SCCP IP 電話機用 SSL VPN クライアント

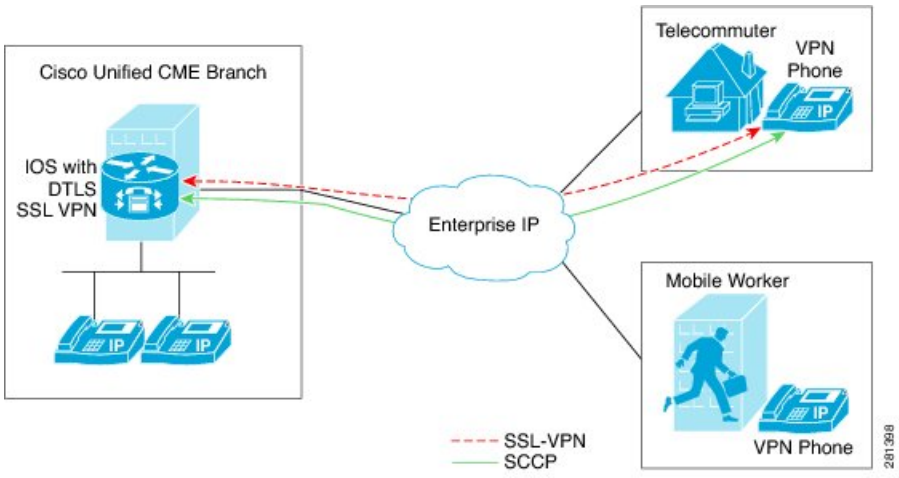
- SSL VPN クライアントについて （1 ページ）
- SSL VPN クライアントの構成 （4 ページ）
- VPN ヘッドエンドとしての Cisco Unified Cisco Mobility Express で DTLS を使用した SSL VPN クライアントの構成例 （23 ページ）
- SSL VPN クライアントの設定例 （30 ページ）
- SSL VPN クライアントの機能情報 （33 ページ）

SSL VPN クライアントについて

DTLS による Cisco Unified Cisco Mobility Express での SSL VPN サポート

Communications Manager Express 8.6 以降のバージョンでは、企業のネットワーク外にある 7945、7965、および 7975 などの Cisco Unified SCCP IP Phone を、SSL VPN 接続により Cisco Unified Cisco Mobility Express に登録できます。SSL VPN 接続は電話機と VPN ヘッドエンドの間でセットアップされます。VPN ヘッドエンドにすることができるのは、Adaptive Secure Appliance（ASA 5500）または Datagram Transport Layer Security（DTLS）対応の IOS SSL VPN ルータです。図 1 : Cisco Unified IP Phone と VPN ヘッドエンド（ASA および DTLS）間の VPN 接続 （2 ページ） を参照してください。ASA ヘッドエンドでの VPN 機能のサポートは、Cisco Unified CME 8.5 で追加されました。詳細については、SCCP IP 電話機用 SSL VPN クライアント （1 ページ）を参照してください。

図 *1 : Cisco Unified IP Phone* と *VPN* ヘッドエンド（*ASA* および *DTLS*）間の *VPN* 接続



Cisco Unified Cisco Mobility Express 8.6 は 、ヘッドエンドまたはゲートウェイとして IOS SSL DTLS を使用します。電話機と VPN ヘッドエンドの間に VPN 接続を確立するには、VPN 構成パラメータを使用して電話機を構成する必要があります。VPN構成パラメータには、VPNヘッドエンドアドレス、VPN ヘッドエンドのログイン情報、ユーザーまたは電話 ID、ログイン情報ポリシーが含まれます。これらのパラメータは機密情報と見なされ、署名付き構成ファイルまたは署名付きで暗号化された構成ファイルを使用してセキュアな環境で配布する必要があります。電話機を企業のネットワーク外に配置できるようにする前に、企業のネットワーク内でプロビジョニングする必要があります。

信頼できる環境で電話機が「ステージング」されると、VPN ヘッドエンドを接続できる場所に、その電話機を展開できます。電話機のVPN構成パラメータは、電話機のユーザーインターフェイスおよび動作を指示します。

電話機またはクライアントの認証

VPN DTLS 経由で Cisco Unified Cisco Mobility Express に登録しようとしているリモート電話機が正規の電話であることを確認するには、電話認証が必要です。電話機またはクライアントの認証は次のタイプの認証で行うことができます。

1. ユーザ名とパスワードによる認証。
2. 証明書ベースの認証（電話機の認証は、電話機の LSC または MIC 証明書を使用して行われます）。証明書ベースの認証は、次の 2 つのレベルで構成されます。
   - 証明書のみの認証：電話機のLSCのみが使用されます（ユーザはユーザ名またはパスワードの入力を電話機で要求されません）。
   - AAA または 2 要素による認証：電話機の LSC とユーザー名およびパスワードの組み合わせが電話機の認証に使用されます。2 要素認証は、ユーザ名の事前入力の有無にかかわらず実行できます。（ユーザー名が事前に入力されていると、電話機はユーザー名を要求せず、関連するトラストポイントの構成に応じてユーザー名を取得します）。

（注） 証明書認証には LSC を使用することをお勧めします。証明書認証に MIC を使用することはお勧めしません。また、証明書認証時は、ephone を「認証済み」（暗号化なし）セキュリティモードで構成することをお勧めします。 証明書のみの認証と 2 要素認証の詳細については、「https://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_ssl_vpn_ps6350_TSD_Products_Configuration_Guide_Chapter.html#wp1465191」を参照してください。

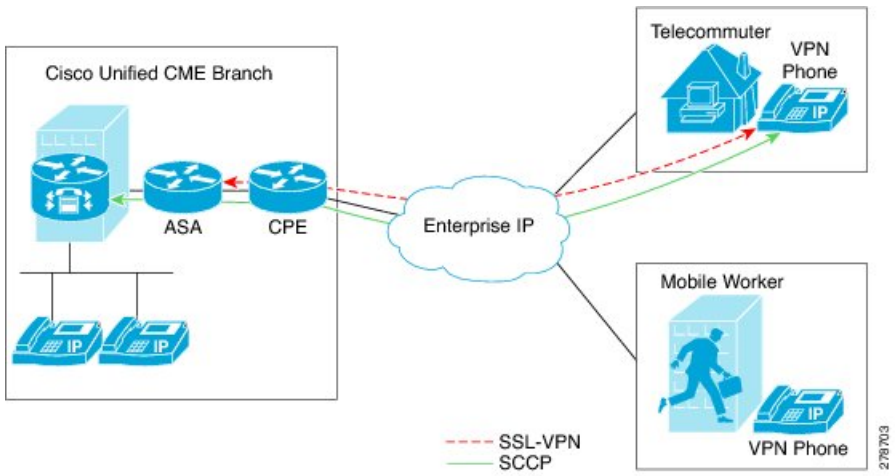
Cisco Unified CME は暗号化モードでセットアップできますが、暗号化された SCCP 電話機のメディア コール フロー サポートが制限されます。認証済みモードで電話機を使用する場合、メディア関連のコール フローに制限はありません。

SCCP IP Phone での SSL VPN クライアントのサポート

Cisco Unified Cisco Mobility Express 8.5 以降のバージョンでは、7945、7965、および 7975 などの SCCP IP Phone で セキュアソケットレイヤ（SSL）仮想プライベートネットワーク（VPN）がサポートされます。

Cisco Unified Cisco Mobility Express 8.5 では、「図 2 : 電話機と VPN ヘッドエンド間の接続 （3 ページ）」が示すように VPN 接続を経由で Cisco Unified Cisco Mobility Express 8.5 に企業ネットワーク外の SCCP IP Phone を登録します。

図 *2 :* 電話機と *VPN* ヘッドエンド間の接続



SSL VPN は、2 つのエンドポイント間で送信されるデータやその他の情報のためのセキュアな通信メカニズムを提供します。VPN 接続は SCCP IP Phone と VPN ヘッドエンドまたは VPN ゲートウェイの間でセットアップされます。Cisco Unified CME 8.5 では、適応型セキュリティ アプライアンス（ASA モデル 55x0）を VPN ヘッドエンドまたはゲートウェイとして使用します。

電話機と VPN ゲートウェイの間の VPN 接続を確立するために、電話機を VPN ゲートウェイ アドレス、VPN ヘッドエンド クレデンシャル、ユーザまたは電話機の ID、クレデンシャル ポ

リシーなどの VPN 設定パラメータで設定する必要があります。これらのパラメータには機密情報が含まれており、署名付き構成ファイルまたは署名付きで暗号化された構成ファイルを使用してセキュアな環境で配布する必要があります。電話機を企業のネットワーク外に配置する前に、企業のネットワーク内でプロビジョニングする必要があります。

信頼できるセキュアな環境で電話機がプロビジョニングされると、VPNヘッドエンドに到達できる場所ならどこからでも、その電話機を Cisco Unified CME に接続できます。電話機の VPN 構成パラメータは電話機のユーザーインターフェイスおよび動作を制御します。SCCP IP Phone での SSL VPN 機能の構成の詳細については、「ASA（ゲートウェイ）を VPN ヘッドエンドとして構成 （14 ページ）」を参照してください。

エクスポート可能なキーでトラストポイントを生成し、それを SAST1 として使用する必要があります。Cisco Mobility Express システム管理者セキュリティトークンの詳細については。

SCCP IP Phone に対して SSL VPN クライアントを構成する際の制限

SSL VPN クライアントは、Unified Cisco Mobility Express 上の Cisco 4000 シリーズ サービス統合型ルータではサポートされていません。

Unified Cisco Mobility Express では、サイト間 VPN 構成のみがサポートされます。

SSL VPN クライアントの構成

ASA を VPN ヘッドエンドとして使用する SSL VPN クライアントの構成

SCCP IP Phone で SSL VPN 機能を設定するには、次の手順を表示されている順に実行します。

1. Cisco Unified CME での基本設定 （5 ページ）
2. CA サーバーとして Cisco Unified Cisco Mobility Express を構成 （10 ページ）
3. 電話機登録および電話機負荷の確認 （13 ページ）
4. ASA（ゲートウェイ）を VPN ヘッドエンドとして構成 （14 ページ）
5. Cisco Unified Cisco Mobility Express での VPN グループおよびプロファイルの構成 （17 ページ）
6. SCCP IP 電話機に VPN グループとプロファイルを関連付ける （19 ページ）
7. 電話機での代替 TFTP アドレスの構成 （22 ページ）
8. 遠隔地からの電話機登録 （23 ページ）

前提条件

- Cisco Unified CME 8.5 以降のバージョン。
- ISR-G2 プラットフォーム用の Securityk9 ライセンス。

- Cisco Unified SCCP IP Phone 7942、7945、7962、7965、および 7975 と phone image 9.0 以降。
- イメージ asa828-7-k8.bin 以降の ASA 5500 シリーズ。
- SSLVPN 機能の設定には、パッケージ anyconnect-win-2.4.1012-k9.pkg が必要。ただし、電話機にはダウンロードされません。
- VPN クライアントで接続できるようにするには、適切な ASA ライセンス（AnyConnect for Cisco VPN Phone）を要求して、ASA にインストールすること。
  `www.cisco.com/go/license` に移動し、PAK と入力すると、新しいアクティベーションキーが E メールで送信されます。

（注） ASDM を介して構成する場合は、互換性のある Adaptive Security Device Manager（ASDM）イメージが必要です。

Cisco Unified CME での基本設定

次の手順は、SSL VPN 機能を組み込むための基本的な Cisco Unified 設定です。

手順の概要

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**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル構成モードを開始します。
ステップ 3	**ip dhcp pool** *pool-name* 例： `Router(config)# ip dhcp pool mypool`	DHCP サーバ アドレス プールの名前を作成し、DHCP プール コンフィギュレーション モードを開始します。 （注） DHCP IP アドレス プールをすでに設定している場合は、ステップ 2 ～ステップ 7 をスキップし、ステップ 8 から続行してください。
ステップ 4	**network** *ip-address* [*mask* | *prefix-length*] 例： `Router(config-dhcp)#network 192.168.11.0 255.255.255.0`	設定する DHCP アドレス プールの IP アドレスを指定します。
ステップ 5	**option 150 ip***ip-address* 例： `Router(config-dhcp)# option 150 ip 192.168.11.1`	Cisco Unified IP Phone でイメージ構成ファイルをダウンロードする TFTP サーバ アドレスを指定します。 • これが、Cisco Unified Cisco Mobility Express ルータのアドレスです。
ステップ 6	**default-router***ip-address* 例： `Router(config-dhcp)# default router 192.168.11.1`	（任意）IP Phone でローカル サブネットの外部にある IP トラフィックを送受信するために使用するルータを指定します。 • Cisco Unified CME ルータがネットワーク上の唯一のルータである場合、このアドレスはCisco Unified CME の IP ソース アドレスにする必要

	コマンドまたはアクション	目的
		があります。IP Phone でローカル サブネット上のデバイスのみと IP トラフィックの送受信を行う必要がある場合は、このコマンドは省略できます。 • デフォルト ルータに指定する IP アドレスは、フォールバックの目的で IP Phone で使用されます。Cisco Unified CME の IP ソース アドレスが到達不能になった場合、IP Phone はこのコマンドで指定されたアドレスへの登録を試行します。
ステップ 7	**exit** 例： `Router(config-dhcp)# end`	DHCP プール コンフィギュレーション モードを終了します。
ステップ 8	**telephony-service** 例： `Router(config)# telephony-service`	telephony-service コンフィギュレーション モードを開始します。
ステップ 9	**max-ephones** *max-phones* 例： `Router(config-telephony)# max-ephones 24`	Cisco Unified CME に登録できる電話機の最大数を設定します。 • 最大数はプラットフォームとバージョンで異なります。範囲には、**?** と入力します。 • Cisco Unified Cisco Mobility Express 7.0/4.3 7.0/4.3 以降のバージョンでは、登録できる電話機の最大数が、構成できる電話機の最大数とは異なります。設定できる電話機の最大数は 1000 です。 • Cisco Unified CME 7.0/4.3 よりも前のバージョンでは、このコマンドがルータで設定できる電話機の数に制限されていました。
ステップ 10	**max-dn** *max-directory-numbers* ［**preference** *preference-order*］［**no-reg primary** ｜ **both**］ 例： `Router(config-telephony)# max-dn 24 no-reg primary`	このルータでサポートされるディレクトリ番号の数を制限します。 • 最大数はプラットフォームとバージョンで異なります。値を表示するには ? と入力します。
ステップ 11	**ip source-address** *ip-address* **port** *port* ［**any-match** ｜ **strict-match**］ 例：	Cisco Unified CME ルータで IP Phone の登録に使用する IP アドレスとポート番号を指定します。

	コマンドまたはアクション	目的
	`Router(config-telephony)# ip source-address 192.168.11.1 port 2000`	• **port** *port*—（オプション）SCCP に使用する TCP/IP ポート番号。範囲は 2000 ～ 9999 です。デフォルトでは 2000 です。 • **any-match**—（オプション）登録のための厳密な IP アドレスチェックを無効にします。これはデフォルトです。 • **strict-match**—（オプション）電話機で使用される IP サーバーアドレスがソースアドレスと厳密に一致していない場合、ルータに IP Phone の登録試行を拒否するように指示します。
ステップ 12	**cnf-file**{**perphone**} 例： `Router(config-telephony)#xnf-file perphone`	システムで各 IP Phone に個別の設定 XML ファイルを生成することを指定します。 • セキュリティのために、各エンドポイントに個別の構成ファイルが必要です。 （注） 各電話に個別の XML ファイルを生成するには、cnf-file（perphone）コマンドを設定する必要があります。
ステップ 13	**load** ［*phone-type firmware-file*］ 例： `Router(config-telephony)# load 7965 SCCP45.9-0-1TD1-36S.loads`	電話タイプを電話機ファームウェア ファイルに関連付けます。ファイルのサフィクスを含めて完全なファイル名を使用する必要があります。電話機のファームウェアバージョンがバージョン 9.0 より新しい場合、すべての電話機のタイプで 7965 SCCP45.9-0-1TD1-36S がロードされます。
ステップ 14	**no shutdown** 例： `Router(config-telephony)# no shutdown`	SCCP サービス リスニング ソケットを有効にできます。
ステップ 15	**exit** 例： `Router(config-telephony)# end`	telephony-service コンフィギュレーション モードを終了します。
ステップ 16	**ephone-dn** *dn-tag* ［dual-line］ 例： `Router(config)# ephone-dn 1`	ephone dn コンフィギュレーション モードを開始して、IP フォンのディレクトリ番号、インターコム回線、音声ポート、またはメッセージ待機インジケータ（MWI）を定義します。 • *dn-tag* — 構成タスク中に特定のディレクトリ番号を指定します。範囲は 1 からルータのプラットフォームで許可されるディレクトリ番号

	コマンドまたはアクション	目的
		の最大数までです。**?** と入力して、範囲を表示します。
ステップ 17	**number** *number*［**secondary** *number*］［**no-reg**［**both** | **primary**］］ 例： `Router(config-ephone-dn)# number 1001`	内線番号をこのディレクトリ番号に関連付けます。 • *number* ― 内線または E.164 電話番号を示す最大 16 桁の文字列。
ステップ 18	**ephone** *phone-tag* 例： `Router(config)# ephone 1`	ephone コンフィギュレーションモードを開始して、ephone 固有のパラメータを設定します。 • *phone-tag* ― 電話機を識別する一意のシーケンス番号。範囲は、バージョンとプラットフォームに依存します。範囲を表示するには、**?** と入力します。
ステップ 19	**description** *string* 例： `Router(config-ephone)description SSL VPN Remote Phone`	拡張マークアップ言語（XML）クエリーを使用して、ネットワーク管理システムに対して Ephone を説明します。 • *string*― スペースを含めて最大 128 文字を使用できます。文字に制限はありません。
ステップ 20	**device-security-mode**{**authenticated** | **none** | **encrypted**} 例： `Router(config-ephone)# device-security-mode none`	デバイスと Cisco Unified CME ルータとのグローバルな、または ephone 単位での通信のための SCCP シグナリングにセキュリティ モードを設定できます。 • authenticated：TCP ポート 2443 上でのセキュアな TLS 接続を介したデバイスと Cisco Unified CME との間の SCCP シグナリング。 • none：SCCP シグナリングはセキュアではありません。 • encrypted：TCP ポート 2443 上でのセキュアな TLS 接続を介したデバイスと Cisco Unified CME との間の SCCP シグナリング。メディアは Secure Real-Time Transport Protocol（SRTP）を使用します。
ステップ 21	**mac-address** *mac-address* 例：	Cisco IP Phone の MAC アドレスを Cisco Unified CME システムの ephone 設定に関連付けます

	コマンドまたはアクション	目的
	`Router(config-ephone)# mac-address 0022.555e.00f1`	• *mac-address* IP Phone の MAC アドレスを指定します。これは、電話機の底面にあるシールに記載されています。
ステップ 22	**type** phone-type［addon 1 module-type［2 module-type］］ 例： `Router(config-ephone)# type 7965`	電話機のタイプを指定します。 • Cisco Unified CME 4.0 以降のバージョン：アドオンモジュールを適用できるタイプは、7960、7961、7961GE、および 7970 のみです。
ステップ 23	**button** *button-number*｛separator｝dn-tag［,dn-tag...］［button-number｛x｝overlay-button-number］［button-number...］ 例： `Router(config-ephone)# button 1:1`	ボタン番号と回線の特性を ephone-dn に関連付けます。ボタンの最大数は電話機のタイプによって決まります。
ステップ 24	**exit** 例： `Router(config-ephone)#exit`	ephone コンフィギュレーション モードを終了します。
ステップ 25	**telephony-service** 例： `Router(config)telephony-service`	telephony-service コンフィギュレーション モードを開始します。
ステップ 26	**create cnf-files** 例： `Router(config-telephony)# create cnf-files`	SCCP 電話機で必要とされる XML 構成ファイルを構築します。
ステップ 27	**end** 例： `Router(config-telephony)# end`	特権 EXEC モードに戻ります。

CA サーバーとして Cisco Unified Cisco Mobility Express を構成

CA サーバでの基本設定では、SSL VPN 機能を有効にするために必要な IP 接続、Network Time Protocol（NTP）、時刻の同期を設定します。

このセクションでは、Cisco Mobility Express と ASA の両方に証明書署名を提供するように Cisco Mobility Express で CA サーバーを構成する方法について説明しますが、実際の展開では、サードパーティの CA がよく使用されます。基本的な要件は、Cisco Mobility Express と ASA がそれぞれサードパーティの CA によって署名された ID 証明書を持ち、Cisco Mobility Express と ASA の両方が同じ CA 証明書を共有することです。つまり、各デバイスには、同じ CA 証明書と、同じ CA によって署名された ID 証明書を含むトラストポイントがあります。

CA サーバを設定するには、次の手順を実行します。

ステップ 1 Cisco Unified CME ルータで IP アドレス、NTP および HTTP サーバを設定します。

例：

```
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
```

（注） クロックを手動で設定して Cisco Unified CME ルータの時刻に合わせていない場合は、NTP の同期化は失敗します。

ステップ 2 CA サーバーとして Cisco Unified Cisco Mobility Express を構成します。Cisco Mobility Express と ASA の両方が CA サーバーから証明書を登録します。次の設定例では、CA サーバとして設定される Cisco Unified CME を示します。

例：

```
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.
```

ステップ 3 別のトラストポイントを作成し、トラストポイントを認証し、CA で登録します。

例：

```
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
```

証明書の確認（オプション）

Cisco Unified Cisco Mobility Express ルータで、**show crypto pki certificates** コマンドを使用して証明書を確認します。

```
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
```

電話機登録および電話機負荷の確認

ステップ 1 **show ephone** コマンドを使用すると、電話機登録詳細を確認できます。

例：

```
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
```

（注） 電話機に正しいファームウェアがインストールされ、電話機が Cisco Unified CME でローカルに登録されているかどうかを確認します。

ステップ 2 **show ephone phone load** コマンドを使用すると電話機の負荷を確認できます。

例：

```
Router# show ephone phoneload

DeviceName        CurrentPhoneload       PreviousPhoneload LastReset

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

ASA（ゲートウェイ）を VPN ヘッドエンドとして構成

このセクションでは、Cisco Mobility Express CA サーバーからの証明書を認証して登録するように ASA を構成します。CA 証明書の指紋は Cisco Mobility Express ルート証明書と同じになるため、電話機は TLS ネゴシエーション中に ASA から送信された証明書を、保存されているハッシュに対して認証できます。

ステップ 1 インターフェイス、IP ルーティング、および NTP を設定します。

例：

```
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
```

ステップ 2 ASA 上にトラストポイントを作成し、CME（CA）の証明書を取得します。

例：

```
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
```

ステップ 3　証明書の確認（オプション）

ASA ルータで **show crypto ca certificate** コマンドを使用して、証明書を確認します。

例：

```
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
```

ステップ 4　SSL パラメータを構成します。

例：

```
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
```

ステップ 5 ローカル IP アドレス プールを設定します。

例：

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

ステップ 6 VPN を介した NAT トラフィックを回避するために、アクセス リストを設定します。

例：

```
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
```

ステップ 7 VPN を設定します。VPN 構成に関する情報は http://www.cisco.com/en/US/docs/security/asa/asa82/configuration/guide/svc.html を参照してください。

例：

```
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)#
```

ステップ 8 SSL VPN トンネルを設定します。詳細については、http://www.cisco.com/en/US/docs/security/asa/asa82/configuration/guide/vpngrp.htmlを参照してください。

例：

```
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
```

ステップ 9 Cisco Unified CME の音声 VLAN へのスタティック ルートを有効にします。詳細については、http://www.cisco.com/en/US/docs/security/asa/asa82/configuration/guide/route_static.htmlを参照してください。

例：

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

ステップ 10 ユーザに対して ASA ローカル データベースを設定します。詳細については、http://www.cisco.com/en/US/docs/security/asa/asa82/configuration/guide/access_aaa.html#wpmkr108を参照してください。

例：

```
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
```

ステップ 11 ASA メディア間トラフィックを有効にします。

例：

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

Cisco Unified Cisco Mobility Express での VPN グループおよびプロファイルの構成

このセクションでは、電話機用の VPN ゲートウェイ IP アドレス、証明書ハッシュアルゴリズム、証明書トラストポイントを指定する VPN グループを構成します。この情報は、後で電話機構成に追加されます。Cisco Unified CME で VPN グループおよびプロファイルを設定するには、次の手順を実行します。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル構成モードを開始します。
ステップ 3	**voice service voip** 例： `Router(config)#voice service voip`	Voice over IP コンフィギュレーション モードを開始します。
ステップ 4	**vpn-group** *tag* 例： `Router (conf-voi-serv)#vpn-group 1`	Voice over IP コンフィギュレーション モードで vpn-group モードを開始します。 • *tag*— VPN グループタグ。範囲：1 または 2。
ステップ 5	**vpn-gateway** [*number* | **url**] 例： `Router(conf-vpn-group)#vpn-gateway 1 https://9.10.60.254/SSLVPNphone`	VPN のゲートウェイ URL を定義できます。 • *number*—number— VPN ゲートウェイとして定義されるゲートウェイ数。範囲は 1 ～ 3 です。 • *url*— VPN ゲートウェイ URL。SSLVPNphone は、ASA で構成された VPN グループポリシーです。
ステップ 6	**vpn-trustpoint** {[*number* [**raw** | **trustpoint**]} 例： `Router(conf-vpn-group)#vpn-trustpoint ?vpn-trustpoint 1 trustpoint cme_cert root`	VPN ゲートウェイ トラストポイントを入力できます。 • **number**—許容できるトラストポイント数。範囲：1 ～ 10。 • **raw**— RAW 形式で VPN ゲートウェイ トラストポイントを入力します。 • **trustpoint**—IOS 形式で作成された VPN ゲートウェイ トラストポイントを入力します。 • **root** – Cisco Mobility Express ルート証明書には ASA の CA 証明書と同じハッシュがあるため、リーフ証明書の代わりにルート証明書を選択するように「root」句が構成されています。

	コマンドまたはアクション	目的
ステップ 7	**vpn-hash-algorithm** *sha-1* 例： `Router(conf-vpn-group)#vpn-hash-algorithm sha-1`	VPN ゲートウェイ トラストポイントの vpn hash 暗号化を入力できます。 • *sha-1*— 暗号化アルゴリズム。
ステップ 8	**exit** 例： `Router(conf-vpn-group)#exit`	VPN-group コンフィギュレーション モードを終了します。
ステップ 9	**vpn-profile** *tag* 例： `Router (conf-voi-serv)#vpn-profile 1`	VPN-profile コンフィギュレーション モードを開始します。 *tag*— VPN プロファイルタグ番号。範囲：1 ～ 6。
ステップ 10	**host-id-check** ［**enable** | **disable**］ 例： `Router(conf-vpn-profile)#host-id-check disable`	VPN プロファイルでホスト ID チェック オプションを設定できます。 • disable：ホスト ID チェック オプションを無効にします。 • enable：ホスト ID チェック オプションを有効にします。デフォルトは enable です。
ステップ 11	**end** 例： `Router(conf-vpn-profile)#end`	特権 EXEC モードに戻ります。

SCCP IP 電話機に VPN グループとプロファイルを関連付ける

VPN グループおよびプロファイルを SCCP IP Phone に関連付けるには、次の手順を実行します。

手順の概要

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** タグ
10. **vpn-profile** タグ

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**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル構成モードを開始します。
ステップ 3	**telephony-service** 例： `Router#(config)telephony-service`	telephony-service コンフィギュレーション モードを開始します。
ステップ 4	**cnf-file perphone** 例： `Router(config-telephony)# create cnf-files`	IP Phone で必要とされる XML 構成ファイルを構築します。
ステップ 5	**ephone** *phone-tag* 例： `Router(config)# ephone 1`	ephone コンフィギュレーション モードを開始して、SCCP 電話機の電話機固有のパラメータを設定します。 • *phone-tag* — 電話機を識別する一意のシーケンス番号。範囲は、バージョンとプラットフォームに依存します。**?** と入力すると、範囲を表示できます。
ステップ 6	**device-security-mode** {authenticated | none | encrypted} 例： `Router(config-telephony)# device-security-mode none`	エンドポイントのセキュリティ モードを有効にします。 • authenticated：暗号化なしで TLS 接続を確立するようにデバイスに指示します。メディア パスにセキュアな Real-Time Transport Protocol（SRTP）がありません。

	コマンドまたはアクション	目的
		• none：SCCP シグナリングはセキュアではありません。これはデフォルトです。 • encrypted：デバイスに、SRTP を使用してセキュアなメディア パスへの暗号化された TLS 接続を確立するように指示します。 • ephone コンフィギュレーション モードでこのコマンドに設定された値は、telephony-service コンフィギュレーション モードで設定された値よりも優先されます。
ステップ 7	**mac-address** [mac-address] 例： `Router(config-ephone)#mac-address 0022.555e.00f1`	設定される IP Phone の MAC アドレスを指定します
ステップ 8	**type** *phone-type* **addon 1** *[module-type* [**2** *module-type*]] 例： `Router(config-ephone)# type 7965`	電話機のタイプを指定します。 • Cisco Unified CME 4.0 以降のバージョン：アドオン モジュールを適用できるタイプは、7960、7961、7961GE、および 7970 のみです。 • Cisco CME 3.4 以前のバージョン：アドオン モジュールを適用できるタイプは 7960 だけです。
ステップ 9	**vpn-group** タグ 例： `Router (config-ephone)# vpn-group 1`	Voice over IP コンフィギュレーション モードで vpn-group モードを開始します。 • tag— VPN グループタグ。範囲：1 または 2。
ステップ 10	**vpn-profile** タグ 例： `Router (config-ephone)#vpn-profile 1`	VPN-profile コンフィギュレーション モードを開始します。 • tag：VPN プロファイル タグ番号。範囲：1 ～ 6。
ステップ 11	**button** *button-number{separator}dn-tag [,dn-tag...][button-number{x}overlay-button-number] [button-number...]* 例： `Router(config-ephone)# button 1:5`	ボタン番号と回線の特性を ephone-dn に関連付けます。ボタンの最大数は電話機のタイプによって決まります。
ステップ 12	**exit** 例： `Router(config-ephone)exit`	ephone コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的
ステップ 13	**telephony-service** 例： `Router(config)# telephony-service`	telephony-service コンフィギュレーション モードを開始します。
ステップ 14	**create cnf-file** 例： `Router(config-telephony)# create cnf-files`	IP Phone で必要とされる XML 構成ファイルを構築します。最初に「no create cnf-files」を使用して既存の構成ファイルをクリアしてから、再度作成することをお勧めします。
ステップ 15	**exit** 例： `Router(Config-telephony)exit`	telephony service コンフィギュレーション モードを終了します。
ステップ 16	**ephone** *phone-tag* 例： `Router(config)# ephone 1`	ephone コンフィギュレーション モードを開始します。 • *phone-tag*— 構成タスク中にこの ephone を識別する一意のシーケンス番号。
ステップ 17	**reset** 例： `Router(config-ephone)# reset`	設定される個々の SCCP 電話機の完全なリブートを実行します。
ステップ 18	**end** 例： `Router(config-ephone)# end`	特権 EXEC モードに戻ります。

電話機での代替 TFTP アドレスの構成

ステップ 1 電話機から、次のように操作します。

例：

```
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.
```

ステップ 2 電話機の設定を保存します。

ステップ 3 電話機から VPN が有効になっていることを確認します。

例：

```
Settings > Security Configuration > VPN

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

ステップ 4 電話機から、次のように操作します。

例：

```
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.
```

ステップ 5 設定を保存します。

ステップ 6 自宅またはリモート サイトから電話機をネットワークに接続します。

例：

```
Settings > Security Settings > VPN Configurations?

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

遠隔地からの電話機登録

リモート サイトから Cisco Unified IP Phone を登録するには、次の手順を実行します。

ステップ 1 自宅またはリモート サイトから電話機をネットワークに接続します。電話機が DHCP を受信します。

ステップ 2 電話機のメニューで **[設定（Settings）]** を選択肢、**[セキュリティ設定（Security Settings）]** に移動します。

ステップ 3 **[VPNを構成（VPN Configurations）]** > **[VPNを有効化（Enable VPN）]** の順に選択します。

ステップ 4 ユーザ名とパスワードを入力します。これで、Cisco Unified Cisco Mobility Express に電話機が登録されます。

VPN ヘッドエンドとしての Cisco Unified Cisco Mobility Express で DTLS を使用した SSL VPN クライアントの構成例

始める前に、基本 SSL VPN 構成 を Cisco Unified Cisco Mobility Express で行ったことを確認します（「Cisco Unified CME での基本設定 （5 ページ）」を参照）。

SCCP IP Phone で DTLS による SSL VPN クライアントを設定するには、次の手順を表示されている順に実行します。

• 時計、ホスト名、およびドメイン名の設定 （24 ページ）
• ラストポイントの構成と証明書を使用した登録 （25 ページ）
• VPN ゲートウェイの設定 （25 ページ）
• ユーザーデータベースの構成 （26 ページ）
• 仮想コンテキストの構成 （26 ページ）
• グループ ポリシーの設定 （27 ページ）
• IOS SSL VPN 接続の確認 （27 ページ）
• SSL VPN 用 Cisco Unified SCCP IP 電話機の構成 （28 ページ）
• Cisco Unified SCCP IP Phone の設定 （28 ページ）
• Cisco Unified Cisco Mobility Express での SSL VPN 構成 （29 ページ）

（注） 設定することを選択した認証のタイプによって、設定のステップ 3 ～ステップ 11 はここに記載されている方法とはやや異なる場合があります。

時計、ホスト名、およびドメイン名の設定

時計、ホスト名、およびドメイン名を設定する必要があります。

ステップ 1 次の例は、構成されたホスト名とドメイン名を示しています。

例：

```
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
```

ステップ 2 IOS のクロックを表示します。

例：

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

a) 時計を直接構成する

例：

```
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
```

または

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

b) NTP を使用して時計を構成する

例：

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

ラストポイントの構成と証明書を使用した登録

トラストポイントの構成と証明書サーバーに登録するには、「CA サーバーとして Cisco Unified Cisco Mobility Express を構成 （10 ページ）」を参照してください。webvpn で生成されるデフォルトの自己署名証明書を使用することもできます。このデフォルト **trustpoint** は、webvpn ゲートウェイ **gateway name** コマンドの初回入力時に、生成されます。

（注） IOS SSL VPN の DTLS は SSL 認証中に子証明書を使用するため、「vpn-trustpoint」を構成中に「leaf」オプションを選択する必要があります。

VPN ゲートウェイの設定

WebVPN ゲートウェイは、SSL VPN のデフォルトのトラストポイント名を使用します。

「webvpn gateway <name>」に入ると、自己署名証明書が生成されます。IP アドレスは、WebVPN ゲートウェイのインターフェイスまたはループバック インターフェイスに構成されたパブリック IP アドレスである必要があります。次に、WebVPN ゲートウェイ上で設定されたパブリック IP アドレスの例を示します。

```
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
```

（注） webvpn 自己生成のトラストポイントではなく、Cisco Unfied Cisco Mobility Express 生成のトラストポイントを使用することをお勧めします。

ユーザーデータベースの構成

ユーザーデータベースは、Cisco Mobility Express でローカルに構成することも、Radius サーバーからリモートで構成することもできます。

ステップ 1 ローカルデータベースの構成

例：

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

ステップ 2 認証用に リモートの AAA Radius サーバーを構成する場合

例：

```
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
```

詳細については、http://www.cisco.com/en/US/docs/security/asa/asa71/configuration/guide/aaa.html#wp1062044を参照してください。

仮想コンテキストの構成

https://1.5.37.13/SSLVPNphone などの WebVPN ゲートウェイにアクセスする際に、URL に「ドメイン名」を指定すると、ユーザーは、仮想コンテキストにアクセスできます。次に、設定された仮想 VPN コンテキストの例を示します。

```
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**

グループ ポリシーの設定

電話機の SSL VPN クライアントはフル トンネル モードで動作するため、WebVPN ゲートウェイは、ゲートウェイにログインしている各クライアントに IP アドレスを提供します。以下の設定:

```
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
```

ユーザー名とパスワードの認証のみを使用する場合は、次のように構成します。

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

証明書ベースの認証を使用する場合は、次のように構成します。

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

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

IOS SSL VPN 接続の確認

PC のブラウザ（MS Internet Explorer）で、https://1.5.37.13/SSLVPN 電話機に接続し、証明書を許可します。ログインするには、ユーザー名とパスワード、anyone、cisco と入力します。IOS SSL VPN のホームページが表示されます。

ステップ 1 IOS WEBVPN デバッグ：

例：

```
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
```

PC ブラウザから、https://1.5.37.13/SSLVPN 電話を介して IOS（1.5.37.x ネットワーク上）に接続します。デフォルトのバナーがポップアップします。ユーザー名とパスワードを入力します。

ステップ 2 デフォルトの IP ルートを指定します。例：

例：

```
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
```

（この制限されたルートを強制的に使用しないと、失敗します）。

SSL VPN 用 Cisco Unified SCCP IP 電話機の構成

ステップ 1 電話機の負荷は、「Cisco Unified Communications Manager Express Introduction」でダウンロードできます。

ステップ 2 **[互換性情報（Compatibility Information）]** を選択します。

ステップ 3 電話機に該当する電話機ファームウェア バージョンを選択します。

「製品/技術サポート」では、汎用ソフトウェアもダウンロードできます。

ステップ 4 **[Voice and Unified Communications]** > **[IP テレフォニー（IP Telephony）]** > **[IP Phone]** の順に選択します。

（注） 電話機ファームウェア バージョン 8.3 を電話機ファームウェア バージョン 9.0 にアップグレードする前に、電話機ファームウェア バージョン 8.4 をダウンロードすることを推奨します。電話機ファームウェア バージョンを 8.4 にアップグレードしないで電話機ファームウェアを 9.0 にアップグレードしても機能しません。

ステップ 5 ハードリセット（電源が入っている際に**#** を押す）後、*term65.default.loads* を使用して、残りに画像をロードできます。

Cisco Unified SCCP IP Phone の設定

ステップ 1 **[設定（Settings）]** > **[セキュリティ情報 (4)（Security configuration (4)）]** > **[VPN構成(8)（VPN Configuration (8)）]** の順に選択します。

ステップ 2 VPN コンセントレータの IP アドレスを調べます。VPN ヘッドエンドをポイントしている必要があります。

ステップ 3 Alt-TFTP を確認します（**[設定（Settings）]** > **[ネットワーク構成（Network Configuration）]** > **[IPv4構成（IPv4 Configuration）]** の順に選択）。代替 TFTP オプションを「はい」に設定して、TFTP サーバーアドレスを手動入力します。関連付ける IP アドレスは、Cisco Unified CME の IP アドレスです。

ステップ 4 VPN 設定を **[有効（enable）]** に設定します。ユーザーインターフェイスに、[VPN に接続中...（Attempting VPN Connection...）]と表示されます。

ステップ 5 VPN 接続が確立していることを確認します。**[設定（Settings）]** > **[ネットワーク構成（Network Configuration）]** の順に選択します。[VPN] ラベルに、[接続済み（connected）] と表示されます。

（注） セキュアモードで電話機を使用している場合、必ず ephone 構成モードで **capf-ip-in-cnf** コマンドを追加します。

Cisco Unified Cisco Mobility Express での SSL VPN 構成

Cisco Unified Cisco Mobility Express で SSL VPN を構成するには、「Cisco Unified Cisco Mobility Express での VPN グループおよびプロファイルの構成 （17 ページ）」を参照してください。

例：

```
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
```

DTLS による Cisco Unified Cisco Mobility Express 向け VPN 電話機冗長性サポート

VPN 電話機は、IOS および Cisco Unified CME による冗長性を次の 2 とおりの方法によりサポートします。

1. 同じ vpn-group で 2 つ以上の vpn-gateway 構成を使用する。
2. Cisco Unified CME の冗長性設定と 1 つ以上の vpn-gateway 設定を使用する。vpn-gateway が 1 つだけ使用されている場合、DTLS および SSL VPN ヘッドエンド IP が稼働し続ける必要があります。

Cisco Unified Cisco Mobility Express の冗長性は、トラストポイントをプライマリ Cisco Mobility Express からセカンダリ Cisco Mobility Express にインポートすると機能します。「http://www.cisco.com/en/us/docs/ios/security/command/reference/sec_c5.html」を参照してください。冗長 Cisco Unified Cisco Mobility Express の詳細については、「SCCP 電話機の冗長 Cisco Unified Cisco Mobility Express ルータ」を参照してください。

エクスポート可能なキーでトラストポイントを生成し、それを sast1 として使用する必要があります。

SSL VPN クライアントの設定例

ASA を VPN ヘッドエンドとして使用する SSL VPN の構成例

次の例は、ASA を VPN ヘッドエンドとして使用して Cisco Mobility Express を構成する方法を示しています。

```
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
```

VPN ヘッドエンドとしての Cisco Mobility Express での DTLS を使用した SSL VPN の構成例

次の例は、VPN ヘッドエンドとして Cisco Mobility Express で DTLS を使用して Cisco Mobility Express を構成する方法を示しています。

```
!
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
```

次の例では、VPN 設定を示します。

```
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
```

SSL VPN クライアントの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *1 : SSL VPN* クライアントの機能情報

機能名	Cisco Unified Cisco Mobility Express のバージョン	機能情報
DTLS による Cisco Unified CME でのサポート	8.6	DTLS による Cisco Unified CME でのサポートが導入されました。

機能名	Cisco Unified Cisco Mobility Express のバージョン	機能情報
SCCP IP Phone での SSL VPN クライアントのサポート	8.5	SSL VPN クライアント サポート機能が導入されました。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。