
# Anonymous Reporting and Smart Call Home

The Smart Call Home feature provides personalized, e-mail-based and web-based notification to you about critical events involving your individual systems, often before you know that a critical event has occurred.

The Anonymous Reporting feature is a subfeature of the Smart Call Home feature and allows Cisco to anonymously receive minimal error and health information from the device.

This chapter describes how to use and configure Anonymous Reporting and Smart Call Home, and it includes the following sections:



# Information About Anonymous Reporting and Smart Call Home

This section includes the following topics:



## Information About Anonymous Reporting

You can help to improve the ASA platform by enabling Anonymous Reporting, which allows Cisco to securely receive minimal error and health information from the device. If you enable the feature, your customer identity will remain anonymous, and no identifying information will be sent.

Enabling Anonymous Reporting creates a trust point and installs a certificate. A CA certificate is required for your ASA to validate the server certificate present on the Smart Call Home web server and to form the HTTPS session so that your ASA can send messages securely. Cisco imports a certificate that is predefined in the software. If you decide to enable Anonymous Reporting, a certificate is installed

on the ASA with a hardcoded trust point name: _SmartCallHome_ServerCA. When you enable Anonymous Reporting, this trust point is created, the appropriate certificate is installed, and you receive a message about this action. The certificate then appears in your configuration.

If the appropriate certificate already exists in your configuration when you enable Anonymous Reporting, no trust point is created, and no certificate is installed.

**Note** When you enable Anonymous Reporting, you acknowledge your consent to transfer the specified data to Cisco or to vendors operating on Cisco's behalf (including countries outside of the U.S.). Cisco maintains the privacy of all customers. For information about Cisco's treatment of personal information, see the Cisco Privacy Statement at the following URL: http://www.cisco.com/web/siteassets/legal/privacy.html

## DNS Requirement

A DNS server must be configured correctly for your ASA to reach the Cisco Smart Call Home server and send messages to Cisco. Because it is possible that your ASA resides in a private network and does not have access to the public network, Cisco verifies your DNS configuration and then configures it for you, if necessary, by doing the following:

1. Performing a DNS lookup for all DNS servers configured.
2. Getting the DNS server from the DHCP server by sending DHCPINFORM messages on the highest security-level interface.
3. Using the Cisco DNS servers for lookup.
4. Randomly using a static IP addresses for tools.cisco.com.

These tasks are performed without changing the current configuration. (For example, the DNS server that was learned from DHCP will not be added to the configuration.)

If there is no DNS server configured, and your ASA cannot reach the Cisco Smart Call Home Server, Cisco generates a syslog message with the warning severity level for each Smart Call Home message that is sent to remind you to configure DNS correctly.

For information about syslog messages, see the syslog messages guide.

## Anonymous Reporting and Smart Call Home Prompt

When you enter configuration mode, you receive a prompt that requests you to enable the Anonymous Reporting and Smart Call Home features according to the following guidelines:

At the prompt, you may choose [Y]es, [N]o, [A]sk later. If you choose [A]sk later, then you are reminded again in seven days or when the ASA reloads. If you continue to choose [A]sk later, the ASA prompts two more times at seven-day intervals before it assumes a [N]o response and does not ask again.

At the ASDM prompt, you can select from the following options:

- Anonymous—Enables Anonymous Reporting.
- Registered (enter an e-mail address)—Enables Smart Call Home and registers your ASA with Cisco TAC.
- Do not enable Smart Call Home—Does not enable Smart Call Home and does not ask again.
- Remind Me Later—Defers the decision. You are reminded again in seven days or whenever the ASA reloads. The ASA prompts two more times at seven-day intervals before it assumes a "Do not enable Smart Call Home response" and does not ask again.

If you did not receive the prompt, you may enable Anonymous Reporting or Smart Call Home by performing the steps in the Configuring Anonymous Reporting, page 49-5 or the Configuring Smart Call Home, page 49-6.

## Information About Smart Call Home

When fully configured, Smart Call Home detects issues at your site and reports them back to Cisco or through other user-defined channels (such as e-mail or directly to you), often before you know that these issues exist. Depending upon the seriousness of these problems, Cisco responds to you regarding your system configuration issues, product end-of-life announcements, security advisory issues, and so on.

In this manner, Smart Call Home offers proactive diagnostics and real-time alerts on the ASA and provides high network availability and increased operational efficiency through proactive and quick issue resolution by doing the following:

- Identifying issues quickly with continuous monitoring, real-time proactive alerts, and detailed diagnostics.
- Making you aware of potential problems through Smart Call Home notifications, in which a service request has been opened, with all diagnostic data attached.
- Resolving critical problems faster with direct, automatic access to experts in Cisco TAC.

Smart Call Home offers increased operational efficiency by providing you with the ability to do the following:

- Use staff resources more efficiently by reducing troubleshooting time.
- Generate service requests to Cisco TAC automatically (if you have a service contract), routed to the appropriate support team, which provides detailed diagnostic information that speeds problem resolution.

The Smart Call Home Portal offers quick, web-based access to required information that provides you with the ability to do the following:

- Review all Smart Call Home messages, diagnostics, and recommendations in one place.
- Check service request status quickly.
- View the most up-to-date inventory and configuration information for all Smart Call Home-enabled devices.

# Licensing Requirements for Anonymous Reporting and Smart Call Home

| Model | License Requirement |
|---|---|
| ASAv | Standard or Premium License. |
| All other models | Base License. |

# Prerequisites for Smart Call Home and Anonymous Reporting

Smart Call Home and Anonymous Reporting have the following prerequisite:

- DNS must be configured. See DNS Requirement, page 49-2 and the Configuring the DNS Server, page 15-13.

# Guidelines and Limitations

### Firewall Mode Guidelines

Supported in routed and transparent firewall modes.

### Context Mode Guidelines

Supported in single mode and multiple context mode.

### IPv6 Guidelines

Supports IPv6.

### Additional Guidelines for Anonymous Reporting

- If an Anonymous Reporting message cannot be sent on the first try, the ASA retries two more times before dropping the message.
- Anonymous Reporting can coexist with other Smart Call Home configurations without changing the existing configuration. For example, if Smart Call Home is off before enabling Anonymous Reporting, it remains off, even after enabling Anonymous Reporting.
- If Anonymous Reporting is enabled, you cannot remove the trust point, and when Anonymous Reporting is disabled, the trust point remains. If Anonymous Reporting is disabled, you can remove the trust point, but disabling Anonymous Reporting does not cause the trust point to be removed.
- If you are using a multiple context mode configuration, the **dns**, **interface**, and **trustpoint** commands are in the admin context, and the **call-home** commands are in the system context.

### Additional Guidelines for Smart Call Home

- In multiple context mode, the **subscribe-to-alert-group snapshot periodic** command is divided into two commands: one to obtain information from the system configuration and one to obtain information from the user context.
- The Smart Call Home back-end server can accept messages in XML format only.
- A Smart Call Home message is sent to Cisco to report important cluster events if you have enabled clustering and configured Smart Call Home to subscribe to the diagnostic alert group with a critical severity level. A Smart Call Home clustering message is sent for only the following events:
  - When a unit joins the cluster
  - When a unit leaves the cluster
  - When a cluster unit becomes the cluster master
  - When a secondary unit fails in the cluster

  Each message that is sent includes the following information:
  - The active cluster member count

– The output of the **show cluster info** command and the **show cluster history** command on the cluster master

# Configuring Anonymous Reporting and Smart Call Home

While Anonymous Reporting is a subfeature of the Smart Call Home feature and allows Cisco to anonymously receive minimal error and health information from the device, the Smart Call Home feature provides customized support of your system health, enabling Cisco TAC to monitor your devices and open a case when there is an issue, often before you know the issue has occurred.

Generally speaking, you can have both features configured on your system at the same time, yet configuring the Smart Call Home feature provides the same functionality as Anonymous reporting, plus customized services.

This section includes the following topics:



## Configuring Anonymous Reporting

To configure Anonymous Reporting and securely provide minimal error and health information to Cisco, perform the following steps:

### Detailed Steps

| | Command | Purpose |
|---|---|---|
| **Step 1** | **call-home reporting anonymous**<br><br>**Example:**<br>`ciscoasa(config)# call-home reporting anonymous` | Enables the Anonymous Reporting feature and creates a new anonymous profile.<br><br>Entering this command creates a trust point and installs a certificate that is used to verify the identity of the Cisco web server. |
| **Step 2** | **call-home test reporting anonymous**<br><br>**Example:**<br>`ciscoasa(config)# call-home test reporting anonymous`<br><br>`INFO: Sending test message to https://tools.cisco.com/its/service/oddce/services/DDCEService...`<br>`INFO: Succeeded` | (Optional) Ensures that you have connectivity to the server and that your system can send messages.<br><br>A success or error message returns test results. |

# Configuring Smart Call Home

This section includes the following topics:



## Enabling Smart Call Home

To enable Smart Call Home and activate your call-home profile, perform the following steps:

| | | |
|---|---|---|
| **Step 1** | **service call-home**<br><br>**Example:**<br>`hostname(config)# service call-home` | Enables the Smart Call Home service. |
| **Step 2** | **call-home**<br><br>**Example:**<br>`hostname(config)# call-home` | Enters call-home configuration mode. |
| **Step 3** | **contact-email-addr** *email*<br><br>**Example:**<br>`hostname(cfg-call-home)# contact-email-addr username@example.com` | Configures the mandatory contact address. The address should be the Cisco.com ID account associated with the device. This account is the e-mail address that you used to register the ASA with Cisco on Cisco.com. |
| **Step 4** | **profile** *profile-name*<br><br>**Example:**<br>`hostname(cfg-call-home)# profile CiscoTAC-1` | Enables the profile.<br><br>The default profile name is CiscoTAC-1. |
| **Step 5** | **active**<br><br>**Example:**<br>`hostname(cfg-call-home-profile)# active` | Activates the call home profile.<br><br>To disable this profile, enter the **no active** command. |
| **Step 6** | **destination transport-method http**<br><br>**Example:**<br>`hostname(cfg-call-home-profile)# destination transport-method http` | Configures the destination transport method for the smart call-home message receiver.<br><br>The default destination transport method is e-mail. To configure e-mail, see Enabling Smart Call Home, page 49-6. |

## Declaring and Authenticating a CA Trust Point

If Smart Call Home is configured to send messages to a web server through HTTPS, you need to configure the ASA to trust the certificate of the web server or the certificate of the Certificate Authority (CA) that issued the certificate. The Cisco Smart Call Home Production server certificate is issued by Verisign. The Cisco Smart Call Home Staging server certificate is issued by the Digital Signature Trust Co.

**Note** You should set the trust point for no client-types/no validation-usage to prevent it from being used for VPN validation.

### Detailed Steps

To declare and authenticate the Cisco server security certificate and establish communication with the Cisco HTTPS server for Smart Call Home service, perform the following steps:

| | | |
|---|---|---|
| **Step 1** | **changeto context** *admincontext*<br><br>**Example:**<br>`ciscoasa(config)# changeto context contextA` | (Multiple Context Mode only) Installs the certificate in the admin context. |
| **Step 2** | **crypto ca trustpoint** *trustpoint-name*<br><br>**Example:**<br>`ciscoasa(config)# crypto ca trustpoint cisco` | Configures a trust point and prepares for certificate enrollment.<br><br>**Note** If you use HTTP as the transport method, you must install a security certificate through a trust point, which is required for HTTPS. Find the specific certificate to install at the following URL:<br><br>http://www.cisco.com/en/US/docs/switches/lan/smart_call_home/SCH31_Ch6.html#wp1035380 |
| **Step 3** | **enroll terminal**<br><br>**Example:**<br>`ciscoasa(ca-trustpoint)# enroll terminal` | Specifies a manual cut-and-paste method of certificate enrollment. |
| **Step 4** | **crypto ca authenticate** *trustpoint*<br><br>**Example:**<br>`ciscoasa(ca-trustpoint)# crypto ca authenticate cisco` | Authenticates the named CA. The CA name should match the trust point name specified in the **crypto ca trustpoint** command. At the prompt, paste the security certificate text. |
| **Step 5** | **quit**<br><br>**Example:**<br>`ciscoasa(ca-trustpoint)# quit`<br><br>`%Do you accept this certificate [yes/no]:`<br><br>**yes** | Specifies the end of the security certificate text and confirms acceptance of the entered security certificate. |

## Subscribing to Alert Groups

An alert group is a predefined subset of the Smart Call Home alerts that are supported on the ASA. Different types of Smart Call Home alerts are grouped into different alert groups, depending on their type. Each alert group reports the output of certains CLIs. The supported Smart Call Home alert groups are the following:

- syslog
- diagnostic
- environment
- inventory
- configuration
- threat
- snapshot
- telemetry
- test

This section includes the following topics:



### Attributes of Alert Groups

Alert groups have the following attributes:

- Events first register with one alert group.
- A group can associate with multiple events.
- You can subscribe to specific alert groups.
- You can enable and disable specific alert groups. The default setting is enabled for all alert groups.
- The diagnostic and environment alert groups support subscription for periodic messages.
- The syslog alert group supports message ID-based subscription.
- You can configure a threshold for CPU and memory usage for the environment alert group. When a certain parameter has exceeded a predefined threshold, a message is sent. Most of the threshold values are platform-dependent and cannot be changed.
- You configure the snapshot alert group to send the output of CLIs that you specify.

### Information Sent to Cisco by Alert Groups

Messages are sent to Cisco periodically and whenever the ASA reloads. These messages are categorized by alert groups.

Inventory alerts consist of output from the following commands:

- **show version**—Displays the ASA software version, hardware configuration, license key, and related uptime data for the device.
- **show inventory—**Retrieves and displays inventory information about each Cisco product that is installed in the networking device. Each product is identified by unique device information, called the UDI, which is a combination of three separate data elements: the product identifier (PID), the version identifier (VID), and the serial number (SN).
- **show failover state**—Displays the failover state of both units in a failover pair. The information displayed includes the primary or secondary status of the unit, the Active/Standby status of the unit, and the last reported reason for failover.
- **show module**—Shows information about any modules installed on the ASAs, for example, information about an AIP SSC installed on the ASA 5505 or information about an SSP installed on the ASA 5585-X, and information about an IPS SSP installed on an ASA 5585-X.
- **show environment**—Shows system environment information for ASA system components, such as hardware operational status for the chassis, drivers, fans, and power supplies, as well as temperature status, voltage, and CPU usage.

Configuration alerts consist of output from the following commands:

- **show context**—Shows allocated interfaces and the configuration file URL, the number of contexts configured, or if you enable Anonymous Reporting in the system execution space, from a list of all contexts.
- **show call-home registered-module status**—Shows the registered module status. If you use system configuration mode, the command displays system module status based on the entire device, not per context.
- **show running-config**—Shows the configuration that is currently running on the ASA.
- **show startup-config**—Show the startup configuration.
- **show access-list | include elements**—Shows the hit counters and a timestamp value for an access list.

Diagnostic alerts consist of output from the following commands:

- **show failover**—Displays information about the failover status of the unit.
- **show interface**—Displays interface statistics.
- **show cluster info**—Displays cluster information.
- **show cluster history**—Displays the cluster history.
- **show crashinfo** (truncated)—After an unexpected software reload, the device sends a modified crash information file with only the traceback section of the file included, so only function calls, register values, and stack dumps are reported to Cisco.
- **show tech-support no-config**—Displays the information that is used for diagnosis by technical support analysts.

Environment alerts consist of output from the following command:

- **show environment**—Shows system environment information for ASA system components, such as hardware operational status for the chassis, drivers, fans, and power supplies, as well as temperature status, voltage, and CPU usage.
- **show cpu usage**—Displays CPU usage information.
- **show memory detail**—Displays details of the free and allocated system memory.

Threat alerts consist of output from the following commands:

- **show threat-detection rate**—Displays threat detection statistics.
- **show threat-detection shun**—Displays currently shunned hosts.
- **show shun**—Displays shun information.
- **show dynamic-filter reports top**—Generates reports of the top 10 malware sites, ports, and infected hosts classified by the Botnet Traffic Filter.

Snapshot alerts may consist of output from the following commands (for example):

- **show conn count**—Shows the number of active connections.
- **show asp drop**—Shows the accelerated security path dropped packets or connections.

Telemetry alerts consist of output from the following commands:

- **show perfmon detail**—Shows ASA performance details.
- **show traffic**—Displays interface transmit and receive activity.
- **show conn count**—Shows the number of active connections.
- **show vpn-sessiondb summary**—Shows VPN session summary information.
- **show vpn load-balancing**—Displays the runtime statistics for the VPN load-balancing virtual cluster configuration.
- **show local-host | include interface**—Shows the network states of local hosts.
- **show memory**—Displays a summary of the maximum physical memory and current free memory available to the operating system.
- **show context**—Shows allocated interfaces and the configuration file URL, the number of contexts configured, or if you enable Anonymous Reporting in the system execution space, from a list of all contexts.
- **show access-list | include elements**—Shows the hit counters and a timestamp value for an access list.
- **show interface**—Displays interface statistics.
- **show threat-detection statistics protocol**—Shows IP protocol statistics.
- **show phone-proxy media-sessions count**—Displays the number of corresponding media sessions stored by the Phone Proxy.
- **show phone-proxy secure-phones count**—Displays the number of phones capable of secure mode stored in the database.
- **show route**—Displays the routing table.
- **show xlate count**—Shows the number of NAT sessions (xlates).

## Information About the Message Severity Threshold

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

Table 49-1 shows the mapping between message severity levels and syslog severity levels.

***Table 49-1 Message Severity Level and Syslog Level Mapping***

| Level | Message Severity Level | Syslog Severity Level | Description |
|---|---|---|---|
| 9 | Catastrophic | N/A | Network-wide catastrophic failure. |
| 8 | Disaster | N/A | Significant network impact. |
| 7 | Determined by the specified CLI keyword: **subscribe-to-alert-group** *name of alert group* **severity** *severity level* | 0 | Emergency. System is unusable. |
| 6 | | 1 | Alert. Critical conditions; immediate attention needed. |
| 5 | | 2 | Critical. Major conditions. |
| 4 | | 3 | Error. Minor conditions. |
| 3 | Warning | 4 | Warning conditions. |
| 2 | Notification | 5 | Basic notification and informational messages. Possibly independently insignificant. |
| 1 | Normal | 6 | Information. Normal event, signifying a return to normal state. |
| 0 | Debugging | 7 | Debugging messages (default setting). |

## Information About Subscription Profiles

A subscription profile allows you to associate the destination recipients with interested groups. When an event registered with a subscribed group in a profile is triggered, the message associated with the event is sent to the configured recipients. Subscription profiles have the following attributes:

- You can create and configure multiple profiles.
- A profile may configure multiple e-mail or HTTPS recipients.
- A profile may subscribe multiple groups to a specified severity level.
- A profile supports three message formats: short text, long text, and XML.
- You can enable and disable a specific profile. Profiles are disabled by default.
- You can specify the maximum message size. The default is 3 MB.

A default profile, "Cisco TAC," has been provided. The default profile has a predefined set of groups (diagnostic, environment, inventory, configuration, and telemetry) to monitor and predefined destination e-mail and HTTPS URLs. The default profile is created automatically when you initially configure Smart Call Home. The destination e-mail is callhome@cisco.com and the destination URL is https://tools.cisco.com/its/service/oddce/services/DDCEService.

**Note** You cannot change the destination e-mail or the destination URL of the default profile.

When you subscribe a destination profile to the configuration, inventory, telemetry, or snapshot alert groups, you can choose to receive the alert group messages asynchronously or periodically at a specified time.

Table 49-2 maps the default alert group to its severity level subscription and period (if applicable):

***Table 49-2 Alert Group to Severity Level Subscription Mapping***

| Group | Severity Level | Period |
|---|---|---|
| Configuration | Informational | Monthly |
| Diagnostic | Informational and higher | N/A |
| Environment | Notification and higher | N/A |
| Inventory | Informational | Monthly |
| Snapshot | Informational | N/A |
| Syslog | Equivalent syslog | N/A |
| Telemetry | Informational | Daily |
| Test | N/A | N/A |
| Threat | Notification | N/A |

### Configuring the Environment and Snapshot Alert Groups

To configure the environment and snapshot alert groups, enter the following command:

| Command | Purpose |
|---|---|
| **alert-group-config** {**environment** \| **snapshot**}<br><br>**Example:**<br>`hostname(config)# alert-group-config environment` | Enters alert-group-configuration mode. |

## Configuring Alert Group Subscription

To subscribe a destination profile to an alert group, perform the following steps:

### Detailed Steps

| | Command | Purpose |
|---|---|---|
| **Step 1** | **call-home**<br><br>**Example:**<br>`hostname(config)# call-home` | Enters call-home configuration mode. |
| **Step 2** | **alert-group** {**all** \| **configuration** \| **diagnostic** \| **environment** \| **inventory** \| **syslog**}<br><br>**Example:**<br>`ciscoasa(cfg-call-home)# alert-group syslog` | Enables the specified Smart Call Home alert group. Use the **all** keyword to enable all alert groups. By default, all alert groups are enabled. |
| **Step 3** | **profile** *profile-name*<br><br>**Example:**<br>`ciscoasa(cfg-call-home)# profile CiscoTAC-1` | Enters the profile configuration submode for the specified destination profile.<br><br>**Note** This is the same profile that you used in the Enabling Smart Call Home, page 49-6. |
| **Step 4** | **subscribe-to-alert-group all**<br><br>**Example:**<br>`ciscoasa(cfg-call-home-profile)# subscribe-to-alert-group all` | Subscribes to all available alert groups. |
| **Step 5** | **subscribe-to-alert-group configuration periodic** {**daily** *hh:mm* \| **monthly** *date hh:mm* \| **weekly** *day hh:mm*}<br><br>**Example:**<br>`ciscoasa(cfg-call-home-profile)# subscribe-to-alert-group configuration periodic weekly Wednesday 23:30` | Subscribes this destination profile to the configuration alert group.<br><br>The **periodic** keyword configures the configuration alert group for periodic notification. The default period is daily.<br><br>The **daily** keyword specifies the time of the day to send, in the *hh:mm* format, with a 24-hour clock (for example, 14:30).<br><br>The **weekly** keyword specifies the day of the week and time of day in the *day hh:mm* format, where the day of the week is spelled out (for example, Monday).<br><br>The **monthly** keyword specifies the numeric date, from 1 to 31, and the time of day, in the *date hh:mm* format. |

| | Command | Purpose |
|---|---|---|
| Step 6 | **subscribe-to-alert-group environment** [**severity**] {**catastrophic** \| **disaster** \| **emergencies** \| **alert** \| **critical** \| **errors** \| **warnings** \| **notifications** \| **informational** \| **debugging**}<br><br>**Example:**<br>`ciscoasa(cfg-call-home-profile)# subscribe-to-alert-group environment severity critical` | Subscribes to environment events with the specified optional severity level.<br><br>The **severity** keyword filters messages based on the severity level, as described in Table 49-1. The default severity level is 6 (informational). |
| Step 7 | **subscribe-to-alert-group syslog** [**severity**] {**catastrophic** \| **disaster** \| **fatal** \| **critical** \| **major** \| **minor** \| **warning** \| **notification** \| **normal** \| **debugging**} [**pattern** *string*]]<br><br>**Example:**<br>`ciscoasa(cfg-call-home-profile)# subscribe-to-alert-group syslog severity notification pattern UPDOWN` | Subscribes to syslog events with an optional severity level or message ID.<br><br>The **severity** keyword filters messages based on the severity level, as described in Table 49-1. The default severity level is 6 (informational).<br><br>The **pattern** *string* keyword argument pair is available only if you specify the optional syslog severity level or message ID. |
| Step 8 | **subscribe-to-alert-group inventory periodic** {**daily** *hh:mm* \| **monthly** *date hh:mm* \| **weekly** *day hh:mm*}<br><br>**Example:**<br>`ciscoasa(cfg-call-home-profile)# subscribe-to-alert-group inventory periodic daily 06:30` | Subscribes to inventory periodic events. The default period is daily.<br><br>The **daily** keyword specifies the time of the day to send, in the *hh:mm* format, with a 24-hour clock (for example, 14:30).<br><br>The **weekly** keyword specifies the day of the week and time of day in the *day hh:mm* format, where the day of the week is spelled out (for example, Monday).<br><br>The **monthly** keyword specifies the numeric date, from 1 to 31, and the time of day, in the *date hh:mm* format. |

| | Command | Purpose |
|---|---|---|
| Step 9 | **subscribe-to-alert-group telemetry periodic** {**hourly** \| **daily** \| **monthly** *day* \| **weekly** *day* [*hh:mm*]}<br><br>**Example:**<br>`ciscoasa(cfg-call-home-profile)# subscribe-to-alert-group monthly 15` | Subscribes to telemetry periodic events. The default period is daily.<br>The **daily** keyword specifies the time of the day to send, in the *hh:mm* format, with a 24-hour clock (for example, 14:30).<br>The **weekly** keyword specifies the day of the week and time of day in the *day hh:mm* format, where the day of the week is spelled out (for example, Monday).<br>The **monthly** keyword specifies the numeric date, from 1 to 31, and the time of day, in the *date hh:mm* format. |
| Step 10 | **subscribe-to-alert-group snapshot periodic** {**interval** **minutes** \| **hourly** \| **daily** \| **monthly** *day_of_month* \| **weekly** *day_of_week* [*hh:mm*]}<br><br>**Example:**<br>`ciscoasa(cfg-call-home-profile)# subscribe-to-alert-group snapshot periodic interval weekly wednesday 23:15` | Subscribes to snapshot periodic events. The default period is daily.<br>The **interval** keyword specifies the notification interval.<br>The **daily** keyword specifies the time of the day to send, in the *hh:mm* format, with a 24-hour clock (for example, 14:30).<br>The **weekly** keyword specifies the day of the week and time of day in the *day hh:mm* format, where the day of the week is spelled out (for example, Monday).<br>The **monthly** keyword specifies the numeric date, from 1 to 31, and the time of day, in the *date hh:mm* format. |

## Optional Configuration Procedures

This section includes the following topics:



### Configuring Smart Call Home Customer Contact Information

You have already configured the customer e-mail address as part of the Enabling Smart Call Home, page 49-6. This section describes how to configure additional optional customer contact information. You can specify one or more of the following:

- Phone number
- Street address
- Customer Contract ID

- Customer name
- Cisco Customer ID
- Customer Site ID

To configure customer contact information, perform the following steps:

### Detailed Steps

| | Command | Purpose |
|---|---|---|
| **Step 1** | **call-home**<br><br>**Example:**<br>`hostname(config)# call-home` | Enters call-home configuration mode. |
| **Step 2** | (Optional) **phone-number** *phone-number-string*<br><br>**Example:**<br>`ciscoasa(cfg-call-home)# phone-number 8005551122` | Specifies the customer phone number. Spaces are allowed, but you must use quotes around the string if it includes spaces. |
| **Step 3** | (Optional) **street-address** *street-address*<br><br>**Example:**<br>`ciscoasa(cfg-call-home)# street-address "1234 Any Street, Any city, Any state, 12345"` | Specifies the customer address, which is a free-format string that can be up to 255 characters long. Spaces are allowed, but you must use quotes around the string if it includes spaces. |
| **Step 4** | (Optional) **contact-name** *contact-name*<br><br>**Example:**<br>`ciscoasa(cfg-call-home)# contact-name contactname1234` | Specifies the customer name, which can be up to 128 characters long. Spaces are allowed, but you must use quotes around the string if it includes spaces. |
| **Step 5** | (Optional) **customer-id** *customer-id-string*<br><br>**Example:**<br>`ciscoasa(cfg-call-home)# customer-id customer1234` | Specifies the Cisco customer ID, which can be up to 64 characters long. Spaces are allowed, but you must use quotes around the string if it includes spaces. |
| **Step 6** | (Optional) **site-id** *site-id-string*<br><br>**Example:**<br>`ciscoasa(cfg-call-home)# site-id site1234` | Specifies the customer site ID, which can be up to 64 characters long. Spaces are allowed, but you must use quotes around the string if it includes spaces. |
| **Step 7** | (Optional) **contract-id** *contract-id-string*<br><br>**Example:**<br>`ciscoasa(cfg-call-home)# contract-id contract1234` | Specifies the customer contract identification, which can be up to 128 characters long. Spaces are allowed, but you must use quotes around the string if it includes spaces. |

### Example

The following example shows how to configure contact information:

```
hostname(config)# call-home
ciscoasa(cfg-call-home)# contact-email-addr username@example.com
ciscoasa(cfg-call-home)# phone-number 8005551122
```

```
ciscoasa(cfg-call-home)# street-address "1234 Any Street, Any city, Any state, 12345"
ciscoasa(cfg-call-home)# contact-name contactname1234
ciscoasa(cfg-call-home)# customer-id customer1234
ciscoasa(cfg-call-home)# site-id site1234
ciscoasa(cfg-call-home)# contract-id contract1234
```

### Configuring the Mail Server

We recommend that you use HTTPS for message transport because it is the most secure. However, you can configure an e-mail destination for Smart Call Home and then configure the mail server to use the e-mail message transport.

To configure the mail server, perform the following steps:

### Detailed Steps

| | Command | Purpose |
|---|---|---|
| **Step 1** | **call-home**<br><br>**Example:**<br>`hostname(config)# call-home` | Enters call-home configuration mode. |
| **Step 2** | **mail-server** *ip-address* **name priority** [**1-100**] [**all**]<br><br>**Example:**<br>`ciscoasa(cfg-call-home)# mail-server 10.10.1.1 smtp.example.com priority 1` | Specifies the SMTP mail server. You can specify up to five mail servers, using five separate commands. You must configure at least one mail server for using e-mail transport of Smart Call Home messages.<br><br>The lower the number, the higher the priority of the mail server.<br><br>The *ip-address* argument can be an IPv4 or IPv6 mail server address. |

### Example

The following example shows how to configure a primary mail server (named"smtp.example.com") and a secondary mail server at IP address 10.10.1.1:

```
hostname(config)# call-home
ciscoasa(cfg-call-home)# mail-server smtp.example.com priority 1
ciscoasa(cfg-call-home)# mail-server 10.10.1.1 priority 2
ciscoasa(cfg-call-home)# exit
hostname(config)#
```

### Configuring Call Home Traffic Rate Limiting

You can configure this optional setting to specify the number of messages that Smart Call Home sends per minute.

To configure Smart Call Home traffic rate limiting, perform the following steps:

### Detailed Steps

| | Command | Purpose |
|---|---|---|
| **Step 1** | **call-home**<br><br>**Example:**<br>`hostname(config)# call-home` | Enters call-home configuration mode. |
| **Step 2** | **rate-limit** *msg-count*<br><br>**Example:**<br>`ciscoasa(cfg-call-home)# rate-limit 5` | Specifies the number of messages that Smart Call Home can send per minute. The default value is 10 messages per minute. |

### Example

The following example shows how to configure Smart Call Home traffic rate limiting:

```
hostname(config)# call-home
ciscoasa(cfg-call-home)# rate-limit 5
```

### Testing Smart Call Home Communications

You can optionally test Smart Call Home communications by sending messages manually using two command types.

To manually send a Smart Call Home test message, enter the following command:

| Command | Purpose |
|---|---|
| **call-home test** [*test-message*] **profile** *profile-name*<br><br>**Example:**<br>`ciscoasa# call-home test [testing123] profile CiscoTAC-1` | Sends a test message using a profile configuration. |

To manually trigger a Call Home alert group message, enter the following command:

| Command | Purpose |
|---|---|
| **call-home send alert-group** {**inventory** \| **configuration** \| **snapshot** \| **telemetry**} [**profile** *profile-name*]<br><br>**Example:**<br>`ciscoasa# call-home send alert-group inventory` | Sends an alert group message to one destination profile, if specified. If no profile is specified, sends messages to all profiles that are subscribed to the inventory, configuration, snapshot, or telemetry alert groups. |

To execute a CLI command and e-mail the command output to Cisco TAC or to an e-mail address that you specify, enter the following command:

| Command | Purpose |
|---|---|
| **call-home send** *cli command* [**email** *email*]<br><br>**Example:**<br>`ciscoasa# call-home send cli destination email username@example.com` | Sends command output to an e-mail address. The specified CLI command can be any command, including commands for all registered modules.<br><br>If you specify an e-mail address, the command output is sent to that address. If no e-mail address is specified, the output is sent to Cisco TAC. The e-mail is sent in log text format with the service number, if specified, in the subject line.<br><br>The service number is required only if no e-mail address is specified, or if a Cisco TAC e-mail address is specified. |

### Managing a Destination Profile

This section includes the following topics:

### Configuring a Destination Profile

To configure a destination profile for e-mail or for HTTP, perform the following steps:

## Detailed Steps

| | | |
|---|---|---|
| **Step 1** | **call-home**<br><br>**Example:**<br>`hostname(config)# call-home` | Enters call-home configuration mode. |
| **Step 2** | **profile** *profile-name*<br><br>**Example:**<br>`ciscoasa(cfg-call-home)# profile newprofile` | Enters the profile configuration mode for the specified destination profile. If the specified destination profile does not exist, it is created.<br><br>You can create a maximum of 10 active profiles. The default profile is to report back to Cisco TAC. If you want to send call home information to a different location (for example, your own server), you can configure a separate profile. |
| **Step 3** | **destination** {**email** *address* \| **http** *url*} \| **message-size-limit** *size* \| **preferred-msg-format** {**long-text** \| **short-text** \| **xml**} **transport-method** {**email** \| **http**}}<br><br>**Example:**<br>`ciscoasa(cfg-call-home-profile)# destination address email username@example.com`<br><br>`ciscoasa(cfg-call-home-profile)# destination preferred-msg-format long-text` | Configures the destination, message size, message format, and transport method for the smart call-home message receiver. The default message format is XML, and the default enabled transport method is e-mail. The e-mail-address is the e-mail address of the smart call-home message receiver, which can be up to 100 characters long. By default, the maximum URL size is 5 MB.<br><br>Use the short-text format to send and read a message on a mobile device, and use the long text format to send and read a message on a computer.<br><br>If the message receiver is the Smart Call Home back-end server, ensure that the **preferred-msg-format** value is XML because the back-end server can accept messages in XML format only.<br><br>The Enabling Smart Call Home, page 49-6 specifies how to set the transport method to HTTP. You can use this command to change the transport method back to e-mail. |

### Copying a Destination Profile

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

## Detailed Steps

| | Command | Purpose |
|---|---|---|
| **Step 1** | **call-home**<br><br>**Example:**<br>`ciscoasa(config)# call-home` | Enters call-home configuration mode. |
| **Step 2** | **profile** *profile-name*<br><br>**Example:**<br>`ciscoasa(cfg-call-home)# profile newprofile` | Specifies the profile to copy. |
| **Step 3** | **copy profile** *src-profile-name dest-profile-name*<br><br>**Example:**<br>`ciscoasa(cfg-call-home)# copy profile newprofile profile1` | Copies the content of an existing profile (*src-profile-name*, which can be up to 23 characters long) to a new profile (*dest-profile-name*, which can be up to 23 characters long). |

## Example

The following example shows how to copy an existing profile:

```
hostname(config)# call-home
ciscoasa(cfg-call-home)# profile newprofile
ciscoasa(cfg-call-home-profile)# copy profile newprofile profile1
```

### Renaming a Destination Profile

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

## Detailed Steps

| | Command | Purpose |
|---|---|---|
| **Step 1** | **call-home**<br><br>**Example:**<br>`hostname(config)# call-home` | Enters call-home configuration mode. |

| | Command | Purpose |
|---|---|---|
| **Step 2** | **profile** *profilename*<br><br>**Example:**<br>`ciscoasa(cfg-call-home)# profile newprofile` | Specifies the profile to rename. |
| **Step 3** | **rename profile** *src-profile-name dest-profile-name*<br><br>**Example:**<br>`ciscoasa(cfg-call-home)# rename profile newprofile profile1` | Changes the name of an existing profile, the *src-profile-name* (an existing profile name can be up to 23 characters long), and the *dest-profile-name* (a new profile name can be up to 23 characters long). |

### Example

The following example shows how to rename an existing profile:

```
hostname(config)# call-home
ciscoasa(cfg-call-home)# profile newprofile
ciscoasa(cfg-call-home-profile)# rename profile newprofile profile1
```

# Monitoring Anonymous Reporting and Smart Call Home

To monitor the Anonymous Reporting and Smart Call Home features,enter one of the following commands:

| Command | Purpose |
|---|---|
| **show call-home detail** | Shows the current Smart Call Home detail configuration. |
| **show call-home mail-server status** | Shows the current mail server status. |
| **show call-home profile** {*profile name* \| **all**} | Shows the configuration of Smart Call Home profiles. |
| **show call-home registered-module status** [all] | Shows the registered module status. |
| **show call-home statistics** | Shows call-home detail status. |
| **show call-home** | Shows the current Smart Call Home configuration. |
| **show running-config call-home** | Shows the current Smart Call Home running configuration. |

| Command | Purpose |
|---|---|
| **show smart-call-home alert-group** | Shows the current status of Smart Call Home alert groups. |
| **show running-config all** | Shows details about the Anonymous Reporting user profile. |

# Configuration Example for Smart Call Home

The following example shows how to configure the Smart Call Home feature:

```
ciscoasa (config)# service call-home
ciscoasa (config)# call-home
ciscoasa (cfg-call-home)# contact-email-addr customer@example.com
ciscoasa (cfg-call-home)# profile CiscoTAC-1
ciscoasa (cfg-call-home-profile)# destination address http
https://example.cisco.com/its/service/example/services/ExampleService
ciscoasa (cfg-call-home-profile)# destination address email callhome@example.com
ciscoasa (cfg-call-home-profile)# destination transport-method http
ciscoasa (cfg-call-home-profile)# subscribe-to-alert-group inventory periodic daily 23:30
ciscoasa (cfg-call-home-profile)# subscribe-to-alert-group configuration periodic weekly
Wednesday 23:30
ciscoasa (cfg-call-home-profile)# subscribe-to-alert-group environment
ciscoasa (cfg-call-home-profile)# subscribe-to-alert-group diagnostic
ciscoasa (cfg-call-home-profile)# subscribe-to-alert-group telemetry periodic weekly
Monday 23:30
```

# Feature History for Anonymous Reporting and Smart Call Home

Table 49-3 lists each feature change and the platform release in which it was implemented.

*Table 49-3 Feature History for Anonymous Reporting and Smart Call Home*

| Feature Name | Platform Releases | Feature Information |
|---|---|---|
| Smart Call Home | 8.2(2) | The Smart Call Home feature offers proactive diagnostics and real-time alerts on the ASA, and provides higher network availability and increased operational efficiency.<br>We introduced or modified the following commands:<br>**active (call home)**, **call-home, call-home send alert-group, call-home test, contact-email-addr**, **customer-id (call home)**, **destination (call home)**, **profile**, **rename profile**, **service call-home, show call-home, show call-home detail**, **show smart-call-home alert-group**, **show call-home profile**, **show call-home statistics**, **show call-home mail-server status**, **show running-config call-home**, **show call-home registered-module status all**, **site-id**, **street-address**, **subscribe-to-alert-group all**, **alert-group-config**, **subscribe-to-alert-group configuration**, **subscribe-to-alert-group diagnostic**, **subscribe-to-alert-group environment**, **subscribe-to-alert-group inventory periodic**, **subscribe-to-alert-group snapshot periodic**, **subscribe-to-alert-group syslog**, **subscribe-to-alert-group telemetry periodic**. |
| Anonymous Reporting | 9.0(1) | You can help to improve the ASA platform by enabling Anonymous Reporting, which allows Cisco to securely receive minimal error and health information from a device.<br>We introduced the following commands: **call-home reporting anonymous**, **call-home test reporting anonymous**. |

*Table 49-3 Feature History for Anonymous Reporting and Smart Call Home (continued)*

| Feature Name | Platform Releases | Feature Information |
|---|---|---|
| Smart Call Home | 9.1(2) | The **show local-host** command was changed to the **show local-host \| include interface** command for telemetry alert group reporting. |
| Smart Call Home | 9.1(3) | A Smart Call Home message is sent to Cisco to report important cluster events if you have enabled clustering and configured Smart Call Home to subscribe to the Diagnostic alert group with a Critical severity level. A Smart Call Home clustering message is sent for only the following three events:<br>• When a unit joins the cluster<br>• When a unit leaves the cluster<br>• When a cluster unit becomes the cluster master<br>Each message that is sent includes the following information:<br>• The active cluster member count<br>• The output of the **show cluster info** command and the **show cluster history** command on the cluster master |