Anonymous Reporting and Smart Call Home

This chapter describes how to configure the Anonymous Reporting and Smart Call Home services.

About Anonymous Reporting

You can help to improve the Cisco 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

When the ASA configures Smart Call Home anonymous reporting in the background, the ASA automatically creates a trustpoint containing the certificate of the CA that issues the Call Home server certificate. The ASA now supports validation of the certificate if the issuing hierarchy of the server certificate changes, without the need for customer involvement to make certificate hierarchy changes. You can also automatically import the trustpool certificates so that ASA renews the certificate hierarchy without any manual intervention.

DNS Requirement

A DNS server must be configured correctly for the ASA to reach the Cisco Smart Call Home server and send messages to Cisco. Because it is possible that the 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 the 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.

See the syslog messages guide for information about syslog messages.

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 on the seriousness of these problems, Cisco responds to your system configuration issues, product end-of-life announcements, security advisory issues, and so on by providing the following services:

- 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.
- Using staff resources more efficiently by reducing troubleshooting time.

- Generating 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 access to required information that enables you to do the following:

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

Subscribe 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 certain CLIs. The supported Smart Call Home alert groups are the following:

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

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.

Messages 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 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 time stamp 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 commands:

- **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:

- **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 time stamp 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).**

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.

The following table shows the mapping between message severity levels and syslog severity levels.

Table 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	Determined by the specified CLI keyword: **subscribe-to-alert-group** *name of alert group* **severity** *severity level*	1	Alert. Critical conditions; immediate attention needed.
5	Determined by the specified CLI keyword: **subscribe-to-alert-group** *name of alert group* **severity** *severity level*	2	Critical. Major conditions.
4	Determined by the specified CLI keyword: **subscribe-to-alert-group** *name of alert group* **severity** *severity level*	3	Error. Minor conditions.
3	Warning	4	Warning conditions.
2	Notification	5	Basic notification and informational messages. Possibly independently insignificant.

Level	Message Severity Level	Syslog Severity Level	Description
1	Normal	6	Information. Normal event, signifying a return to normal state.
0	Debugging	7	Debugging messages (default setting).

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.

The following table maps the default alert group to its severity level subscription and period (if applicable):

Table 2: Alert Group to Severity Level Subscription Mapping

Alert 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

Alert Group	Severity Level	Period
Telemetry	Informational	Daily
Test	N/A	N/A
Threat	Notification	N/A

Guidelines for Anonymous Reporting and Smart Call Home

This section includes the guidelines and limitation that you should review before configuring Anonymous reporting and Smart Call Home.

Anonymous Reporting Guidelines

- DNS must be configured.
- If an Anonymous Reporting message cannot be sent on the first try, the ASA retries two more times before dropping the message.
- Anonymous Reporting may coexist with other Smart Call Home configurations without changing the existing configuration. For example, if Smart Call Home is disabled before enabling Anonymous Reporting, it remains disabled, even after Anonymous Reporting has been enabled.
- 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.
- You can automate the update of the trustpool bundle at periodic intervals so that Smart Call Home can remain active if the self-signed certificate of the CA server changes. This trustpool auto renewal feature is not supported under multi-context deployments.

Smart Call Home Guidelines

- 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 control unit
  - 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 control unit

Configure Anonymous Reporting and Smart Call Home

While Anonymous Reporting is part of the Smart Call Home service and allows Cisco to anonymously receive minimal error and health information from your device, the Smart Call Home service 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.

You can have both services configured on your system at the same time, although configuring the Smart Call Home service provides the same functionality as Anonymous Reporting, plus customized services.

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

- At the prompt, you may choose [Y]es, [N]o, or [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.
- If you did not receive the prompt, you may enable Anonymous Reporting or Smart Call Home by performing the steps in Configure Anonymous Reporting, on page 9 or in Configure Smart Call Home, on page 10.

Configure Anonymous Reporting

To configure Anonymous Reporting, perform the following steps:

Procedure

Step 1 Enable the Anonymous Reporting feature and create a new anonymous profile.

call-home reporting anonymous

Example:

```
ciscoasa(config)# call-home reporting anonymous
```

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 (Optional) Make sure that you have connectivity to the server and that your system can send messages.

call-home test reporting anonymous

Example:

```
ciscoasa(config)# call-home test reporting anonymous

INFO: Sending test message to
https://tools.cisco.com/its/service/oddce/services/DDCEService...

INFO: Succeeded
```

A success or error message returns test results.

Configure Smart Call Home

Configuring the Smart Call Home service on your ASA includes the following tasks:

Procedure

Step 1 Enable the Smart Call Home service. See Enable Smart Call Home, on page 10.

Step 2 Configure the mail server through which Smart Call Home messages are delivered to subscribers. See Configure the Mail Server, on page 15.

Step 3 Set up contact information for the Smart Call Home messages. See Configure Customer Contact Information, on page 13.

Step 4 Define alert processing parameters, such as the maximum rate of events that can be handled. See Configure Alert Group Subscription, on page 12.

Step 5 Set up alert subscription profiles. See Configure a Destination Profile, on page 17.

Each alert subscription profile identifies the following:

- The subscribers to whom the Smart Call Home messages are sent, such as a Smart Call Home server at Cisco or a list of e-mail recipients.
- Information categories for which you want to receive alerts, such as configuration or inventory information.

Enable Smart Call Home

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

Procedure

Step 1 Enable the Smart Call Home service.

service call-home

Example:

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

Step 2 Enter call-home configuration mode.

call-home

Example:

```
ciscoasa(config)# call home
```

Declare and Authenticate a Certificate Authority 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 Company.

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

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:

Procedure

Step 1 (Multiple Context Mode only) Install the certificate in the admin context.

changeto context *admincontext*

Example:

```
ciscoasa(config)# changeto context contextA
```

Step 2 Configure a trust point and prepare for certificate enrollment.

crypto ca trustpoint *trustpoint-name*

Example:

```
ciscoasa(config)# crypto ca trustpoint cisco
```

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:

http://www.cisco.com/en/US/docs/switches/lan/smart_call_home/SCH31_Ch6.html#wp1035380

Step 3 Specify a manual cut-and-paste method of certificate enrollment.

enroll terminal

Example:

```
ciscoasa(ca-trustpoint)# enroll terminal
```

Step 4 Authenticate 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.

crypto ca authenticate trustpoint

Example:

```
ciscoasa(ca-trustpoint)# crypto ca authenticate cisco
```

Step 5 Specify the end of the security certificate text and confirm acceptance of the entered security certificate.

quit

Example:

```
ciscoasa(ca-trustpoint)# quit
%Do you accept this certificate [yes/no]:
yes
```

Configure the Environment and Snapshot Alert Groups

To configure the environment and snapshot alert groups, perform the following steps:

Procedure

Enter alert-group-configuration mode.

alert-group-config {**environment** | **snapshot**}

Example:

```
ciscoasa(config)# alert-group-config environment
```

Configure Alert Group Subscription

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

Procedure

Step 1 Enter call-home configuration mode.

call-home

Example:

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

Step 2 Enable the specified Smart Call Home alert group.

alert-group {**all** | **configuration** | **diagnostic** | **environment** | **inventory** | **syslog**}

Example:

```
ciscoasa(cfg-call-home)# alert-group syslog
```

Use the **all** keyword to enable all alert groups. By default, all alert groups are enabled.

Step 3 Enter the profile configuration mode for the specified destination profile.

profile *profile-name*

Example:

```
ciscoasa(cfg-call-home)# profile CiscoTAC-1
```

Step 4 Subscribe to all available alert groups.

subscribe-to-alert-group all

Example:

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

Step 5 Subscribe this destination profile to the configuration alert group.

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

Example:

```
ciscoasa(cfg-call-home-profile)# subscribe-to-alert-group configuration periodic weekly
Wednesday 23:30
```

The **periodic** keyword configures the configuration alert group for periodic notification. The default period is daily.

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).

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).

The **monthly** keyword specifies the numeric date, from 1 to 31, and the time of day, in the *date hh:mm* format.

Configure Customer Contact Information

To configure customer contact information, perform the following steps:

Procedure

Step 1 Enter call-home configuration mode.

call-home

Example:

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

Step 2 Specify the customer phone number. Spaces are allowed, but you must use quotes around the string if it includes spaces.

phone-number *phone-number-string*

Example:

```
ciscoasa(cfg-call-home)# phone-number 8005551122
```

Step 3 Specify the customer address, which is a free-format string that may be up to 255 characters long. Spaces are allowed, but you must use quotes around the string if it includes spaces.

street-address *street-address*

Example:

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

Step 4 Specify the customer name, which may be up to 128 characters long. Spaces are allowed, but you must use quotes around the string if it includes spaces.

contact-name *contact-name*

Example:

```
ciscoasa(cfg-call-home)# contact-name contactname1234
```

Step 5 Specify the Cisco customer ID, which may be up to 64 characters long. Spaces are allowed, but you must use quotes around the string if it includes spaces.

customer-id *customer-id-string*

Example:

```
ciscoasa(cfg-call-home)# customer-id customer1234
```

Step 6 Specify the customer site ID, which may be up to 64 characters long. Spaces are allowed, but you must use quotes around the string if it includes spaces.

site-id *site-id-string*

Example:

```
ciscoasa(cfg-call-home)# site-id site1234
```

Step 7 Specify the customer contract identification, which may be up to 128 characters long. Spaces are allowed, but you must use quotes around the string if it includes spaces.

contract-id *contract-id-string*

Example:

```
ciscoasa(cfg-call-home)# contract-id contract1234
```

Example

The following example shows how to configure contact information:

```
ciscoasa(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
```

Configure the Mail Server

We recommend that you use HTTPS for message transport because it is the most secure. However, you may 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:

Procedure

Step 1 Enter call-home configuration mode.

call-home

Example:

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

Step 2 Specify the SMTP mail server.

mail-server*ip-address* **name priority** [**1-100**] [**all**]

Example:

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

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.

The lower the number, the higher the priority of the mail server.

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:

```
ciscoasa(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
ciscoasa(config)#
```

Configure Traffic Rate Limiting

To configure traffic rate limiting, perform the following steps:

Procedure

Step 1 Enter call-home configuration mode.

call-home

Example:

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

Step 2 Specify the number of messages that Smart Call Home can send per minute. The default value is 10 messages per minute.

rate-limit *msg-count*

Example:

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

Send Smart Call Home Communications

To send specific Smart Call Home communications, perform the following steps:

Procedure

Choose one of the following options:

- Option 1—Send a test message manually using a profile configuration.

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

  Example:

  ```
  ciscoasa# call-home test [testing123] profile CiscoTAC-1
  ```

- Option 2—Send an alert group message to one destination profile, if specified. If no profile is specified, send messages to all profiles that are subscribed to the inventory, configuration, snapshot, or telemetry alert groups.

  call-home send alert-group inventory { | **configuration** | **snapshot** | **telemetry**} [**profile** *profile-name*]

  Example:

  ```
  ciscoasa# call-home send alert-group inventory
  ```

- Option 3—Send command output to an e-mail address. The specified CLI command can be any command, including commands for all registered modules.

  call-home send*cli command* [**email** *email*]

  Example:

  ```
  ciscoasa# call-home send cli destination email username@example.com
  ```

  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.

  The service number is required only if no e-mail address is specified, or if a Cisco TAC e-mail address is specified.

Configure a Destination Profile

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

Procedure

Step 1 Enter call-home configuration mode.

call-home

Example:

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

Step 2 Enter the profile configuration mode for the specified destination profile. If the specified destination profile does not exist, it is created.

profile *profile-name*

Example:

```
ciscoasa(cfg-call-home)# profile newprofile
```

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 Configure 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.

destination address {**email** *address* | **http** *url*[**reference-identity** *ref-id-name*]} | **message-size-limit** *size* | **preferred-msg-format** {**long-text** | **short-text** | **xml**} **transport-method** {**email** | **http**}}

Example:

```
ciscoasa(cfg-call-home-profile)# destination address http
https://example.cisco.com/its/service/example/services/ExampleService reference-identity
ExampleService
ciscoasa(cfg-call-home-profile)# destination address email username@example.com
ciscoasa(cfg-call-home-profile)# destination preferred-msg-format long-text
```

The **reference-identity** option enables RFC 6125 reference identity checks on the received server certificate. These only apply to destinations configured with an http address. ID checks are made based on a previously configured reference identity object. See Configure Reference Identities for details on the reference identity object.

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.

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.

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.

Use this command to change the transport method back to e-mail.

Copy a Destination Profile

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

Procedure

Step 1 Enter call-home configuration mode.

call-home

Example:

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

Step 2 Specify the profile to copy.

profile *profile-name*

Example:

```
ciscoasa(cfg-call-home)# profile newprofile
```

Step 3 Copy the content of an existing profile to a new profile.

copy profile *src-profile-name dest-profile-name*

Example:

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

The existing profile (*src-profile-name*) and the new profile (*dest-profile-name*) may be up to 23 characters long.

Example

The following example shows how to copy an existing profile:

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

Rename a Destination Profile

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

Procedure

Step 1 Enter call-home configuration mode.

call-home

Example:

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

Step 2 Specify the profile to rename.

profile *profilename*

Example:

```
ciscoasa(cfg-call-home)# profile newprofile
```

Step 3 Change the name of an existing profile.

rename profile *src-profile-name dest-profile-name*

Example:

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

The existing profile (*src-profile-name*) and the new profile (*dest-profile-name*) may be up to 23 characters long.

Example

The following example shows how to rename an existing profile:

```
ciscoasa(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

See the following commands for monitoring Anonymous Reporting and Smart Call Home services.

- **show call-home detail**

  This command shows the current Smart Call Home detail configuration.

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

  This command shows the current mail server status.

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

  This command shows the configuration of Smart Call Home profiles.

- **show call-home registered-module status** [**all**]

  This command shows the registered module status.

- **show call-home statistics**

This command shows call-home detail status.

- **show call-home**

  This command shows the current Smart Call Home configuration.

- **show running-config call-home**

  This command shows the current Smart Call Home running configuration.

- **show smart-call-home alert-group**

  This command shows the current status of Smart Call Home alert groups.

- **show running-config all**

  This command shows details about the Anonymous Reporting user profile.

Examples for Smart Call Home

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

```
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
```

History for Anonymous Reporting and Smart Call Home

Table 3: History for Anonymous Reporting and Smart Call Home

Feature Name	Platform Releases	Description
Smart Call Home	8.2(2)	The Smart Call Home service offers proactive diagnostics and real-time alerts on the ASA, and provides higher network availability and increased operational efficiency. We introduced or modified the following commands: **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. We introduced the following commands: **call-home reporting anonymous**, **call-home test reporting anonymous**.

Feature Name	Platform Releases	Description
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: • When a unit joins the cluster • When a unit leaves the cluster • When a cluster unit becomes the cluster control unit 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 control unit
Reference Identities for Secure Smart Call Home Server connections	9.6(2)	TLS client processing now supports rules for verification of a server identity defined in RFC 6125, Section 6. Identity verification will be done during PKI validation for TLS connections to the Smart Call Home Server. If the presented identity cannot be matched against the configured reference identity, the connection is not established. We added or modified the following commands: **[no] crypto ca reference-identity**, **call home profile destination address http**.