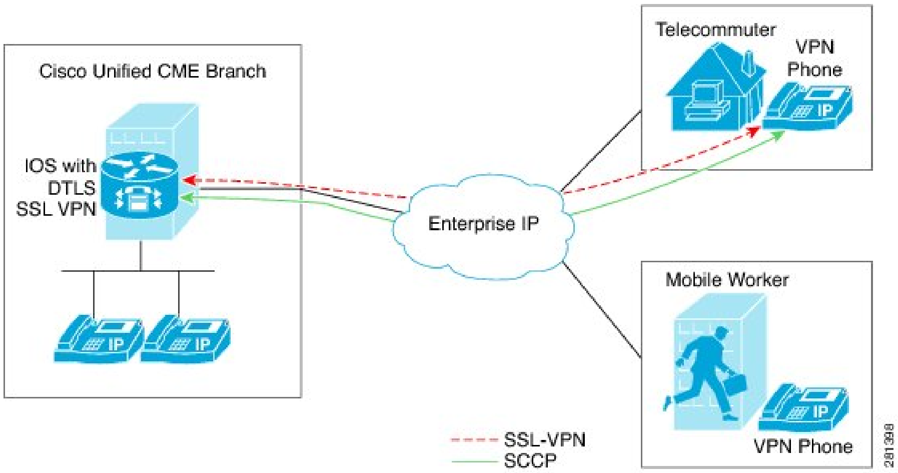
SSL VPN Client for SCCP IP Phones

Information About SSL VPN Client

SSL VPN Support on Cisco Unified CME with DTLS

In Communications Manager Express 8.6 and later versions, Cisco Unified SCCP IP phones such as 7945, 7965, and 7975 located outside of the corporate network are able to register to Cisco Unified CME through an SSL VPN connection. The SSL VPN connection is set up between a phone and a VPN headend. The VPN headend can either be an Adaptive Secure Appliance (ASA 5500) or the Datagram Transport Layer Security (DTLS) enabled IOS SSL VPN router, see Figure 1: VPN connection between Cisco Unified IP Phone and VPN head ends (ASA and DTLS), on page 1. Support for VPN feature on ASA headend was added in Cisco Unified CME 8.5. For more information, see SSL VPN Client for SCCP IP Phones, on page 1.

Figure 1: VPN connection between Cisco Unified IP Phone and VPN head ends (ASA and DTLS)



Cisco Unified CME 8.6 uses IOS SSL DTLS as a headend or gateway. To establish a VPN connection between a phone and a VPN head end, the phone must be configured with VPN configuration parameters. The VPN configuration parameters include VPN head end addresses, VPN head end credentials, user or phone ID, and credential policy. These parameters are considered as sensitive information and must be delivered in a secure environment using a signed configuration file or a signed and encrypted configuration file. The phone is required to be provisioned within the corporate network before the phone can be placed outside the corporate network.

After the phone is “staged” in a trusted environment, the phone can be deployed to a location where a VPN head end can be connected. The VPN configuration parameters for the phone dictate the user interface and behavior of the phone.

Phone or Client Authentication

Phone authentication is required to verify that the remote phone trying to register with Cisco Unified CME via, VPN DTLS is a legitimate phone. Phone or client authentication can be done with the following types of authentication:

1. Username and Password Authentication.

2. Certificate-based authentication (where the phone's authentication is done using the LSC or MIC certificate on the phone). The certificated-based authentication consists of two levels:

    - Certificate only Authentication - Where only the LSC of the phone is used (the user is not required to enter a username or password on the phone.)

    - Certification with AAA or two-factor - Where the LSC of the phone and username and password combination is used to authenticate phone. Two-factor authentication can be performed with or without the username prefill. (With the username prefilled, the phone does not ask for a username and a username is picked up depending on the configuration under the relevant trustpoint.)

Note We recommend using LSC for certificate authentication. Use of MIC for certificate authentication is not recommended. We also recommend configuring ephone in “authenticated” (not encrypted) security mode when doing certificate authentication. More information on certificate-only authentication and two-factor authentication is available at the following location: https://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_ssl_vpn_ps6350_TSD_Products_Configuration_Guide_Chapter.html#wp1465191.

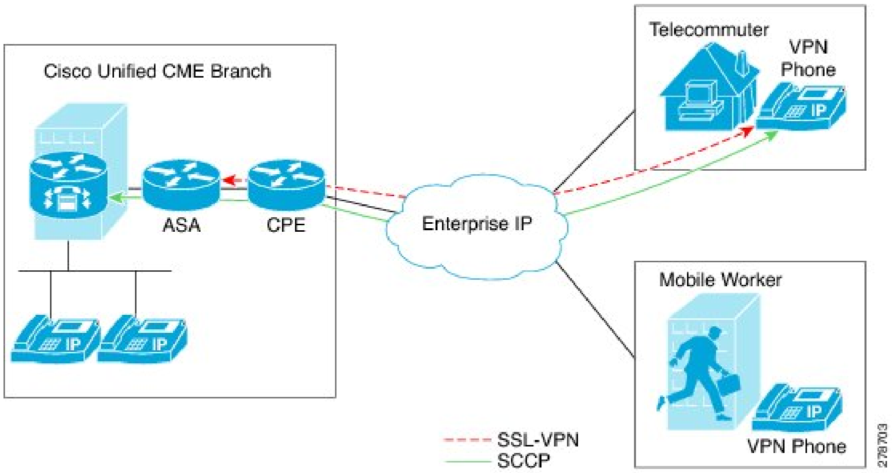
You can set up Cisco Unified CME with an encrypted mode, but encrypted SCCP phone has limited media call-flow support. Using a phone with authenticated mode does not have any media-related call-flow limitations.

SSL VPN Client Support on SCCP IP Phones

Cisco Unified CME 8.5 and later versions support Secure Sockets Layer (SSL) Virtual Private Network (VPN) on SCCP IP phones such as 7945, 7965, and 7975.

In Cisco Unified CME 8.5, SCCP IP phones outside of the corporate network can register with the Cisco Unified CME 8.5 through a VPN connection as shown in Figure 2: Connection between a phone and a VPN head end, on page 3.

Figure 2: Connection between a phone and a VPN head end



An SSL VPN provides secure communication mechanism for data and other information transmitted between two endpoints. The VPN connection is set up between a SCCP IP phone and a VPN head end or VPN gateway. Cisco Unified CME 8.5 uses an Adaptive Security Appliances (ASA model 55x0) as a VPN head end or gateway.

To establish a VPN connection between a phone and a VPN gateway, the phone is required to be configured with VPN configuration parameters such as VPN gateway addresses, VPN head end credentials, user or phone ID, and credential policy. These parameters contain sensitive information and should be delivered in a secure environment using a signed configuration file or a signed and encrypted configuration file. The phone is required to be provisioned within the corporate network before the phone is placed outside the corporate network.

After the phone is provisioned in a trusted secure environment, the phone can be connected to Cisco Unified CME from any location, from where VPN head end can be reached. The VPN configuration parameters for the phone control the user interface and behavior of the phone. For more information on configuring the SSL VPN feature on SCCP IP phones, see Configure ASA (Gateway) as VPN Headend, on page 12.

You need to generate a trustpoint with exportable keys and use that as SAST1. For more information about CME System Administrator Security Token.

Restrictions for Configuring SSL VPN Client for SCCP IP Phones

SSL VPN Client is not supported with Cisco 4000 Series Integrated Services Routers on Unified CME.

Only Site-to-Site VPN configuration is supported on Unified CME.

Configure SSL VPN Client

Configure SSL VPN Client with ASA as VPN Headend

To configure the SSL VPN feature on SCCP IP phones, follow these steps in the order in which they are presented here:

1. Basic Configuration on Cisco Unified CME, on page 4

2. Configure Cisco Unified CME as CA Server, on page 9
3. Verify Phone Registration and Phone Load, on page 12
4. Configure ASA (Gateway) as VPN Headend, on page 12
5. Configure VPN Group and Profile on Cisco Unified CME, on page 16
6. Associate VPN Group and Profile to SCCP IP Phone, on page 17
7. Configure Alternate TFTP Address on Phone, on page 20
8. Register Phone from a Remote Location, on page 21

Prerequisites

- Cisco Unified CME 8.5 or later versions.
- Securityk9 license for ISR-G2 platforms.
- Cisco Unified SCCP IP phones 7942, 7945, 7962, 7965, and 7975 with phone image 9.0 or later.
- ASA 5500 series router with image asa828-7-k8.bin or higher.
- The package anyconnect-win-2.4.1012-k9.pkg is required for configuring the SSLVPN feature but would not be downloaded to the phone.
- You must request the appropriate ASA licenses (AnyConnect for Cisco VPN Phone) to be installed on an ASA in order to allow the VPN client to connect. Go to: `www.cisco.com/go/license` and enter the PAK and the new activation key will be e-mailed back to you.

Note A compatible Adaptive Security Device Manager (ASDM) Image is required if configuring through ASDM.

Basic Configuration on Cisco Unified CME

The following steps are basic Cisco Unified configuration allowing the SSL VPN feature to be built on:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip dhcp pool** *pool-name*
4. **network** *ip-address* [*mask* | *prefix-length*]
5. **option 150 ip** *ip-address*
6. **default-router** *ip-address*
7. **exit**
8. **telephony-service**
9. **max-ephones** *max-phones*
10. **max-dn** *max-directory-numbers* [**preference** *preference-order*] [**no-reg primary** | **both**]
11. **ip source-address** *ip-address* **port** *port* [**any-match** | **strict-match**]
12. **cnf-file** {**perphone**}

13. **load** [*phone-type firmware-file*]
14. **no shutdown**
15. **exit**
16. **ephone-dn** *dn-tag* [dual-line]
17. **number** *number* [**secondary** *number*] [**no-reg** [**both** | **primary**]]
18. **ephone** *phone-tag*
19. **description** *string*
20. **device-security-mode**{**authenticated** | **none** | **encrypted**}
21. **mac-address** *mac-address*
22. **type** phone-type [addon 1 module-type [2 module-type]]
23. **button** *button-number* {separator}dn-tag [,dn-tag...] [button-number{x}overlay-button-number] [button-number...]
24. **exit**
25. **telephony-service**
26. **create cnf-files**
27. **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	**ip dhcp pool** *pool-name* **Example:** `Router(config)# ip dhcp pool mypool`	Creates a name for the DHCP server address pool and enters DHCP pool configuration mode. **Note** If you have already configured DHCP IP Address Pool, then skip Step 2 to Step 7 and continue from Step 8.
Step 4	**network** *ip-address* [*mask* | *prefix-length*] **Example:** `Router(config-dhcp)#network 192.168.11.0 255.255.255.0`	Specifies the IP address of the DHCP address pool to be configured.
Step 5	**option 150 ip** *ip-address* **Example:** `Router(config-dhcp)# option 150 ip 192.168.11.1`	Specifies the TFTP server address from which the Cisco Unified IP phone downloads the image configuration file. • This is your Cisco Unified CME router's address.

	Command or Action	Purpose
Step 6	**default-router** *ip-address* **Example:** `Router(config-dhcp)# default router 192.168.11.1`	(Optional) Specifies the router that the IP phones will use to send or receive IP traffic that is external to their local subnet. • If the Cisco Unified CME router is the only router on the network, this address should be the Cisco Unified CME IP source address. This command can be omitted if IP phones need to send or receive IP traffic only to or from devices on their local subnet. • The IP address that you specify for default router will be used by the IP phones for fallback purposes. If the Cisco Unified CME IP source address becomes unreachable, IP phones will attempt to register to the address specified in this command.
Step 7	**exit** **Example:** `Router(config-dhcp)# end`	Exits DHCP pool configuration mode.
Step 8	**telephony-service** **Example:** `Router(config)# telephony-service`	Enters telephony-service configuration mode.
Step 9	**max-ephones** *max-phones* **Example:** `Router(config-telephony)# max-ephones 24`	Sets the maximum number of phones that can register to Cisco Unified CME. • Maximum number is platform and version-specific. Type **?** for range. • In Cisco Unified CME 7.0/4.3 and later versions, the maximum number of phones that can register is different than the maximum number of phones that can be configured. The maximum number of phones that can be configured is 1000. • In versions earlier than Cisco Unified CME 7.0/4.3, this command restricted the number of phones that could be configured on the router.
Step 10	**max-dn** *max-directory-numbers* [**preference** *preference-order*] [**no-reg primary** | **both**] **Example:** `Router(config-telephony)# max-dn 24 no-reg primary`	Limits number of directory numbers to be supported by this router. • Maximum number is platform and version-specific. Type ? for value.
Step 11	**ip source-address** *ip-address* **port** *port* [**any-match** | **strict-match**] **Example:**	Identifies the IP address and port number that the Cisco Unified CME router uses for IP phone registration.

	Command or Action	Purpose
	`Router(config-telephony)# ip source-address 192.168.11.1 port 2000`	• **port** *port*—(Optional) TCP/IP port number to use for SCCP. Range is 2000 to 9999. Default is 2000. • **any-match**—(Optional) Disables strict IP address checking for registration. This is the default. • **strict-match**—(Optional)) Instructs the router to reject IP phone registration attempts if the IP server address used by the phone does not exactly match the source address.

Step 12	**cnf-file**{**perphone**}
	Example:
	`Router(config-telephony)#xnf-file perphone`
		Specifies that system generate a separate configuration XML file for each IP phone.
		• Separate configuration files for each endpoint are required for security.
		Note You must configure the cnf-file (perphone) command to generate a separate XML file for each phone.

Step 13	**load** [*phone-type firmware-file*] **Example:** `Router(config-telephony)# load 7965 SCCP45.9-0-1TD1-36S.loads`	Associates a phone type with a phone firmware file. You must use the complete filename, including the file suffix, for phone firmware versions later than version 9.0 for all phone types load 7965 SCCP45.9-0-1TD1-36S
Step 14	**no shutdown** **Example:** `Router(config-telephony)# no shutdown`	Allows to enable SCCP service listening socket.
Step 15	**exit** **Example:** `Router(config-telephony)# end`	Exits telephony-service configuration mode.
Step 16	**ephone-dn** *dn-tag* [dual-line] **Example:** `Router(config)# ephone-dn 1`	Enters ephone dn configuration mode to define a directory number for an IP phone, intercom line, voice port, or a message-waiting indicator (MWI). • *dn-tag*—identifies a particular directory number during configuration tasks. Range is 1 to the maximum number of directory numbers allowed on the router platform. Type **?** to display the range.
Step 17	**number** *number* [**secondary** *number*] [**no-reg** [**both** | **primary**]] **Example:** `Router(config-ephone-dn)# number 1001`	Associates an extension number with this directory number. • *number*—String of up to 16 digits that represents an extension or E.164 telephone number.

	Command or Action	Purpose
Step 18	**ephone** *phone-tag* **Example:** `Router(config)# ephone 1`	Enters ephone configuration mode to set ephone specific parameters. • *phone-tag*—Unique sequence number that identifies the phone. Range is version and platform-dependent; type **?** to display range.
Step 19	**description** *string* **Example:** `Router(config-ephone)description SSL VPN Remote Phone`	Ephone descriptions for network management systems using an eXtensible Markup Language (XML) query. • *string*—Allows for a maximum of 128 characters, including spaces. There are no character restrictions.

Step 20	**device-security-mode** { **authenticated** | **none** | **encrypted** }
	Example:
	`Router(config-ephone)# device-security-mode none`
		Allows to set the security mode for SCCP signaling for devices communicating with the Cisco Unified CME router globally or per ephone.
		• authenticated— SCCP signaling between a device and Cisco Unified CME through the secure TLS connection on TCP port 2443.
		• none— SCCP signaling is not secure.
		• encrypted — SCCP signaling between a device and Cisco Unified CME through the secure TLS connection on TCP port 2443, and the media uses Secure Real-Time Transport Protocol (SRTP).

Step 21	**mac-address** *mac-address* **Example:** `Router(config-ephone)# mac-address 0022.555e.00f1`	Associates the MAC address of a Cisco IP phone with an ephone configuration in a Cisco Unified CME system • *mac-address*—identifying MAC address of an IP phone, which is found on a sticker located on the bottom of the phone.
Step 22	**type** phone-type [addon 1 module-type [2 module-type]] **Example:** `Router(config-ephone)# type 7965`	Specifies the type of phone. • Cisco Unified CME 4.0 and later versions—The only types to which you can apply an add-on module are 7960, 7961, 7961GE, and 7970.
Step 23	**button** *button-number* { separator } dn-tag [,dn-tag...] [button-number { x } overlay-button-number] [button-number...] **Example:** `Router(config-ephone)# button 1:1`	Associates a button number and line characteristics with an ephone-dn. Maximum number of buttons is determined by phone type.
Step 24	**exit** **Example:** `Router(config-ephone)#exit`	Exits ephone configuration mode.

	Command or Action	Purpose
Step 25	**telephony-service** **Example:** `Router(config)telephony-service`	Enters telephony-service configuration mode.
Step 26	**create cnf-files** **Example:** `Router(config-telephony)# create cnf-files`	Builds XML configuration files required for SCCP phones.

Step 27	**end**
	Example:
	`Router(config-telephony)# end`
		Returns to privileged EXEC mode.

Configure Cisco Unified CME as CA Server

The basic configuration on the CA server ensures IP connectivity, Network Time Protocol (NTP), time synchronization which are necessary for enabling the SSL VPN feature.

Though this section describes configuring CA server on the CME to provide certificate signing for both CME and ASA, in real world deployments third party CA is often used. The basic requirement is that CME and ASA each has an identity certificate signed by the third party CA, and both CME and ASA share the same CA certificate. That is, each device has a trustpoint containing the same CA certificate as well as an identity certificate signed by the same CA.

To configure the CA server, follow these steps:

Step 1 Configure IP Address, NTP and HTTP Server on your Cisco Unified CME router:

Example:

```
Router(config)# Interface GigabitEthernet0/0
Router(config-if)# no ip address
Router(config-if)# interface GigabitEthernet0/0.10
Router(config-subif)# description DATA VLAN
Router(config-subif)# encapsulation dot1Q 10 native
Router(config-subif)# ip address 192.168.10.1 255.255.255.0

Router(config)# interface GigabitEthernet0/0.11
Router(config-subif)# description VOICE VLAN
Router(config-subif)# encapsulation dot1Q 11
Router(config-subif)# ip address 192.168.11.1 255.255.255.0

Router(config)# interface GigabitEthernet0/1
Router(config-if)# description INTERFACE CONNECTED TO ASA
Router(config-if)# ip address 192.168.20.1 255.255.255.0

Router(config)# ! Default router is ASA Inside Interface
Router(config)# ip route 0.0.0.0 0.0.0.0 192.168.20.254
Router(config)# clock timezone PST -8
Router(config)# clock summer-time PST recurring

Router# ! Set clock to current time
Router# clock set 10:10:00 15 oct 2010
```

```
Router(config)# ntp source GigabitEthernet0/1
Router(config)# ntp master 2

Router(config)# ip http server
Router(config)# ip domain-name cisco.com
```

Note NTP synchronization will fail if you do not set the clock manually to match the time on Cisco Unified CME router.

Step 2 Configure Cisco Unified CME as CA Server. Both CME and ASA will enroll a certificate from the CA Server. The following sample configuration shows Cisco Unified CME being configured as the CA Server:

Example:

```
Router(config)# crypto pki server cme_root
Router(config)# database level complete
Router(cs-server)# database url nvram:
Router(cs-server)# grant auto
Router(cs-server)# lifetime certificate 7305
Router(cs-server)# lifetime ca-certificate 7305
Router(cs-server)# exit

Router(config)# crypto pki trustpoint cme_root
Router(ca-trustpoint)# enrollment url http://192.168.20.1:80
Router(ca-trustpoint)# revocation-check none
Router(ca-trustpoint)# rsakeypair cme_root
Router(cs-server)# exit

Router(config)# crypto pki server cme_root
Router(cs-server)#no shutdown
%Some server settings cannot be changed after CA certificate generation.
% Please enter a passphrase to protect the private key
% or type Return to exit
Password: *****
Re-enter password: ****
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 1 seconds)
Mar 10 16:44:00.576: %SSH-5-ENABLED: SSH 1.99 has been enabled% Exporting Certificate
Server signing certificate and keys...
% Certificate Server enabled.
Router(cs-server)#
Mar 10 16:44:41.812: %PKI-6-CS_ENABLED: Certificate server now enabled.
```

Step 3 Create a second trustpoint, then authenticate the trustpoint and enroll it with CA.

Example:

```
Router(config)# crypto pki trustpoint cme_cert
Router(ca-trustpoint)# enrollment url http://192.168.20.1:80
Router(ca-trustpoint)# revocation-check none
Router(ca-trustpoint)# exit

Router(config)# crypto pki authenticate cme_cert
Certificate has the following attributes:
Fingerprint MD5: 995C157D AABB8EE2 494E7B35 00A75A88
Fingerprint SHA1: F934871E 7E2934B1 1C0B4C9A A32B7316 18A5858F
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
Router(config)# crypto pki enroll cme_cert
%
% Start certificate enrollment ..
% Create a challenge password.
```

```
You will need to verbally provide this password to the CA Administrator in order to revoke
your certificate. For security reasons your password will not be saved in the
configuration. Please make a note of it.
Password:
Jan 20 16:03:24.833: %CRYPTO-6-AUTOGEN: Generated new 512 bit key pair
Re-enter password:
% The subject name in the certificate will include: CME1.cisco.com
% Include the router serial number in the subject name? [yes/no]: no
% Include an IP address in the subject name? [no]: no
Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
% The 'show crypto pki certificate verbose cme_cert' command will show the fingerprint.
! Verify Certificates
```

Verify Certificates (Optional)

Use the **show crypto pki certificates** command on your Cisco Unified CME router to verify the certificates.

```
Router# sh crypto pki certificates
Certificate
Status: Available
Certificate Serial Number (hex): 07
Certificate Usage: General Purpose
Issuer:
cn=cme_root
Subject:
Name: CME1.cisco.com
hostname=CME1.cisco.com
Validity Date:
start date: 15:32:23 PST Apr 1 2010
end date: 09:44:00 PST Mar 10 2030
Associated Trustpoints: cisco2
Storage: nvram:cme_root#7.cer

Certificate
Status: Available
Certificate Serial Number (hex): 06
Certificate Usage: General Purpose
Issuer:
cn=cme_root
Subject:
Name: CME1.cisco.com
hostname=CME1.cisco.com
Validity Date:
start date: 15:30:11 PST Apr 1 2010
end date: 09:44:00 PST Mar 10 2030
Associated Trustpoints: cisco1
Storage: nvram:cme_root#6.cer

Certificate
Status: Available
Certificate Serial Number (hex): 02
Certificate Usage: General Purpose
Issuer:
cn=cme_root
Subject:
Name: CME1.cisco.com
hostname=CME1.cisco.com
Validity Date:
start date: 08:47:42 PST Mar 10 2010
end date: 09:44:00 PST Mar 10 2030
Associated Trustpoints: cme_cert
Storage: nvram:cme_root#2.cer

CA Certificate
```

```
Status: Available
Certificate Serial Number (hex): 01
Certificate Usage: Signature
Issuer:
cn=cme_root
Subject:
cn=cme_root
Validity Date:
start date: 08:44:00 PST Mar 10 2010
end date: 09:44:00 PST Mar 10 2030
Associated Trustpoints: cisco2 cisco1 cme_cert cme_root
Storage: nvram:cme_root#1CA.cer
```

Verify Phone Registration and Phone Load

Step 1 Use the **show ephone** command to verify the phone registration details.

Example:

```
Router# show ephone

ephone-1[0] Mac:0022.555E.00F1 TCP socket:[2] activeLine:0 whisperLine:0 REGISTERED in SCCP ver 19/17
 max_streams=5 mediaActive:0 whisper_mediaActive:0 startMedia:0 offhook:0 ringing:0 reset:0 reset_sent:0
 paging 0 debug:0 caps:9
IP:192.168.11.4 * 49269 7965 keepalive 0 max_line 6 available_line 6
button 1: cw:1 ccw:(0 0) dn 1 number 1001 CH1   IDLE CH2   IDLE
Preferred Codec: g711ulaw
Lpcor Type: none
```

Note Make sure the phone has the right phone firmware and verify if the phone registers locally with Cisco Unified CME.

Step 2 Use the **show ephone phone load** command to verify phone load.

Example:

```
Router# show ephone phoneload

DeviceName        CurrentPhoneload       PreviousPhoneload LastReset

SEP0016C7EF9B13    9.0(1TD1.36S)          9.0(1TD1.36S) UCM-closed-TCP
```

Configure ASA (Gateway) as VPN Headend

In this section ASA will be configured to authenticate and enroll a certificate from CME CA server. The fingerprint of the CA certificate will be the same as the CME root certificate, so that the phone can authenticate the certificates sent from ASA during TLS negotiation against the hash it has in store.

Step 1 Configure Interfaces, IP Routing, and NTP.

Example:

```
ciscoasa(config)# Interface Ethernet0/1
ciscoasa(config-if)# nameif Inside
ciscoasa(config-if)# description INTERFACE CONNECTED TO CUCME
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 192.168.20.254 255.255.255.0

ciscoasa(config)# interface Ethernet 0/0
ciscoasa(config-if)# description INTERFACE CONNECTED TO WAN
ciscoasa(config-if)# nameif Outside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address 9.10.60.254 255.255.255.0
ciscoasa(config)# router ospf 100
ciscoasa(config-router)# network 9.10.60.0 255.255.255.0 area 1

ciscoasa(config-if)# ntp server 192.168.20.1
```

Step 2 Create Trustpoint on ASA and obtain CME (CA) Certificate.

Example:

```
ciscoasa(config)# crypto key generate rsa label cmeasa
ciscoasa(config)# crypto ca trustpoint asatrust
ciscoasa(config)# ! Enrollment URL = CA Server = CUCME
ciscoasa(config-ca-trustpoint)# enrollment url http://192.168.20.1:80
ciscoasa(config-ca-trustpoint)# subject-name cn=cmeasa.cisco.com
ciscoasa(config-ca-trustpoint)# crl nocheck
ciscoasa(config-ca-trustpoint)# keypair cmeasa

ciscoasa (config)# crypto ca authenticate asatrust
INFO: Certificate has the following attributes:
Fingerprint: 27d00cdf 1144c8b9 90621472 786da0cf
Do you accept this certificate? [yes/no]: yes
! Enroll the Trustpoint
ciscoasa(config)# crypto ca enroll asatrust
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
password to the CA Administrator in order to revoke your certificate.
For security reasons your password will not be saved in the configuration.
Please make a note of it.
Password: ********
Re-enter password: ********
% The subject name in the certificate will be: cn=cmeasa.cisco.com
% The fully-qualified domain name in the certificate will be: ciscoasa.cisco.com
% Include the device serial number in the subject name? [yes/no]: no
Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
ciscoasa(config)# The certificate has been granted by CA!
ciscoasa# show crypto ca certificates
```

Step 3 Verify Certificates (optional)

Use the **show crypto ca certificate** command on your ASA router to verify the certificates.

Example:

```
ciscoasa# show crypto ca certificate
Certificate
Status: Available
Certificate Serial Number: 03
Certificate Usage: General Purpose
Public Key Type: RSA (1024 bits)
Issuer Name:
```

```
cn=cme_root
Subject Name:
hostname=ciscoasa.cisco.com
cn=cmeasa.cisco.com
Validity Date:
start date: 09:04:40 PST Mar 10 2010
end date: 08:44:00 PST Mar 10 2030
Associated Trustpoints: asatrust

CA Certificate
Status: Available
Certificate Serial Number: 01
Certificate Usage: Signature
Public Key Type: RSA (1024 bits)
Issuer Name:
cn=cme_root
Subject Name:
cn=cme_root
Validity Date:
start date: 08:44:00 PST Mar 10 2010
end date: 08:44:00 PST Mar 10 2030
Associated Trustpoints: asatrust
```

Step 4 Configure SSL Parameters.

Example:

```
ciscoasa(config)# ssl encryption 3des-sha1 aes128-sha1 aes256-sha1 des-sha1 null-sha1
ciscoasa(config)#
ciscoasa(config)# ssl trust-point asatrust
ciscoasa(config)# ssl trust-point asatrust inside
ciscoasa(config)# ssl trust-point asatrust outside
ciscoasa(config)# no ssl certificate-authentication interface outside port 443
ciscoasa(config)# ssl certificate-authentication interface inside port 443
```

Step 5 Configure local IP address pool.

Example:

```
ciscoasa(config)# ip local pool SSLVPNphone_pool 192.168.20.50-192.168.20.70 mask
255.255.255.0
```

Step 6 Configure Access List to prevent NAT traffic via VPN.

Example:

```
ciscoasa(config)# access-list no_nat_to_vpn extended permit ip any 9.10.60.0 255.255.255.0
ciscoasa(config)# ! 9.10.60.0/24 is the Outside subnet
ciscoasa(config)# nat (inside) 0 access-list no_nat_to_vpn
```

Step 7 Configure VPN. Follow this link for information on configuring VPN: http://www.cisco.com/en/US/docs/security/asa/asa82/configuration/guide/svc.html.

Example:

```
ciscoasa(config-webvpn)# enable inside
INFO: WebVPN and DTLS are enabled on 'Inside'.
ciscoasa(config-webvpn)# enable outside
INFO: WebVPN and DTLS are enabled on 'Outside'.
ciscoasa(config-webvpn)# svc image disk0:/anyconnect-win-2.4.1012-k9.pkg 1
ciscoasa(config-webvpn)# svc enable
ciscoasa(config-webvpn)# group-policy SSLVPNphone internal
ciscoasa(config)# group-policy SSLVPNphone attribute
ciscoasa(config-group-policy)# banner none
ciscoasa(config-group-policy)# vpn-simultaneous-logins 10
ciscoasa(config-group-policy)# vpn-idle-timeout none
ciscoasa(config-group-policy)# vpn-session-timeout none
ciscoasa(config-group-policy)# vpn-tunnel-protocol svc webvpn
ciscoasa(config-group-policy)# address-pools value SSLVPNphone_pool
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# svc dtls enable
ciscoasa(config-group-webvpn)# svc keepalive 120
ciscoasa(config-group-webvpn)# svc ask none
ciscoasa(config-group-webvpn)#
```

Step 8 Configure SSL VPN tunnel. For more information, see http://www.cisco.com/en/US/docs/security/asa/asa82/configuration/guide/vpngrp.html.

Example:

```
ciscoasa(config)# tunnel-group SSLVPN_tunnel type remote-access
ciscoasa(config)# tunnel-group SSLVPN_tunnel general-attributes
ciscoasa(config-tunnel-general)#
ciscoasa(config-tunnel-general)#
ciscoasa(config-tunnel-general)# address-pool SSLVPNphone_pool
ciscoasa(config-tunnel-general)# default-group-policy SSLVPNphone
ciscoasa(config-tunnel-general)# tunnel-group SSLVPN_tunnel webvpn-attributes
ciscoasa(config-tunnel-webvpn)# group-url https://9.10.60.254/SSLVPNphone enable
```

Step 9 Enable static route to Cisco Unified CME voice VLAN. For more information, see http://www.cisco.com/en/US/docs/security/asa/asa82/configuration/guide/route_static.html.

Example:

```
ciscoasa(config)# route Inside 192.168.11.0 255.255.255.0 192.168.20.254 1
```

Step 10 Configure the ASA local database for users. For more information, see http://www.cisco.com/en/US/docs/security/asa/asa82/configuration/guide/access_aaa.html#wpmkr108.

Example:

```
ciscoasa(config)# username anyone password cisco
ciscoasa(config)# ! These credentials will be entered on the phone to log in.
ciscoasa(config)# username anyone attributes
ciscoasa(config-username)# vpn-group-policy SSLVPNphone
ciscoasa(config-username)# vpn-tunnel-protocol IPSec l2tp-ipsec svc webvpn
ciscoasa(config-username)# webvpn
ciscoasa(config-username-webvpn)# svc dtls enable
ciscoasa(config-username-webvpn)# svc ask none
```

Step 11 Enable Inter-ASA media traffic.

Example:

```
ciscoasa(config)# same-security-traffic permit inter-interface
ciscoasa(config)# same-security-traffic permit intra-interface
```

Configure VPN Group and Profile on Cisco Unified CME

In this section a VPN-group is configured which dictates the VPN gateway IP address, certificate hash algorithm and certificate trustpoint for phones. This information will be added to phone configuration later. To configure VPN group and profile on Cisco Unified CME, follow these steps:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **vpn-group** *tag*
5. **vpn-gateway** [*number* | **url**]
6. **vpn-trustpoint** {[*number* [**raw** | **trustpoint**]}
7. **vpn-hash-algorithm** *sha-1*
8. **exit**
9. **vpn-profile** *tag*
10. **host-id-check** [**enable** | **disable**]
11. **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	**voice service voip** **Example:** `Router(config)#voice service voip`	Enters voice over IP configuration mode.
Step 4	**vpn-group** *tag* **Example:** `Router (conf-voi-serv)#vpn-group 1`	Enters vpn-group mode under voice over IP configuration mode. • *tag*—vpn-group tag. Range: 1 or 2.
Step 5	**vpn-gateway** [*number*	**url**] **Example:** `Router(conf-vpn-group)#vpn-gateway 1 https://9.10.60.254/SSLVPNphone`	Allows you to define gateway url for vpn. • *number*—number—Number of gateways that can be defined as a vpn-gateway. Range is from 1 to 3. • *url*—VPN-gateway url. SSLVPNphone is the VPN group policy configured on ASA.
Step 6	**vpn-trustpoint** {[*number* [**raw**	**trustpoint**]}	Allows you to enter a vpn-gateway trustpoint.

	Command or Action	Purpose
	Example: `Router(conf-vpn-group)#vpn-trustpoint ?vpn-trustpoint 1 trustpoint cme_cert root`	• **number**—Number of trustpoints allowed. Range:1 to 10. • **raw**—allows you to enter vpn-gateway trustpoint in raw format. • **trustpoint**—allows you to enter VPN Gateway trustpoint as created in IOS format. • **root** – Since the CME root certificate has the same hash as ASA's CA certificate, therefore the "root" clause is configured to select the root certificate instead of leaf certificate.
Step 7	**vpn-hash-algorithm** *sha-1* **Example:** `Router(conf-vpn-group)#vpn-hash-algorithm sha-1`	Allows you to enter vpn hash encryption for the trustpoints. • *sha-1*—Encryption algorithm.
Step 8	**exit** **Example:** `Router(conf-vpn-group)#exit`	Exits VPN-group configuration mode.
Step 9	**vpn-profile** *tag* **Example:** `Router (conf-voi-serv)#vpn-profile 1`	Enters VPN-profile configuration mode. *tag*—VPN-profile tag number. Range: 1-6.
Step 10	**host-id-check** [**enable** | **disable**] **Example:** `Router(conf-vpn-profile)#host-id-check disable`	Allows you to configure host id check option in VPN-profile. • disable— Disable host ID check option. • enable— Enable host ID check option. Default is Enable.

Step 11	**end**
	Example:
	`Router(conf-vpn-profile)#end`
		Exits to privileged EXEC mode.

Associate VPN Group and Profile to SCCP IP Phone

To associate VPN group and profile to SCCP IP phones, follow these steps:

SUMMARY STEPS

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

3. **telephony-service**
4. **cnf-file perphone**
5. **ephone** *phone-tag*
6. **device-security-mode** {authenticated | none | encrypted}
7. **mac-address** [mac-address]
8. **type** *phone-type* **addon 1** *[module-type* [**2** *module-type*]]
9. **vpn-group** *tag*
10. **vpn-profile** *tag*
11. **button** *button-number{separator}dn-tag [,dn-tag...][button-number{x}overlay-button-number] [button-number...]*
12. **exit**
13. **telephony-service**
14. **create cnf-file**
15. **exit**
16. **ephone** *phone-tag*
17. **reset**
18. **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	**telephony-service** **Example:** `Router#(config)telephony-service`	Enters telephony-service configuration mode.
Step 4	**cnf-file perphone** **Example:** `Router(config-telephony)# create cnf-files`	Builds the XML configuration files required for IP phones.
Step 5	**ephone** *phone-tag* **Example:** `Router(config)# ephone 1`	Enters ephone configuration mode to set phone-specific parameters for an SCCP phone. • *phone-tag*—Unique sequence number that identifies the phone. Range is version and platform-dependent; type **?** to display range
Step 6	**device-security-mode** {authenticated | none | encrypted} **Example:**	Enables security mode for endpoints.

	Command or Action	Purpose
	`Router(config-telephony)# device-security-mode none`	• authenticated—Instructs device to establish a TLS connection with no encryption. There is no Secure Real-Time Transport Protocol (SRTP) in the media path. • none—SCCP signaling is not secure. This is the default. • encrypted—Instructs device to establish an encrypted TLS connection to secure media path using SRTP. • The value set for this command in ephone configuration mode has priority over the value set in telephony-service configuration mode.
Step 7	**mac-address** [mac-address] **Example:** `Router(config-ephone)#mac-address 0022.555e.00f1`	Specifies the MAC address of the IP phone that is being configured
Step 8	**type** *phone-type* **addon 1** *[module-type* [**2** *module-type*]] **Example:** `Router(config-ephone)# type 7965`	Specifies the type of phone. • Cisco Unified CME 4.0 and later versions—The only types to which you can apply an add-on module are 7960, 7961, 7961GE, and 7970. • Cisco CME 3.4 and earlier versions—The only type to which you can apply an add-on module is 7960.
Step 9	**vpn-group** *tag* **Example:** `Router (config-ephone)# vpn-group 1`	Enters vpn-group mode under voice over IP configuration mode. • tag—vpn-group tag. Range: 1 or 2.
Step 10	**vpn-profile** *tag* **Example:** `Router (config-ephone)#vpn-profile 1`	Enters VPN-profile configuration mode. • tag—VPN-profile tag number. Range: 1-6.
Step 11	**button** *button-number{separator}dn-tag [,dn-tag...][button-number{x}overlay-button-number] [button-number...]* **Example:** `Router(config-ephone)# button 1:5`	Associates a button number and line characteristics with an ephone-dn. Maximum number of buttons is determined by phone type.
Step 12	**exit** **Example:** `Router(config-ephone)exit`	Exits ephone configuration mode.
Step 13	**telephony-service** **Example:**	Enters telephony-service configuration mode.

	Command or Action	Purpose
	`Router(config)# telephony-service`	
Step 14	**create cnf-file** **Example:** `Router(config-telephony)# create cnf-files`	Builds the XML configuration files required for IP phones. It is recommended to first clear the existing config files using "no create cnf-files" and then create again.
Step 15	**exit** **Example:** `Router(Config-telephony)exit`	Exits telephony service configuration mode.
Step 16	**ephone** *phone-tag* **Example:** `Router(config)# ephone 1`	Enters ephone configuration mode. • *phone-tag*—Unique sequence number that identifies this ephone during configuration tasks.
Step 17	**reset** **Example:** `Router(config-ephone)# reset`	Performs a complete reboot of the individual SCCP phone being configured.

Step 18	**end**
	Example:
	`Router(config-ephone)# end`
		Exits to privileged EXEC mode.

Configure Alternate TFTP Address on Phone

Step 1 From the phone, go to:

Example:

```
Settings > Network Configuration > IPv4 Configuration > Alternate TFTP

Press **# to unlock
Select YES

If the phone is already registered, "TFTP Server 1" will already be populated. Otherwise, enter the
 CUCME address as the alternate TFTP Server 1.
```

Step 2 Save the phone configuration.

Step 3 Verify if the VPN is enabled from the phone.

Example:

```
Settings > Security Configuration > VPN

When you press "Enable" from this menu, it should prompt for username and password.
```

Step 4 From the phone, go to:

Example:

```
Settings > Network Configuration > IPv4 Configuration > Alternate TFTP

Press **# to unlock and select YES.
```

```
If the phone is already registered, "TFTP Server 1" will already be populated. Otherwise, enter the
 CUCME address as the alternate TFTP Server 1.
```

Step 5 Save the configuration.

Step 6 Connect the phone to the network from home or a remote location.

Example:

```
Settings > Security Settings > VPN Configurations?

Enable VPN
Enter Username and Password. Phone will register with CUCME.
```

Register Phone from a Remote Location

To register a Cisco Unified IP phone from a remote location, follow these steps:

Step 1 Connect the phone to the network from a home or remote location. Phone receives DHCP.

Step 2 Select **Settings** from the phone menu and go to **Security Settings**.

Step 3 Select **VPN Configurations**. and then select **Enable VPN**.

Step 4 Enter your username and password. Your phone will now register with Cisco Unified CME.

Configure SSL VPN Client with DTLS on Cisco Unified CME as VPN Headend

Before you begin, make sure you have configured the basic SSL VPN configuration on Cisco Unified CME (see Basic Configuration on Cisco Unified CME, on page 4).

To configure the SSL VPN client with DTLS on SCCP IP phones, follow these steps in the order in which they are presented here:

- Set Up the Clock, Hostname, and Domain Name, on page 22
- Configure Trustpoint and Enroll with the Certificates, on page 23
- Configure VPN Gateway, on page 23
- Configure User Database, on page 23
- Configure Virtual Context, on page 24
- Configure Group Policy, on page 24
- Verify the IOS SSL VPN Connection, on page 25
- Configure Cisco Unified SCCP IP Phones for SSL VPN, on page 25
- Configuration on Cisco Unified SCCP IP Phone, on page 26

- Configure SSL VPN on Cisco Unified CME, on page 26

Note Depending upon the type of authentication you choose to configure, configuration steps 3 to step 11 may vary a little from the way they are documented in this section.

Set Up the Clock, Hostname, and Domain Name

The clock, hostname, and domain name must be set up.

Step 1 The following example shows the hostname and domain name configured:

Example:

```
hostname Router2811
ip domain name cisco.com

Interfaces on the Router_2811:

interface FastEthernet0/0
ip address 1.5.37.13 255.255.0.0
duplex auto
speed auto

interface FastEthernet0/1
ip address 30.0.0.1 255.255.255.0
duplex auto
speed auto
```

Step 2 Show clock on IOS:

Example:

```
Router# show clock
*10:07:57.109 pacific Thu Oct 7 2010
```

a) Set clock directly:

Example:

```
Router# clock set 9:53:0 Oct 7 2010

Set time zone (Pacific Standard Time)
Router# configure terminal
Router(config)# clock timezone pst -8

(optional)
Set summer-time
Router# configure terminal

Router(config)# clock summer-time pst recurring
```

OR

```
Router(config)# clock summer-time pst date apr 11 2010 12:00 nov 11 2010 12:00
```

b) Set clock using NTP:

Example:

```
Router(config)# ntp server 192.18.2.1
Router(config)# ntp master 2
```

Configure Trustpoint and Enroll with the Certificates

To configure a trustpoint and enroll with the certificate server, see Configure Cisco Unified CME as CA Server, on page 9. You can also use the default self-signed certificate generated by the webvpn. This default **trustpoint** is generated when the webvpn gateway **gateway name** command is entered for the first time.

Note The DTLS in IOS SSL VPN uses the child certificate during SSL authentication, therefore, you must select the “leaf” option when configuring the “vpn-trustpoint”.

Configure VPN Gateway

The WebVPN gateway uses a default trustpoint name of SSL VPN.

When entering “webvpn gateway <name>”, a self-signed certificate is generated. The IP address must be a public IP address configured on an interface or loopback interface on the WebVPN gateway. The following example shows a public IP address configured on the WebVPN gateway:

```
Router(config)# webvpn gateway sslvpn_gw
Router(config-webvpn-gateway)# ip address 1.5.37.13 port 443
Router(config-webvpn-gateway)# ssl encryption 3des-sha1 aes-sha1
Router(config-webvpn-gateway)# ssl trustpoint cme_cert
Router(config-webvpn-gateway)# inservice
```

Note We recommend using Cisco Unfied CME generated trustpoint rather than webvpn self generated trustpoint.

Configure User Database

User database can be either locally configured on CME, or remotely from Radius server.

Step 1 Configure the local database:

Example:

```
Router(config)# aaa new-model
username anyone password 0 cisco
aaa authentication login default local
```

Step 2 Configure a remote AAA Radius server for authentication:

Example:

```
Router(config)# aaa new-model
aaa authentication login default group radius
radius-server host 172.19.159.150 auth-port 1923 acct-port 1924
radius-server key cisco
```

For more information, see http://www.cisco.com/en/US/docs/security/asa/asa71/configuration/guide/aaa.html#wp1062044.

Configure Virtual Context

Users can get access to the virtual context by specifying the “domain name” in the URL when accessing the WebVPN gateway such as: https://1.5.37.13/SSLVPNphone. The following example shows a virtual VPN context configured:

```
Router(config)# webvpn context sslvpn_context
 ssl encryption 3des-sha1 aes-sha1
 ssl authenticate verify all
 gateway sslvpn_gw domain SSLVPNphone
 inservice
```

When **inservice** was entered, the system prompted: **000304: Jan 7 00:30:01.206: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1, changed state to up**

Configure Group Policy

Because the SSL VPN client on phone operates in full-tunnel mode, WebVPN gateway supplies an IP address to each of the clients logged in to the gateway. Configure the following:

```
Router(config)# ip local pool SSLVPNphone_pool 30.0.0.50 30.0.0.70
Router(config)# webvpn context SSLVPNphone
Router(config-webvpn-context)# policy group SSLVPNphone
Router(config-webvpn-group)# functions svc-enabled
Router(config-webvpn-group)# hide-url-bar
Router(config-webvpn-group)# svc address-pool "SSLVPNphone_pool" netmask 255.255.255.0
Router(config-webvpn-group)# svc default-domain "cisco.com"
Router(config-webvpn-group)# exit
Router(config-webvpn-context)# default-group-policy SSLVPNphone
Router(config-webvpn-context)# no aaa authentication domain local
Router(config-webvpn-context)# gateway sslvpn_gw domain SSLVPNphone
```

If using only username and password authentication, configure:

```
Router(config-webvpn-context)# no authentication certificate
```

If using certificate-based authentication, configure:

```
Router(config-webvpn-context)# authentication certificate

Router(config-webvpn-context)# ca trustpoint cme_cert
Router(config-webvpn-context)# inservice
```

Verify the IOS SSL VPN Connection

On your PC's browser (MS Internet Explorer), connect to https://1.5.37.13/SSLVPN phone and accept the certificate. To login, enter username and password, anyone and cisco. You should be able to see the home page of the IOS SSL VPN.

Step 1 IOS WEBVPN DEBUG:

Example:

```
debug ssl openssl errors
debug ssl openssl msg
debug ssl openssl states

debug webvpn sdps
debug webvpn aaa (login authentication)

debug webvpn http verbose (for authentication)
debug webvpn webservice verbose
debug webvpn tunnel

debug crypto pki transactions
debug crypto pki validations
debug crypto pki messages
```

From PC browser, connect to IOS (on the 1.5.37.x network) through https://1.5.37.13/SSLVPN phone. The default banner pops up. Enter username and password.

Step 2 Provide the default IP route. For example:

Example:

```
Router (c3745): ip route 30.0.0.0 255.255.255.0 FastEthernet0/
Router (c3745): ip route 10.0.0.0 255.255.255.0 1.5.37.11
```

(Must force this limited route or else it will fail).

Configure Cisco Unified SCCP IP Phones for SSL VPN

Step 1 Phone loads are available for download at Cisco Unified Communications Manager Express Introduction.

Step 2 Choose **Compatibility Information**.

Step 3 Choose appropriate phone load version for your phone.

A generic software download is also available at Product/Technology Support.

Step 4 Choose **Voice and Unified Communications** > **IP Telephony** > **IP Phones**.

Note We recommend downloading phone load version 8.4 before upgrading phone load version 8.3 to phone load version 9.0. Upgrading phone load to 9.0 without upgrading the phone load version to 8.4 will not work.

Step 5 After a hard reset (press # while power up), the *term65.default.loads* can be used to load the rest of the images.

Configuration on Cisco Unified SCCP IP Phone

Step 1 Go to **Settings** > **Security configuration (4)** > **VPN Configuration (8)** .

Step 2 Check the IP address of the VPN concentrator. It should point to the VPN headend.

Step 3 Verify Alt-TFTP (under **Settings** > **Network Configuration** > **IPv4 Configuration**). Set the Alternate TFTP option to "Yes" to manually enter the TFTP server address. The associated IP address is the IP address of Cisco Unified CME.

Step 4 Set the VPN setting to **enable**. The user interface shows, "`Attempting VPN Connection...`".

Step 5 Verify that the VPN connection is established. Go to **Settings** > **Network Configuration** . The "VPN" label shows "`connected`".

Note If you are using phones in secure mode, remember to add the **capf-ip-in-cnf** command under ephone configuration mode.

Configure SSL VPN on Cisco Unified CME

To configure SSL VPN on Cisco Unified CME, see Configure VPN Group and Profile on Cisco Unified CME, on page 16.

Example:

```
voice service voip
 vpn-group 1
  vpn-gateway 1 https://1.5.37.13/SSLVPNphone
  vpn-trustpoint 1 trustpoint R2811_cert leaf
 vpn-profile 1
  host-id-check disable

crypto pki server R2811_root
 database level complete
 grant auto
 lifetime certificate 7305
 lifetime ca-certificate 7305
crypto pki token default removal timeout 0
!
crypto pki trustpoint R2811_root
 enrollment url http://30.0.0.1:80
 revocation-check none
 rsakeypair R2811_root
!
crypto pki trustpoint R2811_cert
 enrollment url http://30.0.0.1:80
 serial-number
 revocation-check none

telephony-service
 cnf-file perphone

ephone 2
```

```
 device-security-mode none
 mac-address 001E.7AC4.DD25
 type 7965
 vpn-group 1
 vpn-profile 1
 button 1:5

telephony-service
 create cnf-files

ephone 2
 reset
```

VPN Phone Redundancy Support for Cisco Unified CME with DTLS

VPN phone supports redundancy with IOS and Cisco Unified CME in two ways:

1. Using two or more vpn-gateway configurations in the same vpn-group.
2. Using Cisco Unified CME redundancy configuration and one or more vpn-gateway configurations. This requires the DTLS and SSL VPN headend IP to stay up, if only one vpn-gateway is used.

Cisco Unified CME redundancy works when you import a trustpoint from primary CME to secondary CME. See http://www.cisco.com/en/us/docs/ios/security/command/reference/sec_c5.html. For more information on reduntant Cisco Unified CME, see Redundant Cisco Unified CME Router for SCCP Phones.

You need to generate a trustpoint with exportable keys and use that as sast1.

Configuration Examples for SSL VPN Client

Example for Configuring SSL VPN with ASA as VPN Headend

The following example shows how to configure CME using ASA as VPN Headend:

```
Router# show running config
!
!
!
crypto pki server cme_root
 database level complete
 no database archive
 grant auto
 lifetime certificate 7305
 lifetime ca-certificate 7305
!
crypto pki trustpoint cme_root
 enrollment url http://10.201.160.201:80
 revocation-check none
 rsakeypair cme_root
!
crypto pki trustpoint cme_cert
 enrollment url http://10.201.160.201:80
 revocation-check none
!
!
!
```

```
!
voice service voip
vpn-group 1
 vpn-gateway 1 https://10.201.174.36/SSLVPNphone
 vpn-trustpoint 1 trustpoint cme_cert root
 vpn-hash-algorithm sha-1
vpn-profile 1
 host-id-check disable
 sip
!
!
!
ip http server
no ip http secure-server
!
telephony-service
 max-ephones 20
 max-dn 10
 ip source-address 10.201.160.201 port 2000
 cnf-file location flash:
 cnf-file perphone
 max-conferences 8 gain -6
 transfer-system full-consult
 create cnf-files version-stamp Jan 01 2002 00:00:00
!
!
ephone-dn 1
 number 2223
 label TestPhone
!
!
ephone 1
 device-security-mode none
 mac-address 001F.6C81.110E
 type 7965
 vpn-group 1
 vpn-profile 1
 button 1:1
!
end
```

Example for Configuring SSL VPN with DTLS on CME as VPN Headend

The following example shows how to configure CME using DTLS on CME as VPN Headend:

```
!
ip domain-name cisco.com
!
aaa new-model
!
!
aaa authentication login default local
!
!
!
crypto pki server cme_root
 database level complete
 no database archive
 grant auto
 lifetime certificate 7305
 lifetime ca-certificate 7305
!
```

```
crypto pki trustpoint cme_root
 enrollment url http://10.201.160.201:80
 revocation-check none
 rsakeypair cme_root
!
crypto pki trustpoint cme_cert
 enrollment url http://10.201.160.201:80
 revocation-check none
!
crypto pki trustpoint TP-self-signed-4067918560
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-4067918560
 revocation-check none
 rsakeypair TP-self-signed-4067918560
!
!
!
voice service voip
vpn-group 1
 vpn-gateway 1 https://10.201.160.201/SSLVPNphone
 vpn-trustpoint 1 trustpoint cme_cert leaf
 vpn-hash-algorithm sha-1
vpn-profile 1
 host-id-check disable
sip
!
username kurt privilege 15 password 0 cisco
!
!
interface GigabitEthernet0/0
 ip address 10.201.160.201 255.255.255.192
 duplex auto
 speed auto
!
ip local pool SSLVPNphone_pool 10.201.160.202 10.201.160.203
ip forward-protocol nd
!
ip http server
no ip http secure-server
!
!
telephony-service
 max-ephones 20
 max-dn 10
 ip source-address 10.201.160.201 port 2000
 cnf-file location flash:
 cnf-file perphone
 max-conferences 8 gain -6
 transfer-system full-consult
 create cnf-files version-stamp Jan 01 2002 00:00:00
!
!
ephone-dn 1
 number 2223
 label TestPhone
!
!
ephone 1
 device-security-mode none
 mac-address 001F.6C81.110E
 type 7965
 vpn-group 1
 vpn-profile 1
 button 1:1
```

```
!
webvpn gateway sslvpn_gw
 ip address 10.201.160.201 port 443
 ssl encryption 3des-sha1 aes128-sha1
 ssl trustpoint cme_cert
 inservice
!
webvpn context SSLVPNphone
gateway sslvpn_gw domain SSLVPNphone
ca trustpoint cme_cert
!
ssl authenticate verify all
inservice
!
policy group SSLVPNphone
 functions svc-enabled
 svc address-pool "SSLVPNphone_pool" netmask 255.255.255.224
 svc default-domain "cisco.com"
 hide-url-bar
 default-group-policy SSLVPNphone
!
end
```

The following example shows the vpn configuration:

```
Router #show voice vpn
The Voice Service VPN Group 1 setting:
VPN Gateway 1 URL https://9.10.60.254/SSLVPNphone
VPN Trustpoint hash in sha-1
VPN Trustpoint 1 trustpoint cme_cert root fbUqFIbtWtaYSGSlTP/Umshcgyk= The Voice Service
VPN Profile 1 setting:
The host_id_check setting: 0
```

Feature Information for SSL VPN Client

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to https://cfnng.cisco.com/. An account on Cisco.com is not required.

Table 1: Feature Information for SSL VPN Client

Feature Name	Cisco Unified CME Versions	Feature Information
Support on Cisco Unified CME with DTLS	8.6	Introduced support on Cisco Unified CME with DTLS.
SSL VPN Client Support on SCCP IP Phones	8.5	Introduced the SSL VPN Client Support feature.