Configuring Secure Signaling and Media Encryption for the Cisco VG224

Last Updated: March 19, 2010

This chapter describes the Secure Signaling and Media Encryption for a analog phones that are connected to Foreign Exchange Station (FXS) ports on a Cisco VG224 Analog Phone Gateway and controlled by Cisco Unified Communications Manager Express (Cisco Unified CME).

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this chapter. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the "Feature Information for Secure Signaling and Media Encryption for the Cisco VG224" section on page 212.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Contents

Prerequisites for Secure Signaling and Media Encryption for the Cisco VG224

Cisco IOS Gateway

- Cisco IOS Release 12.4(11)XW or a later release.
- Set the system clock by using one of the following methods. For configuration information, see the "Performing Basic System Management" chapter of the *Cisco IOS Network Management Configuration Guide* for your Cisco IOS release.
  - Configure Network Time Protocol (NTP).
  - Manually set the software clock by using the **clock set** command. On Cisco integrated services routers, use the **clock set** and **clock update-calendar** commands.

Analog Endpoints in Cisco Unified CME

- Cisco Unified CME 4.2 or a later version.

Restrictions for Secure Signaling and Media Encryption for the Cisco VG224

- This feature is not supported for analog SCCP endpoints in Cisco Unified Communications Manager.

Information About Secure Signaling and Media Encryption for the Cisco VG224

To enable Secure Signaling and Media Encryption for the Cisco VG224, you should understand the following concept:

- Media Encryption (SRTP), page 194

Media Encryption (SRTP)

Media Encryption (SRTP) and companion voice security Cisco IOS features in Cisco Unified CME 4.2 and later versions provide secure voice call capabilities including secure analog endpoints connected to Cisco VG224 Analog Phone Gateway endpoints.

The Media Encryption (SRTP) on Cisco Unified CME feature supports the following features:

- Secure voice calls using SRTP for SCCP endpoints
- Secure voice calls in a mixed shared line environment that allows both RTP and SRTP capable endpoints; shared line media security depends on the endpoint configuration.
- Secure supplementary services using H.450 including:
  - Call forward
  - Call transfer

- Call hold and resume
- Call park and call pickup
- Nonsecure software conferenc

Note SRTP conference calls over H.323 may experience a 0 to 2 second noise interval when the call is joined to the conference.

- Secure calls in a nonH.450 environment
- Secure Cisco Unified CME interaction with secure Cisco Unity
- Secure Cisco Unified CME interaction with Cisco Unity Express (interaction is supported and calls are downgraded to nonsecure mode)
- Secure transcoding for remote phones with DSP farm transcoding configured.

For information about these features in Cisco Unified CME, see the "Configuring Security" module of the *Cisco Unified CME System Administration Guide*.

To configure SRTP for a Cisco VG224 Analog Phone Gateway, see the "How to Configure Secure Signaling and Media Encryption for the Cisco VG224" section on page 195.

How to Configure Secure Signaling and Media Encryption for the Cisco VG224

Media Encryption (SRTP) on Cisco Unified CME provides secure voice call capabilities including secure Cisco VG224 Analog Phone Gateway endpoints.

Note For information about this feature in Cisco Unified CME, see the "Configuring Security" module in the *Cisco Unified CME System Administration Guide*.

To add a Cisco VG224 Analog Phone Gateway to a secure Cisco Unified CME system, perform the following tasks:

- Configuring an External CA Server, page 195 (required)
- Creating a Trustpoint on the VG224, page 198 (required)
- Configuring STCAPP, Trustpoint, and Security, page 201 (required)
- Verifying and Troubleshooting Secure Signaling and Media Encryption on the Cisco VG224, page 203 (optional)

Configuring an External CA Server

To configure an external certificate authority (CA) server, perform the following steps:

SUMMARY STEPS

1. **enable**
2. **configure terminal**

3. **crypto pki server** *cs-label*
4. **database level {minimal | names | complete}**
5. **grant auto**
6. **database url** *root-url*
7. **no shutdown**
8. **exit**
9. **crypto pki trustpoint** *label*
10. **revocation-check** *method1* [*method2*[*method3*]]
11. **rsakeypair** *key-label* [*key-size* [*encryption-key-size*]]
12. **exit**
13. **ip http server**
14. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**crypto pki server** *cs-label* **Example:** `Router(config)# crypto pki server cserver1`	Defines a label for the certificate server and enters certificate server configuration mode. • *cs-label*—Name for CA certificate server.
Step 4	**database level** {**minimal** | **names** | **complete**} **Example:** `Router(cs-server)# database level complete`	(Optional) Controls the type of data stored in the certificate enrollment database. • **minimal**—Enough information is stored only to continue issuing new certificates without conflict. This is the default functionality. • **names**—The serial number and subject name of each certificate are stored in the database, providing enough information for the administrator to find and revoke a particular certificate, if necessary. • **complete**—In addition to the information given in the minimal and names levels, each issued certificate is written to the database. **Note** The **complete** keyword produces a large amount of information; so specify an external TFTP server in which to store the data using of the **database url** command.

	Command or Action	Purpose
Step 5	**grant auto** **Example:** `Router(cs-server)# grant auto`	(Optional) Allows an automatic certificate to be issued to any requester. The recommended method and default if this command is not used is manual enrollment. **Tip** Use this command only during enrollment when testing and building simple networks. A security best practice is to disable this functionality using the **no grant auto** command after configuration so that certificates cannot be continually granted.
Step 6	**database url** *root-url* **Example:** `Router(cs-server)# database url nvram:`	(Optional) Specifies the location where all database entries for the certificate server are to be written out. If this command is not specified, all database entries are written to NVRAM. • *root-url*—Location where database entries will be written out. The URL can be any URL that is supported by the Cisco IOS file system. • If the CA is going to issue a large number of certificates, select an appropriate storage location like flash or other storage device to store the certificates. **Note** When the storage location chosen is flash and the file system type on this device is Class B (LEFS), make sure to check free space on the device periodically and use the **squeeze** command to free the space used up by deleted files. This process may take several minutes and should be done during scheduled maintenance periods or off-peak hours.
Step 7	**no shutdown** **Example:** `Router(cs-server)# no shutdown`	(Optional) Enables the CA. • You should use this command only after you have completely configured the CA. • Enter your password when prompted.
Step 8	**exit** **Example:** `Router(cs-server)# exit`	Exits certificate server configuration mode.
Step 9	**crypto pki trustpoint** *label* **Example:** `Router(config)# crypto pki trustpoint cserver1`	(Optional) Declares a trustpoint and enters CA-trustpoint configuration mode. • Use this command and the **enrollment url** command if this CA is local to the Cisco Unified CME router. These commands are not needed for a CA running on an external router. • *label*—Name for the trustpoint. The *label* in this step should be the same as the *cs-label* in Step 3.

	Command or Action	Purpose
Step 10	**revocation-check** *method1* [*method2*[*method3*]] **Example:** `Router(ca-trustpoint)# revocation-check crl`	(Optional) Checks the revocation status of a certificate and specifies one or more methods to check the status. If a second and third method are specified, each method is used only if the previous method returns an error, such as a server being down. Valid values for the *method* argument are as follows: • **crl**—Certificate checking is performed by a certificate revocation list (CRL). This is the default behavior. • **none**—Certificate checking is not required. • **ocsp**—Certificate checking is performed by an Online Certificate Status Protocol (OCSP) server.
Step 11	**rsakeypair** *key-label* [*key-size* [*encryption-key-size*]] **Example:** `Router(ca-trustpoint)# rsakeypair exampleCAkeys 1024 1024`	(Optional) Specifies an RSA key pair to use with a certificate. • *key-label*—Name of the key pair, which is generated during enrollment if it does not already exist or if the **auto-enroll regenerate** command is used. • *key-size*—(Optional) Size of the desired RSA key. If not specified, the existing key size is used. • *encryption-key-size*—(Optional) Size of the second key, which is used to request separate encryption, signature keys, and certificates. **Note** Multiple trustpoints can share the same key.
Step 12	**exit** **Example:** `Router(ca-trustpoint)# exit`	Exits CA-trustpoint configuration mode.
Step 13	**ip http server** **Example:** `Router(config)# ip http server`	Enables the Cisco web-browser user interface on the local Cisco Unified CME router.
Step 14	**exit** **Example:** `Router (config)# exit`	Exits global configuration mode.

Creating a Trustpoint on the VG224

To create a trustpoint on the Cisco VG224, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**

3. **crypto key generate rsa general-keys label** *key-label*
4. **crypto pki trustpoint** *label*
5. **enrollment url** *ca-url*
6. **serial-number none**
7. **fqdn none**
8. **ip-address none**
9. **subject-name** [*x.500-name*]
10. **revocation-check none**
11. **rsakeypair** *key-label* [*key-size* [*encryption-key-size*]]
12. **exit**
13. **crypto pki authenticate** *trustpoint-label*
14. **crypto pki enroll** *trustpoint-label*
15. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**crypto key generate rsa general-keys label** *key-label* **Example:** `Router(config)# crypto key generate rsa general-keys label VG224`	(Optional) Generates Rivest, Shamir, and Adelman (RSA) key pairs. • **general-keys**—Specifies that the general-purpose key pair should be generated. • **label** *key-label*—(Optional) Name that is used for an RSA key pair when they are being exported.
Step 4	**crypto pki trustpoint** *label* **Example:** `Router(config)# crypto pki trustpoint VG224`	Declares the trustpoint that your RA mode certificate server should use and enters CA-trustpoint configuration mode. • *label*—Name for the trustpoint and RA.
Step 5	**enrollment url** *ca-url* **Example:** `Router(ca-trustpoint)# enrollment url http://10.3.105.40:80`	Specifies the enrollment URL of the issuing CA certificate server (root certificate server). • *ca-url*—URL of the router on which the root CA has been installed.

	Command or Action	Purpose
Step 6	**serial-number none** **Example:** `Router(ca-trustpoint)# serial-number none`	Specifies whether the router serial number should be included in the certificate request. • **none**—Specifies that a serial number will not be included in the certificate request.
Step 7	**fqdn none** **Example:** `Router(ca-trustpoint)# fqdn none`	Specifies a fully qualified domain name (FQDN) that will be included as "unstructuredName" in the certificate request. • **none**—Router FQDN will not be included in the certificate request.
Step 8	**ip-address none** **Example:** `Router(ca-trustpoint)# ip-address none`	Specifies a dotted IP address or an interface that will be included as "unstructuredAddress" in the certificate request. • **none**—Specifies that an IP address is not to be included in the certificate request.
Step 9	**subject-name** [*x.500-name*] **Example:** `Router(ca-trustpoint)# subject-name cn=VG224, ou=ABU, o=Cisco Systems Inc.`	Specifies the subject name in the certificate request. **Note** The example shows how to format the certificate subject name to be similar to that of an IP phone's.
Step 10	**revocation-check none** **Example:** `Router(ca-trustpoint)# revocation-check none`	(Optional) Checks the revocation status of a certificate and specifies one or more methods to check the status. If a second and third method are specified, each method is used only if the previous method returns an error, such as a server being down. • **none**—Certificate checking is not required.
Step 11	**rsakeypair** *key-label* [*key-size* [*encryption-key-size*]] **Example:** `Router(ca-trustpoint)# rsakeypair VG224`	(Optional) Specifies an RSA key pair to use with a certificate. • *key-label*—Name of the key pair, which is generated during enrollment if it does not already exist or if the **auto-enroll regenerate** command is used. • *key-size*—(Optional) Size of the desired RSA key. If not specified, the existing key size is used. • *encryption-key-size*—(Optional) Size of the second key, which is used to request separate encryption, signature keys, and certificates. **Note** Multiple trustpoints can share the same key.
Step 12	**exit** **Example:** `Router(ca-trustpoint)# exit`	Exits CA-trustpoint configuration mode.

	Command or Action	Purpose
Step 13	**crypto pki authenticate** *trustpoint-label* **Example:** `Router(config)# crypto pki authenticate VG224`	Retrieves the CA certificate and authenticates it. Checks the certificate fingerprint if prompted. • *trustpoint-label*—Trustpoint label. **Note** This command is optional if the CA certificate is already loaded into the configuration.
Step 14	**crypto pki enroll** trustpoint-label **Example:** `Router(config)# crypto pki enroll VG224`	Enrolls with the CA and obtains the certificate for this trustpoint. • *trustpoint-label*—Trustpoint label.
Step 15	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.

Configuring STCAPP, Trustpoint, and Security

To configure STCAPP, trustpoint, and security mode, perform the following steps on the Cisco VG224.

Prerequisites

- SCCP is enabled on the Cisco voice gateway. STC application group to be configured is created. For configuration information, see the "Enabling SCCP on the Voice Gateway" section on page 21.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **stcapp ccm-group** *group-id*
4. **stcapp security trustpoint** *line*
5. **stcapp security mode** [**authenticated** | **encrypted** | **none**]
6. **stcapp**
7. **dial-peer voice** *tag* **pots**
8. **security mode** [**authenticated** | **encrypted** | **none**]
9. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**stcapp ccm-group** *group-id* **Example:** `Router(config)# stcapp ccm-group 1`	Configures an STC application group. • Group to be configured is already created by using the **sccp ccm group** command. See the "Enabling SCCP on the Voice Gateway" section on page 21.
Step 4	**stcapp security trustpoint** *line* **Example:** `Router(config)# stcapp security trustpoint VG224`	Specifies the trustpoint to be used for setting up the TLS connection for STCAPP endpoints. • This command must be configured for the STCAPP service to start.
Step 5	**stcapp security mode [authenticated | encrypted | none]** **Example:** `Router(config)# stcapp security mode encrypted`	Enables security for STCAPP endpoints. • This command and the **stcapp security trustpoint** command in the previous step must be configured for security to be enabled for the STCAPP endpoint.
Step 6	**stcapp** **Example:** `Router(config)# stcapp`	Enables the STCAPP at the global level.
Step 7	**dial-peer voice** *tag* **pots** **Example:** `Router(config)# dial-peer voice 1 pots`	(Optional) Enters dial peer voice configuration mode.
Step 8	**security mode** [**authenticated** | **encrypted** | **none**] **Example:** `Router(config-dialpeer)# security mode encrypted`	(Optional) Enables dialpeer level STCAPP endpoint security and overrides global configuration. • **authenticated**—Enables STCAPP endpoints using signaling authentication. • **encrypted**—Enables STCAPP endpoints using data encryption. • **none**—Disables dialpeer level STCAPP endpoint security configuration and defaults to global level configuration.
Step 9	**end** **Example:** `Router(config-dialpeer)# end`	Exits dial-peer configuration mode and returns to privileged EXEC mode.

Verifying and Troubleshooting Secure Signaling and Media Encryption on the Cisco VG224

To verify and troubleshoot secure signaling and media encryption on the VG224, perform the following steps:

SUMMARY STEPS

1. **show sccp**
2. **show dial-peer voice**
3. **debug sccp tls**
4. **debug sccp message**
5. **debug voip application stcapp all**
6. **show stcapp device voice-port** *port*
7. **show call active voice brief**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**show sccp** **Example:** `Router> show sccp`	Displays SCCP information such as administrative and operational status.
Step 2	**show dial-peer voice** **Example:** `Router> show dial-peer voice`	Displays dial peer information including security mode
Step 3	**debug sccp tls** **Example:** `Router# configure terminal`	Displays debugging information for SCCP and its related applications (transcoding and conferencing).
Step 4	**debug sccp message** **Example:** `Router# debug sccp message`	Displays debugging information for SCCP and its related applications (transcoding and conferencing).
Step 5	**debug voip application stcapp all** **Example:** `Router# debug voip application stcapp all`	Displays debugging information for the components of the STCAPP.

	Command or Action	Purpose
Step 6	**show stcapp device voice-port** *port* **Example:** `Router# show stcapp device voice-port 1/0/0`	Displays configuration information about a specified STCAPP analog voice port.
Step 7	**show call active voice brief** **Example:** `Router# show call active voice brief`	Displays a truncated version of call information for voice calls in progress.

Examples

The following examples show sample output for commands used to verify and troubleshoot STCAPP and security mode configuration:

show dial-peer voice: Example

```
Show dial-peer voice 5001

VoiceEncapPeer5001
peer type = voice, system default peer = FALSE, information type = voice,
description = `',
tag = 5001, destination-pattern = `',
voice reg type = 0, corresponding tag = 0,
…….
      …….
digit_strip = enabled,
register E.164 number with H323 GK and/or SIP Registrar = TRUE
fax rate = system,   payload size =  20 bytes
supported-language = ''
preemption level = `routine'
bandwidth:
    maximum = 64 KBits/sec, minimum = 64 KBits/sec
voice class called-number:
    inbound = `', outbound = `'
dial tone generation after remote onhook = enabled
```

The following lines show encryption enabled:

```
 Signaling and Media Security = Encrypted

Time elapsed since last clearing of voice call statistics never
Connect Time = 0, Charged Units = 0,
Successful Calls = 0, Failed Calls = 0, Incomplete Calls = 0
Accepted Calls = 0, Refused Calls = 0,
Last Disconnect Cause is "",
Last Disconnect Text is "",
Last Setup Time = 0.
Last Disconnect Time = 0.
```

show sccp: Example

```
show sccp
SCCP Admin State: UP
Gateway IP Address: 10.4.177.53, Port Number: 2000
IP Precedence: 5
User Masked Codec list: None
```

```
Call Manager: 10.4.177.51, Port Number: 2000
       Priority: N/A, Version: 4.0, Identifier: 1

Alg_Phone Oper State: ACTIVE - Cause Code: NONE
Active Call Manager: 10.4.177.51, Port Number: 2443
TCP Link Status: CONNECTED, Device Name: AN0C8639A24D400
```

The following lines show secure media and signaling status:

```
Security
 Signaling Security: ENCRYPTED TLS
Media Security: SRTP
Supported crypto suites :AES_CM_128_HMAC_SHA1_32
Reported Max Streams: 1, Reported Max OOS Streams: 0
Supported Codec: RFC 2833 dtmf, Maximum Packetization Period: 30
Supported Codec: g711ulaw, Maximum Packetization Period: 20
Supported Codec: g711alaw, Maximum Packetization Period: 20
Supported Codec: g729r8, Maximum Packetization Period: 220
Supported Codec: g729ar8, Maximum Packetization Period: 220
Supported Codec: g729br8, Maximum Packetization Period: 220
Supported Codec: g729r8, Maximum Packetization Period: 220

Alg_Phone Oper State: ACTIVE - Cause Code: NONE
Active Call Manager: 10.4.177.51, Port Number: 2000
TCP Link Status: CONNECTED, Device Name: AN0C8639A24D401
```

The following lines show secure media and signaling status:

```
Security
 Signaling Security: AUTHENTICATED TLS
Reported Max Streams: 1, Reported Max OOS Streams: 0
Supported Codec: RFC 2833 dtmf, Maximum Packetization Period: 30
Supported Codec: g711ulaw, Maximum Packetization Period: 20
Supported Codec: g711alaw, Maximum Packetization Period: 20
Supported Codec: g729r8, Maximum Packetization Period: 220
Supported Codec: g729ar8, Maximum Packetization Period: 220
Supported Codec: g729br8, Maximum Packetization Period: 220
Supported Codec: g729r8, Maximum Packetization Period: 220

Alg_Phone Oper State: ACTIVE - Cause Code: NONE
Active Call Manager: 10.4.177.51, Port Number: 2000
TCP Link Status: CONNECTED, Device Name: AN0C8639A24D402
Reported Max Streams: 1, Reported Max OOS Streams: 0
Supported Codec: RFC 2833 dtmf, Maximum Packetization Period: 30
Supported Codec: g711ulaw, Maximum Packetization Period: 20
Supported Codec: g711alaw, Maximum Packetization Period: 20
Supported Codec: g729r8, Maximum Packetization Period: 220
Supported Codec: g729ar8, Maximum Packetization Period: 220
Supported Codec: g729br8, Maximum Packetization Period: 220
Supported Codec: g729r8, Maximum Packetization Period: 220
```

show stcapp device voice-port: Example

```
Show stcapp device voice-port 2/0
Port Identifier:  2/0
Device Type:      ALG
Device Id:        2
Device Name:      AN0C8639A24D400
```

The following line shows device security status:

```
Device Security Mode : Encrypted
Modem Capability: None
Device State:     IS
```

```
Diagnostic:       None
Directory Number: 5001
Dial Peer(s):     5001
Dialtone after remote onhook feature: activated
Last Event:       STCAPP_CC_EV_CALL_DISCONNECT_DONE
Line State:       IDLE
Hook State:       ONHOOK
mwi:              DISABLE
vmwi:             OFF
PLAR:             DISABLE
Number of CCBs:   0
Global call info:
    Total CCB count      = 0
    Total call leg count = 0
```

Configuration Examples for Secure Signaling and Media Encryption for the Cisco VG224

The following examples show STCAPP security enabled at the system level and the security mode configured on the dial peer:

```
Router# show running-config
Building configuration...
Current configuration : 8906 bytes
!
! Last configuration change at 15:41:09 PDT Mon Oct 23 2006
!
version 12.4
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname akash
!
boot-start-marker
boot-end-marker
!
logging buffered 400000 debugging
no logging console
enable password lab
!
no aaa new-model
!
resource policy
!
clock timezone PST -8
clock summer-time PDT recurring
no ip domain lookup
!
!
!
```

The following lines show STCAPP security enabled at the system level:

```
stcapp ccm-group 1
stcapp security trustpoint analog
stcapp security mode encrypted
stcapp
!
voice-card 0
dsp services dspfarm
!
crypto pki trustpoint analog
enrollment url http://10.4.177.51:80
serial-number
revocation-check none
certificate ca 01
30820201 3082016A A0030201 02020101 300D0609 2A864886 F70D0101 04050030
14311230 10060355 04031309 756E6974 69746573 74301E17 0D303630 35303132
33303130 335A170D 30393034 33303233 30313033 5A301431 12301006 03550403
1309756E 69746974 65737430 819F300D 06092A86 4886F70D 01010105 0003818D
00308189 02818100 C2D07857 B8DF7F55 3C2365B3 2E1524CF EE898D1F D7A04075
D36F0229 392803DF B45246B4 A447506F A3FCDD00 9FC93CD7 5B5573E0 7BFD25E1
AB2F24E2 740D5765 7F628B6E 0FD39BEE 940D80FF 3B9F9F17 7ACA8F82 1A9E3179
458781E8 87C95E1B 17E6A61C 7D138AC1 D8E30F3C 88BFAFEE A94D5F8C E433DF71
F076E96C 9BB5327F 02030100 01A36330 61300F06 03551D13 0101FF04 05300301
01FF300E 0603551D 0F0101FF 04040302 0186301F 0603551D 23041830 168014B5
418287D0 61FE277C 9A1862B3 673BF7F7 0E47DD30 1D060355 1D0E0416 0414B541
8287D061 FE277C9A 1862B367 3BF7F70E 47DD300D 06092A86 4886F70D 01010405
00038181 002BB76E 22A59D73 6DBB62BA BAC3D5B4 2F739A26 D5FFF911 EDEB9BDC
7B29FECC E0B68E0F 22A3C0D0 8BA64592 30C6B628 5EFA3905 1B13BFE7 7CEB1456
55214435 07F752A6 73D5646A 4BB7B3C2 61E2C185 3A638FCA AE5AC6A1 3DB3590B
C3C6C924 D1E1E365 FE041B07 F3E2AF24 3701B664 A7879229 AFDF163A 00AA12AA
85866101 53
quit
crypto pki certificate chain analog
certificate 0A
308201BF 30820128 A0030201 0202010A 300D0609 2A864886 F70D0101 04050030
14311230 10060355 04031309 756E6974 69746573 74301E17 0D303630 35333032
31313630 345A170D 30373035 33303231 31363034 5A302A31 28301206 03550405
130B4648 4B303930 37463050 47301206 092A8648 86F70D01 09021605 616B6173
68305C30 0D06092A 864886F7 0D010101 0500034B 00304802 4100A6AD 0A376A6C
9EB668CC D0DF2A17 180E6CA2 FA5F243B 861EAA29 BE5FC488 A22AD4E8 5DFC22AC
13B43337 2F9FBA64 14E838EA 888E79DE 93AB63E4 4B4E2ECD 256D0203 010001A3
4F304D30 0B060355 1D0F0404 030205A0 301F0603 551D2304 18301680 14B54182
87D061FE 277C9A18 62B3673B F7F70E47 DD301D06 03551D0E 04160414 34D2D41C
274AB6E3 71A3A32C EC19D533 D3C0A020 300D0609 2A864886 F70D0101 04050003
818100A2 3947B1D0 FC5E9B79 0C1A28E7 BCB34C6C BB68C5F6 356F3F61 7525053E
0AED7325 9F286888 887810A6 B62FBAF3 BDC81542 C9828BBF 6A9FE936 AD3ED33B
D4F5AD22 E703C8E0 C3DDEAC8 2097A209 542551F7 6340A2A4 55A25A99 6A87367F
A0CBD9B6 E38D5E40 6479EB71 EFA644B3 93222D6F 235039AE BB9AA7B7 B1D07B3C FC6339
quit
certificate ca 01
30820201 3082016A A0030201 02020101 300D0609 2A864886 F70D0101 04050030
14311230 10060355 04031309 756E6974 69746573 74301E17 0D303630 35303132
33303130 335A170D 30393034 33303233 30313033 5A301431 12301006 03550403
1309756E 69746974 65737430 819F300D 06092A86 4886F70D 01010105 0003818D
00308189 02818100 C2D07857 B8DF7F55 3C2365B3 2E1524CF EE898D1F D7A04075
D36F0229 392803DF B45246B4 A447506F A3FCDD00 9FC93CD7 5B5573E0 7BFD25E1
AB2F24E2 740D5765 7F628B6E 0FD39BEE 940D80FF 3B9F9F17 7ACA8F82 1A9E3179
458781E8 87C95E1B 17E6A61C 7D138AC1 D8E30F3C 88BFAFEE A94D5F8C E433DF71
F076E96C 9BB5327F 02030100 01A36330 61300F06 03551D13 0101FF04 05300301
01FF300E 0603551D 0F0101FF 04040302 0186301F 0603551D 23041830 168014B5
418287D0 61FE277C 9A1862B3 673BF7F7 0E47DD30 1D060355 1D0E0416 0414B541
8287D061 FE277C9A 1862B367 3BF7F70E 47DD300D 06092A86 4886F70D 01010405
00038181 002BB76E 22A59D73 6DBB62BA BAC3D5B4 2F739A26 D5FFF911 EDEB9BDC
```

```
7B29FECC E0B68E0F 22A3C0D0 8BA64592 30C6B628 5EFA3905 1B13BFE7 7CEB1456
55214435 07F752A6 73D5646A 4BB7B3C2 61E2C185 3A638FCA AE5AC6A1 3DB3590B
C3C6C924 D1E1E365 FE041B07 F3E2AF24 3701B664 A7879229 AFDF163A 00AA12AA
85866101 53
quit
!
!
voice service voip
!
!
interface FastEthernet0/0
ip address 10.4.177.53 255.255.0.0
duplex auto
speed auto
!
interface FastEthernet0/1
no ip address
shutdown
duplex auto
speed auto
!
ip route 0.0.0.0 0.0.0.0 1.4.0.1
!
ip http server
no ip http secure-server
!
no cdp advertise-v2
!
!
control-plane
!
!
voice-port 2/0
!
voice-port 2/1
!
voice-port 2/2
!
voice-port 2/3
!
voice-port 2/4
!
.
.
.
!
voice-port 2/23
!
!
!
sccp local FastEthernet0/0
sccp ccm 10.4.177.51 identifier 1 version 4.0
sccp
!
sccp ccm group 1
associate ccm 1 priority 1
!
dial-peer voice 5001 pots
service stcapp
port 2/0
!
dial-peer voice 5002 pots
service stcapp
```

The following line shows the security mode configured on the dial peer:

```
security mode authenticated
port 2/1
!
dial-peer voice 5003 pots
service stcapp
security mode none
port 2/2
!
dial-peer voice 2000 voip
destination-pattern 7...
session target ipv4:10.4.177.100
incoming called-number 7000
codec g711ulaw
!
dial-peer voice 1 pots
!
dial-peer voice 5004 pots
service stcapp
shutdown
port 2/3
!
dial-peer voice 5005 pots
shutdown
destination-pattern 3001
port 2/4
!
.
.
.
!
dial-peer voice 5018 pots
service stcapp
shutdown
port 2/17
!
dial-peer voice 2001 pots
destination-pattern 2001
port 2/18
!
dial-peer voice 1000 voip
destination-pattern 1...
session target ipv4:10.3.105.5
!
dial-peer voice 5900 voip
destination-pattern 59..
session target ipv4:10.3.105.5
!
dial-peer voice 500 voip
destination-pattern 5...
session target ipv4:10.4.177.51
!
dial-peer voice 5019 pots
service stcapp
shutdown
port 2/18
!
dial-peer voice 5020 pots
service stcapp
shutdown
port 2/19
!
.
```

```
.
.
!
dial-peer voice 5024 pots
service stcapp
shutdown
port 2/23
!
!
!
!
line con 0
transport output all
line aux 0
transport output all
line vty 0 4
password lab
login
transport input all
transport output all
!
ntp clock-period 17179541
ntp server 10.4.177.51
end
```

Additional References

The following sections provide references related to SCCP analog phone support for FXS ports on the Cisco voice gateway.

Related Documents

Related Topic	Document Title
Cisco Unified Communications Manager	*Cisco Unified Communications Manager documentation*
Cisco Unified Communications Manager Express	*Cisco Unified Communications Manager Express documentation*
Cisco IOS debugging	*Cisco IOS Debug Command Reference*
Cisco IOS voice commands	*Cisco IOS Voice Command Reference*
Cisco IOS voice configuration	*Cisco IOS Voice Configuration Library*
Cisco voice gateway	• *Cisco VG200 Series documentation* • *Cisco 1800 Series Integrated Services Routers documentation* • *Cisco 2800 Integrated Services Routers documentation* • *Cisco 3800 Series Integrated services Routers documentation* • *Cisco Unified 500 Series documentation*
Conferencing and transcoding resources	• "Configuring Enhanced Conferencing and Transcoding for Voice Gateway Routers" chapter in the *Cisco Unified CallManager and Cisco IOS Interoperability Guide*. • *Cisco CallManager and IOS Gateway DSP Farm Configuration Example*

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Feature Information for Secure Signaling and Media Encryption for the Cisco VG224

Table 1 lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Release 12.4(20)YA or a later release appear in the table.

For information on a feature in this technology that is not documented here, see the "Supplementary Services Features Roadmap" section on page 1.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 Feature Information

Feature Name	Releases	Feature Information
Secure Signaling and Media Encryption for the Cisco VG224	12.4(11)XW	Provides secure voice call capabilities for analog phones that are connected to FXS ports on a Cisco VG224 Analog Phone Gateway and controlled by Cisco Unified CME. The following sections provide information about this feature: • Media Encryption (SRTP), page 194 • How to Configure Secure Signaling and Media Encryption for the Cisco VG224, page 195