# Call Home

Call Home offers diagnostics and real-time alerts on select Cisco devices, which provide higher network availability and increased operational efficiency. Smart Call Home is a secure connected service of Cisco SMARTnet for the Cisco cBR routers.

### Finding Feature Information

Your software release may not support all the features that are documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. The Feature Information Table at the end of this document provides information about the documented features and lists the releases in which each feature is supported.

### Contents



# Hardware Compatibility Matrix for the Cisco cBR Series Routers

**Note** The hardware components that are introduced in a given Cisco IOS-XE Release are supported in all subsequent releases unless otherwise specified.

*Table 1: Hardware Compatibility Matrix for the Cisco cBR Series Routers*

| Cisco CMTS Platform | Processor Engine | Interface Cards |
|---|---|---|
| Cisco cBR-8 Converged Broadband Router | **Cisco IOS-XE Release 16.5.1 and Later Releases**<br>Cisco cBR-8 Supervisor:<br>• PID—CBR-SUP-250G<br>• PID—CBR-CCAP-SUP-160G<br>• PID—CBR-CCAP-SUP-60G<br>• PID—CBR-SUP-8X10G-PIC | **Cisco IOS-XE Release 16.5.1 and Later Releases**<br>Cisco cBR-8 CCAP Line Cards:<br>• PID—CBR-LC-8D30-16U30<br>• PID—CBR-LC-8D31-16U30<br>• PID—CBR-RF-PIC<br>• PID—CBR-RF-PROT-PIC<br>• PID—CBR-CCAP-LC-40G<br>• PID—CBR-CCAP-LC-40G-R<br>Cisco cBR-8 Downstream PHY Modules:<br>• PID—CBR-D30-DS-MOD<br>• PID—CBR-D31-DS-MOD<br>Cisco cBR-8 Upstream PHY Modules:<br>• PID—CBR-D30-US-MOD<br>• PID—CBR-D31-US-MOD |

# Prerequisites for Call Home

- Contact email address (required for full registration with Smart Call Home, optional if Call Home is enabled in anonymous mode), phone number (optional), and street address information (optional) must be configured so that the receiver can determine the origin of messages received.

**Note** Contact email address is not required if you enable Smart Call Home by enabling smart licensing.

- At least one destination profile (predefined or user-defined) must be configured. The destination profiles configured depends on whether the receiving entity is a pager, email, or automated service such as Cisco Smart Call Home.
  - If the destination profile uses email message delivery, you must specify a Simple Mail Transfer Protocol (SMTP) server.
  - Configuring the trustpool certificate authority (CA) is not required for HTTPS server connection as the trustpool feature is enabled by default.

- The router must have IP connectivity to an email server or the destination HTTP(S) server.
- To use Cisco Smart Call Home service, you require an active service contract covering the device, which provides full Smart Call Home service.

**Note** An active service contract is only required for full Smart Call Home services like automatically raising a Cisco Technical Assistance Center (TAC) case.

# Restrictions for Call Home

- If there is no IP connectivity or if the interface in the VRF to the profile destination is down, Smart Call Home messages cannot be sent.
- Smart Call Home operates with any SMTP server.
- You can configure up to five SMTP servers for Smart Call Home.

# Information About Call Home

The Call Home feature provides email-based and web-based notification of critical system events. A versatile range of message formats are available for optimal compatibility with pager services, standard email, or XML-based automated parsing applications.

Common uses of this feature may include:

- Direct paging of a network support engineer
- Email notification to a network operations center
- XML delivery to a support website
- Use of Cisco Smart Call Home services for direct case generation with the Cisco Technical Assistance Center (TAC).

The Call Home feature can deliver alert messages containing information about configuration, environmental conditions, inventory, syslog, snapshot, and crash events.

The Call Home feature can deliver alerts to multiple recipients, which are seen as *Call Home destination profiles*, each with configurable message formats and content categories. A predefined destination profile (CiscoTAC-1) is provided, and you can also define your own destination profiles. The CiscoTAC-1 profile is used to send alerts to the backend server of the Smart Call Home service. It can be used to create service requests to Cisco TAC. This service depends on the Smart Call Home service support in place for your device and the severity of the alert.

Flexible message delivery and format options make it easy to integrate specific support requirements.

## Benefits of Call Home

- Automatic execution and attachment of the relevant CLI command output.

- Multiple message-format options such as the following:
  - Short Text—Suitable for pagers or printed reports.
  - Full Text—Fully formatted message information suitable for human reading.
  - XML—Matching readable format using Extensible Markup Language (XML). The XML format enables communication with the Cisco TAC.
- Multiple concurrent message destinations.
- Multiple message categories including configuration, crash, diagnostic, environment, inventory, snapshot, and syslog.
- Filtering of messages that are based on the severity and pattern matching.
- Scheduling of periodic message sending.

# Obtaining Smart Call Home Services

If you have a service contract directly with Cisco, you can register for the Smart Call Home service. Smart Call Home analyzes Smart Call Home messages and provides background information and recommendations. For critical issues, Automatic Service Requests are generated with the Cisco TAC.

Smart Call Home offers the following features:

- Continuous device health monitoring and real-time alerts.
- Analysis of Smart Call Home messages. Optional generation of the Automatic Service Request report, including detailed diagnostic information that speeds up the problem resolution, which is routed to the correct TAC team.
- Direct secure message transportion from your device, through an HTTP proxy server, or a downloadable Transport Gateway (TG). You can use a TG aggregation point to support multiple devices. Or, you can use it in scenario where security dictates that your devices may not be connected directly to the Internet.
- Web-based access that provides Smart Call Home messages and recommendations, inventory, and configuration information for all Smart Call Home devices. This access provides associated field notices, security advisories, and end-of-life information.

You need the following items to register for Smart Call Home:

- SMARTnet contract number for your router.
- Your email address
- Your Cisco.com username

For information about how to configure Call Home to work with the Smart Call Home service, see the Cisco Smart Call Home Support Community forum.

## Anonymous Reporting

Smart Call Home is a service capability that is included with many Cisco service contracts and is designed to assist you help resolve problems quickly. In addition, the information gained from crash messages helps Cisco understand equipment and issues occurring in the field. You can enable Anonymous Reporting without

Smart Call Home. Anonymous Reporting allows Cisco to securely receive minimal error and health information from the device. If you enable Anonymous Reporting, your identity remains anonymous, and no identifying information is sent.

**Note** When you enable Anonymous Reporting, you acknowledge your consent to transfer specified data. The data is shared with Cisco or to vendors operating on behalf of Cisco (including countries outside the United States). Cisco maintains the privacy of all customers. For information about how Cisco treats personal information, see the Cisco Privacy Statement at Cisco Online Privacy Statement.

When Call Home is configured in an anonymous way, only crash, inventory, and test messages are sent to Cisco. No identifying information is sent.

For more information about what is sent in these messages, see the Alert Group Trigger Events and Commands section.

### Smart Licensing

Smart Licensing uses the Smart Call Home service.

The Smart Licensing service is an alternative licensing architecture to Cisco Software Licensing (CSL). Smart Licensing uses the Cisco Smart Software Manager as a backend tool for managing licenses. Smart Call Home must be configured before using the Smart Licensing. By default, Smart Licensing and Smart Call Home are enabled on the Cisco cBR routers.

For more information about Smart Licensing, see the Cisco Smart Licensing on the Cisco cBR Router topic.

# How to Configure Call Home

## Configuring Smart Call Home (Single Command)

Smart Call Home is enabled by default on the router. The CiscoTAC-1 profile to send data to Cisco is also enabled by default.

Unless you change to anonymous mode or add HTTP proxy, the single command is not used to enable Smart Call Home on the router.

To enable all Call Home basic configurations using a single command, perform the following steps:

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 2** | **call-home reporting** { **anonymous** \| **contact-email-addr** *email-address* } [ **http-proxy** { *ipv4-address* \| *ipv6-address* \| **name** } **port** *port number* ]<br>**Example:**<br>`Device(config)#`<br>**`call-home reporting contact-email-addr email@company.com`** | Enables all Call Home basic configurations using a single command.<br>• **anonymous** —Enables the Call-Home TAC profile to only send crash, inventory, test messages, and send the messages in an anonymous way.<br>• **contact-email-addr** —Enables Smart Call Home service full reporting capability. The service also sends a full inventory message from the Call-Home TAC profile to the Smart Call Home server to start full registration process.<br>• **http-proxy** { *ipv4-address* \| *ipv6-address* \| **name** —An IPv4 or IPv6 address or server name. Maximum length is 64.<br>• **port** *port number* —Port number. Range is 1 to 65535.<br>**Note** HTTP proxy option allows you to set your own proxy server to buffer and secure the internet connections from your devices.<br>**Note** After successfully enabling Call Home either in anonymous or full registration mode using the **call-home reporting** command, an inventory message is sent out. If Call Home is enabled in anonymous mode, an anonymous inventory message is sent out. If Call Home is enabled in full registration mode, a Full Inventory message for full registration mode is sent. For more information about what is sent in these messages, see the Alert Groups Trigger Events and Commands, on page 48 topic. |

# Configuring Call Home

For security reasons, we recommend that you use the HTTPS transport options, due to the additional payload encryption that HTTPS offers. The Transport Gateway software is downloadable from Cisco.com and is available if you require an aggregation point or a proxy for connection to the Internet.

The implementation on the router supports the trustpool feature (embedded CA certificates in Cisco IOS images). The trustpool feature simplifies configuration to enable Smart Call Home service on configured devices. It eliminates the requirement of manually configuring the trustpool and provides the automatic update of the CA certificate, if it changes in the future.

## Enabling and Disabling Call Home

To enable or disable the Call Home feature, complete the following steps:

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`Router#`<br>**`configure terminal`** | Enters global configuration mode. |
| **Step 2** | **service call-home**<br>**Example:**<br>`Router(config)#`<br>**`service call-home`** | Enables the Call Home feature. |
| **Step 3** | **no service call-home**<br>**Example:**<br>`Router(config)#`<br>**`no service call-home`** | Disables the Call Home feature. |

## Configuring Contact Information

Each router must include a contact email address. You can optionally include a phone number, street address, contract ID, customer ID, and site ID.

To assign the contact information, complete the following steps:

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`Router>`<br>**`configure terminal`** | Enters global configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 2** | **call-home**<br>**Example:**<br>`Router(config)#`<br>**`call-home`** | Enters call home configuration mode. |
| **Step 3** | **contact-email-addr** *email-address*<br>**Example:**<br>`Router(cfg-call-home)#`<br>**`contact-email-addr username@example.com`** | Assigns the customer's email address. Enter up to 200 characters in email address format with no spaces. |
| **Step 4** | **phone-number** + *phone-number*<br>**Example:**<br>`Router(cfg-call-home)#`<br>**`phone-number +1-222-333-4444`** | (Optional) Assigns the customer's phone number.<br>**Note** The number must start 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 within double quotation marks (" "). |
| **Step 5** | **street-address** *street-address*<br>**Example:**<br>`Router(cfg-call-home)#`<br>**`street-address "1234 Any Street, Any city, Any state, 12345"`** | (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 within double quotation marks (" "). |
| **Step 6** | **customer-id** *text*<br>**Example:**<br>`Router(cfg-call-home)#`<br>**`customer-id Customer1234`** | (Optional) Identifies the customer ID. Enter up to 64 characters. If you include spaces, you must enclose your entry within double quotation marks (" "). |
| **Step 7** | **site-id** *text*<br>**Example:**<br>`Router(cfg-call-home)#`<br>**`site-id Site1ManhattanNY`** | (Optional) Identifies the customer site ID. Enter up to 200 characters. If you include spaces, you must enclose your entry within double quotation marks (" "). |
| **Step 8** | **contract-id** *text*<br>**Example:** | (Optional) Identifies the customer's contract ID for the router. Enter up to 64 characters. If you |

| | Command or Action | Purpose |
|---|---|---|
| | `Router(cfg-call-home)#` **`contract-id Company1234`** | include spaces, you must enclose your entry within double quotation marks (“ ”). |

## Configuring Destination Profiles

A destination profile contains the required delivery information for an alert notification. At least one destination profile is required. You can configure multiple destination profiles of one or more types.

You can create and define a new destination profile or copy and use the predefined destination profile. If you define a new destination profile, you must assign a profile name. You can control which profile to be used for Smart Licensing by enabling or disabling smart-licensing data of that profile. Only one active profile can have a data enabled smart-license.

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

A destination profile includes the following information:

- Profile name—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.
- Transport method—Transport mechanism, either email or HTTP (including HTTPS), for delivery of alerts.
  - For user-defined destination profiles, email is the default, and you can enable either or both transport mechanisms. If you disable both methods, email is enabled.
  - For the predefined CiscoTAC-1 profile, you can enable either transport mechanism, but not both.
- Destination address—The actual address that is related to the transport method by which the alert is sent. You can change the destination of the CiscoTAC-1 profile.
- Message formatting—The message format that is used for sending the alert. The format options for a user-defined destination profile are long-text, short-text, or XML. The default is XML. For the predefined CiscoTAC-1 profile, only XML is allowed.
- Message size—The maximum destination message size. The valid range is 50 to 3,145,728 bytes. The default is 3,145,728 bytes.
- Reporting method—You can choose which data to report for a profile. You can enable reporting of Smart Call Home data or Smart Licensing data, or both. Only one active profile is allowed to report Smart Licensing data at a time.
- Anonymous reporting—You can choose for your customer identity to remain anonymous, and no identifying information is sent.
- Subscribing to interesting alert-groups—You can choose to subscribe to alert-groups highlighting your interests.
- Message severity level—The Call Home severity level that the alert must meet before a Call Home message is generated. The Call Home message is then delivered to all email addresses in the destination

profile. An alert is not generated if the Call Home severity level of the alert is lower than the message severity level set for the destination profile.

You can also configure a destination profile to allow periodic inventory update messages by using the inventory alert group.

A predefined destination profile CiscoTAC-1 is supported. It supports the XML message format. This profile is preconfigured with the Cisco Smart Call Home server HTTPS URL. This profile contains information such as the email address to reach the server, maximum message size, and message severity level for each alert group.

**Important** We recommend that you do not use the message severity level 0. If you use message severity level 0, all syslogs trigger Call Home messages, which can cause CPU and memory issues.

This section contains the following:

## Creating a New Destination Profile

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password, if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **call-home**<br>**Example:**<br>`Router(config)# call-home` | Enters Call Home configuration mode. |
| **Step 4** | **profile** *name*<br>**Example:**<br>`Router(cfg-call-home)# profile profile1` | Enters the Call Home destination profile configuration mode for the specified destination profile. If the specified destination profile does not exist, it is created. |
| **Step 5** | **destination transport-method** { **email** \| **http** }<br>**Example:**<br>`Router(cfg-call-home-profile)# destination transport-method email` | (Optional) Enables the message transport method.<br>• **email** —Sets the email message transport method.<br>• **http** —Sets the HTTP message transport method.<br>**Note** The **no** option disables the method. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 6** | **destination address** { **email** *email-address* \| **http** *url* }<br>**Example:**<br>`Router(cfg-call-home-profile)# destination address email myaddress@example.com` | Configures the destination email address or URL to which Call Home messages are sent.<br>**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 trustpool CA. |
| **Step 7** | **destination preferred-msg-format** { **long-text** \| **short-text** \| **xml** }<br>**Example:**<br>`Router(cfg-call-home-profile)# destination preferred-msg-format xml` | (Optional) Configures a preferred message format. The default is XML.<br>• **long-text** —Configures the long text message format.<br>• **short-text** —Configures the short text message format.<br>• **xml** —Configures the XML message format. |
| **Step 8** | **destination message-size** *bytes*<br>**Example:**<br>`Router(cfg-call-home-profile)# destination message-size 3,145,728` | (Optional) Configures a maximum destination message size for the destination profile. |
| **Step 9** | **active**<br>**Example:**<br>`Router(cfg-call-home-profile)# active` | Enables the destination profile. By default, the profile is enabled when it is created.<br>If you activate a profile which enables smart-licensing data while smart-licensing data is already being reported in another active profile, you will receive an error message. |
| **Step 10** | **reporting** { **all** \| **smart-call-home-data** \| **smart-licensing-data** }<br>**Example:**<br>`Router(cfg-call-home-profile)# reporting smart-call-home-data` | Configures the type of data to report for a profile.<br>You can select either to report Smart Call Home data or Smart Licensing data. Selecting the **all** option reports data for both types of data. |
| **Step 11** | **end**<br>**Example:**<br>`Router(cfg-call-home-profile)# end` | Returns to privileged EXEC mode. |
| **Step 12** | **show call-home profile** { *name* \| **all** }<br>**Example:** | Displays destination profile configuration for the specified profile or all configured profiles. |

| | Command or Action | Purpose |
|---|---|---|
| | `Router# show call-home profile profile1` | |
| **Step 13** | **show call-home smart-licensing**<br>**Example:**<br>`Router# show call-home smart-licensing` | Displays the current Call Home Smart Licensing settings for the configured destination profiles. |
| **Step 14** | **show call-home smart-licensing statistics**<br>**Example:**<br>`Router# show call-home smart-licensing statistics` | Displays the Call Home Smart Licensing statistics. |

## Copying a Destination Profile

You can create a new destination profile by copying an existing profile.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password, if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **call-home**<br>**Example:**<br>`Router(config)# call-home` | Enters Call Home configuration mode. |
| **Step 4** | **copy profile** *source-profile target-profile*<br>**Example:**<br>`Router(cfg-call-home)# copy profile profile1 profile2` | Creates a new destination profile with the same configuration settings as the existing destination profile.<br>• *source-profile* —Name of the source destination profile.<br>• *target-profile* —Name of the target or new destination profile. |

## Renaming a Destination Profile

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable** | Enables privileged EXEC mode. |

| | Command or Action | Purpose |
|---|---|---|
| | **Example:**<br>`Router> enable` | • Enter your password, if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **call-home**<br>**Example:**<br>`Router(config)# call-home` | Enters Call Home configuration mode. |
| **Step 4** | **rename profile** *source-profile target-profile*<br>**Example:**<br>`Router(cfg-call-home)# rename profile profile1 profile2` | Renames the existing destination profile.<br>• *source-profile* —Name of the source destination profile.<br>• *target-profile* —Name of the target destination profile. |

## Setting Profiles to Anonymous Mode

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password, if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **call-home**<br>**Example:**<br>`Router(config)# call-home` | Enters Call Home configuration mode. |
| **Step 4** | **profile** *name*<br>**Example:**<br>`Router(cfg-call-home)# profile profile1` | Enters the Call Home destination profile configuration mode for the specified destination profile. If the specified destination profile does not exist, it is created. |
| **Step 5** | **anonymous-reporting-only**<br>**Example:** | Sets the profile to anonymous mode. |

| | Command or Action | Purpose |
|---|---|---|
| | `Router(cfg-call-home-profile)# anonymous-reporting-only` | **Note** By default, the profile sends a full report of all types of events that are subscribed in the profile. When **anonymous-reporting-only** is set, only crash, inventory, and test messages are sent. |

## Subscribing to Alert Groups

An alert group is a predefined subset of Call Home alerts that are supported. A destination profile can receive one or more selected alert groups.

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

The triggering events for each alert group are listed in the Alert Groups Trigger Events and Commands, and the contents of the alert group messages are listed in the Message Contents.

**Note** Call Home alerts are only sent to destination profiles that have subscribed to the alert group containing that Call Home alert. The alert group must be enabled. The Call Home event severity must be at or above the message severity set in the destination profile.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password, if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **call-home**<br>**Example:** | Enters Call Home configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| | `Router(config)# call-home` | |
| **Step 4** | **alert-group** { **all** \| **configuration** \| **crash** \| **diagnostic** \| **environment** \| **inventory** \| **snapshot** \| **syslog** }<br>**Example:**<br>`Router(cfg-call-home)# alert-group all` | Enables the specified alert group. Use the keyword **all** to enable all alert groups. By default, all alert groups are enabled. |
| **Step 5** | **profile** *name*<br>**Example:**<br>`Router(cfg-call-home)# profile profile1` | Enters the Call Home destination profile configuration mode for the specified destination profile. If the specified destination profile does not exist, it is created. |
| **Step 6** | **subscribe-to-alert-group configuration** [ **periodic** { **daily** *hh:mm* \| **monthly** *date hh:mm* \| **weekly** *day hh:mm* } ]<br>**Example:**<br>`Router(cfg-call-home-profile)# subscribe-to-alert-group configuration periodic daily 12:00` | Subscribes this destination profile to the Configuration alert group. The Configuration alert group can be configured for periodic notification. |
| **Step 7** | **subscribe-to-alert-group crash**<br>**Example:**<br>`Router(cfg-call-home-profile)# subscribe-to-alert-group crash` | Subscribes to the Crash alert group in the user profile. By default, Cisco TAC profile subscribes to the Crash alert group and cannot be unsubscribed. |
| **Step 8** | **subscribe-to-alert-group diagnostic** [ **severity** { **catastrophic** \| **disaster** \| **fatal** \| **critical** \| **major** \| **minor** \| **warning** \| **notification** \| **normal** \| **debugging** } ]<br>**Example:**<br>`Router(cfg-call-home-profile)# subscribe-to-alert-group syslog severity major` | Subscribes this destination profile to the Diagnostic alert group. The Diagnostic alert group can be configured to filter messages based on severity. |
| **Step 9** | **subscribe-to-alert-group environment** [ **severity** { **catastrophic** \| **disaster** \| **fatal** \| **critical** \| **major** \| **minor** \| **warning** \| **notification** \| **normal** \| **debugging** } ]<br>**Example:**<br>`Router(cfg-call-home-profile)# subscribe-to-alert-group environment severity major` | Subscribes this destination profile to the Environment alert group. The Environment alert group can be configured to filter messages based on severity. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 10** | **subscribe-to-alert-group inventory** [ **periodic** { **daily** *hh:mm* \| **monthly** *date hh:mm* \| **weekly** *day hh:mm* } ]<br>**Example:**<br>`Router(cfg-call-home-profile)# subscribe-to-alert-group inventory periodic daily 12:00` | Subscribes this destination profile to the Inventory alert group. The Inventory alert group can be configured for periodic notification. |
| **Step 11** | **subscribe-to-alert-group snapshot** [ **periodic** { **daily** *hh:mm* \| **monthly** *date hh:mm* \| **weekly** *day hh:mm* \| **hourly** *mm* \| **interval** *mm* } ]<br>**Example:**<br>`Router(cfg-call-home-profile)# subscribe-to-alert-group snapshot periodic daily 12:00` | Subscribes this destination profile to the Snapshot alert group. The Snapshot alert group can be configured for periodic notification.<br>By default, the Snapshot alert group has no command to run. You can add commands into the alert group. The output of commands that are added in the Snapshot alert group are included in the snapshot message. |
| **Step 12** | **subscribe-to-alert-group syslog** [ **severity** { **catastrophic** \| **disaster** \| **fatal** \| **critical** \| **major** \| **minor** \| **warning** \| **notification** \| **normal** \| **debugging** } ] [ **pattern** *string* ]<br>**Example:**<br>`Router(cfg-call-home-profile)# subscribe-to-alert-group syslog severity major` | Subscribes this destination profile to the Syslog alert group. The Syslog alert group can be configured to filter messages based on the severity. You can specify a pattern to be matched in the syslog message. If the pattern contains spaces, you must enclose it in quotes (").<br>You can specify a text pattern to be matched within each syslog message. If you configure a pattern, a Syslog alert group message is sent only if it contains the specified pattern and meets the severity threshold. If the pattern contains spaces, you must enclose it in quotes ("). You can specify up to five patterns for each destination profile. |
| **Step 13** | **subscribe-to-alert-group all**<br>**Example:**<br>`Router(cfg-call-home-profile)# subscribe-to-alert-group all` | (Optional) Subscribes to all available alert groups.<br>**Important** Entering this command generates many syslog messages. We recommend that you subscribe to alert groups individually, using appropriate severity levels and patterns when possible. |

## Periodic Notification

For destination profile subscriptions to either the Configuration, Inventory, or Snapshot alert group, you can choose to receive the alert group messages asynchronously or periodically. The following time intervals are available:

- Daily—Specify the time of day to send, using an hour:minute format *hh:mm*, with a 24-hour clock (for example, 14:30).
- Weekly—Specify the day of the week and time of day in the format day *hh:mm*. 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*.
- Interval—Specifies the interval at which the periodic message is sent, from 1 to 60 minutes.
- Hourly—Specifies the minute of the hour at which the periodic message is sent, from 0 to 59 minutes.

**Note** Hourly and by interval periodic notifications are available for the Snapshot alert group only.

## Message Severity Threshold

Call Home allows you to filter messages based on the severity. You can associate each predefined or user-defined destination profile with a Call Home threshold from 0 (least urgent) to 9 (most urgent). The default is 0 (all messages are sent).

When subscribing a destination profile to the Environment or Syslog alert group, set a threshold for relay of alert group messages. The threshold can be based on the message severity level. Messages with a value lower than the destination profile threshold is not sent to the destination.

Subscribing to an alert group in a destination profile with a specified severity also includes messages. Events that have same or higher severity in that alert group trigger these messages.

**Note** Subscribing to syslog message with a low severity level is not recommended. This subscription would trigger too many syslog messages that would lower the system performance.

**Note** Call Home severity levels and severity levels of the system message logging are different.

***Table 2: Severity and Syslog Level Mapping***

| Smart Call Home Level | Keyword | Syslog Level | Description |
|---|---|---|---|
| 9 | **catastrophic** | — | Network-wide catastrophic failure. |
| 8 | **disaster** | — | Significant network impact. |
| 7 | **fatal** | Emergency (0) | System is unusable. |
| 6 | **critical** | Alert (1) | Critical conditions that indicate that immediate attention is needed. |
| 5 | **major** | Critical (2) | Major conditions. |

| Smart Call Home Level | Keyword | Syslog Level | Description |
|---|---|---|---|
| 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. |

### 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 is 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. You can specify up to five patterns for each destination profile.

### Configuring Snapshot Command List

To configure the snapshot command list, perform the following steps:

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`Device#`<br>**`configure terminal`** | Enters global configuration mode. |
| **Step 2** | **call-home**<br>**Example:**<br>`Device(config)#`<br>**`call-home`** | Enters Call Home configuration mode. |
| **Step 3** | [ **no** \| **default** ] **alert-group-config snapshot**<br>**Example:**<br>`Device(cfg-call-home)#`<br>**`alert-group-config snapshot`** | Enters snapshot configuration mode.<br>The **no** or **default** command removes the snapshot command. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 4** | [ **no** \| **default** ] **add-command** *command string*<br>**Example:**<br>`Device(cfg-call-home-snapshot)# add-command "show version"` | Adds the command to the Snapshot alert group. The **no** or **default** command removes the corresponding command.<br>• *command string* —Cisco IOS command. Maximum length is 128. |
| **Step 5** | **end**<br>**Example:**<br>`Device(cfg-call-home-snapshot)# exit` | Exits and saves the configuration. |

## Configuring General Email Options

### Configuring the Mail Server

To use the email message transport, you must configure at least one Simple Mail Transfer Protocol (SMTP) email server address. You can specify up to four backup email servers, for a maximum of five total mail-server definitions.

Consider the following guidelines when configuring the mail server:

- Backup email 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) is tried first.

To configure general email options, perform the following steps:

#### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 2** | **call-home**<br>**Example:**<br>`Device(config)#` | Enters call home configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| | `call-home` | |
| **Step 3** | **mail-server** { *ipv4-address* \| *name* } **priority** *number*<br>**Example:**<br>`Device(cfg-call-home)# mail-server stmp.example.com priority 1` | Assigns an email server address and its relative priority among configured email servers.<br>Provide either of the following:<br>• The email server's IP address or<br>• The email server's fully qualified domain name (FQDN) of 64 characters or less.<br>Assign a priority number between 1 (highest priority) and 100 (lowest priority). |
| **Step 4** | **sender from** *email-address*<br>**Example:**<br>`Device(cfg-call-home)# sender from username@example.com` | (Optional) Assigns the email address that appears in the from field in Call Home email messages. If no address is specified, the contact email address is used. |
| **Step 5** | **sender reply-to** *email-address*<br>**Example:**<br>`Device(cfg-call-home)# sender reply-to username@example.com` | (Optional) Assigns the email address that appears in the reply-to field in Call Home email messages. |
| **Step 6** | **source-interface** *interface-name*<br>**Example:**<br>`Device(cfg-call-home)# source-interface loopback1` | Assigns the source interface name to send call-home messages.<br>*interface-name* —Source interface name. Maximum length is 64.<br>**Note** For HTTP messages, use the **ip http client source-interface** *interface-name* command in global configuration mode to configure the source interface name. This command allows all HTTP clients on the device to use the same source interface. |
| **Step 7** | **source-ip-address** *ipv4/ipv6 address*<br>**Example:**<br>`Device(cfg-call-home)#` | Assigns source IP address to send call-home messages.<br>• *ipv4/ipv6 address* —Source IP (IPv4 or IPv6) address. Maximum length is 64. |

| | Command or Action | Purpose |
|---|---|---|
| | **ip-address 209.165.200.226** | |
| **Step 8** | **vrf** *vrf-name*<br>**Example:**<br>`Device(cfg-call-home)#`<br>**vrf**<br>*vpn1* | (Optional) Specifies the VRF instance to send call-home email messages. If no vrf is specified, the global routing table is used.<br>**Note** For HTTP messages, if the source interface is associated with a VRF, use the **ip http client source-interface** *interface-name* command in global configuration mode. This command would specify the VRF instance that is used for all HTTP clients on the device. |

## Specifying Rate Limit for Sending Call Home Messages

To specify the rate limit for sending Call Home messages, perform the following steps:

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`Device#`<br>**configure terminal** | Enters global configuration mode. |
| **Step 2** | **call-home**<br>**Example:**<br>`Device(config)#`<br>**call-home** | Enters call home configuration mode. |
| **Step 3** | **rate-limit** *number*<br>**Example:**<br>`Device(cfg-call-home)#`<br>**rate-limit 40** | Specifies a limit on the number of messages that are sent per minute.<br>• *number* —Range 1 to 60. The default is 20. |

## Specifying HTTP Proxy Server

To specify an HTTP proxy server for sending Call Home HTTP(S) messages to a destination, perform the following steps:

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 2** | **call-home**<br>**Example:**<br>`Device(config)# call-home` | Enters call home configuration mode. |
| **Step 3** | **http-proxy** {*ipv4-address* \| *ipv6-address name*} *name*<br>**Example:**<br>`Device(config)# http-proxy 10.1.1.1 port 1` | Specifies the proxy server for the HTTP request. |

## Enabling AAA Authorization to Run Cisco IOS Commands for Call Home Messages

To enable AAA authorization to run Cisco IOS commands that enable the collection of output for a Call Home message, perform the following steps:

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 2** | **call-home**<br>**Example:**<br>`Device(config)# call-home` | Enters call home configuration mode. |
| **Step 3** | **aaa-authorization**<br>**Example:**<br>`Device(cfg-call-home)# aaa-authorization` | Enables AAA authorization.<br>**Note** By default, AAA authorization is disabled for Call Home. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 4** | **aaa-authorization** [ **username** *username* ]<br>**Example:**<br>`Device(cfg-call-home)#`<br>**`aaa-authorization username`** *`username`* | Specifies the username for authorization.<br>• **username** *user* —Default username is callhome. Maximum length is 64. |

## Configuring Syslog Throttling

To enable or disable Call Home syslog message throttling and avoid sending repetitive Call Home syslog messages, perform the following steps:

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`Device#`<br>**`configure terminal`** | Enters global configuration mode. |
| **Step 2** | **call-home**<br>**Example:**<br>`Device(config)#`<br>**`call-home`** | Enters call home configuration mode. |
| **Step 3** | [ **no** ] **syslog-throttling**<br>**Example:**<br>`Device(cfg-call-home)#`<br>**`syslog-throttling`** | Enables or disables Call Home syslog message throttling and avoids sending repetitive Call Home syslog messages. By default, syslog message throttling is enabled. |

## Configuring Call Home Data Privacy

The **data-privacy** command scrubs data, such as passwords and IP addresses, from running configuration files to protect the privacy of customers. Enabling the **data-privacy** command can affect CPU utilization when scrubbing a large amount of data. Currently, **show** command output is not being scrubbed except for configuration messages in the **show running-config** all and show startup-config data.

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`Device#`<br>**`configure terminal`** | Enters global configuration mode. |
| **Step 2** | **call-home**<br>**Example:**<br>`Device(config)#`<br>**`call-home`** | Enters call home configuration mode. |
| **Step 3** | **data-privacy** { **level** {**normal** \| **high** } \| **hostname** }<br>**Example:**<br>`Device(cfg-call-home)#`<br>**`data-privacy level high`** | Scrubs data from running configuration file to protect the privacy of the user. The default data-privacy level is normal.<br>**Note** Enabling the data-privacy command can affect CPU utilization when scrubbing a large amount of data.<br>• **normal** —Scrubs sensitive data such as passwords.<br>• **high** —Scrubs all normal-level commands plus the IP domain name and IP address commands.<br>• **hostname** —Scrubs all high-level commands plus the hostname command.<br>**Note** Scrubbing the hostname from configuration messages can cause Smart Call Home processing failure on some platforms. |

# Sending Call Home Messages Manually

## Sending a Call Home Test Message Manually

You can use the **call-home test** command to send a user-defined Call Home test message.

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **call-home test** [ **"** *test-message* **"** ] **profile** *name* | Sends a test message to the specified destination profile. The user-defined test message text is |

| | Command or Action | Purpose |
|---|---|---|
| | **Example:**<br>`Router#`<br>**`call-home test profile profile1`** | optional, but must be enclosed in quotes (“ ”) if it contains spaces. If no user-defined message is configured, a default message is sent. |

## Sending Call Home Alert Group Messages Manually

### Before you begin

- Only the snapshot, crash, configuration, and inventory alert groups can be sent manually. Syslog alert groups cannot be sent manually.
- When you manually trigger a snapshot, configuration, or inventory 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 snapshot, configuration, or inventory 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.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Router>` **`enable`** | Enables privileged EXEC mode.<br>• Enter your password, if prompted. |
| **Step 2** | **call-home send alert-group snapshot** [ **profile** *name* ]<br>**Example:**<br>`Router#` **`call-home send alert-group snapshot profile profile1`** | Sends a snapshot alert group message to one destination profile if specified, or to all subscribed destination profiles. |
| **Step 3** | **call-home send alert-group crash** [ **profile** *name* ]<br>**Example:**<br>`Router#` **`call-home send alert-group configuration profile profile1`** | Sends a crash alert group message to one destination profile if specified, or to all subscribed destination profiles. |
| **Step 4** | **call-home send alert-group configuration** [ **profile** *name* ]<br>**Example:**<br>`Router#` **`call-home send alert-group configuration profile profile1`** | Sends a configuration alert group message to one destination profile if specified, or to all subscribed destination profiles. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 5** | **call-home send alert-group inventory** [ **profile** *name* ]<br>**Example:**<br>`Router# call-home send alert-group inventory` | Sends an inventory alert group message to one destination profile if specified, or to all subscribed destination profiles. |

## Submitting Call Home Analysis and Report Requests

The **call-home request** command allows you to submit the system information to Cisco Systems. The report provides helpful analysis and information specific to your system. You can request various reports, including security alerts, known bugs, recommendations, and the command references.

Note the following guidelines when manually sending Call Home analysis and report requests:

- If a **profile** *name* is specified, the request is sent to the profile. If no profile is specified, the request is sent to the Cisco TAC profile. The Call-home request can have a recipient profile that is not enabled. The recipient profile specifies the email address where the transport gateway is configured. The recipient profile allows the request message to be forwarded to the Cisco TAC and you can receive the reply from the Smart Call Home service.
- The **ccoid** *user-id* is the registered identifier of the Smart Call Home user. If the *user-id* is specified, the response is sent to the email address of the registered user. If no *user-id* is specified, the response is sent to the contact email address of the device.
- Based on the keyword specifying the type of report that is requested, the following information is returned:
  - **config-sanity** —Information on the recommendations for 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. The PSIRT includes End of Life (EOL) or End of Sales (EOS) notices, or field notices (FN) that may affect devices in your network.

To submit a request for analysis and report information from the Cisco Output Interpreter tool, complete the following steps:

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **call-home request output-analysis** " *show-command* "<br>**Example:**<br>`[`<br>`profile` | Sends the output of the specified **show** command for analysis. The **show** command must be contained in quotes ("). |

| | Command or Action | Purpose |
|---|---|---|
| | *name*<br>] [<br>**ccoid**<br><br>*user-id*<br>]<br>**Example:**<br><br>Device#<br>**call-home request output-analysis "show diag" profile TG** | |
| **Step 2** | **call-home request** { **config-sanity** \| **bugs-list** \| **command-reference** \| **product-advisory** }<br>**Example:**<br><br>[<br>**profile**<br><br>*name*<br>] [<br>**ccoid**<br><br>*user-id*<br>]<br>**Example:**<br><br>Device#<br>**call-home request config-sanity profile TG** | Sends the output of a predetermined set of commands, such as the **show running-config all** and **show version** commands, for analysis. In addition, the **call home request product-advisory** subcommand includes all inventory alert group commands. The keyword that is specified after the **call-home request** command specifies the type of report requested. |

### Manually Sending Command Output Message for One Command or a Command List

The **call-home send** command runs a CLI command and emails the command output to Cisco, or to an email address that is specified.

Note the following guidelines when sending the output of a command:

- The specified Cisco IOS command or list of Cisco IOS commands can be any run command, including commands for all modules. The command must be contained in quotes (").
- If the email option is selected using the "email" keyword and an email address is specified, the command output is sent to that address. If email or HTTP option is not specified, the output is sent in long-text format to the Cisco TAC (attach@cisco.com). The output has information on the specified service request number.

- Ensure that a service request number is provided if no “email” nor the “http” keyword is specified. The service request number is required for both long-text and XML message formats and is provided in the subject line of the email.
- If the HTTP option is specified without a profile name or destination URL, the CiscoTac-1 profile destination HTTP or HTTPS URL is used as the destination. The destination email address can be specified so that Smart Call Home can forward the message to the email address. You can specify the destination email address and the SR number, or you can specify either of them.
- If a profile is specified and the profile has callhome@cisco.com as one of its email destinations, you must use XML as the message format. If you use long-text format, an error message is displayed.

To execute a command and send the command output, complete the following step:

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Use one of the following commands:<br>• **call-home send** {*cli command* \| *cli list*} [**email** [**profile** *profile-name* \| *email*] [**msg-format** {**long-text** \| **xml**}]] [**tac-sevice-request** *SR#*]<br>• **call-home send** {*cli command* \| *cli list*} [**http** [**profile** *profile-name* \| *URL-dest*] [**destination-email-address** *email*]] [**tac-sevice-request** *SR#*]<br>**Example:**<br>`Router# call-home send "show version;show running-config show inventory" email support@example.com msg-format xml` | Executes the CLI or CLI list and sends output via email or HTTP.<br>• {*cli command* \| *cli list*}—Specifies the Cisco IOS command or list of Cisco IOS commands (separated by ‘;’). It can be any run command, including commands for all modules. The commands must be contained in quotes (").<br>• **email** [**profile** *profile-name* \| *email*] [**msg-format** {**long-text** \| **xml**}]<br>If the email option is chosen and a profile name is specified, the command output is sent to the email address configured in the profile. If an email address is specified, the command output is sent to the specified email address. The message is in long-text or XML format with the service request number in the subject. The profile name or email address, the service request number, or both must be specified. The service request number is required if the profile name or email address is not specified. The default is attach@cisco.com for long-text format and callhome@cisco.com for XML format.<br>• **http** [**profile** *profile-name* \| *URL-dest*] [**destination-email-address** *email*]<br>You can choose the HTTP option without a profile name or destination URL. The command output is in XML format and is sent to the Smart Call Home backend |

| | Command or Action | Purpose |
|---|---|---|
| | | server (URL specified in the TAC profile). If a profile name or destination URL is specified, the command output is sent to the destination URLs. The destination URLs can be configured in the profile (profile-name case), or the destination URL can be specified in the command.<br><br>**destination-email-address** *email* can be specified so that the backend server can forward the message to the email address. The email address, the service request number, or both must be specified.<br><br>• **tac-service-request** *SR#*<br><br>Specifies the service request number. The service request number is required if the email address is not specified. |

# Configuring Diagnostic Signatures

The Diagnostic Signatures feature downloads digitally signed signatures to devices. Diagnostic Signatures (DS) files are formatted files that collate knowledge of diagnostic events. DS files provide methods to troubleshoot them without a need to upgrade the Cisco software. The aim of DS is to deliver flexible intelligence that can detect and collect troubleshooting information. This information can be used to resolve known problems in customer networks.

## Prerequisites for Diagnostic Signatures

Before you download and configure diagnostic signatures (DSs) on a device, you must ensure that the following conditions are met:

- Ensure that you assign a diagnostic signature to the device. Refer to the “Diagnostic Signature Downloading” section for more information about how to assign DSs to devices.
- HTTP/Secure HTTP (HTTPS) transport is required for downloading DS files. Install the certification authority (CA) certificate to enable the authentication of the destination HTTPS server.

**Note** If you configure the trustpool feature, the CA certificate is not required.

# Information About Diagnostic Signatures

## Diagnostic Signature Overview

Diagnostic signatures (DS) for the Call Home system provides a flexible framework that allows the defining of new events and corresponding CLIs. DSs can analyze these events without upgrading the Cisco software.

DSs enable you to define more types of events and trigger types than the standard Call Home feature supports. The DS subsystem downloads and processes files on a device and also handles callbacks for diagnostic signature events.

The Diagnostic Signature feature downloads digitally signed signatures that are in the form of files to devices. DS files are formatted files that collate the knowledge of diagnostic events and provide methods to troubleshoot these events.

DS files contain XML data to specify the event description, and these files include CLI commands or scripts to perform required actions. Cisco or a third party digitally signs the DSs. The signing ensures their integrity, reliability, and security.

The structure of a DS file can be one of the following formats.

- Metadata-based simple signature. This format specifies the event type. The format also has information to match the event and perform actions such as collecting information by using the CLI. The signature can also change configurations on the device as a workaround for certain bugs.
- Embedded Event Manager (EEM) Tool Command Language (Tcl) script-based signature. This format specifies new events in the event register line and more action in the Tcl script.
- Combination of both the preceding formats.

The following basic information is contained in a DS file:

- ID (unique number)—unique key that represents a DS file that can be used to search a DS.
- Name (ShortDescription)—unique description of the DS file that can be used in lists for selection.
- Description—long description about the signature.
- Revision—version number, which increments when the DS content is updated.
- Event & Action—defines the event to be detected and the action to be performed after the event happens.

## Diagnostic Signature Downloading

To download the diagnostic signature (DS) file, you require the secure HTTP (HTTPS) protocol. If you have configured an email transport method to download files on your device, change your assigned profile transport method to HTTPS.

Cisco software uses a PKI Trustpool Management feature, and this feature is enabled by default. The trustpool feature creates a scheme to provision, store, and manage a pool of certificates from known certification authorities (CAs) on devices. The trustpool feature also installs the CA certificate automatically. The CA certificate is required for the authentication of the destination HTTPS servers.

There are two types of DS update requests to download DS files: regular and forced-download.

Regular download requests DS files that were recently updated. You can trigger a regular download request either by using a periodic configuration or by initiating an on-demand CLI. The regular download update

happens only when the version of the requested DS is different from the version of the DS on the device. Periodic download is only started after there is any DS assigned to the device from DS web portal. After the assignment, responses to the periodic inventory message from the same device will include a field. The field notifies the device to start its periodic DS download or an update. In a DS update request message, the status and revision number of the DS is included. However, only a DS with the latest revision number is downloaded.

Forced-download downloads a specific DS or a set of DSs. You can trigger the forced-download update request only by initiating an on-demand CLI. In a force-download update request, the latest version of the DS file is downloaded irrespective of the current DS file version on the device.

The DS file is digitally signed, and signature verification is performed on every downloaded DS file to make sure it is from a trusted source.

## Diagnostic Signature Signing

The diagnostic signature (DS) files are digitally signed before they are made available for downloading. The following methods are used for digitally signing DS files:

- Signing algorithm (Rivest Shamir and Adleman [RSA] 2048 bits).
- Request key pairs to the Abraxas system, which is the digital signing client.
- DS signed through the secure socket layer (SSL) through a code signing client, where the signature is embedded using XML tags.
- Public keys that are embedded in the DS subsystem (Cisco-signed, partner-signed, third-party signed) in the Cisco software. The digitally signed DS file contains the product name such as Diagnostic_Signatures (Cisco signed), Diagnostic_Signatures_Partner, Diagnostic_Signatures_3rd_Party. The product names are only used to sign the DS files.

The digital signing client can be found at the https://abraxas.cisco.com/SignEngine/submit.jsp link.

These conditions that must be met to verify the digital signature in a DS file:

- Code sign component support must be available in Cisco software.
- Various public keys that verify the different kinds of diagnostic signatures must be included in platforms where DS is supported.
- After parsing and retrieving the DS, the DS must execute the verification application program interface (API) to verify that the DS is valid.

## Diagnostic Signature Workflow

The diagnostic signature feature is enabled by default in Cisco software. The following is the workflow for creating diagnostic signatures:

1. Find the DSs you want to download and assign them to the device. This step is mandatory for a regular periodic download, but not required for a forced download.
2. The device downloads every assigned DS or a specific DS by regular periodic download or by on-demand forced download.
3. The device verifies the digital signature of every DS. After verification, the device stores the DS file into a nonremovable disk. This nonremovable disk can be a bootflash or hard disk, where that DS files can be read after the device is reloaded. On the routers, the DS file is stored in the bootflash:/call home directory.

4. The device continues sending periodic regular DS download requests to get the latest revision of DS and replace the older one in the device.
5. The device monitors the event and executes the actions that are defined in the DS when the event happens.

## Diagnostic Signature Events and Actions

The events and actions sections are the key areas that are used in diagnostic signatures. The event section defines all event attributes that are used for the event detection. The action section lists all the steps to be completed after the event. The actions include collecting **show** command outputs and sending them to Smart Call Home to parse.

### Diagnostic Signature Event Detection

Event detection in a DS is defined in two ways: single event detection and multiple event detection.

#### Single Event Detection

In single event detection, only one event detector is defined within a DS. The event specification format is one of the following two types:

- DS event specification type: syslog, periodic, configuration, Online Insertion Removal (OIR) immediate, and callhome are the supported event types, where “immediate” indicates that this type of DS does not detect any events, its actions are performed once it is downloaded, and the call-home type modifies the current CLI commands defined for existing alert-group.
- The Embedded Event Manager (EEM) specification type: supports any new EEM event detector without having to modify the Cisco software.

  Other than using EEM to detect events, a DS is triggered when a Tool Command Language (Tcl) script is used to specify event detection types.

#### Multiple Event Detection

Multiple event detection involves defining two or more event detectors, two ore more corresponding tracked object states, and a time period for the events to occur. The specification format for multiple event detection can include complex event correlation for tracked event detectors. For example, three event detectors (syslog, OIR, and IPSLA) are defined during the creation of a DS file. The correlation that is specified for these event detectors is that the DS will execute its action if both syslog and OIR events are triggered simultaneously, or if IPSLA is triggered alone.

### Diagnostic Signature Actions

The diagnostic signature (DS) file consists of various actions that must be initiated when an evnt occurs. The action type indicates the kind of action that will be initiated in response to a certain event.

Variables are elements within a DS file that are used to customize the files.

DS actions are categorized into the following five types:

- call-home
- command
- emailto
- script
- message

DS action types call-home and emailto collect event data and send a message to call-home servers or to the defined email addresses. The message uses "diagnostic-signature" as its message type and DS ID as the message sub-type.

The commands defined for the DS action type initiate CLI commands that can change configuration of the device, collect show command outputs, or run any EXEC command on the device. The DS action type script executes Tcl scripts.

DS action type message defines action to generate message to notify or remind user certain important information. The message could be broadcasted to all TTY lines or generated as a syslog entry.

### *Action Types*

DS actions are categorized into the following four types:

- Call-home
- Command
- Emailto
- Script

DS action types call-home and emailto collect event data and send a message to call-home servers or to the defined email addresses. The message includes the following elements:

- Message type—diagnostic-signature
- Message subtype—ds-id
- Message description—event-id : ds name

The commands defined for the DS action type initiates CLI commands that can change configuration of the device. The DS action type script executes Tcl scripts.

### *Diagnostic Signature Variables*

Variables are referenced within a DS and are used to customize the DS file. All DS variable names have the prefix ds_ to separate them from other variables. The following are the supported DS variable types:

- System variable: variables assigned automatically by the device without any configuration changes. The Diagnostic Signatures feature supports two system variables: ds_hostname and ds_signature_id.
- Environment variable: values assigned manually by using the **environment** *variable-name variable-value* command in call-home diagnostic-signature configuration mode. Use the **show call-home diagnostic-signature** command to display the name and value of all DS environment variables. If the DS file contains unresolved environment variables, this DS will stay in pending status until the variable gets resolved.
- Prompt variable: values assigned manually by using the **call-home diagnostic-signature install** *ds-id* command in privileged EXEC mode. If you do not set this value, the status of the DS indicates pending.
- Regular expression variable: values assigned from a regular expression pattern match with predefined CLI command outputs. The value is assigned during the DS run.
- Syslog event variable: values assigned during a syslog event detection in the DS file. This variable is valid only for syslog event detection.

# How to Configure Diagnostic Signatures

## Configuring the Service Call Home for Diagnostic Signatures

Configure the Service Call Home feature to set attributes such as the contact email address where notifications related with diagnostic signatures (DS) are sent and destination HTTP/secure HTTP (HTTPS) URL to download the DS files from.

You can also create a new user profile, configure correct attributes, and assign it as the DS profile. For periodic downloads, the request is sent out just following full inventory message. By changing the inventory periodic configuration, the DS periodic download also gets rescheduled.

**Note** The predefined CiscoTAC-1 profile is enabled as a DS profile by default and Cisco recommends using it. Ensure that you change the destination transport-method to the **http** setting, when you use the predefined CiscoTAC-1 profile.

### Before you begin

Before you download and configure diagnostic signatures (DSs) on a device, you must ensure that the following conditions are met:

- Assign one or more DSs to the device.
- HTTP/Secure HTTP (HTTPS) transport is required for downloading DS files. Install the certification authority (CA) certificate to enable the authentication of the destination HTTPS server.

**Note** If you configure the trustpool feature, the CA certificate is not required.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password, if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **service call-home**<br>**Example:**<br>`Router(config)# service call-home` | Enables Call Home service on a device. |
| **Step 4** | **call-home**<br>**Example:** | Enters Call Home configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| | `Router(config)# call-home` | |
| **Step 5** | **contact-email-addr** *email-address*<br>**Example:**<br>`Router(cfg-call-home)# contact-email-addr username@example.com` | Assigns customer's email address. You can enter a maximum of 200 characters in email address format with no spaces.<br>**Note** You can use any valid email address. You cannot use spaces. |
| **Step 6** | **mail-server** { *ipv4-address* \| *name* } **priority** *number*<br>**Example:**<br>`Router(cfg-call-home)# mail-server 10.1.1.1 priority 4` | (Optional) Configures a Simple Mail Transfer Protocol (SMTP) email server address for Call Home. This command is only used when sending email is part of the actions that are defined in any DS. |
| **Step 7** | **profile** *name*<br>**Example:**<br>`Router(cfg-call-home)# profile profile1` | Enters the Call Home destination profile configuration mode for the specified destination profile. If the specified destination profile does not exist, it is created. |
| **Step 8** | **destination transport-method** { **email** \| **http** }<br>**Example:**<br>`Router(cfg-call-home-profile)# destination transport-method email` | (Optional) Enables the message transport method.<br>• **email** —Sets the email message transport method.<br>• **http** —Sets the HTTP message transport method.<br>**Note** To configure diagnostic signatures, you must use the **http** option. |
| **Step 9** | **destination address** { **email** *email-address* \| **http** *url* }<br>**Example:**<br>`Router(cfg-call-home-profile)# destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService` | Configures the destination email address or URL to which Call Home messages are sent.<br>**Note** To configure diagnostic signatures, you must use the **http** option. |
| **Step 10** | **subscribe-to-alert-group inventory** [ **periodic** { **daily** *hh:mm* \| **monthly** *date hh:mm* \| **weekly** *day hh:mm* } ]<br>**Example:**<br>`Router(cfg-call-home-profile)# subscribe-to-alert-group inventory periodic daily 12:00` | Subscribes this destination profile to the Inventory alert group. The Inventory alert group can be configured for periodic notification.<br>**Note** This command is used only for the periodic downloading of DS files. |

### What to do next

Set the configured profile from the previous procedure as the DS profile and configure other DS parameters.

## Configuring Diagnostic Signatures

### Before you begin

Configure the Service Call Home feature to set attributes for the Call Home profile. You can either use the default CiscoTAC-1 profile or use the newly created user profile.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password, if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **call-home**<br>**Example:**<br>`Router(config)# call-home` | Enters Call Home configuration mode. |
| **Step 4** | **diagnostic-signature**<br>**Example:**<br>`Router(cfg-call-home)# diagnostic-signature` | Enters call-home diagnostic signature mode. |
| **Step 5** | **profile** *ds-profile-name*<br>**Example:**<br>`Router(cfg-call-home-diag-sign)# profile user1` | Specifies the destination profile on a device that DS uses. |
| **Step 6** | **environment** *ds_env-var-name ds-env-var-value*<br>**Example:**<br>`Router(cfg-call-home-diag-sign)# environment ds_env1 envarval` | Sets the environment variable value for DS on a device. |
| **Step 7** | **end**<br>**Example:**<br>`Router(cfg-call-home-diag-sign)# end` | Exits call-home diagnostic signature mode and returns to privileged EXEC mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 8** | **call-home diagnostic-signature** { { **deinstall** \| **download** } { *ds-id* \| **all** } \| **install** *ds-id* }<br>**Example:**<br>`Router# call-home diagnostic-signature download 6030` | Downloads, installs, and uninstalls diagnostic signature files on a device. |
| **Step 9** | **show call-home diagnostic-signature** [ *ds-id* [ **actions** \| **events** \| **prerequisite** \| **prompt** \| **variables** ] \| **failure** \| **statistics** [ download ] ]<br>**Example:**<br>`Router# show call-home diagnostic-signature actions` | Displays the call-home diagnostic signature information. |

# Verifying the Call Home Configuration

- **show call-home** —Displays the Call Home configuration summary.

  Following is a sample output of the command:

```
Router# show call-home

Current call home settings:
    call home feature : enable
    call home message's from address: Not yet set up
    call home message's reply-to address: Not yet set up

    vrf for call-home messages: Not yet set up

    contact person's email address: sch-smart-licensing@cisco.com (default)

    contact person's phone number: Not yet set up
    street address: Not yet set up
    customer ID: Not yet set up
    contract ID: Not yet set up
    site ID: Not yet set up

    source ip address: Not yet set up
    source interface: TenGigabitEthernet4/1/1
    Mail-server[1]: Address: 173.36.13.143 Priority: 60
    http proxy: Not yet set up

    Diagnostic signature: enabled
    Profile: CiscoTAC-1 (status: ACTIVE)

    Smart licensing messages: enabled
    Profile: CiscoTAC-1 (status: ACTIVE)

    aaa-authorization: disable
    aaa-authorization username: callhome (default)
    data-privacy: normal
    syslog throttling: enable
```

```
    Rate-limit: 20 message(s) per minute

    Snapshot command[0]: show cable modem summary totalb
    Snapshot command[1]: show cable modem summary total

Available alert groups:
    Keyword                  State   Description
    ------------------------ ------- --------------------------------
    configuration            Enable  configuration info
    crash                    Enable  crash and traceback info
    diagnostic               Enable  diagnostic info
    environment              Enable  environmental info
    inventory                Enable  inventory info
    snapshot                 Enable  snapshot info
    syslog                   Enable  syslog info

Profiles:
    Profile Name: CiscoTAC-1
    Profile Name: test
```

- **show call-home detail**—Displays the Call Home configuration in detail.

  Following is a sample output of the command:

```
Router# show call-home detail

Current call home settings:
    call home feature : enable
    call home message's from address: Not yet set up
    call home message's reply-to address: Not yet set up

    vrf for call-home messages: Not yet set up

    contact person's email address: sch-smart-licensing@cisco.com (default)

    contact person's phone number: Not yet set up
    street address: Not yet set up
    customer ID: Not yet set up
    contract ID: Not yet set up
    site ID: Not yet set up

    source ip address: Not yet set up
    source interface: TenGigabitEthernet4/1/1
    Mail-server[1]: Address: 173.36.13.143 Priority: 60
    http proxy: Not yet set up

    Diagnostic signature: enabled
    Profile: CiscoTAC-1 (status: ACTIVE)

    Smart licensing messages: enabled
    Profile: CiscoTAC-1 (status: ACTIVE)

    aaa-authorization: disable
    aaa-authorization username: callhome (default)
    data-privacy: normal
    syslog throttling: enable

    Rate-limit: 20 message(s) per minute

    Snapshot command[0]: show cable modem summary totalb
    Snapshot command[1]: show cable modem summary total

Available alert groups:
    Keyword                  State   Description
```

```
    ------------------------ ------- --------------------------------
    configuration            Enable  configuration info
    crash                    Enable  crash and traceback info
    diagnostic               Enable  diagnostic info
    environment              Enable  environmental info
    inventory                Enable  inventory info
    snapshot                 Enable  snapshot info
    syslog                   Enable  syslog info

Profiles:

Profile Name: CiscoTAC-1
    Profile status: ACTIVE
    Profile mode: Anonymous Reporting Only
    Reporting Data: Smart Call Home, Smart Licensing
    Preferred Message Format: xml
    Message Size Limit: 3145728 Bytes
    Transport Method: http
    Email address(es): callhome@cisco.com
    HTTP  address(es): https://tools.cisco.com/its/service/oddce/services/DDCEService

   Periodic configuration info message is scheduled every 17 day of the month at 09:39


    Periodic inventory info message is scheduled every 17 day of the month at 09:24

    Alert-group              Severity
    -----------------------  ------------
    crash                    debug
    diagnostic               minor
    environment              minor
    inventory                normal

    Syslog-Pattern           Severity
    -----------------------  ------------
    .*                       major
```

- **show call-home alert-group** —Displays the available alert groups and their status.

  Following is a sample output of the command:

```
Router# show call-home alert-group

Available alert groups:
    Keyword                  State   Description
    ------------------------ ------- --------------------------------
    configuration            Enable  configuration info
    crash                    Enable  crash and traceback info
    diagnostic               Enable  diagnostic info
    environment              Enable  environmental info
    inventory                Enable  inventory info
    snapshot                 Enable  snapshot info
    syslog                   Enable  syslog info
```

- **show call-home mail-server status**—Checks and displays the availability of the configured email servers.

  Following is a sample output of the command:

```
Router# show call-home mail-server status

    Mail-server[1]: Address: 173.36.13.143 Priority: 60
```

- **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.

  Following is a sample output of the command:

```
Router# show call-home profile CiscoTac-1

Profile Name: CiscoTAC-1
    Profile status: ACTIVE
    Profile mode: Full Reporting
    Reporting Data: Smart Call Home, Smart Licensing
    Preferred Message Format: xml
    Message Size Limit: 3145728 Bytes
    Transport Method: email
    Email address(es): callhome@cisco.com
    HTTP  address(es): http://10.22.183.117:8080/ddce/services/DDCEService

    Periodic configuration info message is scheduled every 17 day of the month at 09:39


    Periodic inventory info message is scheduled every 17 day of the month at 09:24

    Alert-group               Severity
    ------------------------  ------------
    crash                     debug
    diagnostic                minor
    environment               minor
    inventory                 normal

    Syslog-Pattern            Severity
    ------------------------  ------------
    .*                        major
```

- **show call-home statistics** [**detail** | **profile** *profile-name*]—Displays the statistics of Call Home events.

  Following is a sample output of the command:

```
Router# show call-home statistics

Message Types    Total                Email                HTTP
-------------   -------------------- -------------------- ------------------
Total Success   4                    3                    1
    Config      1                    1                    0
    Crash       0                    0                    0
    Diagnostic  0                    0                    0
    Environment 0                    0                    0
    Inventory   1                    0                    1
    Snapshot    0                    0                    0
    SysLog      2                    2                    0
    Test        0                    0                    0
    Request     0                    0                    0
    Send-CLI    0                    0                    0
    SCH         0                    0                    0

Total In-Queue  0                    0                    0
    Config      0                    0                    0
    Crash       0                    0                    0
    Diagnostic  0                    0                    0
    Environment 0                    0                    0
    Inventory   0                    0                    0
    Snapshot    0                    0                    0
    SysLog      0                    0                    0
```

```
    Test        0                   0                   0
    Request     0                   0                   0
    Send-CLI    0                   0                   0
    SCH         0                   0                   0

Total Failed    0                   0                   0
    Config      0                   0                   0
    Crash       0                   0                   0
    Diagnostic  0                   0                   0
    Environment 0                   0                   0
    Inventory   0                   0                   0
    Snapshot    0                   0                   0
    SysLog      0                   0                   0
    Test        0                   0                   0
    Request     0                   0                   0
    Send-CLI    0                   0                   0
    SCH         0                   0                   0

Total Ratelimit
      -dropped  0                   0                   0
    Config      0                   0                   0
    Crash       0                   0                   0
    Diagnostic  0                   0                   0
    Environment 0                   0                   0
    Inventory   0                   0                   0
    Snapshot    0                   0                   0
    SysLog      0                   0                   0
    Test        0                   0                   0
    Request     0                   0                   0
    Send-CLI    0                   0                   0
    SCH         0                   0                   0

Last call-home message sent time: 2015-03-06 18:21:49 GMT+00:00
```

- **show call-home diagnostic-signature**—Displays the configuration of diagnostic signature information.

  Following is a sample output of the command:

```
Router# show call-home diagnostic-signature

Current diagnostic-signature settings:
 Diagnostic-signature: enabled
 Profile: CiscoTAC-1 (status: ACTIVE)
 Environment variable:
           Not yet set up

Downloaded DSes:
                                                                  Last Update
DS ID    DS Name                          Revision Status     (GMT-05:00)
-------- -------------------------------- -------- ---------- -------------------
```

- **show call-home version**—Displays the Call Home version information.

  Following is a sample output of the command:

```
Router# show call-home version

Call-Home Version 3.0
Component Version:
 call-home: (rel4)1.0.15
 eem-call-home: (rel2)1.0.5
```

# Configuration Example for Call Home

## Example: Call Home Configuration

Following is a configuration example for configuring the HTTPS transport:

```
ip host tools.cisco.com 72.163.4.38
vrf definition smart-vrf
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
interface TenGigabitEthernet4/1/1
 vrf forwarding smart-vrf
 ip address 172.22.11.25 255.255.255.128
 no ip proxy-arp
!
ip route vrf smart-vrf 72.163.4.38 255.255.255.255 172.22.11.1
!
ip http client source-interface TenGigabitEthernet4/1/1
!
```

Following is a configuration example for configuring email options:

```
call-home
 mail-server 173.36.13.143 priority 60
 source-interface TenGigabitEthernet4/1/1
 vrf smart-vrf
 alert-group-config snapshot
  add-command "show cable modem summary total"
 profile "test"
  active
  destination transport-method email
  destination address email call-home@cisco.com
  subscribe-to-alert-group configuration
  subscribe-to-alert-group crash
  subscribe-to-alert-group diagnostic severity debug
  subscribe-to-alert-group environment severity debug
  subscribe-to-alert-group inventory
  subscribe-to-alert-group syslog severity major pattern .*
  subscribe-to-alert-group syslog severity notification pattern "^.+UPDOWN.+changed state
to (down|up)$"
  subscribe-to-alert-group snapshot periodic daily 12:00
!
ip route vrf smart-vrf 173.36.13.143 255.255.255.255 172.22.11.1
!
```

# Example: Configuring HTTP Transport for Call Home on the Cisco cBR Series Router

### Procedure

**Step 1** Back up the current running configuration file.

**Step 2** Verify the built-in router certificates.

**Example:**

```
Router# show crypto pki trustpool | include Class 3 Public

    ou=Class 3 Public Primary Certification Authority
    ou=Class 3 Public Primary Certification Authority
```

**Step 3** (Optional) Configure VRF.

**Example:**

```
Router(config)# vrf def smart-vrf
Router(config-vrf)# address-family ipv4
Router(config-vrf-af)# exit-address-family
Router(config-vrf)# address-family ipv6
Router(config-vrf-af)# exit-address-family
```

**Step 4** Set up the network interface.

**Example:**

```
Router(config)# interface TenGigabitEthernet4/1/1
Router(config)# vrf forward smart-vrf
Router(config-if)# ip address 172.22.11.25 255.255.255.128
Router(config-if)# no ip proxy-arp
Router(config-if)# no shut
```

**Note** If IPv6 is enabled, you must configure the IPv6 address.

**Step 5** Set up the Cisco portal.

**Example:**

```
Router(config)# ip host tools.cisco.com 72.163.4.38
Router(config)# ip route vrf smart-vrf 72.163.4.38 255.255.255.255 172.22.11.1
```

**Step 6** Verify the data path.

**Example:**

```
!Verify the connectivity to TenGigabitEthernet4/1/1 interface
Router# ping vrf smart-vrf 172.22.11.25

!Verify the connectivity to TenGigabitEthernet4//1/1 gateway
Router# ping vrf smart-vrf 172.22.11.1

!Verify the connectivity to tools.cisco.com
Router# ping vrf smart-vrf 72.163.4.38
```

**Step 7** Configure the HTTP client interface.

**Example:**

```
Router(config)# ip http client source-interface TenGigabitEthernet4/1/1
```

**Step 8** Send the Call Home alert group message manually and verify the configuration.

**Example:**

```
Router# call-home send alert inventory profile CiscoTAC-1

Sending inventory info call-home message ...
Please wait. This may take some time ...

Router# show call-home statistics | include Total
Message Types    Total               Email               HTTP
Total Success   0                   0                   0
Total In-Queue  1                   0                   1
Total Failed    0                   0                   0
Total Ratelimit

Router# show call-home statistics | include Total
Message Types    Total               Email               HTTP
Total Success   1                   0                   1
Total In-Queue  0                   0                   0
Total Failed    0                   0                   0
Total Ratelimit
```

**Step 9** Display the Call Home configuration.

**Example:**

```
Router# show call-home profile CiscoTAC-1

Profile Name: CiscoTAC-1
    Profile status: ACTIVE
    Profile mode: Full Reporting
    Reporting Data: Smart Call Home, Smart Licensing
    Preferred Message Format: xml
    Message Size Limit: 3145728 Bytes
    Transport Method: http
    Email address(es): callhome@cisco.com
    HTTP  address(es): https://tools.cisco.com/its/service/oddce/services/DDCEService

    Periodic configuration info message is scheduled every 15 day of the month at 15:37

    Periodic inventory info message is scheduled every 15 day of the month at 15:22
Alert-group              Severity
    ------------------------  ------------
    crash                     debug
    diagnostic                minor
    environment               minor
    inventory                 normal

    Syslog-Pattern            Severity
    ------------------------  ------------
    .*                        major
```

# Example: Configuring Email Transport for Call Home on the Cisco cBR Series Router

**Procedure**

**Step 1** Back up the current running configuration file.

**Step 2** (Optional) Configure VRF.

**Example:**

```
Router(config)# vrf def smart-vrf
Router(config-vrf)# address-family ipv4
Router(config-vrf-af)# exit-address-family
Router(config-vrf)# address-family ipv6
Router(config-vrf-af)# exit-address-family
```

**Step 3** Set up the network interface.

**Example:**

```
Router(config)# interface TenGigabitEthernet4/1/1
Router(config)# vrf forward smart-vrf
Router(config-if)# ip address 172.22.11.25 255.255.255.128
Router(config-if)# no ip proxy-arp
Router(config-if)# no shut
```

**Note** If IPv6 is enabled, you must configure the IPv6 address.

**Step 4** Verify the data path.

**Example:**

```
!Verify the connectivity to TenGigabitEthernet4/1/1 interface
Router# ping vrf smart-vrf 172.22.11.25

!Verify the connectivity to TenGigabitEthernet4//1/1 gateway
Router# ping vrf smart-vrf 172.22.11.1

!Verify the connectivity to tools.cisco.com
Router# ping vrf smart-vrf 72.163.4.38
```

**Step 5** (Optional) Configure Call Home.

**Example:**

```
Router(config)# call-home

!Configure the TenGigabitEthernet 4/1/1
Router(cfg-call-home)# source-ip-address 172.22.11.25
```

**Step 6** Configure the mail server and verify the configuration.

**Example:**

```
Router(config)# call-home
Router(cfg-call-home)# mail-server 173.36.13.143 priority 60
Router(cfg-call-home)# vrf smart-vrf
```

```
Router(cfg-call-home)# exit
Router(config)# ip route vrf smart-vrf 173.36.13.143 255.255.255.255 172.22.11.1
Router(config)# end

Router# ping vrf smart-vrf 173.36.13.143
…

Router# show call-home mail status

Please wait. Checking for mail server status ...

Mail-server[1]: Address: 173.36.13.143 Priority: 60 [Available]
```

**Note** The VRF configuration is optional.

**Step 7** Create a new destination profile and subscribe to alert the group.

**Example:**

```
Router(config)# call-home
Router(cfg-call-home)# alert-group-config snapshot
Router(cfg-call-home-snapshot)# add-command "show cable modem summary total”
Router(cfg-call-home-snapshot)# exit
Router(cfg-call-home)# profile test
Router(cfg-call-home-profile)# active
Router(cfg-call-home-profile)# destination transport-method email
Router(cfg-call-home-profile)# destination address email xyz@company.com
Router(cfg-call-home-profile)# subscribe syslog severity notification pattern
"^.+UPDOWN.+changed state to (down|up)$”
Router(cfg-call-home-profile)# subscribe-to-alert-group snapshot periodic daily 12:00
Router(cfg-call-home-profile)# end
```

**Step 8** Send the Call Home alert group message manually and verify the configuration.

**Example:**

```
Router# call-home send alert-group inventory profile test
Sending inventory info call-home message ...
Please wait. This may take some time ...

Router# show call-home statistics | include Total
Message Types    Total               Email               HTTP
Total Success   1                   0                   1
Total In-Queue  2                   2                   0
Total Failed    0                   0                   0
Total Ratelimit

Router# show call-home statistics | include Total
Message Types    Total               Email               HTTP
Total Success   3                   2                   1
Total In-Queue  0                   0                   0
Total Failed    0                   0                   0
Total Ratelimit
```

**Step 9** Display the Call Home configuration.

**Example:**

```
Router# show call-home profile test

Profile Name: test
    Profile status: ACTIVE
```

```
    Profile mode: Full Reporting
    Reporting Data: Smart Call Home
    Preferred Message Format: xml
    Message Size Limit: 3145728 Bytes
    Transport Method: email
    Email address(es): abcd@company.com
    HTTP  address(es): Not yet set up

    Periodic snapshot info message is scheduled daily at 12:00

    Alert-group               Severity
    ------------------------  ------------
    configuration             normal
    crash                     debug
    diagnostic                debug
    environment               debug
    inventory                 normal
Syslog-Pattern            Severity
    ------------------------  ------------
    ^.+UPDOWN.+changed state
     to (down|up)$            notification
```

# Default Settings

*Table 3: Default Call Home Parameters*

| Parameters | Default |
|---|---|
| Call Home feature status | Enabled |
| User-defined profile status | Active |
| Predefined CiscoTAC-1 profile status | Active |
| Transport method | HTTP |
| Message-format type | XML |
| Alert group status | Enabled |
| Call Home message severity threshold | Debug |
| Message rate limit for messages per minute | 20 |
| AAA authorization | Disabled |
| Call Home syslog message throttling | Enabled |
| Data privacy level | Normal |

# Alert Groups Trigger Events and Commands

The following table lists the supported alert groups and the default command output. The command output is included in Call Home messages that are generated for the alert group.

*Table 4: Call Home Alert Groups, Events, and Actions*

| Alert Group | Call Home Trigger Event | Syslog Event | Severity | Description and Executed Commands |
|---|---|---|---|---|
| Configuration | — | — | **normal**<br>**periodic** | Periodic events that are related to configuration sent monthly.<br>Commands executed:<br>• **show platform**<br>• **show version**<br>• **show inventory**<br>• **show running-config all**<br>• **show startup-config** |

| Alert Group | Call Home Trigger Event | Syslog Event | Severity | Description and Executed Commands |
|---|---|---|---|---|
| Crash | — | — | **debug** | A router crash can generate events. For example, a Supervisor or line card crash.<br>Commands executed:<br>Crash traceback<br>• **show version**<br>• **show logging**<br>• **show region**<br>• **show stack**<br>Crash system<br>• **show version**<br>• **show inventory**<br>• **show logging**<br>• **show region**<br>• **show stack**<br>• **more crashinfo-file**<br>Crash module<br>• **show version**<br>• **show inventory**<br>• **show platform**<br>• **show logging**<br>• **show region**<br>• **show stack**<br>• **more crashinfo-file** |

| Alert Group | Call Home Trigger Event | Syslog Event | Severity | Description and Executed Commands |
|---|---|---|---|---|
| Diagnostic | — | — | **minor** | Diagnostics can generate events.<br>Commands executed:<br>• **show platform**<br>• **show version**<br>• **show diagnostic event slot detail**<br>• **show inventory**<br>• **show buffers**<br>• **show logging**<br>• **show diagnostic events slot all** |
| Environmental | FAN_FAILURE | CBR_PEM-6-FANOK<br>CBR_PEM-3-FANFAIL | **minor** | Events that are related to power, fan, and environment sensing elements, such as temperature alarms.<br>Commands executed:<br>• **show platform**<br>• **show environment**<br>• **show inventory**<br>• **show logging** |
| | TEMPERATURE_ALARM | ENVIRONMENTAL-1-ALERT | | |
| | POWER_SUPPLY_FAILURE | CBR_PEM-6-PEMOK<br>CBR_PEM-3-PEMFAIL | | |

| Alert Group | Call Home Trigger Event | Syslog Event | Severity | Description and Executed Commands |
|---|---|---|---|---|
| Inventory | OIR_REMOVE<br>OIR_INSERTION | — | **normal** | Inventory status that is provided whenever a unit is cold booted, or when FRUs are inserted or removed. This alert is considered as a noncritical event, and the information is used for status and entitlement.<br>Command executed:<br>• **show platform**<br>• **show version**<br>• **show inventory oid**<br>• **show diag all eeprom detail**<br>• **show interfaces**<br>• **show file systems**<br>• **show bootflash: all**<br>• **show data-corruption**<br>• **show memory statistics**<br>• **show process memory**<br>• **show process cpu**<br>• **show process cpu history**<br>• **show license udi**<br>• **show license detail**<br>• **show buffers**<br>• **show platform software proc slot monitor cycle** |
| Snapshot | — | — | **normal** | User-generated CLI commands. |
| Syslog | — | — | **major** | Syslog messages can generate events.<br>Commands executed:<br>• **show inventory**<br>• **show logging** |

| Alert Group | Call Home Trigger Event | Syslog Event | Severity | Description and Executed Commands |
|---|---|---|---|---|
| Test | — | — | **normal** | User-generated test message sent to the destination profile.<br>Commands executed:<br>• **show inventory**<br>• **show platform**<br>• **show version** |

# Message Contents

Smart Call Home supports the following message formats:

- Short Text Message Format
- Common Fields for Full Text and XML Messages
- Fields Specific to Alert Group Messages for Full Text and XML Messages
- Inserted Fields for a Reactive and Proactive Event Message
- Inserted Fields for an Inventory Event Message
- Inserted Fields for a User-Generated Test Message

The following table describes the short text formatting option for all the message types.

***Table 5: Short Text Message Format***

| Data Item | Description |
|---|---|
| Device identification | Configured device name. |
| Date and time stamp | Time stamp of the triggering event. |
| Error isolation message | Plain English description of triggering the event. |
| Alarm urgency level | Error level such as that applied to the system message. |

The following table describes the first set of common event message fields for full text or XML messages.

*Table 6: Common Fields for Full Text and XML Messages*

| Data Item (Plain Text and XML) | Description (Plain Text and XML) | Call-Home Message Tag (XML Only) |
|---|---|---|
| Time stamp | Date and time stamp of the event in the ISO time notation:<br>*YYYY-MM-DD HH:MM:SS GMT + HH:MM.* | CallHome/EventTime |
| Message name | Name of message. | For short text message only |
| Message type | Name of the message type, specifically "Call Home." | CallHome/Event/Type |
| Message subtype | Specific type of message: full, delta, test. | CallHome/Event/SubType |
| Message group | Name of the alert group, specifically "reactive." Optional, because the default is "reactive". | For long-text message only |
| Severity level | Severity level of message | Body/Block/Severity |
| Source ID | Product type for routing through the workflow engine. The Source ID is typically the product family name. | For long-text message only |
| Device ID | Unique device identifier (UDI) for the end device that generated the message. Ensure that the field is empty if the message is nonspecific to a device. The format is *type@Sid@serial*.<br>• The *type* is the product model number from the backplane IDPROM.<br>• @ is a separator character.<br>• *Sid* is C, identifying the serial ID as a chassis serial number.<br>• The Sid field identifies the *serial* number.<br>An example is WS-C6509@C@12345678. | CallHome/CustomerData/ContractData/DeviceId |
| Customer ID | Optional user-configurable field that is used for the contract information or other ID by any support service. | CallHome/CustomerData/ContractData/CustomerId |
| Contract ID | Optional user-configurable field that is used for the contract information or other ID by any support service. | CallHome/CustomerData/ContractData/ContractId |

| Data Item (Plain Text and XML) | Description (Plain Text and XML) | Call-Home Message Tag (XML Only) |
|---|---|---|
| Site ID | Optional user-configurable field that is used for Cisco-supplied site ID or other data meaningful to alternate support service. | CallHome/CustomerData/ContractData/SiteId |
| Server ID | If the message is generated from the device, the Server ID is the unique device identifier (UDI) of the device. The format is *type@Sid@serial*.<br>• The *type* is the product model number from the backplane IDPROM.<br>• @ is a separator character.<br>• *Sid* is C, identifying the serial ID as a chassis serial number.<br>• The Sid field identifies the *serial* number.<br>An example is WS-C6509@C@12345678. | For long text message only |
| Message description | Short text that describes the error. | CallHome/MessageDescription |
| Device name | Node that experienced the event (hostname of the device). | CallHome/CustomerData/SystemInfo/NameName |
| Contact name | Name of the contact person for issues that are associated with the node that experienced the event. | CallHome/CustomerData/SystemInfo/Contact |
| Contact email | Email address of the contact person for this unit. | CallHome/CustomerData/SystemInfo/ContactEmail |
| Contact phone number | Phone number of the contact person for this unit. | CallHome/CustomerData/SystemInfo/ContactPhoneNumber |
| Street address | Optional field that contains the street address for RMA part shipments that are associated with this unit. | CallHome/CustomerData/SystemInfo/StreetAddress |
| Model name | Model name of the device (the specific model as part of a product family name). | CallHome/Device/Cisco_Chassis/Model |
| Serial number | Chassis serial number of the unit. | CallHome/Device/Cisco_Chassis/SerialNumber |
| Chassis part number | Top assembly number of the chassis. | /aml/body/chassis/partNo |
| System object ID | System Object ID that uniquely identifies the system. | CallHome/Device/Cisco_Chassis/ AdditionalInformation/AD@name=“sysObjectID” |

| Data Item (Plain Text and XML) | Description (Plain Text and XML) | Call-Home Message Tag (XML Only) |
|---|---|---|
| System description | System description for the managed element. | CallHome/Device/Cisco_Chassis/ AdditionalInformation/AD@name="sysDescr" |

The following table describes the fields specific to alert group messages for full text and XML. These fields may be repeated if multiple commands are executed for an alert group.

*Table 7: Fields Specific to Alert Group Messages for Full Text and XML Messages*

| Data Item (Plain Text and XML) | Description (Plain Text and XML) | XML Tag (XML Only) |
|---|---|---|
| Command output name | Exact name of the issued command. | /aml/attachments/attachment/name |
| Attachment type | The specific command output. | /aml/attachments/attachment/type |
| MIME type | Either plain text or encoding type. | /aml/attachments/attachment/mime |
| Command output text | Output of the command that is automatically executed. | /mml/attachments/attachment/atdata |

The following table describes the event message format for full text or XML messages.

*Table 8: Inserted Fields for a Reactive and Proactive Event Message*

| Data Item (Plain Text and XML) | Description (Plain Text and XML) | XML Tag (XML Only) |
|---|---|---|
| Chassis hardware version | Hardware version of chassis. | /aml/body/chassis/hwVersion |
| Supervisor module software version | Top-level software version. | /aml/body/chassis/swVersion |
| Affected FRU name | Name of the affected FRU that is generating the event message. | /aml/body/fru/name |
| Affected FRU serial number | Serial number of the affected FRU. | /aml/body/fru/serialNo |
| Affected FRU part number | Part number of the affected FRU. | /aml/body/fru/partNo |
| FRU slot | Slot number of the FRU that is generating the event message. | /aml/body/fru/slot |
| FRU hardware version | Hardware version of the affected FRU. | /aml/body/fru/hwVersion |
| FRU software version | Software version that is running on the affected FRU. | /aml/body/fru/swVersion |

The following table describes the inventory event message format for full text or XML messages.

*Table 9: Inserted Fields for an Inventory Event Message*

| Data Item (Plain Text and XML) | Description (Plain Text and XML) | XML Tag (XML Only) |
|---|---|---|
| Chassis hardware version | Hardware version of the chassis. | /aml/body/chassis/hwVersion |
| Supervisor module software version | Top-level software version. | /aml/body/chassis/swVersion |

| Data Item (Plain Text and XML) | Description (Plain Text and XML) | XML Tag (XML Only) |
|---|---|---|
| FRU name | Name of the affected FRU that is generating the event message. | /aml/body/fru/name |
| FRU s/n | Serial number of the FRU. | /aml/body/fru/serialNo |
| FRU part number | Part number of the FRU. | /aml/body/fru/partNo |
| FRU slot | Slot number of the FRU. | /aml/body/fru/slot |
| FRU hardware version | Hardware version of the FRU. | /aml/body/fru/hwVersion |
| FRU software version | Software version that is running on the FRU. | /aml/body/fru/swVersion |

The following table describes the user-generated test message format for full text or XML.

***Table 10: Inserted Fields for a User-Generated Test Message***

| Data Item (Plain Text and XML) | Description (Plain Text and XML) | XML Tag (XML Only) |
|---|---|---|
| Process ID | Unique process ID. | /aml/body/process/id |
| Process state | State of process (for example, running or halted). | /aml/body/process/processState |
| Process exception | Exception or reason code. | /aml/body/process/exception |

# Sample syslog Alert Notification in XML Format

```
<?xml version="1.0" encoding="UTF-8"?>
<soap-env:Envelope
xmlns:soap-env="http://www.w3.org/2003/05/soap-envelope">
<soap-env:Header>
<aml-session:Session
xmlns:aml-session="http://www.cisco.com/2004/01/aml-session"
soap-env:mustUnderstand="true"
soap-env:role="http://www.w3.org/2003/05/soap-envelope/role/next">
<aml-session:To>http://tools.cisco.com/neddce/services/DDCEService</aml
-session:To>
<aml-session:Path>
<aml-session:Via>http://www.cisco.com/appliance/uri</aml-session:Via>
</aml-session:Path>
<aml-session:From>http://www.cisco.com/appliance/uri</aml-session:From>
<aml-session:MessageId>MA:FXS1739Q0NR:548F4417</aml-session:MessageId>
</aml-session:Session>
</soap-env:Header>
<soap-env:Body>
<aml-block:Block
xmlns:aml-block="http://www.cisco.com/2004/01/aml-block">
<aml-block:Header>
<aml-block:Type>http://www.cisco.com/2005/05/callhome/syslog</aml-block
:Type>
<aml-block:CreationDate>2014-12-16 04:27:03
GMT+08:00</aml-block:CreationDate>
<aml-block:Builder>
<aml-block:Name>CBR8</aml-block:Name>
<aml-block:Version>2.0</aml-block:Version>
</aml-block:Builder>
<aml-block:BlockGroup>
```

```
<aml-block:GroupId>GB:FXS1739Q0NR:548F4417</aml-block:GroupId>
<aml-block:Number>0</aml-block:Number>
<aml-block:IsLast>true</aml-block:IsLast>
<aml-block:IsPrimary>true</aml-block:IsPrimary>
<aml-block:WaitForPrimary>false</aml-block:WaitForPrimary>
</aml-block:BlockGroup>
<aml-block:Severity>6</aml-block:Severity>
</aml-block:Header>
<aml-block:Content>
<ch:CallHome xmlns:ch="http://www.cisco.com/2005/05/callhome"
version="1.0">
<ch:EventTime>2014-12-16 04:26:59 GMT+08:00</ch:EventTime>
<ch:MessageDescription>Dec 16 04:26:59.885 CST: %ENVIRONMENTAL-1-ALERT:
Temp: INLET, Location: 6, State: Critical, Reading: 53
Celsius</ch:MessageDescription> <ch:Event> <ch:Type>syslog</ch:Type>
<ch:SubType></ch:SubType> <ch:Brand>Cisco Systems</ch:Brand>
<ch:Series>CBR8 Series Routers</ch:Series> </ch:Event>
<ch:CustomerData> <ch:UserData> <ch:Email>xxxx@company.com</ch:Email>
</ch:UserData>
<ch:ContractData>
<ch:CustomerId></ch:CustomerId>
<ch:SiteId></ch:SiteId>
<ch:ContractId></ch:ContractId>
<ch:DeviceId>CBR-8-CCAP-CHASS@C@FXS1739Q0NR</ch:DeviceId>
</ch:ContractData>
<ch:SystemInfo>
<ch:Name>sig-cbr</ch:Name>
<ch:Contact></ch:Contact>
<ch:ContactEmail>xxxx@company.com</ch:ContactEmail>
<ch:ContactPhoneNumber></ch:ContactPhoneNumber>
<ch:StreetAddress></ch:StreetAddress>
</ch:SystemInfo>
<ch:CCOID></ch:CCOID>
</ch:CustomerData>
<ch:Device>
<rme:Chassis xmlns:rme="http://www.cisco.com/rme/4.0">
<rme:Model>CBR-8-CCAP-CHASS</rme:Model>
<rme:HardwareVersion>0.1</rme:HardwareVersion>
<rme:SerialNumber>FXS1739Q0NR</rme:SerialNumber>
<rme:AdditionalInformation>
<rme:AD name="PartNumber" value="000-00000-00" /> <rme:AD
name="SoftwareVersion" value="15.5(20141214:005145) " /> <rme:AD
name="SystemObjectId" value="1.3.6.1.4.1.9.1.2141" /> <rme:AD
name="SystemDescription" value="Cisco IOS Software, IOS-XE Software
(X86_64_LINUX_IOSD-ADVENTERPRISEK9-M), Experimental Version
15.5(20141214:005145) [ece5_throttle_ios-ram-ece5-bk 105] Copyright (c)
1986-2014 by Cisco Systems, Inc.
Compiled Sun 14-Dec-14 00:20 by ram" /> <rme:AD name="ServiceNumber"
value="" /> <rme:AD name="ForwardAddress" value="" />
</rme:AdditionalInformation> </rme:Chassis> </ch:Device> </ch:CallHome>
</aml-block:Content> <aml-block:Attachments> <aml-block:Attachment
type="inline"> <aml-block:Name>show inventory</aml-block:Name>
<aml-block:Data encoding="plain"> <![CDATA[show inventory Load for five
secs: 2%/0%; one minute: 2%; five minutes: 2% Time source is NTP,
04:27:02.278 CST Tue Dec 16 2014
NAME: "Chassis", DESCR: "Cisco cBR-8 CCAP Chassis"
PID: CBR-8-CCAP-CHASS  , VID: V01, SN: FXS1739Q0NR

NAME: "sup 0", DESCR: "Cisco cBR CCAP Supervisor Card"
PID: CBR-CCAP-SUP-160G , VID: V01, SN: CAT1736E05L

NAME: "harddisk 4/1", DESCR: "Hard Disk"
PID: UGB88RTB100HE3-BCU-DID, VID:    , SN: 11000072780
```

```
NAME: "sup-pic 4/1", DESCR: "Cisco cBR CCAP Supervisor Card PIC"
PID: CBR-SUPPIC-8X10G  , VID: V01, SN: CAT1735E004

NAME: "SFP+ module 4/1/0", DESCR: "iNSI xcvr"
PID: SFP+ 10GBASE-SR   , VID: A   , SN: FNS1727294V

NAME: "SFP+ module 4/1/1", DESCR: "iNSI xcvr"
PID: SFP+ 10GBASE-SR   , VID: A   , SN: FNS172727WZ

NAME: "SFP+ module 4/1/4", DESCR: "iNSI xcvr"
PID: 10GE ZR           , VID:     , SN: AGM120525EW

NAME: "sup 1", DESCR: "Cisco cBR CCAP Supervisor Card"
PID: CBR-CCAP-SUP-160G , VID: V01, SN: CAT1736E05L

NAME: "clc 6", DESCR: "Cisco cBR CCAP Line Card"
PID: CBR-CCAP-LC-40G   , VID: V01, SN: CAT1736E0EN

NAME: "Cable PHY Module", DESCR: "CLC Downstream PHY Module 6/0"
PID: cBR-8-GEMINI      , VID: V01 , SN: CSJ13152101

NAME: "Cable PHY Module", DESCR: "CLC Upstream PHY Module 6/2"
PID: cBR-8-LEOBEN      , VID: V01 , SN: TST98765432

NAME: "Power Supply Module 0", DESCR: "Cisco cBR CCAP AC Power Supply"
PID: PWR-3KW-AC-V2     , VID: V02, SN: DTM173702KQ

NAME: "Power Supply Module 2", DESCR: "Cisco cBR CCAP AC Power Supply"
PID: PWR-3KW-AC-V2     , VID: V02, SN: DTM173702GD


sig-cbr#]]></aml-block:Data>
</aml-block:Attachment>
<aml-block:Attachment type="inline">
<aml-block:Name>show logging</aml-block:Name> <aml-block:Data
encoding="plain"> <![CDATA[show logging Load for five secs: 2%/0%; one
minute: 2%; five minutes: 2% Time source is NTP, 04:27:02.886 CST Tue
Dec 16 2014

Syslog logging: enabled (0 messages dropped, 51 messages rate-limited,
0 flushes, 0 overruns, xml disabled, filtering disabled)

No Active Message Discriminator.



No Inactive Message Discriminator.


    Console logging: level debugging, 213 messages logged, xml disabled,
                     filtering disabled
    Monitor logging: level debugging, 0 messages logged, xml disabled,
                     filtering disabled
    Buffer logging:  level debugging, 262 messages logged, xml disabled,
                    filtering disabled
    Exception Logging: size (4096 bytes)
    Count and timestamp logging messages: disabled
    Persistent logging: disabled

No active filter modules.

    Trap logging: level informational, 209 message lines logged
        Logging Source-Interface:       VRF Name:
```

```
Log Buffer (1000000 bytes):

*Dec 15 20:20:16.188: Rommon debug: debugFlagsStr[7], flags[0x7] *Dec
15 20:20:16.188: TRACE - Debug flag set 0x7 *Dec 15 20:20:16.188: TRACE
- Register NV N:systemInitByEvent V:True with no CallBack *Dec 15
20:20:16.188: TRACE - Register NV N:routingReadyByEvent V:True with no
CallBack *Dec 15 20:20:16.188: TRACE - Smart agent init started.
Version=1.2.0_dev/22
*Dec 15 20:20:16.188: ERROR - PD init failed: The requested operation
is not supported *Dec 15 20:20:16.188: ERROR - Pre Role Init Failed:
The requested operation is not supported *Dec 15 20:20:16.188: TRACE -
Smart agent init Done. status 10, state 4294967295, init 0 enable 0
Current Role Invalid *Dec 15 20:20:16.188: TRACE - Shutdown Started
*Dec 15 20:20:16.188: DEBUG - Scheduler shutdown start *Dec 15
20:20:16.188: ERROR - Failed to set shutdown watched boolean (code
Invalid argument (22)). Going the hard way!!!
*Dec 15 20:20:16.188: DEBUG - Destroying XOS stuff to exit dispatch
loop *Dec 15 20:20:16.188: DEBUG - XDM dispatch loop about to exit *Dec
15 20:20:16.188: DEBUG - Scheduler shutdown end *Dec 15 20:20:16.188:
ERROR - SmartAgent not initialized.
*Dec 15 20:20:16.188: ERROR - Smart Agent not a RF client *Dec 15
20:20:16.188: ERROR - Smart Agent not a CF client *Dec 15 20:20:16.188:
TRACE - Setting Ha Mgmt Init FALSE *Dec 15 20:20:16.188: TRACE -
Shutting down Any Role *Dec 15 20:20:17.432: (DBMS RPHA) Client
initialization; status=success *Dec 15 20:20:17.432: CABLE Parser
Trace:  cable_parser_init:82 *Dec 15 20:20:17.774: ****
mcprp_ubr_punt_init: Initialized*****
-->RF_STATUS_SEND_RF_STATE received-->RF_PROG_INITIALIZATION received
*Dec 15 20:20:20.790: CWAN OIR debugging enabled (ROMMON variable
DEBUG_CWAN_OIR set)-->RF_PROG_ACTIVE_FAST
received-->RF_PROG_ACTIVE_DRAIN
received-->RF_PROG_ACTIVE_PRECONFIG
received-->received-->RF_PROG_ACTIVE_POSTCONFIG
received-->RF_PROG_ACTIVE received
*Dec 15 20:20:20.841: **** IPC port 0x1000E created!
*Dec 15 20:20:20.841:  **** CIPC RP Server created UBRCCE_CIPC_14/0 !
*Dec 15 20:20:28.294: %SPANTREE-5-EXTENDED_SYSID: Extended SysId
enabled for type vlan *Dec 15 20:20:31.944: %VOICE_HA-7-STATUS: CUBE
HA-supported platform detected.
*Dec 15 20:20:33.391:  instant_msg_handle_proc_sup started!!
*Dec 15 20:20:33.391:  queue_msg_handle_proc_sup started!!
*Dec 15 20:20:35.603: %IOSXE_MGMTVRF-6-CREATE_SUCCESS_INFO: Management
vrf Mgmt-intf created with ID 1, ipv4 table-id 0x1, ipv6 table-id
0x1E000001
*Dec 15 20:20:34.513: %IOSXE-6-PLATFORM: CLC4: cpp_cp: Process
CPP_PFILTER_EA_EVENT__API_CALL__REGISTER
*Dec 15 20:20:03.806: %HW_PFU-3-PFU_IDPROM_CORRUPT: R0/0: cmand:  The
PEM/FM idprom could be read, but is corrupt in slot P11 The system will
run without environmental monitoring for this component *Dec 15
20:20:09.012: %SYSTEM-3-SYSTEM_SHELL_LOG: R0/0:  2014/12/15
20:20:08 : <anon>
*Dec 15 20:20:13.919: %IOSXE-4-PLATFORM: R0/0: kernel: astro: FD open
*Dec 15 20:20:13.919: %IOSXE-4-PLATFORM: R0/0: kernel: astro: astro:
mmio_start=d0000000 mmio_len=2000000
*Dec 15 20:20:13.919: %IOSXE-4-PLATFORM: R0/0: kernel: astro: Done
astro Memory map base_ptr ffffc90016600000, astro_reg_ptr ffffc90016600000...
*Dec 15 20:20:16.259: %IOSXE-4-PLATFORM: R0/0: kernel: astro: FD open
*Dec 15 20:20:16.553: %CPPHA-7-START: F0: cpp_ha:  CPP 0 preparing
ucode *Dec 15 20:20:17.220: %CPPHA-7-START: F0: cpp_ha:  CPP 0 startup
init *Dec 15 20:20:18.549: %PMAN-3-PROC_EMPTY_EXEC_FILE: F0: pvp.sh:
Empty executable used for process iosdb *Dec 15 20:20:20.003:
%PMAN-3-PROC_EMPTY_EXEC_FILE: CLC4: pvp.sh:  Empty executable used for
process iosdb *Dec 15 20:20:20.783: %PMAN-3-PROC_EMPTY_EXEC_FILE: CLC4:
pvp.sh:  Empty executable used for process iosdb *Dec 15 20:20:24.061:
```

```
%HW_PFU-3-PFU_IDPROM_CORRUPT: R0/0: cmand:  The PEM/FM idprom could be
read, but is corrupt in slot P11 The system will run without
environmental monitoring for this component *Dec 15 20:20:31.722:
%CPPHA-7-START: F0: cpp_ha:  CPP 0 running init *Dec 15 20:20:32.070:
%CPPHA-7-READY: F0: cpp_ha:  CPP 0 loading and initialization complete
*Dec 15 20:20:36.528 UTC: TRACE - Platform EventCB invoked. EventType:
8 *Dec 15 20:20:36.528 UTC: DEBUG - Hostname changed. Old:sig-cbr
New:sig-cbr *Dec 15 20:20:36.528 UTC: %CNS IQ:0.1 ID:0
Changed:[sig-cbr] *Dec 15 20:20:36.528 UTC: %CNS IQ:0.2 ID:1
Changed:[sig-cbr] *Dec 15 20:20:36.528 UTC: %CNS IQ:0.3 ID:2
Changed:[sig-cbr] *Dec 15 20:20:36.594 UTC: %SYS-5-LOG_CONFIG_CHANGE:
Buffer logging: level debugging, xml disabled, filtering disabled, size
(1000000) *Dec 16 04:20:36.597 CST: %SYS-6-CLOCKUPDATE: System clock
has been updated from 20:20:36 UTC Mon Dec 15 2014 to 04:20:36 CST Tue
Dec 16 2014, configured from console by console.
*Dec 16 04:20:36.607 CST: spa_type 2946 ports 8 *Dec 16 04:20:36.622
CST: spa_type 2946 ports 8 *Dec 16 04:20:37.350 CST:
cmts_set_int_us_qos_flags: move US-QOS flags 0 to CDMAN *Dec 16
04:20:37.350 CST: cmts_set_int_us_default_weights: move US-QOS weights
to CDMAN *Dec 16 04:20:36.625 CST: %IOSXE-4-PLATFORM: R0/0: kernel:
astro: FD open *Dec 16 04:20:43.221 CST: %LINEPROTO-5-UPDOWN: Line
protocol on Interface Video6/0/0, changed state to up *Dec 16
04:20:43.223 CST: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Video6/0/1, changed state to up *Dec 16 04:20:43.502 CST: % Redundancy
mode change to SSO

*Dec 16 04:20:43.502 CST: %VOICE_HA-7-STATUS: NONE->SSO; SSO mode will
not take effect until after a platform
reload.-->RF_STATUS_REDUNDANCY_MODE_CHANGE received *Dec 16
04:20:44.220 CST: %SYS-5-CONFIG_I: Configured from memory by console
*Dec 16 04:20:44.228 CST: %IOSXE_OIR-6-INSCARD: Card (rp) inserted in
slot R1 *Dec 16 04:20:44.229 CST: %IOSXE_OIR-6-INSCARD: Card (fp)
inserted in slot F0 *Dec 16 04:20:44.229 CST: %IOSXE_OIR-6-ONLINECARD:
Card (fp) online in slot F0 *Dec 16 04:20:44.263 CST:
%IOSXE_OIR-6-INSCARD: Card (fp) inserted in slot F1 *Dec 16
04:20:44.263 CST: %IOSXE_OIR-6-INSCARD: Card (cc) inserted in slot 4
*Dec 16 04:20:44.263 CST: %IOSXE_OIR-6-ONLINECARD: Card (cc) online in
slot 4 *Dec 16 04:20:44.264 CST: %IOSXE_OIR-6-INSCARD: Card (cc)
inserted in slot 5 *Dec 16 04:20:44.264 CST: %IOSXE_OIR-6-INSCARD: Card
(cc) inserted in slot 6 *Dec 16 04:20:44.330 CST: %IOSXE_OIR-6-INSSPA:
SPA inserted in subslot 4/1 *Dec 16 04:20:44.751 CST: %SYS-5-RESTART:
System restarted -- Cisco IOS Software, IOS-XE Software
(X86_64_LINUX_IOSD-ADVENTERPRISEK9-M), Experimental Version
15.5(20141214:005145) [ece5_throttle_ios-ram-ece5-bk 105] Copyright (c)
1986-2014 by Cisco Systems, Inc.
Compiled Sun 14-Dec-14 00:20 by ram
*Dec 16 04:20:44.775 CST: %XML-SRVC: Security Enforcement XML
Service(111) OK. PID=574
*Dec 16 04:20:44.775 CST: %SSH-5-ENABLED: SSH 1.99 has been enabled
*Dec 16 04:20:45.453 CST: %LINK-3-UPDOWN: Interface GigabitEthernet0,
changed state to up *Dec 16 04:20:45.543 CST: %LINK-5-CHANGED:
Interface TenGigabitEthernet4/1/2, changed state to administratively
down *Dec 16 04:20:45.546 CST: %LINK-5-CHANGED: Interface
TenGigabitEthernet4/1/3, changed state to administratively down *Dec 16
04:20:45.548 CST: %LINK-5-CHANGED: Interface TenGigabitEthernet4/1/4,
changed state to administratively down *Dec 16 04:20:45.551 CST:
%LINK-5-CHANGED: Interface TenGigabitEthernet4/1/5, changed state to
administratively down *Dec 16 04:20:45.571 CST: %LINK-5-CHANGED:
Interface TenGigabitEthernet4/1/6, changed state to administratively
down *Dec 16 04:20:45.574 CST: %LINK-5-CHANGED: Interface
TenGigabitEthernet4/1/7, changed state to administratively down *Dec 16
04:20:45.576 CST: %LINK-5-CHANGED: Interface TenGigabitEthernet5/1/0,
changed state to administratively down *Dec 16 04:20:45.578 CST:
%LINK-5-CHANGED: Interface TenGigabitEthernet5/1/1, changed state to
```

```
administratively down *Dec 16 04:20:45.580 CST: %LINK-5-CHANGED:
Interface TenGigabitEthernet5/1/2, changed state to administratively
down *Dec 16 04:20:45.582 CST: %LINK-5-CHANGED: Interface
TenGigabitEthernet5/1/3, changed state to administratively down *Dec 16
04:20:45.584 CST: %LINK-5-CHANGED: Interface TenGigabitEthernet5/1/4,
changed state to administratively down *Dec 16 04:20:45.586 CST:
%LINK-5-CHANGED: Interface TenGigabitEthernet5/1/5, changed state to
administratively down *Dec 16 04:20:45.588 CST: %LINK-5-CHANGED:
Interface TenGigabitEthernet5/1/6, changed state to administratively
down *Dec 16 04:20:45.590 CST: %LINK-5-CHANGED: Interface
TenGigabitEthernet5/1/7, changed state to administratively down *Dec 16
04:20:45.596 CST: %LINK-3-UPDOWN: Interface Integrated-Cable6/0/0:0,
changed state to down *Dec 16 04:20:45.602 CST: %LINK-3-UPDOWN:
Interface Integrated-Cable6/0/0:1, changed state to down *Dec 16
04:20:45.603 CST: %LINK-3-UPDOWN: Interface Integrated-Cable6/0/0:2,
changed state to down *Dec 16 04:20:45.604 CST: %LINK-3-UPDOWN:
Interface Integrated-Cable6/0/0:3, changed state to down *Dec 16
04:20:45.606 CST: %LINK-3-UPDOWN: Interface Integrated-Cable6/0/0:4,
changed state to down *Dec 16 04:20:45.607 CST: %LINK-3-UPDOWN:
Interface Integrated-Cable6/0/0:5, changed state to down *Dec 16
04:20:45.608 CST: %LINK-3-UPDOWN: Interface Integrated-Cable6/0/0:6,
changed state to down *Dec 16 04:20:45.610 CST: %LINK-3-UPDOWN:
Interface Integrated-Cable6/0/0:7, changed state to down *Dec 16
04:20:45.648 CST: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Bundle1, changed state to up *Dec 16 04:20:45.649 CST: %LINK-3-UPDOWN:
Interface Bundle1, changed state to up *Dec 16 04:20:45.649 CST:
%LINK-3-UPDOWN: Interface Cable6/0/0, changed state to down *Dec 16
04:20:45.649 CST: %SNMP-5-LINK_DOWN: LinkDown:Interface
Cable6/0/0 changed state to down
*Dec 16 04:20:45.666 CST: %LINK-3-UPDOWN: Interface
Wideband-Cable6/0/0:0, changed state to down *Dec 16 04:20:45.666 CST:
%LINK-3-UPDOWN: Interface Wideband-Cable6/0/0:1, changed state to down
*Dec 16 04:20:45.681 CST: %LINK-3-UPDOWN: Interface
Wideband-Cable6/0/0:2, changed state to down *Dec 16 04:20:45.681 CST:
%LINK-3-UPDOWN: Interface Wideband-Cable6/0/0:3, changed state to down
*Dec 16 04:20:45.681 CST: %LINK-3-UPDOWN: Interface
Wideband-Cable6/0/0:4, changed state to down *Dec 16 04:20:45.681 CST:
%LINK-3-UPDOWN: Interface Wideband-Cable6/0/0:5, changed state to down
*Dec 16 04:20:45.682 CST: %LINK-3-UPDOWN: Interface
Wideband-Cable6/0/0:6, changed state to down *Dec 16 04:20:45.682 CST:
%LINK-3-UPDOWN: Interface Wideband-Cable6/0/0:7, changed state to down
*Dec 16 04:20:45.685 CST: %LINK-3-UPDOWN: Interface
Integrated-Cable6/0/1:0, changed state to down *Dec 16 04:20:45.694
CST: %LINK-3-UPDOWN: Interface Integrated-Cable6/0/1:1, changed state
to down *Dec 16 04:20:45.694 CST: %LINK-3-UPDOWN: Interface Cable6/0/1,
changed state to down *Dec 16 04:20:45.694 CST: %SNMP-5-LINK_DOWN:
LinkDown:Interface
Cable6/0/1 changed state to down
*Dec 16 04:20:45.699 CST: %LINK-3-UPDOWN: Interface
Wideband-Cable6/0/1:0, changed state to down *Dec 16 04:20:45.703 CST:
%LINK-3-UPDOWN: Interface Wideband-Cable6/0/1:1, changed state to down
*Dec 16 04:20:45.706 CST: %LINK-3-UPDOWN: Interface
Integrated-Cable6/0/1:2, changed state to down *Dec 16 04:20:45.707
CST: %LINK-3-UPDOWN: Interface Integrated-Cable6/0/1:3, changed state
to down *Dec 16 04:20:45.709 CST: %LINK-3-UPDOWN: Interface
Wideband-Cable6/0/2:0, changed state to down *Dec 16 04:20:46.469 CST:
%SNMP-5-COLDSTART: SNMP agent on host sig-cbr is undergoing a cold
start *Dec 16 04:20:46.472 CST: %LINEPROTO-5-UPDOWN: Line protocol on
Interface GigabitEthernet0, changed state to up *Dec 16 04:20:46.543
CST: %LINEPROTO-5-UPDOWN: Line protocol on Interface
TenGigabitEthernet4/1/2, changed state to down *Dec 16 04:20:46.546
CST: %LINEPROTO-5-UPDOWN: Line protocol on Interface
TenGigabitEthernet4/1/3, changed state to down *Dec 16 04:20:46.548
CST: %LINEPROTO-5-UPDOWN: Line protocol on Interface
```

```
TenGigabitEthernet4/1/4, changed state to down *Dec 16 04:20:46.551
CST: %LINEPROTO-5-UPDOWN: Line protocol on Interface
TenGigabitEthernet4/1/5, changed state to down *Dec 16 04:20:46.571
CST: %LINEPROTO-5-UPDOWN: Line protocol on Interface
TenGigabitEthernet4/1/6, changed state to down *Dec 16 04:20:46.574
CST: %LINEPROTO-5-UPDOWN: Line protocol on Interface
TenGigabitEthernet4/1/7, changed state to down *Dec 16 04:20:46.576
CST: %LINEPROTO-5-UPDOWN: Line protocol on Interface
TenGigabitEthernet5/1/0, changed state to down *Dec 16 04:20:46.578
CST: %LINEPROTO-5-UPDOWN: Line protocol on Interface
TenGigabitEthernet5/1/1, changed state to down *Dec 16 04:20:46.580
CST: %LINEPROTO-5-UPDOWN: Line protocol on Interface
TenGigabitEthernet5/1/2, changed state to down *Dec 16 04:20:46.582
CST: %LINEPROTO-5-UPDOWN: Line protocol on Interface
TenGigabitEthernet5/1/3, changed state to down *Dec 16 04:20:46.584
CST: %LINEPROTO-5-UPDOWN: Line protocol on Interface
TenGigabitEthernet5/1/4, changed state to down *Dec 16 04:20:46.586
CST: %LINEPROTO-5-UPDOWN: Line protocol on Interface
TenGigabitEthernet5/1/5, changed state to down *Dec 16 04:20:46.588
CST: %LINEPROTO-5-UPDOWN: Line protocol on Interface
TenGigabitEthernet5/1/6, changed state to down *Dec 16 04:20:46.590
CST: %LINEPROTO-5-UPDOWN: Line protocol on Interface
TenGigabitEthernet5/1/7, changed state to down *Dec 16 04:20:46.641
CST: %SYS-6-BOOTTIME: Time taken to reboot after reload =  374 seconds
*Dec 16 04:20:53.697 CST: %IOSXE-1-PLATFORM: R0/0: kernel: Raptor MAC
image download wrote 55917152 bytes *Dec 16 04:21:23.432 CST:
%TRANSCEIVER-6-INSERTED: CLC4: iomd:
transceiver module inserted in TenGigabitEthernet4/1/0 *Dec 16
04:21:23.435 CST: %TRANSCEIVER-6-INSERTED: CLC4: iomd:
transceiver module inserted in TenGigabitEthernet4/1/1 *Dec 16
04:21:23.440 CST: %TRANSCEIVER-6-INSERTED: CLC4: iomd:
transceiver module inserted in TenGigabitEthernet4/1/4 *Dec 16
04:21:29.430 CST: %CBRDTI-5-DTISLOT: DTI slot 4/1: card role changed to
Active

*Dec 16 04:21:29.454 CST: %SPA_OIR-6-ONLINECARD: SPA (CBR-SUPPIC-8X10G)
online in subslot 4/1 *Dec 16 04:21:31.403 CST: %LINK-3-UPDOWN:
Interface TenGigabitEthernet4/1/0, changed state to up *Dec 16
04:21:31.405 CST: %CBR_SPA-7-RAPTOR_ESI_EGRESS_HDR_LO_INTERRUPT:
CLC4: iomd:  LOCAL RAPTOR, DP 0, channel_not_found_err *Dec 16
04:21:31.412 CST: %LINK-3-UPDOWN: Interface TenGigabitEthernet4/1/1,
changed state to up *Dec 16 04:21:32.403 CST: %LINEPROTO-5-UPDOWN: Line
protocol on Interface TenGigabitEthernet4/1/0, changed state to up *Dec
16 04:21:32.412 CST: %LINEPROTO-5-UPDOWN: Line protocol on Interface
TenGigabitEthernet4/1/1, changed state to up *Dec 16 04:21:41.171 CST:
%IOSXE-3-PLATFORM: R0/0: kernel: i801_smbus
0000:00:1f.3: Transaction timeout
*Dec 16 04:21:41.174 CST: %IOSXE-3-PLATFORM: R0/0: kernel:
/nobackup/ram/ece5-bk/binos/os/linux/drivers/binos/i2c/max3674/max3674_
mai n.c:show_reg_pll (line 88): show_reg_pll failed *Dec 16
04:21:58.237 CST: %IOSXE-5-PLATFORM: CLC6: cdman: Basestar FPGA rev_id
0x00000002, fpga_rev_id 0x00000032 *Dec 16 04:21:59.074 CST:
%CMRP-3-BAD_ID_HW: R0/0: cmand:  Failed Identification Test in CBR
linecard. The module linecard slot 6 in this router may not be a
genuine Cisco product. Cisco warranties and support programs only apply
to genuine Cisco products. If Cisco determines that your insertion of
non-Cisco memory, WIC cards, AIM cards,  Network Modules, SPA cards,
GBICs or other modules into a  Cisco product is the cause of a support
issue, Cisco may  deny support under your warranty or under a Cisco
support  pro *Dec 16 04:21:59.075 CST: %IOSXE_OIR-6-ONLINECARD: Card
(cc) online in slot 6 *Dec 16 04:22:08.825 CST:
%ASR1000_INFRA-3-EOBC_SOCK: CLC6:
ubrclc-k9lc-ms:  Socket event for  EO6/0/1, fd 11, failed to bind;
Address already in use success *Dec 16 04:22:09.605 CST:  SNMP IPC
```

```
session up(RP <-> slot 6)!
*Dec 16 04:22:09.605 CST:  CMTS IPC session up!
*Dec 16 04:22:14.564 CST: %SNMP-5-LINK_UP: LinkUp:Interface
Cable6/0/0-upstream0 changed state to up *Dec 16 04:22:14.565 CST:
%SNMP-5-LINK_UP: LinkUp:Interface
Cable6/0/0-upstream1 changed state to up *Dec 16 04:22:14.566 CST:
%SNMP-5-LINK_UP: LinkUp:Interface
Cable6/0/2-upstream0 changed state to up *Dec 16 04:22:14.566 CST:
%SNMP-5-LINK_UP: LinkUp:Interface
Cable6/0/2-upstream1 changed state to up *Dec 16 04:22:15.051 CST:
%SNMP-5-LINK_UP: LinkUp:Interface Cable6/0/0 changed state to up *Dec
16 04:22:15.258 CST: %SNMP-5-LINK_UP: LinkUp:Interface Cable6/0/1
changed state to up *Dec 16 04:22:15.258 CST: %SNMP-5-LINK_UP:
LinkUp:Interface Cable6/0/2 changed state to up *Dec 16 04:22:15.259
CST: %SNMP-5-LINK_UP: LinkUp:Interface Cable6/0/3 changed state to up
*Dec 16 04:22:15.259 CST: %SNMP-5-LINK_UP: LinkUp:Interface Cable6/0/4
changed state to up *Dec 16 04:22:15.411 CST: %SNMP-5-LINK_UP:
LinkUp:Interface Cable6/0/5 changed state to up *Dec 16 04:22:15.411
CST: %SNMP-5-LINK_UP: LinkUp:Interface Cable6/0/6 changed state to up
*Dec 16 04:22:15.411 CST: %SNMP-5-LINK_UP: LinkUp:Interface Cable6/0/7
changed state to up *Dec 16 04:22:15.411 CST: %SNMP-5-LINK_UP:
LinkUp:Interface Cable6/0/8 changed state to up *Dec 16 04:22:15.432
CST: %SNMP-5-LINK_UP: LinkUp:Interface Cable6/0/9 changed state to up
*Dec 16 04:22:15.432 CST: %SNMP-5-LINK_UP: LinkUp:Interface Cable6/0/10
changed state to up *Dec 16 04:22:15.433 CST: %SNMP-5-LINK_UP:
LinkUp:Interface Cable6/0/11 changed state to up *Dec 16 04:22:15.433
CST: %SNMP-5-LINK_UP: LinkUp:Interface Cable6/0/12 changed state to up
*Dec 16 04:22:15.433 CST: %SNMP-5-LINK_UP: LinkUp:Interface Cable6/0/13
changed state to up *Dec 16 04:22:15.433 CST: %SNMP-5-LINK_UP:
LinkUp:Interface Cable6/0/14 changed state to up *Dec 16 04:22:15.433
CST: %SNMP-5-LINK_UP: LinkUp:Interface Cable6/0/15 changed state to up
*Dec 16 04:22:15.677 CST: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Cable6/0/8, changed state to up *Dec 16 04:22:15.678 CST:
%LINEPROTO-5-UPDOWN: Line protocol on Interface Cable6/0/9, changed
state to up *Dec 16 04:22:15.901 CST: %LINEPROTO-5-UPDOWN: Line
protocol on Interface Cable6/0/10, changed state to up *Dec 16
04:22:15.902 CST: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Cable6/0/11, changed state to up *Dec 16 04:22:15.902 CST:
%LINEPROTO-5-UPDOWN: Line protocol on Interface Cable6/0/12, changed
state to up *Dec 16 04:22:15.903 CST: %LINEPROTO-5-UPDOWN: Line
protocol on Interface Cable6/0/13, changed state to up *Dec 16
04:22:15.903 CST: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Cable6/0/14, changed state to up *Dec 16 04:22:15.904 CST:
%LINEPROTO-5-UPDOWN: Line protocol on Interface Cable6/0/15, changed
state to up *Dec 16 04:22:17.046 CST: %LINEPROTO-5-UPDOWN: Line
protocol on Interface Cable6/0/0, changed state to up *Dec 16
04:22:17.047 CST: %LINK-3-UPDOWN: Interface Cable6/0/0, changed state
to up *Dec 16 04:22:17.256 CST: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Cable6/0/1, changed state to up *Dec 16 04:22:17.257 CST:
%LINK-3-UPDOWN: Interface Cable6/0/1, changed state to up *Dec 16
04:22:17.259 CST: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Cable6/0/2, changed state to up *Dec 16 04:22:17.260 CST:
%LINK-3-UPDOWN: Interface Cable6/0/2, changed state to up *Dec 16
04:22:17.260 CST: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Cable6/0/3, changed state to up *Dec 16 04:22:17.260 CST:
%LINK-3-UPDOWN: Interface Cable6/0/3, changed state to up *Dec 16
04:22:17.260 CST: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Cable6/0/4, changed state to up *Dec 16 04:22:17.260 CST:
%LINK-3-UPDOWN: Interface Cable6/0/4, changed state to up *Dec 16
04:22:17.411 CST: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Cable6/0/5, changed state to up *Dec 16 04:22:17.411 CST:
%LINK-3-UPDOWN: Interface Cable6/0/5, changed state to up *Dec 16
04:22:17.411 CST: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Cable6/0/6, changed state to up *Dec 16 04:22:17.411 CST:
```

```
%LINK-3-UPDOWN: Interface Cable6/0/6, changed state to up *Dec 16
04:22:17.411 CST: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Cable6/0/7, changed state to up *Dec 16 04:22:17.412 CST:
%LINK-3-UPDOWN: Interface Cable6/0/7, changed state to up *Dec 16
04:22:16.714 CST: %IOSXE-5-PLATFORM: CLC6: cdman: DS-JIB:ILK Interrupts
Enabled. (Init:20539, Check:9566 1stPKO:8942) *Dec 16 04:22:17.809 CST:
%CMRP-3-IDPROM_SENSOR: R0/0: cmand:  One or more sensor fields from the
idprom failed to parse properly because Invalid argument.
Dec 16 04:22:57.161 CST: %SNMP-5-LINK_DOWN: LinkDown:Interface
Integrated-Cable6/0/0-downstream0 changed state to down Dec 16
04:22:57.161 CST: %SNMP-5-LINK_DOWN: LinkDown:Interface
Integrated-Cable6/0/0-downstream1 changed state to down Dec 16
04:22:57.161 CST: %SNMP-5-LINK_DOWN: LinkDown:Interface
Integrated-Cable6/0/0-downstream2 changed state to down Dec 16
04:22:57.162 CST: %SNMP-5-LINK_DOWN: LinkDown:Interface
Integrated-Cable6/0/0-downstream3 changed state to down Dec 16
04:22:57.162 CST: %SNMP-5-LINK_DOWN: LinkDown:Interface
Integrated-Cable6/0/0-downstream4 changed state to down Dec 16
04:22:57.162 CST: %SNMP-5-LINK_DOWN: LinkDown:Interface
Integrated-Cable6/0/0-downstream5 changed state to down Dec 16
04:22:57.162 CST: %SNMP-5-LINK_DOWN: LinkDown:Interface
Integrated-Cable6/0/0-downstream6 changed state to down Dec 16
04:22:57.162 CST: %SNMP-5-LINK_DOWN: LinkDown:Interface
Integrated-Cable6/0/0-downstream7 changed state to down Dec 16
04:22:57.163 CST: %SNMP-5-LINK_DOWN: LinkDown:Interface
Integrated-Cable6/0/0-downstream8 changed state to down Dec 16
04:22:57.163 CST: %SNMP-5-LINK_DOWN: LinkDown:Interface
Integrated-Cable6/0/0-downstream9 changed state to down Dec 16
04:22:57.163 CST: %SNMP-5-LINK_DOWN: LinkDown:Interface
Integrated-Cable6/0/0-downstream10 changed state to down Dec 16
04:22:57.163 CST: %SNMP-5-LINK_DOWN: LinkDown:Interface
Integrated-Cable6/0/1-downstream0 changed state to down Dec 16
04:22:57.164 CST: %SNMP-5-LINK_DOWN: LinkDown:Interface
Integrated-Cable6/0/1-downstream1 changed state to down Dec 16
04:22:57.164 CST: %SNMP-5-LINK_DOWN: LinkDown:Interface
Integrated-Cable6/0/1-downstream2 changed state to down Dec 16
04:22:57.164 CST: %SNMP-5-LINK_DOWN: LinkDown:Interface
Integrated-Cable6/0/1-downstream3 changed state to down Dec 16
04:22:57.164 CST: %SNMP-5-LINK_DOWN: LinkDown:Interface
Integrated-Cable6/0/1-downstream4 changed state to down Dec 16
04:22:57.164 CST: %SNMP-5-LINK_DOWN: LinkDown:Interface
Integrated-Cable6/0/1-downstream5 changed state to down Dec 16
04:22:57.183 CST: %SNMP-5-LINK_UP: LinkUp:Interface
Integrated-Cable6/0/0-downstream0 changed state to up Dec 16
04:22:57.184 CST: %SNMP-5-LINK_UP: LinkUp:Interface
Integrated-Cable6/0/0-downstream1 changed state to up Dec 16
04:22:57.189 CST: %SNMP-5-LINK_UP: LinkUp:Interface
Integrated-Cable6/0/0-downstream2 changed state to up Dec 16
04:22:57.211 CST: %SNMP-5-LINK_UP: LinkUp:Interface
Integrated-Cable6/0/0-downstream3 changed state to up Dec 16
04:22:57.212 CST: %SNMP-5-LINK_UP: LinkUp:Interface
Integrated-Cable6/0/0-downstream4 changed state to up Dec 16
04:22:57.212 CST: %SNMP-5-LINK_UP: LinkUp:Interface
Integrated-Cable6/0/0-downstream6 changed state to up Dec 16
04:22:57.213 CST: %SNMP-5-LINK_UP: LinkUp:Interface
Integrated-Cable6/0/0-downstream7 changed state to up Dec 16
04:22:57.213 CST: %SNMP-5-LINK_UP: LinkUp:Interface
Integrated-Cable6/0/0-downstream8 changed state to up Dec 16
04:22:57.213 CST: %SNMP-5-LINK_UP: LinkUp:Interface
Integrated-Cable6/0/0-downstream9 changed state to up Dec 16
04:22:57.213 CST: %SNMP-5-LINK_UP: LinkUp:Interface
Integrated-Cable6/0/0-downstream10 changed state to up Dec 16
04:22:57.214 CST: %SNMP-5-LINK_UP: LinkUp:Interface
Integrated-Cable6/0/1-downstream0 changed state to up Dec 16
```

```
04:22:57.424 CST: %SNMP-5-LINK_UP: LinkUp:Interface
Integrated-Cable6/0/1-downstream1 changed state to up Dec 16
04:22:57.426 CST: %SNMP-5-LINK_UP: LinkUp:Interface
Integrated-Cable6/0/1-downstream2 changed state to up Dec 16
04:22:57.435 CST: %SNMP-5-LINK_UP: LinkUp:Interface
Integrated-Cable6/0/1-downstream3 changed state to up Dec 16
04:22:57.437 CST: %SNMP-5-LINK_UP: LinkUp:Interface
Integrated-Cable6/0/1-downstream4 changed state to up Dec 16
04:22:57.449 CST: %SNMP-5-LINK_UP: LinkUp:Interface
Integrated-Cable6/0/1-downstream5 changed state to up Dec 16
04:22:59.219 CST: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Integrated-Cable6/0/1:0, changed state to up Dec 16 04:22:59.219 CST:
%LINK-3-UPDOWN: Interface Integrated-Cable6/0/1:0, changed state to up
Dec 16 04:22:59.427 CST: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Integrated-Cable6/0/1:1, changed state to up Dec 16
04:22:59.427 CST: %LINK-3-UPDOWN: Interface Integrated-Cable6/0/1:1,
changed state to up Dec 16 04:22:59.449 CST: %LINEPROTO-5-UPDOWN: Line
protocol on Interface Wideband-Cable6/0/0:0, changed state to up Dec 16
04:22:59.450 CST: %LINK-3-UPDOWN: Interface Wideband-Cable6/0/0:0,
changed state to up Dec 16 04:22:59.450 CST: %LINK-3-UPDOWN: Interface
Wideband-Cable6/0/0:1, changed state to up Dec 16 04:22:59.450 CST:
%LINK-3-UPDOWN: Interface Wideband-Cable6/0/0:2, changed state to up
Dec 16 04:22:59.450 CST: %LINK-3-UPDOWN: Interface
Wideband-Cable6/0/0:3, changed state to up Dec 16 04:22:59.450 CST:
%LINK-3-UPDOWN: Interface Wideband-Cable6/0/0:4, changed state to up
Dec 16 04:22:59.450 CST: %LINK-3-UPDOWN: Interface
Wideband-Cable6/0/0:5, changed state to up Dec 16 04:22:59.451 CST:
%LINK-3-UPDOWN: Interface Wideband-Cable6/0/0:6, changed state to up
Dec 16 04:22:59.451 CST: %LINK-3-UPDOWN: Interface
Wideband-Cable6/0/0:7, changed state to up Dec 16 04:22:59.451 CST:
%LINEPROTO-5-UPDOWN: Line protocol on Interface Wideband-Cable6/0/1:0,
changed state to up Dec 16 04:22:59.451 CST: %LINK-3-UPDOWN: Interface
Wideband-Cable6/0/1:0, changed state to up Dec 16 04:22:59.451 CST:
%LINEPROTO-5-UPDOWN: Line protocol on Interface Wideband-Cable6/0/1:1,
changed state to up Dec 16 04:22:59.452 CST: %LINK-3-UPDOWN: Interface
Wideband-Cable6/0/1:1, changed state to up Dec 16 04:22:59.452 CST:
%LINK-3-UPDOWN: Interface Wideband-Cable6/0/2:0, changed state to up
Dec 16 04:23:27.352 CST: %IOSXE-5-PLATFORM: CLC6: cdman: DSPHY Gemini
module  1 was not present Dec 16 04:26:59.885 CST:
%ENVIRONMENTAL-1-ALERT: Temp: INLET, Location:
6, State: Critical, Reading: 53 Celsius sig-cbr#]]></aml-block:Data>
</aml-block:Attachment> </aml-block:Attachments> </aml-block:Block>
</soap-env:Body> </soap-env:Envelope>
```

# Additional References

### Related Documents

| Related Topic | Document Title |
|---|---|
| Smart Call Home site page on Cisco.com for access to all related product information. | Cisco Smart Call Home site |
| The User Guide explains how the Smart Call Home service offers web-based access to important information on select Cisco devices. The User Guide also describes the higher network availability and increased operational efficiency by providing real-time alerts. | Smart Call Home User Guide |

| Related Topic | Document Title |
|---|---|
| Call Home Quick Start Guide | Smart Call Home Quick Start Configuration Guide for Cisco cBR Series Routers |

### MIBs

| MIB | MIBs Link |
|---|---|
| CISCO-CALLHOME-MIB | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br>http://www.cisco.com/go/mibs |

### Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.<br>You can subscribe to various services to receive security and technical information about your products. The services include the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.<br>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. | http://www.cisco.com/support |

# Feature Information for Call Home

Use Cisco Feature Navigator to find information about the platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to the www.cisco.com/go/cfn link. An account on the Cisco.com page is not required.

**Note** The following table lists the software release in which a given feature is introduced. Unless noted otherwise, subsequent releases of that software release train also support that feature.

*Table 11: Feature Information for Call Home*

| Feature Name | Releases | Feature Information |
|---|---|---|
| Smart Call Home | Cisco IOS XE Everest 16.6.1 | This feature was integrated into the Cisco IOS XE Everest 16.6.1 on theCisco cBR Series Converged Broadband Routers. |