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

- Restrictions for Secure Signaling and Media Encryption for the Cisco VG224, page 194
- Information About Secure Signaling and Media Encryption for the Cisco VG224, page 194
- How to Configure Secure Signaling and Media Encryption for the Cisco VG224, page 195
- Configuration Examples for Secure Signaling and Media Encryption for the Cisco VG224, page 206
- Additional References, page 211
- Feature Information for Secure Signaling and Media Encryption for the Cisco VG224, page 212
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
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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> crypto pki server cs-label</td>
<td>Defines a label for the certificate server and enters certificate server configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# crypto pki server cs-server1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> database level {minimal</td>
<td>names</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(cs-server)# database level complete</td>
<td></td>
</tr>
</tbody>
</table>

- **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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 5</strong></td>
<td>grant auto</td>
<td>(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. <strong>Tip</strong> Use this command only during enrollment when testing and building simple networks. A security best practice is to disable this functionality using the <code>no grant auto</code> command after configuration so that certificates cannot be continually granted.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>database url root-url</td>
<td>(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. <strong>root-url</strong>—Location where database entries will be written out. The URL can be any URL that is supported by the Cisco IOS file system. <strong>Note</strong> 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 <code>squeeze</code> 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.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>no shutdown</td>
<td>(Optional) Enables the CA. <strong>Note</strong> You should use this command only after you have completely configured the CA. <strong>Tip</strong> Enter your password when prompted.</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>exit</td>
<td>Exits certificate server configuration mode.</td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>crypto pki trustpoint label</td>
<td>(Optional) Declares a trustpoint and enters CA-trustpoint configuration mode. <strong>Note</strong> Use this command and the <code>enrollment url</code> 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. <strong>label</strong>—Name for the trustpoint. The <code>label</code> in this step should be the same as the <code>cs-label</code> in Step 3.</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td><code>crypto key generate rsa general-keys label key-label</code></td>
<td>(Optional) Generates Rivest, Shamir, and Adelman (RSA) key pairs.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router(config)# crypto key generate rsa general-keys label VG224</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td><code>crypto pki trustpoint label</code></td>
<td>Declares the trustpoint that your RA mode certificate server should use and enters CA-trustpoint configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router(config)# crypto pki trustpoint VG224</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td></td>
</tr>
<tr>
<td><code>enrollment url ca-url</code></td>
<td>Specifies the enrollment URL of the issuing CA certificate server.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router(ca-trustpoint)# enrollment url http://10.3.105.40:80</code></td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
</tr>
<tr>
<td>--------</td>
<td>---------------------------------------</td>
</tr>
<tr>
<td>Step 6</td>
<td>serial-number none</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Router(ca-trustpoint)# serial-number none</td>
</tr>
<tr>
<td>Step 7</td>
<td>fqdn none</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Router(ca-trustpoint)# fqdn none</td>
</tr>
<tr>
<td>Step 8</td>
<td>ip-address none</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Router(ca-trustpoint)# ip-address none</td>
</tr>
<tr>
<td>Step 9</td>
<td>subject-name [x.500-name]</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Router(ca-trustpoint)# subject-name cn=VG224, ou=ABU, o=Cisco Systems Inc.</td>
</tr>
<tr>
<td>Step 10</td>
<td>revocation-check none</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Router(ca-trustpoint)# revocation-check none</td>
</tr>
<tr>
<td>Step 11</td>
<td>rsakeypair key-label [key-size [encryption-key-size]]</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Router(ca-trustpoint)# rsakeypair VG224</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 12</td>
<td>exit</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Router(ca-trustpoint)# exit</td>
</tr>
</tbody>
</table>
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

---

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 13</strong></td>
<td>crypto pki authenticate <em>trustpoint-label</em>&lt;br&gt;Example: Router(config)# crypto pki authenticate VG224</td>
</tr>
<tr>
<td><strong>Step 14</strong></td>
<td>crypto pki enroll <em>trustpoint-label</em>&lt;br&gt;Example: Router(config)# crypto pki enroll VG224</td>
</tr>
<tr>
<td><strong>Step 15</strong></td>
<td>exit&lt;br&gt;Example: Router(config)# exit</td>
</tr>
</tbody>
</table>

**Note**<br>This command is optional if the CA certificate is already loaded into the configuration.
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Enter your password if prompted.</td>
</tr>
</tbody>
</table>

| **Step 2** configure terminal | Enters global configuration mode. |
| **Example:** | |

| **Step 3** stcapp ccm-group group-id | Configures an STC application group. |
| **Example:** | 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 | Specifies the trustpoint to be used for setting up the TLS connection for STCAPP endpoints. |
| **Example:** | This command must be configured for the STCAPP service to start. |

| **Step 5** stcapp security mode [authenticated | encrypted | none] | Enables security for STCAPP endpoints. |
| **Example:** | 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 | Enables the STCAPP at the global level. |
| **Example:** | |

| **Step 7** dial-peer voice tag pots | (Optional) Enters dial peer voice configuration mode. |
| **Example:** | |

| **Step 8** security mode [authenticated | encrypted | none] | (Optional) Enables dialpeer level STCAPP endpoint security and overrides global configuration. |
| **Example:** | 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 | Exits dial-peer configuration mode and returns to privileged EXEC mode. |
| **Example:** | |
Verifying and Troubleshooting Secure Signaling and Media Encryption on the Cisco VG224

To verify and troubleshoot secure signaling and media encryption on the VG24, 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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** 
* show sccp | Displays SCCP information such as administrative and operational status. |
| **Example:** 
Router> show sccp | |
| **Step 2** 
* show dial-peer voice | Displays dial peer information including security mode. |
| **Example:** 
Router> show dial-peer voice | |
| **Step 3** 
* debug sccp tls | Displays debugging information for SCCP and its related applications (transcoding and conferencing). |
| **Example:** 
Router# configure terminal | |
| **Step 4** 
* debug sccp message | Displays debugging information for SCCP and its related applications (transcoding and conferencing). |
| **Example:** 
Router# debug sccp message | |
| **Step 5** 
* debug voip application stcapp all | Displays debugging information for the components of the STCAPP. |
| **Example:** 
Router# debug voip application stcapp all | |
How to Configure Secure Signaling and Media Encryption for the Cisco VG224

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
```

**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
```

**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
```
Configuring Secure Signaling and Media Encryption for the Cisco VG224

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

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

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

The following line shows device security status:

Device Security Mode: Encrypted
Modem Capability: None
Device State: IS
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 dmap农场
!
crypto pki trustpoint analog
enrollment url http://10.4.177.51:80
serial-number
revocation-check none
certificate ca 01
03820201 0382016A A0030201 02020101 0030D609 2A864886 F70D0101 04050030
14311230 10060355 04031309 756E6974 69746573 74301E17 DD03630 35330312
33303130 335A170D 30330323 33031303 SA031431 12301006 03550043
1309756E 69746574 65737430 819F300D 06092A86 4886F70D 01010105 0003818D
00308189 02818100 C2D07857 B8DF7F55 3C2365B3 2E1524CF EE98D9F D7A4075F
D36F0229 392803DF B4524B4A A447506F A3FCD0D0 9FC93CD7 5B5573B0 7BD25E1
AB2F24E2 740D5765 7F62BB6E 0F039BEE 940D80FF 3BFF9F17 7ACAB8F2 1AE1E197
458781B8 87C95E1B 1B6A61C 7D138AC1 D8E303FC 88BFAFEE 94AD5F8C E433DF71
F076E96C 9B85127F 02030100 01A36330 61300F06 03551D13 0101FF04 05300301
01FF300E 0603551D 0F0101FP 04040302 0186301F 0603551D 23041380 160814B5
418287DD 61FE277C 9A1862B3 573BF7F7 0847D30D 1D060355 1D0E0416 0414B541
82BD7D67 1862B367 3BFF700E 47DD300D 06092A86 4886F70D 01010405
00038189 0281B76E 2A5A97D3 6DBB62BA BACD3DB4 2F739A26 3701B664 A7897229 AFDF163A 00A12AA8 85866101 53
quit
crypto pki trustpoint chain analog
certificate 0A
038201BF 03820128 A0030201 02020101 0030D609 2A864886 F70D0101 04050030
14311230 10060355 04031309 756E6974 69746573 74301E17 DD03630 35330312
31363363 3A5A170D 30330323 33031303 SA03A2A1 28301206 03550405
130B4648 4B303930 37463050 47301206 092A8648 86F70D01 09021605 61861736
68305C30 0D06092A 864886F7 0D010101 05003408 03048802 4100A6AD 0A37A6A6C
9BEB68CC D0D2FA17 180EBCA2 F5F243B 86E1A29 BEFC4882 A2AD4828 5DPC22AC
13B43337 2F9FBA64 14E838ED 886B79DE 9AB638B4 4B4E2ECD 256D0203 010001A3
4F304D01 0B060355 1D0F0404 030205A0 01F0603 51D2304 18301608 14B5418
87D061FE 277CA18 62B6363B F7F70E47 DD01D06 03551D0E 04160414 34D2D41C
27A4B638 71A3A32C EC19D533 D3CA0200 036D0069 2A864886 F70D0101 04050003
818010A8 3947BD1F FCE59B79 0C1A28E7 BCB436C6 BB6C5F65 356F3F61 7525053E
0AED7325 9F286888 887810A6 B62F2AF3 BDC81542 C9B28B6F 6A9FE936 AD1ED33B
D4F5AD22 E703C8E0 C3DDEAC8 2097A209 542515F7 36402A24 5A5A2999 6A87367F
A0CBB9D8 E385E4A0 6479EB71 EFA644B3 932224D6 235039AE B9B9AB77 B1D07B3C FC6339
quit
certificate ca 01
03820201 0382016A A0030201 02020101 0030D609 2A864886 F70D0101 04050030
14311230 10060355 04031309 756E6974 69746573 74301E17 DD03630 35330312
33303130 335A170D 30330323 33031303 SA031431 12301006 03550403
1309756E 69746574 65737430 819F300D 06092A86 4886F70D 01010505 0003818D
00308189 0281B76E 2A5A97D3 6DBB62BA BACD3DB4 2F739A26 3701B664 A7897229 AFDF163A 00A12AA8 85866101 53
quit
```
7B29FECC E0B68E0F 22A3C0D0 8BA64592 30C6B628 5EFA3905 1B13BFE7 7CEB1456
55214435 07F752A6 73D5646A 4BB7B3C2 61E2C185 3A638FCA AE5AC6A1 3DB3590B
C3C6C924 D1E365 FE041B07 F3E2AF24 3701B664 A7879229 AFDF163A 00AA12AA
8586101 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:

```plaintext
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
!
.
```
```plaintext
.d.
! 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

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Unified Communications Manager</td>
<td>Cisco Unified Communications Manager documentation</td>
</tr>
<tr>
<td>Cisco Unified Communications Manager Express</td>
<td>Cisco Unified Communications Manager Express documentation</td>
</tr>
<tr>
<td>Cisco IOS debugging</td>
<td>Cisco IOS Debug Command Reference</td>
</tr>
<tr>
<td>Cisco IOS voice commands</td>
<td>Cisco IOS Voice Command Reference</td>
</tr>
<tr>
<td>Cisco IOS voice configuration</td>
<td>Cisco IOS Voice Configuration Library</td>
</tr>
</tbody>
</table>
| 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

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td><a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a></td>
</tr>
</tbody>
</table>
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>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
</table>
| 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 |