Installation and Configuration

Revised: December 13, 2013 Smart Call Home 3.5

Resources for Installing and Configuring Smart Call Home

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

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

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

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

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

Enabling Smart Call Home

There are four steps to enable Smart Call Home:

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

Identify Devices

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

Select the transport method

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

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

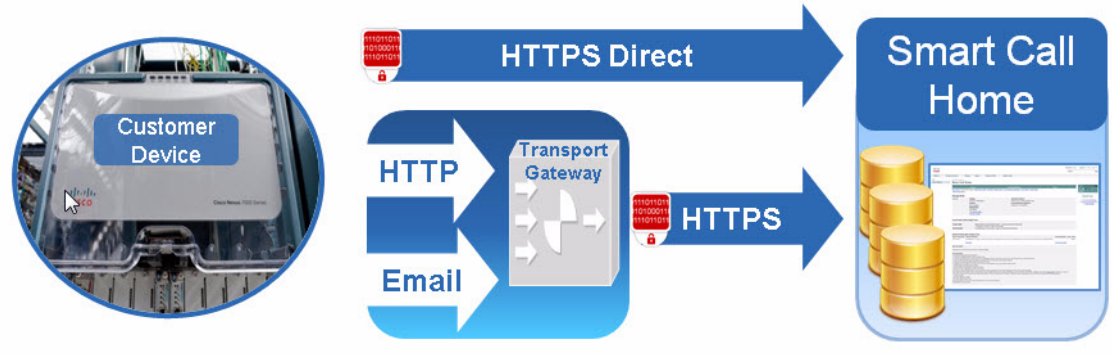

Figure 2-1 Transport Options

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

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

The transport gateway is not required when:

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

The transport gateway is required when:

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

The transport gateway is desirable when:

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

Configure Devices

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

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

Call Home Profiles

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

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

Alert Groups

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

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

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

Register Devices

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

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

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

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

Call Home Alert Groups and CLI Commands

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

Using AAA on the Cisco Device

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

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

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

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