Smart Call Home Guide

Cisco Services

Smart Call Home Feature Guide

CISCO

Contents

Smart Call Home Feature Guide

| Introduction | Plan | Install/Deploy | Configure | Maintain/Upgrade | Monitor | Troubleshoot | Resources | Contents |

Smart Call Home Feature Guide

Smart Call Home Feature Guide

Introduction

About Smart Call Home

Smart Call Home is an automated support capability that combines with the Call Home IOS feature to provide a mechanism to generate, transport, store, process and analyze device system messages and information. To the user, it is a Web-based application and notification system that provides diagnostic and reporting capabilities for better network and device management. The Smart Call Home system provides proactive messaging by capturing and processing Call Home diagnostics and flags issues and initiates notifications, corrective action recommendations and resolution before business operations are affected.

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 PSIRT (Product Security Incident Response Team), Field Notices and End of Life notifications

Smart Call Home Interaction with Call Home

Call Home is a product feature embedded in the operating system of Cisco devices that allows the end user to monitor the state of the Cisco router or switch device. The Call Home feature detects and notifies the user of a variety of fault conditions. Smart Call Home facilitates faster resolution of system problems by analyzing Call Home messages sent from your devices and providing background information and recommendations.

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. A device can send Call Home messages to Smart Call Home using one of the following transport methods:

- HTTPS from the client device to the back-end

- E-mail direct from device to Cisco back-end via a local mail server

- HTTP(S) via the transport gateway to Cisco

  - HTTP from device to the transport gateway

  - E-mail from device to the transport gateway

Smart Call Home Feature Guide

ıllııllıı
CISCO

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

Key Benefits

Smart Call Home offers fast, web-based access to required information and 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

- 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

Audience

This user guide is for networking professionals and experienced network administrators who are responsible for configuring Smart Call Home feature on Cisco Devices and who are managing Smart Call Home web application.

Scope

To use the Smart Call Home capabilities, your device must be covered by a valid Cisco service contract, such as Cisco SMARTnet® or Smart Net Total Care.

To successfully register a device for Smart Call Home, a user must have:

- A valid Cisco service contract that covers the device and entitles the user to submit service requests to the Cisco Technical Assistance Center

- A valid Cisco.com User ID, which includes the service contract that covers a device

Note

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 Feature Guide

Planning for Deployment

Existing and Supported Topology
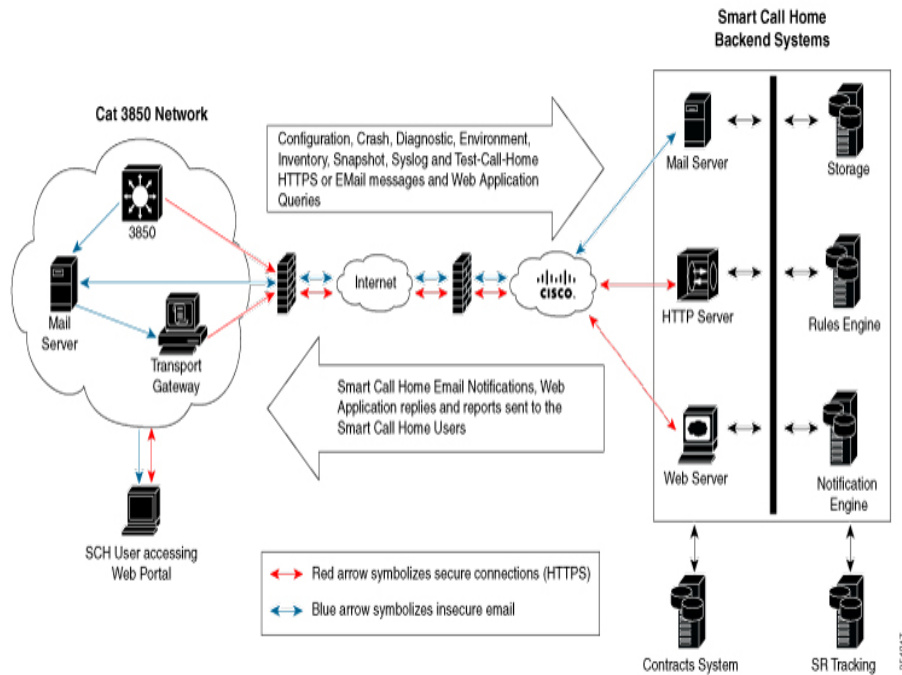
Figure 1Network Topology for Smart Call Home Deployment – Wired
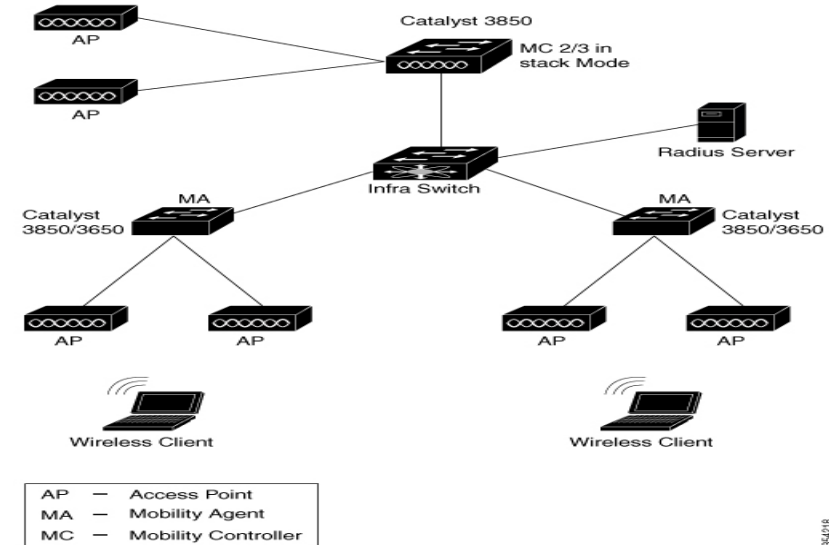
Figure 2 Network Topology for Smart Call Home Deployment - Wireless

System Overview

The operation of Smart Call Home System may be divided into four main areas:

Smart Call Home Feature Guide
PLAN

- The client devices using the IOS Call Home feature to collect and package local information for transmission using one of the Communications options to the back-end systems.

- The Communication options used to transmit the data between the client devices and back-end system, and between the Web Application/notification system and the user systems.

- The Smart Call Home back-end systems that process and store information collected on client devices.

- User systems receiving notifications from the back-end notification system and using the Web Application to access the information stored in the back-end.
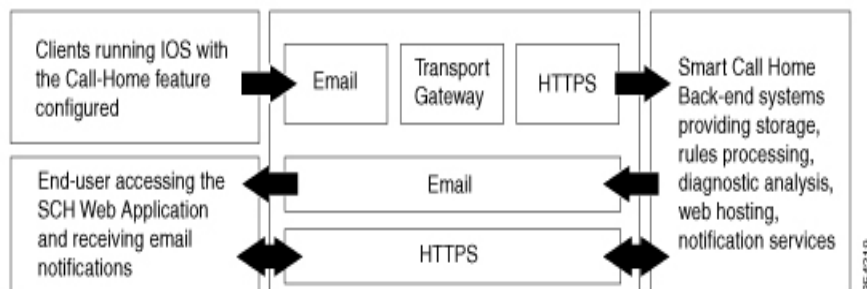
Figure 3 System Overview of Smart Call Home

Prerequisites

System Requirements
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 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. If the correct contracts are not associated to your Cisco.com ID, contact the Smart Services Bureau to correct the discrepancy.

Smart Call Home Feature Guide

Other System Requirements

If the selected transport method is e-mail or HTTP via Transport Gateway, transport gateway software must be downloaded and installed to enable the Call Home environment to securely send messages to Smart Call Home via the Transport Gateway. You can use a TG aggregation point in cases requiring support for multiple devices or in cases where security requirements mandate that your devices may not be connected directly to the Internet.

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.

- To use the e-mail message transport, you must configure at least one Simple Mail Transfer Protocol (SMTP) e-mail server address.

- To use the HTTP option for message transport, you must configure at least one HTTP server.

- To use the secure HTTP (HTTPS) message transport, you must configure a trustpoint certificate authority (CA).

Tip

From the Smart Call Home web application, you can download a basic configuration script to assist you in the configuration of the Call Home feature for use with Smart Call Home and the Cisco TAC. The script will also assist in configuring the trustpoint CA for secure communications with the Smart Call Home service. The script,

provided on an as-is basis, can be downloaded from this URL: http://supportforums.cisco.com/community/netpro/solutions/smart_servi ces/smartcallhome

Guidelines and Limitations

- For Call Home operation to take place, it has to be enabled using the *service call-home* IOS configuration command.

- At least one Call Home Profile (default or user defined) must be active. If the preferred transport method in any profile is email, then at least one email server address must be configured. Call Home will not send any message until the contact person's email address is configured. If the preferred transport method in any profile is HTTPS, a trustpoint certificate authority (CA) must be configured on the Call Home device.

- Only one HTTP address or one email address may be used to send messages to the Smart Call Home System. Therefore, if both transport methods are enabled, only one should be used to send messages to the Smart Call Home System. Since destination addresses cannot be configured in the CiscoTAC-1 default profile, only one transport method can be enabled.

- Call Home may be configured with optional administrative information. The contact person's phone number, a street address, a site ID, a customer ID, and a contract ID are all optional. This information is included in the XML header of the Call-Home message but is not required by the Smart Call Home System. The message sender's email

address and the sender's reply-to email address may be configured. If the message sender's reply-to email address is not configured, Call Home will use the contact's email address as the sender's reply-to email address in all Call Home messages.

- Call Home may be configured to send messages to backup email servers if the email transport method in any profile is enabled. The name or address of each email server and a priority must be configured. The priority number is used to determine which server will be used as the active server initially and during failures. The priority numbers range from the highest priority of 1 to the lowest priority of 100. The server with the highest priority that the device is able to establish a connection with will become the active email server.

- A Call Home configuration script may be downloaded from the software center to automate the Call Home configuration and configuring the trustpoint certificate authority (CA) for secure communications with the Smart Call Home service. This script will be updated periodically with a newer copy of the CA certificate and may be downloaded and installed prior to expiration of the certificate that is in use by the device.

Checklist

Before starting to configure and register your devices to use Smart Call Home, there are some preliminary steps you must take to make sure the configuration and registration process moves forward without issue:

1. Validate that the Smart Call Home feature is available for your device(s) and that they have the appropriate OS installed by checking the list of supported products.

If the supported device does not have the appropriate OS installed, visit Cisco online support and follow the steps required to install the OS on the device(s).

2. Ensure the device is covered by an active and valid service contract.

3. Ensure the person who will register Smart Call Home devices has a Cisco.com account and is logged in. If not, register for a Cisco.com account.

4. Validate that the contract covering the device is associated with your Cisco.com account:

Step 1. Log into Cisco.com and click the Account link at the top of the page.

Step 2. Click **Profile Manager**.

Step 3. Click the **Access** tab.

Step 4. Contracts associated with your profile will appear. If needed, associate the contract to your profile.

a. Click **Add Access**.

b. Select **Full Support** and click **Go**.

c. Select **Contract Numbers** and enter the contract number in the field

`

Smart Call Home Feature Guide

provided.

d. Click **Submit**.

Once you click Submit, if all criteria are met, the contract association will be processed immediately. If any critical criterion fail, the failure reason and support direction are provided.

5. Ensure that serial number of the device is covered by the contract.

If the serial number is not covered under a contract, but you believe that it should be, contact the Smart Services Bureau to correct the discrepancy. Once the serial number is associated correctly, continue with the Smart Call Home registration.

`

Smart Call Home Feature Guide
INSTALL/DEPLOY

| Introduction | Plan | Install/Deploy | Configure | Maintain/Upgrade | Monitor | Troubleshoot | Resources | Contents |

Installing /Deploying

Deployment

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, see Transport Gateway Registration.

Note

You must also configure its CA as a trustpoint if the Smart Call Home service uses HTTPS as the transport method

4. Configure your device.

5. Send an initial inventory message to start the registration process.

6. 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.

7. Monitor the contact email address for email from call-home-notify@cisco.com to confirm that registration is complete.

Testing the Deployment

Deployment of Smart Call Home must be tested between the client devices and Smart Call Home back-end systems to ensure connectivity to Cisco.

For testing Call Home communications, see Chapter 4 - Configuration, section Testing Call Home Communications.

`

Smart Call Home Feature Guide
CONFIGURE

CISCO

Configuring

This chapter describes how to configure the Call Home feature and Smart Call Home feature on your Switch.

This chapter includes the following sections:

Call Home Alert Groups

Call Home Alert Groups allow the system to group detectable events of a specific category for monitoring without having to specify each individual event. Each Alert Group has a fixed set of CLI commands that are invoked when an event in the Alert Group occurs. The purpose of the CLI commands is to obtain more information about the system and event at the time of the event. The output from each CLI commands is included in the Call Home message that is sent. Different types of Call Home alerts are grouped into different alert groups depending on their type. These alert groups are available:

- Configuration
- Crash
- Diagnostic
- Environment
- Inventory
- Snapshot
- Syslog
- Test

An Alert Group may be completely disabled within the Call Home subsystem. When an Alert Group is disabled, a Call Home message will not be sent for an event in that Alert Group. But if the Syslog Alert Group is enabled and the event in the disabled Alert Group generates a Syslog message, then a Syslog Call Home message may be sent. The triggering events for each alert group are listed in the Alert Group Trigger Events and Commands section.

Call Home Profiles

The Call Home Profile provides a structure to bundle together several Alert Groups, to select transport methods, to assign multiple destination addresses and to specify message format options. A destination profile contains the required delivery information for an alert notification. At least one destination profile is required. Call Home provides a default destination profile that is pre-configured for use with the Smart Call Home System. The default profile is called CiscoTAC-1. You can configure multiple destination profiles of one or more types. You can use the predefined destination profile or define a desired profile. If you define a new destination profile, you must assign a profile name. A profile may be configured but its status may be inactive.

Only one HTTP address or one email address may be used to send messages to the Smart Call Home System. Therefore, if both transport methods are enabled, only one should be used to send messages to the Smart Call Home System. The CiscoTAC-1 default profile includes the Smart Call Home email and HTTP addresses. Since the destination addresses cannot be configured in the CiscoTAC-1 default profile, only

Introduction	Plan	Install/Deploy	Configure	Maintain/Upgrade	Monitor	Troubleshoot	Resources	Contents

one transport method can be enabled. The default profile is defined to send periodic configuration and inventory messages.

Call Home Message Formats
The Call Home feature offers the following message formats:

- Short Text — Suitable for pagers or printed reports.

- Plain Text — Full formatted message information suitable for human reading.

- XML — Matching readable format using Extensible Markup Language (XML) and Adaptive Markup Language (AML) document type definitions (DTDs). The XML format enables communication with the Cisco TAC.

For user-defined destination profiles, the format options are long-text, short-text, or XML. The default is XML. For the predefined Cisco TAC profile, only XML is allowed.

Configuring Call Home
Consider the following information before you configure Call Home:

- The contact e-mail, phone, and street address information should be configured so that the receiver can determine the origin of messages received.

- The switch must have IP connectivity to an e-mail server or the destination HTTP server using the *ip domain name* command.

- If email message delivery transport method is selected, the name or IPv4/IPv6 address of a primary Simple Mail Transfer Protocol (SMTP) server and any backup servers must be configured.

- If secure HTTP (HTTPS) message delivery is selected, a trustpoint certificate authority (CA) must be configured.

Note
A buit-in certificate is ported in the device trustpool. So, in most cases, the user does not need to import the certificate.

- If Cisco Smart Call Home is used, an active service contract must cover the device being configured.

Task Flow for Configuring Call Home
To configure Call Home, follow these steps:

1. Configure your site's contact information. See the Configuring Contact Information section.

2. Configure destination profiles for each of your intended recipients. See the Configuring Destination Profiles section.

3. Subscribe each destination profile to one or more alert groups, and set alert options. See the Subscribing to Alert Groups section.

4. Configure e-mail settings or HTTPS settings (including CA certificate), depending on the transport method. See the Configuring General E-Mail Options section.

5. Enable the Call Home feature. See the Enabling Call Home section.

6. Test Call Home messages. See the Testing Call Home Communications section.

Configuring Contact Information

Each switch must include a contact e-mail address. You can optionally include a phone number, street address, contract ID, customer ID, and site ID.

To assign the contact information, perform this task:

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters configuration mode.
Step 2	`Switch(config)# call-home`	Enters the Call Home configuration submode.
Step 3	`Switch(cfg-call-home)# contact-email-addr email-address`	Assigns the customer's e-mail address. Enter up to 200 characters in e-mail address format with no spaces.
Step 4	`Switch(cfg-call-home)# phone-number +phone-number`	(Optional) Assigns the customer's phone number. **Note** The number must begin with a plus (**+**) prefix, and may contain only dashes (-) and numbers. Enter up to 16 characters. If you include spaces, you must enclose your entry in quotes ("")
Step 5	`Switch(cfg-call-home)# street-address street-address`	(Optional) Assigns the customer's street address where RMA equipment can be shipped. Enter up to 200 characters. If you include spaces, you must enclose your entry in quotes ("").
Step 6	`Switch(cfg-call-home)# customer-id text`	(Optional) Identifies the customer ID. Enter up to 64 characters. If you include spaces, you must enclose your entry in quotes ("").
Step 7	`Switch(cfg-call-home)# site-id text`	(Optional) Identifies the customer site ID. Enter up to 200 characters. If you include spaces, you must enclose your entry in quotes ("").
Step 8	`Switch(cfg-call-home)# contract-id text`	(Optional) Identifies the customer's contract ID for the switch. Enter up to 64 characters. If you include spaces, you must enclose your entry in quotes ("").

Configuring Destination Profiles

You can configure the following attributes for a destination profile:

- Profile name— A string that uniquely identifies each user-defined destination profile. The profile name is limited to 31 characters and is not case-sensitive. You cannot use "all" as a profile name.

Smart Call Home Feature Guide

CONFIGURE

ıllıllıı
CISCO™

- Transport method — The transport mechanism, either e-mail or HTTP (including HTTPS), for delivery of alerts.

  - For user-defined destination profiles, e-mail is the default, and you can enable either or both transport mechanisms. If you disable both methods, e-mail will be enabled.

  - For the predefined Cisco TAC profile, you can enable either transport mechanism, but not both.

- Destination address — The actual address related to the transport method to which the alert should be sent.

- Message formatting — The message format used for sending the alert.

  - For user-defined destination profiles, the format options are long text, short-text, or XML. The default is XML.

  - For the predefined Cisco TAC profile, only XML is allowed.

Note

If you use the Cisco Smart Call Home service, the destination profile must use the XML message format.

- Message size — The maximum destination message size. The valid range is 50 to 3,145,728 bytes and the default is 3,145,728 bytes.

To create and configure a destination profile, perform this task:

	Command	Purpose
Step 1	`Switch# ` **`configure terminal`**	Enters configuration mode.

	Command	Purpose
Step 2	`Switch(config)# ` **`call-home`**	Enters the Call Home configuration submode.
Step 3	`Switch(cfg-call-home)# ` **`profile`** `name`	Enters the Call Home destination profile configuration submode for the specified destination profile. If the specified destination profile does not exist, it is created.
Step 4	`Switch(cfg-call-home-profile)# ` **`[no]`** **`destination transport-method`** `{`**`email`** `|` **`http`**`}`	(Optional) Enables the message transport method. The **no** option disables the method.
Step 5	`Switch(cfg-call-home-profile)# ` **`destination address`** `{`**`email`** `email-address |` **`http`** `url}`	Configures the destination e-mail address or URL to which Call Home messages will be sent. **Note** When entering a destination URL, include either **http**:// or **https**://, depending on whether the server is a secure server. If the destination is a secure server, you must also configure a trustpoint CA.

Step 6	`Switch(cfg-call-home-profile)#` **`destination preferred-msg-format`** `{`**`long-text`** `|` **`short-text`** `|` **`xml`**`}`	(Optional) Configures a preferred message format. The default is XML.
Step 7	`Switch(cfg-call-home-profile)#` **`destination message-size-limit`** `bytes`	(Optional) Configures a maximum destination message size for the destination profile.
Step 8	`Switch(cfg-call-home-profile)#` **`active`**	Enables the destination profile. By default, the profile is enabled when it is created.
Step 9	`Switch(cfg-call-home-profile)#` **`exit`**	Exits the Call Home destination profile configuration submode and returns to the Call Home configuration submode.
Step 10	`Switch(cfg-call-home)#` **`end`**	Returns to privileged EXEC mode.
Step 11	`Switch#` **`show call-home profile`** `{`*name* `|` **`all`**`}`	Displays the destination profile configuration for a specified profile or all configured profiles.

Copying a Destination Profile
To create a new destination profile by copying an existing profile,

perform this task:

	Command	Purpose
Step 1	`Switch#` **`configure terminal`**	Enters configuration mode.
Step 2	`Switch(config)#` **`call-home`**	Enters the Call Home configuration submode.
Step 3	`Switch(cfg-call-home)#` **`copy profile`** *source-profile target-profile*	Creates a new destination profile with the same configuration settings as the existing destination profile.

Subscribing to Alert Groups
You can select one or more alert groups to be received by a destination profile.

To subscribe a destination profile to an alert group, perform this task:

	Command	Purpose
Step 1	`Switch#` **`configure terminal`**	Enters configuration mode.
Step 2	`Switch(config)#` **`call-home`**	Enters Call Home configuration submode.
Step 3	`Switch(cfg-call-home)#` **`alert-group`** `{`**`all`**`|`**`configuration`**`|`**`crash`**`|`**`diagnostic`**`|` **`environment`**`|`**`inventory`**`|`**`snapshot`**`|`**`syslog`**`}`	Enables the specified alert group. Use the keyword **all** to enable all alert groups. By default, all alert groups are enabled.

`

Smart Call Home Feature Guide

CONFIGURE

Step 4	`Switch(cfg-call-home)#` **profile** *name*	Enters the Call Home destination profile configuration submode for the specified destination profile.	**Step 8**	`Switch(cfg-call-home-profile)#` **subscribe-to-alert-group diagnostic** [**severity catastrophic|disaster|fatal|critical|major|minor|warning|notification|normal|debugging**]	Subscribes this destination profile to the Diagnostic alert group. The Diagnostic alert group can be configured to filter messages based on severity, as described in the Configuring Message Severity Threshold.
Step 5	`Switch(cfg-call-home-profile)#` **subscribe-to-alert-group all**	Subscribes to all available alert groups.			
Step 6	`Switch(cfg-call-home-profile)#` **subscribe-to-alert-group configuration** [**periodic** {**daily** *hh:mm* | **monthly** *date hh:mm* | **weekly** *day hh:mm*}]	Subscribes this destination profile to the Configuration alert group. The Configuration alert group can be configured for periodic notification, as described in the Configuring Periodic Notification.	**Step 9**	`Switch(cfg-call-home-profile)#` **subscribe-to-alert-group environment** [**severity catastrophic|disaster|fatal|critical|major|minor|warning|notification|normal|debugging**]	Subscribes this destination profile to the Environment alert group. The Environment alert group can be configured to filter messages based on severity, as described in the Configuring Message Severity Threshold section.
Step 7	`Switch(cfg-call-home-profile)#` **subscribe-to-alert-group crash**	Subscribes this destination profile to the Crash alert group.			

Step 10	`Switch(cfg-call-home-profile)# ` **`subscribe-to-alert-group inventory`** `[`**`periodic`** `{`**`daily`** `hh:mm |` **`monthly`** `date hh:mm |` **`weekly`** `day hh:mm}]`	Subscribes this destination profile to the Inventory alert group. The Inventory alert group can be configured for periodic notification, as described in the Configuring Periodic Notification section.
Step 11	`Switch(cfg-call-home-profile)# ` **`subscribe-to-alert-group snapshot`** `{`**`periodic`** `{`**`daily`** `hh:mm |` **`hourly`** `mm |` **`interval`** `minutes |` **`monthly`** `date hh:mm |` **`weekly`** `day hh:mm}}`	Subscribes this destination profile to the Snapshot alert group. The Inventory alert group can be configured for periodic notification, as described in the Configuring Periodic Notification section.
Step 12	`Switch(cfg-call-home-profile)# ` **`subscribe-to-alert-group syslog`** `[`**`severity catastrophic|disaster|fatal|critical|major|minor|warning|notification|normal|debugging`**`] [`**`pattern`** `string]`	Subscribes this destination profile to the Syslog alert group. The Syslog alert group can be configured to filter messages based on severity, as described in the Configuring Message Severity Threshold section. You can specify a pattern to be matched in the syslog message. If the pattern contains spaces, you must enclose it in quotes ("").
Step 13	`Switch(cfg-call-home-profile)# ` **`exit`**	Exits the Call Home destination profile configuration submode.

Configuring Periodic Notification

When you subscribe a destination profile to the Configuration, Inventory and Snapshot alert group, you can choose to receive the alert group messages asynchronously or periodically at a specified time. The sending period can be one of the following:

- Daily—Specify the time of day to send, using an hour:minute format hh:mm, with a 24-hour clock (for example, 14:30).

- Hourly—Specify the minute of the hour, from, 0 to 59.

- Interval—Specify the interval of minutes, from 1 to 60.

- Weekly—Specify the day of the week and time of day in the format day hh:mm, where the day of the week is spelled out (for example, monday).

- Monthly—Specify the numeric date, from 1 to 31, and the time of day, in the format date hh:mm.

Configuring Message Severity Threshold

When you subscribe a destination profile to the Diagnostic, Environment, or Syslog alert group, you can set a threshold for sending alert group messages based on the message's level of severity. Any message with a value lower than the threshold is not sent to the destination.

The severity threshold is configured using the keywords in Table 1, and ranges from catastrophic (level 9, highest level of urgency) to debugging (level 0, lowest level of urgency). If no severity threshold is

configured, the default is normal (level 1).

Table 1 Severity and Syslog Level Mapping

Level	Keyword	Syslog Level	Description
9	`catastrophic`	N/A	Network-wide catastrophic failure
8	`disaster`	N/A	Significant network impact
7	`fatal`	Emergency (0)	System unusable
6	`critical`	Alert (1)	Critical conditions, immediate attention needed
5	`major`	Critical (2)	Major conditions
4	`minor`	Error (3)	Minor conditions
3	`warning`	Warning (4)	Warning conditions
2	`notification`	Notice (5)	Basic notification and informational messages; possibly independently insignificant
1	`normal`	Information (6)	Normal event signifying return to normal state
0	`debugging`	Debug (7)	Debugging messages

Configuring Syslog Pattern Matching

When you subscribe a destination profile to the Syslog alert group, you can optionally specify a text pattern to be matched within each syslog message. If you configure a pattern, a Syslog alert group message will be sent only if it contains the specified pattern and meets the severity threshold. If the pattern contains spaces, you must enclose it in quotes ("") when configuring it. You can specify up to five patterns for each destination profile.

Note

For Catalyst 3850 WLC, Syslog pattern is predefined as in the CiscoTAC-1 destination profile.

Configuring General E-Mail Options

To use the e-mail message transport, you must configure at least one Simple Mail Transfer Protocol (SMTP) e-mail server address. You can configure the from and reply-to e-mail addresses. You can also set a rate limit on e-mail or HTTP messages.

You can also configure the vrf and source interface or source IP address to send the e-mail messages. If you want to configure similar options to send http messages, you must enter the **ip http client source-interface** *interface-name* command where the source-interface can be associated with the vrf you want to set.

To configure general e-mail options, perform this task:

Smart Call Home Feature Guide
CONFIGURE

	Command	Purpose
Step 1	Switch# **configure terminal**	Enters configuration mode.
Step 2	Switch(config)# **call-home**	Enters Call Home configuration submode.
Step 3	Switch(cfg-call-home)# **mail-server** {*ipv4-address* | *ipv6-address* | *name*} **priority** *number*	Assigns an e-mail server address and its relative priority among configured e-mail servers. Provide either of these: • The e-mail server's IP address • The e-mail server's fully qualified domain *name* (FQDN) of 64 characters or less. Assign a priority *number* between 1 (highest priority) and 100 (lowest priority).
Step 4	Switch(cfg-call-home)# **sender from** *email-address*	(Optional) Assigns the e-mail address that will appear in the from field in Call Home e-mail messages. If no address is specified, the contact e-mail address is used.
Step 5	Switch(cfg-call-home)# **sender reply-to** *email-address*	(Optional) Assigns the e-mail address that will appear in the reply-to field in Call Home e-mail messages.
Step 6	Switch(cfg-call-home)# **rate-limit** *number*	(Optional) Specifies a limit on the number of messages sent per minute, from 1 to 60.
Step 7	Switch(cfg-call-home)# **vrf** *vrf-name*	(Optional) Specifies the source interface name to send Call Home e-mail messages. If no source interface name or source ip address is specified, an interface in the routing table is used.
Step 8	Switch(cfg-call-home)# **source-interface** *interface-name*	(Optional) Specifies the source IP address to send Call Home e-mail messages. If no source IP address or source interface name is specified, an interface in the routing table is used. **Note** At one time, you can specify the source-interface name or the source-ip-address, but not both.

`

Smart Call Home Feature Guide
CONFIGURE

Step 9	`Switch(cfg-call-home)# ` **`source-ip-address`** `ip-address`	(Optional) Specifies the source IP address to send Call Home e-mail messages. If no source IP address or source interface name is specified, an interface in the routing table is used. **Note** At one time, you can specify the source-interface name or the source-ip-address, but not both.

`

Smart Call Home Feature Guide
CONFIGURE

The following notes apply when configuring general e-mail options:

- Backup e-mail servers can be defined by repeating the **mail-server** command using different priority numbers.

- The **mail-server priority** number parameter can be configured from 1 to 100. The server with the highest priority (lowest priority number) will be tried first.

Enabling Call Home
To enable or disable the Call Home feature, perform this task:

	Command	Purpose
Step 1	`Switch#` **`configure terminal`**	Enters configuration mode.
Step 2	`Switch(config)#` **`service call-home`**	Enables the Call Home feature.

Testing Call Home Communications
You can test Call Home communications by sending messages manually using two command types.

- To send a user-defined Call Home test message, use the call-home test command.

- To send a specific alert group message, use the call-home send command.

Sending a Call Home Test Message Manually

To manually send a Call Home test message, perform this task:

	Command	Purpose
Step 1	`Switch#` **`call-home test`** `[`**`"`**`test-message`**`"`**`]` **`profile`** `name`	Sends a test message to the specified destination profile. The user-defined test message text is optional, but must be enclosed in quotes ("") if it contains spaces. If no user-defined message is configured, a default message will be sent.

This example shows how to manually send a Call Home test message:

```
Switch# call-home test "test of the day" profile CiscoTAC-1
```

Sending a Call Home Alert Group Message Manually

To manually trigger a Call Home alert group message, perform this task:

Smart Call Home Feature Guide
CONFIGURE

Introduction	Plan	Install/Deploy	Configure	Maintain/Upgrade	Monitor	Troubleshoot	Resources	Contents

	Command	Purpose
Step 1	Switch# **call-home send alert-group configuration** [**profile** *name*]	Sends a configuration alert group message to one destination profile if specified, or to all subscribed destination profiles.
Step 2	Switch# **call-home send alert-group crash** [**profile** *name*]	Sends a crash alert group message to one destination profile if specified, or to all subscribed destination profiles.
Step 3	Switch# **call-home send alert-group diagnostic** {**switch 1** [**profile** *name*]}	Sends a diagnostic alert group message to the configured destination profile if specified, or to all subscribed destination profiles. You must specify the switch number whose diagnostic information should be sent. **Note** **1** indicates the switch number.
Step 4	Switch# **call-home send alert-group inventory** [**profile** *name*]	Sends an inventory alert group message to one destination profile if specified, or to all subscribed destination profiles.
Step 5	Switch# **call-home send alert-group snapshot** [**profile** *name*]	Sends a snapshot alert group message to one destination profile if specified, or to all subscribed destination profiles.

When manually sending Call Home alert group messages, note the following guidelines:

- You can only manually send the configuration, crash, diagnostic, inventory and snapshot alert groups.

- When you manually trigger a configuration, crash, diagnostic, inventory, or snapshot alert group message and you specify a destination profile name, a message is sent to the destination profile regardless of the profile's active status, subscription status, or severity setting.

- When you manually trigger a configuration, inventory, or snapshot alert group message and do not specify a destination profile name, a message is sent to all active profiles that have either a normal or periodic subscription to the specified alert group.

- When you manually trigger a diagnostic alert group message and do not specify a destination profile name, the command will cause the following actions:

  - For any active profile that subscribes to diagnostic events with a severity level of less than minor, a message is sent

regardless of whether the module or interface has observed a diagnostic event.

– For any active profile that subscribes to diagnostic events with a severity level of minor or higher, a message is sent only if the specified switch has observed a diagnostic event of at least the subscribed severity level; otherwise, no diagnostic message is sent to the destination profile.

This example shows how to send the configuration alert-group message to all the destination profiles:

```
Switch#  call-home send alert-group configuration
```

This example shows how to send the crash call-home message:

```
Switch#  call-home send alert-group crash
```

This example shows how to send the diagnostic alert-group message to the destination profile for a specific switch.

```
Switch#  call-home send alert-group diagnostic switch 1 profile CiscoTAC-1
```

This example shows how to send the diagnostic alert-group message to all destination profiles for a specific switch.

```
Switch#  call-home send alert-group diagnostic switch 1
```

This example shows how to send the inventory call-home message:

– `Switch#  call-home send alert-group inventory`

Sending a Request for an Analysis and Report

You can use the **call-home request** command 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.

To submit a request for report and analysis information from the Cisco Output Interpreter tool, perform one of these tasks:

	Command	Purpose
Step 1	`Switch# `**`call-home request output-analysis`**` "`*show-command*`" [`**`profile`** *name*`] [`**`ccoid`** *user-id*`]`	Sends the output of the specified **show** command for analysis. The **show** command must be contained in quotes ("" ").
Step 2	`Switch# `**`call-home request {config-sanity	bugs-list	command-reference	product-advisory	registration-info} [profile`** *name*`] [`**`ccoid`** *user-id*`]`	Sends the output of a predetermined set of commands for analysis such as **show running-config all**, **show version**, or **show module** commands. In addition, the **call-home request product-advisory** command includes all inventory alert group commands.

`

Smart Call Home Feature Guide
CONFIGURE

Cisco

| Introduction | Plan | Install/Deploy | Configure | Maintain/Upgrade | Monitor | Troubleshoot | Resources | Contents |

When manually sending a Call Home report and analysis request, note the following guidelines:

- If you specify a **profile** *name* value, the request is sent to the profile. If you do not specify a profile name, the request is sent to the Cisco TAC profile. The recipient profile does not need to be enabled for the Call Home request. The profile should specify the e-mail address where the transport gateway is configured so that the request message can be forwarded to the Cisco TAC and you can receive the reply from the Smart Call Home service.

- The **ccoid** *user-id* value is the registered identifier of the Smart Call Home user. If you specify a user-id, the response is sent to the e-mail address of the registered user. If do not specify a user-id, the response is sent to the contact e-mail address of the device.

- Based on the keyword specifying the type of report requested, the following information is returned:

    - **config-sanity**—Information on best practices as related to the current running configuration

    - **bugs-list**—Known bugs in the running version and in the currently applied features

    - **command-reference**—Reference links to all commands in the running configuration

    - **product-advisory**—Product Security Incident Response Team (PSIRT) notices, End of Life (EOL) or End of Sales

(EOS) notices, or field notices (FN) that may affect devices in your network

    - **registration-info**—Registration information about the device

This example shows a request for analysis of a user-specified **show** command:

```
Switch# call-home request output-analysis "show diagnostic result switch all" profile TG
```

Sending the Output of a Command

You can use the **call-home send** command to execute a CLI command and e-mail the command output to Cisco or to an e-mail address that you specify. To execute a CLI command and e-mail the command output, perform this task:

	Command	Purpose
Step 1	Switch# **call-home send** **"***command***"** [**email** *email-addr*] [**http** *url*] [**tac-service-request** *SR*]	Executes the specified CLI command and e-mails the output.

When sending the output of a command, note the following guidelines:

- The specified CLI command can be any run command, including commands for all modules. The command must be contained in quotes ("").

Smart Call Home Feature Guide | © 2016 Cisco and/or its affiliates. All rights reserved.

- If an e-mail address is specified, the command output will be sent to that address. If no e-mail address is specified, the output will be sent to the Cisco TAC (callhome@cisco.com). The e-mail will be sent in long text format with the service number, if specified, in the subject line.

- The service number is required only if no e-mail address is specified, or if a Cisco TAC e-mail address is specified.

This example shows how to send the output of a CLI command to a user-specified e-mail address:

```
Switch# call-home send "show diagnostic result switch all" email
support@example.com
```

Displaying Call Home Configuration Information
To display the configured Call Home information, perform these tasks:

Command	Purpose
Switch# **show call-home**	Displays the Call Home configuration in summary.
Switch# **show call-home detail**	Displays the Call Home configuration in detail.
Switch# **show call-home alert-group**	Displays the available alert groups and their status.
Switch# **show call-home mail-server status**	Checks and displays the availability of the configured e-mail server(s).

Switch# **show call-home profile** {**all** | *name*}	Displays the configuration of the specified destination profile. Use the keyword **all** to display the configuration of all destination profiles.
Switch# **show call-home statistics**	Displays the statistics of Call Home events.
Switch# **show wireless client statistics**	Displays the protocol statistics of wireless client.
Switch# **show ap dot11** {**24ghz** | **5ghz**} **channel statistics**	Displays the statistics for channel change and causes for the specified frequency band.
Switch# **show ap dot11** {**24ghz** | **5ghz**} **txpower statistics**	Displays the statistics for power change and causes for the specified frequency band.

Alert Group Trigger Events and Commands
Call Home trigger events are grouped into alert groups, with each alert group assigned CLI commands to execute when an event occurs. The CLI command output is included in the transmitted message.

Following table lists the trigger events included in each alert group, including the severity level of each event and the executed CLI commands for the alert group.

Smart Call Home Feature Guide

CONFIGURE

Table 2 Call Home Alert Group Events and Actions

Alert Group	Event Type	Syslog Event	Description	Send to Gold EEM/TAC	CLI Commands Executed
Diagnostic	ONDEMAND	DIAG	DiagGoldPktTest: The GOLD packet Loopback test verifies the MAC level loopback functionality. In this test, a GOLD packet, for which Doppler provides the support in hardware, is sent. The packet loops back at MAC level and is matched against the stored packet. It is a non -disruptive test. DiagThermalTest : This test verifies the temperature reading from the sensor is below the yellow temperature threshold. It is a non-disruptive test and can be run as a health monitoring test.	Yes	show module show diagnostic result switch <num> detail show version show inventory show buffers show logging show diagnostic post show diagnostic result switch all

Smart Call Home Feature Guide
CONFIGURE

| Introduction | Plan | Install/Deploy | Configure | Maintain/Upgrade | Monitor | Troubleshoot | Resources | Contents |

Alert Group	Event Type	Syslog Event	Description	Send to Gold EEM/TAC	CLI Commands Executed
			DiagFanTest : This test verifies all fan modules have been inserted and working properly on the board. It is a non-disruptive test and can be run as a health monitoring test. DiagPhyLoopbackTest : The PHY Loopback test verifies the PHY level loopback functionality. In this test, a packet is sent which loops back at PHY level and is matched against the stored packet. It is a disruptive test and cannot be run as a health monitoring test.		

Smart Call Home Feature Guide

CONFIGURE

Alert Group	Event Type	Syslog Event	Description	Send to Gold EEM/TAC	CLI Commands Executed
			DiagScratchRegisterTest :The Scratch Register test monitors the health of application-specific integrated circuits (ASICs) by writing values into registers and reading back the values from these registers.		
			DiagPoETest : This test checks the PoE controller functionality. This is a disruptive test and should not be performed during normal switch operation.		
			DiagStackCableTest : This test verifies the stack ring loopback functionality in the stacking environment. It is a disruptive test and cannot be run as a health monitoring test.		

Smart Call Home Feature Guide

CONFIGURE

Alert Group	Event Type	Syslog Event	Description	Send to Gold EEM/TAC	CLI Commands Executed
			DiagMemoryTest : This test runs the exhaustive ASIC memory test during normal switch operation. NG3K utilizes mbist for this test. Memory test is very disruptive in nature and requires switch reboot after the test.		

Smart Call Home Feature Guide

CONFIGURE

Alert Group	Event Type	Syslog Event	Description	Send to Gold EEM/TAC	CLI Commands Executed
Inventory	INSERTION/REMOVAL	Switch	A switch has been inserted into a stack.	Yes	**Full:** show module show version show version running show inventory fru show power inline show interfaces show file systems show data-corruption show memory statistics show process memory show process cpu show buffers show crypto tech-support show ip arp show ip nat statistics show ip traffic

`

Smart Call Home Feature Guide
CONFIGURE

Alert Group	Event Type	Syslog Event	Description	Send to Gold EEM/TAC	CLI Commands Executed
Inventory	INSERTION/REMOVAL	PowerSupply(FEP)	A Power Supply has been inserted		Delta: show module show version show inventory fru
Inventory	INSERTION/REMOVAL	FanTray	A Fan has been inserted		

Smart Call Home Feature Guide
CONFIGURE

cisco

| Introduction | Plan | Install/Deploy | Configure | Maintain/Upgrade | Monitor | Troubleshoot | Resources | Contents |

Alert Group	Event Type	Syslog Event	Description	Send to Gold EEM/TAC	CLI Commands Executed
Inventory	INSERTION/REMOVAL	Module	A FRU module like (hamm, frulink) is inserted or removed.		
Inventory	INSERTION/REMOVAL	SFP	Not supported-insertion/removal of sfp.		

Smart Call Home Feature Guide
CONFIGURE

Alert Group	Event Type	Syslog Event	Description	Send to Gold EEM/TAC	CLI Commands Executed
Environmental	TEMP_FAILURE	TempHigh	The temperature of the chassis is above the normal threshold	Yes	show environment all show inventory
	TEMP_FAILURE	CriticalTemp	The temperature of the chassis has risen above the critical threshold		

`

Smart Call Home Feature Guide
CONFIGURE

Alert Group	Event Type	Syslog Event	Description	Send to Gold EEM/TAC	CLI Commands Executed
	TEMP_FAILURE	ShutdownTemp	The temperature of the chassis is very high and the system will be shut down		
	TEMP_RECOVER	TempOk	The temperature of the chassis is normal		

`

Smart Call Home Feature Guide
CONFIGURE

Alert Group	Event Type	Syslog Event	Description	Send to Gold EEM/TAC	CLI Commands Executed
	POWER_FAILURE	PowerSupplyBad	A power supply has failed or has been turned off		
	POWER_RECOVERY	PowerSupplyGood	A failed power supply has been fixed		

`

Smart Call Home Feature Guide

CONFIGURE

ılıılı
CISCO

| Introduction | Plan | Install/Deploy | Configure | Maintain/Upgrade | Monitor | Troubleshoot | Resources | Contents |

Alert Group	Event Type	Syslog Event	Description	Send to Gold EEM/TAC	CLI Commands Executed
	POWER_FAULTY	PowerSupplyFaulty	A Power supply state has been faulty		
	POWER_CRITICAL	PowerSupplyCritical	A Power supply state has been critical		

`

Smart Call Home Feature Guide
CONFIGURE

Alert Group	Event Type	Syslog Event	Description	Send to Gold EEM/TAC	CLI Commands Executed
	POWER_SHUTDOWN	PowerSupplyShutdown	A Power supply state has been shutdown		
	POWER_FAILURE	PowerSupplyFanBad	A power supply fan has failed		

Smart Call Home Feature Guide
CONFIGURE

Introduction	Plan	Install/Deploy	Configure	Maintain/Upgrade	Monitor	Troubleshoot	Resources	Contents

Alert Group	Event Type	Syslog Event	Description	Send to Gold EEM/TAC	CLI Commands Executed
	POWER_RECOVERY	PowerSupplyFanGood	A failed power supply fan has been fixed		
	POWER_RECOVERY	PowerSupplyOutputIncreased	A power supply output has increased		

`

Smart Call Home Feature Guide
CONFIGURE

| Introduction | Plan | Install/Deploy | Configure | Maintain/Upgrade | Monitor | Troubleshoot | Resources | Contents |

Alert Group	Event Type	Syslog Event	Description	Send to Gold EEM/TAC	CLI Commands Executed
	POWER_FAILURE	PowerSupplyOutputDecreased	A power supply output has decreased		
	POWER_FAILURE	InlinePowerSupplyBad	Inline power source from a power supply has failed or turned off.		

`

Smart Call Home Feature Guide
CONFIGURE

ıı|ıı|ı
CISCO

| Introduction | Plan | Install/Deploy | Configure | Maintain/Upgrade | Monitor | Troubleshoot | Resources | Contents |

Alert Group	Event Type	Syslog Event	Description	Send to Gold EEM/TAC	CLI Commands Executed
	POWER_RECOVERY	InlinePowerSupplyGood	A failed source for inline power has been fixed.		
	POWER_FAILURE	MixInPowerDetected	Mixed power supplies are in Chassis		

Smart Call Home Feature Guide
CONFIGURE

Alert Group	Event Type	Syslog Event	Description	Send to Gold EEM/TAC	CLI Commands Executed
	POWER_RECOVERY	MixInPowerNotDetected	Mixed power supply is no longer found in chassis (maybe due to power supply removal)		
	POWER_FAILURE	InsufficientPowerDetected	Not enough power in chassis		

`

Smart Call Home Feature Guide

CONFIGURE

| Introduction | Plan | Install/Deploy | Configure | Maintain/Upgrade | Monitor | Troubleshoot | Resources | Contents |

Alert Group	Event Type	Syslog Event	Description	Send to Gold EEM/TAC	CLI Commands Executed
	POWER_RECOVERY	SufficientPowerDetected	Enough power in chassis		
	POWER_FAILURE	RedundantPowerSupplyFailure	The redundant power supply has failed (there is atleast one power source available)		

`

Smart Call Home Feature Guide
CONFIGURE

Alert Group	Event Type	Syslog Event	Description	Send to Gold EEM/TAC	CLI Commands Executed
	POWER_RECOVERY	RedundantPowerSupplyOk	Redundant power supply is fine ,multiple power supplies available		
	FANTRAY_FAILURE	FanTrayBad	Fan tray has failed		

`

Smart Call Home Feature Guide
CONFIGURE

Alert Group	Event Type	Syslog Event	Description	Send to Gold EEM/TAC	CLI Commands Executed
	FANTRAY_RECOVERY	FanTrayGood	Failed fan tray has been fixed		
	FANTRAY_FAULTY	FanTrayFaulty	Fan tray has been faulty		

`

Smart Call Home Feature Guide
CONFIGURE

infrastructure

Alert Group	Event Type	Syslog Event	Description	Send to Gold EEM/TAC	CLI Commands Executed
	FANTRY_NOTPRESENT	FanTrayNotPresent	Fan tray is not present		
Test			User-generated test message		show module show version show inventory fru

`

Smart Call Home Feature Guide
CONFIGURE

Alert Group	Event Type	Syslog Event	Description	Send to Gold EEM/TAC	CLI Commands Executed
Syslog			Events generated by specific "interesting" syslog messages		show logging show inventory
Configuration			User-generated request for configuration		show module show version show running-config all show startup-config show inventory

Smart Call Home Feature Guide

CONFIGURE

Alert Group	Event Type	Syslog Event	Description	Send to Gold EEM/TAC	CLI Commands Executed
Crash			Crash dump reporting allows crashinfo to be collected and send to cisco backend when a system is reloaded due to reload. Process crash will be reported in all switch members. For module crash triggered by critical process crashing, it is detected as process crash		**System crash:** show version show logging show region show inventory show stacks dir crashinfo | i crashinfo dir crashinfo | i core show platform software trace message hostmanager switch active R0 show bootlog switch active R0 show platform software trace message hostmanager switch standby R0 show bootlog switch standby R0 show redundancy show redundancy switchover history

Alert Group	Event Type	Syslog Event	Description	Send to Gold EEM/TAC	CLI Commands Executed
					Traceback: show version
					show logging
					show region
					show stacks
					dir crashinfo: | i crashinfo
					dir crashinfo: | i core
					show redundancy
					show redundancy switchover history
					Note: In standalone case, the redundancy/history information will be empty.
					Process and module crash: show version
					dir flash:corecore
					dir flash-1:corecore
					dir flash-2:corecore

Smart Call Home Feature Guide
CONFIGURE

ı|ıı|ıı
CISCO

Alert Group	Event Type	Syslog Event	Description	Send to Gold EEM/TAC	CLI Commands Executed
Snapshot			Snapshot alert group allows customer to send user configurable CLI output to user or SCH server periodically or on-demand. When entering the alert group snapshot, it allows user to add commands to the snapshot.		CLI set defined by users via CLI

Smart Call Home Feature Guide
CONFIGURE

Call Home Trigger Events for Wireless Controller

Wireless controller continuously monitors the wireless network for events, such as client join and roam failures, and, power and channel fluctuations and initiates call home notifications. Call Home notifications for wireless controller are disabled by default. When notifications are enabled, messages are sent to the user for the events that may have occurred in wireless deployment of Smart Call Home. Notifications are sent to the default CiscoTAC-1 profile.

The specific trigger events that are identified for generating notifications are listed below.

AP Crash: Access Point crash occurs when there is a software crash on the AP. Following this, the AP reboots and attempts to join the wireless controller again.

Note

For an AP Crash event, notifications are enabled by default.

Multiple Client Failure: Multiple client failures are associated with authentication and roaming failures of a wireless client. Smart Call Home detects two types of failures - AAA failures (client association and roaming) and Roaming (authentication and mobility) failures – and sends a notification when the number of failed attempts exceed the threshold set by the user. The threshold is the percentage of number of failed attempts over number of total attempts within the specified time interval.

TPC Power Fluctuation: TPC Power Fluctuation is associated with RRM metrics based on power level adjustment. Alert notification is sent to the user when the threshold for power change measured over a period of time interval, is exceeded.

Multiple Channel Fluctuation: Multiple Channel Fluctuation is associated with DCA based on the number of channel change events within the specified time interval.

Tip

The wireless controller detects events based on the threshold set by the users. Due to high variance of the wireless medium, it is recommended that the users customize the threshold parameter to suit their specific deployment.

Smart Call Home Feature Guide
CONFIGURE

ılıılı
CISCO

| Introduction | | Plan | | Install/Deploy | | Configure | | Maintain/Upgrade | | Monitor | | Troubleshoot | | Resources | | Contents |

Table 3 Alert Group Trigger Events for Wireless Client and Commands

Event	Description	Facility-Severity-Mnemonic	CLI Commands Executed	Type/Subtype
AP Crash	Software crash on AP, rebooted	CAPWAP-2-AP_CRASH	more crashinfo:/ap_crash/<filename e>	Crash/AP Crash
Multiple client failure	More than <threshold> client failed to join/roam in specified time window	APF-4-WLC_CLIENT_FAIL_THRESHOLD APF-3-WLC_ROAM_FAIL_THRESHOLD	show wireless client statistic	Syslog/WCM
TPC power fluctuation	The TPC computed TX power for an AP changed more than <threshold> in <time_window>	APF-3-WLC_POWER_THRESHOLD	show ap dot11 24ghz txpower statistics show ap dot11 5ghz txpower statistics	Syslog/WCM
Multiple channel fluctuation	The DCA computed used channel list has changed more than <threshold> times in <time_window>	APF-3-WLC_CHANNEL_THRESHOLD	show ap dot11 24ghz channel statistics show ap dot11 5ghz channel statistics	Syslog/WCM

`

Smart Call Home Feature Guide
CONFIGURE

Enabling Call Home Notifications for Wireless Controller

Call Home notifications for wireless controller can be enabled mainly for two types of events:

- Join and Roam Failures

- Power and Channel Change Fluctuations

Join and Roam Failures

To enable call home notifications for wireless client join and roam failures, perform this task:

	Command	Purpose
Step 1	switch# **configure terminal**	Enters configuration mode.
Step 2	switch(config)# [**no**] **wireless client notification join-failure aaa** [**threshold** *number*]	Enables notifications for client join and authentication failures. A threshold can be specified for triggering notifications. The **no** option disables the notifications. Assigns a percentage *number* between 1 to 100. The default is 20.

Step 3	switch(config)# [**no**]**wireless client notification roam-failure** [**threshold** *number*]	Enables notifications for client roaming failures. A threshold can be specified for triggering notifications. The **no** option disables the notifications. Assigns a percentage *number* between 1 to 100. The default is 20.
Step 4	switch(config) # **wireless client notification interval** *minutes*	Configures the time interval in *minutes* for measuring client failures. Assigns *minutes* between 1 to 1440. The default is 10.

Power and Channel Change Fluctuations

To enable call home notifications for power and channel fluctuations in a wireless channel, perform this task:

	Command	Purpose
Step 1	switch# **configure terminal**	Enters configuration mode.

Step 2	`switch# ap dot11 {24ghz	5ghz} rrm notification power-change [threshold upper number lower number]`	Enables notifications for power change events. A threshold can be specified for triggering notifications.
		Assigns the upper and lower threshold between 3 to 30 dBm. The default is 6 dBm.
		Note Upper threshold for power indicates an upward adjustment in power levels and lower threshold indicates a downward adjustment in power levels.
Step 3	`switch# ap dot11 {24ghz	5ghz} rrm notification channel-change [threshold number]`	Enables notifications for channel change events. A threshold can be specified for triggering notifications.
		Assigns the number of channel change events between 1 to 1000. The default is 1.

Step 4	`switch# ap dot11 {24ghz	5ghz} rrm notification interval minutes`	Configures the time interval in *minutes* for measuring power and channel change events.
		Assigns minutes between 1 to 10080. The default is 60.

Configuring and Enabling Smart Call Home

Smart Call Home can be enabled using any of the following configurations of Call Home:

- HTTPS
- Email to Smart Call Home
- Email to Transport Gateway and HTTPS to Cisco

Call Home Configuration – HTTPS

To configure Smart Call Home using the HTTPS transport method, perform the following task:

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters configuration mode.
Step 2	`Switch# service call-home`	Enables the Call Home feature.
Step 3	`Switch# call-home`	Enters the Call Home configuration submode.

Step 4	`Switch(cfg-call-home)#` **`contact-email-addr`** `email-address`	Assigns the customer's e-mail address. Enter up to 200 characters in e-mail address format with no spaces.
Step 5	`Switch(cfg-call-home)#` **`profile`** `name`	Enters the Call Home destination profile configuration submode for the specified destination profile. If the specified destination profile does not exist, it is created.
Step 6	`Switch(cfg-call-home-profile)#` **`active`**	Enables the destination profile. By default, the profile is enabled when it is created.
Step 7	`Switch(cfg-call-home-profile#` **`destination transport-method http`**	Enables the HTTP transport method.

Step 8	`Install Security Certificate.`	(Optional) Obtain the Cisco server certificate from the Security Certificate.
		Note Installation of security certificate and configuring a trustpoint is required only in the case when your device does not come with a built-in security certificate or if the PKI trustpool feature is not enabled. To check if the PKI trustpool feature is enabled on your device, type this command in EXEC mode - **show crypto pki trustpool**.
Step 9	`Declare and Authenticate CA Trustpoint`	(Optional) Perform the following steps to configure a security trustpoint.
	`Switch(config)#` **`crypto pki trustpoint`** `trustpoint_name`	(Optional) Declares a CA trustpoint on your device and enters CA trustpoint configuration mode.

	`Switch(ca-trustpoint)#` **`enrollment terminal`**	(Optional) Specifies cut and paste enrollment with this trustpoint (also known as manual enrollment).
	`Switch(ca-trustpoint#` **`exit`**	(Optional) Exits from the CA Trustpoint configuration mode.
	`Switch(config)#` **`crypto pki authenticate`** *`trustpoint_name`* `Enter the base 64 encoded CA certificate. End with a blank line or the word "quit" on a line by itself [paste the certificate here and accept it] % Do you accept this certificate? [yes/no]: yes Trustpoint CA certificate accepted. % Certificate successfully imported`	(Optional) Installs and authenticates the CA certificates associated with a trustpoint created for the local entity. Where trustpoint specifies the trustpoint from which to obtain the CA certificate. Maximum name length is 128 characters. The device prompts you to paste the base-64 formatted CA certificate onto the terminal.
	`Switch(config)#` **`exit`**	(Optional)Exits the configuration mode.
Step 10	`Switch(cfg-call-home-profile#` **`end`**	Exits the global configuration mode.

Step 11	`Switch#` **`copy running-config startup-config`**	Saves the configuration.
Step 12	`Switch#` **`call-home send alert-group inventory`** `Sending inventory info call-home message ... Please wait. This may take some time ... Call-home message is sent.`	Sends a Call Home Inventory message to start the registration process.

After the Smart Call Home service is registered, you will receive an email from Cisco Systems. Follow the instructions in the email. The instructions include these procedures:

- To complete the device registration, launch the Smart Call Home web application at the following URL: http://tools.cisco.com/sch/

- Accept the Legal Agreement.

- Confirm device registration for Call Home devices with pending registration.

Call Home Configuration - Call Home Messages to Transport Gateway / HTTPS to Cisco

To configure Smart Call Home using HTTPS via the Transport Gateway method, perform the following task:

`

Smart Call Home Feature Guide
CONFIGURE

	Command	Purpose
Step 1	`Switch#` **`configure terminal`**	Enters configuration mode.
Step 2	`Switch#` **`service call-home`**	Enables the Call Home feature.
Step 3	`Switch#` **`call-home`**	Enters the Call Home configuration submode.
Step 4	`Switch(cfg-call-home)#` **`contact-email-addr`** *`email-address`*	Assigns the customer's e-mail address. Enter up to 200 characters in e-mail address format with no spaces.
Step 5	`Switch(cfg-call-home)#` **`mail-server`** *`address`* **`priority`** *`number`*	Assigns an e-mail server address and its relative priority among configured e-mail servers.
Step 6	`Switch(cfg-call-home)#`**`profile`** `CiscoTAC-1`	Enters the CiscoTAC-1 destination profile configuration submode.
Step 7	`Switch(cfg-call-home-profile)` **`#no active`**	Deactivate the default CiscoTAC-1 profile.
Step 8	`Switch(cfg-call-home)#`**`profile`** *`name`*	Enters the Call Home destination profile configuration submode for the specified destination profile. If the specified destination profile does not exist, it is created.

	Command	Purpose
Step 9	`Switch(cfg-call-home-profile)` **`#active`**	Enables the destination profile. By default, the profile is enabled when it is created.
Step 10	`Switch(cfg-call-home-profile)` **`# destination transport-method email`**	Enables the Email transport method.
Step 11	`Switch(cfg-call-home-profile)` **`# destination address email`** *`email-address`*	Configures the destination email address to which Call Home messages are sent.
Step 12	`Switch(cfg-call-home-profile)` **`# subscribe-to-alert-group`** {**`configuration`** |	Subscribes this destination profile to the specified alert group.
Step 13	`Switch(cfg-call-home-profile)` **`# exit`**	Exits the destination profile configuration submode.
Step 14	`Switch(cfg-call-home)#` **`exit`**	Exits the call home configuration mode.
Step 15	`Switch(config)#` **`end`**	Exits the global configuration mode.
Step 16	`Switch#` **`copy running-config startup-config`**	Saves the configuration.

Step 17	`Download the Transport Gateway, configure and register it for Smart Call Home.`	See the Transport Gateway Installation chapter in Smart Call Home User Guide.
Step 18	`Switch#` **`call-home send alert-group inventory`** `Sending inventory info call-home message ... Please wait. This may take some time ... Call-home message is sent.`	Sends a Call Home Inventory message to start the registration process.

After the Smart Call Home service is registered, you will receive an email from Cisco Systems. Follow the instructions in the email to complete registration for Smart Call Home.

Call Home Configuration - Email to Smart Call Home

To configure Smart Call Home using the Email transport method, perform the following task:

	Command	Purpose
Step 1	`Switch#` **`configure terminal`**	Enters configuration mode.
Step 2	`Switch#` **`service call-home`**	Enables the Call Home feature.
Step 3	`Switch#` **`call-home`**	Enters the Call Home configuration submode.

Step 4	`Switch(cfg-call-home)#` **`contact-email-addr`** `email-address`	Assigns the customer's e-mail address. Enter up to 200 characters in e-mail address format with no spaces.
Step 5	`Switch(cfg-call-home)#` **`mail-server`** `address` **`priority`** `number`	Assigns an e-mail server address and its relative priority among configured e-mail servers.
Step 6	`Switch(cfg-call-home)#` **`profile`** `name`	Enters the Call Home destination profile configuration submode for the specified destination profile. If the specified destination profile does not exist, it is created.
Step 7	`Switch(cfg-call-home-profile)#` **`active`**	Enables the destination profile. By default, the profile is enabled when it is created.
Step 8	`Switch(cfg-call-home-profile)#` **`destination transport-method email`**	Enables the Email transport method.
Step 9	`Switch(cfg-call-home-profile)#` **`exit`**	Exits the destination profile configuration submode.
Step 10	`Switch(cfg-call-home)#` **`exit`**	Exits the call home configuration mode.

Step 11	`Switch(config)# end`	Exits the global configuration mode.
Step 12	`Switch# copy running-config startup-config`	Saves the configuration.
Step 13	`Switch# call-home send alert-group inventory` Sending inventory info call-home message ... Please wait. This may take some time ... Call-home message is sent.	Sends a Call Home Inventory message to start the registration process.

After the Smart Call Home service is registered, you will receive an email from Cisco Systems. Follow the instructions in the email to complete registration for Smart Call Home.

Configuring Call Home When Not Using the Transport Gateway

When not using the Transport Gateway follow the instructions listed below:

- The Cisco device regardless of the protocol (HTTP/SMTP/HTTPS), always scrubs sensitive information such as passwords and SNMP Community strings in the configuration before sending it over the wire.

- SMTP is not a secure protocol and hence is not the recommended method for sending Smart Call Home messages to the back-end server. The preferred mechanism is HTTPS, which is the default.

- The certificate of the Certification Authority must be installed on the Cisco device, before HTTPS communication with the back-end server can occur.

Note

The Cisco server certificate used by Smart Call home needs to be installed on your Cisco device, even if you are already using HTTPS and have a server certificate installed; you need to install the server certificate for Smart Call Home. The Security Certificate is available in Smart Call Home User Guide. The Security Certificate is installed using the crypto pki authenticate command. The sequence of commands used to install the CA certificate on the Cisco device is given below.

```
Switch(config)#crypto pki trustpoint cisco
Switch(ca-trustpoint)#enrollment terminal
Switch(ca-trustpoint)#crypto pki authenticate cisco
```

Note

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
Paste the certificate here and accept it

```
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported
```

Depending on the configuration deployed by the customer, the protocols and ports defined in Table 4 need to be allowed on the firewall between the stated source and destination. In a typical configuration where the Cisco devices are installed on the internal

network, this communication will be seamless without a need for a configuration change on the firewall as the traffic will flow from the Cisco device on the high-security internal network zone to the Internet on the low-security zone.

Table 4 Protocols and Ports without the Transport Gateway

Source	Destination	Protocol	Port	Purpose
Cisco Device	Cisco's back-end server	HTTPS	443	Device to send SCH messages to the back-end server – Option 1
Cisco Device	Customer's email server en route to Cisco's back-end server	SMTP	25	Device to send SCH messages to the back-end server – Option 2
Cisco Device	Customer's Local web server for Customer to process and initiate action	HTTP	80	Device to send SCH messages to the customer server

`

Smart Call Home Feature Guide
CONFIGURE

Configuring Smart Call Home on the Web User Interface
Enabling the Smart Call Home Service

1. On the **General Settings > Smart Call Home** page, set the **Service** field to *Enable*. This allows you to use Smart Call Home on your device.
2. Click **Apply.**

Using Smart Call Home Profiles
Your device contains a default profile called CiscoTAC-1 that is pre-configured for use with Smart Call Home. Although you can update most sections of the default profile, you cannot change alert group subscriptions. To configure different alert groups or transport modes to suit your requirements, you can configure custom smart call home profiles.

Updating the Default CiscoTAC-1 Profile
1. On the **General Settings > Smart Call Home** page, choose the default profile *CisoTAC-1*. Details of the profile are displayed in the Smart Call Home Details section. You can then enter contact information, update transport modes, wireless events and advanced profile settings.
2. Click **Save**.

Creating a Custom Profile
On the **General Settings > Smart Call Home** Home page, click **Add**. The **Add Smart Call Home Settings** window is displayed. Add contact information, configure transport modes, wireless events and advanced profile settings.

Configuring Profile General Settings

Note: General settings are applicable to CiscoTAC-1 and all the custom profiles on your device.

1. On the **General** tab, enter the email address using which Cisco Technical Assistance (Cisco TAC) can contact your organization. This information is mandatory.
2. If you choose email as the transport mode for your notifications, you must configure a mail server for your e-mail. Click **Add**. Select the **Mail Server IP/HostName** check box and specify a mail server name or IP address. You can configure your device to send messages to backup email servers as well. Specify the name or IP address of each email server. Use the **Move Up** and **Move Down** buttons to assign a priority to each server. The priority you assign here determines which server is used as the active server initially, and which servers are used during failure. The priority numbers range from the highest priority of 1 to the lowest priority of 100. The server with the highest priority that the device is able to establish a connection with becomes the active email server.
3. Enter your telephone and address information, your customer ID, contract ID, and the site ID. This information is only used in the XML header of the Call-Home message and is not required by the Smart Call Home System.
4. You can specify a source interface name or source IP address, and a virtual routing and forwarding (VRF) interface to send Smart Call Home notifications. You can enter a source interface name, or a

source IP address, not both.

5. In the **Sender From** field, specify the email address that you want displayed in the From field in the Smart Call Home email notifications sent to you.

6. In the **Recipient** field, specify the email address that you want displayed in the Reply-To field in the Smart Call Home email notifications sent to you. If the reply-to recipient's email address is not configured, the ID provided in the **Contact Email-Address** field, is used as the sender's reply-to email address in all notification messages.

7. Click **Save** or click **Next**.

Configuring Custom Profile Settings

Create a customized profile to suit your delivery format requirements and alert specifications.

1. On the **Create Profile** tab, specify a name for the new profile.
2. To apply the profile to your device, set the **Status** button to *Active*. Multiple profiles can be active on your device.
3. Choose a transport mode to determine how Smart Call Home notifications should be delivered to you. You must choose at least one transport mode.
4. Choose **Email**, to have all Smart Call Home notifications sent via email. In the **Address** field, specify the email address to which to send notifications, and click **+**. You can add multiple email addresses. If you choose Email, you must specify at least one email address, and ensure that you configure a mail server for your email.

5. Choose **HTTP/HTTPS**, to have all your Smart Call Home notifications sent to a specified portal or website. Specify the location to which you want to send notifications, in the **URL** field and click **+**. If you choose HTTP/HTTPS, the HTTP URL is required information. If you provide an HTTPS location as the URL, ensure that you have configured a certificate authorities (CA) trustpoint on your device.

6. Optionally, you can set an HTTP/HTTPS proxy server using which notifications can be sent.

7. Click **Next**.

Configuring Alerts (For Custom Profiles Only)

1. On the **Alerts** tab, choose the alert group to which you want to subscribe. When an event occurs in the alert group that you subscribed to, your device is monitored to obtain more information about the event, at the time of the event, and the output is included in the Smart Call Home message that is sent to Cisco and other configured recipients. You can subscribe to multiple alert groups.

2. To subscribe to **Diagnostic**, **Environment**, **Syslog**, and **Crash** alert groups, and set the same severity level for all the alerts, select **All**. From the **Severity** drop-down list, choose the severity threshold based on which to filter messages in the alert group.

3. To subscribe to only one, or a few of the Smart Call Home alert groups, select the check box for the alert group you want. From the **Severity** drop-down list, choose the severity threshold based on

which to filter messages in the alert group.

4. When you subscribe to the **Syslog** alert group, you can optionally specify a text pattern to be matched within each syslog message. Click **+** to add a design pattern. If you configure a pattern, a Syslog alert group message will be sent only if it contains the specified pattern and meets the severity threshold.

5. When you subscribe to the **Configuration**, **Inventory**, and **Snapshot** alert groups, you can choose to receive the alert group messages asynchronously or periodically at a specified time. For the **Snapshot** alert group, you can only choose to receive the alert group messages periodically. You can configure the time when alerts are sent in the following way:

- Daily—Specify the time of day, using an hour:minute format hh:mm, with a 24-hour clock (for example, 14:30).

- Hourly—Specify the minute of the hour, from 0 to 59. This option is available for the Snapshot alert group.

- Interval—Specify the interval of minutes, from 1 to 60. This option is available for the Snapshot alert group.

- Weekly—Specify the day of the week and time of day in the format day hh:mm, where the day of the week is spelled out (for example, Monday).

- Monthly—Specify the numeric date, from 1 to 31, and the time of day, in the format date hh:mm.

  As part of the snapshot, you can periodically record command line interface (CLI) command output. The output is included in the

smart call home notification sent to you.

6. Click **Next**.

Configuring Smart Call Home Wireless Events
Choose the wireless events that should trigger Smart Call Home notifications. By default, for an AP crash event, notifications are already enabled.

1. On the **Events** page, select the **Client Failure** check box to monitor authentication and roaming failures associated with wireless clients. Smart Call Home detects both AAA failures and roaming (authentication and mobility) failures, and sends a notification when the number of failed attempts exceeds the set threshold set.

2. Set the **Client Join Failure** threshold or the percentage of failed client join attempts within the specified time interval, at which to send notifications.

3. Set the **Client Roam Failure** threshold or the percentage of failed roaming attempts within the specified time interval, at which to send notifications.

4. Specify the interval or the time period, in minutes, during which to measure client join failures.

5. Select the **RRM Threshold** check box to monitor power fluctuations based on Radio Resource Management (RRM) metrics, and channel fluctuations based on Dynamic Channel Assignment (DCA). Smart Call Home sends notifications when the power change measured over a specified period interval, exceeds the set threshold. You can configure RRM events for both 2.5 GHz and 5 GHz radios.

6. In the **Channel Change** field, set the threshold or the number of

`

Smart Call Home Feature Guide
CONFIGURE

CISCO

| Introduction | Plan | Install/Deploy | Configure | Maintain/Upgrade | Monitor | Troubleshoot | Resources | Contents |

channel changes after which to send Smart Call Home notifications.

7. In the **Power Change Upper** and **Power Change Lower** fields, assign the upper and lower threshold between 3 to 30 dBm. The default is 6 dBm.
8. Set the time interval, between 1 and 10080 minutes, during which to measure power and channel change events. The default is 60 minutes.
9. Click **Save** or click **Next**.

Configuring Advanced Profile Settings
Use the **General Settings > Smart Call Home > Advanced** page to configure advanced settings for all profiles on your device.

1. To aviod sending repetitive syslog messages, enable Smart Call Home syslog message throttling. By default, **Syslog Throttling** is enabled.
2. From the **Data Privacy Level** drop-down list, choose the privacy level to scrub data from Smart Call Home messages to protect your privacy. The default data-privacy level is *Normal*. Setting the privacy level to *High* scrubs data from the IP address and IP domain name from the messages.
3. Select the **Remove Host Name** check box to remove the host name from the subject line of the Smart Call Home notification email that is sent.
4. To enable AAA authorization for Smart Call Home messages, select the **AAA Authorization** check box. Specify the user name for authorization. The default user name is *callhome*.
5. Click **Save** and **Apply** to save your changes.

Smart Call Home Feature Guide
MAINTAIN

Maintaining/Upgrading

Obtaining and Upgrading the latest Software files

For obtaining the latest software files and any upgradation, visit the Smart Call Home page.

Administering

System Access

The Smart Call Home System offers two access levels for customers - Administrator and User. The higher level of access is the Administrator and is attained by confirming a device registration associated with a Company or when an Administrator registers another person as an Administrator. The User access level is achieved when an Administrator grants a person User access associated with a Company.

These access levels provide different access to the Smart Call Home System. The Administrator has permission to administer device registrations and preferences, administer Transport Gateway registrations and preferences, add and delete user registrations, view device and user lists, and generate reports for associated Companies.

A User is able to view device and user lists, and is able to generate reports for associated Companies, but is not able to:

- Delete any device or user registrations for a Company

- Edit any device registrations for a Company

- Add any user registrations for a Company

- View or delete any Transport Gateway registrations for a Company

- Be a Service Request contact person for any device registered to a Company

- Modify device preferences for a Company

A user can access the Smart Call Home Customer Web application with a valid Cisco.com ID and password.

Use of the Smart Call Home Customer Web Application requires acceptance of the application's current Legal Agreement. The Legal Agreement will be presented if the user has not accepted the latest copy of the agreement.

The user must agree to the legal terms and conditions before further access is granted within the Smart Call Home Customer Web Application. A User who was added by an Administrator will have status 'Pending Legal Agreement' until the Legal Agreement is accepted.

Monitoring

An important aspect of Smart Call Home System is monitoring devices constantly and generating notifications.

Notifications and Web Application

A Smart Call Home user has the option to receive e-mail notifications, from the Smart Call Home system, when messages are received from client devices. These notifications may indicate one of the following:

- The need to register a device

- That updated inventory or configuration information is available

- Information about user events that are occurring on the client device

Analyses of events that have occurred on the device are stored along with the messages. A Smart Call Home user may choose to have service requests created in the TAC Service Request Tracking System, if the results of the analyses include service request creation or updating. This option may be set per device by the Smart Call Home user. If the user has chosen this option, notifications related to Service Request (SR) activity will be sent to the user.

The user has access to the data stored in the Smart Call Home back-end systems with the Smart Call Home Web application. The Web application is used to register client devices and users with the Smart Call Home system. The Web application is also used to generate device and Call Home history reports. The user who has administration privileges is also able to manage user access to the system.

Registration Management Processes

On the Smart Call Home web application all registration related activities are consolidated under one tab, the Registration Management tab. This tab provides access to registration for devices, users and Transport Gateways.

This section describes the various registration functions for the following areas:

- Device Registration

- User Registration

- Transport Gateway Registration

Overview of Registration Processes

In order for customer Cisco devices to communicate in the Smart Call Home environment there are several types of registrations that must occur first; there are three basic types of registrations:

- Device Registration – Devices are associated with a Cisco.com user id, valid contract or warranty, and Company. This registration is required for Call Home messages sent by the device to be processed. See the Device Registration in Smart Call Home Web Application chapter of Smart Call Home User Guide for detailed steps.

- User Registration – Users get registered to a company and gets automatically created when the customer confirms the device

registration. The user registration is needed so the customer can get access to the reports in the web application. A customer can register additional users. See User Registration in Smart Call Home Web Application chapter of Smart Call Home User Guide for detailed steps.

- Transport Gateway Registration – Transport Gateways get associated to a company. The Transport Gateway registration is needed only when the customer wants to use a Transport Gateway to send Call Home messages to the backend. See Transport Gateway Registration in Smart Call Home Web Application chapter of Smart Call Home User Guide for detailed steps.

All of the previous registration options are available on the Smart Call Home web application under the Registration Management tab.
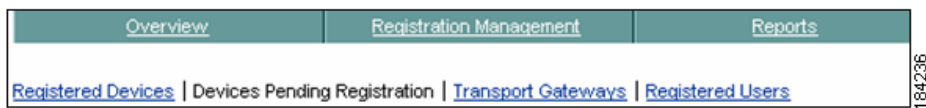
This tab provides access to the following registration functions for:

- Registered Devices – Lets you manage device registrations for registered devices.

- Devices Pending Registration – Lets you confirm device registrations in order for the device to become registered in Smart Call Home.

- Transport Gateways – Lets you manage Transport Gateway registrations.

- Registered Users – Lets you manage user registrations and add users.

Report Generation

The Smart Call Home Customer Web Application currently offers access to three types of reports. These are Device Reports, Call Home History Reports, and Network Summary Reports. Each report provides information on registered devices only.

All displayed reports may be exported to PDF or Excel formats.

Reports are only available for registered devices and when a customer is registered to one or more companies, they can view the reports for the devices registered to those same companies.

This section explains how to perform the following tasks:

- Access the different types of Reports:

  – Device Reports – 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. See Device Reports for detailed steps.

  – 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. See Call Home History Report for detailed steps.

  – Network Summary Report – identifies and summarizes all

the different types of devices that make up the customers network. See Network Summary Report for detailed steps.

- 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. See Registration Summary Report for detailed steps.

- Specify Report Criteria to generate reports for specific devices.

- Obtain information about View Device Details, contacts, and different types of messages.

Troubleshooting

This chapter covers the following topics:

Troubleshooting Call Home Errors

Topics in this section include Transport Gateway problems dealing with:

- Troubleshooting AAA Authorization Failure Errors

- Troubleshooting Call Home HTTP Destination Errors

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.

Troubleshooting Call Home Wireless Client Errors

CAPWAP-2-AP_CRASH
This error is caused due to crash of the access point.

Symptom/Cause:

- Possible cause is software crash on the access point.

Fix:

- Check the version for the access point images.

APF-4-WLC_CLIENT_FAIL_THRESHOLD
This error is associated with client join failures.

Symptom/Cause:

- Possible cause is authentication failure - AAA failure.

Fix:

- If number of clients failing to join is higher than expected, it could be due to issues with authentication services or due to an attack. Check AAA settings and status of AAA services, like RADIUS.

APF-3-WLC_ROAM_FAIL_THRESHOLD
This error is associated with client roam failures.

Symptom/Cause:

- Possible causes are authentication failures and capacity issues.

| Introduction | Plan | Install/Deploy | Configure | Maintain/Upgrade | Monitor | Troubleshoot | Resources | Contents |

Fix:

- Check configuration consistency among MC and MA, especially authentication credentials. Check number of clients on the Access Points and communication links between MA-MA, MA-MC, MC-MC, MA-RADIUS and MC-RADIUS.

APF-3-WLC_CHANNEL_THRESHOLD

This error is associated with channel changes within the specified time interval.

Symptom/Cause:

Possible causes are channel changes in the 24 GHz and 5 GHz band during the specified monitoring interval.

Fix:

Check the reason for channel change using the command: **show ap dot11 {24 | 5} channel statistics**.

## 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

Transport Gateway Configuration

There are two configuration scenarios that relate to the same error message, but are caused for different reasons. The first configuration scenario is related to specifying the connection between the Transport Gateway and the mail server. The second configuration scenario is related to specifying the IMAP folder name. The following information contains more details about each scenario:

- Configuration error 1 is an unsecured connection between the Transport Gateway and mail server.

- Configuration error 2 is associated with configuring the IMAP folder name by manually editing the property file.
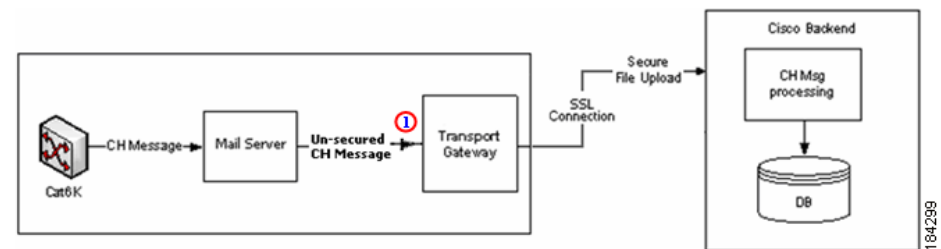
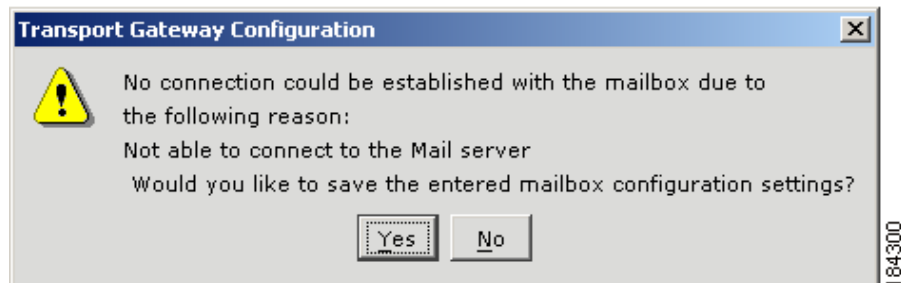*Cannot establish an un-secured connection to the Mail server*

During configuration of the Transport Gateway, you want to configure an un-secured connection to the mail server but get the following warning message when trying to establish a connection.

| Introduction | | Plan | | Install/Deploy | | Configure | | Maintain/Upgrade | | Monitor | | Troubleshoot | | Resources | | Contents |

Symptom / Cause:

- User may not have configured the mail server to support the unsecured mail port numbers.

- User may not have configured the mail server to mail server type POP3 or IMAP.

Fix:

- Configure the mail server to support the unsecured mail port numbers.

- Configure the mail server to mail server type POP3 or IMAP.

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 get the following warning message when trying to establish a connection
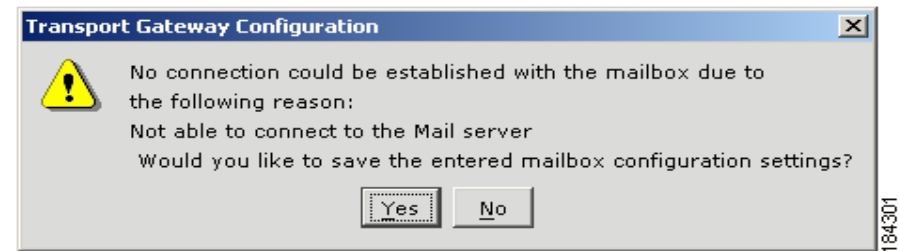
Symptom / Cause:

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

Fix:

- The Transport Gateway GUI does not provide the ability to specify which protocol will contain the INBOX; this specification is made by manually editing the properties file.

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.

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 <TGROOT>/Transport Gateway/Conf/an/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.
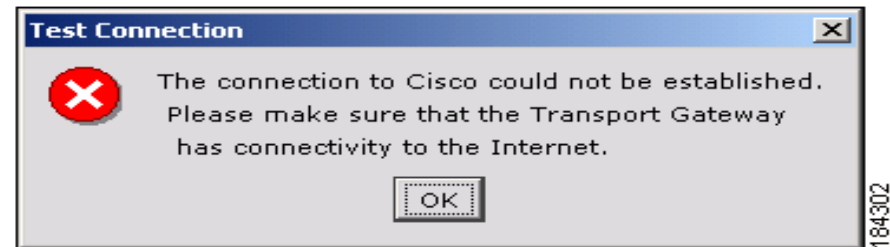
Transport Gateway Connectivity

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

- Connection to Cisco backend could not be established

- Cisco.com ID is invalid

Transport Gateway is not able to connect to the Cisco backend.

When you click **Test Connection** on the Transport Gateway application, the following error window appears.

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.

- Contact your IT representative for details on proxy settings, if they are not known.

Cisco.com ID is invalid

When you to 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 and/or password the application will notify you about this problem via a pop-up message.

- To register a Transport Gateway a valid Cisco.com ID and password are required.

Fix:

- Verify if the entered Cisco.com ID and password are correct.

- If you do not yet have a valid Cisco.com ID or password you can create a new Cisco.com ID via the Cisco.com Registration tool.

Transport Gateway Start Up

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

- Transport Gateway does not start in Linux Environment

- Can Not See GUI Through Raritan Remote Client

- Transport Gateway GUI Does Not Start

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.ma
in(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
```

| Introduction | Plan | Install/Deploy | Configure | Maintain/Upgrade | Monitor | Troubleshoot | Resources | Contents |

```
    * 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!
```

Can Not See GUI Through Raritan Remote Client

Symptom / Cause:

- Proper setup command has not been issued.

Fix:

- Issue the following command:

Command: **xhost +local:root (or) xhost + localhost**

Transport Gateway GUI Does Not Start

After configuring the Transport Gateway, the Transport Gateway service is started but the GUI crashes as soon as it is started.

Symptom / Cause:

There are two probable causes for this error:

- The Transport Gateway is being started on a device that also has RDP installed and running.

- The Transport Gateway is being started in an unsupported environment (i.e. the device is running a virtual server like VMWare). In this situation the VMWare application has already obtained resources that the Transport Gateway GUI needs to operate, but now cannot obtain.

Both of the above situations will cause the Transport Gateway GUI to crash as soon as it is started, and stop the background process.

Fix: (for RDP)

If the Transport Gateway device has RDP installed and running perform the following steps:

Step 1 Stop the TG service

Step 2 Close the RDP Connections

Step 3 Re-launch the RDP using the following command

```
mstsc /v <ip add> /admin
```

Note

<ip add> is the ip address the Transport Gateway is installed on.

Step 4 Launch the Transport Gateway.

Work around: (for unsupported Transport Gateway environment)

If the environment (hardware / software) does not support the Transport Gateway then there are two other options that can be utilized to communicate with Smart Call Home, instead of using the Transport Gateway.

Use one of the following Call Home configurations to communicate with Smart Call Home:

Call Home Configuration - HTTPS

Call Home Configuration - Email to Smart Call Home

Transport Gateway Operation

The following error could be encountered when trying to send Call Home messages from the Transport Gateway to the Cisco Backend:

Transport Gateway Keeps Sending Failed Call Home Messages with Duplicate Message IDs

Symptom / Cause:

- SCH backend throws Connection time out exception, the Transport Gateway continuously tries to send failed Call Home message(s) to the Cisco Backend.

Fix:

- Upgrade the Transport Gateway to the latest version.

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.

Introduction	Plan	Install/Deploy	Configure	Maintain/Upgrade	Monitor	Troubleshoot	Resources	Contents

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

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

Introduction	Plan	Install/Deploy	Configure	Maintain/Upgrade	Monitor	Troubleshoot	Resources	Contents

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.

| Introduction | Plan | Install/Deploy | Configure | Maintain/Upgrade | Monitor | Troubleshoot | Resources | Contents |

- 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.

Cannot 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.

Introduction	Plan	Install/Deploy	Configure	Maintain/Upgrade	Monitor	Troubleshoot	Resources	Contents

- 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

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:

Cannot 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.

Smart Call Home Feature Guide

Introduction	Plan	Install/Deploy	Configure	Maintain/Upgrade	Monitor	Troubleshoot	Resources	Contents

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

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.

| Introduction | Plan | Install/Deploy | Configure | Maintain/Upgrade | Monitor | Troubleshoot | Resources | Contents |

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.

Smart Call Feature Guide

RESOURCE AND SUPPORT INFORMATION

Resources/Support Information

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

- For More Information
- Terminology
- Technical Support Information

For More Information

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

- https://supportforums.cisco.com/community/4816/smart-call-home
- Use the feedback box on the Smart Call Home web application
- Contact Smart Call Home at email address - sch-support@cisco.com
- Smart Call Home Technical White Paper – Catalyst 6500 http://www.cisco.com/c/dam/en/us/td/docs/switches/lan/smart_call_home/Smart_Call_Home_Technical_White_Paper.pdf

Terminology

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

- **Call Home (CH)** - Product feature in Cisco IOS XE Denali 16.1.1 that uses SMTP or HTTP connections established with a configurable

destination to send formatted messages. The messages contain Inventory and Configuration information that are collected at scheduled intervals. Configuration, Crash, Diagnostics, Environmental, Inventory, System Log (syslog) information is collected during real-time events; Test, Inventory, Configuration Diagnostic, Environmental and Snapshot 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, Crash, Diagnostics, Environmental, Inventory Snapshot 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, Crash, Diagnostics, Environmental, Inventory, Test, Snapshot 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, Crash, Gold major, minor or normal Diagnostics information, minor or major Environmental information, Test, Snapshot 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.

Smart Call Feature Guide
RESOURCE AND SUPPORT INFORMATION

- 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.

- **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), Crash, Diagnostics (major & minor), Environmental (major & minor), Inventory (full), Test, Snapshot 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.

Technical Support Information

For technical support, please contact Cisco Smart Services Bureau (SSB) via:

Email:ask-smart-services@cisco.com<mailto:ask-smart-services@cisco.com>

Telephone:

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

Smart Call Feature Guide
RESOURCE AND SUPPORT INFORMATION

| Introduction | Plan | Install/Deploy | Configure | Maintain/Upgrade | Monitor | Troubleshoot | Resources | Contents |

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

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

Smart Call Feature Guide

RESOURCE AND SUPPORT INFORMATION

TOMORROW
starts here.

ıllııllı
CISCO™