



Secure SRST の設定

Revised: July 11, 2008

この章では、認証、保水性、およびメディア暗号化など、新しい Secure SRST セキュリティ機能について説明します。

内容

- [Secure SRST を設定するための前提条件 \(P.152\)](#)
- [Secure SRST を設定する場合の制約事項 \(P.153\)](#)
- [Secure SRST の設定について \(P.154\)](#)
- [Secure SRST の設定方法 \(P.160\)](#)
- [Secure SRST の設定例 \(P.187\)](#)
- [関連情報 \(P.192\)](#)

Secure SRST を設定するための前提条件

概要

- Secure SRST でサポートされている Secure Cisco Unified IP Phone には、証明書がインストールされている必要があり、暗号化が有効になっている必要があります。
- SRST ルータには、証明書が必要です。この証明書は、サードパーティまたは Cisco IOS Certificate Authority (CA; 認証局) から生成できます。Cisco IOS CA は、Cisco Unified SRST と同じゲートウェイで実行できます。
- Cisco Unified Communications Manager 4.1(2) またはそれ以降がインストールされており、セキュリティ モード (認証および暗号化モード) をサポートしている必要があります。
- Cisco Unified Communications Manager の Certificate Trust List (CTL) が有効になっている必要があります。詳細な手順については、『[Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways](#)』の「Configuring Secure IP Telephony Calls」の手順を参照してください。
- Secure SRST を実行するゲートウェイ ルータは、音声およびセキュリティ対応の Cisco IOS イメージ (「k9」暗号ソフトウェア イメージ) をサポートしている必要があります。次の 2 つのイメージがサポートされています。
 - 拡張 IP サービス。このイメージには、いくつかの拡張セキュリティ機能が含まれます。
 - 拡張エンタープライズ サービス。このイメージには、Cisco IOS ソフトウェアがすべて含まれます。

PKI

- 手動または Network Time Protocol (NTP; ネットワーク タイム プロトコル) を使用して、クロックを設定します。クロックを設定することで、Cisco Unified Communications Manager と確実に同期を取ることができます。
- IP HTTP サーバ (Cisco IOS プロセッサ) が有効になっていない場合は、`ip http server` コマンドを使用して、IP HTTP サーバ (Cisco IOS プロセッサ) を有効にします。PKI (Public Key Infrastructure; 公開鍵インフラストラクチャ) 構成の詳細については、『[Cisco IOS Certificate Server](#)』を参照してください。
- 証明書サーバがスタートアップ コンフィギュレーションに含まれる場合、起動手順で次のメッセージが表示されることがあります。

```
% Failed to find Certificate Server's trustpoint at startup
% Failed to find Certificate Server's cert.
```

これらのメッセージは通知目的のメッセージであり、スタートアップ コンフィギュレーションがまだ完全に解析されていないので証明書サーバの設定を一時的に実行できないことを示します。このメッセージは、スタートアップ コンフィギュレーションが破損した場合のデバッグに役立ちます。

起動手順の後、`show crypto pki server` コマンドを使用して、証明書サーバのステータスを確認できます。

SRST

- Secure SRST サービスは、Cisco Unified SRST がアクティブな間は登録できません。そのため、`no call-manager-fallback` コマンドを使用して、Cisco Unified SRST を無効にします。

サポートされている Cisco Unified IP Phone、プラットフォーム、およびメモリの要件

- Secure SRST でサポートされている Cisco Unified IP Phone、ルータ、ネットワーク モジュール、およびコーデックのリストについては、『[Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways](#)』を参照してください。
- Cisco Unified IP Phone の最大数、電話番号 (DN) または仮想音声ポートの最大数、およびメモリ要件に関する最新情報については、『[Cisco Unified SRST 4.3 Supported Firmware, Platforms, Memory, and Voice Products](#)』を参照してください。

Secure SRST を設定する場合の制約事項

概要

- 暗号ソフトウェア機能（「k9」）は、輸出が規制されています。本製品には暗号化機能が備わっており、輸入、輸出、配布および使用に適用される米国および他の国での法律を順守するものとします。シスコの暗号化製品を譲渡された第三者は、その暗号化技術の輸入、輸出、配布、および使用を許可されたわけではありません。輸入業者、輸出業者、販売業者、およびユーザーは、米国および他の国での法律を順守する責任があります。本製品を使用するにあたっては、関係法令の順守に同意する必要があります。米国および他の国の法律を順守できない場合は、本製品を至急送り返してください。

シスコの暗号化製品に適用される米国の法律の概要については、次の URL で参照できます。
<http://www.cisco.com/wwl/export/crypto/tool/>

ご不明な点がある場合は、export@cisco.com まで電子メールで連絡してください。

- Secure Real-Time Transport Protocol (SRTP) 暗号化コールは、Cisco Unified IP Phone エンドポイント間、または Cisco Unified IP Phone からゲートウェイ エンドポイントに対して行われます。IP Phone には、ロック アイコンが表示されます。ロックは、コールの IP レッグのみに対するセキュリティを示します。PSTN レッグのセキュリティは含まれていません。
- Secure SRST がサポートされるのは、1 つのルータの範囲内だけです。

Secure SRST モードでサポートされていない内容

- 4.1(2) 以前の Cisco Unified Communications Manager バージョン
- 安全な Music On Hold (MOH; 保留音)。MOH はアクティブの状態ですが、保護されていない状態に戻ります。
- 安全な変換または会議
- Secure H.323 または SIP トランク
- SIP 電話機の相互運用性
- [Hot Standby Router Protocol](#) (HSRP; ホットスタンバイ ルータ プロトコル)

Secure SRST モードでサポートされているコール

Secure SRST モードでは、音声コールだけがサポートされています。具体的には、次の音声コールがサポートされています。

- 基本的なコール
- コール転送（打診およびブラインド）
- 自動転送（ビジジー、無応答、すべて）
- 共有回線（IP Phone）
- 保留および再開

Secure SRST の設定について

Secure SRST を設定するには、次の概念を理解する必要があります。

- [Secure SRST の利点 \(P.154\)](#)
- [SRST での Cisco IP Phone のクリアテキスト フォールバック \(P.154\)](#)
- [SRST ルータおよび TLS プロトコル \(P.155\)](#)
- [Cisco Unified SRST ルータおよび PKI \(P.155\)](#)
- [Secure SRST の認証および暗号化 \(P.156\)](#)
- [Secure SRST ルータの Cisco IOS クレデンシャル サーバ \(P.158\)](#)
- [Cisco Unified IP Phone への Secure Cisco Unified SRST の確立 \(P.158\)](#)

Secure SRST の利点

リモート サイトに設置され、ゲートウェイ ルータに接続されている Secure Cisco Unified IP Phone は、WAN を使用して Cisco Unified Communications Manager と安全に通信を行うことができます。ただし、WAN リンクまたは Cisco Unified Communications Manager がダウンすると、リモート電話機を使用したすべての通信が安全でなくなります。この状況を克服するために、ゲートウェイ ルータが Secure SRST モードで機能できるようになりました。このモードは、WAN リンクまたは Cisco Unified Communications Manager がダウンしたときに起動します。WAN リンクまたは Cisco Unified Communications Manager が復帰すると、Cisco Unified Communications Manager が安全なコール処理機能を再開します。

Secure SRST は、認証、保全性、およびメディア暗号化など、新しい Cisco Unified SRST セキュリティ機能を提供します。認証は、ユーザに対して、通話相手の身元が正しいことを保証します。保全性は、特定のデータがエンティティ間で変更されていないことを保証します。暗号化は機密性を意味します。つまり、対象となる受信者以外の人はデータを読み取れないということです。これらのセキュリティ機能は、Cisco Unified SRST 音声コールのプライバシーを守り、音声セキュリティ違反およびなりすまし犯罪から保護します。

SRST セキュリティが実現されるための条件は、次のとおりです。

- エンドデバイスが、証明書を使用して認証される
- シグナリングが、TCP に対する Transport Layer Security (TLS) を使用して認証および暗号化される
- 安全なメディア パスが、SRTP を使用して暗号化される
- 証明書が CA によって生成および配布される

SRST での Cisco IP Phone のクリアテキスト フォールバック

12.3(14)T より以前の Cisco Unified SRST バージョンでは、安全な接続をサポートしたり、セキュリティを有効にしたりすることができませんでした。SRST ルータがフォールバック モードとして Secure SRST を実行できない場合（つまり、Cisco Unified Communications Manager との TLS ハンドシェイクを完了できない場合）、証明書は Cisco IP Phone のコンフィギュレーション ファイルに追加されません。Cisco Unified SRST ルータの証明書がないと、Cisco Unified SRST がフォールバック モードのときに、Cisco Unified IP Phone が保護されていない（クリアテキスト）通信を使用する原因となります。クリアテキスト モードでの検出およびフォールバックの機能は、Cisco Unified IP Phone ファームウェアに組み込まれています。クリアテキスト モードの詳細については、『[Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways](#)』を参照してください。

SRST ルータおよび TLS プロトコル

TLS バージョン 1.0 は、Cisco Unified IP Phone、Secure Cisco Unified SRST ルータ、および Cisco Unified Communications Manager の間に Secure TCP チャンネルを提供します。TLS プロセスは、Cisco Unified Communications Manager の登録時に、Cisco Unified IP Phone が TLS 接続を確立することから始まります。Cisco Unified Communications Manager が Cisco Unified SRST にフォールバックするように設定されていると仮定すると、Cisco Unified IP Phone と Secure Cisco Unified SRST ルータ間の TLS 接続も確立されます。WAN リンクまたは Cisco Unified Communications Manager で障害が発生すると、コール制御が Cisco Unified SRST ルータに戻ります。

Cisco Unified SRST ルータおよび PKI

Cisco Unified SRST ルータと Cisco Unified Communications Manager 間の証明書の転送は、Secure SRST 機能では必須です。PKI コマンドは、Secure Cisco Unified SRST の証明書を生成、インポート、およびエクスポートするために使用されます。表 9 に、Secure SRST 対応の Cisco Unified IP Phone および各電話機に該当する証明書を示します。P.169 の「[Secure SRST ルータへの電話機の証明書ファイル \(PEM 形式\) のインポート](#)」には、PKI コマンドを使用した証明書の生成、インポート、およびエクスポートに関する情報と設定が記載されています。



(注)

証明書のテキストは、設定によって異なる場合があります。また、Manufacturing Installed Certificate (MIC) をサポートする古い電話機では、CAP-RTP-00X または CAP-SJC-00X が必要になる場合があります。



(注)

シスコでは、MIC または Locally Significant Certificate (LSC) 証明書を使用する、Cisco IP Phone 7900 シリーズの電話機メモリを再利用した電話機をサポートしています。

表 9 サポートされている Cisco Unified IP Phone および証明書

Cisco Unified IP Phone 7940	Cisco Unified IP Phone 7960	Cisco Unified IP Phone 7970
<p>電話機は Distinguished Encoding Rules (DER) 形式の Certificate Authority Proxy Function (CAPF) から Locally Significant Certificate (LSC) を受け取ります。</p> <ul style="list-style-type: none"> 59fe77ccd.0 <p>ファイル名は、CAPF 証明書サブジェクト名および CAPF 証明書発行元に基づいて変更される場合があります。</p> <p>Cisco Unified Communications Manager がサードパーティ証明書プロバイダーを使用している場合、複数の .0 ファイルが存在する場合があります (2 ~ 10)。各 .0 証明書ファイルは、設定時に個別にインポートする必要があります。</p> <p>手動の登録だけがサポートされています。</p>	<p>電話機は Distinguished Encoding Rules (DER) 形式の Certificate Authority Proxy Function (CAPF) から Locally Significant Certificate (LSC) を受け取ります。</p> <ul style="list-style-type: none"> 59fe77ccd.0 <p>ファイル名は、CAPF 証明書サブジェクト名および CAPF 証明書発行元に基づいて変更される場合があります。</p> <p>Cisco Unified Communications Manager がサードパーティ証明書プロバイダーを使用している場合、複数の .0 ファイルが存在する場合があります (2 ~ 10)。各 .0 証明書ファイルは、設定時に個別にインポートする必要があります。</p> <p>手動の登録だけがサポートされています。</p>	<p>電話機には、デバイス認証に使用する Manufacturing Installed Certificate (MIC) が含まれています。Cisco 7970 が MIC を実装する場合、2 つの公開証明書ファイルが必要です。</p> <ul style="list-style-type: none"> CiscoCA.pem (証明書を認証するのに使用する Cisco Root CA) <p>(注) MIC の名前は、設定によって異なる場合があります。</p> <ul style="list-style-type: none"> a69d2e04.0. Privacy Enhanced Mail (PEM) 形式 <p>Cisco Unified Communications Manager がサードパーティ証明書プロバイダーを使用している場合、複数の .0 ファイルが存在する場合があります (2 ~ 10)。各 .0 証明書ファイルは、設定時に個別にインポートする必要があります。</p> <p>手動の登録だけがサポートされています。</p>

Secure SRST の認証および暗号化

図 7 に、Secure SRST 認証および暗号化のプロセスを示します。表 10 では、プロセスの内容について説明します。

図 7 Secure Cisco Unified SRST の認証および暗号化

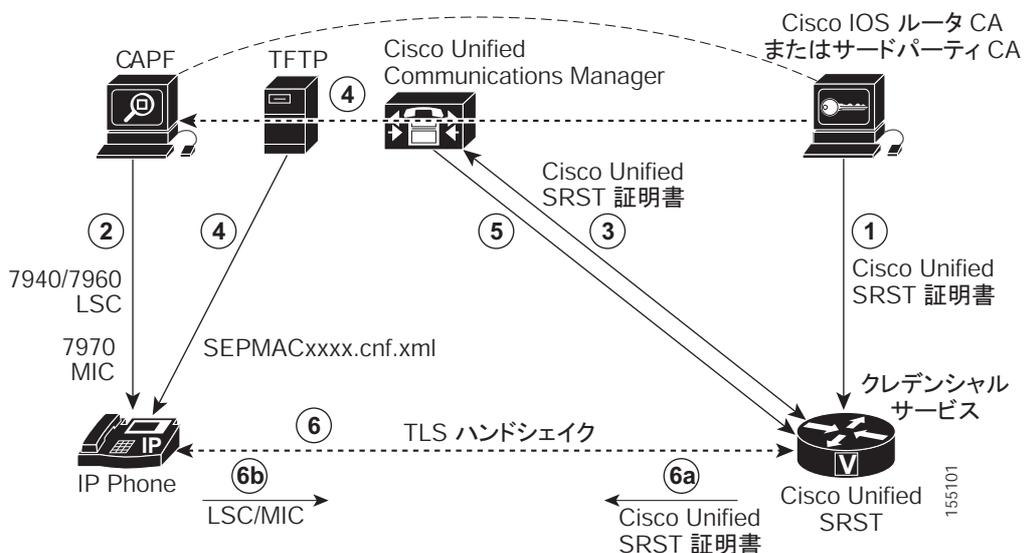


表 10 Secure SRST の認証および暗号化プロセスの概要

プロセス手順	説明または詳細
1.	<p>CA サーバが Cisco IOS ルータ CA またはサードパーティ CA であるかどうかに関わらず、CA サーバは、デバイスの証明書を SRST ゲートウェイに発行し、クレデンシャルサービスを有効にします。オプションで、Cisco IOS CA サーバを使用して SRST ルータで証明書を独自に生成することもできます。</p> <p>CA ルータは、CAPF の最終トラストポイントです。CAPF の詳細については、『Cisco Communications Manager Security Guide』を参照してください。</p>
2.	<p>CAPF は、サポートされているデバイスが LSC を要求できるプロセスです。CAPF ユーティリティはキーペアおよび CAPF に特有の証明書を生成し、クラスタ内のすべての Cisco Unified Communications Manager サーバにこの証明書をコピーし、LSC を Cisco Unified IP Phone に提供します。</p> <p>LSC は、MIC を持たない Cisco Unified IP Phone で必要です。Cisco 7970 には MIC が装備されているので、CAPF プロセスを行う必要はありません。</p>
3.	Cisco Unified Communications Manager はクレデンシャルサーバに SRST 証明書を要求し、クレデンシャルサーバは証明書で応答します。
4.	デバイスごとに、Cisco Unified Communications Manager は TFTP プロセスを使用し、Cisco Unified IP Phone の SEPMACxxxx.cnf.xml コンフィギュレーションファイルに証明書を挿入します。
5.	<p>Cisco Unified Communications Manager は、電話機の証明書情報を含む PEM 形式のファイルを Cisco Unified SRST ルータに提供します。Cisco Unified SRST ルータに PEM ファイルを提供する作業は、手動で行います。詳細については、P.155 の「Cisco Unified SRST ルータおよび PKI」を参照してください。</p> <p>Cisco Unified SRST ルータに PEM ファイルがある場合、Cisco Unified SRST ルータは IP Phone を認証して、TLS ハンドシェイクの際に IP Phone 証明書の発行元を検証できます。</p>
6.	TLS ハンドシェイクが発生すると、証明書が交換され、Cisco Unified IP Phone と Cisco Unified SRST ルータの間で相互の認証と登録が行われます。
a.	Cisco Unified SRST ルータは証明書を送信し、電話機は手順 4 で Cisco Unified Communications Manager から受信した証明書に対して証明書を検証します。
b.	Cisco Unified IP Phone は Cisco Unified SRST ルータに LSC または MIC を提供します。ルータは、手順 5 で提供された PEM 形式のファイルを使用して LSC または MIC を検証します。



(注)

電話機とルータの証明書が交換された後、メディアが自動的に暗号化され、SRST ルータとの TLS 接続が確立されます。

Secure SRST ルータの Cisco IOS クレデンシャル サーバ

Secure SRST は、Secure SRST ルータで実行されるクレデンシャル サーバを導入しています。クライアントである Cisco Unified Communications Manager が TLS チャンネルを介して証明書を要求する場合、クレデンシャル サーバは SRST ルータの証明書を Cisco Unified Communications Manager に提供します。Cisco Unified Communications Manager は、Cisco Unified IP Phone コンフィギュレーション ファイルに SRST ルータの証明書を挿入し、電話機にコンフィギュレーション ファイルをダウンロードします。Secure Cisco Unified IP Phone は、証明書を使用して、フォールバック操作時に SRST ルータを認証します。クレデンシャル サービスは、デフォルトの TCP ポート 2445 で実行されます。

call-manager-fallback モードでクレデンシャル サーバを設定するには、次の 3 つの Cisco IOS コマンドを使用します。

- `credentials`
- `ip source-address (credentials)`
- `trustpoint (credentials)`

2 つの Cisco IOS コマンドが、クレデンシャル サーバのデバッグおよび検証機能を提供します。

- `debug credentials`
- `show credentials`

Cisco Unified IP Phone への Secure Cisco Unified SRST の確立

図 8 および表 11 は、SRST ルータ、Cisco Unified Communications Manager、および Cisco Unified IP Phone のクレデンシャル サーバの相互作用を示し、Cisco Unified IP Phone への Secure SRST の確立について説明します。

図 8 SRST ルータ、Cisco Unified Communications Manager、および Cisco Unified IP Phone のクレデンシャル サーバの相互作用



表 11 Secure SRST の確立

モード	プロセス	説明または詳細
標準モード	Cisco Unified IP Phone は DHCP を設定し、TFTP サーバのアドレスを取得します。	—
	Cisco Unified IP Phone は、TFTP サーバから CTL ファイルを取得します。	CTL ファイルには、電話機が信頼する必要がある証明書が含まれます。
	Cisco IP Phone は TLS プロトコル チャネルを開き、Cisco Unified Communications Manager に登録します。	Cisco Unified Communications Manager は、Secure Cisco Unified SRST ルータ情報および Cisco Unified SRST ルータの証明書を Cisco Unified IP Phone にエクスポートします。電話機は証明書をコンフィギュレーションに保管します。電話機に Cisco Unified SRST 証明書が保管されると、Cisco Unified SRST ルータが安全であると見なされます。 図 8 を参照してください。
	Cisco Unified IP Phone が「認証済み」または「暗号化済み」として設定されており、Cisco Unified Communications Manager が混合モードに設定されている場合、電話機はコンフィギュレーションファイルで SRST 証明書を検索します。SRST 証明書が検出されると、デフォルトポートへのスタンバイ TLS 接続が開きます。デフォルトのポートは Cisco Unified IP Phone TCP ポートに 443 を追記した数字です。つまり、Cisco Unified SRST ルータのポート 2443 です。	セカンダリ Cisco Unified Communications Manager が存在しておらず、Cisco Unified SRST がバックアップデバイスとして設定されていると仮定して、SRST ルータへの接続が自動的に行われます。 図 8 を参照してください。 Cisco Unified Communications Manager が、安全なモードである混合モードに設定されている必要があります。
WAN に障害が発生した場合、Cisco Unified IP Phone が Cisco Unified SRST 登録を開始します。		
SRST モード	Cisco Unified IP Phone は、安全な通信を行うためにデフォルトポートで SRST ルータに登録します。	—

Secure SRST の設定方法

設定に関する次の項では、Secure Cisco Unified SRST ルータと Cisco Unified IP Phone が TLS ハンドシェイク時に確実に相互の認証を要求できるようにします。TLS ハンドシェイクは、WAN リンク障害の前後に関係なく、電話機が Cisco Unified SRST ルータに登録するときに行われます。

ここでは、次の内容について説明します。

- [安全に通信を行うための Cisco Unified SRST ルータの準備 \(P.160\)](#) (必須)
- [Secure SRST ルータへの電話機の証明書ファイル \(PEM 形式\) のインポート \(P.169\)](#) (必須)
- [Secure Cisco Unified SRST ルータへの Cisco Unified Communications Manager の設定 \(P.176\)](#) (必須)
- [Secure Cisco Unified SRST ルータでの SRST モードの有効化 \(P.180\)](#) (必須)
- [電話機のステータスおよび登録の確認 \(P.182\)](#) (必須)

安全に通信を行うための Cisco Unified SRST ルータの準備

次の作業では、安全な通信を行うために Cisco Unified SRST ルータを準備します。

- [Cisco IOS 証明書サーバへの CA サーバの設定 \(P.160\)](#) (オプション)
- [CA サーバに対する Secure Cisco Unified SRST ルータの自動登録と認証 \(P.162\)](#) (必須)
- [自動証明書登録の無効化 \(P.164\)](#) (必須)
- [証明書登録の確認 \(P.165\)](#) (オプション)
- [Secure Cisco Unified SRST ルータでのクレデンシャルサービスの有効化 \(P.167\)](#) (必須)
- [クレデンシャル設定のトラブルシューティング \(P.168\)](#) (オプション)

Cisco IOS 証明書サーバへの CA サーバの設定

Cisco Unified SRST ルータが安全な通信を提供するためには、ネットワークのデバイス証明書を発行する CA サーバが 1 台必要です。CA サーバは、サードパーティ CA でも、Cisco IOS 証明書サーバから生成されたものでも構いません。

Cisco IOS 証明書サーバは、ネットワークにサードパーティ CA を持たないユーザに対して証明書生成オプションを提供します。Cisco IOS 証明書サーバは、SRST ルータまたは異なる Cisco IOS ルータで実行できます。

サードパーティ CA を持っていない場合、CA サーバの有効化および設定の詳細については、『[Cisco IOS Certificate Server](#)』を参照してください。次に、設定例を示します。

要約手順

1. `crypto pki server cs-label`
2. `database level {minimal | names | complete}`
3. `database url root-url`
4. `issuer-name DN-string`
5. `grant auto`
6. `no shutdown`

詳細手順

	コマンドまたはアクション	目的
ステップ 1	<pre>crypto pki server cs-label</pre> <pre>Router (config)# crypto pki server srstcaserver</pre>	<p>証明書サーバを有効にし、certificate server コンフィギュレーション モードを開始します。</p> <p> (注) RSA キー ペアを手動で生成した場合、<i>cs-label</i> 引数がキー ペアの名前と一致する必要があります。</p> <p>証明書サーバの詳細については、『Cisco IOS Certificate Server』を参照してください。</p>
ステップ 2	<pre>database level {minimal names complete}</pre> <pre>Router (cs-server)# database level complete</pre>	<p>証明書登録データベースに保存されるデータ タイプを制御します。</p> <ul style="list-style-type: none"> • minimal: 競合を発生させずに新しい証明書を発行し続けるために、十分な情報だけを保存します。これがデフォルト値です。 • names: minimal レベルで提供される情報に加えて、各証明書のシリアル番号と件名を保存します。 • complete: minimal および names レベルで提供される情報に加えて、発行した各証明書をデータベースに書き込みます。 <p> (注) complete キーワードを指定すると、大量の情報が生成されます。このキーワードを使用する場合は、database url コマンドを使用して、データを保存する外部 TFTP サーバも指定する必要があります。</p>
ステップ 3	<pre>database url root-url</pre> <pre>Router (cs-server)# database url nvram</pre>	<p>証明書サーバのすべてのデータベース エントリを書き込む場所を指定します。crypto pki server コマンドを使用して証明書サーバを作成したら、このコマンドを使用して、発行されたすべての証明書の結合リストを指定します。<i>root-url</i> 引数は、データベース エントリを書き込む場所を指定します。</p> <ul style="list-style-type: none"> • データベース エントリが書き込まれるデフォルトの場所はフラッシュですが、この作業には NVRAM が推奨されます。
ステップ 4	<pre>issuer-name DN-string</pre> <pre>Router (cs-server)# issuer-name CN=srstcaserver</pre>	<p>CA 発行元名を指定した認定者名 (DN ストリング) に設定します。デフォルト値は次のとおりです。</p> <p>issuer-name CN=<i>cs-label</i></p>
ステップ 5	<pre>grant auto</pre> <pre>Router (cs-server)# grant auto</pre>	<p>自動的な証明書がすべての要求者に発行されるようにします。</p> <ul style="list-style-type: none"> • このコマンドは登録時のみに使用され、P.164 の「自動証明書登録の無効化」で削除されます。
ステップ 6	<pre>no shutdown</pre> <pre>Router (cs-server)# no shutdown</pre>	<p>Cisco IOS 証明書サーバを有効にします。</p> <ul style="list-style-type: none"> • このコマンドを使用できるのは、すべての証明書サーバの設定が完了してからだけです。

例

次の例は、CA を生成する 1 つの方法を示しています。

```
Router(config)# crypto pki server srstcaserver
Router(cs-server)# database level complete
Router(cs-server)# database url nvram
Router(cs-server)# issuer-name CN=srstcaserver
Router(cs-server)# grant auto

% This will cause all certificate requests to be automatically granted.
Are you sure you want to do this? [yes/no]: y
Router(cs-server)# no shutdown
% Once you start the server, you can no longer change some of
% the configuration.
Are you sure you want to do this? [yes/no]: y
% Generating 1024 bit RSA keys ...[OK]
% Certificate Server enabled.
```

CA サーバに対する Secure Cisco Unified SRST ルータの自動登録と認証

Secure Cisco Unified SRST ルータでは、トラストポイントを定義する必要があります。つまり、CA サーバからデバイスの証明書を取得する必要があります。この手順は、証明書の登録と呼ばれます。登録されると、Secure Cisco Unified SRST ルータは Secure SRST ルータとして Cisco Unified Communications Manager に認識されます。

CA サーバに Secure Cisco Unified SRST ルータを登録するためのオプションは、自動登録、カットアンドペースト、および TFTP の 3 つです。CA サーバが Cisco IOS 証明書サーバの場合、自動登録を使用できます。それ以外の場合は、手動の登録が必要です。手動の登録とは、カットアンドペーストまたは TFTP を指します。

自動登録に対しては、**enrollment url** コマンドを使用します。SRST ルータを認証するには、**crypto pki authenticate** コマンドを使用します。コマンドの使用方法については、『[Certification Authority Interoperability Commands](#)』を参照してください。自動登録の例は、『[Certificate Enrollment Enhancements](#)』から入手できます。P.164 の「例」に、設定例を示します。

要約手順

1. **crypto pki trustpoint name**
2. **enrollment url url**
3. **revocation-check method l**
4. **exit**
5. **crypto pki authenticate name**
6. **crypto pki enroll name**

詳細手順

	コマンドまたはアクション	目的
ステップ 1	<pre>crypto pki trustpoint name Router(config)# crypto pki trustpoint srstca</pre>	<p>ルータが使用する必要がある CA を宣言し、ca-trustpoint コンフィギュレーション モードを開始します。</p> <ul style="list-style-type: none"> 指定される名前は、P.167 の「Secure Cisco Unified SRST ルータでのクレデンシャル サービスの有効化」で宣言されるトラストポイント名と同じになります。
ステップ 2	<pre>enrollment url url Router(ca-trustpoint)# enrollment url http://10.1.1.22</pre>	<p>CA の登録パラメータを指定します。</p> <ul style="list-style-type: none"> url url : ルータが証明書要求を送信する CA の URL を指定します。 登録にシスコ独自の SCEP を使用している場合、url は <code>http://CA_name</code> という形式にする必要があります。ここで、CA_name は、Cisco IOS CA のホスト Domain Name System (DNS; ドメインネームシステム) 名または IP アドレスを表します。 P.160 の「Cisco IOS 証明書サーバへの CA サーバの設定」に記載されている手順を使用した場合、URL は、手順 1 で設定した証明書サーバルータの IP アドレスです。サードパーティ CA が使用された場合、IP アドレスは外部 CA になります。
ステップ 3	<pre>revocation-check method1 Router(ca-trustpoint)# revocation-check none</pre>	<p>証明書の失効ステータスをチェックします。method1 引数は、ルータが証明書の失効ステータスをチェックするために使用する方法です。この作業で使用できる方法は、none だけです。none キーワードは、失効チェックが実行されず、証明書が常に受け入れられることを意味します。</p> <ul style="list-style-type: none"> この作業では、none キーワードを使用することが必須です。
ステップ 4	<pre>exit Router(ca-trustpoint)# exit</pre>	<p>ca-trustpoint コンフィギュレーション モードを終了し、global コンフィギュレーション モードに戻ります。</p>
ステップ 5	<pre>crypto pki authenticate name Router(config)# crypto pki authenticate srstca</pre>	<p>CA から証明書を取得することにより、CA を認証します。</p> <ul style="list-style-type: none"> CA の名前を引数として取得します。
ステップ 6	<pre>crypto pki enroll name Router(config)# crypto pki enroll srstca</pre>	<p>CA から SRST ルータの証明書を取得します。</p> <ul style="list-style-type: none"> CA の名前を引数として取得します。

例

次の例では、Cisco Unified SRST ルータを自動登録および認証します。

```
Router(config)# crypto pki trustpoint srstca
Router(ca-trustpoint)# enrollment url http://10.1.1.22
Router(ca-trustpoint)# revocation-check none
Router(ca-trustpoint)# exit
Router(config)# crypto pki authenticate srstca

Certificate has the following attributes:
Fingerprint MD5: 4C894B7D 71DBA53F 50C65FD7 75DDBFCA
Fingerprint SHA1: 5C3B6B9E EFA40927 9DF6A826 58DA618A BF39F291
% Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.

Router(config)# crypto pki enroll srstca
%
% 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 fully-qualified domain name in the certificate will be: router.cisco.com
% The subject name in the certificate will be: router.cisco.com
% Include the router serial number in the subject name? [yes/no]: y
% The serial number in the certificate will be: D0B9E79C
% Include an IP address in the subject name? [no]: n
Request certificate from CA? [yes/no]: y
% Certificate request sent to Certificate Authority
% The certificate request fingerprint will be displayed.
% The 'show crypto pki certificate' command will also show the fingerprint.

Sep 29 00:41:55.427: CRYPTO_PKI: Certificate Request Fingerprint MD5: D154FB75
2524A24D 3D1F5C2B 46A7B9E4
Sep 29 00:41:55.427: CRYPTO_PKI: Certificate Request Fingerprint SHA1: 0573FBB2
98CD1AD0 F37D591A C595252D A17523C1
Sep 29 00:41:57.339: %PKI-6-CERTRET: Certificate received from Certificate Authority
```

自動証明書登録の無効化

grant auto コマンドを使用すると証明書が発行されます。このコマンドは、P.160の「Cisco IOS 証明書サーバへの CA サーバの設定」に記載されているオプションの作業でアクティブ化されます。



(注)

セキュリティ上の最善策は、証明書が引き続き許可されないように、**grant auto** コマンドを無効にすることです。

要約手順

1. **crypto pki server cs-label**
2. **shutdown**
3. **no grant auto**
4. **no shutdown**

詳細手順

	コマンドまたはアクション	目的
ステップ 1	<code>crypto pki server cs-label</code> Router (config)# <code>crypto pki server srstcaserver</code>	証明書サーバを有効にし、certificate server コンフィギュレーションモードを開始します。  (注) RSA キー ペアを手動で生成した場合、 <code>cs-label</code> 引数がキー ペアの名前と一致する必要があります。
ステップ 2	<code>shutdown</code> Router (cs-server)# <code>shutdown</code>	Cisco IOS 証明書サーバを無効にします。
ステップ 3	<code>no grant auto</code> Router (cs-server)# <code>no grant auto</code>	自動的な証明書がすべての要求者に発行されないようにします。 <ul style="list-style-type: none"> このコマンドは登録時にのみ使用するので、この作業で削除する必要があります。
ステップ 4	<code>no shutdown</code> Router (cs-server)# <code>no shutdown</code>	Cisco IOS 証明書サーバを有効にします。 <ul style="list-style-type: none"> このコマンドを使用できるのは、すべての証明書サーバの設定が完了してからだけです。

次の作業

手動の登録手順については、『[Manual Certificate Enrollment \(TFTP and Cut-and-Paste\)](#)』を参照してください。

証明書登録の確認

Cisco IOS 証明書サーバを CA として使用した場合、証明書登録を確認するには `show running-config` コマンドを使用し、CA サーバのステータスを確認するには `show crypto pki server` コマンドを使用します。

要約手順

1. `show running-config`
2. `show crypto pki server`

詳細手順

ステップ 1 `show running-config`

CA サーバ (01) およびデバイス (02) の証明書の作成を確認するには、`show running-config` コマンドを使用します。この例は、登録された証明書を示します。

```

Router# show running-config
.
.
.
! SRST router device certificate.
crypto pki certificate chain srstca
certificate 02
 308201AD 30820116 A0030201 02020102 300D0609 2A864886 F70D0101 04050030
17311530 13060355 0403130C 73727374 63617365 72766572 301E170D 30343034
31323139 35323233 5A170D30 35303431 32313935 3232335A 30343132 300F0603
55040513 08443042 39453739 43301F06 092A8648 86F70D01 09021612 6A61736F
32363931 2E636973 636F2E63 6F6D305C 300D0609 2A864886 F70D0101 01050003
4B003048 024100D7 0CC354FB 5F7C1AE7 7A25C3F2 056E0485 22896D36 6CA70C19
C98F9BAE AE9D1F9B D4BB7A67 F3251174 193BB1A3 12946123 E5C1CCD7 A23E6155
FA2ED743 3FB8B902 03010001 A330302E 300B0603 551D0F04 04030205 A0301F06
03551D23 04183016 8014F829 CE97AD60 18D05467 FC293963 C2470691 F9BD300D
06092A86 4886F70D 01010405 00038181 007EB48E CAE9E1B3 D1E7A185 D7F0D565
CB84B17B 1151BD78 B3E39763 59EC650E 49371F6D 99CBD267 EB8ADF9D 9E43A5F2
FB2B18A0 34AF6564 11239473 41478AFC A86E6DA1 AC518E0B 8657CEBB ED2BDE8E
B586FE67 00C358D4 EFDD8D44 3F423141 C2D331D3 1EE43B6E 6CB29EE7 0B8C2752
C3AF4A66 BD007348 D013000A EA3C206D CF
quit
certificate ca 01
30820207 30820170 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
17311530 13060355 0403130C 73727374 63617365 72766572 301E170D 30343034
31323139 34353136 5A170D30 37303431 32313934 3531365A 30173115 30130603
55040313 0C737273 74636173 65727665 7230819F 300D0609 2A864886 F70D0101
01050003 818D0030 81890281 8100C3AF EE1E4BB1 9922A8DA 2BB9DC8E 5B1BD332
1051C9FE 32A971B3 3C336635 74691954 98E765B1 059E24B6 32154E99 105CA989
9619993F CC72C525 7357EBAC E6335A32 2AAF9391 99325BFD 9B8355EB C10F8963
9D8FC222 EE8AC831 71ACD3A7 4E918A8F D5775159 76FBF499 5AD0849D CAA41417
DD866902 21E5DD03 C37D4B28 0FAB0203 010001A3 63306130 0F060355 1D130101
FF040530 030101FF 300E0603 551D0F01 01FF0404 03020186 301D0603 551D0E04
160414F8 29CE97AD 6018D054 67FC2939 63C24706 91F9BD30 1F060355 1D230418
30168014 F829CE97 AD6018D0 5467FC29 3963C247 0691F9BD 300D0609 2A864886
F70D0101 04050003 8181007A F71B25F9 73D74552 25DFD03A D8D1338F 6792C805
47A81019 795B5AAE 035400BB F859DABF 21892B5B E71A8283 08950414 8633A8B2
C98565A6 C09CA641 88661402 ACC424FD 36F23360 ABFF4C55 BB23C66A C80A3A57
5EE85FF8 C1B1A540 E818CE6D 58131726 BB060974 4E1A2F4B E6195522 122457F3
DEDBAAD7 3780136E B112A6
quit

```

ステップ 2 show crypto pki server

起動手順の後に CA サーバのステータスを確認するには、**show crypto pki server** コマンドを使用します。

```

Router# show crypto pki server

Certificate Server srstcaserver:
Status: enabled
Server's configuration is locked (enter "shut" to unlock it)
Issuer name: CN=srstcaserver
CA cert fingerprint: AC9919F5 CAFE0560 92B3478A CFF5EC00
Granting mode is: auto
Last certificate issued serial number: 0x2
CA certificate expiration timer: 13:46:57 PST Dec 1 2007
CRL NextUpdate timer: 14:54:57 PST Jan 19 2005
Current storage dir: nvram
Database Level: Complete - all issued certs written as <serialnum>.cer

```

Secure Cisco Unified SRST ルータでのクレデンシャル サービスの有効化

Cisco Unified SRST ルータが独自の証明書を取得したら、Cisco Unified Communications Manager に証明書を提供する必要があります。クレデンシャル サービスを有効にすると、Cisco Unified Communications Manager は Secure SRST デバイスの証明書を取得して、Cisco Unified IP Phone のコンフィギュレーションファイルに保管することができます。

すべての Cisco Unified SRST ルータのクレデンシャル サービスをアクティブにします。



(注)

セキュリティ上の最善策は、コントロールプレーン ポリシングを使用してクレデンシャル サービスポートを保護することです。コントロールプレーン ポリシングは、ゲートウェイを保護し、トラフィックの負荷が大きいときもパケットの転送とプロトコルの状態を維持します。コントロールプレーンの詳細については、『[Control Plane Policing](#)』を参照してください。また、[P.192](#) の「[コントロールプレーン ポリシング：例](#)」に設定例を示します。

要約手順

1. `credentials`
2. `ip source-address ip-address [port port]`
3. `trustpoint trustpoint-name`
4. `exit`

詳細手順

	コマンドまたはアクション	目的
ステップ 1	<code>credentials</code> Router(config)# <code>credentials</code>	Cisco Unified SRST ルータの証明書を Cisco Unified Communications Manager に提供し、 <code>credentials</code> コンフィギュレーションモードを開始します。
ステップ 2	<code>ip source-address ip-address [port port]</code> Router(config-credentials)# <code>ip source-address 10.1.1.22 port 2445</code>	Cisco Unified SRST ルータが、指定した IP アドレスとポートを介して Cisco Unified Communications Manager からメッセージを受信できるようにします。 <ul style="list-style-type: none"> • <code>ip-address</code> : IP アドレスは既存のルータの IP アドレスです。通常、ルータのイーサネットポートのアドレスの 1 つです。 • <code>port port</code> : (オプション) Cisco Unified Communications Manager からメッセージを受信するためにゲートウェイ ルータが接続されるポート。ポート番号は 2000 ~ 9999 です。デフォルトのポート番号は 2445 です。
ステップ 3	<code>trustpoint trustpoint-name</code> Router(config-credentials)# <code>trustpoint srstca</code>	Cisco Unified SRST ルータの証明書と関連付けるトラストポイントの名前を指定します。 <code>trustpoint-name</code> 引数はトラストポイント名で、SRST デバイスの証明書に対応します。 <ul style="list-style-type: none"> • トラストポイント名は、P.162 の「CA サーバに対する Secure Cisco Unified SRST ルータの自動登録と認証」で宣言したトラストポイント名と同じにする必要があります。

	コマンドまたはアクション	目的
ステップ 4	<code>exit</code> Router(config-credentials)# <code>exit</code>	credentials コンフィギュレーション モードを終了します。

例

```
Router(config)# credentials
Router(config-credentials)# ip source-address 10.1.1.22 port 2445
Router(config-credentials)# trustpoint srstca
Router(config-credentials)# exit
```

クレデンシャル設定のトラブルシューティング

次の手順では、クレデンシャル設定を表示するか、Cisco Unified SRST ルータのクレデンシャル設定のデバッグを設定します。

要約手順

1. **show credentials**
2. **debug credentials**

詳細手順

ステップ 1 show credentials

Secure Cisco Unified SRST のフォールバック時に使用する Cisco Unified Communications Manager に提供される Cisco Unified SRST ルータのクレデンシャル設定を表示するには、**show credentials** コマンドを使用します。

```
Router# show credentials

Credentials IP: 10.1.1.22
Credentials PORT: 2445
Trustpoint: srstca
```

ステップ 2 debug credentials

Cisco Unified SRST ルータのクレデンシャル設定のデバッグを設定するには、**debug credentials** コマンドを使用します。

```
Router# debug credentials

Credentials server debugging is enabled
Router#
Sep 29 01:01:50.903: Credentials service: Start TLS Handshake 1 10.1.1.13 2187
Sep 29 01:01:50.903: Credentials service: TLS Handshake returns OPSSLReadWouldBlockErr
Sep 29 01:01:51.903: Credentials service: TLS Handshake returns OPSSLReadWouldBlockErr
Sep 29 01:01:52.907: Credentials service: TLS Handshake returns OPSSLReadWouldBlockErr
Sep 29 01:01:53.927: Credentials service: TLS Handshake completes.
```

関連コマンド

次のコマンドを使用して、証明書が見つからない（認証しようとする証明書が欠落している）かどうかを表示したり、特定の証明書が照合されたことを表示したりします（したがって、電話機の認証に使用されたルータがわかります）。

- `debug crypto pki messages`
- `debug crypto pki transactions`

Secure SRST ルータへの電話機の証明書ファイル（PEM 形式）のインポート

この作業では、Cisco IP Unified Phone に必要な作業のプロビジョニングを完了して、Secure SRST を認証します。

Cisco Unified Communications Manager 4.X.X およびそれ以前のバージョン

Cisco Unified Communications Manager 4.X.X およびそれ以前のバージョンを実行しているシステムの場合、Secure Cisco Unified SRST ルータは電話機の証明書を取得して、TLS ハンドシェイク時に Cisco Unified IP Phone を認証できるようにする必要があります。Cisco Unified IP Phone が異なると、異なる証明書が使用されます。表 9 (P.156) に、電話機の各タイプに必要な証明書を示します。

証明書は、Cisco Unified Communications Manager から Cisco Unified SRST ルータに手動でインポートする必要があります。証明書の数は、Cisco Unified Communications Manager の設定によって異なります。手動の登録とは、カットアンドペーストまたは TFTP を指します。手動の登録手順については、『*Manual Certificate Enrollment (TFTP and Cut-and-Paste)*』を参照してください。各電話機または PEM ファイルに対して、登録手順を繰り返します。

Cisco Unified Communications Manager 5.0 およびそれ以降のバージョン

Cisco Unified Communications Manager 5.0 およびそれ以降のバージョンを実行しているシステムには、表 9 に示されている要件に加えて、4 つの証明書（CAPF、CiscoCA、CiscoManufactureCA、および CiscoRootCA2048）が必要です。これらの証明書は、Cisco Unified SRST ルータにコピーアンドペーストする必要があります。



(注)

CiscoRootCA は、CiscoRoot2048CA と呼ばれます。

前提条件

最後のコンフィギュレーション コマンド (`crypto pki authenticate`) が次のプロンプトを発行するときに、有効な証明書が必要になります。

```
Enter the base 64 encoded CA certificate.  
End with a blank line or the word "quit" on a line by itself
```

Cisco Unified Communications Manager 4.X.X およびそれ以前のバージョン

Cisco Unified Communications Manager 4.X.X およびそれ以前のバージョンの場合、Cisco Unified Communications Manager のメニュー バーで、**Program Files > Cisco > Certificates** を選択することで、証明書を検索できます。

Windows Wordpad または Notepad を使用して .0 ファイルを開き、内容を SRST ルータ コンソールにコピー アンド ペーストします。次に、.pem ファイルに対して同じ手順を繰り返します。「-----BEGIN CERTIFICATE-----」と「-----END CERTIFICATE-----」の間に表示されるすべての内容をコピーします。

Cisco Unified Communications Manager 5.0 およびそれ以降のバージョン

Cisco Unified Communications Manager 5.0 およびそれ以降のバージョンの場合、次の手順を実行します。

-
- ステップ 1** Cisco Unified Communications Manager にログインします。
 - ステップ 2** **Security > Certificate Management > Download Certificate/CTL** に進みます。
 - ステップ 3** **Download Trust Cert** を選択し、**Next** をクリックします。
 - ステップ 4** **CAPF-trust** を選択し、**Next** をクリックします。
 - ステップ 5** **CiscoCA** を選択し、**Next** をクリックします。
 - ステップ 6** **Continue** をクリックします。
 - ステップ 7** ファイル名をクリックします。
 - ステップ 8** 「-----BEGIN CERTIFICATE-----」と「-----END CERTIFICATE-----」の間に表示されるすべての内容を、後で取得できる場所にコピーします。
 - ステップ 9** CiscoManufactureCA、CiscoRootCA2048、および CAPF に対して、手順 5～8 を繰り返します。
-

制約事項

仮想 Web サーバを介した Cisco Unified Communications Manager からの HTTP 自動登録は、サポートされていません。

要約手順

1. `crypto pki trustpoint name`
2. `revocation-check method l`
3. `enrollment terminal`
4. `exit`
5. `crypto pki authenticate name`

詳細手順

	コマンドまたはアクション	目的
ステップ 1	<pre>crypto pki trustpoint name</pre> <pre>Router (config)# crypto pki trustpoint 7970</pre>	<p>ルータが使用する必要がある CA を宣言し、<code>ca-trustpoint</code> コンフィギュレーション モードを開始します。</p> <ul style="list-style-type: none"> • Cisco Unified Communications Manager 5.0 を使用している場合、4 つの <code>name</code> 引数 (CAPF、CiscoCA、CiscoManufactureCA、および CiscoRootCA2048) を個別に設定する必要があります。P.175 の「Cisco Unified Communications Manager 5.0 およびそれ以降のバージョンの例」を参照してください。
ステップ 2	<pre>revocation-check method1</pre> <pre>Router(ca-trustpoint)# revocation-check none</pre>	<p>証明書の失効ステータスをチェックします。<code>method1</code> 引数は、ルータが証明書の失効ステータスをチェックするために使用する的方法です。この作業で使用できる方法は、none だけです。none キーワードは、失効チェックが実行されず、証明書が常に受け入れられることを意味します。</p> <ul style="list-style-type: none"> • この作業では、none キーワードを使用することが必須です。
ステップ 3	<pre>enrollment terminal</pre> <pre>Router(ca-trustpoint)# enrollment terminal</pre>	<p>手動のカット アンド ペースト証明書登録を指定します。</p>
ステップ 4	<pre>exit</pre> <pre>Router(ca-trustpoint)# exit</pre>	<p><code>ca-trustpoint</code> コンフィギュレーション モードを終了し、<code>global</code> コンフィギュレーションに戻ります。</p>
ステップ 5	<pre>crypto pki authenticate name</pre> <pre>Router(config)# crypto pki authenticate 7970</pre>	<p>CA から証明書を取得することにより、CA を認証します。</p> <ul style="list-style-type: none"> • <code>crypto pki trustpoint</code> コマンドで使用したのと同じ <code>name</code> 引数を入力します。

例

ここでは、次の内容について説明します。

- Cisco Unified Communications Manager 4.X.X およびそれ以前のバージョンの例 (P.172)
- Cisco Unified Communications Manager 5.0 およびそれ以降のバージョンの例 (P.175)

Cisco Unified Communications Manager 4.X.X およびそれ以前のバージョンの例

次の例は、Cisco Unified SRST ルータ（Cisco 7970、7960、PEM）にインポートされた3つの証明書を示しています。

```
Router(config)# crypto pki trustpoint 7970
Router(ca-trustpoint)# revocation-check none
Router(ca-trustpoint)# enrollment terminal
Router(ca-trustpoint)# exit
Router(config)# crypto pki authenticate 7970

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
MIIDQCcAPCgAwIBAgIQNT+yS9cPFKNGwfOprHJWdTANBgkqhkiG9w0BAQUFADAu
MRyWfAYDVQQKEw1DaXNjbjBTExN0ZW1zMRQwEgYDVQQDEwTDQVAtUlRQLTAwMjAe
Fw0wMzEwMTAyMDE4NDlaFw0yMzEwMTAyMDI3MzdaMC4xZjAUBGNVBAoTDUNpc2Nv
IFN5c3R1bXN5c3R1bXN5c3R1bXN5c3R1bXN5c3R1bXN5c3R1bXN5c3R1bXN5c3
AAOCAQ0AMIIBCAKCAQEAAxZlBK19w/2NZVVvpjCPrpW1cCY7V1q9lhZl85RZZdnQ
2M4CufgIzNa3zYxGJIAYeFfcRECNMB3f5A+x7xNiEuzE87UPvK+7S80uWCY0Uhtl
AVVf5NQgZ3YDN0NXg5MmONb81T86F55EZYVacOXGne77TSIbIdejrTgYQXGP2MJx
Qhg+ZQlGFDRzbhFM84Duv2Msez+l+SqmQ080kIckqE9Nr3/XCSj1hXZNNVg8D+mv
Hth2P6KZqAKXAAStGRLSZX3jNbS8tveJ3Gi5+s9+66KKK2PD0iDwHcRkKcUhb7g
lI++U/5nswjUDIAPH715Ds2rn9ehkMGipGLF8kpuCwIBA60BwzCBwDALBgNVHQ8E
BAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUUpI4ojuLgmKTn5wLFal
mrTUm5YwbwYDVR0fBGgwZjBkoGKgYIYtaHR0cDovL2NhC1ydHAtMDAyL0N1cnRf
bnJvbGwvQ0FQLVJUUC0wMDIuY3Jshi9maWx1Oj8vXFxjYXAtcnRwLTAwM1xZDzXJ0
RW5yb2xsXENBUC1SVFAtMDAyLmNybDAQBgkrBgEAAI3FQEEAwIBADANBgkqhkiG
9w0BAQUFAAOCAQEAVoOM78TaOtHqj7sVL/5u5VChlyvU168f0piJLNWip2vDRihm
E+DlXdwMS5JaqUtuaSd/m/xzxpCRJm4ZRRwPq6VeaiiQGKjFuZEE5jSKiSAK7eHg
tup4HP/ZfKSwPA40DlsGSYsKNMm3OmVOCQUMH02lPkS/eEQ9sIw6QS7uuHN4y4CJ
NPNRbpFRLw06hnStCZhtGpKEHnY213QOy3h/EWhbnpOMZ+hdr20Fujsi6G1+L39l
aRjjeD708f2fYoz9wnEpZbnt2Kzse3uhU1Ygq1D1x9yuPq388C18HwDmCj4OVTXux
V6Y47H1yv/GJM8FvdgvKlExbGTFnlHpPiaG9tQ==
quit
Certificate has the following attributes:
Fingerprint MD5: F7E150EA 5E6E3AC5 615FC696 66415C9F
Fingerprint SHA1: 1BE2B503 DC72EE28 0C0F6B18 798236D8 D3B18BE6
% Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.
% Certificate successfully imported

Router(config)# crypto pki trustpoint 7960
Router(ca-trustpoint)# revocation-check none
Router(ca-trustpoint)# enrollment terminal
Router(ca-trustpoint)# exit
Router(config)# crypto pki authenticate 7960

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
MIICKDCCAZGgAwIBAgIC8wEwDQYJKoZIhvcNAQEFBQAwQDELMAkGA1UEBhMCVVMx
GjAYBgNVBAoTEUNpc2NvIFN5c3R1bXN5c3R1bXN5c3R1bXN5c3R1bXN5c3R1bXN5
QzAwHhcnMDQwNzE1MjIzODMyWhcNMTkwNzE1MjIzODMxWjBAMQswCQYDVQQGEwJV
UzEaMBGGA1UEChMRQ2l2Y28gU3lzdGVtcyBjb250bWFTATBGNVBAoTDENBUEYtN0Q3
RDBDMDCBnzANBgkqhkiG9w0BAQEFAAOBjQAwYkCgYEA0hvMOZZ9ENYWme11YGY1
it2rvE3Nk/eqhmv8P9eqBliqt+fFBeAG0WZ5b05FetdU+BCmPnddvAeSpsfr3Z+h
x+r58f0EIBRHQLgndZ+nwYH39uwXcRWWqWw1W147YHjV7M5c/R8T6daCx4B5NBo6
kdQdQNOvR3IP7kQaCSHdM/kCAwEAAAMxMC8wDgYDVR0PAQH/BAQDAgKEMB0GA1Ud
JQQWMBQGCCGAQUFBwMBBggrBgEFBQcDBTANBgkqhkiG9w0BAQUFAAOBGCANi6x
sL6M5N1DezpsB03QmUVyXMFrONV2ysrSwcXzHu0Gj9MSJ8TwiQmVaJ47hST1F5a8
YVYJ0IdifXbXRo+/EEO7kkmFE8MZta5rM7UWj8bAer42iqA3RzQaDwuJgNWT9Fhh
GgfUNAl05h1AikxsxvixmD1LdZyCMoqJJd7B2Q==
quit
Certificate has the following attributes:
Fingerprint MD5: 4B9636DF 0F3BA6B7 5F54BE72 24762DBC
Fingerprint SHA1: A9917775 F86BB37A 5C130ED2 3E528BB8 286E8C2D
% Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.
% Certificate successfully imported
```


登録が成功し、5つのCA証明書が許可されたことを表示するには、**show crypto pki trustpoint status** コマンドを使用します。5つの証明書には、入力したばかりの3つの証明書、CAサーバの証明書、およびSRSTルータの証明書が含まれます。

```
Router# show crypto pki trustpoint status

Trustpoint 7970:
Issuing CA certificate configured:
Subject Name:
cn=CAP-RTP-002,o=Cisco Systems
Fingerprint MD5: F7E150EA 5E6E3AC5 615FC696 66415C9F
Fingerprint SHA1: 1BE2B503 DC72EE28 0C0F6B18 798236D8 D3B18BE6
State:
Keys generated ..... Yes (General Purpose)
Issuing CA authenticated ..... Yes
Certificate request(s) ..... None

Trustpoint 7960:
Issuing CA certificate configured:
Subject Name:
cn=CAPF-508A3754,o=Cisco Systems Inc,c=US
Fingerprint MD5: 6BAE18C2 0BCE391E DAE2FE4C 5810F576
Fingerprint SHA1: B7735A2E 3A5C274F C311D7F1 3BE89942 355102DE
State:
Keys generated ..... Yes (General Purpose)
Issuing CA authenticated ..... Yes
Certificate request(s) ..... None

Trustpoint PEM:
Issuing CA certificate configured:
Subject Name:
cn=CAP-RTP-001,o=Cisco Systems
Fingerprint MD5: 233C8E33 8632EA4E 76D79FEB FFB061C6
Fingerprint SHA1: F7B40B94 5831D2AB 447AB8F2 25990732 227631BE
State:
Keys generated ..... Yes (General Purpose)
Issuing CA authenticated ..... Yes
Certificate request(s) ..... None

Trustpoint srstcaserver:
Issuing CA certificate configured:
Subject Name:
cn=srstcaserver
Fingerprint MD5: 6AF5B084 79C93F2B 76CC8FE6 8781AF5E
Fingerprint SHA1: 47D30503 38FF1524 711448B4 9763FAF6 3A8E7DCF
State:
Keys generated ..... Yes (General Purpose)
Issuing CA authenticated ..... Yes
Certificate request(s) ..... None

Trustpoint srstca:
Issuing CA certificate configured:
Subject Name:
cn=srstcaserver
Fingerprint MD5: 6AF5B084 79C93F2B 76CC8FE6 8781AF5E
Fingerprint SHA1: 47D30503 38FF1524 711448B4 9763FAF6 3A8E7DCF
Router General Purpose certificate configured:
Subject Name:
serialNumber=F3246544+hostname=c2611XM-sSRST.cisco.com
Fingerprint: 35471295 1C907EC1 45B347BC 7A9C4B86
State:
Keys generated ..... Yes (General Purpose)
Issuing CA authenticated ..... Yes
Certificate request(s) ..... Yes
```

Cisco Unified Communications Manager 5.0 およびそれ以降のバージョンの例

次の例は、Cisco Unified Communications Manager 5.0 を実行するのに必要な 4 つの証明書（CAPF、CiscoCA、CiscoManufactureCA、および CiscoRootCA2048）の設定を示します。

```
Router(config)# crypto pki trustpoint CAPF
Router(ca-trustpoint)# revocation-check none
Router(ca-trustpoint)# enrollment terminal
Router(ca-trustpoint)# exit
Router(config)# crypto pki authenticate CAPF
```

```
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
MIICKjCCAZOGAwIBAgIC8wEwDQYJKoZIhvcNAQEFBQAwQTELMakGA1UEBhMCVVMx
GjAYBgNVBAoTEUNpc2NvIFN5c3RlbXMGSW5jMRYwFAYDVQQDEw1DQVBGLTU4RUFE
MkQyMB4XDTA2MDMwMTIxMjc1MloXDTEyMDIyNTIxMjc1MVowQTELMakGA1UEBhMC
VVMxGjAYBgNVBAoTEUNpc2NvIFN5c3RlbXMGSW5jMRYwFAYDVQQDEw1DQVBGLTU4
RUFEMkQyMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC99KgZT94qhozw4bOB
f8Z0tYwT214L++mC6403s3AshDi8xe8Y8sN/f/ZKRRhNixBlK4SWafXnHKJBqKZn
WtSgkRjJ3Dh0XtqcWYt8VS2sC69g8sX091skKl3m+TpWsr2T/mDXv6CceaKN+mch
gcrnNo8kamOOIG8OsQc4L6XzQIDAQABoZEWLzAOBgNVHQ8BAf8EBAMCAoQwHQYD
quit
Certificate has the following attributes:
Fingerprint MD5: 1951DJ4E 76D79FEB FFB061C6 233C8E33
Fingerprint SHA1: 222891BE Z7B89B94 447AB8F2 5831D2AB 25990732
% Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.
% Certificate successfully imported
```

```
Router(config)# crypto pki trustpoint CiscoCA
Router(ca-trustpoint)# revocation-check none
Router(ca-trustpoint)# enrollment terminal
Router(ca-trustpoint)# exit
Router(config)# crypto pki authenticate CiscoCA
```

```
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
MIIDqDCcApCgAwIBAgIQdhlL5YBU9b590QiAgMrcjVjANBgkqhkiG9w0BAQUFADAu
MRYwFAYDVQQKEw1DaXNjbyBTeXN0ZW1zMRQwEgYDVQQDEwtDQVAtUlRQLTAwMTAe
Vd54qlpc/hQDFWlbrIFkCcYhHws7vwnPsLuy1Kw2L2cP0UXxYghSsx8H4vGqdPFQ
NnYy7aKJ43SvDft4zn37n8jrvlRuz0x3mdbcBEedHbA825Yo7a8sk12tshMJ/YdMm
vny0pmDNZxmeHjgEgV03UFUn6GVCO+K1y1dUU1qpYJNYtqLkqj7wgccGjsHdHr3a
U+bw1uLgSGsQnxMWeMaWo8+6hMxw1ANPweufgZMaywIBA60BwzCBwDALBgNVHQ8E
c6Ea7fm53nQR1cSPmUVLjDBzKYDNbnEji zptaIC5fgB/S9S6C1q0YpTZF5tjUjy
WXzeYSXPrxcb0UH7IQJlogpONAAUKLoPaZU7tVDSH3hd4+VjmLyysaLUhksGFrrN
phzZrsVvllK17qpqCP11KLGAS4fSbkruq3r/6S/SpXS6/gAoljBKixP7ZW2PxcGU
1aU9cURLP095NDOFN3jBk3Sips7cVidcogowPQ==
quit
Certificate has the following attributes:
Fingerprint MD5: 21956CBR 4B9706DF 0F3BA6B7 7P54AZ72
Fingerprint SHA1: A9917775 F86BB37A 7H130ED2 3E528BB8 286E8C2D
% Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.
% Certificate successfully imported
```

```
Router(config)# crypto pki trustpoint CiscoManufactureCA
Router(ca-trustpoint)# revocation-check none
Router(ca-trustpoint)# enrollment terminal
Router(ca-trustpoint)# exit
Router(config)# crypto pki authenticate CiscoManufactureCA
```

```
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
MIIE2TCCA8GgAwIBAgIKamlnswAAAAAAZANBgkqhkiG9w0BAQUFADA1MRYwFAYD
D/g2qgFEMkHFp68dGf/2c5k5WnNnYhM0DR9eLXBSZBcG7FNcXNtq6jUAQQIBA60C
AecwggHjMBIGA1UdEwEB/wQIMAYBAf8CAQAwHQYDVR0OBBYEFNDFIiarT0Zg7K4F
kcfWtGwR/dsMASGALUdDwQEAWIBhJAQBgkrBgEEAYI3FQSEAwIBADAZBgkrBgEE
AYI3FAIEDB4KAFMAdQBIAEMAQTAfBgNVHSMEGDAwBQn88gVHm6aAgkWrSugjWBf
2nsvqjBDBgNVHR8EPDA6MDIgdGQwA0hjJodHRwOi8vd3d3LmNpc2NvLmNvbS9zZW11
```

```

cml0eS9wa2kvY3Jsl2NyY2EyMDQ4LmNybDBQBgrBgEFBQcBAQREMEIwQAYIKwYB
BQUHMAKGNGh0dHA6Ly93d3cuY2l2Y28uY29tL3NlY3VyaXR5L3BraS9jZXJ0cy9j
cmNhMjA0OC5jZXIwXAYDVR0gBFUwUzBRBgorBgEEAQkVAQIAMEMwQQYIKwYBBQUH
I+i6itvaSN6go4cTAnPpE+rhC836WVg0ZrG2PML9d7QJwBcbx2RvdFOWFEdyeP3
OOfTC9Fovo4ipUsG4eakqjN9GnW6JvNwxmEApCn5J1unGdGTjaubEBEPH6GC/f08
S25l3JNFBemvM2tnIwcGhiLa69yHz1khQhrpz3B1iOAKPV19TpY4gJfVb/Cbcdi6
YBmlsGGGrd1lZva5J6LuL2GbuqEwYf2+rDUU+bgtlwvww+9tzD0865XpgdOKXrbO
+nmka9eiV2TEP0zJ2+iC7AFm1BCIo1blPFft6QKoSJFjB6thJksaE5/k3Npf
quit
Certificate has the following attributes:
Fingerprint MD5: 0F3BA6E7 4B9636DF 5F54BE72 24762SBR
Fingerprint SHA1: L92BB37A S9919925 5C130ED2 3E528UP8 286E8C2D
% Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.
% Certificate successfully imported

Router(config)# crypto pki trustpoint CiscoRootCA2048
Router(ca-trustpoint)# revocation-check none
Router(ca-trustpoint)# enrollment terminal
Router(ca-trustpoint)# exit
Router(config)# crypto pki authenticate CiscoRootCA2048

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
MIIDQzCCAiugAwIBAgIQX/h7KctU3I1CoxW1aMmt/zANBgkqhkiG9w0BAQUFADA1
MRYwFAYDVQQKEw1DaXNjb3R5bWVudDQwZDQxY290IENBIDFwNDgwHhcNMDQwNTE0MjA5NzEyWWhcNMjkwNTE0MjAyNTQyWjA1MRYwFAYDVQQK
Ew1DaXNjb3R5bWVudDQwZDQxY290IENBIDFwNDgwggEgMA0GCSqGSIb3DQEBAQUAA4IBDQAwggEIAoIBAQCwmmrmp68Kd6ficba0ZmKUeIhH
FR5umgIJFq0roIlgX9p7L6owEAYJKwYBBAGCNxUBBAMCAQAwDQYJKoZIhvcNAQEF
BQADggEBBAJ2dhISjQa18dwy3U8pORFbi71R803UXHOjgxxkLtv5MOhmBvrBW7hmW
Yppao2TB9k5UM8Z3/sUcuVdJcr18JOagxEu5sv4dEX+5wW4q+ffY0vhN4TauYuX
cB7w4ovXsNgOnbFp1iqRe6lJT37mjpXYgyc81WhJdTsd9i7rp77rMKsS0T81asz
Bvt9YaretIjjsJyp8qS5UwGH0GikJ3+r/+n6yUA4iGe0OcaEb1fJU9u6ju7AQ7L4
CYNu/2bPPu8Xs1gYJQk0XuPL1hS27PKSb3TkL4Eq1ZKR4OCXPDJJoBYVL0fdX41Id
kxpUnwVwwEpxYB5DC2Ae/qPOgrnhCzU=
quit
Certificate has the following attributes:
Fingerprint MD5: 2G3LZ6B7 2R1995ER 6KE4WE72 3E528BB8
Fingerprint SHA1: M9912245 5C130ED2 24762JBC 3E528VF8 956E8S5H
% Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.
% Certificate successfully imported

```

Secure Cisco Unified SRST ルータへの Cisco Unified Communications Manager の設定

次の作業を Cisco Unified Communications Manager で実行します。

- [Cisco Unified Communications Manager への SRST リファレンスの追加 \(P.176\)](#) (必須)
- [Cisco Unified Communications Manager での SRST フォールバックの設定 \(P.178\)](#) (必須)
- [Cisco Unified Communications Manager への CAPF の設定 \(P.180\)](#) (必須)

Cisco Unified Communications Manager への SRST リファレンスの追加

SRST リファレンスを Cisco Unified Communications Manager に追加する手順は、次のとおりです。

この手順に従う前に、Cisco Unified SRST ルータでクレデンシャル サービスが実行されていることを確認してください。Cisco Unified Communications Manager は、デバイスの証明書のために Cisco Unified SRST ルータに接続します。クレデンシャル サービスを有効にするには、[P.167](#) の「[Secure Cisco Unified SRST ルータでのクレデンシャル サービスの有効化](#)」を参照してください。

Cisco Unified Communications Manager に Cisco Unified SRST を追加する方法については、実行している Cisco Unified Communications Manager バージョンの「Survivable Remote Site Telephony Configuration」を参照してください。すべての Cisco Unified Communications Manager アドミニストレーションガイドは、http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html にあります。

要約手順

1. Cisco Unified Communications Manager メニュー バーの **SRST** を選択します。
2. 新しい SRST リファレンスを追加します。
3. SRST フィールドに適切な設定値を入力します。
4. **Insert** をクリックします。
5. 他の SRST リファレンスについて、手順 2 ~ 4 を繰り返します。

詳細手順

-
- ステップ 1** Cisco Unified Communications Manager のメニュー バーで、**CCMAdmin > System > SRST** の順に選択します。
- ステップ 2** **Add New SRST Reference** をクリックします。
- ステップ 3** 適切な設定値を入力します。図 9 に、SRST Reference Configuration ウィンドウで使用可能なフィールドを示します。
- a. SRST ゲートウェイの名前、IP アドレス、およびポートを入力します。
 - b. SRST ゲートウェイが安全かどうかを尋ねるボックスをオンにします。
 - c. 証明書プロバイダー（クレデンシャル サービス）のポート番号を入力します。クレデンシャル サービスは、デフォルトのポート 2445 で実行されます。

図 9 SRST Reference Configuration ウィンドウ

System Route Plan Service Feature Device User Application Help

Cisco CallManager Administration
For Cisco IP Telephony Solutions

CISCO SYSTEMS

SRST Reference Configuration

[Add New SRST Reference](#)
[Back to Find/List SRST References](#)

SRST Reference: New
Status: Ready

Insert Cancel

SRST Reference Name* SRST Gateway

IP Address* 10.1.1.22

Port* 2000

Is SRST Secure?

SRST Certificate Provider Port* 2445

* indicates required item

127020

ステップ 4 新しい SRST リファレンスを追加するには、**Insert** をクリックします。「Status: Insert completed」メッセージが表示されます。

ステップ 5 さらに SRST リファレンスを追加するには、手順 2～4 を繰り返します。

Cisco Unified Communications Manager での SRST フォールバックの設定

デバイス プールを SRST に割り当てることにより、Cisco Unified Communications Manager に SRST フォールバックを設定する手順は、次のとおりです。

デバイス プールを Cisco Unified Communications Manager に追加する方法については、実行している Cisco Unified Communications Manager バージョンの『Cisco Unified Communications Manager Administration Guide』の「Device Pool Configuration」を参照してください。すべての Cisco Unified Communications Manager アドミニストレーション ガイドは、http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html にあります。

要約手順

1. Cisco Unified Communications Manager メニュー バーの **Device Pool** を選択します。
2. デバイス プールを追加します。
3. **Add New Device Pool** をクリックします。
4. SRST リファレンスを入力します。
5. **Update** をクリックします。

詳細手順

- ステップ 1** Cisco Unified Communications Manager のメニュー バーで、**CCMAdmin > System > Device Pool** の順に選択します。
- ステップ 2** デバイス プールを追加するには、次のいずれかの方法を使用します。
- 追加するデバイス プールと同様の設定を持つデバイス プールがすでに存在する場合は、設定を表示するために既存のデバイス プールを選択し、**Copy** をクリックして、必要に応じて設定を変更してください。**ステップ 4**に進みます。
 - 既存のものをコピーせずにデバイス プールを追加するには、**ステップ 3**に進みます。
- ステップ 3** ウィンドウの右上隅で、**Add New Device Pool** リンクをクリックします。Device Pool Configuration ウィンドウが表示されます (図 10 を参照)。

図 10 Device Pool Configuration ウィンドウ

System Route Plan Service Feature Device User Application Help

Cisco CallManager Administration
For Cisco IP Telephony Solutions

CISCO SYSTEMS

Device Pool Configuration

[Add new Device Pool](#)
[Back to Find/List Device Pools](#)
[Dependency Records](#)

Device Pool: Default (13 members)**
Status: Ready

Copy Update Delete Reset Devices

Device Pool Settings

Device Pool Name*	Default
Cisco CallManager Group*	Default
Date/Time Group*	CMLocal
Region*	Default
Softkey Template*	Standard User
SRST Reference*	jaso2691
Calling Search Space for Auto-registration	— Not Selected — Disable Use Default Gateway jaso2691 SRST GW
Media Resource Group List	
Network Hold MOH Audio Source	SRST GW
User Hold MOH Audio Source	< None >
Network Locale	< None >

127021

- ステップ 4** SRST リファレンスを入力します。
- ステップ 5** **Update** をクリックして、デバイス プール情報をデータベースに保存します。

Cisco Unified Communications Manager への CAPF の設定

CAPF プロセスでは、Cisco Unified Communications Manager などのサポート対象デバイスが、Cisco Unified IP Phone から LSC 証明書を要求できます。CAPF ユーティリティは、キー ペアおよび CAPF に特有の証明書を生成し、クラスタ内のすべての Cisco Unified Communications Manager サービスにこの証明書をコピーします。

Cisco Unified Communications Manager への CAPF の設定方法については、『[Cisco IP Phone Authentication and Encryption for Cisco Communications Manager](#)』を参照してください。

Secure Cisco Unified SRST ルータでの SRST モードの有効化

Cisco Unified IP Phone 機能をサポートするようにルータ上の Secure SRST を設定するには、global コンフィギュレーション モードを開始して、次のコマンドを使用します。

要約手順

1. `call-manager-fallback`
2. `secondary-dialtone digit-string`
3. `transfer-system {blind | full-blind | full-consult | local-consult}`
4. `ip source-address ip-address [port port]`
5. `max-ephones max-phones`
6. `max-dn max-directory-numbers`
7. `transfer-pattern transfer-pattern`
8. `exit`

詳細手順

	コマンドまたはアクション	目的
ステップ 1	<code>call-manager-fallback</code> Router(config)# <code>call-manager-fallback</code>	<code>call-manager-fallback</code> コンフィギュレーション モードを開始します。
ステップ 2	<code>secondary-dialtone digit-string</code> Router(config-cm-fallback)# <code>secondary-dialtone 9</code>	数字列がダイヤルされたときに第 2 発信音をアクティブにします。

	コマンドまたはアクション	目的
ステップ 3	<pre>transfer-system {blind full-blind full-consult local-consult} Router(config-cm-fallback)# transfer-system full-consult</pre>	<p>Cisco Unified SRST ルータが提供するすべての回線のコール転送方法を定義します。</p> <ul style="list-style-type: none"> • blind : シスコ独自の方法を使用して、単一電話回線で、打診を行わずにコールを転送します。 • full-blind : H.450.2 標準方式を使用して、打診を行わずにコールを転送します。 • full-consult : 使用可能な 2 番目の電話回線を使用し、打診を行ってコールを転送します。2 番目の回線が使用できない場合、コールは full-blind にフォールバックします。 • local-consult : 使用可能な 2 番目の電話回線を使用し、ローカルで打診を行ってコールを転送します。打診先または転送先がローカル以外の場合、コールは blind にフォールバックします。
ステップ 4	<pre>ip source-address ip-address [port port] Router(config-cm-fallback)# ip source-address 10.1.1.22 port 2000</pre>	<p>指定した IP アドレスを使用してルータが Cisco IP Phone からメッセージを受信できるようにし、厳密な IP アドレスの検証を提供します。デフォルトのポート番号は 2000 です。</p>
ステップ 5	<pre>max-ephones max-phones Router(config-cm-fallback)# max-ephones 15</pre>	<p>ルータがサポートできる Cisco IP Phone の最大数を設定します。最大数は、プラットフォームによって異なります。デフォルトは 0 です。詳細については、P.31 の「プラットフォームとメモリのサポート」を参照してください。</p>
ステップ 6	<pre>max-dn max-directory-numbers Router(config-cm-fallback)# max-dn 30</pre>	<p>ルータがサポート可能な DN または仮想音声ポートの最大数を設定します。</p> <ul style="list-style-type: none"> • max-directory-numbers : ルータでサポートされる電話番号または仮想音声ポートの最大数。最大数は、プラットフォームによって異なります。デフォルトは 0 です。詳細については、P.31 の「プラットフォームとメモリのサポート」を参照してください。
ステップ 7	<pre>transfer-pattern transfer-pattern Router(config-cm-fallback)# transfer-pattern</pre>	<p>Cisco Unified IP Phone による電話コールを指定の電話番号パターンに転送できるようにします。</p> <ul style="list-style-type: none"> • transfer-pattern : 許可するコール転送の数字列。ワイルドカードが使用可能です。
ステップ 8	<pre>exit Router(config-cm-fallback)# exit</pre>	<p>call-manager-fallback コンフィギュレーション モードを終了します。</p>

例

次の例では、ルータで SRST モードを有効にします。

```
Router(config)# call-manager-fallback
Router(config-cm-fallback)# secondary-dialtone 9
Router(config-cm-fallback)# transfer-system full-consult
Router(config-cm-fallback)# ip source-address 10.1.1.22 port 2000
Router(config-cm-fallback)# max-ephones 15
Router(config-cm-fallback)# max-dn 30
Router(config-cm-fallback)# transfer-pattern .....
Router(config-cm-fallback)# exit
```

電話機のステータスおよび登録の確認

Cisco Unified IP Phone のステータスおよび登録について、確認またはトラブルシューティングを行うには、特権 EXEC モードを開始して、次の手順を実行します。

要約手順

1. `show ephone`
2. `show ephone offhook`
3. `show voice call status`
4. `debug ephone register`
5. `debug ephone state`

詳細手順

ステップ 1 `show ephone`

登録された Cisco Unified IP Phone およびその機能を表示するには、このコマンドを使用します。`show ephone` コマンドは、Secure SRST に対して使用されると、認証と暗号化のステータスも表示します。この例では、TLS 接続で認証と暗号化のステータスがアクティブになっています。

```
Router# show ephone
```

```
ephone-1 Mac:1000.1111.0002 TCP socket:[5] activeLine:0 REGISTERED in SCCP ver 5
+ Authentication + Encryption with TLS connection
mediaActive:0 offhook:0 ringing:0 reset:0 reset_sent:0 paging 0 debug:0
IP:10.1.1.40 32626 7970 keepalive 390 max_line 8
button 1: dn 14 number 2002 CM Fallback CH1 IDLE
```

```
ephone-2 Mac:1000.1111.000B TCP socket:[12] activeLine:0 REGISTERED in SCCP ver
5 + Authentication + Encryption with TLS connection
mediaActive:0 offhook:0 ringing:0 reset:0 reset_sent:0 paging 0 debug:0
IP:10.1.1.40 32718 7970 keepalive 390 max_line 8
button 1: dn 21 number 2011 CM Fallback CH1 IDLE
```

```
ephone-3 Mac:1000.1111.000A TCP socket:[16] activeLine:0 REGISTERED in SCCP ver
5 + Authentication + Encryption with TLS connection
mediaActive:0 offhook:0 ringing:0 reset:0 reset_sent:0 paging 0 debug:0
IP:10.1.1.40 32862 7970 keepalive 390 max_line 8
button 1: dn 2 number 2010 CM Fallback CH1 IDLE
```

ステップ 2 show ephone offhook

Cisco IP Phone のステータスおよびオフフック状態のすべての電話機の品質を表示するには、このコマンドを使用します。この例では、TLS 接続で認証と暗号化のステータスがアクティブで、さらにアクティブな保護されたコールが存在します。

```
Router# show ephone offhook

ephone-1 Mac:1000.1111.0002 TCP socket:[5] activeLine:1 REGISTERED in SCCP ver 5
+ Authentication + Encryption with TLS connection
mediaActive:1 offhook:1 ringing:0 reset:0 reset_sent:0 paging 0
:0
IP:10.1.1.40 32626 7970 keepalive 391 max_line 8
button 1: dn 14 number 2002 CM Fallback CH1 CONNECTED
Active Secure Call on DN 14 chan 1 :2002 10.1.1.40 29632 to 10.1.1.40 25616 via
10.1.1.40
G711Ulaw64k 160 bytes no vad
Tx Pkts 295 bytes 49468 Rx Pkts 277 bytes 46531 Lost 0
Jitter 0 Latency 0 callingDn 22 calledDn -1

ephone-2 Mac:1000.1111.000B TCP socket:[12] activeLine:1 REGISTERED in SCCP ver
5 + Authentication + Encryption with TLS connection
mediaActive:1 offhook:1 ringing:0 reset:0 reset_sent:0 paging 0 debug:0
IP:10.1.1.40 32718 7970 keepalive 391 max_line 8
button 1: dn 21 number 2011 CM Fallback CH1 CONNECTED
Active Secure Call on DN 21 chan 1 :2011 10.1.1.40 16382 to 10.1.1.40 16382 via
10.1.1.40
G711Ulaw64k 160 bytes no vad
Tx Pkts 295 bytes 49468 Rx Pkts 277 bytes 46531 Lost 0
Jitter 0 Latency 0 callingDn -1 calledDn 11
```

ステップ 3 show voice call status

Cisco Unified SRST ルータのすべての音声ポートのコール ステータスを表示するには、このコマンドを使用します。このコマンドは、2つの POTS ダイアルピア間のコールには適用できません。

```
Router# show voice call status

CallID CID ccVdb Port DSP/Ch Called # Codec Dial-peers
0x1164 2BFE 0x8619A460 50/0/35.0 2014 g711ulaw 20035/20027
0x1165 2BFE 0x86144B78 50/0/27.0 *2014 g711ulaw 20027/20035
0x1166 2C01 0x861043D8 50/0/21.0 2012 g711ulaw 20021/20011
0x1168 2C01 0x860984C4 50/0/11.0 *2012 g711ulaw 20011/20021
0x1167 2C04 0x8610EC7C 50/0/22.0 2002 g711ulaw 20022/20014
0x1169 2C04 0x860B8894 50/0/14.0 *2002 g711ulaw 20014/20022
0x116A 2C07 0x860A374C 50/0/12.0 2010 g711ulaw 20012/20002
0x116B 2C07 0x86039700 50/0/2.0 *2010 g711ulaw 20002/20012
0x116C 2C0A 0x86119520 50/0/23.0 2034 g711ulaw 20023/20020
0x116D 2C0A 0x860F9150 50/0/20.0 *2034 g711ulaw 20020/20023
0x116E 2C0D 0x8608DC20 50/0/10.0 2022 g711ulaw 20010/20008
0x116F 2C0D 0x86078AD8 50/0/8.0 *2022 g711ulaw 20008/20010
0x1170 2C10 0x861398F0 50/0/26.0 2016 g711ulaw 20026/20028
0x1171 2C10 0x8614F41C 50/0/28.0 *2016 g711ulaw 20028/20026
0x1172 2C13 0x86159CC0 50/0/29.0 2018 g711ulaw 20029/20004
0x1173 2C13 0x8604E848 50/0/4.0 *2018 g711ulaw 20004/20029
0x1174 2C16 0x8612F04C 50/0/25.0 2026 g711ulaw 20025/20030
0x1175 2C16 0x86164F48 50/0/30.0 *2026 g711ulaw 20030/20025
0x1176 2C19 0x860D8C64 50/0/17.0 2032 g711ulaw 20017/20018
0x1177 2C19 0x860E4008 50/0/18.0 *2032 g711ulaw 20018/20017
0x1178 2C1C 0x860CE3C0 50/0/16.0 2004 g711ulaw 20016/20019
0x1179 2C1C 0x860EE8AC 50/0/19.0 *2004 g711ulaw 20019/20016
0x117A 2C1F 0x86043FA4 50/0/3.0 2008 g711ulaw 20003/20024
0x117B 2C1F 0x861247A8 50/0/24.0 *2008 g711ulaw 20024/20003
0x117C 2C22 0x8608337C 50/0/9.0 2020 g711ulaw 20009/20031
0x117D 2C22 0x8616F7EC 50/0/31.0 *2020 g711ulaw 20031/20009
```

```

0x117E 2C25 0x86063990 50/0/6.0 2006 g711ulaw 20006/20001
0x117F 2C25 0x85C6BE6C 50/0/1.0 *2006 g711ulaw 20001/20006
0x1180 2C28 0x860ADFF0 50/0/13.0 2029 g711ulaw 20013/20034
0x1181 2C28 0x8618FBBC 50/0/34.0 *2029 g711ulaw 20034/20013
0x1182 2C2B 0x860C3B1C 50/0/15.0 2036 g711ulaw 20015/20005
0x1183 2C2B 0x860590EC 50/0/5.0 *2036 g711ulaw 20005/20015
0x1184 2C2E 0x8617A090 50/0/32.0 2024 g711ulaw 20032/20007
0x1185 2C2E 0x8606E234 50/0/7.0 *2024 g711ulaw 20007/20032
0x1186 2C31 0x861A56E8 50/0/36.0 2030 g711ulaw 20036/20033
0x1187 2C31 0x86185318 50/0/33.0 *2030 g711ulaw 20033/20036
18 active calls found

```

ステップ 4 debug ephone register

Cisco IP Pone の登録のプロセスをデバッグするには、このコマンドを使用します。

```
Router# debug ephone register
```

```

EPHONE registration debugging is enabled
*Jun 29 09:16:02.180: New Skinny socket accepted [2] (0 active)
*Jun 29 09:16:02.180: sin_family 2, sin_port 51617, in_addr 10.5.43.177
*Jun 29 09:16:02.180: skinny_socket_process: secure skinny sessions = 1
*Jun 29 09:16:02.180: add_skinny_secure_socket: pid =155, new_sock=0, ip address =
10.5.43.177
*Jun 29 09:16:02.180: skinny_secure_handshake: pid =155, sock=0, args->pid=155, ip
address = 10.5.43.177
*Jun 29 09:16:02.184: Start TLS Handshake 0 10.5.43.177 51617
*Jun 29 09:16:02.184: TLS Handshake retcode OPSSLReadWouldBlockErr
*Jun 29 09:16:03.188: TLS Handshake retcode OPSSLReadWouldBlockErr
*Jun 29 09:16:04.188: TLS Handshake retcode OPSSLReadWouldBlockErr
*Jun 29 09:16:05.188: TLS Handshake retcode OPSSLReadWouldBlockErr
*Jun 29 09:16:06.188: TLS Handshake retcode OPSSLReadWouldBlockErr
*Jun 29 09:16:07.188: TLS Handshake retcode OPSSLReadWouldBlockErr
*Jun 29 09:16:08.188: CRYPTO_PKI_OPSSL - Verifying 1 Certs

*Jun 29 09:16:08.212: TLS Handshake completes

```

ステップ 5 debug ephone state

2つの Secure Cisco Unified IP Phone 間のコール設定を見直すには、このコマンドを使用します。**debug ephone state** トレースは、2つの電話機間の暗号化および複合化キーの生成と配布を示します。

```
Router# debug ephone state
```

```

*Jan 11 18:33:09.231:%SYS-5-CONFIG_I:Configured from console by console
*Jan 11 18:33:11.747:ephone-2[2]:OFFHOOK
*Jan 11 18:33:11.747:ephone-2[2]:---SkinnySyncPhoneDnOverlays is onhook
*Jan 11 18:33:11.747:ephone-2[2]:SIEZE on activeLine 0 activeChan 1
*Jan 11 18:33:11.747:ephone-2[2]:SetCallState line 1 DN 2(-1) chan 1 ref 6 TsOffHook
*Jan 11 18:33:11.747:ephone-2[2]:Check Plar Number
*Jan 11 18:33:11.751:DN 2 chan 1 Voice_Mode
*Jan 11 18:33:11.751:dn_tone_control DN=2 chan 1 tonetype=33:DtInsideDialTone onoff=1
pid=232
*Jan 11 18:33:15.031:dn_tone_control DN=2 chan 1 tonetype=0:DtSilence onoff=0 pid=232
*Jan 11 18:33:16.039:ephone-2[2]:Skinny-to-Skinny call DN 2 chan 1 to DN 4 chan 1
instance 1
*Jan 11 18:33:16.039:ephone-2[2]:SetCallState line 1 DN 2(-1) chan 1 ref 6 TsProceed
*Jan 11 18:33:16.039:ephone-2[2]:SetCallState line 1 DN 2(-1) chan 1 ref 6 TsRingOut
*Jan 11 18:33:16.039:ephone-2[2]:callingNumber 6000

*Jan 11 18:33:16.039:ephone-2[2]:callingParty 6000

*Jan 11 18:33:16.039:ephone-2[2]:Call Info DN 2 line 1 ref 6 call state 1 called 6001
calling 6000 origcalled

```

```
*Jan 11 18:33:16.039:ephone-2[2]:Call Info DN 2 line 1 ref 6 called 6001 calling 6000
origcalled 6001 calltype 2
*Jan 11 18:33:16.039:ephone-2[2]:Call Info for chan 1
*Jan 11 18:33:16.039:ephone-2[2]:Original Called Name 6001
*Jan 11 18:33:16.039:ephone-2[2]:6000 calling
*Jan 11 18:33:16.039:ephone-2[2]:6001
*Jan 11 18:33:16.047:ephone-3[3]:SetCallState line 1 DN 4(4) chan 1 ref 7 TsRingIn
*Jan 11 18:33:16.047:ephone-3[3]:callingNumber 6000

*Jan 11 18:33:16.047:ephone-3[3]:callingParty 6000

*Jan 11 18:33:16.047:ephone-3[3]:Call Info DN 4 line 1 ref 7 call state 7 called 6001
calling 6000 origcalled
*Jan 11 18:33:16.047:ephone-3[3]:Call Info DN 4 line 1 ref 7 called 6001 calling 6000
origcalled 6001 calltype 1
*Jan 11 18:33:16.047:ephone-3[3]:Call Info for chan 1
*Jan 11 18:33:16.047:ephone-3[3]:Original Called Name 6001
*Jan 11 18:33:16.047:ephone-3[3]:6000 calling
*Jan 11 18:33:16.047:ephone-3[3]:6001
*Jan 11 18:33:16.047:ephone-3[3]:Ringer Inside Ring On
*Jan 11 18:33:16.051:dn_tone_control DN=2 chan 1 tonetype=36:DtAlertingTone onoff=1
pid=232
*Jan 11 18:33:20.831:ephone-3[3]:OFFHOOK
*Jan 11 18:33:20.831:ephone-3[3]:---SkinnySyncPhoneDnOverlays is onhook
*Jan 11 18:33:20.831:ephone-3[3]:Ringer Off
*Jan 11 18:33:20.831:ephone-3[3]:ANSWER call
*Jan 11 18:33:20.831:ephone-3[3]:SetCallState line 1 DN 4(-1) chan 1 ref 7 TsOffHook
*Jan 11 18:33:20.831:ephone-3[3]:[SEP000DEDAB3EBF]:Answer Incoming call from ephone-(2)
DN 2 chan 1
*Jan 11 18:33:20.831:ephone-3[3]:SetCallState line 1 DN 4(-1) chan 1 ref 7 TsConnected
*Jan 11 18:33:20.831:defer_start for DN 2 chan 1 at CONNECTED
*Jan 11 18:33:20.831:ephone-2[2]:SetCallState line 1 DN 2(-1) chan 1 ref 6 TsConnected
*Jan 11 18:33:20.835:ephone-3[3]:callingNumber 6000

*Jan 11 18:33:20.835:ephone-3[3]:callingParty 6000

*Jan 11 18:33:20.835:ephone-3[3]:Call Info DN 4 line 1 ref 7 call state 4 called 6001
calling 6000 origcalled
*Jan 11 18:33:20.835:ephone-3[3]:Call Info DN 4 line 1 ref 7 called 6001 calling 6000
origcalled 6001 calltype 1
*Jan 11 18:33:20.835:ephone-3[3]:Call Info for chan 1
*Jan 11 18:33:20.835:ephone-3[3]:Original Called Name 6001
*Jan 11 18:33:20.835:ephone-3[3]:6000 calling
*Jan 11 18:33:20.835:ephone-3[3]:6001
*Jan 11 18:33:20.835:ephone-2[2]:Security Key Generation
! Ephone 2 generates a security key.

*Jan 11 18:33:20.835:ephone-2[2]:OpenReceive DN 2 chan 1 codec 4:G711Ulaw64k duration
20 ms bytes 160
*Jan 11 18:33:20.835:ephone-2[2]:Send Decryption Key
! Ephone 2 sends the decryption key.

*Jan 11 18:33:20.835:ephone-3[3]:Security Key Generation
!Ephone 3 generates its security key.

*Jan 11 18:33:20.835:ephone-3[3]:OpenReceive DN 4 chan 1 codec 4:G711Ulaw64k duration
20 ms bytes 160
*Jan 11 18:33:20.835:ephone-3[3]:Send Decryption Key
! Ephone 3 sends its decryption key.

*Jan 11 18:33:21.087:dn_tone_control DN=2 chan 1 tonetype=0:DtSilence onoff=0 pid=232
*Jan 11 18:33:21.087:DN 4 chan 1 Voice_Mode
*Jan 11 18:33:21.091:DN 2 chan 1 End Voice_Mode
*Jan 11 18:33:21.091:DN 2 chan 1 Voice_Mode
*Jan 11 18:33:21.095:ephone-2[2]:OpenReceiveChannelAck:IP 1.1.1.8, port=25552,
dn_index=2, dn=2, chan=1
*Jan 11 18:33:21.095:ephone-3[3]:StartMedia 1.1.1.8 port=25552
*Jan 11 18:33:21.095:DN 2 chan 1 codec 4:G711Ulaw64k duration 20 ms bytes 160
*Jan 11 18:33:21.095:ephone-3[3]:Send Encryption Key
```

```
! Ephone 3 sends its encryption key.

*Jan 11 18:33:21.347:ephone-3[3]:OpenReceiveChannelAck:IP 1.1.1.9, port=17520,
    dn_index=4, dn=4, chan=1
*Jan 11 18:33:21.347:ephone-2[2]:StartMedia 1.1.1.9 port=17520
*Jan 11 18:33:21.347:DN 2 chan 1 codec 4:G711Ulaw64k duration 20 ms bytes 160
*Jan 11 18:33:21.347:ephone-2[2]:Send Encryption Key
!Ephone 2 sends its encryption key.*Jan 11 18:33:21.851:ephone-2[2]::callingNumber
6000

*Jan 11 18:33:21.851:ephone-2[2]::callingParty 6000
*Jan 11 18:33:21.851:ephone-2[2]:Call Info DN 2 line 1 ref 6 call state 4 called 6001
calling 6000 origcalled
*Jan 11 18:33:21.851:ephone-2[2]:Call Info DN 2 line 1 ref 6 called 6001 calling 6000
origcalled 6001 calltype 2
*Jan 11 18:33:21.851:ephone-2[2]:Call Info for chan 1
*Jan 11 18:33:21.851:ephone-2[2]:Original Called Name 6001
*Jan 11 18:33:21.851:ephone-2[2]:6000 calling
*Jan 11 18:33:21.851:ephone-2[2]:6001
```

Secure SRST の設定例

ここでは、次の設定例を示します。

- [Secure SRST : 例 \(P.187\)](#)
- [コントロールプレーン ポリシング : 例 \(P.192\)](#)



(注) この例の IP アドレスとホスト名は架空のものです。

Secure SRST : 例

ここでは、前の項で特定された設定作業に一致する設定例を示します。この例には、サードパーティ CA の使用は含まれていません。Cisco IOS 証明書サーバを使用して、証明書を生成することを前提とします。

```
Router# show running-config
.
.
.
! Define Unified Communications Manager.
ccm-manager fallback-mgcp
ccm-manager mgcp
ccm-manager music-on-hold
ccm-manager config server 10.1.1.13
ccm-manager config
!
! Define root CA.
crypto pki server srstcaserver
  database level complete
  database url nvram
  issuer-name CN=srstcaserver

!
crypto pki trustpoint srstca
  enrollment url http://10.1.1.22:80
  revocation-check none
!
crypto pki trustpoint srstcaserver
  revocation-check none
  rsakeypair srstcaserver
!
! Define CTL/7970 trustpoint.
crypto pki trustpoint 7970
  enrollment terminal
  revocation-check none
!
crypto pki trustpoint PEM
  enrollment terminal
  revocation-check none
!
! Define CAPF/7960 trustpoint.
crypto pki trustpoint 7960
  enrollment terminal
  revocation-check none
!
! SRST router device certificate.
crypto pki certificate chain srstca
certificate 02
  308201AD 30820116 A0030201 02020102 300D0609 2A864886 F70D0101 04050030
  17311530 13060355 0403130C 73727374 63617365 72766572 301E170D 30343034
  31323139 35323233 5A170D30 35303431 32313935 32323335A 30343132 300F0603
  55040513 08443042 39453739 43301F06 092A8648 86F70D01 09021612 6A61736F
  32363931 2E636973 636F2E63 6F6D305C 300D0609 2A864886 F70D0101 01050003
```

```

4B003048 024100D7 0CC354FB 5F7C1AE7 7A25C3F2 056E0485 22896D36 6CA70C19
C98F9BAE AE9D1F9B D4BB7A67 F3251174 193BB1A3 12946123 E5C1CCD7 A23E6155
FA2ED743 3FB8B902 03010001 A330302E 300B0603 551D0F04 04030205 A0301F06
03551D23 04183016 8014F829 CE97AD60 18D05467 FC293963 C2470691 F9BD300D
06092A86 4886F70D 01010405 00038181 007EB48E CAE9E1B3 D1E7A185 D7F0D565
CB84B17B 1151BD78 B3E39763 59EC650E 49371F6D 99CBD267 EB8ADF9D 9E43A5F2
FB2B18A0 34AF6564 11239473 41478AFC A86E6DA1 AC518E0B 8657CEBB ED2BDE8E
B586FE67 00C358D4 EFDD8D44 3F423141 C2D331D3 1EE43B6E 6CB29EE7 0B8C2752
C3AF4A66 BD007348 D013000A EA3C206D CF
quit
certificate ca 01
30820207 30820170 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
17311530 13060355 0403130C 73727374 63617365 72766572 301E170D 30343034
31323139 34353136 5A170D30 37303431 32313934 3531365A 30173115 30130603
55040313 0C737273 74636173 65727665 7230819F 300D0609 2A864886 F70D0101
01050003 818D0030 81890281 8100C3AF EE1E4BB1 9922A8DA 2BB9DC8E 5B1BD332
1051C9FE 32A971B3 3C336635 74691954 98E765B1 059E24B6 32154E99 105CA989
9619993F CC72C525 7357EBAC E6335A32 2AAF9391 99325BFD 9B8355EB C10F8963
9D8FC222 EE8AC831 71ACD3A7 4E918A8F D5775159 76FBF499 5AD0849D CAA41417
DD866902 21E5DD03 C37D4B28 0FAB0203 010001A3 63306130 0F060355 1D130101
FF040530 030101FF 300E0603 551D0F01 01FF0404 03020186 301D0603 551D0E04
160414F8 29CE97AD 6018D054 67FC2939 63C24706 91F9BD30 1F060355 1D230418
30168014 F829CE97 AD6018D0 5467FC29 3963C247 0691F9BD 300D0609 2A864886
F70D0101 04050003 8181007A F71B25F9 73D74552 25DFD03A D8D1338F 6792C805
47A81019 795B5AAE 035400BB F859DABF 21892B5B E71A8283 08950414 8633A8B2
C98565A6 C09CA641 88661402 ACC424FD 36F23360 ABFF4C55 BB23C66A C80A3A57
5EE85FF8 C1B1A540 E818CE6D 58131726 BB060974 4E1A2F4B E6195522 122457F3
DEDBAAD7 3780136E B112A6
quit
crypto pki certificate chain srstcaserver
certificate ca 01
30820207 30820170 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
17311530 13060355 0403130C 73727374 63617365 72766572 301E170D 30343034
31323139 34353136 5A170D30 37303431 32313934 3531365A 30173115 30130603
55040313 0C737273 74636173 65727665 7230819F 300D0609 2A864886 F70D0101
01050003 818D0030 81890281 8100C3AF EE1E4BB1 9922A8DA 2BB9DC8E 5B1BD332
1051C9FE 32A971B3 3C336635 74691954 98E765B1 059E24B6 32154E99 105CA989
9619993F CC72C525 7357EBAC E6335A32 2AAF9391 99325BFD 9B8355EB C10F8963
9D8FC222 EE8AC831 71ACD3A7 4E918A8F D5775159 76FBF499 5AD0849D CAA41417
DD866902 21E5DD03 C37D4B28 0FAB0203 010001A3 63306130 0F060355 1D130101
FF040530 030101FF 300E0603 551D0F01 01FF0404 03020186 301D0603 551D0E04
160414F8 29CE97AD 6018D054 67FC2939 63C24706 91F9BD30 1F060355 1D230418
30168014 F829CE97 AD6018D0 5467FC29 3963C247 0691F9BD 300D0609 2A864886
F70D0101 04050003 8181007A F71B25F9 73D74552 25DFD03A D8D1338F 6792C805
47A81019 795B5AAE 035400BB F859DABF 21892B5B E71A8283 08950414 8633A8B2
C98565A6 C09CA641 88661402 ACC424FD 36F23360 ABFF4C55 BB23C66A C80A3A57
5EE85FF8 C1B1A540 E818CE6D 58131726 BB060974 4E1A2F4B E6195522 122457F3
DEDBAAD7 3780136E B112A6
quit
crypto pki certificate chain 7970
certificate ca 353FB24BD70F14A346C1F3A9AC725675
308203A8 30820290 A0030201 02021035 3FB24BD7 0F14A346 C1F3A9AC 72567530
0D06092A 864886F7 0D010105 0500302E 31163014 06035504 0A130D43 6973636F
20537973 74656D73 31143012 06035504 03130B43 41502D52 54502D30 3032301E
170D3033 31303130 32303138 34395A17 0D323331 30313032 30323733 375A302E
31163014 06035504 0A130D43 6973636F 20537973 74656D73 31143012 06035504
03130B43 41502D52 54502D30 30323082 0120300D 06092A86 4886F70D 01010105
00038201 0D003082 01080282 010100C4 266504AD 7DC3FD8D 65556FA6 308FAE95
B570263B 575ABD96 1CC8F394 5965D9D0 D8CE02B9 F808CCD6 B7CD8C46 24801878
57DC4440 A7301DDF E40FB1EF 136212EC C4F3B50F BCAFB4B4 CD2E5826 34521B65
01555FE4 D4206776 03368357 83932638 D6FC953F 3A179E44 67255A73 45C69DEE
FB4D221B 21D7A3AD 38184171 8FD8C271 42183E65 09461434 736C77CC F380EEBF
632C7B3F A5F92AA6 A8EF3490 8724A84F 4DAF7FD7 0928F585 764D3558 3C0FE9AF
1ED8763F A299A802 970004AD 1912D265 7DE335B4 BCB6F789 DC68B9FA C8FDF85E
8A28AD8F 0F4883C0 77112A47 141DBEE0 948FBE53 FE67B308 D40C8029 87BD790E
CDAB9FD7 A190C1A2 A462C5F2 4A6E0B02 0103A381 C33081C0 300B0603 551D0F04
04030201 86300F06 03551D13 0101FF04 05300301 01FF301D 0603551D 0E041604
1452922B E288EE2E 098A4E7E 702C56A5 9AB4D49B 96306F06 03551D1F 04683066
3064A062 A060862D 68747470 3A2F2F63 61702D72 74702D30 30322F43 65727445

```

```

6E726F6C 6C2F4341 502D5254 502D3030 322E6372 6C862F66 696C653A 2F2F5C5C
6361702D 7274702D 3030325C 43657274 456E726F 6C6C5C43 41502D52 54502D30
30322E63 726C3010 06092B06 01040182 37150104 03020100 300D0609 2A864886
F70D0101 05050003 82010100 56838CEF C4DA3AD1 EA8FBB15 2FFE6EE5 50A1972B
D4D7AF1F D298892C D5A2A76B C3462866 13E0E55D DC0C4B92 5AA94B6E 69277F9B
FC73C697 11266E19 451C0FAB A55E6A28 901A48C5 B9911EE6 348A8920 0AEDE1E0
B6EA781C FFD97CA4 B03C0E34 0E5B0649 8B0A34C9 B73A654E 09050C1F 4DA53E44
BF78443D B08C3A41 2EEEB873 78CB8089 34F9D16E 91512F0D 3A8674AD 0991ED1A
92841E76 36D7740E CB787F11 685B9E9D 0C67E85D AF6D05BA 3488E86D 7E2F7F65
6918DE0F BD3C7F67 D8A33F70 9C4A596E D9F62B3B 1EDEE854 D5882AD4 3D71F72B
8FAB7F3C 0B5F0759 D9828F83 954D7BB1 57A638EC 7D72BFF1 8933C16F 760BCA94
4C5B1931 67947A4F 89A1BDB5
quit
crypto pki certificate chain PEM
certificate ca 7612F960153D6F9F4E42202032B72356
308203A8 30820290 A0030201 02021076 12F96015 3D6F9F4E 42202032 B7235630
0D06092A 864886F7 0D010105 0500302E 31163014 06035504 0A130D43 6973636F
20537973 74656D73 31143012 06035504 03130B43 41502D52 54502D30 3031301E
170D3033 30323036 32333237 31335A17 0D323330 32303632 33333633 345A302E
31163014 06035504 0A130D43 6973636F 20537973 74656D73 31143012 06035504
03130B43 41502D52 54502D30 30313082 0120300D 06092A86 4886F70D 01010105
00038201 0D003082 01080282 010100AC 55BBED18 DE9B8709 FFC8F2D 509AB83A
21C1967F DEA7F4B0 969694B7 80CC196A 463DA516 54A28F47 5D903B5F 104A3D54
A981389B 2FC7AC49 956262B8 1C143038 5345BB2E 273FA7A6 46860573 CE5C998D
55DE78AA 5A5CFE14 037D695B AC816409 C6211F0B 3BBF09CF B0BBB2D4 AC362F67
0FD145F1 620852B3 1F07E2F1 AA74F150 367632ED A289E374 AF0C5B78 CE7DFB9F
C8EBBE54 6ECF4C77 99D6DC04 47476C0F 36E58A3B 6BCB24D7 6B6C84C2 7F61D326
BE7CB4A6 60CD6579 9E1E3A84 8153B750 5527E865 423BE2B5 CB575453 5AA96093
58B6A2E4 AA3EF081 C7068EC1 DD1EBDDA 53E6F0D6 E2E0486B 109F1316 78C696A3
CFBA84CC 7094034F C1EB9F81 931ACB02 0103A381 C33081C0 300B0603 551D0F04
04030201 86300F06 03551D13 0101FF04 05300301 01FF301D 0603551D 0E041604
14E917B1 82C71FCF ACA91B6E F4A9269C 70AE05A0 9A306F06 03551D1F 04683066
3064A062 A060862D 68747470 3A2F2F63 61702D72 74702D30 30312F43 65727445
6E726F6C 6C2F4341 502D5254 502D3030 312E6372 6C862F66 696C653A 2F2F5C5C
6361702D 7274702D 3030315C 43657274 456E726F 6C6C5C43 41502D52 54502D30
30312E63 726C3010 06092B06 01040182 37150104 03020100 300D0609 2A864886
F70D0101 05050003 82010100 AB64FDEB F60C32DC 360F0E10 5FE175FA 0D574AB5
02ACDCA3 C7BBED15 A4431F20 7E9286F0 770929A2 17E4CDF4 F2629244 2F3575AF
E90C468C AE67BA08 AAA71C12 BA0C0E79 E6780A5C F814466C 326A4B56 73938380
73A11AED F9B9DE74 1195C48F 99454B8C 30732980 CD6E7123 8B3A6D68 80B97E00
7F4BD4BA 0B5AB462 94D9167E 6D8D48F2 597CDE61 25CFADCC 5BD141FB 210275A2
0A4E3400 1428BA0F 69953BB5 50D21F78 43E3E563 98BCB2B1 A2D4864B 0616BACD
A61CD9AE C5558A52 B5EEAA6A 08F96528 B1804B87 D26E4AEE AB7AFFE9 2FD2A574
BAFE0028 96304A8B 13FB656D 8FC60094 D5A53D71 444B3CEF 79343385 3778C193
74A2A6CE DC56275C A20A303D
quit
crypto pki certificate chain 7960
certificate ca F301
308201F7 30820160 A0030201 020202F3 01300D06 092A8648 86F70D01 01050500
3041310B 30090603 55040613 02555331 1A301806 0355040A 13114369 73636F20
53797374 656D7320 496E6331 16301406 03550403 130D4341 50462D33 35453038
33333230 1E170D30 34303430 39323035 3530325A 170D3139 30343036 32303535
30315A30 41310B30 09060355 04061302 5553311A 30180603 55040A13 11436973
636F2053 79737465 6D732049 6E633116 30140603 55040313 0D434150 462D3335
45303833 33323081 9F300D06 092A8648 86F70D01 01010500 03818D00 30818902
818100C8 BD9B6035 366B44E8 0F693A47 250FF865 D76C35F7 89B1C4FD 1D122CE0
F5E5CDFF A4A87EFF 41AD936F E5C93163 3E55D11A AF82A5F6 D563E21C EB89EBFA
F5271423 C3E875DC E0E07967 6E1AAB4F D3823E12 53547480 23BA1A09 295179B6
85A0E83A 77DD0633 B9710A88 0890CD4D DB55ADD0 964369BA 489043BB B667E60F
93954B02 03010001 300D0609 2A864886 F70D0101 05050003 81810056 60FD3AB3
6F98D2AD 40C309E2 C05B841C 5189271F 01D864E8 98BCE665 2AFBCC8C 54007A84
8F772C67 E3047A6C C62F6508 B36A6174 B68C1D78 C2228FEA A89ECEFB CC8BA9FC
0F30E151 431670F9 918514D9 868D1235 18137F1E 50DFD32E 1DC29CB7 95EF4096
421AF22F 5C1D5804 B83F8E8E 95B04F45 86563BFE DF976C5B FB490A
quit
!
!
no crypto isakmp enable
!
```

```

! Enable IPsec.
crypto isakmp policy 1
  authentication pre-share
  lifetime 28800
crypto isakmp key cisco123 address 10.1.1.13
! The crypto key should match the key configured on Cisco Unified Communications
Manager.
!
! The crypto IPsec configuration should match your Cisco Unified Communications
Manager configuration.

crypto ipsec transform-set rtpset esp-des esp-md5-hmac
!
!
crypto map rtp 1 ipsec-isakmp
  set peer 10.1.1.13
  set transform-set rtpset
  match address 116
!
!
interface FastEthernet0/0
  ip address 10.1.1.22 255.255.255.0
  duplex auto
  speed auto
  crypto map rtp
!
interface FastEthernet0/1
  no ip address
  shutdown
  duplex auto
  speed auto
!
ip classless
!
ip http server
no ip http secure-server
!
!
! Define traffic to be encrypted by IPsec.
access-list 116 permit ip host 10.1.1.22 host 10.1.1.13
!
!
control-plane
!
!
call application alternate DEFAULT
!
!
voice-port 1/0/0
!
voice-port 1/0/1
!
voice-port 1/0/2
!
voice-port 1/0/3
!
voice-port 1/1/0
  timing hookflash-out 50
!
voice-port 1/1/1
!
voice-port 1/1/2
!
voice-port 1/1/3
!
! Enable MGCP voice protocol.
mgcp
mgcp call-agent 10.1.1.13 2427 service-type mgcp version 0.1
mgcp dtmf-relay voip codec all mode out-of-band

```

```
mgcp rtp unreachable timeout 1000 action notify
mgcp package-capability rtp-package
mgcp package-capability sst-package
no mgcp package-capability fxr-package
no mgcp timer receive-rtcp
mgcp sdp simple
mgcp fax t38 inhibit
mgcp rtp payload-type g726r16 static
!
mgcp profile default
!
!
dial-peer voice 81235 pots
  application mgcpapp
  destination-pattern 81235
  port 1/1/0
  forward-digits all
!
dial-peer voice 81234 pots
  application mgcpapp
  destination-pattern 81234
  port 1/0/0
!
dial-peer voice 999100 pots
  application mgcpapp
  port 1/0/0
!
dial-peer voice 999110 pots
  application mgcpapp
  port 1/1/0
!
!
! Enable credentials service on the gateway.
credentials
  ip source-address 10.1.1.22 port 2445
  trustpoint srstca
!
!
! Enable SRST mode.
call-manager-fallback
  secondary-dialtone 9
  transfer-system full-consult
  ip source-address 10.1.1.22 port 2000
  max-ephones 15
  max-dn 30
  transfer-pattern .....
.
.
.
```

コントロールプレーンポリシング：例

ここでは、コントロールプレーンポリシングを使用してクレデンシャルサービスを保護するための、セキュリティ上の最善策の設定例を示します。コントロールプレーンポリシングは、ゲートウェイを保護し、トラフィックの負荷が大きいたともパケットの転送とプロトコルの状態を維持します。コントロールプレーンの詳細については、『[Control Plane Policing](#)』を参照してください。

```
Router# show running-config
.
.
.
! Allow trusted host traffic.
access-list 140 deny tcp host 10.1.1.11 any eq 2445

! Rate-limit all other traffic.
access-list 140 permit tcp any any eq 2445
access-list 140 deny ip any any

! Define class-map "sccp-class."
class-map match-all sccp-class
match access-group 140

policy-map control-plane-policy
class sccp-class
police 8000 1500 1500 conform-action drop exceed-action drop

! Define aggregate control plane service for the active Route Processor.
control-plane
service-policy input control-plane-policy
.
.
.
```

関連情報

ボイスメールが必要な場合、ボイスメールの設定方法について、[P.193](#)の「[Cisco Unified SRST へのボイスメールの統合](#)」を参照してください。[P.227](#)の「[Cisco Unified SRST の監視と保守](#)」も参照してください。

追加情報については、[P.25](#)の「[Cisco Unified SRST の概要](#)」の [P.40](#)の「[その他の資料](#)」を参照してください。