

Configure Call Home

The Call Home feature provides e-mail-based and web-based notification of critical system events. A versatile range of message formats are available for optimal compatibility with pager services, standard e-mail, or XML-based automated parsing applications. Common uses of this feature may include direct paging of a network support engineer, e-mail notification to a Network Operations Center, XML delivery to a support website, and use of Cisco Smart Call Home services for direct case generation with the Cisco Systems Technical Assistance Center (TAC).

This chapter includes these sections:

- Find feature information, on page 1
- Prerequisites for Call Home, on page 1
- Information about Call Home, on page 2
- How to configure Call Home, on page 4
- Configure Diagnostic Signatures, on page 25
- Display Call Home Configuration Information, on page 33
- Default Call Home settings, on page 38
- Alert Group trigger events and commands, on page 39
- Message Contents, on page 46

Find feature information

Your software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

Use the Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. A Cisco account is not required to access the Cisco Feature Navigator.

Prerequisites for Call Home

These are the prerequisites before you configure Call Home:

- Contact e-mail 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) should be configured so that the receiver can determine the origin of messages received.

- At least one destination profile (predefined or user-defined) must be configured. The destination profile you use depends on whether the receiving entity is a pager, an e-mail address, or an automated service such as Cisco Smart Call Home.

  If the destination profile uses e-mail message delivery, you must specify a Simple Mail Transfer Protocol (SMTP) server.

- The router must have IP connectivity to an e-mail server or the destination HTTP server.
- If Cisco Smart Call Home is used, an active service contract covering the device is required to provide full Cisco Smart Call Home service.

Information about Call Home

The Call Home feature can deliver alert messages containing information on configuration, environmental conditions, inventory, syslog, snapshot, and crash events. It provides these alert messages as either e-mail-based or web-based messages. Multiple message formats are available, allowing for compatibility with pager services, standard e-mail, or XML-based automated parsing applications. This feature can deliver alerts to multiple recipients, referred to as Call Home destination profiles, each with configurable message formats and content categories. A predefined destination profile is provided for sending alerts to the Cisco TAC (callhome@cisco.com). You can also define your own destination profiles.

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

This section contains these subsections:

- Benefits of Using Call Home
- Obtaining Smart Call Home Services

Benefits of Call Home

The Call Home feature offers these benefits:

- Multiple message-format options, which include:

  Short Text—Suitable for pagers or printed reports.

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

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

- Multiple concurrent message destinations.
- Multiple message categories including configuration, environmental conditions, inventory, syslog, snapshot, and crash events.
- Filtering of messages by 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 known issues, particularly online diagnostics failures, Automatic Service Requests are generated with the Cisco TAC.

Smart Call Home offers these features:

- Continuous device health monitoring and real-time diagnostic alerts.
- Analysis of Smart Call Home messages and, if needed, Automatic Service Request generation routed to the correct TAC team, including detailed diagnostic information to speed problem resolution.
- Secure message transport directly from your device or through an HTTP proxy server or a downloadable Transport Gateway (TG). You can use a TG aggregation point to support multiple devices or in cases where security dictates that your devices may not be connected directly to the Internet.
- Web-based access to Smart Call Home messages and recommendations, inventory, and configuration information for all Smart Call Home devices provides access to 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 e-mail address
- Your Cisco.com username

For more information about Smart Call Home, see https://supportforums.cisco.com/community/4816/smart-call-home.

Anonymous Reporting

Smart Call Home is a service capability included with many Cisco service contracts and is designed to assist customers resolve problems more quickly. In addition, the information gained from crash messages helps Cisco understand equipment and issues occurring in the field. If you decide not to use Smart Call Home, you can still enable Anonymous Reporting to allow Cisco to securely receive minimal error and health information from the device. If you enable Anonymous Reporting, your customer identity will remain anonymous, and no identifying information will be sent.

Note When you enable Anonymous Reporting, you acknowledge your consent to transfer the specified data to 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 http://www.cisco.com/web/siteassets/legal/privacy.html.

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

For more information about what is sent in these messages, see Alert Group trigger events and commands, on page 39.

How to configure Call Home

These sections show how to configure Call Home using a single command:

- Configure Smart Call Home (Single Command), on page 4
- Configure and Enable Smart Call Home, on page 5

These sections show detailed or optional configurations:

- Enable and Disable Call Home, on page 5
- Configure contact information, on page 6
- Configure destination profiles, on page 7
- Subscribe to alert groups, on page 11
- Configure general e-mail options, on page 16
- Specify rate limit for sending Call Home messages, on page 18
- Specify HTTP proxy server, on page 18
- Enable AAA authorization to run IOS commands for Call Home messages, on page 19
- Configure syslog throttling, on page 20
- Configure Call Home data privacy, on page 20
- Send Call Home communications manually, on page 21

Configure Smart Call Home (Single Command)

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

Procedure

Step 1 **configure terminal**

Example:

```
Router# configure terminal
```

Enters configuration mode.

Step 2 **call-home reporting** {**anonymous** | **contact-email-addr** *email-address*} [**http-proxy** {*ipv4-address* | *ipv6-address* | *name*} **port** *port-number*]

Example:

```
Router(config)# call-home reporting contact-email-addr email@company.com
```

Enables the basic configurations for Call Home using a single command.

- **anonymous**—Enables Call-Home TAC profile to send only crash, inventory, and test messages and send the messages anonymously.
- **contact-email-addr**—Enables Smart Call Home service full reporting capability and sends a full inventory message from Call-Home TAC profile to Smart Call Home server to start full registration process.
- **http-proxy** {*ipv4-address* | *ipv6-address* | *name*}—Configures an ipv4 or ipv6 address or server name. Maximum length is 64 characters.
- **port** *port-number*—Port number.

  Range is 1 to 65535.

Note
The HTTP proxy option allows you to make use of your own proxy server to buffer and secure Internet connections from your devices.

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 full registration mode, a Full Inventory message for full registration mode is sent out. If Call Home is enabled in anonymous mode, an anonymous inventory message is sent out. For more information about what is sent in these messages, see Alert Group trigger events and commands, on page 39.

Configure and Enable Smart Call Home

For application and configuration information about the Cisco Smart Call Home service, see the "Getting Started" section of the Smart Call Home User Guide at https://supportforums.cisco.com/community/4816/smart-call-home. This document includes configuration examples for sending Smart Call Home messages directly from your device or through a transport gateway (TG) aggregation point.



Note 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.

Enable and Disable Call Home

To enable or disable the Call Home feature, perform these steps:

Procedure

Step 1 **configure terminal**

Example:

```
Router# configure terminal
```

Enters configuration mode.

Step 2 **service call-home**

Example:

```
Router(config)# service call-home
```

Enables the Call Home feature.

Step 3 **no service call-home**

Example:

```
Router(config)# no service call-home
```

Disables the Call Home feature.

Configure contact information

Each router must include a contact e-mail address (except if Call Home is enabled in anonymous mode). You can optionally include a phone number, street address, contract ID, customer ID, and site ID.

To assign the contact information, perform these steps:

Procedure

Step 1 **configure terminal**

Example:

```
Router# configure terminal
```

Enters configuration mode.

Step 2 **call-home**

Example:

```
Router(config)# call-home
```

Enters the Call Home configuration submode.

Step 3 **contact-email-addr** *email-address*

Example:

```
Router(cfg-call-home)# contact-email-addr username@example.com
```

Designates your e-mail address. Enter up to 200 characters in e-mail address format with no spaces.

Step 4 **phone-number** *+phone-number*

Example:

```
Router(cfg-call-home)# phone-number +1-800-555-4567
```

(Optional) Assigns your phone number.

Note

The number must begin with a plus (+) prefix and may contain only dashes (-) and numbers. Enter up to 17 characters. If you include spaces, you must enclose your entry in quotes (“”).

Step 5 **street-address** *street-address*

Example:

```
Router(cfg-call-home)# street-address “1234 Picaboo Street, Any city, Any state, 12345“
```

(Optional) Assigns your street address where RMA equipment can be shipped. Enter up to 200 characters. If you include spaces, you must enclose your entry in quotes (“”).

Step 6 **customer-id** *text*

Example:

```
Router(cfg-call-home)# customer-id Customer1234
```

(Optional) Identifies customer ID. Enter up to 64 characters. If you include spaces, you must enclose your entry in quotes (“”).

Step 7 **site-id** *text*

Example:

```
Router(cfg-call-home)# site-id Site1ManhattanNY
```

(Optional) Identifies customer site ID. Enter up to 200 characters. If you include spaces, you must enclose your entry in quotes (“”).

Step 8 **contract-id** *text*

Example:

```
Router(cfg-call-home)# contract-id Company1234
```

(Optional) Identifies your contract ID for the router. Enter up to 64 characters. If you include spaces, you must enclose your entry in quotes (“”).

Example

This example shows how to configure contact information:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# call-home
Router(cfg-call-home)# contact-email-addr username@example.com
Router(cfg-call-home)# phone-number +1-800-555-4567
Router(cfg-call-home)# street-address “1234 Picaboo Street, Any city, Any state, 12345”
Router(cfg-call-home)# customer-id Customer1234
Router(cfg-call-home)# site-id Site1ManhattanNY
Router(cfg-call-home)# contract-id Company1234
Router(cfg-call-home)# exit
```

Configure 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.

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

You can configure the following attributes for a destination profile:

- Profile name—String that uniquely identifies each user-defined destination profile. The profile name is limited to 31 characters and is not case-sensitive.

Note You cannot use **all** as a profile name.

- Transport method—Transport mechanism, either e-mail or HTTP (including HTTPS), for delivery of alerts.
  - For user-defined destination profiles, e-mail is the default, and you can enable either or both transport mechanisms. If you disable both methods, e-mail is enabled.
  - For the predefined Cisco TAC profile, you can enable either transport mechanism, but not both.
- Destination address—The actual address related to the transport method to which the alert should be sent.
- Message formatting—The message format used for sending the alert. The format options for a user-defined destination profile are long-text, short-text, or XML. The default is XML. For the predefined Cisco TAC 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.

  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.

This section contains these subsections:

- Create a new destination profile, on page 8
- Copy a destination profile, on page 10
- Set profiles to anonymous mode, on page 10

Create a new destination profile

To create and configure a new destination profile, perform these steps:

Procedure

Step 1 **configure terminal**

Example:

```
Router# configure terminal
```

Enters configuration mode.

Step 2 **call-home**

Example:

```
Router(config)# call-home
```

Enters the Call Home configuration submode.

Step 3 **profile** *name*

Example:

```
Router(config-call-home)# profile profile1
```

Enters the Call Home destination profile configuration submode for the specified destination profile. If the specified destination profile does not exist, it is created.

Step 4 [**no**] **destination transport-method** {**email** | **http**}

Example:

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

(Optional) Enables the message transport method. The **no** option disables the method.

Step 5 **destination address** {**email** *email-address* | **http** *url*}

Example:

```
Router(cfg-call-home-profile)# destination address email myaddress@example.com
```

Configures the destination e-mail address or URL to which Call Home messages are sent.

Note
When entering a destination URL, include either **http://** or **https://**, depending on whether the server is a secure server.

Step 6 **destination preferred-msg-format** {**long-text** | **short-text** | **xml**}

Example:

```
Router(cfg-call-home-profile)# destination preferred-msg-format xml
```

(Optional) Configures a preferred message format. The default is XML.

Step 7 **destination message-size-limit** *bytes*

Example:

```
Router(cfg-call-home-profile)# destination message-size-limit 3145728
```

(Optional) Configures a maximum destination message size for the destination profile.

Step 8 **active**

Example:

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

Enables the destination profile. By default, the profile is enabled when it is created.

Step 9 **end**

Example:

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

Returns to privileged EXEC mode.

Step 10 **show call-home profile** {*name* | **all**}

Example:

```
Router# show call-home profile profile1
```

Displays the destination profile configuration for the specified profile or all configured profiles.

Copy a destination profile

To create a new destination profile by copying an existing profile, perform these steps:

Procedure

Step 1 **configure terminal**

Example:

```
Router# configure terminal
```

Enters configuration mode.

Step 2 **call-home**

Example:

```
Router(config)# call-home
```

Enters the Call Home configuration submode.

Step 3 **copy profile** *source-profile target-profile*

Example:

```
Router(cfg-call-home)# copy profile profile1 profile2
```

Creates a new destination profile with the same configuration settings as the existing destination profile.

Set profiles to anonymous mode

To set an anonymous profile, perform these steps:

Procedure

Step 1 **configure terminal**

Example:

```
Router# configure terminal
```

Enters configuration mode.

Step 2 **call-home**

Example:

```
Router(config)# call-home
```

Enters the Call Home configuration submode.

Step 3 **profile** *name*

Example:

```
Router(cfg-call-home) profile Profile-1
```

Enables the profile configuration mode.

Step 4 **anonymous-reporting-only**

Example:

```
Router(cfg-call-home-profile)# anonymous-reporting-only
```

Sets the profile to anonymous mode.

Note
By default, Call Home sends a full report of all types of events subscribed in the profile. When **anonymous-reporting-only** is set, only crash, inventory, and test messages will be sent.

Subscribe to alert groups

An alert group is a predefined subset of Call Home alerts supported in all routers. Different types of Call Home alerts are grouped into different alert groups depending on their type. These alert groups are available:

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

This section contains these subsections:

- Periodic notification, on page 14
- Message severity threshold, on page 14
- Configure a snapshot command list, on page 15

The triggering events for each alert group are listed in Alert Group trigger events and commands, on page 39, and the contents of the alert group messages are listed in Message Contents, on page 46.

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

Note A Call Home alert is only sent to destination profiles that have subscribed to the alert group containing that Call Home alert. In addition, the alert group must be enabled.

To subscribe a destination profile to one or more alert groups, perform these steps:

Procedure

Step 1 **configure terminal**

Example:

```
Router# configure terminal
```

Enters configuration mode.

Step 2 **call-home**

Example:

```
Router(config)# call-home
```

Enters Call Home configuration submode.

Step 3 **alert-group** {**all** | **configuration** | **environment** | **inventory** | **syslog** | **crash** | **snapshot**}

Example:

```
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 4 **profile** *name*

Example:

```
Router(cfg-call-home)# profile profile1
```

Enters the Call Home destination profile configuration submode for the specified destination profile.

Step 5 **subscribe-to-alert-group all**

Example:

```
Router(cfg-call-home-profile)# subscribe-to-alert-group all
```

Subscribes to all available alert groups using the lowest severity.

You can subscribe to alert groups individually by specific type, as described in Step 6 through Step 11.

Note
This command subscribes to the syslog debug default severity. This causes a large number of syslog messages to generate. You should subscribe to alert groups individually, using appropriate severity levels and patterns when possible.

Step 6 **subscribe-to-alert-group configuration** [**periodic** {**daily** *hh:mm* | **monthly** *date hh:mm* | **weekly** *day hh:mm*}]

Example:

```
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, as described in Periodic notification, on page 14.

Step 7 **subscribe-to-alert-group environment** [**severity** {**catastrophic** | **disaster** | **fatal** | **critical** | **major** | **minor** | **warning** | **notification** | **normal** | **debugging**}]

Example:

```
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, as described in Message severity threshold, on page 14.

Step 8 **subscribe-to-alert-group inventory** [**periodic** {**daily** *hh:mm* | **monthly** *date hh:mm* | **weekly** *day hh:mm*}]

Example:

```
Router(cfg-call-home-profile)# subscribe-to-alert-group inventory periodic monthly 1 12:00
```

Subscribes this destination profile to the Inventory alert group. The Inventory alert group can be configured for periodic notification, as described in Periodic notification, on page 14.

Step 9 **subscribe-to-alert-group syslog** [**severity** {**catastrophic** | **disaster** | **fatal** | **critical** | **major** | **minor** | **warning** | **notification** | **normal** | **debugging**}]

Example:

```
Router(cfg-call-home-profile)# subscribe-to-alert-group environment severity major
```

Subscribes this destination profile to the Syslog alert group. The Syslog alert group can be configured to filter messages based on severity, as described in Message severity threshold, on page 14.

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 10 **subscribe-to-alert-group crash**

Example:

```
Router(cfg-call-home-profile)# [no | default]
subscribe-to-alert-group crash
```

Subscribes to the Crash alert group in user profile. By default, TAC profile subscribes to the Crash alert group and cannot be unsubscribed.

Step 11 **subscribe-to-alert-group snapshot periodic** {**daily** *hh:mm* | **hourly** *mm* | **interval** *mm* | **monthly** *date hh:mm* | **weekly** *day hh:mm*}

Example:

```
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, as described in Periodic notification, on page 14.

By default, the Snapshot alert group has no command to run. You can add commands into the alert group, as described in Configure a snapshot command list, on page 15. In doing so, the output of the commands added in the Snapshot alert group will be included in the snapshot message.

Step 12 **exit**

Example:

```
Router(cfg-call-home-profile)# exit
```

Exits the Call Home destination profile configuration submode.

Periodic notification

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

- Daily—Specifies the time of day to send, using an hour:minute format *hh:mm*, with a 24-hour clock (for example, 14:30).
- Weekly—Specifies the day of the week and time of day in the format *day hh:mm*, where the day of the week is spelled out (for example, Monday).
- Monthly—Specifies 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

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

The severity threshold is configured using the keywords listed in the following table. The severity threshold ranges from catastrophic (level 9, highest level of urgency) to debugging (level 0, lowest level of urgency). If no severity threshold is configured for the Syslog or Environment alert groups, the default is debugging (level 0). The Configuration and Inventory alert groups do not allow severity configuration; severity is always set as normal.

Note Call Home severity levels are not the same as system message logging severity levels.

Table 1: Severity and Syslog level mapping

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, immediate attention needed.
5	major	Critical (2)	Major conditions.
4	minor	Error (3)	Minor conditions.
3	warning	Warning (4)	Warning conditions.
2	notification	Notice (5)	Basic notification and informational messages. Possibly independently insignificant.
1	normal	Information (6)	Normal event signifying return to normal state.
0	debugging	Debug (7)	Debugging messages.

Configure a snapshot command list

To configure a snapshot command list, perform these steps:

Procedure

Step 1 **configure terminal**

Example:

```
Router# configure terminal
```

Enters configuration mode.

Step 2 **call-home**

Example:

```
Router(config)# call-home
```

Enters Call Home configuration submode.

Step 3 [**no** | **default**] **alert-group-config snapshot**

Example:

```
Router(cfg-call-home)# alert-group-config snapshot
```

Enters snapshot configuration mode.

The **no** or **default** command will remove all snapshot command.

Step 4 [**no** | **default**] **add-command** *command string*

Example:

```
Router(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.

- *command string*—IOS command. Maximum length is 128.

Step 5 **exit**

Example:

```
Router(cfg-call-home-snapshot)# exit
```

Exits and saves the configuration.

Configure general e-mail options

To use the e-mail message transport, you must configure at least one Simple Mail Transfer Protocol (SMTP) e-mail server address. You can configure the from and reply-to e-mail addresses, and you can specify up to four backup e-mail servers.

Note these guidelines when configuring general e-mail options:

- Backup e-mail servers can be defined by repeating the **mail-server** command using different priority numbers.
- The **mail-server priority** number parameter can be configured from 1 to 100. The server with the highest priority (lowest priority number) is tried first.

To configure general e-mail options, perform these steps:

Procedure

Step 1 **configure terminal**

Example:

```
Router# configure terminal
```

Enters configuration mode.

Step 2 **call-home**

Example:

```
Router(config)# call-home
```

Enters Call Home configuration submode.

Step 3 **mail-server** [{*ipv4-address* | *ipv6-address*} | *name*] **priority** *number*

Example:

```
Router(cfg-call-home)# mail-server stmp.example.com priority 1
```

Assigns an e-mail server address and its relative priority among configured e-mail servers.

Provide either of these:

- The e-mail server's IP address.

- The e-mail server's fully qualified domain name (FQDN) of 64 characters or less.

Assign a priority number between 1 (highest priority) and 100 (lowest priority).

Step 4 **sender from** *email-address*

Example:

```
Router(cfg-call-home)# sender from username@example.com
```

(Optional) Assigns the e-mail address that appears in the from field in Call Home e-mail messages. If no address is specified, the contact e-mail address is used.

Step 5 **sender reply-to** *email-address*

Example:

```
Router(cfg-call-home)# sender reply-to username@example.com
```

(Optional) Assigns the e-mail address that appears in the reply-to field in Call Home e-mail messages.

Step 6 **source-interface** *interface-name*

Example:

```
Router(cfg-call-home)# source-interface loopback1
```

Assigns the source interface name to send call-home messages.

- *interface-name*—Source interface name. Maximum length is 64.

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 allows all HTTP clients on the device to use the same source interface.

Step 7 **vrf** *vrf-name*

Example:

```
Router(cfg-call-home)# vrf vpn1
```

(Optional) Specifies the VRF instance to send call-home e-mail messages. If no vrf is specified, the global routing table is used.

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 to specify the VRF instance that will be used for all HTTP clients on the device.

Example

This example shows the configuration of general e-mail parameters, including a primary and secondary e-mail server:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# call-home
Router(cfg-call-home)# mail-server smtp.example.com priority 1
Router(cfg-call-home)# mail-server 192.0.2.1 priority 2
Router(cfg-call-home)# sender from username@example.com
```

```
Router(cfg-call-home)# sender reply-to username@example.com
Router(cfg-call-home)# source-interface loopback1
Router(cfg-call-home)# vrf vpn1
Router(cfg-call-home)# exit
Router(config)#
```

Specify rate limit for sending Call Home messages

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

Procedure

Step 1 **configure terminal**

Example:

```
Router# configure terminal
```

Enters configuration mode.

Step 2 **call-home**

Example:

```
Router(config)# call-home
```

Enters Call Home configuration submode.

Step 3 **rate-limit** *number*

Example:

```
Router(cfg-call-home)# rate-limit 40
```

Specifies a limit on the number of messages sent per minute.

- *number*—Range is 1 to 60. The default is 20.

Specify HTTP proxy server

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

Procedure

Step 1 **configure terminal**

Example:

```
Router# configure terminal
```

Enters configuration mode.

Step 2 **call-home**

Example:

```
Router(config)# call-home
```

Enters Call Home configuration submode.

Step 3 **http-proxy** {*ipv4-address* | *ipv6-address* | *name*} **port** *port-number*

Example:

```
Router(cfg-call-home)# http-proxy 192.0.2.1 port 1
```

Specifies the proxy server for the HTTP request.

Enable AAA authorization to run IOS commands for Call Home messages

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

Procedure

Step 1 **configure terminal**

Example:

```
Router# configure terminal
```

Enters configuration mode.

Step 2 **call-home**

Example:

```
Router(config)# call-home
```

Enters Call Home configuration submode.

Step 3 **aaa-authorization**

Example:

```
Router(cfg-call-home)# aaa-authorization
```

Enables AAA authorization.

Note
By default, AAA authorization is disabled for Call Home.

Step 4 **aaa-authorization** [**username** *username*]

Example:

```
Router(cfg-call-home)# aaa-authorization username user
```

Specifies the username for authorization.

- **username** *username*—Default username is callhome. Maximum length is 64.

Configure syslog throttling

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

Procedure

Step 1 **configure terminal**

Example:

```
Router# configure terminal
```

Enters configuration mode.

Step 2 **call-home**

Example:

```
Router(config)# call-home
```

Enters Call Home configuration submode.

Step 3 [**no**] **syslog-throttling**

Example:

```
Router(cfg-call-home)# syslog-throttling
```

Enables or disables call-home syslog message throttling and avoids sending repetitive call-home syslog messages.

Note
By default, syslog message throttling is enabled.

Configure Call Home data privacy

The data-privacy command scrubs data, such as 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, the **show** command output is not being scrubbed except for configuration messages in the outputs for the **show running-config all** and the**show startup-config data** commands.

Procedure

Step 1 **configure terminal**

Example:

```
Router# configure terminal
```

Enters configuration mode.

Step 2 **call-home**

Example:

```
Router(config)# call-home
```

Enters Call Home configuration submode.

Step 3 **data-privacy** {**level** {**normal** | **high**} | **hostname**}

Example:

```
Router(cfg-call-home)# data-privacy level high
```

Scrubs data from running configuration file to protect the privacy of the user. The default data-privacy level is normal.

Note
Enabling the data-privacy command can affect CPU utilization when scrubbing a large amount of data.

- **normal**—Scrubs all normal-level commands.
- **high**—Scrubs all normal-level commands plus the IP domain name and IP address commands.
- **hostname**—Scrubs all high-level commands plus the hostname command.

Note
Scrubbing the hostname from configuration messages can cause Smart Call Home processing failure on some platforms.

Send Call Home communications manually

You can manually send several types of Call Home communications. To send Call Home communications, perform the tasks in this section. This section contains these subsections:

- Send a Call Home Test Message Manually, on page 21
- Send Call Home alert group messages manually, on page 22
- Submit Call Home analysis and report requests, on page 23
- Manually send command output message for one command or a command list, on page 24

Send a Call Home Test Message Manually

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

To manually send a Call Home test message, perform these step:

Procedure

call-home test [*"test-message"*] **profile** *name*

Example:

```
Router# call-home test profile profile1
```

Sends a test message to the specified destination profile. The user-defined test message text is optional but must be enclosed in quotes (“”) if it contains spaces. If no user-defined message is configured, a default message is sent.

Send Call Home alert group messages manually

You can use the **call-home send** command to manually send a specific alert group message.

Note these guidelines when manually sending a Call Home alert group message:

- Only the crash, snapshot, configuration, and inventory alert groups can be sent manually.
- When you manually trigger a crash, 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 crash, 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.

To manually trigger Call Home alert group messages, perform these steps:

Procedure

Step 1 **call-home send alert-group snapshot** [**profile** *name*]

Example:

```
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 2 **call-home send alert-group crash** [**profile** *name*]

Example:

```
Router# call-home send alert-group crash profile profile1
```

Sends a crash alert group message to one destination profile if specified, or to all subscribed destination profiles.

Step 3 **call-home send alert-group configuration** [**profile** *name*]

Example:

```
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.

Step 4 **call-home send alert-group inventory** [**profile** *name*]

Example:

```
Router# call-home send alert-group inventory profile profile1
```

Sends an inventory alert group message to one destination profile if specified, or to all subscribed destination profiles.

Submit Call Home analysis and report requests

You can use the **call-home request** command to submit information about your system to Cisco to receive helpful analysis and report information specific to your system. You can request a variety of reports, including security alerts, known bugs, best practices, and command references.

Note these 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 recipient profile does not need to be enabled for the call-home request. The profile should specify the e-mail address where the transport gateway is configured so that the request message can be forwarded to the Cisco TAC and the user 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 e-mail address of the registered user. If no *user-id* is specified, the response is sent to the contact e-mail address of the device.
- Based on the keyword specifying the type of report requested, the following information is returned:
  - **config-sanity**—Information on best practices as related to the current running configuration.
  - **bugs-list**—Known bugs in the running version and in the currently applied features.
  - **command-reference**—Reference links to all commands in the running configuration.
  - **product-advisory**—Product Security Incident Response Team (PSIRT) notices, End of Life (EOL) or End of Sales (EOS) notices, or field notices (FN) that may affect the devices in your network.

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

Procedure

Step 1 **call-home request output-analysis** *"show-command"* [**profile** *name*] [**ccoid** *user-id*]

Example:

```
Router# call-home request output-analysis "show diag" profile TG
```

Sends the output of the specified show command for analysis. The show command must be contained in quotes ("").

Step 2 **call-home request** {**config-sanity** | **bugs-list** | **command-reference** | **product-advisory**} [**profile** *name*] [**ccoid** *user-id*]

Example:

```
Router# call-home request config-sanity profile TG
```

Sends the output of a predetermined set of commands such as the **show running-config all**, **show version** or **show module** commands, for analysis. In addition, the **call home request product-advisory** sub-command includes all inventory alert group commands. The keyword specified after **request** specifies the type of report requested.

Example

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

```
Router# call-home request output-analysis "show diag" profile TG
```

Manually send command output message for one command or a command list

You can use the **call-home send** command to execute an IOS command or a list of IOS commands and send the command output through HTTP or e-mail protocol.

Note these guidelines when sending the output of a command:

- The specified IOS command or list of IOS commands can be any run command, including commands for all modules. The command must be contained in quotes (“”).
- If the e-mail option is selected using the “email” keyword and an e-mail address is specified, the command output is sent to that address. If neither the e-mail nor the HTTP option is specified, the output is sent in long-text format with the specified service request number to the Cisco TAC (attach@cisco.com).
- If neither the “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 e-mail.
- If the HTTP option is specified, the CiscoTac-1 profile destination HTTP or HTTPS URL is used as the destination. The destination e-mail address can be specified so that Smart Call Home can forward the message to the e-mail address. The user must specify either the destination e-mail address or an SR number but they can also specify both.

To execute a command and send the command output, perform these step:

Procedure

call-home send {*cli command* | *cli list*} [**email** *email* **msg-format** {**long-text** | **xml**} | **http** {**destination-email-address** *email*}] [**tac-service-request** *SR#*]

Example:

```
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 e-mail or HTTP.

- {*cli command* | *cli list*}—Specifies the IOS command or list of IOS commands (separated by ‘;’). It can be any run command, including commands for all modules. The commands must be contained in quotes (“”).
- **email** *email* **msg-format {long-text | xml}**—If the **email** option is selected, the command output will be sent to the specified e-mail address in long-text or XML format with the service request number in the subject. The e-mail

address, the service request number, or both must be specified. The service request number is required if the e-mail address is not specified (default is attach@cisco.com for long-text format and callhome@cisco.com for XML format).

- **http** {**destination-email-address** *email*}—If the **http** option is selected, the command output will be sent to Smart Call Home backend server (URL specified in TAC profile) in XML format.

  destination-email-address *email* can be specified so that the backend server can forward the message to the e-mail address. The e-mail address, the service request number, or both must be specified.

- **tac-service-request** *SR#*—Specifies the service request number. The service request number is required if the e-mail address is not specified.

Example

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

```
Router# call-home send "show diag" email support@example.com
```

This example shows the command output sent in long-text format to attach@cisco.com, with the SR number specified:

```
Router# call-home send "show version; show run" tac-service-request 123456
```

This example shows the command output sent in XML message format to callhome@cisco.com:

```
Router# call-home send "show version; show run" email callhome@cisco.com msg-format xml
```

This example shows the command output sent in XML message format to the Cisco TAC backend server, with the SR number specified:

```
Router# call-home send "show version; show run" http tac-service-request 123456
```

This example shows the command output sent to the Cisco TAC backend server through the HTTP protocol and forwarded to a user-specified email address:

```
Router# call-home send "show version; show run" http destination-email-address
user@company.com
```

Configure 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 and 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 that can be used to resolve known problems in customers networks.

Information about Diagnostic Signatures

- Diagnostic Signatures, on page 26

- Prerequisites for Diagnostic Signatures, on page 26
- Download Diagnostic Signatures, on page 27
- Diagnostic Signature Workflow, on page 27
- Diagnostic Signature events and actions, on page 28
- Diagnostic Signature event detection, on page 28
- Diagnostic Signature actions , on page 28
- Diagnostic Signature variables, on page 29

Diagnostic Signatures

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

Diagnostic Signature provides the ability to define more types of events and trigger types than the standard Call Home feature supports. The Diagnostic Signature subsystem downloads and processes files on a device as well as 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. These files are digitally signed by Cisco or a third party to certify their integrity, reliability, and security.

The structure of a DS file can be in one of these formats:

- Metadata-based simple signature that specifies the event type and contains other information that can be used 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 that specifies new events in the event register line and additional action in the Tcl script.
- Combination of both the formats above.

The basic information 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.

Prerequisites for Diagnostic Signatures

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

- You must assign one or more DSs to the device. For more information on how to assign DSs to devices, see Download Diagnostic Signatures, on page 27.
- HTTP/Secure HTTP (HTTPS) transport is required for downloading DS files. You must 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.

Download Diagnostic Signatures

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

Cisco software uses a PKI Trustpool Management feature, which is enabled by default on devices, to create a scheme to provision, store, and manage a pool of certificates from known certification authorities (CAs). The trustpool feature 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 happens, the response to the periodic inventory message from the same device will include a field to notify device to start its periodic DS download/update. In a DS update request message, the status and revision number of the DS is included such that only a DS with the latest revision number is downloaded.

Forced-download downloads a specific DS or a set of DSes. 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 Workflow

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

- Find the DS(es) you want to download and assign them to the device. This step is mandatory for regular periodic download, but not required for forced download.
- The device downloads all assigned DS(es) or a specific DS by regular periodic download or by on-demand forced download.
- The device verifies the digital signature of every single DS. If verification passes, the device stores the DS file into a non-removable disk, such as bootflash or hard disk, so that DS files can be read after the device is reloaded. On the router, the DS file is stored in the bootflash:/call home directory.
- The device continues sending periodic regular DS download requests to get the latest revision of DS and replace the older one in device.

- The device monitors the event and executes the actions defined in the DS when the event happens.

Diagnostic Signature events and actions

The events and actions sections are the key areas used in diagnostic signatures. The event section defines all event attributes that are used for event detection. The action section lists all actions which should be performed after the event happens, such as 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 in one of these two types:

- DS event specification type: syslog, periodic, configuration, Online Insertion Removal (OIR) immediate, and call home 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 event 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 that are used to customize the files.

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 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.

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 supported DS variable types are:

- 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

- Configure the Call Home Service for Diagnostic Signatures, on page 29
- Configure Diagnostic Signatures, on page 31

Configure the Call Home Service for Diagnostic Signatures

Configure the Call Home Service 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 we recommend that you use it. If used, you only need to change the destination transport-method to the **http** setting.

Procedure

Step 1 **configure terminal**

Example:

```
Router# configure terminal
```

Enters global configuration mode.

Step 2 **service call-home**

Example:

```
Router(config)# service call-home
```

Enables Call Home service on a device.

Step 3 **call-home**

Example:

```
Router(config)# call-home
```

Enters call-home configuration mode for the configuration of Call Home settings.

Step 4 **contact-email-addr** *email-address*

Example:

```
Router(cfg-call-home)# contact-email-addr userid@example.com
```

(Optional) Assigns an email address to be used for Call Home customer contact.

Step 5 **mail-server** {*ipv4-addr* | *name*} **priority** *number*

Example:

```
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 defined in any DS.

Step 6 **profile** *profile-name*

Example:

```
Router(cfg-call-home)# profile user1
```

Configures a destination profile for Call Home and enters call-home profile configuration mode.

Step 7 **destination transport-method** {**email** | **http**}

Example:

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

Specifies a transport method for a destination profile in the Call Home.

Note
To configure diagnostic signatures, you must use the **http** option.

Step 8 **destination address** {**email** *address* | **http** *url*}

Example:

```
Router(cfg-call-home-profile)# destination address http
https://tools.cisco.com/its/service/oddce/services/DDCEService
```

Configures the address type and location to which call-home messages are sent.

Note
To configure diagnostic signatures, you must use the **http** option.

Step 9 **subscribe-to-alert-group inventory** [**periodic** {**daily** *hh:mm* | **monthly** *day hh:mm* | **weekly** *day hh:mm*}]

Example:

```
Router(cfg-call-home-profile)# subscribe-to-alert-group inventory periodic daily 14:30
```

Configures a destination profile to send messages for the Inventory alert group for Call Home.

- This command is used only for the periodic downloading of DS files.

Step 10 **exit**

Example:

```
Router(cfg-call-home-profile)# exit
```

Exits call-home profile configuration mode and returns to call-home configuration mode.

What to do next

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

Configure Diagnostic Signatures

Before you begin

Configure the 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

Step 1 **call-home**

Example:

```
Router(config)# call-home
```

Enters call-home configuration mode for the configuration of Call Home settings.

Step 2 **diagnostic-signature**

Example:

```
Router(cfg-call-home)# diagnostic-signature
```

Enters call-home diagnostic signature mode.

Step 3 **profile** *ds-profile-name*

Example:

```
Router(cfg-call-home-diag-sign)# profile user1
```

Specifies the destination profile on a device that DS uses.

Step 4 **environment** *ds_env-var-name ds-env-var-value*

Example:

```
Router(cfg-call-home-diag-sign)# environment ds_env1 envarval
```

Sets the environment variable value for DS on a device.

Step 5 **end**

Example:

```
Router(cfg-call-home-diag-sign)# end
```

Exits call-home diagnostic signature mode and returns to privileged EXEC mode.

Step 6 **call-home diagnostic-signature** [{**deinstall** | **download**} {*ds-id* | **all**} | **install** *ds-id*]

Example:

```
Router# call-home diagnostic-signature download 6030
```

Downloads, installs, and uninstalls diagnostic signature files on a device.

Step 7 **show call-home diagnostic-signature** [*ds-id* {**actions** | **events** | **prerequisite** | **prompt** | **variables** | **failure** | **statistics** | **download**}]

Example:

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

Displays the call-home diagnostic signature information.

Configuration Examples for Diagnostic Signatures

The following example shows how to enable the periodic downloading request for diagnostic signature (DS) files. This configuration will send download requests to the service call-home server daily at 2:30 p.m. to check for updated DS files. The transport method is set to HTTP.

```
Router> enable
Router# configure terminal
Router(config)# service call-home
Router(config)# call-home
Router(cfg-call-home)# contact-email-addr userid@example.com
Router(cfg-call-home)# mail-server 10.1.1.1 priority 4
Router(cfg-call-home)# profile user-1
Router(cfg-call-home-profile)# destination transport-method http
Router(cfg-call-home-profile)# destination address http
https://tools.cisco.com/its/service/oddce/services/DDCEService
Router(cfg-call-home-profile)# subscribe-to-alert-group inventory periodic daily 14:30
Router(cfg-call-home-profile)# exit
Router(cfg-call-home)# diagnostic-signature
Router(cfg-call-home-diag-sign)# profile user1
Router(cfg-call-home-diag-sign)# environment ds_env1 envarval
Router(cfg-call-home-diag-sign)# end
```

The following is sample output from the **show call-home diagnostic-signature** command for the configuration displayed above:

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

Current diagnostic-signature settings:
Diagnostic-signature: enabled
Profile: user1 (status: ACTIVE)
Environment variable:
ds_env1: abc
Downloaded DSes:
DS ID    DS Name                          Revision Status     Last Update (GMT+00:00)
-------- -------------------------------- -------- ---------- -------------------
6015     CronInterval                     1.0      registered 2013-01-16 04:49:52
6030     ActCH                            1.0      registered 2013-01-16 06:10:22
6032     MultiEvents                      1.0      registered 2013-01-16 06:10:37
6033     PureTCL                          1.0      registered 2013-01-16 06:11:48
```

Display Call Home Configuration Information

You can use variations of the **show call-home** command to display Call Home configuration information.

Procedure

Step 1 **show call-home**

Example:

```
Router# show call-home
```

Displays the Call Home configuration in summary.

Step 2 **show call-home detail**

Example:

```
Router# show call-home detail
```

Displays the Call Home configuration in detail.

Step 3 **show call-home alert-group**

Example:

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

Displays the available alert groups and their status.

Step 4 **show call-home mail-server status**

Example:

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

Checks and displays the availability of the configured e-mail server(s).

Step 5 **show call-home profile** {**all** | *name*}

Example:

```
Router# show call-home profile all
```

Displays the configuration of the specified destination profile. Use the **all** keyword to display the configuration of all destination profiles.

Step 6 **show call-home statistics** [**detail** | **profile** *profile_name*]

Example:

```
Router# show call-home statistics
```

Displays the statistics of Call Home events.

Examples

Call Home information in summary

Call Home information in detail

Available Call Home alert groups

E-mail server status information

Information for all destination profiles

Information for a user-defined destination profile

Call Home statistics

These examples show the sample output when using different options of the **show call-home** command.

```
Router# show call-home
Current call home settings:
    call home feature : enable
    call home message's from address: router@example.com
    call home message's reply-to address: support@example.com

    vrf for call-home messages: Not yet set up

    contact person's email address: technical@example.com

    contact person's phone number: +1-408-555-1234
    street address: 1234 Picaboo Street, Any city, Any state, 12345
    customer ID: ExampleCorp
    contract ID: X123456789
    site ID: SantaClara

    source ip address: Not yet set up
    source interface: GigabitEthernet0/0
    Mail-server[1]: Address: 192.0.2.1 Priority: 1
    Mail-server[2]: Address: 209.165.202.254 Priority: 2
    http proxy: 192.0.2.2:80

    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 version
    Snapshot command[1]: show clock

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

Profiles:
    Profile Name: campus-noc
    Profile Name: CiscoTAC-1
Router#
```

```
Router# show call-home detail
Current call home settings:
    call home feature : enable
    call home message's from address: router@example.com
    call home message's reply-to address: support@example.com

    vrf for call-home messages: Not yet set up

    contact person's email address: technical@example.com

    contact person's phone number: +1-408-555-1234
    street address: 1234 Picaboo Street, Any city, Any state, 12345
    customer ID: ExampleCorp
    contract ID: X123456789
    site ID: SantaClara

    source ip address: Not yet set up
    source interface: GigabitEthernet0/0
    Mail-server[1]: Address: 192.0.2.1 Priority: 1
    Mail-server[2]: Address: 209.165.202.254 Priority: 2
    http proxy: 192.0.2.2:80

    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 version
    Snapshot command[1]: show clock

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

```
Profiles:

Profile Name: campus-noc
    Profile status: ACTIVE
    Preferred Message Format: xml
    Message Size Limit: 3145728 Bytes
    Transport Method: email
    Email address(es): noc@example.com
    HTTP  address(es): Not yet set up

    Alert-group               Severity
    ------------------------  ------------
    configuration             normal
    crash                     normal
    environment               debug
    inventory                 normal

    Syslog-Pattern            Severity
    ------------------------  ------------
 .*CALL_LOOP.*             debug

Profile Name: CiscoTAC-1
    Profile status: INACTIVE
    Profile mode: Full Reporting
    Preferred Message Format: xml
    Message Size Limit: 3145728 Bytes
    Transport Method: email
    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 14 day of the month at 11:12

    Periodic inventory info message is scheduled every 14 day of the month at 10:57

    Alert-group               Severity
    ------------------------  ------------
    crash                     normal
    environment               minor

    Syslog-Pattern            Severity
    ------------------------  ------------
 .*CALL_LOOP.*             debug
Router#
```

```
Router# show call-home alert-group
Available alert groups:
    Keyword                   State   Description
    ------------------------ ------- --------------------------------
    configuration             Enable  configuration info
    crash                     Enable  crash and traceback info
    environment               Enable  environmental info
    inventory                 Enable  inventory info
    snapshot                  Enable  snapshot info
    syslog                    Enable  syslog info
Router#
```

```
Router# show call-home mail-server status
Please wait. Checking for mail server status ...

    Mail-server[1]: Address: 192.0.2.1 Priority: 1 [Not Available]
    Mail-server[2]: Address: 209.165.202.254 Priority: 2 [Available]
Router#
```

```
Router# show call-home profile all

Profile Name: campus-noc
    Profile status: ACTIVE
    Preferred Message Format: xml
    Message Size Limit: 3145728 Bytes
    Transport Method: email
    Email address(es): noc@example.com
    HTTP  address(es): Not yet set up

    Alert-group               Severity
    ------------------------  ------------
    configuration             normal
    crash                     normal
    environment               debug
    inventory                 normal

    Syslog-Pattern            Severity
    ------------------------  ------------
 .*CALL_LOOP.*             debug

Profile Name: CiscoTAC-1
    Profile status: INACTIVE
    Profile mode: Full Reporting
    Preferred Message Format: xml
    Message Size Limit: 3145728 Bytes
    Transport Method: email
    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 14 day of the month at 11:12

    Periodic inventory info message is scheduled every 14 day of the month at 10:57

    Alert-group               Severity
    ------------------------  ------------
    crash                     normal
    environment               minor

    Syslog-Pattern            Severity
    ------------------------  ------------
 .*CALL_LOOP.*             debug
Router#
```

```
Router# show call-home profile campus-noc
Profile Name: campus-noc
    Profile status: ACTIVE
    Preferred Message Format: xml
    Message Size Limit: 3145728 Bytes
    Transport Method: email
    Email address(es): noc@example.com
    HTTP  address(es): Not yet set up

    Alert-group               Severity
    ------------------------  ------------
    configuration             normal
    crash                     normal
    environment               debug
    inventory                 normal

    Syslog-Pattern            Severity
    ------------------------  ------------
 .*CALL_LOOP.*             debug

Router#
```

```
Router# show call-home statistics
Message Types    Total                Email                HTTP
-------------    -------------------- -------------------- -------------------
Total Success   3                    3                    0
    Config      3                    3                    0
    Crash       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

Total In-Queue  0                    0                    0
    Config      0                    0                    0
    Crash       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

Total Failed    0                    0                    0
    Config      0                    0                    0
    Crash       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

Total Ratelimit
      -dropped  0                    0                    0
    Config      0                    0                    0
    Crash       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

Last call-home message sent time: 2011-09-26 23:26:50 GMT-08:00
Router#
```

Default Call Home settings

The table lists the default Call Home settings.

Table 2: Default Call Home settings

Parameters	Default
Call Home feature status	Disabled
User-defined profile status	Active
Predefined Cisco TAC profile status	Inactive
Transport method	E-mail
Message format type	XML
Destination message size for a message sent in long text, short text, or XML format	3,145,728
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 Group trigger events and commands

Call Home trigger events are grouped into alert groups, with each alert group assigned commands to execute when an event occurs. The command output is included in the transmitted message. The following table lists the trigger events included in each alert group, including the severity level of each event and the executed commands for the alert group.

Table 3: Call Home Alert Groups, Events, and Actions

Alert Group	Call Home Trigger Event	Syslog Event	Severity	Description and Commands Executed
Crash	SYSTEM_ CRASH	–	–	Events related to software crash. The following commands are executed: **show version** **show logging** **show region** **show inventory** **show stack** **crashinfo file** (this command shows the contents of the crashinfo file)
–	TRACEBACK	–	–	Detects software traceback events. The following commands are executed: **show version** **show logging** **show region** **show stack**

Alert Group	Call Home Trigger Event	Syslog Event	Severity	Description and Commands Executed
Configuration	–	–	–	User-generated request for configuration or configuration change event. The following commands are executed: **show platform** **show inventory** **show running-config all** **show startup-config** **show version**
Environmental	–	–	–	Events related to power, fan, and environment sensing elements such as temperature alarms. The following commands are executed: **show environment** **show inventory** **show platform** **show logging**
–	–	SHUT	0	Environmental Monitor initiated shutdown.
–	–	ENVCRIT	2	Temperature or voltage measurement exceeded critical threshold.
–	–	BLOWER	3	Required number of fan trays is not present.

Alert Group	Call Home Trigger Event	Syslog Event	Severity	Description and Commands Executed
–	–	ENVWARN	4	Temperature or voltage measurement exceeded warning threshold.
–	–	RPSFAIL	4	Power supply may have a failed channel.
–	ENVM	PSCHANGE	6	Power supply name change.
–	–	PSLEV	6	Power supply state change.
–	–	PSOK	6	Power supply now appears to be working correctly.

Alert Group	Call Home Trigger Event	Syslog Event	Severity	Description and Commands Executed
Inventory	–	–	–	

Alert Group	Call Home Trigger Event	Syslog Event	Severity	Description and Commands Executed
				Inventory status should be provided whenever a unit is cold-booted or when FRUs are inserted or removed. This is considered a noncritical event, and the information is used for status and entitlement. Commands executed for all Inventory messages sent in anonymous mode and for Delta Inventory message sent in full registration mode: **show diag all eeprom detail** **show version** **show inventory oid** **show platform** Commands executed for Full Inventory message sent in full registration mode: **show platform** **show diag all eeprom detail** **show version** **show inventory oid** **show bootflash: all** **show data-corruption** **show interfaces** **show file systems** **show memory statistics**

Alert Group	Call Home Trigger Event	Syslog Event	Severity	Description and Commands Executed
				show process memory **show process cpu** **show process cpu history** **show license udi** **show license detail** **show buffers**
–	HARDWARE_ REMOVAL	REMCARD	6	Card removed from slot %d, interfaces disabled.
–	HARDWARE_ INSERTION	INSCARD	6	Card inserted in slot %d, interfaces administratively shut down.
Syslog	–	–	–	Event logged to syslog. The following commands are executed: **show inventory** **show logging**
–	SYSLOG	LOG_EMERG	0	System is unusable.
–	SYSLOG	LOG_ALERT	1	Action must be taken immediately.
–	SYSLOG	LOG_CRIT	2	Critical conditions.
–	SYSLOG	LOG_ERR	3	Error conditions.
–	SYSLOG	LOG_WARNING	4	Warning conditions.
–	SYSLOG	LOG_NOTICE	5	Normal but signification condition.
–	SYSLOG	LOG_INFO	6	Informational.
–	SYSLOG	LOG_DEBUG	7	Debug-level messages.

Alert Group	Call Home Trigger Event	Syslog Event	Severity	Description and Commands Executed
Test	–	TEST	–	User-generated test message. The following commands are executed: **show platform** **show inventory** **show version**

Message Contents

This section consists of tables which list the content formats of alert group messages.

The table lists the content fields of a short text message.

Table 4: Format for a short text message

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

The table shows the content fields that are common to all long text and XML messages. The fields specific to a particular alert group message are inserted at a point between the common fields. The insertion point is identified in the table.

Table 5: Common Fields for all long 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 event in ISO time notation: *YYYY-MM-DD HH:MM:SS GMT+HH:MM*.	CallHome/EventTime
Message name	Name of message. Specific event names are listed in the Alert Group trigger events and commands, on page 39.	For short text message only
Message type	Specifically “Call Home”.	CallHome/Event/Type

Data Item (Plain Text and XML)	Description (Plain Text and XML)	Call-Home Message Tag (XML Only)
Message subtype	Specific type of message: full, delta, test	CallHome/Event/SubType
Message group	Specifically “reactive”. Optional because default is “reactive”.	For long-text message only
Severity level	Severity level of message (see Message severity threshold, on page 14).	Body/Block/Severity
Source ID	Product type for routing through the workflow engine. This is typically the product family name.	For long-text message only
Device ID	Unique device identifier (UDI) for end device generating message. This field should be empty if the message is nonspecific to a fabric switch. The format is *type@Sid@serial*. • *type* is the product model number from backplane IDPROM. • @ is a separator character. • *Sid* is C, identifying the serial ID as a chassis serial number. • *serial* is the number identified by the Sid field. Example: CISCO3845@C@12345678	CallHome/CustomerData/ ContractData/DeviceId
Customer ID	Optional user-configurable field used for contract information or other ID by any support service.	CallHome/CustomerData/ ContractData/CustomerId
Contract ID	Optional user-configurable field used for contract information or other ID by any support service.	CallHome/CustomerData/ ContractData/CustomerId
Site ID	Optional user-configurable field used for Cisco-supplied site ID or other data meaningful to alternate support service.	CallHome/CustomerData/ ContractData/CustomerId

Data Item (Plain Text and XML)	Description (Plain Text and XML)	Call-Home Message Tag (XML Only)
Server ID	If the message is generated from the fabric switch, this is the unique device identifier (UDI) of the switch. • *type* is the product model number from backplane IDPROM. • @ is a separator character. • *Sid* is C, identifying the serial ID as a chassis serial number. • *serial* is the number identified by the Sid field. Example: CISCO3845@C@12345678	For long text message only.
Message description	Short text describing the error.	CallHome/MessageDescription
Device name	Node that experienced the event. This is the host name of the device.	CallHome/CustomerData/ SystemInfo/NameName
Contact name	Name of person to contact for issues associated with the node experiencing the event.	CallHome/CustomerData/ SystemInfo/Contact
Contact e-mail	E-mail address of person identified as contact for this unit.	CallHome/CustomerData/ SystemInfo/ContactEmail
Contact phone number	Phone number of the person identified as the contact for this unit.	CallHome/CustomerData/ SystemInfo/ContactPhoneNumber
Street address	Optional field containing street address for RMA part shipments associated with this unit.	CallHome/CustomerData/ SystemInfo/StreetAddress
Model name	Model name of the router. This is 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.	CallHome/Device/ Cisco_Chassis/AdditionalInformation/ AD@name=“PartNumber”

Data Item (Plain Text and XML)	Description (Plain Text and XML)	Call-Home Message Tag (XML Only)
System object ID	System Object ID that uniquely identifies the system.	CallHome/Device/ Cisco_Chassis/AdditionalInformation/ AD@name="sysObjectID"
System description	System description for the managed element.	CallHome/Device/ Cisco_Chassis/AdditionalInformation/ AD@name="sysDescr"

The table shows the inserted fields specific to a particular alert group message.

Note These fields may be repeated if multiple commands are executed for this alert group.

Table 6: Inserted fields specific to a particular Alert Group message

Command output name	Exact name of the issued command.	/aml/Attachments/Attachment/Name
Attachment type	Attachment type. Usually "inline".	/aml/Attachments/Attachment@type
MIME type	Normally "text" or "plain" or encoding type.	/aml/Attachments/Attachment/ Data@encoding
Command output text	Output of command automatically executed (see Alert Group trigger events and commands, on page 39).	/mml/attachments/attachment/atdata

The table shows the inserted content fields for reactive messages (system failures that require a TAC case) and proactive messages (issues that might result in degraded system performance).

Table 7: Inserted fields for a reactive or proactive Event Message

Data Item (Plain Text and XML)	Description (Plain Text and XML)	Call-Home Message Tag (XML Only)
Chassis hardware version	Hardware version of chassis	CallHome/Device/Cisco_Chassis/ HardwareVersion
Supervisor module software version	Top-level software version	CallHome/Device/Cisco_Chassis/ AdditionalInformation/AD@name= "SoftwareVersion"
Affected FRU name	Name of the affected FRU generating the event message	CallHome/Device/Cisco_Chassis/ Cisco_Card/Model
Affected FRU serial number	Serial number of affected FRU	CallHome/Device/Cisco_Chassis/ Cisco_Card/SerialNumber
Affected FRU part number	Part number of affected FRU	CallHome/Device/Cisco_Chassis/ Cisco_Card/PartNumber

Data Item (Plain Text and XML)	Description (Plain Text and XML)	Call-Home Message Tag (XML Only)
FRU slot	Slot number of FRU generating the event message	CallHome/Device/Cisco_Chassis/ Cisco_Card/LocationWithinContainer
FRU hardware version	Hardware version of affected FRU	CallHome/Device/Cisco_Chassis/ Cisco_Card/HardwareVersion
FRU software version	Software version(s) running on affected FRU	CallHome/Device/Cisco_Chassis/ Cisco_Card/SoftwareIdentity/ VersionString

The table shows the inserted content fields for an inventory message.

Table 8: Inserted fields for an inventory event message

Data Item (Plain Text and XML)	Description (Plain Text and XML)	Call-Home Message Tag (XML Only)
Chassis hardware version	Hardware version of chassis	CallHome/Device/Cisco_Chassis/ HardwareVersion
Supervisor module software version	Top-level software version	CallHome/Device/Cisco_Chassis/ AdditionalInformation/AD@name= “SoftwareVersion”
FRU name	Name of the affected FRU generating the event message	CallHome/Device/Cisco_Chassis/ Cisco_Card/Model
FRU s/n	Serial number of FRU	CallHome/Device/Cisco_Chassis/ Cisco_Card/SerialNumber
FRU part number	Part number of FRU	CallHome/Device/Cisco_Chassis/ Cisco_Card/PartNumber
FRU slot	Slot number of FRU	CallHome/Device/Cisco_Chassis/ Cisco_Card/LocationWithinContainer
FRU hardware version	Hardware version of FRU	CallHome/Device/Cisco_Chassis/ CiscoCard/HardwareVersion
FRU software version	Software version(s) running on FRU	CallHome/Device/Cisco_Chassis /Cisco_Card/SoftwareIdentity/ VersionString