Call Home Installation and Configuration

There are several types of Call Home configurations you can use on a Cisco device. This chapter shows three basic different configurations; the configurations are Call Home configurations to:

- HTTPS
- Email to Smart Call Home
- Email to Transport Gateway and HTTPS to Cisco

The last section of this chapter explains the security considerations for configuring Smart Call Home when not using a Transport Gateway

Call Home Configuration - HTTPS

The following is a sample configuration showing the minimum steps required to configure Call Home on a Cisco device to communicate securely with the Smart Call Home System using HTTPS and a command to start the registration process. All the following commands are displayed in red.

Step 1 **Enable Call Home** – In global configuration mode enter the service call-home command to activate the call-home feature and enter the call-home configuration command to enter call-home configuration mode.

```
Hostname#configure terminal
Hostname(config)#service call-home
```

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

Step 2   **Configure the mandatory contact email address -**

```
Hostname(cfg-call-home)#contact-email-addr username@domain-name
```

Step 3   **Activate the default CiscoTAC-1 Profile and set the transport option to HTTP -**

```
Hostname(cfg-call-home)#profile CiscoTAC-1
Hostname(cfg-call-home-profile)#active
Hostname(cfg-call-home-profile)#destination transport-method http
```

Step 4   **Install a security certificate** – Obtain the Cisco server certificate from the Security Certificate in Chapter 6.

Step 5   **Configure a trust-point and prepare to enroll the certificate via the terminal using copy and paste when prompted**.

```
Hostname(config)#crypto ca trustpoint cisco
Hostname(ca-trustpoint)#enroll terminal
Hostname(ca-trustpoint)#crypto ca authenticate cisco

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
[paste the certificate here and accept it]


% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported
```

Step 6   **Exit and Save the configuration -**

```
Hostname(config-cert-chain)#end
Hostname#copy running-config startup-config
```

Step 7   **Send a Call Home Inventory message to start the registration process -**

```
Hostname#call-home send alert-group inventory
Sending inventory info call-home message ...
Please wait. This may take some time ...
Call-home message is sent.
```

Step 8   **Receive an email from Cisco and follow the link to complete registration for Smart Call home**.

For information about troubleshooting HTTP destination errors see Call Home Configuration - HTTPS.

Call Home Configuration - Email to Smart Call Home

The following is a sample configuration showing the minimum steps required to configure Call Home on a Cisco device to communicate using email with the Smart Call Home System and a command to start the registration process. All the following commands are displayed in red.

Step 1   **Enable Call Home** – In global configuration mode enter the service call-home command to activate the call-home feature and enter the call-home configuration command to enter call-home configuration mode.

```
Hostname#configure terminal
Hostname(config)#service call-home
Hostname(config)#call-home
```

Step 2   **Configure the mandatory contact email address -**

```
Hostname(cfg-call-home)#contact-email-addr username@domain-name
```

Step 3   **Configure the mandatory email server information** – The mail-server address is an IP address or domain-name of a SMTP server that Call Home will send email messages to. If more than one mail-server address is configured for redundancy the mail-server priority is used to determine which server is the active primary server. Call Home will send messages to the active server with the lowest priority number.

```
Hostname(cfg-call-home)#mail-server <address> priority
<server_priority_number>
```

Step 4   **Activate the default CiscoTAC-1 Profile and set the transport option to Email-**

```
Hostname(cfg-call-home)#profile CiscoTAC-1
Hostname(cfg-call-home-profile)#active
Hostname(cfg-call-home-profile)#destination transport-method email
```

Step 5   **Exit and Save the configuration -**

```
Hostname(config-cert-chain)#end
Hostname#copy running-config startup-config
```

Step 6   **Send a Call Home Inventory message to start the registration process -**

```
Hostname#call-home send alert-group inventory
Sending inventory info call-home message ...
Please wait. This may take some time ...
Call-home message is sent.
```

Step 7   **Receive an email from Cisco and follow the link to complete registration for Smart Call home -**

Call Home Configuration - Email to Transport Gateway and HTTPS to Cisco

The following is a sample configuration showing the minimum steps required to configure Call Home on a Cisco device to communicate via a Transport Gateway with the Smart Call Home System using HTTPS and a command to start the registration process. All the following commands are displayed in red.

Step 1   **Enable Call Home** – In global configuration mode enter the service call-home command to activate the call-home feature and enter the call-home configuration command to enter call-home configuration mode.

Hostname#configure terminal

Hostname(config)#service call-home

Hostname(config)#call-home

Step 2   **Configure the mandatory contact email address -**

```
Hostname(cfg-call-home)#contact-email-addr username@domain-name
```

Step 3   **Configure the mandatory email server information** – The mail-server address is an IP address or domain-name of a SMTP server that Call Home will send email messages to.

```
Hostname(cfg-call-home)#mail-server <address> priority
<server_priority_number>
```

Step 4 **De-activate the default CiscoTAC-1 Profile -**

```
Hostname(cfg-call-home)#profile CiscoTAC-1
Hostname(cfg-call-home-profile)#no active
```

Step 5 **Configure a user profile** – The profile's alert-group subscriptions will be similar
to the default CiscoTAC-1 profile with the destination email transport-method
and with a destination email address which is for the email account used by the
Transport Gateway.

```
Hostname(cfg-call-home)#profile Your_profile_name
Hostname(cfg-call-home-profile)#active
Hostname(cfg-call-home-profile)#destination transport-method email
Hostname(cfg-call-home-profile)#destination address email
account_for_TG@yourCompany.com
Hostname(cfg-call-home-profile)#subscribe-to-alert-group diagnostic
severity minor
Hostname(cfg-call-home-profile)#subscribe-to-alert-group environment
severity minor
Hostname(cfg-call-home-profile)#subscribe-to-alert-group syslog
severity major pattern ".*"
Hostname(cfg-call-home-profile)#subscribe-to-alert-group configuration
periodic monthly 23 15:00
Hostname(cfg-call-home-profile)#subscribe-to-alert-group inventory
periodic monthly 23 15:00
```

Step 6 **Exit and Save the configuration -**

```
Hostname(config-cert-chain)#end
Hostname#copy running-config startup-config
```

Step 7 **Download the Transport Gateway, Configure and Register it for Smart Call
Home** – Refer to the Smart Call Home Users' Guide for further information on
configuring the Transport Gateway

Step 8 **Send a Call Home Inventory message to start the registration process -**

```
Hostname#call-home send alert-group inventory
Sending inventory info call-home message ...
Please wait. This may take some time ...
Call-home message is sent.
```

Step 9   **Receive the email from Cisco and follow the link to complete registration for Smart Call home -**

Security Considerations For Call Home Configuration

This section covers the following areas:

- Configuring Call Home When Not Using the Transport Gateway.
- Using AAA on the Cisco Device.

Configuring Call Home When Not Using the Transport Gateway

When not using the Transport Gateway follow the instructions listed below:

- The Cisco device regardless of the protocol (HTTP/SMTP/HTTPS), always scrubs sensitive information such as passwords and SNMP Community strings in the configuration before sending it over the wire.

- SMTP is not a secure protocol and hence is not the recommended method for sending Smart Call Home messages to the back-end server. The preferred mechanism is HTTPS, which is the default.

- The certificate of the Certification Authority must be installed on the Cisco device, before HTTPS communication with the back-end server can occur.

Note   The Cisco server certificate used by Smart Call home needs to be installed on your Cisco device, even if you are already using HTTPS and have a server certificate installed; you need to install the server certificate for Smart Call Home. The Security Certificate is available at the end of this User Guide. All the following commands are displayed in red.

The Security Certificate is installed using the crypto ca authenticate command. The sequence of commands used to install the CA certificate on the Cisco device is given below.

```
Hostname(config)#crypto ca trustpoint cisco
Hostname(ca-trustpoint)#enroll terminal
Hostname(ca-trustpoint)#crypto ca authenticate cisco
```

Note   Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
[paste the certificate here and accept it

```
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported
```

- Depending on the configuration deployed by the customer, the protocols and
  ports defined in Table 1 need to be allowed on the firewall between the stated
  source and destination. In a typical configuration where the Cisco devices are
  installed on the internal network, this communication will be seamless
  without a need for a configuration change on the firewall as the traffic will
  flow from the Cisco device on the high-security internal network zone to the
  Internet on the low-security zone.

Table 2-1   **Protocols and Ports without the Transport Gateway**

Source	Destination	Proto-col	Port	Purpose
Cisco Device	Cisco's back-end server	HTTPS	443	Device to send SCH messages to the back-end server – Option 1
Cisco Device	Customer's email server en route to Cisco's back-end server	SMTP	25	Device to send SCH messages to the back-end server – Option 2
Cisco Device	Customer's Local web server for Customer to process and initiate action	HTTP	80	Device to send SCH messages to the customer server

Using AAA on the Cisco Device

If AAA is configured on the Cisco device then a user account with username = callhome must be configured on the AAA server. The password options for the account may be defined by the server administrator.

The following list contains all the currently supported authorization commands:

config message:

- show module
- show version
- show install running (ION only)
- show running-config all
- show startup-config
- remote command switch show version

diagnostic message:

- show module
- show diagnostic result module x detail
- show version
- show install running (ION only)
- show inventory
- show buffers
- show logging
- show diagnostic result module all
- remote command switch show version
- show logging system last 100

environment message:

- show module
- show environment

- show logging
- show power

inventory message:

- show module
- show version
- show install running (ION only)
- show inventory
- show idprom all
- remote command switch show version
- show diagbus

syslog message:

- show logging

test message:

- show module
- show version
- show install running (ION only)
- remote command switch show version

Security Considerations For Call Home Configuration