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 Device Diagnostics
- Email to Transport Gateway and HTTPS to Cisco

The last section of this chapter explains the security considerations for configuring Device Diagnostics when not using a Transport Gateway

Warning **It is very important that you setup your NOC and Admin contact email addresses and associate them to the bill-to-id in your CCO profile, before performing your configurations. These email addresses are very important because they are used by the application to notify you of failures and administrative events on the devices that are under your services contracts. Failure to do this can result in important device events occurring that you cannot be contacted for, since no valid email contact information is available. To set up these email addresses on the smart portal, click Reports on the smart portal overview page; on the Reports portal click the Device Diagnostics primary tab, then the Registered Devices secondary tab, then click the Email Setup button. The Email Setup pod lets you specify the NOC and Admin contact email addresses.**

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 Device Diagnostics 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 CA Root Certificate Update Process in Chapter 6.

Note There are two different types of certificate processes, depending on if you are setting up a Nexus 7000 device, or a non-Nexus 7000 type device.

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

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

Note Be aware that the certificate starts AFTER the "---Begin" line and ends BEFORE the "---end---" line

```
% 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 Device Diagnostics.

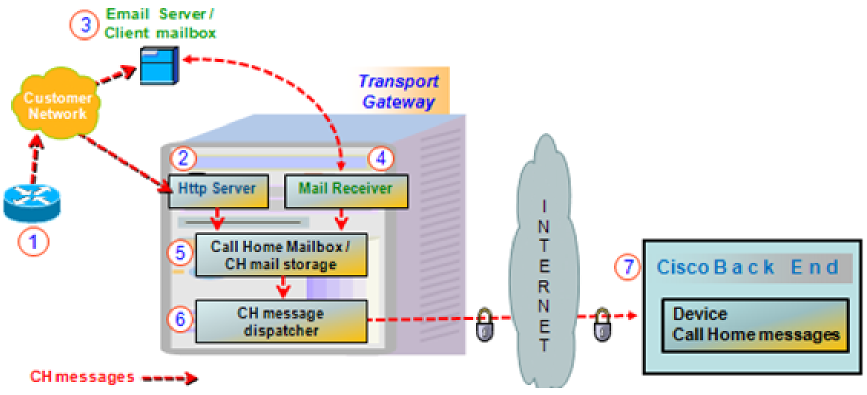
For information about troubleshooting HTTP destination errors see Call Home Configuration - HTTPS.

Transmission of Call Home Messages Using a Transport Gateway

Two methods may be utilized to send messages to a Transport Gateway. One method is for the call-home message sender to utilize the HTTP server option on the Transport Gateway. The second method is for the call-home message sender to send email to an email account that would be read by the built-in email client ④ on the Transport Gateway.

Note All IOS versions and Nexus OS versions starting from 4.1(3) for the MDS 9000 and Nexus 7000 products support the HTTP transport option. SAN-OS and Nexus OS for the Nexus 5000 products only support the email option.

The following diagram illustrates the two methods for sending call-home messages to a Transport Gateway.



Step 1 The partner device ① sends Call Home messages to either the http server ② or to the Email server ③ that the partner has set up as an email client account.

Step 2 If sent to an email account, the Transport Gateway requests the email from the email server ③ and receives the messages. ④

Step 3 All Call Home messages, whether sent using the http or email, are temporarily stored in a message storage location, also referred to as the Call Home mail storage area. ⑤ The messages stay in Call Home mail storage until they are sent either manually or automatically.

Step 4 Call Home messages are sent through the CH message dispatcher ⑥ securely over the internet to the Cisco Back End. ⑦

Note During Transport Gateway configuration if the Send Call Home messages check box is checked, then messages are sent automatically to the Cisco Backend; otherwise the messages are kept in the Call Home mail storage until manually sent.

During Transport Gateway configuration you can also specify the size of the Call Home mail storage (mail store) area.The size indicates when the mail storage is getting full and an email notification is sent.

The Call Home messages are sent securely across the internet to the Cisco Back End, where they are processed further.

Call Home Configuration - Call Home Messages to Transport Gateway / 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 Device Diagnostics 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 Device Diagnostics** – Refer to the Device Diagnostics Users' Guide for Partners 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 Device Diagnostics.

Call Home Configuration - Email to Device Diagnostics

If the device has not yet been registered via bulk registration, follow the link and instructions in email received from Cisco to complete the device registration.

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 Device Diagnostics 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 Device Diagnostics -

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 Device Diagnostics 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 Device Diagnostics 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 Device Diagnostics. The Security Certificate is available at the end of this User Guide.

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

```
Hostname(config)#crypto pki trustpoint cisco
Hostname(ca-trustpoint)#enroll terminal
Hostname(ca-trustpoint)#crypto pki 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 partner, 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	End customer's email server or local web server.	SMTP	25	Device to send SCH messages to the back-end server – Option 2
Cisco Device	Partner’s Local web server for Partner to process and initiate action	HTTP	80	Device to send SCH messages to the partner 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		DMORS V		O		
show hardware			D M	D M		
show idprom all				R S		
show idprom switch all				V		

Table 2-3

CLI COMMAND	CFG	ENV	DIAG	INV	SYS LOG	TEST
show install running (ION only)	S V		S V	S V		S V
show interface transceiver				O	O	O
show inventory	RSV	RSV	RSV	DMORS V	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			
show tech-support platform			DM			
show tech-support platform callhome		O	O			

Table 2-3

CLI COMMAND	CFG	ENV	DIAG	INV	SYS LOG	TEST
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	DMORS V	DMO	DMORS V	DMORS V	O	DMORS V
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.