Configuring Anonymous Reporting and Smart Call Home

The Smart Call Home feature provides personalized, e-mail-based and web-based notification to customers about critical events involving their individual systems, often before customers 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.

Note You might have received a popup dialog that invites you to do the following:

- Enable Anonymous Reporting to help improve the ASA platform.
- Register for Smart Home Notifications to receive personalized, proactive assistance from Cisco.

For information about the dialog, see the "Anonymous Reporting and Smart Call Home Prompt" section on page 77-3.

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

Customers 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 shows up 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

What is Sent to Cisco?

Messages are sent to Cisco once a month and whenever the ASA reloads. These messages are categorized by alert groups, which are predefined subsets of Smart Call Home alerts that are supported on the ASA: configuration alerts, inventory alerts, and crash information alerts.

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 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 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.

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 AR in the system execution space, from a list of all contexts.

- **show call-home registered-module status**—Displays the registered module status. If you use system configuration mode, the command displays system module status based on the entire device, not per context.

Upon a system crash, modified information from the following command is sent:

- **show crashinfo** (truncated)—Upon 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.

For more information about ASA commands, see the Cisco ASA 5500 Series Command Reference document.

DNS Requirement

A DNS server must be configured properly 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.

The above tasks are performed without changing the current configuration. (For example, the DNS server 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 for every Smart Call Home message sent to remind you to configure DNS properly.

For information about system log messages, see the *Cisco ASA 5500 Series System Log Messages*.

Anonymous Reporting and Smart Call Home Prompt

When you enter configuration mode you receive a prompt that invites you to enable the Anonymous Reporting and Smart Call Home features if the following criteria are met:

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 or the .

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 customers regarding their 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, 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

The following table shows the licensing requirements for Anonymous Reporting and Smart Call Home:

Model	License Requirement
All models	Base License.

Prerequisites for Smart Call Home and Anonymous Reporting

Smart Call Home and Anonymous Reporting have the following prerequisites:

- DNS must be configured. (See the "DNS Requirement" section on page 77-3 and see the "Configuring the DNS Server" section on page 8-6.)

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.
- Output from the **show running-config all** command shows details about the Anonymous Reporting user profile.
- 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, users can remove the trustpoint, but disabling Anonymous Reporting will not cause the trustpoint to be removed.

Additional Guidelines for Smart Call Home

- In multiple context mode, the **snapshots** command is divided into two commands: one to obtain information from the system context and one to obtain information from the regular context.
- The Smart Call Home back-end server can accept messages in XML format only.

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 is more robust and allows for customized support of your system health, allowing Cisco TAC to monitor your devices and open a case when there is an issue, often before you know the issue occurred.

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

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`
	
	Example:
	`hostname(config)# call-home reporting anonymous`
		Enables the Anonymous Reporting feature and creates a new anonymous profile.
		
		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`
	
	Example:
	`hostname(config)# call-home test reporting anonymous`
		(Optional) Tests that the Anonymous Reporting feature is fully enabled. Also ensures that you have connectivity to the server and that your system is able to send messages.
		
		A success or error message returns test results.

Configuring Smart Call Home

This section describes how to configure the Smart Call Home feature.

This section includes the following topics:

Enabling Smart Call Home

This section contains information about performing basic setup for the Smart Call Home feature.

To enable Smart Call Home and activate your call-home profile, perform this task:

Step 1	`service call-home`
	
	Example:
	`hostname(config)# service call-home`
		Enables the smart call home service.

Step 2	`call-home`
	
	Example:
	`hostname(config)# call-home`
		Enters call-home configuration mode.

Step 3	`contact-email-addr` *email* **Example:** `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.
Step 4	`profile` *profile-name* **Example:** `hostname(cfg-call-home)# profile CiscoTAC-1`	Enables the profile. The default profile name is CiscoTAC-1.

Step 5	`active`
	
	Example:
	`hostname(cfg-call-home-profile)# active`
		Activates the call home profile.
		
		To disable this profile, enter the **no active** command.

Step 6	`destination transport-method http`
	
	Example:
	`hostname(cfg-call-home-profile)# destination transport-method http`
		Configures the destination transport method for the smart call-home message receiver.
		
		The default destination transport method is e-mail. To configure e-mail see the "Sending the Output of a Command" section on page 77-12.

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 Digital Signature Trust Co.

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 this task:

Step 1	**crypto ca truspoint** *trustpoint-name* **Example:** hostname(config)# crypto ca trustpoint cisco	Configures a trustpoint and prepares for certificate enrollment. **Note** If you use HTTP as the transport method, you must install a security certificate through a trustpoint, 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 2	**enroll terminal** **Example:** hostname(ca-trustpoint)# enroll terminal	Specifies a manual cut-and-paste method of certificate enrollment.
Step 3	**exit** hostname(ca-trustpoint)# exit	Exits CA trustpoint configuration mode and returns to global configuration mode.
Step 4	**crypto ca authenticate** *trustpoint* **Example:** hostname(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** **Example:** hostname(ca-trustpoint)# quit %Do you accept this certificate [yes/no]: **yes**	Specifies the end of the security certificate text and confirms acceptance of th entered security certificate.

Configuring DNS

You must configure DNS so that the HTTPS URLs in the Smart Call Home profile can successfully resolve.

To configure DNS, perform the following tasks:

Step 1	`dns domain-lookup` *name* **Example:** `hostname(config)# dns domain-lookup corp`	Enables DNS lookup on a specific interface.
Step 2	`dns server-group` *group name* **Example:** `hostname(config)# DNS server-group DefaultDNS`	Enters the server group submode to configure the parameters for that server group. We suggest that you use the default server group name: DefaultDNS.
Step 3	`name-server` *name* **Example:** `hostname(config-dns-server-group)# name-server 192.168.1.1`	Specifies the IP address of the DNS server.
Step 4	(Optional) `domain-name` *name* **Example:** `hostname(config-dns-server-group)# domain name domainexample`	Specifies the domain name.

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 upon their type.

This section includes the following alert group topics:

- Configuring Periodic Notification, page 77-9
- Information about the Message Severity Threshold, page 77-9
- Configuring Alert Group Subscription, page 77-10

Configuring 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 the 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*.

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 upon the message level severity. (See Table 77-1). Any message with a value lower than the destination profile's specified threshold is not sent to the destination.

Table 77-1   Severity and Syslog Level Mapping

Level	Keyword	Equivalent 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 (default setting).

Configuring Alert Group Subscription

To subscribe a destination profile to an alert group, perform this task:

Detailed Steps

	Command	Purpose

Step 1	`call-home`
	
	Example:
	`hostname(config) # call-home`
		Enters call-home configuration mode.

Step 2	`alert-group {all	configuration	diagnostic	environment	inventory	syslog}`  **Example:** `ciscoasa(cfg-call-home)# alert-group all`	Enables the specified Smart Call Home group. Use the keyword **all** to enable all alert groups. By default, all alert groups are enabled.

Step 3	`profile profile-name`
	
	Example:
	`hostname(cfg-call-home)# profile profile1`
		Enters the profile configuration submode for the specified destination profile.

Step 4	`subscribe-to-alert-group configuration [periodic {daily hh:mm	monthly date hh:mm	weekly day hh:mm}]`  **Example:** `hostname(cfg-call-home-profile)# subscribe-to-alert-group configuration periodic weekly Wednesday 23:30`	Subscribes this destination profile to the configuration alert group. The configuration alert group can be configured for periodic notification, as described in the "Subscribing to Alert Groups" section on page 77-9. To subscribe to all available alert groups, use the **subscribe-to-alert-group all** command.

	Command	Purpose
Step 5	`subscribe-to-alert-group environment [severity {catastrophic	disaster	emergencies	alert	critical	errors	warnings	notifications	informational	debugging}]`  **Example:** `hostname(cfg-call-home-profile)# subscribe-to-alert-group examplealertgroupname severity critical`	Subscribes to group events with the specified severity level. The alert group can be configured to filter messages based on severity, as described in Table 77-1.
Step 6	`subscribe-to-alert-group syslog [severity {catastrophic	disaster	fatal	critical	major	minor	warning	notification	normal	debugging} [pattern string]]`  **Example:** `hostname(cfg-call-home-profile)# subscribe-to-alert-group syslog severity notification pattern UPDOWN`	Subscribes to syslog events with a severity level or message ID. The syslog alert group can be configured to filter messages based on severity, as described in Table 77-1.
Step 7	`subscribe-to-alert-group inventory [periodic {daily hh:mm	monthly date hh:mm	weekly day hh:mm}]`  **Example:** `hostname(cfg-call-home-profile)# subscribe-to-alert-group inventory periodic daily 06:30`	Subscribes to inventory events. The configuration alert group can be configured for periodic notification, as described in the "Subscribing to Alert Groups" section on page 77-9.
Step 8	`subscribe-to-alert-group telemetry periodic {hourly	daily	monthly day	weekly day [hh:mm]}`  **Example:** `hostname(cfg-call-home-profile)# subscribe-to-alert-group monthly 15`	Subscribes to telemetry periodic events. The configuration alert group can be configured for periodic notification, as described in the "Subscribing to Alert Groups" section on page 77-9.
Step 9	`subscribe-to-alert-group snapshot periodic {interval minutes	hourly	daily	monthly day_of_month	weekly day_of_week [hh:mm]}`  **Example:** `hostname(cfg-call-home-profile)# subscribe-to-alert-group snapshot periodic interval weekly wendesday 23:15`	Subscribes to snapshot periodic events. The configuration alert group can be configured for periodic notification, as described in the "Subscribing to Alert Groups" section on page 77-9.

Testing Call Home Communications

You can test Smart Call Home communications by sending messages manually using two command types. To send a user-defined Smart Call Home test message, use the **call-home test** command. To send a specific alert group message, use the **call-home send** command.

These sections describe Smart Call Home communication:

- Sending a Smart Call Home Test Message Manually, page 77-12
- Sending a Smart Call Home Alert Group Message Manually, page 77-12
- Sending the Output of a Command, page 77-12

Sending a Smart Call Home Test Message Manually

To manually send a Smart Call Home test message, perform this task:

Command	Purpose
call-home test [*test-message*] **profile** *profile-name* **Example:** `hostname# call-home test [testing123] profile profile1`	Sends a test message using a profile configuration.

Sending a Smart Call Home Alert Group Message Manually

To manually trigger a Call Home alert group message, perform this task:

	Command	Purpose
Step 1	**call-home send alert-group** {**inventory** | **configuration** | **snapshot** | **telemetry**} [**profile** *profile-name*] **Example:** `hostname# call-home send alert-group inventory`	Sends an inventory 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 or configuration group.

Sending the Output of a Command

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.

When sending the output of a command, the following guidelines apply:

- The specified CLI command can be any run command, including commands for all modules.
- 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.

To execute a CLI command and e-mail the command output, perform this task:

Command	Purpose
call-home send *cli command* [**email** *email*] **Example:** `hostname# call-home send cli command email username@example.com`	Sends command output to an e-mail address.

Optional Configuration Procedures

This section includes the following topics:

Configuring Smart Call Home Customer Contact Information

Obtain the following customer contact information to configure this task:

- E-mail address (required)
- Phone number (optional)
- Street address (optional)
- Contract ID (optional)
- Customer name (optional)
- Customer ID (optional)
- Site ID (optional)

To configure customer contact information, perform this task:

	Command	Purpose

Step 1	`call-home`
	
	Example:
	`hostname(config)# call-home`
		Enters call home configuration mode.

Step 2	`contact-email-addr` *email-address*
	
	Example:
	`ciscoasa(cfg-call-home)# contact-email-addr`
	`username@example.com`
		Configures the mandatory customer contact e-mail address (if you have not already done so). The *email-address* should be the Cisco.com ID account that is associated with the device.

Step 3	(Optional)
	`phone-number phone-number-string`
	
	Example:
	`ciscoasa(cfg-call-home)# phone-number 8005551122`
		Specifies a customer phone number.

Step 4	(Optional)
	`street-address street-address`
	
	Example:
	`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.

	Command	Purpose
Step 5	(Optional) **contact-name** *contact name* **Example:** ciscoasa(cfg-call-home)# contact-name contactname1234	Specifies the customer name, which can be up to 128 characters long.
Step 6	(Optional) **customer-id customer-id-string** **Example:** ciscoasa(cfg-call-home)# customer-id customer1234	Specifies the customer ID, which can be up to 64 characters long.
Step 7	(Optional) **site-id site-id-string** **Example:** ciscoasa(cfg-call-home)# site-id site1234	Specifies a customer site ID.
Step 8	(Optional) **contract-id** *contract-id-string* **Example:** ciscoasa(cfg-call-home)# contract-id contract1234	Specifies the customer contract identification, which can be up to 128 characters long.

This example shows the configuration of contact information:

```
hostname# configure terminal
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, as 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 this task:

	Command	Purpose

Step 1	`call-home`
	
	Example:
	`hostname(config)# call-home`
		Enters call home configuration mode.

Step 2	`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`
		Specifies the SMTP mail server. Customers can specify up to five mail servers. At least one mail server is required for using e-mail transport for Smart Call Home messages.
		
		The lower the number, the higher the priority of the mail server.
		
		The **ip-address** option can be an IPv4 or IPv6 mail server address.

This example shows the configuration of a primary mail server (named"smtp.example.com") and a secondary mail server at IP address 10.10.1.1:

```
hostname# configure terminal
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 this task:

	Command	Purpose

Step 1	`call-home`
	
	Example:
	`hostname(config)# call-home`
		Enters call home configuration mode.

Step 2	`rate-limit` *msg-count* **Example:** `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.

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

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

Destination Profile Management

These sections describe destination profile management:

Configuring a Destination Profile

To configure a destination profile for e-mail or for HTTP, perform this task:

Step 1	**call-home** **Example:** `hostname(config)# call-home`	Enters call home configuration mode.
Step 2	**profile** *profile-name* **Example:** `hostname(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.

Step 3	**destination {email** *address* **| http** *url***} | message-size-limit** *size* **| preferred-msg-format {long-text | short-text | xml} transport-method {email | http}}**
	
	Example:
	`hostname(cfg-call-home-profile)# destination address email username@example.com`
	
	`hostname(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 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 is XML, as the back-end server can accept messages in XML format only.

Activating and Deactivating a Destination Profile

Smart Call Home destination profiles are automatically activated when you create them. If you do not want to use a profile right away, you can deactivate the profile.

To activate or deactivate a destination profile, perform this task:

	Command	Purpose

Step 1	`call-home`
	
	Example:
	`hostname(config)# call-home`
		Enters call home configuration mode.

Step 2	`profile` *profile-name* **Example:** `hostname(cfg-call-home)# profile newprofile`	Enters the profile configuration mode. Creates, edits, or deletes a profile, which can be up to 20 characters long.

Step 3	`active`
	
	Example:
	`ciscoasa(cfg-call-home-profile)# active`
		Enables or disables a profile. By default, a new profile is enabled when it is created.

Step 4	`no active`
	
	Example:
	`ciscoasa(cfg-call-home-profile)# no active`
		Disables the destination profile.

This example shows how to activate a destination profile:

```
hostname# configure terminal
hostname(config)# call-home
ciscoasa(cfg-call-home)# profile newprofile
ciscoasa(cfg-call-home-profile)# active
ciscoasa(cfg-call-home)# end
```

This example shows how to deactivate a destination profile:

```
hostname# configure terminal
hostname(config)# call-home
ciscoasa(cfg-call-home)# profile newprofile
ciscoasa(cfg-call-home-profile)# no active
ciscoasa(cfg-call-home)# end
```

Copying a Destination Profile

To create a new destination profile by copying an existing profile, perform this task:

	Command	Purpose

Step 1	`call-home`
	
	Example:
	`hostname(config)# call-home`
		Enters call home configuration mode.

Step 2	`profile` *profilename* **Example:** `ciscoasa(cfg-call-home)# profile newprofile`	Specifies the profile to copy.
Step 3	`copy profile` *src-profile-name dest-profile-name* **Example:** `ciscoasa(cfg-call-home)# copy profile profile1 profile2`	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).

This example shows how to copy an existing profile:

```
hostname# configure terminal
hostname(config)# call-home
ciscoasa(cfg-call-home)# profile newprofile
ciscoasa(cfg-call-home-profile)# copy profile profile1 profile2
```

Renaming a Destination Profile

To change the name of an existing profile, perform this task:

	Command	Purpose

Step 1	`call-home`
	
	Example:
	`hostname(config)# call-home`
		Enters call home configuration mode.

Step 2	`profile` *profilename* **Example:** `ciscoasa(cfg-call-home)# profile newprofile`	Specifies the profile to rename.
Step 3	`rename profile` *src-profile-name dest-profile-name* **Example:** `ciscoasa(cfg-call-home)# rename profile profile1 profile2`	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).

This example shows how to rename an existing profile:

```
hostname# configure terminal
hostname(config)# call-home
ciscoasa(cfg-call-home)# profile newprofile
```

```
ciscoasa(cfg-call-home-profile)# rename profile profile1 profile2
```

Monitoring Smart Call Home

To monitor the Smart Call Home feature,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.
show smart-call-home alert-group	Shows the current status of Smart Call Home alert groups.

Configuration Example for Smart Call Home

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

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

Feature History for Anonymous Reporting and Smart Call Home

Table 77-2 lists each feature change and the platform release in which it was implemented. ASDM is backwards-compatible with multiple platform releases, so the specific ASDM release in which support was added is not listed.

Table 77-2   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. 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, subscribe-to-alert-group configuration, subscribe-to-alert-group diagnostic, subscribe-to-alert-group environment, subscribe-to-alert-group inventory, subscribe-to-alert-group syslog.**
Anonymous Reporting	8.2(5)/8.4(2)	Customers 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**.