



Configuring 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 utilization of Cisco Smart Call Home services for direct case generation with the Cisco Systems Technical Assistance Center (TAC).

This document describes how to configure the Call Home feature on Cisco ASR 1000 Series Aggregation Services Routers beginning with Cisco IOS XE Release 2.6.

- [Finding Feature Information, page 1](#)
- [Prerequisites for Call Home, page 1](#)
- [Information About Call Home, page 2](#)
- [How to Configure Call Home, page 4](#)
- [Additional References, page 58](#)
- [Feature Information for Call Home, page 59](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Call Home

How you configure Call Home depends on how you intend to use the feature. Consider the following requirements before you configure Call Home:

- Obtain e-mail, phone, and street address information for the Call Home contact to be configured so that the receiver can determine the origin of messages received.
- Identify the name or IPv4 address of a primary Simple Mail Transfer Protocol (SMTP) server and any backup servers, if using e-mail message delivery.
- Verify IP connectivity from the router to the e-mail server(s) or the destination HTTP server.
- If Cisco Smart Call Home is used, an active service contract covering the device is required to provide full SCH service.

Information About Call Home

Call Home 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 utilization of Cisco Smart Call Home services for direct case generation with the Cisco Systems Technical Assistance Center (TAC).

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

The Call Home 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 (CiscoTAC-1) is provided, and you also can define your own destination profiles. The CiscoTAC-1 profile is used to send alerts to the backend server of the Smart Call Home service, which can be used to create service requests to Cisco TAC, the service will depend 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 Using Call Home

The Call Home feature offers the following benefits:

- Multiple message-format options:
 - Short Text—Suitable for pagers or printed reports.
 - Plain Text—Full formatted message information suitable for human reading.
 - XML—Matching readable format using Extensible Markup Language (XML) and Adaptive Markup Language (AML) document type definitions (DTDs). The XML format enables communication with the Cisco Smart Call Home server.
- Multiple concurrent message destinations.
- Multiple message categories, including configuration, environmental conditions, inventory, syslog, and crash events and diagnostics.
- 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 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 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 information about how to configure Call Home to work with the Smart Call Home service, see the [How To Configure Call Home to Support the Smart Call Home Service](#).

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 is 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 [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 Call Home is required to use the Smart Licensing service.

The Smart Licensing service is an alternative licensing architecture to Cisco Software Licensing (CSL). Smart Call Licensing uses the Cisco Smart Software Manager as a backend tool for managing licenses. You must configure Cisco Smart Call Home before you can use Cisco Smart Licensing. For more information, see the Configuring and Enabling Smart Call Home section.

How to Configure Call Home

Configuring the Management Interface VRF

The Call Home feature on the Cisco ASR 1000 Series Routers requires use of the Gigabit Ethernet Management interface virtual routing and forwarding (VRF) instance. The Gigabit Ethernet Management interface is automatically part of its own VRF named “Mgmt-intf.”

To configure the Management interface VRF, complete the following steps:

or

ipv6 address {*X:X:X:X::X link-local* | *X:X:X:X::X/prefix* [*anycast* | **eui-64**] | **autoconfig** [*default*]}

SUMMARY STEPS

1. **configure terminal**
2. **interface GigabitEthernet 0**
3. **vrf forwarding Mgmt-intf**
4. Do one of the following:
 - **ip address** *ip-address mask* [**secondary** [*vrf vrf-name*]]
 -
 -
 - **ipv6 address** {*X:X:X:X::X link-local* | *X:X:X:X::X/prefix* [*anycast* | **eui-64**] | **autoconfig** [*default*]}

DETAILED STEPS

| | Command or Action | Purpose |
|--------|--|-----------------------------------|
| Step 1 | configure terminal | Enters global configuration mode. |
| | Example: Device# configure terminal | |

| | Command or Action | Purpose |
|---------------|---|--|
| Step 2 | interface GigabitEthernet 0 Example: Router(config)# interface GigabitEthernet0 | (Required) Specifies the Gigabit Ethernet Management interface on the Cisco ASR 1000 Series Router. |
| Step 3 | vrf forwarding Mgmt-intf Example: Router(config-if)# vrf forwarding Mgmt-intf | (Required) Associates the Mgmt-intf VRF with the Gigabit Ethernet Management interface. This command is configured by default. |
| Step 4 | Do one of the following: <ul style="list-style-type: none"> • ip address <i>ip-address mask</i> [secondary [vrf vrf-name]] • • • ipv6 address {<i>X:X:X:X::X link-local</i> <i>X:X:X:X::X/prefix</i> [anycast eui-64] autoconfig [default]} Example: Router(config-if)# ip address 10.10.10.10 0.0.0.0 | (Required) Specifies the IPv4 or IPv6 addressing for the interface. |

Configuring Smart Call Home (Single Command)

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

SUMMARY STEPS

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

DETAILED STEPS

| | Command or Action | Purpose |
|---------------|---|-----------------------------------|
| Step 1 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |

| | Command or Action | Purpose |
|---------------|---|---|
| Step 2 | <p>call-home reporting {anonymous contact-email-addr <i>email-address</i>} [http-proxy {<i>ipv4-address</i> <i>ipv6-address</i> name} port <i>port number</i>]</p> <p>Example:</p> <pre>Device(config)# call-home reporting contact-email-addr email@company.com</pre> | <p>Enables all Call Home basic configurations using a single command.</p> <ul style="list-style-type: none"> • anonymous—Enables Call-Home TAC profile to only send crash, inventory, and test messages and send the messages in an anonymous way. • 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 {<i>ipv4-address</i> <i>ipv6-address</i> name—An ipv4 or ipv6 address or server name. Maximum length is 64. • port <i>port number</i>—Port number. Range is 1 to 65535. <p>Note HTTP proxy option allows you to make use of your own proxy server to buffer and secure internet connections from your devices.</p> <p>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 Group Trigger Events and Commands” section.</p> |

Configuring and Enabling Smart Call Home

SUMMARY STEPS

1. **configure terminal**
2. **call-home**
3. **profile CiscoTAC-1**
4. **destination transport-method http**
5. **active**
6. **exit**
7. **contact-email-addr** *email-address*
8. **exit**
9. **service call-home**
10. **exit**
11. **copy running-config startup-config**

DETAILED STEPS

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 2 | call-home Example: Device(config)# call-home | Enters call home configuration mode. |
| Step 3 | profile CiscoTAC-1 Example: Device(config-call-home)# profile CiscoTAC-1 | Enters call home destination profile configuration mode for the CiscoTAC-1 destination profile. |
| Step 4 | destination transport-method http Example: Device(cfg-call-home-profile)# destination transport-method http | (Required only if using HTTPS) Configures the message transport method for http. |
| Step 5 | active Example: Device(cfg-call-home-profile)# active | Enables the destination profile. |
| Step 6 | exit Example: Device(cfg-call-home-profile)# exit | Exits call home destination profile configuration mode and returns to call home configuration mode. |
| Step 7 | contact-email-addr email-address Example: Device(cfg-call-home)# contact-email-addr username@example.com | Assigns the customer's e-mail address. Enter up to 200 characters in e-mail address format with no spaces. |
| Step 8 | exit Example: Device(cfg-call-home)# exit | Exits call home configuration mode and returns to global configuration mode. |

| | Command or Action | Purpose |
|----------------|--|--|
| Step 9 | service call-home Example: Device(config)# service call-home | Enables the Call Home feature. |
| Step 10 | exit Example: Device(config)# exit | Exits global configuration mode and returns to privileged EXEC mode. |
| Step 11 | copy running-config startup-config Example: Device# copy running-config startup-config | Saves the configuration to NVRAM. |

Enabling and Disabling Call Home

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

SUMMARY STEPS

1. **configure terminal**
2. **service call-home**
3. **no service call-home**

DETAILED STEPS

| | Command or Action | Purpose |
|---------------|--|-----------------------------------|
| Step 1 | configure terminal Example: Router# configure terminal | Enters global configuration mode. |
| Step 2 | service call-home Example: Router(config)# service call-home | Enables the Call Home feature. |

| | Command or Action | Purpose |
|---------------|---|---------------------------------|
| Step 3 | no service call-home Example: <code>Router(config)# no service call-home</code> | Disables the Call Home feature. |

Configuring Contact Information

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

To assign the contact information, complete the following steps:

SUMMARY STEPS

1. **configure terminal**
2. **call-home**
3. **contact-email-addr** *email-address*
4. **phone-number** *+phone-number*
5. **street-address** *street-address*
6. **customer-id** *text*
7. **site-id** *text*
8. **contract-id** *text*

DETAILED STEPS

| | Command or Action | Purpose |
|---------------|--|--------------------------------------|
| Step 1 | configure terminal Example: <code>Router> configure terminal</code> | Enters global configuration mode. |
| Step 2 | call-home Example: <code>Router(config)# call-home</code> | Enters call home configuration mode. |

| | Command or Action | Purpose |
|---------------|---|--|
| Step 3 | contact-email-addr <i>email-address</i> Example: Router (cfg-call-home) # contact-email-addr username@example.com | Assigns the customer's e-mail address. Enter up to 200 characters in e-mail address format with no spaces. |
| Step 4 | phone-number <i>+phone-number</i> Example: Router (cfg-call-home) # phone-number +1-222-333-4444 | (Optional) Assigns the customer's phone number. Note The number must begin with a plus (+) prefix, and may contain only dashes (-) and numbers. Enter up to 16 characters. If you include spaces, you must enclose your entry within double quotation marks (" "). |
| Step 5 | street-address <i>street-address</i> Example: Router (cfg-call-home) # 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 <i>text</i> Example: Router (cfg-call-home) # 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 <i>text</i> Example: Router (cfg-call-home) # 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 <i>text</i> Example: Router (cfg-call-home) # contract-id Company1234 | (Optional) Identifies the customer's contract ID for the router. Enter up to 64 characters. If you include spaces, you must enclose your entry within double quotation marks (" "). |

Example

The following example shows the configuration of contact information:

```
Device# configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

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

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

```
Device(cfg-call-home)# phone-number +1-222-333-4444
```

```
Device(cfg-call-home)# street-address "1234 Any Street, Any city, Any state, 12345"
```

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

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

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

```
Device(cfg-call-home)# exit
```

Configuring a Destination Profile

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

You can create and define a new destination profile or copy and use another destination profile. If you define a new destination profile, you must assign a profile name. 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 smart-license data enabled. For more information about Smart Licensing, see the “Managing Cisco CSR 1000V Licenses” section.

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



Note

The Call Home feature provides a predefined profile named CiscoTAC-1 that is inactive by default. The CiscoTAC-1 profile is intended for use with the Smart Call Home service, which requires certain additional configuration steps to enable the service with the Call Home feature. For more information about this profile, see the [Using the Predefined CiscoTAC-1 Destination Profile](#).



Note

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. You cannot use **all** as a profile name.
- Transport method—The transport mechanism, either e-mail or HTTP (including HTTPS), for delivery of alerts.
 - For user-defined destination profiles, e-mail is the default, and you can enable one 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 by which the alert should be sent.
In Call Home version 3, you can change the destination of the CiscoTAC-1 profile.
- **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. If you use the Cisco Smart Call Home service, the destination profile must use the XML message format.
- **Message size**—The maximum destination message size. The valid range is 50 to 3,145,728 bytes and the default is 3,145,728 bytes.
- **Reporting method**—You can choose which data to report for a profile. You can report Smart Call Home data or Smart Licensing data for a profile. 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.

This section includes the following tasks:

Creating a New Destination Profile

To create and configure a new destination profile, complete the following steps:

SUMMARY STEPS

1. **configure terminal**
2. **call-home**
3. **profile** *name*
4. **destination transport-method** **email**
5. **destination address email** *email-address*
6. **destination preferred-msg-format** {**long-text** | **short-text** | **xml**}
7. **destination message-size** *bytes*
8. **active**
9. **exit**
10. **end**

DETAILED STEPS

| | Command or Action | Purpose |
|---------------|--|-----------------------------------|
| Step 1 | configure terminal | Enters global configuration mode. |
| | Example: Device# configure terminal | |

| | Command or Action | Purpose |
|---------------|--|---|
| Step 2 | call-home Example: Device(config) # call-home | Enters call home configuration mode. |
| Step 3 | profile <i>name</i> Example: Device(config-call-home) # profile profile1 | Enters call home destination profile configuration mode for the specified destination profile name. If the specified destination profile does not exist, it is created. |
| Step 4 | destination transport-method email Example: Device(cfg-call-home-profile) # destination transport-method email | (Optional) Configures the message transport method for email. This is the default. |
| Step 5 | destination address email <i>email-address</i> Example: Device(cfg-call-home-profile) # destination address email myaddress@example.com | (Required) Configures the destination e-mail address to which Call Home messages are sent. |
| Step 6 | destination preferred-msg-format {long-text short-text xml} Example: Device(cfg-call-home-profile) # destination preferred-msg-format xml | (Optional) Configures a preferred message format. The default is XML. |
| Step 7 | destination message-size <i>bytes</i> Example: Device(cfg-call-home-profile) # destination message-size 3145728 | (Optional) Configures a maximum destination message size (from 50 to 3145728 bytes) for the destination profile. The default is 3145728 bytes. |
| Step 8 | active Example: Device(cfg-call-home-profile) # active | (Optional) Enables the destination profile. By default, a user-defined profile is enabled when it is created. |
| Step 9 | exit Example: Device(cfg-call-home-profile) # exit | Exits call home destination profile configuration mode and returns to call home configuration mode. |

| | Command or Action | Purpose |
|----------------|---|----------------------------------|
| Step 10 | end Example: Device(cfg-call-home) # end | Returns to privileged EXEC mode. |

Setting Profiles to Anonymous Mode

To create a new destination profile by copying an existing profile, complete the following steps:

SUMMARY STEPS

1. **configure terminal**
2. **call-home**
3. **copy profile** *source-profile target-profile*

DETAILED STEPS

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 2 | call-home Example: Device(config) # call-home | Enters call home configuration mode. |
| Step 3 | copy profile <i>source-profile target-profile</i> Example: Device(cfg-call-home) # copy profile profile1 profile2 | Creates a new destination profile with the same configuration settings as the existing destination profile, where: <ul style="list-style-type: none"> • <i>source-profile</i> —Specifies the existing name of the profile. • <i>target-profile</i> —Specifies a name for the new copy of the profile. |

Subscribing 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. The following alert groups are available:

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

The triggering events for each alert group are listed in the [Alert Group Trigger Events and Commands](#), and the contents of the alert group messages are listed in the [Message Contents](#).

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.

Periodic Notification

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

- Daily—Specify the time of day to send, using an hour:minute format hh:mm, with a 24-hour clock (for example, 14:30).
- Weekly—Specify the day of the week and time of day in the format day hh:mm, where the day of the week is spelled out (for example, monday).
- Monthly—Specify the numeric date, from 1 to 31, and the time of day, in the format date hh:mm.

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 message's level of severity. Any message with a severity lower than the specified threshold of the destination profile is not sent to the destination.

**Note**

When syslog level is changed via IOS CLI, the new value is propagated to non-IOS processes as well, with the result that these processes no longer send syslog messages of lower priority to IOS to process, thus "saving" CPU cycles for IOS.

The table below lists the keywords used to configure the severity, which range from catastrophic (level 9, highest level of urgency) to debugging (level 0, lowest level of urgency). If no severity threshold is configured, the default is debugging (level 0). However, the default is not recommended due to the number of messages that will be triggered.

**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 | N/A | Network-wide catastrophic failure. |
| 8 | disaster | N/A | 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. |

Configuring Snapshot Command List

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

SUMMARY STEPS

1. **configure terminal**
2. **call-home**
3. **[no | default] alert-group-config snapshot**
4. **[no | default] add-command *command string***
5. **end**

DETAILED STEPS

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 2 | call-home Example: Device(config)# call-home | Enters Call Home configuration mode. |
| Step 3 | [no default] alert-group-config snapshot Example: Device(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 <i>command string</i> Example: Device(cfg-call-home-snapshot)# add-command "show version" | Adds the command to the Snapshot alert group. The no or default command will remove the corresponding command. • <i>command string</i> —IOS command. Maximum length is 128. |
| Step 5 | end Example: Device(cfg-call-home-snapshot)# exit | Exits and saves the configuration. |

Configuring General email Options

Configuring the Mail Server

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

Consider the following guidelines when configuring the mail server:

- 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 email options, perform the following steps:

SUMMARY STEPS

1. **configure terminal**
2. **call-home**
3. **mail-server** {*ipv4-address* | *name*} **priority number**
4. **sender from** *email-address*
5. **sender reply-to** *email-address*
6. **source-interface** *interface-name*
7. **source-ip-address** *ipv4/ipv6 address*
8. **vrfvrf-name**

DETAILED STEPS

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 2 | call-home Example: Device(config)# call-home | Enters call home configuration mode. |
| Step 3 | mail-server { <i>ipv4-address</i> <i>name</i> } priority number | Assigns an email server address and its relative priority among configured email servers. |

| | Command or Action | Purpose |
|---------------|---|--|
| | Example: <pre>Device(cfg-call-home) # mail-server smtp.example.com priority 1</pre> | Provide either of these: <ul style="list-style-type: none"> • The email server's IP address or • The email 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 <i>email-address</i> Example: <pre>Device(cfg-call-home) # sender from username@example.com</pre> | (Optional) Assigns the e-mail address that will appear in the from field in Call Home e-mail messages. If no address is specified, the contact e-mail address is used. |
| Step 5 | sender reply-to <i>email-address</i> Example: <pre>Device(cfg-call-home) # sender reply-to username@example.com</pre> | (Optional) Assigns the e-mail address that will appear in the reply-to field in Call Home e-mail messages. |
| Step 6 | source-interface <i>interface-name</i> Example: <pre>Device(cfg-call-home) # source-interface loopback1</pre> | Assigns the source interface name to send call-home messages. <i>interface-name</i> —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 | source-ip-address <i>ipv4/ipv6 address</i> Example: <pre>Device(cfg-call-home) # ip-address 209.165.200.226</pre> | Assigns source IP address to send call-home messages. <ul style="list-style-type: none"> • <i>ipv4/ipv6 address</i>—Source IP (ipv4 or ipv6) address. Maximum length is 64. |
| Step 8 | vrf <i>vrf-name</i> Example: <pre>Device(cfg-call-home) # vrf vpn1</pre> | (Optional) Specifies the VRF instance to send call-home email 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: General email Options

The following example shows general email options:

```
Device# configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

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

```
Device(cfg-call-home)# mail-server smtp.example.com priority 1
```

```
Device(cfg-call-home)# mail-server 192.168.0.1 priority 2
```

```
Device(cfg-call-home)# exit
```

Specifying Rate Limit for Sending Call Home Messages

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

SUMMARY STEPS

1. **configure terminal**
2. **call-home**
3. **rate-limit** *number*

DETAILED STEPS

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 2 | call-home Example: Device(config)# call-home | Enters call home configuration mode. |
| Step 3 | rate-limit <i>number</i> Example: Device(cfg-call-home)# rate-limit 40 | Specifies a limit on the number of messages sent per minute. <ul style="list-style-type: none"> • <i>number</i>—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:

SUMMARY STEPS

1. **configure terminal**
2. **call-home**
3. **http-proxy** {*ipv4-address* | *ipv6-address name*} *name*

DETAILED STEPS

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 2 | call-home Example: Device(config)# call-home | Enters call home configuration mode. |
| Step 3 | http-proxy { <i>ipv4-address</i> <i>ipv6-address name</i> } <i>name</i> Example: Device(config)# http-proxy 1.1.1.1 port 1 | Specifies the proxy server for the HTTP request. |

Enabling AAA Authorization to Run IOS Commands for Call Home Messages

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

SUMMARY STEPS

1. **configure terminal**
2. **call-home**
3. **aaa-authorization**
4. **aaa-authorization** [*username username*]

DETAILED STEPS

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 2 | call-home Example: Device (config) # call-home | Enters call home configuration mode. |
| Step 3 | aaa-authorization Example: Device (cfg-call-home) # aaa-authorization | Enables AAA authorization. Note By default, AAA authorization is disabled for Call Home. |
| Step 4 | aaa-authorization [username <i>username</i>] Example: Device (cfg-call-home) # aaa-authorization username <i>username</i> | Specifies the username for authorization. <ul style="list-style-type: none"> • username <i>user</i>—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:

SUMMARY STEPS

1. **configure terminal**
2. **call-home**
3. **[no] syslog-throttling**

DETAILED STEPS

| | Command or Action | Purpose |
|---------------|---|-----------------------------------|
| Step 1 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |

| | Command or Action | Purpose |
|---------------|---|--|
| Step 2 | call-home Example: Device (config) # call-home | Enters call home configuration mode. |
| Step 3 | [no] syslog-throttling Example: Device (cfg-call-home) # 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 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.

SUMMARY STEPS

1. **configure terminal**
2. **call-home**
3. **data-privacy {level {normal | high} | hostname}**

DETAILED STEPS

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 2 | call-home Example: Device (config) # call-home | Enters call home configuration mode. |
| Step 3 | data-privacy {level {normal high} hostname} | Scrubs data from running configuration file to protect the privacy of the user. The default data-privacy level is normal. |

| | Command or Action | Purpose |
|--|---|--|
| | Example: <pre>Device(cfg-call-home) # data-privacy level high</pre> | <p>Note Enabling the data-privacy command can affect CPU utilization when scrubbing a large amount of data.</p> <ul style="list-style-type: none"> • 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. <p>Note Scrubbing the hostname from configuration messages can cause Smart Call Home processing failure on some platforms.</p> |

Working With Destination Profiles

This section describes some of the tasks that you can complete with destination profiles:

Activating and Deactivating a Destination Profile

Except for the predefined CiscoTAC-1 profile, all Call Home destination profiles are automatically activated once you create them. If you do not want to use a profile right way, you can deactivate the profile. The CiscoTAC-1 profile is inactive by default and must be activated to be used.

To activate or deactivate a destination profile, complete the following steps:

SUMMARY STEPS

1. **configure terminal**
2. **call-home**
3. **profile** *name*
4. **active**
5. **no active**
6. **end**

DETAILED STEPS

| | Command or Action | Purpose |
|---------------|---|-----------------------------------|
| Step 1 | configure terminal Example: <pre>Router# configure terminal</pre> | Enters global configuration mode. |

| | Command or Action | Purpose |
|---------------|--|--|
| Step 2 | call-home Example: Router(config) # call-home | Enters call home configuration mode. |
| Step 3 | profile name Example: Router(config-call-home) # profile test | Enters call home destination profile configuration mode for the specified destination profile. If the specified destination profile does not exist, it is created. |
| Step 4 | active Example: Router(cfg-call-home-profile) # active | Enables the destination profile. By default, a new profile is enabled when it is created. |
| Step 5 | no active Example: Router(cfg-call-home-profile) # no active | Disables the destination profile. |
| Step 6 | end Example: Router(cfg-call-home) # end | Exits call home destination profile configuration mode and returns to privileged EXEC mode. |

Renaming a Destination Profile

To change the name of an existing profile, complete the following steps:

SUMMARY STEPS

1. **configure terminal**
2. **call-home**
3. **rename profile** *source-profile target-profile*

DETAILED STEPS

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | configure terminal Example: Router# configure terminal | Enters global configuration mode. |
| Step 2 | call-home Example: Router(config)# call-home | Enters call home configuration mode. |
| Step 3 | rename profile source-profile target-profile Example: Router(cfg-call-home)# rename profile2 testprofile | Renames an existing source file, where: <ul style="list-style-type: none"> • <i>source-profile</i> —Specifies the existing name of the profile. • <i>target-profile</i> —Specifies a new name for the existing profile. |

Using the Predefined CiscoTAC-1 Destination Profile

The CiscoTAC-1 profile is automatically configured in the Call Home feature for your use with the Cisco Smart Call Home service. This profile includes certain information, such as the destination e-mail address and HTTPS URL, and default alert groups for communication with the Smart Call Home service. Some of these attributes, such as the destination e-mail address, HTTPS URL, and message format cannot be modified.

You can use either email or http transport to communicate with the Smart Call Home service backend server. By default, the CiscoTAC-1 profile is inactive and uses email as the default transport method. To use email transport, you only need to enable the profile. However, to use this profile with the Cisco Smart Call Home service secure server (via HTTPS), you not only must enable the profile, but you must also change the transport method to HTTP as shown in the following example:

```
Router# configure terminal
Router(config)# call-home
Router(config-call-home)# profile CiscoTAC-1
Router(cfg-call-home-profile)# destination transport-method http
Router(cfg-call-home-profile)# active
```

For more information about additional requirements for Configuring the Smart Call Home service, see the [How To Configure Call Home to Support the Smart Call Home Service](#) section.

Verifying the Call Home Profile Configuration

To verify the profile configuration for Call Home, use the **show call-home profile** command. See [Displaying Call Home Configuration Information](#) for more information and examples.

Sending Call Home Communications Manually

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

Sending a Call Home Test Message Manually

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

SUMMARY STEPS

1. **call-home test** [*“test-message”*] *profile name*

DETAILED STEPS

| | Command or Action | Purpose |
|--------|--|---|
| Step 1 | call-home test [<i>“test-message”</i>] <i>profile name</i> 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. |

Sending Call Home Alert Group Messages Manually

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

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

- Configuration, diagnostic, and inventory alert groups can be sent manually.
- When you manually trigger an alert group message and you specify a destination profile name, a message is sent to the destination profile regardless of the active status, subscription status, or severity setting of the profile.
- When you manually trigger a 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.
- When you manually trigger a diagnostic alert group message and do not specify a destination profile name, a message is sent to all active profiles that have a lower severity subscription than the severity of the diagnostic results of the specified slot.

To manually trigger Call Home alert group messages, complete the following steps:

SUMMARY STEPS

1. `call-home send alert-group configuration [profile name]`
2. `call-home send alert-group diagnostic slot R0 [profile name]`
3. `call-home send alert-group inventory [profile name]`

DETAILED STEPS

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | <code>call-home send alert-group configuration [profile name]</code> Example: Device# <code>call-home send alert-group configuration profile CiscoTAC-1</code> | Sends a configuration alert group message to one destination profile if specified, or to all subscribed destination profiles. |
| Step 2 | <code>call-home send alert-group diagnostic slot R0 [profile name]</code> Example: Device# <code>call-home send alert-group diagnostic slot R0 profile CiscoTAC-1</code> | Sends a diagnostic alert group message to one destination profile if specified, or to all subscribed destination profiles with a lower severity subscription than the diagnostic result for route processor slot 0. |
| Step 3 | <code>call-home send alert-group inventory [profile name]</code> Example: Device# <code>call-home send alert-group inventory</code> | 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

You can use the **call-home request** command to submit information about your system to Cisco Systems 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 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 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 devices in your network.

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

SUMMARY STEPS

1. **call-home request output-analysis "show-command"**
2. **call-home request {config-sanity | bugs-list | command-reference | product-advisory}**

DETAILED STEPS

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | call-home request output-analysis "show-command" Example: <code>[profile name] [ccoid user-id]</code> Example: <code>Device# call-home request output-analysis "show diag" profile TG</code> | 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} Example: <code>[profile name] [ccoid user-id]</code> Example: <code>Device# call-home request config-sanity profile TG</code> | 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 specified after the call-home request command specifies the type of report requested. |

Example

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

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

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

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

Note the following 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 email option is selected using the “email” keyword and an email address is specified, the command output is sent to that address. If neither the email 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 email.
- If the HTTP option is specified, 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. The user must specify either the destination email address or an SR number but they can also specify both.

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

SUMMARY STEPS

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

DETAILED STEPS

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | call-home send { <i>cli command</i> <i>cli list</i> } [email <i>email</i> msg-format { long-text xml } http { <i>destination-email-addressemail</i> }][tac-service-request SR#] Example: Router# call-home send “show version;show running-config show inventory” emailsupport@example.com msg-format xml | Executes the CLI or CLI list and sends output via email or HTTP. <ul style="list-style-type: none"> • {<i>cli command</i> <i>cli list</i>}—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 <i>email</i> msg-format {long-text xml}—If the email option is selected, the command output will be sent to the specified email address in long-text or XML format with the service request number in the subject. The email address, the service request number, or both must be specified. The service request number is required if the email address is not specified (default is attach@cisco.com for long-text format and callhome@cisco.com for XML format). • http {<i>destination-email-addressemail</i>}—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. |

| Command or Action | Purpose |
|-------------------|--|
| | <p>destination-email-address<i>email</i> 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.</p> <ul style="list-style-type: none"> • tac-service-request SR#—Specifies the service request number. The service request number is required if the email address is not specified. |

Example

The following example shows how to send the output of a CLI command to a user-specified email address:

Device# **call-home send "show diag" email support@example.com**

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

Device# **call-home send "show version"; "show run tac-service-request 123456**

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

Device# **call-home send "show diag" email callhome@example.com msg-format xml**

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 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 customer networks.

Prerequisites for Diagnostic Signatures

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

- You must assign a DS to the device. Refer to the “Diagnostic Signature Downloading” section for more information on how to assign DSES to devices.
- 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.
- Target URLs must be one of the Cisco Technical Assistance Center (TAC) HTTPS URLs:
 - <https://tools-stage.cisco.com/its/service/oddce/services/DDCEService>
 - <https://tools-dev.cisco.com/its/service/oddce/services/DDCEService>

Information About Diagnostic Signatures

Diagnostic Signatures Overview

Diagnostic signatures (DS) subsystem is introduced within the call-home system to provide a flexible framework that allows the defining of new events and corresponding CLIs that can analyze these events without upgrading the Cisco software.

DS provides you the ability to define more types of events and trigger types to perform the required actions than the Call-Home feature. The DS 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 a CLI to perform required actions. These files are digitally signed by Cisco or a third party to certify its integrity, reliability, and security.

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

- Metadata-based simple signature that specifies event type and contains other information that can be used to match the event, perform actions such as collecting information by using the CLI or resetting the line card in the device if there is an event match.
- 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 mentioned above.

The following basic information is contained in a DS file:

- ID (unique string)—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.
- ProductFamily
 - OsVersion (multiple values)—a list of operating system versions for each product family.
 - Technology—technology that the DS belongs to.

Diagnostic Signature Downloading

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. Therefore, to enable the HTTPS protocol, the firewall is

bypassed to access the service call-home (SCH) HTTPS server. The target URLs, which are defined in the SCH HTTPS server, must be one of the Technical Assistance Center (TAC) HTTPS URLs:

- <https://tools-stage.cisco.com/its/service/oddce/services/DDCEService>
- <https://tools-dev.cisco.com/its/service/oddce/services/DDCEService>

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 enabled by checking responses to periodic inventory messages. When an inventory message checks for any assigned DS on the device, the device sends a DS update request message that requests for an updated DS. 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.

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 keypairs to Abraxas system, which is the digital signing client
- DS signed via secure socket layer (SSL) through a code signing client, where the signature is embedded using XML tags
- Public keys 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 <https://abraxas.cisco.com/SignEngine/submit.jsp>

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 is enabled by default on the Cisco software.

- Use the **destination transport-method http** command to configure both email and HTTP data transfer methods to download DSes.
- Download all DS files or specific DS files either by using the on-demand or periodic download.
- Store the downloaded DS files on nonremovable disks, such as bootflash or harddisk, so that DS files can be read after a device reload. Syslog messages are displayed if the disk space is not sufficient.
- Use periodic download to verify if the same version of DS is already available on the device. If a different version of DS is available on the device, the older version is uninstalled and the newer version is installed. Service disruption may occur during this time because of the unavailability of the DS.
- Associate the DS on your device with only one profile. Associating a DS with two different profiles may lead to unexpected results.
- Use the severity and pattern of occurrence of events on the device to determine the CLI commands that must be included in the new DS to trigger actions. For events that have already been identified, the metadata of the DS is in a much simpler format.

The DS metadata is parsed and stored in a database for event registration and information collection. When an event occurs, the action specified in the DS is performed.

Diagnostic Signature Events and Actions

Diagnostic signature (DS) events and actions are defined while digitally signing a DS. The DS events and actions data are included after the administrator metadata and operational metadata in the DS.

Diagnostic Signature Event Detection

Event detection in 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, environment, diagnostic, periodic, configuration, Online Insertion Removal (OIR), immediate, and call-home are the supported event types, where “immediate” indicates that these types of DSes do not contain any event detection part and “call-home” type modifies the existing CLI commands. After the registration of the event types, the DS performs the associated action immediately.
- Embedded Event Manager (EEM) specification type—supports all existing EEM event types. The EEM specification type also supports a new EEM event detector without having to modify the Cisco software.

Other than using EEM to detect events, 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 or 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 and Variables

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 file that are used to customize the files.

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

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. In some situations, DS runs a set of commands simultaneously based on the last command result or a set of commands based on the variables defined within a DS. The following are the supported DS variable types:

- System variable—values assigned automatically by the device without any configuration changes. The Diagnostic Signatures feature supports two types of 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.
- 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.
- Syslog event variable—values assigned during an event detection in the DS file. This variable is valid only for syslog event detection.

How to Configure Diagnostic Signatures

Configuring Service Call-Home for Diagnostic Signatures

Configure the service call-home feature to set attributes such as the contact email address where notifications regarding diagnostic signature (DS) downloads are sent and destination HTTP/secure HTTP (HTTPS) URL to download the DS files from. These attributes are set for the call-home profile user1. For periodic downloads, schedule the time when the diagnostic signature files must be downloaded.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **service call-home**
4. **call-home**
5. **contact-email-addr** *email-address*
6. **mail-server** {*ipv4-addr* | *name*} **priority** *number*
7. **profile** *profile-name*
8. **destination transport-method** {**email** | **http**}
9. **destination address** {*email address* | *http url*}
10. **subscribe-to-alert-group inventory** [**periodic** {**daily** *hh:mm* | **monthly** *day hh:mm* | **weekly** *day hh:mm*}]
11. **exit**

DETAILED STEPS

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | enable Example: Device> enable | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 3 | service call-home Example: Device(config)# service call-home | Enables call-home service on a device. |
| Step 4 | call-home Example: Device(config)# call-home | Enters call-home configuration mode for the configuration of call-home settings. |

| | Command or Action | Purpose |
|----------------|---|---|
| Step 5 | contact-email-addr <i>email-address</i> Example: Device(cfg-call-home)# contact-email-addr userid@example.com | (Optional) Assigns an email address to be used for call-home customer contact. |
| Step 6 | mail-server { <i>ipv4-addr</i> <i>name</i> } priority number Example: Device(cfg-call-home)# mail-server 10.1.1.1 priority 4 | Configures a Simple Mail Transfer Protocol (SMTP) email server address for call-home. |
| Step 7 | profile <i>profile-name</i> Example: Device(cfg-call-home)# profile user1 | Configures a destination profile for call-home and enters call-home profile configuration mode. |
| Step 8 | destination transport-method { email http } Example: Device(cfg-call-home-profile)# destination transport-method http | Specifies a transport method for a destination profile in the call-home. |
| Step 9 | destination address { <i>email address</i> http url } Example: Device(cfg-call-home-profile)# destination address http https://tools-stage.cisco.com/its/service/oddce/services/DDCEService | Configures the address type and location to which call-home messages are sent. |
| Step 10 | subscribe-to-alert-group inventory [periodic { daily <i>hh:mm</i> monthly <i>day hh:mm</i> weekly <i>day hh:mm</i> }] Example: Device(cfg-call-home-profile)# subscribe-to-alert-group inventory periodic daily 14:30 | Configures a destination profile to receive messages for the Inventory alert group for call-home. <ul style="list-style-type: none"> This command is used only for the periodic downloading of DS files. |
| Step 11 | exit Example: Device(cfg-call-home-profile)# exit | Exits call-home profile configuration mode and returns to call-home configuration mode. |

What to Do Next

Configure DS with profile user1 as described in the “Configuring Diagnostic Signatures” section. The attributes set for the call-home profile user1 apply to DS.

Configuring Diagnostic Signatures

Before You Begin

Configure the Service Call-Home feature to set attributes for the call-home profile user1 as described in the “Configuring Service Call-Home for Diagnostic Signatures” section. When you configure diagnostic signatures (DSes), define the same profile name user1. DS then uses the attributes set for user1.

SUMMARY STEPS

1. **diagnostic-signature**
2. **profile** *ds-profile-name*
3. **environment** *ds_ env-varname ds-env-varvalue*
4. **end**
5. **call-home diagnostic-signature** {{**deinstall** | **download**} {*ds-id* | **all**} | **install** *ds-id*}
6. **show call-home diagnostic-signature** [*ds-id* [**actions** | **events** | **prerequisite** | **prompt** | **variables**] | **failure** | **statistics** [**download**]]
7. **debug call-home diagnostic-signature** {**action** | **all** | **api** | **cli** | **download** | **event-registration** | **parsing**}

DETAILED STEPS

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | diagnostic-signature Example: Device(cfg-call-home)# diagnostic-signature | Enters call-home diagnostic signature mode. |
| Step 2 | profile <i>ds-profile-name</i> Example: Device(cfg-call-home-diag-sign)# profile user1 | Specifies the destination profile on a device that DS uses. |
| Step 3 | environment <i>ds_ env-varname ds-env-varvalue</i> Example: Device(cfg-call-home-diag-sign)# environment ds_env1 envvarval | Sets the environment variable value for DS on a device. |
| Step 4 | end Example: Device(cfg-call-home-diag-sign)# end | Exits call-home diagnostic signature mode and returns to privileged EXEC mode. |
| Step 5 | call-home diagnostic-signature {{ deinstall download } { <i>ds-id</i> all } install <i>ds-id</i> } Example: Device# call-home diagnostic-signature download 6030 | Downloads, installs, and uninstalls diagnostic signature files on a device. |

| | Command or Action | Purpose |
|---------------|---|--|
| Step 6 | show call-home diagnostic-signature [<i>ds-id</i> [actions events prerequisite prompt variables] failure statistics download]] Example: Device# show call-home diagnostic-signature | Displays the attributes and statistics of a call-home diagnostic signature file on a device. |
| Step 7 | debug call-home diagnostic-signature { action all api cli download event-registration parsing } Example: Device# debug call-home diagnostic-signature all | Displays debugging of one or all of the call-home diagnostic signature flags on a device. |

Configuration Examples for Diagnostic Signatures

Examples: Configuring 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.

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

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

```
Device# 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 |

Configuring 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 utilization of Cisco Smart Call Home services for direct case generation with the Cisco Systems Technical Assistance Center (TAC).

This document describes how to configure the Call Home feature on Cisco ASR 1000 Series Aggregation Services Routers beginning with Cisco IOS XE Release 2.6.

How To Configure Call Home to Support the Smart Call Home Service

This section provides an overview of the minimum steps required to configure the Call Home feature on a Cisco device, and other required supporting configuration to communicate securely with the Smart Call Home service using HTTPS:

Prerequisites

Before you configure and use the Smart Call Home Service, be sure that you have completed the following prerequisites:

- Verify that you have an active Cisco Systems service contract for the device being configured.
- Verify that you have IP connectivity to the Cisco HTTPS server.
- Obtain the latest Cisco Systems server security certificate. In Cisco IOS XE Release 2.6.0, the following shows the latest text for the Cisco Systems server security certificate:

```
MIIDAjCCAmSCeH3Z/gfPqB63EHln+6eJNMYwDQYJKoZIhvcNAQEFBQAwgcExCzAJ
BgNVBAYTAlVTMRcwFQYDVQQKEw5WZXJpU2lnbiwgSW5jLjE8MDoGA1UECxMzQ2xh
c3MgMyBQdWJsawMgUHJpbWVyeSBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eSAtIEcy
MTowOAYDVQQLEzEoYykgMTk5OCBwZXJpU2lnbiwgSW5jLiAtIEZvciBhdXRob3Jp
emVkiHVzZSBvbm5MR8wHQYDVQQLExZWZXJpU2lnbiBUCnVzdCB0ZXR3b3JrMB4X
DTk4MDUxODAwMDAwMFOxDTI4MDgwMTIzNTk1OVowgcExCzAJBgNVBAYTAlVTMRcw
FQYDVQQKEw5WZXJpU2lnbiwgSW5jLjE8MDoGA1UECxMzQ2xhc3MgMyBQdWJsawMg
UHJpbWVyeSBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eSAtIEcyMTowOAYDVQQLEzEo
YykgMTk5OCBwZXJpU2lnbiwgSW5jLiAtIEZvciBhdXRob3JpemVkiHVzZSBvbm5
MR8wHQYDVQQLExZWZXJpU2lnbiBUCnVzdCB0ZXR3b3JrMIGfMA0GCScqGSIB3DQEB
AQUAAAGNADCBiQKBgQDMXtERXVxp0KvTuWpMmR9ZmDCOFoUgRm1HP9SFIIThbbP4
p00M8RcPO/mn+SXXwc+EY/J8Y8+iR/LGWzOOZEAEaMGAAuWQcRXfH2G71lSk8U0g0
13gfgLptQ5GVj0VXXn7F+8qkBOvqlzdUMG+7AUcyM83cV5tkaWH4mx0ciU9cZwID
AQABMA0GCScqGSIB3DQEBBQUAA4GBAFFNzb5cy5gZnBWYAT14Lk0PZ3BwmcYQWpSk
U01UbSuvDV1Ai2TT1+7eVmGSX6bEHRBhNtMsJzZoKQm5EWR0zLVznxxIqbxhAe7i
F6YM4OAIOW7n60RzKprxaZLvcRTDOaxxp5EJb+RxBrO6WVcmeQD2+A2iMzAo1KpY
oJ2daZH9
```

Declare and Authenticate a CA Trustpoint

To establish communication with the Cisco HTTPS server for Smart Call Home service, you must declare and authenticate the Cisco server security certificate.

SUMMARY STEPS

1. **configure terminal**
2. **crypto pki trustpoint** *name*
3. **enrollment terminal**
4. **exit**
5. **crypto pki authenticate** *name*
6. At the prompt, paste the security certificate text.
7. **quit**
8. **yes**
9. **end**
10. copy running-config startup-config

DETAILED STEPS

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | configure terminal Example: Router# configure terminal | Enters global configuration mode. |
| Step 2 | crypto pki trustpoint <i>name</i> Example: Router(config)# crypto pki trustpoint cisco | Declares a CA trustpoint on your router and enters CA trustpoint configuration mode. |
| Step 3 | enrollment terminal Example: Router(ca-trustpoint)# enrollment terminal | Specifies a manual cut-and-paste method of certificate enrollment. |
| Step 4 | exit Example: Router(ca-trustpoint)# exit | Exits CA trustpoint configuration mode and returns to global configuration mode. |
| Step 5 | crypto pki authenticate <i>name</i> Example: Router(config)# crypto pki authenticate cisco | Authenticates the named CA. Note The CA name should match the <i>name</i> specified in the crypto pki trustpoint command. |

| | Command or Action | Purpose |
|----------------|---|--|
| Step 6 | <p>At the prompt, paste the security certificate text.</p> <p>Example:</p> <p>Enter the base 64 encoded CA certificate.</p> <p>Example:</p> <p>End with a blank line or the word "quit" on a line by itself</p> <p>Example:</p> <p><Paste certificate text here></p> | Specifies the security certificate text. |
| Step 7 | <p>quit</p> <p>Example:</p> <p>quit</p> | Specifies the end of the security certificate text. |
| Step 8 | <p>yes</p> <p>Example:</p> <p>% Do you accept this certificate? [yes/no]: yes</p> | Confirms acceptance of the entered security certificate. |
| Step 9 | <p>end</p> <p>Example:</p> <p>Router# end</p> | Exits global configuration mode and returns to privileged EXEC mode. |
| Step 10 | <p>copy running-config startup-config</p> <p>Example:</p> <p>Router# copy running-config startup-config</p> | Saves the configuration to NVRAM. |

Examples

The following example shows the configuration for declaring and authenticating the Cisco server security certificate:

```
Router# configure terminal
Router(config)# crypto pki trustpoint cisco
Router(ca-trustpoint)# enrollment terminal
Router(ca-trustpoint)# exit
Router(config)# crypto pki authenticate cisco
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
MIIDAjCCAmCEH3Z/gfPqB63EHln+6eJNMYwDQYJKoZIhvcNAQEFBQAwgcExCzAJ
BgNVBAYTA1VTMRcwFQYDVQQKEw5WZXJpU2lnbiwgSW5jLjE8MDoGA1UECzMzQ2xh
c3MgMyBQdWJsaWMgUHJpbWVyeSBkZmZ0aWZpY2F0aW9uIEF1dGhvcml0eSAtIEcy
MTowOAYDVQQLEzEoYykgMTk5OCBwZXJpU2lnbiwgSW5jLiAtIEZvciBhdXRob3Jp
emVkiHVzZSBvbm5MR8wHQYDVQQLExZWZlbnBiBUCnVzdCBOZXR3b3JrMB4X
DTk4MDUxODAwMDAwMFOXDTE4MDgwMTIzNTk1OVowgcExCzAJBgNVBAYTA1VTMRcw
```

```

FQYDVQKKEw5WZXJpU2lnbiwgSW5jLjE8MDoGA1UECzMzQ2xhc3MgMyBQdWJsaWMg
UHJpbWFeSBdZXJ0aWZpY2F0aW9uIEFldGhvcml0eSAtIEcyMTowOAYDVQQLEzEo
YykgMTk5OCBWXJpU2lnbiwgSW5jLiAtIEZvciBhdXRob3JpemVkIHVzZSBvbm5
MR8wHQYDVQKKEw5WZXJpU2lnbiBUCnVzdCB0ZXR3b3JrMIGfMA0GCSqGSIb3DQEB
AQUAA4GNADCBiQKBgQDMXtERXVxp0KvTuWpMmR9ZmDCOFoUgRm1HP9SFIIThbbP4
p00M8RcPO/mn+SXXwc+EY/J8Y8+iR/LGWzOOZEAEaMGauWQcRXfh2G711Sk8UOg0
13gfgLptQ5GVj0VXXn7F+8qkBOvqlzdUMG+7AUcyM83cV5tkaWH4mx0ciU9cZwID
AQABMA0GCSqGSIb3DQEBBQUAA4GBAFFNzb5cy5gZnBWYATl4Lk0PZ3BwmcYQWpSk
U01UbSuvDV1Ai2TT1+7eVmGSX6bEHRBhNtMsJzZoKQm5EWR0zLVznxxIqbxAe7i
F6YM40AIow7n60RzKprxaZLvcRTDOaxxp5EJb+RxBr06WVcmeQD2+A2iMzAo1KpY
oJ2daZH9
quit
Certificate has the following attributes:
    Fingerprint MD5: A2339B4C 747873D4 6CE7C1F3 8DCB5CE9
    Fingerprint SHA1: 85371CA6 E550143D CE280347 1BDE3A09 E8F8770F
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported
Router(config)# end
Router# copy running-config startup-config

```

Start Smart Call Home Registration

To start the Smart Call Home registration process, manually send an inventory alert-group message to the CiscoTAC-1 profile.

SUMMARY STEPS

1. call-home send alert-group inventory profile CiscoTAC-1

DETAILED STEPS

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | call-home send alert-group inventory profile CiscoTAC-1 Example: Device# call-home send alert-group inventory profile CiscoTAC-1 | Sends an inventory alert group message to the CiscoTAC-1 destination profile. |

What To Do Next

To receive an email from Cisco Systems and follow the instructions to complete the device registration in the Smart Call Home web application:

- Launch the Smart Call Home web application at the following URL:

<https://tools.cisco.com/sch/>

- Accept the Legal Agreement.
- Confirm device registration for Call Home devices with pending registration.

For more information about using the Smart Call Home web application, see *Smart Call Home User Guide*. This user guide also includes configuration examples for sending Smart Call Home messages directly from your device or through a transport gateway (TG) aggregation point. You can use a TG aggregation point in

cases requiring support for multiple devices or in cases where security requirements mandate that your devices must not be connected directly to the Internet.

Displaying Call Home Configuration Information

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

To display the configured Call Home information, use one or more of the following commands:

SUMMARY STEPS

1. **show call-home**
2. **show call-home detail**
3. **show call-home alert-group**
4. **show call-home mail-server status**
5. **show call-home profile {all | name}**
6. **show call-home statistics**

DETAILED STEPS

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | show call-home Example: Device# show call-home | Displays the Call Home configuration in summary. |
| Step 2 | show call-home detail Example: Device# show call-home detail | Displays the Call Home configuration in detail. |
| Step 3 | show call-home alert-group Example: Device# show call-home alert-group | Displays the available alert groups and their status. |
| Step 4 | show call-home mail-server status Example: Device# 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: Device# 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. |

| | Command or Action | Purpose |
|--------|---|--|
| Step 6 | show call-home statistics Example: Device# show call-home statistics | Displays the statistics of Call Home events. |

Configuration Examples for Call Home

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

Example: Call Home Information in Summary

```
Device# show call-home
Current call home settings:
  call home feature : disable
  call home message's from address: username@example.com
  call home message's reply-to address: username@example.com
  vrf for call-home messages: Mgmt-intf
  contact person's email address: username@example.com
  contact person's phone number: +14085551234
  street address: 1234 Any Street Any city Any state 12345
  customer ID: customer@example.com
  contract ID: 123456789
  site ID: example.com
  Mail-server[1]: Address: smtp.example.com Priority: 1
  Mail-server[2]: Address: 192.168.0.1 Priority: 2
  Rate-limit: 20 message(s) per minute
Available alert groups:
  Keyword          State   Description
  -----
  configuration     Enable  configuration info
  diagnostic        Enable  diagnostic info
  environment       Enable  environmental info
  inventory         Enable  inventory info
  syslog           Enable  syslog info
Profiles:
  Profile Name: campus-noc
  Profile Name: CiscoTAC-1
```

Example: Configured Call Home Information in Detail

```
Device# 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: GigabitEthernet1
  Mail-server[1]: Address: 192.168.2.1 Priority: 1
  Mail-server[2]: Address: 223.255.254.254 Priority: 2
  http proxy: 192.168.1.1:80
  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
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
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
Syslog-Pattern          Severity
-----
.*CALL_LOOP.*          debug

```

Example: Available Call Home Alert Groups

```

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

```

Example: Email Server Status Information

```

Device# show call-home mail-server status
Please wait. Checking for mail server status ...
Mail-server[1]: Address: 192.168.2.1 Priority: 1 [Not Available]
Mail-server[2]: Address: 223.255.254.254 Priority: 2 [Available]

```

Examples: Information for All Destination Profiles

```

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

```

Example: Information for a User-Defined Destination Profile

```

Device# 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
inventory                    normal
Syslog-Pattern                Severity
-----
.*CALL_LOOP.*                debug

```

Example: Call Home Statistics

```

Device# show call-home statistics
Message Types    Total    Email    HTTP
-----
Total Success    3        3        0
Config           3        3        0
Diagnostic        0        0        0
Environment       0        0        0
Inventory         2        2        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
Diagnostic        0        0        0
Environment       0        0        0
Inventory         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
Diagnostic    0          0          0
Environment   0          0          0
Inventory     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
Diagnostic    0          0          0
Environment   0          0          0
Inventory     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: 2010-01-11 18:32:32 GMT+00:00

```

Default Settings

Lists of 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 | 0 (debugging) |
| 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 CLI commands to execute when an event occurs. The CLI command output is included in the transmitted message. [Table 2: Call Home Alert Groups, Events, and Actions](#), on page 49 lists the trigger events included in each alert group, including the severity level of each event and the executed CLI commands for the alert group.

Table 2: Call Home Alert Groups, Events, and Actions

| Alert Group | Call Home Trigger Event | Syslog Event | Severity | Description and CLI Commands Executed |
|---------------|-------------------------|--------------|----------|---|
| Crash | SYSTEM_CRASH | — | — | Events related to system crash. Commands executed: show version show logging show region show stack |
| — | TRACEBACK | — | — | Detects software traceback events. Commands executed: show version show logging show region show stack |
| Configuration | — | — | — | User-generated request for configuration. (Sent to TAC.) CLI commands executed: show platform show inventory show running-config all show startup-config show version |
| Diagnostic | — | — | — | CLI commands executed: show platform show diagnostic result slot x detail show version show inventory show buffers show logging show diagnostic result slot all show diagnostic events slot all |

| Alert Group | Call Home Trigger Event | Syslog Event | Severity | Description and CLI Commands Executed |
|---------------|-------------------------|--------------|----------|--|
| Environmental | — | — | — | <p>Events related to power, fan, and environment sensing elements, such as temperature alarms. (Sent to TAC.)</p> <p>CLI commands executed:</p> <p>show platform show environment show inventory show logging</p> |
| Inventory | — | — | — | <p>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. (Sent to TAC.)</p> <p>CLI commands executed:</p> <p>show diag all eeprom detail include MAC show license all show platform show platform hardware qfp active infrastructure chipset 0 capabilities show platform software vnic-if interface-mapping show version</p> |
| Syslog | — | — | — | <p>Event logged to syslog.</p> <p>CLI commands executed:</p> <p>show logging</p> |

Message Contents

The following tables display the content formats of alert group messages:

- The **Format for a Short Text Message** table describes the content fields of a short text message.

- The **Common Fields for All Long Text and XML Messages** table describes 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.
- The **Inserted Fields for a Reactive or Proactive Event Message** table describes 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).
- The **Inserted Fields for an Inventory Event Message** table describes the inserted content fields for an inventory message.

This section also includes the following subsections that provide sample messages:

Table 3: 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 |

Table 4: Common Fields for All Long Text and XML Messages

| Data Item (Plain Text and XML) | Description (Plain Text and XML) | MML Tag (XML Only) | |
|--------------------------------|---|--|--|
| Time stamp | Date and time stamp of event in ISO time notation: <i>YYYY-MM-DD HH:MM:SS GMT+HH:MM.</i> | CallHome/EventTime | |
| Message name | Name of message. Specific event names are listed in the Alert Group Trigger Events and Commands section. | For short text message only | |
| Message type | Specifically “Call Home”. | CallHome/Event/Type | |
| Message subtype | Specific type of message: full, delta, test | CallHome/Event/SubType | |
| Message group | Specifically “reactive”. Optional, because default is “reactive”. | Not applicable. For long-text message only | |
| Severity level | Severity level of message. | 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 | |

| Data Item (Plain Text and XML) | Description (Plain Text and XML) | MML Tag (XML Only) |
|--------------------------------|--|---|
| Device ID | <p>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 <i>type@Sid@serial</i>.</p> <ul style="list-style-type: none"> • <i>type</i> is the product model number from backplane IDPROM. • <i>@</i> is a separator character. • <i>Sid</i> is C, identifying the serial ID as a chassis serial number. • <i>serial</i> is the number identified by the Sid field. <p>Example: ASR1006@C@FOX105101DH</p> | 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/ContractId |
| Site ID | Optional user-configurable field used for site IDs supplied by Cisco Systems or other data meaningful to alternate support services. | CallHome/CustomerData/ ContractData/SiteId |
| Server ID | <p>If the message is generated from the fabric switch, this is the unique device identifier (UDI) of the switch.</p> <p>The format is <i>type@Sid@serial</i>.</p> <ul style="list-style-type: none"> • <i>type</i> is the product model number from backplane IDPROM. • <i>@</i> is a separator character. • <i>Sid</i> is C, identifying the serial ID as a chassis serial number. • <i>serial</i> is the number identified by the Sid field. <p>Example: ASR1006@C@FOX105101DH</p> | 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 |

| Data Item (Plain Text and XML) | Description (Plain Text and XML) | MML Tag (XML Only) |
|--|--|---|
| 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” |
| 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” |
| Fields specific to a particular alert group message are inserted here. | The following fields may be repeated if multiple CLI commands are executed for this alert group. | |
| | Command output name | The exact name of the issued CLI command. /aml/Attachments/AttachmentName |
| | 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. /aml/Attachments/Attachment/Data |

Table 5: Inserted Fields for a Reactive or Proactive Event Message

| Data Item (Plain Text and XML) | Description (Plain Text and XML) | MML 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 |
| 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 |

Table 6: Inserted Fields for an Inventory Event Message

| Data Item (Plain Text and XML) | Description (Plain Text and XML) | MML 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 |

| Data Item (Plain Text and XML) | Description (Plain Text and XML) | MML Tag (XML Only) |
|--------------------------------|-------------------------------------|---|
| 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 |

Sample Syslog Alert Notification in XML Format

The following example shows a 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>M8:9S1NMSF22DW:51AEAC68</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>2013-06-05 03:11:36 GMT+00:00</aml-block:CreationDate>
        <aml-block:Builder>
          <aml-block:Name>CSR1000v</aml-block:Name>
          <aml-block:Version>2.0</aml-block:Version>
        </aml-block:Builder>
        <aml-block:BlockGroup>
          <aml-block:GroupId>G9:9S1NMSF22DW:51AEAC68</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>2</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>2013-06-05 03:11:36 GMT+00:00</ch:EventTime> <ch:MessageDescription>*Jun 5
            03:11:36.041: %CLEAR-5-COUNTERS: Clear counter on all interfaces by
            console</ch:MessageDescription> <ch:Event> <ch:Type>syslog</ch:Type>
          <ch:SubType></ch:SubType> <ch:Brand>Cisco Systems</ch:Brand> <ch:Series>CSR1000v Cloud
            Services Router</ch:Series> </ch:Event> <ch:CustomerData> <ch:UserData>
            <ch:Email>weijuhua@cisco.com</ch:Email>
          </ch:UserData>
          <ch:ContractData>
            <ch:CustomerId></ch:CustomerId>
            <ch:SiteId></ch:SiteId>
            <ch:ContractId></ch:ContractId>
            <ch:DeviceId>CSR1000V@C@9S1NMSF22DW</ch:DeviceId>
          </ch:ContractData>
        </ch:CallHome>
      </aml-block:Content>
    </aml-block:Block>
  </soap-env:Body>
</soap-env:Envelope>
```

```

<ch:SystemInfo>
<ch:Name>qiang-vm</ch:Name>
<ch:Contact></ch:Contact>
<ch:ContactEmail>weijuhua@cisco.com</ch:ContactEmail>
<ch:ContactPhoneNumber></ch:ContactPhoneNumber>
<ch:StreetAddress></ch:StreetAddress>
</ch:SystemInfo>
<ch:CCOID></ch:CCOID>
<ch:IdToken></ch:IdToken>
</ch:CustomerData>
<ch:Device>
<rme:Chassis xmlns:rme="http://www.cisco.com/rme/4.0">
<rme:Model>CSR1000V</rme:Model>
<rme:HardwareVersion></rme:HardwareVersion>
<rme:SerialNumber>9S1NMSF22DW</rme:SerialNumber>
<rme:AdditionalInformation>
<rme:AD name="PartNumber" value="" />
<rme:AD name="SoftwareVersion" value="15.4(20130604:093915)" /> <rme:AD
name="SystemObjectId" value="1.3.6.1.4.1.9.1.1537" /> <rme:AD name="SystemDescription"
value="Cisco IOS Software, CSR1000V Software (X86_64_LINUX_IOSD-ADVENTERPRISEK9-M),
Experimental Version 15.4(20130604:093915) [mcp_dev-qiazhou-ultra_ut 100] Copyright (c)
1986-2013 by Cisco Systems, Inc.
Compiled Tue 04-Jun-13 02:39 by jsmith" /> <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 logging</aml-block:Name>
<aml-block:Data encoding="plain"> <![CDATA[show logging Syslog logging: enabled (0
messages dropped, 1 messages rate-limited, 0 flushes, 0 overruns, xml disabled, filtering
disabled)
No Active Message Discriminator.
No Inactive Message Discriminator.
Console logging: level debugging, 391 messages logged, xml disabled,
filtering disabled
Monitor logging: level debugging, 0 messages logged, xml disabled,
filtering disabled
Buffer logging: level debugging, 391 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, 56 message lines logged
Logging Source-Interface: VRF Name:
Log Buffer (4096 bytes):
*Jun 5 03:11:18.295: %SYS-5-CONFIG_I: Configured from console by console
qiang-vm#]]></aml-block:Data> </aml-block:Attachment> </aml-block:Attachments>
</aml-block:Block> </soap-env:Body> </soap-env:Envelope>

```

Sample Smart Licensing Alert Notification in XML Format

The following example shows a Smart Licensing 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>M2:98I1W09R72W:5136E366</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/license</aml-block:Type>

```



```

<aml-block:CreationDate>2013-03-06 06:34:14 GMT+00:00</aml-block:CreationDate>
<aml-block:Builder>
<aml-block:Name>CSR1000v</aml-block:Name>
<aml-block:Version>2.0</aml-block:Version>
</aml-block:Builder>
<aml-block:BlockGroup>
<aml-block:GroupId>G3:9811W09R72W:5136E366</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>1</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>2013-04-10 07:47:28 GMT+08:00</ch:EventTime>
<ch:MessageDescription>Smart Licensing </ch:MessageDescription>
<ch:Event>
<ch:Type>License</ch:Type>
<ch:SubType>Register</ch:SubType> <!--maybe other values like certificate_renewal,
id_certificate_ack, poll_for_data, license_disable, license_usage, entitlement_request>
<ch:Brand>Cisco Systems</ch:Brand>
<ch:Series>CSR1000v Cloud Services Router</ch:Series>
</ch:Event>
<ch:CustomerData>
<ch:UserData>
<ch:Email>test@cisco.com</ch:Email>
</ch:UserData>
<ch:ContractData>
<ch:CustomerId></ch:CustomerId>
<ch:SiteId></ch:SiteId>
<ch:ContractId></ch:ContractId>
<ch:DeviceId>CSR1000V@C@9811W09R72W</ch:DeviceId>
</ch:ContractData>
<ch:SystemInfo>
<ch:Name>router</ch:Name>
<ch:Contact></ch:Contact>
<ch:ContactEmail>test@cisco.com</ch:ContactEmail>
<ch:ContactPhoneNumber></ch:ContactPhoneNumber>
<ch:StreetAddress></ch:StreetAddress>
</ch:SystemInfo>
<ch-inv:CCOID>xxxx</ch-inv:CCOID>
<ch:IdToken>yyyy</ch:IdToken> <!--either CCOID or IdToken needs to be specified when
subtype is Register>
</ch:CustomerData>
<ch:Device>
<rme:Chassis xmlns:rme="http://www.cisco.com/rme/4.0">
<rme:Model>CSR1000V</rme:Model>
<rme:HardwareVersion>1.4</rme:HardwareVersion>
<rme:SerialNumber>9811W09R72W</rme:SerialNumber>
<rme:AdditionalInformation>
<rme:AD name="PartNumber" value="68-3376-01" />
<rme:AD name="SoftwareVersion" value="15.3(20130303:013635)" />
<rme:AD name="SystemObjectId" value="1.3.6.1.4.1.9.1.1537" />
<rme:AD name="SystemDescription" value="Cisco IOS Software, IOS-XE Software
(X86_64_LINUX_IOSD-ADVENTERPRISEK9-M), Experimental Version 15.3(20130303:013635)
[mcp_dev-BLD-BLD MCP DEV LATEST 20130303_000028-ios 171]
Copyright (c) 1986-2013 by Cisco Systems, Inc.
Compiled Sat 02-Mar-13 20:49 by mcpre" />
<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>smart_licensing_data</aml-block:Name>
<aml-block:Data encoding="plain">
<![CDATA[...licensing data... ]]></aml-block:Data>
</aml-block:Attachment>

```

```

</aml-block:Attachments>
</aml-block:Block>
</soap-env:Body>
</soap-env:Envelope>
<response><![CDATA[{"signature":{"type":"SHA_1","value":"SIG_SIGNED_VALUE"},"response":{"\
"header\":"null","\status_code\":"ERROR","\status_message\":"Failed to process the
request.\","\response_data\":"\""}]]></response>
    <email>xxx@yyy.com</email><result xmlns="">succeeded</result>
  </soapenv:Body>
</soapenv:Envelope>

```

Additional References

The following sections provide references related to the Call Home feature.

Related Documents

| Related Topic | Title |
|---|--|
| Cisco IOS XE commands | Cisco IOS Master Commands List, All Releases |
| Explains how the Smart Call Home service offers web-based access to important information on select Cisco devices and offers higher network availability, and increased operational efficiency by providing proactive diagnostics and real-time alerts. | Smart Call Home User Guide |
| Smart Call Home site page on Cisco.com for access to all related product information. | Cisco Smart Call Home site |
| Public Key Infrastructure (PKI) and Certificate Authority configuration in Cisco IOS XE software | Cisco IOS XE Security Configuration Guide: Secure Connectivity |

Standards

| Standard | Title |
|---|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | — |

MIBs

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

RFCs

| RFC | Title |
|---|-------|
| No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature. | — |

Technical Assistance

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

Feature Information for Call Home

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

**Note**

The Feature Information table below lists only the Cisco IOS XE software release that introduced support for a given feature in a given Cisco IOS XE software release train. Unless noted otherwise, subsequent releases of that Cisco IOS XE software release train also support that feature.

Table 7: Feature Information for Call Home

| Feature Name | Releases | Feature Information |
|-----------------|-----------------------------------|--|
| Call Home | Cisco IOS XE Release 3.13S | <p>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.</p> <p>In Cisco IOS XE Release 2.6, support was added for the Cisco ASR 1000 Series Aggregation Services Routers.</p> <p>The following commands were introduced or modified:</p> <p>None</p> <p>show diagnostic commands</p> |
| Smart Licensing | Cisco IOS XE Release 3.12S, 3.13S | <p>The Smart Call Home feature is required to use the Smart Licensing service. The Smart Licensing service is an alternative licensing architecture to Cisco Software Licensing (CSL). Smart Call Licensing uses the Cisco Smart Software Manager as a backend tool for managing licenses.</p> <p>Smart Licensing support has been provided on the Cisco CSR 1000V on a controlled-availability basis beginning with Cisco IOS XE Release 3.12S.</p> <p>The following commands are new or modified: show diagnostic commands.</p> |