Configuring the Cisco VG420 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 the Cisco VG420 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.

Configuring Host Name and Password

Procedure

	Command or Action	Purpose

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

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

	Command or Action	Purpose
Step 3	Router(config)# hostname 420	Changes the name of the Cisco VG420 Voice Gateway to a meaningful name. Substitutes the host name to Router.
Step 4	Router(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 (Router>), you must enter the enable secret password to gain access to configuration mode. Substitute your enable secret password for guessme.
Step 5	Router(config)# line con 0	Enters line configuration mode to configure the console port.
Step 6	Router(config-line)# exec-timeout 0 0	Prevents the Cisco VG420 Voice Gateway, EXEC mode from timing out when you do not enter any information on the console screen for an extended period.
Step 7	Router(config-line)# exit	Exits from the config-line mode and enters into the 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 Enter the **show config** command.

Example:

```
Router# show config
Using 2745 out of 262136 bytes
!
version XX.X
.
.
.
!
hostname 420
!
enable secret 5 $1$60L4$X2JYOwoDc0.kqa1loO/w8/
.
.
.
```

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

Step 2 Exit the Global Configuration mode and attempt to re-enter it using the new enable password:

Example:

```
Router# exit
.
.
.
Router con0 is now available
```

```
Press RETURN
 to get started.
Router> enable
Password: guessme
Router#
```

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

The TLS 1.2 support on SCCP Gateways feature details the configuration of TLS 1.2 on SCCP protocol for digital signal processor (DSP) farm including Unicast conference bridge

(CFB), Media Termination Point (MTP), and SCCP telephony control (STC) application (STCAPP).

DSP on gateways can be used as media resources for transrating or transcoding. Each media resource uses Secure Skinny Client Control Protocol (SCCP) to communicate with Cisco Unified Communications Manager. Currently SSL 3.1, which is equivalent to TLS1.0, is used for sending secure signals. This feature enhances the support to TLS 1.2. From Cisco IOS XE Cupertino 17.7.1a, TLS 1.2 is enhanced to support the Next-Generation Encryption (NGE) cipher suites.

Note Cisco Unified Communications Manager (CUCM) Version 14SU2 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 TLS handshaking is complete, SCCP is notified and SCCP kills the process.

If the handshaking is completed successfully, a REGISTER message is sent to Cisco Unified Communications Manager through the secure tunnel. If handshaking fails and a retry is needed, a new process is initiated.

Note For SCCP-based signalling, only TLS_RSA_WITH_AES_128_CBC_SHA cipher suite is supported.

Cipher Suites

For SCCP-based signaling, TLS_RSA_WITH_AES_128_CBC_SHA cipher suite is supported.

From Cisco IOS XE Cupertino 17.7.1a, 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 both STCAPP analog phone and SCCP DSPFarm 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 the CUCM Release 14.1 SU1 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. These 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.

Supported Platforms

The TLS 1.2 support on SCCP Gateways feature is supported on the following platforms:

- Cisco VG400, VG420, and VG450 Analog Voice Gateways

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.

Configuring TLS version in Secure Mode for DSP Farm Profile

Perform the following task to configure the TLS version in secure mode for DSP farm profile:

```
enable
configure terminal
dspfarm profile 7 conference security
  tls-version v1.2
  exit
```

Note Note: The **tls** command can be configured only in security mode.

Verifying TLS version and Cipher Suites

Perform the following task to verify the TLS version and cipher suite:

```
# show dspfarm profile 100
Dspfarm Profile Configuration

 Profile ID = 100, Service = CONFERENCING, Resource ID = 2
 Profile Service Mode : secure
 Trustpoint : Overlord_DSPFarm_GW
 TLS Version  : v1.2
 TLS Cipher   : ECDHE-RSA-AES256-GCM-SHA384
 Profile Admin State : UP
 Profile Operation State : ACTIVE
 Application : SCCP   Status : ASSOCIATED
 Resource Provider : FLEX_DSPRM   Status : UP
 Total Number of Resources Configured : 10
 Total Number of Resources Available : 10
 Total Number of Resources Out of Service : 0
 Total Number of Resources Active : 0
 Maximum conference participants : 8
 Codec Configuration: num_of_codecs:6
 Codec : g711ulaw, Maximum Packetization Period : 30 , Transcoder: Not Required
 Codec : g711alaw, Maximum Packetization Period : 30 , Transcoder: Not Required
 Codec : g729ar8, Maximum Packetization Period : 60 , Transcoder: Not Required
 Codec : g729abr8, Maximum Packetization Period : 60 , Transcoder: Not Required
 Codec : g729r8, Maximum Packetization Period : 60 , Transcoder: Not Required
 Codec : g729br8, Maximum Packetization Period : 60 , Transcoder: Not Required
```

Verifying STCAPP Application TLS version

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

```
Device# 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

# 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
```

Perform the following task to verify the sRTP cipher suite for the DSPfarm connection.

```
# show sccp connection detail

bridge-info(bid, cid) - Normal bridge information(Bridge id, Calleg id)
mmbridge-info(bid, cid) - Mixed mode bridge information(Bridge id, Calleg id)

sess_id    conn_id    call-id    codec   pkt-period dtmf_method    type
bridge-info(bid, cid)   mmbridge-info(bid, cid) srtp_cryptosuite          dscp
                        call_ref   spid       conn_id_tx

16778224   -          125        N/A     N/A        rfc2833_pthru     confmsp   All RTPSPI
 Callegs      All MM-MSP Callegs      N/A                        N/A
                        -          -          -

16778224   16777232   126        g711u   20         rfc2833_pthru  s- rtpspi    (101,125)
               N/A                       AEAD_AES_256_GCM          184
                        30751576   16777219   -

16778224   16777231   124        g711u   20         rfc2833_pthru  s- rtpspi    (100,125)
               N/A                       AEAD_AES_256_GCM          184
                        30751576   16777219   -
```

```
Total number of active session(s) 1, connection(s) 2, and callegs 3
```

Verifying Call Information

To display call information for TDM and IVR calls stored in the Forwarding Plane Interface (FPI), use the **showvoipfpi calls** command. You can select a call ID and verify the cipher suite using the command **show voip fpi calls confID** *call_id_number*. 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
.........
```

Table 1: Feature Information for TLS 1.2 support on SCCP Gateways

Feature Name	Releases	Feature Information
Support for NGE Cipher Suites	Cisco IOS XE Cupertino 17.7.1a	This feature supports NGE cipher suites for secure voice signaling and secure media. These cipher suites are applicable for both STCAPP analog phone and SCCP DSPFarm conferencing service.