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 48-5 or the Configuring Smart Call Home, page 48-5.

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 48-2 and the Configuring the DNS Server, page 17-9.

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:

Step 1 Choose **Configuration** > **Device Management** > **Smart Call Home**.

Step 2 Check the **Enable Anonymous Reporting** check box.

Step 3 Click **Test Connection** to ensure that your system is able to send messages.

ASDM returns a success or error message to notify you of test results.

Step 4 Click **Apply** to save the configuration and enable Anonymous Reporting.

At any time you may also choose to enable the full Smart Call Home feature so that you may receive notification from Cisco about critical events involving your system. You can enable Smart Call Home from the same pane in which you enable Anonymous Reporting. (See Monitoring Anonymous Reporting and Smart Call Home, page 48-9.)

Configuring Smart Call Home

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

- Enabling the Smart Call Home service.
- Configuring the mail server through which Smart Call Home messages are delivered to subscribers.
- Setting up contact information for the Smart Call Home messages.
- Defining alert processing parameters, such as the maximum rate of events that can be handled.
- Setting up alert subscription profiles. 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.

Detailed Steps

To configure the Smart Call Home service, system setup, and alert subscription profiles, perform the following steps.

Step 1 Choose **Configuration > Device Management > Smart Call Home**.

Step 2 Check the **Enable Smart Call Home** check box to enable the feature.

Step 3 Double-click **Advanced System Setup**. This area consists of three panes. Each pane can be expanded or collapsed by double-clicking the title row.

a. In the Mail Servers pane, you can set up mail servers through which Smart Call Home messages are delivered to e-mail subscribers.

b. In the Contact Information pane, you can enter the information of the person to contact for the ASA that appears in Smart Call Home messages. This pane includes the following information:

- The name of the contact person.
- The contact phone number.
- The postal address of the contact person.
- The e-mail address of the contact.
- The “from” e-mail address in Smart Call Home e-mail.
- The “reply-to” e-mail address in Smart Call Home e-mail.
- The customer ID.
- The site ID.
- The contract ID.

c. In the Alert Control pane, you can adjust alert control parameters. This pane includes the Alert group status pane, which lists the status (enabled or disabled) of the following alert groups:

- The diagnostics alert group.
- The configuration alert group.
- The environmental alert group.
- The inventory alert group.
- The snapshot alert group.
- The syslog alert group.
- The telemetry alert group.
- The threat alert group.
- The maximum number of Smart Call Home messages processed per minute.
- The “from” e-mail address in Smart Call Home e-mail.

Step 4 Double-click **Alert Subscription Profiles**. Each named subscription profile identifies subscribers and alert groups of interest.

a. Click **Add** or **Edit** to display the Subscription Profile Editor, in which you can create a new subscription profile or edit an existing subscription profile.

b. Click **Delete** to remove the selected profile.

c. Check the **Active** check box to send a Smart Call Home message of the selected subscription profile to subscribers.

Step 5 When you click **Add** or **Edit**, the Add or Edit Alert Subscription Profile dialog box appears.

a. The Name field is read-only and cannot be edited.

b. Check the **Enable this subscription profile** check box to enable or disable this particular profile.

c. Click either the **HTTP** or **Email** radio button in the Alert Delivery Method area.

d. In the Subscribers field, enter the e-mail address or web address.

e. The Alert Dispatch area lets the administrator specify which type of Smart Call Home information to send to subscribers and under what conditions. There are two types of alerts, time-based and event-based, chosen according to how the alert is triggered. The following alert groups are time-based: Configuration, Inventory, Snapshot, and Telemetry. The following alert groups are event-based: Diagnostic, Environmental, Syslog, and Threat.

f. The Message Parameters area lets you adjust parameters that control messages sent to the subscriber, including the preferred message format and the maximum message size.

Step 6 For time-based alerts, in the Alert Dispatch area, click **Add** or **Edit** to display the Add or Edit Configuration Alert Dispatch Condition dialog box.

a. In the Alert Dispatch Frequency area, specify the frequency in which to send the information to subscribers:

- For a monthly subscription, specify the day of the month, as well as the time of the day to send the information. If they are not specified, the ASA chooses appropriate values for them.
- For a weekly subscription, specify the day of the week, as well as the time of the day to send the information. If they are not specified, the ASA chooses appropriate values for them.
- For a daily subscription, specify the time of the day to send the information. If it is not specified, the ASA chooses an appropriate value for it.
- For an hourly subscription, specify the minute of the hour to send the information. If it is not specified, the ASA chooses an appropriate value for it. Hourly subscriptions are applicable to the snapshot and telemetry alert groups only.

b. Click the **Basic** or **Detailed** radio button to provide the desired level of information to subscribers.

c. Click **OK** to save the configuration.

Step 7 For diagnostic, environment, and threat event-based alerts, in the Alert Dispatch area, click **Add** or **Edit** to display the Create or Edit Diagnostic Alert Dispatch Condition dialog box.

Step 8 Specify the event severity that triggers dispatch of the alert to subscribers in the Event Severity drop-down list, and then click **OK**.

Step 9 For inventory time-based alerts, in the Alert Dispatch area, click **Add** or **Edit** to display the Create or Edit Inventory Alert Dispatch Condition dialog box.

Step 10 Specify how often to dispatch alerts to subscribers in the Alert Dispatch Frequency drop-down list, and then click **OK**.

Step 11 For snapshot time-based alerts, in the Alert Dispatch area, click **Add** or **Edit** to display the Create or Edit Snapshot Alert Dispatch Condition dialog box.

a. In the Alert Dispatch Frequency area, specify the frequency in which to send the information to subscribers:

- For a monthly subscription, specify the day of the month, as well as the time of the day to send the information. If they are not specified, the ASA chooses appropriate values for them.
- For a weekly subscription, specify the day of the week, as well as the time of the day to send the information. If they are not specified, the ASA chooses appropriate values for them.
- For a daily subscription, specify the time of the day to send the information. If it is not specified, the ASA chooses an appropriate value for it.
- For an hourly subscription, specify the minute of the hour to send the information. If it is not specified, the ASA chooses an appropriate value for it. Hourly subscriptions are applicable to the snapshot and telemetry alert groups only.
- For an interval subscription, specify how often, in minutes, the formation is sent to the subscribers. This requirement is applicable to the snapshot alert group only.

b. Click **OK** to save the configuration.

Step 12 For syslog event-based alerts, in the Alert Dispatch area, click **Add** or **Edit** to display the Create or Edit Syslog Alert Dispatch Condition dialog box.

a. Check the **Specify the event severity which triggers the dispatch of alert to subscribers check box**, and choose the event severity from the drop-down list.

b. Check the **Specify the message IDs of syslogs which trigger the dispatch of alert to subscribers** check box.

c. Specify the syslog message IDs that trigger dispatch of the alert to subscribers according to the on-screen instructions.

d. Click **OK** to save the configuration.

Step 13 For telemetry event-based alerts, in the Alert Dispatch area, click **Add** or **Edit** to display the Create or Edit Telemetry Alert Dispatch Condition dialog box.

a. In the Alert Dispatch Frequency area, specify the frequency in which to send the information to subscribers:

- For a monthly subscription, specify the day of the month, as well as the time of the day to send the information. If they are not specified, the ASA chooses appropriate values for them.
- For a weekly subscription, specify the day of the week, as well as the time of the day to send the information. If they are not specified, the ASA chooses appropriate values for them.
- For a daily subscription, specify the time of the day to send the information. If it is not specified, the ASA chooses an appropriate value for it.
- For an hourly subscription, specify the minute of the hour to send the information. If it is not specified, the ASA chooses an appropriate value for it. Hourly subscriptions are applicable to the snapshot and telemetry alert groups only.

b. Click **OK** to save the configuration.

Step 14 To determine if the configured alerts are operating correctly, click **Test**.

Monitoring Anonymous Reporting and Smart Call Home

To monitor the Anonymous Reporting and Smart Call Home features, navigate to the specified path and enter the specified command:

Path	Purpose
Tools > Command Line Interface Enter the **show call- home detail** command, and click **Send**.	Shows the current Smart Call Home detail configuration.
Tools > Command Line Interface Enter the **show call-home mail-server status** command, and click **Send**.	Shows the current mail server status.
Tools > Command Line Interface Enter the **show smart-call- home profile {***profile name* **| all** command, and click **Send**.	Shows the configuration of Smart Call Home profiles.
Tools > Command Line Interface Enter the **show call-home registered-module all** command, and click **Send**.	Shows the registered module status.
Tools > Command Line Interface Enter the **show smart-call statistics** command, and click **Send**.	Shows call-home detail status.
Tools > Command Line Interface Enter the **show call-home** command, and click **Send**.	Shows the current Smart Call Home configuration.
Tools > Command Line Interface Enter the **show running-config call-home** command, and click **Send**.	Shows the current Smart Call Home running configuration.
Tools > Command Line Interface Enter the **show smart-call-home alert-group** command, and click **Send**.	Shows the current status of Smart Call Home alert groups.
Tools > Command Line Interface Enter the **show running-config all** command, and click **Send**.	Shows details about the Anonymous Reporting user profile.

Feature History for Anonymous Reporting and Smart Call Home

Table 48-1 lists each feature change and the platform release in which it was implemented. ASDM is backward-compatible with multiple platform releases, so the specific ASDM release in which support was added is not listed.

Table 48-1 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 the following screen: Configuration > Device Management > Smart Call Home.
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 modified the following screen: Configuration > Device Management > Smart Call Home.
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 master 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