report** - contains detailed inventory information on the customer's registered device(s), provides information about the device's registration contact and the device's latest Inventory and Configuration details.

- **Call Home History Report -** provides access to the different Call Home messages, and the processed results on those messages, sent within the last three months.

- **Registration Summary Report -** displays contract information for the customer's devices that are registered in Smart Call Home; only the companies you have access to will be displayed.

Tip Each report starts by asking users to Specify Report Criteria. Once the report criteria is entered, click **Run Report** to view the results.

Device Report

The Device Report provides inventory and configuration data for devices. The data for this report is retrieved from the inventory and/or configuration call home messages.

Note To view a device report, the user must be registered under at least one company.
A device might not be included in the Device Report if:

- The device registration was deleted (status Unregistered).

- The device has a pending device registration.

This section describes how to:

- **Generate Device Reports** and obtain information about the device's latest Inventory and Configuration details and the device's registration contact.

- **Specify Report Criteria** and filter the devices to include in the report.

- View Device Report Results

- View Device Details

- Edit Device Preferences

- Edit Device Contract

To perform any of the report processes you must first launch the Smart Call Home web application (portal).

Generate Device Reports

Inventory and configuration call home messages are used by the Smart Call Home portal to display device detail information and configuration data in device reports.

To generate a device report:

Step 1   Go to **Reports > Device Report**.

Step 2   Choose a company for which the customer has a completed user registration, or choose **All** to see device reports for all the companies to which the user is registered.

> **Note**   The **All** option is available only when the user is registered to more than one company.

Step 3   Optionally enter one or more of the following search criteria:

Host Name - full or partial host name (case insensitive)

> **Note**   A search on host name for a Cisco Unified Computing System (UCS) device supports a search for both the UCS system name as well as the hostname of the Cisco UCS 6100 Series Fabric Interconnect

Serial Number - full or partial serial number (serial number of a chassis or of a component in the chassis).

> **Note**   Searching on a partial serial number will return matching results for primary serial number and component serial numbers.

Product ID - a full or partial product id; allows a search on a chassis or components in the chassis.

> **Note**   Use an asterisk (*) as a wildcard character for a partial search.

Select a contract number to retrieve information on devices within the contract, or select the default All to retrieve information on all devices regardless of their contract number.

Check the **Include only devices with Product Advisory Information** check box to retrieve information on only those devices with product advisories associated to them.

Step 4   Click **Run Report.** The Device Report Results page appears.

View Device Report Results

This page displays those entries that match the search criteria specified on the Specify Report Criteria page. From this page, you can:

• Export the report to Excel or PDF formats

- View advisory notices for devices by clicking on the Advisory icons under the serial number of the device
- Sort results on any column by clicking the column header
- Specify new report parameters and run a new report
- View device details by clicking on the device serial number

Device Details Category List Table

The categories in the Device Details vary depending on the type of device. The table below identifies which categories are associated to each device type.

Table 3-2   Device Detail Categories

Products	Contact	Hardware Module	Hardware Submodule	Power Supply	Fan Uni	Fabric Extender	Fabric Module	System	License	VDC Membership	Config	Advisories	Blade Chassis	Threat	Telemetry	Snapshot	Cluster Overview	Nodes Details	Rack Server
Nexus 5000	X	X		X	X	X		X	X		X	X							
Nexus 7000	X	X		X	X		X	X	X	X	X	X							
UCS 6100	X	X		X	X			X					X						
UCS 6248	X								X		X				X		X	X	
UCS 6296	X								X		X				X		X	X	
UCSC Rack Server	X	X		X	X	X		X					X						X
Catalyst 2960	X	X	X	X				X	X		X	X							
Catalyst 3560	X	X	X	X				X	X		X	X							
Catalyst 3750	X	X	X	X				X	X		X	X							
Catalyst 4500	X	X	X	X	X			X			X	X							
Catalyst 4900	X	X	X	X	X			X			X	X							
Catalyst 6509	X	X	X	X	X			X			X	X							
Cisco 7200	X	X		X				X			X	X							
Cisco 7301	X	X		X				X			X	X							
Cisco 7600	x	x	x	x	x			x			x	x							
ISR 800, 1800, 2800, 3800	X	X	X	X	X			X			X	X							
ISR G2 1900, 2900, 3900	X	X	X	X	X			X	X		X	X							
ASA 5500	X	X		X				X	X		X	X		X	X	X			
Cisco ASR 1000 Series Router	x	x	x	x	x			x			x	x							
Cisco ASR 5000 Series Router	X	X	X	X	X			X	X		X	X							
Cisco ASR 9000 Series Router	X	X	X	X	X			X			X	X							
Cisco CRS Routers	X	X		X	X			X			X	X							
Cisco ME 3400	X	X	X	X				X	X		X	X							
Cisco ME 3750	X	X	X	X				X	X		X	X							
Cisco ME 4924	X	X	X	X				X	X		X	X							
Cisco ME 6500	X	X	X	X				X			X	X							
Cisco UBR 7000	X	X	X	X	X			X	X		X	X							
Cisco UBR 10000	X	X	X	X	X			X	X		X	X							
Cisco XR 12000 Series Router	X	X	X	X	X			X			X	X							
Cisco Unified Communications Manager (8.6(1))	X								X		X				X		X	X	

View Device Details

To view device details within the Device Report:

Step 1   From the Device Report Results, in the Serial Number column, click a device serial number. The Device Details for the selected device appears.

This page contains the Device Details summary info, including:

- Device serial number
- Device host name
- Device product id
- Hardware and software versions
- Part number/revision

- Date of last inventory

- Date configuration was last updated

- Top Assembly Number

- Time Based License - indicates number of days left before license expires

- Failover Status can have the following states:

> Primary/Active
>
> Primary/Standby
>
> Secondary/Active
>
> Secondary /Standby
>
> Primary/Disabled
>
> Secondary/Disabled

Step 2 Click **Show Detail** under any of the device detail options to obtain more information about the device. Refer to Device Detail Categories to see available categories for each device type. Data can be exported to XLS or PDF formats for each device detail category.

Contact Details

The Contact Details table contains information about the user who performed the device registration. The Contact Detail table contains the following information:

- Contract Number - Contract Number the device is registered under

- Contact Name - First and last name of the SR Contact

- Contact Email - Email address of the SR Contact

- Contact Phone Number - Phone number of the SR Contact

Hardware Module Details

The Hardware Module Details table contains information about the hardware modules of the selected device, if present. The table contains detailed information about the modules in the device, including:

- Module - Slot Number of module

- Ports - Number of ports the module has

- Card Type - Description of the type card

- Product ID - Product ID of the device

- HW - Hardware Version

- Serial Number - Serial Number of the module

- Part Number - Part Number of the module

- Part Number Revision - Revision Part Number of the module

- Top Assembly Part Number - Number is for the processor only

- Status - Current operating status of the module

Note   The table columns can be sorted when you click a column header;   the selected column toggles between ascending and descending order.

Hardware Submodule Details

The Hardware Submodule table contains information about the hardware submodules, if present, on the selected device.

Hardware Details (Sub-module) Details table contains detailed information about the sub-modules plugged into the device, including:

- Module - Slot Number of the module containing the sub-module
- Sub-Module - Name of the sub-module feature
- Product ID - Product id of the sub-module
- Part Number - Part number of the sub-module
- Part Number Revision - Part Number Revision for the sub-module
- Serial Number - Serial number of the device that contains the sub-module
- HW - Hardware version of the sub-module
- Status - Operational status of the sub-module

Power-Supply Details

The Power-Supply Details table contains information about the power supplies on the selected device, including:

- Power Supply Number - Slot the Power-Supply is plugged into and the power supply description
- Product ID - Product ID of the Power-Supply
- Serial Number - Serial Number of the Power-Supply

Fan Unit Details

The Fan Unit table contains information about the fan units on the selected device, including:

- Name - The number the fan is referred to in the device (i.e., fan number 1)
- Description - A brief description of the type of fan installed on the device
- Product ID - Product ID of the Power-Supply
- Serial Number - Serial Number of the Power-Supply
- Part Number - Part Number of the Power-Supply
- Part Number Revision - Revision Part Number of the Power-Supply
- HW Revision - Hardware Revision of the Power-Supply
- Status - Current operating status of the fan

Fabric Extender Details

The Fabric Extender table contains information about the extenders, if present, on the selected device, including:

- Fabric Extender ID - Fabric extender ID
- Product ID - Product ID of the fabric extender
- Serial Number - Serial Number of the fabric extender
- HW version - HW version of the fabric extender
- SW Version - SW version of the fabric extender
- Part Number/Revision - Manufacturing Assembly number
- Description - Description

Fabric Module Details

The Fabric Module table contains information about the hardware submodules, if present, on the selected device, including:

- Name - Slot Number of the module containing the fabric card module
- Product ID - Product id of the fabric card module
- Serial Number - Serial number of the device that contains the fabric card module
- Part Number - Part number of the fabric card module
- Part Number Revision - Part Number Revision for the fabric card module
- HW Revision- Hardware version of the fabric card module
- Status - Operational status of the fabric card module

System Details

The System Details table contains information about the system and software installed on the selected device, including:

- Processor - Type of processor
- Image Name - Image name of the IOS
- IOS Version - Version of the IOS being used
- Feature Set - Name of the Feature Set
- ROM Version - Version of the ROM being used
- Amount of memory being used (in Kilobytes) for the following storage areas:
  - Main Memory
  - I0 Memory
  - Install Memory
  - Non Volatile Memory
  - Slot0
  - Slot1 (if installed)

          – Boot Flash

- Last Restart Time- When the last restart of the device occurred

- Last Reload Reason - Reason for the last reload that occurred

- Last Reset Reason - Identifies the reason for the last reset

- System Uptime - Amount of time the device has been operational

- Config Register - Config Register number

- Bandwidth Points: - Indicates the amount of bandwidth points that are configured on the PCI bus for the various slots to utilize

License Details

The License table contains information about the license associated to the selected device, including:

- Licensed Package - Name of the license package associated to the device

- Installed - Indicates if the package is installed

- License Count - Indicates the number of licenses installed on the switch

- Status - Operational status of the license

- Expiry Date - The date that license will expire and no longer be valid

- Comments - Any comments associated to the device

VDC Membership Details

VDC Membership table contains information on the ports and interfaces that are allocated per VDC and the name assigned to the VDC, including:

- VDC ID - Id number of the specified VDC

- VDC Name - Name of the VDC

- Ports/Interfaces - Identifies all the interfaces and ports that are associated to this specific VDC

Configuration Details

The Configuration Details section contains information about the configurations on the selected device; the configuration details are only available if the device has sent at least one configuration message. Information provided includes:

- Hyperlink access to view the running config and startup config

- Hyperlink access to the technologies and features running on the selected device

> ✎
>
> **Note**   This list does not include those features that are enabled on the device by default.

- The Configuration Sanity Analysis link provides a link to a page that contains Best Practices Results with notices categorized into four different types and sorted by severity

- Best Practices Results are based on show command outputs

Advisories

Displays any advisories that are associated to the device, to include:

- Hardware End of Life/Sales/Support/Engineering
- Software End of Life/Sales/Support/Engineering
- Hardware Field Notice
- Security Advisories

Edit Device Preferences

Smart Call Home sends a variety of email notifications about the health of a device. These notifications may be suppressed by message type, i.e. inventory, configuration, test, diagnostic, and others. The service request contact and email addresses for notifications can also be modified. To perform these tasks:

Step 1 Go to the Smart Call Home portal and login with your Cisco.com ID.

Step 2 From the Overview page, select **Registered Devices**. The Registered Device Report appears.

Step 3 Use search criteria to narrow the report to display those devices for which preferences are to be edited.

Step 4 Select the desired devices and click **Edit Device Preferences**. The Edit Device Preferences page appears.

Step 5 Select the devices for which preferences are to be edited. Note that option to preserve the current configuration is always selected by default.

Step 6 Choose one or more message types to restrict those types of notifications for the devices selected.

Step 7 Make desired changes to the service request contact.

Step 8 Make desired changes to the list of email addresses that receive Smart CallHome notifications using **Add** and **Remove** options.

Step 9 Add additional email addresses for notifications in the field provided.

Step 10 Click **Submit**.

Edit Device Contract

Perform the following steps to change the contract under which a device is covered:

Step 1 Go to the Smart Call Home portal and login with your Cisco.com ID.

Step 2 From the Overview page, select **Registered Devices**. The Registered Device Report appears.

Step 3 Use search criteria to narrow the report to display the device(s) for which contracts are to be edited.

Step 4 In the serial number column for the desired device, hover your cursor over the Info caption and click **Edit Device Contract**. The Edit Device Contract page appears, which contains the current device information and contract number.

Step 5   In the Select New Contract section, select the contract to which you wish to move your device.

Step 6   Click **Submit**.

Call Home History Report

The Call Home History Report allows you to search for and access all Call Home messages sent within the past three months from the Call Home device to the Smart Call Home backend.

Note The customer must be registered under at least one Company. Customers can view the Call Home History report for only their registered devices.The Call Home History report may not be available if:

- The device registration was deleted (status 'Unregistered').
- The device has a pending device registration.
- The contract used to register the device has expired and hence the device registration has expired. When the device is successfully registered then the report will be accessible again.

This section describes how to perform Call Home History Report processes on the Smart Call Home web application and explains how to perform the following tasks:

- Generate a Call Home History Report and view the Call Home messages and message processing results.
- Specify Report Criteria and filter the list of devices you want a report on.
- Specify Message Processed Time Frames
- View Call Home History Report Results and message processing results.
- Export the Call Home Report to Excel or PDF.

Generate a Call Home History Report

To generate a Call Home History Report:

Step 1   Launch the Smart Call Home web application. The Smart Call Home Overview page appears.

Step 2   Click **Call Home History Report.**

Note From anywhere in the Smart Call Home web application you can click the **Reports** tab and then click **Call Home History Report**.

The Specify Report Criteria page for the Call Home History Report appears. This page allows you to specify search criteria to generate a Call Home History Report.
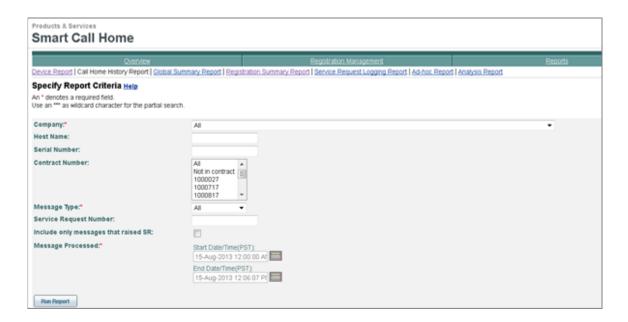
Figure 3-4   Specify report Criteria Snapshot

Step 3   Select or enter desired search criteria. An asterisk (*) may be used as the wildcard for partial searches. To see only those messages that raised a service request, check the **Include only messages that raised SR:** check box.

Step 4   In the Messages Processed time frames area you must specify a time frame that is within three months of the current date.

Step 5   Click **Run Report.** The Call Home History Report Results page displays entries that match the search criteria.

View Call Home History Report Results

This page lists all the Call Home messages that met the specified search criteria from the previous Selection Criteria page.
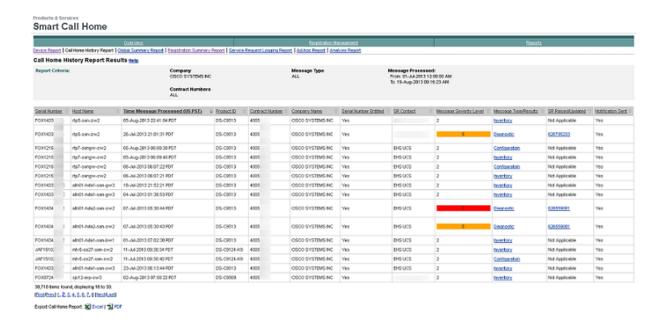
Figure 3-5   Call Home History Report Snapshot

The Call Home History Report Results page indicates the selection criteria   used to obtain the displayed results. Complete any of the following steps to perform the associated functions on the Call Home History Report Results page:

Step 1   Export the Call Home Report to Excel or PDF formats by clicking the corresponding option at the bottom of the report results.

Step 2   See the details of a specific message by clicking a message in the Message Type/Results column. This displays the Message Details page for the selected message type. You can view details for the following types of messages:

Configuration Message	Performance Message	Telemetry Message
Crash Message	Request Message	Test Message
Diagnostic Message	Send CLI Message	Threat Message
Environmental Message	Snapshot Message	
Inventory Message	Syslog Message	

Step 3   When a TAC case is created or updated, the SR Raised/Updated column displays the case number, which provides a hyperlink to detailed information about the selected TAC case.

Step 4   You can specify different report criteria at the bottom of the page. This area contains previously used criteria used to generate the current report results.

Note   Most devices have a one serial number for one host name relationship. VDC devices (Cisco Nexus 7000 Series) will have a one serial number to one or more hostname relationship. VSS devices (Cisco Catalyst 6500 Series) will have a one hostname to one or more serial number relationship.

Network Summary Report

This report presents a summarized report on devices registered with Smart Call Home for the selected company. The numbers and percentages for each device are computed on the data that is collected via inventory and configuration Call Home messages from registered devices in a customer's network.

The device data in the Network Summary Report is based on devices to which the logged-in customer has access via the Smart Call Home web application. This report is available for registered customers and contains a summarized view that includes all or some of the following information, depending on device type:

- Company selected and total number of devices registered with Smart Call Home
- Product IDs
- Modules
- Sub-modules
- Power supplies
- Fan units
- Software releases
- Software licenses
- Software feature sets and images
- Advisories
- List of technologies and features

Note   The Network Summary Report for the Cisco Unified Computing System contains additional information detailed in the **Network Summary Report Results** for a Cisco Unified Computing System section of this document.

This section describes how to perform the following Network Summary Report actions on the Smart Call Home web application:

- Generate a Network Summary Report and view the Call Home messages and message processing results
- Specify Report Criteria and filter the list of devices for which you want a report
- View Network Summary Report Results for ALL Products
- View Network Summary Report Results for a Specific Product (Catalyst 6500)
- Network Summary Report Results for Cisco Unified Computing System
- Export the Call Home Report to an Excel or a PDF format

Generate a Network Summary Report

When Smart Call Home generates a Network Summary Report, it retrieves the data for all Cisco devices for which the application has received and processed inventory and configuration Call Home messages.

Step 1   Launch the Smart Call Home web application; the Smart Call Home Overview page appears.

There are two ways to get to the Network Summary Report page:

- If you are on the Overview page click **Network Summary Report**
- If not on the Overview page, go to **Reports** > **Network Summary Report**

Step 2   Choose a company for which the customer has a completed user registration, or choose **All** to see reports for all companies the customer has registration/access.

✎
Note   The **All** option is available only when the user is registered to more than one company.

Step 3   Choose a product from the Product menu, or **All** if you want to view all registered devices.

Step 4   Click **Run Report.**

View Network Summary Report Results for ALL Products

If the **All** option is selected from the Product menu, then the following page is displayed as shown in the figure.
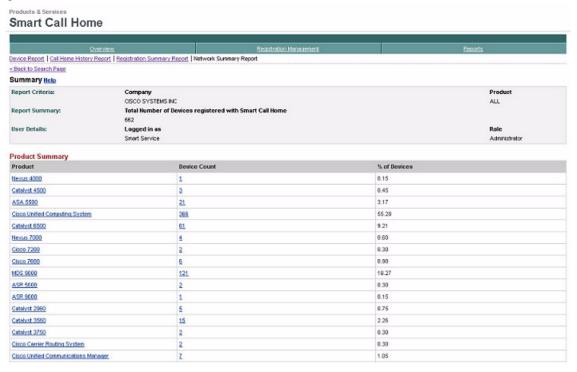

Figure 3-6   Network Summary Report - All Products

- The Summary section identifies:
    - Report Criteria - Company and Product selected for the report
    - Report Summary - The number of devices registered with Smart CallHome, for the specified company or companies

✎
Note This is the total number of registered devices in customer's network/selected company for which Smart Call Home has received and processed Configuration or Inventory messages.

    - **User Details** - The ID of the person who logged in and requested the report, and their role in the customer network

- The Product Summary section identifies:
    - Product - the product types that are in the customer network (based on user selection for the report). Click the linked product name in this column to view the summary information for the device(s).
    - Device Count - represents the number of each product type in the customer network. Click the linked number in this column to view Device Report information for the device(s).
    - % of Devices - from the device count a percentage of devices number is derived, identifying what percentage this product type represents in the customer's network

✎
Note If the **All** option was not specified then the above interim page will not be displayed, you will instead go directly to the summary page for the specified product (see next section).

View Network Summary Report Results for a Specific Product (Catalyst 6500)

This page displays those entries that match the search criteria specified on the Specify Report Criteria page. The next set of examples represent the Network Summary Report results for a Catalyst 6500 product.

- The Summary section identifies:
    - **Report Criteria** - Company and Product selected for the report
    - **Report Summary** - The number of devices registered with Smart Call

Home, for the specified company or companies

✎
Note This is the total number of registered devices in customer's network/selected company for which Smart Call Home has received and processed configuration or inventory messages.

    - User Details - The ID of the person who logged in and requested the report, and their role in the customer network

Step 1 Click **Show Detail** under one of the device detail options to obtain more information about the detail areas noted below:

- Product ID

- Module
- Sub-Module
- Power Supply
- Fan Unit
- Software Releases
- Software - Feature Sets and Images
- Advisories
- Technology & Features

Step 2   Each section may be exported to Excel or PDF by clicking the appropriate link underneath the expanded section.

> **Note**   All the previously listed areas have column headers in their respective sections; these columns can be sorted by clicking the column header.

Product ID

The Product ID (PID) area contains the:

- PID Name
- PID Count
- % 6500s with PID

Module

The Module area contains the:

- Module Name
- Module Count
- % of all Modules
- Device Count with Module
- % 6500s with Module

Submittal

The Sub-module area contains the:

- Sub-Module Name
- Sub-Module Count
- % of all Sub-Modules
- Device Count with Sub-Module
- % 6500s with Sub-Module

Power-Supply

The Power-Supply area contains the:

- Power Supply Name
- Power Supply Count

 – % of all Power Supplies

 – Device Count with Power Supply

 – % 6500s with Power Supply

Fan Unit

The Fan Unit area contains the:

 – Power Supply Name

 – Power Supply Count

 – % of all Power Supplies

 – Device Count with Power Supply

 – % 6500s with Power Supply

Software Releases

The Software Releases area contains the:

 – Release

 – Device Count with Release

 – % 6500s with Release

 – % of all Release

Software - Feature Sets and Images

The Software - Feature Sets and Images area contains the:

 – Feature Set

 – Image Name

 – Device Count with Image

 – % 6500s with Image

 – % of all Image

Advisories

The Advisories area contains the:

 – Advisory Type - Advisory Type (examples: HW End of Sale, HW End of Life, Field Notice)

 – Product Advisory - Advisory Title with link to the advisory notice

 – Device Count with Advisory - Number of devices for which at least one advisory of this type has been discovered

 – Percentage of devices with Advisory - Percentage of devices (of all devices belonging to the selected product family) for which at least one advisory of this type has been discovered

 – Percentage of All Advisories - Percentage of this advisory of all advisories discovered for Smart Call Home inventory

Technology & Features

The Technology & Features area contains the following information:

- – Feature Names (associated with each Technology / Sub-Technology, on a row-by-row basis)
- – Device Count with Feature
- – % 6500s with Feature

Technology & Features

This is a list of technologies and features supported by the devices currently registered with Smart Call Home. This list of features is derived from the show running config. Some features are enabled in the devices by default and may not appear in the show running config.
For a complete list of features, please refer to Feature Navigator tool

Hide Details

Technology	Sub-Technology	Feature	Device Count With Feature	% 6500s with Feature
ATM	Interim Local Management Interface (ILMI)	ATM PVC Trap Support	5	8.19
ATM	Not Available	ATM Tag Switch Router (TSR)	20	32.78
Additional and Legacy Protocols	AppleTalk Routing	AppleTalk 1 and 2	3	4.91
Additional and Legacy Protocols	Novell / IPX Routing	Novell IPX	2	3.27
Additional and Legacy Protocols	Not Available	AppleTalk Load Balancing	1	1.63
Additional and Legacy Protocols	Not Available	AppleTalk Routing over ISL and IEEE 802.10 in Virtual LANs	2	3.27
Availability	HDLC	SSO - HDLC	1	1.63
Availability	Multilink PPP	SSO - Multilink PPP (MLP)	1	1.63
Availability	PPP	SSO - PPP	1	1.63
Availability	Virtual Switch System	VSS - Virtual Switch System	2	3.27
Content Networking	Not Available	Manual certificate enrollment (TFTP and cut-and-paste)	21	34.42
Content Networking	BRIDGE CONTROL PROTOCOL	Bridge Control Protocol (BCP) Quality of Service (QoS)	16	26.22
Content Networking	File Transfer Protocol (FTP)	FTP Support for Downloading Software Images	7	11.47
Content Networking	Not Available	Gateway Load Balancing Protocol (GLBP)	1	1.63
Content Networking	Not Available	Redundancy Facility Protocol	29	47.54

187 items found, displaying 1 to 15.
[First/Prev] 1, 2, 3, 4, 5, 6, 7, 8 [Next/Last]

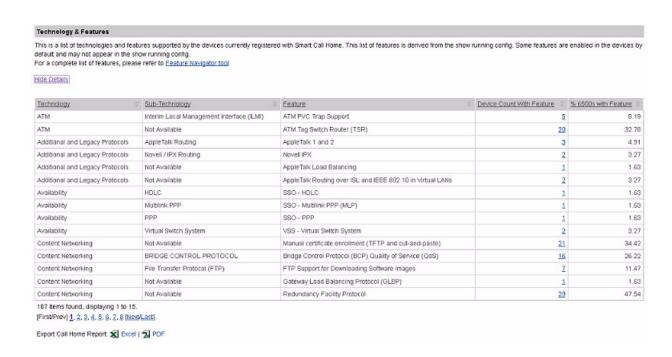Export Call Home Report: Excel | PDF

Figure 3-7   Technology and Features for Cisco Catalyst 6500 Series Switch

Network Summary Report Results for a Cisco Unified Computing System

The Network Summary Report for the Cisco Unified Computing System contains most of the same informational areas as the Catalyst 6500, with the exception of the following areas:

- Sub-Module
- Software - Feature Sets and Image
- Technology and Features

The following are additional informational areas available for the Cisco Unified Computing System.

Blade Chassis

The Blade Chassis area contains the:

- – Blade Chassis Name - Product ID of the blade chassis
- – Blade Chassis Count - Number of blade chassis having that product ID
- – % of Blade Chassis -% of blade chassis having that product ID
- – Customers with Blade Chassis - Number of customers having at least one blade chassis with that product ID

–   % Customers with Blade Chassis -% of customers having at least one blade chassis with that product ID

Fabric Extender

The Fabric Extender area contains the:

–   Fabric Extender Name - Product ID of the fabric extender

–   Fabric Extender Count - Number of fabric extenders having that product ID

–   % of all Fabric Extenders -% of fabric extenders having that product ID

–   Blade Chassis Count with Fabric Extender - Number of Blade Chassis having at least one fabric extender with this product ID

–   % of Blade Chassis with Fabric Extender -% of Blade Chassis having at least one fabric extender with this product ID

–   Customers with Fabric Extender - Number of customers having at least one fabric extender with this product ID

–   % Customers with Fabric Extender -% of customers having at least one fabric extender with this product ID

Blade Power Supply

The Blade Power Supply area contains the:

–   Power Supply Name - Product ID of the power supply existing in a Blade Chassis

–   Power Supply Count - Number of power supplies having that product ID

–   % of all Power Supplies -% of power supplies having that product ID

–   Blade Chassis Count with Power Supply - Number of Blade Chassis having at least one power supply with this product ID

–   % of Blade Chassis with Power Supply -% of Blade Chassis having at least one power supply with this product ID

–   Customers with Power Supply - Number of customers having at least one power supply with this product ID

–   % Customers with Power Supply -% of customers having at least one power supply with this product ID

Blade Fan Unit

The Blade Fan Unit area contains the:

–   Fan Unit Name - Product ID of the fan unit existing in a Blade Chassis

–   Fan Unit Count - Number of fan units having that product ID

–   % of all Fan Units -% of fan units having that product ID

–   Blade Chassis Count with Fan Unit - Number of Blade Chassis having at least one fan unit with this product ID

–   % of Blade Chassis with Fan Unit -% of Blade Chassis having at least one fan unit with this product ID

- Customers with Fan Unit - Number of customers having at least one fan unit with this product ID

- % Customers with Fan Unit -% of customers having at least one fan unit with this product ID

Blade

The Blade area contains the:

- Blade Name - Product ID of the blade

- Blade Count - Number of blades having that product ID

- % of Blades -% of blades having that product ID

- Customers with Blade - Number of customers having at least one blade with that product ID

- % Customers with Blade -% of customers having at least one blade with that product ID

Mezzanine Card

The Mezzanine Card area contains the:

- Mezzanine Card Name - Product ID of the mezzanine card existing in a Blade

- Mezzanine Card Count - Number of mezzanine cards having that product ID

- % of all Mezzanine Cards - % of mezzanine cards having that product ID

- Blade Count with Mezzanine Card - Number of Blades having at least one mezzanine card with this product ID

- % of Blades with Mezzanine Card - % of Blades having at least one mezzanine card with this product ID

- Customers with Mezzanine Card - Number of customers having at least one mezzanine card with this product ID

- % Customers with Mezzanine Card - % of customers having at least one mezzanine card with this product ID

Disk Drive

The Disk Drive area contains the:

- Disk Drive Name - Product ID of the Disk Drive existing in a Blade

- Disk Drive Count - Number of disk drives having that product ID

- % of all Disk Drives - % of disk drives having that product ID

- Blade Count with Disk Drives - Number of Blades having at least one disk drive with this product ID

- % of Blades with Disk Drives - % of Blades having at least one disk drive with this product ID

- Customers with Disk Drive - Number of customers having at least one disk drive with this product ID

- % Customers with Disk Drive - % of customers having at least one disk drive with this product ID

Network Summary Report Results for a Nexus 5000

The Network Summary Report for Cisco Nexus devices contains much of the same informational areas as the Catalyst 6500.

Additional informational areas for the Cisco Nexus 5000 Series Switches are:

Software Licenses

The Software License area contains the following information:

- Licensed Package
- Release
- Devices
- Installed - In Use
- Installed - Unused
- Uninstalled - In Use
- Uninstalled - Unused

Network Summary Report Results for a Nexus 7000

The Network Summary Report results for the Nexus 7000 contains many of the same informational areas as the Catalyst 6500. Additional informational areas for the Cisco Nexus 7000 Series Switches are:

Fabric Unit

The Fabric Unit area contains the:

- Fabric Name
- Fabric Count
- % of All Fabrics
- Device Count with Fabric Module
- % 7000s with Fabric

Software Licenses

The Software License area contains the:

- Licensed Package
- Release
- Devices
- Installed - In Use
- Installed - Unused
- Uninstalled - In Use
- Uninstalled - Unused

Registration Summary Report

This report displays registered device and contract information for customer devices that are registered with Smart Call Home; only the companies you have access to are displayed in the report.

This section describes how to perform Registration Summary Report activities on the Smart Call Home web application. The following tasks are explained:

- Generate a Registration Summary Report and view registered device and contract information
- Specify Report Criteria and filter the list of devices
- View Registration Summary Report Results
- Export the Call Home Report to an Excel or a PDF format.

Generate a Registration Summary Report

Step 1 Launch the Smart Call Home web application; the Smart Call Home Overview page appears. There are two ways to get to the Registration Summary Report page:

- If you are on the Overview page click **Registration Summary Report.**
- If not on the Overview page, go to **Reports > Registration Summary Report.**

Note To see pending devices in the Devices Available to Register area:

- The user must be an administrator and be associated to the company whose devices are pending registration.
- There must be devices pending registration and those devices must have a valid contract
  If any of the above conditions are not met, then the devices pending registration information will not be displayed.

Specify Report Criteria

This page lets you specify search criteria to generate a Registration Summary Report. To specify search criteria:

Step 1 Choose a company from the Company menu or choose **All** to see reports for all the companies for which the user is registered.

Note The All option is available only when the user is registered to more then one company.

Step 2 Enter optional search criteria, as desired:

- Host Name
- Serial Number; wildcard (an *) can be used
- Product ID: wildcard (an *) can be used
- Select a specific contract number to see only devices that have the associated contract number, or select the default All.

Step 3 Click **Run Report.** The Registration Summary Report results window appears.

View Registration Summary Report Results

From the Registration Summary Report Results page, you can perform the following options:

- The Report Criteria area indicates the selection criteria used to obtain the displayed results
- All columns can be sorted by clicking the column header

Perform the following steps to use the associated functions on the Registration Summary Report Results page:

Step 1 View the device details for a specific device by clicking a device in the Serial Number column; this displays the Device Report.

Step 2 View the contract details of a selected device by selecting a hyperlinked contract number in the contract number column.

Step 3 For Cisco UCS devices, follow the hostname link to view blade chassis information.

Step 4 Export the report to either an Excel or a PDF format by clicking the corresponding option at the bottom of the report page.

Step 5 To run a new Registration Summary Report, specify different report criteria at the bottom of the page.

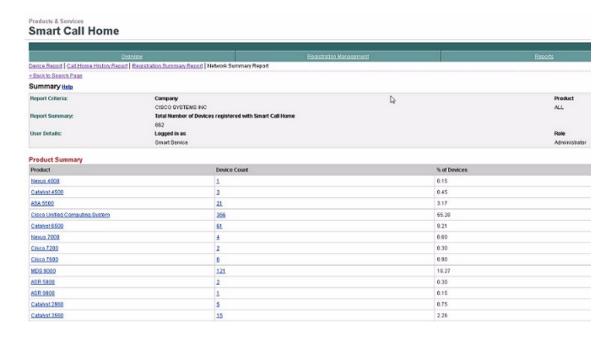**Step 6** Click **Run Report**. The Device Report Results page appears that matches the newly specified parameters.

Figure 3-8   Registration Summary Report

ASA Security Related Details

Support for ASA devices provides additional details on three threat related categories:

- Threat (single context and multi-context)
- Telemetry (single context and multi-context)
- Snapshot (single context and multi-context)

✎

Note   The Threat and Telemetry data can be viewed in a single context or possibly multi-context format, depending on how the ASA security device is configured. You can partition a single security appliance into multiple virtual devices, known as security contexts. Each context is an independent device, with its own security policy, interfaces, and administrators.

Threat, Telemetry, and Snapshot information is available only if you have subscribed to those alert groups when configuring your ASA device (see the ASA Configuration Guide). If the default profile is used during configuration of the device, then threat, telemetry, and snapshot alert groups are subscribed to.

To view the Threat, Telemetry, and Snapshot information:

Step 1   From the main device details page for the ASA device, click the Threat, Telemetry, or Snapshot links.

Step 2   Click **Show Detail** to view details about Threat, Telemetry, or Snapshot information.

Threat (single context)

The threat details section displays three different types of threat reports; one or more threat reports can be displayed at a time:

- Threat Detection Rate (single context)
- Threat Detection Statistics (single context)
- Latest Target and Latest Attacker

Threat Detection Rate (single context)

The Threat Detection Rate table for a single context provides information about various rates at which different threats occur on the device. The Threat Detection Rate table for a single context contains the following threat related items:

- Average (eps)
- Current (eps)
- Event Trigger
- Total Events

The above threat items are provided at varying rates from various security sources, which are listed on the left side of the table. Those sources are:

- 1-hour Interface
- 10-min Scanning
- 10-min Firewall 0
- 10-min ACL drop
- 1-hour ACL drop
- 1-hour SYN attck
- 1-hour Scanning
- 1-hour Firewall 0
- 10-min DoS attck
- 1-hour DoS attck
- 10-min Interface

Threat Detection Statistics (single context)

Provides statistics about various security items on which different threats occur, including traffic, ACL, hosts and servers under attack, including:

- Device Details summary information, which has important details about the selected device.
- Threat Detection Statistics provide information about traffic, ACL hits, latest target hosts, and latest attacker hosts. A single context contains the following threat related information:
- Top 10 1-hour egress traffic (bytes) hosts
- Top 10 1-hour egress traffic (pkts) hosts
- Top 10 20-min egress packet drop hosts
- Top 10 1-hour ingress traffic (bytes) hosts
- Top 10 1-hour ingress traffic (pkts) hosts
- Top 10 20-min ingress packet drop hosts
- Top 10 1-hour egress traffic (bytes) protocols
- Top 10 1-hour egress traffic (pkts) protocols
- Top 10 1-hour ingress traffic (bytes) protocols
- Top 10 1-hour ingress traffic (pkts) protocols
- Top 10 8-hour egress traffic (bytes) protocols
- Top 10 8-hour egress traffic (pkts) protocols
- Top 10 8-hour ingress traffic (bytes) protocols
- Top 10 8-hour ingress traffic (pkts) protocols
- Top 10 24-hour egress traffic (bytes) protocols
- Top 10 24-hour egress traffic (pkts) protocols
- Top 10 24-hour ingress traffic (bytes) protocols
- Top 10 24-hour ingress traffic (pkts) protocols

- Top 10 1-hour ACL hits
- Top 10 8-hour ACL hits
- Top 10 24-hour ACL hits
- Top 10 protected servers under attack

Threat (multi-context)

The Threat category (multi-context) provides a link to threat information in a new Threat Detection Statistics window.

Threat Detection Statistics (multi-context)

The Threat Detection Statistics information is viewed in a new window, which provides statistics about various security items, including:

- Device Details summary information, which has important details about the selected device.
- The Threat Detection Statistic section provides the following threat related information:
  - Top 10 Infected Hosts
  - Top 10 Blocked Ports
  - Shun Host List
  - Dynamic Filter Statistics

Telemetry (single context)

The Telemetry category displays connection/session attributes and provides interface specific attributes. Click **Show Detail** to view the Telemetry information.

From the interfaces list, click a desired interface to see the associated details, which appear below the selected interface.

Telemetry (multi-context)

Depending on how the security appliance is configured, the Telemetry category can represent a multi-context view. The telemetry data in a multi-context configuration displays information for each context from the last telemetry message received by Smart Call Home.

Click **Show Detail** to view the Telemetry information. There are three different types of context representation in the Telemetry

Detection Statistics details:

- System
- Admin
- Userx (where x can be number 1-20)

Telemetry Detection Statistics: System Details

To view the system details of the Telemetry Detection Statistics:

Step 1   In the Telemetry context list, click the **system context;** the Telemetry Detection Statistics page appears, with the system details.

The Telemetry Detection Statistics page, with the system details, contains the following information:

- The top of the page contains the Device Details summary information, which has important details about the selected device.

- The Telemetry summary information provides details about the amount of different types of memory, and identifies the total number of configured contexts.

- The bottom half of this page contains the interface information.

Step 2   Click a specific interface to see the associated details for the selected interface; details of the specific interface appear below the selected interface.

> **Note**   The interfaces for the system context contain all the device interfaces

Telemetry Detection Statistics: Admin Details

To view the admin details of the Telemetry Detection Statistics, perform the following steps:

Step 1   In the Telemetry context list, click the **admin** context; the Telemetry Detection

Statistics page appears, with the admin details. The Telemetry Detection Statistics page, with the admin details, contains the following information:

- The top of the page contains the Device Details summary information, which has important details about the selected device.

- The Telemetry summary information provides details about firewall connections, connection per second and various system resource data (amount and availability of different types of memory, and routing table information).

- The bottom half of the page contains the interface information.

Step 2   From the **interfaces** list, click a specific interface to see the associated details for the selected interface; **details of the specific interface** appear below the selected interface.

Telemetry Detection Statistics: User Details

To view the admin details of the Telemetry Detection Statistics, perform the following steps:

In the Telemetry context list, click one of the user contexts; the Telemetry Detection Statistics page appears, with that specific users details.

The Telemetry Detection Statistics page, with the user details, is very similar to the admin details, but the user context does not have any interface details. The user context details contains the following information:

- The top of the page contains the Device Details summary information, which has important details about the selected device.

- The Telemetry summary information provides details about firewall connections, connection per second and various system resource data (amount and availability of different types of memory, and routing table information).

Snapshot (single-context)

Snapshot data can represent either single or multi-context views, depending on how the security appliance is configured. The snapshot data displays information from the last Snapshot message received by Smart Call Home. To see snapshot data, click **Show Detail** link. Each associated CLI show command name from the last snapshot message is displayed. Click the CLI show command link to view the CLI output for that specific CLI command.

Figure 3-9   Snapshot - Single Context

Figure 3-10   Snapshot Message highlighting show blocks

Snapshot (multi-context)

Snapshot data can represent a multi-context view, depending on how the security appliance is configured. The snapshot data displays information for each context from the last Snapshot message received by Smart Call Home.

The Snapshot Detail page contains the following information:

- The top of the page contains the Device Details summary information, which has important details about the selected device.

- The Snapshot Detail items show the CLI commands that were used since the last snapshot.

Figure 3-11   Snapshot Message - System Context

Cisco Unified Computing System Devices

Device details for Cisco UCS devices contain additional information for system components, including details for chassis, blades, and fabric extenders. To view these details:

Step 1   From the main device details page for the UCS device, click the blade chassis ID link for the component.

Figure 3-12   Device Details Snapshot

Step 2   Click **Show Detail** to view details about the chassis, fabric extender, power supplies, fan units, and blades.

Chassis ID Details

The Chassis ID table contains information about the chassis and the number of slots it contains.

- Chassis ID - Chassis ID
- Description - High-level generic description identifying the type of component
- Product ID - Product ID of the blade chassis
- Serial Number - Serial Number of the blade chassis
- HW Version - HW version of the blade chassis
- Switch ID - Identification of the switch the blade chassis is connected to (A or B)
- Status - Operational state of the blade chassis

Fabric Extender Details

The Fabric Extender detail table contains details of the fabric externder, including:

- Slot - Slot number
- Product ID - Product ID of the fabric extender
- Serial Number - Serial Number of the fabric extender
- HW Version - HW version of the fabric extender
- Switch ID - Switch ID of the fabric extender
- Side - Status of the blade
- Status - operational status of the fabric extender

Blades Details

The Blades detail table contains details of the blades in the blade chassis, including:

- Slot - Slot number - States the slot no.
- Mezzanine Card - provides the card details
- Disk Drive
- CPU
- Memory
- Description - High-level generic description of the blade
- Product ID - Product ID of the blade
- Serial Number - Serial Number of the blade
- HW version - HW version of the blade
- Status - Status of the blade

Cisco Unified Communication Manager (CUCM) Device

Device details for CUCM devices contain additional information for system components, including details for cluster, nodes, license information, telemetry etc. To view these details:

■ **Reports**

Step 1   Enter the search criteria as *UCMGR* for **product ID** to get various CUCM cluster details.

Products & Services
Smart Call Home

Overview	Registration Management	Reports

Device Report | Call Home History Report | Global Summary Report | Registration Summary Report | Service Request Logging Report | Ad-hoc Report | Analysis Report

Cluster Details

< Back to Report Results

Device Details:	Serial Number	Host Name	Product ID	HW Version
	1b4fa266-7384-4517-831c-b22028606b49	10.65.104.31	UCMGR	1.0
	SW Version	**Part Number/Rev**	**Inventory Updated**	**Configuration Updated**
	5.0.0.0-2.i386	Not Available	16-Apr-2013 06:04:58 AM	16-Apr-2013 06:05:34 AM
	Top Assembly Number	**Time Based License**	**Failover Status**	
	Not Available	Not Available	Not Available	

Contact

Show Detail

Cluster Overview

Show Detail

Cluster Name	Publisher Name	Publisher IP
StandAloneCluster	10.65.104.31	10.65.104.31

Provisioned Servers

Name	IP Address	Description
10.65.104.31	10.65.104.31	Not Available
10.65.104.32	10.65.104.32	Not Available

License Information

Show Detail

License Requirements by Type

License Type	Users	Unassigned Devices	Current Usage
CUWL Standard	0	0	0
Enhanced	50	5	5
Enhanced Plus	0	Not Available	0
Essential	0	0	0
TelePresence Room	0	0	0

Total Users and Un-assigned Devices

Total Users	Un assigned Devices
10	15

Enterprise License Manager

Server-Host Name/IP Address	Last-Sucessful-Synchronization
None	No Synchronization has occurred.

Nodes Details

Show Detail

Model	Name	Serial No	Product Type	Product Version	OS Version	BIOS Version	Firmware Version	BIOS Info	CPU Speed	Main Memory
VMware	10.65.104.31	VMware-56 4d aa 04 eb 98 69 8d-03 18 c2 47 93 42 b2 fb	ELM	10.0.0.96000-292	5.0.0.0-2.i386	Not Available	Not Available	PhoenixTechnologiesLTD 6.00 09/22/2009	2670	6G
VMware	10.65.104.32	VMware-56 4d 24 27 97 2b 34 73-9f 9d 7d 8b e8 47 6e e8	ELM	10.0.0.96000-292	5.0.0.0-2.i386	Not Available	Not Available	PhoenixTechnologiesLTD 6.00 09/22/2009	2530	3G

Figure 3-13   CUCM Report - Cluster Details Snapshot

Step 2   Click **Show Detail** to view details about the cluster overview, license information, node details, telemetry and configuration.

Cluster Overview

The Cluster overview table contains information about the cluster and the provisioned servers information:

- Cluster Name - Name of each cluster
- Publisher Name: the name of cluster's publisher
- Publisher IP: the IP address of cluster's publisher
- Provisioned Server name and IP Address with Description

License Information Details

The details contain three tables including:

License requirements by Type

- License Type
- Users
- Unassigned Devices
- Current Usage

Total Users and Unassigned Devices

- Total Users
- Unassigned Devices

Enterprise License Manager

- Server-Host Name /IP Address
- Last-Successful-Synchronization

Nodes Details

The Node details table contains information about different nodes:

- Model
- Name
- Serial No
- Product Type
- Product Version
- OS Version
- BIOS Version
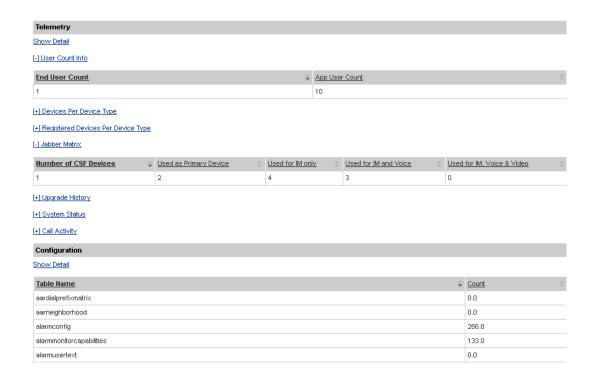- Firmware version
- BIOS info
- CPU Speed
- Main Memory

Figure 3-14   Telemetry and Configuration Details Snapshot

Telemetry

The Telemetry details contains information about user count, device type, history, call activity and status:

User Count Info

- End User Count
- App User Count

Devices per Device Type

- Cluster Name
- Publisher Name
- Device Count
- Model
- Number of Devices

Registered Devices per Device type

Jabber Matrix

- Number of CSF Devices
- Used as Primary Device
- Used for IM only

- Used for IM and Voice
- Used for IM, Voice and Video

Upgrade History

- Hostname
- Info
- Date
- Time

System Status

- Host Name
- Date
- Locale
- Product Version
- OS Version
- License MAC
- Uptime

Call Activity

- Hostname
- Inprogress
- Attempted
- Completed

Configuration

The Configuration details contains information about count per tablename:

- Table name
- Count

Message Details

Configuration Message

The details of this message are displayed as a result of selecting this message type in the Type/Results column of the Call Home History Report Results page.

The details of the selected configuration message contains the following information:

- **Company Name** - The company that is associated with the currently selected device
- **Host Name** - Provides a link to the Device Report Results page, which contains the results for the specified hostname only
- **Message Name** - Indicates the type of message displayed
- **View Message Header** - Provides a hyperlink to the AML Header section of the Call Home message.

- **View Device Output** - Provides a hyperlink to the Device Output (attachments) in the Call Home message.
- **Configuration Details** - provides the date and time the device was last configured
- **Image Name and Feature**
- **Device Configuration**
  - **Running configuration**
  - **Startup configuration**
  - **Technologies and features** running on the selected device (links to Feature Navigator Tool)
  - **Configuration Sanity Analysis** with warnings and recommended actions based on Cisco standard practices. **startup configurations**, technologies and features, and a configuration sanity analysis for the device.

Crash and Diagnostic Messages

The details of these messages are displayed as a result of selecting this message type in the Type/Results column of the Call Home History Report Results page. The details of the selected crash or diagnostic message contains the following information:

- **Company Name** - the company that is associated with the currently selected device
- **Host Name** - provides a link to the Device Report Results page, which contains the results for the specified hostname only
- **Message Name** - indicates the type of message displayed
- **View Message Header** - provides a hyperlink to the AML Header section of the Call Home message.
- **View Device Output** - provides a hyperlink to the Device Output (attachments) in the Call Home message.
- **Overall Results within Analysis Period** contains an overview of the diagnostic failure and contains the following information:
  - Service Request - if a TAC case was opened, a link to the case is provided
  - Technology - indicates the technology that experienced the error; this appears only if a TAC case was opened
  - Sub-technology - Identifies what sub-technology experienced the error; this appears only if a TAC case was opened
  - Problem Code - provided by the diagnostic results; this appears only if a TAC case was opened
  - Problem Details
  - Recommendation
- **Individual Results within Analysis Period** provides details on individual tests and contains the following information:
  - Device - serial number of the device
  - Test Name - click **Show Details** to view the Test Description and Impact of Failure information
  - Recommendation - click **Show Details** to view steps to resolve the issue
  - Count - total number of failures that were encountered when running the diagnostic
  - Status - the ending status of the diagnostic or crash

Note Service Request (SR) information appears in the report only if an SR was successfully raised. The SR parameter information is available only for diagnostic and environmental messages.
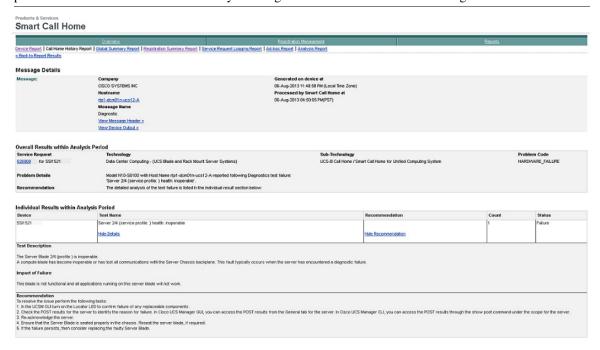

Figure 3-15   Diagnostic Message Snapshot

Environmental Message

The Results for the Environmental messages are based on the analysis done by the system on Call Home messages that are processed within a certain time period, called the "aggregation period". The default value of this time period is five minutes. This time period may be changed by a Cisco administrator.

The details of this message are displayed as a result of selecting this message type in the Type/Results column of the Call Home History Report Results page. The details of the selected environmental message contains the following information:

- **Company Name** - the company that is associated with the currently selected device
- **Host Name** - provides a link to the Device Report Results page, which contains the results for the specified hostname only
- **Message Name** - indicates the type of message displayed.
- **View Message Header** - provides a hyperlink to the AML Header section of the Call Home message.
- **View Device Output** - provides a hyperlink to the Device Output (attachments) in the Call Home message.
- **Overall Results within Analysis Period** contains an overview of the diagnostic failure and contains the following information:
  - Service Request - if a TAC case was opened, a link to the case is provided
  - Technology - indicates the technology that experienced the error; this appears only if a TAC case was opened

- Sub-technology - Identifies what sub-technology experienced the error; this appears only if a TAC case was opened

- Problem Code - provided by the diagnostic results; this appears only if a TAC case was opened

- Problem Details - model number and hostname of the device and the environmental event that occurred

- Recommendation

- **Individual Results within Analysis Period** provides details on individual tests and contains the following information:

  - Device - serial number of the device

  - Test Name - click **Show Details** to view the Test Description and Impact of Failure information

  - Recommendation - click **Show Details** to view steps to resolve the issue

  - Count - The number of times this failure was reported within the time frame of the aggregation timer. The default value of this aggregation period is five minutes.

  - Status - indicates if this is a failure or if the failure is recovered.

Note Service Request (SR) information appears in the report only if a TAC case was successfully raised.

Products & Services

Smart Call Home

| Overview | Registration Management | Reports |

Device Report | Call Home History Report | Global Summary Report | Registration Summary Report | Service Request Logging Report | Ad-hoc Report | Analysis Report

< Back to Report Results

Message Details

Message:	Company	Generated on device at
	CISCO SYSTEMS INC	31-Jul-2013 07:51:09 PM (Local Time Zone)
	Hostname	**Processed by Smart Call Home at**
	rcdn9-dci04n-ucs21-B	31-Jul-2013 12:51:23 PM(PST)
	Message Name	
	Environmental	
	View Message Header >	
	View Device Output >	

Overall Results within Analysis Period

Service Request	Technology	Sub-Technology	Problem Code
626843 for SSI1422	Data Center Computing - (UCS Blade and Rack Mount Server Systems)	UCS-B Call Home / Smart Call Home for Unified Computing System	Error Messages, Logs, Debugs
Problem Details	Model N10-S6100 with Host Name rcdn9-dci04n-ucs21-B reported following Environmental event: 'System minor alarm on power supply 2 failed'.		
Recommendation	The environmental related issues were listed below with an analysis for each condition. Please see the individual results section below for troubleshooting:		

Individual Results within Analysis Period

Device	Test Name	Recommendation	Count	Status
SSI1422			1	Failure
	Hide Details	Hide Recommendation		

Test Description

A Failure is recorded in the Power supply unit. Execute the show environment power command to view the status of power-supply unit that has problem.

Impact of Failure

The device is currently working with only one power-supply unit.

Recommendation

Check if the power cord is properly connected to the power supply and power source. Also ensure that the switch is supplied with 220V. This is the only supported power supply configuration. Also ensure that the power supply is properly inserted and plugged in. If problem persists try re-seating the power-supply unit. If the power supply light is still not green and the status continues to show fail/shutdown then consider replacing the faulty power supply unit.
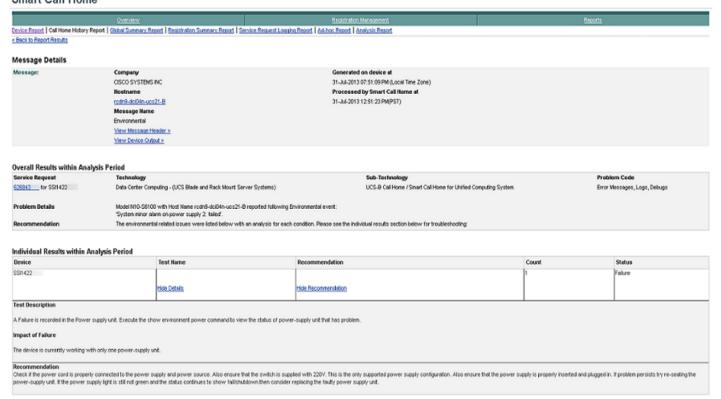
Figure 3-16   Environment Message Snapshot

Inventory Message

The details of this message are displayed as a result of selecting this message type in the Type/Results column of the Call Home History Report Results page.

This page provides information about the details of the selected inventory message. Inventory messages contain the following information:

- Company Name - The company associated with the currently selected device.
- Host Name - Contains the specified host name and provides a link back to the Device Report Results page that contains results for the specified hostname only.
- Message Name - Indicates the type of message displayed.
- View Message Header - Provides a hyperlink to the AML header portion of the Call Home message.
- View Device Output - Provides a hyperlink to the Device Output
  - (attachments) in the Call Home message.
- The Detail area contains an overview of the inventory and contains the following information:
  - Serial Number (hyperlinked to the View Device Details page that shows additional details for the device)
  - Host Name
  - Description
  - Company Name
  - Product ID (PID)
  - Hardware Version
  - Software Version
  - Part Number
  - Top Assembly Number (if applicable)
  - Time Based License
  - Failover Status
  - Inventory Updated (date)

The Serial Number has a hyperlink to the View Device Details page that shows additional details for that device.

> **Note**   Most devices have a one serial number for one host name relationship. VDC devices (Cisco Nexus 7000 Series) will have a one serial number to one or more hostname relationship. VSS devices (Cisco Catalyst 6500 Series) will have a one hostname to one or more serial number relationship.

Performance Message

Performance messages are available for the Cisco Unified Communications Manager (CUCM) only. These messages reflect performance issues raised as the result of a diagnostic test or threshold breech. The details of these messages are displayed by selecting this message type in the Type/Results column of the Call Home History Report Results page. The details of the selected performance message contains the following information:

- **Company Name** - The company that is associated with the currently selected device
- **Host Name** - Provides a link to the Device Report Results page, which contains the results for the specified hostname only
- **Message Name** - Indicates the type of message displayed
- **View Message Header** - Provides a hyperlink to the AML Header section of the Call Home message
- **View Device Output** - Provides a hyperlink to the Device Output (attachments) in the Call Home message.
- **Overall Results within Analysis Period** contains an overview of the performance issue and contains the following information:
  - Problem Details
  - Recommendation
- Individual Results within Analysis Period provides details on individual tests and contains the following information:
  - Device - serial number of the device
  - Test Name - click Show Details to view the Test Description and Impact of Failure information
  - Recommendation - click Show Details to view steps to resolve the issue
  - Count - total number of failures that were encountered when running the diagnostic
  - Status - the ending status of the diagnostic

Request Message

You can use the **call-home request** command on any supported Cisco IOS device to submit information about your system to Cisco in order to receive helpful information specific to your system. You can request a variety of reports, including security alerts, known bugs, best practices, and command references. Smart Call Home passes the required data to the appropriate web application, such as the bug toolkit or output interpreter. That application processes the request and then sends the results back to Smart Call Home to display on the web application.

When a Call Home message of type Request is sent, one of the following Request sub-types is also specified:

- Output-analysis
- Command-reference
- Config-sanity
- Bugs-list
- Product-advisory

The details of this message are displayed as a result of selecting this message type in the Type/Results column of the Call Home History Report Results page.

Note All devices that are Cisco IOS based (Catalyst 4500/4900/6500, Cisco 7200/7300/7600) have availability to CH Request messages. Processing for Call Home Request message is different and depends on the sub-type that is associated to the Call Home Request.

Call Home Request Message - Details

This page provides information about the details of the Call Home Request message. The details of the selected Call Home Request message contains the following information:

- The Message Details area contains a summary of the following information:
  - Company name, device message generation, and Smart Call Home processing times.
  - **Hostname** - Provides a link back to the Device Report Results page, which contains the results for only the specified Hostname

    Company Name - Is the company associated with the selected device.

    Host Name - Contains the specified host name.

> ![Note pencil icon]
>
> **Note**   From the **Back to Report Results** link, you can run the report with the existing pre-filled data, or enter data in any of the other fields.

  - **Message Name** - Indicates the type history report message being displayed; in this case, Request.
  - **View Message Header** - Provides a hyperlink to the AML Header part of the Call Home message.
  - **View Device Output** - Provides a hyperlink to the Device Output attachments) in the Call Home message.
- The Call Home Request Result area contains information germane to the Call Home Request command issued by the user, and contains the following information:

> ![Note pencil icon]
>
> **Note**   The information will vary in the Call Home Request Result area; the information is dependent upon the type of Call Home Request sub-type that was issued in the request.

Figure 3-17   Sample output from request command (config-sanity)

Snapshot Message

Snapshot data can represent either single or a multi-context view, depending on how the security appliance is configured. The snapshot data displays information about CLI commands used since the last Snapshot message was received by Smart Call Home. Both the single context and multi-context versions are described.

Snapshot (Single Context)

The details of this message are displayed as a result of selecting this message type in the Type/Results column of the Call Home History Report Results page.

The snapshot details section for a single context displays the following information:.

Figure 3-18   Snapshot- Single Context

- The top of the page contains message details information, which has important details about the selected message.
- The snapshot details section displays each associated CLI show command that was issued since the last snapshot message.

To see more details about a specific CLI command:

Step 1   Click a CLI command in the list, which opens a new window where the CLI output for that specific CLI command is displayed.

Step 2   The CLI command is above the CLI command output; click **Close Window** to close the Message Details window.

Snapshot (Multi-Context)

The details of this message are displayed as a result of selecting this message type in the Type/Results column of the Call Home History Report Results page.

The snapshot details section, for a multi-context, displays the following information:

Figure 3-19   Snapshot message details (multi-context)

- The top of the page contains the Message Details of the Snapshot message.
- The Context Names section displays the different configured contexts for this device.

To see more details about a specific context, click the link of the context details you want to view; details for that context appear in a new window.

There are three different types of context representation they are:

- System
- Admin
- User (where x can be number 1-20)

Snapshot: System Details

Step 1   In Context Names list, click the system context; the Snapshot message details for the system context appears on another page.

- The top of the page contains the Snapshot message details information.
- The Snapshot CLI command list shows the CLI commands that were used since the last snapshot.

Step 2   Click one of the CLI commands in the list, which opens a new Snapshot Detail window where all the CLI output for that specific CLI command is displayed.

Step 3   Click **Close Window** to close the Snapshot Message Details window.

Step 4   The CLI command is above the CLI command output; click **Close Window** to close the Snapshot Detail window.

Syslog Message

Incoming syslog messages are stored in the message log with each syslog message reporting a distinct problem that is contained in the AML Message description (text, code, time). Only one problem is reported per syslog message, and the details of this message are displayed by selecting this syslog message in the Type/Results column of the Call Home History Report Results page.

During analysis of syslog messages, rules will determine if the syslog message is either supported or unsupported. Unsupported messages will not have any additional rules processing performed and will display only the syslog message information and indicate that this is an unsupported syslog message.

Supported syslog entries have additional rules processing performed, which will include details that are displayed, in most cases, in the Recommendation and Impact of Failure areas.

Rules, on the Cisco backend, perform an analysis of each incoming syslog message. Rules will report those syslog entries in the message log, which are associated with the primary syslog error, in the Overall Recommendation and Individual Results areas.

Rules analyze the message log to see if the same syslog error is reported multiple times, if this is the case then rules will communicate this repetitive nature in the Recommendation and Individual Results areas.

Recommendations for the customer:

- Buffer logging should be enabled since the rules will not have any additional information on the syslog error.
- The time format should be kept in the regular DateTimeStamp format.

Supported Syslog Message - Details

This page provides information about the details of the selected supported syslog message.

Figure 3-20   Supported Syslog Message Details

The details of the supported syslog message contains the following information:

- The Message Details contains a summary of the following information:
  - Company name, device message generation and Smart Call Home processing times.

- **Hostname** - Provides a link back to the Device Report Results page, which contains the results for only the specified hostname. The bottom of the linked Device Report Results page has search parameter fields that you can use to run a new report.

- **Message Name** - Indicates the type history report message being displayed.

- **View Message Header** - Provides a hyperlink to the AML Header part of the Call Home message, lets you view the message content for the syslog information.

- **View Device Output** - Provides a hyperlink to the Device Output (attachments) in the Call Home message.

- The Overall Results area contains an overview of the problem and contains the following information:

- **Service Request -** if a service request was automatically opened based on the Syslog event, details regarding the service request are shown.

- **Problem Details** - reports the error specific to this particular syslog message. The message contains the syslog error/code, from the AML's message description, along with the reporting device's PID and hostname.

Note The problem reported by the Syslog is specific to one message and not based on problems reported by multiple messages that are received within an aggregation period, like Diagnostic and Environmental messages.

- **Recommendation** - points to the Recommendation area in the Individual Results analysis section.

Note You will see information in the Recommendations section only when the message is a supported syslog message; otherwise, you will see 'None' specified.

- The Individual Results area has detailed Syslog message information in the following areas:

- **Syslog Error -** Indicates the name of the syslog message being displayed. Also provides a toggle that shows the test/alert description details for the current syslog message and impact of failure, if applicable.

- **Recommendation** - Identifies the steps to take to either resolve the problem or obtain more information about the problem. This section also provides a toggle that shows the recommendation details for the current syslog message, which identifies recommended steps that should be performed.

Note You will see information in the Impact of Test Failure and Recommendation sections only when the message is a supported syslog message.

Unsupported Syslog Message - Details

The information for unsupported Syslog messages is very similar to the supported Syslog message details. Unsupported syslog messages:

- Have no additional rules processing performed and displays only the syslog message information and indicates that this is an unsupported syslog message.

- The Impact of Failure information will state "Unsupported System Error Message."

- The report displays the reported error and indicates that analysis results are not available.

Telemetry Message

Telemetry data can represent either single or a multi-context view, depending on how the security appliance is configured. The telemetry data displays different connection/session attributes, and provides interface specific attributes.

Telemetry (Single Context)

The details of this message are displayed as a result of selecting this message type in the Type/Results column of the Call Home History Report Results page.

The telemetry message page has two areas of information:

- Telemetry Message details

- Interfaces information

Figure 3-21   Telemetry Message

To see more details about the information on this page, perform the following steps:

Step 1 Export the Call Home Report to Excel or PDF formats by clicking the corresponding option at the bottom of the associated section.

Step 2 Click a specific interface in the interfaces list to see the associated details for the selected interface.

Step 3 Export the Call Home Report to either an Excel or a PDF format by clicking the corresponding option at the bottom of the associated section

Step 4 Click a displayed interface command to hide the details.

Step 5   At the top left-corner of the page click **Back To Report Results**, to return back to the Call Home History Report results page.

Telemetry (Multi-Context)

The Telemetry category can represent a multi-context view, depending on how the security appliance is configured. The telemetry data in a multi-context configuration displays information for each context from the last telemetry message received by Smart Call Home.

The details of this message are displayed as a result of selecting this message type in the Type/Results column of the Call Home History Report Results page.

To see telemetry data for a multi-context, perform the following steps:

In the Telemetry context list, click the context whose details you want to see; the corresponding Telemetry Detection Statistics window appears.

There are three different types of context representation in the Telemetry Detection Statistics details:

- System
- Admin
- User x (where x can be number 1-20)

Telemetry Detection Statistics: System Details

To view and/or export the system details of the Telemetry Detection Statistics:

Step 1   In the Telemetry context list, click the **system** context; the Telemetry Detection Statistics page appears, with the system details.

The Telemetry Detection Statistics page, with the system details, contains the following information:

- The top of the page contains the Message details information, which has important details about the selected message.
- The Telemetry summary information provides details about the amount of different types of memory, and identifies the total number of configured contexts.
- The bottom half of this page contains the interface information.

Step 2   Export the Call Home Report to either an Excel or a PDF format, by clicking the corresponding option at the bottom of the report page.

Step 3   Click a specific interface, in the interfaces list, to see the associated details for the selected interface; details of the specific interface appear below the selected interface.

✎
Note   The interfaces for the system context contain all the device interfaces.

Step 4   Click **Close Window** to close the Telemetry Detection Statistics window.

Telemetry Detection Statistics: Admin Details

To view the admin details of the Telemetry Detection Statistics:

Step 1   In the Telemetry context list, click the admin context; the Telemetry Detection Statistics page appears, with the admin details.

The Telemetry Detection Statistics page, with the admin details, contains the following information:

- The top of the page contains the message details information, which has important details about the message.

- The Telemetry summary information provides details about firewall connections, connection per second and various system resource data (amount and availability of different types of memory, and routing table information).

- The bottom half of the page contains the interface information (see next graphic).

Step 2   Export the Call Home Report to either an Excel or a PDF format, by clicking the corresponding option at the bottom of the report page.

Step 3   Click **Show Detail** for a specific interface, in the interfaces list, to see the associated details for the selected interface; details of the specific interface appear below the selected interface.

Step 4   Click **Close Window** to close the Telemetry Detection Statistics window.

Telemetry Detection Statistics: User Details

To view the admin details of the Telemetry Detection Statistics:

Step 1   In the telemetry context list, click one of the user contexts; the Telemetry Detection Statistics page appears, with that specific users' details.

The Telemetry Detection Statistics page, with users' details, is very similar to the admin details, but the user context does not have any interface details. The user context details contain the following information:

- The top of the page contains the Device Details summary information, which has important details about the selected device.

- The telemetry summary information provides details about firewall connections, connection per second and various system resource data (amount and availability of different types of memory, and routing table information).

Step 2   Export the Call Home Report to either an Excel or a PDF format, by clicking the corresponding option at the bottom of the report page.

Step 3   Click **Close Window** to close the Telemetry Detection Statistics window.

Test Message

The details of this message are displayed as a result of selecting this message type in the Type/Results column of the Call Home History Report Results page.

The details of the selected test message contains the following information:

- The Message Details area contains a summary of the following information:

  - **Company name**, device message generation and Smart Call Home processing times.

  – **Hostname** - Provides a link back to the Device Report Results page, which contains the results for only the specified Hostname (i.e. R1-2). The bottom of the Device Report Results page has search parameter fields that you can use to run a new report; the fields have the following information pre-filled:

  • **Company Name** - Is the company associated with the currently selected device.

  • **Host Name** - Contains the specified host name.

> **Note**   From the linked Device Report Results page you can run the report with the existing pre-filled data, or enter data in any of the other fields.

  – Message Name - Indicates the type history report message being displayed.

  – View Message Header - Provides a hyperlink to the AML Header part of the CH message, lets you view the message content for the Configuration information.

  – View Device Output - Provides a hyperlink to the Device Output (attachments) in the CH message.

• The lower Message Details area contains the test text, which is information contained in the <ch:MessageDescription> tag of the AML Header.

Threat Message

The Threat category, for a single context, provides three different areas of threat assessment information that are associated to the device:

• Threat Detection Rate

• Threat Detection Statistics
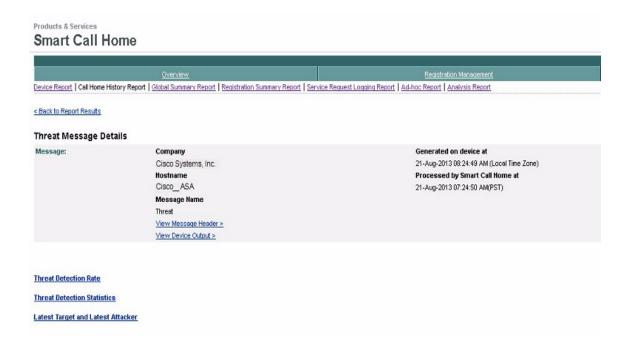
• Latest Target and Latest Attacker

Figure 3-22   Threat Message Details

The threat details section displays three different types of threat reports. One or more threat reports can be displayed at a time:

*   Threat Detection Rate (single context)
*   Threat Detection Statistics (single context)
*   Latest Target and Latest Attacker

Threat Detection Rate (single context)

The Threat Detection Rate table for a single context provides information about various rates at which different threats occur on the device. To view the Threat Detection Rate details for a single context:

Step 1   Click **Threat Detection Rate**; the following information appears below the selected item.

The Threat Detection Rate table for a single context contains the following threat related items:

*   Average (eps)
*   Current (eps)
*   Event Trigger
*   Total Events

The above threat items are provided at varying rates from various security sources, which are listed on the left side of the table; those sources are:

*   1-hour Interface
*   10-min Scanning
*   1-hour Scanning

- 10-min Firewall
- 1-hour Firewall
- 10-min ACL drop
- 1-hour ACL drop
- 10-min Bad pkts
- 10-min ICMP attk
- 1-hour ICMP attk
- 10-min SYN attck
- 1-hour SYN attck
- 1-hour Bad pkts
- 10-min DoS attck
- 1-hour DoS attck
- 10-min Interface

Step 2   Export the Call Home Report to either an Excel or a PDF format by clicking the corresponding option at the bottom of this selected item.

Step 3   Click **Threat Detection Rate** to close the tables.

Threat Detection Statistics (single context)

The Threat Detection Statistics information is viewed in a new window, which provides statistics about various security items (traffic, ACL, hosts, and servers under attack) on which different threats occur. To view the Threat Detection Statistics for single context:

Step 1   Click **Threat Detection Statistics**, which opens the Threat Detection Statistics window.

The Threat Detection Statistics page contains the following information:

- The top of the page contains the Device Details summary information, which has important details about the selected device.
- The Threat Detection Statistic items provide various information about traffic, ACL hits, latest target hosts and latest attacker hosts. A single context contains the following threat related information:
    - Top 10 1-hour egress traffic (bytes) hosts
    - Top 10 1-hour egress traffic (pkts) hosts
    - Top 10 20-min egress packet drop hosts
    - Top 10 1-hour ingress traffic (bytes) hosts
    - Top 10 1-hour ingress traffic (pkts) hosts
    - Top 10 20-min ingress packet drop hosts
    - Top 10 1-hour egress traffic (bytes) protocols
    - Top 10 1-hour egress traffic (pkts) protocols
    - Top 10 1-hour ingress traffic (bytes) protocols
    - Top 10 1-hour ingress traffic (pkts) protocols
    - Top 10 8-hour egress traffic (bytes) protocols

- Top 10 8-hour egress traffic (pkts) protocols
- Top 10 8-hour ingress traffic (bytes) protocols
- Top 10 8-hour ingress traffic (pkts) protocols
- Top 10 24-hour egress traffic (bytes) protocols
- Top 10 24-hour egress traffic (pkts) protocols
- Top 10 24-hour ingress traffic (bytes) protocols
- Top 10 24-hour ingress traffic (pkts) protocols
- Top 10 1-hour ACL hits
- Top 10 8-hour ACL hits
- Top 10 24-hour ACL hits
- Top 10 protected servers under attack

Step 2   Click **Show Detail** on any item in the Threat Detection Statistics table to obtain more information about that related item.

Step 3   Click **Close Window** to close the Threat Detection Statistics window.

Latest Target and Latest Attacker

The Latest Target and Latest Attacker link provides the latest target host and subnet list. To view the Latest Target and Latest Attacker details:

Step 1   Click **Latest Target and Latest Attacker**; the following information appears below the selected item.

- Latest Attacker Hosts
- Latest Target Hosts

Step 2   You may Export the Call Home Report to either an Excel or a PDF format by selecting the corresponding option at the bottom of the section.

Step 3   Click **Latest Target and Latest Attacker** link to close the table.

Product Advisories

The product advisory feature performs several tasks that keep the customer up-to-date on any advisory that may affect the devices on their network. The tasks that the product advisory feature performs are:

- Finds the latest product advisory data based on inventory messages from the device.
- Monitors for any new or updated advisory data and maintains the latest advisory data for all devices.
- Utilizes the device's latest advisory data to display on device reports.
- Utilizes all advisory data discovered from Inventory associated with the selected company and displays advisory summary for the customer
- From registered devices, process request messages that have a sub-type of "Product Advisory" and send a notification to the customer.
- Reflects the results from the Request message in the Device and History Reports.

The three scenarios that trigger product advisory action are:

- An inventory Call Home message has arrived from a device and Smart Call Home has detected new or updated inventory at the component level. Smart Call Home checks to see if there are any product advisories for the new inventory in the following areas:

  - Hardware EOX

  - Software EOX

  - Field Notices

  - PSIRTs

- A Call Home Request with a Product Advisory sub-type message arrived from a device and Smart Call Home detected a new or updated inventory at component level. Smart Call Home checks to see if there are any product advisories in the following areas:

  - Hardware EOX

  - Software EOX

  - Field Notices

  - PSIRTs

- A Configuration Call Home message arrived from a device and Smart Call Home detected a new or updated configuration. Smart Call Home checks to see if there are any product advisories for the configuration in the following areas:

  - Software EOX

  - PSIRTs