



CHAPTER 2

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.](#)
- [Message Types & CLI Content Per Platform.](#)
- [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.

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 2-1 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	Protocol	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

Message Types & CLI Content Per Platform

This section provides information on the message types that are sent by the Call-home feature.

Table 2-2

D = NX-7000 Switch	O = NX-5000 Switch	M = MDS 9000 (4.x)
R = Cisco7600 Router	S = Standalone Catalyst 6500	V = Catalyst 6500 VSS

Table 2-3 shows the CLI data sent with call-home messages by type and by the platform supported .



Note RMON alerts from an MDS 9000 are sent in diagnostic messages which do not contain any CLI.

Table 2-3

CLI COMMAND	CFG	ENV	DIAG	INV	SYS LOG	TEST
remote command switch show version	R S V		R S V	R S V		R S V
show buffers			R S V			
show diagbus				R S V		
show diagnostic result module all			D O R S			
show diagnostic result module x detail			D R S			
show diagnostic result switch all			V			
show diagnostic result switch x module x detail			V			
show environment		DMORSV		O		

Table 2-3

CLI COMMAND	CFG	ENV	DIAG	INV	SYS LOG	TEST
show hardware			D M	D M		
show idprom all				R S		
show idprom switch all				V		
show install running (ION only)	S V		S V	S V		S V
show interface transceiver				O	O	O
show inventory	RSV	RSV	RSV	DMORSV	ORSV	ORSV
show license usage				DMO	DMO	O
show logging		DRSV	RSV		DRSV	
show logging last 1000		O				
show logging logfile tail -n 200		M			M	
show logging system last 100			RSV			
show module	DMORS	DMORS	DMORS	DMORS	O	DMORS
show module switch all	V	V	V	V		V
show power		RS				
show power switch all		V				
show running-config	M					
show running-config all	ORSV					
show running-config vdc-all all	D					
show snmp user		M			M	
show sprom all			DM	DMO	O	O
show startup-config	MORSV					
show startup-config vdc-all	D					
show switch virtual	V		V	V		
show system uptime				DMO	O	O
show tech-support ethpm			D			
show tech-support GOLD			D			

Table 2-3

CLI COMMAND	CFG	ENV	DIAG	INV	SYS LOG	TEST
show tech-support platform			DM			
show tech-support platform callhome		O	O			
show tech-support sysmgr			DM			
show vdc current-vdc	D	D	D	D	D	D
show vdc membership	D	D	D	D	D	D
show version	DMORSV	DMO	DMORSV	DMORSV	O	DMORSV
show module		S	S	S		S
show module switch all	V	V	V	V		V
show running-config all	SV	SV	SV	SV		SV
show tech					SV	
show version	SV	SV	SV	SV		SV

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 commands listed in [Table 2-3](#) need to be authorized on the Call Home device so that the Call Home service can be authorized to issue these commands. Authorize only those commands that are appropriate for the type device in your network.