Configuring the Cisco VG410 Voice Gateway

This chapter describes how to use the Cisco IOS software CLI to configure basic analog functionalities. Follow the procedures in this chapter to configure Cisco VG410 Voice Gateway, or if you want to change the configuration after you have run the setup command facility.

This chapter does not describe every configuration possible—only a small portion of the most commonly used configuration procedures. For advanced configuration topics, refer to the respective technology configuration guides.

One of the first configuration tasks you might want to do is to configure the host name and set an encrypted password. Configuring a host name allows you to distinguish a router from another. Setting an encrypted password allows you to prevent unauthorized configuration changes. Read on to know how to perform these configurations.

Configuring the Host Name and Password

Procedure

	Command or Action	Purpose

Step 1	**Device> enable**
	Example:
	`Password: password`
	Example:
	`Device#`
		Enables privileged EXEC mode. Enter your password, if prompted.

Step 2	**configure terminal** **Example:** `Device(config)#`	Enters global configuration mode. Enter configuration commands, one per line. End with CNTL/Z.

	Command or Action	Purpose
Step 3	**hostname vg410** **Example:** `Device(config)# hostname vg410`	Changes the name of Cisco VG410 Voice Gateway to a meaningful name. Substitutes the host name to Device.
Step 4	**enable secret <password>** **Example:** `vg410(config)# enable secret guessme`	Enters an enable secret password. This password provides access to privileged EXEC mode. When you enter enable at the user EXEC prompt, you must enter the enable secret password to gain access to configuration mode. Enter the secret password, for example, guessme.
Step 5	**line con 0** **Example:** `vg410(config)# line con 0`	Enters line configuration mode to configure the console port.
Step 6	**exec-timeout 0 0** **Example:** `vg410(config-line)# exec-timeout 0 0`	Prevents Cisco VG410 Voice Gateway EXEC mode from timing out when you do not enter any information on the console screen for an extended period.
Step 7	**exit** **Example:** `vg410(config-line)# exit`	Exits config-line mode and enters global configuration mode.

Verifying the Host Name and Password

To verify that you configured the correct host name and password, perform the following steps:

Step 1 Run the **show config** command.

Example:

```
vg410# show config
Using 2745 out of 262136 bytes
!
version 17.12
.
.
.
!
hostname vg410
!
enable secret 5 $1$60L4$X2JYOwoDc0.kqa1loO/w8/
.
.
.
```

Check the host name and the encrypted password displayed near the top of the command output.

Step 2 Run the **exit** command to exit global configuration mode and re-enter it using the new enable password:

Example:

```
vg410# exit
.
.
.vg410 con0 is now available
Press RETURN to get started.

vg410> enable
Password: guessme
vg410#
```

If you face any issues, check whether:

- The caps lock is off.
- You entered the correct password. Passwords are case sensitive.

TLS 1.2 support on SCCP Gateways

This chapter provides details on TLS 1.2 support for SCCP Gateways.

Note Cisco Unified Communications Manager (CUCM) Version 15 and later has been enhanced to support Secured SCCP gateways with the Subject Name field (CN Name) with or without colons, for example, AA:22:BB:44:55 or AA22BB4455.

CUCM checks the CN field of the incoming certificate from the SCCP Gateway and verifies it against the DeviceName configured in CUCM for this gateway. DeviceName contains MAC address of the gateway. CUCM converts the MAC address in the DeviceName to MAC address with colons (for example: AA:22:BB:44:55) and validates with the CN name in the Gateway's certificate. Therefore, CUCM mandates Gateway to use MAC address with colons for the CN field in the certificate, that is, subject name.

Due to new guidelines from Defense Information Systems Agency (DISA), it is a requirement not to use colons for the subject name field CN. For example, AA22BB4455.

SCCP TLS connection

CiscoSSL is based on OpenSSL. SCCP uses CiscoSSL to secure the communication signals.

If a resource is configured in the secure mode, the SCCP application initiates a process to complete Transport Layer Security (TLS) handshaking. During the handshake, the server sends information to CiscoSSL about the TLS version and cipher suites supported. Previously, only SSL3.1 was supported for SCCP secure signalling. SSL3.1 is equivalent to TLS 1.0. The TLS 1.2 Support feature introduces TLS1.2 support to SCCP secure signalling.

After the TLS handshake is complete, SCCP is notified and SCCP ends the process.

If the handshake is completed successfully, a REGISTER message is sent to CUCM through the secure tunnel. If the handshake fails and a retry is needed, a new process is initiated.

Cipher Suites

For SCCP-based signaling, TLS_RSA_WITH_AES_128_CBC_SHA cipher suite is supported. Additionally, the following NGE cipher suites are also supported:

- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES256-GCM-SHA384

These cipher suites enable secure voice signaling for STCAPP analog phone conferencing service. The cipher suite selection is negotiated between GW and CUCM.

The following prerequisites are applicable for using NGE cipher suites:

- Configure TLS 1.2. For more information, see *Configuring TLS*.
- Use CUCM Release 15 or later, and Voice Gateways or platforms that support TLS 1.2.
- From CUCM Web UI, navigate to Cipher Management and set the CIPHER switch as NGE. For more information, Cipher Management.

For more information about verifying these cipher suites, see *Verifying TLS version and Cipher Suites*.

For the SRTP encrypted media, you can use higher-grade cipher suites: AEAD-AES-128-GCM or AEAD-AES-256-GCM. Legacy suites AES_CM_128_HMAC_SHA1_80 and AES_CM_128_HMAC_SHA1_32 are also supported. The cipher suites selection is automatically negotiated between GW and CUCM for both secure analog voice and hardware conference bridge voice media. Authenticated Encryption with Associated Data (AEAD) ciphers simultaneously provide confidentiality, integrity, and authenticity, without built-in SHA algorithms to validate message integrity.

Configuring TLS version for STC application

Perform the following task to configure a TLS version for the STC application:

```
enable
configure terminal
stcapp security tls-version v1.2
exit
```

Note The **stcapp security tls** command sets the TLS version to v.1.0, v1.1, or v1.2 only. If not configured explicitly, TLS v1.0 is selected by default.

Verifying STCAPP Application TLS version

Perform the following tasks to verify TLS version of the STCAPP application:

```
vg410# show call application voice stcapp
App Status: Active
CCM Status: UP
CCM Group: 120
Registration Mode: CCM
Total Devices: 0
Total Calls in Progress: 0
Total Call Legs in Use: 0
ROH Timeout: 45
TLS Version: v1.2
```

```
vg410# show stcapp dev voice 0/1/0
Port Identifier:  0/1/0
Device Type:      ALG
Device Id:        585
Device Name:      ANB3176C85F0080
Device Security Mode : Encrypted
  TLS version        : TLS version 1.2
  TLS cipher         : ECDHE-RSA-AES256-GCM-SHA384
Modem Capability: None
Device State:     IS
Diagnostic:       None
Directory Number: 80010
Dial Peer(s):     100
Dialtone after remote onhook feature: activated
Busytone after remote onhook feature: not activated
Last Event:       STCAPP_CC_EV_CALL_MODIFY_DONE
Line State:       ACTIVE
Line Mode:        CALL_CONF
Hook State:       OFFHOOK
mwi:              DISABLE
vmwi:             OFF
mwi config:       Both
Privacy:          Not configured
HG Status:        Unknown
PLAR:             DISABLE
Callback State:   DISABLED
CWT Repetition Interval: 0 second(s) (no repetition)
Number of CCBs:   1
Global call info:
    Total CCB count      = 3
    Total call leg count = 6

Call State for Connection 2 (ACTIVE): TsConnected
Connected Call Info:
   Call Reference: 33535871
   Call ID (DSP):  187
   Local IP Addr:  172.19.155.8
   Local IP Port:  8234
   Remote IP Addr: 172.19.155.61
   Remote IP Port: 8154
   Calling Number: 80010
   Called Number:
   Codec:          g711ulaw
   SRTP:           on
   RX Cipher:      AEAD_AES_256_GCM
   TX Cipher:      AEAD_AES_256_GCM
```

Verifying Call Information

To display call information for TDM and IVR calls stored in the Forwarding Plane Interface (FPI), run the **show voip fpi calls** command. You can select a call ID and verify the cipher suite using the **show voip fpi calls confID** *call_id_number* command . In this example, cipher suite 6 is AES_256_GCM.

```
#show voip fpi calls
Number of Calls : 2
---------- ---------- ---------- ---------- --------------- ---------------
    confID correlator    AcallID     BcallID           state           event
---------- ---------- ---------- ---------- --------------- ---------------
         1          1         87         88       ALLOCATED DETAIL_STAT_RSP
        21         21         89         90       ALLOCATED DETAIL_STAT_RSP

#show voip fpi calls confID 1
--------------------------------------------------------------------------------
```

```
VoIP-FPI call entry details:
------------------------------------------------------------------------------
Call Type        :           TDM_IP     confID          :                1
correlator       :                1     call_state      :         ALLOCATED
last_event       :  DETAIL_STAT_RSP     alloc_start_time :       1796860810
modify_start_time:                0     delete_start_time:                0
Media Type(SideA):             SRTP     cipher suite    :                6
------------------------------------------------------------------------------
FPI State Machine Stats:
------------------------
create_req_call_entry_inserted              :         1
……
```