SMART CALL HOME

Software Release 4.2.4.1

Septemeber, 2018

Cisco Systems, Inc.
www.cisco.com

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

Introduction to Cisco Smart Call Home

This chapter provides an overview of the Cisco® Smart Call Home service and covers the following areas:

Features and Benefits

Smart Call Home is an automated support capability that monitors Cisco devices on your network. It flags issues and initiates resolution before your business operations are affected.

Smart Call Home is included with many Cisco service contracts, including Cisco SMARTnet®, Smart Net Total Care, Partner Support Service, Smart Care, and Mission Critical Support Service.

Smart Call Home includes:

- Automated around the clock device monitoring and analysis of potential problems
- Proactive alerts sent to your inbox
- Expedited support from the Cisco Technical Assistance Center (TAC)
- Customized status reports and performance analysis
- Product alerts like PSIRTs and field notices

Smart Call Home offers increased operational efficiency by providing customers the ability to:

- Use staff resources more efficiently by reducing troubleshooting time.
- Generate Support cases to Cisco TAC automatically, routed to the appropriate support team, which provides detailed diagnostic information that speeds problem resolution

Smart Call Home offers fast, web-based access to needed information that provides customers the ability to:

- Review all Call Home messages, diagnostics, and recommendations for remediation in one place
- Check TAC case status quickly
- View the most up-to-date inventory and configuration information for all Call Home devices

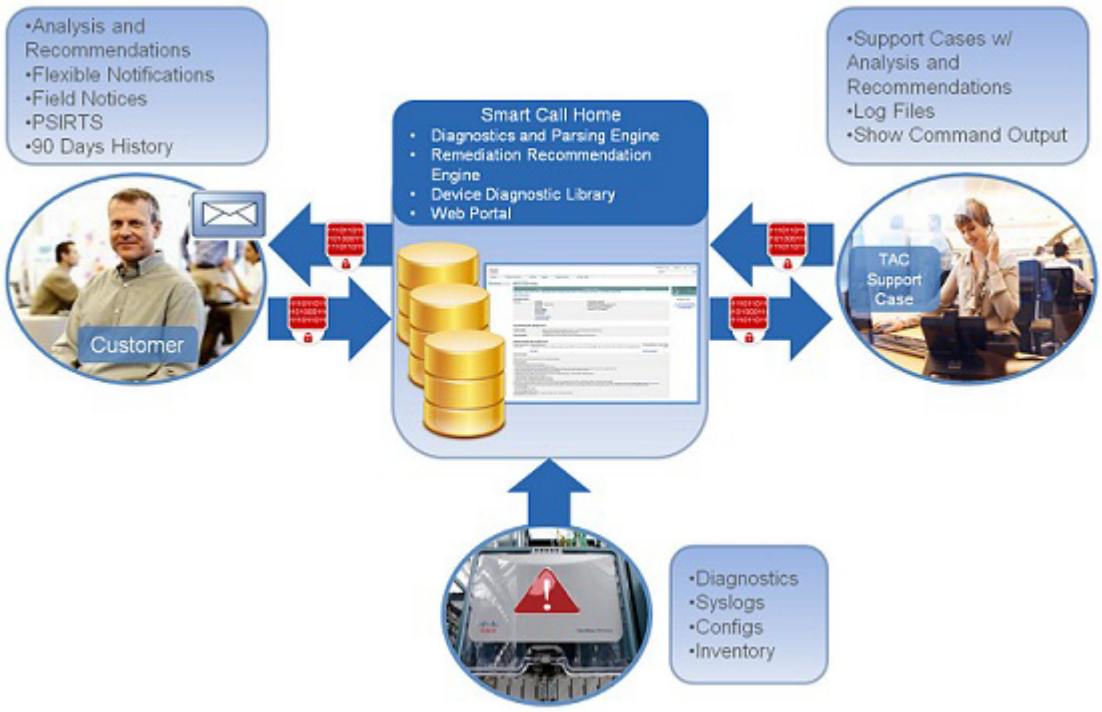


Figure 1-1 Overview of Smart Call Home

Smart Call Home Interaction with Call Home

Call Home is a product feature embedded in the operating system of Cisco devices. It detects and notifies the user of a variety of fault conditions. Smart Call Home is a service capability that adds Cisco intellectual capital as well as automation and convenience features designed to enhance the basic Call Home functionality.

Smart Call Home provides proactive messaging by capturing and processing Call Home diagnostics and inventory alarms. The Call Home feature on the Cisco device provides the capability for a customer to configure Call Home profiles that define:

- Events/severity levels of interest
- Destination addresses
- Transport methods
- Message formats

A profile combines alert group subscriptions with a transport type and destination. Within a profile a customer can select events of interest by subscribing to specific alert groups which define specific actions to take when certain events occur. Figure1- 2 is an example of possible Call Home alert groups that can be configured for Cisco IOS® devices. Consult the Call Home chapter of your product's configuration guide to understand all of the possible alert groups and severity levels.

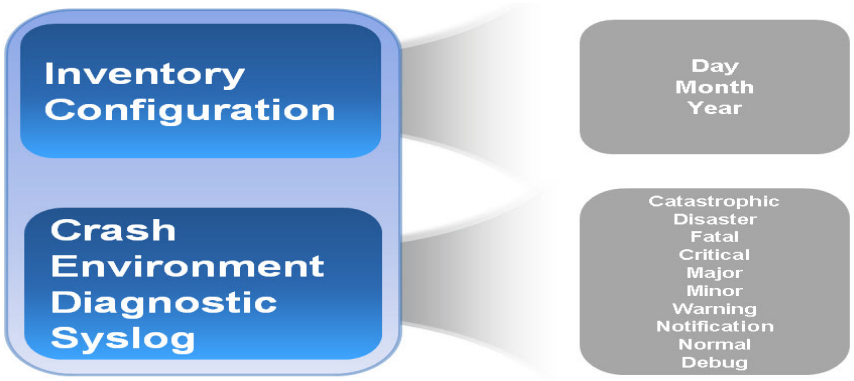


Figure 1-2 Call Home Alert Groups for Cisco IOS Devices

A device can send Call Home messages to Smart Call Home using one of the following transport methods Figure 1-3:

- HTTP(S) direct from device to Cisco
- HTTP(S) via the transport gateway to Cisco
  - HTTP from device to the transport gateway
  - Email from device to the transport gateway

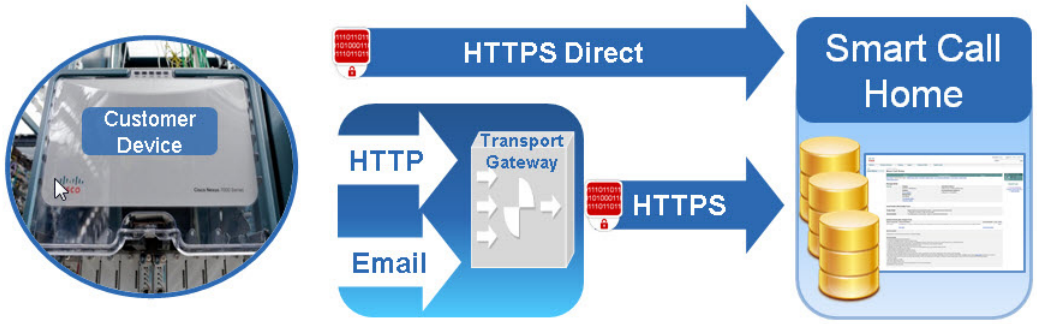


Figure 1-3 Transport Options

Once Smart Call Home is enabled, Call Home messages/alerts are sent to Smart Call Home. These messages/alerts include:

- Inventory
- Configuration
- Diagnostic
- Environmental
- Syslog

If a diagnostic, environmental, or syslog alert is critical enough, a Cisco TAC case is automatically generated, with debug and other CLI output attached to the case. For information regarding generated alerts and if those alerts create TAC cases, review the Smart Call Home Monitoring Details.

Customers receive email notification of Call Home alerts and events. These emails contain links to the Smart Call Home web application, or portal, as well as links to the Cisco TAC case if one was automatically created.

System Requirements for Smart Call Home

The following are the system requirements that are needed to support the Smart Call Home service:

- The Cisco device must be supported under a valid Cisco service contract. If the device is not covered by a service contract, the device can be registered for a 120-day trial period. The contact person's Cisco user profile must be associated with a valid service contract to entitle access to TAC cases/service requests. For more information, consult the Smart Call Home preliminary checklist.
- The Cisco device must be able to reach the Smart Call Home Cisco backend, which receives the Call Home messages from the Cisco device and sends out Smart Call Home email notifications, reports, and information.
- The device must be supported by Smart Call Home and have the minimum OS requirements.
- A Cisco.com ID associated with an appropriate Cisco service contract for your company. Example service contracts include Cisco SMARTnet®, Smart Net Total Care, Partner Support Service, Smart Care, and Mission Critical Support Service. To check what contracts are associated to your Cisco.com ID, go to https://tools.cisco.com/RPFA/profile/profile_management.do.

Transport Gateway Software Package

The Transport Gateway is an optional software package that can be downloaded and installed to enable the Call Home environment to securely send messages to Smart Call Home via the Transport Gateway. The transport gateway software can be installed on a Windows or Linux server. The transport gateway receives HTTP messages or emails from various devices or retrieves messages from a local email inbox and then forwards these messages to Smart Call Home.

Note

- The software package must be installed and configured before Call Home messages can be successfully sent to and received by Smart Call Home.
- The Transport Gateway software download is available to registered Cisco.com users only.

Getting Started with Smart Call Home

The following identifies the high-level steps to enable and use Smart Call Home.

1. Register for a Cisco.com ID, ensuring that the appropriate service contracts are associated to that Cisco.com ID.
2. Identify the devices and software supported by Smart Call Home.
3. Decide what type of transport option to use. If using a transport gateway, refer to the Transport Gateway Deployment Guide and Using the Transport Gateway
4. Download the Smart Call Home Quick Start Guide for your device type.
5. Configure your device.

6. Send an initial inventory message to start the registration process.
7. When the email is received, follow the link to register the device. If the device is not under an active support contract, it will be granted a 120-day pilot registration. First time users are prompted to accept the Smart Call Home user agreement during the first login.
8. Monitor the contact email address for email from call-home-notify@cisco.com to confirm that registration is complete.

For more information, consult the Smart Call Home Deployment Guide.

Installation and Configuration

Resources for Installing and Configuring Smart Call Home

Preliminary checklist: Use this checklist to make sure your Cisco.com ID, Bill-to ID, and contract information are appropriately related for entitlement.

Deployment Guide: This is your go-to document for deploying Smart Call Home. Use this document to configure and register your devices.

Transport Gateway Deployment Guide: This details how to implement the transport gateway software for use as a proxy for Call Home messages.

Quick Start Guides: These documents exist for each product and contain the CLI commands needed to configure your devices to use Smart Call Home, by transport option. Use these in conjunction with the Deployment Guide.

Configuration Guides: These are Call Home chapters from the product configuration guides. They contain detailed information about Call Home, such as alert groups and executed commands, severity and syslog level mapping, how to modify a destination profile, and adding show commands to an alert group. Use this document to fine-tune Call Home functionality.

Enabling Smart Call Home

There are four steps to enable Smart Call Home:

1. Identify devices
2. Select the transport method
3. Configure devices
4. Register devices

Identify Devices

Consult the supported products table to identify those devices supported by Smart Call Home. Some devices may require a code update to a version of the operating system that has the Call Home feature. The supported products table contains the minimum software requirements.

Select the transport method

Choose the transport method to send Call Home messages from your devices to Cisco. The available transport methods are:

- HTTPS direct
- HTTPS via the transport gateway
- Email via the transport gateway

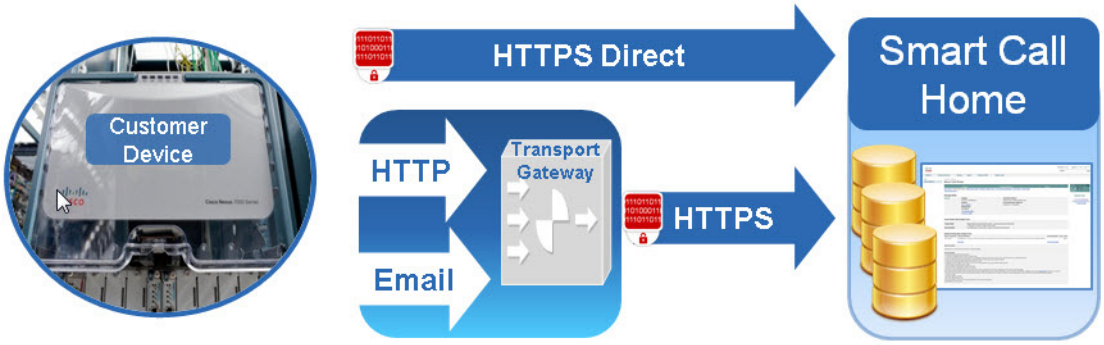


Figure 2-1 Transport Options

HTTPS direct is the Cisco recommended and most commonly used method. Very few devices do not support the HTTPS direct transport method.

The transport gateway is software that can be installed on a Windows or Linux server. The transport gateway receives HTTP messages or emails from various devices or retrieves messages from a local email inbox and then forwards these messages to Smart Call Home. To install a transport gateway, consult the Smart Call Home: Deploying the Transport Gateway on a Cisco Unified Computing System and Red Hat Linux. Refer Chapter 4, "Using the Transport Gateway"

The transport gateway is not required when:

- All devices can send messages directly to Cisco.com using HTTPS
- The encryption capabilities of all managed devices meet the customer's security requirements

The transport gateway is required when:

- Managed devices do not have direct access to Cisco.com
- An HTTP proxy server is required to reach Cisco.com
- Encryption is required for devices that support SMTP communication only

The transport gateway is desirable when:

- The customer wishes all outbound traffic to be sourced from a single device
- The customer does not wish to install a certificate on every managed device
- The customer wishes to use SMTP on the LAN while communicating securely over the Internet

Configure Devices

Each device must be configured for the Call Home feature to start monitoring the device for common environmental alarms, periodic diagnostic tests, and system logs (syslogs).

Cisco IOS configuration tasks are performed with level 15 user access and in configuration mode. A network operations engineer can take these configuration tasks and repeat them on multiple similar platforms to quickly accomplish the deployment task. To configure devices, refer the SCH Deployment Guide and the Quick Start Guide for your devices.

Call Home Profiles

A profile combines alert group subscriptions with a transport type and destination. For Cisco IOS devices, the default profile CiscoTAC1 subscribes to common alert groups and sends messages to Smart Call Home via email. It is possible to adjust some of these options and to create additional custom profiles.

Each product configuration guide contains instructions for creating a custom user profile. Links to the Call Home chapters of the device configuration guides for supported devices are available on Cisco.com.

Alert Groups

An alert group enables and configures access to specific source of data within the device. For example, common alert groups exist for the system log (syslog), booth and run-time diagnostics, environmental sensors, the start and running configurations, and inventory.

For Cisco IOS® devices, you can choose the alert group subscriptions included in the default profile, or create a custom profile to subscribe to specific alert groups. Each alert group can then be further specified by frequency and severity. For Cisco Nexus® and Cisco UCS® devices, the severity is set at the profile level.

Each product configuration guide contains the options for alert group subscriptions. Links to the Call Home chapters of the device configuration guides for supported devices are available on Cisco.com.

Register Devices

Once devices have been configured, the contact email address specified in your configuration will receive one of three emails (for each device):

Confirm registration: The first device on a contract much be confirmed in the Smart Call Home portal in order to verify that the user is entitled to raise support cases for the contract. Follow the instructions contained in the email to confirm registration.

Success: The device and user are successfully registered for the full Smart Call Home service.

POC: The device is registered for 120 days. The contact email address will receive notifications, analysis, and recommendations from Smart Call home, but any support cases raised will not be routed to a TAC engineer for resolution. This is because either the user or the device are not linked to a valid service contract.

Call Home Alert Groups and CLI Commands

Each product configuration guide contains the alert groups and the executed CLI commands for each alert group. Links to the Call Home chapters of the device configuration guides for supported devices are available on Cisco.com.

Using AAA on the Cisco Device

If AAA is configured on the Cisco device then a user account with username **callhome** must be configured on the AAA server. The password options for the account may be defined by the server administrator.

Commands listed in the configuration guides need to be authorized on the Call Home device so that the Call Home service can be authorized to issue these commands. Authorize only those commands that are appropriate for the type device in your network.

Callhome will only verify the authorization of command execution and will not send any authentication requests to ACS. Callhome will just pass its username (callhome) to AAA module if device has authorization on command execution enabled.

Note If username callhome with privilege level 15 is configured on AAA server then it is not required to configure callhome user on the device. For respective device families, refer to the device configuration guides on enabling aaa-authorization for call home .

Smart Call Home Portal Web Application

: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 Related Tools section, the Registered Devices link, and the links under the Manage Device Groups heading are available on the Overview page only.

Product Eligibility Tool

This tool allows users to upload SNTC and PSS generated inventory details in the form of either ANSR Reports or Contract Insight Reports. The Product Eligibility tool analyses the Item List page of these reports and returns an updated report indicating:

- whether devices are SCH-capable
- the minimum OS needed for eligible devices
- device contract status

The tool uses specific product SKUs or PIDs to generate a definitive ‘yes’ or ‘no’ answer for product eligibility and provide the minimum OS version required for each device chassis. If a device is SCH-capable but below the minimum OS version required, then the report will list the specific OS version to which it must be upgraded before SCH can be enabled.

Procedure to upload an inventory file:

Step 1 In the Related Tools section, click **Product Eligibility Tool.**

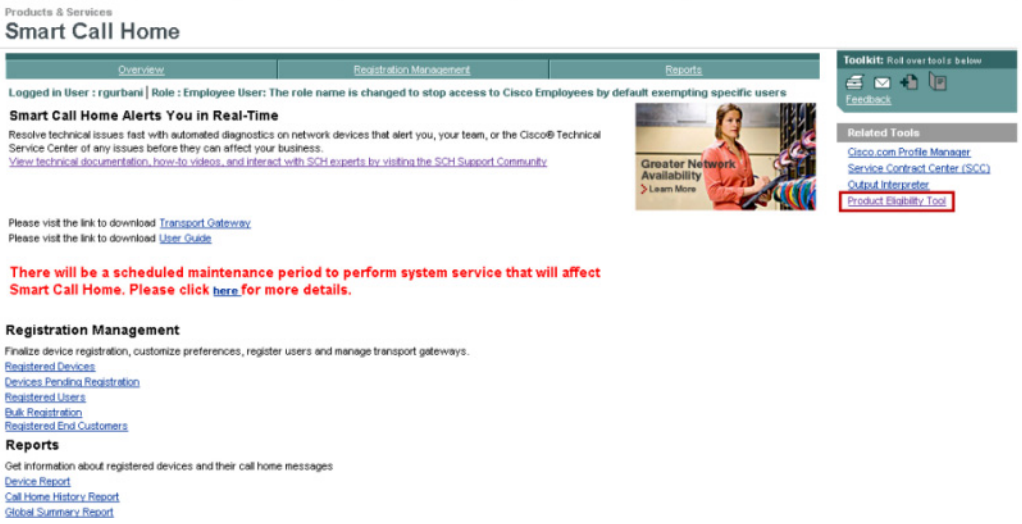


Figure 3-1 Smart Call Home Overview page Snapshot

The Product Eligibility Tool page appears.

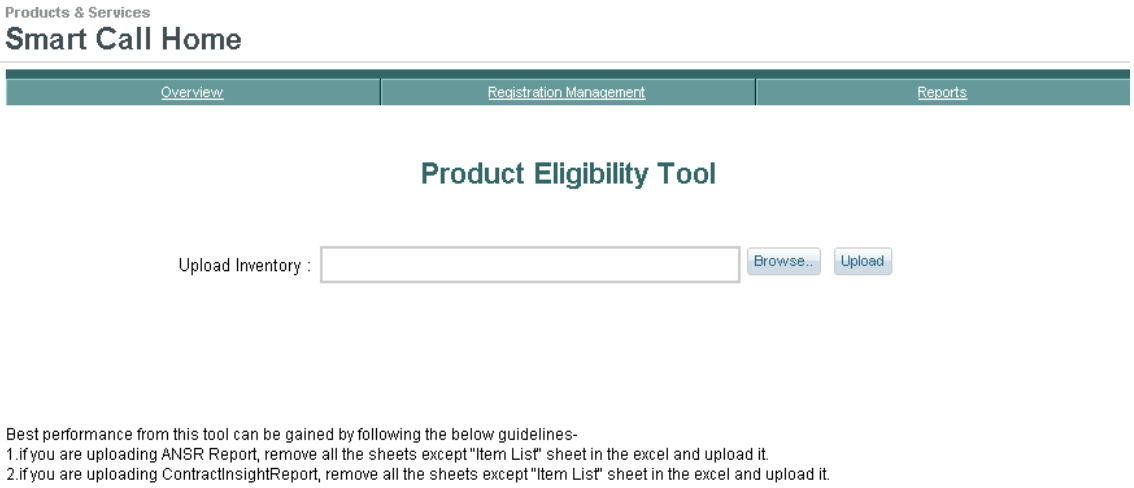


Figure 3-2 Product Eligibility Tool Snapshot

Step 2 Click **Browse** to navigate to the location of an inventory file. Users can upload two types of files: ANSR Reports and Contract Insight Reports. Chosen files should have either .xlsm or .xls file extensions. Ensure the size of each file is less than 5MB before uploading. You can either upload both the files or any one file of a product.

Note Before uploading your report, ensure to remove all the sheets except the **Item List** sheet in the Excel file. These instructions are provided on-screen below the Upload Inventory field.

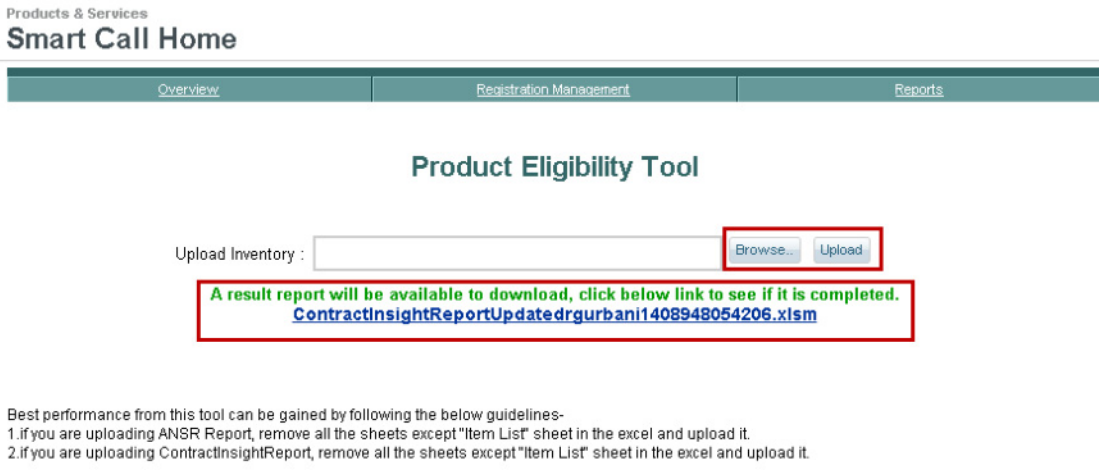


Figure 3-3 Uploading Files

Step 3 Click **Upload** to upload the selected file.
The tool displays the report status and provides a link to download the processed report. If you want to upload a second file, refer **step 2**.

Note If you upload more than 2 files in one session, the tool will display the following error message: *The tool is currently loaded with enough requests and is processing. Try after sometime.*

Step 4 Click on the report link to download the report. Once the report is processed successfully, you can download the report **only once.**

The generated report adds 3 columns to the Excel spreadsheet titled SCH Capable, OS Version, and Contract Status. If the device is SCH-capable but below the minimum OS version required, then the OS version column displays the specific version to which the device must be upgraded.

SCH Readiness Check Tool

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.

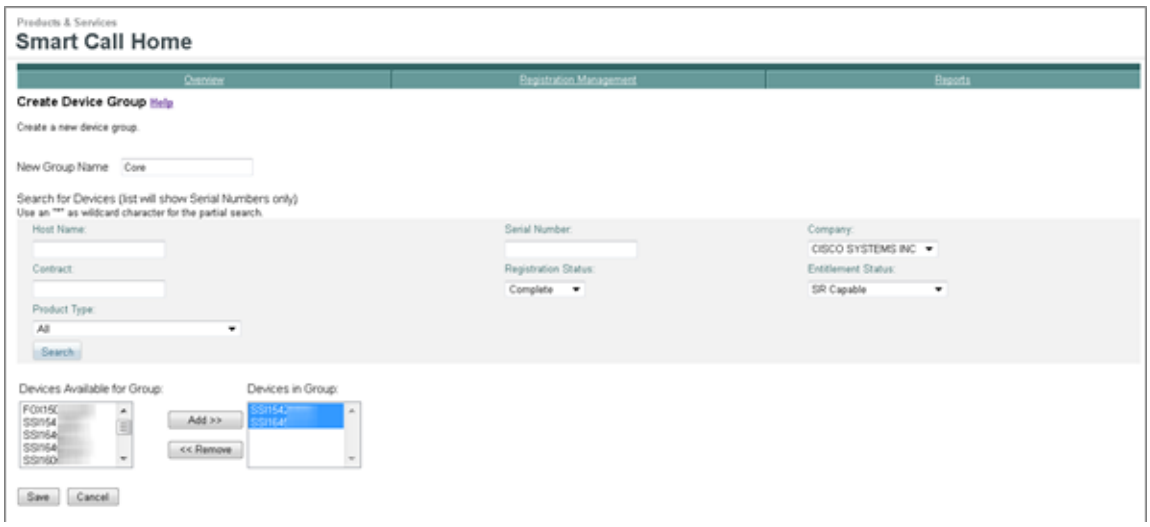


Figure 3-4 Create Device Group

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 Table3-1 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 3-5 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.**

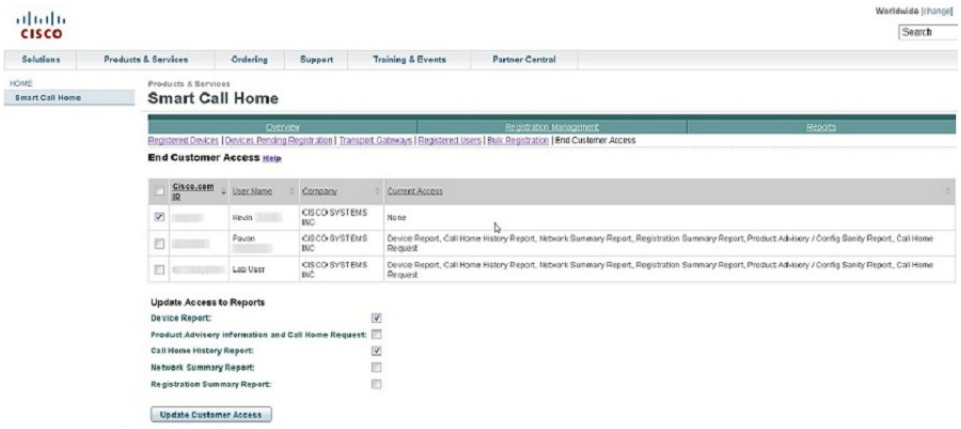


Figure 3-6 End Customer Access

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	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 Select the preferred service request communication as **Email** or **Phone**. By default, **Email** is the preferred communication.

Note
- To apply service request communication to all the devices, choose **Apply to all the devices for this company**.
- To reset all the devices, choose **Reset all the devices for this company**.

Step 9 Make desired changes to the list of email addresses that receive Smart CallHome notifications using **Add** and **Remove** options.

Step 10 Add additional email addresses for notifications in the field provided.

Step 11 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.

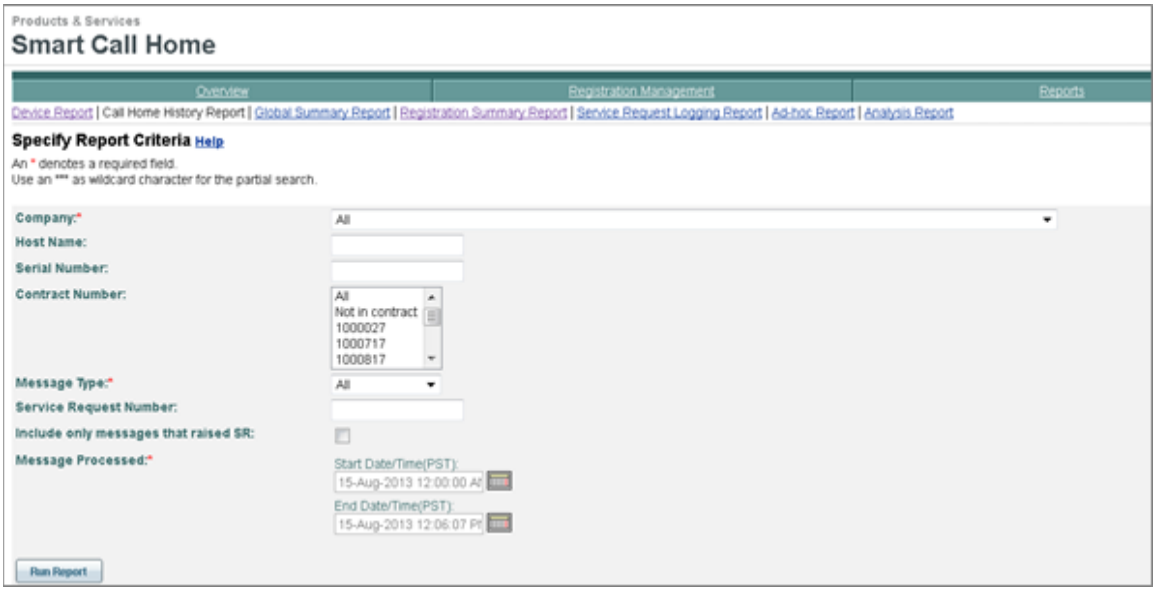


Figure 3-7 Specify report Criteria Snapshot

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.

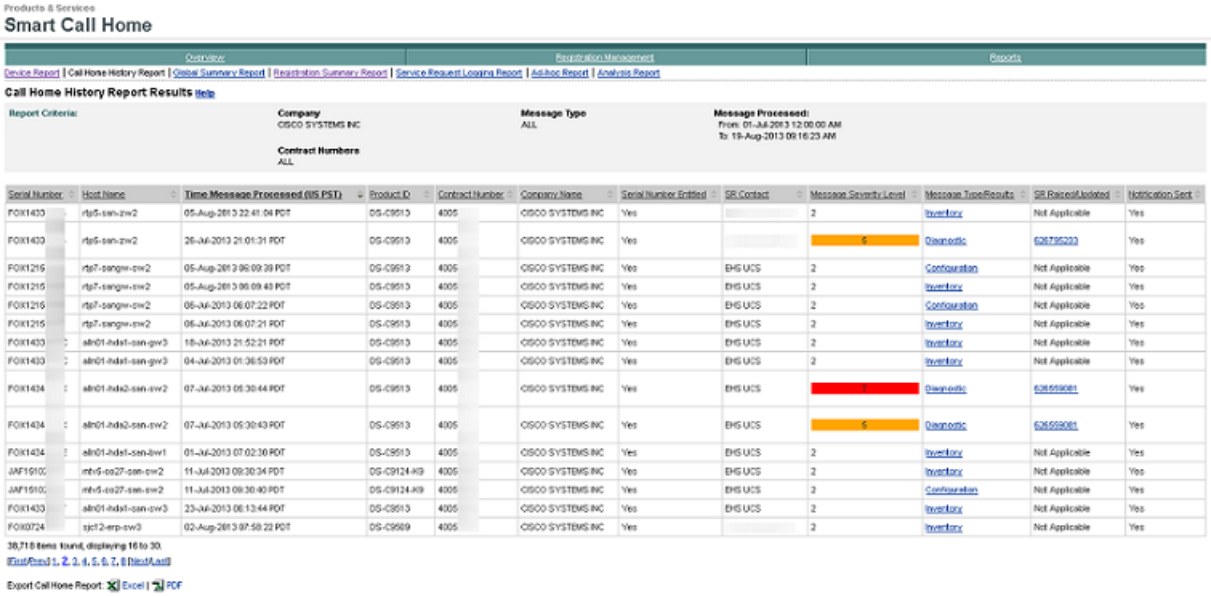


Figure 3-8 Call Home History Report Snapshot

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.

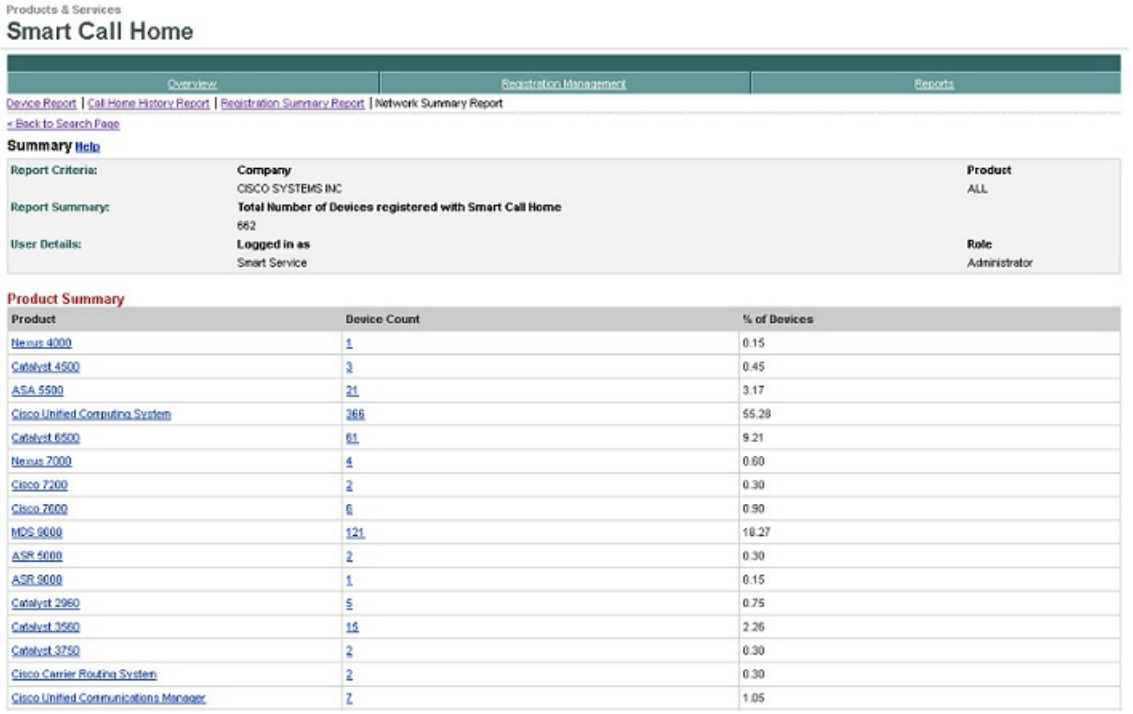
Note The **All** option is available only when the user is registered to more than one company.

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.


Products & Services

Smart Call Home

Overview | Registration Management | Reports

Device Report | Call Home History Report | Registration Summary Report | Network Summary Report

< Back to Search Page

Summary Help

Report Criteria:	Company CISCO SYSTEMS INC	Product ALL
Report Summary:	Total Number of Devices registered with Smart Call Home 662	
User Details:	Logged in as Smart Service	Role Administrator

Product Summary

Product	Device Count	% of Devices
Nexus 4000	1	0.15
Catalyst 4500	3	0.45
ASA 5500	21	3.17
Cisco Unified Computing System	366	55.28
Catalyst 6500	61	9.21
Nexus 7000	4	0.60
Cisco 7200	2	0.30
Cisco 7600	6	0.90
MDS 9000	121	18.27
ASR 5000	2	0.30
ASR 9000	1	0.15
Catalyst 2960	5	0.75
Catalyst 3560	15	2.26
Catalyst 3750	2	0.30
Cisco Carrier Routing System	2	0.30
Cisco Unified Communications Manager	7	1.05

Figure 3-9 Network Summary Report - All Products

This page contains two sections:

- 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

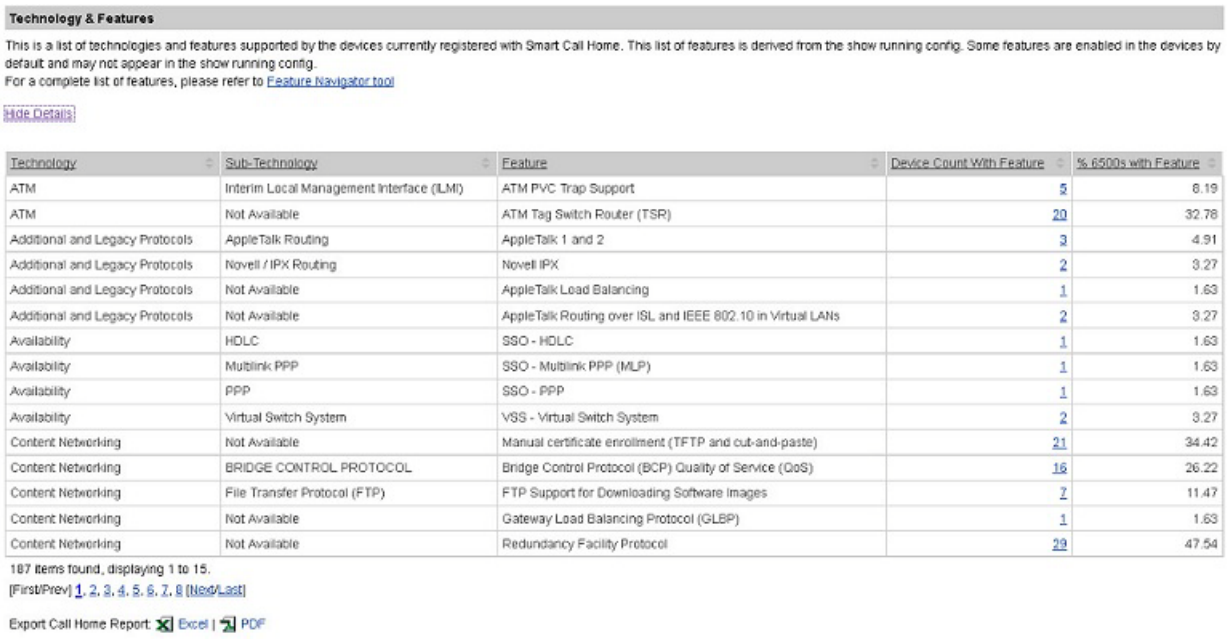
The Advisories area contains the:

- 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 3-10 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.

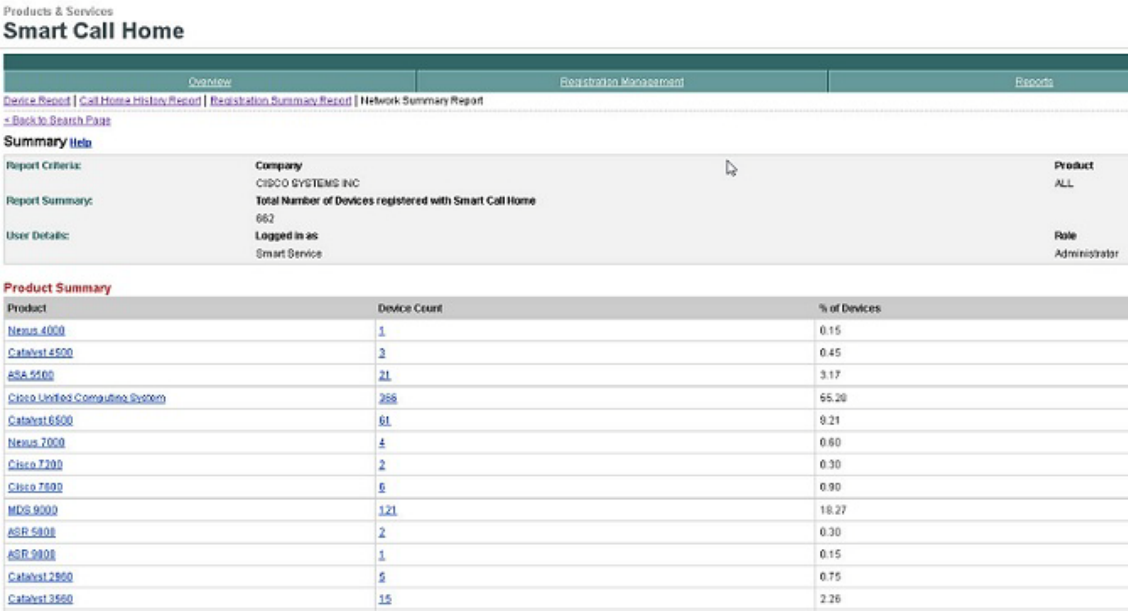


Figure 3-11 Registration Summary Report

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 3-12 Snapshot - Single Context

Figure 3-13 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.

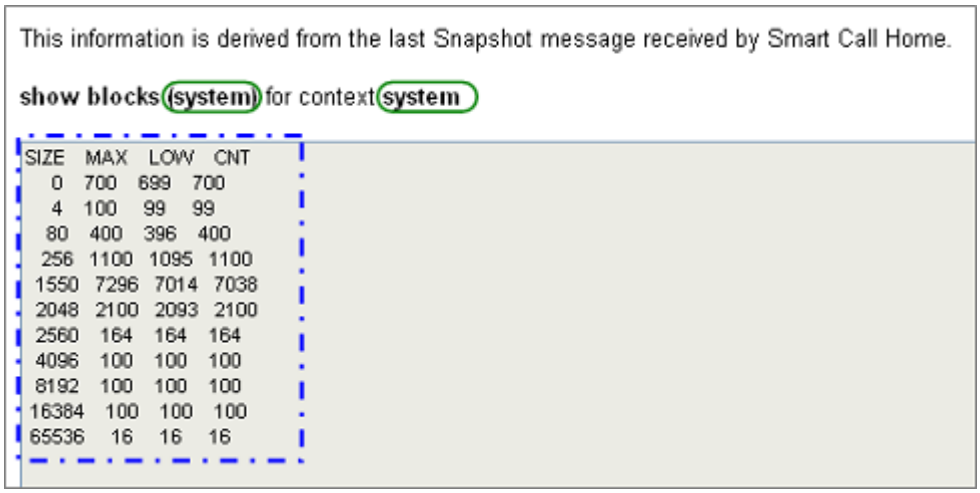


Figure 3-14 Snapshot Message - System Context

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.

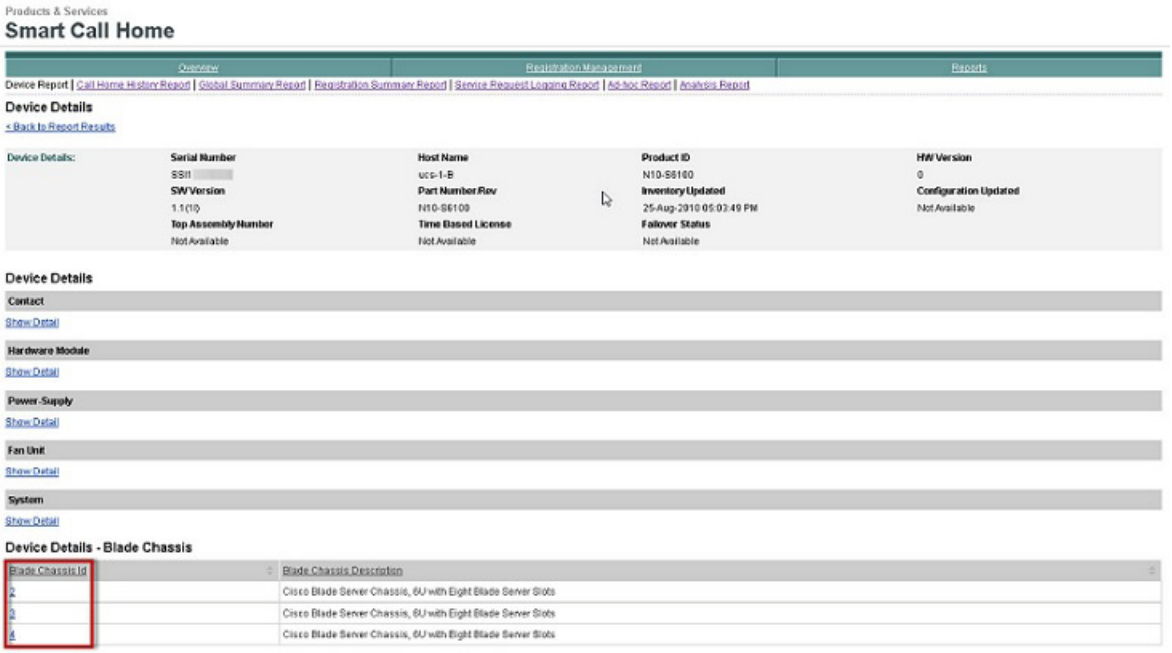


Figure 3-15 Device Details Snapshot

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:

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 3-16 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

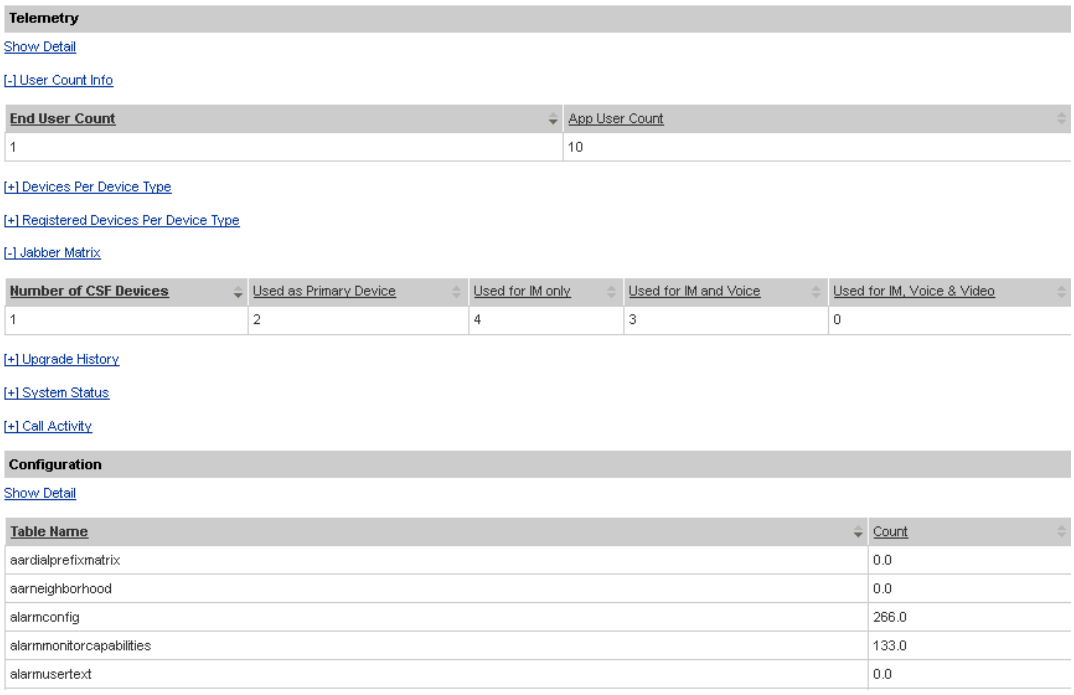
Enterprise License Manager

- 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



Telemetry

Show Detail

[-] User Count Info

End User Count	App User Count
1	10

[+] Devices Per Device Type

[+] 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 & Video
1	2	4	3	0

[+] Upgrade History

[+] System Status

[+] Call Activity

Configuration

Show Detail

Table Name	Count
aardialprefixmatrix	0.0
aarneighborhood	0.0
alarmconfig	266.0
alarmmonitorcapabilities	133.0
alarmusertext	0.0

Figure 3-17 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.

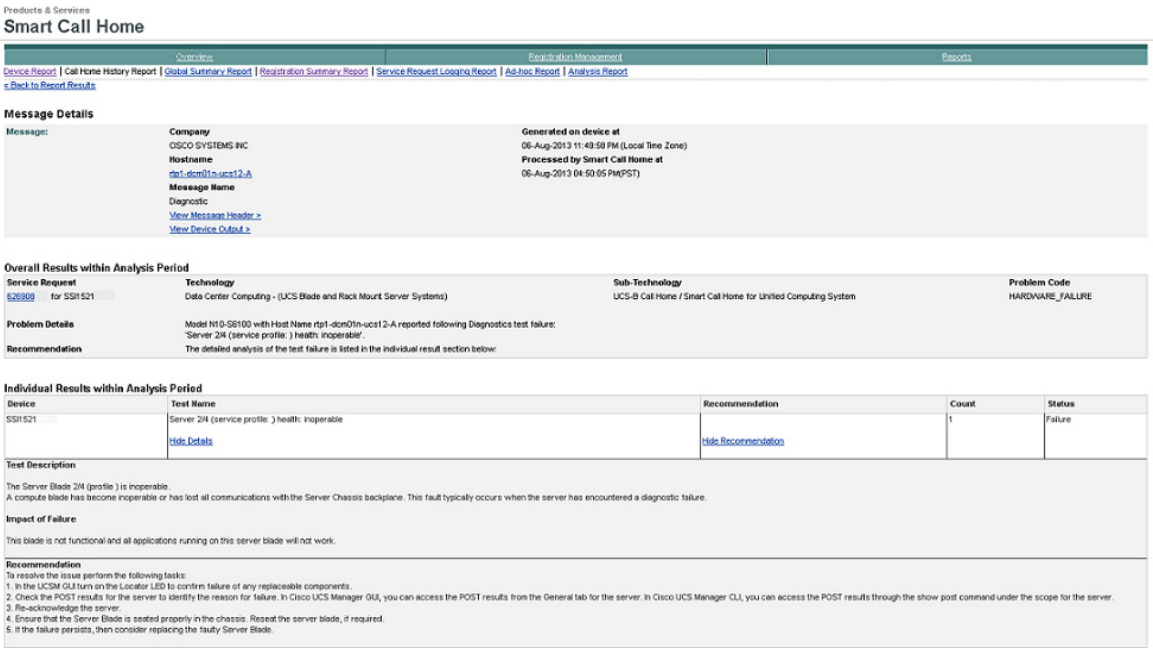


Figure 3-18 Diagnostic Message Snapshot

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.

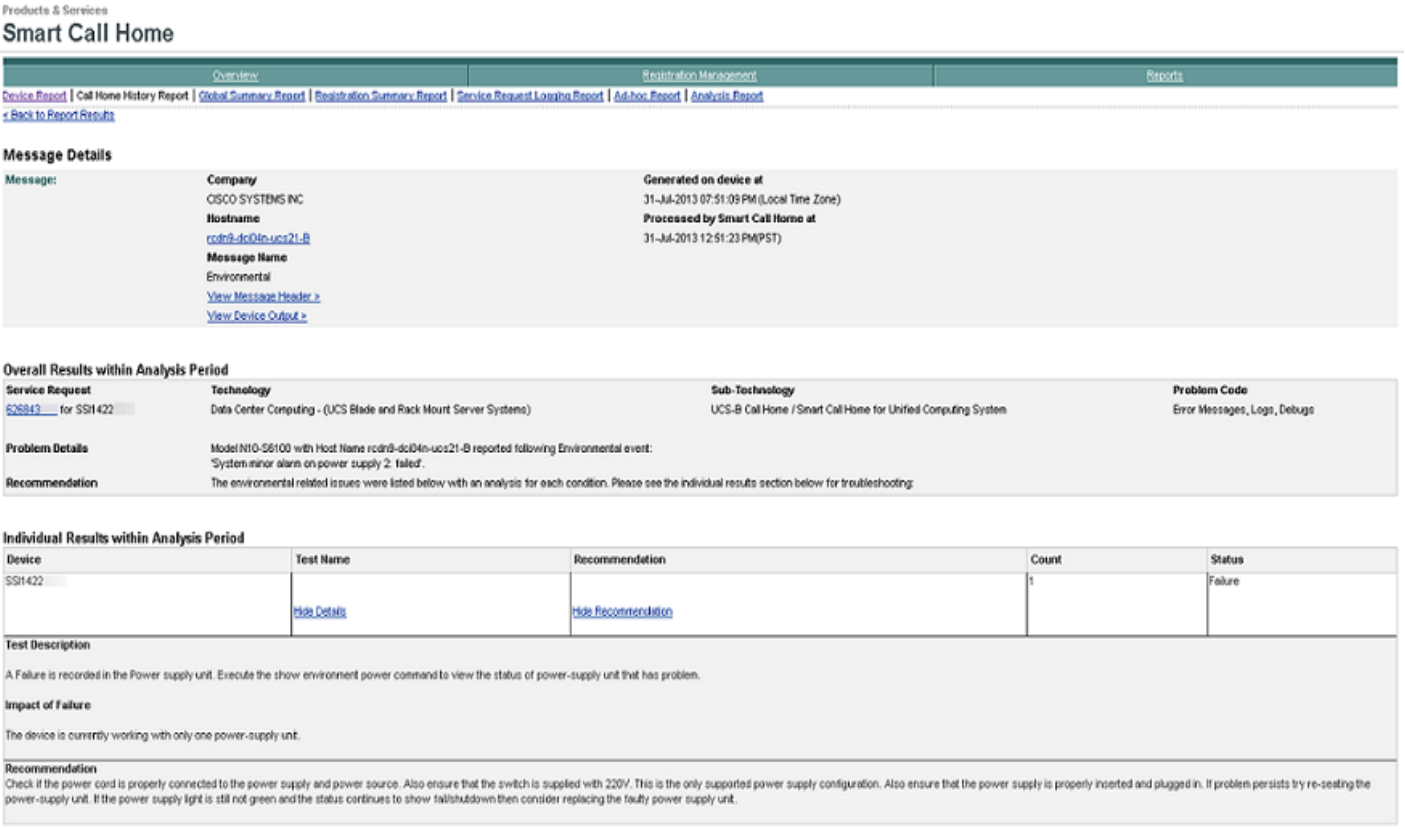


Figure 3-19 Environment Message Snapshot

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 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 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.

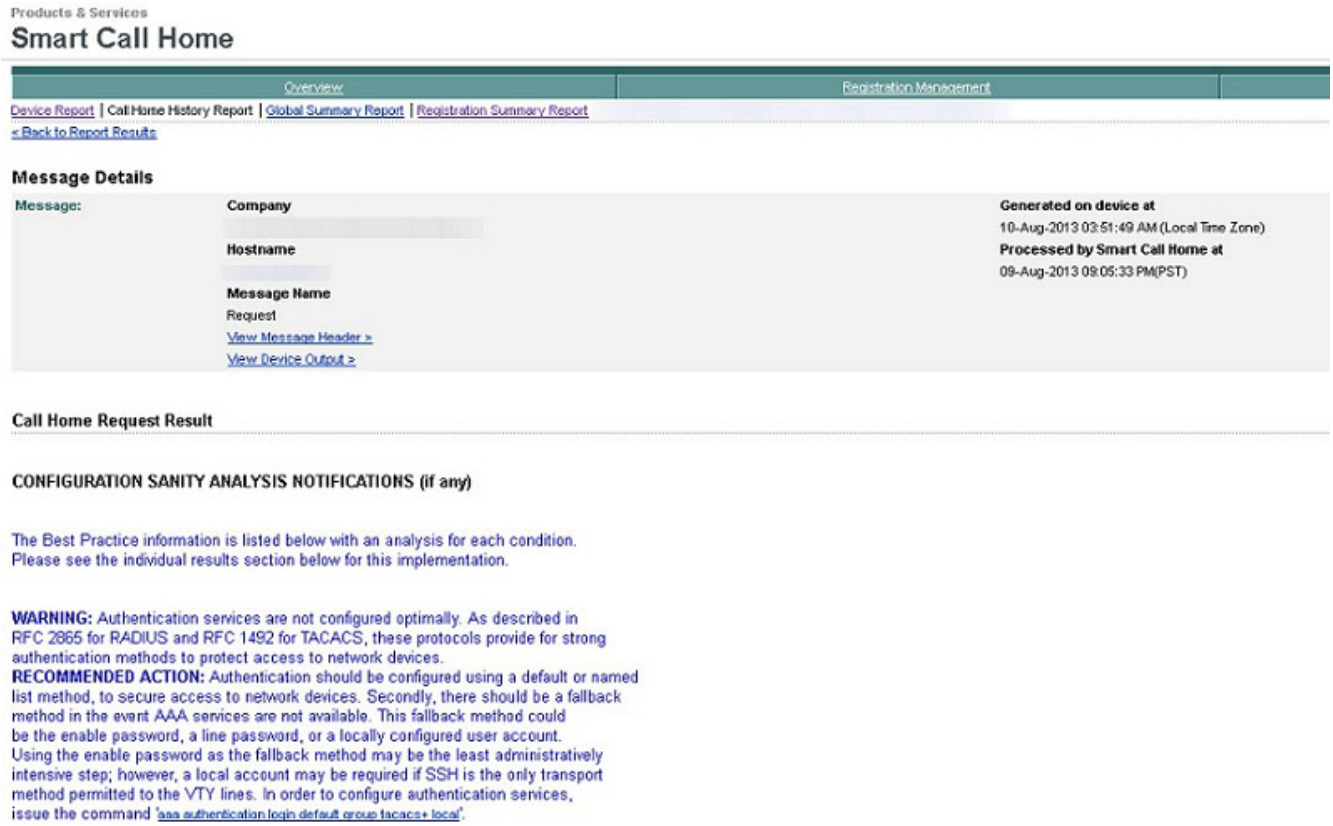


Figure 3-20 Sample output from request command (config-sanity)

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:.

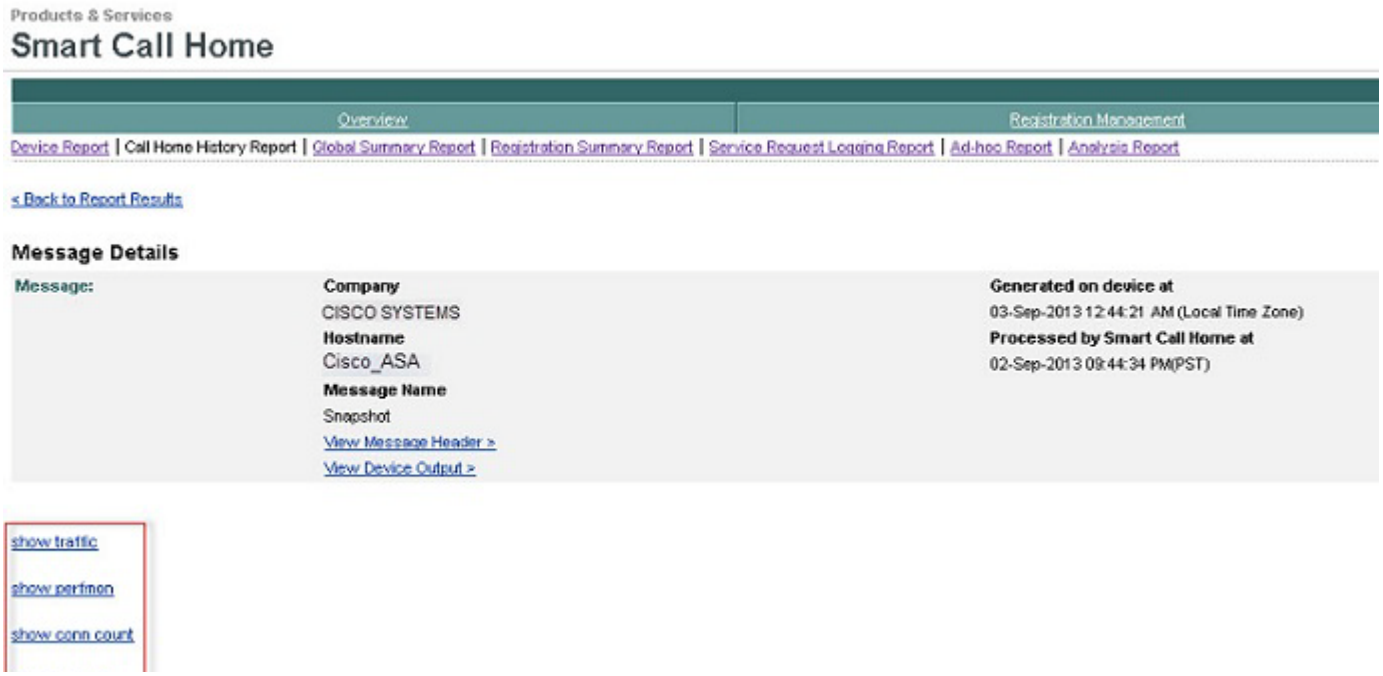


Figure 3-21 Snapshot- Single Context

- 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 3-22 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.

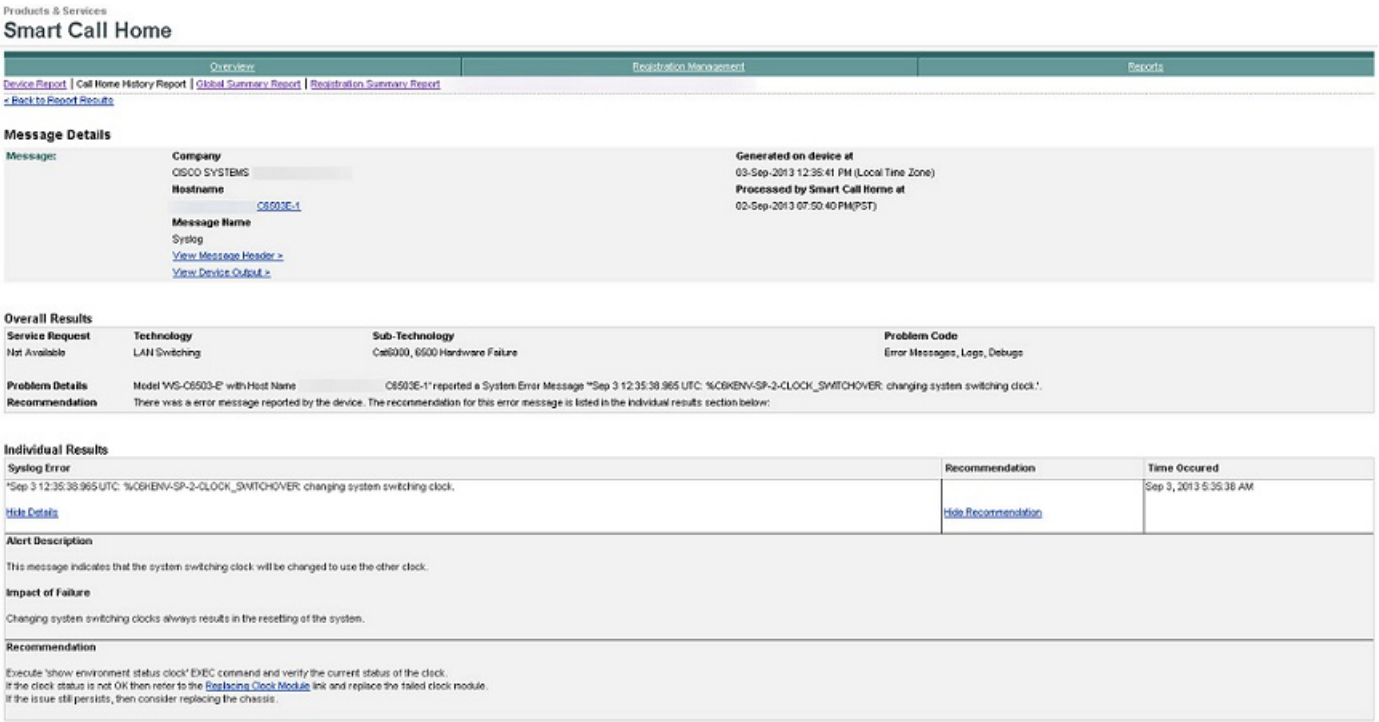


Figure 3-23 Supported Syslog Message Details

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

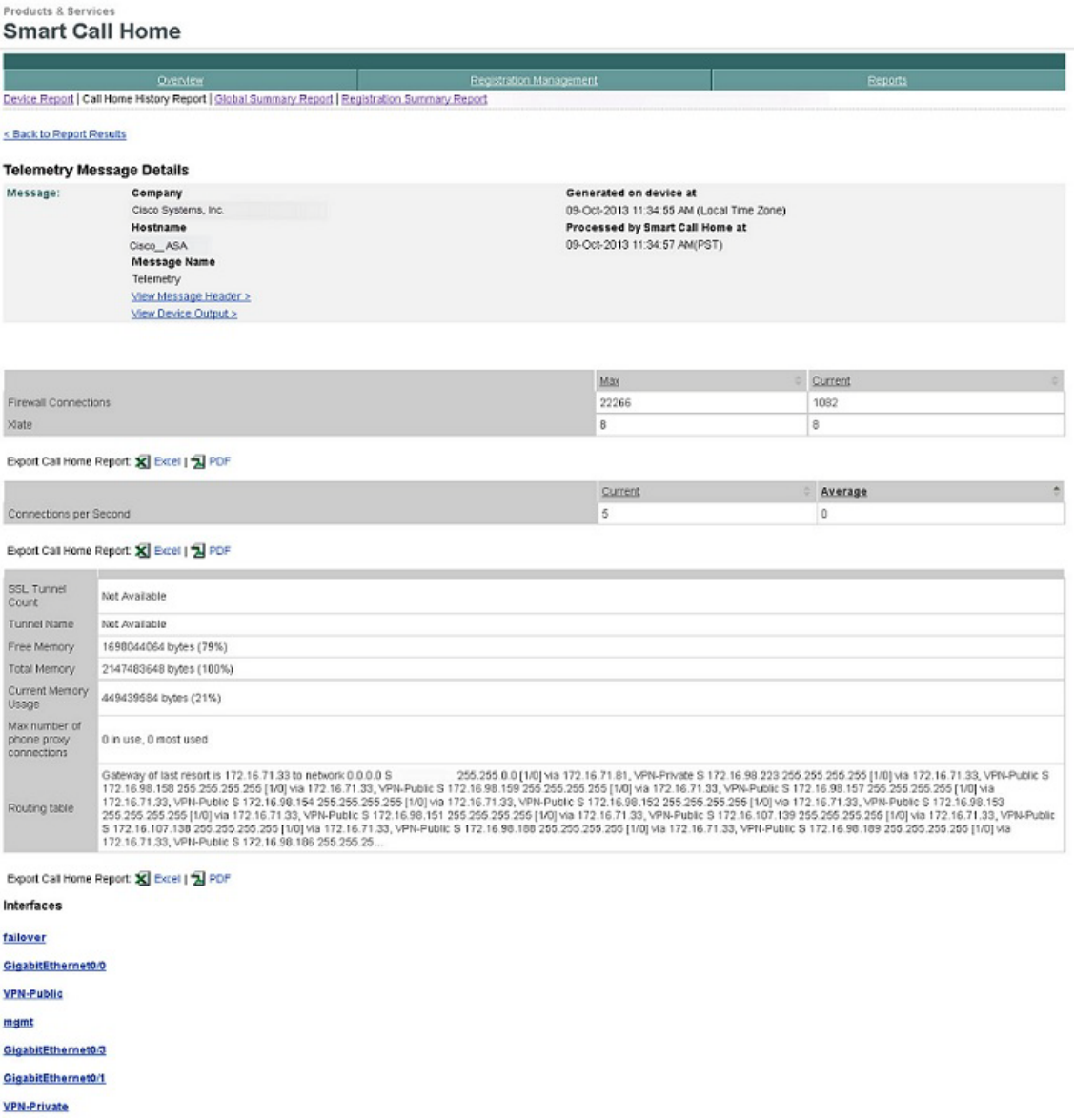


Figure 3-24 Telemetry Message

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

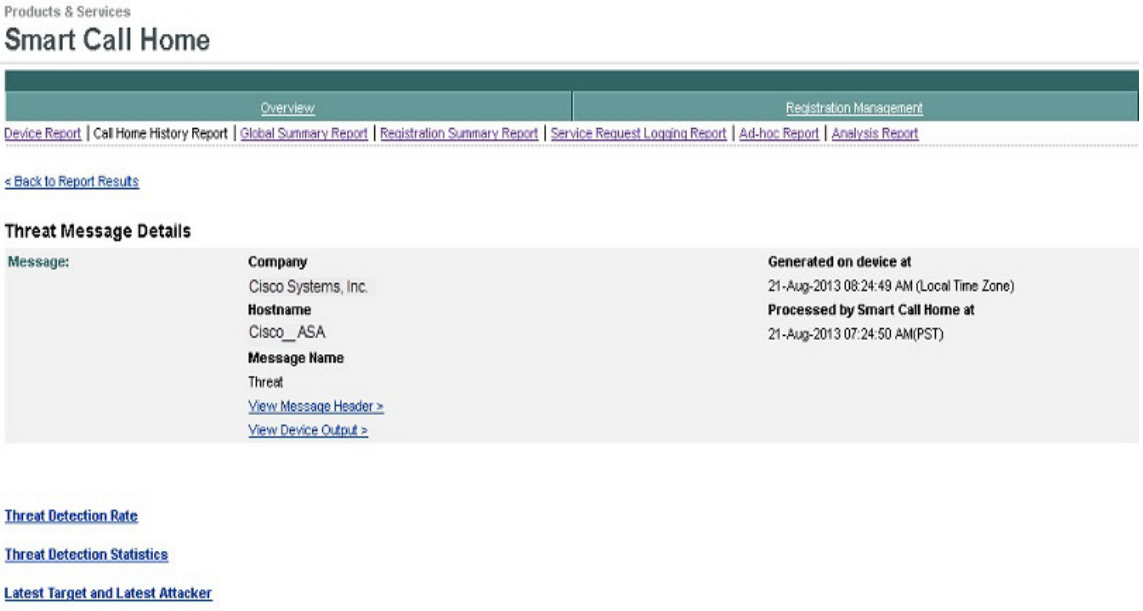


Figure 3-25 Threat Message Details

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

Using the Transport Gateway

This chapter covers the following areas:

Transport Gateway Requirements

The Transport gateway is operational on the following 64-bit operating systems with Java 8 installed:

- Redhat Linux v5 and v6
- Windows 7
- Windows Server 2008 R2 platforms
- Windows Server 2012 R2 platforms

Note Transport Gateway is supported on hosts with above Operating Systems on VMware virtualization platform.

The Transport Gateway uses the ports and protocols listed in the Table 4-1

Table 4-1 Ports and Protocols used with Transport Gateway

Source	Destination	Protocol	Port	Purpose
Cisco Device	Customer Email Server	SMTP	25	Cisco device to send mail to the Transport Gateway
Transport Gateway	Customer Email Server	POP3/IMAP /Secure POP3/Secure IMAP	110/143/995/993 respectively	Transport Gateway to pick up the email from the Customer Email Server.
Transport Gateway	Customer proxy server en route to Cisco backend server	HTTPS	Customer Supplied	Transport Gateway to send Smart Call Home messages to the backend server using a proxy server - Option 2
Transport Gateway	tools.cisco.com	HTTPS	443	Provides access to tools.cisco.com

System Requirements for Redhat Linux

For installing the Transport Gateway software on a Redhat Linux platform, system requirements are:

- Operating System - Red Hat Linux v5 or v6 recommended, 64 bit
- PC or laptop or VM (created using VMware virtualization platform) with 2 GB of RAM.
- Hard disk: 10 GB + (Approx. 1MB for every Call Home message. Message size varies from 15KB - 1MB)
- Java 8 to be installed before starting TG installation

System Requirements for Windows

For installing the Transport Gateway software on a Windows platform, system requirements are:

- 64 bit Operating Systems:
  - Windows Server 2008 R2
  - Windows 7
  - Windows Server 2012 R2
- 2 GB RAM
- Hard disk: 10 GB + (Approx. 1MB for every Call Home message. Message size varies from 15KB - 1MB)
- Java 8 to be installed before starting TG installation

Security Considerations while using a Transport Gateway

Consider the following security information when using the Transport Gateway:

- The SMTP protocol is not encrypted, so the path between the Cisco device and the Transport Gateway through the SMTP server should be located in a secure zone.
- Sensitive information in the device configuration, such as passwords and SNMP Community strings, are masked before leaving the device to mitigate exposure within the LAN or over the Internet.
- It is recommended that the Transport Gateway is installed on the secure internal network, rather than off another segment on the firewall. In a typical configuration, this setup provides access to the proxy server, the email server, and the Internet. This does not require changes to the firewall configuration, as all communication is initiated by the Transport Gateway from the internal network on the highest security zone to other segments in lower security zones.
- Any return communication passes through the firewall as the traffic is part of an existing session.
- As part of Transport Gateway registration, the Transport Gateway sends a registration request to the Cisco backend. The Cisco backend generates a unique Transport Gateway ID and a password and sends these back to the Transport Gateway in the response. This ID and Password are sent in any request to the Cisco backend after the initial registration.
- This communication is through HTTPS and using port 443; see Table 4-1 for a list of the protocols and ports used between the source and destination devices in this mode of communication.
- For customers who need to proxy any traffic between their network and the outside world, the Transport Gateway can communicate with a HTTPS proxy server.

Installation Process Overview for the Transport Gateway

Figure 4-1 is an overview of the Transport Gateway installation and registration process:

Figure 4-1 Transport Gateway Steps

Note Configuring Proxy Settings is optional step.

Download and Install the Transport Gateway Software

Browse to the Transport Gateway software on Cisco.com.This page is available to registered Cisco.com users with a Cisco service contract. Choose the desired version and click **Download**.

Linux

To install the Transport Gateway software on a Linux system:

Step 1 Initiate a terminal session and navigate to the directory where the installation files were saved. Two files, *install.sh* and *SCH-TG.tar.gz*, are present in the unzipped folder.

Step 2 Run the command *chmod +x install.sh*

Step 3 Run the *install.sh* file

Note If TG needs to be installed as a non-root user, follow the below steps:
- Create a Linux user *tguser*
- Copy the installation file to */home/tguser* and proceed with installation under *tguser*

Step 4 Browse to *http://<ip address of Linux machine>/Transportgateway* to access the Transport Gateway application.

Once installed, follow the instructions for configuration and registration contained in Configuration and Registration of the Transport Gateway section

Windows

Note To install TG on Windows VM, ensure you download the correct executable ending with "*_VM.exe"*.

To install the Transport Gateway software on a Windows system, browse to the location of the downloaded files for the Transport Gateway. Double-click on the Transport Gateway executable (*TransportGatewayWin64_<x>.exe)* and follow the installation wizard. Here <*x*> stands for the TG release version.

Once installed, follow the instructions for configuration and registration contained in Configuration and Registration of the Transport Gateway section

OVA Image

To install the Transport Gateway software on Open Virtualization Appliance Image Format

Prerequisites:

1. Download and install vSphere Client version 5.5.
2. Create an ESXi server.

Perform the following steps:

Step 1 OVA image file can be locally stored or remote location, that is accessible

Step 2 Enter **Installation Name** for the OVA image installation then click **Next**.

Step 3 Select *Thin Provision* option under **Disk Format** and click **Next.**

Step 4 Verify the information displayed and click **Next.**

Step 5 Check the *Power on after deployment* checkbox and click **Finish** to install the image.

After installation, OVA Installation image will be created, that is visible on the left pane. It displays the name of the installation entered in step 4.

Note Incase the VM is not ON, then right-click on the OVA installation name and select **Power ON**. You must use *sudo* prefix for some of the commands that cannot be executed from tguser.

Step 6 Go to CONSOLE tab on the right panel, double click on the console screen to activate the console mode.

Step 7 Login with **username:** *tguser* and **password**: *tguser.* [Change the password after first time login]

Step 8 TG installation directory will be available at */home/tguser/CSCOSchtg*.

Step 9 Run the command: *sh/home/tguser/CSCOSchtg/tg/bin/sh.script status* to verify the TG Service.

Step 10 Run the command *ifconfig* to locate the IP address.

If **IP address is not assigned** or IP address need to be changed, then perform the following steps:

1. Edit the file */etc/sysconfig/network-scripts/ifcfg-eth0* by using sudo access privilege and update the following information and save it.
   Eg. *sudo vi /etc/sysconfig/network-scripts/ifcfg-eth0*

   DEVICE=eth0

   TYPE=Ethernet

   ONBOOT=yes

   BOOTPROTO=static

   IPADDR=x.x.x.x [available IP from the network IP pool can be used]

   NETMASK=255.255.255.0

   GATEWAY=x.x.x.1
2. Restart the service by running command with sudo access privilege

   $sudo service network restart
3. Run *ifconfig* to verify newly assigned IP Address.
4. Restart TG Service and access TG UI with new IP Address assigned

   To restart TG, go to */home/tguser/CSCOSchtg/tg/bin/*

   Run *./sh.script restart*

Note Using the IP address, access the TG UI with URL http://<IP Address>:8080/Transportgateway

If **Test Connection** fails, then perform the following steps:

- Check if you can reach to *tools.cisco.com* e.g:ping tools.cisco.com.
  - If this fails then it could be due to the fact that domain name resolution might have failed. One of the reason for this is that ESXi host where this OVA is getting deployed is not DHCP enabled.

In such cases please follow the below steps:-

- Check */etc/resolv.conf file* and ensure that it has the entries corresponding to your name servers. If not, then overwrite the entries with your name server details.

Note To know your name server you can issue a command *nslookup www.cisco.com* from a system which is connected to Internet to list the name servers.

Once installed, follow the instructions for configuration and registration contained in Configuration and Registration of the Transport Gateway section.

Applying Security Patch for Linux Vulnerabilities

Applicable TG OVA Images: 4.1.3, 4.1.4, 4.1.5.

Follow the below steps to apply the security patch for linux vulnerabilities:

Step 1 Download the patch **linux-vulnerability-patch.zip**.

Step 2 Login to system where the TG OVA image is installed.

Step 3 Execute the following commands:

unzip linux-vulnerability-patch.zip

sudo ./install.sh

VM gets restarted and new patch will be applied.

Applying Security Patch for glibc Vulnerabilities

Affected TG OVA Images: 4.0, 4.1, 4.1.1, 4.1.2, 4.1.2.1, 4.1.3

Note Applying glibc vulnerability patch is not required, if **linux vulnerability** patch is already applied.

Follow the below steps to apply the security patch for glibc vulnerability (CVE-2015-7547):

Step 1 Download the patch **glibc-vulnerability-patch.zip**.

Step 2 Login to system where the TG OVA image is installed.

Step 3 Execute the following commands:

unzip glibc-vulnerabiltiy-patch.zip

cd glibc-vulnerability-patch

sudo ./install.sh

sudo reboot

VM gets restarted and new patch will be applied.

Applying Security Patch for bash shell vulnerability

Affected TG Image: Cisco Transport Gateway **4.0** Linux Build - OVA Image

Note Applying bash shell vulnerability patch is not required, if **linux vulnerability** patch is already applied.

Follow the below steps to apply the security patch for bash shell vulnerability:

Step 1 Download the patch (bash-security-patch.zip) from : http://software.cisco.com

Step 2 Login to system where the TG OVA image is installed as root

Step 3 Unzip the patch obtained in Step 1

Step 4 cd to directory "bash-patch"

Step 5 Execute *./install.sh*

Step 6 Machine will get auto rebooted after patch is installed.

Uninstall the Transport Gateway for Linux

To uninstall the Transport Gateway application, go to the installation directory and run the *uninstall.sh* script in the *tg/bin* folder.

Uninstall the Transport Gateway for Windows

To uninstall the Transport Gateway application, go to the folder containing the installation files. Double-click on the uninstall icon to start the uninstallation. Follow the wizard until uninstallation is complete.

Configuration and Registration of the Transport Gateway

Once the software is installed, configure the Transport Gateway. To do this:

Step 1 Browse to http://<ip-address>/Transportgateway or http://<ip-address>/Transportgateway/home.jsp to access the Transport Gateway application.

Step 2 At first time login, enter the default username and password of **admin/admin**.

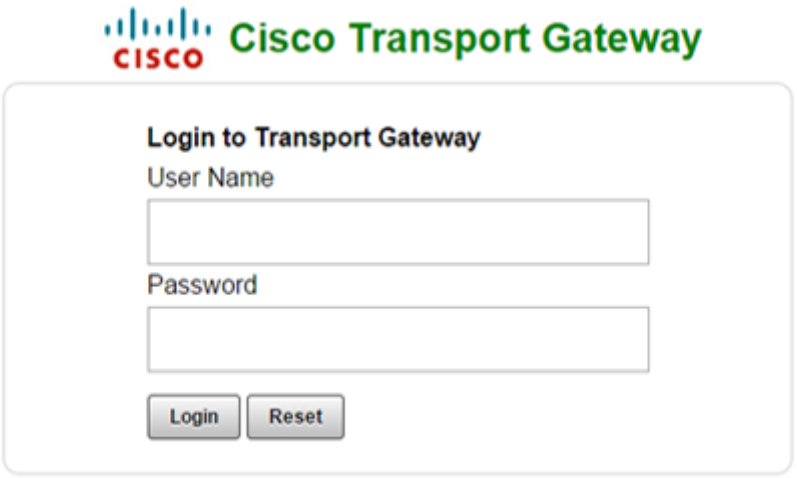


Figure 4-2 Transport gateway Login screen

The system prompts the user to enter new password, select a security question and provide an answer to that question that can be used for future prospects.

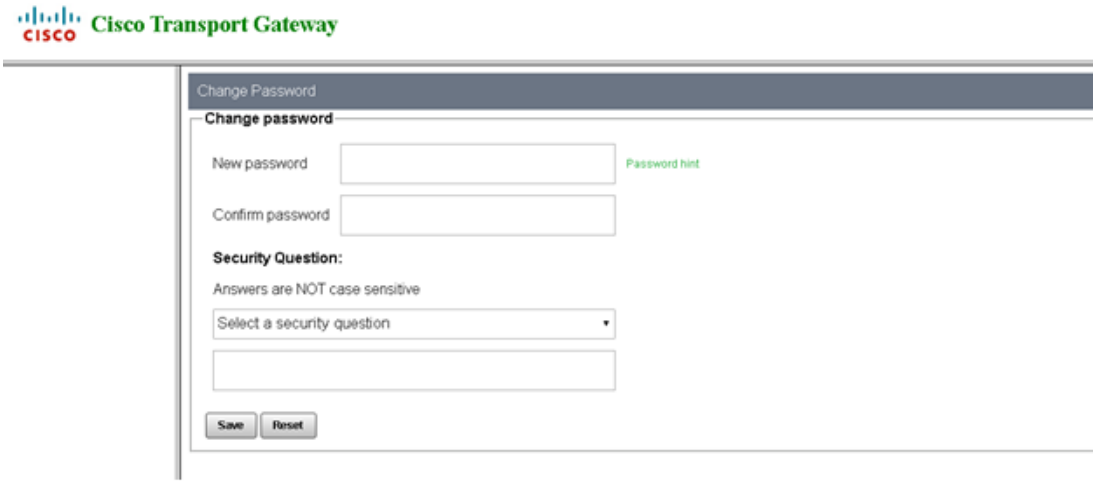


Figure 4-3 Change Password

Step 3 The Set Proxy Settings window appears. This allows you to specify an HTTPS proxy for communication with the Smart Call Home servers at Cisco.com.

Note Configuring proxy settings is optional. If the network has HTTPS proxy, then these settings can be configured.

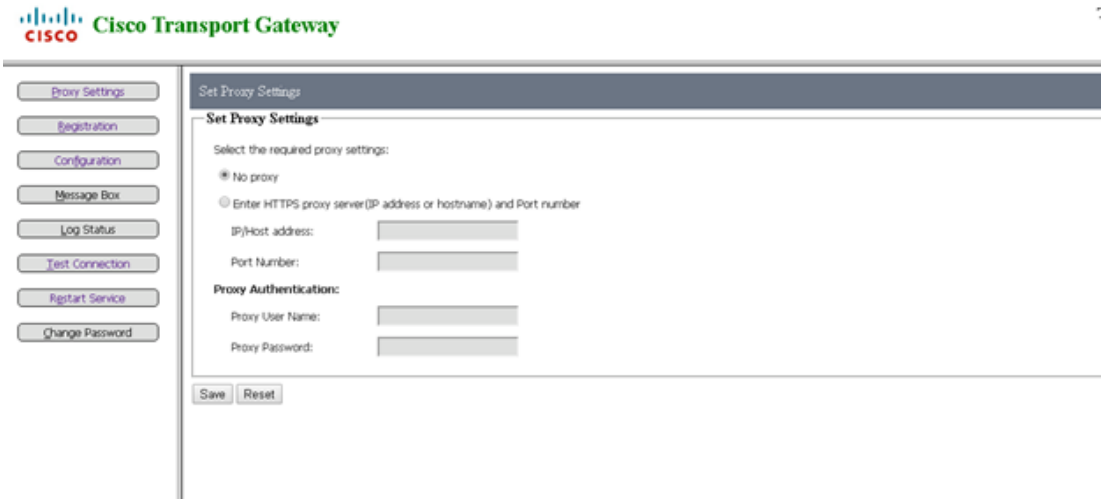


Figure 4-4 Set Proxy Settings

Step 4 Enter the IP address or Hostname, Port Number, Proxy User Name, and Proxy Password. Click **Save**.

Step 5 After the proxy server is configured, click **Test Connection** to test the connection to Cisco.com.

Step 6 Click **Registration** to register the Transport Gateway with the Smart Call Home servers. The Register Transport Gateway screen appears.

Step 7 Enter the Cisco.com ID, password, a name and description for the Transport Gateway (user defined), and an email address (optional) for registration failure notification.

Step 8 Click **Register with SCH**. Upon successful registration, the Registration Status will be changed to Registered and **TG SSL Certificate & Reset Password** buttons will be shown in Left navigation pane. To know more details on TG SSL Certificate, please refer the corresponding section.

Step 9 Once registration is successful, the email address for failure notification can be changed by entering an email address in the Notify Email Address field and clicking **Update**.

Figure 4-5 Register Transport Gateway

Step 10 **Re-register Transport Gateway** option is provided to the user to register with an alternate Cisco.com Id. User can check this option and enable the screen to register TG once again.

Note If you are using the CSSM Satellite OVA image, the feature **TG SSL Certificate** will not be shown even after successful registration.

Forgot Password

To get the password, use the Forgot password link on the login screen that is visible on subsequent logins. Perform the following steps to get the forgotten password:

Step 1 On the login screen, click **Forgot password?** link.

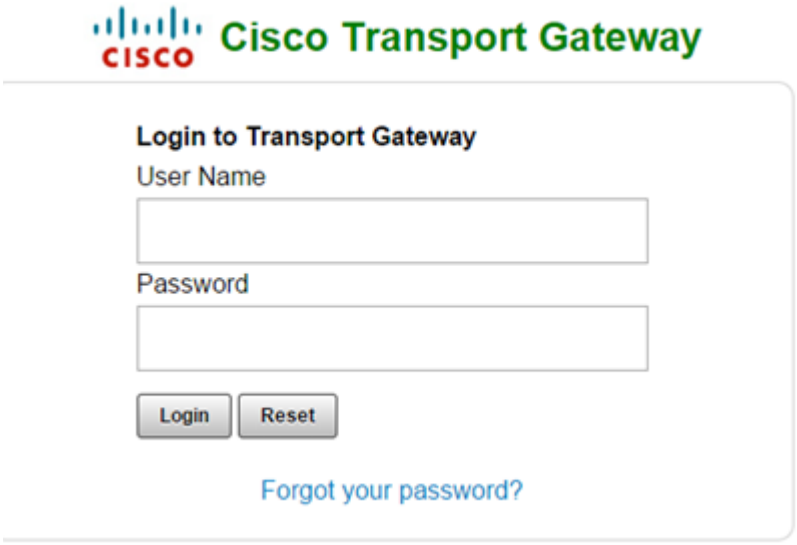


Figure 4-6 Login screen with Forgot Password link

The application directs to a new screen to enter new password and answer the security question as entered while creating passowrd.

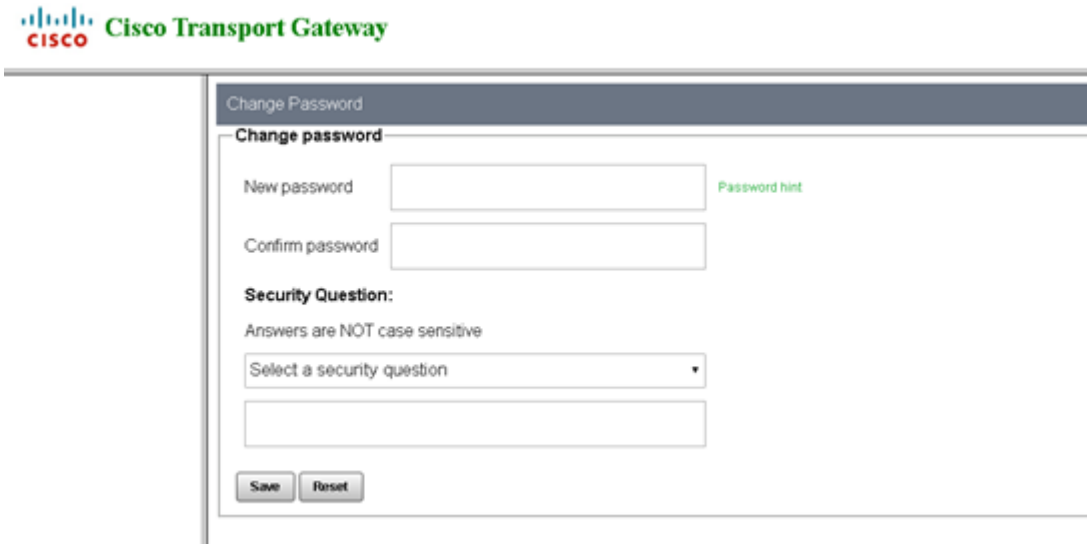


Figure 4-7 Set New Password

Step 2 Enter the answer to the security question, new password and also renter the password to confirm.

Step 3 Click **Save**.

Note Security answer should match with the answer entered while configuration else the password change fails. If you have forgotten the answer to the security question please contact the support team to reset the password and security question.

Configure mailbox

If using email to send Call Home messages from the device to the Transport Gateway, configure the mailbox as follows:

Step 1 From the Mail Server Type drop-down menu, choose the appropriate mail server protocol. The Mail Server Port Number automatically populates with the corresponding port number.

Step 2 Enter the name of the Mail Server Folder that will receive the Call Home messages.

Step 3 Enter the Account Name and Password that has access to the mail server.

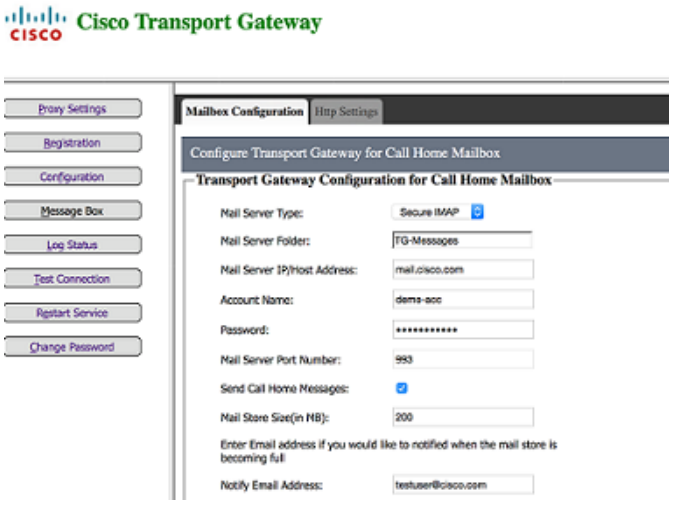
Step 4 Check the Send Call Home Messages checkbox to upload Call Home messages to Cisco.com. If this option is unchecked, the Call Home messages are stored locally. This option must be checked in order to realize the full benefits of Smart Call Home.

Step 5 Enter the desired Mail Store Size. This defines the capacity of the local mail store. Note that if this limit is exceeded, Call Home messages are not processed.

Step 6 Enter the email address of the person to notify in the event the mail store approaches capacity.

Step 7 Click **Save**.

Note The Transport Gateway must be restarted to effect changes in the mailbox configuration. Once restarted,



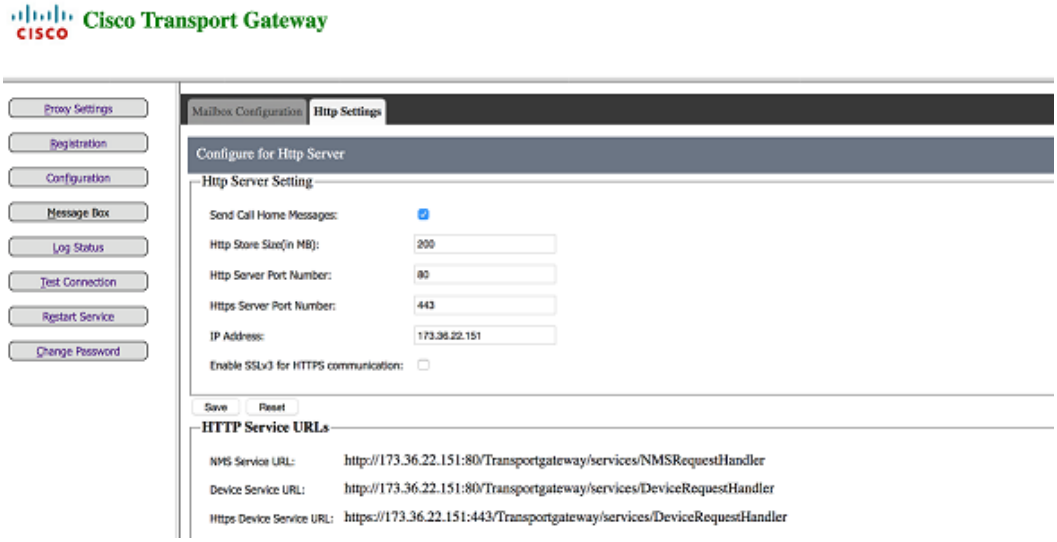
Call Home messages are received by the Transport Gateway, stored locally, and uploaded to Cisco.com.

Configure HTTP settings

If you are using HTTP to send Call Home messages from the device to the Transport Gateway, configure the HTTP Settings as follows:

Step 1 Click **Configuration** and then click the HTTP Settings tab

Step 2 Port numbers and IP address are editable.



Note If you want to change the default port numbers:
1. Ensure, you input the available free port number
2. Restart Service, when the TG restart is in progress, access the UI by giving the new port number in the URL

Step 3 Enter the desired Http Store Size. This defines the capacity of the local mail store (Httpmsgstore). Note that if this limit is exceeded, Call Home messages are not processed.

Note All other fields are automatically populated.

Step 4 **Enable SSLv3 for HTTPS communication**: By default, SSLv3 is disabled on TG due to security vulnerabilities associated with SSLv3. However if there are some devices in your network which still use SSLv3 for SSL handshake, and you are not in a position to upgrade the OS image on those devices, then you can use this option to enable SSLv3 on TG. Enabling SSLv3 on TG poses serious security risks and it is strongly discouraged to turn it ON. Instead try to upgrade the device OS to get the TLS capability for SSL handshake. By default, it is unchecked.
To enable SSLv3 on TG, check **Enable SSLv3 for HTTPS communication**, below warning message appears:

Step 5 Click **Save**.

Step 6 **Restart** TG to reflect the **Http Settings** configuration changes.

Note The Transport Gateway must be restarted to effect changes in the HTTP settings. Once restarted, Call Home messages are received by the Transport Gateway, stored locally, and uploaded to Cisco.com.

Step 7 If you are using HTTP for communication from device to TG, copy the URL under "*Device Service URL:*" If you are using HTTPS for communication from device to TG, copy the URL under "*Https Device Service URL:*"

and use it in call home profile on device, as below:

Router# configure terminal

Router(config)# call-home

Router(cfg-call-home)# contact-email-addr username@domain-name

Router(cfg-call-home)# profile CiscoTAC-1

Router(cfg-call-home-profile)#no active

Router(cfg-call-home-profile)# #profile {Your_profile_name}

Router(cfg-call-home-profile)# active

Router(cfg-call-home-profile)# destination transport-method http

Router(cfg-call-home-profile)# no destination transport-method email

Router(cfg-call-home-profile)# destination address http {Device Service URL from TG to be pasted here}

Router(cfg-call-home-profile)#end

Router#copy running-config startup-config

Reset Password

Allows the user to reset the password that transport gateway uses to communicate with Cisco backend.

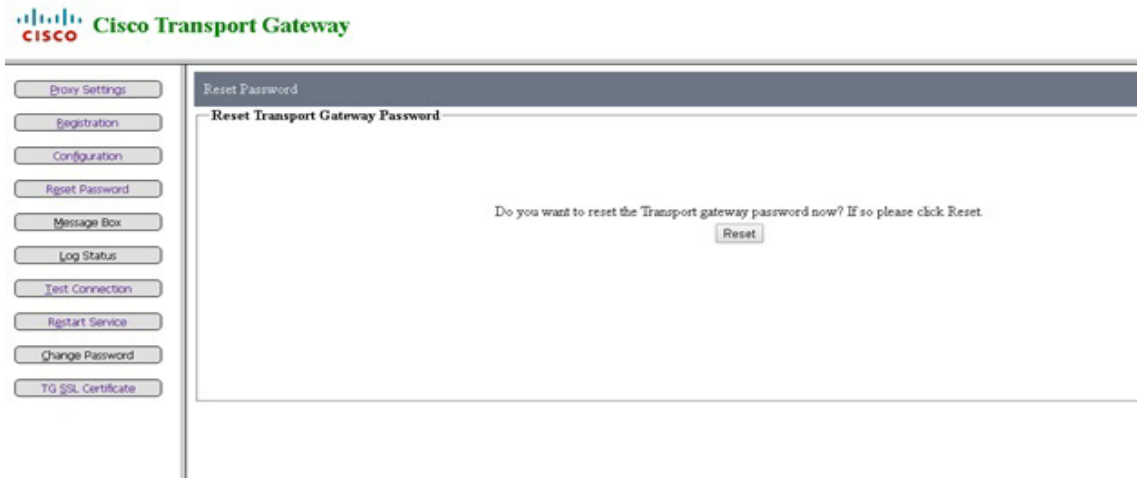


Figure 4-8 Reset Password Snapshot

Message Box

The Transport Gateway allows you to view the Call Home messages that are available to be sent to Cisco. This list contains Call Home messages that have been received in the mailbox more than four hours previous, but less than two days previous, and have not been successfully sent to Cisco. If the message is not sent to Cisco within four hours, it is stored and viewable in the message box. If the message is not sent to Cisco within two days, it is automatically deleted.

In the Transport Gateway application, click **Message Box**. In the **Email Messages** tab, you can view a list of mails from devices configured to send mails to Cisco via the Transport Gateway (Figure 4-1). You may send email messages to Cisco or delete selected messages. If using HTTP, click the **HTTP Messages** tab to view the HTTP mailbox.

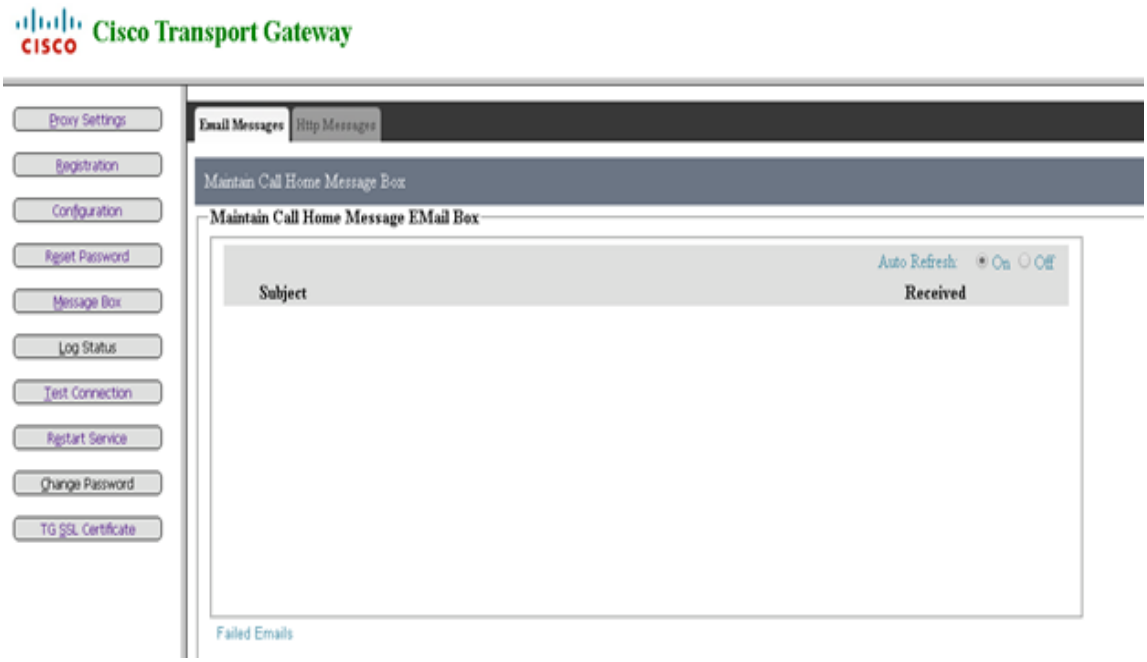


Figure 4-9 Message Box

Subject	Received
System Notification From rbml-test-router 2 Test123	Sep 23 2015 03:06:50 PDT
System Notification From rbml-test-router 0 Test123	Sep 23 2015 03:07:08 PDT
System Notification From rbml-test-router 4 Test123	Sep 23 2015 03:06:45 PDT

Figure 4-10 Sample Email Messages

Log Status

In the Transport Gateway application, click **Log Status**. From here you can:

- View the list of Warning or Informational logs by choosing the appropriate Log Mode from the drop-down menu.
- Change the log mode.
- View log files by checking the box next to the desired log file and click **View**.
- Send log files to Cisco support by checking the box next to the desired log files and click **Zip**. Save the .zip file to a local machine. Enter an email address in the Support Email ID field and click **Upload to Support.**

Figure 4-11 Log Status

To view, change the log mode, or zip the log status file perform the following steps:

Step 1 On the Transport Gateway Application click Log Status; the **Log Status** area appears.

Step 2 Select the desired status log by clicking the Log Mode drop-down menu and selecting the Warn or Info log mode.

Step 3 Click **Change Mode**. An informational message appears indicating:

- What the Log Mode was changed to.
- You must restart the Transport Gateway to effect the change in log mode.

Step 4 Once the log mode has been specified, and activated if changed, then:

- Click **View** to view the status log file; the Status Of TG file opens with the status information displayed.
- Click **Zip**; a Save window appears with a filename for the log status zip file.

Step 5 Click **Save.**

Step 6 In the Support Email ID field, enter an email address to send the zip file. Click **Upload to support** to select the zip file and send it to the support email address.

Test Connection

The Test Connection option tests the connection between the Transport Gateway and Cisco. Click **Begin Test** to test the connection. A success or failure message is returned.

Restart Service

This option restarts the Transport Gateway service. Restarting the service effects any changes to the Transport Gateway configuration.

Change Password

This option enables you to change the password for the Transport Gateway. The default user name and password is admin/admin. Select **Change Password** from the left menu navigation.

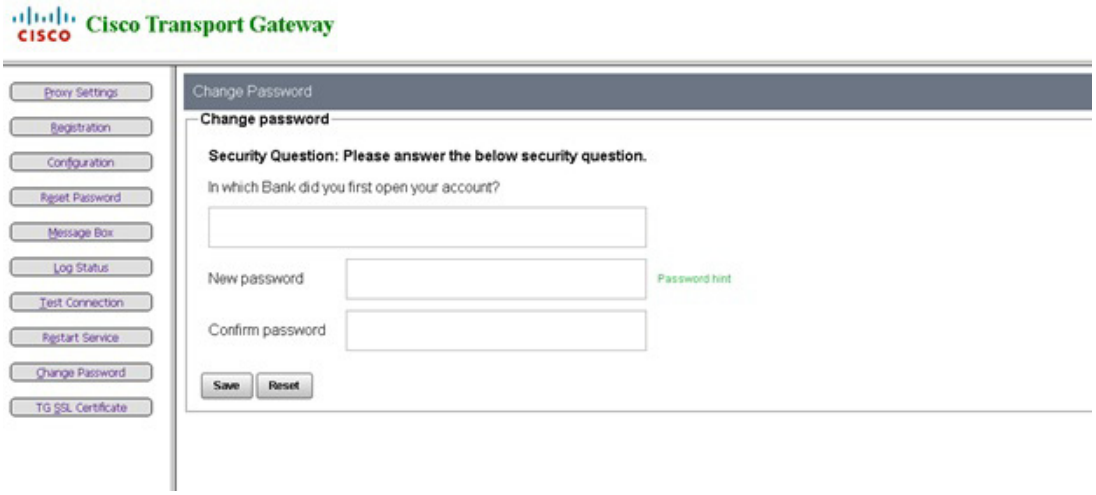


Figure 4-12 Change Password

Enter the answer to the security question, new password and also renter the password to confirm. Click **Save** to save the changed password details.

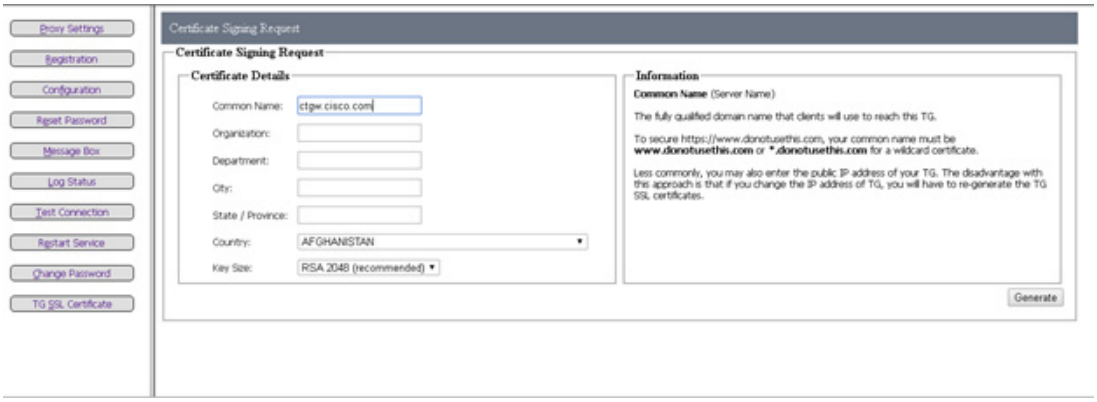
Note Security answer should match with the answer entered while configuration else the password change fails. If you have forgotten the answer to the security question please contact the support team to reset the password and security question.

Using HTTPS for device to TG communication

If you want to use HTTPS for the communication from device to Transport Gateway, then install the TG SSL certificate. By default, the current version of TG comes with Self-signed certificate that was part of previous releases. This is retained for backward compatibility. If you have some of your devices which are leveraging this certificate from previous TG releases, then you can continue to use that. However we strongly encourage using this new feature – **TG SSL Certificate**

This option is available once the TG is registered. It enables the users to generate and install Cisco CA signed TG SSL certificates on TG. The generated Certificates will be used for all the HTTPS communication from device to TG. Once you have generated these certificates, self-signed certificates that were part of TG are no more valid. For more detailed usages of these certificates, refer to the Frequently Asked Questions section.

Step 1 Go to **TG SSL Certificate**, you will get the below screen.

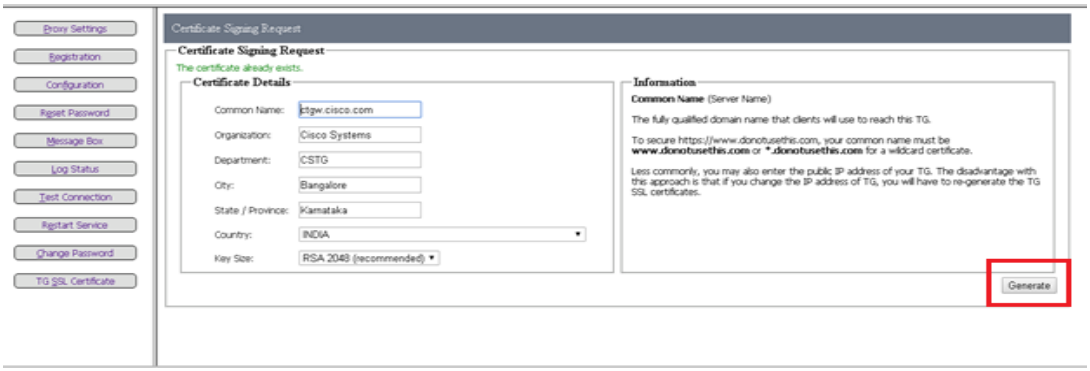


Step 2 Common Name (Server name/IP address of the TG) is auto populated, and it is editable. It is strongly recommended that you enter the fully qualified domain name (FQDN) of the host (hostname) as common name. This will avoid re-generating the certificates in case the IP address of this host changes.

Step 3 Enter details of Organization, Department, City, State/Province.

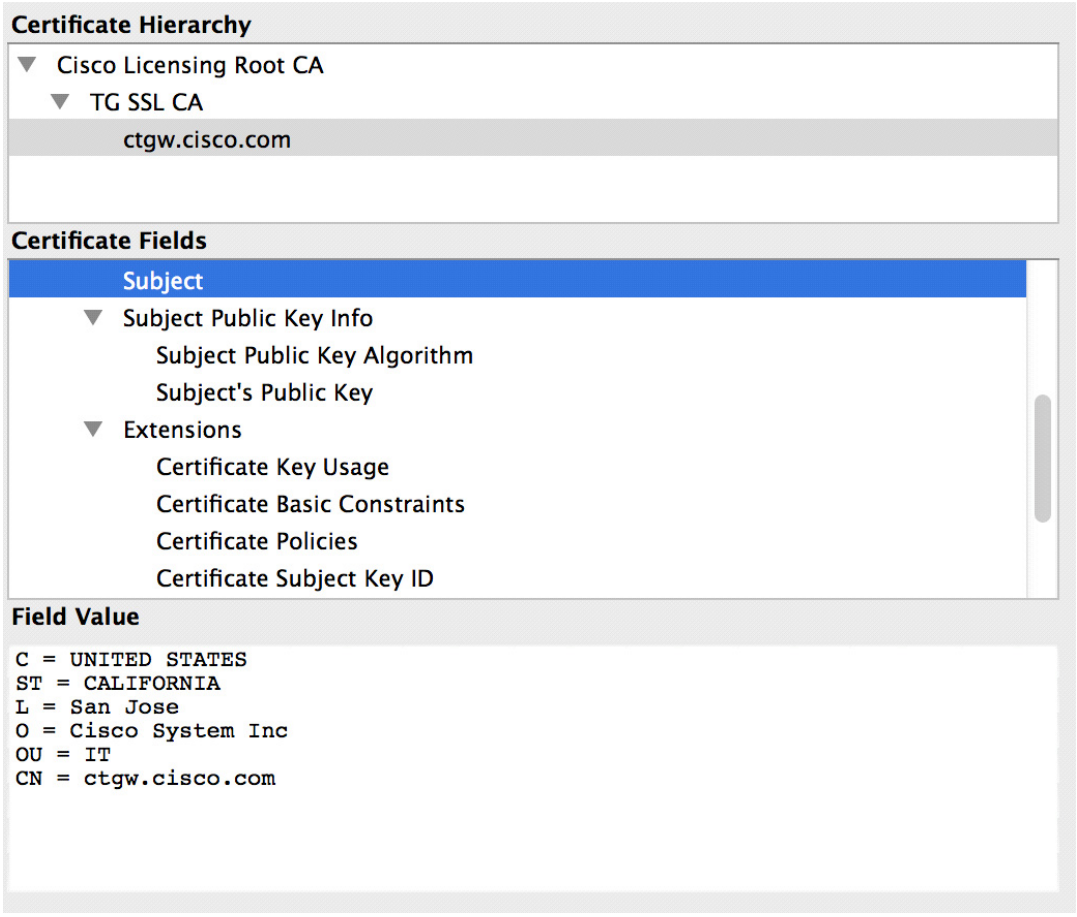
Step 4 Select Country and Key Size

Step 5 Click **Generate** to generate and install TG SSL certificates automatically.



Column	Description
Common Name	The fully qualified domain name that clients will use to reach this TG.
Organization	The exact legal name of your organization.
Department	Department within your organization, which you want to appear in the certificate. It will be listed in the certificate's subject as Organizational Unit, or "ou."
City	The city where your organization is legally located.
Country	The country where your organization is legally located
Key Size	Key Size to be used in encryption. Key size smaller than 2048 are considered insecure

The installed Certificate can be viewed from your browser using “View Certificate” option.



Note This option will not be available in **CSSM Satellite OVA** images.

Transport Gateway Processing of Call Home Messages

Devices use one of two methods to deliver Call Home messages to a Transport Gateway:

- HTTP
- EMAIL

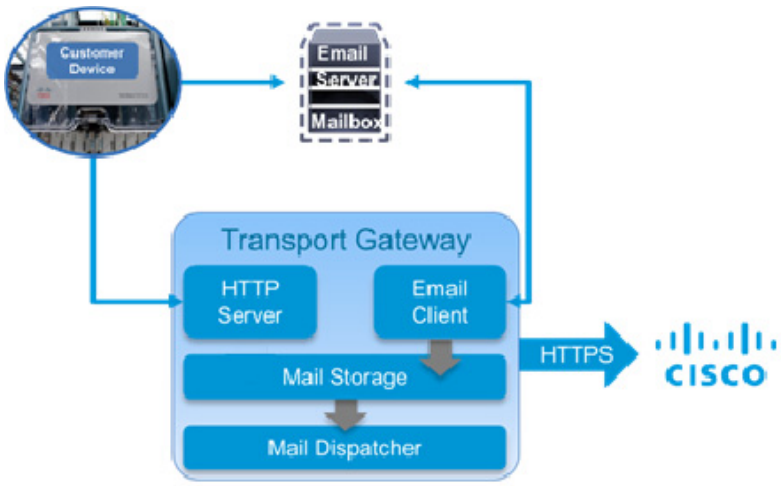


Figure 4-13 Call Home message path through the Transport Gateway

Using an HTTP Server to Process Call Home Messages

In the first method, Call Home devices make an HTTP connection on a specified port and deliver messages directly to the Transport Gateway.

The steps in processing Call Home messages using an HTTP server are:

Step 1 Device(s) send generated Call Home messages to the Transport Gateway.

Step 2 The Transport Gateway passes the Call Home messages to the embedded HTTP server.

Step 3 The embedded HTTP server sends the Call Home messages to the Cisco Backend.

Using a Mail Server to Process Call Home Messages

Alternatively, the Transport Gateway's email client can retrieve messages from an email inbox. This section explains how the Transport Gateway processes the Call Home messages sent to a client server/mailbox and retrieved to the Transport Gateway Call Home mailbox.

The Transport Gateway automatically retrieves Call Home messages from the client mailbox, and those messages are forwarded automatically to Cisco.

The following describes the process the Transport Gateway uses to retrieve Call Home messages from the client mailbox, then sends to Cisco:

- Device(s) send generated Call Home messages to the client mailbox.
- The Transport Gateway connects to the client mailbox to retrieve the CallHome messages.
- The Transport Gateway checks at regular intervals to see if any Call Home messages have arrived in the client mailbox.

Note When the Transport Gateway cannot connect to the client mailbox, an error is logged indicating the date/time, event and reason of the error. The Transport Gateway will try to connect to the client mailbox every 60 seconds until the connection is restored.

- When new Call Home messages arrive in the client mailbox, they are retrieved by the Transport Gateway, then deleted from the client mailbox.
- The Transport Gateway automatically sends the Call Home messages to Cisco.

Temporarily disable automatic message forwarding.

By default, the Transport Gateway automatically forwards messages to Cisco as they arrive. This behavior is controlled by the "Send Call Home Messages" option in the HTTP and SMTP configuration. Automated message forwarding can be temporarily disabled by unchecking this option for one or both transports. When automatic forwarding is disabled, the Transport Gateway stores messages until they are sent manually using the configuration GUI.

Note HTTP and SMTP messages are stored in separate inbox. If both are disabled, it will be necessary to check both inbox for queued messages.

Manually Forwarding messages:

In order for the Transport Gateway to forward Call Home messages to Cisco, the following tasks must be completed:

- Transport Gateway is registered with Cisco
- Transport Gateway has been successfully configured
- The user checks the **Send Call Home Messages** check box in the configuration window
- Transport Gateway has a connection to Cisco

The Transport Gateway forwards Call Home messages to Cisco without user interaction if the above tasks are complete.

If for some reason the Transport Gateway is not able to send messages to Cisco, the Transport Gateway continues attempting to send them for four hours. If messages cannot be sent to Cisco after four hours, the messages become available in the Transport Gateway mail store, which is accessible by clicking the **Message Box** option. The user can manually send the messages to Cisco or delete them from the mail store without sending. Messages older than 2 days that are not sent to Cisco are deleted automatically.

Notifying the Customer When Mail Store Reaches the Size Limit

During configuration the customer has the option to specify a mail store size for each inbox to indicate when they want to be notified when a Transport Gateway mail store is becoming full.

The configuration also has a corresponding option to specify a notification email address that the system uses to send an email notification when the mail store is reaching its size limit. When the mail store is reaching its size limit, an email notification is sent to the email address specified in the Notify Email Address field under Registration tab.

Transport Gateway and SNTC Collectors

This section describes how to install Transport Gateway (TG) for SCH on Cisco hardware collector appliances. There are several supported host environments for the Transport Gateway application:

1. Customer-provided Windows or Linux host server
2. Customer-provided VMware ESX host server
3. Cisco hardware collector appliance (purchased via Smart Net Total Care)

Option 1 is covered in detail earlier in this chapter of the User Guide. Refer Transport Gateway Requirements.

Option 2 applies to both SNTC and non-SNTC scenarios. For example, SNTC customers who have deployed the software version of the SNTC collector on a VMware host system may also install Transport Gateway as an additional VM on the same ESX host.

Option 3 scenarios as stated in below section.

Cisco Hardware Collector Appliance

The Transport Gateway application may be installed on Smart Net Total Care (SNTC) hardware collectors running CSPC version 2.4.1 or higher. In fact, SNTC hardware collectors purchased and shipped after December 2014 will include both Transport Gateway and the latest CSPC version in the factory software image. On these hardware collector appliances, Transport Gateway simply needs to be enabled using the steps described below:

Pre-Requisite:

- Cisco hardware collector appliance 2.4.1 or higher installed.
- Appropriate network IP configured.

Installing Transport Gateway on CSPC server:

SCH Transport Gateway is located at */root/cstg/SCH.zip* of a CSPC server version 2.4.1 or higher.

Step 1 Use console or SSH onto the CSPC server and login as super user. (If SSH is not enabled on the server than login as admin and enable ssh using command *ssh enable*.)

Step 2 TG is stored in the SCH.zip file at */root/cstg*
[root@localhost collectorlogin]# cd /root/cstg

Step 3 Unzip *SCH.zip* file.

[root@localhost cstg]# unzip SCH.zip

Step 4 Change director to SCH directory

[root@localhost cstg]# cd SCH

Step 5 Install TG by running install.sh file.

[root@localhost SCH]# nohup ./install.sh &

```
[root@localhost collectorlogin]# cd /root/cstg
[root@localhost cstg]# ls
SCH.zip
[root@localhost cstg]# unzip SCH.zip
Archive:  SCH.zip
   creating: SCH/
  inflating: SCH/SCH-TG.tar.gz
 extracting: SCH/uninstall.sh
  inflating: SCH/install.sh
  inflating: SCH/info.xml
[root@localhost cstg]# cd SCH
[root@localhost SCH]# ls
info.xml  install.sh  SCH-TG.tar.gz  uninstall.sh
[root@localhost SCH]# nohup ./install.sh &
[1] 6641
[root@localhost SCH]# nohup: ignoring input and appending output to `nohup.out'
^C
[1]+  Done                    nohup ./install.sh
```

Smart Call Home Transport Gateway is now installed and can be accessed by URL:

http://<ip-address>/transportgateway/

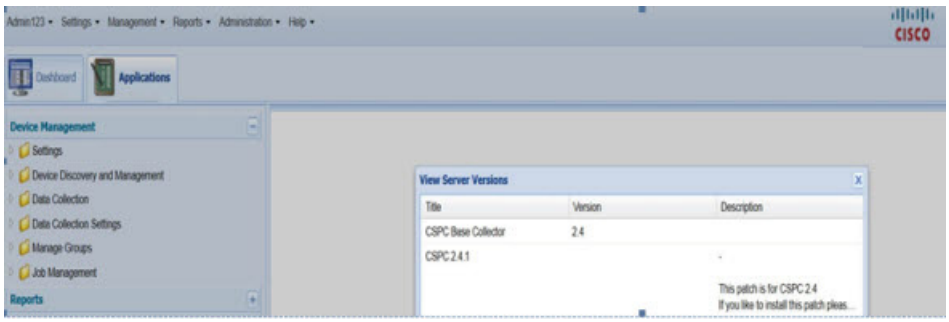
Note If the URL does not load the UI page than there may be a need to update the IP Table. Execute the following commands to do IPtable updates on the server.
[root@localhost collectorlogin]# iptables -I INPUT -p tcp --dport 80 --syn -j ACCEPT
[root@localhost collectorlogin]# iptables -I INPUT -p tcp --dport 443 --syn -j ACCEPT

To further configure and customize the Transport Gateway, refer SCH Deployment guide.

Earlier versions of the Cisco hardware collector appliance may be upgraded to CSPC 2.4.1 by using the software upgrade capability built into the appliance. Refer CSPC Quick Start Guide for more information.

Once the CSPC version has been upgraded to 2.4.1 or later, the latest version of Transport Gateway may be downloaded from Software.cisco.com and install to the */root/cstg* directory of the collector appliance.

To view the version of CSPC base collector, add-ons and other optional packages installed on CSPC on the **View Server Versions** screen. Once logged into CSPC, Select the **Help menu > About > View Versions**.



For more information about SNTC Deployment and/or the SNTC hardware collector appliance, please visit the SNTC Support Community.

To Open a Support Case for Transport Gateway support:

1. Create a support case at the Cisco support website: https://tools.cisco.com/ServiceRequestTool/scm/mgmt/case?referring_site=shp_contacts_support_cases
2. Ensure to select the Product as "**Smart Services Capabilities > Smart Call Home**" so the right team is engaged.

To Open a Support Case for support on the collector appliance:

1. Create a support case at the Cisco support website: https://tools.cisco.com/ServiceRequestTool/scm/mgmt/case?referring_site=shp_contacts_support_cases
2. Ensure to select the Product as "**Smart Services Capabilities > Collector and Inventory Uploads**" so the right team is engaged.

Troubleshooting Cisco Transport Gateway Errors

Topics in this section include Transport Gateway problems dealing with:

- Transport Gateway Configuration
- Transport Gateway Connectivity
- Transport Gateway Start Up
- Transport Gateway Operation
- Device to TG communication Troubleshooting

Transport Gateway Configuration

The configuration scenario is related to specifying the IMAP folder name.

Cannot establish a connection to the Mail server Inbox

During configuration of the Transport Gateway, you want a connection to the mail server's Inbox but fails when trying to establish a connection

Symptom / Cause:

- The default mailbox folder name is INBOX for both the IMAP and POP3 protocol.

Fix:

Perform the following procedure to configure the Transport Gateway to receive Call Home mails from a mail folder other than 'Inbox'.

Step 1 Click **Configuration**.

Step 2 Make sure you have selected the **IMAP** mail server type.

Step 3 Provide the rest of the configurations and save the configurations.

Step 4 Stop the service

Step 5 Go to the following property in the <**TG_Install_Dir**>/CSCOSchtg/tg/conf/an/properties/mailbox.properties

Step 6 In the mailbox.properties file set the mail.imap.inbox value to the same target mailbox folder name as is noted in the mail server

Note The folder name might be a case sensitive based on your mail server configuration (e.g. Mail.imap.inbox=<folder name>)

Step 7 Save the mailbox.properties file

Step 8 Restart the Transport Gateway Service for immediate effect of the new mail folder configuration.

Note The default receiving mailbox folder name in the Transport Gateway cannot be modified while using the POP3 protocol. It can be done only when using the IMAP protocol.

Transport Gateway Connectivity

The following errors could be encountered when trying to obtain Transport Gateway connectivity:

- Transport Gateway is not able to connect to the Cisco backend
- Cisco.com ID is invalid
- Unavailability of DNS results in failure

Transport Gateway is not able to connect to the Cisco backend

When you click **Test Connection** on the Transport Gateway application, the following error message appears:

"The connection with the Cisco backend could not be established"

Symptom / Cause:

- User may not have configured the Transport Gateway with the correct proxy settings and proxy authentication.
- You may not have internet connectivity.
- The Cisco servers on the backend might be down.

Fix:

- Make sure your system has internet connectivity.
- If you are behind a firewall, then the respective proxy settings and proxy authentication information needs to be configured to the Transport Gateway.
- Delete the file **lb-truststore.jks** available at: **{TG_Install_Dir}\CSCOSchtg\tg\resources\security**. Restart TG service and try to test the connection again.
- Contact your IT representative for details on proxy settings, if they are not known.

Cisco.com ID is invalid

When you register the Transport Gateway and a message is displayed indicating that the Cisco.com ID is invalid.

Symptom / Cause:

- When you enter an invalid Cisco.com ID, the application will notify you about this problem via a pop-up message.
- To register a Transport Gateway a valid Cisco.com ID is required.

Fix:

- Verify if the entered Cisco.com ID is correct.
- If you do not have a valid Cisco.com ID then you can create a new Cisco.com ID via the Cisco.com Registration tool.

Unavailability of DNS results in failure

Symptom / Cause:

If the test connection fails due to unavailability of DNS

Fix:

Step 1 Get the IP address of **tools.cisco.com**. Run the command *ping tools.cisco.com* from a host which has the internet connection.

Step 2 Run the script *updateschurl.sh* (for Linux) OR *updateschurl.bat* (for Windows) in {**TG_Install_Dir**} */CSCOSchtg/tg/bin* by passing the IP address obtained in Step1 as an argument.

Eg. *sh updateschurl.sh <IP address>*

Transport Gateway Start Up

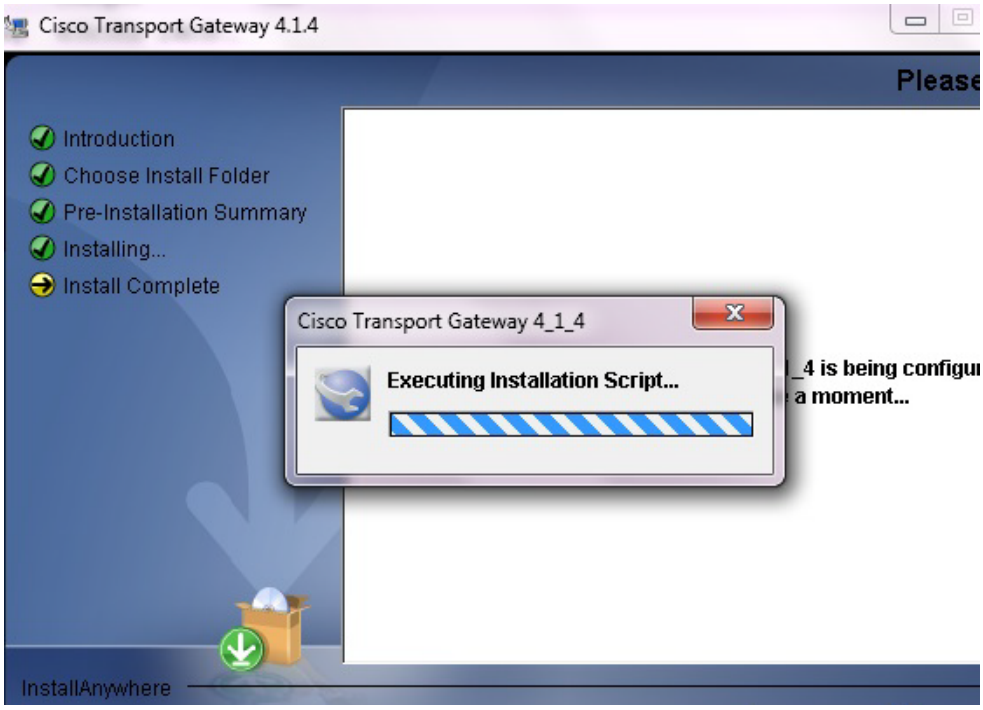
The following errors could be encountered when trying to start the Transport Gateway:

- Transport Gateway Installation hangs
- Transport Gateway does not start in Windows Environment
- Transport Gateway does not start in Linux Environment
- Transport Gateway UI Does Not Load
- Transport Gateway does not start or remains in running mode for long time

Transport Gateway Installation hangs

Symptom / Cause:

TG does not have the privileges to create a temporary folder as **Temp**, so hangs as shown in snapshot:



Fix:

- Kill the installtion on wizard using Windows Task manager.
- Create a folder name with name 'Temp'in the path:

  C:\Windows\system32\config\systemprofile\AppData\Local
- Install TG again. On the Installation wizard, click **Re-install**.

Transport Gateway does not start in Windows Environment

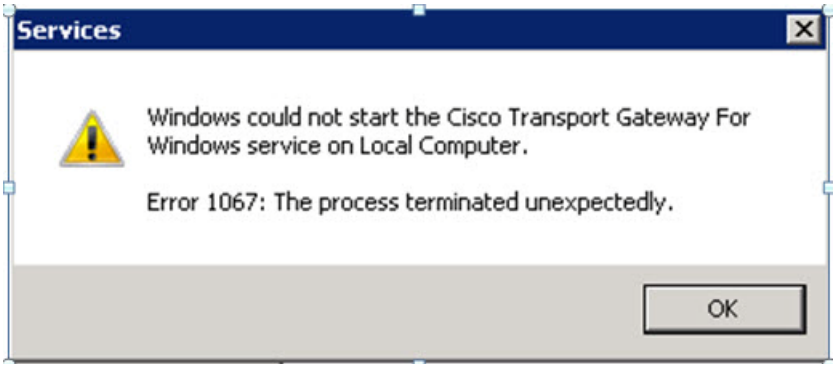
Symptom/Cause:

TG does not have the privileges to create a **Temp** folder and displays the following error on log.

```
java.lang.IllegalStateException: Cannot create tmp dir in
C:\Windows\system32\config\systemprofile\AppData\Local\Temp\ for context
o.e.j.w.WebAppContext{/Transportgateway,null},C:\Program Files\Cisco Transport Gateway
4.1\CSCOSchtg\tg\WebContent at
org.eclipse.jetty.webapp.WebInfConfiguration.resolveTempDirectory(WebInfConfiguration.j
ava:309)at
org.eclipse.jetty.webapp.WebInfConfiguration.preConfigure(WebInfConfiguration.java:49)
at org.eclipse.jetty.webapp.WebAppContext.preConfigure(WebAppContext.java:430)
at org.eclipse.jetty.webapp.WebAppContext.doStart(WebAppContext.java:466)
at org.eclipse.jetty.util.component.AbstractLifeCycle.start(AbstractLifeCycle.java:59)
at org.eclipse.jetty.server.handler.HandlerWrapper.doStart(HandlerWrapper.java:90)
at org.eclipse.jetty.server.Server.doStart(Server.java:262)
at org.eclipse.jetty.util.component.AbstractLifeCycle.start(AbstractLifeCycle.java:59)
at
com.cisco.ca.csp.cso.conn.tg.httpserver.JettyHttpReceiver.doConnect(JettyHttpReceiver.j
ava:126)
at com.cisco.ca.csp.cso.conn.tg.service.RunTGService.<init>(RunTGService.java:115)
at com.cisco.ca.csp.cso.conn.tg.service.TGServiceMain.start(TGServiceMain.java:77)
at org.tanukisoftware.wrapper.WrapperManager.startInner(WrapperManager.java:2909)
```

```
at org.tanukisoftware.wrapper.WrapperManager.handleSocket(WrapperManager.java:3761)
at org.tanukisoftware.wrapper.WrapperManager.run(WrapperManager.java:4158)at
java.lang.Thread.run(Unknown Source)
```

Throws an error as in snapshot:



Fix:

- Create a folder name with name ‘Temp’in the path:

  C:\Windows\system32\config\systemprofile\AppData\Local
- Start TG service.

Transport Gateway does not start in Linux Environment

Symptom / Cause:

- The Linux Environment does not have the required **libXp.so.6** library and receives the following error:

```
Exception in thread "main" java.lang.UnsatisfiedLinkError:
/opt/CSCOSchtg/_jvm/lib/i386/libawt.so: libXp.so.6: cannot open shared object file: No
such file or directory
    at java.lang.ClassLoader$NativeLibrary.load(Native Method)
    at java.lang.ClassLoader.loadLibrary0(Unknown Source)
    at java.lang.ClassLoader.loadLibrary(Unknown Source)
    at java.lang.Runtime.loadLibrary0(Unknown Source)
    at java.lang.System.loadLibrary(Unknown Source)
    at sun.security.action.LoadLibraryAction.run(Unknown Source)
    at java.security.AccessController.doPrivileged(Native Method)
    at sun.awt.NativeLibLoader.loadLibraries(Unknown Source)
    at sun.awt.DebugHelper.<clinit>(Unknown Source)
    at java.awt.Component.<clinit>(Unknown Source)
    at
com.cisco.zbase.app.transportgateway.service.ConfigureService.main(ConfigureService.ja
va:169)
```

Fix:

- TG expects the libXp.so.6 library to be available; need to install “xorg-x11-deprecated-libs" to fix this exception.Issue the following command:
- [root@brontitall logs]# yum install xorg-x11-deprecated-libs
- The issued command displays the following details:

```
Loading "fastestmirror" plugin
    Loading mirror speeds from cached hostfile
```

```
 * base: mirror.sanctuaryhost.com
 * updates: ftp.lug.udel.edu
 * addons: ftp.linux.ncsu.edu
 * extras: mirrors.easynews.com
Setting up Install Process
Parsing package install arguments
Resolving Dependencies
--> Running transaction check
---> Package libXp.i386 0:1.0.0-8.1.el5 set to be updated
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================
 Package          Arch       Version          Repository Size
================================================================================
Installing:
 libXp                   i386       1.0.0-8.1.el5    base 23 k

Transaction Summary
================================================================================
Install      1 Package(s)
Update       0 Package(s)
Remove       0 Package(s)

Total download size: 23 k
Is this ok [y/N]: y
Downloading Packages:
(1/1): libXp-1.0.0-8.1.el 100% |==================|  23 kB 0:00
Running rpm_check_debug
Running Transaction Test
Finished Transaction Test
Transaction Test Succeeded
Running Transaction
  Installing: libXp                         ########################### [1/1]

Installed: libXp.i386 0:1.0.0-8.1.el5
Complete!
```

Transport Gateway UI Does Not Load

Symptom:

Transport Gateway UI is not accessible on browser in Windows. The browser displays a message related to connection time out.

Cause:

Windows firewall might have blocked TG HTTP or HTTPs port.

Fix:

Check the firewall settings on the machine and configure firewall to allow TG HTTP or HTTPs port.

Symptom/Cause:

After installing the Transport Gateway in Linux, unable to load UI.

Fix:

Linux:

- Open hosts file from the location /etc/hosts
- Add new line to the existing entries [do not alter any existing entries]

```
Entry :  <<ip-address>> <<Hostname>> <<Domain-name>>
Eg. x.x.x.x vm-xxxx-003 vm-xxx-003.cisco.com
```

- Save the entry and restart linux server
- Restart TG service and access the UI.

Symptom/Cause:

HTTP 500 Error: ClassNotFoundException: Unable to load UI

Fix:

Windows:

- Restart the Cisco Transport gateway Service from Windows service (Type services.msc in run prompt)
- Restart the machine after TG installation (Not Mandatory).

Symptom/Cause:

HTTP 500 Error: JasperException: Unable to load class for JSP

Fix:

Windows:

- Open Transportgateway Installation folder/directory and go to lib folder eg.C:\Program Files (x86)\Cisco Connectivity Transport Gateway 3.5\CSCOSchtg\tg\lib
- Perform this initial step : Restart the Cisco Transport gateway Service from Windows service (Type services.msc in run prompt).

Symptoms:

- TG is not accessible from the devices
- TG UI is not accessible from external hosts/machines

Cause:

- TG service would have bound to VMware Network Adapter IP address and this IP address is not reachable from other hosts or devices (This can happen if virtualization software like VMware workstation/player/fusion is installed on the same host/machine)
- IP address not reachable from other hosts or devices

Fix: Two troubleshooting scenarios:

Troubleshooting 1:

1. Find the IP address of the host where TG is installed. This IP address should be accessible from the other hosts or devices.
   E.g. ipconfig on windows / ifconfig on linux
2. Edit the file
   <Install dir>CSCOSchtg\tg\conf\properties\jettyconfig.properties
3. Update jettyconfig.Host value with the IP address as derived from #1.
4. Update *jettyconfig.auto.ip* value to **false**.

5. Delete the file
   <Install dir>\CSCOSchtg\XML\ConfigHttp.xml
6. Restart the TG service

Troubleshooting 2:

1. Find the IP address of the host where TG is installed. This IP address should be accessible from the other hosts or devices.
   E.g. *ipconfig on windows / ifconfig on linux*
2. Launch the TG UI
3. Go to Http Settings under Configuration tab
4. Update the IP address as derived from #1.
5. Save the configurations
6. Restart TG service

Transport Gateway Uninstallation

Symptom:

Transport Gateway is not getting uninstalled completely

Fix:

Windows:

- Run **sc delete CONCSOSCHTG** from command prompt
- If TG is not getting uninstalled, run
  REG DELETE HKEY_LOCAL_MACHINE\SOFTWARE\CONCSOSCHTG /f
  from command prompt
- Remove the installation folder and restart the machine.

Transport Gateway does not start or remains in running mode for long time

If the Transport Gateway does not start or is in running state for longer time then follow a set of commands and manually start the TG service or check the status.

Symptom / Cause:

- The Transport Gateway is not started by following the steps of GUI.
- TG service is running

Fix: (for RDP)

- Browse to the **bin** folder of TG location
- To Start the TG service in the background execute **`/opt/CSCOSchtg/tg/bin> ./start.script`**
- To check whether the TG service is running or not execute
  `/opt/CSCOSchtg/tg/bin> ./sh.script status`
- To stop the TG service execute
  `/opt/CSCOSchtg/tg/bin> ./stop.script`

Transport Gateway Operation

For Linux after reboot

Symptom/Cause:

- TG service not running

Fix:

Start the service **./start.script** at **/opt/CSCOSchtg/tg/bin/**

Device to TG communication Troubleshooting

If using HTTP from device to TG:

1. Ensure TG is up and running
2. Ensure TG is reachable from device
   - Ping the TG host from device (either IP address OR host name as seen in "Device Service URL" under "HTTP Settings" of TG UI)
     E.g.: ping {IP Address/Host}
   - Check if TG HTTP port is reachable from device
     E.g.: telnet {IP Address/Host} {HTTP Port}
3. Ensure there are no ACLs or other security restrictions in your network which prevent the communications from device to TG.

If using SMTP(Email) from device to TG:

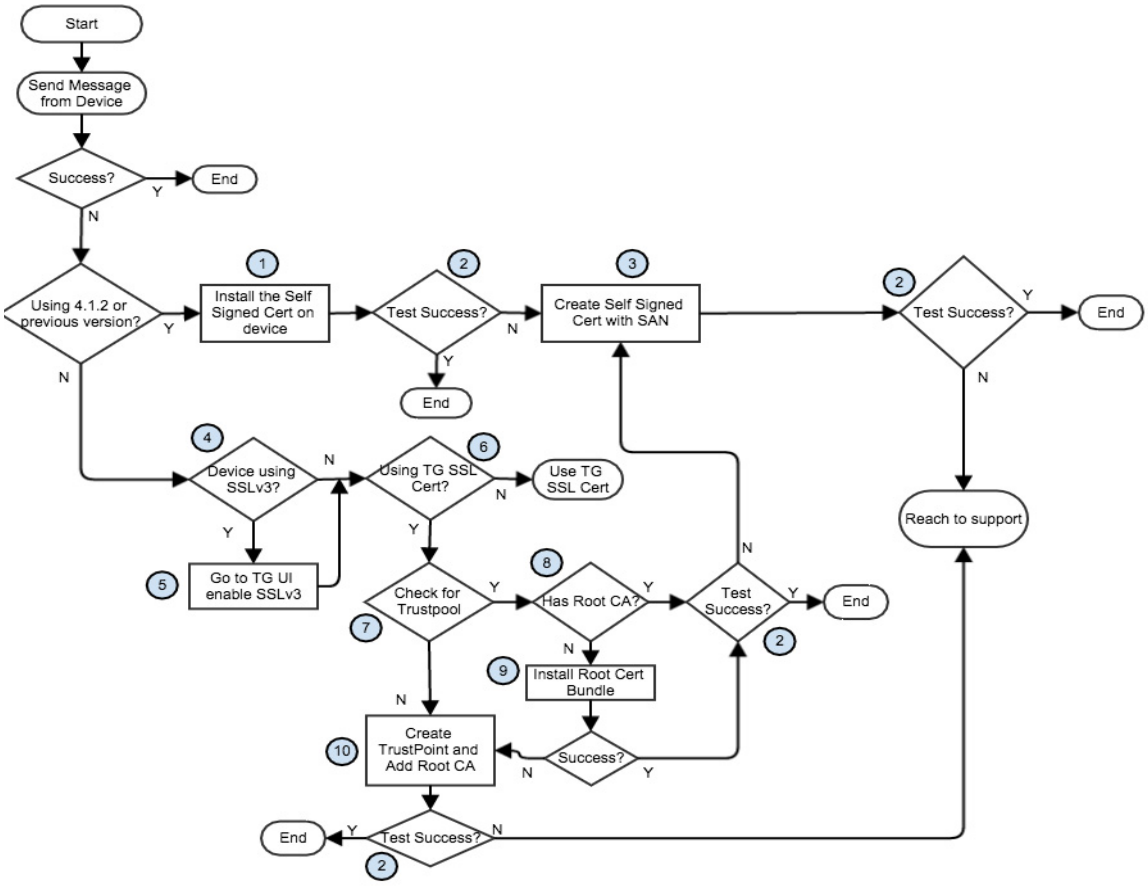
1. Ensure you have successfully configured the Mailbox using “Mailbox Configuration” in TG UI.
2. Ensure device can connect to SMTP port on mail server

   E.g.: telnet {IP address of mail server} {SMTP_PORT}
3. Ensure device IP address is allowed (white list) in the SMTP server relay list

If using HTTPS from device to TG:

Below flow chart will guide you to get the HTTPS working from device to TG. Please follow the numbers & their descriptions to understand how to verify at each step.

Figure 4-14 Using HTTPs from device to TG Flow Chart



1. **Install the Self-signed certificate**: Please follow the steps given below to install the Self-signed certificates that come along with TG on the device.
   a. Download TG-HTTPS-Cert.zip and unzip it to desired location
   b. Open the "*tgserver.pem*" file in a text editor
   c. Go to device console and issue the below commands:

      configure terminal

      crypto ca trustpoint cisco

      enrollment terminal

      revocation-check none

      crypto ca authenticate cisco

Note Copy and paste the base 64 encoded certificate from the text editor (obtained in step b). End with a blank line or type the word "quit" on a line.

2. **Test Success:** This step will help you to check if the HTTPS communication from device to TG is successful. As part of this step, you can trigger a message from device & check if it has reached TG. Refer to FAQs: How to check if TG has received a message from device?
3. **Create Self-signed Certificate with SAN**: This step will guide you to create a new Self-signed certificate with SAN (Subject Alternative Name) in it. Refer to Appendix -A
4. **Device Using SSLv3**: Here you will check if the device is using SSLv3 for SSL handshake. If your devices are using older OS images, then they might be using SSLv3. Refer to FAQs: How to check if device is using SSLv3 for SSL handshake with TG?.
5. **Goto TG UI enable SSLv3**: If you detect device using SSLv3, then HTTPS from device to TG will not work. This is because from TG 4.1.3 SSLv3 is disabled due to security vulnerabilities. You will have to go to TG UI and enable it by accepting the security risks. You can do so by going to "Http Settings" tab under "Configuration" section of TG UI.
6. **Using TG SSL Cert**: If you have used the "TG SSL Certificate" feature to generate the Cisco CA signed certificates, then the answer is YES.
7. **Check for Trustpool:** Some devices have trustpool feature. Please follow the steps given in FAQ (Frequently Asked Questions to check if the device is having trustpool.- How to verify if my device has trustpool or not?
8. **Has Root CA**: Here you will check if the trustpool has the "Cisco Licensing Root CA" certificate in it. If yes, then the HTTPS communication from device to TG will work seamlessly. Please follow the steps given in FAQ (My device has trustpool, but how do I know if the trustpool has the Cisco Licensing Root CA?) to check if the trustpool is having Cisco Licensing Root CA.
9. **Install Root Cert Bundle**: If the device trustpool doesn't have the Cisco Licensing Root CA, then you can install the latest Root Cert Bundle. Please follow the steps given in FAQ (TG SSL Certificates Frequently Asked Questions - My device trustpool does not have the Cisco Licensing Root CA. How do I install it?) on how to install the Root Cert Bundle.
10. **Create Trustpoint and Add Root CA**: Here you can add the Cisco Licensing Root CA certificate manually onto the device by creating a trust point. Please follow the steps given in FAQ (TG SSL Certificates Frequently Asked Questions - My device trustpool does not have the Cisco Licensing Root CA. How do I install it?) on how to create a trustpoint on device and add the certificate.

Frequently Asked Questions

TG SSL Certificate FAQs

Q. What are the advantage of using SSL Certificate option?

A. If your devices are having the trust pool feature and the trust pool has "Cisco Licensing Root CA" certificate, then HTTPS from device to TG will work seamlessly without any manual intervention.

Q. How to verify if my device has trustpool or not?

A. Execute the below command on device console. If the device has trust pool, then it will display the certificates that are part of trust pool.
For **IOS/IOS-XE**: *crdc_ch1921#sh crypto pki trustpool*

For **NX-OS/IOS-XR**: *crdc_ch1921# show crypto ca trustpool*

Q. My device has trustpool, but how do I know if the trustpool has the Cisco Licensing Root CA?

A. Go to device console and execute the below command:

*For **IOS/IOS-XE**:*
crdc_ch1921#sh crypto pki trustpool | i Licensing Root CA
cn=Cisco Licensing Root CA
cn=Cisco Licensing Root CA

*For **NX-OS/IOS-XR:***
crdc_ch1921#show crypto ca trust pool | i Licensing Root CA
cn=Cisco Licensing Root CA
cn=Cisco Licensing Root CA

Q. My device trustpool does not have the Cisco Licensing Root CA. How do I install it?

A.

- Goto device console
- Issue these commands

O2_bot#conf t

O2_bot(config)#crypto pki trustpool import url
http://www.cisco.com/security/pki/trs/ios_core.p7b

E.g.: O2_bot#conf t

O2_bot(config)#crypto pki trustpool import url
http://www.cisco.com/security/pki/trs/ios_core.p7b

Translating "www.cisco.com"...domain server (xx.xxx.xx.xxx) [OK]

Reading file from http://www.cisco.com/security/pki/trs/ios_core.p7b

Loading http://www.cisco.com/security/pki/trs/ios_core.p7b

% PEM files import succeeded.

Q. My device does not have trustpool. How can I use this feature?

A. In this case you need to create the trustpoint. Download the TG_SSL_Certificate.zip file from Cisco.com and extract it. Open the "CiscoLicensingRootCA.cer" in a text editor.

Follow these commands on device console:

O2_bot#conf t
O2_bot(config)#crypto pki trustpoint {trust point name}
O2_bot(ca-trustpoint)#enrollment terminal
O2_bot(ca-trustpoint)#revocation-check none
O2_bot(ca-trustpoint)#exit
O2_bot(config)#crypto pki authenticate {trust point name}
<Paste the contents of the certificate from the text editor here>

E.g.:

O2_bot#conf t
O2_bot(config)#crypto pki trustpoint LicRoot
O2_bot(ca-trustpoint)#enrollment terminal
O2_bot(ca-trustpoint)#revocation-check none
O2_bot(ca-trustpoint)#exit
O2_bot(config)#crypto pki authenticate LicRoot
Enter the base 64 encoded CA certificate.
End with a blank line or the word ""quit"" on a line by itself
<Enter your certificate here>
Certificate has the following attributes:

Fingerprint MD5: 1468DC18 250BDFCF 769C29DF E1F7E5A8
Fingerprint SHA1: 5CA95FB6 E2980EC1 5AFB681B BB7E62B5 AD3FA8B8
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported"

Q. How to check if device is using SSLv3 for SSL handshake with TG?

A. Please run these commands on devices:

*For **IOS/IOS-XE**:*

debug ssl openssl errors
debug ssl openssl ext
debug ssl openssl msg
debug ssl openssl states

*For **IOS-XR:***

debug ssl errors
debug ssl ext
debug ssl msg
debug ssl states

And then try to send the message from device again. Check the device logs for occurrences of below string:

SSL_connect:failed in SSLv3 read server hello A

If you find any matches, that means that device could be using SSLv3 for the SSL handshake.

General TG Operational FAQs

Q. How to check if TG is up and running?

A.

Linux:

– Go to *{TG_Install_Dir}/CSCOSchtg/tg/bin/*

– Execute command: *./sh.script status*

Windows:

– Go to services console

– Check if the TG service (Cisco Transport Gateway For Windows) is running

Q. How to check if TG has received a message from device?

A. Open the TG log file (StatusOfTG.log) and search for below lines:

Using **HTTP/S** between device and TG:

Received a message over HTTP/S on TG.....

Using **CSSM Satellite** image:

Received a SL message to be processed via Lindos.....

Using **SMTP** between device and TG:

com.cisco.ca.csp.cso.conn.tg.email.MailHandlerImpl - New Call Home message found!

Q. How to check if the TG message store has reached its limit?

A. Open the TG log file (StatusOfTG.log) and search for below command line:

isDiscOverflow :true

Q. How to check if the message has been successfully sent to Cisco from TG?

A. Open the TG log file (StatusOfTG.log) and search for below line:

Forward status: success

Troubleshooting and Support

This chapter covers the following topics:

Note For information on troubleshooting the Transport Gateway errors refer TG User Guide, Troubleshooting Cisco Transport Gateway Errors section.

Troubleshooting Call Home Errors

Topics in this section include Transport Gateway problems dealing with:

Troubleshooting AAA Authorization Failure Errors

Received error message - command authorization failed

AAA is configured in the customer's network and the Cisco device, which has Call Home configured, sends a Call Home message indicating “command authorization failed”.

Symptom / Cause:

- There may be no working connection between the Cisco device and the AAA server.
- Callhome may not be properly configured on the AAA server.

Fix:

- Verify that there is a working connection between the Cisco device and the AAA server.

- Verify that callhome is properly configured on the AAA server; a user account with username = callhome must be configured on the AAA server.

Troubleshooting Call Home HTTP Destination Errors

Call-Home HTTP request failed (ERR 0)

The following error may be logged on the Cisco device when sending Call-Home messages to Smart Call Home, using the HTTP destination transport method.

%CALL_HOME-3-HTTP_REQUEST_FAILED: Call-Home HTTP request failed (ERR 0)

Symptom / Cause:

- This error indicates that a connection could not be established with the Smart Call Home HTTPS server.

Fix:

To troubleshoot, please verify the following:

- If the device is not using the CiscoTAC-1 profile, then confirm that the destination HTTP address configured in the user defined profile is: https://tools.cisco.com/its/service/oddce/services/DDCEService.
- Confirm that the Cisco public key certificate, found at the back of the Smart Call Home user's guide, is installed.
- Confirm that traffic for TCP port 443 is not being blocked between the Cisco device and the Smart Call Home HTTPS server.
- Confirm that traffic for TCP port 80 is not being blocked between the Cisco device and the Certificate Revocation List (CRL) Server. If traffic for TCP port 80 must be blocked then the “revocation-check none” option may be configured under the crypto trust-point configuration

Note Failing to check certificate revocation is NOT recommended

- Check network connectivity from the Cisco device to the Smart Call Home HTTPS server (tools.cisco.com). If ICMP echo's or echo replies are not blocked in your network, then use the ping network tool to confirm a communication path. Also, connectivity may also be confirmed by performing a telnet to tools.cisco.com on port 443 or port 80.

Call-Home HTTP request failed (ERR 500)

The following error may be logged on the Cisco device when sending Call-Home messages to Smart Call Home, using the HTTP destination transport method:

%CALL_HOME-3-HTTP_REQUEST_FAILED: Call-Home HTTP request failed (ERR 500)

Symptom / Cause:

- This error indicates that the Smart Call Home HTTPS server encountered an unexpected condition that prevented it from completing the request from the client.
- Possible causes may include network failures, Web server software or hardware failures, or latency resulting in connection time-outs.

Fix:

- For further assistance with troubleshooting or to report these failures, please open a service request with the Cisco Technical Assistance Center.

General Web Application Troubleshooting

The following error can occur when using the Smart Call Home web application.

Received Application Error on web page

An Application error page appears when processing a request on the Smart Call Home web application

Symptom / Cause:

- When an application error occurs, an Application Error appears in the web application.
- This page contains a link to request support.

Fix:

- Click on the link to request support and enter the information related to the action you were trying to execute in the web application, search parameters used, etc.
- This information will be sent to the Smart Call Home support team.
- No further action is required from your side.

Device Registration Troubleshooting

Topics in this section include Device Registration Troubleshooting problems dealing with the following areas:

- Troubleshooting Entitlement
- Troubleshooting for Edit Device Preferences
- Troubleshooting for Edit Device Registration

Troubleshooting Entitlement

Confirming a device registration requires:

- Valid and contract in your Cisco.com profile that is supported by Smart Call Home.
- Case Management permissions to query, create and update service requests.
- Valid security token.

If one of the previous requirements is missing, Smart Call Home will not be able to complete your device registration. The following can occur:

Contract does not exist in your Cisco.com profile

The device you are trying to register is covered by a contract but this contract does not exist in your Cisco.com profile.

Symptom / Cause:

- Smart Call Home will notify you about this problem by displaying a UI message and will not complete the device registration.
- Error occurs when you are trying to confirm the device registration and the contract covering the device does not exist in your Cisco.com profile.

Fix:

- You do not have to take any action because Smart Call Home will automatically send a request to the appropriate Cisco team to add the contract to your Cisco.com profile.
- Once the contract has been added you will be notified by Cisco and can confirm the device registration in Smart Call Home.

Contract is not supported by Smart Call Home

The device you are trying to register is covered by a contract but the contract is not supported by Smart Call Home.

Symptom / Cause:

- When you are trying to confirm a device registration and the contract covering the device is not supported by Smart Call Home the application will notify you about this problem via a UI message.

Fix:

- Currently Smart Call Home does not support Partner Branded contracts (i.e. contracts Cisco has with your Cisco Partner). Partner Branded contracts will be supported in the future.

Do not have a contract that allows registration for Smart Call Home

The device you are trying to register is not covered by a contract and you do not have a contract in your Cisco.com profile that allows registration for Smart Call Home.

Symptom / Cause:

- To confirm a device registration you need to have at least one contract supported by Smart Call Home in your Cisco.com profile.
- When the application does not find a contract in your Cisco.com profile that can be used to register your device, you will be notified about this via a UI message.
- This UI message will also include instructions on steps to be taken to register your device for Smart Call Home.

Fix:

Based on the instructions included in the displayed UI message, choose one of the following solutions:

- Contact your partner/reseller or Service Sales Manager to cover this device by adding it to an existing or new service contract.

- Use the Service Contract Center to purchase a contract to cover this device, or use the Service Support Center and submit a case to add the serial number to a service contract that already covers this device (for Partners/Resellers only).
- Add a newly purchased or existing contract to your Cisco.com profile using the Central Profile Repository (CPR) Profile Update tool.

Warranty entitlement failed

The device you are trying to register is covered by an active warranty. The warranty entitlement failed and you do not have a contract in your Cisco.com profile that allows registration for Smart Call Home.

Symptom / Cause:

- Do not have company name in Cisco.com profile
- The company name of the firm that purchased this product from Cisco does not match the company name in your Cisco.com profile.

Fix:

Based on the instructions included in the displayed UI message, choose one of the following solutions:

- When you need to update the company associated with your Cisco.com profile, use the Central Profile Repository (CPR) Profile Update tool.
- Entitle this device for Smart Call Home under a valid service contract that exists in your Cisco.com profile.
- Contact your partner/reseller or Service Sales Manager if you want to cover this device by adding it to an existing or new service contract.
- Use the Service Contract Center to purchase a contract to cover this device, or use the Service Support Center and submit a case to add the serial number to a service contract that already covers this device (for Partners/Resellers only).
- Add a newly purchased or existing contract to your Cisco.com profile using the Central Profile Repository (CPR) Profile Update tool.

Do not have proper permissions to update Service Requests

Do not have required Case Management Permissions that let you query, create and update Service Requests.

Symptom / Cause:

- To confirm a device registration you need case management permissions that allow you to query, create and update Service Requests.
- When you do not have the required permissions, the application will notify you about this via a UI message including the action required to get the required case management permissions.

Fix:

- Either add a contract to your Cisco.com profile, using the Central Profile Repository (CPR) Profile Update Tool that would entitle you to submit Service Requests, or
- Contact your Partner or Service Sales Manager to purchase a service contract that you can use for this purpose.

An Invalid Security Token was entered

An Invalid Security Token was entered when trying to confirm a device registration

Symptom / Cause:

- When using a security token to confirm a device registration, need to make sure that the security token is correct.
- When the security token is not correct or invalid, the system will notify you about this via a UI message.

Fix:

- In the email notification you received about the pending device registration, verify whether the security token you entered matches with the security token included in the email for the device you would like to register, OR
- Click on the link available in the email notification, which will enter the security token automatically for you.

Exceeded the maximum number of invalid security tokens you can enter

The application indicates that the maximum number of invalid security tokens has been entered and does not allow you to confirm a device registration.

Symptom / Cause:

- Smart Call Home will not allow you to enter more than 10 invalid security tokens.
- When 10 invalid security tokens have been entered the system will not allow you to confirm a device registration anymore.
- You will be notified about this via a UI message.

Fix:

- To be able to confirm a device registration, contact the Smart Call Home support team.
- This can be done by clicking on the link provided in the displayed UI message and submitting a support request.

Troubleshooting for Edit Device Preferences

The following error can occur when editing device preferences on the Smart Call Home web application.

The person is not listed in the Service Request Contact person drop-down list.

The person you would like assign as Service Request Contact person is not listed in the Service Request Contact person drop-down list in the Device Preferences page.

Symptom / Cause:

- Only users registered as Administrators for the same company the device is registered for can be a Service Request contact person for the device.
- Only these persons will be available in the Service Request Contact person drop-down list.

Fix:

- Verify if the person you would like to assign as SR contact person is registered as Administrator for the same company the device is registered for.
- If they are registered as User, delete the existing user registration and create a new registration as Administrator for the company.

Troubleshooting for Edit Device Registration

The following error can occur when editing a device registration on the Smart Call Home web application.

Can not associate a device registration with a different contract number

You would like to associate a device registration with a different contract number but the application does not let you do this.

Symptom / Cause:

- When a device is covered by a contract or an active warranty, you can only use this contract or warranty to register the device.
- When the device is not covered by a contract or active warranty, you can associate a different contract with the device registration in case you have another contract in your Cisco.com profile that is supported by Smart Call Home.
- When you do not have another contract in your Cisco.com profile that can be used to register the device, the application will indicate that no other contracts are available.

Fix:

- When your device is covered by a contract or active warranty, you will not be able to register the device for another contract.
- When your device is not covered by a contract or active warranty, add the contract you would like to use for the device registration to your Cisco.com profile using the Central Profile Repository (CPR) Profile Update tool.
- If your device is covered by more than one contract that is supported by Smart Call Home you can associate the device registration with another contract that is covering your device.

User Registration Troubleshooting

Topics in this section include User registration problems dealing with:

- New User Registration Troubleshooting.
- Delete User Registration Troubleshooting.

New User Registration Troubleshooting

Creating a new user registration requires:

- Valid Cisco.com ID for the to-be registered person.

- At least one valid contract for the company that is supported by Smart Call Home, when the to-be registered person needs to be registered as an Administrator.

The following problems can occur:

Can not register yourself to Smart Call Home

During the registration process you enter your Cisco.com ID, to register yourself, and find out that you cannot register yourself.

Symptom / Cause:

- When you enter your own Cisco.com ID during the user registration process Smart Call Home notifies you, via a UI message, that self-registration is not supported.

Fix:

- When you need a registration for another company, either register a device for this other company (using a contract for this same company) OR
- Ask one of your colleagues, who is already registered to that company, to register you.

Entered an invalid Cisco.com ID

You entered a Cisco.com ID that is invalid.

Symptom / Cause:

- When you enter a Cisco.com ID that does not exist, during the user registration process, the application will notify you about this via a UI message.

Fix:

- Verify if the entered Cisco.com ID is correct. When the user you are trying to register does not have a Cisco.com ID, create a new Cisco.com ID via the Cisco.com Registration tool.

Trying to register someone as an administrator and only have the User role available

During the user registration process, you want to register someone as an Administrator but the only role that is available in the drop-down list is the User role option.

Symptom / Cause:

- When a person needs to be registered as Administrator, they need to have at least one supported contract with that corresponding company, in their Cisco.com Profile.

Fix:

- Add a contract to the Cisco.com profile using the Central Profile Repository (CPR) Profile Update tool.

Delete User Registration Troubleshooting

You can obtain an error deleting a user registration in one of the following scenarios.

Can not delete user registration for a Service Request contact person

Service Request contact person for one or more devices registered for the company on this registration.

Symptom / Cause:

- Smart Call Home does not allow a user registration to be deleted when the owner of the registration is a Service Request contact person for one or more devices registered for the company on this registration

Fix:

- Assign a new Service Request contact person to the devices for which this user is a Service Request contact person.
- After a new Service Request contact person has been assigned, the user registration can be deleted.

Can not delete user registration for last administrator

The user is the last administrator associated with a Transport Gateway registration for the company on this registration.

Symptom / Cause:

- Smart Call Home does not allow a user registration to be deleted when the owner of the registration is the last administrator associated with a Transport Gateway registration for the company on this registration.

Fix:

- Delete the Transport Gateway registration for which the user is an administrator.
- Owner of the registration is a Service Request contact person for one or more devices registered for the company on this registration
- After the Transport Gateway registration has been deleted, the user registration can be deleted.

Reports Troubleshooting

Three types of Report troubleshooting are covered in this section:

- Device Report Troubleshooting
- Call Home History Report Troubleshooting
- Message Processing Troubleshooting

Device Report Troubleshooting

The data displayed in the Device Report is based primarily on the content of the Inventory Call Home messages.

The following situations can cause the Device Report to be not available or only partly available.

Report does not display the current inventory and configuration

You ran the Device Report and the report does not display the current inventory and configuration of your device.

Symptom / Cause:

- The data in the Device Report is retrieved from the most recently received inventory and configuration messages sent by your device.

Fix:

- Verify when the last inventory and/or configuration message was sent by your device (you can do this via the Call Home History report).
- If needed, trigger the device to send a new inventory and/or configuration message.

No data was found for the requested device

You ran the Device Report for a specific device and Smart Call Home indicates that no data was found for the requested device.

Symptom / Cause:

- The Device Report is only generated when a registered device has sent at least one inventory Call Home message.
- Problem occurs when one of the following situations occur:
  - No Inventory Call Home message was sent by the device
  - The device is not registered in Smart Call Home
  - You run the Device Report for this device a UI message is displayed indicating that no data was found.

Fix:

- Verify whether the device is registered for Smart Call Home (registration status 'Complete').
- If the device is registered for Smart Call Home, verify if the device has already sent an inventory Call Home message to the Cisco backend (you can do this via the Call Home History report).
- When no inventory message has been sent yet, trigger the device to send an inventory Call Home message.

One or more devices are not displayed in the Report

You ran the Device Report for all your devices and one or more devices are not being displayed in the Report.

Symptom / Cause:

- The Device Report is being displayed but one or more of the devices you expect to be included in the report are missing.
- The Device Report is generated for only registered devices.

Fix:

- Make sure that the devices are registered in Smart Call Home (registration status 'Complete').

- When the device is registered for Smart Call Home, verify if the device has already sent an inventory Call Home message to the Cisco backend (you can do this via the Call Home History report).
- When no inventory message has been sent yet, trigger the device to send an inventory Call Home message.

Configuration details are not being displayed

You ran the Device Report, in the Device Details page, the Configuration details are not being displayed in the report.

Symptom / Cause:

- The Configuration Details are retrieved from a configuration message sent by the device.
- If no Configuration Call Home message has been sent by the device yet, then the application will indicate that the configuration data is not available.

Fix:

- Verify if the device already sent a Configuration Call Home message to the Cisco backend (you can do this via the Call Home History report).
- If no configuration message was sent yet, trigger the device to send a full configuration message to the Cisco backend.

Call Home History Report Troubleshooting

The following situations can cause the Call Home History Report to be not available or only partly available.

No data was found for a specific device

You are trying to run the Call Home History Report for a specific device and Smart Call Home indicates that no data was found.

Symptom / Cause:

- When no supported Call Home message was sent by the device or the device is not registered in Smart Call Home and you try to run the report for this device, a UI message will be displayed indicating that no data was found.

  The Call Home History Report is only generated when a registered device has sent at least one supported Call Home message.

Fix:

- Verify whether the device is registered for Smart Call Home (registration status 'Complete').
- When the device is registered for Smart Call Home, verify if the device has already sent a supported Call Home message to the Cisco backend.
- If no supported message has been sent yet, trigger the device to send a Call Home message.

One or more devices are not being displayed in the Report

You ran the Call Home History Report for all your devices and one or more devices are not being displayed in the Report

Symptom / Cause:

- The Call Home History Report that is being displayed is missing one or more devices you expect to be included in the report.
- The report only includes devices that are registered for Smart Call Home.

Fix:

- Make sure that the devices are registered in Smart Call Home (registration status 'Complete').
- If the device is registered for Smart Call Home, verify if the device has already sent an inventory Call Home message to the Cisco backend.
- When no inventory message has been sent yet, trigger the device to send an inventory Call Home message.

Message Processing Troubleshooting

The following scenarios are related to problems processing different types of messages.

Message Processing Problems impacting the Reports

The following message processing problems are ones that affect the Smart Call Home reports:

Call Home message failed

You received an email notification indicating that the processing of a Call Home message failed

Symptom / Cause:

- The device sent a Call Home message to the Cisco backend and there was a problem with the message processing,

Fix:

- You do not need to take any action. The Smart Call Home support team is automatically notified and will look into the problem.

Inventory Call Home message failed

You received an email notification indicating that the processing of an Inventory Call Home message failed.

Symptom / Cause:

- The device sent an Inventory message to the Cisco backend.
- There was a problem with the message processing and you received an email notification indicating that the processing for the Call Home message failed.

Fix:

You do not need to take any action. The Smart Call Home support team is automatically notified and will look into the problem.

Device Report is either not available or does not reflect the last inventory message.

Symptom / Cause:

- When you run the Device Report for this device, the report is not available for this device or the data in the report does not reflect the new data included in the last inventory message.

Fix:

- You do not need to take any action. The Smart Call Home support team is automatically notified and will look into the problem.

Call Home History Report does not have the message processing results

Symptom / Cause:

- When you run the Call Home History report for this device, the inventory message will be included in the report but the message processing results will not be available

Fix:

- You do not need to take any action. The Smart Call Home support team is automatically notified and will look into the problem.

Configuration details are not available or do not reflect the current configuration

You received an email notification indicating that the processing of a configuration Call Home message failed. When you run the Device Report, the configuration details are not available or do not reflect the current configuration of your device.

Symptom / Cause:

- The device sent a configuration message to the Cisco backend.
- Since there was a problem with the message processing, you received an email notification indicating that the processing for the Call Home message failed.

Fix:

- You do not need to take any action. The Smart Call Home support team is automatically notified and will look into the problem.

Message Processing Problems Impacting Service Request Creation/Update

The following message processing problems are ones that affect the creation or updating of service requests:

Service Request creation or update failed

You received an email notification indicating that the Service Request creation or update failed.

Symptom / Cause:

- Receive an email notification indicating that the creation or update of a Service Request failed.
- Due to a problem in the Cisco backend, creating or updating a Service Request failed.

Fix:

- Review the message processing results in the Call Home History report.
- When any recommended steps to resolve the problem are included in the results, verify these steps.
- If these do not resolve the problem you can manually raise a Service Request.

Service Request not created due to missing Case Management permissions.

You received an email notification indicating that a Service Request could not be created due to missing Case Management permissions:

Symptom / Cause:

- For a Service Request to be created, the Cisco.com user id used as Service Request contact person needs to have the appropriate Case Management Permissions.
- If the person assigned as Service Request contact person for the device in Smart Call Home does not have permissions to query, update and create service requests, an email notification will be sent when Smart Call Home tries to create a Service Request for this device.

Fix:

Perform one of the following tasks:

- Assign another person as Service Request contact for this device in Smart Call Home.
- Add a contract to your profile that would entitle you to submit Service Requests.
- Contact your Cisco partner, reseller, or Cisco service sales representative to purchase a service contract.

Service Request not created because device is not entitled.

You received an email notification indicating that a Service Request could not be created because the device is not entitled.

Symptom / Cause:

- To create a Service Request, the contract that was used to create the Service Request needs to support entitlement for the specified device.
- Smart Call Home uses the contract that is associated with the device registration to create Service Requests.
- This contract may have expired.

Fix:

Perform one of the following tasks:

- Purchase a contract for this product from your Cisco service sales representative, Cisco partner or reseller.
- Contact Service Relations if you believe this product should be covered under the contract or warranty that is associated with the device registration in Smart Call Home.

Technical Support Information

For technical support, please contact Cisco Technical Support via:

Email:tac@cisco.com <mailto:tac@cisco.com>

Telephone:

US and Canada: +1-877-330-9746

Europe: Austria0800 006 206

Belgium 0800 49913

France 0805 119 745

Germany 0800 589 1725

Italy 800 085 681

Netherlands 0800 0201 276

Spain 800 600472

Switzerland 0800 840011

UK 0800 2795112

From the rest of the world, choose the appropriate phone number from http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

References

See the following items for additional information about Call Home feature and Smart Call Home service:

- For more information.
- Resources for Smart Call Home.
- Terminology.
- CA Root Certificate Update Process.

For More Information

For more information about Smart Call Home, there are several options available, you can:

- “Smart Call Home Service Introduction - http://www.cisco.com/en/US/products/ps7334/serv_home.html
- Smart Call Home presentation
- Catalyst 6500 Call Home Configuration Guide – http://www.cisco.com/en/US/products/hw/switches/ps708/products_configuration_guide_book09186a00801609ea.html
- Catalyst 6500 Command Reference – http://cisco.com/en/US/products/hw/switches/ps708/products_command_reference_book09186a0080160cd0.html
- Generic Online Diagnostics on the Cisco Catalyst 6500 Series Switch – http://www.cisco.com/en/US/products/hw/switches/ps708/products_white_paper0900aecd801e659f.shtml
- Cisco Catalyst 6500 Series with Cisco IOS Software Modularity – http://www.cisco.com/en/US/products/hw/switches/ps708/prod_bulletin0900aecd80313e15.html
- Embedded Event Manager (EEM) on the Cisco Catalyst 6500 Series – http://cisco.com/en/US/products/hw/switches/ps708/products_white_paper0900aecd805457c3.shtml
- Cisco 7600 Series Command References - http://www.cisco.com/en/US/products/hw/routers/ps368/prod_command_reference_list.html
- Cisco 7600 Series Cisco IOS Software Configuration Guide, 12.2SX - http://www.cisco.com/en/US/partner/docs/routers/7600/ios/12.2SXF/configuration/guide/swcg.html

- Cisco 7600 Series Technical References - http://www.cisco.com/en/US/products/hw/routers/ps368/prod_technical_reference_list.html
- Cisco 7600 White Papers - http://www.cisco.com/en/US/products/hw/routers/ps368/prod_white_papers_list.html
- Use the feedback box on the Smart Call Home web application
- Access the Smart Call Home Technical Overview – http://www.cisco.com/application/pdf/en/us/guest/products/ps7334/c1266/cdccont_0900aecd8063c595.pdf
- Contact Smart Call Home at email address – sch-support@cisco.com

Resources for Smart Call Home

For more information about Smart Call Home:

- Smart Call Home Support Community http://www.cisco.com/en/US/products/ps7334/serv_home.html
- Smart Call Home on Cisco.com http://www.cisco.com/en/US/products/ps10600/tsd_products_support_series_home.html
- Smart Call Home web application (portal) https://tools.cisco.com/sch

Terminology

The following list defines the different components, tools and terms used in Smart Call Home:

- **Call Home (CH)** – Product feature in IOS version 12.3(33)SXH that uses SMTP or HTTP connections established with a configurable destination to send formatted messages. The messages contain Inventory or Configuration information that are collected at scheduled intervals. Configuration, Diagnostics, Environmental, Inventory or System Log (syslog) information is collected during real-time events; Test, Inventory, Configuration Diagnostic and Environmental information are collected on-demand.

The IOS code incorporates device diagnostics (i.e. GOLD) that enables the sending of the following outbound alerts and alarms in email messages to Smart Call Home.

- **Call Home Alert Group** – Is a configurable Call Home feature that groups detectable events from one of the Configuration, Diagnostics, Environmental, Inventory or System Log categories for monitoring.
- **Call Home Profile** – Is a configurable Call Home feature that provides a structure to bundle together several Alert Groups, to select transport methods, to assign multiple destination addresses and to specify message format options.
- **Call Home message formats** – Are configurable formatting options used by the IOS Call Home feature when creating messages. The Short Text format is suitable for pagers or printed reports and the Long Text format contains Full formatted message information suitable for human reading. The XML Messages contain the same data as the Long Message, but with the addition of XML tagging and AML specific transport information to allow machine-readable parsing and routing of the message in the Smart Call Home System.

- **Call Home message type** – Is a field within an IOS Call Home message that indicates what type of message it contains: Configuration, Diagnostics, Environmental, Inventory, Test or System Log (syslog) information.
- **Call Home message sub-type** – Is a field within an IOS Call Home message that indicates that the message contains full or delta Configuration or Inventory information, Gold major, minor or normal Diagnostics information, minor or major Environmental information, Test or System Log (syslog) information.
- **Cisco.com profile** – Where information on Cisco contracts, case management permissions and user's company are kept for use by the Smart Call Home service.
- **Cisco Backend (CBE)** – Contains a collection of various tools and information:
  - Smart Call Home service.
  - Guided searches for the Smart Call Home reporting process.
  - Generation of customized reports for Smart Call Home users.
  - Device install-base data and their associated contracts.
  - Customer device-based troubleshooting tools.
- **Cisco Contracts**:

  Contract information is kept in the Cisco.com profile. A customer can register a device using one of the following types of branded contracts:
  - **Cisco Branded – Direct**: Customer bought product directly from Cisco and contacts Cisco directly if they need support.
  - **Cisco Branded – CBR (Cisco Branded Reseller)**: Customer bought product from Cisco reseller and customer contacts Cisco directly if they need support.
  - Other types of contracts will become supported in a future release.
- **Customer Specific Network Alerts** – Smart Call Home supports the following Call Home message types:
  - **Configuration** – Contains image name and feature, running and startup configs, SW features technologies and sub-technologies.
  - **Environment** – Contains information about environmental alarms for the device clock, VTT, power supply and modules. Depending on the type of alert, a notification is sent to the customer and a Service Request is generated.
  - **GOLD** – Contains information about diagnostic tests, what tests were run, their status, and results. Depending on the type of failure, a Service Request is generated.
  - **Inventory** – Contains information about the device, software, modules.
  - **Test** – Contains information that is common to all message types. The content of test messages is not processed by Smart Call Home and hence no specific message processing results will be available for test messages.
  - **Embedded Event Manager (EEM)** – Detects real time events and takes action based on a pre-defined rules policy. EEM has event detectors with which Call Home registers; the registration is dependent upon which alert-groups the EEM profile is configured. The profile can subscribe to alert-groups for the following type events:
    - GOLD diagnostic
    - Environmental
    - Configuration

  - Inventory
- **Generic Online Diagnostics (GOLD)** – Provides a common command-line interface (CLI) for manually generating Smart Call Home messages and scheduling run-time diagnostics.

  GOLD can detect faults in hardware and provides the triggers that proactively engage high-availability features and actions, such as the switch-hitter of modules or turning off modules or individual ports. The GOLD test suite also gives support personnel the tools to test the functioning of hardware modules and troubleshoot down to the field-replaceable unit (FRU) level.
- **Smart Call Home service**– Is a service that captures and processes Call Home diagnostics and inventory alarms that are sent from a device containing the Smart Call Home feature. This service provides proactive messaging that resolves issues before they become problems and for those problems that occur, resolving them faster using enhanced diagnostics
- **Smart Call Home Client** – A device that sends or forwards IOS Call Home or other supported messages to Smart Call Home using SMTP or HTTPS connections; the messages must be registered with the Smart Call Home system.
- **Smart Call Home supported messages** – Currently is an AML/XML message, created by a device using the IOS Call Home Feature, that contains Configuration (full), Diagnostics (major & minor), Environmental (major & minor), Inventory (full), Test or System Log information.
- **Transport Gateway (TG)** – Securely transports Call Home messages from the customer hardware to the Smart Call Home service on the Cisco Backend. A Smart Call Home software client that runs on a device under the Windows 2000, Windows 2003, Windows XP, Solaris or Linux operating systems. The Transport Gateway acts as an intermediary device and is capable of forwarding supported messages collected from Smart Call Home Client devices and sends them to the Smart Call Home System using an HTTPS connection.

CA Root Certificate Update Process

Periodically, Cisco updates security credentials to ensure the continued secure communications to the Smart Call Home back-end. This section applies to those who are using the HTTPS method for communicating to the back-end.

When there is a security credential update from Cisco, instructions will be sent via e-mail to SCH-registered user e-mail addresses that are linked to a valid CCO ID. Instructions for updating security credentials are as follows:

- HTTPS Certificate Process for Nexus 7000 Devices uses either the "chained" certificate content from this section of the Smart Call Home User Guide, or use the combined contents of the certificate files in the QuoVadisRootCA2.zip file.

HTTPS Certificate Process for Nexus 7000 Devices

There are two different time frames when you will be using HTTPS certificate content on your Nexus 7000 device, when you are:

- Adding the certificate to a Nexus 7000 device, for the first time; you will perform the steps and use the certificate data identified below in this document.
- When you are updating an expired security certificate on a Nexus 7000 device, you will use the script files and certificate data contained in the QuoVadisRootCA2.zip file.

Adding the Certificate to a Nexus 7000 Device

For Nexus 7000 devices, use the following instructions to install a security root certificates chain:

- Copy the root certificates chain below.
- Configure a trust-point and prepare to enroll the certificate via the terminal using copy and paste when prompted.

```
NX-7000(config)#crypto ca trustpoint cisco
NX-7000(config-trustpoint)#enroll terminal
NX-7000(config-trustpoint)#crypto ca authenticate cisco
Input (cut & paste) the CA certificate (chain) in PEM format.
```

IMPORTANT: PLEASE COPY THE CERTIFICATE CONTENT BELOW USING A PLAIN TEXT EDITOR AND PASTE THE CONTENT AS PLAIN TEXT; THIS REMOVES ANY POSSIBLE FORMATTING SYMBOLS, WHICH ALTER THE CERTIFICATE CONTENT.

Note Your copy of the security certificate should include each and every character, including the certificate markers. Remove any blank lines either after or before the certificate markers.

-----BEGIN CERTIFICATE-----
MIIFtzCCA5+gAwIBAgICBQkwDQYJKoZIhvcNAQEFBQAwRTELMAkGA1UEBhMCQk0x
GTAXBgNVBAoTEFF1b1ZhZGlzIExpbWl0ZWQxGzAZBgNVBAMTElF1b1ZhZGlzIFJv
b3QgQ0EgMjAeFw0wNjExMjQxODI3MDBaFw0zMTExMjQxODIzMzNaMEUxCzAJBgNV
BAYTAkJNMRkwFwYDVQQKExBRdW9WYWRpcyBMaW1pdGVkMRswGQYDVQQDExJRdW9
WYWRpcyBSb290IENBIDIwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQCa
GMpLlA0ALa8DKYrwD4HIrkwZhR0In6spRIXzL4GtMh6QRr+jhiYaHv5+HBg6XJxg
Fyo6dIMzMH1hVBHL7avg5tKifvVrbxi3Cgst/ek+7wrGsxDp3MJGF/hd/aTa/55J
WpzmM+Yklvc/ulsrHHo1wtZn/qtmUIttKGAr79dgw8eTvI02kfN/+NsRE8Scd3bB
rrcCaoF6qUWD4gXmuVbBlDePSHFjIuwXZQeVikvfj8ZaCuWw419eaxGrDPmF60Tp
+ARz8un+XJiM9XOva7R+zdRcAitMOeGylZUtQofX1bOQQ7dsE/He3fbE+Ik/0XX1
ksOR1YqI0JDs3G3eicJlcZaLDQP9nL9bFqyS2+r+eXyt66/3FsvbzSUr5R/7mp/i
Ucw6UwxI5g69ybR2BlLmEROFcmMDBOAENisgGQLodKcftslWZvB1JdxnwQ5hYIiz
PtGo/KPaHbDRsSNU30R2be1B2MGyIrZTHN81Hdyhdyox5C315eXbyOD/5YDXC2Og
/zOhD7osFRXql7PSorW+8oyWHhqPHWykYTe5hnMz15eWniN9gqRMgeKh0bpnX5UH
oycR7hYQe7xFSkyyBNKr79X9DFHOUGoIMfmR2gyPZFwDwzqLID9ujWc9Otb+fVuI
yV77zGHcizN300QyNQliBJIWENieJ0f7OyHj+OsdWwIDAQABo4GwMIGtMA8GA1Ud
EwEB/wQFMAMBAf8wCwYDVR0PBAQDAgEGMB0GA1UdDgQWBBQahGK8SEwzJQTU7tD2
A8QZRtGUazBuBgNVHSMEZzBlgBQahGK8SEwzJQTU7tD2A8QZRtGUa6FJpEcwRTEL
MAkGA1UEBhMCQk0xGTAXBgNVBAoTEFF1b1ZhZGlzIExpbWl0ZWQxGzAZBgNVBAMT
ElF1b1ZhZGlzIFJvb3QgQ0EgMoICBQkwDQYJKoZIhvcNAQEFBQADggIBAD4KFk2f
BluornFdLwUvZ+YTRYPENvbzwCYMDbVHZF34tHLJRqUDGCdViXh9duqWNIAXINzn
g/iN/Ae42l9NLmeyhP3ZRPx3UIHmfLTJDQtyU/h2BwdBR5YM++CCJpNVjP4iH2Bl
fF/nJrP3MpCYUNQ3cVX2kiF495V5+vgtJodmVjB3pjd4M1IQWK4/YY7yarHvGH5K
WWPKjaJW1acvvFYfzznB4vsKqBUsfU16Y8Zsl0Q80m/DShcK+JDSV6IZUaUtl0Ha
B0+pUNqQjZRG4T7wlP0QADj1O+hA4bRuVhogzG9Yje0uRY/W6ZM/57Es3zrWIozc
hLsib9D45MY56QSIPMO661V6bYCZJPVsAfv4l7CUW+v90m/xd2gNNWQjrLhVoQPR
TUIZ3Ph1WVaj+ahJefivDrkRoHy3au000LYmYjgahwz46P0u05B/B5EqHdZ+XIWD
mbA4CD/pXvk1B+TJYm5Xf6dQlfe6yJvmjqIBxdZmv3lh8zwc4bmCXF2gw+nYSL0Z
ohEUGW6yhhtoPkg3Goi3XZZenMfvJ2II4pEZXNLxId26F0KCl3GBUzGpn/Z9Yr9y
4aOTHcyKJloJONDO1w2AFrR4pTqHTI2KpdVGl/IsELm8VCLAAVBpQ570su9t+Oza
8eOx79+Rj1QqCyXBJhnEUhAFZdWCEOrCMc0u
-----END CERTIFICATE-----

On the next line following the certificate content, end the input by entering **END OF INPUT:**

Hit **Enter**, a prompt appears asking "Do you accept this certificate? [yes/no]:"; enter **yes**

Exit configuration mode and save the configuration -

NX-7000(config)#**end**

NX-7000#**copy running-config startup-config**

Downloading a New Certificate for a Nexus 7000 Device

If you need the new certificate files that comprise the CA Root certificate, perform the following steps:

Go to the following URL:

https://software.cisco.com/download/home/282152778/type/283490182/release/4.1.8

On the Download Software window, click the **Download Now** button to download the **QuoVadisRootCA2.zip** file.

Figure 6-1 Downloading a certificate

Unzip the **QuoVadisRootCA2.zip** file to the directory of your choice.

Additional Information

For more information on the SSL certificate, see the information at the following URL:

https://security.googleblog.com/2017/09/chromes-plan-to-distrust-symantec.html

For technical support, **Email:** tac@cisco.com<mailto:tac@cisco.com>

Telephone:

US and Canada:	**+1-877-330-9746**	
Europe:	Austria	0800 006 206
	Belgium	0800 49913
	France	0805 119 745
	Germany	0800 589 1725
	Italy	800 085 681
	Netherlands	0800 0201 276
	Spain	800 600472

US and Canada:	**+1-877-330-9746**	
	Switzerland	0800 840011
	UK	0800 2795112

From the rest of the world, choose the appropriate phone number from http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

Transport Gateway Communication over HTTPs

Devices in order to communicate with TG via HTTPS, SSL certificates need to be installed on devices. In addition to the TG SSL Certificate option there is also a provision for Self-signed certificates.

The Transport Gateway is shipped with Self-signed certificates that works for IOS devices. The below use case explains the process to setup Self-signed SSL certificates to enable HTTPS communication between devices and TG.

Use case

Customer Using Self-signed certificates shipped with TG

TG is shipped with self-signed certificate and configured by default. Customer needs to import the certificate in device following the standard instructions on device. A section (Using HTTPS for device to TG communication) in the TG user guide document entails this information.

Reference: Using HTTPS for device to TG communication

Customer installs own certificate on TG

We shall consider below scenario in this use case:

- Creating and Installing Self-signed certificates with Subject Alternative Name (SAN) (mandatory for IOS-XR devices).

Creating and Installing Self-signed certificates with Subject Alternative Name (mandatory for IOS-XR devices)

Note

- Ensure JDK 1.7 or higher is installed on the system where the below commands are executed.
- If you are trying to install the certificates, using Cisco Smart Software Manager Satellite, contact Cisco Support team for support.

1. Generate the keystore. (Please enter relevant values being asked by java keytool. Replace "1.1.1.1" with the actual IP address of the system where TG is installed). Remember the keystore password/note down.

keytool -genkey -alias tgservernew -keyalg RSA -sigalg SHA256withRSA -keysize 2048 -keystore tgservernew.jks -ext SAN= ip:1.1.1.1 -validity 3650

2. Export the certificate (tgservernew.cer) and install it onto the device.

keytool -keystore tgservernew.jks -exportcert -alias tgservernew -rfc -file tgservernew.pem

This will generate the java keystore (*tgservernew.jks*) and the certificate *(tgservernew.pem*) file.

Follow the below steps to add the keystore to TG and install the certificate onto the device:

Step:1 Copy the *tgservernew.jks* file to *<TG_INSTALL_DIR>/CSCOSchtg/tg/resources/security*

Step:2 Open the file *<TG_INSTALL_DIR>/CSCOSchtg/tg/conf/properties/jettyconfig.properties*

Step:3 Edit the below line so that it becomes like below

jettyconfig.pki.certclient.keystore_file= tgservernew.jks
jettyconfig.pki.certclient.keystore_pass=<key store password>
jettyconfig.sslCertificateExists=false

Step:4 Restart TG

Step:5 Open the certificate file "*tgservernew.pem*" using a text editor and follow the commands given in step 3 in below user guide in order to install it onto the device.

Reference: Using HTTPS for device to TG communication

Email Notifications and Category

The type of emails which fall into the new Admin and Fault categories customers can now configure different recipients for notifications.

Administrative Emails [Notifications]	Fault Notification Emails
Contract expiration	Inventory or config upload confirmation
Contract update	Syslog error
Data upload confirmation	Diagnostic failure
Device Unregistered	Environmental warning
Message processing failure	Software crash
New user registration	Call Home Analysis results
Registration confirmation	Message processing failure
Registration confirmation required	Partner support request
Registration deletion	SR creation failure
Registration failure	SR creation success
Registration success	Update to existing SR
Serial number update	
Test Message	
Trial period expiration	
User Management	

Note The above list represents the most common types of email notifications and the category to which they belong. It is not an exhaustive list of all SCH notifications.