Media and Signaling Encryption (SRTP/TLS) on DSP Farm Conferencing

First Published: June 22, 2007
Last Updated: November 25, 2008

The Media and Signaling Encryption (SRTP/TLS) on DSP Farm Conferencing feature provides secure conferencing capability for Cisco Unified Communications Manager (Unified CM) networks, including authentication, integrity and encryption of voice media and related call control signaling to and from the digital signal processor (DSP) farm.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. 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 Media and Signaling Encryption (SRTP/TLS) on DSP Farm Conferencing" section on page 30.

Finding Support Information for Platforms and Cisco IOS and Catalyst OS 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

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Prerequisites for Media and Signaling Encryption (SRTP/TLS) on DSP Farm Conferencing

Make sure that the following tasks have been completed before configuring the Media and Signaling Encryption (SRTP/TLS) on DSP Farm Conferencing feature:

- Cisco IOS gateways have the prerequisite Cisco IOS images installed. Voice security features are delivered on Advanced IP Services or Advanced Enterprise Services images.
- Cisco Unified Communications Manager 6.1 or a later release is running if the Media and Signaling Encryption (SRTP/TLS) on DSP Farm Conferencing feature is deployed in a Unified CM network. For more information on configuring Unified CM, refer to *Cisco CallManager Security Guide, Release 5.0.*

Restrictions for Media and Signaling Encryption (SRTP/TLS) on DSP Farm Conferencing

- Secure transcoding and secure media termination points (MTP) are not supported in Unified CM networks.
- Secure Real-Time Transport Protocol (RTCP) is not supported.
- Multicast (hoot-and-holler) conferencing is not supported.
- TI 549 and TI 5421 DSP-based conferencing is not secure.
- Calls to Cisco Unity Express are not secure.
- Music on Hold (MOH) is not secure.
- Video calls are not secure.
- Modem relay and T.3 fax relay calls are not secure.
- Media forking is not supported.
- Conversion between inband tone and RFC2833 DTMF is not supported. RFC2833 DTMF handling is supported when encryption keys are sent to secure DSP farm devices but is not supported for codec passthrough.

See the "Supported Platforms, DSP Modules, and Conference Provisioning" section on page 5 for supported gateways, network modules, codecs, and conference session for the Media and Signaling Encryption (SRTP/TLS) on DSP Farm Conferencing feature.

Information About Media and Signaling Encryption (SRTP/TLS) on DSP Farm Conferencing

To configure Media and Signaling Encryption (SRTP/TLS) on DSP Farm Conferencing feature, you should understand the following concepts:

Benefits of Media and Signaling Encryption (SRTP/TLS) on DSP Farm Conferencing

The Media and Signaling Encryption (SRTP/TLS) on DSP Farm Conferencing feature provides privacy and confidentiality for secure conference calls by encrypting and decrypting media streams between the DSP farm and endpoints, and by protecting the signaling channel between the Unified CM and the DSP farm.

Feature Design of Media and Signaling Encryption (SRTP/TLS) on DSP Farm Conferencing

With the new Media and Signaling Encryption (SRTP/TLS) on DSP Farm Conferencing feature, Cisco extends encryption of voice media and related call control signaling to secure conferencing for Cisco Unified Communications Manager networks using the secure DSP farm feature. Cisco enhances DSP farm conferencing by securing both the media and signaling paths between the Unified CM, and Cisco IOS gateways and endpoints.

Voice conferencing involves adding several parties to a phone conversation. In a traditional circuit-switched voice network, all voice traffic passes through a central device, such as a PBX, with conference services provided within this central device. In contrast, IP phones normally send voice signals directly between phones without going through a central device. Conference services, however, require a network-based conference bridge. In an IP telephony network using Cisco Unified Communications Manager, the DSP-based conferencing provides the conference-bridging service. Cisco Unified CallManager uses a DSP farm, a collection of DSP resources that support conference, transcoding, and media termination point (MTP) services, to mix voice streams from multiple participants into a single conference-call stream. The mixed stream is played out to all conference attendees, minus the voice of the receiving attendee. DSP farms are configured on the Cisco IOS voice gateway and managed by Cisco Unified CM through SCCP.

DSP farm profiles are created to allocate DSP farm resources. Under the DSP farm profile, you select the service type (conference, transcode, and MTP), associate an application, and specify service-specific parameters, such as codecs and maximum number of conferences. A DSP farm profile allows you to group DSP resources based on the service type. Applications associated with the DSP farm profile, such as SCCP, can use the resources allocated under the profile. You can configure multiple DSP farm profiles

for the same service, each can register with one Cisco Unified CM group. The profile ID and service type uniquely identify a DSP farm profile, allowing the profile to uniquely map to a Unified CM group that contains a single pool of Cisco Unified CM servers.

DSP resources can reside on the voice gateway router in packet-voice DSP modules (PVDMs) installed in voice network modules, for example the NM-HDV2, or directly in the network module, for example the NM-HD-2V. Cisco 2800 series and 3800 series voice gateway routers have onboard DSP resources located on PVDM2s installed directly on the motherboard. Your router supports one or more voice network modules.

Figure 1 shows a typical topology where the Media and Signaling Encryption (SRTP/TLS) on DSP Farm Conferencing feature is deployed. Users establish a conference call across the public switched telephone network (PSTN) between locations. Tranport layer security (TLS) connections between the DSP farm and Unified CM secure SCCP signaling traffic, allowing for mutual authentication between the two. The DSP farm registers its resources with Cisco Unified CallManager and operates in secure mode to decrypt, decompress, mix, compress and encrypt voice packets. SRTP protected media streams connect to the DSP farm where they are mixed and played back to conference participants.

Figure 1 Secure DSP Farm Conferencing in the IP Telephony Network

Security Technologies and DSP Farm Conferencing

Cisco implements secure voice conferencing over the IP telephony network by establishing and maintaining authenticated and encrypted communications using the following security technologies:

- Signaling authentication validates that no tampering has occurred with signaling packets during transmission.
- Encryption, the process of converting clear-text data into enciphered data, provides data integrity and authentication.

- Call control signaling is encrypted using TLS, while Public Key Infrastructure (PKI) supports secure public key distribution. The DSP farm mutually authenticates with Unified CM through the use of certificates.
- Media encryption using standards-based SRTP ensures that media streams between supported devices are secure.
- Cisco IOS H.323 supports the AES_CM_128_HMAC_SHA1_32 cryptographic suite, which includes the AES-128-countermode encryption algorithm and the Hashed Message Authentication Codes (HMAC) Secure Hash Algorithm1 (SHA1) authentication algorithm.
- Cisco IOS H.323 supports H.235.8 compliant procedures for the signaling, negotiation, and transport of the SRTP cryptographic keys, authentication and encryption algorithm identifiers, and other session parameters between H.323 endpoints.

Supported Platforms, DSP Modules, and Conference Provisioning

The Media and Signaling Encryption (SRTP/TLS) on DSP Farm Conferencing feature is supported on the following platforms with on-board DSP modules or NM-HDV2 network modules:

- Cisco 2600XM
- Cisco 2691
- Cisco 2801
- Cisco 2811
- Cisco 2821
- Cisco 2851
- Cisco 3725
- Cisco 3745
- Cisco 3825
- Cisco 3845

DSP modules support the maximum number of TI 5510 DSPs listed:

- NM-HDV2: up to 16 TI 5510 DSPs in 4 PVDM2s
- Integrated Services Routers (ISRs) on-board PVDM2: up to 8 TI 5510 DSPs in 2 PVDM2s

The following network modules (NMs) provide the number of conferences and participants, up to the maximums listed by codec type:

Codec Type		NM-HDV2 (16 TI 5510 DSPs)	NM-HD-2VE (3 TI 5510 DSPs)	NM-HD-1V / NM-HD-2V (1TI 5510 DSP)
G.711	conferences participants	50 400	12 96	4 32
G.729	conferences participants	32 256	6 48	2 16

The maximum number of conferences for a DSP farm profile is dependent on DSP resources.

How to Configure Media and Signaling Encryption (SRTP/TLS) on DSP Farm Conferencing

This section contains the following procedures:

Prerequisites

Set the system clock using one of these methods:

- Configure Network Time Protocol (NTP).
- Manually set the software clock using the **clock set** command.

Both methods are explained in the "Performing Basic System Management" chapter of the *Cisco IOS Network Management Configuration Guide* for your Cisco IOS release.

Enabling HTTP server on both the external Cisco IOS certificate authority (CA) server and the Cisco IOS DSP farm gateway is required for TLS operation. Use the **ip http server** command to enable the Cisco web browser user interface.

Configuring an External CA Server

To configure an external CA server, perform the following steps:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip http server**
4. **crypto pki server** *cs-label*
5. **database level {minimal | names | complete}**
6. **grant auto**
7. **database url** *root-url*
8. **no shutdown**

9. **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	**ip http server** **Example:** `Router(config)# ip http server`	Enables the Cisco web browser user interface on the CA server.
Step 4	**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 5	**database level complete** **Example:** `Router(cs-server)# database level complete`	(Optional) Controls the type of data stored in the certificate enrollment database. The default if this command is not used is **minimal**. • **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.
Step 6	**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.

	Command or Action	Purpose
Step 7	**database url** *root-url* **Example:** `Router(cs-server)# database url nvram:`	(Optional) Specifies the location where all database entries for the certificate server are written. If this command is not specified, all database entries are written to NVRAM. • *root-url*—Location where database entries are written. The URL can be any URL that is supported by the Cisco IOS file system. **Note** 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 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 8	**no shutdown** **Example:** `Router(cs-server)# no shutdown`	(Optional) Enables the CA. **Note** Use this command only after you have completely configured the CA. You are prompted for a password.
Step 9	**exit** **Example:** `Router(cs-server)# exit`	Exits certificate server configuration mode.

Exporting the Cisco Unified CM Certificate

To configure secure conferencing, you must first obtain a certificate from Cisco Unified CM. To select the certificate file from Cisco Unified CM Certificate Management and download it to your PC desktop (to later upload into the Cisco IOS configuration), perform the following steps.

SUMMARY STEPS

1. Go to Cisco Unified Communications Operating System Administration and choose **Security>Certificate Management**.
2. Click **Find>File Name>Begins with** and enter “CallManager” in the search field.
3. Click **CallManager.pem**. The Certificate Configuration screen appears.
4. Find the line that reads: **CN=***ccmhostname*. Make note of the *ccmhostname*—You will need this name later in the configuration.
5. Click **download** and save this file to your PC desktop.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Go to Cisco Unified Communications Operating System Administration and choose **Security>Certificate Management**.	Accesses the resource needed to obtain a certificate file.
Step 2	Click **Find>File Name>Begins with** and enter "CallManager" in the search field.	Provides search capability to display all files that begin with CallManager.
Step 3	Click **CallManager.pem**. The Certificate Configuration screen appears.	Selects the appropriate .pem file for download.
Step 4	Find the line that reads: **CN=***ccmhostname*. Make note of the *ccmhostname*—You will need this name later in the configuration.	Provides the specific name for the file that you will need later in the configuration.
Step 5	Click **download** and save this file to your PC desktop.	Downloads the selected file from Cisco Unified CM to your desktop.

Configuring a Trustpoint on the Secure DSP Farm Gateway

To create a trustpoint on the Cisco IOS DSP farm gateway, perform the following steps.

Creating a Trustpoint

This trustpoint stores the digital certificate for the DSP farm. To create a trustpoint, perform the following steps:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto pki trustpoint** *label*
4. **enrollment url** *ca-url*
5. **serial-number none**
6. **fqdn none**
7. **ip-address none**
8. **subject-name** [*x.500-name*]
9. **revocation-check none**
10. **rsakeypair** *key-label*

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 trustpoint** *label* **Example:** `Router(config)# crypto pki trustpoint dspcert`	Declares the trustpoint that your RA mode certificate server uses and enters CA-trustpoint configuration mode. • *label*—Name for the trustpoint.
Step 4	**enrollment url** *ca-url* **Example:** `Router(ca-trustpoint)# enrollment url http://10.1.105.40:80`	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.
Step 5	**serial-number none** **Example:** `Router(ca-trustpoint)# serial-number none`	Specifies whether the router serial number is included in the certificate request. • **none**—Specifies that a serial number is not included in the certificate request.
Step 6	**fqdn none** **Example:** `Router(ca-trustpoint)# fqdn none`	Specifies a fully qualified domain name (FQDN) that is included as "unstructuredName" in the certificate request. • **none**—Router FQDN is not included in the certificate request.
Step 7	**ip-address none** **Example:** `Router(ca-trustpoint)# ip-address none`	Specifies a dotted IP address or an interface that is included as "unstructuredAddress" in the certificate request. • **none**—Specifies that an IP address is not to be included in the certificate request.
Step 8	**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.

	Command or Action	Purpose
Step 9	**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 or third method is specified, that method is used only if the previous method returns an error, such as a server being down. • **none**—Certificate checking is not required.
Step 10	**rsakeypair** *key-label* **Example:** `Router(ca-trustpoint)# rsakeypair dspcert`	(Optional) Specifies an RSA key pair to use with a certificate. • *key-label*—Name of the key pair, which is generated during enrollment if the key pair does not already exist or if the **auto-enroll regenerate** command is used. **Note** Multiple trustpoints can share the same key. The *key-label* is the same as the *label* in Step 3.

Authenticating and Enrolling the Certificate with the CA Server

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto pki authenticate** *trustpoint-label*
4. **crypto pki enroll** *trustpoint-label*

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.

	Command or Action	Purpose
Step 3	**crypto pki authenticate** *trustpoint-label* **Example:** `Router(config)# crypto pki authenticate dspcert`	Retrieves the CA certificate and authenticates it. Checks the certificate fingerprint if prompted. • *trustpoint-label*—Trustpoint label. **Note** The *trustpoint-label* is the trustpoint label specified in the "Configuring a Trustpoint on the Secure DSP Farm Gateway" section on page 8, step 3.
Step 4	**crypto pki enroll** trustpoint-label **Example:** `Router(config)# crypto pki enroll dspcert`	Enrolls with the CA and obtains the certificate for this trustpoint. • *trustpoint-label*—Trustpoint label. **Note** The *trustpoint-label* is the trustpoint label specified in the "Configuring a Trustpoint on the Secure DSP Farm Gateway" section on page 8, step 3.

Copying the CA Root Certificate of the DSP Farm Router to the Cisco Unified CallManager

The DSP farm router and Unified CM router exchange certificates during the registration process. These certificates are digitally signed by the CA server of the respective router. For the routers to accept each other's digital certificate, they must have the CA root certificate for each other. Manually copy the CA root certificate of the DSP farm and the Unified CM router for each other.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto pki export** *trustpoint* **pem** *url* **flash:**
4. You are prompted to confirm destination filenames for the CA certificate and router certificate. These file names are the same as the *trustpoint* name (with a .ca suffix and a .crt suffix, respectively) entered in step 3. To accept the names, press **Enter** after each prompt. The files are written to flash.
5. **tftp-server flash:***trustpoint***.ca**
6. **tftp-server flash:***trustpoint***.crt**
7. **end**
8. From your PC, connect to the router via TFTP and download the .ca and .crt files to your PC.
9. Go to Cisco Unified Communications Operating System Administration and choose **Security>Certificate Management**. Click **Upload Certificate**.
10. Upload the .ca and .crt files one at a time. Select **CallManager-trust** as the **Certificate Name** for both files. Leave the **Root Certificate** field blank for both files.
11. Restart CCM services on all nodes.

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 export** *trustpoint* **pem** *url* **flash:** **Example:** `Router(config)# crypto pki export sec2800-cfb.ca pem 10.1.1.1 flash:`	Exports the CA certificate and the router certificate associated with a trustpoint and writes the certificates to flash memory. **Note** Format for the files is privacy-enhanced mail (PEM).
Step 4	You are prompted to confirm destination filenames for the CA certificate and router certificate. These file names are the same as the *trustpoint* name (with a .ca suffix and a .crt suffix, respectively) entered in step 3. To accept the names, press **Enter** after each prompt. The files are written to flash.	Confirms the file names and writes the files to flash memory.
Step 5	**tftp-server flash:***trustpoint***.ca** **Example:** `Router(config)# tftp-server flash:sec2800-cfb.ca`	Makes the file available via TFTP. • *trustpoint* is the name of the file.
Step 6	**tftp-server flash:***trustpoint***.crt** **Example:** `Router(config)# tftp-server flash:sec2800-cfb.crt`	Makes the file available via TFTP. • *trustpoint* is the name of the file.
Step 7	**end** **Example:** `Router(config)# end`	Exits global configuration mode.
Step 8	From your PC, connect to the router via TFTP and download the .ca and .crt files to your PC.	Moves the files to your PC desktop so they are available for uploading
Step 9	Go to Cisco Unified Communications Operating System Administration and choose **Security>Certificate Management**. Click **Upload Certificate**.	
Step 10	Upload the .ca and .crt files one at a time. Select **CallManager-trust** as the **Certificate Name** for both files. Leave the **Root Certificate** field blank for both files.	
Step 11	Restart Cisco Unified CM services on all nodes.	

Configuring the Cisco Unified CM Trustpoint and Loading the Certificate

1. **enable**
2. **configure terminal**
3. **crypto pki trustpoint** *cucm hostname*
4. **enrollment terminal pem**
5. **subject-name CN=***ccmhostname*
6. **revocation-check none**
7. Copy the contents of the **CallManager.pem** file downloaded into the cut and paste buffer.
8. **crypto pki authenticate** *trustpoint-label*
9. Paste in the certificate and hit **enter**. Type **quit** and press **enter**. Type **yes** and press **enter** when you are prompted to accept the certificate.

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 trustpoint** *cucm hostname* **Example:** `Router(config)# crypto pki trustpoint sanjose1`	Declares the CA that your router should use and enters CA-trustpoint configuration mode. • *name*—CA trustpoint name.
Step 4	**enrollment terminal pem** **Example:** `Router(ca-trustpoint)# enrollment terminal pem`	Specifies manual (copy-and-paste) certificate enrollment.
Step 5	**subject-name CN=***ccmhostname* **Example:** `Router(ca-trustpoint)# subject-name CN=sec2800-cfb`	
Step 6	**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 or third method is specified, that method is used only if the previous method returns an error, such as a server being down. • **none**—Certificate checking is not required.

	Command or Action	Purpose
Step 7	Copy the contents of the **CallManager.pem** file downloaded into the cut and paste buffer.	Copies the CallManager.pem file so it can be pasted in later in the procedure.
Step 8	**crypto pki authenticate** *trustpoint label* **Example:** `Router(ca-trustpoint)# crypto pki authenticate sanjose1`	Authenticates the CA (by getting the certificate from the CA). • *name*—Name of the CA.
Step 9	Paste in the certificate and hit **enter**. Type **quit** and press **enter**. Type **yes** and press **enter** when you are prompted to accept the certificate.	Completes the configuration and loads the certificate.

Configuring the DSP Farm to Securely Register with Cisco Unified CM

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice-card** *slot*
4. **dsp service dspfarm**
5. **dspfarm profile** *profile-identifier* **conference security**
6. **trustpoint** *trustpoint-label*
7. **codec** {*codec-type* | **pass-through**}
8. **maximum sessions** *number*
9. **associate application sccp**
10. **no shutdown**
11. **exit**
12. **sccp local** *interface-type interface-number*
13. **sccp ccm** {*ip-address* | *dns*} **identifier** *identifier-number*
14. **sccp**
15. **sccp ccm group** *group-number*
16. **associate ccm** *identifier-number* **priority** *priority-number*
17. **associate profile** *profile-identifier* **register** *device-name*

18. **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	**voice-card** *slot* **Example:** `Router(config)# voice-card 1`	Enters voice-card configuration mode and configures a voice card. **Note** *slot* is the slot where the DSP farm resides.
Step 4	**dsp service dspfarm** **Example:** `Router(config)# dsp service dspfarm`	Enables digital signal processor (DSP) farm services for a particular voice network module.
Step 5	**dspfarm profile** *profile-identifier* **conference security** **Example:** `Router(config)# dspfarm profile 101 conference security`	Enters DSP farm profile configuration mode and defines a profile for DSP farm services. • **conference**—Enables profile for conferencing • **security**—Enables profile for secure DSP farm services.
Step 6	**trustpoint** *trustpoint-label* **Example:** `Router(config-dspfarm-profile)# trustpoint dspfarm`	Associates a trustpoint with a DSP farm profile.
Step 7	**codec** {*codec-type* | **pass-through**} **Example:** `Router(config-dspfarm-profile)# codec g711ulaw`	Specifies the codecs supported by a DSP farm profile. **Note** Repeat this step as necessary to specify all the supported codecs.
Step 8	**maximum sessions** *number* **Example:** `Router(config-dspfarm-profile)# maximum sessions 4`	Specifies the maximum number of sessions supported by the profile.
Step 9	**associate application sccp** **Example:** `Router(config-dspfarm-profile)# associate application sccp`	Associates the Skinny Client Control Protocol (SCCP) application to the digital signal processor (DSP) farm profile.

	Command or Action	Purpose
Step 10	**no shutdown** **Example:** `Router(config-dspfarm-profile)# no shutdown`	Enables the DSP farm profile.
Step 11	**exit** **Example:** `Router(config-sccp-ccm)# exit`	Exits the current configuration mode.
Step 12	**sccp local** *interface-type interface-number* **Example:** `Router(config)# sccp local FastEthernet0/0`	Selects the local interface that SCCP applications (transcoding and conferencing) use to register with Unified CM.
Step 13	**sccp ccm** {*ip-address* | *dns*} **identifier** *identifier-number* **Example:** `Router(config)# sccp ccm 10.3.105.6 identifier 2`	Adds a Unified CM server to the list of available servers and sets various parameters—including IP address or Domain Name System (DNS) name, port number, and version number. • *ip-address* is the IP address of the primary Unified CM
Step 14	**sccp** **Example:** `Router(config)# sccp`	Enables the SCCP protocol and its related applications.
Step 15	**sccp ccm group** *group-number* **Example:** `Router(config)# sccp ccm group 1`	Creates a Unified CM group and enters SCCP Unified CM configuration mode.
Step 16	**associate ccm** *identifier-number* **priority** *priority-number* **Example:** `Router(config-sccp-ccm)# associate ccm 1 priority 2`	Associates a Unified CM with a Unified CM group and establishes the Unified CM's priority within the group.
Step 17	**associate profile** *profile-identifier* **register** *device-name* **Example:** `Router(config-sccp-ccm)# associate profile 101 register gw`	Associates a DSP farm profile with a Unified CM group. • The *profile-identifier* should be the same as subject name field in the trustpoint created in the "Configuring a Trustpoint on the Secure DSP Farm Gateway" section on page 8.
Step 18	**exit** **Example:** `Router(config-sccp-ccm)# exit`	Exits the current configuration mode.

Configuring Secure Conferencing on Cisco Unified CM

Perform the following steps to configure secure conferencing on Unified CM.

SUMMARY STEPS

1. From the Unified CM Admistration page pulldown menu, choose **Service**, **Media Resources**, **Conference Bridge Configuration**.
2. Choose **Add a New Conference Bridge**.
3. Choose **Cisco IOS Enhanced Conference Bridge , Conference Bridge Type.**
4. Enter the conference identifier that you configured for **Conference Bridge Name**.
5. Select the default **Device Pool**.
6. Choose **Insert and Reset the Conference Bridge.**
7. Create an **MRG** and **MRGL** for the Conference Bridge. Use the same MRGL for participating IP Phones and gateways

DETAILED STEPS

	Command or Action	Purpose
Step 1	From the Unified CM Admistration page pulldown menu, select **Service**, then **Media Resources**, then **Conference Bridge Configuration**.	Enters Cisco Unified CallManager administration mode.
Step 2	Select **Add a New Conference Bridge**.	Configures a new conference bridge.
Step 3	Select **Cisco IOS Enhanced Conference Bridge** for **Conference Bridge Type**.	Configures conference bridge type.
Step 4	Enter the conference identifier that you configured for **Conference Bridge Name**.	Specifies the conference bridge name.
Step 5	Choose the default **Device Pool**.	Specifies the secure conference bridge device pool.
Step 6	Choose **Insert and Reset the Conference Bridge**.	Configures the conference bridge
Step 7	Create an **MRG** and **MRGL** for the Conference Bridge. Use the same MRGL for participating IP Phones and gateways.	Creates a media resource group and media resource group list. Completes secure conference bridge configuration.

Verifying and Troubleshooting Media and Signaling Encryption (SRTP/TLS) on DSP Farm Conferencing

Use the following commands to verify the configuration.

SUMMARY STEPS

1. **show crypto ca trustpoints status**
2. **show dspfarm dsp stats** *id*
3. **show dspfarm profile** *id*
4. **show media resource status**

5. **show rtpspi statistics**
6. **show sccp**
7. **show sccp ccm group** *id*
8. **show sccp statistics**
9. **show voice dsp group** *slot*

DETAILED STEPS

Step 1 Use the **show crypto ca trustpoints** command to display information about the trustpoints that are configured on the router.

```
Router# show crypto ca trustpoints status

Trustpoint dspfarm-mgcp:
  Issuing CA certificate configured:
    Subject Name:
     cn=IOSCAServer
……..
  Router General Purpose certificate configured:
    Subject Name:
     cn=sMgcpCFB,ou=ATG,o=Cisco
    …….
  State:
    Keys generated ..... Yes (General Purpose, …)
    Issuing CA authenticated ..... Yes
    Certificate request(s) ..... Yes

Trustpoint mgcp-ccm:
  Issuing CA certificate configured:
    Subject Name:
     cn=choc1.cisco.com
……….
  State:
    Keys generated ..... No
    Issuing CA authenticated ..... Yes
    Certificate request(s) ..... None
```

Step 2 Use the **show dspfarm dsp stats** *id* command to display configured digital signal processor (DSP) farm statistics for a specific conference bridge.

```
Router# show dspfarm dsp stats 1

Gathering total stats...

Bridge-id=0x1 Conferee-id=1 Call-id=0x2

PacketsReceived=13089 PacketTransmitted=13126 PacketsTossed=0 AverageJitter=0
MaxObservedJitter=0 TalkerFrameCount=26267

ConfereeStatus=1

Srtp Stats:

TotalPacketsEncrypted=13126 TotalPacketsDecrypted=13089 DecryptionFailurePacketCount=0
TotalPacketsAuthenticated=13089 AuthenticationFailurePacketCount=0
DuplicateReplayPacketCount=0 OutsideWindowReplayPacketCount=0 PacketsBadReceivedSSRC=0

Conference Stats:
```

```
ConferenceState=1

ConfereeList=0x7 TalkerList=0x7
```

Step 3 Use the **show dspfarm profile** *id* command to display configured digital signal processor (DSP) farm profile information for a selected Unified CM group.

```
Router# show dspfarm profile 22

Dspfarm Profile Configuration

 Profile ID = 22, Service = CONFERENCING, Resource ID = 1
 Profile Description :
 Profile Service Mode : secure
 Trustpoint : dspfarm-mgcp
 Profile Admin State : UP
 Profile Operation State : ACTIVE
 Application : SCCP   Status : ASSOCIATED
 Resource Provider : FLEX_DSPRM   Status : UP
 Number of Resource Configured : 16
 Number of Resource Available : 16
 Codec Configuration
 Codec : g711ulaw, Maximum Packetization Period : 30 , Transcoder: Not Required
 Codec : g711alaw,
```

Step 4 Use the **show media resource status** command to display the current media resource status.

Step 5 Use the **show rtpspi statistics** command to display Real-Time Transport Protocol (RTP) statistics.

Step 6 Use the **show sccp all** and **show sccp connections** commands to display Skinny Client Control Protocol (SCCP) information about administrative and operational status.

```
Router# show sccp
SCCP Admin State: UP
Gateway IP Address: 10.22.1.1, Port Number: 2000
IP Precedence: 5
User Masked Codec list: None
Call Manager: 1.3.105.6, Port Number: 2000
                Priority: 2, Version: 5.0.1, Identifier: 2
Call Manager: 1.3.105.5, Port Number: 2000
                Priority: 1, Version: 5.0.1, Identifier: 1

Conferencing Oper State: ACTIVE - Cause Code: NONE
Active Call Manager: 1.3.105.5, Port Number: 2000
TCP Link Status: CONNECTED, Profile Identifier: 22
Signaling Security: ENCRYPTED TLS
Media Security: SRTP
Supported crypto suites :AES_CM_128_HMAC_SHA1_32
Reported Max Streams: 128, Reported Max OOS Streams: 0
Supported Codec: g711ulaw, Maximum Packetization Period: 30
```

Step 7 Use the **show sccp ccm group** *id* command todisplay the groups that are configured on a specific Unified CM.

Step 8 Use the**show sccp statistics** command to display statistical information for SCCP transcoding and conferencing applications.

```
Router# show sccp stat

SCCP Application Service(s) Statistics:

Profile Identifier: 1, Service Type: Transcoding
TCP packets rx 16, tx 19
Unsupported pkts rx 0, Unrecognized pkts rx 0
Register tx 1, successful 1, rejected 0, failed 0
```

```
KeepAlive tx 13, successful 13, failed 0
OpenReceiveChannel rx 0, successful 0, failed 0 Encrypted :0
CloseReceiveChannel rx 0, successful 0, failed 0 Encrypted : 0
StartMediaTransmission rx 0, successful 0, failed 0  Encrypted : 0
StopMediaTransmission rx 0, successful 0, failed 0 Encrypted: 0
PortReq rx 0
PortRes tx 0, successful 0, failed 0
PortClose rx 0
```

Step 9 Use the **show voice dsp group** *slot* command to display the current status or selective statistics of digital signal processor (DSP) voice channels on the specified slot.

```
Router #show voice dsp group slot 1
dsp 13:
  State: UP, firmware: 4.4.706

  Max signal/voice channel: 16/16
  Max credits: 240
  Group: FLEX_GROUP_VOICE, complexity: FLEX
    Shared credits: 180, reserved credits: 0
    Signaling channels allocated: 2
    Voice channels allocated: 0
    Credits used: 0
  Group: FLEX_GROUP_XCODE, complexity: SECURE MEDIUM
    Shared credits: 0, reserved credits: 60
    Transcoding channels allocated: 0
    Credits used: 0
dsp 14:
  State: UP, firmware: 1.0.6
  Max signal/voice channel: 16/16
  Max credits: 240
  Group: FLEX_GROUP_CONF, complexity: SECURE CONFERENCE
    Shared credits: 0, reserved credits: 240
    Conference session: 1
    Credits used: 0
```

Use the following **debug** commands to troubleshoot the secure DSPFarm conferencing configuration.

- **debug dspfarm**
- **debug hpi all**
- **debug media resource provider**
- **debug sccp**
- **debug ssl**
- **debug voip confmsp**
- **debug voip dsmp**
- **debug voip xcodemsp**

Configuration Examples for Media and Signaling Encryption (SRTP/TLS) on DSP Farm Conferencing

This section contains the following examples:

Media and Signaling Encryption (SRTP/TLS) on DSP Farm Conferencing: Example

```
Router# show running-config

Building configuration...

Current configuration : 5874 bytes
!
! Last configuration change at 16:31:45 EDT Sun Mar 9 2008
! NVRAM config last updated at 16:33:36 EDT Sun Mar 9 2008
!
version 12.4
service config
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname sec2800-cfb
!
boot-start-marker
boot-end-marker
!
enable secret *****
!
aaa new-model
!
!
aaa authentication login default local
aaa authentication enable default enable
!
!
aaa session-id common
clock timezone EST -5
clock summer-time EDT recurring
no network-clock-participate wic 2
!
!
!
ip cef
!
!
no ip domain lookup
ip host ps-611 10.1.69.61
!
multilink bundle-name authenticated
!
!
!
voice-card 0
 no dspfarm
 dsp services dspfarm
!
!
crypto pki trustpoint sec2800-cfb
 enrollment url http://10.1.103.247:80
 serial-number none
 fqdn none
 ip-address none
 subject-name cn=sec2800-cfb
 revocation-check none
 rsakeypair sec2800-cfb
```

```
!
crypto pki trustpoint ps-611
 enrollment terminal pem
 subject-name CN=ps-611
 revocation-check none
!
!
crypto pki certificate chain sec2800-cfb
 certificate 02
  308201AC 30820115 A0030201 02020102 300D0609 2A864886 F70D0101 04050030
  15311330 11060355 0403130A 736C6F77 33383030 2D31301E 170D3038 30333039
  31373136 33305A17 0D303930 33303931 37313633 305A3016 31143012 06035504
  03130B73 65633238 30302D63 6662305C 300D0609 2A864886 F70D0101 01050003
  4B003048 024100E3 118E8F15 9D2FDB61 EDA795B1 DC99425C 73E6BC65 C9AE270D
  18524123 53FD79E2 14132298 9A78D88A 8DEEBA9D CCF33A4E 2A12E386 91048431
  E292A5B0 16014102 03010001 A34F304D 300B0603 551D0F04 04030205 A0301F06
  03551D23 04183016 80141E6E 7779EEEC EB38ED13 534EC8B2 DB5B35F8 B241301D
  0603551D 0E041604 14694EFD 66E1E1D7 5BAB7F00 2A2CDE23 CCE58D4D 09300D06
  092A8648 86F70D01 01040500 03818100 0B51AC95 EA362BD6 4FD38CC8 C70614FE
  74A5E161 511C3AAB CBE2200C 6E1357AE DC59911A AAA3B53B 280F5EF7 2374BF45
  6574E675 C6590767 7B281C53 A890E40B 0E24DEA7 3E15CA79 C066D478 60406495
  8B308540 77DA5C51 72F8002C 4E19BD65 BF7269B0 29C14433 D91AE773 BB11040F
  20EA42F5 BA3021B3 6479FBF9 D94CC407
        quit
 certificate ca 01
  30820203 3082016C A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  15311330 11060355 0403130A 736C6F77 33383030 2D31301E 170D3038 30333039
  31373039 30315A17 0D313130 33303931 37303930 315A3015 31133011 06035504
  03130A73 6C6F7733 3830302D 3130819F 300D0609 2A864886 F70D0101 01050003
  818D0030 81890281 8100CC33 AC934AE8 C14D92DD E1DB6224 89F73AD2 26FBDB03
  FB2F9A97 07817BCC DF47413F 04310C37 0CA02435 AB92C9FB 32088007 85EFFDDE
  B2FED7D5 A35CFAAF 4986B87F AF9C5B4E 076E8DE1 519D0DD7 6C71588D 079B4640
  EA9805E4 51793023 5C2DBB45 18DD77BF 5ED443C7 079FD057 497B5FA4 C7D77D95
  B3EB63D7 0473B827 E6C90203 010001A3 63306130 0F060355 1D130101 FF040530
  030101FF 300E0603 551D0F01 01FF0404 03020186 301F0603 551D2304 18301680
  141E6E77 79EEECEB 38ED1353 4EC8B2DB 5B35F8B2 41301D06 03551D0E 04160414
  1E6E7779 EEECEB38 ED13534E C8B2DB5B 35F8B241 300D0609 2A864886 F70D0101
  04050003 81810049 3AA6B14F 86C49FC4 4AF9A235 87B4AA90 B6617980 720CE2D0
  1E69719F 9B933051 7FE1BF14 D48B5741 F7ABC51C F2F46C75 480C951A 98252580
  42028CB2 713031F2 1BA9ECCE B42798A9 D7A4C8CB 92B45C4A 1C0CFF3F 1D47C551
  BB2AD9B8 1022F05A B0404EEC B6495105 0A4203E4 93D7C2F7 1B77C7D4 F6EFD414
  644C612D BB8438
        quit
crypto pki certificate chain ps-611
 certificate ca 43721CB69965859C
  30820210 30820179 A0030201 02020843 721CB699 65859C30 0D06092A 864886F7
  0D010105 05003011 310F300D 06035504 03130670 732D3631 31301E17 0D303830
  33303532 33343633 375A170D 31333033 30353233 34363337 5A301131 0F300D06
  03550403 13067073 2D363131 30819F30 0D06092A 864886F7 0D010101 05000381
  8D003081 89028181 00CB52A8 3B6E7CEE 90EAE54E C8A876A9 1E089F2A D29EE685
  09A70AB8 C4974915 78ECFCF0 318AC510 899AA401 88440791 8A1FBFC1 1FCF0727
  A8A7F937 840790DD B87D958E 551DD4EA 209CA0E3 8D7D5F19 B2A48490 EC392805
  274D76C9 1E624D30 55FA6FB5 7C07D4D0 14A0C54B E1B478CB AA1BA644 FF528245
  E30BEB70 8844899A 3F020301 0001A371 306F300B 0603551D 0F040403 0202BC30
  27060355 1D250420 301E0608 2B060105 05070301 06082B06 01050507 03020608
  2B060105 05070305 30180603 551D1104 11300F86 0D736970 3A434E3D 70732D36
  3131301D 0603551D 0E041604 140022A7 15A36D80 5AD42DDF 552A1BE5 E9505E19
  3A300D06 092A8648 86F70D01 01050500 03818100 AF16B927 BEA287C4 11FCF90D
  6EB7D31E 0F78AF93 A582EDDC 451B34EA 0152A9A6 34FA8E59 9B87BCD8 F084478A
  8F2D9B0C 12F27C79 61CAC398 7890D66E 3D13C6CD 440050F9 EE67B6F9 CEC569CA
  006598DC 6788BCD6 8FDF6C19 4B04723B BC652932 C45C41E2 C282C4DB AFDA475E
  79FACE13 C99179A3 B1FC9822 BD3CCAD7 6A864C8F
        quit
!
```

```
!
!
!
username pslow password *****
archive
 log config
  hidekeys
!
!
controller T1 0/2/0
 framing esf
 linecode b8zs
!
controller T1 0/2/1
 framing esf
 linecode b8zs
!
ip ssh version 1
!
!
!
!
interface GigabitEthernet0/0
 ip address 10.1.20.29 255.255.255.0
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/0 10.1.20.1
!
!
ip http server
no ip http secure-server
!
!
!
!
!
!
tftp-server flash:sec2800-cfb.ca
tftp-server flash:sec2800-cfb.crt
!
control-plane
!
!
!
!
!
sccp local GigabitEthernet0/0
sccp ccm 10.1.69.61 identifier 58 version 6.0 trustpoint ps-611
sccp
!
sccp ccm group 59
 associate ccm 58 priority 2
 associate profile 57 register sec2800-cfb
!
dspfarm profile 57 conference security
 trustpoint sec2800-cfb
 codec g711ulaw
```

```
 codec g711alaw
 codec g729ar8
 codec g729abr8
 codec g729r8
 codec g729br8
 maximum sessions 2
 associate application SCCP
!
!
!
!
!
line con 0
line aux 0
line vty 0 4
!
scheduler allocate 20000 1000
ntp clock-period 17180179
ntp server 10.1.108.15

!
webvpn cef
!
end
```

External Certificate Authority Router: Example

```
Router# show running-config
Building configuration...

Current configuration : 3017 bytes
!
! Last configuration change at 14:14:12 EDT Sun Mar 9 2008 by pslow
! NVRAM config last updated at 14:14:14 EDT Sun Mar 9 2008 by pslow
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname slow3800-1
!
boot-start-marker
boot-end-marker
!
enable secret 5 BLAH
!
aaa new-model
!
!
aaa authentication login default local
aaa authentication enable default enable
!
!
aaa session-id common
clock timezone EST -5
clock summer-time EDT recurring
no network-clock-participate wic 0
no network-clock-participate wic 1
!
ip cef
```

```
!
!
no ip domain lookup
multilink bundle-name authenticated
!
!
voice-card 0
 no dspfarm
!
!
!
!
crypto pki server slow3800-1
 database level complete
 grant auto
 database url flash:
!
crypto pki trustpoint slow3800-1
 revocation-check crl
 rsakeypair slow3800-1
!
!
crypto pki certificate chain slow3800-1
 certificate ca 01
  30820203 3082016C A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  15311330 11060355 0403130A 736C6F77 33383030 2D31301E 170D3038 30333039
  31373039 30315A17 0D313130 33303931 37303930 315A3015 31133011 06035504
  03130A73 6C6F7733 3830302D 3130819F 300D0609 2A864886 F70D0101 01050003
  818D0030 81890281 8100CC33 AC934AE8 C14D92DD E1DB6224 89F73AD2 26FBDB03
  FB2F9A97 07817BCC DF47413F 04310C37 0CA02435 AB92C9FB 32088007 85EFFDDE
  B2FED7D5 A35CFAAF 4986B87F AF9C5B4E 076E8DE1 519D0DD7 6C71588D 079B4640
  EA9805E4 51793023 5C2DBB45 18DD77BF 5ED443C7 079FD057 497B5FA4 C7D77D95
  B3EB63D7 0473B827 E6C90203 010001A3 63306130 0F060355 1D130101 FF040530
  030101FF 300E0603 551D0F01 01FF0404 03020186 301F0603 551D2304 18301680
  141E6E77 79EEECEB 38ED1353 4EC8B2DB 5B35F8B2 41301D06 03551D0E 04160414
  1E6E7779 EEECEB38 ED13534E C8B2DB5B 35F8B241 300D0609 2A864886 F70D0101
  04050003 81810049 3AA6B14F 86C49FC4 4AF9A235 87B4AA90 B6617980 720CE2D0
  1E69719F 9B933051 7FE1BF14 D48B5741 F7ABC51C F2F46C75 480C951A 98252580
  42028CB2 713031F2 1BA9ECCE B42798A9 D7A4C8CB 92B45C4A 1C0CFF3F 1D47C551
  BB2AD9B8 1022F05A B0404EEC B6495105 0A4203E4 93D7C2F7 1B77C7D4 F6EFD414
  644C612D BB8438
        quit
!
!
username pslow password 7 BLAH
archive
 log config
  hidekeys
!
!
controller T1 0/0/0
 framing esf
 linecode b8zs
!
controller T1 0/0/1
 framing esf
 linecode b8zs
!
controller T1 0/1/0
 framing esf
 linecode b8zs
!
controller T1 0/1/1
 framing esf
```

```
 linecode b8zs
!
!
!
interface GigabitEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
 media-type rj45
 no keepalive
!
interface GigabitEthernet0/1
 ip address 10.1.103.247 255.255.255.0
 duplex auto
 speed auto
 media-type rj45
 no keepalive
!
ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/1 10.1.103.1
!
!
ip http server
no ip http secure-server
!
!!
control-plane
!
!
line con 0
line aux 0
line vty 0 4
!
scheduler allocate 20000 1000
ntp clock-period 17179581
ntp server 10.18.108.15
!
end
```

Additional References

The following sections provide references related to the Media and Signaling Encryption (SRTP/TLS) on DSP Farm Conferencing feature.

Related Documents

Related Topic	Document Title
Cisco Unified Communications Manager interoperability	*Cisco CallManager and Cisco IOS Interoperability Guide*
Cisco IOS H.323 network secure calls	• *Media and Signaling Authentication and Encryption Feature for Cisco IOS H.323 Gateways*
Cisco Unified CME configuration	• *Cisco Unified CallManager Express System Administrator Guide* • *Cisco Unified CallManager Express Command Reference*
Cisco IOS voice configuration	• *Cisco IOS Voice Configuration Library* • *Cisco IOS Voice Command Reference*
Phone documentation for Cisco Unified CME	• User Guides
Cisco Unified CM security configuration	*Cisco CallManager Security Guide,* Release 5.0
Cisco Unified CME and Cisco Unity Express integration	*Integrating Cisco Unity Express with Cisco CallManager Express 3.0 and Later*

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIB	MIBs Link
CISCO-CCME-MIB MIB CISCO-VOICE-DIAL-CONTROL-MIB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

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

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Voice Command Reference* at http://www.cisco.com/en/US/docs/ios/voice/command/reference/vr_book.html. For information about all Cisco IOS commands, use the Command Lookup Tool at http://tools.cisco.com/Support/CLILookup or a Cisco IOS master commands list.

- **dspfarm profile**
- **show sccp**
- **trustpoint (DSP Farm profile)**

Feature Information for Media and Signaling Encryption (SRTP/TLS) on DSP Farm Conferencing

Table 1 lists the release history for this feature.

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 for Media and Signaling Encryption (SRTP/TLS) on DSP Farm Conferencing

Feature Name	Releases	Feature Information
Media and Signaling Encryption (SRTP/TLS) on DSP Farm Conferencing	12.4(11)XW1 12.4(20)T	The Media and Signaling Encryption (SRTP/TLS) on DSP Farm Conferencing feature provides secure conferencing capability for Unified CM networks, that includes authentication, integrity, and encryption of voice media and related call control signaling to and from the digital signal processor (DSP) farm. This feature was introduced in Cisco IOS Release 12.4(11)XW1 and integrated into Release 12.4(20)T.